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/

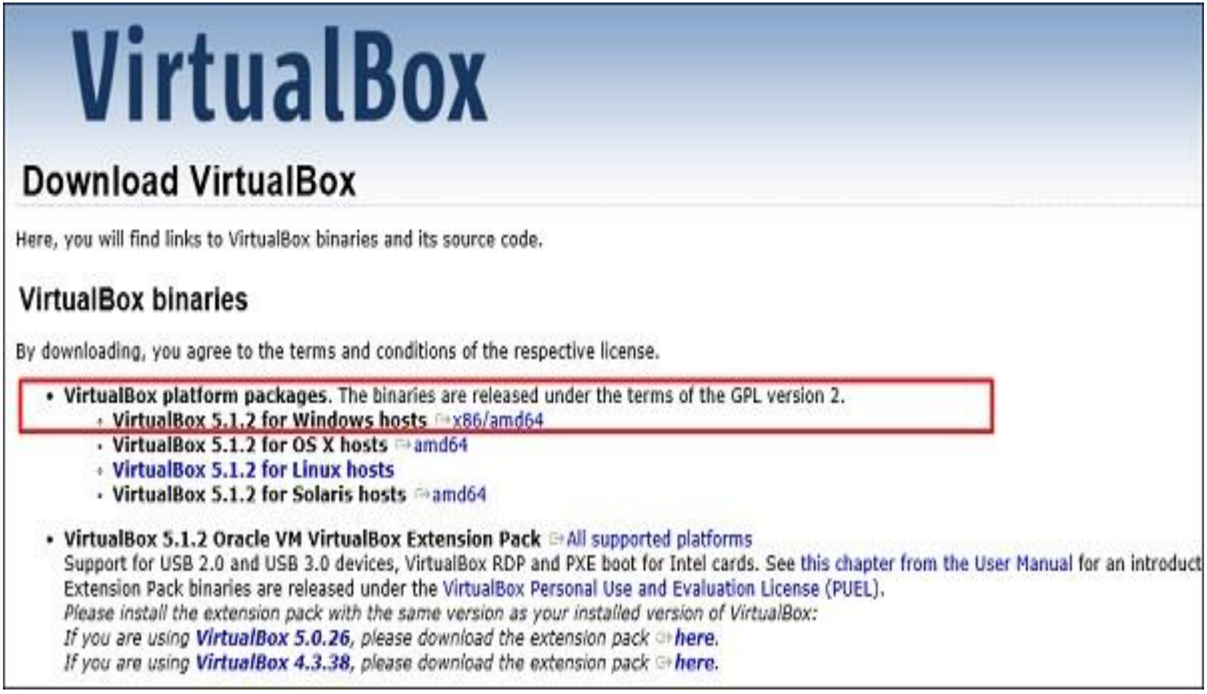
Download and Install the Virtual Box

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.



VirtualBox

Download VirtualBox

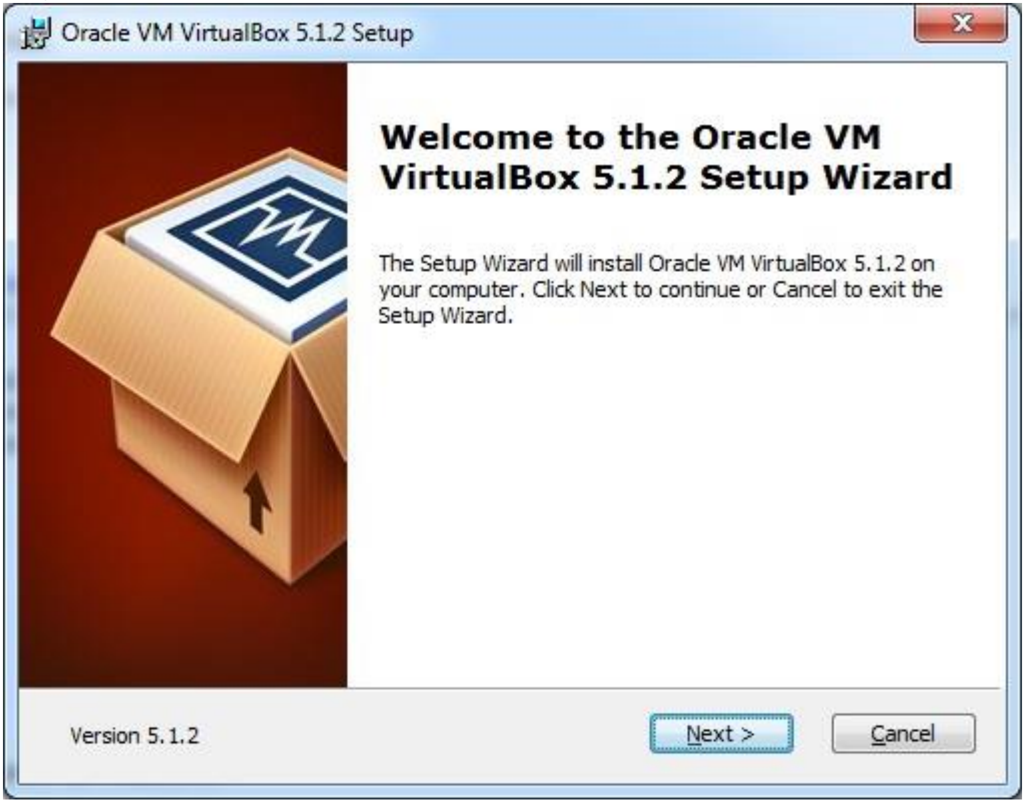
Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
    - **VirtualBox 5.1.2 for Windows hosts** x86/amd64
    - **VirtualBox 5.1.2 for OS X hosts** amd64
    - **VirtualBox 5.1.2 for Linux hosts**
    - **VirtualBox 5.1.2 for Solaris hosts** amd64
- **VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack** All supported platforms
  Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP and PXE boot for Intel cards. See this chapter from the User Manual for an introduct
  Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL).
  Please install the extension pack with the same version as your installed version of VirtualBox:
  *If you are using **VirtualBox 5.0.26**, please download the extension pack **here**.*
  *If you are using **VirtualBox 4.3.38**, please download the extension pack **here**.*

Step 2 – Click **Next**.



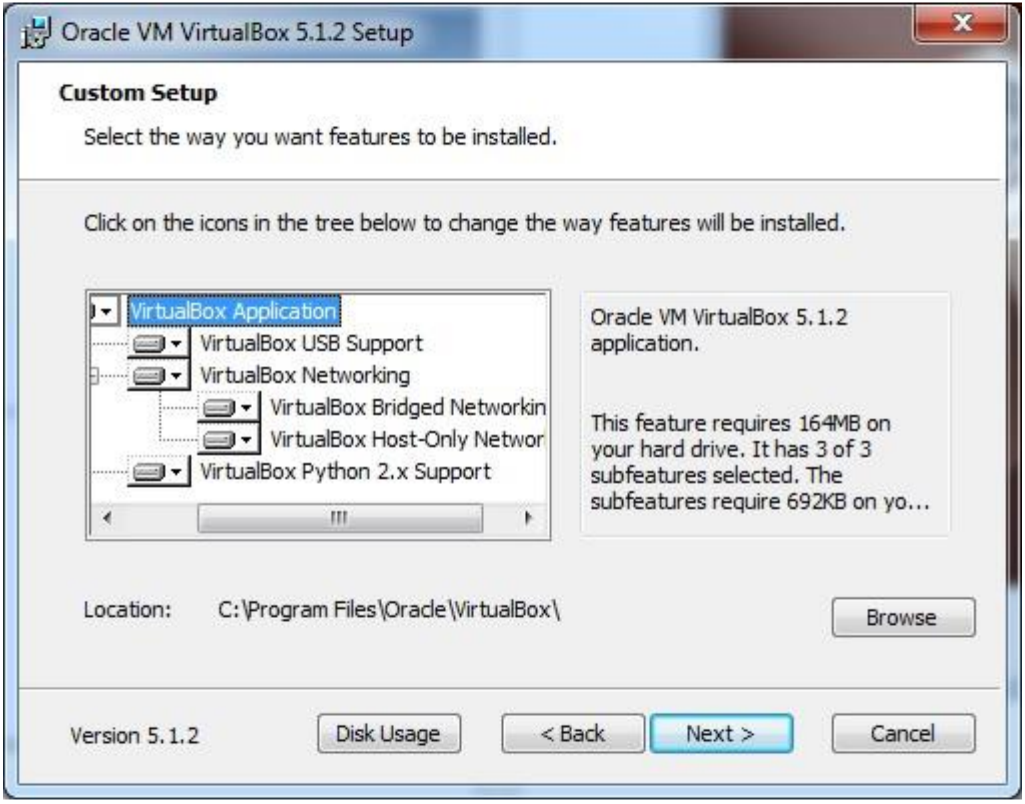
Oracle VM VirtualBox 5.1.2 Setup

Welcome to the Oracle VM VirtualBox 5.1.2 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 5.1.2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Version 5.1.2

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**.



Oracle VM VirtualBox 5.1.2 Setup

Custom Setup

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

- VirtualBox Application
  - VirtualBox USB Support
  - VirtualBox Networking
    - VirtualBox Bridged Networkin
    - VirtualBox Host-Only Networ
  - VirtualBox Python 2.x Support

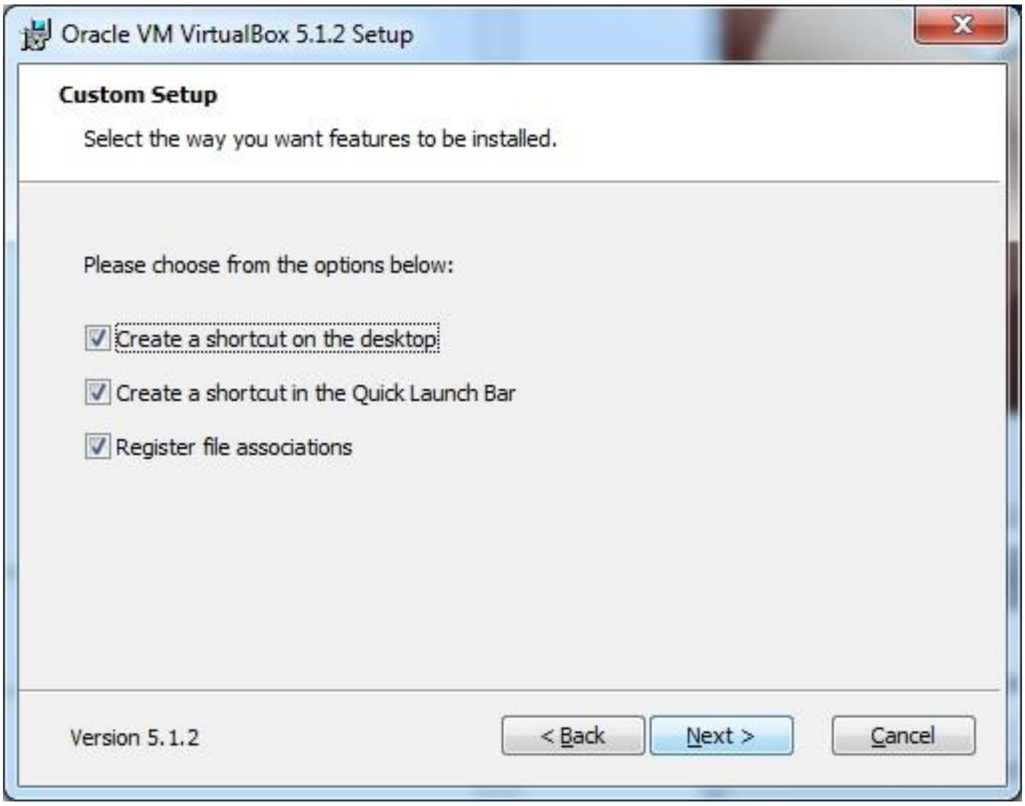
Oracle VM VirtualBox 5.1.2 application.

This feature requires 164MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 692KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

Version 5.1.2

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



Oracle VM VirtualBox 5.1.2 Setup

Custom Setup

Select the way you want features to be installed.

Please choose from the options below:

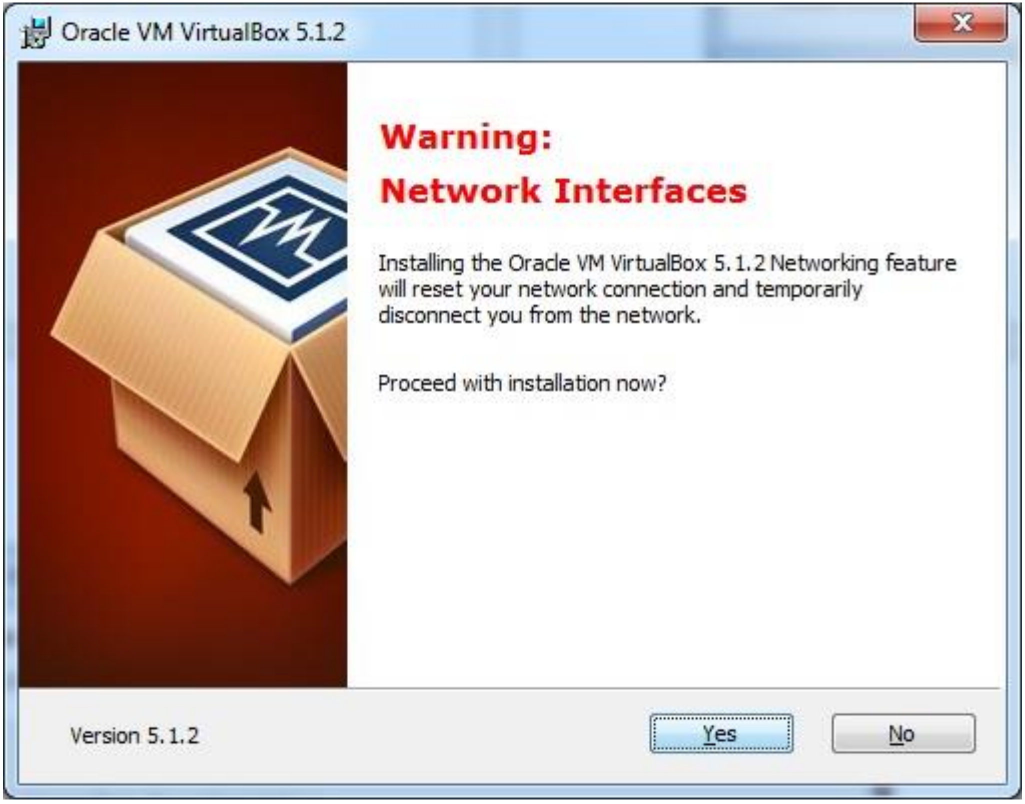
☑ Create a shortcut on the desktop

☑ Create a shortcut in the Quick Launch Bar

☑ Register file associations

Version 5.1.2

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



Oracle VM VirtualBox 5.1.2

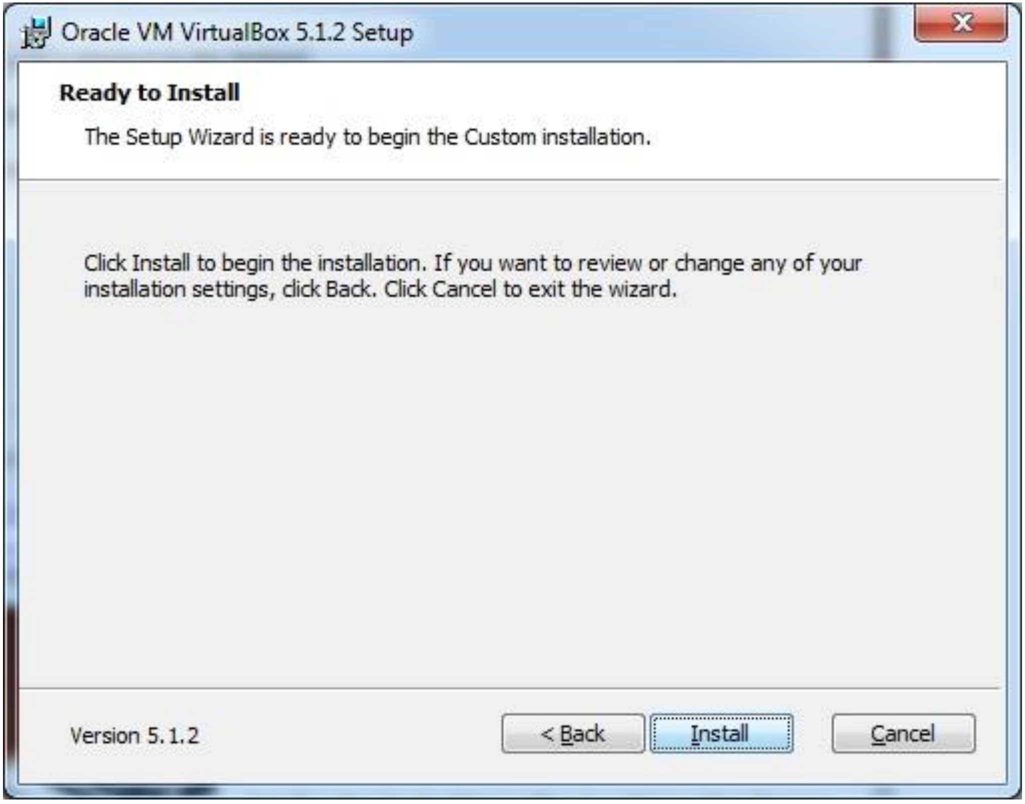
Warning:
Network Interfaces

Installing the Oracle VM VirtualBox 5.1.2 Networking feature will reset your network connection and temporarily disconnect you from the network.

Proceed with installation now?

Version 5.1.2

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



Oracle VM VirtualBox 5.1.2 Setup

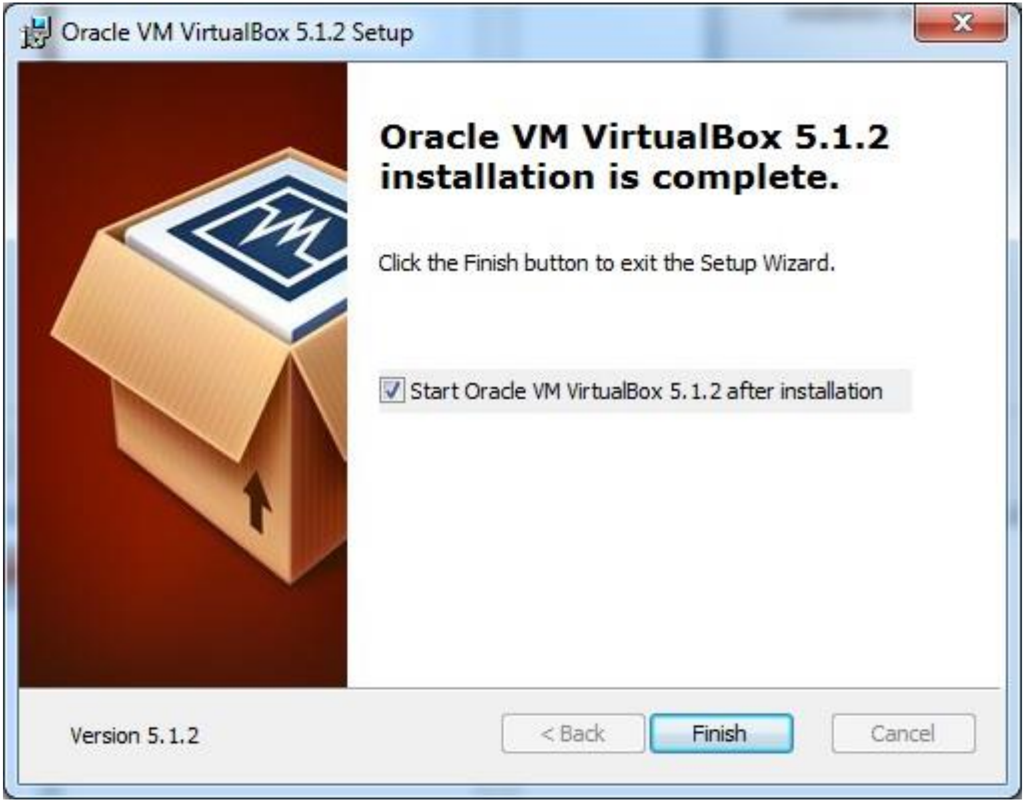
Ready to Install

The Setup Wizard is ready to begin the Custom installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Version 5.1.2

Step 7 – Click the **Finish** button.



Oracle VM VirtualBox 5.1.2 Setup

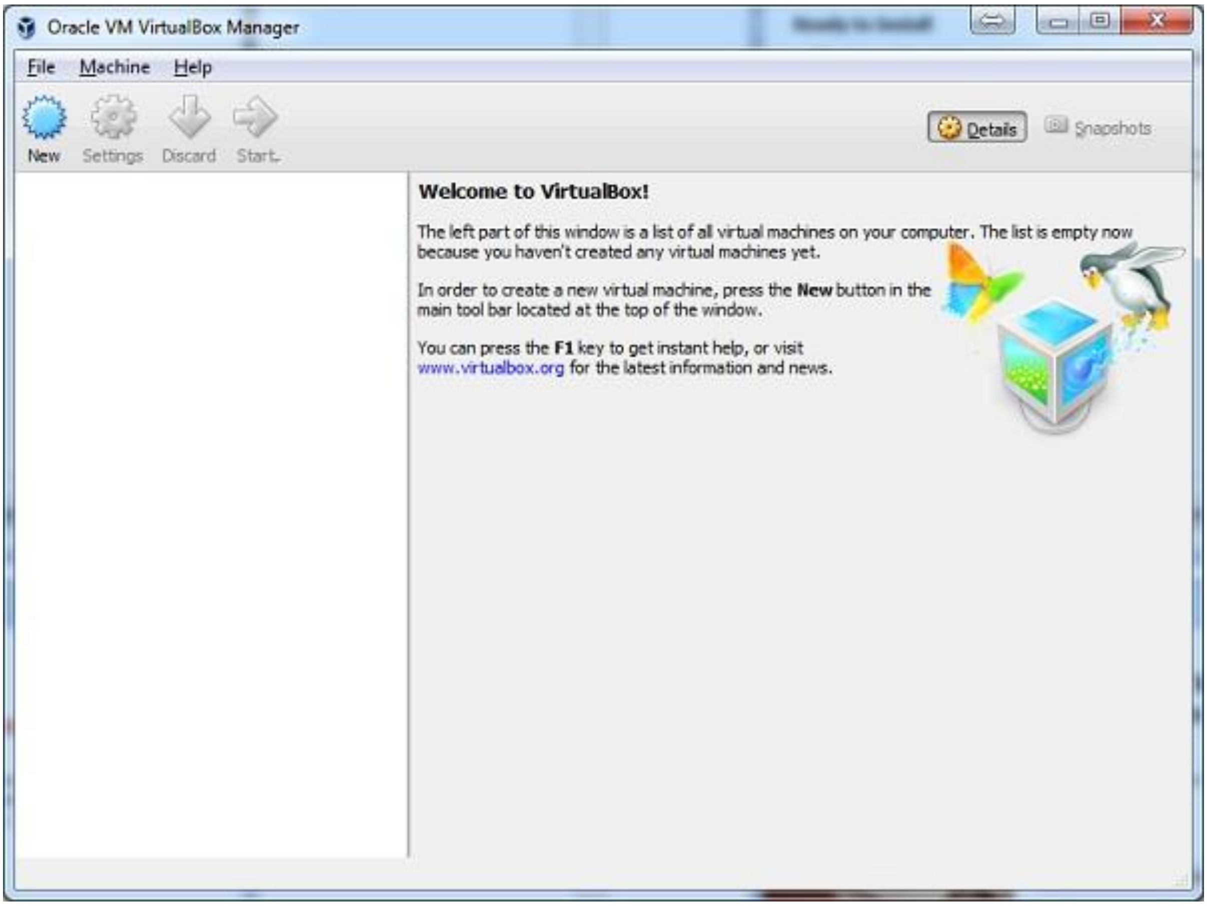
Oracle VM VirtualBox 5.1.2 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 5.1.2 after installation

Version 5.1.2

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.



Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

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/

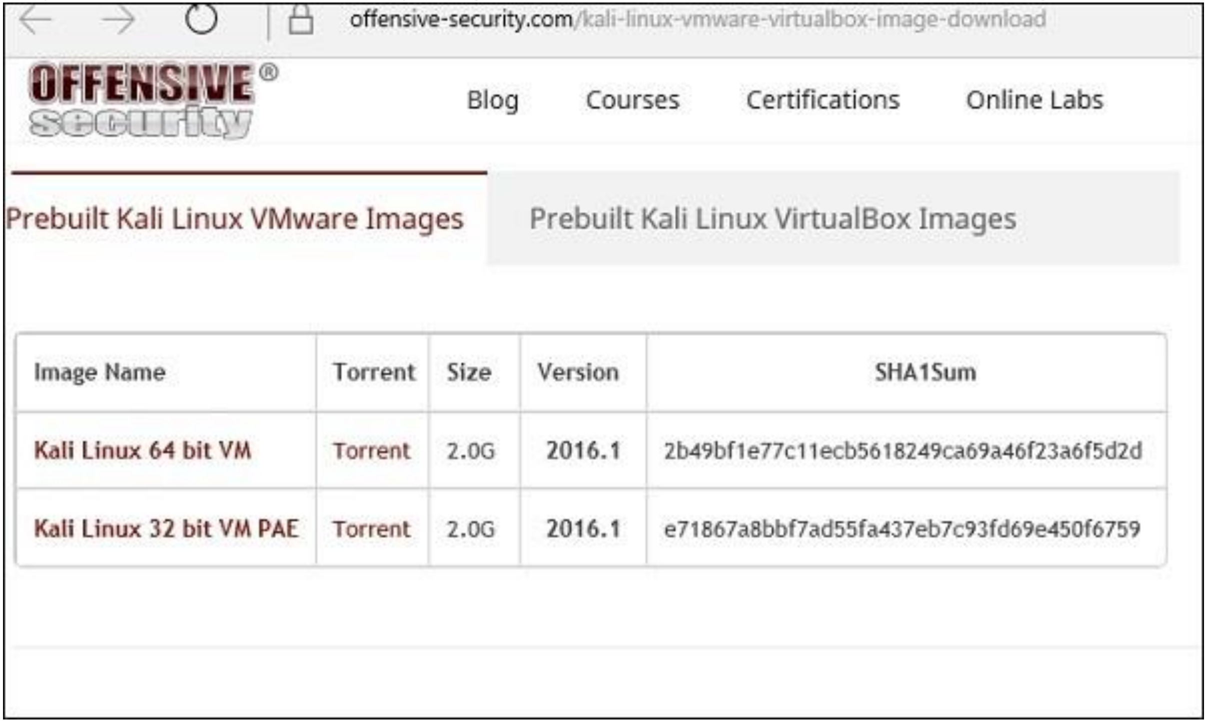
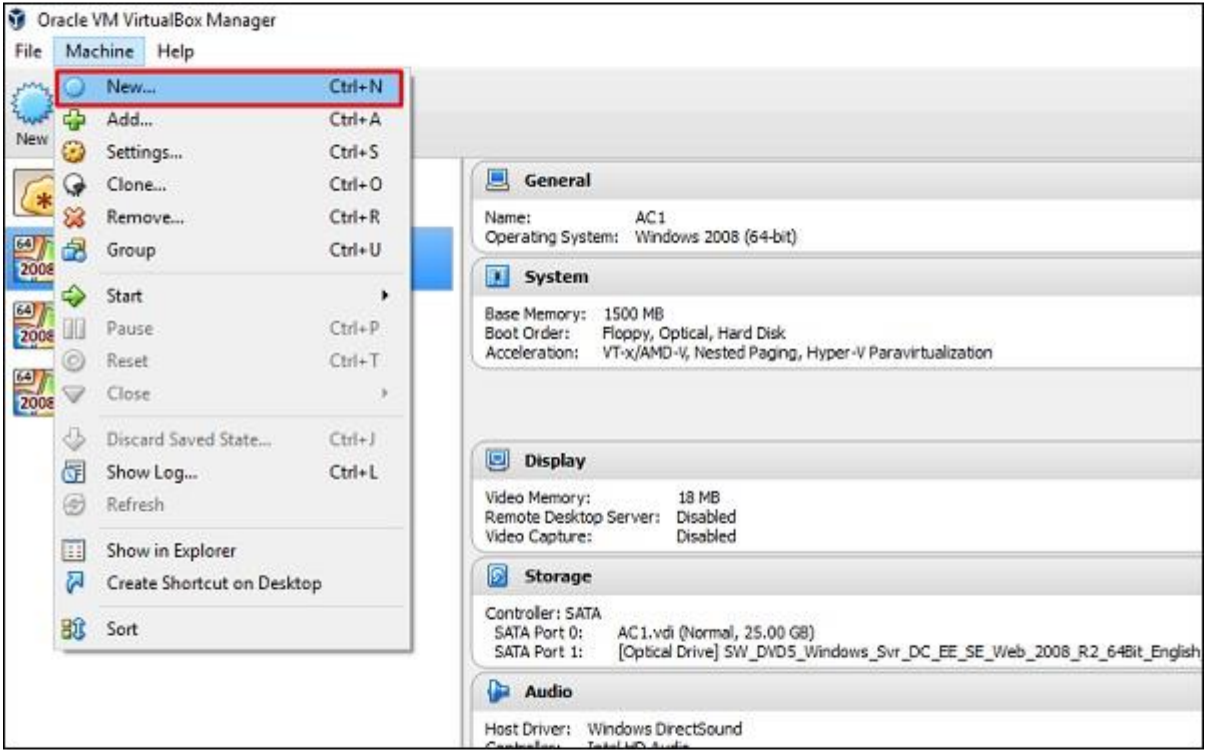

offensive-security.com/kali-linux-vmware-virtualbox-image-download
OFFENSIVE security
Blog Courses Certifications Online Labs
Prebuilt Kali Linux VMware Images
Prebuilt Kali Linux VirtualBox Images

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

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



General
Name: AC1
Operating System: Windows 2008 (64-bit)

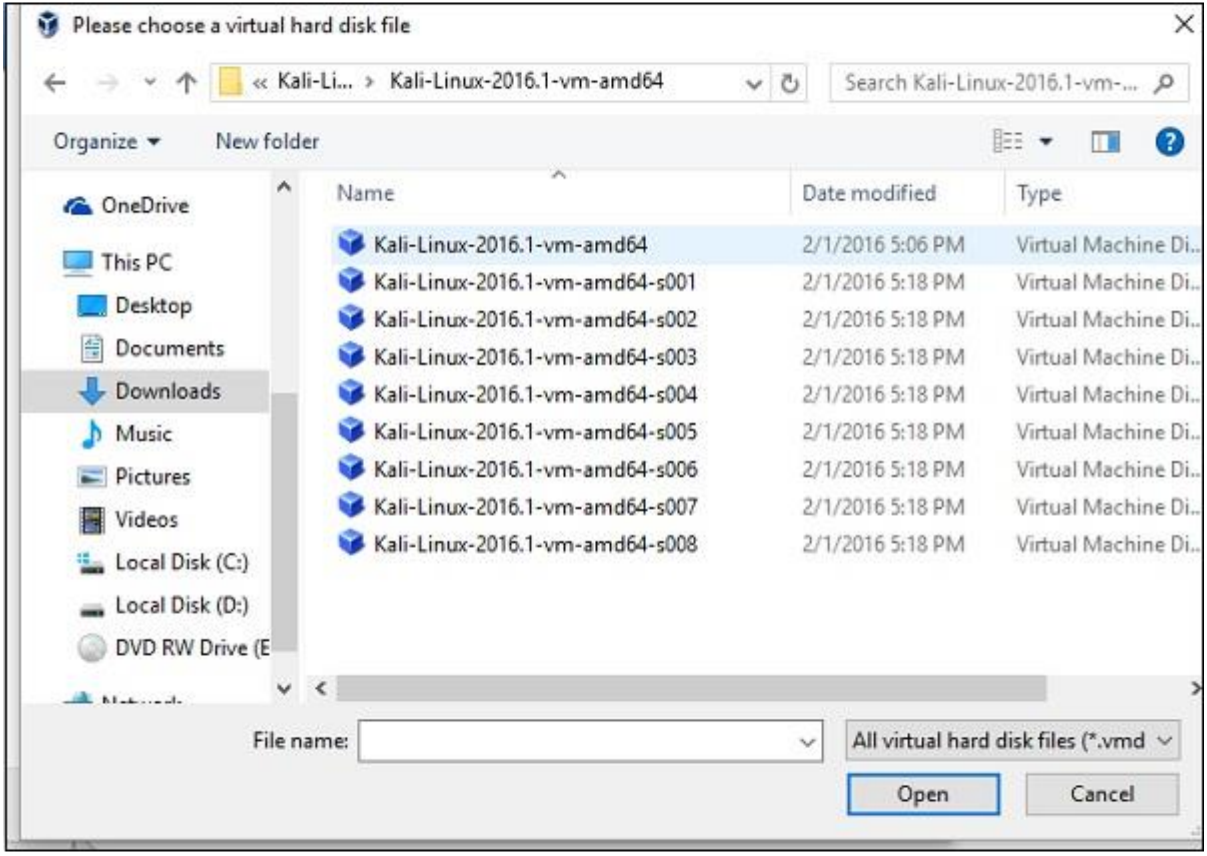
System
Base Memory: 1500 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 18 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: SATA
SATA Port 0: AC1.vdi (Normal, 25.00 GB)
SATA Port 1: [Optical Drive] SW_DVD5_Windows_Svr_DC_EE_SE_Web_2008_R2_64Bit_English

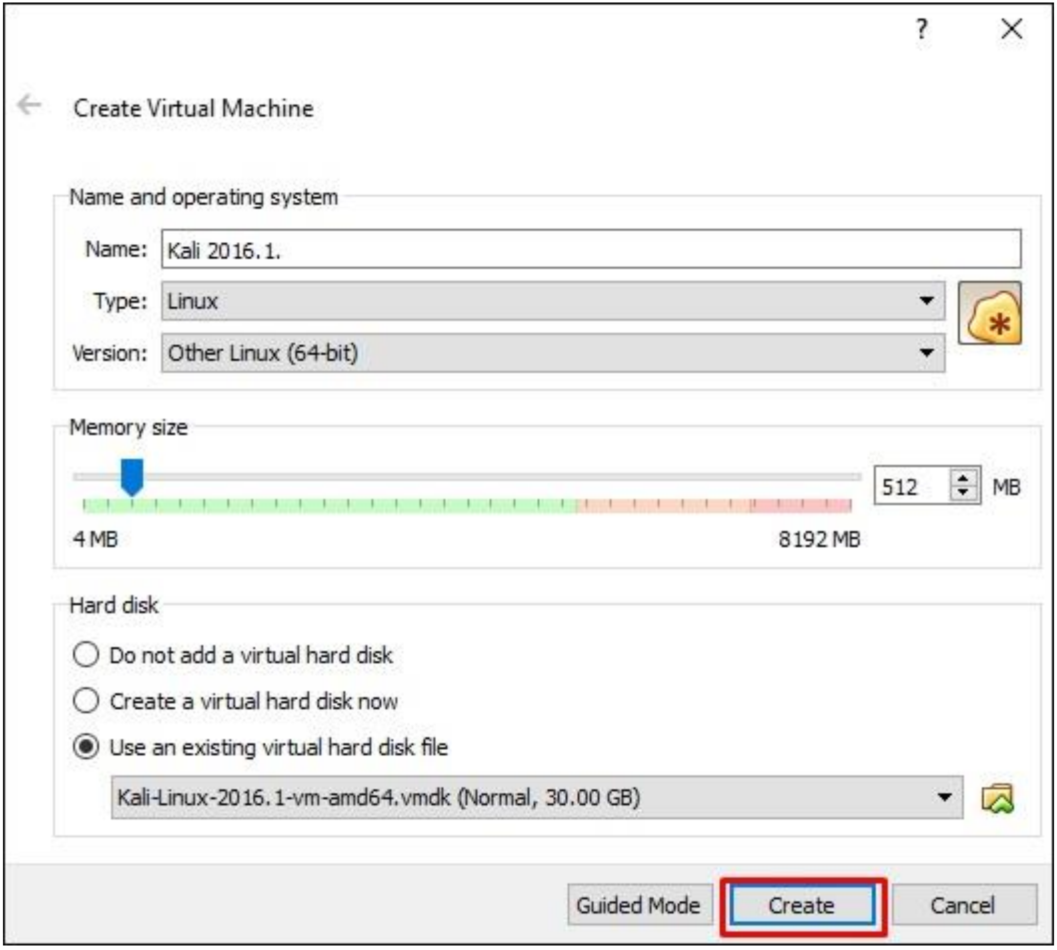
Audio
Host Driver: Windows DirectSound

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



Name	Date modified	Type
Kali-Linux-2016.1-vm-amd64	2/1/2016 5:06 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s001	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s002	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s003	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s004	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s005	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s006	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s007	2/1/2016 5:18 PM	Virtual Machine Di...
Kali-Linux-2016.1-vm-amd64-s008	2/1/2016 5:18 PM	Virtual Machine Di...

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



Create Virtual Machine

Name and operating system

Name: Kali 2016.1.

Type: Linux

Version: Other Linux (64-bit)

Memory size

512 MB

Hard disk

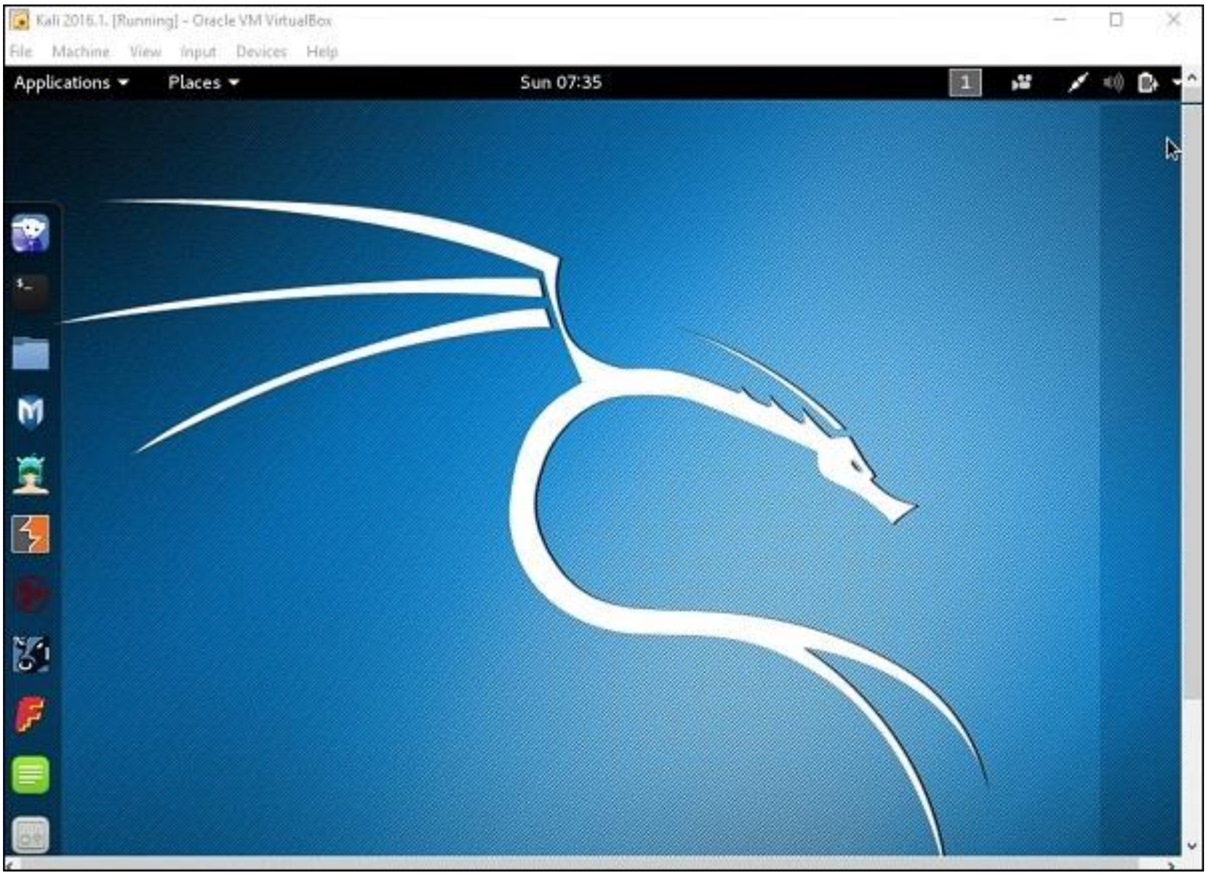
○ Do not add a virtual hard disk

○ Create a virtual hard disk now

● Use an existing virtual hard disk file

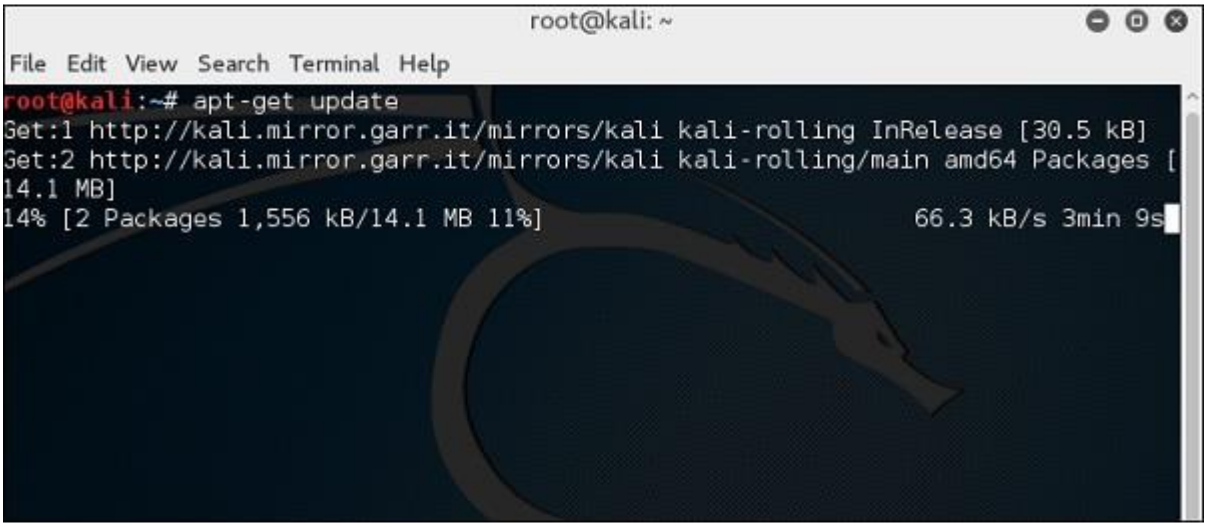
Kali-Linux-2016.1-vm-amd64.vmdk (Normal, 30.00 GB)

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

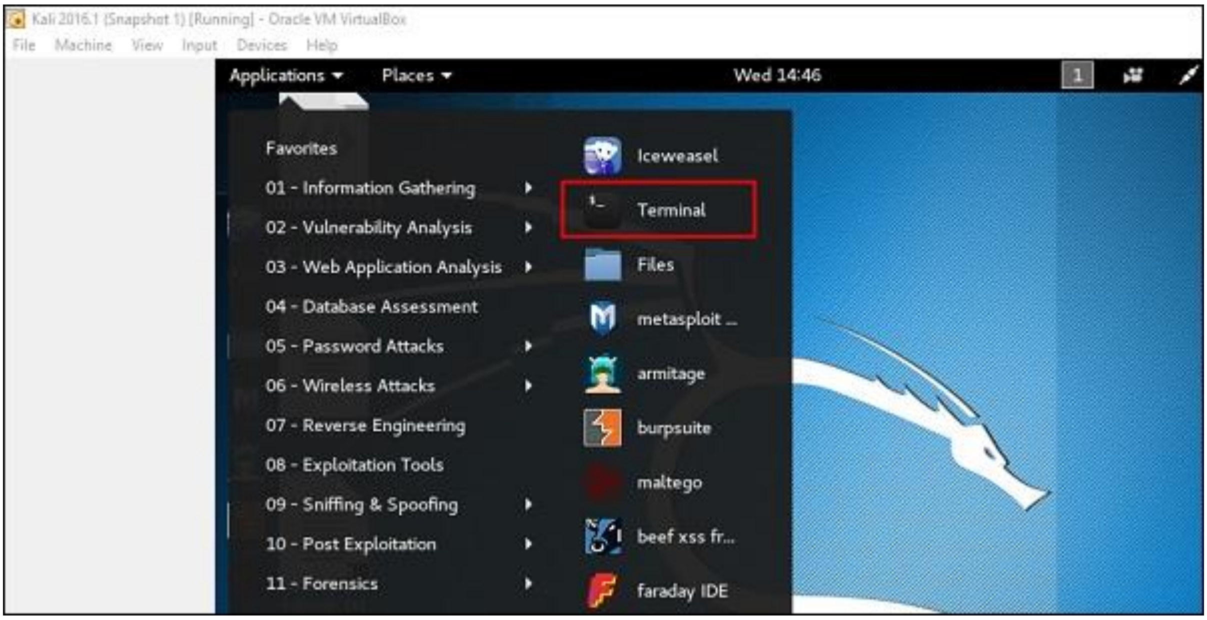

Kali 2016.1. [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Sun 07:35

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

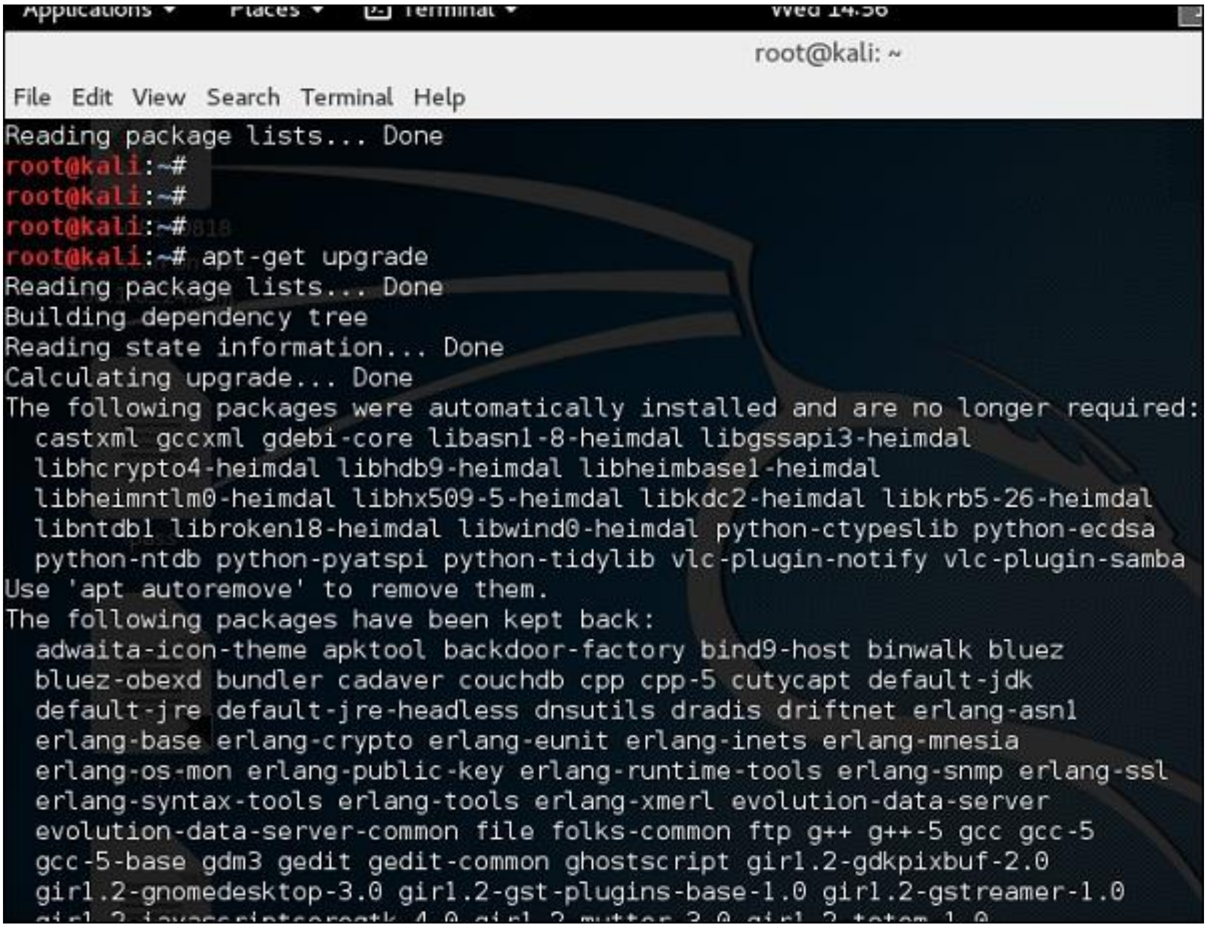
Step 1 – Go to Application → Terminal. Then, type "apt-get update" and the update will take place as shown in the following screenshot.



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

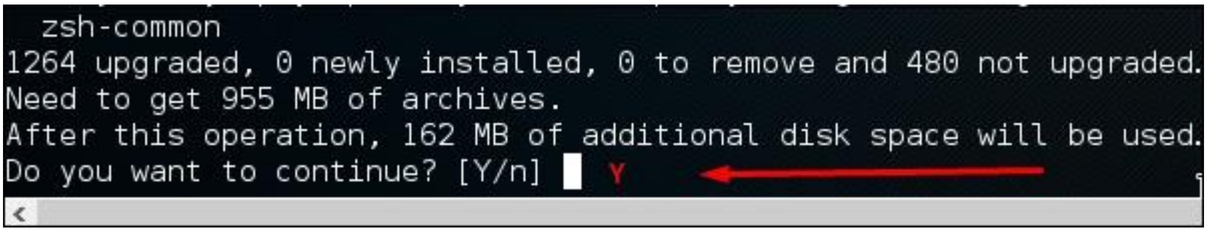


Step 2 – Now to upgrade the tools, type “apt-get upgrade” and the new packages will be downloaded.


Applications ▾ Places ▾ Terminal ▾
Wed 14:56
root@kali: ~
File Edit View Search Terminal Help

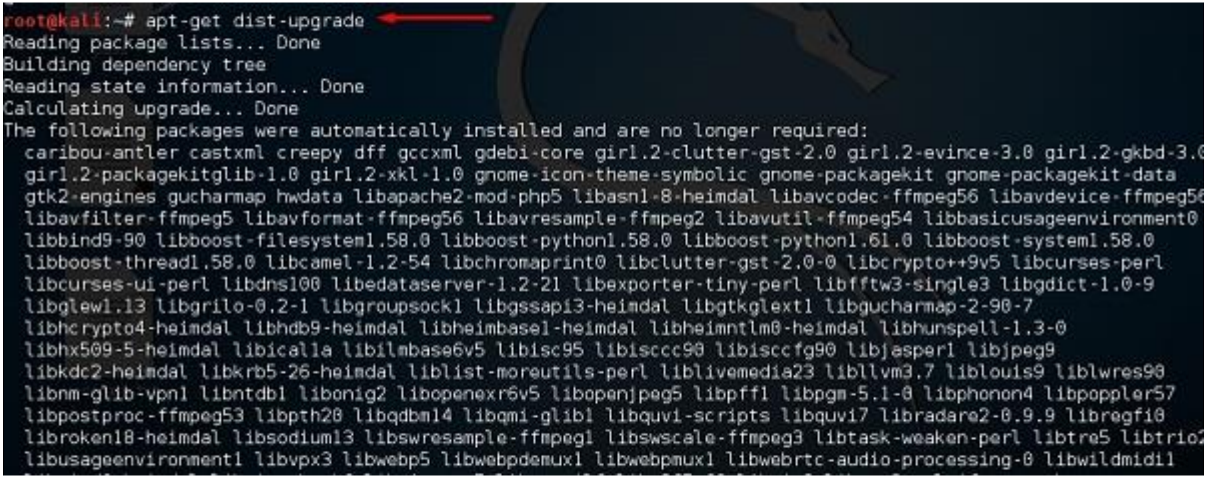
```
Reading package lists... Done
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  castxml gccxml gdebi-core libasn1-8-heimdal libgssapi3-heimdal
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhx509-5-heimdal libkdc2-heimdal libkrb5-26-heimdal
  libntdb1 libroken18-heimdal libwind0-heimdal python-ctypeslib python-ecdsa
  python-ntdb python-pyatspi python-tidylib vlc-plugin-notify vlc-plugin-samba
Use 'apt autoremove' to remove them.
The following packages have been kept back:
  adwaita-icon-theme apktool backdoor-factory bind9-host binwalk bluez
  bluez-obexd bundler cadaver couchdb cpp cpp-5 cutycapt default-jdk
  default-jre default-jre-headless dnsutils dradis driftnet erlang-asn1
  erlang-base erlang-crypto erlang-eunit erlang-inets erlang-mnesia
  erlang-os-mon erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl evolution-data-server
  evolution-data-server-common file folks-common ftp g++ g++-5 gcc gcc-5
  gcc-5-base gdm3 gedit gedit-common ghostscript gir1.2-gdkpixbuf-2.0
  gir1.2-gnomedesktop-3.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
  gir1.2-javascriptcoregtk-4.0 gir1.2-mutter-3.0 gir1.2-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 480 not upgraded.
Need to get 955 MB of archives.
After this operation, 162 MB of additional disk space will be used.
Do you want to continue? [Y/n] █ Y
```

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



```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  caribou-antler castxml creepy dff gccxml gdebi-core gir1.2-clutter-gst-2.0 gir1.2-evince-3.0 gir1.2-gkbd-3.0
  gir1.2-packagekitglib-1.0 gir1.2-xkl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
  gtk2-engines gucharmap hwdata libapache2-mod-php5 libasn1-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56
  libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
  libbind9-90 libboost-filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.0 libboost-system1.58.0
  libboost-thread1.58.0 libcamel-1.2-54 libchromaprint0 libclutter-gst-2.0-0 libcrypto++9v5 libcurses-perl
  libcurses-ui-perl libdns100 libedataserver-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 libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
  libhx509-5-heimdal libicall1a libilmbase6v5 libisc95 libisccc90 libisccfg90 libjasper1 libjpeg9
  libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 libllvm3.7 liblouis9 liblwres90
  libnm-glib-vpn1 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-0 libphonon4 libpoppler57
  libpostproc-ffmpeg53 libpth20 libqdbm14 libqmi-glib1 libquvi-scripts libquvi7 libradare2-0.9.9 libregfi0
  libroken18-heimdal libsodium13 libswresample-ffmpeg1 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtrio2
  libusageenvironment1 libvpx3 libwebp5 libwebpdemux1 libwebpmux1 libwebrtc-audio-processing-0 libwildmidi1
```

Kali Linux-Information Gathering Tools

Information Gathering means gathering different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) tries to gather all the information about the target, in order to use it for Hacking. To obtain more relevant results, we have to gather more information about the target to increase the probability of a successful attack.

Information gathering is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing. It is a method used by analysts to determine the needs of customers and users. Techniques that provide safety, utility, usability, learnability, etc. for collaborators result in their collaboration, commitment, and honesty. Various tools and techniques are available, including public sources such as Whois, nslookup which can help hackers to gather user information. This step is very important because while performing attacks on any target information (such as his pet name, best friend’s name, age, or phone number to perform password guessing attacks(brute force) or other kinds of attacks) are required.
Information gathering can be classified into the following categories:

- Footprinting
- Scanning
- Enumeration
- Reconnaissance

1. Nmap Tool

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It could even be used for host discovery, operating system detection, or scanning for open ports. It is one of the most popular reconnaissance tools.

To use nmap:

- Ping the host with the ping command to get the IP address

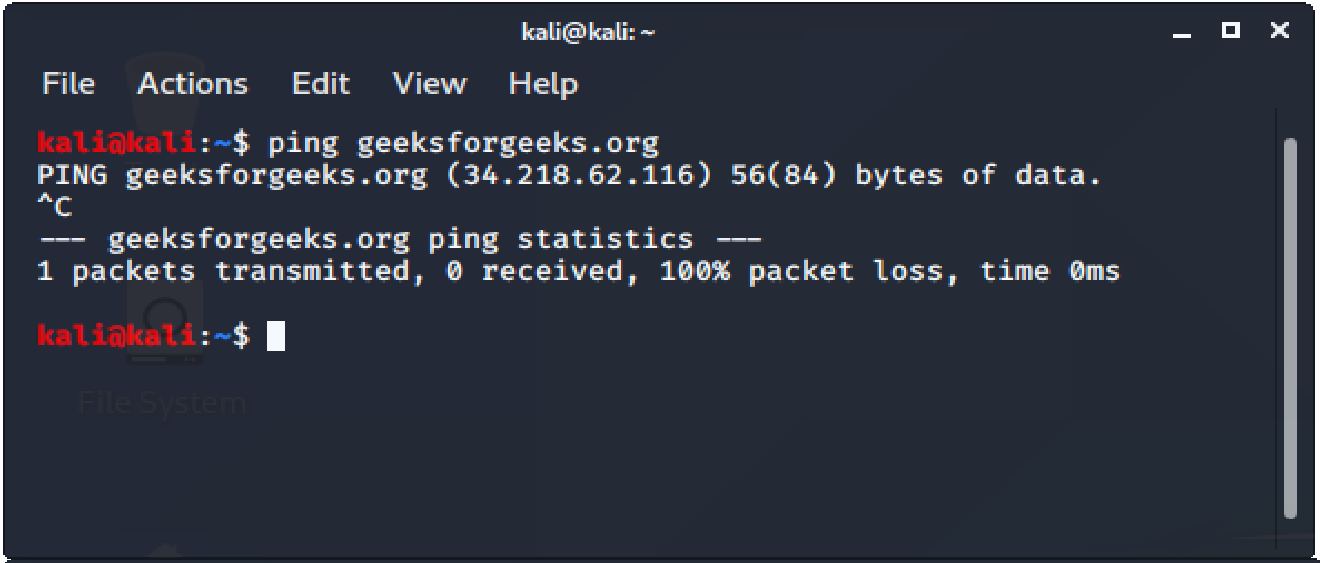
ping hostname

- Open the terminal and enter the following command there.

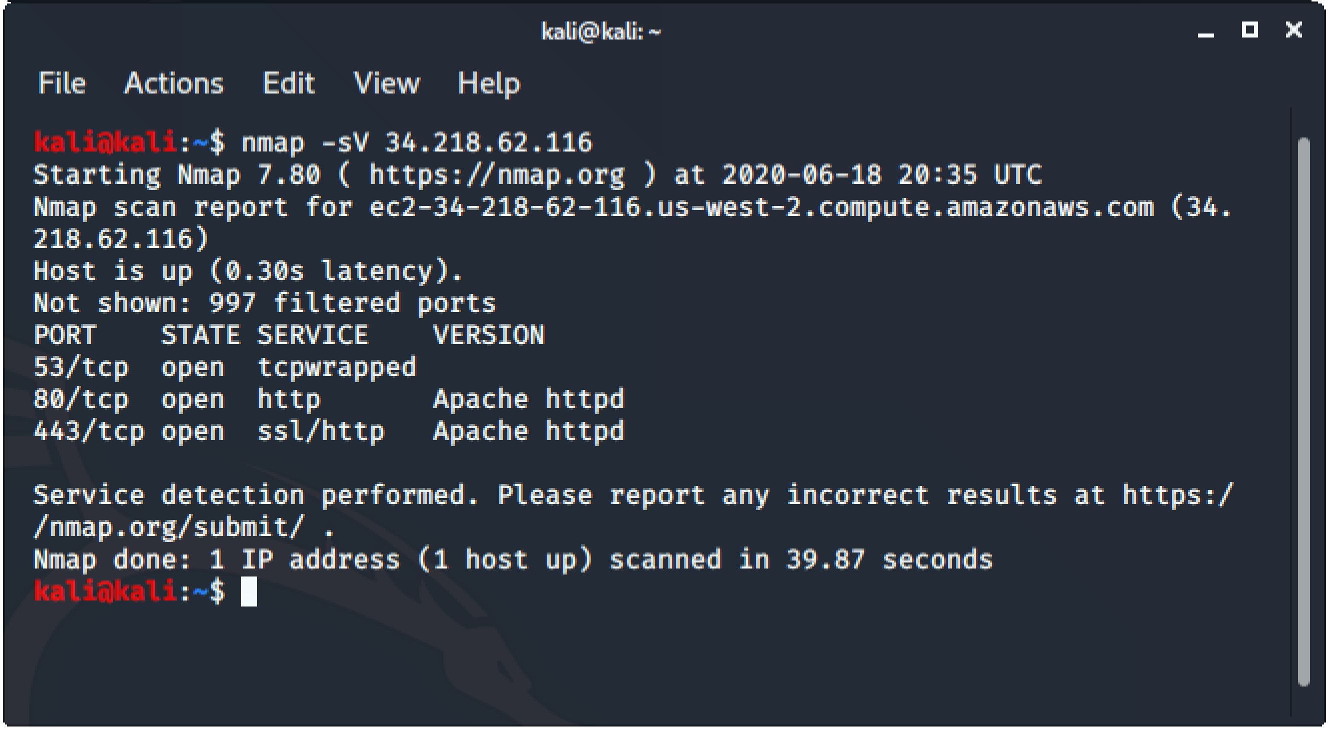
nmap -sV ipaddress

Replace the IP address with the IP address of the host you want to scan.

- It will display all the captured details of the host.



```
kali@kali:~$ ping geeksforgeeks.org
PING geeksforgeeks.org (34.218.62.116) 56(84) bytes of data.
^C
--- geeksforgeeks.org ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

kali@kali:~$ 
```

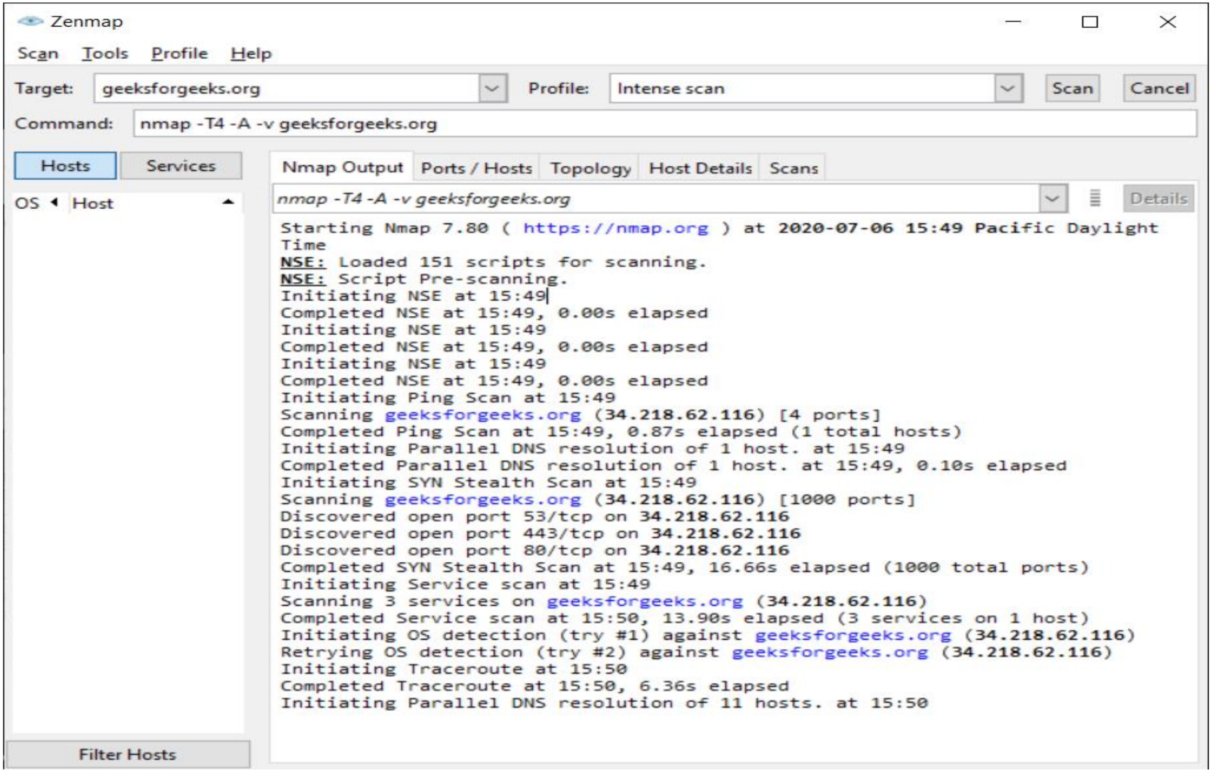


```
kali@kali:~$ nmap -sV 34.218.62.116
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-18 20:35 UTC
Nmap scan report for ec2-34-218-62-116.us-west-2.compute.amazonaws.com (34.
218.62.116)
Host is up (0.30s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
80/tcp  open  http       Apache httpd
443/tcp open  ssl/http   Apache httpd

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.87 seconds
kali@kali:~$ 
```

ZenMAP

It is another useful tool for the scanning phase of Ethical Hacking in Kali Linux. It uses the Graphical User Interface. It is a great tool for network discovery and security auditing. It does the same functions as that of the Nmap tool or in other words, it is the graphical Interface version of the Nmap tool. It uses command line Interface. It is a free utility tool for network discovery and security auditing. Tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime are considered really useful by systems and network administrators.

To use Zenmap, enter the target URL in the target field to scan the target.



Target: geeksforgeeks.org
Profile: Intense scan
Command: nmap -T4 -A -v geeksforgeeks.org

```
nmap -T4 -A -v geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 15:49 Pacific Daylight
Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating Ping Scan at 15:49
Scanning geeksforgeeks.org (34.218.62.116) [4 ports]
Completed Ping Scan at 15:49, 0.87s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:49
Completed Parallel DNS resolution of 1 host. at 15:49, 0.10s elapsed
Initiating SYN Stealth Scan at 15:49
Scanning geeksforgeeks.org (34.218.62.116) [1000 ports]
Discovered open port 53/tcp on 34.218.62.116
Discovered open port 443/tcp on 34.218.62.116
Discovered open port 80/tcp on 34.218.62.116
Completed SYN Stealth Scan at 15:49, 16.66s elapsed (1000 total ports)
Initiating Service scan at 15:49
Scanning 3 services on geeksforgeeks.org (34.218.62.116)
Completed Service scan at 15:50, 13.90s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against geeksforgeeks.org (34.218.62.116)
Retrying OS detection (try #2) against geeksforgeeks.org (34.218.62.116)
Initiating Traceroute at 15:50
Completed Traceroute at 15:50, 6.36s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 15:50
```

3. whois lookup

whois is a database record of all the registered domains over the internet. It is used for many purposes, a few of them are listed below.

- It is used by Network Administrators in order to identify and fix DNS or domain-related issues.
- It is used to check the availability of domain names.
- It is used to identify trademark infringement.
- It could even be used to track down the registrants of the Fraud domain.

To use whois lookup, enter the following command in the terminal

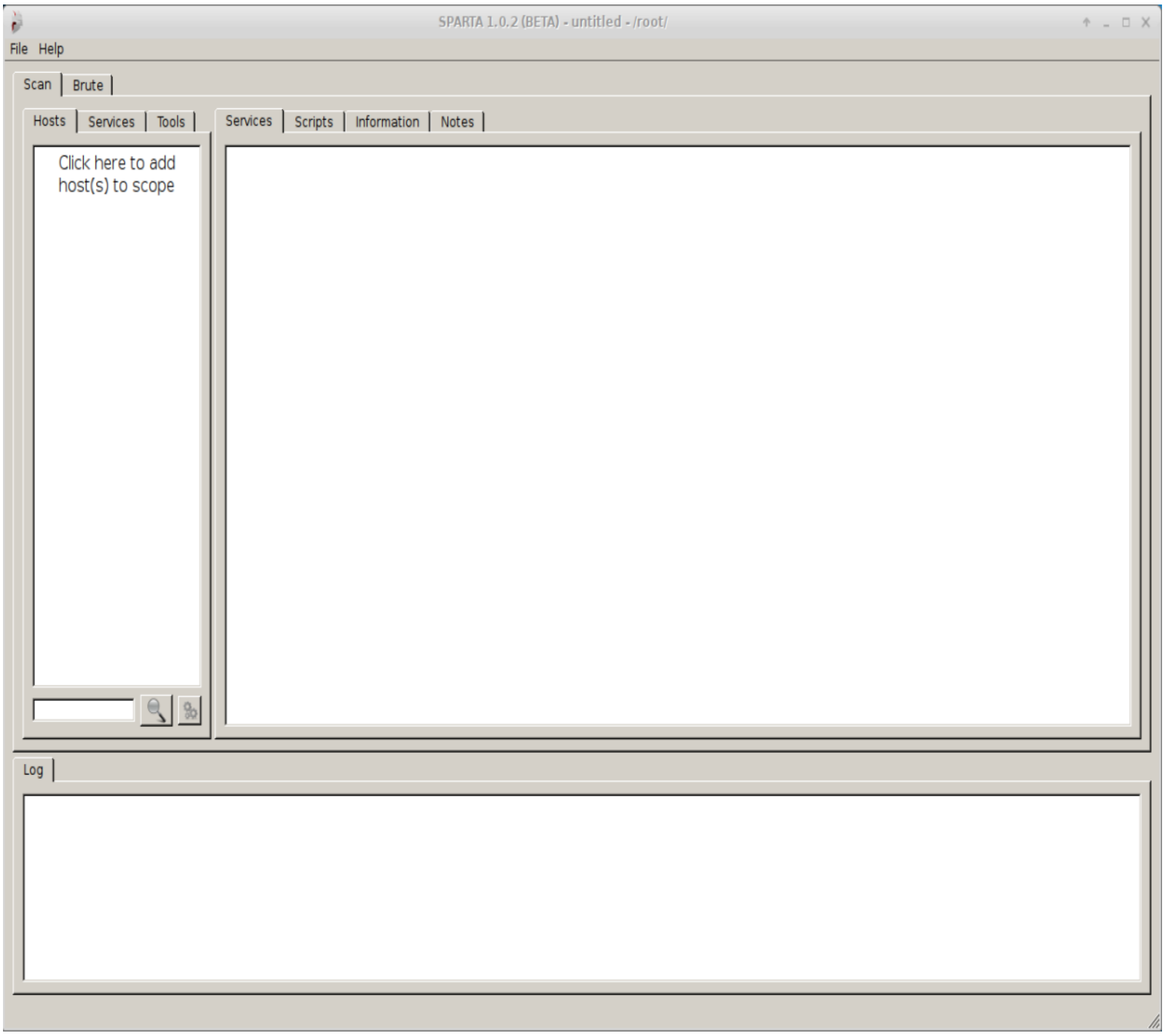
```
EX--   whois paruluniversity.ac.in
```

4. SPARTA

SPARTA is a python based Graphical User Interface tool which is used in the scanning and enumeration phase of information gathering. It is a toolkit having a collection of some useful tools for information gathering. It is used for many purposes, a few of them are listed below.

- It is used to export Nmap output to an XML file.
- It is used to automate the process of Nikto tool to every HTTP service or any other service.
- It is used to save the scan of the hosts you have scanned earlier in order to save time.
- It is used to reuse the password which is already found and is not present in the wordlist.

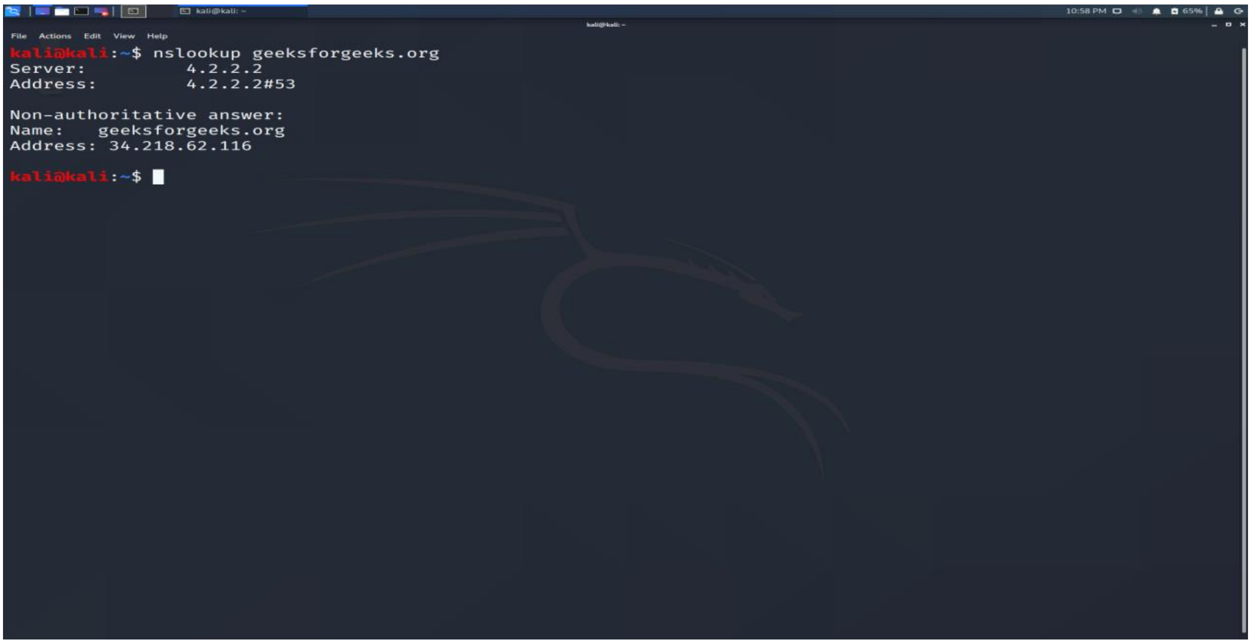
To use SPARTA, enter the IP address of the host you want to scan in the host section to start scanning.


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

5. nslookup

nslookup stands for nameserver lookup, which is a command used to get the information from the DNS server. It queries DNS to obtain a domain name, IP address mapping, or any other DNS record. It even helps in troubleshooting DNS-related problems. It is used for many purposes, a few of them are listed below.

- To get the IP address of a domain.
- For reverse DNS lookup
- For lookup for any record
- Lookup for an SOA record
- Lookup for an ns record
- Lookup for an MX record
- Lookup for a txt record

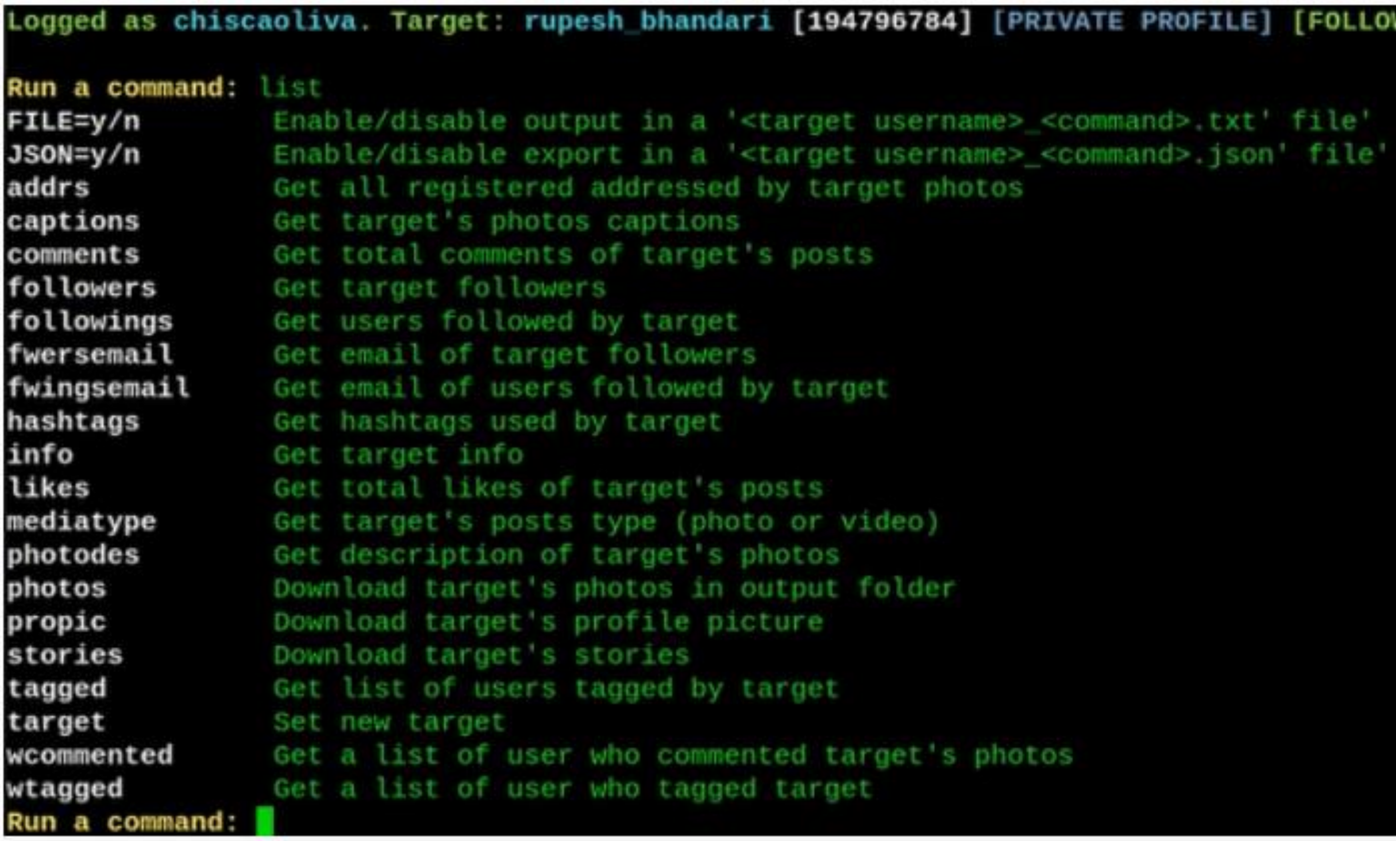


```
kali@kali:~$ nslookup geeksforgeeks.org
Server:         4.2.2.2
Address:        4.2.2.2#53

Non-authoritative answer:
Name:   geeksforgeeks.org
Address: 34.218.62.116

kali@kali:~$ 
```

6. Osintgram

Osintgram is an OSINT tool to run on reconnaissance Instagram to collect and analyze. It offers an interactive shell to perform analysis on account of any users by its nickname. One can get:

- – addrs : It gets all registered addressed by target photos.
- – captions : It gets the user’s photos captions.
- – comments : It gets total comments of the target’s posts.
- – followers : It gets target followers.
- – followings : It gets users followed by the target.
- – fwersemail : It gets emails of target followers.
- – fwingsemail : It gets an email of users followed by the target.
- – fwersnumber : It gets the phone number of target followers.
- – fwingsnumber : It gets the phone number of users followed by the target.
- – hashtags : It gets hashtags used by the target.



```
Logged as chiscaoliva. Target: rupesh_bhandari [194796784] [PRIVATE PROFILE] [FOLLO

Run a command: list
FILE=y/n        Enable/disable output in a '<target username>_<command>.txt' file'
JSON=y/n        Enable/disable export in a '<target username>_<command>.json' file'
addrs           Get all registered addressed by target photos
captions        Get target's photos captions
comments        Get total comments of target's posts
followers       Get target followers
followings      Get users followed by target
fwersemail      Get email of target followers
fwingsemail     Get email of users followed by target
hashtags        Get hashtags used by target
info            Get target info
likes           Get total likes of target's posts
mediatype       Get target's posts type (photo or video)
photodes        Get description of target's photos
photos          Download target's photos in output folder
propic          Download target's profile picture
stories         Download target's stories
tagged          Get list of users tagged by target
target          Set new target
wcommented      Get a list of user who commented target's photos
wtagged         Get a list of user who tagged target
Run a command:
```

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It is widely utilized by network administrators and security professionals to map out networks, manage network inventory, and detect devices, services, operating systems, and potential security vulnerabilities.

Key Features of Nmap

1. **Network Scanning**:
   - Nmap can scan large networks, discovering hosts and services available on those networks. This helps in identifying active devices and the open ports on them.
2. **Port Scanning**:
   - Nmap identifies open, closed, and filtered ports on a target machine. This is crucial for detecting available services and assessing potential security risks.
3. **Service Detection**:
   - Nmap can determine the version of the services running on a machine, providing insights into potential vulnerabilities based on outdated or insecure software versions.
4. **Operating System Detection**:
   - Nmap can guess the operating system running on a target machine by analyzing TCP/IP stack responses.
5. **Scripting Engine (NSE)**:
   - Nmap includes a scripting engine that allows for the automation of a wide variety of tasks. This can include vulnerability detection, network discovery, and more.
6. **Flexible Output**:

- Nmap supports multiple output formats such as plain text, XML, and a grepable format for easy parsing and analysis.

Common Use Cases

1. **Network Inventory**:
    - Administrators use Nmap to maintain an up-to-date inventory of devices and services in their network.
2. **Security Audits**:
    - Security professionals utilize Nmap to audit network security by identifying open ports, running services, and potential vulnerabilities.
3. **Compliance Testing**:
    - Nmap assists in ensuring compliance with security policies and standards by verifying the configuration of network devices and services.
4. **Penetration Testing**:
    - Penetration testers use Nmap as a reconnaissance tool to gather information about target networks before launching targeted attacks.

Basic Nmap Commands

1. **Scan a Single Host**:

Copy code

```
nmap <target_ip>
```

2. **Scan a Range of IPs**:

Copy code

```
nmap <start_ip>-<end_ip>
```

3. **Scan a Subnet**:

Copy code

```
nmap <target_subnet>/24
```

4. **Port Scan**:

Copy code

```
nmap -p <port_range> <target_ip>
```

5. **Service Version Detection**:

Copy code

```
nmap -sV <target_ip>
```

6. **Operating System Detection**:

Copy code

```
nmap -O <target_ip>
```

7. **Using Nmap Scripting Engine (NSE)**:

Copy code

```
nmap --script <script_name> <target_ip>
```

Example Workflow

1. **Host Discovery**:
    - Identify live hosts within a network.

Copy code

```
nmap -sn 192.168.1.0/24
```

2. **Port Scanning**:
    - Scan the identified hosts for open ports.

Copy code

```
nmap -p 1-65535 192.168.1.10
```

3. **Service Version Detection**:
    - Identify running services and their versions on the open ports.

Copy code

```
nmap -sV 192.168.1.10
```

4. **Operating System Detection**:
    - Determine the operating system of the target machine.

Copy code

```
nmap -O 192.168.1.10
```

5. **Vulnerability Detection using NSE**:
    - Use NSE scripts to check for known vulnerabilities.

Copy code

```
nmap --script=vuln 192.168.1.10
```

Introduction to NMAP

Nmap is a tool used for determining the hosts that are running and what services the hosts are running. Nmap can be a valuable diagnostic tool for network administrators while they can be also a potent reconnaissance tool for the Black-hat community (Hackers, Crackers, Script Kiddies, etc). Once the network is charted out using tools like Lan MapShot, the Nmap can be used to determine the type of services and hosts running in the network.

Primary Uses of Nmap

1. Determining open ports and services running in an host:
2. Determine the Operating System running on a host
3. Alter the source IP of the scan (One way is to use –S option)[1]

Nmap using Redhat 9.0

In the Cyberdefense lab scenario, it is recommended that Nmap be run from a Redhat Linux machine. Nmap can be run from a terminal using command lines or it can be run using a front end. Using the front end is more user-friendly. It also automatically shows the command being used. More information on Nmap can be obtained from the manual pages of Redhat using the command ‘man nmap’.

Usage of Nmap

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, and maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.
- DNS queries and subdomain search

Basic Scanning Commands

Goal	**Command**	**Example**
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc	nmap 192.168.0.1 192.168.0.2
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] –exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] –excludefile [list.txt]	nmap 192.168.0.1/24 –excludefile notargets.txt
Perform an	nmap -A [target]	nmap -A 192.168.0.1

Goal	Command	Example
Aggressive Scan		
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe

Discovery Options

Goal	Command	Example
Perform a Ping Only Scan	nmap -sP [target]	nmap -sP 192.168.0.1
Don’t Ping	nmap -PN [target]	nmap -PN 192.168.0.1
TCP SYN Ping	nmap -PS [target]	nmap -PS 192.168.0.1
TCP ACK Ping	nmap -PA [target]	nmap -PA 192.168.0.1
UDP Ping	nmap -PU [target]	nmap -PU 192.168.0.1
SCTP INIT Ping	nmap -PY [target]	nmap -PY 192.168.0.1
ICMP Echo Ping	nmap -PE [target]	nmap -PE 192.168.0.1
ICMP Timestamp Ping	nmap -PP [target]	nmap -PP 192.168.0.1
CMP Address Mask Ping	nmap -PM [target]	nmap -PM 192.168.0.1
IP Protocol Ping	nmap -PO [target]	nmap -PO 192.168.0.1
ARP Ping	**nmap -PR [target]**	**nmap -PR 192.168.0.1**
Traceroute	nmap –traceroute [target]	nmap –traceroute 192.168.0.1
Force Reverse DNS Resolution	nmap -R [target]	nmap -R 192.168.0.1
Disable Reverse DNS Resolution	nmap -n [target]	nmap -n 192.168.0.1
Alternative DNS Lookup	nmap –system-dns [target]	nmap –system-dns 192.168.0.1
Manually Specify DNS Server(s)	nmap –dns-servers [servers] [target]	nmap –dns-servers 201.56.212.54 192.168.0.1
Create a Host List	nmap -sL [targets]	nmap -sL 192.168.0.1/24

Advanced Scanning Options

Goal	Command	Example
TCP SYN Scan	nmap -sS [target]	nmap -sS 192.168.0.1
TCP Connect Scan	nmap -sT [target]	nmap -sT 192.168.0.1
UDP Scan	nmap -sU [target]	nmap -sU 192.168.0.1
TCP NULL Scan	nmap -sN [target]	nmap -sN 192.168.0.1
TCP FIN Scan	nmap -sF [target]	nmap -sF 192.168.0.1
Xmas Scan	nmap -sX [target]	nmap -sX 192.168.0.1
TCP ACK Scan	nmap -sA [target]	nmap -sA 192.168.0.1
Custom TCP Scan	nmap –scanflags [flags] [target]	nmap –scanflags SYNFIN 192.168.0.1
IP Protocol Scan	nmap -sO [target]	nmap -sO 192.168.0.1
Send Raw Ethernet Packets	nmap –send-eth [target]	nmap –send-eth 192.168.0.1
Send IP Packets	nmap –send-ip [target]	nmap –send-ip 192.168.0.1

Port Scanning Options

Goal	Command	Example
Perform a Fast Scan	nmap -F [target]	nmap -F 192.168.0.1
Scan Specific Ports	nmap -p [port(s)] [target]	nmap -p 21-25,80,139,8080 192.168.1.1
Scan Ports by Name	nmap -p [port name(s)] [target]	nmap -p ftp,http* 192.168.0.1
Scan Ports by Protocol	nmap -sU -sT -p U:[ports],T:[ports] [target]	nmap -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.0.1
Scan All Ports	nmap -p ‘*’ [target]	nmap -p ‘*’ 192.168.0.1
Scan Top Ports	nmap –top-ports [number] [target]	nmap –top-ports 10 192.168.0.1
Perform a Sequential Port Scan	nmap -r [target]	nmap -r 192.168.0.1

Version Detection

Goal	Command	Example
Operating System Detection	nmap -O [target]	nmap -O 192.168.0.1
Submit TCP/IP Fingerprints	www.nmap.org/submit/	
Fingerprints		
Attempt to Guess an Unknown OS	nmap -O –osscan guess [target]	nmap -O –osscan-guess 192.168.0.1
Service Version Detection	nmap -sV [target]	nmap -sV 192.168.0.1
Troubleshooting Version Scans	nmap -sV –version trace [target]	nmap -sV –version-trace 192.168.0.1
Perform a RPC Scan	nmap -sR [target]	nmap -sR 192.168.0.1

Firewall Evasion Techniques

Goal	Command	Example
augment Packets	nmap -f [target]	nmap -f 192.168.0.1
pacify a Specific MTU	nmap –mtu [MTU] [target]	nmap –mtu 32 192.168.0.
Use a Decoy	nmap -D RND:[number] [target]	nmap -D RND:10 192.168.0.1
le Zombie Scan	nmap -sI [zombie] [target]	nmap -sI 192.168.0.38
Manually Specify a Source Port	nmap –source-port [port] [target]	nmap –source-port 10 192.168.0.1
Append Random Data	nmap –data-length [size] [target]	nmap –data-length 2 192.168.0.1
Randomize Target Scan Order	nmap –randomize-hosts [target]	nmap –randomize-ho 192.168.0.1-20
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]	nmap –spoof-mac Cis 192.168.0.1
Send Bad Checksums	nmap –badsum [target]	nmap –badsum 192.168.0.1

Troubleshooting And Debugging

Goal	Command	Example
Getting Help	nmap -h	nmap -h
Display Nmap Version	nmap -V	nmap -V
Verbose Output	nmap -v [target]	nmap -v 192.168.0.1
Debugging	nmap -d [target]	nmap -d 192.168.0.1
Display Port State Reason	nmap –reason [target]	nmap –reason 192.168.0.1
Only Display Open Ports	nmap –open [target]	nmap –open 192.168.0.1
Trace Packets	nmap –packet-trace [target]	nmap –packet-trace 192.168.0.1
Display Host Networking	nmap –iflist	nmap –iflist
Specify a Network Interface	nmap -e [interface] [target]	nmap -e eth0 192.168.0.1

NMAP Scripting Engine

Goal	Command	Example
Execute Individual Scripts	nmap –script [script.nse] [target]	nmap –script banner.nse 192.168.0.1
Execute Multiple Scripts	nmap –script [expression] [target]	nmap –script 'http-*' 192.168.0.1
Script Categories	all, auth, default, discovery, external, intrusive, malware, safe, vuln	
Execute Scripts by Category	nmap –script [category] [target]	nmap –script 'not intrusive' 192.168.0.1
Execute Multiple Script Categories	nmap –script [category1,category2,etc]	nmap –script 'default or safe' 192.168.0.1
Troubleshoot Scripts	nmap –script [script] –script trace [target]	nmap –script banner.nse –script-trace 192.168.0.1
Update the Script Database	nmap –script-updatedb	nmap –script-updatedb

Kali Linux – Forensics Tools

These tools even allow us to encrypt our messages in images or other files to hide it from those who want to read the message because of their malicious intentions. We could analyze or even open the code of any file using the following mentioned tools. Below is the list of the Basic tools for Forensics Tools

p0f

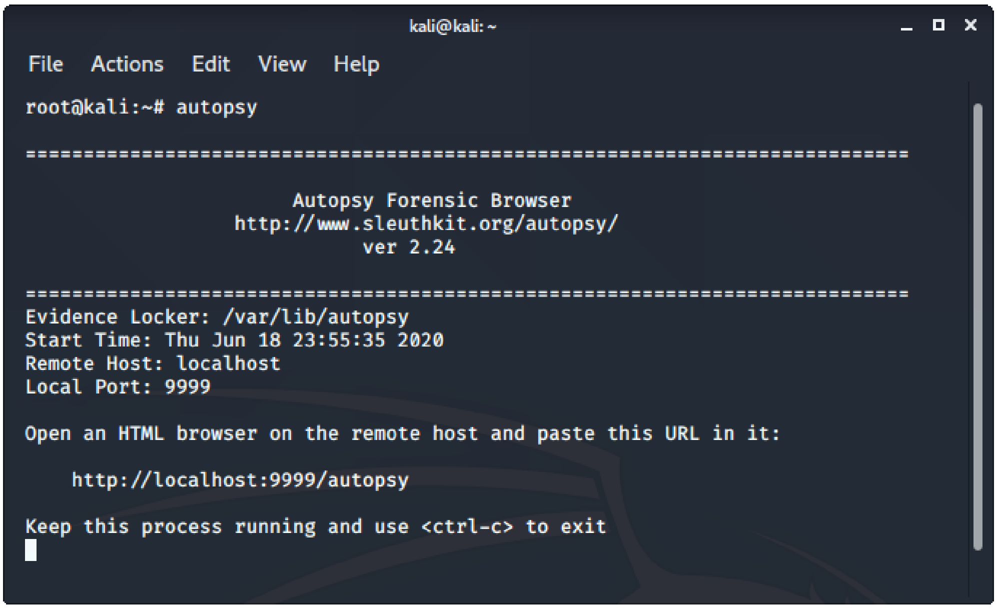
p0f is a great tool when we have to analyze network captured packages. p0f is used to gather the information of the host like the IP address, Operating System, and much more from the package. This tool may prove to be a great tool when there is a firewall over the network of the captured packet. It is very highly scalable and allows the fast identification of host details. It also allows us to perform information gathering while performing vulnerability tests and to monitor the network.
To use p0f: Enter the following command in the terminal.

p0f -h

Autopsy

Autopsy is a digital forensics tool that is used to gather the information form forensics. Or in other words, this tool is used to investigate files or logs to learn about what exactly was done with the system. It could even be used as a recovery software to recover files from a memory card or a pen drive.
To use autopsy tool

- Autopsy comes pre-installed in Kali Linux
- Just type “**autopsy**” in the terminal.



```
root@kali:~# autopsy

============================================================================

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                              ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Thu Jun 18 23:55:35 2020
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Tools	Description
Binwalk	It is a tool for searching a given binary image for embedded files and executable code.
bulk-extractor	It extracts information without parsing file systems such as e-mail addresses, credit card numbers, URLs, and other types of details from digital evidence files.
Capstone	It is a framework used for binary analysis and reversing. It supports multiple hardware architectures and provides semantics of the disassembled instruction.
chntpw	It is used to view information and change user passwords in Windows NT/2000 user database file.
Cuckoo	It is a malware analysis system that can provide you the details of suspicious files you asking for.
dc3dd	It is a patched version of GNU dd with added features for computer forensics.
ddrescue	It duplicates data from one file or block device to another specified file or block.
DFF	DFF stands for Digital Forensic Framework. It is used to quickly and easily collect, preserve, and reveal digital evidence without compromising systems and data.
diStorm3	It is a lightweight, easy-to-use, and fast decomposer library that disassembles a staged reverse shell generated by msfpayload.
Dumpzilla	Dumpzilla is a tool to extract all forensic related information of Firefox, Iceweasel, and Seamonkey browsers to analyse.
extundelete	This tool is used to recover deleted files from ext3/ext4 file system partition.
Foremost	It is a forensic tool to recover lost files based on their headers, footers, and internal data structures.
Galleta	It is a forensic tool that examines the content of cookies produced by Internet explorer.
Guymager	It is a free forensic imager for media access. It generates flat, EWF, and AFF images support disk cloning.

iPhone Backup Analyzer	It is a backup utility designed to browse easily through the backup folder of an iPhone.
p0f	It is a traffic fingerprinting mechanism to identify the process behind any incidental TCP/IP communications without disturbing the process in any way.
Pdf-parser	It is used to parse a PDF document to identify the fundamental elements used in the analysed file.
pdfid	It scans a file to look for certain pdf keywords, allowing you to identify PDF documents that contain JavaScript.
pdgmail	It extracts Gmail artefacts from a pd process memory dump
peepdf	It is a pdf analysis tool to explore PDF files in order to find if the file can be harmful or not.
RegRipper	It extracts information from the windows registry and presents it for analysis.
Volatility	It is a memory forensic analysis platform to extracts the digital artefacts from the RAM samples.
Xplico	It is a network forensic analysis tool that extracts application data from internet traffic.

Kali linux Pentesting tools

John the Ripper (JtR) is one of the hacking tools the Varonis IR Team used in the first Live Cyber Attack demo, and one of the most popular password cracking programs out there. In this blog post, we are going to dive into John the Ripper, show you how it works, and explain why it's important.

How Does John the Ripper Work?

JtR supports several common encryption technologies out-of-the-box for UNIX and Windows-based systems. (ed. Mac is UNIX based). JtR autodetects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match. Simple.

In our amazing Live Cyber Attack demo, the Varonis IR team demonstrates how to steal a hashed password, use JtR to find the true password, and use it to log into an administrative account. That is a very common use case for JtR!

JtR also includes its own wordlists of common passwords for 20+ languages. These wordlists provide

JtR with thousands of possible passwords from which it can generate the corresponding hash values to make a high-value guess of the target password. Since most people choose easy-to-remember passwords, JtR is often very effective even with its out-of-the-box wordlists of passwords.
JtR is included in the pentesting versions of Kali Linux.

What is John the Ripper Used for?

JtR is primarily a password cracker used during pentesting exercises that can help IT staff spot weak passwords and poor password policies.

Here is the list of encryption technologies found in JtR:

- UNIX crypt(3)
- Traditional DES-based
- “bigcrypt”
- BSDI extended DES-based
- FreeBSD MD5-based (linux and Cisco IOS)
- OpenBSD Blowfish-based
- Kerberos/AFS
- Windows LM (DES-based)
- DES-based tripcodes
- SHA-crypt hashes (newer versions of Fedora and Ubuntu)
- SHA-crypt and SUNMD5 hashes (Solaris)

That’s the “official” list. JtR is open-source, so if your encryption of choice isn’t on the list do some digging. Someone might have already written an extension for it.

Tutorials for Using John the Ripper

We are going to go over several of the basic commands that you need to know to start using John the Ripper. To get started all you need is a file that contains a hash value to decrypt.

If you ever need to see a list of commands in JtR, run this command:

```
.\john.exe
```

Cracking Passwords

John the Ripper’s primary modes to crack passwords are single crack mode, wordlist mode, and incremental. The single crack mode is the fastest and best mode if you have a full password file to crack. Wordlist mode compares the hash to a known list of potential password matches. Incremental mode is the most powerful and possibly won’t complete. This is your classic brute force mode that tries every possible character combination until you have a possible result.

The easiest way to try cracking a password is to let JtR go through a series of common cracking modes. This command below tells JtR to try “simple” mode, then the default wordlists containing likely passwords, and then “incremental” mode.

```
.\john.exe passwordfile
```

You can also download different wordlists from the Internet, and you can create your own new wordlists for JtR to use with the –wordlist parameter.

```
.\john.exe passwordfile –wordlist=”wordlist.txt”
```

If you want to specify a cracking mode use the exact parameter for the mode.

```
.\john.exe --single passwordfile

.\john.exe --incremental passwordfile
```

Word Mangling Rules

Mangling is a preprocessor in JtR that optimizes the wordlist to make the cracking process faster. Use the –rules parameter to set the mangling rules.

```
.\john.exe --wordlist=”wordlist.txt” --rules --passwordfile
```

Viewing Your Output

When you want to see the list of passwords that you have cracked, use the –show parameter.

```
.\john.exe –show passwordfile
```

If your cracked password list is long, you can filter the list with additional parameters. You can also redirect the output using basic redirection in your shell. For example, if you want to see if you cracked any root users (UID=0) use the –users parameter.

```
.\john.exe --show --users=0 passwordfile
```

Or if you want to show users from privileged groups use –groups.

```
.\john.exe --show --groups=0,1 passwordfile
```

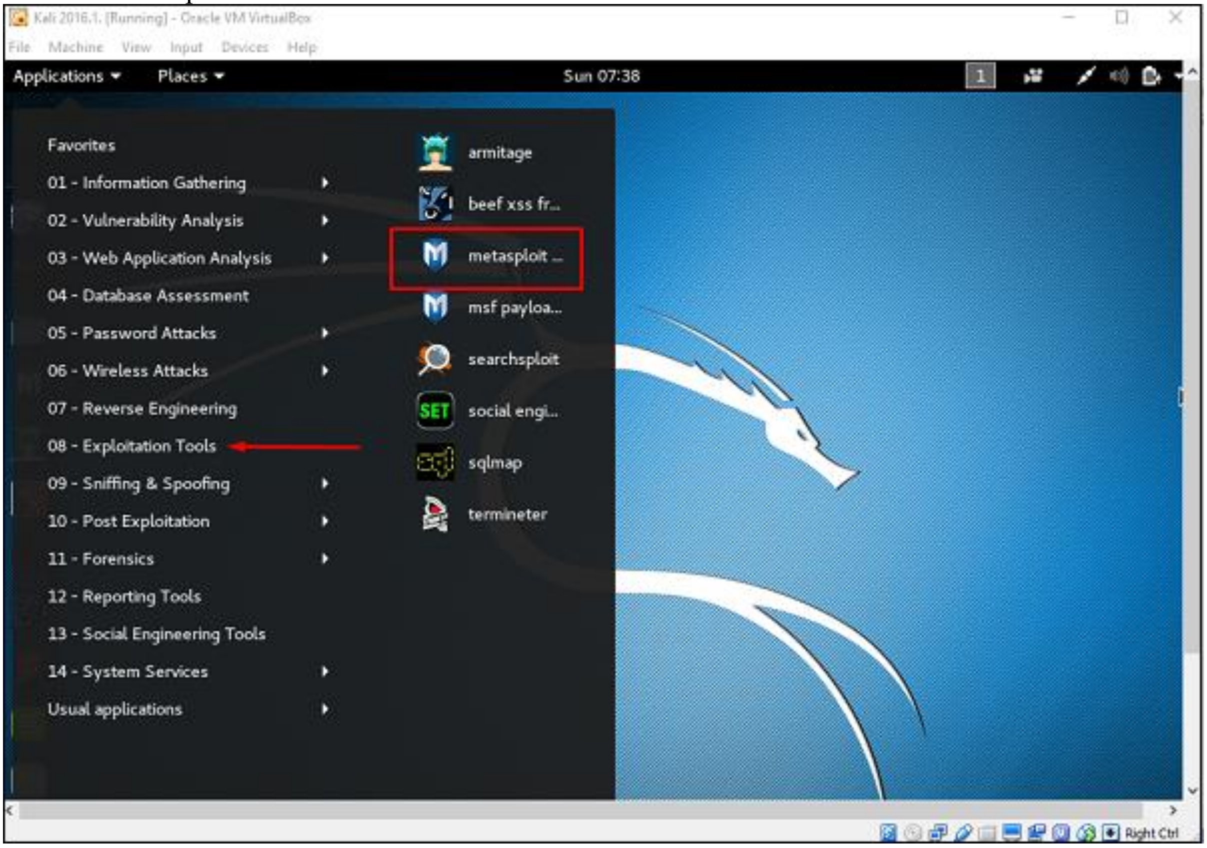
Below is the JtR command from our Live Cyber Attack Webinar. In this scenario, our hacker used kerberoast to steal a Kerberos ticket granting ticket(TGT) containing the hash to be cracked, which was saved in a file called ticket.txt. In our case, the wordlist used is the classic rockyou password file from Kali Linux, and the command was set to report progress every 3 seconds.

```
.\john.exe "--format=krb5tgs" "ticket.txt" "--
wordlist=”rockyou.txt" "--progress-every=3"
```

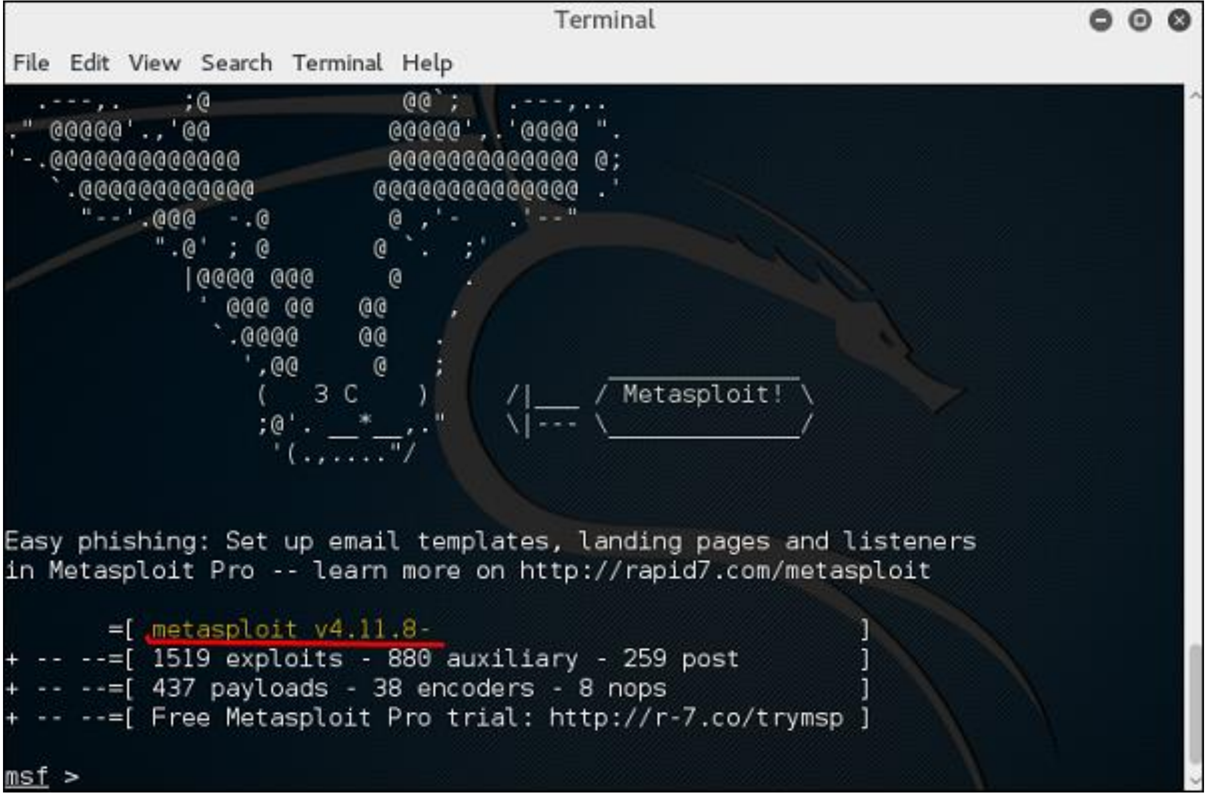
Metasploit

Metasploit is one of the most powerful and widely used tools for penetration testing. In this tutorial, we will take you through the various concepts and techniques of Metasploit and explain how you can use them in a real-time environment.

open the Metasploit console in Kali. You can do so by following the path: Applications → Exploitation Tools → Metasploit.



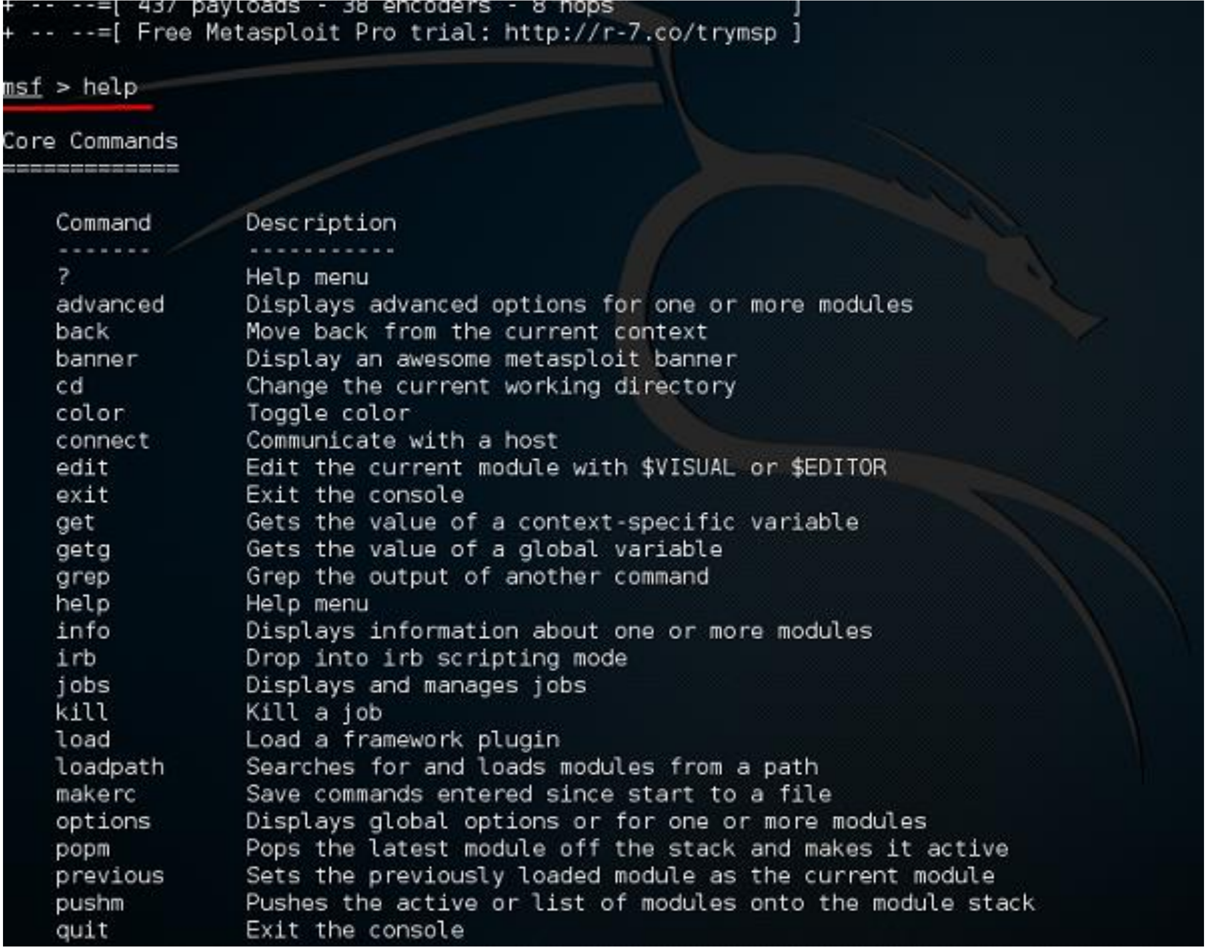
Once you open the Metasploit console, you will get to see the following screen. Highlighted in red underline is the version of Metasploit.



```
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / 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 >
```

Help Command

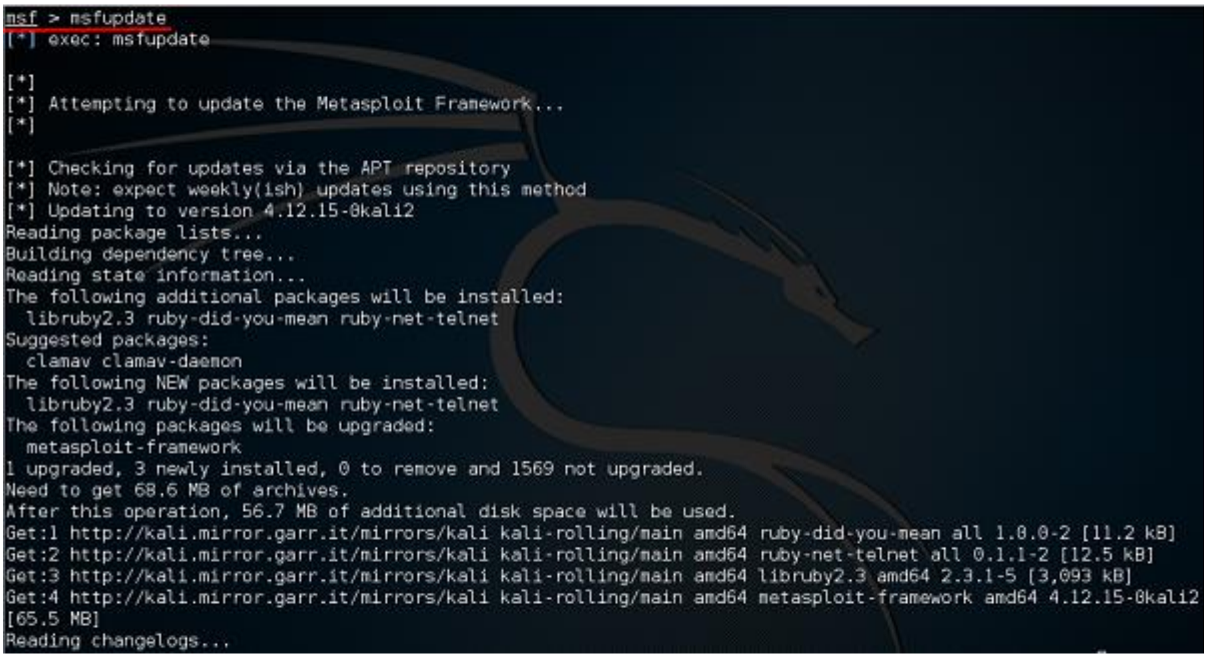
If you type the **help** command on the console, it will show you a list of core commands in Metasploit along with their description.



```
+ -- --=[ 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
```

msfupdate Command

msfupdate is an important administration command. It is used to update Metasploit with the latest vulnerability exploits. After running this command, you will have to wait several minutes until the update completes.



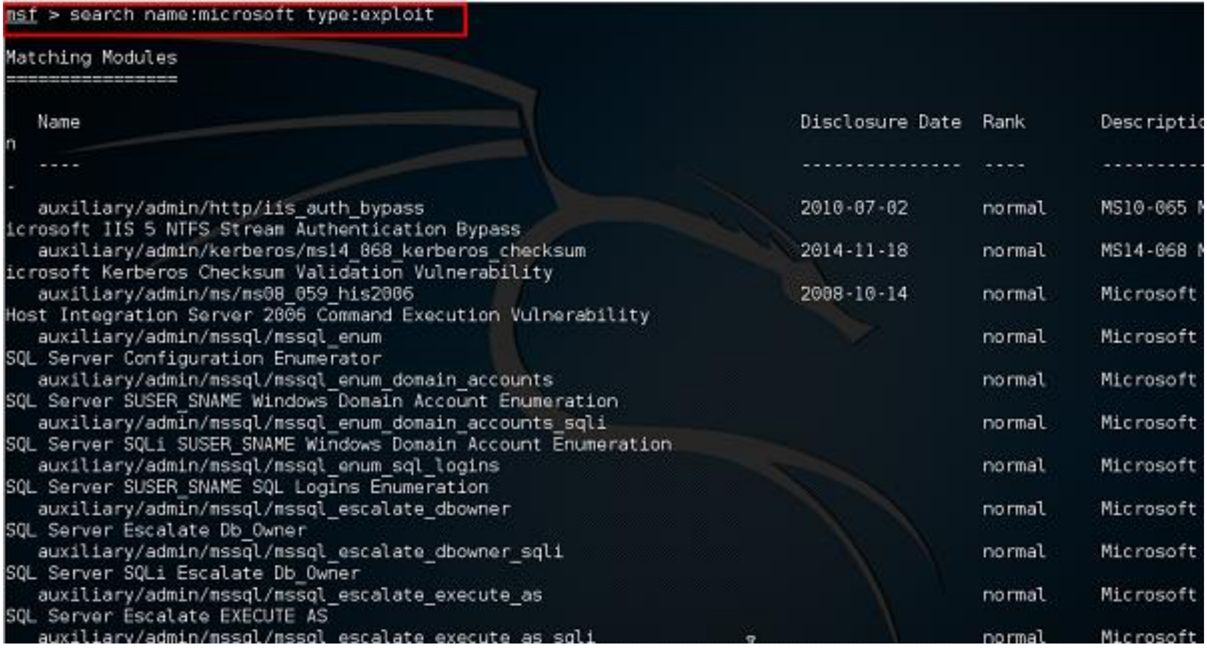
```
msf > msfupdate
[*] exec: msfupdate

[*]
[*] 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...
```

Search Command

Search is a powerful command in Metasploit that you can use to find what you want to locate. For example, if you want to find exploits related to Microsoft, then the command will be –

msf >search name:Microsoft type:exploit

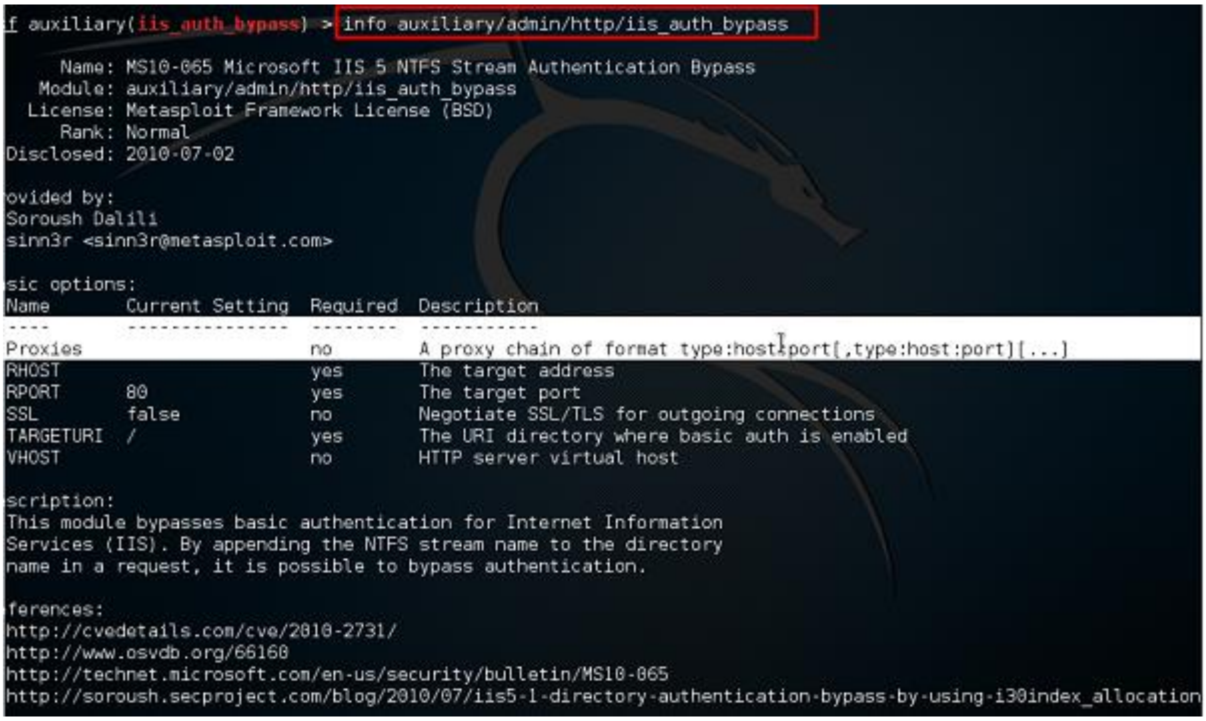
Here, **search** is the command, **name** is the name of the object that you are looking for, and **type** is the kind of script you are searching.



```
msf > search name:microsoft type:exploit

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

   Name                                                                      Disclosure Date  Rank       Descriptio
n
   ----                                                                      ---------------  ----       ----------
-
   auxiliary/admin/http/iis_auth_bypass                                      2010-07-02       normal     MS10-065 M
icrosoft IIS 5 NTFS Stream Authentication Bypass
   auxiliary/admin/kerberos/ms14_068_kerberos_checksum                       2014-11-18       normal     MS14-068 M
icrosoft Kerberos Checksum Validation Vulnerability
   auxiliary/admin/ms/ms08_059_his2006                                       2008-10-14       normal     Microsoft
Host Integration Server 2006 Command Execution Vulnerability
   auxiliary/admin/mssql/mssql_enum                                                           normal     Microsoft
SQL Server Configuration Enumerator
   auxiliary/admin/mssql/mssql_enum_domain_accounts                                           normal     Microsoft
SQL Server SUSER_SNAME Windows Domain Account Enumeration
   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                                      normal     Microsoft
SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration
   auxiliary/admin/mssql/mssql_enum_sql_logins                                                normal     Microsoft
SQL Server SUSER_SNAME SQL Logins Enumeration
   auxiliary/admin/mssql/mssql_escalate_dbowner                                               normal     Microsoft
SQL Server Escalate Db_Owner
   auxiliary/admin/mssql/mssql_escalate_dbowner_sqli                                          normal     Microsoft
SQL Server SQLi Escalate Db_Owner
   auxiliary/admin/mssql/mssql_escalate_execute_as                                            normal     Microsoft
SQL Server Escalate EXECUTE AS
   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli                                       normal     Microsoft
```

Info Command

The **info** command provides information regarding a module or platform, such as where it is used, who is the author, vulnerability reference, and its payload restriction.



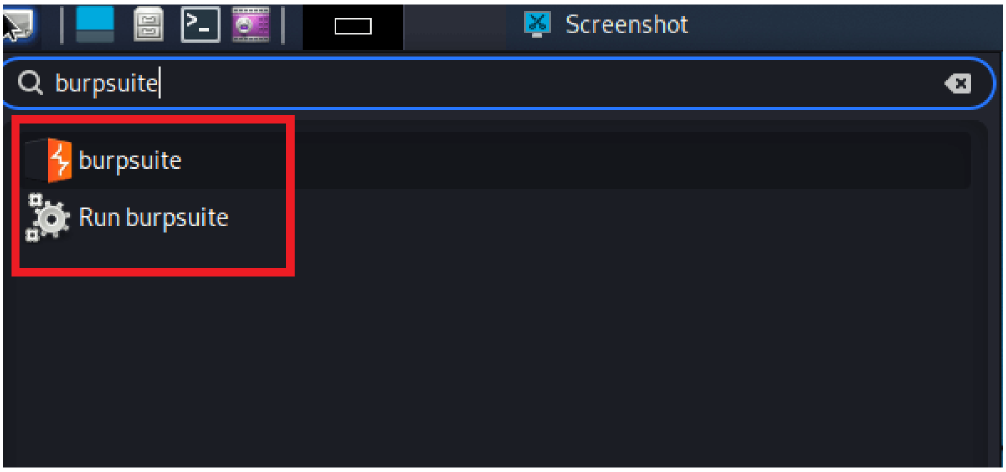
```
f auxiliary(iis_auth_bypass) > info auxiliary/admin/http/iis_auth_bypass

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

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

sic options:
Name        Current Setting  Required  Description
----        ---------------  --------  -----------
Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST                        yes       The target address
RPORT       80               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

scription:
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.

ferences:
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
```

Burp Suite

One of the most widely used web application security testing tools is **Burp Suite**. It is utilized as a proxy, so all the requests from the browser with the proxy pass through it. And, because the requests run through the burp suite, we can make changes to it as needed, which is useful for testing vulnerabilities such as **XSS** or **SQLi** as well as any other web-related issue. Burp suite community edition is free with Kali Linux. Still, there is a premium version of this tool called burp suite professional that has a lot more features than the burp suite community edition.

To Use Burp Suite:

- First, we have to open the terminal and type **"burpsuite"** on the terminal.
- Then we have to go to the **proxy tab** and turn the interceptor switch on.
- Now visit any **UR**L, and we will see that the request has been captured.



SQL Map

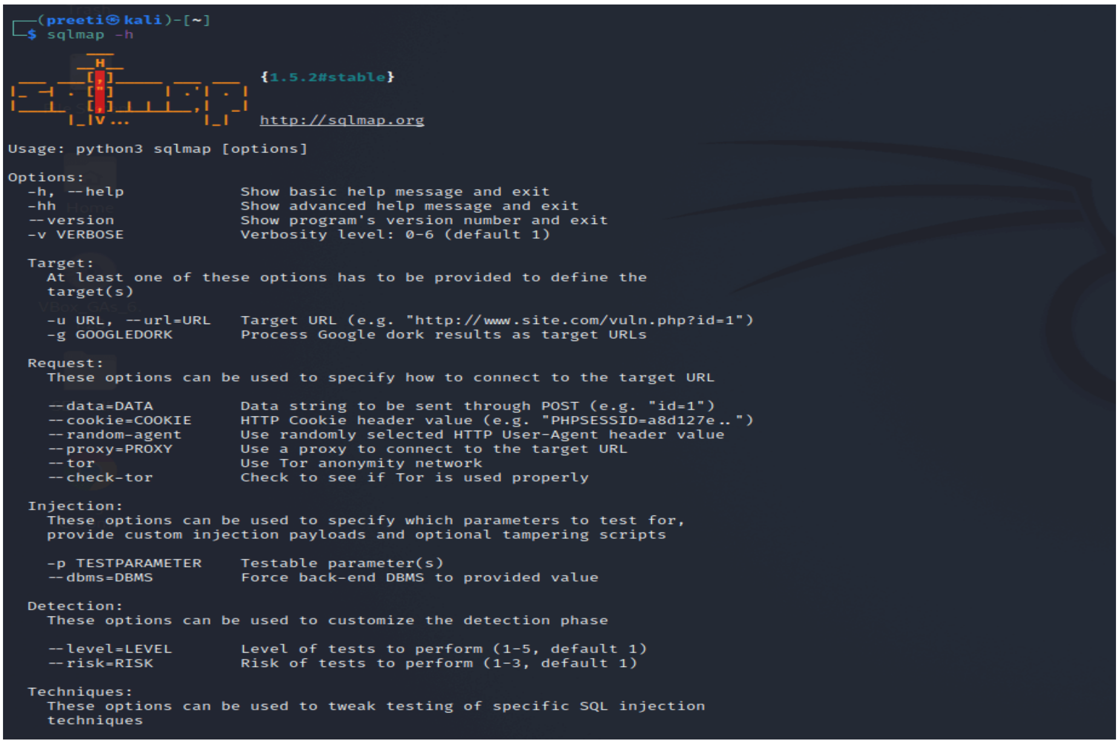
SQLMap is an **open-source** tool that we can use to automate the process of **manual SQL injection** over a parameter on a website. It can detect and exploit the SQL injection parameters itself, all we need to do is to provide it with a proper request or URL. It supports **34 databases**, including **MySQL, Oracle, PostgreSQL**, etc.

To Use Sqlmap tool:

In order to use sqlmap, we have to follow the following steps:

- Kali Linux comes with s**qlmap** pre-installed.
- To use this tool, simply type the following command on the terminal:

```
Sqlmap -h
```



```
┌──(preeti㉿kali)-[~]
└─$ sqlmap -h
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]

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

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

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

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques
```

Maltego

Maltego is a platform designed to communicate and present a clear image of the environment in which an organization owns and operates. Maltego provides a unique perspective to **network** as well as **resource-based** entities, which is the aggregation of the information delivered all over the internet- whether it is the current configuration of a router poised on the edge of our network or any other information, **Maltego** can **locate, aggregate** and **visualize** this information. It provides the user with extraordinary information that is leveraged and powerful.
Maltego's Uses
The following are the uses of Maltego:

- Maltego helps us to discover **"hidden"**
- It helps us in the **thinking process** by visually presenting interconnected links between searched items.
- It is used in the collection of information for all **security-related** It will save time and enable us to work more correctly and efficiently.
- It offers a much more powerful search, providing smarter results.
- We used this tool to show the complexity and severity of single points of failure, as well as the existing state of trust relationships within the infrastructure.

If we want to use **Maltego**, we have to Go to the **applications menu** and then select the **"Maltego"** tool to execute it.

Hydra

Hydra is an open source, password brute-forcing tool designed around flexibility and high performance in online brute-force attacks. Online brute force refers to brute forcing used in online network protocols, such as SSH, Remote Desktop Protocol (RDP) and HTTP (e.g., HTTP basic authentication), as well as on HTML forms. Hydra provides brute-forcing capabilities for these protocols and situations, as well as numerous others. It was designed to be parallelized, meaning multiple threads can operate in parallel to optimize efficiency and speed up the brute-forcing process.
Offline password cracking, such as using an automated tool to try to crack a Windows Security Account Manager database or the contents of a Linux password shadow file (i.e., /etc/shadow), requires different tools, such as hashcat or John the Ripper.

How to download Hydra

There are a few different ways to obtain and use Hydra:

- Download it, and build it yourself from source.
- Pull it down in a docker container (docker pull vanhauser/hydra).
- Find it preconfigured in most penetration testing Linux distributions, including Kali, Parrot and BlackArch.

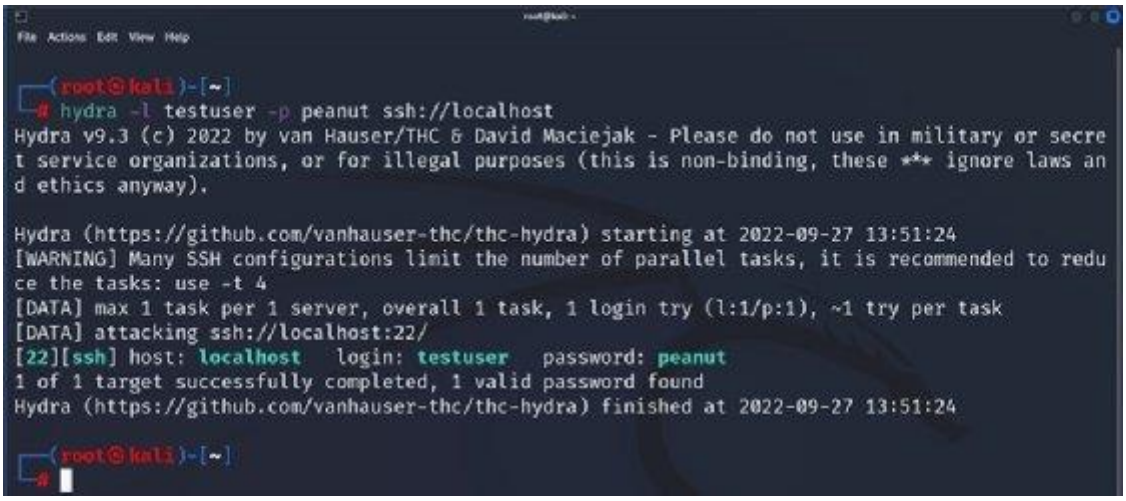
Extensive Hydra documentation is available online. Note, some sources refer to the tool as THC Hydra in reference to the hacking group THC that developed the tool. For the purpose of this discussion, we refer to it as just Hydra in keeping with the tool's documentation.

How to use Hydra

While an extremely powerful tool, the Hydra interface is both simple and intuitive. In general, only three pieces of information need to be supplied to Hydra:

1. the username(s) to use during the brute-force attack;
2. the password; and
3. the remote resource to be attacked.

In its simplest incarnation, use the -l (lowercase L) option to specify a single user account to try and the -p option to specify a specific password, as well as the protocol and address of the resource. In the example below, the -l flag indicates a specific user, -p indicates a specific password and the URL ssh://localhost to cause it to test the local machine.



```
┌──(root㉿kali)-[~]
└─# hydra -l testuser -p peanut ssh://localhost
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-27 13:51:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
ce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://localhost:22/
[22][ssh] host: localhost   login: testuser   password: peanut
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-27 13:51:24

┌──(root㉿kali)-[~]
└─#
```

All the Best!