

**MANAV RACHNA INTERNATIONAL
INSTITUTE OF REASEARCH &
STUDIES**

**FACULTY OF ENGINEERING AND
TECHNOLOGY**



**PRACTICAL FILE
FOR
VIIth SEMESTER (ACADEMIC YEAR 2021-2022)**

SUBJECT NAME: ITNS Lab

SUBJECT CODE: BCS-DS-774

SUBMITTED BY:-

**STUDENT NAME: Yash Sharma
ROLL NO.: 1/19/FET/BCS/061**

SUBMITTED TO:-

**FACULTY NAME: Dr. Savita
DEPARTMENT: FET**

INDEX

<u>PRACTICAL NO.</u>	AIM OF PRACTICAL	DATE ON WHICH CONDUCTED	TEACHER'S SIGNATURE
1.	To Install Kali Linux		
2.	To Install Windows 7		
3.	To Implement all commands on NMAP for Network Scanning		
4.	To Implement ARP Spoofing		
5.	To Implement Nessus basic Scan		
6.	To Perform DNS Spoofing Attack		
7.	To use Metasploit framework to exploit system		
8.	Implementation of Foot Printing Lab		
9.	Implementation of Cryptography Labs		
10.	Implementation of File System Security		
11.	Implementation of Network Security Tools and Technologies Lab		

EXPERIMENT -01

AIM- Installation of virtual box and windows 7

VirtualBox is a cross-platform virtualization application. What does that mean? For one thing, it installs on your existing Intel or AMD-based computers, whether they are running Windows, Mac, Linux or Solaris operating systems. Secondly, it extends the capabilities of your existing computer so that it can run multiple operating systems (inside multiple virtual machines) at the same time. So, for example, you can run Windows and Linux on your Mac, run Windows Server 2008 on your Linux server, run Linux on your Windows PC, and so on, all alongside your existing applications. You can install and run as many virtual machines as you like -- the only practical limits are disk space and memory.

VirtualBox is deceptively simple yet also very powerful. It can run everywhere from small embedded systems or desktop class machines all the way up to datacentre deployments and even Cloud environments.

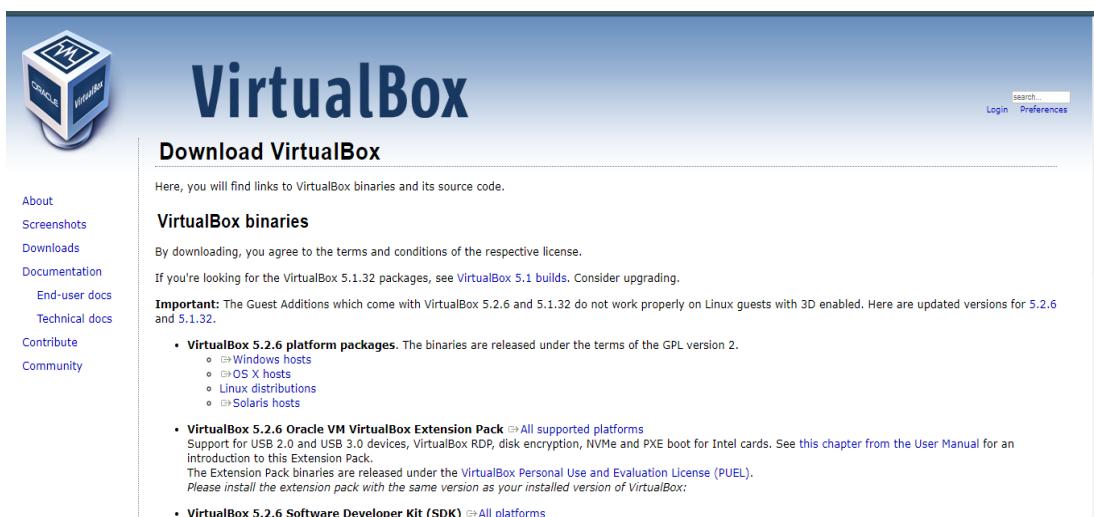
The following screenshot shows you how VirtualBox, installed on a Mac computer, is running Windows 8 in a virtual machine window:

STEPS FOR INSTALLATION OF VIRTUAL BOX: -

PART-1: CREATE THE VIRTUAL MACHINE

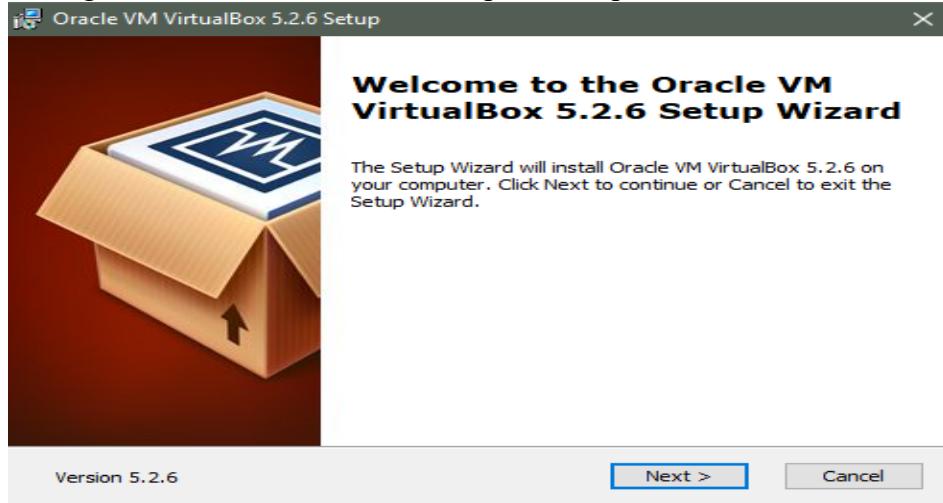
STEP-1: Download VirtualBox. VirtualBox from Oracle is available for free from the developer's website. Make sure that you download the correct version for your operating system.

- There are multiple choices for Linux or Windows versions. Choose the package that matches your Linux or Windows distribution or use the "All distributions" option if your Linux distribution is not listed.

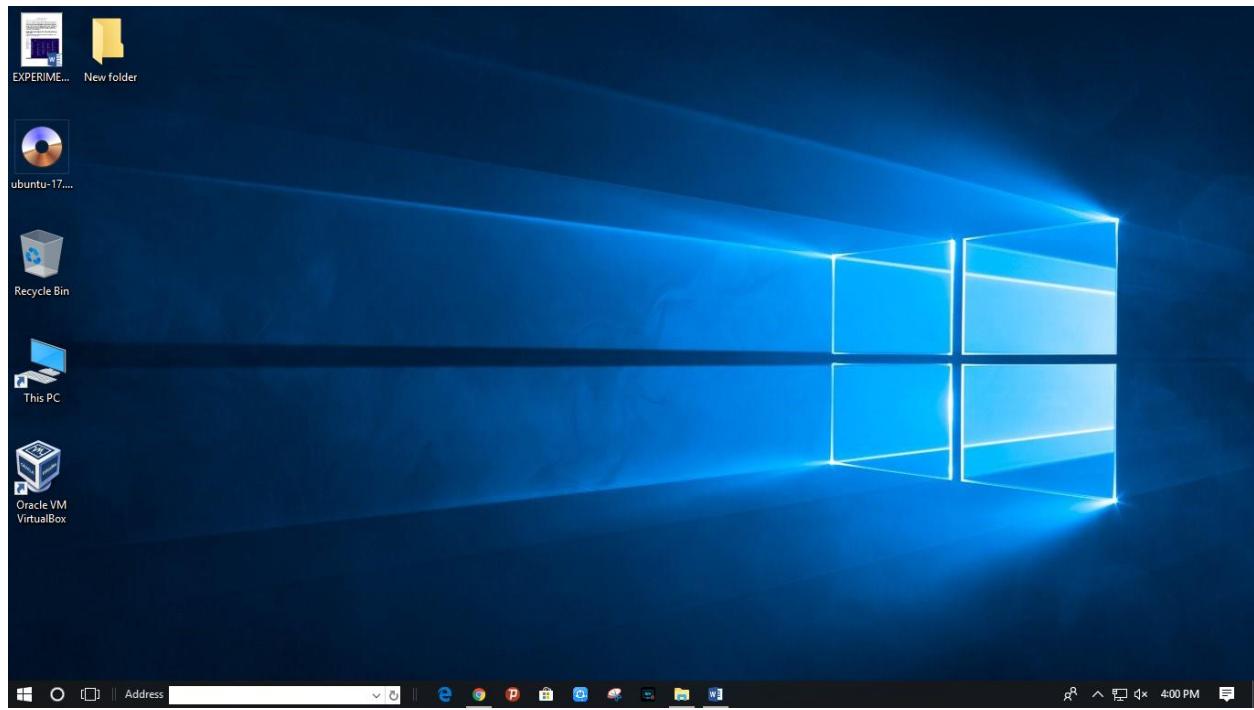


STEP-2: Install the VirtualBox program. If you are using Windows, double-click the setup file and follow the prompts to install. If you are using a Mac, open the DMG file that you downloaded and drag the VirtualBox file to your Applications folder.

- During the Windows installation, keep all the options set to their default.



STEP-3: Start the program. VirtualBox allows you to manage your various virtual machines, and easily create new ones. You can run VirtualBox directly from the installation program, or you can start it from the desktop icon.

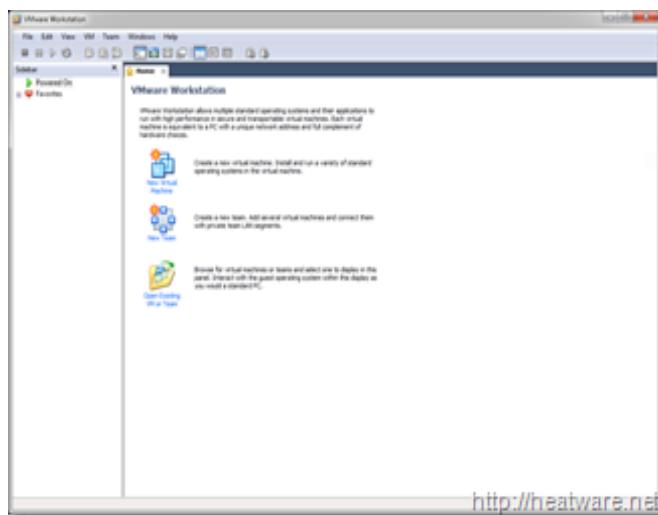


STEP-4: Gather your installation disc(s). When creating a virtual machine, you will need to install the operating system just like you would on a regular computer. This means that you will need the installation discs for the operating system you want to install on the virtual machine.

- If you download the ISO file for the installation disc, you can burn it to a blank DVD, or install it directly from the ISO file.

PART-2: Windows installation in Virtual Box

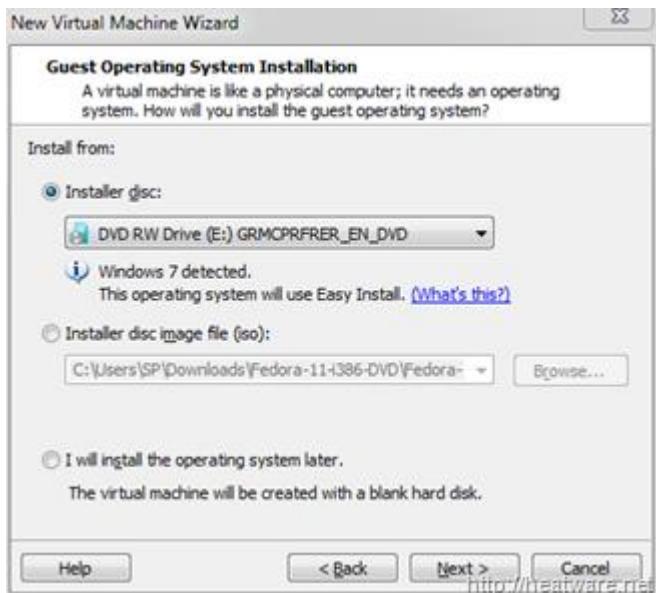
- **To Install Windows 7 inside of VMware Workstation**
- Download and install VM ware
- Insert the Windows 7 install DVD into your drive
- Run VMware Workstation 7.0 from the Start menu
- Click **New Virtual Machine**



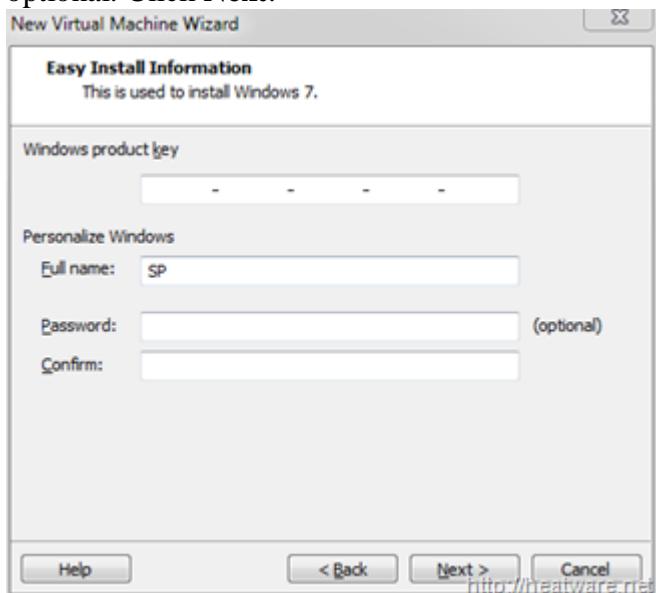
- Choose **Typical** and click **Next**



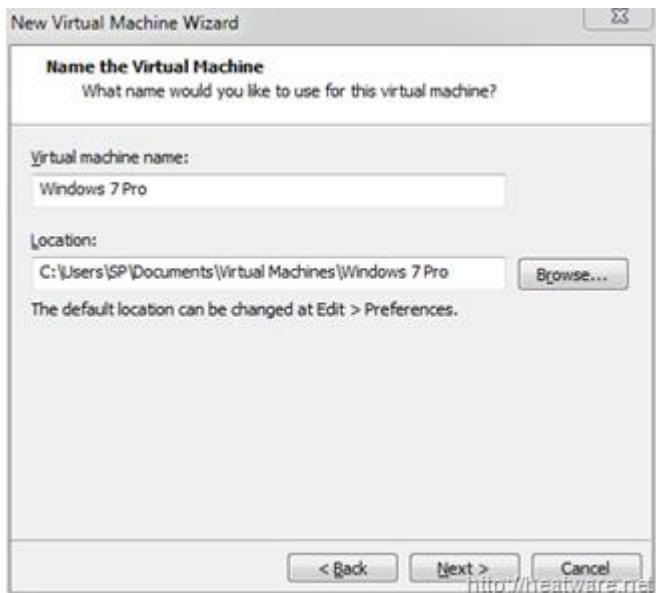
- Choose the option **Installer Disc** and ensure that the optical drive that has the Windows 7 installation DVD is selected.
Note: If you have Windows 7 as an ISO image, choose the option labelled: Installed disc image file (iso)



- A convenient new feature is the ability to specify your Windows 7 product key prior to starting the installation to allow for a fully-unattended install. No more coming back to your computer an hour later after you think the installation finished only to find it stuck on a screen asking for a serial number! Go ahead and enter your **Windows product key** and **Full name**. The password is optional. Click **Next**.



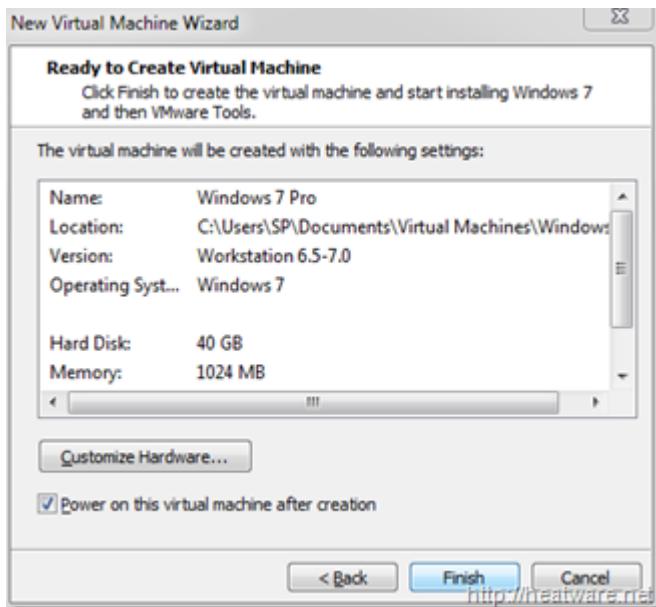
- Now it is time to name the virtual machine and choose the location. We will keep the default location and name the VM **Windows 7 Pro**



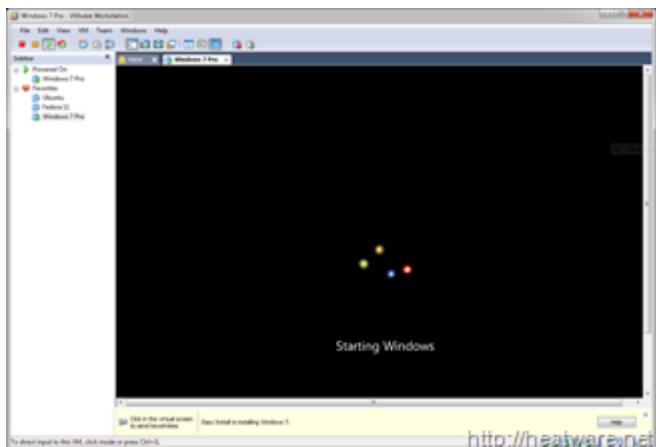
- VMware needs to know how hard drive space to allocate to the Windows 7 disk. Lets stick with the 40.0 GB default and click **Next**.



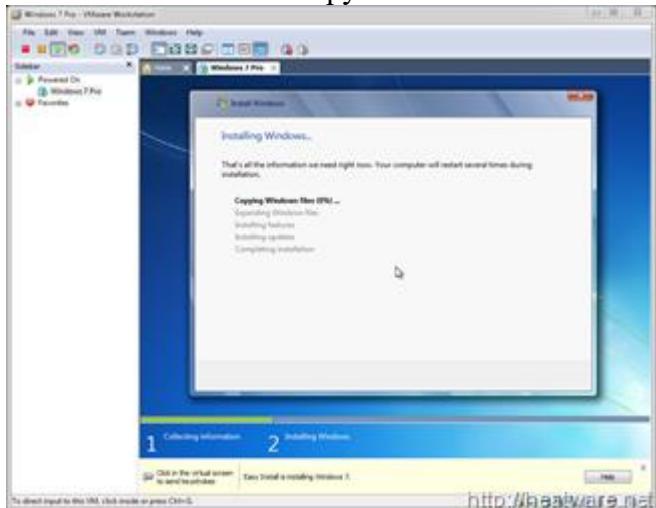
Now you will be presented with a summary screen that shows all the VM configuration parameters. Don't worry, you can change most of these at any time! Click **Finish** to begin the installation!



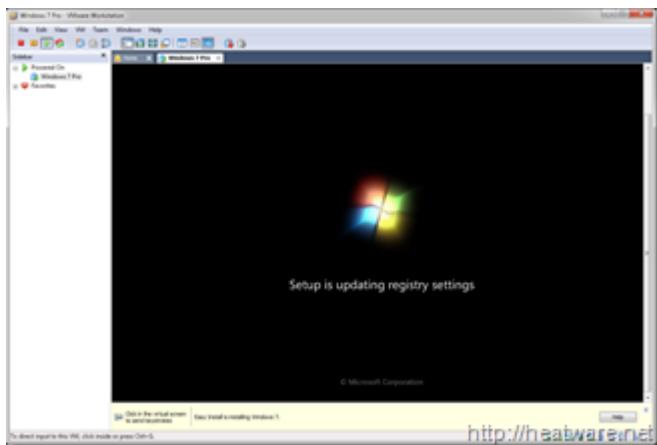
- The virtual machine will now boot up and load the Windows 7 installer from the DVD. If you need to step away from the computer, go ahead, no more user-intervention is needed.



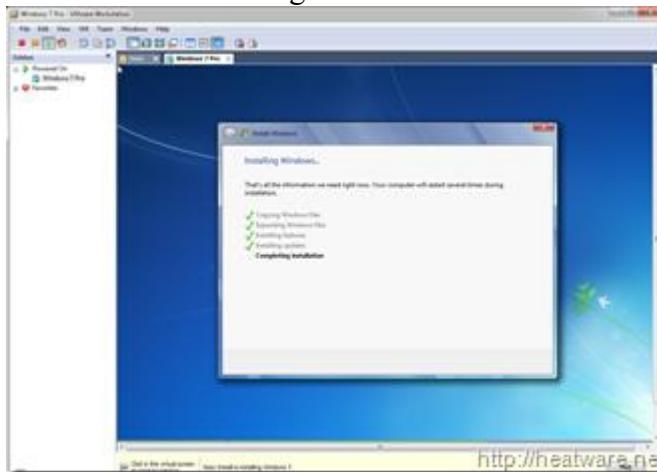
- The installer will now copy files... This will take a while...



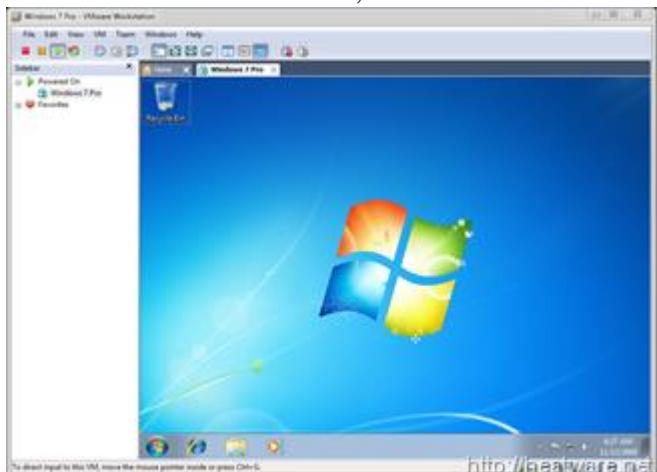
- Your system will reboot...



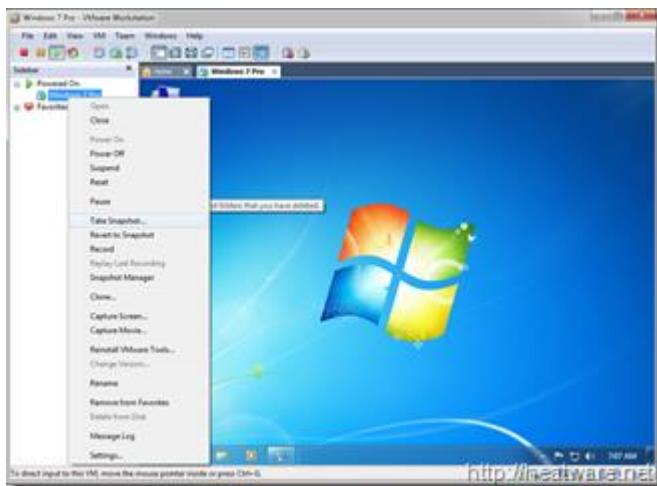
- And continue installing...



- And about 30 minutes later, its all done!



- Now is a great time to save the state of your VM by taking a snapshot. This way, if you shut down VMware, you don't have to start all over again! Right click on *Windows 7 Pro* in the left panel and choose **Take Snapshot**



EXPERIMENT -02

AIM- Installation of Kali Linux

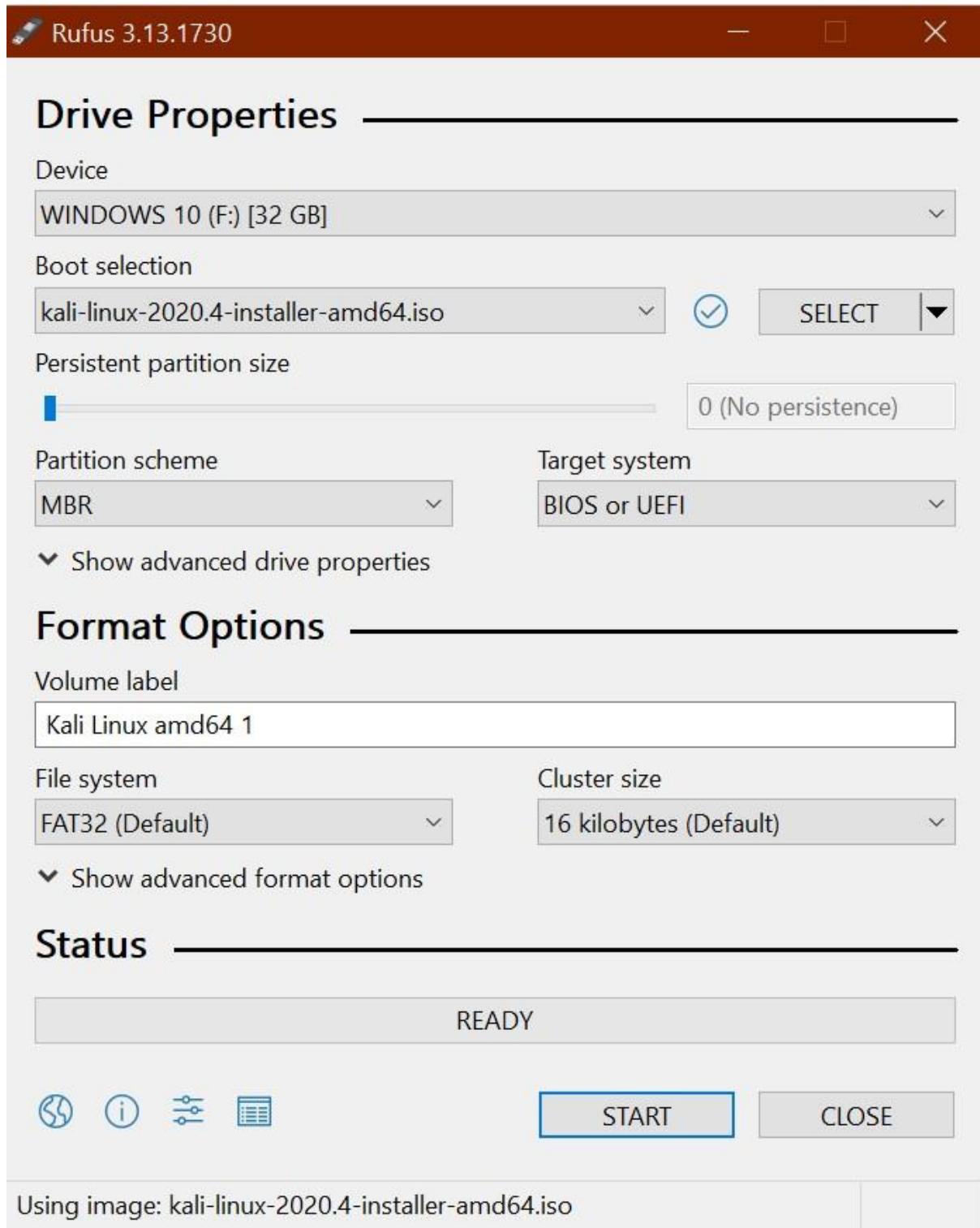
Kali is an operating system based on Debian that is used by security experts called penetration testers to test the security of hardened systems. Kali comes with an extensive list of tools that you can use to test how secure your server is, ranging from testing anti-virus software to social engineering attacks and malware. This operating system is for intermediate to advance users and while it does come with the Gnome Desktop Environment, most of its features will require you to be proficient in the use of the terminal. Don't let that scare you, the terminal is often easier and quicker than graphical user interfaces.

Let's get started; Install Kali Linux 2021.1:

Step 1: Create a USB installer

Kali Linux 2021.1 Release Notes 8			
Image Name	Torrent	Size	SHA256sum
 Kali Linux 64-Bit (Installer)	Torrent	4.0G	265812bc13ab11d4 0c610424871bd91 98b9e7cad99b0654 0d96fac67dd704de
 Kali Linux 64-Bit (Live)	Torrent	3.4G	8e5af78e93424336 f787d4d0fd89b4 29675d5ae67b1c16 34ea1b53c5659677

First thing is first, you are going to need to boot into a USB installer to start the installation process. This involves two parts; first, download a copy of Kali Linux 2021.1 from their [Official Website](#). There are two versions of the ISO, one is an installer, the other is for the live version of kali. Choose the one labelled installer.



Then download [Rufus](#) which is the tool you will need to create your USB installer with a few simple clicks. [Click here](#) to download version 3.13 of Rufus or go to [Rufus.ie](#) and download the latest version.

Step 2: Boot to the USB drive

Make sure your recently created USB installer is plugged into the computer you would like to install Kali Linux 2021.1 into then power it on and as it boots continuously tap either the F10

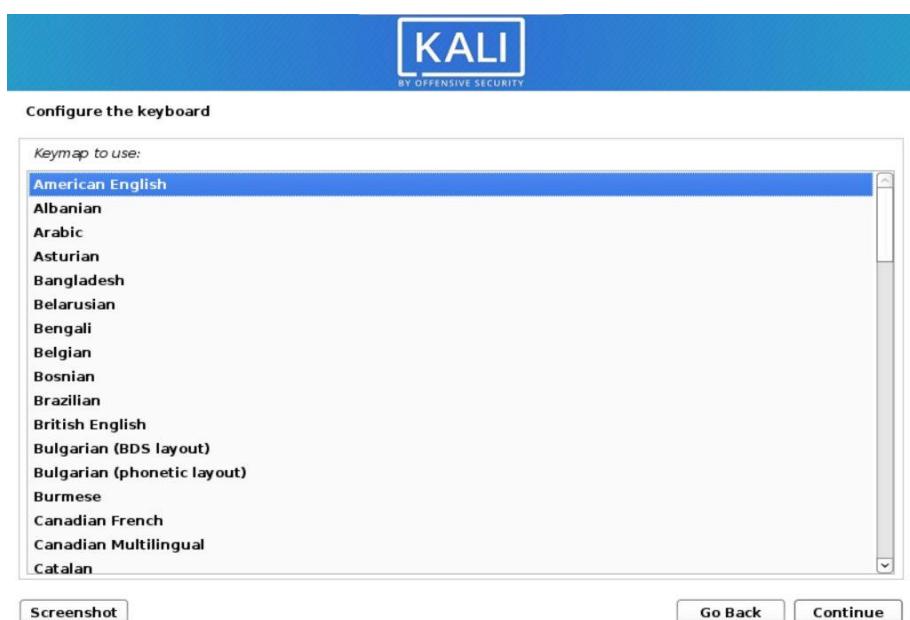
or F12 (depends on your computer) function key on your keyboard to enter the boot menu then choose your USB drive to boot into.

Step 3: Start the installation

The Kali USB installer unlike many Linux distro's does not come with a version of the operating system already installed on the USB drive called "live USB". If you would like to run Kali as a live USB you will need to create a bootable USB from the live ISO available on the Kali Downloads page.

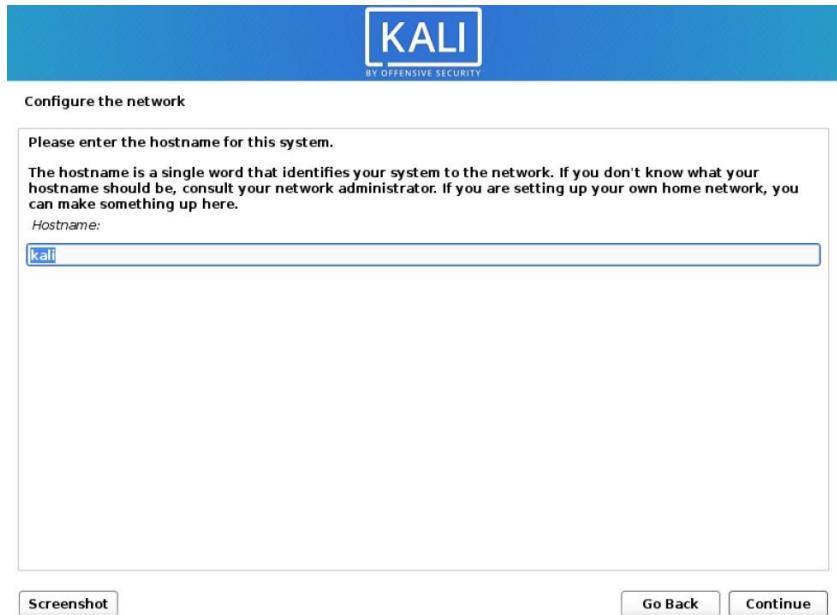


You can choose "Graphical install" to get started; If you run into any problems then select the regular "Install" option.

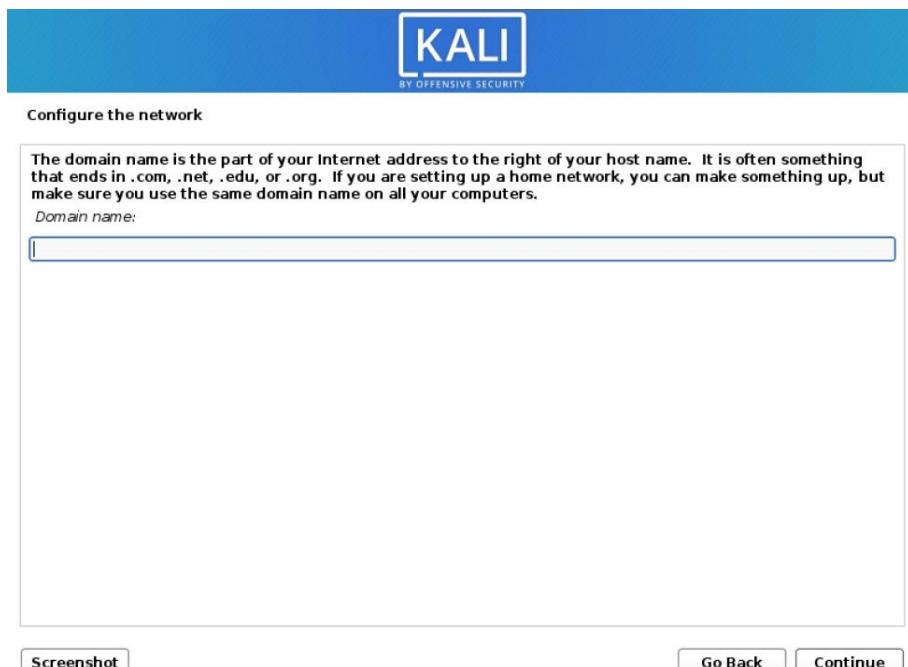


Next, pick your desired language and click continue. Then choose your location before you continue; then choose your keyboard layout and go through any other options you are prompted with.

Step 4: Choose some options

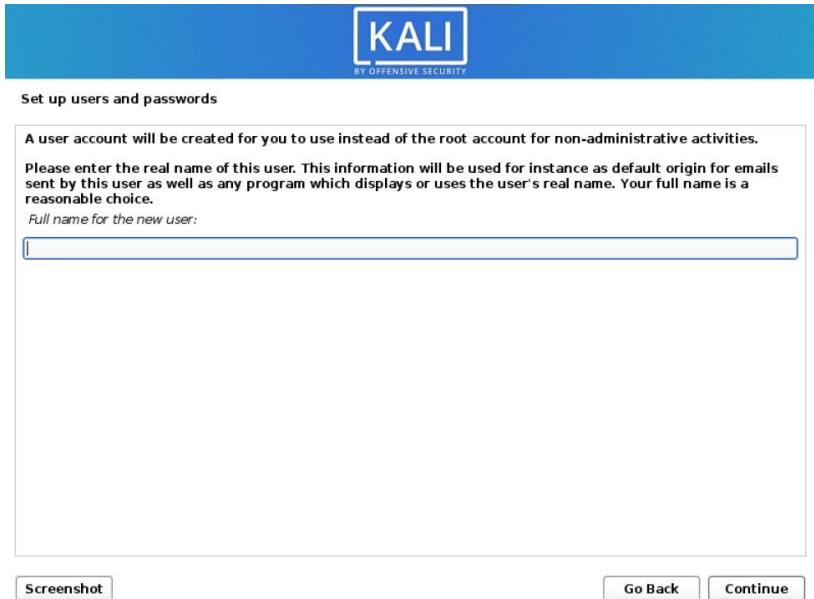


Enter your desired hostname then move on to the next option; a hostname is what identified your computer to the network you connect to.



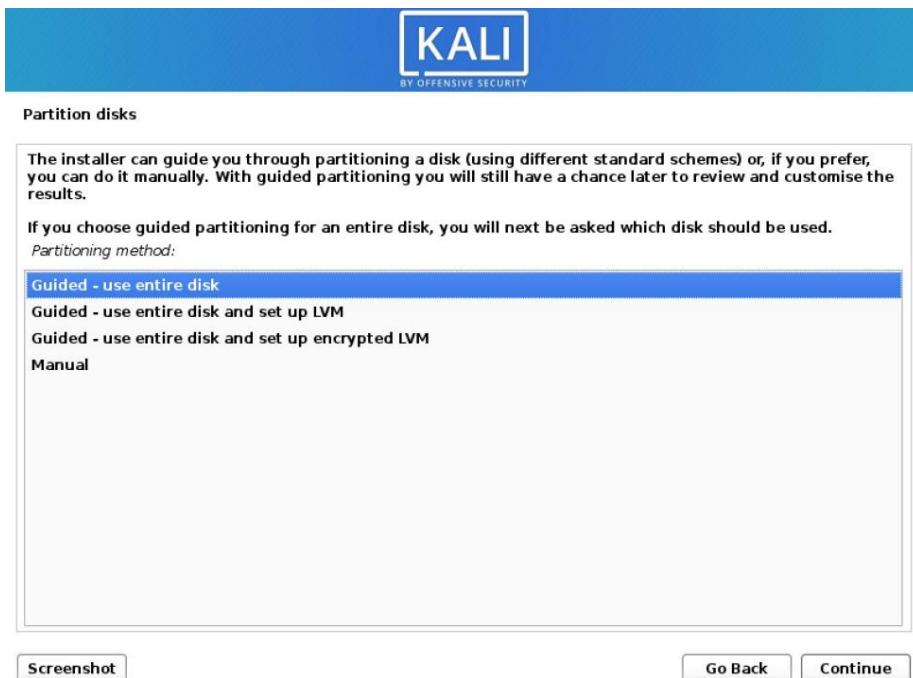
Enter a domain name here if you would like to or leave it blank if you do not have one;

Since Kali 2020.1 you are required to create a Non-Root user which will serve as the default user instead of the traditional root from versions of Kali prior to 2020.1. After installation, if you prefer to use Root you can activate it and set a password if that is the direction you would like to go.



For now enter your desired name, followed by a username, and finally a password.

Step 5: Partition the Drive

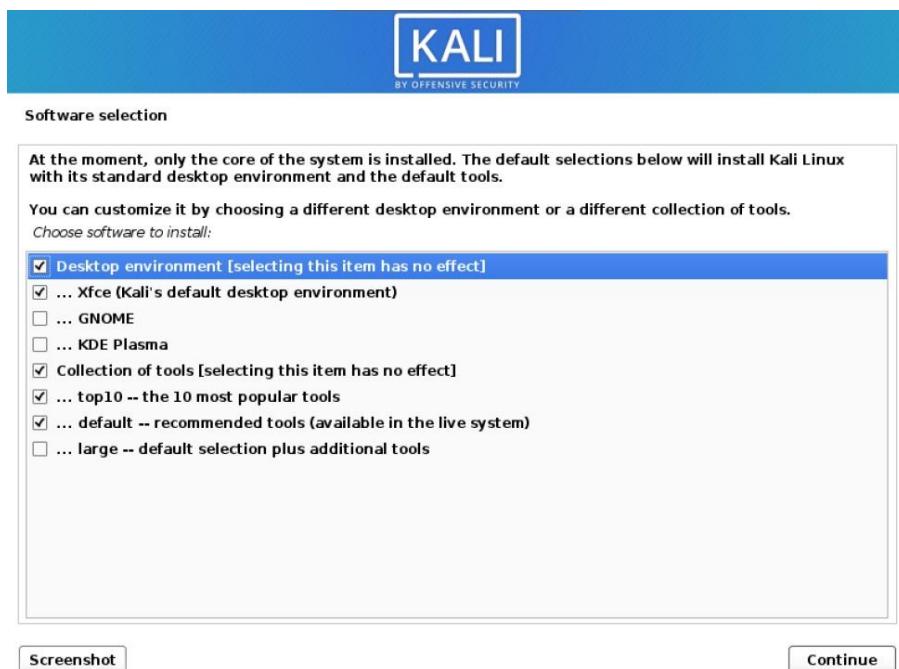


Here you may choose partition options and you may choose to enable and configure whole disk encryption or LVM (logical volume management) or customize your partitions to your own liking. For most people, the default options are probably going to be just fine. Click continue then follow the onscreen instructions to confirm the partition you have chosen.

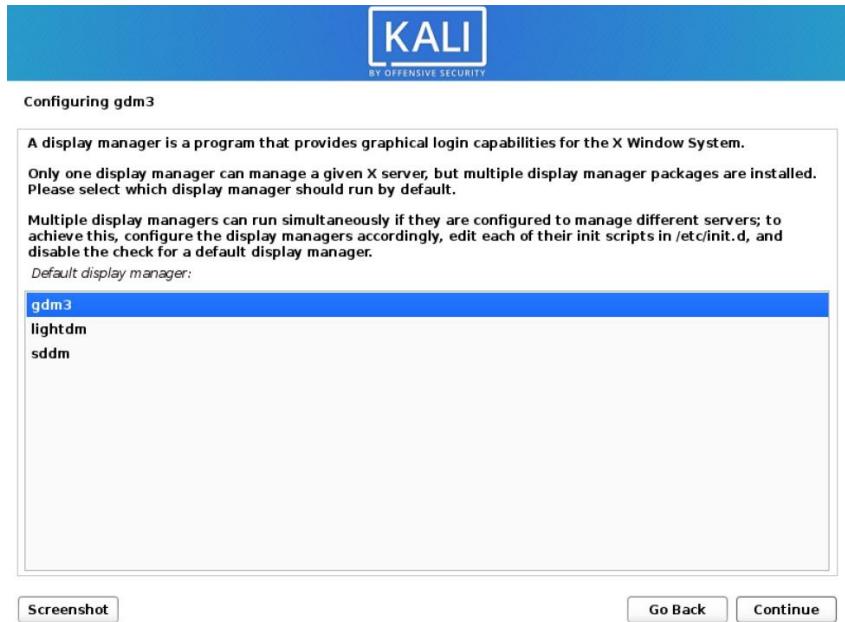
Step 6: Finalize the Installation



Your installation has begun now, note that this will take several minutes depending on how fast your system is.



You will be prompted with some software options, which include desktop environments, and what tools you would like to install. Do note that you can install these tools later should you change your mind. Or find that you require more tools than you originally had chosen at installation. XFCE is Kali's default desktop environment, but you can choose GNOME or KDE plasma if you prefer.



Shortly after you may be prompted to choose a display manager. This may occur if you have chosen to install more than one desktop environment. Select whichever display manager you like best and click continue.

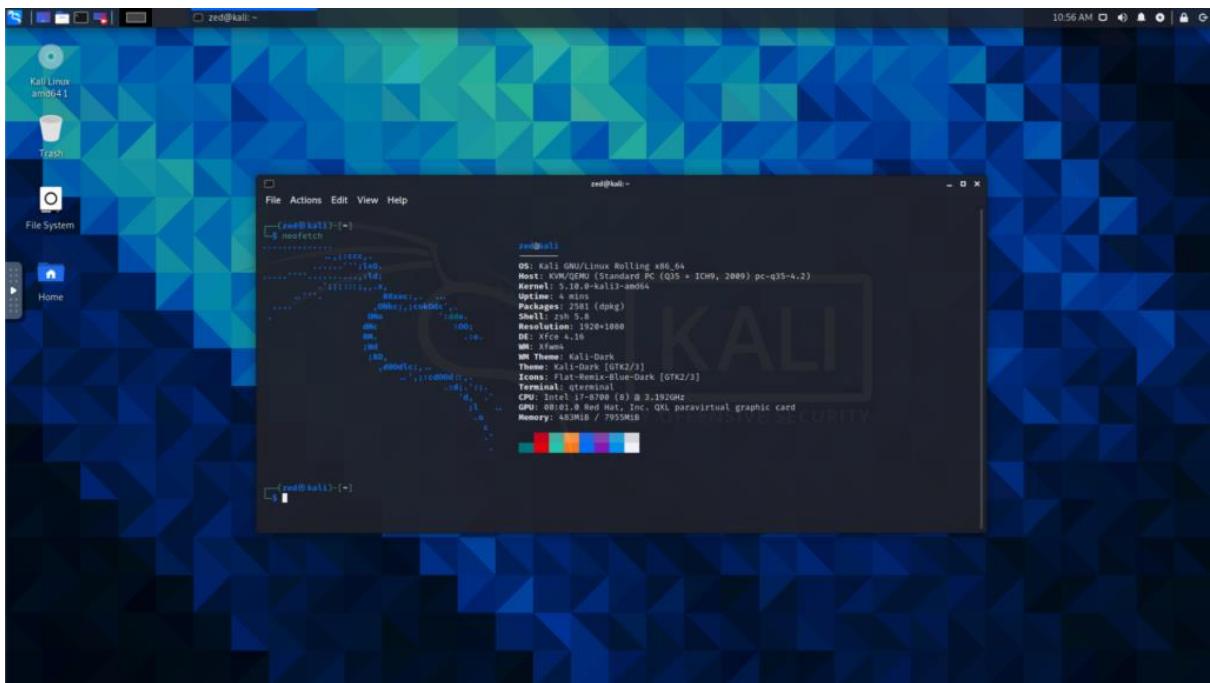


The installation will then continue; this should take a few more minutes depending on how fast your system is. When your installation is complete you will be prompted to restart your system. Click continue and in no time you will be greeted with a login prompt.

Welcome to your Desktop;



Your installation does not immediately boot up, it does require that you first key in a username and password. Use the username and password you set earlier during setup;



Now that you have installed Kali Linux you can log in. Next, you will be greeted by the desktop environment that you have chosen during installation.

EXPERIMENT -03

Aim: Arp spoofing attack & Mitm Attack using Bettercap Tool

Theory: Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works –

- When one machine needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the **ARP_request** is broadcasted over the network.
- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine.

- ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
- The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.

A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

Practical:

Step1: Check Attacker's IP(Kali Linux) & MAC Address (ether)

```
ach@hv: ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.64.133 netmask 255.255.255.0 broadcast 192.168.64.255
        inet6 fe80::20c:29ff:feb0:5907 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:b0:59:07 txqueuelen 1000 (Ethernet)
                RX packets 3537 bytes 1375006 (1.3 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 23379 bytes 2717453 (2.5 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 6257 bytes 661690 (646.1 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 6257 bytes 661690 (646.1 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step2: Check Victim's IP (Windows 7)

```
C:\ Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\maleficient>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : Dlink
IPv6 Address . . . . . : 2405:201:400e:4d68:95b2:5710:24c9:1693
Temporary IPv6 Address . . . . . : 2405:201:400e:4d68:3017:39c:df1e:ab6e
Link-local IPv6 Address . . . . . : fe80::95b2:5710:24c9:1693%11
IPv4 Address . . . . . : 192.168.29.189
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::461c:a8ff:fe78:726a%11
                           192.168.29.1

Tunnel adapter isatap.{869534DF-5479-47F5-8C43-15D33CA58191}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : Dlink
```

Step3: From attacker's machine, run the tool (sudo bettercap -iface eth0). This command will execute the code of the bettercap tool and you just have to select your interface.

```

ach@hv: ~ 151x27
└─(ach@hv)─[~]
$ sudo bettercap -iface eth0
bettercap v2.31.1 (built for linux amd64 with go1.15.9) [type 'help' for a list of commands]

192.168.64.0/24 > 192.168.64.133 » [10:52:59] [sys.log] [inf] gateway monitor started ...
192.168.64.0/24 > 192.168.64.133 » ┌

```

Step4: Now by the following command we are gathering information of the devices that are connected in our network.

```

192.168.64.0/24 > 192.168.64.133 » net.probe on
192.168.64.0/24 > 192.168.64.133 » [10:54:36] [sys.log] [inf] net.probe probing 256 addresses on 192.168.64.0/24
192.168.64.0/24 > 192.168.64.133 » [10:54:36] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.64.0/24 > 192.168.64.133 » [10:54:36] [endpoint.new] endpoint 192.168.64.254 detected as 00:50:56:fd:82:d1 (VMware, Inc.)
192.168.64.0/24 > 192.168.64.133 » [10:54:36] [endpoint.new] endpoint 192.168.64.1 detected as 00:50:56:c0:00:08 (VMware, Inc.)
192.168.64.0/24 > 192.168.64.133 » [10:54:36] [endpoint.new] endpoint 192.168.64.134 detected as 00:0c:29:77:43:fe (VMware, Inc.)
192.168.64.0/24 > 192.168.64.133 » ┌

```

Step5: The following command will show the connected devices in that network in a tabular view. From here you can select the victim.

```

192.168.64.0/24 > 192.168.64.133 » net.show



| IP ▲           | MAC               | Name            | Vendor       | Sent   | Recv   | Seen     |
|----------------|-------------------|-----------------|--------------|--------|--------|----------|
| 192.168.64.133 | 00:0c:29:b0:59:07 | eth0            | VMware, Inc. | 0 B    | 0 B    | 10:52:59 |
| 192.168.64.2   | 00:50:56:ed:25:74 | gateway         | VMware, Inc. | 5.7 kB | 3.1 kB | 10:52:59 |
| 192.168.64.1   | 00:50:56:c0:00:08 | LAPTOP-DFS28409 | VMware, Inc. | 2.2 kB | 1.3 kB | 10:55:00 |
| 192.168.64.134 | 00:0c:29:77:43:fe |                 | VMware, Inc. | 4.0 kB | 7.5 kB | 10:54:53 |
| 192.168.64.254 | 00:50:56:fd:82:d1 |                 | VMware, Inc. | 342 B  | 632 B  | 10:54:52 |


↑ 53 kB / ↓ 155 kB / 3064 pkts

```

Step6: We have to turn the ful duplex mode on, so that we can intercept the traffic of our router and the victim at the same time. Also we select our target (192.168.64.134) or the list of targets to whom we want to attack. Finally turn on the arp spoofing to execute the attack.

```

192.168.64.0/24 > 192.168.64.133 » set arp.spoof.fullduplex true
192.168.64.0/24 > 192.168.64.133 » set arp.spoof.targets 192.168.64.134
192.168.64.0/24 > 192.168.64.133 » arp.spoof on
[10:56:14] [sys.log] [inf] arp.spoof enabling forwarding
192.168.64.0/24 > 192.168.64.133 » [10:56:14] [sys.log] [inf] arp.spoof arp spoofing started, probing 1 targets.
192.168.64.0/24 > 192.168.64.133 » [10:56:14] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.64.0/24 > 192.168.64.133 » ┌

```

Step7: If we go and check the victim's PC, we found that the mac address of the gateway/router(192.168.64.2) and the attacker(192.168.64.133) are same. It means arp spoofing successfully executed.

```

C:\ Command Prompt
C:\Users\maleficient>arp -a

Interface: 192.168.29.189 --- 0xb
  Internet Address      Physical Address          Type
  192.168.29.1           44-1c-a8-78-72-6a    dynamic
  192.168.29.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.252             01-00-5e-00-00-fc    static
  255.255.255.255        ff-ff-ff-ff-ff-ff    static

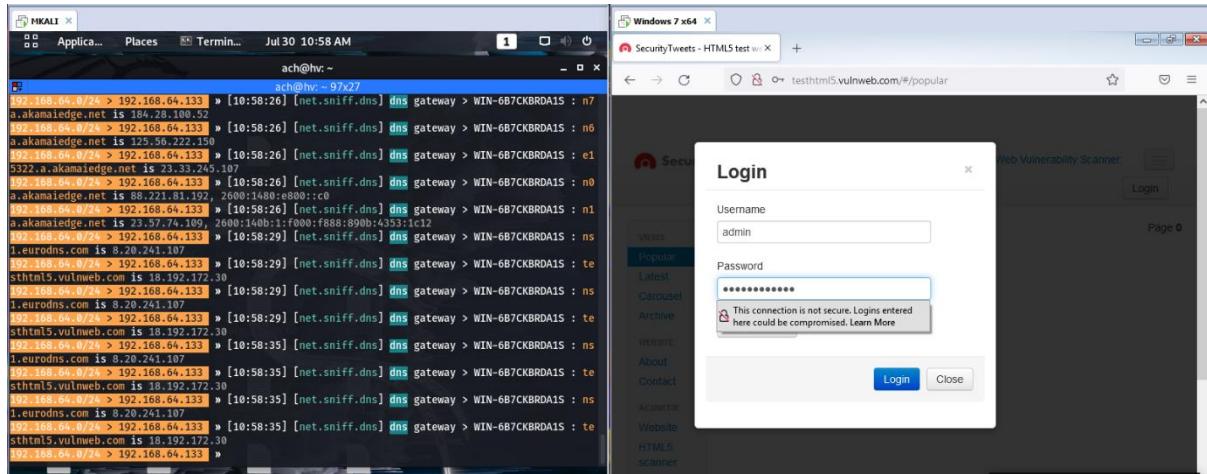
C:\Users\maleficient>_

```

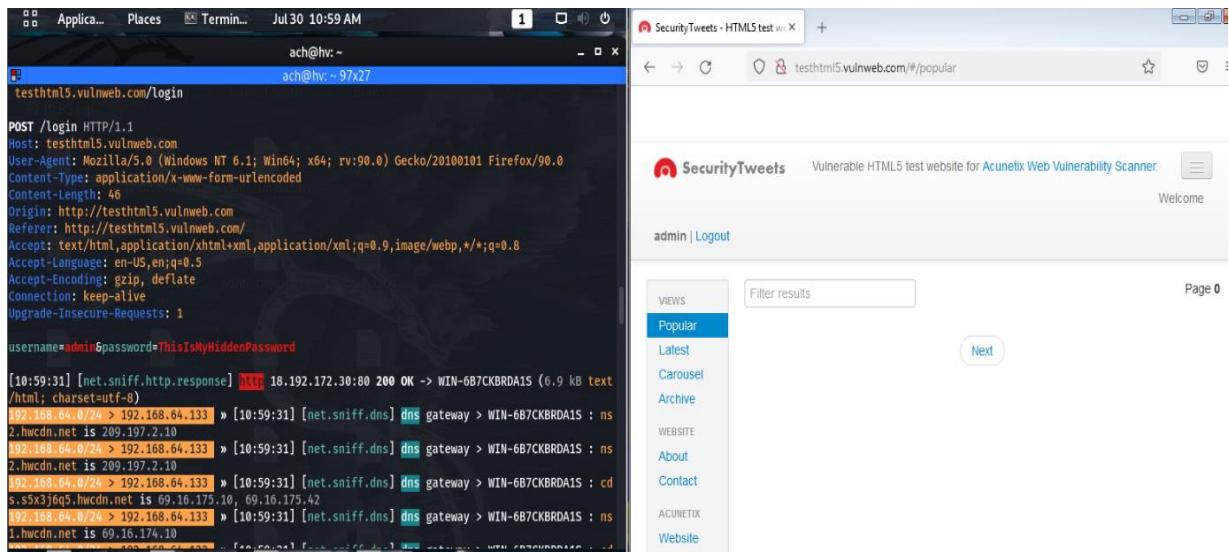
Step8: Now in this final step we only have to turn on the sniffer which will sniff packets of the victim and acts as a mitm (man in the middle) attack.

192.168.64.0/24 > 192.168.64.133 » net.sniff on

Step9: Now if the victim enters his credentials in his browser that information also goes to attacker first then to the router.



Step10: Credentials intercepted as you can see the account and password of the victim in clear text format.



EXPERIMENT -04

Aim: DNS (Domain name System) poisioning attack using Bettercap Tool

Theory: DNS Spoofing is the result of alterations to a DNS server's records resulting in the malicious redirection of traffic. DNS spoofing can be performed by a direct attack on the DNS server (what we will be talking about here) or through any form of a Man-in-the-Middle attack specifically targeting DNS traffic.

DNS Cache spoofing works explicitly in a way that exploits the way in which DNS communication is structured. When a DNS server attempts to perform a lookup on a domain, it will forward the request along to the root authoritative DNS and iteratively proceed down the chain of DNS servers until it reaches the DNS server authoritative over the domain. Since the local DNS server does not know which server is in charge of which domain, and does not know the full route to each authoritative server, it accepts replies to its queries from anywhere so long as the reply matches the query and is formatted correctly. The attacker can exploit this design by beating the actual Authoritative DNS server in replying to the local DNS server, and if it does so, the local DNS server will use the attacker's DNS record instead of the actual Authoritative answer. Due to the nature of DNS, the local DNS server has no way of determining which reply is real and which is fake.

Steps:

1. Start the windows device and note its IP Address and Subnet Mask using 'ipconfig command'.

```
ca Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\maleficient>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . : Dlink
  IPv6 Address . . . . . : 2405:201:400e:4d68:95b2:5710:24c9:1693
  Temporary IPv6 Address . . . . . : 2405:201:400e:4d68:3017:39c:df1e:ab6e
  Link-local IPv6 Address . . . . . : fe80::95b2:5710:24c9:1693%11
  IPv4 Address . . . . . : 192.168.29.189
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::461c:a8ff:fe78:726a%11
                             192.168.29.1

Tunnel adapter isatap.{869534DF-5479-47F5-8C43-15D33CA58191}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . : Dlink
```

2. Enable Apache Service and open 'etter.dns' file using the command, sudo nano /etc/ettercap/etter.dns.

```

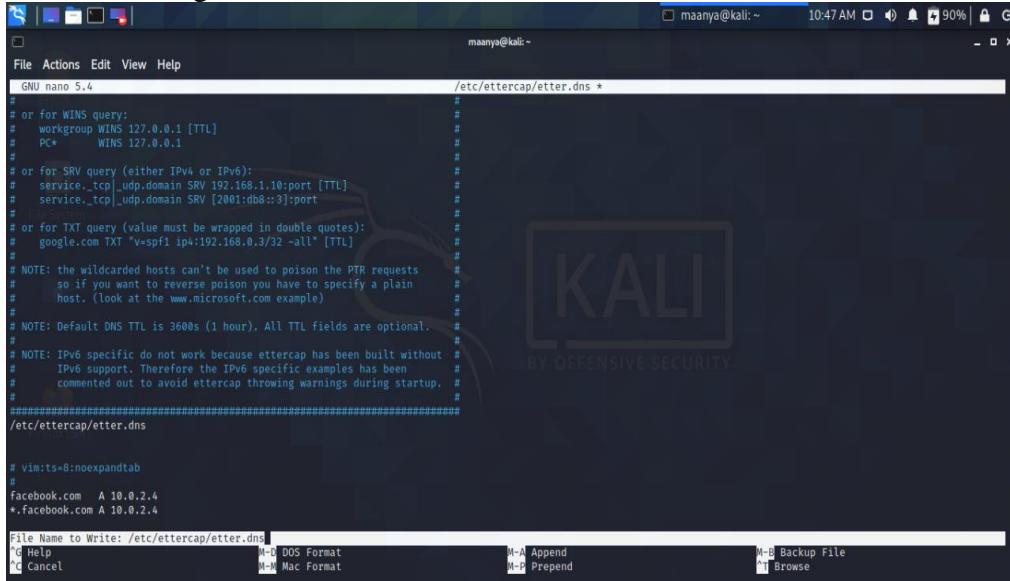
└─(maleficient㉿Maleficient)~]
└─$ sudo service apache2 start
└─(maleficient㉿Maleficient)~]
└─$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.71 netmask 255.255.255.0 broadcast 192.168.29.255
        inet6 2405:201:400e:4d68:a00:27ff:fe9e:dbf3 prefixlen 64 scopeid 0x0<global>
        inet6 2405:201:400e:4d68:27be:ac6c:ac42:139d prefixlen 64 scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe9e:dbf3 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:9e:db:f3 txqueuelen 1000 (Ethernet)
    RX packets 13116 bytes 12190717 (11.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19091 bytes 1446970 (1.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1360 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1360 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

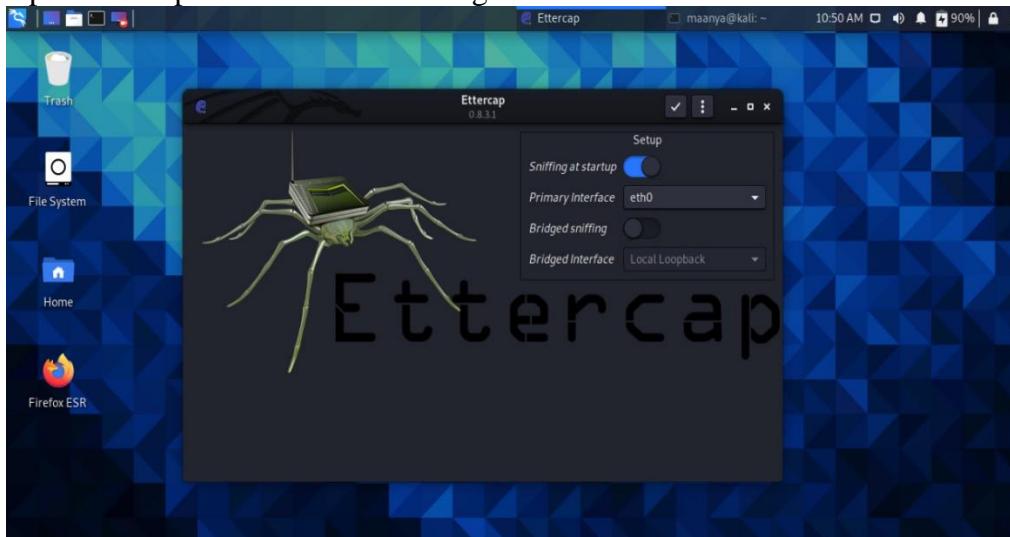
└─(maleficient㉿Maleficient)~]
└─$ sudo nano /etc/ettercap/etter.dns

```

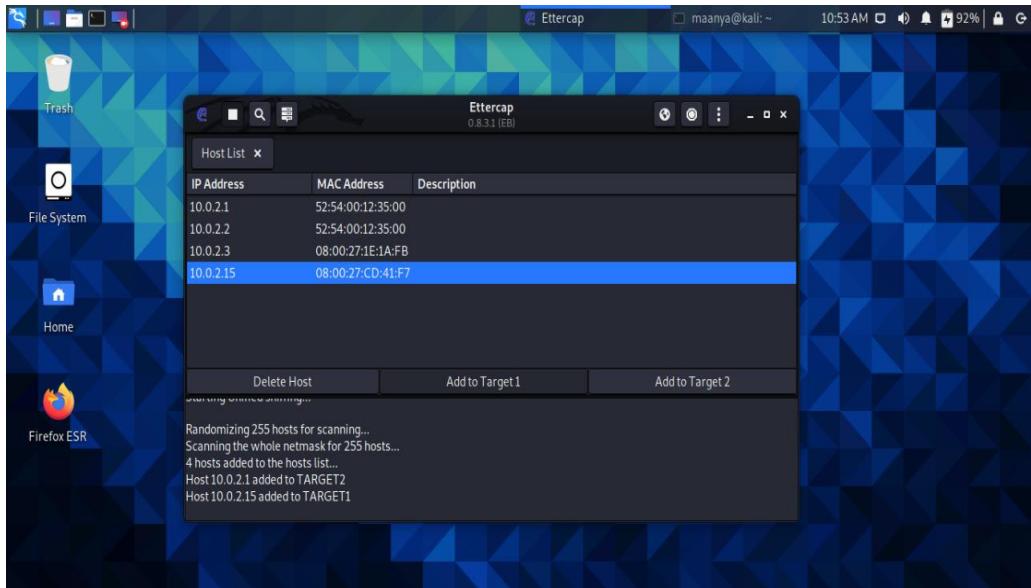
3. Make the changes in dns file.



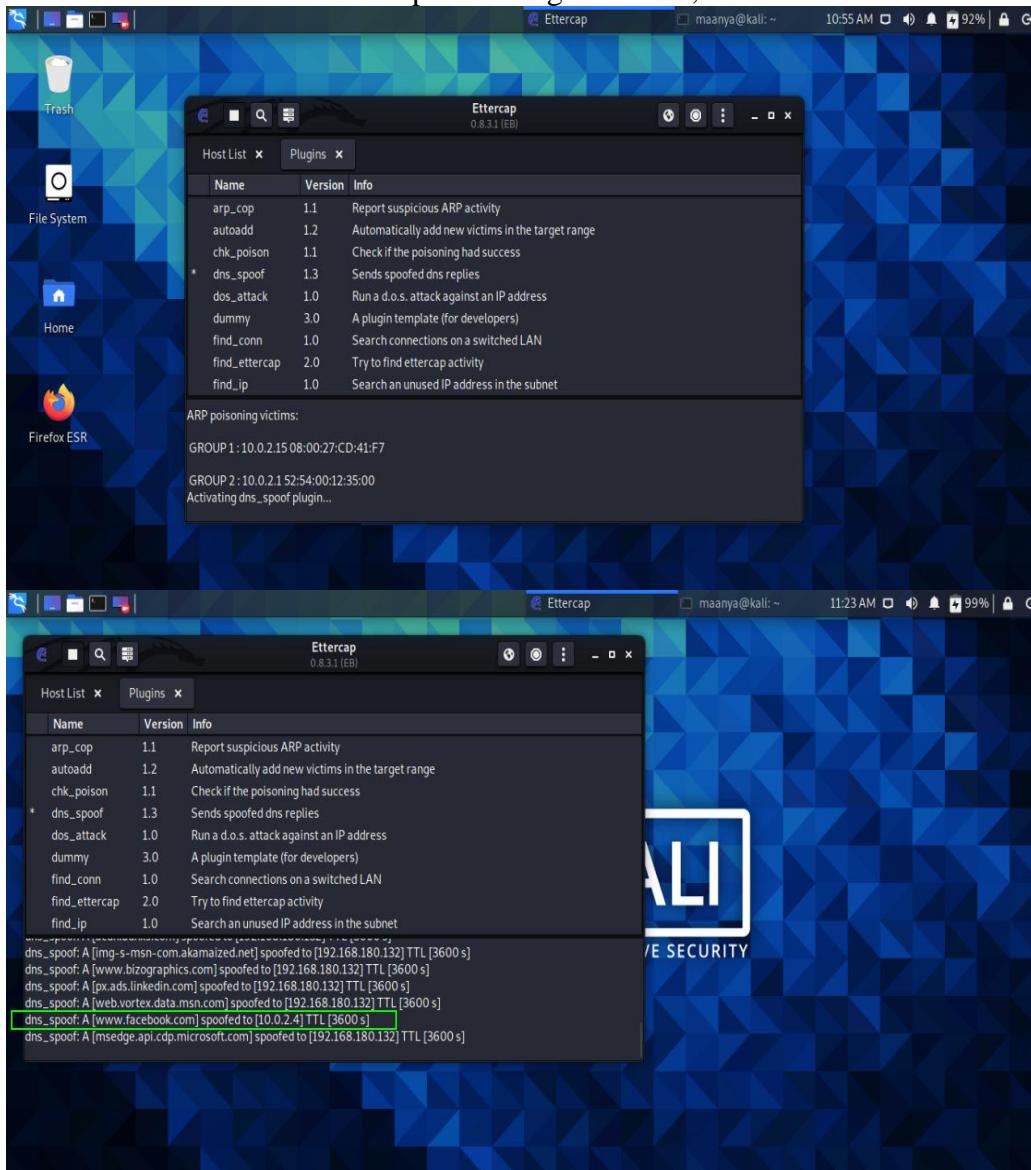
4. Open Ettercap tool and select the target hosts from the scanned hosts list.

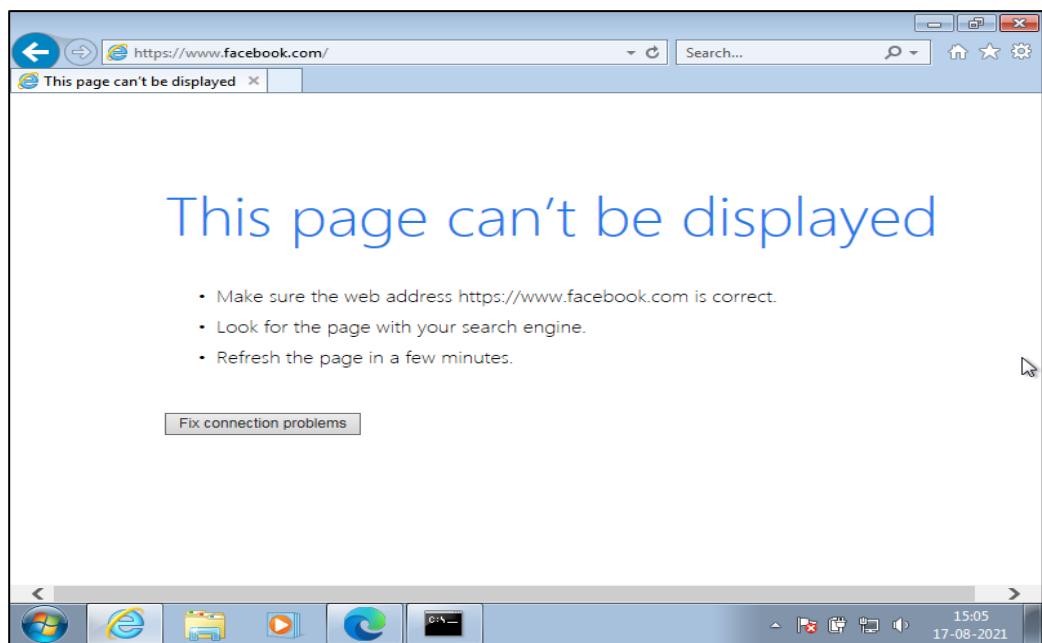


5. Open Plugins and activate the dns spoof plugin by double clicking it.



6. Now in the windows machine open the target website, here Facebook.com.





EXPERIMENT – 05

AIM – To implement different commands using NMAP

Theory

Nmap (“Network Mapper”) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

Nmap is:

- Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more.
- Powerful: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- Easy: While Nmap offers a rich set of advanced features for power users, you can start out as simply as “nmap -v -A targethost”. Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.

Steps:

1. Start the nmap tool in the terminal by writing the command sudo nmap.
2. To Scan a System with Hostname and IP address write the command in the terminal sudo nmap google.com or give the IP address of the desired target.
3. We can use -v command to get more detailed information about the remote machines.
4. Nmap also have the feature to scan multiple hosts at a time. Command used: sudo nmap <multiple IP addresses of different websites>.
5. Nmap can also be used to identify hostnames of the given IP's by using the command sudo nmap -sL <Random IP Adress>.
6. Nmap also have a command -A which indicates Aggressive it will let Us Know The Extra Information's like OS Detection (-O), version detection, script scanning (-sC),

and traceroute (-traceroute) even it provides a lot of valuable information About The Host.

7. Implement all the above mentioned commands in the Kali Linux Terminal.

```
maleficient@Maleficient: ~
maleficient@Maleficient: ~ 98x29
(maleficient@Maleficient)[~]
$ sudo nmap -h
[sudo] password for maleficient:
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
DST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
(maleficient@Maleficient)[~]
$ sudo nmap google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 20:38 IST
Nmap scan report for google.com (142.250.192.174)
Host is up (0.016s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:829::200e
rDNS record for 142.250.192.174: del11s11-in-f14.1e100.net
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

```
[(maleficient㉿Maleficient)-[~]
$ sudo nmap 172.217.27.174
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 20:39 IST
Nmap scan report for kix05s07-in-f174.1e100.net (172.217.27.174)
Host is up (0.046s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 12.68 seconds
```

```
[(maleficient㉿Maleficient)-[~]
$ sudo nmap -v www.google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 20:40 IST
Initiating Ping Scan at 20:40
Scanning www.google.com (142.250.76.164) [4 ports]
Completed Ping Scan at 20:40, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:40
Completed Parallel DNS resolution of 1 host. at 20:40, 0.02s elapsed
Initiating SYN Stealth Scan at 20:40
Scanning www.google.com (142.250.76.164) [1000 ports]
Discovered open port 554/tcp on 142.250.76.164
Discovered open port 80/tcp on 142.250.76.164
Discovered open port 1723/tcp on 142.250.76.164
Discovered open port 21/tcp on 142.250.76.164
Discovered open port 443/tcp on 142.250.76.164
Completed SYN Stealth Scan at 20:40, 4.87s elapsed (1000 total ports)
Nmap scan report for www.google.com (142.250.76.164)
Host is up (0.028s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.76.164: bom12s09-in-f4.1e100.net
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.14 seconds
    Raw packets sent: 2002 (88.064KB) | Rcvd: 36 (1.500KB)
```

```
(maleficient㉿Maleficient)-[~]
└─$ sudo nmap 103.76.228.244 157.248.198.35 172.217.27.174
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 20:41 IST
Nmap scan report for cs-mum-21.webhostbox.net (103.76.228.244)
Host is up (0.040s latency).
Not shown: 978 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    open     smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
139/tcp   filtered netbios-ssn
143/tcp   open     imap
179/tcp   filtered bgp
443/tcp   open     https
445/tcp   filtered microsoft-ds
465/tcp   open     smtps
554/tcp   open     rtsp
587/tcp   open     submission
646/tcp   filtered ldp
993/tcp   open     imaps
995/tcp   open     pop3s
1723/tcp  open     pptp
2222/tcp  open     EtherNetIP-1
2525/tcp  filtered ms-v-worlds
3306/tcp  open     mysql

Nmap scan report for kix05s07-in-f174.1e100.net (172.217.27.174)
Host is up (0.014s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open     ftp
80/tcp    open     http
443/tcp   open     https
554/tcp   open     rtsp
1723/tcp  open     pptp
```

```
(maleficient㉿Maleficient)-[~]
└─$ sudo nmap -sL 103.76.228.244
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 20:42 IST
Nmap scan report for cs-mum-21.webhostbox.net (103.76.228.244)
Nmap done: 1 IP address (0 hosts up) scanned in 0.33 seconds
```

```
(maleficient㉿Maleficient)-[~]
$ sudo nmap -A www.geeksforgeeks.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 20:43 IST
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.00% done; ETC: 20:47 (0:01:37 remaining)
Nmap scan report for www.geeksforgeeks.org (49.44.95.138)
Host is up (0.011s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1604::312c:5f8a 2405:200:1604::312c:3250 49.44.50.80
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
80/tcp    open  http   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-title: Access Denied
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-server-header: nginx
|_http-title: Access Denied
| ssl-cert: Subject: commonName=www.geeksforgeeks.org
| Subject Alternative Name: DNS:api.geeksforgeeks.org, DNS:auth.geeksforgeeks.org, DNS:authcdn.geeksforgeeks.org, DNS:cdncontribute.geeksforgeeks.org, DNS:cdnpractice.geeksforgeeks.org, DNS:cdnvideas.geeksforgeeks.org, DNS:contribute.geeksforgeeks.org, DNS:ide.geeksforgeeks.org, DNS:media.geeksforgeeks.org, DNS:practice.geeksforgeeks.org, DNS:www.geeksforgeeks.org
| Not valid before: 2021-08-09T12:27:32
| Not valid after:  2021-11-07T12:27:30
|_ssl-date: TLS randomness does not represent time
  tls-alpn:
    http/1.1
  - http/1.0
  tls-nextprotoneg:
    http/1.1
  - http/1.0
554/tcp   open  rtsp?
1723/tcp  open  pptp?
|_pptp-version: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|load balancer
Running (JUST GUESSING): FreeBSD 6.X (90%), F5 Networks embedded (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (90%), F5 BIG-IP Edge Gateway (86%)
```

EXPERIMENT – 06

AIM – To perform vulnerability scanning using Nessus tool.

Theory

What is Nessus?

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Why Nessus?

If you are familiar with other network vulnerability scanners, you might be wondering what advantages Nessus has over them. Key points include:

- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.
- Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. Its also provides a plug-in interface, and many free plug-ins are available from the Nessus plug-in site. These plugs are often specific to detecting a common virus or vulnerability.
- Up to date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize the window between an exploit appearing in the wild, and you being able to detect it with Nessus.
- Open-source. Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.
- Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

STEPS:

- 1) Create a Scan. To create a scan go to top navigation bar and click Scans or go to upper right corner of the My Scans page, click on the New Scan button.
- 2) Choose a Scan Template. Click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set.
- 3) Configure Scan Settings.

Practical

OUTPUT:

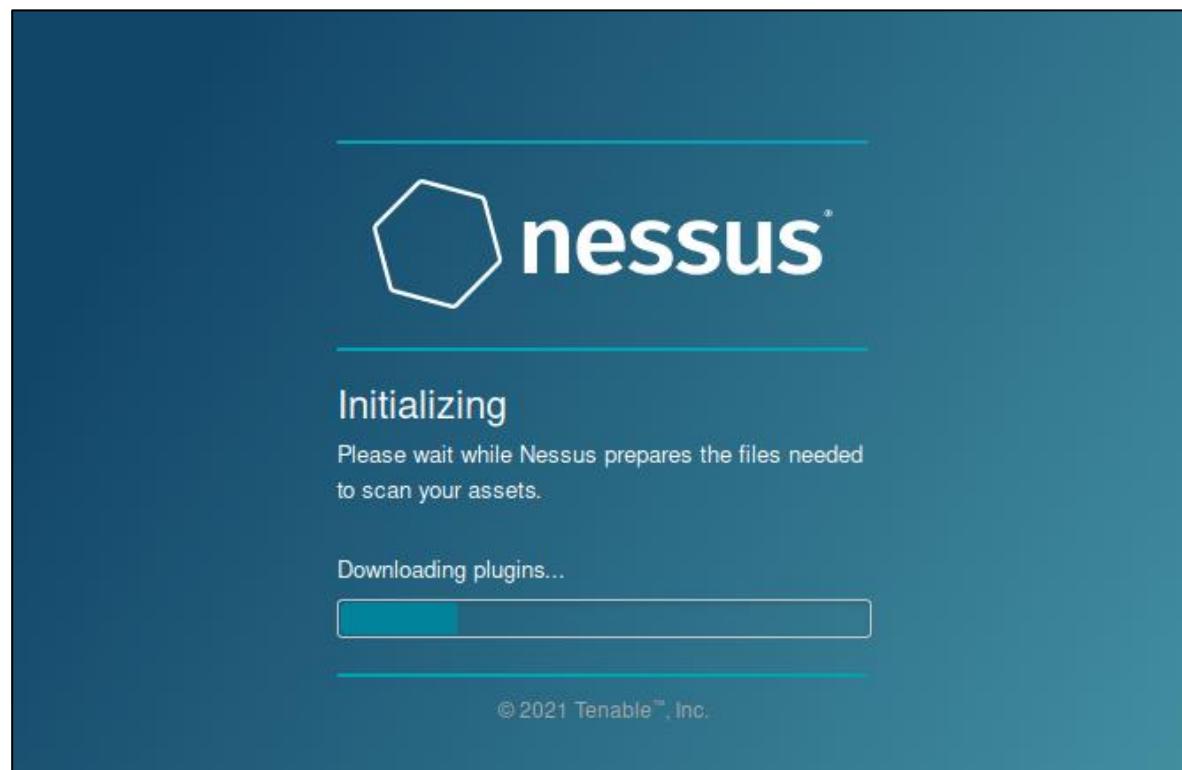
```
maleficient@Maleficient: ~/Downloads
(maleficient@Maleficient)-[~]
$ cd Downloads

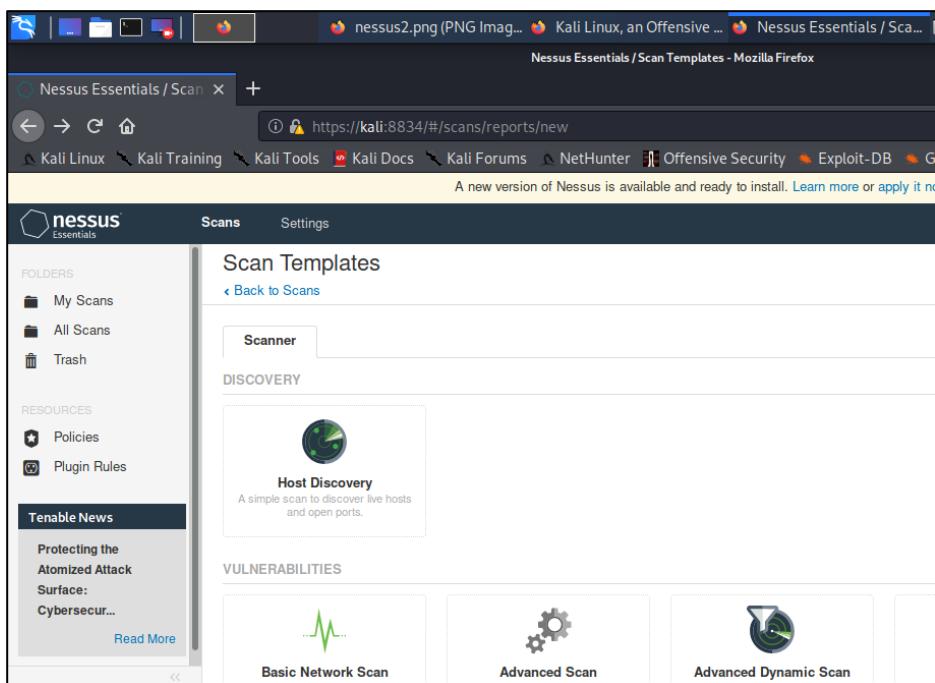
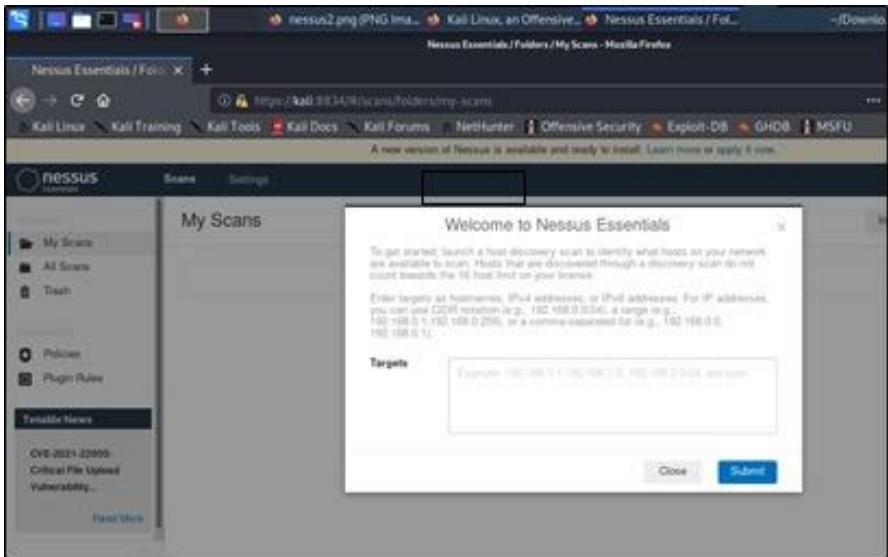
(maleficient@Maleficient)-[~/Downloads]
$ ls
brainpan.exe          'Nessus-8.15.2-debian6_i386(1).deb'
Nessus-8.15.2-debian6_amd64.deb  Nessus-8.15.2-debian6_i386.deb

(maleficient@Maleficient)-[~/Downloads]
$ sudo dpkg -i Nessus-8.15.2-debian6_amd64.deb
[sudo] password for maleficient:
Selecting previously unselected package nessus.
(Reading database ... 394099 files and directories currently installed.)
Preparing to unpack Nessus-8.15.2-debian6_amd64.deb ...
Unpacking nessus (8.15.2) ...
Setting up nessus (8.15.2) ...
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://Maleficient:8834/ to configure your scanner

(maleficient@Maleficient)-[~/Downloads]
$ /bin/systemctl start nessusd.service
```





Nessus Essentials / Folders / My Scans - Mozilla Firefox

Kali Linux, an Offensive Secu ✎ Nessus Essentials / Fold... +

https://kali:8834/#/scans/folders/my-scans

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

nessus Essentials

Scans Settings

My Scans

Import New Folder + New Scan

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules

Tenable News

Multiple Vulnerabilities in LandAirSea SilverCloud... [Read More](#)

Search Scans 1 Scan

Name	Schedule	Last Modified
ITNS LAB	On Demand	N/A

Nessus Essentials / Folders / View Scan - Mozilla Firefox

Kali Linux, an Offensive Secu ✎ Nessus Essentials / Fold... +

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

nessus Essentials

Scans Settings

Vulnerabilities 22

Filter Search Vulnerabilities 22 Vulnerabilities

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules

Tenable News

Spotlight on the Kingdom of Saudi Arabia: The New ... [Read More](#)

Sev	Name	Family	Count	Actions
MIXED	SSL (Multiple Issues)	General	5	○ ⚒
INFO	SSH (Multiple Issues)	General	3	○ ⚒
INFO	HTTP (Multiple Issues)	Web Servers	2	○ ⚒
INFO	TLS (Multiple Issues)	Service detection	2	○ ⚒
INFO	Service Detection	Service detection	2	○ ⚒
INFO	Authenticated Check : OS Name and I...	Settings	1	○ ⚒
INFO	Common Platform Enumeration (CPE)	General	1	○ ⚒

Host Details

IP: 192.168.1.2
MAC: 08:00:27:A6:E6:F4
OS: Linux Kernel 5.7.0-kali3-amd64
Start: Today at 11:01 AM
End: Today at 11:02 AM
Elapsed: a minute
KB: [Download](#)

Vulnerabilities

Critical (Red) High (Orange) Medium (Yellow)

EXPERIMENT – 07

AIM – To implement different commands using Metasploit.

Theory

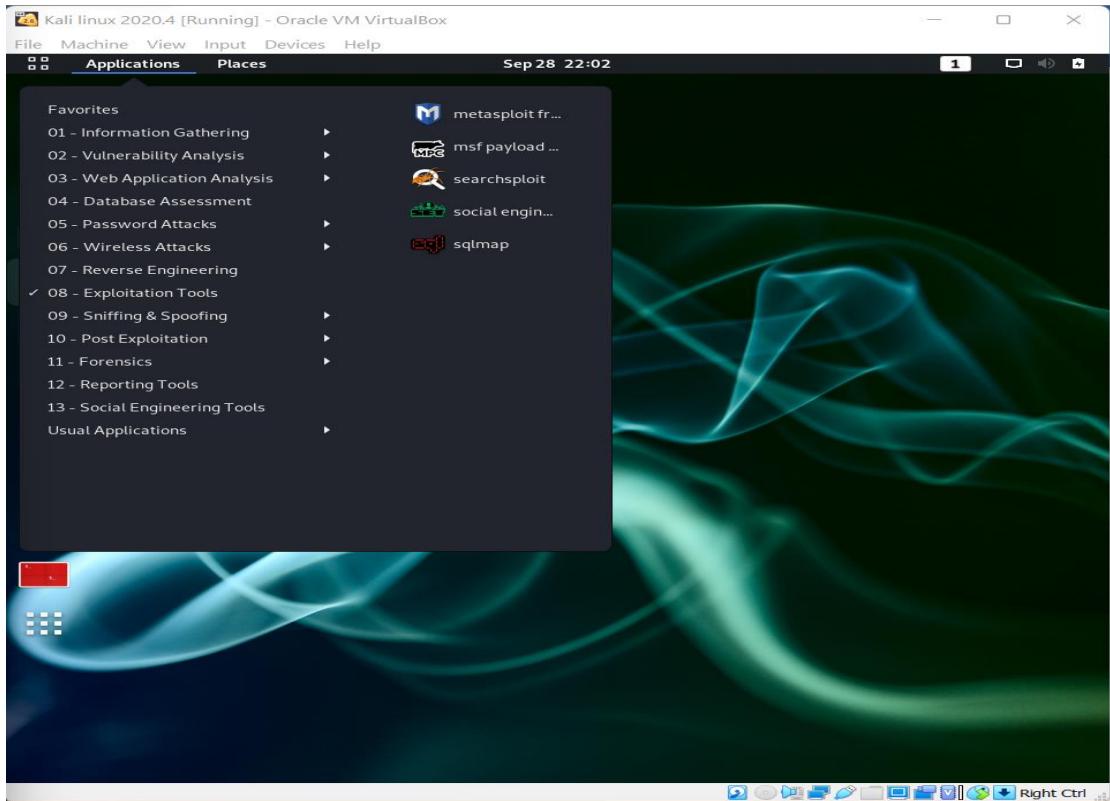
The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

Metasploit now includes more than 1677 exploits organized over 25 platforms, including Android, PHP, Python, Java, Cisco, and more. The framework also carries nearly 500 payloads, some of which include:

- Command shell payloads that enable users to run scripts or random commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
- Static payloads that enable port forwarding and communications between networks.

Steps to perform basic commands:

- 1) First of all, open the Metasploit console in Kali. You can do so by following the path: Applications → Exploitation Tools → Metasploit.



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

```
Terminal
> Executing "sudo msfdb init && msfconsole"
[sudo] password for maleficient:
[+] Starting database
[i] The database appears to be already configured, skipping initialization

      _   _ 
     ((_) o o (_)) 
    \_o_o\ \ M S F  | \
    |||   |_____| / * 
    |||   |WW| | / \ 

=[ metasploit v6.0.15-dev ] 
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post ] 
+ -- --=[ 592 payloads - 45 encoders - 10 nops ] 
+ -- --=[ 7 evasion ] 

Metasploit tip: View advanced module options with advanced

msf6 >
```

- ### 3) Help command

```
msf6 > help

Core Commands
=====
Command      Description
-----      -----
?            Help menu
banner       Display an awesome metasploit banner
cd           Change the current working directory
color         Toggle color
connect      Communicate with a host
debug        Display information useful for debugging
exit         Exit the console
features     Display the list of not yet released features that can be opte
d in to
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
history      Show command history
load         Load a framework plugin
quit         Exit the console
repeat       Repeat a list of commands
route        Route traffic through a session
save         Saves the active datastores
sessions    Dump session listings and display information about sessions
set          Sets a context-specific variable to a value
setg         Sets a global variable to a value
sleep        Do nothing for the specified number of seconds
spool        Write console output into a file as well the screen
threads     View and manipulate background threads
tips         Show a list of useful productivity tips
unload      Unload a framework plugin
unset        Unsets one or more context-specific variables
unsetg      Unsets one or more global variables
version     Show the framework and console library version numbers

Module Commands
=====
```

4) Search Command

```
msf6 > search name:microsoft type:exploit

Matching Modules
=====
#      Name                               Date    Rank     Check  Description
#      ----                               ----    ---     ----  -----
#      0      exploit/multi/fileformat/office_word_macro          2012-01-10
#           excellent  No      Microsoft Office Word Malicious Macro Execution
#      1      exploit/windows/brightstor/sql_agent            2005-08-02
#           average   No      CA BrightStor Agent for Microsoft SQL Overflow
#      2      exploit/windows/browser/ie_cbutton_uaf          2012-12-27
#           normal    No      MS13-008 Microsoft Internet Explorer CButton Object Use-
#           After-Free Vulnerability
#      3      exploit/windows/browser/ie_cgenericelement_uaf        2013-05-03
#           good     No      MS13-038 Microsoft Internet Explorer CGenericElement Obj
#           ect Use-After-Free Vulnerability
#      4      exploit/windows/browser/ie_createobject          2006-04-11
#           excellent No      MS06-014 Microsoft Internet Explorer COM CreateObject Co
#           de Execution
#      5      exploit/windows/browser/ie_execcommand_uaf          2012-09-14
#           good     No      MS12-063 Microsoft Internet Explorer execCommand Use-Aft
#           er-Free Vulnerability
#      6      exploit/windows/browser/ie_iscomponentinstalled        2006-02-24
#           normal    No      Microsoft Internet Explorer isComponentInstalled Overflo
#           w
#      7      exploit/windows/browser/ie_setmousecapture_uaf        2013-09-17
#           normal    No      MS13-080 Microsoft Internet Explorer SetMouseCapture Use
#           -After-Free
#      8      exploit/windows/browser/ie_unsafe_scripting          2010-09-20
#           manual   No      Microsoft Internet Explorer Unsafe Scripting Misconfigur
#           ation
#      9      exploit/windows/browser/ms03_020_ie_objecttype          2003-06-04
#           normal    No      MS03-020 Microsoft Internet Explorer Object Type
#      10     exploit/windows/browser/ms05_054_onload            2005-11-21
#           normal    No      MS05-054 Microsoft Internet Explorer JavaScript OnLoad H
#           andler Remote Code Execution
#      11     exploit/windows/browser/ms06_013_createtextrange        2006-03-19
#           normal    No      MS06-013 Microsoft Internet Explorer createTextRange() C
#           ode Execution
#      12     exploit/windows/browser/ms06_055_vml_method          2006-09-19
#           normal    No      MS06-055 Microsoft Internet Explorer VML Fill Method Cod
```

5) Info Command

```
msf6 > info auxiliary/admin/http/iis_auth_bypass

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

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

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
----      -----          -----  -----
Proxies          no          A proxy chain of format type:host:port[, type:host:port][...]
RHOSTS         yes          The target host(s), range CIDR identifier
r, or hosts file with syntax 'file:<path>'
RPORT          80          yes          The target port (TCP)
SSL            false         no          Negotiate SSL/TLS for outgoing connectio
ns
TARGETURI      /           yes          The URI directory where basic auth is en
abled
VHOST          no          HTTP server virtual host

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

References:
https://cvedetails.com/cve/CVE-2010-2731/
OSVDB (66160)
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2010/MS10-065
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-byp
ass-by-using-i30index_allocation/
msf6 > 
```

Steps to Perform Scanning for open ports on the client machine with Metasploit:

```
maleficient@Maleficient: ~/Downloads
[maleficient@Maleficient] ~ [~/Downloads]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.71 netmask 255.255.255.0 broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe9e:dbf3 prefixlen 64 scopeid 0x20<link>
        inet6 2405:201:400e:4ddb:a00:27ff:fe9e:dbf3 prefixlen 64 scopeid 0x0<g
local>
    inet6 2405:201:400e:4ddb:b24c:1c19:7b11:7384 prefixlen 64 scopeid 0x0<
global>
    ether 08:00:27:9e:db:f3 txqueuelen 1000 (Ethernet)
    RX packets 76380 bytes 105631263 (100.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24096 bytes 2474792 (2.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 28 bytes 1516 (1.4 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 28 bytes 1516 (1.4 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- 1) We start by launching Metasploit and using the port scanner module.

Msf5 > use auxiliary/scanner/portscan/tcp

- 2) We set the options for this module with ‘show option’.

```

msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

Name      Current Setting  Required  Description
----      -----          -----      -----
CONCURRENCY  10           yes        The number of concurrent ports to che
ck per host
DELAY      0              yes        The delay between connections, per th
read, in milliseconds
JITTER     0              yes        The delay jitter factor (maximum val
ue by which to +/- DELAY) in milliseconds.
PORTS      1-10000         yes        Ports to scan (e.g. 22-25,80,110-900)
RHOSTS    yes            The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
THREADS    1              yes        The number of concurrent threads (max
one per host)
TIMEOUT    1000           yes        The socket connect timeout in millise
conds

msf6 auxiliary(scanner/portscan/tcp) >

```

- 3) We set the RHOSTS with the IP/IP(s) of our client machine and if we want to customize the scan for specific ports we can do that by changing ports.
- Msf5> set PORTS 22,25,80, 110, 21

```

msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21
PORTS => 22,25,80,110,21
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

Name      Current Setting  Required  Description
----      -----          -----      -----
CONCURRENCY  10           yes        The number of concurrent ports to che
ck per host
DELAY      0              yes        The delay between connections, per th
read, in milliseconds
JITTER     0              yes        The delay jitter factor (maximum val
ue by which to +/- DELAY) in milliseconds.
PORTS      22,25,80,110,21  yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS    yes            The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
THREADS    1              yes        The number of concurrent threads (max
one per host)
TIMEOUT    1000           yes        The socket connect timeout in millise
conds

msf6 auxiliary(scanner/portscan/tcp) > 

```

- 4) After running scan we will have an output displaying the open ports on the target client machine we specified earlier.

Combining NMAP with Metasploit for a more detailed and in- depth scan on the client machine:

We can start enumerating the ports to see and fine the running services alongside their version.

Msf5> db_nmap -sV -p 80,22,110, 25 IP address.

```

TIMEOUT      1000      yes      The socket connect timeout in milliseconds
(msf6㉿Maleficent)-[~/Downloads]
$ msfconsole
[*] auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21
PORTS => 22,25,80,110,21
[*] auxiliary(scanner/portscan/tcp) > show options
          Name          Current Value  Required  Description
CONCURRENCY 10      yes      The number of concurrent ports to check per host
DELAY        =[ metasploit v6.0.15-dev ]      [The delay between connections, per thread]
+ -- ---=[ 2071 exploits - 1123 auxiliary - 352 post ]      [The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>']
+ -- ---=[ 592 payloads - 45 encoders - 10 nops ]      [The socket connect timeout in milliseconds]
+ -- ---=[ 7 evasion ]      [The jitter factor (maximum value by which to +/- DELAY) in milliseconds.
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services
[*] msf6 > db_nmap -sV -p 80,22,110,25 192.168.29.71
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-21 15:29 IST
[*] Nmap: Nmap scan report for 192.168.29.71
[*] Nmap: Host is up (0.00071s latency).
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp closed ssh
[*] Nmap: 25/tcp closed smtp
[*] Nmap: 80/tcp closed http
[*] Nmap: 110/tcp closed pop3
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
msf6 >

```

Scanning for vulnerabilities with Nmap and Metasploit:

Msf5> dp_nmap -sV -A -p 80,22,110,25 IP address.

```

msf6 > db_nmap -sV -p 80,22,110,25 192.168.29.71
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-21 15:29 IST
[*] Nmap: Nmap scan report for 192.168.29.71
[*] Nmap: Host is up (0.00071s latency).
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp closed ssh
[*] Nmap: 25/tcp closed smtp
[*] Nmap: 80/tcp closed http
[*] Nmap: 110/tcp closed pop3
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
msf6 > db_nmap -sV -A -p 80,22,110,25 192.168.29.71
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-21 15:30 IST
[*] Nmap: Nmap scan report for 192.168.29.71
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp closed ssh
[*] Nmap: 25/tcp closed smtp
[*] Nmap: 80/tcp closed http
[*] Nmap: 110/tcp closed pop3
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
msf6 > db_nmap 912.168.29.71 -A
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-21 15:31 IST
[*] Nmap: 'Failed to resolve "912.168.29.71".'
[*] Nmap: 'WARNING: No targets were specified, so 0 hosts scanned.'
[*] Nmap: Nmap done: 0 IP addresses (0 hosts up) scanned in 0.49 seconds
msf6 >

```

EXPERIMENT NO – 8

AIM: Implementation of Foot Printing Lab.

THEORY:

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

When used in the computer security lexicon, "Footprinting" generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. Some of the tools used for Footprinting are Sam Spade, nslookup, traceroute, Nmap and neutrace.

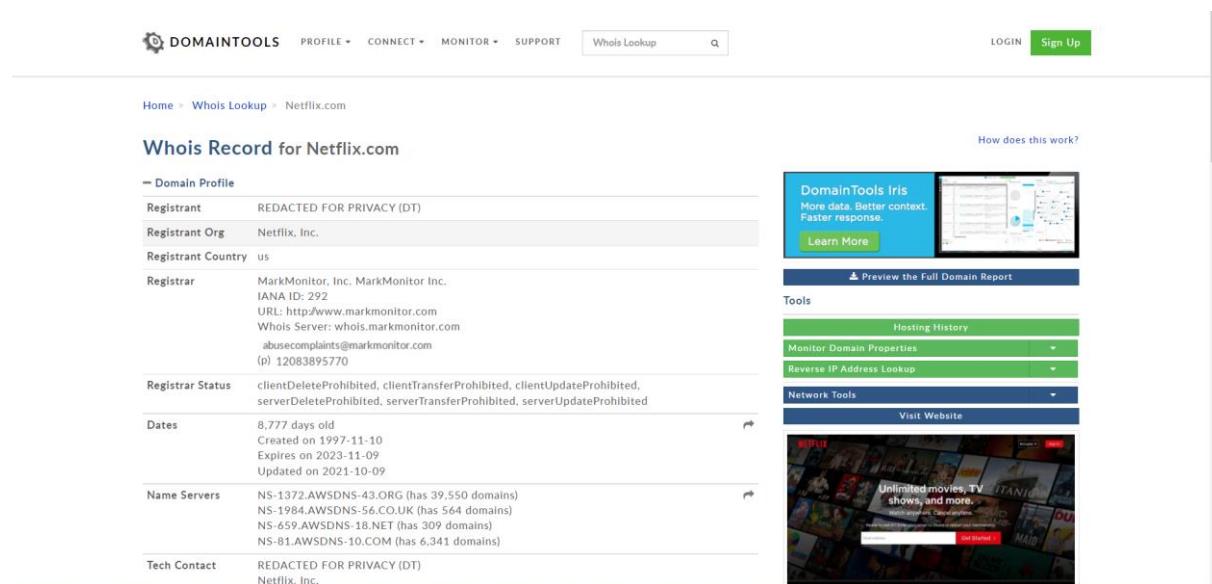
USES OF FOOTPRINTING:

It allows a hacker to gain information about the target system or network. This information can be used to carry out attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed to get a complete and successful resolution of the attack. Footprinting is also used by ethical hackers and penetration testers to find security flaws and vulnerabilities within their own company's network before a malicious hacker does.

Practical:

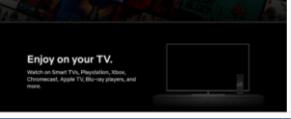
OUTPUT:

WEB TOOL: WHOIS LOOKUP



The screenshot shows the DomainTools Whois Lookup interface for the domain `Netflix.com`. The main content area displays the Whois Record for `Netflix.com`, listing details such as Registrant (REDACTED FOR PRIVACY (DT)), Registrant Org (Netflix, Inc.), Registrant Country (US), Registrar (MarkMonitor, Inc., MarkMonitor Inc.), Dates (Created on 1997-11-10, Expires on 2023-11-09, Updated 2021-10-09), Name Servers (NS-1372.AWSDNS-43.ORG, NS-1984.AWSDNS-56.CO.UK, NS-659.AWSDNS-18.NET, NS-81.AWSDNS-10.COM), and Tech Contact (REDACTED FOR PRIVACY (DT)). To the right of the Whois record, there is a sidebar for **DomainTools Iris** with a call-to-action button "Learn More". Below the Iris section are links for "Preview the Full Domain Report", "Tools", "Hosting History", "Monitor Domain Properties", "Reverse IP Address Lookup", "Network Tools", and a "Visit Website" link to the Netflix homepage.

Tech Contact	REDACTED FOR PRIVACY (DT) Netflix, Inc. 100 Winchester Circle, Los Gatos, CA, 95032, us (p) REDACTED FOR PRIVACY (DT) (f) REDACTED FOR PRIVACY (DT)
IP Address	44.240.158.19 - 2 other sites hosted on this server
IP Location	US - Oregon - Boardman - Amazon.com Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And Active Website
IP History	208 changes on 208 unique IP addresses over 16 years
Registrar History	2 registrars with 1 drop
Hosting History	6 changes on 6 unique name servers over 14 years
— Website	
Website Title	None given.
Terms	13,910 (Unique: 1,525, Linked: 37)
Images	6 (Alt tags missing: 6)
Links	18 (Internal: 16, Outbound: 1)
Whois Record (last updated on 2021-11-21)	
Domain Name: netflix.com Registry Domain ID: Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com Updated Date: 2021-10-09T09:37:28+00:00 2021-10-09 Creation Date: 1997-11-11T05:00:00+00:00 1997-11-11 Registrar Registration Expiration Date: 2023-11-10T00:00:00+00:00 2023-11-10 Registrar: MarkMonitor, Inc. MarkMonitor Inc. Sponsoring Registrar IANA ID: 292 Registrar Abuse Contact Email: abusecomplaints@markmonitor.com Registrar Abuse Contact Phone: 12083895770 Status: clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY (DT) Registrant Organization: Netflix, Inc. Registrant Street: 100 Winchester Circle, Registrant City: Los Gatos Registrant State/Province: CA Registrant Postal Code: 95032 Registrant Country: us Registrant Phone: 14085403700 Registrant Phone Ext: Registrant Fax: 14085403737	



Enjoy on your TV.
Watch on Smart TVs, FireTV, Chromecast, Apple TV, Onkyo players, and more.

[View Screenshot History](#)

Available TLDs

General TLDs **Country TLDs**

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- █ Taken domain.
- █ Available domain.
- █ Deleted previously owned domain.

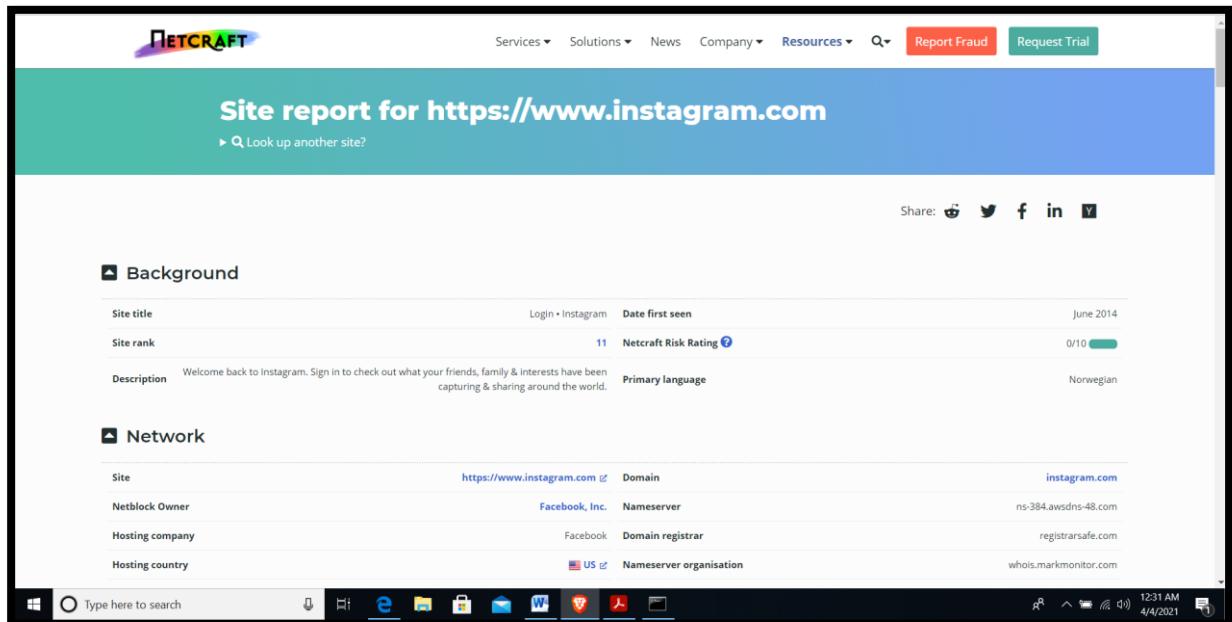
Netflix.com	View Whois
Netflix.net	View Whois
Netflix.org	View Whois
Netflix.info	View Whois
Netflix.biz	View Whois
Netflix.us	View Whois

Whois Record of Netflix.com:

Domain Name: netflix.com
 Registry Domain ID:
 Registrar WHOIS Server: whois.markmonitor.com
 Registrar URL: http://www.markmonitor.com
 Updated Date: 2021-10-09T09:37:28+00:00
 2021-10-09
 Creation Date: 1997-11-11T05:00:00+00:00
 1997-11-11
 Registrar Registration Expiration Date: 2023-11-10T00:00:00+00:00
 2023-11-10
 Registrar: MarkMonitor, Inc.
 MarkMonitor Inc.
 Sponsoring Registrar IANA ID: 292
 Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
 Registrar Abuse Contact Phone: 12083895770
 Status:
 clientDeleteProhibited
 clientTransferProhibited
 clientUpdateProhibited
 serverDeleteProhibited
 serverTransferProhibited
 serverUpdateProhibited
 Registry Registrant ID:
 Registrant Name: REDACTED FOR PRIVACY (DT)
 Registrant Organization: Netflix, Inc.
 Registrant Street: 100 Winchester Circle,
 Registrant City: Los Gatos
 Registrant State/Province: CA
 Registrant Postal Code: 95032
 Registrant Country: us
 Registrant Phone: 14085403700
 Registrant Phone Ext:
 Registrant Fax: 14085403737

Registrant Fax Ext:
Registrant Email: REDACTED FOR PRIVACY (DT)
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY (DT)
Admin Organization: Netflix, Inc.
Admin Street: 100 Winchester Circle,
Admin City: Los Gatos
Admin State/Province: CA
Admin Postal Code: 95032
Admin Country: us
Admin Phone: REDACTED FOR PRIVACY (DT)
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY (DT)
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY (DT)
Tech Organization: Netflix, Inc.
Tech Street: 100 Winchester Circle,
Tech City: Los Gatos
Tech State/Province: CA
Tech Postal Code: 95032
Tech Country: us
Tech Phone: REDACTED FOR PRIVACY (DT)
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY (DT)
Tech Fax Ext:
Tech Email: REDACTED FOR PRIVACY (DT)
Registry Billing ID:
Billing Name:
Billing Organization:
Billing Street:
Billing City:
Billing State/Province:
Billing Postal Code:
Billing Country:
Billing Phone:
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email:
Nameservers:
ns-1372.awsdns-43.org
ns-1984.awsdns-56.co.uk
ns-659.awsdns-18.net
ns-81.awsdns-10.com
Registry ID: 1404215_DOMAIN_COM-VRSN
DNSSEC: unsigned

WEB TOOL: NETCRAFT



The screenshot shows the Netcraft Site report for <https://www.instagram.com>. The top navigation bar includes links for Services, Solutions, News, Company, Resources (highlighted), Report Fraud, and Request Trial. A search bar and a 'Look up another site?' button are also present.

Site report for <https://www.instagram.com>

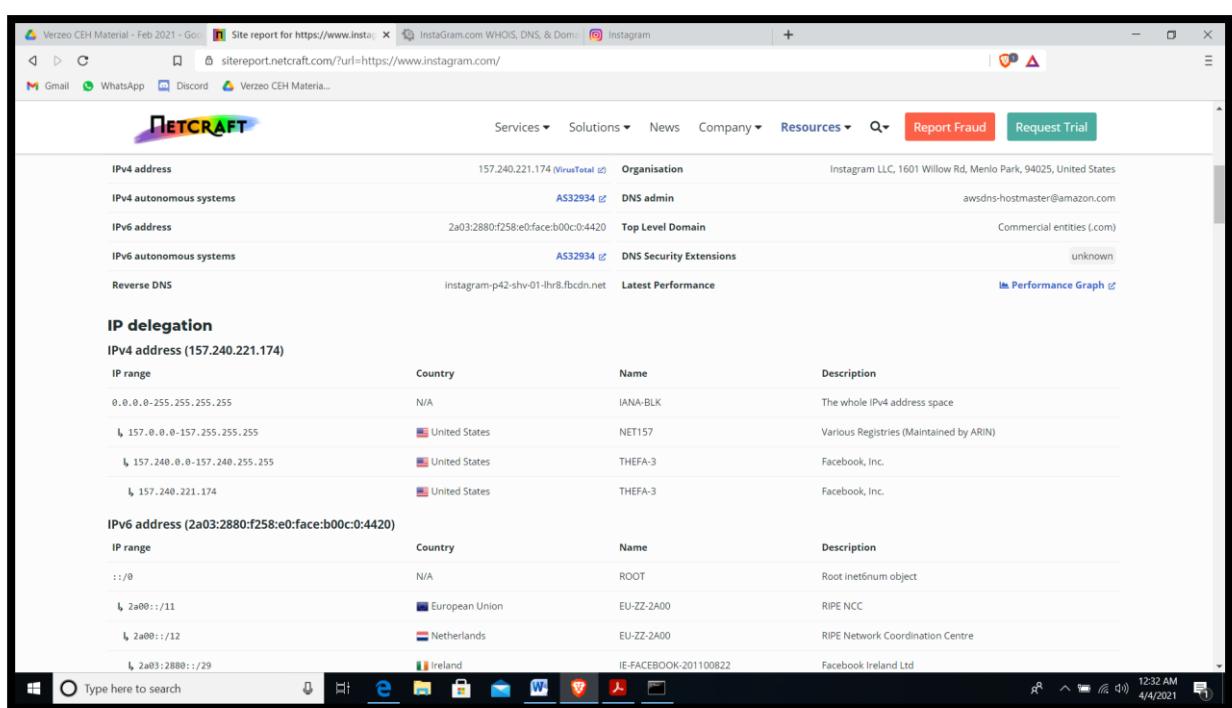
Share: [Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#)

Background

Site title	Login • Instagram	Date first seen	June 2014
Site rank	11	Netcraft Risk Rating	0/10
Description	Welcome back to Instagram. Sign in to check out what your friends, family & interests have been capturing & sharing around the world.	Primary language	Norwegian

Network

Site	https://www.instagram.com	Domain	instagram.com
Netblock Owner	Facebook, Inc.	Nameserver	ns-384.awsdns-48.com
Hosting company	Facebook	Domain registrar	registrarsafe.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com



The second screenshot shows the Netcraft Site report for <https://www.instagram.com>, focusing on IP delegation and network details. The top navigation bar and search bar are identical to the first screenshot.

IP delegation

IPv4 address (157.240.221.174)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 157.0.0.0-157.255.255.255	United States	NET157	Various Registries (Maintained by ARIN)
↳ 157.240.0.0-157.240.255.255	United States	THEFA-3	Facebook, Inc.
↳ 157.240.221.174	United States	THEFA-3	Facebook, Inc.

IPv6 address (2a03:2880:f258:e0:face:b00c:0:4420)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a03:2880::/29	Ireland	IE-FACEBOOK-201100822	Facebook Ireland Ltd

site report.netcraft.com/?url=https://www.instagram.com/

SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	
Common name	*.www.instagram.com	Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC7301 application-layer protocol negotiation
Organisation	Facebook, Inc.	Application-Layer Protocol Negotiation	h2
State	California	Next Protocol Negotiation	Not Present
Country	US	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	DigiCert SHA2 High Assurance Server CA
Subject Alternative Name	*.www.instagram.com, www.instagram.com	Issuer unit	www.digicert.com
Validity period	From Mar 3 2021 to Jun 1 2021 (2 months, 4 weeks, 1 day)	Issuer location	Not Present
Matches hostname		Issuer country	US
Server	Not Present	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl3.digicert.com/sha2-ha-server-g6.crl http://crl4.digicert.com/sha2-ha-server-g6.crl
Protocol version	TLSv1.3	Certificate Hash	GskBNNGcTbPJcJ6QGGaBk9TY9oqQ

Type here to search 12:33 AM 4/4/2021

Verzeo CEH Material - Feb 2021 - Go! Site report for https://www.instagram.com/ sitereport.netcraft.com WHOIS, DNS, & Domains Instagram

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Xenon 2021 f17yyI//1Fv0jMjAypt551Xkrxq54CXBuapdomX41#Nc=	2021-03-03 02:56:05	Success
Certificate	DigiCert Yeti 2021 xbdkv7nq0vEs5a1FbmEDf71fpH3KfzL1Je5v9HDso=	2021-03-03 02:56:05	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

site report.netcraft.com/?url=https://www.instagram.com/

Heartbleed

The site offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate and no longer offers Heartbeat.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests: [More information about Heartbleed detection](#).

SSL Certificate Chain

Common name	DigiCert High Assurance EV Root CA
Organisational unit	www.digicert.com
Organisation	DigiCert Inc
Validity period	From 2006-11-10 to 2031-11-10
Common name	DigiCert SHA2 High Assurance Server CA
Organisational unit	www.digicert.com
Organisation	DigiCert Inc
Validity period	From 2013-10-22 to 2028-10-22

sitereport.netcraft.com/?url=https://www.instagram.com/

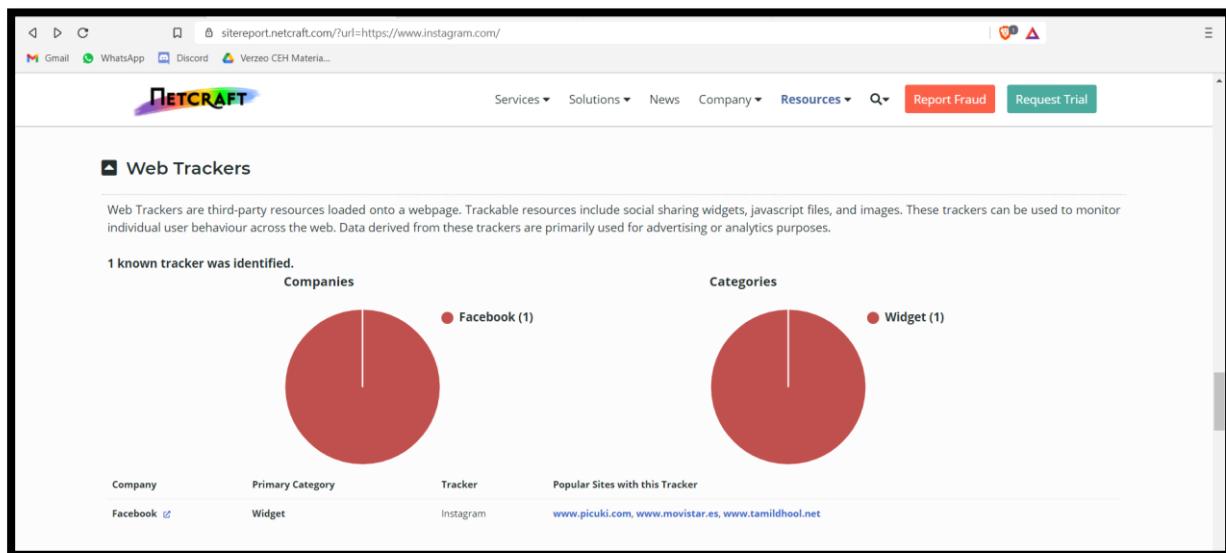
Gmail WhatsApp Discord Verzeo CEH Materia...

NETCRAFT

Services Solutions News Company Resources Report Fraud Request Trial

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	1-Oct-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	15-Sep-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	8-Sep-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	24-Aug-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	16-Aug-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	27-Jul-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	20-Jul-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	6-Jun-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.221.174	Linux	unknown	3-Jun-2020
Facebook, Inc. 1601 Willow Rd. Menlo Park CA US 94025	157.240.1.174	Linux	unknown	20-May-2020



Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
AJAX	No description	www.amazon.it , www.paypal.com , www.instagram.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.newsit.gr , www.varzesh3.com , www.offensive-security.com

WEB TOOL: DOMAIN DOSSIER

The screenshot shows a Microsoft Edge browser window with the URL `centralops.net/co/DomainDossier.aspx`. The search bar contains `netflix.com`. Below the search bar are several checkboxes: domain whois record, DNS records, traceroute, network whois record, and service scan. A `go` button is to the right of these checkboxes. At the bottom left, it says `user: anonymous [49.36.181.64]` and `balance: 50 units`, with links for `log in` and `account info`. On the right, it says `CentralOps.net`.

Address lookup

canonical name netflix.com.

aliases

addresses **3.230.129.93**
52.3.144.142
54.237.226.164
2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf
2600:1f18:631e:2f80:77e5:13a7:6533:7584
2600:1f18:631e:2f84:ceae:e049:1e:6a96

Network Whois record

Queried whois.arin.net with "n ! NET-3-224-0-0-1"...

NetRange: 3.224.0.0 - 3.239.255.255
CIDR: 3.224.0.0/12
NetName: AMAZON-IAD
NetHandle: NET-3-224-0-0-1
Parent: AT-88-Z (NET-3-128-0-0-1)
NetType: Reallocated
OriginAS: AS16509, AS14618
Organization: Amazon Data Services NoVa (ADSN-1)
RegDate: 2018-12-18
Updated: 2018-12-18
Ref: <https://rdap.arin.net/registry/ip/3.224.0.0>

OrgName: Amazon Data Services NoVa
OrgId: ADSN-1
Address: 13200 Woodland Park Road
City: Herndon
StateProv: VA
PostalCode: 20171
Country: US
RegDate: 2018-04-25
Updated: 2019-08-02
Ref: <https://rdap.arin.net/registry/entity/ADSN-1>

```

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-266-4064
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-266-4064
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-266-4064
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

```

DNS records

DNS query for **f.b.d.8.c.a.0.0.2.b.7.2.d.c.8.c.2.8.f.2.e.1.3.6.8.1.f.1.0.0.6.2.ip6.arpa** returned an error from the server: **NameError**

name	class	type	data	time to live
netflix.com	IN	A	54.160.93.182	60s (00:01:00)
netflix.com	IN	A	3.211.157.115	60s (00:01:00)
netflix.com	IN	A	3.225.92.8	60s (00:01:00)
netflix.com	IN	NS	ns-1372.awsdns-43.org	14400s (04:00:00)
netflix.com	IN	NS	ns-1984.awsdns-56.co.uk	14400s (04:00:00)
netflix.com	IN	NS	ns-659.awsdns-18.net	14400s (04:00:00)
netflix.com	IN	NS	ns-81.awsdns-10.com	14400s (04:00:00)
netflix.com	IN	SOA	server: ns-81.awsdns-10.com email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 1800	900s (00:15:00)
netflix.com	IN	MX	preference: 1 exchange: aspmx.l.google.com	60s (00:01:00)
netflix.com	IN	MX	preference: 10 exchange: aspmx2.googlemail.com	60s (00:01:00)
netflix.com	IN	MX	preference: 10 exchange: aspmx3.googlemail.com	60s (00:01:00)
netflix.com	IN	MX	preference: 5 exchange: alt1.aspmx.l.google.com	60s (00:01:00)
netflix.com	IN	MX	preference: 5 exchange: alt2.aspmx.l.google.com	60s (00:01:00)

...
netflix.com	IN	TXT	google-site-verification=YVxAf7gFR4vFk1RkUwIyt3pzl2AVUP6aPdBgViqtwcw		300s (00:05:00)	
netflix.com	IN	TXT	google-site-verification=nClQdIMabPJovtQNCo5KaPyDfwog9pDr3d8IN767YA		300s (00:05:00)	
netflix.com	IN	TXT	loom-verification=0004053852		300s (00:05:00)	
netflix.com	IN	TXT	miro-verification=9ac407d6774b2ec4313b004d40204399e37f3b48		300s (00:05:00)	
netflix.com	IN	TXT	v=spf1 include:_spf_ipv4.netflix.com include:_spf.google.com include:amazonses.com include:servers.mcsv.net -all		300s (00:05:00)	
netflix.com	IN	TXT	zapier-domain-verification-challenge=d740d03c-47a4-491c-934d-c61bdbaa6099e		300s (00:05:00)	
netflix.com	IN	AAAA	2600:1f18:631e:2f80:77e5:13a7:6533:7584		60s (00:01:00)	
netflix.com	IN	AAAA	2600:1f18:631e:2f84:ceae:e049:1e:6a96		60s (00:01:00)	
netflix.com	IN	AAAA	2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf		60s (00:01:00)	
netflix.com	IN	CAA	[no interpretation available] 00 05 69 6F 64 65 66 6D ..iodefm hex dump: 61 69 6C 74 6E 3A 73 65 ailtose (34 bytes) 63 75 72 69 74 79 40 6E curity&n 65 74 66 6C 69 78 2E 63 etflix.c 6F 6D om		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 05 69 73 73 75 65 64 ..issued hex dump: 69 67 69 63 65 72 74 2E igicert. (19 bytes) 63 6F 6D com		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 05 69 73 73 75 65 65 ..issuem hex dump: 6B 74 72 75 73 74 2E 6E ntrust.n (18 bytes) 65 74 et		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 05 69 73 73 75 65 6C ..issuel hex dump: 65 74 73 65 6B 63 72 79 etsencry (22 bytes) 70 74 2E 72 67 pt.org		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 05 69 73 73 75 65 70 ..issuep hex dump: 6B 69 2E 67 6F 6F 67 ki.goog (15 bytes)		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 05 69 73 73 75 65 73 ..issues hex dump: 79 6D 61 6B 74 65 63 2E ymantec. (19 bytes) 63 6F 6D com		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 09 69 73 73 75 65 77 ..issuem hex dump: 69 6C 64 64 69 67 69 63 ilddigic (23 bytes) 74 65 63 2E 63 6F 6D tec.com		300s (00:05:00)	
netflix.com	IN	CAA	[no interpretation available] 00 09 69 73 73 75 65 77 ..issuem hex dump: 69 6C 64 73 79 6D 61 6E ildsyman (23 bytes) 74 65 63 2E 63 6F 6D tec.com		300s (00:05:00)	
93.129.230.3.in-addr.arpa	IN	PTR	ec2-3-230-129-93.compute-1.amazonaws.com			
129.230.3.in-addr.arpa	IN	NS	ns1-24-us-east-1.ec2-rdns.amazonaws.com			
129.230.3.in-addr.arpa	IN	NS	ns2-24-us-east-1.ec2-rdns.amazonaws.com			
129.230.3.in-addr.arpa	IN	NS	ns3-24-us-east-1.ec2-rdns.amazonaws.com			
129.230.3.in-addr.arpa	IN	NS	ns4-24-us-east-1.ec2-rdns.amazonaws.com			
129.230.3.in-addr.arpa	IN	SOA	server: ns-1511.awsdns-60.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400			

Traceroute

Tracing route to netflix.com [3.230.129.93]...

Traceroute

Tracing route to **netflix.com [3.230.129.93]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	1	1	169.254.158.58	
2	1	1	0	169.48.118.158	ae103.ppr02.dal13.networklayer.com
3	0	0	0	169.48.118.138	8a.76.30a9.ip4.static.sl-reverse.com
4	*	2	*	169.45.18.92	ae17.cbs02.eq01.dal03.networklayer.com
5	1	1	1	50.97.17.57	ae34.bbr01.eq01.dal03.networklayer.com
6	1	1	1	50.97.16.59	3b.10.6132.ip4.static.sl-reverse.com
7	*	*	*		
8	*	*	*		
9	*	*	*		
10	*	*	*		

Trace aborted

Service scan

FTP - 21 Error: TimedOut
SMTP - 25 Error: TimedOut
HTTP - 80 HTTP/1.1 301 Moved Permanently
Location: https://netflix.com/
Content-Length: 0
Via: 1.1 i-0ba47e4cc761c644d (us-east-1)
Server: nginx_website_npm_member-prod-release UNKNOWN
X-Add-Protocol: http
X-Add-Block: report=https://www.netflix.com/ichnaea/log/freeform/xssreport
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Originating-URL: http://netflix.com/
Set-Cookie: nfvid=BQfMaaBEBENGwN8b_qeUFkJiLNvcDxyVAoJrektWJ5tIn1m9OkxitKa2DQzSlyA8iUIzLsib5oIjkYcLQ5nhGzEjLminx65E9kgWhLyraa6JY_-dET3Q%3D%3D; Domain=.netflix.com;
Path=/; Max-Age=31536000
X-Network.nfstatus: 1_21
Set-Cookie: memclid=13cbd39-03e1-4f4e-9d6b-99909bd4875c; Max-Age=31536000; Expires=Mon, 21 Nov 2022 10:34:19 GMT; Path=/; Domain=.netflix.com
X-Network.proxy.execution-time: 3

POP3 - 110 Error: TimedOut
IMAP - 143 Error: Timedout
HTTPS - 443 Certificate validation errors: None
Signature algorithm: sha256RSA
Public key size: 2048 bits
Issuer: ComodoGlobe SHA2 Secure Server CA, C=US
Subject: Netflix, Inc., DNS Name=account.netflix.com, DNS Name=ca.netflix.com, DNS Name=netflix.ca, DNS Name=netflix.com, DNS Name.signup.netflix.com, DNS Name=www.netflix.ca, DNS Name=www.netflix.com, DNS Name=www2.netflix.com, DNS Name=www3.netflix.com, DNS Name=develop-stage.netflix.com, DNS Name=release-stage.netflix.com, DNS Name=tv.netflix.com, DNS Name=embed.develop-stage.netflix.com, DNS Name=embed.release-stage.netflix.com
Serial number: 0F2A6275CF975D94B0BDC9FC4C6B34F0
Not valid before: 2020-01-13 00:00:00Z
Not valid after: 2022-01-13 12:00:00Z
SHA1 fingerprint: CES8CC082D6504D4F1D95CC06C7FB96F865A5240
HTTP/1.1 405 Method Not Allowed
Server: nginx_website_npm_member-prod-release 208d8492-0826-4662-b2f8-57627d984a1c
X-frame-options: DENY
allow: GET, OPTIONS, POST
date: Sun, 21 Nov 2021 10:34:24 GMT
x-envoy-upstream-service-time: 12
x-b3-trace-id: 2ef4d558-4445-4921-a9bd-hf50f8f47ee7
x-envoy-decorator-operation: lo_svc
Via: 1.1 i-04dd7a6ac3763e396 (us-east-1)
X-Xss-Protection: 1; mode=block; report=https://www.netflix.com/ichnaea/log/freeform/xssreport
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Originating-URL: http://netflix.com/
Edge-Control: no-store
Cache-Control: no-cache, no-store
Set-Cookie: nfvid=BQfMaaBEBENGwN8b_qeUFkJiLNvcDxyVAoJrektWJ5tIn1m9OkxitKa2DQzSlyA8iUIzLsib5oIjkYcLQ5nhGzEjLminx65E9kgWhLyraa6JY_-dET3Q%3D%3D; Domain=.netflix.com;
Path=/; Max-Age=31536000
X-Network.nfstatus: 1_1
Set-Cookie: memclid=3fa982fc-8af1-4311-9ff9b-53b80b6cb91f; Max-Age=31536000; Expires=Mon, 21 Nov 2022 10:34:24 GMT; Path=/; Domain=.netflix.com
X-Network.proxy.execution-time: 113
transfer-encoding: chunked
Connection: close

-- end --
URL for this output | return to [CentralOps.net](#), a service of Hexillion

DNS RECON:

```
maleficient@Maleficient: ~
maleficient@Maleficient: ~ 101x47
usage: dnsrecon.py [-h] -d DOMAIN [-n NS_SERVER] [-r RANGE] [-D DICTIONARY]
                   [-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS]
                   [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV]
                   [-j JSON] [-iwl] [--disable_check_recursion]
                   [--disable_check_bindversion] [-v] [-t TYPE]
dnsrecon.py: error: the following arguments are required: -d/-domain

[~] $ dnsrecon -d www.netflix.com -w
[*] Performing General Enumeration of Domain: www.netflix.com
[-] DNSSEC is not configured for www.netflix.com
[*]      SOA ns-1566.awsdns-03.co.uk 205.251.198.30
[-] Could not Resolve NS Records for www.netflix.com
[-] Could not Resolve MX Records for www.netflix.com
[*]      CNAME www.netflix.com www.dradis.netflix.com
[*]      CNAME www.dradis.netflix.com www.eu-west-1.internal.dradis.netflix.com
[*]      CNAME www.eu-west-1.internal.dradis.netflix.com dualstack.apiproxy-website-nlb-prod-1-5675d5
ecda6efdd8.elb.eu-west-1.amazonaws.com
[*]      A dualstack.apiproxy-website-nlb-prod-1-5675d5ecda6efdd8.elb.eu-west-1.amazonaws.com 54.170.
196.176
[*]      A dualstack.apiproxy-website-nlb-prod-1-5675d5ecda6efdd8.elb.eu-west-1.amazonaws.com 52.214.
181.141
[*]      A dualstack.apiproxy-website-nlb-prod-1-5675d5ecda6efdd8.elb.eu-west-1.amazonaws.com 54.246.
79.9
[*]      CNAME www.netflix.com www.dradis.netflix.com
[*]      CNAME www.dradis.netflix.com www.eu-west-1.internal.dradis.netflix.com
[*]      CNAME www.eu-west-1.internal.dradis.netflix.com dualstack.apiproxy-website-nlb-prod-1-5675d5
ecda6efdd8.elb.eu-west-1.amazonaws.com
[*]      AAAA dualstack.apiproxy-website-nlb-prod-1-5675d5ecda6efdd8.elb.eu-west-1.amazonaws.com 2a05
:d018:76c:b685:3b38:679d:2640:1ced
[*]      AAAA dualstack.apiproxy-website-nlb-prod-1-5675d5ecda6efdd8.elb.eu-west-1.amazonaws.com 2a05
:d018:76c:b684:8e48:47c9:84aa:b34d
[*]      AAAA dualstack.apiproxy-website-nlb-prod-1-5675d5ecda6efdd8.elb.eu-west-1.amazonaws.com 2a05
:d018:76c:b683:f711:f0cf:5cc7:b815
[*]  Enumerating SRV Records
[+] 0 Records Found
[*]  Performing Whois lookup against records found.
Traceback (most recent call last):
  File "./dnsrecon.py", line 1691, in <module>
    main()
  File "./dnsrecon.py", line 1651, in main
    std_enum_records = general_enum(res, domain, xfr, bing, yandex, spf_enum, do_whois, do_crt, zonewalk)
  File "./dnsrecon.py", line 1048, in general_enum
    whois_rcd = whois_ips(res, ip_for_whois)
  File "./dnsrecon.py", line 555, in whois_ips
    list = get_whois_nets_iplist(unique(ip_list))
  File "./dnsrecon.py", line 523, in get_whois_nets_iplist
```

DNS ENUM:

```
maleficient@Maleficient: ~
maleficient@Maleficient: ~ 101x47

[~] $ dnsenum -F subs.txt thundercloud.co.za
dnsenum VERSION:1.2.6
255 x

----- thundercloud.co.za -----


Host's addresses:
-----
thundercloud.co.za.          600      IN      A      169.239.216.61


Name Servers:
-----
ns1.tld-ns.net.           20619      IN      A      169.239.219.110
ns3.tld-ns.net.           20619      IN      A      51.195.136.240
ns2.tld-ns.com.            43200      IN      A      169.239.216.110
ns4.tld-ns.com.            20618      IN      A      156.38.246.4


Mail (MX) Servers:
-----


Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for thundercloud.co.za on ns1.tld-ns.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for thundercloud.co.za on ns3.tld-ns.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for thundercloud.co.za on ns2.tld-ns.com ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for thundercloud.co.za on ns4.tld-ns.com ...
AXFR record query failed: NOTAUTH


Brute forcing with subs.txt:
-----
```

WEB TOOL: DNS DUMPSTER

Showing results for **netflix.com**

DNS Servers MX Records TXT Records Host (A) Records Domain Map

Hosting (IP block owners)

Host	Count
AMAZON-02	~42
GOOGLE	~5
AMAZON-AES	~50
Reserved (Local Network)	~5
SQUARESPACE	~2
NETFLIX-ASN	~3
AS-SSJ	~1

GeoIP of Host Locations

DNS Servers

Name	IP Address	Owner
ns-1372.awsdns-43.org.	205.251.197.92	AMAZON-02
ns-1372.awsdns-43.org.	ns-1372.awsdns-43.org	United States
ns-1984.awsdns-56.co.uk.	205.251.199.192	AMAZON-02
ns-1984.awsdns-56.co.uk.	ns-1984.awsdns-56.co.uk	United States
ns-659.awsdns-18.net.	205.251.194.147	AMAZON-02
ns-659.awsdns-18.net.	ns-659.awsdns-18.net	United States
ns-81.awsdns-10.com.	205.251.192.81	AMAZON-02
ns-81.awsdns-10.com.	ns-81.awsdns-10.com	United States

MX Records ** This is where email for the domain goes...

Priority	Server	IP Address	Owner
1	aspmx.l.google.com.	142.251.4.26	GOOGLE
1	aspmx.l.google.com.	gm-in-f26.le100.net	United States
10	aspmx2.googlemail.com.	108.177.12.26	GOOGLE
10	aspmx2.googlemail.com.	ua-in-f26.le100.net	United States
10	aspmx3.googlemail.com.	64.233.186.26	GOOGLE
10	aspmx3.googlemail.com.	cb-in-f26.le100.net	United States
5	alt1.aspmx.l.google.com.	209.85.202.27	GOOGLE
5	alt1.aspmx.l.google.com.	dg-in-f27.le100.net	United States
5	alt2.aspmx.l.google.com.	64.233.186.27	GOOGLE
5	alt2.aspmx.l.google.com.	cb-in-f27.le100.net	United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations			
"8cd468d7d5994fcc9d350683a8cb07a1"			
"apple-domain-verification=Ohlo8qLyb9N4JaIm"			
"asv=4853f01b1e9226ed9d0031284948059f"			
"docusign=f249396f-8150-48f8-8bd2-705be6e03826"			
"docusign=f3d36bef-ec7d-42e5-9334-626611acb127"			
"dropbox-domain-verification=htwo11xk2y11"			
"facebook-domain-verification=k65vedr09b2tp2ql44holzewp3xsc6"			
"google-site-verification=9DgwSKXMI1FzcnW-HuGwef6aVVHWDCONehxHTq0Ps9IA"			
"google-site-verification=VQKoV3pv-QYIDfbQa1N4r97x8W07veRTK6JhWUavIuc"			
"google-site-verification=YVxAf7gFR4vFk1RkUiYt3pz12AVUP6aPdBgVlqtwcw"			
"google-site-verification=ci1QdlMabPJ0vtQNCo5KaPyDfwog9pDr3d8IN767YA"			
"loom-verification=0004053852"			
"miro-verification=9ac407d6774b2ec4313b004d40204399e37f3b48"			
"v=spf1 include:_spf_ipv4.netflix.com include:_spf.google.com include:amazonses.com include:servers.mcsv.net -all"			
"zapier-domain-verification-challenge=d740d03c-47a4-491c-934d-c61bdb46099e"			
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)			
netflix.com	54.237.226.164	AMAZON-AES	
■	ec2-54-237-226-164.compute-1.amazonaws.com	United States	
cbp.nccp.us-east-1.prodaa.netflix.com	52.45.101.173	AMAZON-AES	
■	ec2-52-45-101-173.compute-1.amazonaws.com	United States	
HTTP: nccp-modern i-042550ef8138a5177			
HTTPS: nccp-modern i-0e5e70ff89d0118a2			
prod.cloud.us-west-2.prodaa.netflix.com	54.148.37.5	AMAZON-02	
■	ec2-54-148-37-5.us-west-2.compute.amazonaws.com	United States	
HTTP: xnn1 i-0dd2bdc145503e0a5			
appboot.us-east-1.prodaa.netflix.com	54.86.115.134	AMAZON-AES	
■	ec2-54-86-115-134.compute-1.amazonaws.com	United States	
HTTP: appboot- i-0e209603725eb71a6			
HTTPS: appboot- i-0f3bseef791e3aac			
nmtracking.eu-west-1.prodaa.netflix.com	52.213.86.193	AMAZON-02	
■	ec2-52-213-86-193.eu-west-1.compute.amazonaws.com	Ireland	
HTTP: clingeest-secure i-0acfca24bc8392d17			
HTTPS: clingeest-secure i-09afcfc74273ee42797			
ios.nccp.eu-west-1.prodaa.netflix.com	54.77.152.21	AMAZON-02	
■	ec2-54-77-152-21.eu-west-1.compute.amazonaws.com	Ireland	
HTTP: nccp-modern i-03b04a5d80594e901			
HTTPS: nccp-modern i-0d71156703f86865a			
sv1-ddi02.netflix.com	10.31.128.27	Reserved (Local Network)	
■		unknown	
obiwanc-wc.us-east-1.prodaa.netflix.com	54.236.182.108	AMAZON-AES	
■	ec2-54-236-182-108.compute-1.amazonaws.com	United States	
api-us.us-east-1.prodaa.netflix.com	54.175.238.199	AMAZON-AES	
■	ec2-54-175-238-199.compute-1.amazonaws.com	United States	
HTTP: api-prod i-0176a0e16a2445467			
HTTPS: api-prod i-0340af4ab22f1d735			

netflix.com-202111211043.xlsx [Protected View] - Excel

File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

A1 : Hostname

	A	B	C	D	E	F	G	H	I	J
95	api-global.us-east-1.prod.aa.netflix.com	54.84.226.72	A	ec2-54-84-226-72.compute-1.amazonaws.com	AMAZON-AES	United States				
96	api-us.eu-west-1.prod.aa.netflix.com	54.174.173.130	A	ec2-54-174-173-130.compute-1.amazonaws.com	AMAZON-AES	United States			api-prod-i-0cb77aca929e26be title: HTTP Status 404 On: api.netflix.com	
97	customerevents.us-east-1.prod.aa.netflix.com	54.165.159.239	A	ec2-54-165-159-239.compute-1.amazonaws.com	AMAZON-AES	United States				
98	api.eu-west-1.prod.aa.netflix.com	54.229.6.249	A	ec2-54-229-6-249.eu-west-1.compute.amazonaws.com	AMAZON-02	Ireland				
99	ncpp-ndp-31.eu-west-1.prod.aa.netflix.com	54.229.237.110	A	ec2-54-229-237-110.eu-west-1.compute.amazonaws.com	AMAZON-02	Ireland				
100	api-global.eu-west-1.prod.aa.netflix.com	54.77.130.150	A	ec2-54-77-130-150.eu-west-1.compute.amazonaws.com	AMAZON-02	Ireland				
101	help.us-east-1.prod.aa.netflix.com	52.44.120.35	A	ec2-52-44-120-35.compute-1.amazonaws.com	AMAZON-AES	United States				
102	ns-1372.awsdns-43.org.	205.251.197.92	NS	ns-1372.awsdns-43.org	AMAZON-02	United States				
103	ns-1984.awsdns-56.co.uk.	205.251.199.192	NS	ns-1984.awsdns-56.co.uk	AMAZON-02	United States				
104	ns-659.awsdns-18.net.	205.251.194.147	NS	ns-659.awsdns-18.net	AMAZON-02	United States				
105	ns-81.awsdns-10.com.	205.251.192.81	NS	ns-81.awsdns-10.com	AMAZON-02	United States				
106	1.aspmx.l.google.com.	142.251.4.26	MX	gm-in-f26.1e100.net	GOOGLE	United States				
107	10.aspmx2.googlemail.com.	108.177.12.26	MX	ua-in-f26.1e100.net	GOOGLE	United States				
108	10.aspmx3.googlemail.com.	64.233.186.26	MX	cb-in-f26.1e100.net	GOOGLE	United States				
109	5.aspmx.l.google.com.	209.85.202.27	MX	dg-in-f27.1e100.net	GOOGLE	United States				
	5.aspmx2.google.com.	64.233.186.27	MX	cb-in-f27.1e100.net	GOOGLE	United States				

All Hosts +

Ready 100%

EXPERIMENT NO – 9

AIM: Implementation of File System Security.

THEORY:

VeraCrypt is a Free and Open Source utility used for on-the-fly encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication. Individual ciphers supported by VeraCrypt are AES, Serpent, Twofish, Camellia, and Kuznyechik.

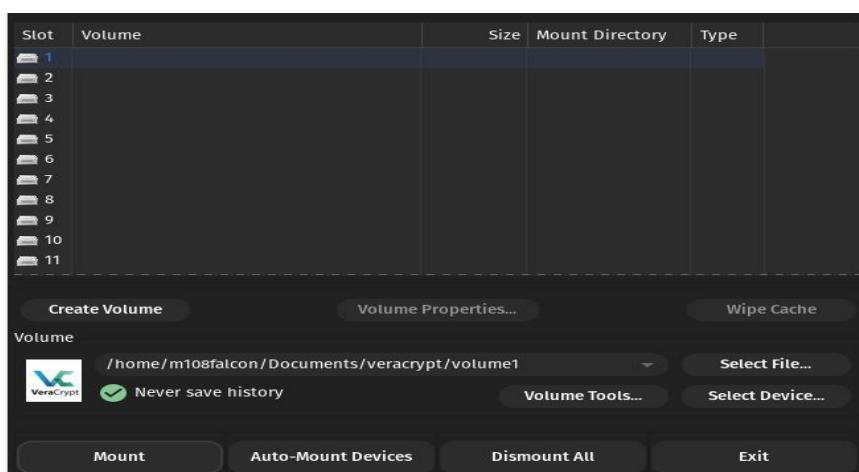
Additionally, ten different combinations of cascaded algorithms are available: AES–Twofish, AES–Twofish–Serpent, Camellia–Kuznyechik, Camellia–Serpent, Kuznyechik–AES, Kuznyechik–Serpent–Camellia, Kuznyechik–Twofish, Serpent–AES, Serpent–Twofish–AES, and Twofish–Serpent.

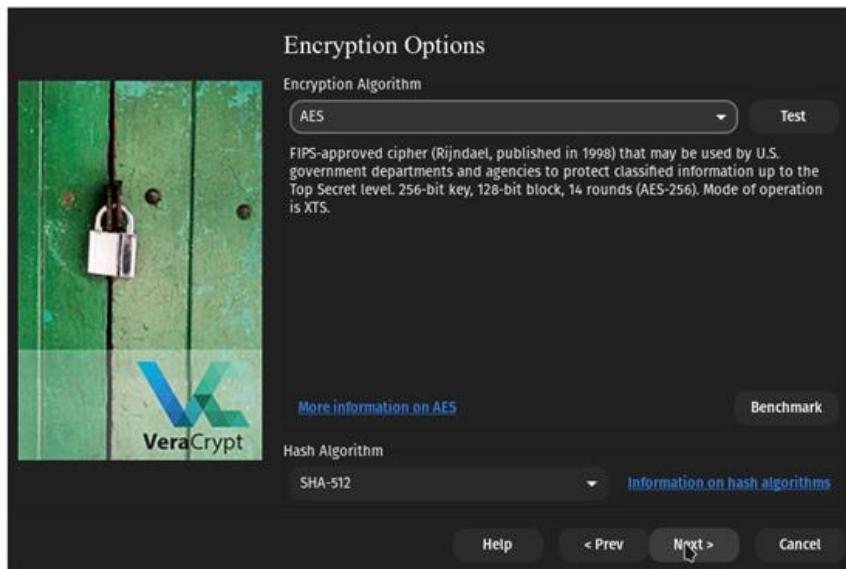
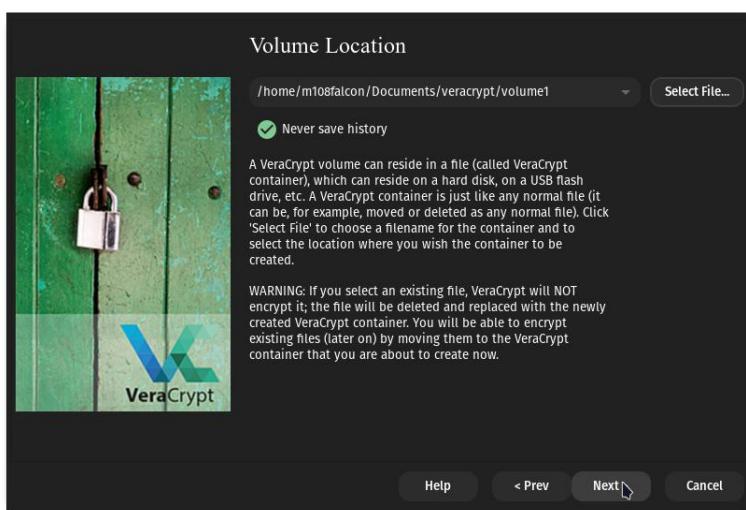
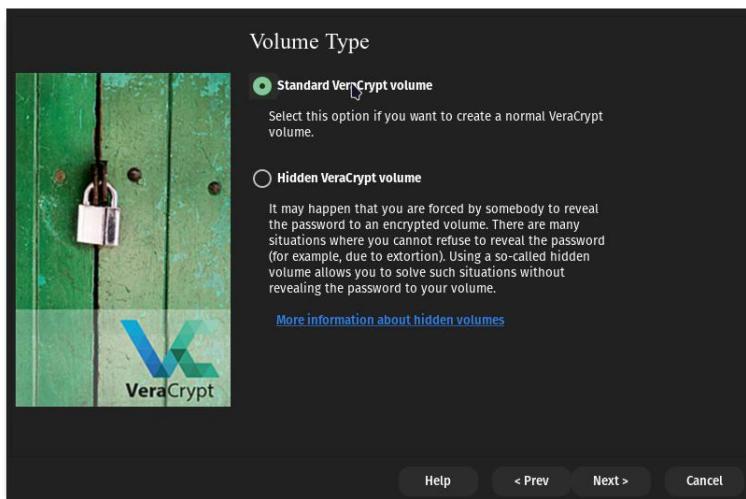
The cryptographic hash functions available for use in VeraCrypt are RIPEMD-160, SHA-256, SHA-512, Streebog and Whirlpool.

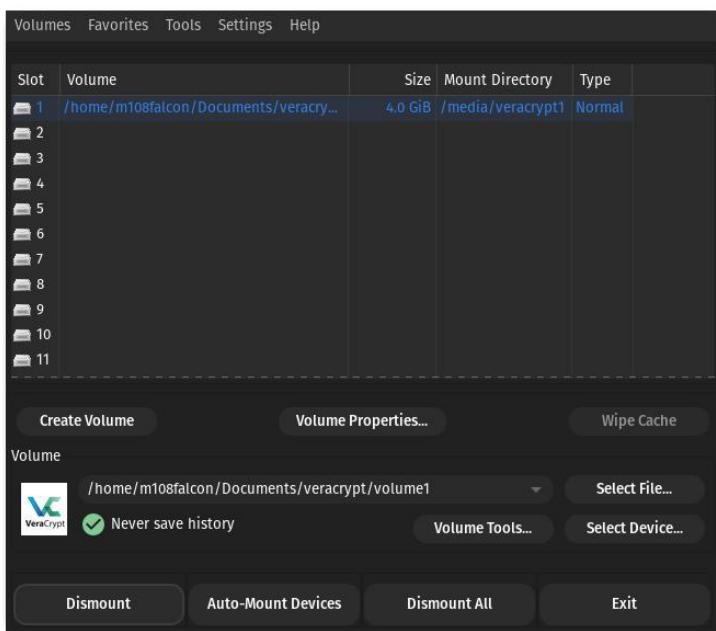
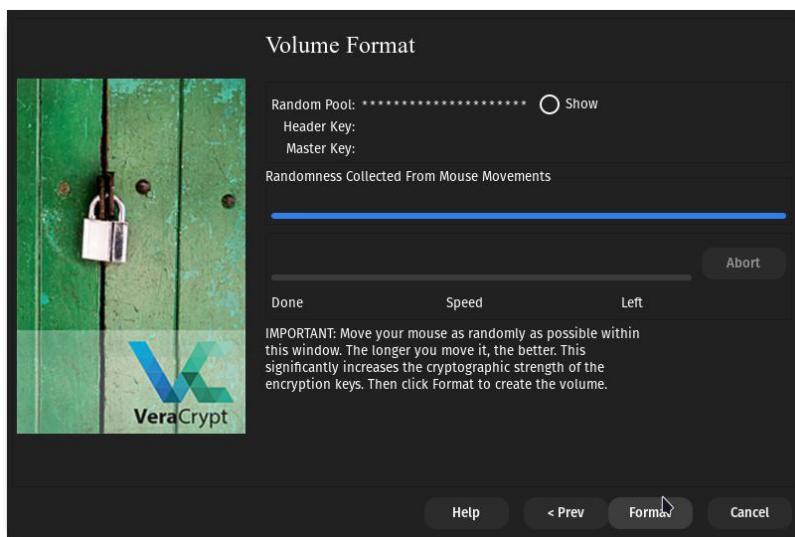
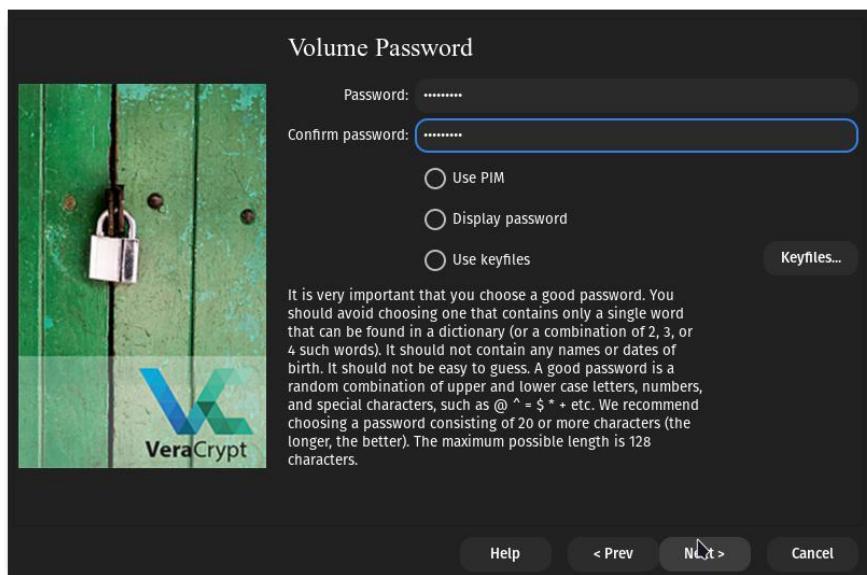
STEPS OF PERFORMING FILE SECURITY:

- 1) Open VeraCrypt tool and Click on the Create Volume.
- 2) Create a Standard Veracrypt volume.
- 3) From the select file menu, point to destination of created volume.
- 4) Choose the Encryption Option.
- 5) Create a password for said volume, be sure to use a complex password and never forget this password you set.
- 6) Move your mouse as randomly as possible, as tool will calculate hash based on mouse movement here, thus more random, more secure it will be once collection is complete click on the format and wait for the formatting of volume to finish.
- 7) Click on mount button and locate your newly create volume, once mounted it'll show itself on the main screen.
- 8) Now the volume has been mounted, you can transfer your folder containing sensitive info into it like a normal drive, and once you unmount, the information in the volume created will no longer will be accessible to anyone.

OUTPUT:







EXPERIMENT NO – 10

AIM: Implementation of Cryptography Lab.

THEORY:

Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/ciphertext, in contrast to asymmetric key cryptography, where the encryption and decryption keys are different. The keys may be identical, or there may be a simple transformation to go between the two keys. Symmetric-key encryption can use either stream ciphers or block ciphers.

1. Stream Cipher encrypt the digits (typically bytes), or letters (in substitution ciphers) of a message one at a time.
2. Block Cipher take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size.

Implementation of DES: Disk Encryption System

Encryption:

Input type: File

File: C:\fakepath\Research Paper 3rd sem.txt [Browse](#)

Function: DES

Mode: ECB (electronic codebook)

Key: (plain) SEMA

Plaintext Hex

[> Encrypt!](#) [> Decrypt!](#)

100%

File was uploaded.

Encrypted text:

00000000	f7 ee d1 14 2b e3 f8 e8 ff 11 7d a7 10 f8 9f 32	÷ ī Ñ . + ä ø è ý . } § . ø . 2
00000010	04 42 d2 9d a6 1a e4 5b 45 85 c9 a4 ff e3 43 a4	. B Ò ☐ ! . ä [E ☐ É ☐ ý ä C ☐
00000020	fa 66 05 24 7e d5 ca 22 d8 99 b3 72 a3 5c 1f 8f	ú f . \$ ~ Õ È " ø . ³ r £ \ . ☐
00000030	f9 b8 0b cc 4e e0 2a 22 55 eb 1c c5 e3 db 03 87	ù . . Ì N à * " U ø . Å ä Ü . .
00000040	dd e3 c0 f4 5d bb 45 57 d4 0b eb 83 fb aa 0e 68	Ý ä Å ô] » E W Ø . ø . Ú ³ . h
00000050	b8 f0 e1 5a 47 eb 42 ec 5e 82 23 7c 5a 41 19 17	. ö á Z G ø B ï ^ . # Z A . .
00000060	25 7c d1 68 96 c0 5e 0a 60 e8 70 4f 84 ca 0d 9d	% Ñ h ☐ Å ^ . ` è p O . È . ☐
00000070	8e ed 78 1c c2 fe 7c 37 38 37 5e 26 aa 06 90 81	. í x . Å þ 7 8 7 ^ & ³ . ☐ .
00000080	78 57 1c eb e8 d0 55 5d 81 89 0b f2 2e aa ab 76	x W . ø è Ø U] . . . ò . ³ « v
00000090	08 95 49 f3 9c b1 bc 15 24 56 31 06 32 55 92 fd	. ☐ I 6 ☐ ± % . \$ V 1 . 2 U . ý

[\[Download as a binary file\]](#) [\[Show more\]](#) [\[Show all\]](#) [\[?\]](#)

Active

Decryption:

Input type: File

File: C:\fakepath\odt-IV-0000000000000000.dat [Browse](#)

Function: DES

Mode: ECB (electronic codebook)

Key: SEMA
(plain)

Plaintext Hex

[> Encrypt!](#) [> Decrypt!](#)

100%

File was uploaded.

Decrypted text:

00000000	42 75 6e 67 6f 20 73 74 72 61 79 20 64 6f 67 73	Bungo stray dogs
00000010	0d 0a 42 6c 61 63 6b 20 62 75 74 6c 65 72 0d 0a	. . Black butler . .
00000020	0d 0a 61 20 74 69 74 6c 65 20 70 61 67 65 3b 0d	. . a title page ; .
00000030	0a 61 6e 20 61 62 73 74 72 61 63 74 3b 0d 0a 61	. an abstract ; . . a
00000040	6e 20 69 6e 74 72 6f 64 75 63 74 69 6f 6e 3b 0d	n introduction ; .
00000050	0a 61 20 6d 65 74 68 6f 64 6f 6c 6f 67 79 20 73	. a methodology s
00000060	65 63 74 69 6f 6e 3b 0d 0a 66 69 6e 64 69 6e 67	ection ; . . finding
00000070	73 2f 72 65 73 75 6c 74 73 3b 0d 0a 64 69 73 63	s / results ; . . disc
00000080	75 73 73 69 6f 6e 3b 0d 0a 63 6f 6e 63 6c 75 73	ussion ; . . conclus
00000090	69 6f 6e 2e 0d 0a 20 0d 0a 68 74 74 70 73 3a 2f	ion . . . https : /

[\[Download as a binary file\]](#) [\[Show more\]](#) [\[Show all\]](#) [\[?\]](#) Inactive

Asymmetric cryptography is a branch of cryptography where a secret key can be divided into two parts, a public key and a private key. The public key can be given to anyone, trusted or not, while the private key must be kept secret (just like the key in symmetric cryptography).

Asymmetric cryptography has two primary use cases: authentication and confidentiality. Using asymmetric cryptography, messages can be signed with a private key, and then anyone with the public key is able to verify that the message was created by someone possessing the corresponding private key.

Implementation of AES: Advanced Encryption Standard

Encryption and Decryption:

Also, you can find the sample usage screenshot below:

AES Online Encryption

Enter text to be Encrypted

This is Symmetric Key encryption showing how to do encryption using [AES](#)

OR

No file chosen

Select Mode

ECB

Key Size in Bits

128

Enter Secret Key

SECRETKEYAESKEYS

Output Text Format: Base64 Hex

AES Online Decryption

Enter text to be Decrypted

61IDRVjwlPOlqMk7UvbDZkjNUvrXEjmSxJ0Zyjlax
s3azL5KPGc/R615GiEZsE8kO/umPBOQQ+pafAyI
2yW0clydPLdzRqxInt9STxThRY=

Input Text Format: Base64 Hex

Select Mode

ECB

Key Size in Bits

128

Enter Secret Key

SECRETKEYAESKEYS

AES Decrypted Output ([Base64](#)):

Output Text Format: Base64 Hex



Ads by Google

[Send feedback](#)

[Why this ad?](#)

AES Encrypted Output:

61IDRVjwlPOlqMk7UvbDZkjNUvrXEjmSxJ0Zyjlax
s3azL5KPGc/R615GiEZsE8kO/umPBOQQ+pafAyI
2yW0clydPLdzRqxInt9STxThRY=

AES Decrypted Output ([Base64](#)):

VGhpccyBpcyBTewItZXRYaWMgS2V5IGVuY3J5
cHRpb24gc2hvd2luZyBob3cgdG8gZG8gZW5jc
nlwdGlvbiB1c2luZyBBRVM=

This is Symmetric Key encryption showing how

EXPERIMENT NO – 11

AIM: Implementation of Network Security Tools and Technologies Lab.

Windows firewall :

Windows Firewall is a stateful firewall that inspects and filters all packets for IP version 4 (IPv4) and IP version 6 (IPv6) traffic. For measuring the performance of windows firewall, first rules are created for inbound and outbound connections and then performance is measured by enabling and disabling the firewall rule. Rule creation In firewall, firewall rules are created to allow this computer to send traffic to or receive traffic from. Firewall rules can be created to take one of two actions for all connections that match the rule's criteria: allow the connection or block the connection. Rules can be created for either inbound traffic or outbound traffic

The rule can be configured to specify the computers, programs, services, ports and protocols. As IT environment changes, user might have to change, create, disable or delete rules. Rule creations involve following steps.

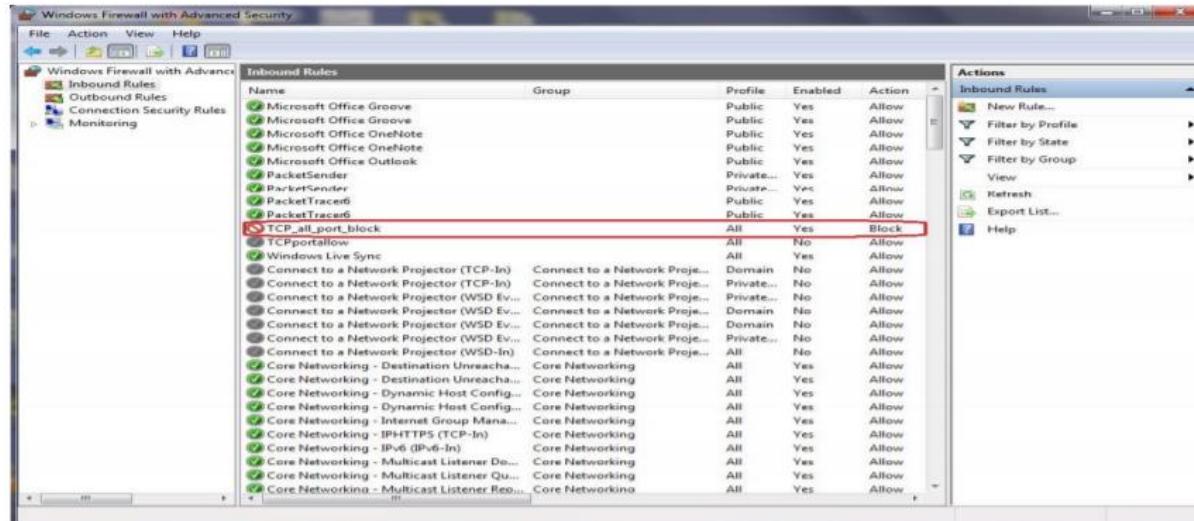
Step 1. Select the rule category either inbound (for incoming connection) or outbound (for outgoing connection)

Step 2. In the second step select the rule type, which type of rule would you like to create? program, port, predefined and custom

Step 3. Select any one rule. For eg. Rule for port has selected, now specified the port number (80,25,20,21) and the protocol (TCP,UDP).

Step 4. Select the action which can be performed if rule matched whether block the connection or allow the connection.

Windows firewall creation:



Linux firewall:

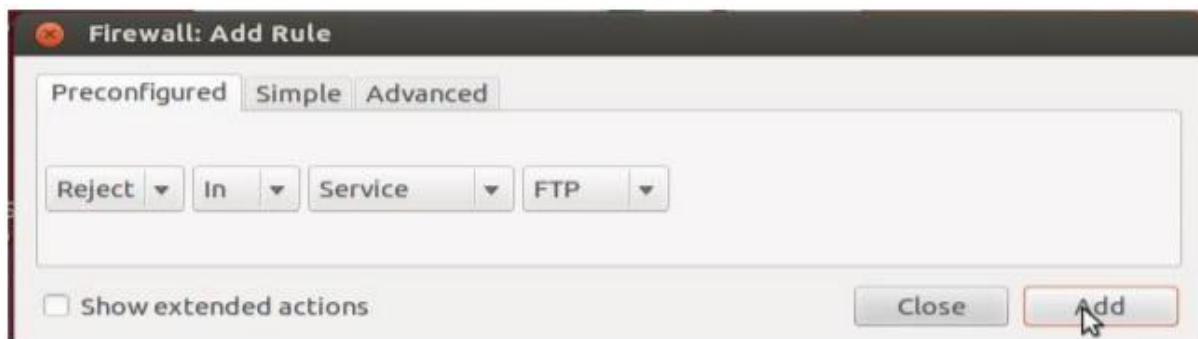
Iptables is an application program that permits a system administrator to configure or manage the iptables provided by the Linux kernel firewall. It is used to setup, maintain and inspect the tables of IP chains. It is a consol based firewall service program that uses policy chains to accept or reject the network traffic. When any connection is tried to establish from any network to private network either inbound or outbound, iptables check for a rule in its stored rule base. If there is a match found then corresponding action take place, otherwise default action is applied. Iptables uses three different chains: input, forward and output.

- Input – This chain is used to control the all incoming connections from the public network. For example, if a user attempts to TELNET or SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.
- Forward – This chain is used for incoming connections that are not actually being delivered locally same as router that forwards the packets to its outgoing links
- Output – This chain is used to control all the outgoing connections from private network to public network. If user tries to access facebook.com, iptables will check its output chain to see what the rules are stored regarding to http before making a decision to allow or deny the connection. There are three types of connection-specific Responses in Iptables
- Accept – Allow the connection.
- Drop – Drop the connection, act like it never happened. This is best when user does not want the source to realize his/her system exists.
- Reject – Do not allow the connection, but send back an error to the originator. This is best if user does not want a particular source to connect to his/her system, but user wants them to know that his/her firewall blocked them.

For measuring the performance of Linux firewall, first rules are created for inbound and outbound connections and then performance is measured by enabling and disabling the firewall.

Rule creation Gufw is a graphical uncomplicated firewall that provides user-friendly frontend to IPTables. It is used to manage the rules and policies of IPTables in easier way. Gufw allows the administrator to create preconfigured, simple and advanced rules

Creating rule to reject FTP:



Shows a firewall rule that will allow tcp port 25 to any address on this host.



Shows ufw status that contains all the created rules.

```
root@jt-OptiPlex-9010:/home/jt
root@jt-OptiPlex-9010:/home/jt# ufw status
Status: active

To                         Action      From
--                         --         --
192.168.33.82/tcp        DENY       192.168.33.20/tcp
21/tcp                     REJECT    Anywhere
25/tcp                     ALLOW OUT  Anywhere

root@jt-OptiPlex-9010:/home/jt#
```