Minor Project-Cyber Security

Cyber Security – An Introductory Practical Guide

Prepared By

Name: Pratik Das

Roll_No: 25/CS-T9/JUNE-5732

Email: daspra0tik@gmail.com

Project Summary

This minor project, titled **"Cyber Security – An Introductory Practical Guide,"** presents a structured exploration of foundational cybersecurity concepts and practical implementations. Designed in a question-and-answer format, the report bridges theoretical understanding with real-world applications through hands-on exercises and demonstrations.

The project begins by classifying the **types of hackers** (White Hat, Black Hat, Grey Hat, etc.) and analyzing the **consequences of hacking in the corporate sector**, including data breaches, financial loss, and reputational damage.

Core cybersecurity practices are demonstrated through:

- **Network Scanning** using *Angry IP Scanner* to identify active hosts and services.
- **Footprinting** via CLI tools and IP geolocation websites to gather target system information.
- **Reconnaissance** using *Recon-ng* to simulate open-source intelligence gathering.
- Assessment of **vulnerabilities**, highlighting their role in exploitation and defense.

Privacy and anonymity tools are covered in detail:

- **Proxy servers** and **VPNs** are explained for secure and anonymous communication.
- The **TOR network** is introduced with a practical on identity switching for private browsing.

Further topics include:

- **Types of malwares** (viruses, worms, trojans, ransomware, etc.) and their impact.
- **Password attacks** such as brute-force and dictionary attacks, and relevant countermeasures.
- **DoS and DDoS attacks**, explaining how service disruption occurs.
- **Sniffing techniques** (active and passive) used for packet capture and analysis.
- Overview of **Kali Linux** and the **Metasploit Framework** for penetration testing.

All practicals are accompanied by relevant screenshots and outputs, ensuring clarity and verification of each task.

1. Explain The various types of Hacker/Hacking. And Consequences of Hacking in the Corporate sector.

➔ Hacking can be explained as the process of gaining access to a System or a server without consent or permission of the rightful owner. It involves bypassing security mechanisms to manipulate or damage data or systems.

There are mainly 3 types of Hackers:

- White Hat Hackers
- Black Hat Hackers
- Grey Hat Hackers

a. White Hat Hackers:

White Hat Hackers, also known as **Penetration Testers** or **Ethical Hackers**, are authorized professionals who test systems for vulnerabilities **with the knowledge and consent of the rightful owners**. Their objective is to help organizations identify and fix security weaknesses before malicious actors can exploit them.

White hat hackers operate within clearly defined **legal and ethical boundaries**, as outlined in formal agreements. These agreements specify the scope of work, limitations, testing procedures, and confidentiality terms. The penetration tester is required to **sign these documents** before conducting any testing activities.

Some common examples of such official agreements include:

- **Rules of Engagement for Penetration Testing**
- **Penetration Testing Authorization Agreement**
- **Security Testing Agreement**
- **Ethical Hacking Engagement Agreement**

These agreements ensure that all testing is conducted safely, legally, and without unintended harm to the target systems.

b. Black Hat Hackers:

Black Hat Hackers are individuals who gain **unauthorized access** to systems, networks, or data with **malicious intent**. Their actions are **illegal and unethical**, often driven by financial gain, sabotage, espionage, or personal challenge.

Unlike white hat hackers, black hats operate **without consent** from the target organization and do not follow any legal agreement or rules. Their methods may include techniques such as:

- Deploying **malware**, **ransomware**, or **spyware**
- Conducting **phishing attacks**
- Exploiting software **vulnerabilities**
- Engaging in **data theft**, **fraud**, or **system disruption**

Black hat activities can lead to severe consequences for organizations, including financial loss, data breaches, legal penalties, and reputational damage. Law enforcement agencies actively pursue and prosecute black hat hackers under cybercrime laws.

c. Grey Hat Hackers:

Grey Hat Hackers fall between white and black hats. They may access systems **without authorization**, but their intentions are not necessarily malicious. In many cases, they identify vulnerabilities in systems and **report them to the organization**—sometimes requesting a reward or public acknowledgment.

However, because grey hats operate **without official permission**, their actions are still considered **unethical and potentially illegal**, even if no harm is caused. Unlike white hats, they do **not sign any formal agreement** or follow an approved scope of testing.

Typical characteristics of grey hat hacking include:

- Scanning websites or networks for vulnerabilities without consent
- Disclosing vulnerabilities publicly if ignored by the affected organization
- Requesting compensation for unsolicited security findings

While grey hats may claim to act in public interest, their lack of authorization means they still pose legal and ethical concerns

2. Explain the below terms. And perform its practical's.

a) Scanning via Angry IP Scanner:

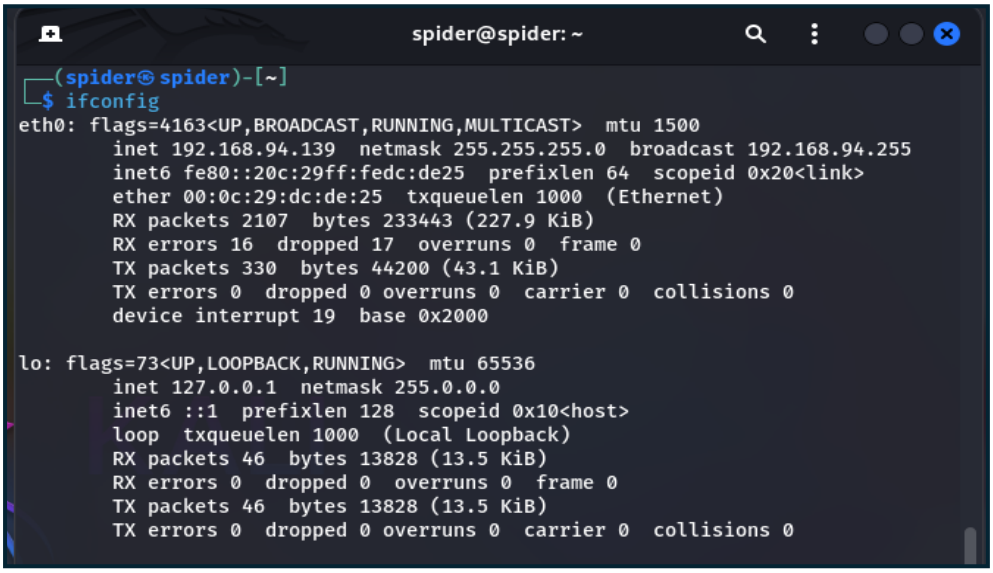
Angry IP Scanner is a lightweight, open-source network scanning tool used to detect **active hosts** and **open ports** within a specified IP range. It is popular for its ease of use, fast scanning capability, and graphical user interface (GUI), making it ideal for beginners and quick assessments.

Key Functions:

- Scans a range of IP addresses.
- Detects which hosts are live (responding).
- Identifies open ports on the detected hosts.
- Displays hostname, ping response time, and NetBIOS information.

Practicals:

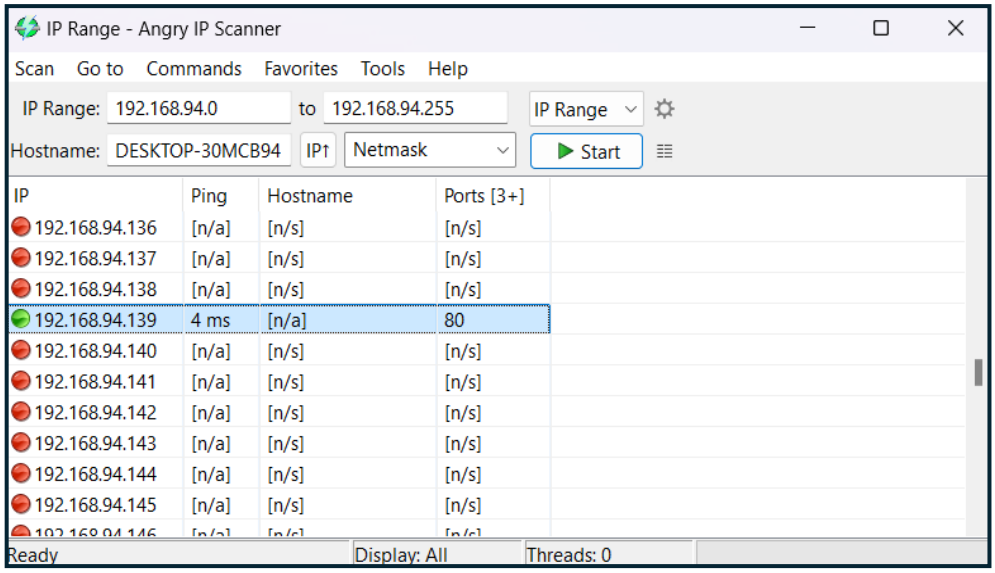
A. Target Ip add: 192.138.94.139



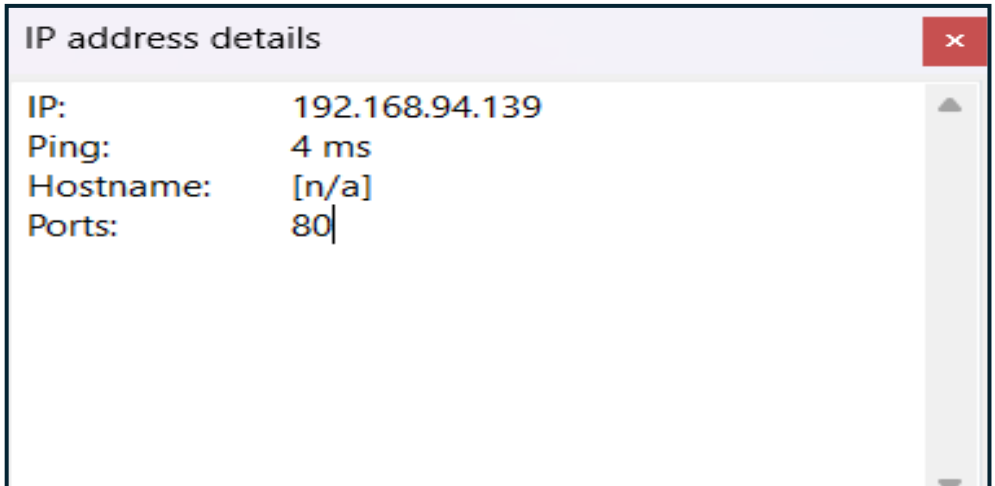
1. This is the target that we are going to scan using Angry Ip scanner

2. We will try to get the host on the Interface and get the target Information like Hostname, Ping and all the open ports of the target.

B. Angry Ip Scanner output:

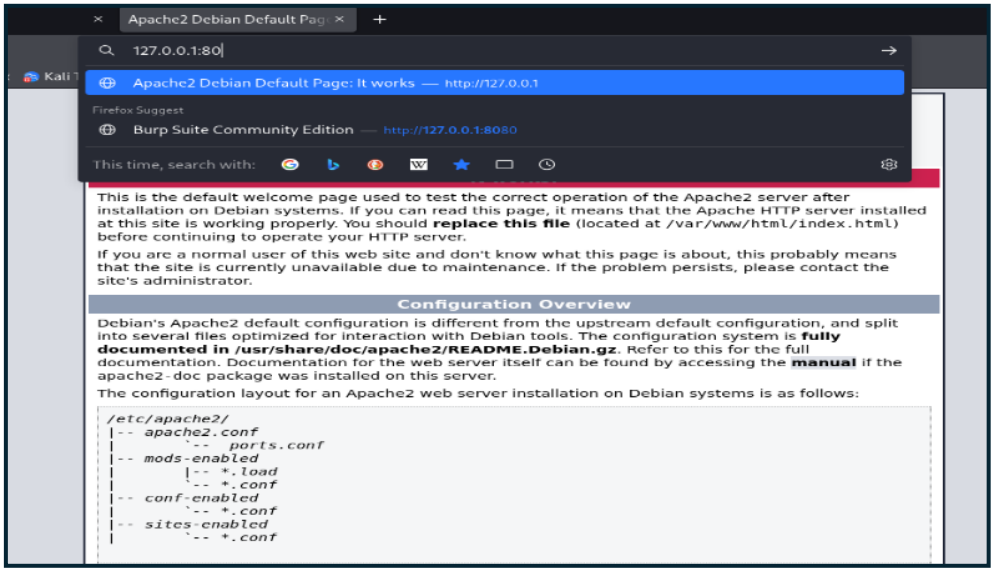


i. So, what we did here is we open the Angry Ip Scanner software and input the Ip range from 192.168.94.0 to 192.168.94.255.
ii. And then we found out target Ip.
iii. We click on it and find its meta data from it like open ports and hostname.



Here we found out the open the information about ping, hostname and the open ports {in this case we can see port 80 is open.

For verification: we can see that on port 80 apache2 web server is online.



b) Foot printing via commands and Ip location through websites.

➔ Footprinting is the first step in the reconnaissance phase of ethical hacking or penetration testing. It involves gathering information about a target system or organization without directly interacting with its internal systems. The goal is to build a profile of the target that includes IP addresses, domain names, network infrastructure, and geographical location.

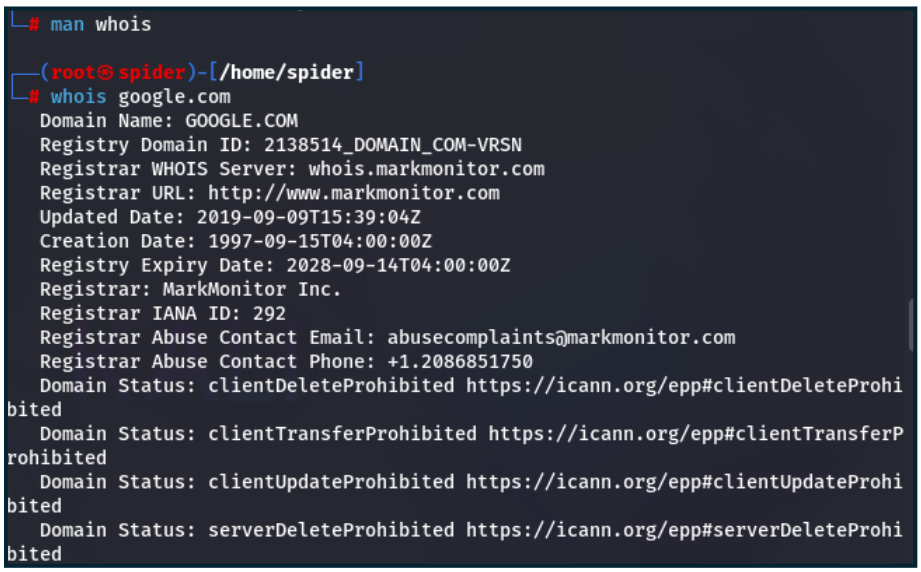
a. Footprinting via Commands (Common Commands)

- nslookup: DNS record lookup
- whois: Domain registration details
- ping: See's weather the host is active or not.

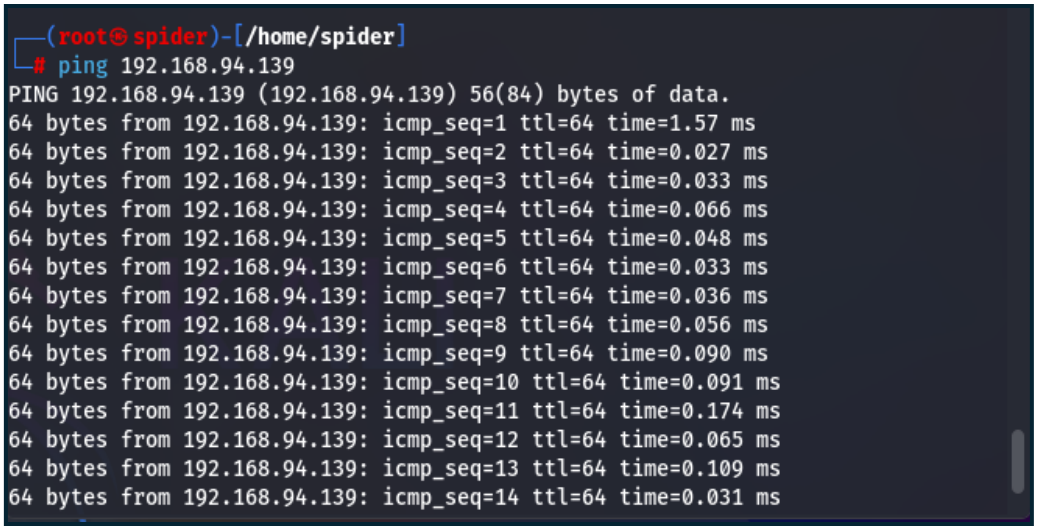
1. nslookup: we found so DNS information like ipv4 Address & ipv6

2. whois: The whois command is used to gather domain registration and ownership information from public records.

And so, on



3. Ping: The ping command checks connectivity between a host and a target IP/domain by sending ICMP echo requests.



Here the ping command will reach the host and return the ICMP sequence. Which is proof that our host is alive.

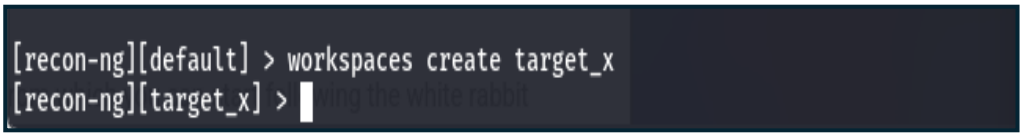
c) Reconnaissance via Recon-ng:

Reconnaissance can be defined as the process of gathering information about a target system, network, or organization. Before launching an attack.

Recon-ng is a powerful open-source web reconnaissance framework written in Python. It automates information gathering by using modules to collect data from public sources like WHOIS, Shodan, and social media.

Practical:

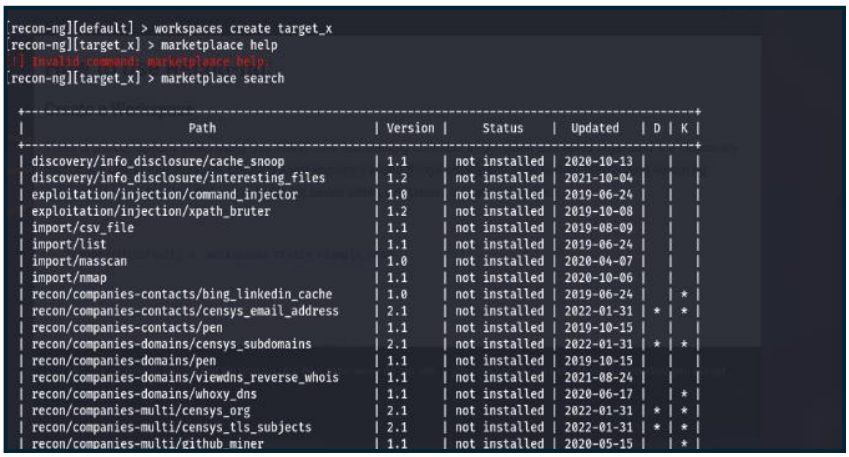
Creating a workspace keeps things orderly and easy to find. When using Recon-ng workspaces, all data located and collected is saved within a database in that workspace.



From the console it is easy to get help and get started with your recon.

Modules are grouped together under various categories and can be found searching on marketplace

- discovery
- exploitation
- import
- recon
- reporting



Example:

To install module: marketplace install hackertarget
→ Installs the recon/domains-hosts/hackertarget module for gathering domain-related information.

Load the Module: modules load hackertarget
→ Loads the module installed into the current workspace for execution

```
[recon-ng][target_x] > modules load hackertarget
[recon-ng][target_x][hackertarget] >
```

Set the Target Domain: options set SOURCE youtube.com
→ Specifies the domain (youtube.com) as the target for reconnaissance

```
[recon-ng][target_x][hackertarget] > options set SOURCE youtube.com
SOURCE => youtube.com
[recon-ng][target_x][hackertarget] >
```

Check Input Configuration: input
→ Confirms the input source (target domain) has been set correctly.

```
recon-ng][target_x][hackertarget] > input

  +---------------+
  | Module Inputs |
  +---------------+
  | youtube.com   |
  +---------------+

recon-ng][target_x][hackertarget] >
```

Run the Module: run
→ Executes the module and displays hostnames and IP addresses related to youtube.com.

```
[recon-ng][target_x][hackertarget] > input

  +---------------+
  | Module Inputs |
  +---------------+
  | youtube.com   |
  +---------------+

[recon-ng][target_x][hackertarget] > run

-----------
YOUTUBE.COM
-----------
[*] Country: None
[*] Host: youtube.com
[*] Ip_Address: 173.194.193.190
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: o-o.preferred.cbf01t01.v3.cache1.c.youtube.com
[*] Ip_Address: 142.250.191.46
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: o-o.preferred.nuq04t11.v1.cache7.c.youtube.com
[*] Ip_Address: 142.250.191.46
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
```

d) Vulnerability:

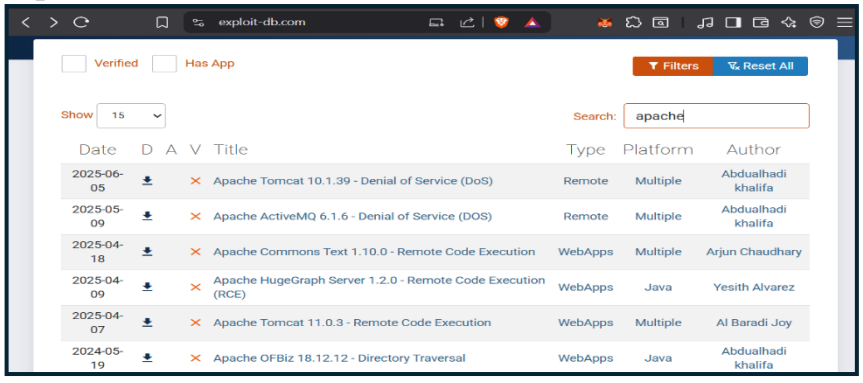
A **vulnerability** is a **weakness or flaw** in a system, application, or network that can be **exploited** by attackers to gain unauthorized access, cause damage, or perform malicious activities.

1. How to Detect Vulnerabilities:

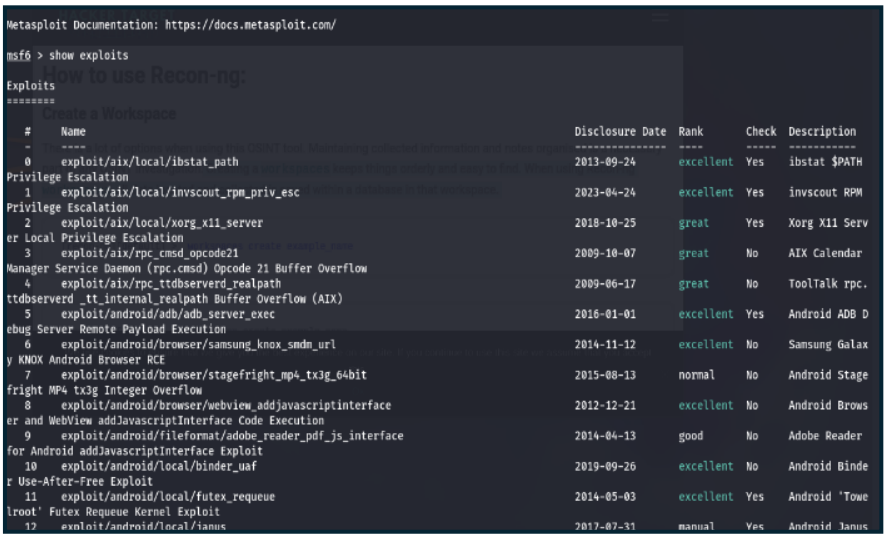
Method	Description
Automated Scanning Tools	Use tools like **Nessus**, **OpenVAS**, **Nikto**, **Nmap (with scripts)** to identify known issues.
Manual Testing	Manually inspecting source code, configurations, or inputs (e.g., SQLi, XSS testing).
Reconnaissance & Enumeration	Information gathering to understand exposed ports, services, and software versions.
Vulnerability Databases	Cross-checking with CVE (Common Vulnerabilities and Exposures), Exploit-DB, or NVD

Commands:

1. Searchsploit/Searchexploit: This command is used to search for exploit vulnerabilities from any open-source platforms like expoiltdb, vulnhub etc.



2.Metasploit is a powerful penetration testing framework that includes a **library of exploits** targeting known vulnerabilities in operating systems, services, and applications



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > show exploits

Exploits
========

   #    Name                                                                Disclosure Date  Rank       Check  Description
   -    ----                                                                ---------------  ----       -----  -----------
   0    exploit/aix/local/ibstat_path                                       2013-09-24       excellent  Yes    ibstat $PATH
Privilege Escalation
   1    exploit/aix/local/invscout_rpm_priv_esc                             2023-04-24       excellent  Yes    invscout RPM
Privilege Escalation
   2    exploit/aix/local/xorg_x11_server                                   2018-10-25       great      Yes    Xorg X11 Serv
er Local Privilege Escalation
   3    exploit/aix/rpc_cmsd_opcode21                                       2009-10-07       great      No     AIX Calendar
Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   4    exploit/aix/rpc_ttdbserverd_realpath                                2009-06-17       great      No     ToolTalk rpc.
ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   5    exploit/android/adb/adb_server_exec                                 2016-01-01       excellent  Yes    Android ADB D
ebug Server Remote Payload Execution
   6    exploit/android/browser/samsung_knox_smdm_url                       2014-11-12       excellent  No     Samsung Galax
y KNOX Android Browser RCE
   7    exploit/android/browser/stagefright_mp4_tx3g_64bit                  2015-08-13       normal     No     Android Stage
fright MP4 tx3g Integer Overflow
   8    exploit/android/browser/webview_addjavascriptinterface              2012-12-21       excellent  No     Android Brows
er and WebView addJavascriptInterface Code Execution
   9    exploit/android/fileformat/adobe_reader_pdf_js_interface            2014-04-13       good       No     Adobe Reader
for Android addJavascriptInterface Exploit
   10   exploit/android/local/binder_uaf                                    2019-09-26       excellent  No     Android Binde
r Use-After-Free Exploit
   11   exploit/android/local/futex_requeue                                 2014-05-03       excellent  Yes    Android 'Towe
lroot' Futex Requeue Kernel Exploit
   12   exploit/android/local/janus                                         2017-07-31       manual     Yes    Android Janus
```

3.Nmap open port scan may lead to many vulnerabilities based on the output {The open ports} and this can give us much information like the OS version details port number and the session running on the specific ports.

```
┌──(root㉿spider)-[/home/spider]
└─# nmap -sV -Pn 10.129.42.195
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 03:52 CDT
Nmap scan report for 10.129.42.195
Host is up (0.18s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp     Postfix smtpd
53/tcp   open  domain   ISC BIND 9.16.1 (Ubuntu Linux)
110/tcp  open  pop3     Dovecot pop3d
143/tcp  open  imap     Dovecot imapd
993/tcp  open  ssl/imap Dovecot imapd
995/tcp  open  ssl/pop3 Dovecot pop3d
3306/tcp open  mysql    MySQL 8.0.27-0ubuntu0.20.04.1
Service Info: Host: InFreight; 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 28.70 seconds
```

3. What is Proxy Server & V.P.N. With Detailed Explanation.

-> A **Proxy Server** acts as an intermediary between a user's device and the internet. When a user makes a request (e.g., visiting a website), the proxy server forwards the request on the user's behalf, retrieves the response, and sends it back to the user. This process hides the user's IP address, providing anonymity and better control over internet access. Proxy servers are widely used for **security**, **content filtering**, and **performance optimization** in both personal and enterprise environments.

In corporate setups, proxy servers help **monitor employee internet activity**, **block malicious content**, and **enforce browsing policies**. Many proxies also catch frequently accessed web content, which reduces bandwidth usage and improves access speed. There are different types of proxy servers—**forward proxy**, **reverse proxy**, **transparent proxy**, and **anonymous proxy**—each with specific roles in managing network traffic.

Key Features of a Proxy Server:

1. ***IP Address Masking: Hides the client's IP address to provide anonymity and privacy.***
2. ***Content Filtering: Blocks access to certain websites or types of content based on predefined rules.***
3. ***Caching: Stores copies of frequently accessed web content to reduce bandwidth usage and improve performance.***
4. ***Access Control: Enforces policies by allowing or denying access to resources based on user credentials or IPs.***
5. ***Security Enhancement: Prevents direct access to internal systems, reducing the risk of attacks like DDoS or unauthorized intrusion.***

➔ VPN stands for Virtual Private Network. It is technology that allows a secure and encrypted connection between a private network and remote device. This allows remote machines to access private networks directly.

- VPNs typically uses the port TCP/1723 for Point-to-point Tunneling Protocol and UDP/500 for IKEv1 VPN connection.

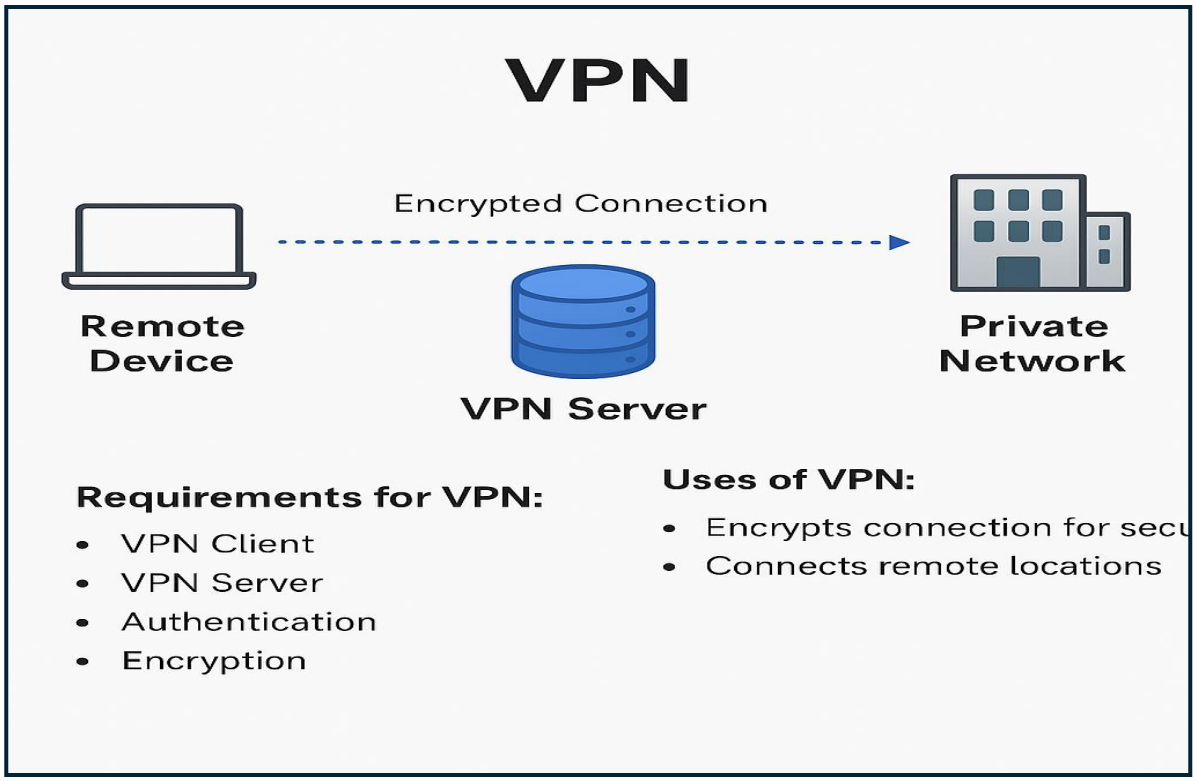
Uses of VPN:

a. VPNs encrypt the connection between the remote device and the private network, making it much more difficult for attackers to intercept and steal sensitive information. With this, the entire communication is more secure.

b. VPNs to connect multiple remote locations, such as branch offices, into a single private network, making it easier to manage and access network resources

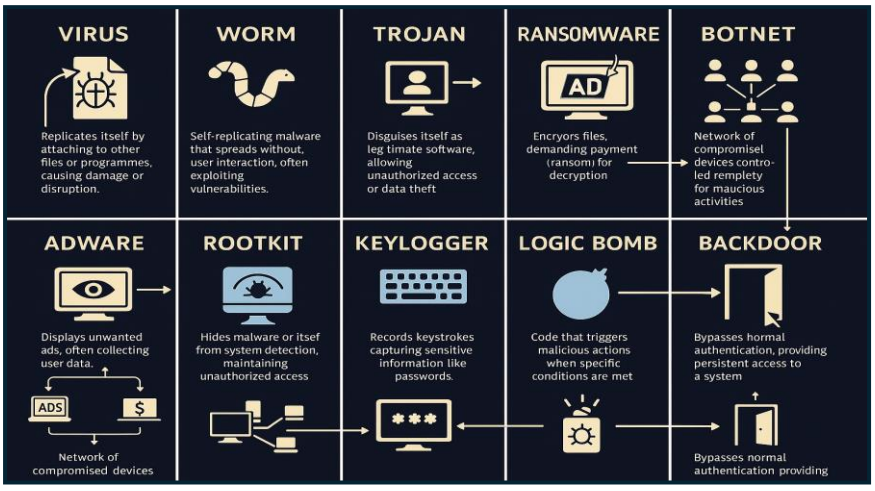
Requirements for VPN to work:

Requirement	Description
VPN Client	Software on the user's device to connect to the VPN.
VPN Server	Accepts connections and routes to traffic to the private network.
Authentication	Verifies client and server identities (e.g., password, certificate).
Encryption	Secures data using protocols like AES or IPsec.


VPN
Encrypted Connection
Remote Device
VPN Server
Private Network
Requirements for VPN:
VPN Client
VPN Server
Authentication
Encryption
Uses of VPN:
Encrypts connection for secu
Connects remote locations

4. What are the Different types of Malwares. Explain it with Detail.

- • Virus – A virus attaches itself to legitimate programs or files and spreads when these are executed. It can corrupt or delete data and damage system functionality.
- • Worm – A worm is a standalone malicious program that replicates itself and spreads across networks, often exploiting security vulnerabilities without user action.
- • Trojan – A Trojan disguise itself as useful software, but once installed, it opens a backdoor for attackers to steal data or gain control over the system.
- • Ransomware – Ransomware locks or encrypts files and demands a ransom from the victim to restore access, often through cryptocurrency payments.
- • Adware – Adware automatically delivers unwanted advertisements and may redirect browser searches while secretly collecting user data for advertisers.
- • Spyware – Spyware secretly observes user behavior, logging keystrokes or capturing screenshots to steal sensitive data like passwords or credit card information.
- • Rootkit – A rootkit hides malicious software or actions, allowing attackers to maintain privileged access to a system while avoiding detection by antivirus tools.
- • Keylogger – A keylogger records every keystroke made on a device, making it easy for attackers to collect usernames, passwords, and confidential information.
- • Botnet – A botnet is a network of infected devices controlled by a hacker, used to launch large-scale attacks like DDoS, spamming, or data theft.
- • Logic **Bomb** – A logic bomb lies dormant in a system until triggered by a specific event or condition, such as a date or user action, then executes malicious code.



5. What is TOR Network and Practically Explain how to Create Identities.

➔ **TOR (The Onion Router)** is a **decentralized anonymous network** that routes your internet traffic through **multiple encrypted relays (nodes)**. This prevents websites, ISPs, or governments from tracking your browsing activity or IP address.

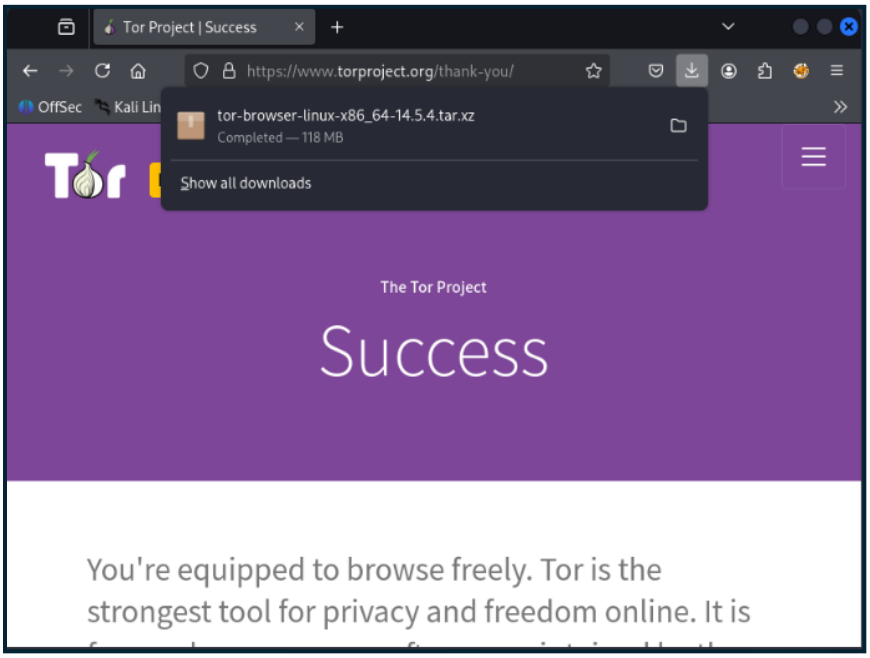
- TOR allows **anonymous communication**.
- It can access. onion **(dark web)** websites not available on normal browsers.
- Mainly used for **privacy**, **research**, or bypassing censorship.

Practical: Step-by-Step Guide to Use TOR & Create Identities:

1.Download and install TOR browser on the machine

a. Go to the official website: https://www.torproject.org

b. Click on the Download as per the machine its available for both windows and Linux.



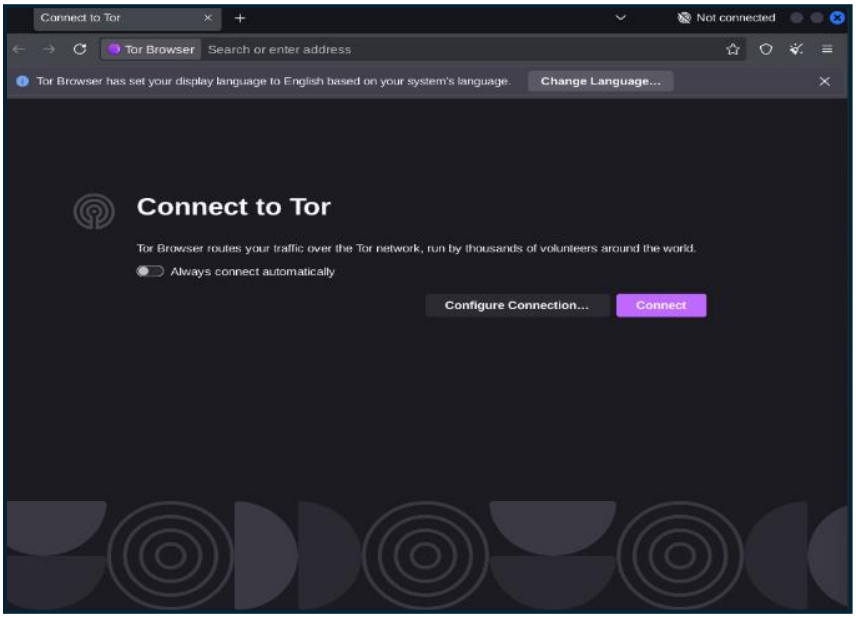
2. Lunch TOR Browser:

a. Open the installed TOR Browser

b. On first launch, it will ask:

i. **"Connect"**: Click this to join the TOR network (works in most regions).

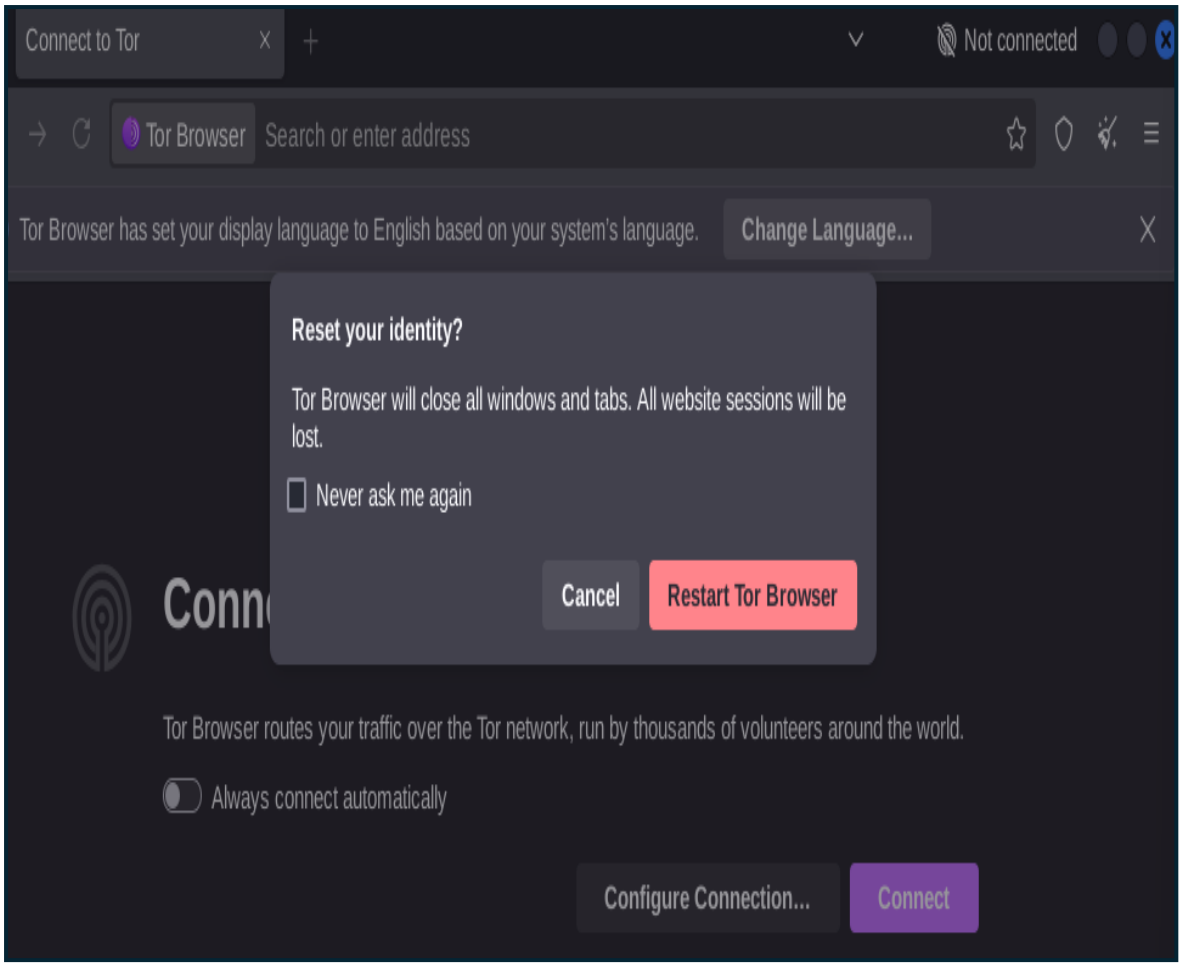
ii. **"Configure"**: If you're behind a firewall/censorship (e.g., in Iran, China).



3. Create New Identities in TOR:

A **"New Identity"** resets your TOR session and gives you a **new IP address**.

- **Keyboard Shortcut**
  - Press: Ctrl + Shift + U
    This does the same thing as "New Identity" in one go.



6. *Explain Password Attacks*.

-> Password **attacks are techniques used by attackers (or ethical hackers during testing) to gain unauthorized access to systems by cracking or guessing passwords.**

The most common types of Password attacks are:

1. Brute-force
2. Dictionary Attack
3. Phishing Attack
4. Keylogging

Explanation:

1. *Brute-Force:*

• Method: Attempts **all possible combinations** of characters.

• Use **Case**: When password complexity is unknown.

• Tools: Hydra

• Cons: Extremely time-consuming for long/complex passwords.

2. ***Dictionary Attack:***
   - **Method**: Tries passwords from a **list of commonly used words**.
   - **Use Case**: Target uses weak or predictable passwords.
   - **Tools**: John the Ripper, Hydra
   - **Faster than brute-force** but limited to the wordlist's content.

3. *Phishing Attack:*

- Method: **Tricks users** into revealing their passwords via fake emails or websites.

- Use **Case**: Social engineering to bypass technical security.

- Tools: SET (Social Engineering Toolkit), Gophish

- Highly **effective** when users are unaware.

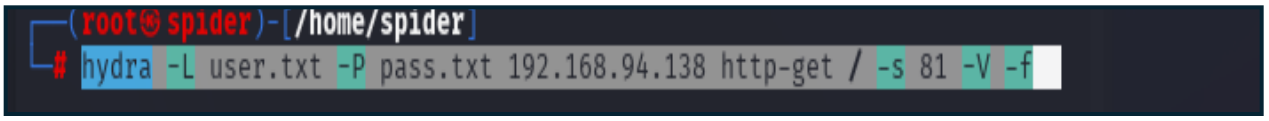
4. ***Keylogging***:

- Method: **Monitors and records keystrokes** to steal credentials.

- Use **Case**: Capturing passwords silently over time.

- Tools: Logkeys, Spyrix Free Keylogger

- Often delivered via **malware** or physical access



Sample Command for Both Dictionary and Brute-force attack.

Where Hydra is the tool used to carry out this attack.

User.txt is the dictionary or list of the possible user on target 192.168.94.138

Pass.txt is the list of the possible passwords for a specific user.

7. What isa Dos & DDos Attack.

-> ***1. DoS (Denial of Service) Attack***

*A **Denial of Service (DoS)** attack is a type of **cyberattack** where an attacker attempts to make a system, service, or network **unavailable** to its intended users. This is done by **flooding the target** with massive amounts of traffic or sending it specially crafted data to **crash or freeze** it.*

- ***How it Works:***
  - *The attacker uses a **single system** to send repeated requests or traffic to a target server.*
  - *This overloads the server's resources (CPU, RAM, bandwidth), making it **slow or completely unresponsive**.*

-> 2. DDoS (Distributed Denial of Service) Attack

*A **Distributed Denial of Service (DDoS)** attack is a **more powerful and dangerous form** of a DoS attack. It involves **multiple compromised systems** (often called a **botnet**) attacking a single target simultaneously.*

- ***How it Works:***
  - *The attacker infects many computers/devices with malware to control them remotely (creating a **botnet**).*
  - *These infected machines are then used to **send traffic or malicious data** to the target system at the same time.*
  - *The large volume of traffic **crashes the server or slows it down severely**.*

Difference Between DoS and DDoS

Feature	***DoS Attack***	***DDoS Attack***
Origin	*Single device*	*Multiple devices (botnet)*
Traffic Volume	*Limited*	*Very large and hard to block*
Detection	*Easier*	*More difficult due to multiple sources*
Risk Level	*Moderate*	*High*

⚙️ ***Common Tools Used in DoS/DDoS***

- ***DoS****: ping of death, slowloris, hping3*
- ***DDoS****: LOIC, HOIC, Botnets like* ***Mirai***

8. ***What is Sniffing and their types.***

-> ***Sniffing*** *is a technique used to* ***capture and monitor network traffic****. It involves intercepting data packets that are transmitted over a network. Sniffing can be:*

- ***Legitimate****: For network analysis and troubleshooting (by admins).*
- ***Malicious****: Used by attackers to steal sensitive data like passwords, emails, or credit card info.*

- ***How Sniffing Works***

  When data travels through a network, it's broken into small units called ***packets****. A sniffer tool* ***listens to these packets****, collecting data like:*

  - *IP addresses*
  - *Usernames & passwords*
  - *Email content*
  - *URLs visited*

Types of Sniffing:

a. Passive Sniffing

- ***Definition****: Listening to traffic* ***without interfering****.*
- ***Where it works****: Only in* ***hub-based networks*** *or* ***Wi-Fi environments****.*
- ***Purpose****: Attacker silently monitors traffic.*
- ***Tools****: Wireshark*

b. Active Sniffing

- ***Definition****: Involves* ***interfering*** *with the network to redirect traffic to the attacker's machine.*
- ***Used in****: Switched networks (most modern networks).*
- ***Techniques****:*
  - ***ARP Spoofing***
  - ***MAC Flooding***
  - ***DHCP Spoofing***
- ***Tools****: Ettercap, Cain & Abel, Bettercap*

Examples of Sniffing Tools

Tool	***Purpose***
Wireshark	*Packet capture & analysis*
Ettercap	***ARP poisoning, MITM***

9. ***Explain about Kali Linux, Metasploit framework and its usage***

-> ***Kali Linux and Metasploit Framework***

1. What is Kali Linux?

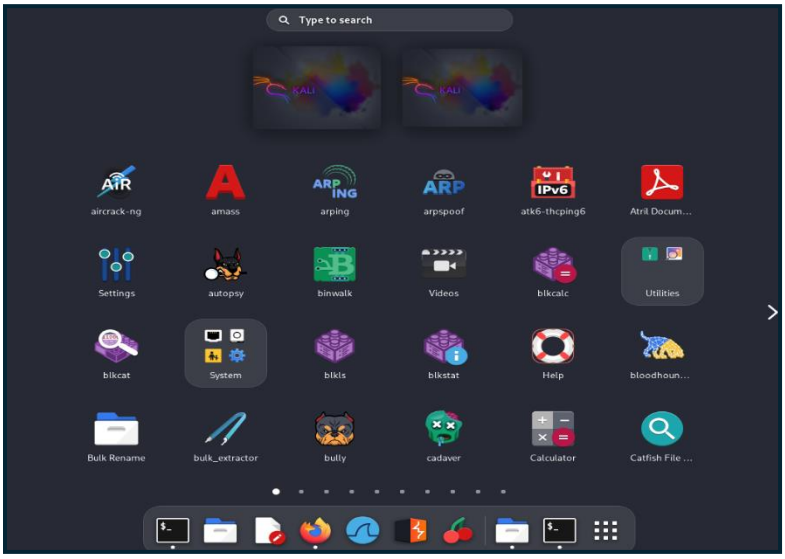
***Kali Linux** is a **Debian-based Linux distribution** specially designed for **penetration testing**, **digital forensics**, and **ethical hacking**.*

a. Key Features:

- *Comes pre-installed with **600+ cybersecurity tools**.*
- *Regularly maintained and updated by **Offensive Security**.*
- *Free and open source.*
- *Lightweight and can run on virtual machines or USB.*

b. Commonly Used Tools in Kali:

- ***Nmap** – Network scanning*
- ***Wireshark** – Packet analysis*
- ***Burp Suite** – Web vulnerability testing*
- ***Hydra** – Brute force attacks*
- ***Metasploit** – Exploitation and payload delivery*



2. What is Metasploit Framework?

*The **Metasploit Framework** is one of the most powerful tools in cybersecurity for:*

- ***Finding vulnerabilities***
- ***Developing exploits***
- ***Testing security defenses***
- ***Gaining access to remote systems***

*It is both **used by ethical hackers** for testing, and **feared by organizations** if used maliciously.*

a. Key Components:

- ***Exploit**: The code used to take advantage of a vulnerability.*
- ***Payload**: The code that runs after exploitation (e.g., reverse shell).*
- ***Module**: Ready-to-use scripts for different attack types.*
- ***Listener (Handler)**: Waits for a connection back from the target.*

***If successful**, you'll get a **meterpreter shell**, allowing remote control of the target.*

🎯 *Use Cases in Cybersecurity:*

Task	*Tool (Kali/Metasploit)*
Network Scanning	*Nmap, Zenmap*
Web Application Testing	*Burp Suite, Nikto*
Password Attacks	*Hydra, John the Ripper*
Exploiting Vulnerabilities	*Metasploit*
Privilege Escalation	*Local exploit modules*
Post-Exploitation (backdoor)	*Meterpreter, persistence scripts*