SCANNING

- **Scanning** is the second phase of Ethical Hacking (after Foot printing).

- It involves **actively collecting detailed information** about the target system, such as open ports, running services, vulnerabilities, and network structure.

What is Scanning ?

- **Scanning** is a network exploration technique used to systematically examine a target system or network to gather detailed, specific information.
- It involves actively interacting with the target to identify active hosts, open ports, available services, operating systems, and potential vulnerabilities.
- It's the phase where an attacker or security professional moves from general information gathering to detailed, technical probing.

Types of Scanning :

1. **Network scanning**
   The involves discovering live hosts and identifying their IP addresses on a network.

   - **Techniques :**

     - **Ping Sweep :** Sending ICMP echo requests (pings) to a range of IP addresses to see which ones respond, indicating an active host.
     - **ARP Scanning :** Used on local networks to discover active devices by sending Address Resolution protocol (ARP) requests.

2. **Port scanning**
   A techniques used to identify open , closed , or filtered ports on a network host. An open port means a service is listening on that port , which is a potential entry point.

- **Techniques :**
    - **TCP connect scan :** Completes the full TCP three -way handshake **(SYN -> SYN / ACK ->ACK).** It is accurate but easily logged.
    - **SYN scan :** Sends a SYN packet but doesn't complete the handshake (SYN -> SYN / ACK -> ACK -> RST). It's "stealthier" because it often avoids full logging on the target.
    - **UDP scan :** Probes UDP ports , which are connectionless. An open UDP port typically yields no response , while a closed port returns an ICMP "port Unreachable" error.

3. Vulnerability scanning

This is the automated process of detecting known vulnerabilities in systems and software by comparing system data against a database of known security flaws.

- **Techniques :**
    - **Process :** The scanner identifies the OS/application/version and checks its vulnerability database for any associated weaknesses.
    - **Output :** Generates a report detecting the vulnerabilities , their severity , and often , remediation steps.

Purpose of scanning

The primary purpose of scanning is to collect intelligence that will inform the subsequent phases of an attack or security assessment. This information includes:

- **Host Discovery:** Identifying which IP addresses within a range correspond to **live systems** (active hosts) on the network.
- **Service Enumeration:** Determining which **services** (like HTTP, FTP, SSH, etc.) are running and the **port numbers** they are listening on.
- **Operating System (OS) Fingerprinting:** Detecting the **operating system** and even the specific version running on a host.
- **Vulnerability Identification:** Locating **known weaknesses** (vulnerabilities) in the target's systems, services, or configurations that could be exploited.
- **Network Mapping:** Creating a **topology map** of the network architecture.

Common Tools:

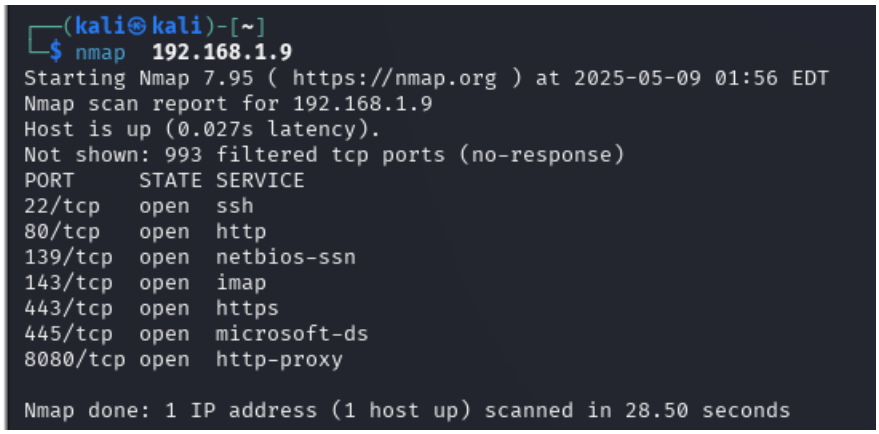
- Nmap – Port and network scanning.
- **Netcat** – Port scanning and banner grabbing.
- **Nessus/OpenVAS** – Vulnerability assessment.
- **Nikto** – Web server vulnerability scanning.
- **Wireshark** – Packet capture and analysis.

1) Nmap :

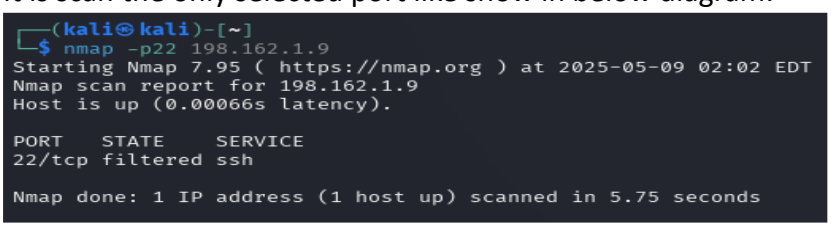
- Nmap, short for Network Mapper, is a free and open-source utility used for network discovery, security auditing, and port scanning.
- It is the most fundamental and widely used tool for the scanning phase of ethical hacking and penetration testing.
- Nmap operates by sending specially crafted **raw IP packets** to a target network or host and then analyzing the responses to gather detailed information.

The common and most used command for scanning the network .

I. **nmap 192.168.1.9**
It is show the all open ports of targeting machines.



II. **nmap -p22 192.168.1.9**
It is scan the only selected port like show in below diagram.



III. nmap -p22–1000 192.168.1.9

In this command we give the range of ports we want to check.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p22-1000 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:08 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.50% done; ETC: 02:18 (0:08:33 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.54% done; ETC: 02:17 (0:06:57 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:05:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.55% done; ETC: 02:14 (0:00:55 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:07:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 02:15 (0:00:00 remaining)
Stats: 0:07:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 02:16 (0:00:00 remaining)
Nmap scan report for 192.168.1.9
Host is up (2.6s latency).
Not shown: 972 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  open     http
139/tcp open     netbios-ssn
143/tcp open     imap
443/tcp open     https
445/tcp open     microsoft-ds
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 468.48 seconds
```

IV. nmap -p22,80,8080,443 192.168.1.9

This command is use to scan given specific ports.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p22,80,8080,443 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:21 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0037s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

V. nmap -p- 192.168.1.9

This command scans all the port of targeted machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 03:07 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0093s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 165.84 seconds
```

VI. nmap -sV 192.168.1.9

This command shows the service versions of ports of targeted machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 01:54 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0043s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2
.6.5 mod_ssl/2.2.14 OpenSSL ... )
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2
.6.5 mod_ssl/2.2.14 OpenSSL ... )
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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 65.13 seconds
```

VII. nmap -O 192.168.1.9

This command is for scanning and it shows the operating system of targeted machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 03:21 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0078s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (93%), Actiontec MI424WR-GEN3I WAP (90%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 SP2 (88%), HP Officejet Pro 8500 printer (87%), Linux 3.2 (87%), Linux 4.4 (87%)
, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (87%), ReactOS 0.3.7 (87%), D-Link DFL-700 firewall (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.28 seconds
```

VIII. nmap -A 192.168.1.9

This Command shows the Operating System, Service version and Trace route of targeted machine.

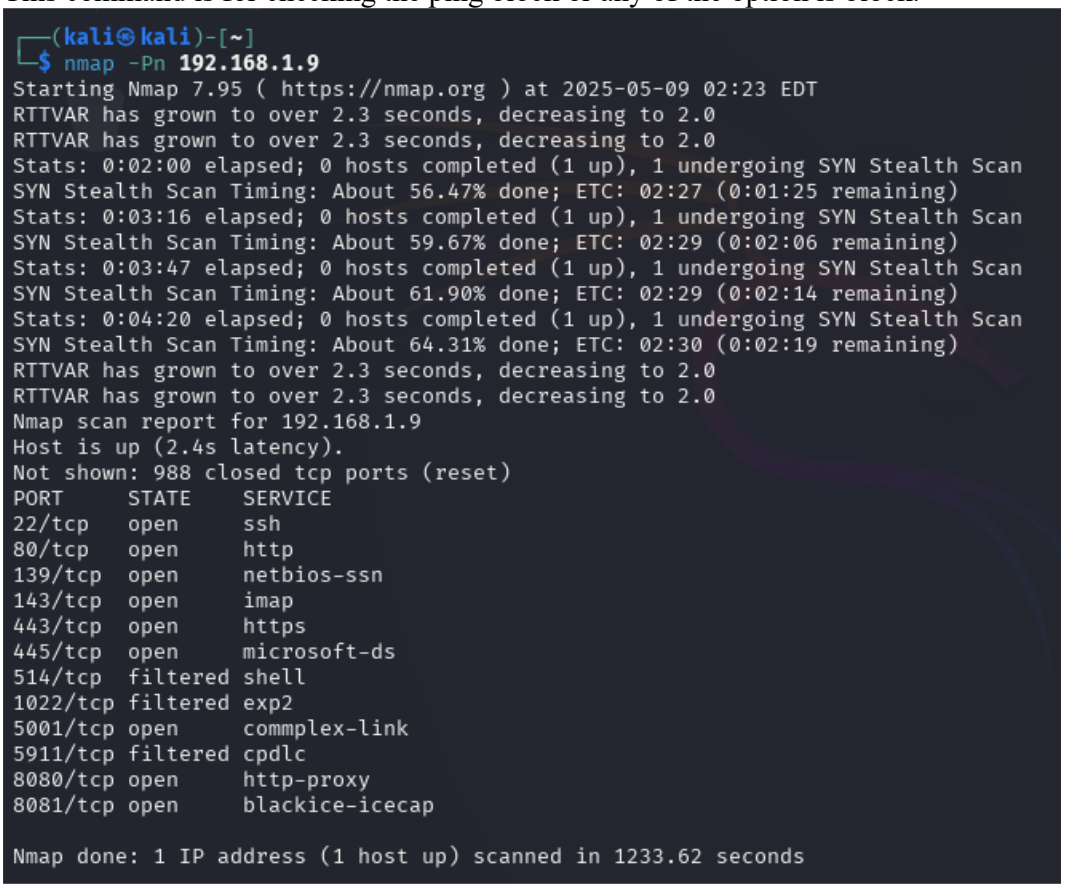
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 03:20 EDT
Nmap scan report for 192.168.1.9
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE VERSION
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (93%), Actiontec MI424WR-GEN3I WAP (90%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 SP2 (88%), HP Officejet Pro 8500 printer (87%), Linux 3.2 (87%), Linux 4.4 (87%)
, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (87%), ReactOS 0.3.7 (87%), D-Link DFL-700 firewall (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.63 ms 192.168.8.2
2   0.68 ms 192.168.1.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.63 seconds
```

IX. nmap -Pn 192.168.1.9

This command is for checking the ping block or any of the option is block.



X. nmap -Sn 192.168.1.9

For checking the Ping.

XI. nmap -sC 192.168.1.9

For finding a basic vulnerability it scans a machine.

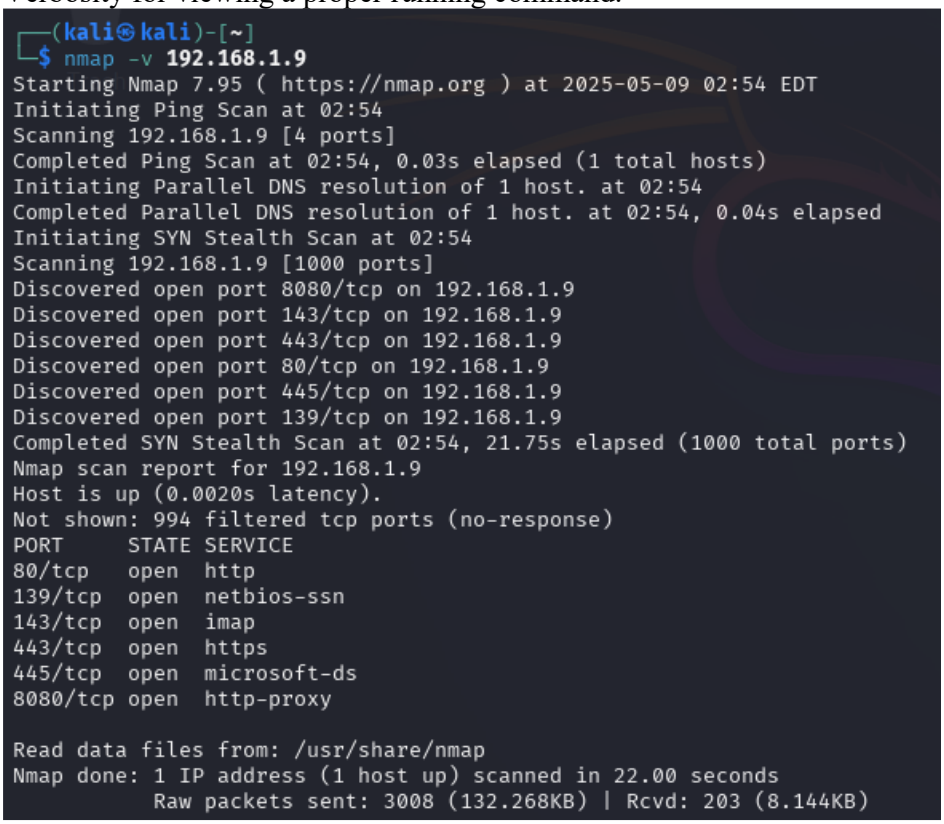
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:51 EDT
Nmap scan report for 192.168.1.9
Host is up (0.044s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp  open  netbios-ssn
143/tcp  open  imap
|_imap-capabilities: SORT CHILDREN OK IMAP4rev1 THREAD=REFERENCES CAPABILITY completed ACL2=UNIONA0001 UIDPLUS ACL QUOTA IDLE THREAD=ORDEREDSUBJECT NAMESPACE
443/tcp  open  https
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=owaspbwa
| Not valid before: 2013-01-02T21:12:38
|_Not valid after:  2022-12-31T21:12:38
|_ssl-date: 2025-05-09T06:52:08+00:00; +7s from scanner time.
|_http-title: owaspbwa OWASP Broken Web Applications
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
|_http-title: Site doesn't have a title.
8081/tcp open  blackice-icecap

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 6s, deviation: 0s, median: 6s
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 68.51 seconds
```

XII. nmap -v 192.168.1.9

Verbosity for viewing a proper running command.

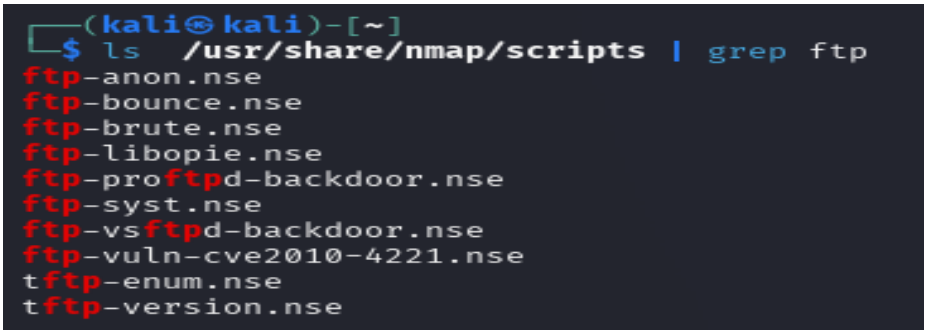


```
┌──(kali㉿kali)-[~]
└─$ nmap -v 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:54 EDT
Initiating Ping Scan at 02:54
Scanning 192.168.1.9 [4 ports]
Completed Ping Scan at 02:54, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:54
Completed Parallel DNS resolution of 1 host. at 02:54, 0.04s elapsed
Initiating SYN Stealth Scan at 02:54
Scanning 192.168.1.9 [1000 ports]
Discovered open port 8080/tcp on 192.168.1.9
Discovered open port 143/tcp on 192.168.1.9
Discovered open port 443/tcp on 192.168.1.9
Discovered open port 80/tcp on 192.168.1.9
Discovered open port 445/tcp on 192.168.1.9
Discovered open port 139/tcp on 192.168.1.9
Completed SYN Stealth Scan at 02:54, 21.75s elapsed (1000 total ports)
Nmap scan report for 192.168.1.9
Host is up (0.0020s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
           Raw packets sent: 3008 (132.268KB) | Rcvd: 203 (8.144KB)
```

XIII. ls/usr/share/nmap/script | grep "ftp"

This command is for accessing the inbuild Script of nmap we can use for hacking any machine. In this example (Command) we are specifically finding the exploit for ftp service.



XIV. nmap –script =___address_of_script_____ 192.168.1.9

In this command we are running script that we take from inbuild nmap scripts for targeted machine.

2) Nikto :

- **Nikto** is an open-source, command-line **web server and web application vulnerability scanner**.
- It is a specialized tool in the scanning phase that focuses specifically on the security of the web server itself (like Apache, Nginx, IIS) and the web applications running on it.

3) Wireshark :

- **Wireshark** is the world's leading **network protocol analyzer** (or packet sniffer).
- It is a free, open-source tool used to capture, inspect, and analyze network traffic in real-time, providing deep visibility into the individual data packets flowing across a network interface.
- It's an essential tool for network administrators, security professionals, developers, and ethical hackers, as it allows users to see exactly what is happening on the network at a granular, packet level.