NETWORK SCANNING & ENUMERATION DASHBOARD

By: Drishti Bhat(2023a7r006)
CSE (Cybersecurity)

Network Scanning

- Process that helps in detecting the live hosts and identifying the open ports
- Maps services that are running over the network
- Reveals the potential vulnerabilities
- Helps cybersecurity professionals plan defense mechanisms

Enumeration

- Process of extracting the detailed information about each system identified during network scanning.
- Actively connects to gather the data.
- Helps in identifying the potential security flaws
- Helps attackers/escalators understand the way to gain higher access.

Objectives

- Automate the discovery of devices in the network.
- Perform service enumeration and OS detection.
- Generate a timestamped dashboard with key scan insights.
- Recommend defenses against potential risks discovered.

Tools Used

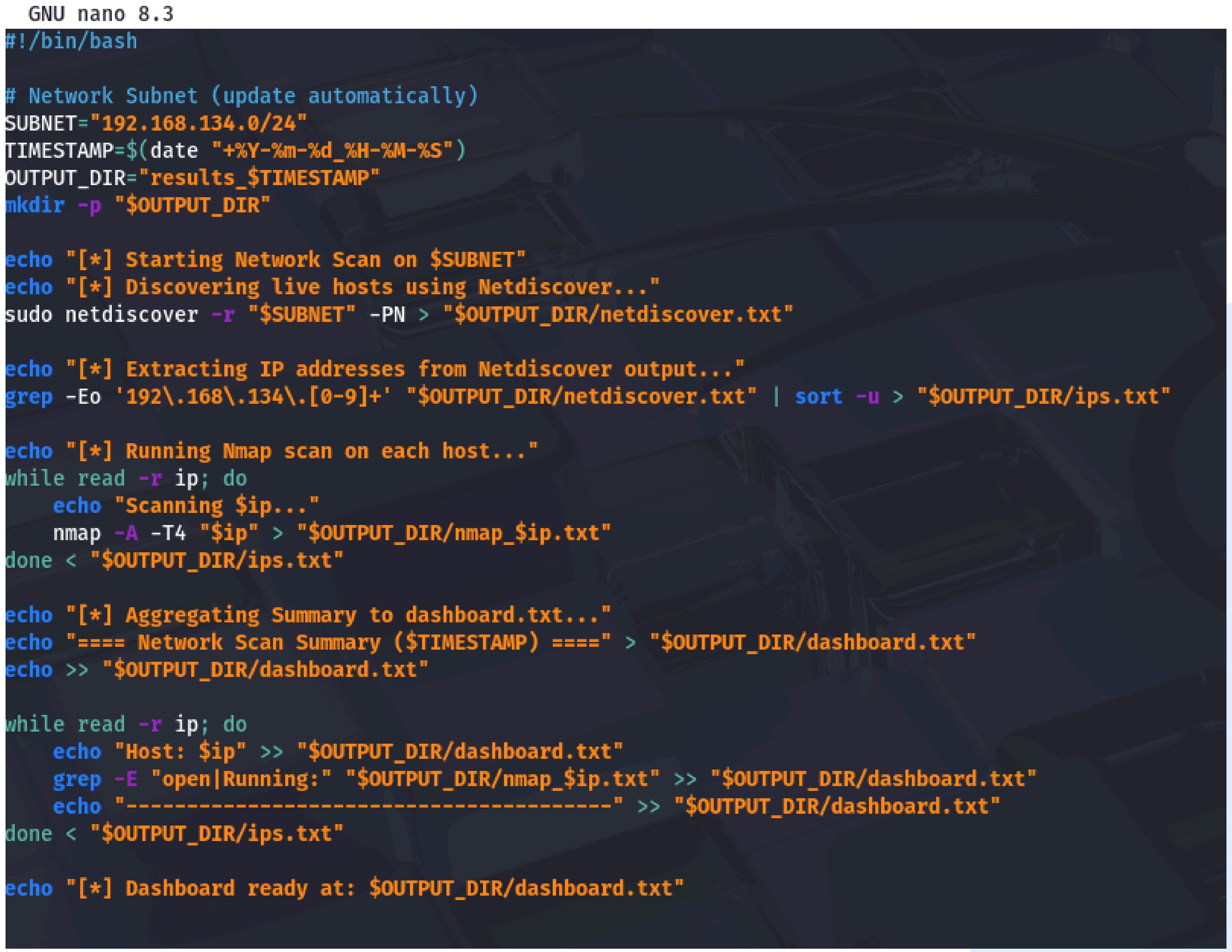
- netdiscover :- Identify live hosts in a subnet
- nmap :- Port scanning, service and OS detection
- bash script :- Automation of scans and result logging
- Text editor :- For script creation and editing
- Terminal(Kali) :- Command execution

Methodology

- First we here used command: **nano diya.sh**

Purpose:

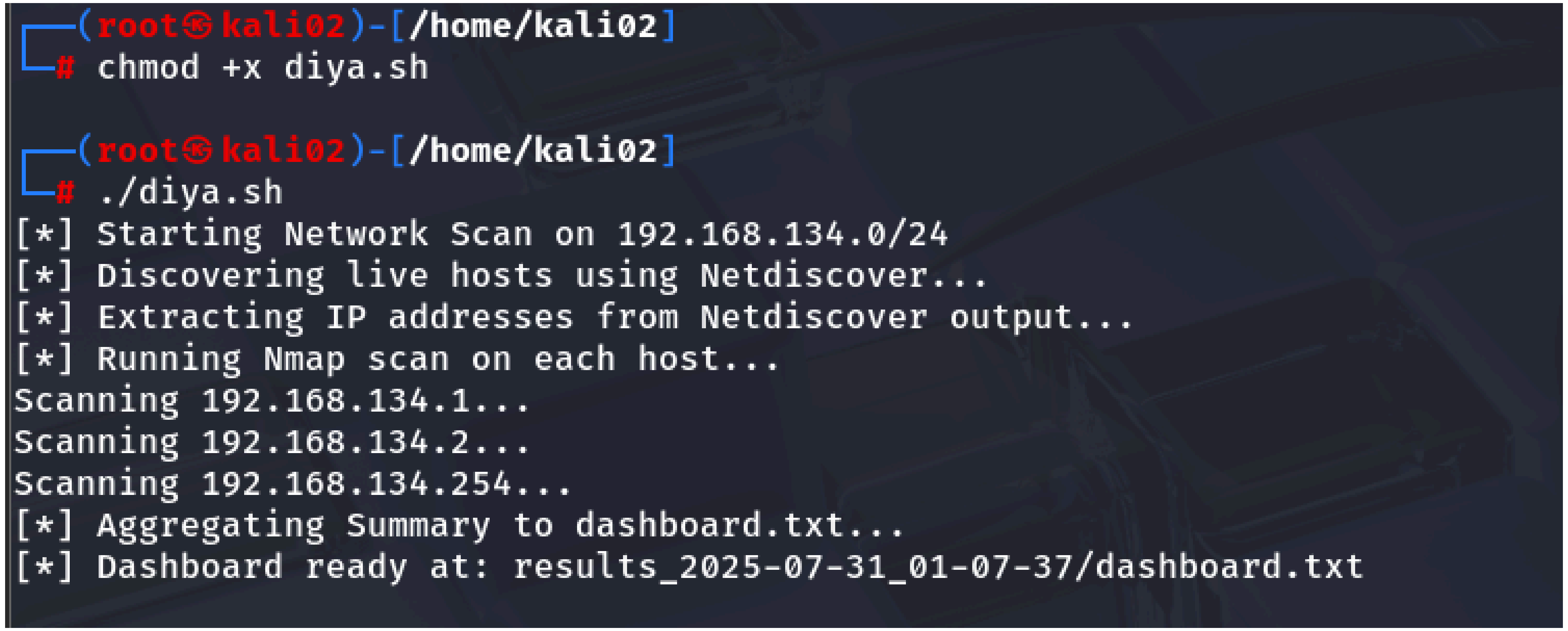
- Opens a terminal-based text editor to create or edit the shell script named diya.sh.
- The script that we will write here will be including in the script is the subnet,the tools netdiscover and nmap and the time stamped dashboard’s text file (the output will be saved here)
- Commands are: netdiscover -r "$SUBNET"(tells which ip’s are alive) and nmap -A -T4 "$ip"(scans the ip’s)



```
  GNU nano 8.3
#!/bin/bash

# Network Subnet (update automatically)
SUBNET="192.168.134.0/24"
TIMESTAMP=$(date "+%Y-%m-%d_%H-%M-%S")
OUTPUT_DIR="results_$TIMESTAMP"
mkdir -p "$OUTPUT_DIR"

echo "[*] Starting Network Scan on $SUBNET"
echo "[*] Discovering live hosts using Netdiscover..."
sudo netdiscover -r "$SUBNET" -PN > "$OUTPUT_DIR/netdiscover.txt"

echo "[*] Extracting IP addresses from Netdiscover output..."
grep -Eo '192\.168\.134\.[0-9]+' "$OUTPUT_DIR/netdiscover.txt" | sort -u > "$OUTPUT_DIR/ips.txt"

echo "[*] Running Nmap scan on each host..."
while read -r ip; do
    echo "Scanning $ip..."
    nmap -A -T4 "$ip" > "$OUTPUT_DIR/nmap_$ip.txt"
done < "$OUTPUT_DIR/ips.txt"

echo "[*] Aggregating Summary to dashboard.txt..."
echo "==== Network Scan Summary ($TIMESTAMP) ====" > "$OUTPUT_DIR/dashboard.txt"
echo >> "$OUTPUT_DIR/dashboard.txt"

while read -r ip; do
    echo "Host: $ip" >> "$OUTPUT_DIR/dashboard.txt"
    grep -E "open|Running:" "$OUTPUT_DIR/nmap_$ip.txt" >> "$OUTPUT_DIR/dashboard.txt"
    echo "----------------------------------------" >> "$OUTPUT_DIR/dashboard.txt"
done < "$OUTPUT_DIR/ips.txt"

echo "[*] Dashboard ready at: $OUTPUT_DIR/dashboard.txt"
```

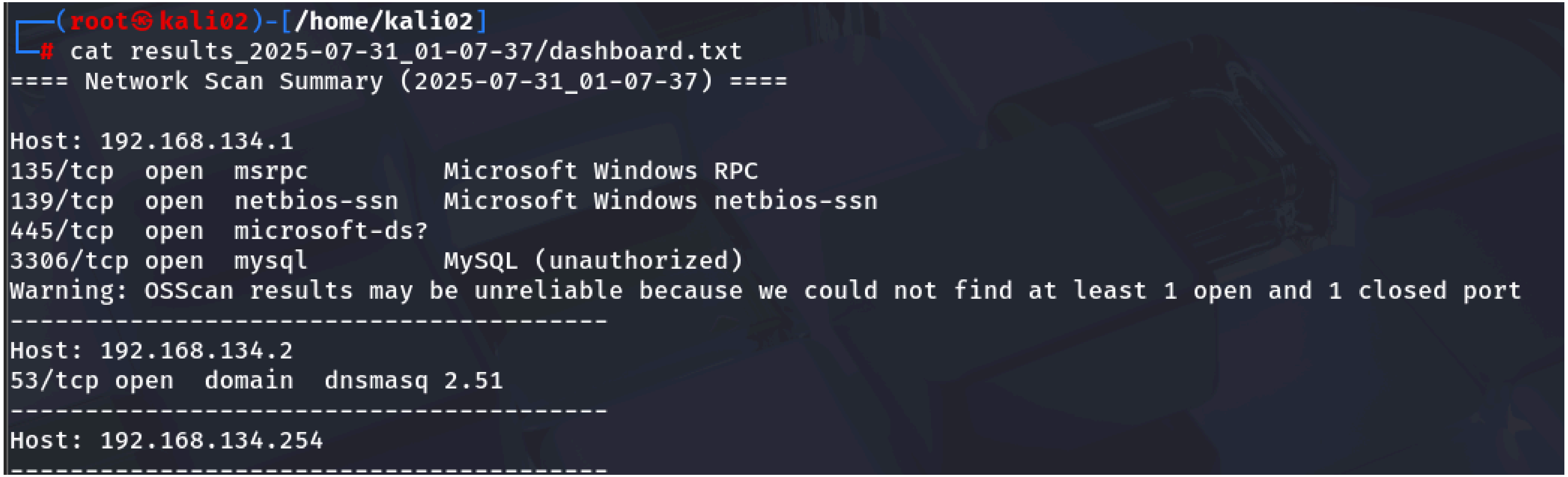
- Now the command we are using here is **chmod +x diya.sh** to make the script named diya.sh executable.

- Then we'll use is **./diya.sh** which helps in running the diya.sh script step by step and automate scanning, IP extraction, Nmap, & report creation.



```
┌──(root㉿kali02)-[/home/kali02]
└─# chmod +x diya.sh

┌──(root㉿kali02)-[/home/kali02]
└─# ./diya.sh
[*] Starting Network Scan on 192.168.134.0/24
[*] Discovering live hosts using Netdiscover...
[*] Extracting IP addresses from Netdiscover output...
[*] Running Nmap scan on each host...
Scanning 192.168.134.1...
Scanning 192.168.134.2...
Scanning 192.168.134.254...
[*] Aggregating Summary to dashboard.txt...
[*] Dashboard ready at: results_2025-07-31_01-07-37/dashboard.txt
```

- Finally the command **cat results_2025-07-31_01-07-37/dashboard.txt** is used here to display the final summary of scan results in terminal which will be including the open ports ,services running and information related to the OS and device.



```
┌──(root㉿kali02)-[/home/kali02]
└─# cat results_2025-07-31_01-07-37/dashboard.txt
==== Network Scan Summary (2025-07-31_01-07-37) ====

Host: 192.168.134.1
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
----------------------------------------
Host: 192.168.134.2
53/tcp open  domain  dnsmasq 2.51
----------------------------------------
Host: 192.168.134.254
----------------------------------------
```

Defense Recommendations

- Close unused ports and services(reduces entry point for attackers)
- Use a Firewall (to control traffic using **Windows Firewall** or **ufw command** in Kali)
- Update your OS, browsers, antivirus, and services regularly.
- Use tools like Wireshark, Snort, or system logs to monitor unusual activity.
- Turn Off Unused Devices/WiFi
- Network segmentation(VLAN’S) should be done.
- Educate All Users(avoid clicking suspicious links,and using unknown USBs).