

NETWORK SCANNING AND ENUMERATION DASHBOARD

**By Sidhima(2023A7R011)
CSE - Cybersecurity**

OBJECTIVES

- Build a dashboard:
 - Devices on the local network
 - Open ports
 - Operating system
- Automate network scanning and enumeration
- Present results in user-friendly format

TOOLS USED

- nano - for editing scripts
- chmod - to make script executable
- ./file_name - run the script step-by-step
- cat - to display and combine output
- Additional tools:

Nmap - For network scanning and OS detection

Netdiscover - For live host on the LAN

Bash Scripting - Automation and logging

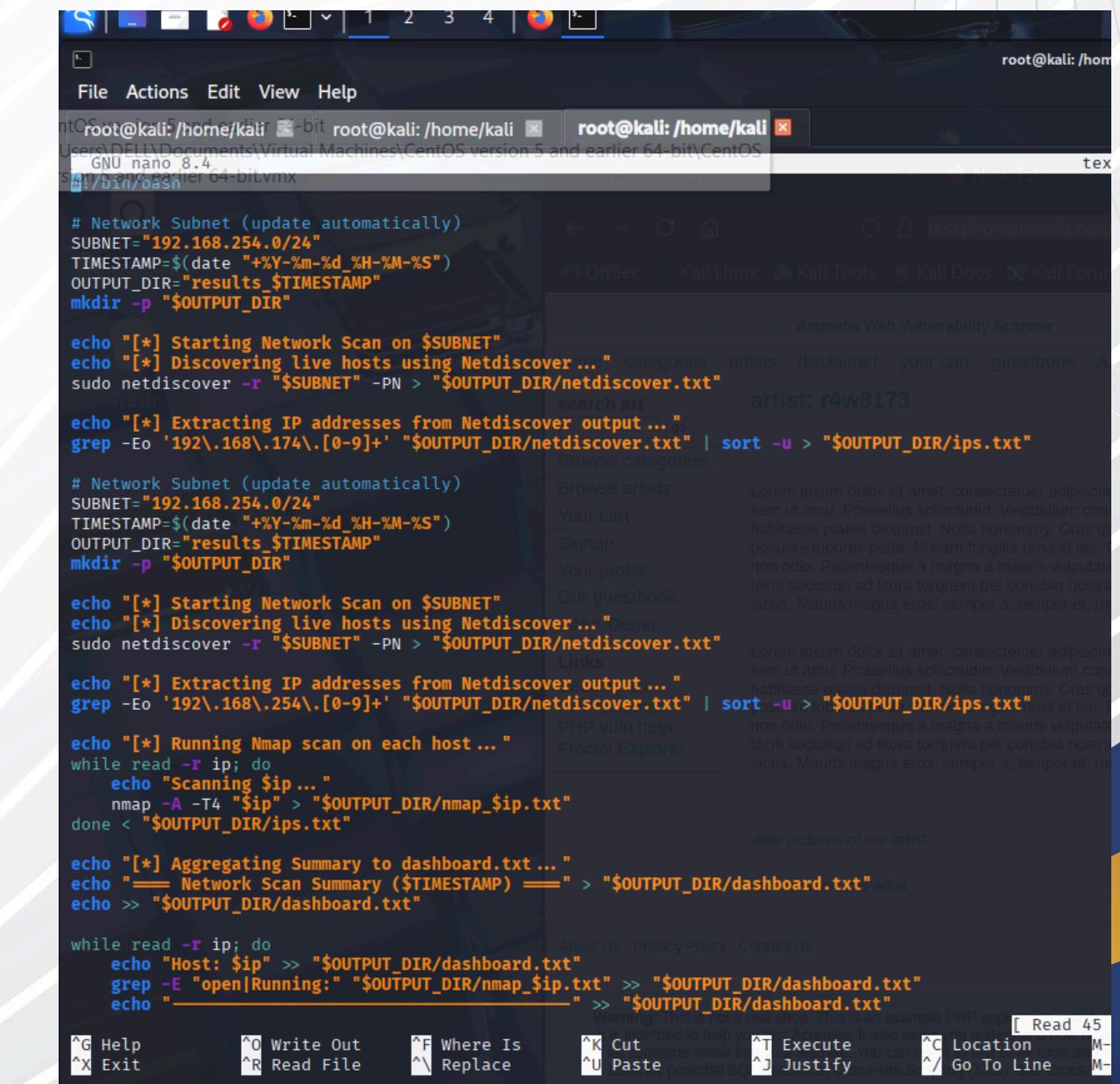
CREATE SCRIPT

- First, we create the script using the nano command.

nano text.exe

SCRIPT PURPOSE

- Script runs nmap to scan the local network for active devices and open ports.
- Logs the results to a file for further viewing and processing.



```
# Network Subnet (update automatically)
SUBNET="192.168.0/24"
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\.[0-9]+\.' "$OUTPUT_DIR/netdiscover.txt" | sort -u > "$OUTPUT_DIR/ips.txt"

# Network Subnet (update automatically)
SUBNET="192.168.254.0/24"
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\.[0-9]+\.' "$OUTPUT_DIR/netdiscover.txt" | sort -u > "$OUTPUT_DIR/ips.txt"

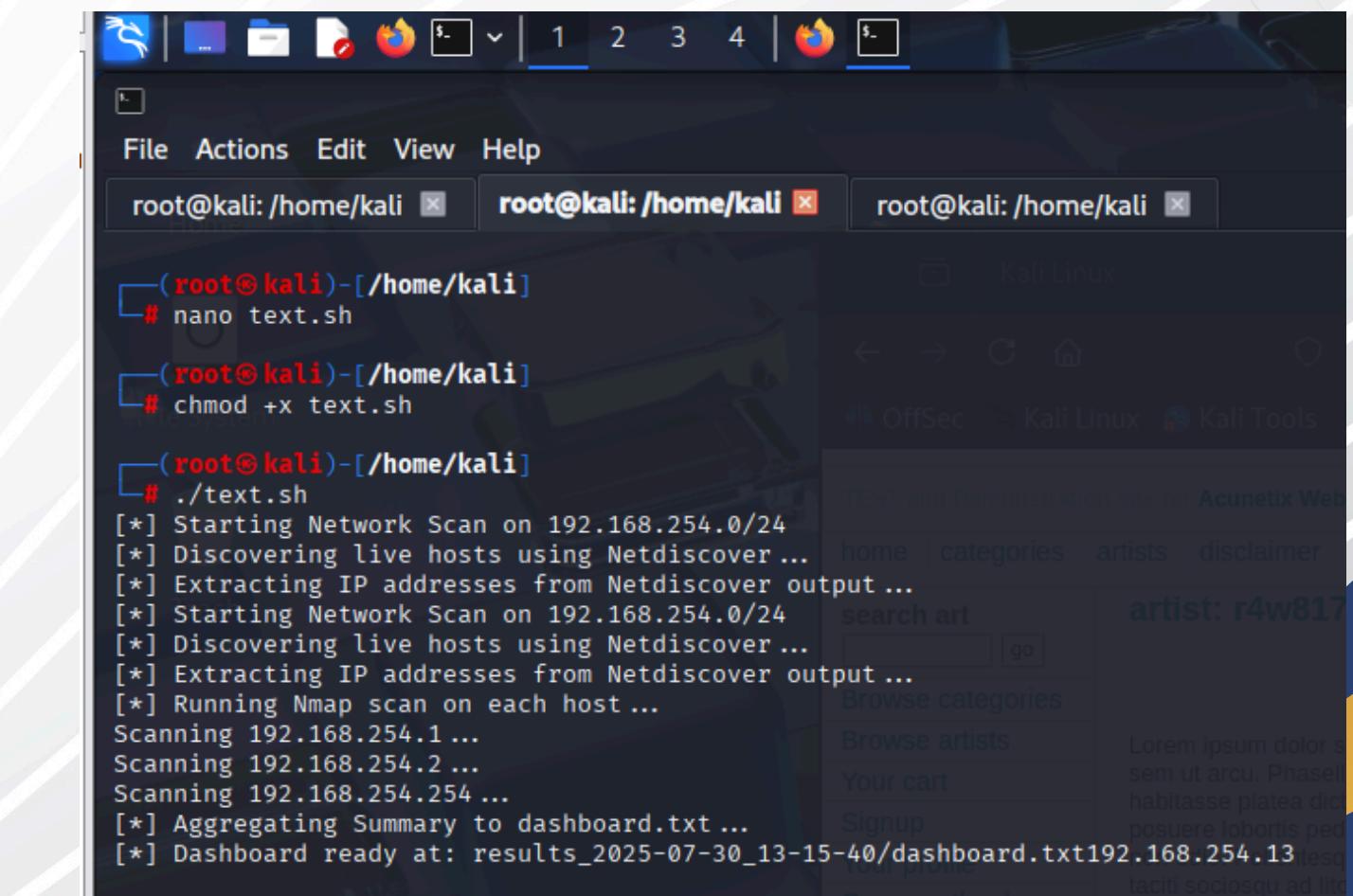
echo "[*] Running Nmap scan on each host ... "
while read -r ip; do
    echo "Scanning $ip ... "
    nmap -A -T4 "$ip" > "$OUTPUT_DIR/nmap_$ip.txt"
done < "$OUTPUT_DIR/ips.txt"

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"
```

MAKE SCRIPT EXECUTABLE

- After scripting we use **chmod +x text.exe** command to grant executable permission to the script file.
- Run the script by using **./text.exe** command.
 - It will executes the script and start network scanning.
 - Results are saved in **result.txt**.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window has three tabs, all showing the root shell at /home/kali. The first tab shows the command `# nano text.sh`. The second tab shows the command `# chmod +x text.sh`. The third tab shows the command `./text.sh`. The output of the script execution is visible in the terminal, detailing a network scan starting on 192.168.254.0/24, discovering live hosts using Netdiscover, extracting IP addresses from Netdiscover output, and running Nmap scan on each host. The results are aggregated into a file named `dashboard.txt`, which is ready at the specified path.

```
(root@kali)-[~/home/kali]
# nano text.sh
(root@kali)-[~/home/kali]
# chmod +x text.sh
(root@kali)-[~/home/kali]
# ./text.sh
[*] Starting Network Scan on 192.168.254.0/24
[*] Discovering live hosts using Netdiscover ...
[*] Extracting IP addresses from Netdiscover output ...
[*] Starting Network Scan on 192.168.254.0/24
[*] Discovering live hosts using Netdiscover ...
[*] Extracting IP addresses from Netdiscover output ...
[*] Running Nmap scan on each host ...
Scanning 192.168.254.1 ...
Scanning 192.168.254.2 ...
Scanning 192.168.254.254 ...
[*] Aggregating Summary to dashboard.txt ...
[*] Dashboard ready at: results_2025-07-30_13-15-40/dashboard.txt
```

DISPLAY RESULT

- To display the result we use cat command.

Purpose:

- Shows the output of the scan in a readable format
- Helps analyze device IPs, open ports, and detected OS

```
(root㉿kali)-[~/home/kali]
└─# cat results_2025-07-30_13-15-40/dashboard.txt
=====
 Network Scan Summary (2025-07-30_13-15-40)
=====

Host: 192.168.254.1
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: 192.168.254.2
53/tcp   open  domain    (generic dns response: NXDOMAIN)

Host: 192.168.254.254
```

DEFENSE RECOMMENDATIONS

- Disable unnecessary open ports
- Use firewalls to block untrusted access
- Enable OS hardening techniques
- Implement network segmentation
- Regularly update antivirus/firewall rules
- Monitor traffic with IDS/IPS