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

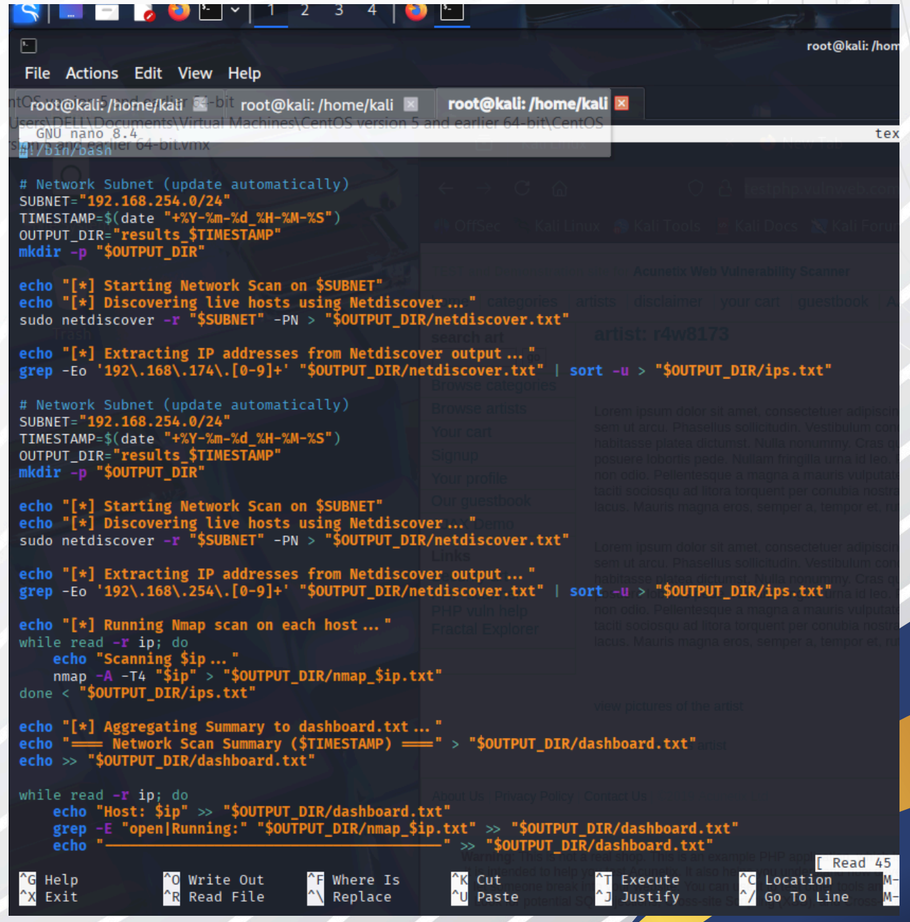
CREATE SCRIPT

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

  nano text.exe

SCRIPT PURPOSE

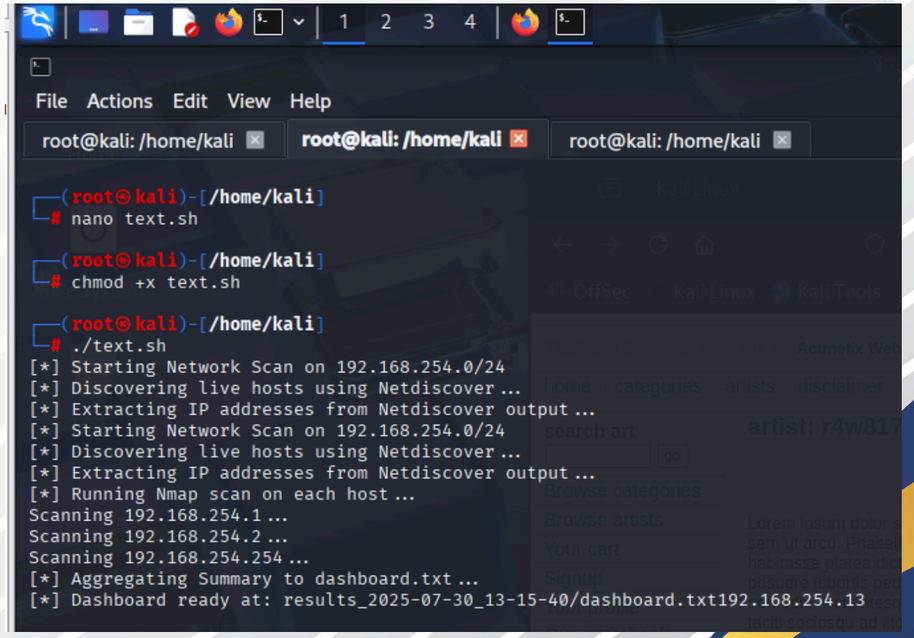
- Script runs nmap to scan the local network for active devices and open ports.
- Logs the results to a file for further viewing and processing.



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**.

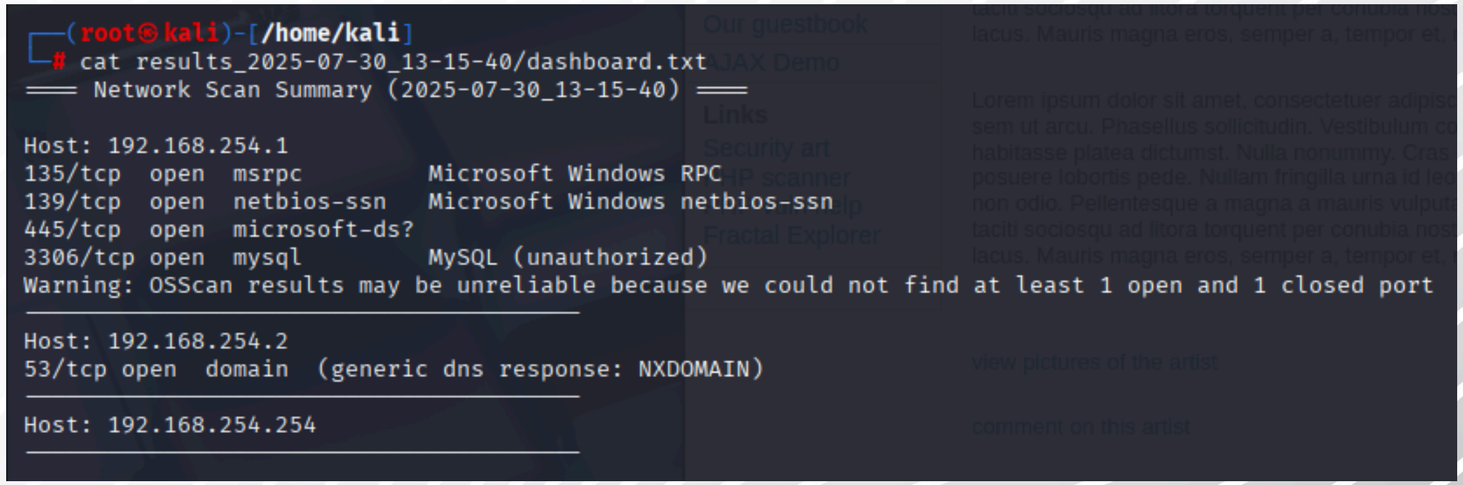


DISPLAY RESULT

- 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



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