Mini Project 3: Network Scanning and Enumeration Dashboard (CLI-Based)

Made using: *Kali Linux, Nmap, Netdiscover, Bash*

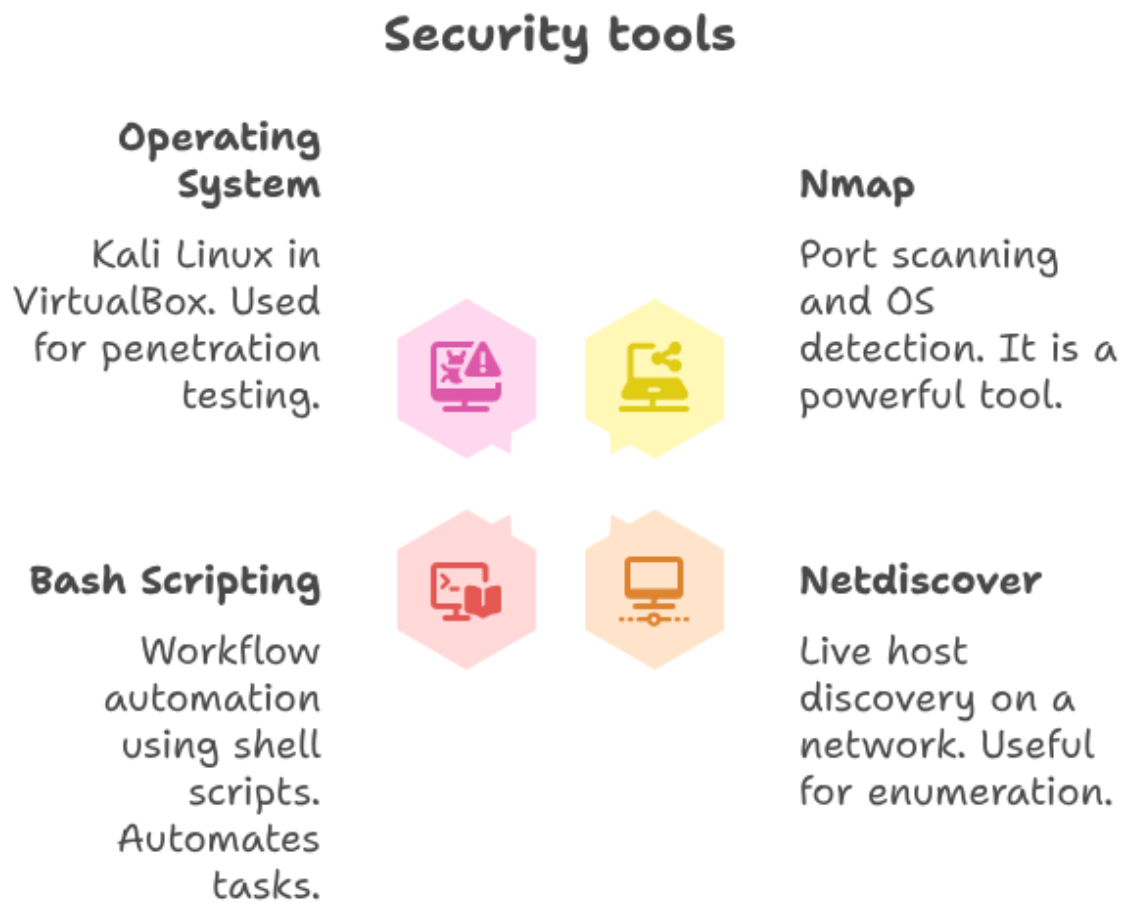
By: *Raghunandan Sharma*

Objective

- Scan local network to identify active devices.
- Detect open ports, OS, and services.
- Log results in a dashboard.
- Recommend basic defense measures.
- Fully CLI-based using Bash scripting

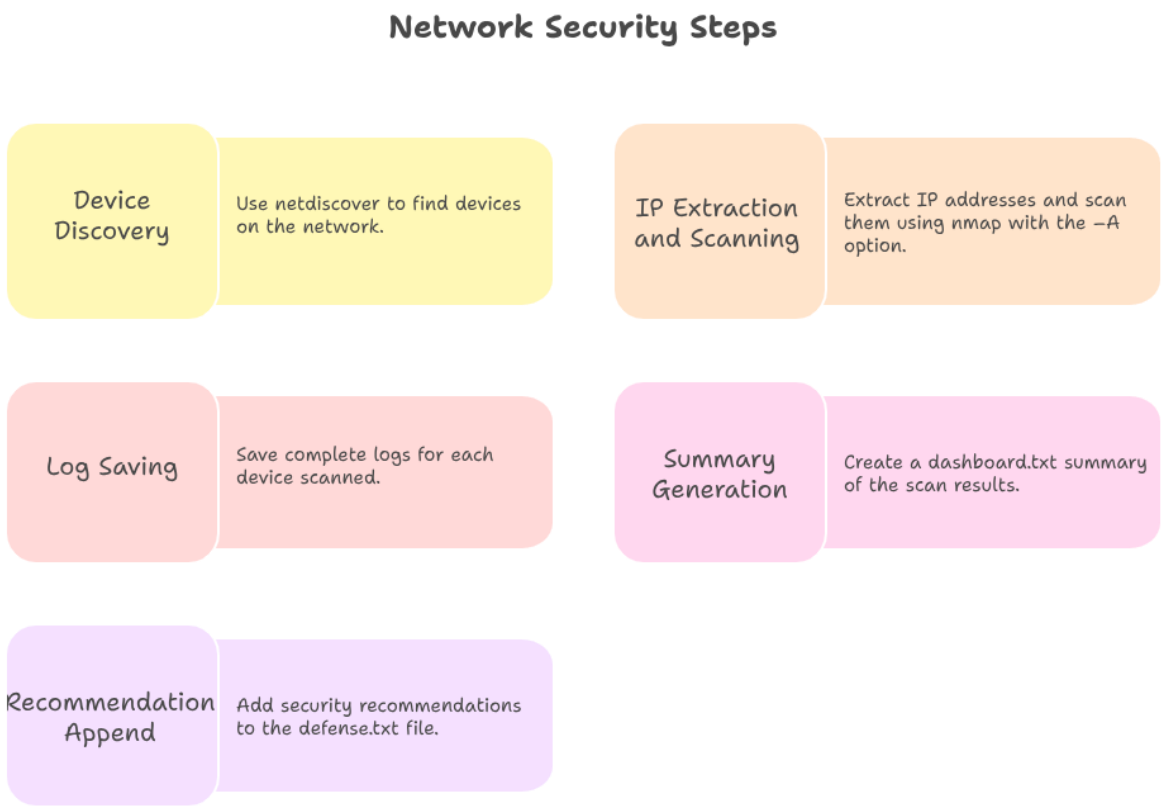
Tools & Technologies

- `Nmap` – Port scanning & OS detection
- `Netdiscover` – Live host discovery
- `Bash Scripting` – Workflow automation
- OS: Kali Linux (in VirtualBox)



How it works

- Discover devices using `netdiscover`.
- Extract IPs and scan using `nmap -A`.
- Save full logs per device.
- Generate `dashboard.txt` summary.
- Append `defense.txt` with recommendations.

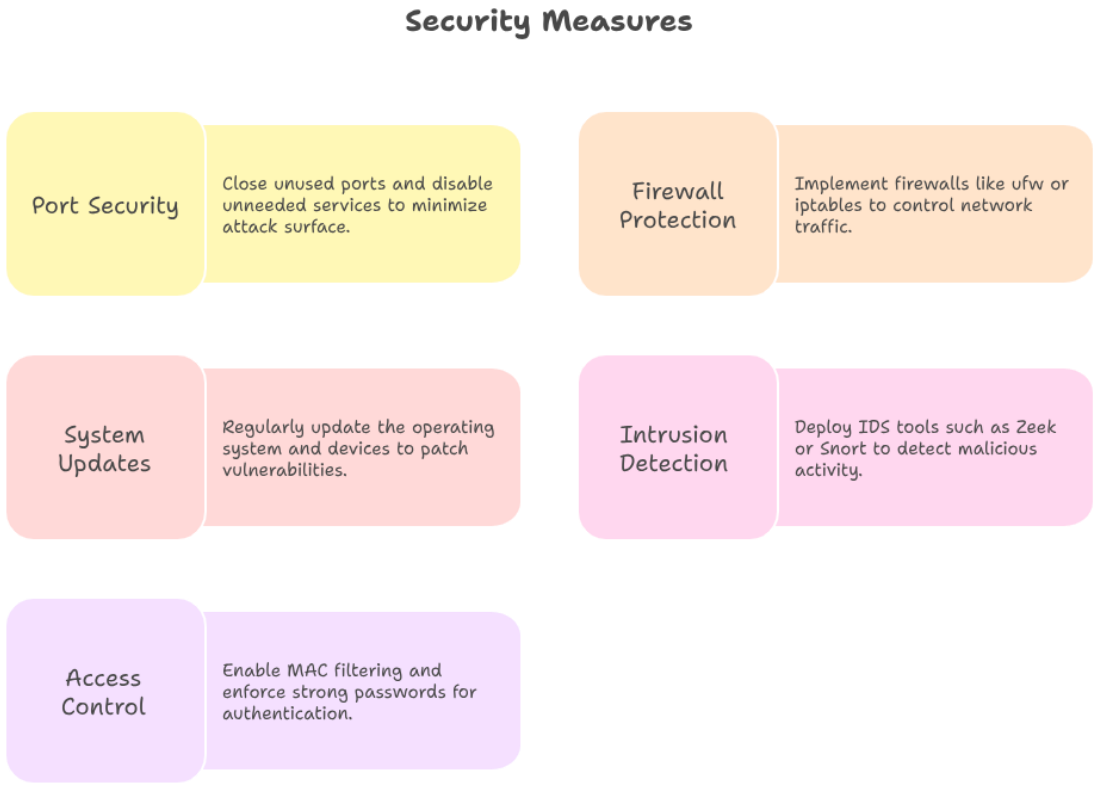


Sample Output

```
┌──(kali㉿kali)-[~/network-dashboard/results_2025-07-28_04-09-53]
└─$ cat dashboard.txt
=== Network Scan Summary (2025-07-28_04-09-53) ===

Host: 192.168.174.1
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC,
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
----------------------------------------

Host: 192.168.174.2
Warning: OSScan results may be unreliable because we could not find at lea
Running: VMware Player
----------------------------------------

Host: 192.168.174.254
----------------------------------------
```

Defense Recommendations

- Close unused ports and disable unneeded services.
- Use firewalls (`ufw`, `iptables`).
- Regular OS/device updates.
- Deploy IDS tools (e.g., Zeek, Snort).
- Enable MAC filtering & strong passwords.



Conclusion

- Simple, efficient Bash-based scanning tool.
- No dependencies beyond Kali defaults.
- Reusable for future auditing tasks.
- CLI dashboard shows clear, useful output.