Linux Hardening

Mohammad Parvin

mParvin.me

Overview

1. What is
2. Private vs Public servers
3. Attack types
4. IDS vs IPS vs SIEM
5. OS hardening
6. SSH hardening
7. Centralized Management
8. Tools

Private 🔥 vs Public 🌐

- Network Exposure & Threats
- Setup Complexity
- Access control
- Resource Allocation & Scalability
- ...

Attack types

Common for both

- **MITM** (Man-in-the-Middle Attack)
- **Malware** Infections (Viruses, Worms, Trojans)
- Data leaks

- Ransomware
- Privilege escalation
- DDOS

IDS and IPS

IDS (Intrusion Detection System)

- The Watchdog

IPS (Intrusion Prevention System)

- The Security Guard

SIEM (Security Information and Event Management)

- The Security Central Command

Common IPS Types

- NIPS (Network IPS)
- HIPS (Host IPS) [OS]
- WIPS (Wireless IPS)
- etc

Softwares

IDS

- Snort
- OSSEC
- Suricata
- SecurityOnion
- Wazuh

IPS

- Snort
- Suricata
- Wazuh

SIEM

- Splunk
- Wazuh
- ELK stack
- Graylog

OS Hardening

Keep everything updated

Minimize Installed Software

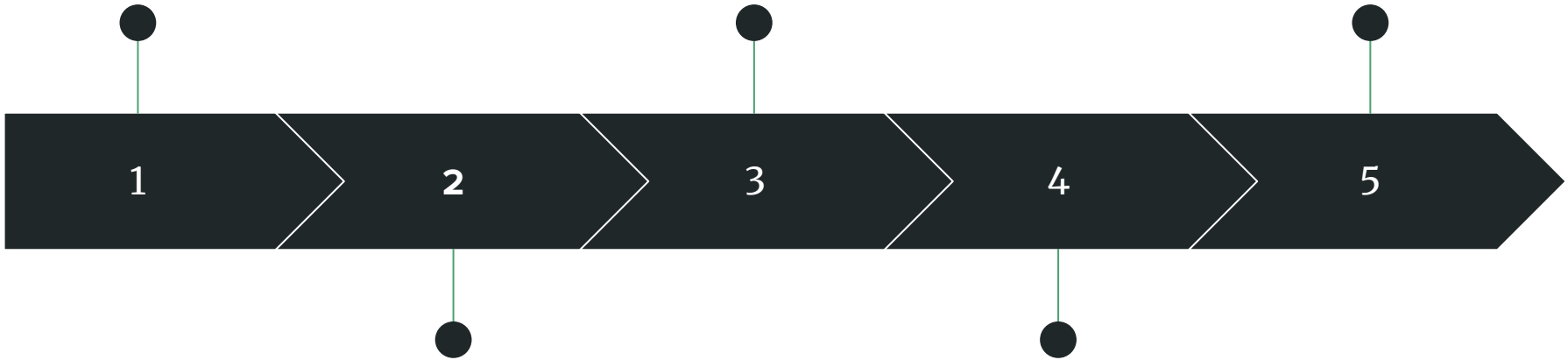
Remove Unused Program

Disable insecure ports

Kernel Hardening

IDS/IPS/SIEM

Security Scanning



Configure Firewall

Backup

SSH Hardening

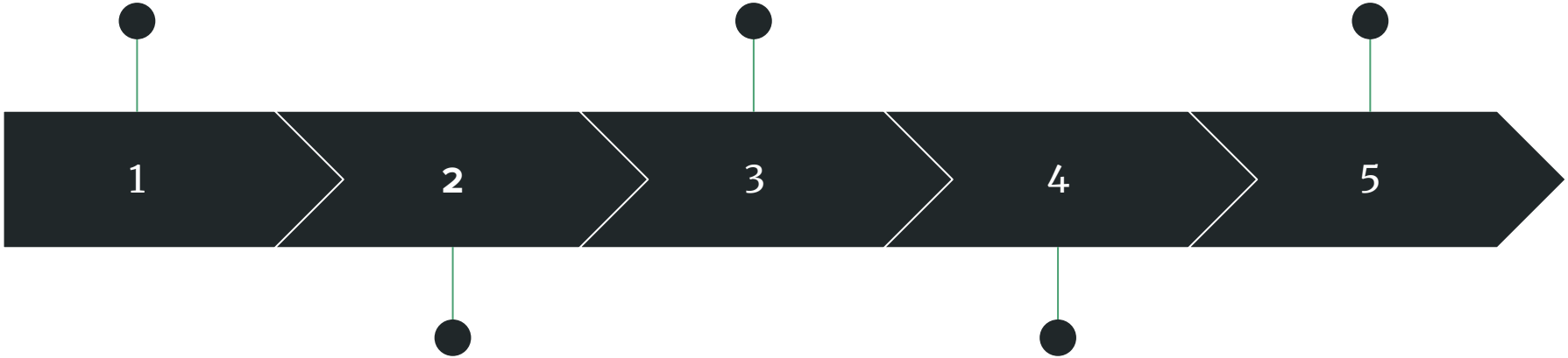
User management

e.g :

AllowUsers, Allow Hosts

Use SSH key instead of password

Use 2FA



Disable Root login

Change SSH Port

Tools

Linux OS

- OpenScap
- OpenVAS
- Lyniss

Containers

- Trivy
- Synk

Solutions

- LDAP
- Config Management (Ansible)
- Cron

Thank You ;)

1. Website mParvin.me
2. Telegram: @mmParvin
3. Github: mParvin

Resources

- More about Wazuh
- SIEM vs IDS
- Wazuh IDS or IPS
- Fail2Ban
- SecurityOnion
- Ansible DevSec
- More about Audit
- Centralized management