CYBERDUDEBIVASH Linux Security Hardening Checklist (2026)

This training document provides the enterprise-grade checklist for securing Linux servers, cloud workloads, and containers using CyberDudeBivash methodologies.

1. SSH & Remote Access Hardening

- Disable PasswordAuthentication
- Enforce SSH key authentication
- Disable root login
- Change default SSH port
- Enable Fail2Ban
- Enable MFA for SSH

2. User & Privilege Management

- Least privilege everywhere
- Restrict sudo and enable sudo logs
- Password aging enforcement
- Monitor new user creation

3. File System & Permission Hardening

- Secure /tmp and /var/tmp with nodev,nosuid,noexec
- Remove world-writable permissions
- Apply immutable bit to critical binaries
- Enable File Integrity Monitoring (FIM)

4. Network Hardening

- Enable firewall (UFW / Firewalld)
- Disable unused services
- Block all non-required ports

- Enable reverse path filtering

5. Kernel & Sysctl Hardening

- Enable SYN flood protection

- Disable IP forwarding

- Restrict kernel pointer exposure

- Enable kernel lockdown mode

6. Logging & Monitoring

- Enable Auditd

- Enable Sysmon for Linux

- Deploy Wazuh or Elastic Agent

- Monitor privilege escalation & unauthorized processes

7. Application Security

- Enforce SELinux or AppArmor

- Use Seccomp profiles

- Disable unused programming runtimes

- Weekly CVE scanning with OpenSCAP, Lynis, Nessus

8. Cloud Linux Hardening (AWS/Azure/GCP)

- Enforce IMDSv2

- Use IAM roles

- Disable public IPs

- Enable cloud-native logging

9. Container & Kubernetes Hardening

- Do not run containers as root

- Enable Kubernetes Pod Security Standards

- Use CIS benchmarks

- Scan images with Trivy, Anchore, Clair

10. Incident Response Checklist

- Collect system logs

- Dump processes

- Check SUID binaries

- Scan for rootkits

- Dump network connections

- Acquire memory snapshot

CyberDudeBivash Ecosystem:

https://www.cyberdudebivash.com