JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Vulnerability Assessment and System Hardening Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Vulnerability Assessment and System Hardening Course

Vulnerability Assessment and System Hardening is a 2-week advanced training course for security engineers, network administrators and technical security specialists who find and close weaknesses in servers, endpoints and networks, and it ends with a technical security assessment report on a lab estate. Attackers now weaponise newly published flaws within days, so the gap between discovery and remediation decides exposure. Jupiter Prime Training runs this course for specialists who own that gap.

Why Vulnerability Assessment and System Hardening Matters Now

Three pressures shape this work today: the volume of newly disclosed software flaws, which outpaces any patch window; hybrid estates where cloud images, containers and legacy servers each drift from their secure baseline; and auditors and insurers who ask for proof of scanning, remediation and configuration control. Specialists who prioritise by exploitability and harden baselines shrink the attack surface steadily; those who chase every scanner finding exhaust their teams and miss the dangerous few. The course aligns its methods with the Identify and Protect functions of the NIST Cybersecurity Framework 2.0 NIST CSF 2.0 and with the control expectations of ISO/IEC 27001:2022.

Who Gains Most from Vulnerability Assessment and System Hardening

- Security engineers who run scanning, validate findings and track remediation across the estate
- Network administrators who harden routers, switches, firewalls and remote access gateways
- Systems administrators who build and maintain Windows and Linux server baselines
- Security operations specialists who tune monitoring to catch exploitation attempts
- Technical assessors who prepare evidence of testing for auditors and clients

An infrastructure group that sends its security engineers and system and network administrators together gains most, because hardening only sticks when those who find the weakness and those who fix it share one method.

Vulnerability Assessment and System Hardening Capabilities

Participants leave able to move from raw scan output to a prioritised, verified and hardened environment.

- Assess vulnerabilities by exploitability, exposure and asset criticality — remediation priority for system owners
- Apply penetration testing methods within agreed rules of engagement — validation of real attack paths
- Build secure configuration baselines for servers, endpoints and network devices — change advisory decisions
- Test hardening through configuration audits and re-scans — evidence for auditors
- Analyse malware behaviour at a basic level to inform containment — incident handlers
- Specify monitoring use cases that detect exploitation attempts — security operations centre

Key Vulnerability Assessment and System Hardening Terms

- Vulnerability — A weakness in software, configuration or process that an attacker could use to gain access or cause harm.
- Attack surface — All the points, such as open ports, services, accounts and interfaces, where an attacker could try to enter a system.
- Secure baseline — An approved, documented configuration that every system of a given type must match before and after changes.
- Rules of engagement — The written scope, timing, methods and limits agreed before any penetration test begins.
- False positive — A scanner finding that reports a weakness which does not actually exist or cannot be exploited.
- Configuration drift — The gradual departure of a system's live settings from its approved secure baseline over time.

Vulnerability Assessment and System Hardening Day by Day

Day 1: The Exposure Landscape

- Vulnerability Disclosure and Exploit Timelines — Urgency of Remediation
- Attack Surface Mapping — Internet-Facing and Internal Exposure
- NIST CSF 2.0 Identify and Protect Functions — Where Assessment Fits
- Asset Discovery Techniques — Unknown Hosts and Shadow Services
- Lab Environment Orientation — Scope of the Assessment Exercise

Day 2: Scanning and Enumeration

- Network Discovery with Nmap — Port and Service Fingerprinting
- Authenticated Versus Unauthenticated Scans — Depth and Accuracy Trade-Offs
- Web Application Scanning — Injection and Misconfiguration Findings
- Scan Scheduling and Throttling — Avoiding Disruption to Production
- Enumeration of Users, Shares and Services — Lateral Movement Clues

Day 3: Validating and Prioritising Findings

- Severity Scoring and Exploitability Signals — Remediation Order
- False Positive Validation Methods — Analyst Effort Where It Counts
- Asset Criticality Weighting — Business Impact of Each Weakness
- Vulnerability Tracking Workflow — Ownership and Service Levels
- Exception and Compensating Control Records — Accepted Residual Exposure

Day 4: Penetration Testing Methods

- Rules of Engagement and Scoping — Legal and Operational Limits
- Reconnaissance and Exploitation Phases — Proof of Real Attack Paths
- Password Attacks and Credential Reuse — Identity Weakness Evidence
- Privilege Escalation Techniques — Local and Domain Exposure
- Post-Exploitation Clean-Up — Leaving Systems as Found

Day 5: Hardening Windows and Linux Servers

- Windows Group Policy Hardening — Account, Audit and Service Settings
- Linux Service Minimisation and SSH Configuration — Reduced Attack Surface
- Local Administrator and Sudo Controls — Privilege Containment
- Host Firewall and Application Allow-Listing — Execution Control Choices
- Baseline Documentation and Golden Images — Repeatable Builds

Day 6: Hardening Networks and Remote Access

- Router and Switch Hardening — Management Plane Protection
- Firewall Rule Base Review — Redundant and Overly Broad Rules
- Network Segmentation and VLAN Design — Containing Compromise
- VPN and Remote Desktop Gateway Configuration — Exposure of Remote Access
- Wireless Security Settings — Authentication and Rogue Access Points

Day 7: Secure Configuration in Cloud and Containers

- Cloud Identity and Storage Misconfigurations — Public Exposure Risks
- Container Image Scanning — Vulnerable Packages Before Deployment
- Infrastructure as Code Checks — Insecure Templates Caught Early
- Configuration Drift Detection — Automated Baseline Comparison
- Patch Management Cadence — Balancing Uptime and Exposure

Day 8: Malware Basics for Defenders

- Malware Families and Delivery Methods — Likely Entry Points
- Static Indicators and File Hashing — Quick Triage of Samples
- Sandbox Behaviour Observation — Network and Persistence Clues
- Endpoint Protection Tuning — Detection Without Excessive Noise
- Manufacturing and Retail Malware Cases — Sector Lessons

Day 9: Security Monitoring and Verification

- Log Sources for Exploitation Detection — Coverage of Hardened Systems
- SIEM Use Case Design — Alerts for Known Attack Techniques
- Intrusion Detection Tuning — Signal Versus Noise
- Re-Scan and Configuration Audit — Proof That Fixes Hold
- Metrics for Vulnerability Programmes — Time to Remediate and Coverage

Day 10: Practising the Technical Security Assessment Report

- Lab Scan and Validation Run — Confirmed Findings List
- Targeted Exploitation of Priority Weaknesses — Demonstrated Impact
- Hardening Recommendations Applied to Lab Hosts — Before and After Evidence
- Executive and Technical Findings Briefing — Clear Asks for Owners
- Technical Security Assessment Report Completion — Findings, Fixes and Verification Steps

Applying Vulnerability Assessment and System Hardening After the Course

- Run an authenticated scan of one critical server group and validate the top findings using the prioritisation method practised in the course
- Draft a secure baseline for one server type and compare live systems against it to measure configuration drift

Vulnerability Assessment and System Hardening Questions FAQ

What is vulnerability assessment and system hardening and why does it matter now?

Vulnerability assessment and system hardening is the practice of finding weaknesses in systems and networks and closing them through secure configuration. It matters now because attackers exploit new flaws within days, and drifting configurations reopen doors that were once shut.

Which roles gain most from vulnerability assessment and system hardening training?

Security engineers, network and systems administrators, security operations specialists and technical assessors gain most. You benefit if you run scans, maintain baselines or must prove to auditors that weaknesses are found and fixed.

How does vulnerability assessment and system hardening training differ from an ethical hacking course?

It balances finding weaknesses with fixing and verifying them, rather than focusing mainly on offensive techniques. Penetration testing methods are taught to validate findings, alongside hardening, secure configuration and monitoring of the systems you defend.

What do you bring back from vulnerability assessment and system hardening training?

You bring back a completed assessment report from a lab environment and the method to repeat it at work. It covers validated findings, priority order, hardening steps and the re-test evidence that shows each fix holds.

Vulnerability Assessment and System Hardening: The Way Forward

The technical security assessment report first informs which weaknesses system owners fix in the next patch cycle and which baselines change. Security engineers maintain it, administrators act on its hardening steps and auditors use its re-test evidence. After the first real assessment, revisit the prioritisation weights, since live estates often show that asset criticality matters more than raw severity.