MERCURY

Network Security Assessment and System Hardening Course

11 – 15 January 2027
London (UK)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Network Security Assessment and System Hardening Course

Ref: 121383_1030334 **Date:** 11 – 15 January 2027 **Location:** London (UK) **Fees:** 5900 Euro

Network Security Assessment and System Hardening Course is a 1-week course for network and system administrators who must find weaknesses in routers, firewalls, servers and endpoints and close them. You scan, rate findings, harden configurations against baselines and tune detection, and leave with a Hardening and Remediation Plan for part of your own estate. Mercury Training Center delivers this network security assessment course.

About This Course

Many breaches start from a default password, an open management port or a server that missed months of patches. You should already configure switches, routers, firewalls or servers at work. You practice in lab exercises on scanning, configuration review, rule cleanup and log analysis drawn from banking, healthcare and utility estates.

Who It Is For

- Configuring and maintaining routers, switches, firewalls and VPN gateways.
- Building, patching and supporting Windows and Linux servers.
- Rolling out and tuning endpoint protection across user devices.
- Running vulnerability scans and following up remediation with asset owners.
- Reviewing technical controls on behalf of IT audit or compliance functions.

This course is not for readers new to IP addressing and routing, who are better served by an introductory networking course, or for testers who want to break into targets, who need an offensive penetration testing course.

Competencies You Will Build

- Attack Surface Mapping: listing exposed hosts, ports and services and who owns each.
- Vulnerability Rating: scoring findings with CVSS and ranking fixes by exposure.
- Device Hardening: applying baseline settings to routers, switches and firewalls.
- Host Hardening: locking down server and workstation builds against CIS Benchmarks.
- Detection Tuning: adjusting IDS/IPS and endpoint alerts so real events stand out.
- Patch Discipline: running a patch cycle with testing, rollout and verification.

What You Will Be Able to Do

By the end of the course you will be able to:

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Given a scan report, remove false positives, score the remaining findings and set fix deadlines.
- From a firewall rule base, find shadowed, unused and overly broad rules and write a cleanup change.
- Using a CIS Benchmark, audit a server build and produce a list of deviations with fixes.
- From a flat site layout, propose segmentation zones and the traffic allowed between them.
- Given a week of IDS and endpoint alerts, separate noise from events and adjust the rules.

Course Content

Day 1: Assessment Scope and Method

- Confidentiality, Integrity and Availability Applied to Infrastructure Assets
- Assessment Planning with NIST SP 800-115 Testing Phases
- Asset Inventory and Attack Surface Mapping for a Branch Site
- Policy and Procedure Review Against Technical Configuration Reality
- Threat Landscape Briefing and Governance Roles for Infrastructure Teams

Day 2: Vulnerability Assessment

- Authenticated and Unauthenticated Scanning of Servers and Devices
- Validating Scan Findings and Removing False Positives
- CVSS Scoring and Remediation Priorities by Exposure
- Application and Service Configuration Checks on Exposed Hosts
- Findings Report Structure for Asset Owners and Auditors

Day 3: Routers, Switches and Firewalls

- Router and Switch Hardening: Management Plane, Services and Credentials
- Segmentation, VLANs and Defense-in-Depth Zones
- Firewall Rule Base Review and Cleanup
- VPN Gateway Settings for Remote Staff and Third Parties
- Network Access Control and Identity-Aware Port Policies

Day 4: Servers, Endpoints and Detection

- Windows and Linux Server Hardening with CIS Benchmarks
- Endpoint Protection and EDR Policy Settings for User Devices
- Patch Management Cycle: Test, Deploy, Verify
- IDS/IPS Placement and Signature Tuning
- Logging, Alert Correlation and Escalation to Incident Response

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Day 5: Practice on a Hardening Engagement

- Scan Triage Exercise on a Hospital Server Segment
- Firewall Cleanup Exercise on a Bank Branch Rule Base
- Server Baseline Audit Exercise Against a CIS Benchmark
- Key Risk Indicators and Resilience Measures for Ongoing Hardening
- Completing Your Hardening and Remediation Plan

Case Studies and Exercises

The items below are suggested activities.

- Case study: a hospital finds medical device servers on the same flat segment as staff laptops; you design zones and the allowed traffic.
- Case study: a utility control center receives a scan with hundreds of findings; you decide which ten to fix first and why.
- Exercise: a bank branch firewall carries years of unused rules; you produce a cleanup change request.
- Exercise: a retail chain rolls out endpoint protection to store devices; you set policies and alert thresholds.

What You Take Back

The Hardening and Remediation Plan lists the weaknesses found in one part of your estate and the fixes, owners and deadlines for each. In your first month back you use it to raise change requests, run the first patch and rule cleanup cycle and report progress to your manager.

- An asset and exposed service inventory.
- A scored findings list with fix deadlines.
- Device and server baseline checklists.
- A firewall and segmentation change list.

Quick Answers FAQ

What should I know before a network security assessment course?

You should be comfortable with IP addressing, routing, firewall rules and basic Windows or Linux administration. No prior scanning experience is needed; tools and reports are introduced in the lab exercises.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

How does network security assessment and hardening differ from penetration testing training?

It is defensive: you find weaknesses, rank them and fix configurations on devices and servers you run. Penetration testing training teaches how to exploit weaknesses from an attacker's point of view, with less time on fixing and hardening.

What is a CIS Benchmark and how is it used in system hardening?

A CIS Benchmark is a published set of recommended configuration settings for a specific operating system, device or application. Administrators compare their builds against it, record deviations and either apply the setting or document why they keep their own.

What do I take back from network security assessment and system hardening training?

You take back a Hardening and Remediation Plan for part of your estate: an exposed service inventory, scored findings with deadlines, baseline checklists and a firewall and segmentation change list.

For Your Manager

After the course, the team member will be able to run and triage vulnerability scans, harden routers, firewalls and servers against baselines, clean up rule bases and tune alerts. They return with a Hardening and Remediation Plan, first used to raise change requests and run the next patch and firewall cleanup cycle.