UNIVERSITÀ DEGLI STUDI FIRENZE

Hardening Linux and Windows
10, 17, 19, 26 Novembre, 01 Dicembre 2025 orario 09:00-13:00

OBIETTIVI	Formazione del personale IT che si occupa di sicurezza informatica sulle strategie preventive finalizzate a ridurre la vulnerabilità dei sistemi operativi Linux e Windows
PREREQUISITI	
DESTINATARI	Corso rivolto al personale tecnico informatico
ENTE ORGANIZZATORE	Università di Firenze
ENTE EROGATORE	Università di Firenze
LUOGO	formazione a distanza
REFERENTE ORGANIZZATIVO	Formazione in collaborazione con Siaf
DOCENTI	Docente NobleProg
DATA INIZIO	
DATA FINE	
DURATA IN ORE	20
SCADENZA PRENOTAZIONI	
MAX PARTECIPANTI	25

UNIVERSITÀ
DEGLI STUDI
FIRENZE

PROGRAMMA	**Introduzione al Corso** • Obiettivi e finalità del corso • Importanza della sicurezza dei sistemi operativi • Panoramica delle minacce informatiche moderne • Differenza tra sicurezza preventiva, difensiva e reattiva **Fondamenti di Sicurezza Informatica** • Principi di sicurezza (CIA: Confidenzialità, Integrità, Disponibilità) • Modelli di accesso e gestione delle autorizzazioni • Hardening: concetto e strategie **Hardening di Linux** **Configurazione Sicura del Sistema** • Disabilitazione di servizi non necessari • Configurazione dei permessi e delle policy di accesso • Protezione dei file di sistema **Gestione Utenti e Autenticazione** • Uso corretto di sudo e privilegi minimi • Autenticazione a due fattori (2FA) • Password Policy e PAM (Pluggable Authentication Modules) **Sicurezza di Rete in Linux** • Firewall (UFW, iptables, nftables) • Protezione SSH (fail2ban, key-based authentication) • VPN e tunneling sicuro **Logging e Monitoraggio** • Configurazione di auditd e logrotate • Analisi dei log con journald e syslog

• Strumenti di monitoraggio (Nagios, OSSEC, Tripwire)

Protezione del Kernel e delle Applicazioni

• Security-Enhanced Linux (SELinux) e AppArmor

• Patch di sicurezza e aggiornamenti automatici

• Contenitori e sicurezza: Docker e Podman

Hardening di Windows

Configurazione Sicura del Sistema

• Disattivazione di servizi non necessari

• Configurazione avanzata delle Group Policies (GPO)

• Controllo degli accessi con Active Directory

Gestione Utenti e Autenticazione

• Implementazione di Microsoft Defender Credential Guard

• Password Policy avanzate e autenticazione biometrica

• Controllo degli accessi con NTFS e BitLocker

Sicurezza di Rete in Windows

• Configurazione avanzata di Windows Firewall

• Protezione RDP e accesso remoto sicuro

• Implementazione di Windows Defender ATP (Advanced Threat Protection)

Logging e Monitoraggio

• Event Viewer e strumenti di analisi log

• Monitoraggio avanzato con Windows Security Baseline

• Introduzione a SIEM per Windows (Microsoft Sentinel)

Protezione del Kernel e delle Applicazioni

• Patch Management e Windows Update for Business

• Isolamento delle applicazioni con Windows Sandbox

• Protezione contro ransomware e malware

Strategie Avanzate di Sicurezza

• Zero Trust Security Model

• Hardening nei sistemi cloud (Azure, AWS, Google Cloud)

• Security Automation e Infrastructure as Code (Ansible, PowerShell DSC)