



3 ore. Un obiettivo. Una competenza chiave.

Corso Difendere le credenziali in Windows e AD





Corso Difendere le credenziali in Windows e AD

Prevenire il credential dumping e limitare l'impatto di account compromessi

Scopri come proteggere le credenziali degli utenti e degli amministratori in ambienti Windows e Active Directory. Questo TechShot mostra le tecniche pratiche per difendere hash, password e token dagli attacchi più comuni, riducendo i rischi e aumentando la sicurezza dell'infrastruttura aziendale.

ISCRIVITI

Dettagli del corso

-  9 aprile 2026 dalle 9.30 - 12.30
-  Online Live
-  €99+IVA a partecipante
-  Posti limitati

Cosa è incluso nel corso

-  Open Badge
-  Registrazione per 3 mesi
-  Materiale didattico

La tua skill in 3 ore

L'obiettivo è proteggere le credenziali e ridurre i rischi legati ad attacchi e malware in ambienti Windows e Active Directory.

Alla fine del corso sarai in grado di:

- Analizzare e simulare attacchi alle credenziali
- Proteggere le credenziali in memoria e sui sistemi con strumenti Microsoft
- Ridurre la superficie di attacco con LAPS 2.0 e PAW
- Applicare pratiche difensive efficaci e monitorare l'ambiente AD

Corso Difendere le credenziali in Windows e AD

Prevenire il credential dumping e limitare l'impatto di account compromessi

Prerequisiti di partecipazione

- Conoscenze base di Windows e Active Directory e concetti fondamentali di security

Programma del corso

Modulo 1: Gli attacchi alle credenziali in Windows e AD

- Analisi del credential dumping
- Target principali: LSASS, SAM, registry, memoria
- Tecniche comuni: Mimikatz, ProcDump, DCSync, token stealing
- Dump ed esfiltrazione hash in real-time

Modulo 2: Proteggere il processo LSASS e le credenziali in memoria

- Abilitare RunAsPPL (LSASS as Protected Process)
- Implementare Credential Guard su client e server
- Configurare WDAC e Attack Surface Reduction
- Confronto pratico: sistema protetto vs vulnerabile

Modulo 3: Ridurre la superficie di attacco: PAM, LAPS e PAW

- LAPS 2.0 per gestione password locali
- Creazione e verifica di PAW (Privileged Access Workstations)
- Tiering model e protezione degli account privilegiati
- Deploy LAPS e verifiche operative su dominio test