CORSO SICUREZZA DELLE CREDENZIALI IN ACTIVE DIRECTORY

Durata: 4 ore

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: ANATOMIA DEGLI ATTACCHI ALLE CREDENZIALI SU WINDOWS E AD

- Credential dumping: LSASS, SAM, registry, DPAPI, memoria
- Tooling aggiornato: Mimikatz, ProcDump/comsvcs.dll, dumper syscall-based (nanodump/Dumpert) per evasione EDR, DCSync
- Token theft / impersonation
- Attacchi Kerberos — Kerberoasting, AS-REP Roasting, Pass-the-Ticket, Overpass-the-Hash, Golden/Silver/Diamond ticket; abuso delle delegation (unconstrained / constrained / RBCD)
- Mappatura su MITRE ATT&CK – Credential Access come filo conduttore

MODULO 2: ATTACCHI MODERNI: CERTIFICATI, IDENTITÀ IBRIDA E DMSA

- AD CS abuse: ESC1–ESC16, Shadow Credentials
- BadSuccessor / dMSA
- Piano cloud/ibrido: furto del Primary Refresh Token (PRT)

MODULO 3: DIFESA: PROTEGGERE LSASS E LE CREDENZIALI IN MEMORIA

- RunAsPPL / LSA Protection
- Credential Guard (oggi default-on su Win11 Enterprise idonei e Server 2025 → aggiorna la slide "come si abilita")
- WDAC + ASR (regola Block credential stealing from lsass.exe)
- Eliminare NTLM e RC4

MODULO 4: RIDURRE LA SUPERFICIE D'ATTACCO E DETECTION

- Windows LAPS 2.0: password locali + cifratura in AD + integrazione Entra ID
- PAW + Enterprise Access Model
- Tiering AD (T0, T1, T2)
- gMSA/dMSA per i service account (mitigazione diretta del Kerberoasting)
- Phishing-resistant auth: Windows Hello for Business, FIDO2/passkeys
- Detection layer: Microsoft Defender for Identity, Sysmon, Event ID chiave, honey account / honeytoken

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO SICUREZZA DELLE CREDENZIALI IN ACTIVE DIRECTORY

Durata: 4 ore

OVERVIEW DEL CORSO

L'accesso e il furto delle credenziali d'identità rappresentano la prima causa di compromissione delle infrastrutture aziendali. Questo Flash Training offre un percorso verticale e altamente tecnico dedicato alla protezione di Active Directory e degli ambienti Windows dai vettori di attacco più diffusi e sofisticati.
In sole 4 ore, analizzeremo l'anatomia delle minacce moderne — dal credential dumping evoluto agli abusi di Kerberos e AD CS — per poi concentrarci sulle contromisure pratiche e sulle strategie di hardening. Il programma integra le ultime novità dei sistemi operativi, tra cui i nuovi vincoli di Windows 11 Enterprise e Windows Server 2025, per fornire ai professionisti IT gli strumenti necessari a ridurre drasticamente la superficie d'attacco.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Amministratori di Sistema e Domain Administrator
- Security Engineer e Cyber Security Specialist
- Network & Infrastructure Manager

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- A riconoscere l'anatomia e le tecniche avanzate di credential dumping (LSASS, SAM, attacchi basati su syscall).
- A identificare e mitigare gli attacchi ai protocolli di autenticazione come Kerberos (Kerberoasting, AS-REP Roasting, Golden Ticket) e gli abusi di Active Directory Certificate Services (AD CS).
- A implementare difese native per proteggere la memoria di Windows (Credential Guard, LSA Protection, regole ASR).
- A ridurre la superficie d'attacco applicando modelli di Tiering amministrativo, Windows LAPS 2.0 e logiche di autenticazione phishing-resistant.
- A configurare i layer di monitoraggio e telemetria (Defender for Identity, Sysmon, Honeytoken) per rilevare tempestivamente i tentativi di movimento laterale.

CONTATTI

info@nexsys.it

www.nexsys.it