CORSO ATTACCHI ALLE IDENTITÀ: ACTIVE DIRECTORY, ENTRA ID E AZURE

Durata: 10,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: ARCHITETTURA E SICUREZZA DI ACTIVE DIRECTORY

- Foreste, domini, trust, OU e Domain Controller
- Utenti, computer account, gruppi e Security Identifiers (SID)
- Account amministrativi, privilegi locali e di dominio
- Access Control Lists (ACL), Access Control Entries (ACE) e deleghe
- Group Policy Objects (GPO) e relativi rischi
- Superfici di attacco dell'infrastruttura AD

MODULO 2: AUTENTICAZIONE WINDOWS: NTLM E KERBEROS

- NTLM e meccanismo challenge-response
- Kerberos: KDC, AS-REQ, AS-REP, TGT, TGS e PAC
- SPN, ticket, chiavi e crittografia
- NTLM relay e principali condizioni di esposizione
- NTLM restrictions, LDAP signing e channel binding
- Gestione degli algoritmi Kerberos e progressiva riduzione di RC4

MODULO 3: ACTIVE DIRECTORY ENUMERATION E ATTACK PATHS

- Enumerazione di utenti, gruppi, computer e account di servizio
- Ricerca di privilegi e configurazioni vulnerabili
- Analisi di ACL, GPO e trust
- PowerShell Active Directory Module e strumenti di ricognizione
- BloodHound e SharpHound: raccolta, analisi e visualizzazione
- Individuazione di percorsi verso account e sistemi privilegiati

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ATTACCHI ALLE IDENTITÀ: ACTIVE DIRECTORY, ENTRA ID E AZURE

Durata: 10,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

LABORATORIO PRATICO 1: ACTIVE DIRECTORY

- Enumerazione di un dominio Active Directory
- Analisi delle deleghe e dei gruppi amministrativi
- Ricostruzione di un percorso di escalation con BloodHound
- Identificazione e classificazione delle misconfigurazioni

MODULO 4: CREDENTIAL ATTACKS E LATERAL MOVEMENT

- Credential dumping e rischi associati a LSASS
- Mimikatz e strumenti equivalenti: principi di funzionamento e rilevamento
- Pass-the-Hash, Overpass-the-Hash e Pass-the-Ticket
- Kerberoasting e AS-REP Roasting
- Abuso degli account di servizio
- Lateral movement tramite SMB, WMI, WinRM e RDP
- Windows LAPS, gMSA e delegated Managed Service Accounts (dMSA)

MODULO 5: KERBEROS ABUSE E COMPROMISSIONE DEL DOMINIO

- Silver Ticket e Golden Ticket
- Abuso delle deleghe Kerberos: Unconstrained Delegation, Constrained Delegation, Resource-Based Constrained Delegation (RBCD)
- DCSync e permessi di replica
- Abuso dei privilegi sugli oggetti Active Directory
- Protezione degli account privilegiati e Tiering amministrativo

MODULO 6: ACTIVE DIRECTORY CERTIFICATE SERVICES ATTACKS

- Architettura PKI e ruolo di AD CS
- Certificate Templates, Enrollment e autenticazione tramite certificati
- Principali classi di misconfigurazione ESC
- NTLM relay verso servizi di enrollment vulnerabili
- Percorsi di escalation e persistenza tramite certificati
- Analisi e hardening di AD CS

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ATTACCHI ALLE IDENTITÀ: ACTIVE DIRECTORY, ENTRA ID E AZURE

Durata: 10,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

LABORATORIO PRATICO 2: CREDENZIALI, KERBEROS E AD CS

- Simulazione controllata di Kerberoasting
- Analisi di una configurazione Kerberos Delegation vulnerabile
- Valutazione di account dotati di permessi DCSync
- Identificazione di template AD CS configurati in modo insicuro
- Verifica delle contromisure

MODULO 7: MICROSOFT ENTRA ID SECURITY ARCHITECTURE

- Tenant, utenti, gruppi e ruoli amministrativi
- Differenze tra Microsoft Entra ID e Active Directory Domain Services
- Identity Plane e Resource Plane
- Microsoft Graph, Entra PowerShell e Azure RBAC
- Enterprise Applications e App Registrations
- Service Principal e Workload Identities
- Privileged Identity Management (PIM)

MODULO 8: CLOUD AUTHENTICATION E TOKEN ATTACKS

- OAuth 2.0, OpenID Connect e SAML
- Access Token, Refresh Token e Primary Refresh Token (PRT)
- Password spraying e rischi delle credenziali compromesse
- Session hijacking e furto di token
- Consent phishing e abuso delle autorizzazioni OAuth
- Abuso delle registrazioni applicative
- Persistenza attraverso applicazioni e credenziali applicative
- Differenze tra MFA tradizionale e MFA phishing-resistant
- Conditional Access, token protection e session controls

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ATTACCHI ALLE IDENTITÀ: ACTIVE DIRECTORY, ENTRA ID E AZURE

Durata: 10,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 9: ENTRA ID PRIVILEGE ESCALATION

- Enumerazione di ruoli, gruppi e permessi
- Relazioni tra identità utente, applicazioni e service principal
- Application permissions e delegated permissions
- Abuso di privilegi Microsoft Graph
- Credenziali e certificati associati alle applicazioni
- Permessi eccessivi sulle workload identities
- Rilevamento delle applicazioni con privilegi critici

LABORATORIO PRATICO 3: ENTRA ID

- Enumerazione di un tenant Entra ID di laboratorio
- Analisi delle autorizzazioni di un'applicazione OAuth
- Identificazione di un service principal con privilegi eccessivi
- Simulazione di un rischio di compromissione di token e sessioni
- Verifica della copertura di Conditional Access e PIM

MODULO 10: AZURE CLOUD PRIVILEGE ESCALATION

- Azure RBAC e scope delle autorizzazioni
- Managed Identities: system-assigned e user-assigned
- Accesso alle risorse attraverso le identità dei workload
- Azure Virtual Machines e permessi di gestione
- Azure Key Vault e protezione dei segreti
- Storage Account, Blob Storage e configurazioni di accesso
- Privilege escalation tramite assegnazioni RBAC errate
- Percorsi di attacco tra identità, risorse e applicazioni Azure

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ATTACCHI ALLE IDENTITÀ: ACTIVE DIRECTORY, ENTRA ID E AZURE

Durata: 10,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 11: HYBRID IDENTITY ATTACKS

- Microsoft Entra Connect Sync e Cloud Sync
- Password Hash Synchronization e Pass-through Authentication
- Seamless Single Sign-On e federazione
- Rischi associati ai sistemi e agli account di sincronizzazione
- Percorsi di compromissione tra Active Directory ed Entra ID
- Protezione degli account di sincronizzazione e delle infrastrutture ibride

MODULO 12: DETECTION, HARDENING E INCIDENT RESPONSE

- Microsoft Defender for Identity e Defender XDR
- Analisi dei Sign-in Logs e Audit Logs di Entra ID
- Correlazione degli eventi tramite Microsoft Sentinel
- Rilevamento di comportamenti Kerberos e NTLM anomali
- Identificazione di modifiche sospette ad ACL, ruoli e applicazioni
- Hardening di Active Directory ed Entra ID
- Identity Security Assessment e prioritizzazione delle remediation

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO ATTACCHI ALLE IDENTITÀ: ACTIVE DIRECTORY, ENTRA ID E AZURE

Durata: 10,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

OVERVIEW DEL CORSO

Nella maggior parte delle aziende le identità sono la via più rapida per compromettere l'infrastruttura. Il corso segue il percorso di un attaccante da Active Directory a Microsoft Entra ID e Azure: meccanismi di autenticazione, tecniche di attacco su credenziali, Kerberos, AD CS, applicazioni OAuth e managed identity, fino ai punti di contatto dell'identità ibrida.

Tre laboratori pratici in ambienti isolati preparati da Nexsys insegnano a cercare le stesse vulnerabilità nel proprio ambiente e a decidere quali correggere per prime. Ogni tecnica è collegata agli eventi da monitorare in Defender e Sentinel e alle contromisure di hardening.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Amministratori di sistema e di Active Directory che vogliono sapere quali configurazioni un attaccante sfrutterebbe per primo
- Amministratori Microsoft 365, Entra ID e Azure che devono controllare permessi, consensi e managed identity
- Security engineer e analisti SOC che devono collegare le tecniche di attacco agli eventi da monitorare
- IT manager e responsabili della sicurezza che devono definire le priorità di remediation su un'infrastruttura di identità ibrida

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Comprendere NTLM, Kerberos, OAuth 2.0 e OpenID Connect e dove nascono le loro debolezze
- Ricostruire i percorsi verso gli account privilegiati in Active Directory ed Entra ID, anche con BloodHound
- Riconoscere gli attacchi alle credenziali e ai ticket Kerberos
- Valutare deleghe, account di servizio e template AD CS
- Individuare applicazioni, service principal e managed identity con privilegi eccessivi
- Capire come una compromissione si sposta tra Active Directory, Entra ID e Azure
- Collegare ogni tecnica a detection, hardening e priorità di remediation

CONTATTI

info@nexsys.it

www.nexsys.it