CORSO RED TEAMING ACTIVE DIRECTORY: ATTACK & DEFENSE

Durata: 2 giorni

NEXSYS
LEARN IT, TRANSFORM IT

TopSelection

PROGRAMMA

MODULO 1: ACTIVE DIRECTORY ENUMERATION AND LOCAL PRIVILEGE ESCALATION

- Enumerare informazioni utili come utenti, gruppi, appartenenze a gruppi, computer, proprietà degli utenti, trust, ACL per mappare i percorsi di attacco.
- Imparare e mettere in pratica diverse tecniche di escalation dei privilegi locali su una macchina Windows.
- Cercare i privilegi di amministratore locale sui computer del dominio di destinazione utilizzando diversi metodi.
- Abusare delle applicazioni aziendali per eseguire percorsi di attacco complessi che comportano l'aggiramento dell'antivirus e il passaggio a macchine diverse.

MODULO 2: LATERAL MOVEMENT, DOMAIN PRIVILEGE ESCALATION AND PERSISTENCE

- Imparare a trovare le credenziali e le sessioni degli account di dominio con privilegi elevati, come gli amministratori di dominio, ed estrarre le loro credenziali.
- Imparare a estrarre le credenziali da un ambiente ristretto in cui viene applicato il whitelisting delle applicazioni.
- Comprendere il classico Kerberoast e le sue varianti per l'escalation dei privilegi.
- Comprendere e sfruttare i problemi di delega
- Imparare ad abusare dei privilegi dei gruppi protetti per aumentare i privilegi.
- Abusare della funzionalità Kerberos per persistere con privilegi DA. Falsificare i ticket per eseguire attacchi come Golden ticket e Silver ticket per persistere.
- Abusare della modalità sicura del DC Administrator per persistere.
- Abusare del meccanismo di protezione come AdminSDHolder per la persistenza.

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO RED TEAMING ACTIVE DIRECTORY: ATTACK & DEFENSE

Durata: 2 giorni

NEXSYS
LEARN IT, TRANSFORM IT

TopSelection

MODULO 3: DOMAIN PERSISTENCE, DOMINANCE AND ESCALATION TO ENTERPRISE ADMINS

- Abusare dei diritti minimi richiesti per attacchi come DCSync modificando le ACL degli oggetti di dominio.
- Imparare a modificare i descrittori di sicurezza dell'host del controller di dominio per persistere ed eseguire comandi senza bisogno di privilegi DA.
- Imparare a elevare i privilegi da Domain Admin di un dominio figlio a Enterprise Admin sulla radice della foresta abusando delle chiavi di fiducia e dell'account krbtgt.
- Eseguire attacchi di fiducia intra-foresta per accedere alle risorse della foresta.
- Abusare dei collegamenti ai database per ottenere l'esecuzione di codice in tutta la foresta utilizzando semplicemente i database.

MODULO 4: MONITORING, ARCHITECTURE CHANGES, BYPASSING ADVANCED THREAT ANALYTICS AND DECEPTION

- Scopri gli eventi utili registrati quando vengono eseguiti gli attacchi discussi
- Scopri brevemente le modifiche all'architettura necessarie in un'organizzazione per evitare gli attacchi discussi: appartenenza a gruppi temporali, controllo ACL, LAPS, filtro SID, autenticazione selettiva, protezione delle credenziali, protezione del dispositivo (WDAC), gruppo di utenti protetti, PAW, amministrazione a livelli ed ESAE o Foresta Rossa
- Scopri come Advanced Threat Analytics di Microsoft e altri strumenti simili rilevano gli attacchi al dominio e come evitare e aggirare tali strumenti
- Comprendere come l'inganno può essere utilizzato efficacemente come meccanismo di difesa in AD

Scopri di più sul **Corso Red Teaming Active Directory: Attack And Defense**

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO RED TEAMING ACTIVE DIRECTORY: ATTACK & DEFENSE

Durata: 2 giorni

NEXSYS
LEARN IT, TRANSFORM IT

TopSelection

OVERVIEW DEL CORSO

Il corso è stato studiato per permettere ai membri del red team di apprendere le tecniche opportune per attaccare e difendere le infrastrutture Active Directory.

La formazione è indirizzata ai professionisti della sicurezza informatica, in modo da identificare e analizzare le minacce in un moderno ambiente Active Directory. Nel corso verranno trattati argomenti come l'enumerazione di AD, la mappatura delle Trust Relationship, l'escalation dei privilegi di dominio, gli attacchi basati su Kerberos, i trust del server SQL, le tecniche di difesa e il relativo bypass.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Amministratori di sistema;
- Security professionals;
- Auditors;
- Red team specialist;
- E in generale a tutti coloro che abbiano interesse ad aumentare la propria competenza sulla sicurezza di AD.

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

Attacco

- Introduzione ad AD e Powershell
- Autenticazione e Domain Controllers
- Recon nelle infrastrutture AD
- Metodi di attacco
- Kerberos e NTLM
- Privilege Escalation
- Password e Hash
- Attacchi Kerberos e mimikatz
- Persistence

Difesa

- Modelli di difesa
- Modelli di logging
- Detection degli attacchi
- Miglioramenti della security di Windows Server e di AD

CONTATTI

info@nexsys.it

www.nexsys.it