

CORSO PENETRATION TEST

Durata: 3 giorni



PROGRAMMA

MODULO 1: INTRODUZIONE

- Introduzione al Penetration Testing
- Distinzione dal Red Teaming
- Come scrivere i report
- Introduzione a NetExec e perché è centrale nel corso
- I cicli di un engagement

MODULO 2: INITIAL ACCESS

- Abuso dei permessi di lettura/scrittura su share NFS
- Abuso di base di applicazioni web

MODULO 3: ENUMERATION

- Uso di NetExec per enumerare NFS nella rete
- Port scanning e service discovery
- Estrazione da Active Directory di informazioni utili: utenti, gruppi, computer e proprietà degli utenti

MODULO 4: PRIVILEGE ESCALATION

- Tecniche di Local Privilege Escalation su macchine Linux e Windows
- Riutilizzo delle credenziali (replay) per individuare privilegi elevati su altre macchine
- Abuso dei privilegi Selpersonate per la privilege escalation su Windows

MODULO 5: ANTI VIRUS EVASION

- Evasione di Windows Defender con obfuscation, string manipulation e altre tecniche

CONTATTI

 info@nexsys.it

 www.nexsys.it

CORSO PENETRATION TEST

Durata: 3 giorni



MODULO 6: TUNNELLING E PIVOTING

- Configurazione del tunnelling tramite SSH per attaccare l'infrastruttura a partire dal proprio foothold
- Pivoting con Ligolo-Ng: General Authentication, Kerberos e Local Authentication
- Abuso di una VPN Layer 2 per accedere a segmenti di rete

MODULO 7: LOOTING DELLE MACCHINE WINDOWS

- Ricerca nei fileshare
- Estrazione di credenziali da LSA, SAM e DPAPI
- Impersonazione della sessione di un utente
- Uso di protocolli non comuni per gli attacchi

MODULO 8: DOMAIN PRIVILEGE ESCALATION

- Individuazione e impersonazione delle sessioni di account ad alti privilegi (Domain Admins) per la privilege escalation
- Abuso dei diritti minimi necessari per attacchi come il DCSync, modificando le ACL degli oggetti di dominio

MODULO 9: RELAYING

- Relay attack con account utente e account macchina
- Cross-protocol relay attack

MODULO 10: ABUSO DI AD CS E SQL SERVER

- Abuso dei SQL Server ed estrazione di segreti dal database
- Active Directory Certificate Services (AD CS)
- Domain Privilege Escalation abusando di AD CS

MODULO 11: SVILUPPO DI MODULI CUSTOM PER NETEXEC

- Sviluppo di un modulo NetExec custom per il tunnelling
- Uso del modulo nel lab per effettuare il pivoting di rete

CORSO PENETRATION TEST

Durata: 3 giorni



OVERVIEW DEL CORSO

Il Corso Penetration Test di Nexsys è un percorso pratico e avanzato che riproduce un vero engagement di penetration testing in ambito aziendale: dall'initial access fino alla compromissione completa del dominio Active Directory. Ogni fase viene affrontata in laboratorio, con gli stessi strumenti e le stesse tecniche usate nei test di sicurezza reali.

Il filo conduttore è NetExec, lo strumento di riferimento per enumerare e attaccare l'infrastruttura di rete e Active Directory, usato in quasi tutte le fasi del corso fino allo sviluppo di un modulo custom per il pivoting. Il corso chiarisce anche la differenza tra penetration test e Red Teaming e dedica spazio a come si scrive un report professionale.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Penetration tester e security specialist che vogliono consolidare le tecniche offensive su Active Directory
- Ethical hacker e membri di Red Team impegnati in assessment interni
- Amministratori di sistema e di rete che vogliono capire come viene attaccata la loro infrastruttura per difenderla meglio
- Analisti SOC e Blue Team che vogliono conoscere le tecniche d'attacco per riconoscerle e contrastarle
- Professionisti della cybersecurity che preparano engagement di penetration test in azienda

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Ottenere un initial access abusando di share NFS e di applicazioni web esposte
- Enumerare rete e Active Directory con NetExec: utenti, gruppi, computer e proprietà degli oggetti
- Effettuare Local Privilege Escalation su Linux e Windows, incluso l'abuso dei privilegi Selpersonate
- Eludere Windows Defender con tecniche di obfuscation e string manipulation
- Muoversi nell'infrastruttura con tunnelling SSH, pivoting con Ligolo-Ng e VPN Layer 2
- Estrarre credenziali da LSA, SAM e DPAPI ed effettuare il looting delle macchine Windows
- Conquistare il dominio con DCSync, relay attack e abuso di AD CS e SQL Server, e sviluppare un modulo NetExec custom

