LABORATORIO HACKING ACTIVE DIRECTORY

Durata: 7 ore

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: PREPARAZIONE DEL LAB

- Setup ambiente virtuale con dominio Windows e macchina Kali Linux
- Configurazione: BloodHound, PowerView, mimikatz, CrackMapExec, Rubeus, Evil-WinRM
- Introduzione all'uso delle shell remote (WinRM / SMB)

MODULO 2: ACCESSO INIZIALE

- Attacchi: password spraying, enumerazione SMB, accessi RDP
- Uso delle prime credenziali in ambienti limitati

MODULO 3: ENUMERATION ACTIVE DIRECTORY

- Raccolta informazioni: utenti, gruppi, computer, deleghe, ACL
- Tool: PowerView, ADRecon, SharpHound
- Analisi grafica delle relazioni con BloodHound

MODULO 4: COMPROMISSIONE DELLE CREDENZIALI

- AS-REP Roasting e Kerberoasting
- Dumping da LSASS con mimikatz
- Cracking hash offline (john/hashcat)
- Enumerazione deleghe e SIDHistory

MODULO 5: ESCALATION DEI PRIVILEGI

- Attacchi RBCD (Resource-Based Constrained Delegation)
- Abuso ACL e privilege escalation orizzontale/verticale
- Tecniche DCSync per diventare Domain Admin

CONTATTI

info@nexsys.it

www.nexsys.it

LABORATORIO HACKING ACTIVE DIRECTORY

Durata: 7 ore

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 6: COMPROMISSIONE DOMINIO ACTIVE DIRECTORY

- Creazione Golden e Silver Ticket
- Attacchi DCShadow
- Modifica persistente dell'AD (adminSDHolder, SIDHistory)

MODULO 7: ATTACCHI AI DATABASE SQL SERVER

- Enumerazione e accesso a SQL Server dal dominio
- Abuso di credenziali per backup e dump del contenuto
- Esecuzione comandi su SQL via xp_cmdshell
- Escalation tramite accesso SQL locale

MODULO 8: ATTACCHI AD ADCS (CERTIFICATE SERVICES)

- Ricognizione su servizi di certificazione attivi nel dominio
- Abuse dei template vulnerabili
- Attacchi ESC1, ESC2, ESC6 (Abuse Enrollment Rights)
- Golden Certificate: autenticazione persistente

MODULO 9: PERSISTENZA E CLEANUP

- Creazione backdoor utente persistente
- Task schedulati, RunKeys, GPO persistenti
- Tecniche di pulizia post-attacco

CONTATTI

info@nexsys.it

www.nexsys.it

LABORATORIO HACKING ACTIVE DIRECTORY

Durata: 7 ore

NEXSYS
LEARN IT, TRANSFORM IT

OVERVIEW DEL CORSO

Un percorso formativo nel mondo dell'Ethical Hacking totalmente hands-on, pensato per chi vuole scoprire le tecniche più utilizzate nei penetration test e nel red teaming applicate specificatamente ad Active Directory. Nel laboratorio i partecipanti sperimenteranno, in un ambiente virtuale controllato, le metodologie di attacco che minacciano quotidianamente i sistemi Windows, SQL Server e Active Directory, con l'obiettivo di comprenderne il funzionamento per poterle riconoscere, contrastare e prevenire in contesti reali di cybersecurity aziendale. La formazione live online è guidata da un trainer certificato Ethical Hackers con una vasta esperienza di tecniche di attacco e difesa su sistemi Microsoft.
Questo laboratorio è il naturale completamento del corso Red Teaming: Active Directory Attack and Defense, pensato per rafforzare le competenze pratiche di ethical hacker, system administrator e professionisti della sicurezza IT.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Ethical hacker
- Penetration tester
- System Administrator
- IT Security Analyst
- Professionisti IT che vogliono conoscere le minacce su AD

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Configurare e utilizzare un laboratorio Active Directory
- Eseguire attacchi di accesso iniziale e password spraying
- Enumerare utenti, gruppi e permessi in AD
- Compromettere e crackare credenziali con tool avanzati
- Escalare privilegi fino a Domain Admin
- Creare e sfruttare Golden e Silver Ticket
- Attaccare SQL Server e sfruttare xp_cmdshell
- Abusare di ADCS per persistenza e autenticazione

CONTATTI

info@nexsys.it

www.nexsys.it