CORSO ACTIVE DIRECTORY SECURITY : ATTACK AND DEFENSE

DURATA: 2 GIORNI

PROGRAMMA

MODULE I: ACTIVE DIRECTORY ENUMERATION AND LOCAL PRIVILEGE ESCALATION

- Enumerate useful information like users, groups, group memberships, computers, user properties, trusts, ACLs in order to map attack paths
- Learn and practice different local privilege escalation techniques on a Windows machine
- Hunt for local admin privileges on machines in the target domain using multiple methods
- Abuse enterprise applications to execute complex attack paths that involve bypassing antivirus and pivoting to different machines

MODULE II: LATERAL MOVEMENT, DOMAIN PRIVILEGE ESCALATION AND PERSISTENCE

- Learn to find credentials and sessions of high privileges domain accounts like Domain Administrators, extracting their credentials
- Learn to extract credentials from a restricted environment where application whitelisting is enforced.
- Understand the classic Kerberoast and its variants to escalate privileges
- Understand and exploit delegation issues
- Learn how to abuse privileges of Protected Groups to escalate privileges
- Abuse Kerberos functionality to persist with DA privileges. Forge tickets to execute attacks like Golden ticket and Silver ticket to persist
- Abuse the DC safe mode Administrator for persistence
- Abuse the protection mechanism like AdminSDHolder for persistence

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

- Abuse minimal rights required for attacks like DCSync by modifying ACLs of domain objects
- Learn to modify the host security descriptors of the domain controller to persist and execute commands without needing DA privileges
- Learn to elevate privileges from Domain Admin of a child domain to Enterprise Admins on the forest root by abusing Trust keys and krbtgt account
- Execute intra-forest trust attacks to access resources across forest
- Abuse database links to achieve code execution across forest by just using the databases

CONTACT

info@nexsys.it

www.nexsys.it

CORSO ACTIVE DIRECTORY SECURITY : ATTACK AND DEFENSE

DURATA: 2 GIORNI

MODULE IV: MONITORING, ARCHITECTURE CHANGES, BYPASSING ADVANCED THREAT ANALYTICS AND DECEPTION

- Learn about useful events logged when the discussed attacks are executed
- Learn briefly about architecture changes required in an organization to avoid the discussed attacks: Temporal group membership, ACL Auditing, LAPS, SID Filtering, Selective Authentication, credential guard, device guard (WDAC), Protected Users Group, PAW, Tiered Administration and ESAE or Red Forest
- Learn how Microsoft's Advanced Threat Analytics and other similar tools detect domain attacks and the ways to avoid and bypass such tools
- Understand how Deception can be effective deployed as a defense mechanism in AD

Scopri di più sul Corso Active Directory Security : Attack and Defense

CONTACT

info@nexsys.it

www.nexsys.it