CORSO PENETRATION TEST ON AZURE: CLOUD SECURITY

Durata: 1,5 giorni

NEXSYS
LEARN IT, TRANSFORM IT

TopSelection

PROGRAMMA

MODULO 1: INTRODUCTION, RECON & DISCOVERY, INITIAL ACCESS

- Introduzione ad Azure
  - Comprendere Azure e Azure AD.
  - Architettura di Azure e assegnazioni di ruolo.
  - Comprendere la metodologia di attacco e Azure Kill Chain.
- Discovery and Recon of services and applications
  - OSINT e tecniche di enumerazione non autenticate
  - Raccogliere informazioni sul tenant target.
  - Convalidare gli ID e-mail per un'organizzazione.
  - Autorizzazioni predefinite di cui dispone un utente di Azure AD in un tenant.
- Initial Access Attacks
  - Errori opsec durante lo spraying delle password nel cloud.
  - Attacco di concessione del consenso illecito per l'accesso iniziale contro simulazioni di più utenti in laboratorio.
  - Abusare delle applicazioni web
  - Abuso Account di archiviazione non sicuri.
  - Attacchi di phishing contro la simulazione di un utente.
  - Utilizzare le credenziali dell'applicazione per accedere al tenant di destinazione.
  - Abusare di CI/CD per ottenere l'accesso a un tenant di Azure.

MODULO 2: ENUMERATION E PRIVILEGE ESCALATION

- Enumeration
  - Enumerare le informazioni da Azure AD.
  - Mappare i percorsi di attacco elencando gli oggetti di proprietà di un oggetto Azure AD.
  - Identità dei dispositivi e mappare i percorsi di attacco
  - Entità servizio e applicazioni soggette a abusi.
  - Enumerare le informazioni da Azure.
  - Enumerare le assegnazioni di ruolo per mappare i percorsi di attacco.
  - ROADRecon e Azure Hound per l'enumerazione.
  - API REST ARM e MS Graph per l'enumerazione.
- Privilege Escalation
  - Servizi di abuso come account di automazione, Key Vault, account di archiviazione, cronologia di distribuzione e altro ancora per l'escalation dei privilegi orizzontale e verticale in Azure.
  - Privilegi in Azure AD e Azure abusando dei ruoli personalizzati.
  - Abusare delle autorizzazioni su altre risorse per aumentare i privilegi.
  - Abusare dell'estensione script personalizzata e dei privilegi RunCommand.
  - Gruppi dinamici e abusare della regola di appartenenza.

CONTATTI info@nexsys.it www.nexsys.it

CORSO PENETRATION TEST ON AZURE: CLOUD SECURITY

Durata: 1,5 giorni

NEXSYS
LEARN IT, TRANSFORM IT

TopSelection

MODULO 3: LATERAL MOVEMENT E PERSISTENCE

- Lateral Movement
  - Abusare dei lavoratori ibridi che utilizzano runbook negli account di Automazione per passare dal tenant di Azure alle macchine locali.
  - Spostamento laterale da GitHub al tenant di Azure.
  - Attacco Pass-The-PRT per riprodurre il cookie PRT di un utente.
  - Abusare di Intune per eseguire comandi su macchine locali.
  - Attacchi contro le applicazioni utilizzando il proxy dell'applicazione.
  - Abusare dei modelli di identità ibrida (PHS, PTA e Federation).
- Persistence
  - Opportunità persistenti quando viene utilizzata un'identità ibrida.
  - Criticità del server Azure AD Connect e il modo in cui la persistenza a livello di sistema operativo su tale macchina può essere utilizzata per compromettere sia l'infrastruttura locale che quella cloud.
  - Attacchi Skeleton key in the cloud e Golden SAML.
  - Opportunità di persistenza per le risorse di Azure come account di archiviazione, applicazioni ed entità servizio, consensi e autorizzazioni, VM e gruppi di rete di Azure, ruoli personalizzati di Azure e Azure AD ecc.

MODULO 4: DATA MINING, DEFENSES E DEFENSES BYPASS

- Data Mining
  - Estrarre segreti da Key Vault abusando dell'identità gestita.
  - Mappatura dei percorsi di attacco leggendo le assegnazioni dei ruoli.
  - Estrarre segreti dalla cronologia di distribuzione.
  - Estrarre password e token dell'applicazione in chiaro dalla workstation di un utente Azure compromessa.
  - Estrarre segreti dall'archiviazione BLOB.
- Defenses
  - Indicazioni sulla difesa di Microsoft in diverse categorie.
  - Politiche di accesso condizionale, della gestione delle identità privilegiate, della protezione dell'identità di Azure AD, di Microsoft Defender for Cloud e delle sue funzionalità
  - Valutazione dell'accesso continuo e il suo impatto sulla riproduzione dei token di accesso.
  - Applicare l'AMF in Azure AD.
- Defenses Bypass
  - Policy di accesso condizionato più utilizzate ed come aggirarle.
  - Opsec per evitare rilevamenti da parte di Azure AD Identity Protection.
  - Metodi che possono essere utilizzati per bypassare l'AMF.
  - Evitare la protezione del carico di lavoro cloud di Microsoft Defender per cloud come JIT, ANH, NSG e firewall di Azure per accedere alle VM.

Scopri di più sul **Corso Penetration Test on Azure: Cloud Security**

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO PENETRATION TEST ON AZURE: CLOUD SECURITY

Durata: 1,5 giorni

NEXSYS
LEARN IT, TRANSFORM IT

TopSelection

OVERVIEW DEL CORSO

Il corso Penetration Test on Azure – Cloud Security insegna ai partecipanti ad eseguire un pen-test efficace in un ambiente di rete aziendale che potrebbe essere attaccato, tramite il bypassas delle misure di Sicurezza e difeso.

Comprendi attraverso la formazione in ambito Cloud Security, le diverse tecniche e metodologie di attacco di Microsoft Azure utilizzate dagli hacker.

Scopri come garantire la sicurezza informatica nell'ecosistema del Public Cloud Microsoft e scopri vari strumenti e tecniche per eseguire con successo i penetration test sulla tua infrastruttura Azure.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a :

- IT Manager
- Professionisti IT
- Architetti del cloud
- Professionisti della sicurezza
- Penetration tester
- Appassionati di sicurezza

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Gestire le tecniche di enumerazione di Azure
- Identificare le configurazioni di Security errate del cloud
- Sfruttare le lacune nel controllo degli accessi
- Padroneggiare i Lateral Movement
- Sfruttare gli attacchi di phishing per la compromissione iniziale
- Condurre controlli di sicurezza del cloud

CONTATTI

info@nexsys.it

www.nexsys.it