

×

RETI-HAC-2A - Hands-On Hacking avanzato parte 1

ITCore Security - IT Security - Cyber Security

Durata: Lingue: Certificazione:

1 Giorno Italiano -

Descrizione del corso

Il corso di una giornata, intensivo, è dedicato ad approfondire alcuni meccanismi fondamentali di Active Directory al fine di capire alcuni tra i più diffusi vettori di attacco (red team) ed elaborare strategie di monitoraggio e protezione (blue team).

Per accedere a questo corso è consiglibile aver partecipato ai corsi Hands-On Hacking base 1 e 2 oppure avere già conoscenze pregresse in ambito IT Security.

Il corso sarà corredato di video ed esempi pratici sugli argomenti più importanti.

Il corso verterà su Active Directory e sulle best practice per effettuare le attività quotidiane come, ad esempio, la configurazione di policy, la gestione di utenze e password e la possibilità di monitorare parte della propria infrastruttura attraverso tool integrati o di terze parti, gli strumenti per il monitoraggio e l'analisi delle vulnerabilità legate all'infrastruttura

Programma

Modulo 1: Active Directory

- Panoramica generale su Active Directory: Foresta, Dominio, Ruoli
- Gestione di gruppi privilegiati, gestione sicura e Best Practice per utenze e gruppi in Active Directory
- Group Policy Object: Gestione, sicurezze e monitoraggio delle policy di dominio

ITCore Group

Via Balestra, 12 6900 Lugano (CH) +41.091.9760019 www.itcoregroup.com



- Gpo Auditing e tool per il monitoraggio degli eventi
- Gestione delle password a dominio: Default Vs Fine Grained Password
- Gestione delle password: errori comuni

Modulo 2: Approfondimento

- Politiche di Least Privilege e zero trust
- Gestione condizionale delle GPO: gli strumenti a nostra disposizione
- DNS, RODC e altri servizi cruciali per l'infrastruttura
- Deleghe, Protected User Account e altre configurazioni per ridurre la superficie d'attacco
- Analisi dei server e dei servizi alla ricerca di configurazioni mancanti o errate

Modulo 3: Attacchi

- Kerberos e Idap
- Attacchi kerberoasting, golden ticket
- Mimikatz tool con alcune dimostrazioni video.
- Come prevenire e proteggere l'infrastruttura da questi attacchi
- L'importanza degli aggiornamenti di sistema e strumenti per compiere queste attività

Modulo 4: Monitoraggio e indagine

- Ping Castle
- Bloodhound (sharpound) e badblood
- A continuo: software per monitorare la propria infrastruttura