Active Directory Security

CODICE	**DT0318**
DURATA	**3 gg**
PREZZO	**1.550,00 €**
EXAM	

DESCRIZIONE

Il corso Active Directory Security è un percorso pratico e intensivo progettato per fornire competenze operative di attacco e difesa su Active Directory, l'infrastruttura più utilizzata nelle aziende per la gestione di utenti, identità e permessi.
Grazie a un approccio laboratoriale, basato su scenari realistici e procedure passo-passo, i partecipanti imparano come gli attaccanti compromettono un dominio e quali strategie implementare per rilevare, bloccare e mitigare le minacce.

Durante il corso vengono affrontate tecniche reali di enumerazione, privilege escalation, movimenti laterali, persistente compromissione del dominio e sfruttamento dei trust tra foreste. Allo stesso tempo, sono fornite metodologie difensive aggiornate per migliorare sicurezza, monitoraggio e resilienza dell'infrastruttura Active Directory.

TARGET

Il corso è ideale per:

- Red teamer, penetration tester e professionisti dell'offensive security
- Blue team, SOC analyst, incident responder e amministratori di domini Windows
- Chi possiede una conoscenza di base di Active Directory e vuole acquisire competenze avanzate operative

PREREQUISTI

Conoscenze di base di Active Directory e Windows

CONTENUTI

Enumerazione AD

- Strumenti per raccogliere utenti, gruppi, GPO, ACL e trust intra-/inter-forest

Tradecraft offensivo

- Tecniche per enumerare, modificare tool e bypassare Defender/AMSI e logging

Persistenza nel dominio

- Ticket Kerberos (Golden/Silver/Diamond), attacchi a livello DC (Skeleton key, DCSync)

Attacchi cross-trust

- Sfruttamento di trust Active Directory per muoversi e scalare privilegi tra foreste.

Escalation privilegi

- Admin locali, abuso di delegations replay di credenziali per ottenere privilegi di dominio

Difese e bypass

- Analisi di come vengono rilevati gli attacchi e le tecniche per evitarli

Mitigazioni e monitoraggio

- Raccomandazioni architetturali, logging utile e uso della deception