

## OEC240

### Active Directory Security : Attack and Defense

Durata: 2 gg

#### Descrizione

Il corso è stato studiato per permettere agli studenti di apprendere le tecniche opportune per attaccare e difendere le infrastrutture Active Directory, nonché di migliorare la capacità di analizzare e scoprire gli attacchi attraverso una miglior conoscenza degli eventi da verificare.

#### A chi è rivolto?

Il corso è rivolto ad amministratori di sistema, security professionals, auditors – in generale a tutti coloro che abbiano interesse ad aumentare la propria competenza sulla sicurezza di AD.

#### Prerequisiti

Conoscenze di base di sicurezza e di sistemi operativi, conoscenza di base di AD.

#### Contenuti

Attacchi

- Introduzione ad AD e Powershell
- Autenticazione e Domain Controllers
- Recon nelle infrastrutture AD
- Metodi di attacco
- Kerberos e NTLM
- Privilege Escalation
- Password e Hash
- Attacchi Kerberos e mimikatz
- Persistence

Difesa

- Modelli di difesa
- Modelli di logging
- Detection degli attacchi
- Miglioramenti della security di Windows Server e di AD