SETA.
Security talent academy

www.seta.academy

FORMAZIONE PER AZIENDE

Sicurezza di Reti e Sistemi

Oggi è fondamentale la presenza all'interno delle linee IT (Management, Compliance, Risk, ...) di una figura che possieda i requisiti per garantire un adeguato livello di sicurezza. I partecipanti al corso impareranno a comprendere e contrastare le sofisticate tecniche di attacco e di intrusione dei criminali informatici. L'obiettivo non è quello di elencare strumenti o exploit 0-day, ma di rivelare il punto di vista che guida gli attaccanti per comprendere come difendere i propri asset al meglio. Gli argomenti trattati verranno verificati attraverso sessioni pratiche guidate in laboratorio.

Durata
4 giorni di lezione (modularizzabili a richiesta)

Modalità di erogazione
Il corso è erogabile sia in aula, sia in aula virtuale.

Prerequisiti
Conoscenza di base dei protocolli di rete TCP/IP. Familiarità con un sistema operativo di tipo GNU/Linux.

Materiale didattico
Dispense utilizzate durante il corso. Immagini delle macchine virtuali utilizzate durante le esercitazioni.

Requisiti tecnici

- Postazione personale con Kali Linux o altra distribuzione GNU/Linux.
- Saranno comunicati ai singoli iscritti i tool da installare nel caso venga utilizzata una postazione personale.

Obiettivi

Obiettivo del corso è quello di far apprendere ai partecipanti come viene compromessa la sicurezza dei sistemi e delle reti IT, utilizzando le tecniche e gli strumenti che vengono adottati dai reali attaccanti. Le competenze trasmesse permetteranno di poter decidere in piena autonomia quali contromisure sia meglio adottare per proteggere le proprie infrastrutture, o quantificarne più precisamente il livello di rischio.

Target

- Amministratori di reti e sistema
- Auditor e analisti di sicurezza
- Responsabili della Sicurezza IT
- Professionisti IT

Metodologia

Il corso ha un approccio teorico-pratico: il docente è un ethical hacker esperto di intrusioni informatiche ed attacchi alle infrastrutture di rete. Oltre a trasmettere le competenze teoriche e la conoscenza delle metodologie per identificarle ed evitarle i partecipanti avranno l'opportunità di sperimentare quanto appreso attraverso attività pratiche ed esercitazioni guidate in laboratorio.

Programma

- ✓ VA e PT: analogie e differenze
- ✓ Metodologie di analisi dei target (NIST, OSSTMM, OWASP)
- ✓ Scansione ed Enumerazione
- ✓ Analisi delle vulnerabilità
- ✓ Attacchi alle infrastrutture di Rete
  - TCP/IP e vulnerabilita' intrinseche
  - Man In The Middle
  - Sniffing, Spoofing e Hijacking
  - Denial of Services
  - Subnet, VLAN e segregazione
- ✓ Privilege Escalation
- ✓ Password e attacchi AAA
- ✓ Windows e Active Directory
- ✓ Attacchi ai Database
- ✓ Storage condivisi

Il corso non prende in considerazione (se non in maniera superficiale) le vulnerabilità specifiche di: applicazioni Web, reti Wireless, infrastrutture VoIP

Docente

Il docente è un ethical hacker esperto di intrusioni informatiche ed attacchi alle infrastrutture di rete con riconosciute capacità divulgative delle tecniche di attacco ed è membro stabile della faculty di SETA.