Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

OEC208

Security for Network & System Administrators

Durata: 4 gg

Descrizione

Il corso si propone fornire le basi di sicurezza classica e di fornire una base di partenza sulla filosofia e sulle tecniche di hacking e di sicurezza offensiva e le relative tecniche di remediation. La parte teorica sarà integrata da una serie di laboratori interattivi che permetteranno al partecipante di iniziare a comprendere il punto di vista degli attaccanti, migliorando così le proprie competenze difensive.

A chi è rivolto?

Il corso è rivolto ad amministratori di sistema, amministratori di rete e chiunque sia interessato a tecnologie relative alla sicurezza di rete.

Contenuti

Day 1

Introduzione alla security

- •CIA : confidenzialità integrità e disponibilità
- •Sicurezza e usabilità
- •SLA : I livelli di servizio

Architettura della sicurezza

- •Le basi della normative : leggi sull'hacking e Privacy
- •Architetture multi-tier
- •La DMZ
- •Architetture per small and medium business.
- •L'hardening dei sistemi
- •Patching
- •Le policy di sicurezza
- •Ambiente di test e ambiente di produzione
- •Le best practices

Day 2

Rispolverare le basi

- • La pila ISO/OSI e il Tcp/IP
- •Apparati di networking e layer ISO/OSI
- • Le basi del DNS e del DHCP
- •Amministrare windows da cmd
- •Hashing e password
- •Il coltellino svizzero del Tcp : netcat
- •Differenze tra win2k, win2k3 e win2k8
- •I firewall
- •Gli IDS

Day 3

Attacco e difesa

- •Nozioni basiche di linux
- •Preparazione di una macchina d’attacco Linux
- •Preparazione di una macchina da attacco Windows
- •Un framework d’attacco : metasploit con esempi
- •Il Vulnerability assessment : nessus con esempi
- •Network Scanning : Nmap
- •Sniffing per la difesa e l’attacco

Day 4

Attacco e difesa al network (Arp poissonning e Mac flodding)

- •Attacco e difesa al DNS (DNS poissonning – Dynamic DNS)
- •Attacco e difesa alle password di windows (LM hash – pass the hash)
- •Attacco fisico e contromisure
- •DEMO : Scrittura di un Buffer Overflow
- •Analisi e modifica di exploit pubblici o di metasploit
- •Funzionalità e limiti degli Antivirus

Day 5

- •Nozioni di attacchi web e sql con Demo
- •Nozioni di OSSTMM
- •Iso 27001 e PCI DSS