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

# OEC217

## Cybersecurity and PenTesting Techniques

Durata: 5 gg

### Descrizione

Il corso è rivolto a tutti coloro che posseggono nozioni di base di ethical hacking e che vogliono approfondire l'argomento, il corso tratta argomenti strettamente correlati al mondo reale e i laboratori sono studiati per garantire una elevata somiglianza alle reti reali che si trovano durante le attività di Penetration Test, compresi host con a bordo software Antivirus.

### A chi è rivolto?

Professionisti IT

### Prerequisiti

Buona conoscenza dei protocolli di rete, familiarità nell'uso dei sistemi operativi windows e linux, conoscenza di base delle tecniche di ethical hacking (consigliata frequenza corso CEH o conoscenza equivalente).

### Contenuti

DAY 1 Scansione ed enumerazione
- •Raccolta passiva di informazioni
- •Discovery bilanciatori e WAF
- •Nmap avanzato e sniffing
- •Banner grabbing manuale
- •Tools di enumerazione : Nmap script NSE, tools di enumerazione SMB, SNMP, DNS.

DAY 2 Buffer Overflow e exploit pubblici
- •Debugger e Basic BOF
- •Mona.py
- •egghunting
- •ASLR e DEP
- •Ricerca e modifica di exploit pubblici

DAY 3 cenni di VA e tecniche di attacco
- •Nessus
- •Metasploit base
- •Gli Antivirus
- •Trojan e backdoor
- •Tecniche di evasione degli antivirus
- •Lab con host con a bordo vari tipi di AV
- •Discovery browser info

DAY 4 tecniche avanzate di attacco, movimenti laterali e pivoting
- •Metasploit advanced
- •Modifica di payload da iniettare con metasploit
- •Mimikatz e WCE

- •QuarkPwdump e server 2012
- •Payload  in powershell, Python e VBS
- •Pivoting (lab con vmware e gns3)
- •Bypass UAC

DAY 5 Attacchi web

- •Sqlmap e sqlninja - enumerazione DB e shell da sql injection
- •Cenni di blind sql injection
- •Uso di shell in php per le RFI
- •XSS
- •Enumerazione file e directory e DirBuster
- •Proxy - Burp suite