Idee e Valori al servizio delle Aziende

ETHICAL HACKING BASIC

Gli Ethical Hacker padroneggiano gli stessi strumenti utilizzati dagli hackers. Sono risorse aziendali che tenteranno di penetrare la rete o i pc aziendali con gli stessi metodi e tecniche utilizzate dagli hacker, assicurando la protezione del know-how e più in generale di tutti i dati sensibili. Per poter ottenere la conoscenza necessaria a diventare un Ethical Hacker c'è bisogno di una formazione specifica effettuata da esperti del settore e basata su scenari di vita reale e su minacce reali identificate tra i security incident più recenti.

Il corso, della durata di cinque giorni, è principalmente volto alla acquisizione di competenze pratiche e lavorative, ma può anche essere un ausilio per sostenere esami di certificazione.

Il corso analizza e passa in rassegna le varie vulnerabilità delle infrastrutture (sistemi operativi, piattaforme applicative come SQL, applicativi, sistemi mobili e wireless, etc) fornendo una ampia panoramica degli strumenti di base per verificare le vulnerabilità, quindi ovviamente aprendo anche gli occhi su quali siano.

CONTENUTI

Il corso tratta i seguenti macro contenuti:

Modulo 1: Penetration Test

- Introduzione: tipologie di Penetration Test
- Metodologie e standard
- Aspetti normativi
- Fasi:
  a. Il Footprinting dell'infrastruttura
  b. Scansione delle porte
  c. Enumerazione risorse, servizi e account
  d. Identificare le vulnerabilità
  e. L'hacking dei sistemi e servizi
  f. Report delle varie fasi con vulnerabilità rilevate

Modulo 2: Social Engineering

- Ingegneria sociale
- Phishing
- SMSishing
- Come cercare di proteggersi

Modulo 3: Individuare gli strumenti utilizzati

- Indice degli strumenti per recuperare informazioni sull'organizzazione, sui domini, sull'infrastuttura di rete
- Introduzione a Kali Linux

Modulo 4: Ricerche DNS

- Utilizzare gli strumenti per interrogazione dei DNS: Nslookup, Dig
- Trasferimenti di zona
- Analizzare i record A, MX, SRV, PTR
- Vulnerabilità e contromisure
- Identificazione dell'architettura della rete target
- Tracert e Traceroute
- Tracerouting con geolocalizzazione

Modulo 5: Tecniche di Footprinting mediante motori di ricercar

- Google Dork: utilizzo di campi chiave di ricerca
- Utilizzo di strumenti frontend per ricerche su motori: Sitedigger
- Footprinting su gruppi di discussion

Modulo 6: Rete anonima TOR (The Onion Router)

- Comprendere le tecniche utilizzate dagli hacker per rendersi anonimi
- Tor-Browser
- Proxychains

Modulo 7: Introduzione alla fase di scansionamento delle reti

- Tipologie di scansionamento
- Aspetti legali inerenti lo scansionamento di porte – TCP, UDP, SNMP scanners
- Strumenti Pinger
- Information Retrieval Tools
- Contromisure
- Query ICMP
- Utilizzo di Nmap e SuperScan
- Tools di scansionamento presenti nella distribuzione Kali Linux
- Scanner per dispositivi mobile

Modulo 8: Esercitazione Pratica

- Footprinting e scansionamento di una rete target

Modulo 9: Introduzione alla fase di Enumerazione

- Enumerazione di servizi "comuni": FTP, TELNET, SSH, SMTP, NETBIOS, etc
- Enumerazione SNMP – Ricercare le condivisioni di rete

Modulo 10: Tecniche di attacco

- Conoscere le principali tecniche di attacco ai sistemi
- Quali sono le principali tipologie di vulnerabilità sfruttabili
- Ricerca di vulnerabilità inerenti i servizi rilevati nella fase di enumerazione

Modulo 11: Esercitazione Pratica

- Ricerca di Vulnerabilità in modo manuale e mediante Vulnerability Scanner

Modulo 12: Sistemi operativi Microsoft Windows

- Hacking di Windows: le vulnerabilità più recenti
- Attacchi senza autenticazione
- Attacchi con autenticazione: scalata di privilegi (tecniche e tools)

Modulo 13: Esercitazione Pratica

- Simulazione dell'hacking di un sistema Windows con Metasploit
- Attacchi di tipo Man-In-The-Middle
- Dirottamento di sessioni
- Attacchi di tipo ARP Poisoning
- Tools Cain&Abel, BetterCap

Modulo 14: Cenni all'Hacking di Unix/Linux

- Principali tipologie di intrusione in sistemi Unix
- Utente root
- Vulenrabilità Servizi

Modulo 15: Esercitazione Pratica

- Simulazione dell'hacking di un sistema Linux

Modulo 16: Cenni sull'Hacking dei Firewall

- Identificare i firewall di rete
- Sfruttare gli errori di configurazione
- Contromisure per evitare le vulnerabilità dei firewall

Modulo 17: Hacking di reti Wireless: le principali vulnerabilità

- Strumenti per effettuare la scansione delle reti wireless
- Packet Sniffer wireless, hacking di WEP, WPA e WPA2
- Strumenti di hacking delle WLAN inclusi in Kali Linux

Modulo 18: Hacking di dispositivi IoT

- Introduzione al mondo IoT, hacking di Smart home e Smart devices

Modulo 19: Hacking di applicazioni WEB

- I principali Framework e CMS utilizzati
- Principali vulnerabilità

Modulo 20: SQL Injection

- Tecnica
- Tools utilizzati
- Contromisure

Modulo 21: Esercitazione Pratica

- Hacking di un web server vulnerabile a SQL Injection

Modulo 22: Hacking nel mondo mobile

- Introduzione al rooting di dispositivi Android
- Introduzione al rooting di dispositivi iOS
- Contromisure

Modulo 23: Cloud Computing

- Architettura cloud e principali vendor
- Sicurezza fisica e logica

Modulo 24: Crittografia

- L' importanza della Crittografia
- Metodi di Crittografia utilizzati
- Attacchi Brute Force

Modulo 25: DoS e DDoS

- Introduzione al Denial of Service e Distributed Denial of Service
- Protezione