Vulnerability assessment e Penetration test di reti

CODICE	DT0115
DURATA	3 gg
PREZZO	1.590,00 €
EXAM	

DESCRIZIONE

Difendersi adeguatamente dagli attacchi, comprendendo le tecniche di hacking utilizzate per penetrare nelle reti informatiche. Ottimizzare il proprio livello di sicurezza ed evitare il superamento delle barriere di protezione. Considerare i bug dei sistemi operativi e dei dispositivi di rete per i quali esistono exploit che consentono di ottenere accesso alle reti. Esercitarsi concretamente grazie alle simulazioni pratiche di Vulnerability Assessment e Penetration Test

TARGET

Responsabili di Sicurezza Informatica, Tecnici di Sicurezza Informatica, IT Security Auditors

PREREQUISTI

Conoscenze base di Sistemi Operativi (Windows, Linux)

CONTENUTI

Definire le fasi di un Penetration Test

- Introduzione: tipologie di Vulnerability Assessment e Penetration Test
- Metodologie e standard, aspetti normativi
- Fase1. Il Footprinting della rete target
- Fase2. Effettuare la scansione delle porte
- Fase3. L'Enumerazione di account, risorse, servizi
- Fase4. Identificare le vulnerabilità
- Fase5. L'Hacking dei sistemi
- Fase6. Elaborare il report delle varie fasi con vulnerabilità riscontrate
- La distribuzione Kali Linux

Individuare gli strumenti utilizzati dagli hacker per il footprinting della rete Target

- Analizzare alcuni tra i molteplici strumenti (ricerche Whois, Maltego, etc.):

- per recuperare informazioni sull'organizzazione
- per indagare sui domini
- per recuperare informazioni sulla rete (indirizzi IP)
- per la perlustrazione della rete

Interrogazione dei DNS

- Imparare ad utilizzare gli strumenti per interrogazione dei DNS: Nslookup, Dig, etc
- Capire le vulnerabilità dovute ai trasferimenti di zona
- Analizzare i record A, MX, SRV, PTR
- Quali contromisure impiegare in questa fase

Identificazione dell'architettura della rete target

- Strumenti di tracerouting
- Tracert, e Traceroute
- Tracerouting con geolocalizzazione

Tecniche di Footprinting mediante motori di ricerca

- Footprinting con Google: utilizzo di campi chiave di ricerca
- Utilizzo di strumenti frontend per ricerche su motori
- Footprinting su gruppi di discussione

ESERCITAZIONE PRATICA: simulare la fase di footprinting di una rete
I partecipanti, con la guida del docente, simuleranno la fase di footprinting per esaminare quali informazioni è possibile reperire sulla rete target.

Introduzione alla fase di scansionamento delle reti

- Tipologie di scansionamento
- TCP, UDP, SNMP scanners
- Strumenti Pinger
- Information Retrieval Tools
- Contromisure agli scansionamenti

Tools per lo scansionamento

- Query ICMP
- Utilizzo di Nmap
- Tools di scansionamento presenti nella distribuzione Kali Linux
- Scanner per dispositivi mobile

ESERCITAZIONE PRATICA: simulare la fase di scansionamento di una rete target

Introduzione alla fase di Enumerazione.
Capire il funzionamento degli strumenti perl'enumerazione delle reti

- Enumerazione di servizi 'comuni': FTP, TELNET, SSH, SMTP, NETBIOS, etc
- Enumerazione SNMP
- Ricercare le condivisioni di rete
- Ricerca di account di rete
- Conoscere le contromisure più efficaci per l'enumerazione

Conoscere l'Hacking dei sistemi per rendere sicure le reti

- Conoscere le principali tecniche di attacco ai sistemi
- Principali tipologie di vulnerabilità sfruttabili
- Ricerca di vulnerabilità inerenti i servizi rilevati nella fase di enumerazione:
    - Ricerca 'Manuale'
    - I Vulnerability Scanner

ESERCITAZIONE PRATICA: Ricerca di Vulnerabilità in modo manuale e mediante Vulnerability Scanner

Comprendere l'Hacking dei sistemi operativi Microsoft Windows

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

ESERCITAZIONE PRATICA: effettuare la simulazione
dell'hacking di un sistema Windows e Linux con Metasploit

Attacchi di tipo Man-In-The-Middle

- Dirottamento di sessioni
- Attacchi di tipo ARP Poisoning
- Tools per attacchi MitM

Comprendere l'Hacking del Web: hacking dei server web ed hacking delle applicazioni

- Identificare la tipologia del server web target
- Verificare le vulnerabilità di IIS e Apache
- Individuare vulnerabilità in applicazioni ASP, PHP, JSP
- Hacking mediante SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, LFI/RFI, Command Injection, etc
- Predisporre efficaci contromisure

ESERCITAZIONE PRATICA: effettuare l'hacking di un web
server

Verrà simulato un tentativo di violazione di un sito web per verificarne la corretta configurazione in termini di sicurezza

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