Informatica

Ethical Hacking - 2 edizione.

Verificare la sicurezza della propria rete informatica da attacchi esterni e adottare le opportune contromisure. Posticipato al 28 novembre

Obiettivi

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 consento di ottenere accesso alle reti.
Esercitarsi concretamente grazie alle simulazioni pratiche di Penetration Test.

Argomenti

Definire le fasi di un Penetration Test
➢ Introduzione: tipologie di 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 Suite 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
• o per indagare sui domini
• o per recuperare informazioni sulla rete (indirizzi IP)
• o per la perlustrazione della rete
Introduzione al Social Engineering

DURATA TOTALE:
24 ore

NUMERO PARTECIPANTI:
8

CALENDARIO:
dal: 28/11/2022
al : 07/12/2022

TERMINE ISCRIZIONI:
22/11/2022

MODALITÀ DI SVOLGIMENTO:
WEBINAR

REFERENTE DEL CORSO:
Nicoletta Dellapina
nicoletta.dellapina@formart.it
338 1065546

QUOTA DI PARTECIPAZIONE:
380.00 € + IVA

Il corso sarà realizzato solo al raggiungimento del numero minimo di iscritti.
Le date potrebbero subire variazioni.

Interrogazione dei DNS
➢ Imparare ad utilizzare gli strumenti per interrogazione dei DNS: Nslookuo, 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: Sitedigger
➢ Footprinting su gruppi di discussione

ESERCITAZIONE PRATICA: simulare la fase difootprinting di una rete target
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
➢ Aspetti legali inerenti lo scansionamento di porte
➢ TCP, UDP, SNMP scanners
➢ Strumenti Pinger
➢ Information Retrieval Tools
➢ Attuare contromisureagli scansionamenti

Tools per lo scansionamento
➢ Query ICMP
➢ Utilizzo di Nmap e SuperScan
➢ Tools di scansionamento presenti nella distribuzione Kali Linux
➢ Scanner per dispositivi mobile
ESERCITAZIONE PRATICA: simulare la fase discansionamento di una rete target

Introduzione alla fase di Enumerazione. Capire il funzionamento degli strumenti per l'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
➢ Quali sono le principali tipologie di vulnerabilità Sfruttabili
➢ Ricerca di vulnerabilità inerenti i servizi rilevati nella fase di

enumerazione:
• o Ricerca “Manuale”
• o 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 con Metasploit

Attacchi di tipo Man-In-The-Middle
➢ Dirottamento di sessioni
➢ Attacchi di tipo ARP Poisoning
➢ Tools per attacchi MitM: Bettercap

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, etc
➢ Predisporre efficaci contromisure

ESERCITAZIONE PRATICA: effettuare l’hacking di un webserver
Verrà simulato l'hacking di una applicazione 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

Destinatari
IT Manager, Tecnici Informatici, Responsabili Sicurezza Informatica

Calendario
28, 29, 30 novembre e 5, 6, 7 dicembre dalle 14:00 alle 18:00 in videoconferenza

Docenti
Gianluca Golinelli
Ingegnere elettronico, si occupa da più di 15 anni di sicurezza informatica per aziende ed enti, per cui svolge attività di formazione e consulenza. E' stato trainer in qualità di CEI di EC - Council per la certificazione CEH (Certified Ethical Hacker). Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d’Ufficio. Certificato CEH, CHFI, CompTiA

Security+, Case.NET, ISACA CSX-P.

Requisiti

Conoscenze base di sistemi operativi e di networking