STUDIO TECNICO DI INGEGNERIA INFORMATICA
ING. GIANLUCA GOLINELLI
Informatica Forense e Sicurezza Informatica
www.gianlucagolinelli.it – g.golinelli@gianlucagolinelli.it

Effettuare il Penetration Test di reti LAN e WLAN
Verificare la sicurezza della propria rete informatica da attacchi esterni ed adottare le opportune contromisure
(Durata: 24h)

DOCENTE
Ing. Gianluca Golinelli

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
IT Manager
Responsabile Sicurezza Informatica
Tecnico di Sicurezza Informatica

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

Prerequisiti: conoscenze base di sistemi operativi e di networking;

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
  - 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: 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

Introduzione a TOR (The Onion Router)
- Comprendere le tecniche utilizzate dagli hacker per rendersi anonimi
- Tor-Browser
- Proxychains

ESERCITAZIONE PRATICA: simulare la fase di footprinting 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 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
- Quali sono le 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 con Metasploit

Attacchi di tipo Man-In-The-Middle
- Dirottamento di sessioni
- Attacchi di tipo ARP Poisoning
- Tools per attacchi MitM: Cain&Abel

Cenni sull' Hacking dei Firewall
- Identificare i firewall di rete
- Sfruttare gli errori di configurazione
- Contromisure per evitare le vulnerabilità dei firewall

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

Cenni all'Hacking di Unix/Linux
- Cercare l'utente root
- Quali sono le principali tipologie di intrusione in sistemi Unix
- Sapere come evitare le intrusioni

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

Cenni all'Hacking nel mondo mobile
- Introduzione al rooting di dispositivi Android
- Introduzione al rooting di dispositivi iOS
- Laboratorio: hacking di un dispostivo Android

Conclusione del corso