



Ethical Hacking e Penetration Testing

Introduzione

In base al nuovo principio di accountability del GDPR, in virtù del quale cambia totalmente l'approccio alla privacy, le aziende devono adottare misure adeguate alla protezione dei dati e devono verificare che dette misure siano efficaci testandone sul campo l'adeguatezza attraverso strumenti interni e/o esterni di valutazione dimostrando così di aver adottato misure adeguate ed efficaci.

Gli strumenti di vulnerability assessment e penetration testing perseguono esattamente l'obiettivo del GDPR: attraverso l'impiego di metodologie definite a livello internazionale, sono in grado di eseguire una approfondita analisi dei sistemi IT per metterne in luce le debolezze e per definire le azioni di mitigazione da intraprendere in base al rischio assunto.

Agenda

Penetration Testing

- Cosa è e cosa non è un Penetration Test
- Penetration Test come strumento per adempiere agli obblighi previsti nel GDPR
- Tipologie di Penetration Test
- Metodologie internazionali, standard e aspetti normativi
- Fasi tipiche di un Penetration Test:
 - ✓ Fase1. Footprinting
 - ✓ Fase2. Scansionamento
 - ✓ Fase3. Enumerazione
 - ✓ Fase4. Identificazione delle vulnerabilità
 - ✓ Fase5. Hacking dei sistemi
 - ✓ Fase6. Produzione della reportistica
- Produzione della documentazione a corredo
- Introduzione alla suite Kali Linux come strumento di attacco

Footprinting

- Gli strumenti di lavoro:
 - ✓ per ricercare 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
- Analizzare i record A, MX, SRV, PTR
- Strumenti di tracerouting
- Tracert e Traceroute
- Tracerouting con geolocalizzazione
- Footprinting con Google: utilizzo di campi chiave di ricerca
- Utilizzo di strumenti front-end per ricerche su motori: Site digger
- Footprinting su gruppi di discussione
- Anonimato: introduzione a TOR - The Onion Router
- TOR-Browser
- Proxychains
- Esercitazione pratica: footprinting di una rete target

Scansionamento

- Tipologie di scansionamento
- Aspetti legali inerenti lo scansionamento di porte

- TCP, UDP, SNMP scanners
- Strumenti Pinger
- Information Retrieval Tools
- Attuare contromisure agli scansionamenti
- Utilizzo di Nmap
- Scanner per dispositivi mobili
- Esercitazione pratica: scansionamento di una rete target

Enumerazione: principi e strumenti di utilità

- Enumerazione di servizi “comuni”: FTP, TELNET, SSH, SMTP, NETBIOS, SNMP.
- Ricercare le condivisioni di rete
- Ricerca di account di rete
- 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

Vettori di attacco per sistemi operativi Microsoft Windows

- Le vulnerabilità più recenti
- Attacchi senza autenticazione
- Attacchi con autenticazione: scalata di privilegi (tecniche e tools)
- Esercitazione pratica: hacking di un sistema Windows con Metasploit

Attacchi di tipo Man-In-The-Middle

- Dirottamento di sessioni
- Attacchi di tipo ARP Poisoning
- Attacchi tipo Responder

Vettori di attacco sui Firewall

- Come identificare i firewall di rete
- Come sfruttare gli errori di configurazione

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
- Esercitazione pratica: violazione di un sito web

Hacking di reti Wireless: le principali vulnerabilità

- Strumenti per effettuare la scansione delle reti wireless
- Packet Sniffer wireless, hacking di WEP, WPA, WPA2 e WPA3

Metodologie didattiche

Il corso integra alla teoria una serie di esercitazioni dimostrative realizzate con il coinvolgimento dei partecipanti. Oltre a discutere gli aspetti di importanza teorica delle tecniche di attacco e difesa, si presenteranno alcuni ambienti di utilità (Kali Linux, NMAP, ..) mettendone in evidenza con appropriate esercitazioni i principali comandi e funzionalità. Il materiale didattico comprende il manuale del corso che integra l'intera collezione delle diapositive mostrate con note, commenti, esempi e casi di studio a corredo.

Ad ogni partecipante sarà consegnato un attestato di partecipazione rilasciato da NCP.

Obiettivi

In questo corso, con simulazioni ed esercitazioni pratiche, i partecipanti apprendono come difendersi adeguatamente dagli attacchi informatici, acquisendo le tecniche di hacking utilizzate per penetrare nei sistemi IT; potenziano il proprio livello di conoscenza per approntare adeguate barriere di sicurezza; acquisiscono dimestichezza nell'individuare i bug dei sistemi operativi e dei dispositivi di rete per i quali esistono exploit che introducono falle pericolose. comprendere i rischi presenti nelle loro architetture e di approntare le soluzioni più idonee a proteggere il proprio sistema.

Destinatari

Il corso è rivolto ai responsabili della sicurezza informatica, ai manager di rete di livello Enterprise, ai System Integrator, ai Service Provider, ai Carrier.

Chiunque abbia l'esigenza di acquisire una solida conoscenza sulle tecniche di penetration testing per operare nel settore della sicurezza con competenza e professionalità.

Prerequisiti

È richiesta una buona conoscenza del TCP/IP e delle reti informatiche. E' caldamente consigliato l'aver frequentato il corso "Cyber Security Fundamentals".