

Documento di sintesi PENETRATION TESTING 2024

Simone Cappabianca - Mat: 5423306
simone.cappabianca@edu.unifi.it

Febbraio 8, 2025

Contents

1	Introduzione	3
2	Panoramica del Corso	3
3	Temi Chiave	3
4	Strumenti Chiave	8
5	Considerazioni sulla Valutazione delle Vulnerabilità	9
6	Conclusione	9

1 Introduzione

Questo documento riassume i concetti chiave, le metodologie e gli strumenti relativi al **penetration testing**, come delineato nei materiali del corso forniti. Il corso si concentra sulla fornitura di una **comprensione pratica dei principi dell'ethical hacking**, delle tecniche e della loro applicazione nella protezione delle infrastrutture IT. Il materiale pone l'accento sull'esperienza pratica all'interno di un ambiente di laboratorio controllato, incoraggiando un approccio pratico all'apprendimento della sicurezza. Il corso è tenuto dal professore associato Gabriele Costa presso IMT Lucca.

2 Panoramica del Corso

- **Materiale Didattico:** Il corso utilizza **slides e risorse open source** distribuite durante le lezioni. Gli studenti sono incoraggiati a segnalare eventuali errori nel materiale fornito.
- **Configurazione del Laboratorio:** L'ambiente di laboratorio è essenziale per il corso. Gli studenti creano un **ambiente virtualizzato** usando strumenti come VirtualBox, QEMU e Docker. Questo permette di eseguire simulazioni in modo sicuro.
- **Apprendimento Pratico:** Il corso enfatizza l'**esperienza pratica** tramite esercizi e laboratori.
- **Coerenza Metodologica:** La metodologia per il penetration testing rimane la stessa indipendentemente dal tipo di azienda che viene valutata.

3 Temi Chiave

1. Ethical Hacking e Penetration Testing

- L'hacking è definito come *"riutilizzare la tecnologia in modi sorprendenti"*.

- L'hacking in ambito sicurezza è un'attività quotidiana per ruoli difensivi e offensivi.
- L'enfasi è sull'utilizzo delle competenze di hacking per **scopi etici**, come il penetration testing.
- Un **ethical hacker** non agisce mai di propria iniziativa, ma in accordo con il cliente.

2. Metodologia del Penetration Test

- Il corso delinea una **metodologia standard** di penetration testing che consiste nelle seguenti **7** fasi:
 - (a) **Information gathering** (Raccolta di informazioni),
 - (b) **Network scanning** (Scansione della rete),
 - (c) **Enumeration** (Enumerazione),
 - (d) **Vulnerability assessment** (Valutazione delle vulnerabilità),
 - (e) **Exploitation** (Sfruttamento),
 - (f) **Post exploitation** (Post-sfruttamento),
 - (g) **Final report** (Rapporto finale).
- Il materiale sottolinea che il processo può essere adattato a seconda delle specifiche esigenze.

3. Fondamenti di Networking

- La comprensione dei concetti di rete è **fondamentale** per l'ethical hacking e la sicurezza informatica.
- Il **modello ISO-OSI** è centrale per comprendere come le reti operano. Il modello ISO-OSI è composto dai seguenti **7** livelli:
 - (a) **Application Layer**: protocolli di alto livello interagiscono tra loro a questo livello. Alcuni di questi protocolli includono (ma non sono limitati a) HTTP, HTTPS e FTP,
 - (b) **Presentation Layer**,
 - (c) **Session Layer**,
 - (d) **Transport Layer**: è qui che vengono effettivamente gestiti gli scambi di dati. In questo livello discutiamo i due noti protocolli TCP e UDP,

- (e) **Network Layer:** questo livello si concentra sulla comunicazione tra diverse reti. In questo caso, utilizzeremo principalmente il protocollo Internet (IP),
- (f) **Data Link Layer:** questo livello ha a che fare con le reti locali (LAN), in una LAN è necessario fare riferimento all'indirizzo MAC di un determinato dispositivo.,
- (g) **Physical Layer:** questo livello include tutto ciò che è correlato al trasferimento di dati all'interno di uno specifico mezzo di comunicazione (rame, fibra ottica o onde radio)..

Il **Session layer** e **Presentation layer** non sono molto rilevanti
hai fine del corso.

- Componenti chiave della rete:
 - **Indirizzi MAC:** identificano univocamente i dispositivi in una LAN.
 - **Indirizzi IP:** identificano i dispositivi su una rete e sono usati per la comunicazione su reti IP; possono essere privati o pubblici.
 - **ARP (Address Resolution Protocol):** si occupa del collegamento tra l'indirizzo **MAC** e l'indirizzo **IP** tramite la *ARP Table*, questo è un protocollo **cross-layer** (data link + network).
 - **NAT (Network Address Translation):** traduce gli indirizzi IP **privati** in indirizzi IP **pubblici** per l'accesso a Internet.
 - **DNS:** traduce i nomi di dominio in indirizzi IP.
 - **DHCP:** assegna automaticamente gli indirizzi IP.
 - **Porte e Servizi:** usate per stabilire connessioni con l'esterno e sono collegate ai servizi eseguiti su porte specifiche.
- Dispositivi di rete:
 - **Switch:** operano all'interno di subnet usando indirizzi MAC.
 - **Router:** inoltrano pacchetti tra reti diverse usando indirizzi IP.
 - **Firewall:** proteggono la rete applicando policy di sicurezza.
- Strumenti di analisi di rete:

- **Wireshark**: analizza il traffico di rete catturando pacchetti.
- **ARP, PING, Traceroute**: identificano problemi di connettività.

4. Fasi del Penetration Testing in Dettaglio

(a) Raccolta di Informazioni:

- Raccogliere più informazioni possibili sull'obiettivo, dal business agli strumenti utilizzati.
- Tecniche:
 - **Google Dorking**: Utilizzo di operatori di ricerca specifici per trovare informazioni sensibili.
 - **Wayback Machine**: Per trovare dati storici.
 - **Analisi dei social media**: Per individuare perdite di informazioni.
 - **Estrazione di metadati**: Dai file.
 - **Query WHOIS**: Per informazioni sui domini.
 - **Query DNS**: Per la mappatura della rete.
 - **Maltego e Recon-ng**: Strumenti per automatizzare la raccolta dati.
 - **Shodan**: Per l'analisi delle vulnerabilità.

(b) Scansione della Rete:

- Identificare host attivi e porte aperte.
- Tipi di scansione:
 - **ARP Scanning**: per scoprire dispositivi nella LAN.
 - **ICMP/Ping Scanning**: per scoprire host e servizi attivi.
 - **TCP Scanning**: include TCP Connect e SYN scans.
 - **UDP Scanning**: identifica porte e servizi UDP aperti.
- Strumento: **Nmap**.

(c) Banner Grabbing:

- Determinare il servizio e la versione in esecuzione su una porta specifica.
- Metodi: **Telnet, Netcat, Nmap**.

- Esempio HTTP: Utilizzo di comandi GET via Telnet.
- Nmap Service Probes utilizza espressioni regolari per identificare servizi.

(d) **Enumerazione:**

- Sfruttare le caratteristiche dei servizi per raccogliere informazioni.
- Servizi comuni:
 - **SMTP**,
 - **DNS**,
 - **NETBIOS**.
- Strumenti:
 - **script Nmap**,
 - **moduli Metasploit**.

(e) **Valutazione delle Vulnerabilità:**

- Identificare e analizzare le debolezze della sicurezza.
- Metodi:
 - scanner automatici,
 - database di vulnerabilità,
 - conoscenza del dominio.
- Strumenti:
 - **Nessus**,
 - **Nexpose**,
 - **OpenVAS**,
 - **OWASP ZAP**.
- Tipi di vulnerabilità':
 - **Cross-Site Scripting (XSS)**: sfrutta l'input dell'utente per iniettare script malevoli.
 - **SQL Injection (SQLi)**: sfrutta le vulnerabilità nelle query del database per accedere o modificare i dati.

(f) **Sfruttamento:**

- Strategie di attacco, movimenti laterali e shell remote.
- Strumenti:

- **Netcat**,
- **Metasploit**,
- **BeEF**.
- Tecniche:
 - Shell binding,
 - reverse shell,
 - sfruttamento lato client.
- (g) **Post-Sfruttamento:**
 - Ottenere persistenza, aumentare i privilegi e mappare la rete interna.
 - Metodi:
 - creazione di servizi,
 - modifica del registro di Windows,
 - cracking degli hash delle password.
 - Strumenti:
 - **moduli Metasploit**,
 - **John The Ripper**.
- (h) **Rapporto Finale:**
 - Presentare risultati, metodologie e piani di correzione.
 - Deve includere:
 - **sintesi**,
 - **metodologia**,
 - **risultati**,
 - **piano di correzione**.

4 Strumenti Chiave

- **Nmap**: scansione e enumerazione della rete.
- **Wireshark**: analisi del traffico di rete.
- **Netcat**: banner grabbing, shell binding e comunicazione di rete.

- **Virtualbox, QEMU, Docker:** creazione e gestione di ambienti virtuali.
- **Metasploit:** framework per exploitation e post-exploitation.
- **OpenVAS:** scansione automatica delle vulnerabilità'.
- **John The Ripper:** cracking degli hash delle password.

5 Considerazioni sulla Valutazione delle Vulnerabilità

- Le vulnerabilità possono essere identificate automaticamente, manualmente tramite database o tramite conoscenza del dominio.
- Gli scanner automatici possono tralasciare vulnerabilità dipendenti dall'applicazione, come XSS memorizzato.
- **Cross-Site Scripting (XSS):** sfrutta l'input dell'utente per iniettare script dannosi.
- **SQL Injection (SQLi):** sfrutta le vulnerabilità nelle query del database per accedere o modificare i dati. Tecniche Blind SQLi possono estrarre informazioni senza output diretto.

6 Conclusione

Il materiale del corso fornisce una panoramica completa del penetration testing, dai concetti di rete alle tecniche di exploitation. Sottolinea l'esperienza pratica e un approccio strutturato all'apprendimento.