UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Magistrale in Informatica

CORSO DI PENETRATION TESTING
AND ETHICAL HACKING

Toppo: 1:
Penetration Testing Report

STUDENTE

Eduardo Scarpa

Matricola: 0522501596

DOCENTE

Prof. **Arcangelo Castiglione**

Università degli studi di Salerno

Anno Accademico 2023-2024

Indice

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Al fine di realizzare il progetto del corso *Penetration Testing and Ethical Hacking* sono state svolte delle attività di Penetration Testing su una macchina virtuale vulnerabile chiamata **Toppo: 1**. — `https://www.vulnhub.com/entry/toppo-1,245/`

Il fine ultimo di tutte le attività svolte è stato semplicemente didattico, con lo scopo di acquisire al meglio tutte le conoscenze fornite durante lo svolgimento del corso. Per l'esecuzione di tutte le attività è stata adottata una strategia di analisi *Black-Box*, quindi senza avere nessuna conoscenza pregressa sull'asset, e sono state realizzate all'interno di un'ambiente simulato con una connessione diretta con l'asset.

Durante le varie attività svolte sono state riscontrate diverse vulnerabilità che possono portare un malintenzionato ad ottenere documenti o file a cui non dovrebbe avere accesso e, nel caso peggiore, alla compromissione totale del sistema.

1.2 Engagement Highlights

Dal momento che il processo di Penetration Testing è stato svolto in un contesto puramente didattico, non è stato necessario definire particolari regole di ingaggio.

1.3 Vulnerability Report

Durante il processo di Penetration Testing, sono state identificate varie vulnerabilità nel sistema target. Di seguito è riportato un elenco delle principali vulnerabilità trovate, classificate in base alla loro gravità:

- **[Severity: Media] Vulnerabilità in versioni obsolete di JQuery**: La presenza di JQuery 1.2 < 3.5.0 espone il sistema a vulnerabilità di tipo Multiple XSS (Cross-Site Scripting), che possono permettere a un attaccante di eseguire script malevoli all'interno del browser degli utenti;
- **[Severity: Media] SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)**: Questa vulnerabilità consente potenziali attacchi alla sicurezza della connessione SSH, riducendo l'integrità dei dati trasmessi;
- **[Severity: Media] OpenSSH User Enumeration Weakness (CVE-2018-15473)**: Questa vulnerabilità permette a un attaccante remoto di verificare l'esistenza di nomi utente validi su un server OpenSSH, differenziando le risposte del server in caso di autenticazione fallita, facilitando potenziali attacchi di brute-force o ingegneria sociale.;
- **[Severity: Low] ICMP Timestamp Request Remote Date Disclosure**: La vulnerabilità può esporre informazioni sulla data e l'ora di un sistema remoto, fornendo potenzialmente indizi utili a un attaccante per scopi di ricognizione.

Altre vulnerabilità meno gravi ma informative includono:

- **Mancanza di protezione X-Frame-Options**: Rende il sito vulnerabile a Clickjacking;
- **Mancanza dell'header X-Content-Type-Options**: Potrebbe portare a attacchi di MIME Confusion;
- **Directory Browsing abilitato**: Potenziale esposizione di file riservati o directory sensibili;
- **Assenza di token Anti-CSRF**: Apre la porta ad attacchi di **Cross-Site Request Forgery**.

1.4 Remediation Report

Durante il processo eseguito, sono state trovate molte vulnerabilità tra cui alcune abbastanza importanti che potrebbero comportare la compromissione completa del sistema e di file e documenti all'interno, nonchè la compromissione dei dati dei visitatori del sito web. Per questa ragione, si forniscono i seguenti consigli per migliorare la sicurezza dell'asset:

- **Aggiornamento di JQuery alla versione più recente**: Utilizzare una versione aggiornata di JQuery superiore alla 3.5.0 per mitigare il rischio di attacchi **Cross-Site Scripting (XSS)**. Le versioni obsolete espongono il sistema a vulnerabilità critiche.
  Azione: Scaricare e implementare l'ultima versione da un CDN affidabile o dai repository ufficiali.

- **Correzione della vulnerabilità SSH Terrapin**: Aggiornare il server SSH per correggere la vulnerabilità di **Prefix Truncation** che può compromettere l'integrità delle comunicazioni.
  Azione: Implementare patch e aggiornamenti di sicurezza che risolvano il problema, disponibili dai fornitori del software SSH.

- **Implementazione di Anti-clickjacking**: Configurare l'header HTTP **X-Frame-Options** per prevenire attacchi di **clickjacking**, limitando il rendering del contenuto del sito solo al dominio del sito stesso.
  Azione: Aggiungere l'header `X-Frame-Options: DENY` o `X-Frame-Options: SAMEORIGIN` nei file di configurazione del server.

- **Impostazione dell'header X-Content-Type-Options**: Aggiungere l'header **X-Content-Type-Options** con il valore **nosniff** per impedire attacchi basati su MIME type confusion, che potrebbero indurre il browser a interpretare i file come tipi di contenuto diversi da quelli dichiarati.
  Azione: Modificare la configurazione del server web per includere `X-Content-Type-Options: nosniff`.

- **Disabilitazione del Directory Browsing**: Il **Directory Browsing** espone i file e le directory del server, permettendo a un attaccante di accedere a informazioni sensibili.
  Azione: Disabilitare l'accesso alle directory non necessarie nella configurazione del server web, inserendo `Options -Indexes` nei file di configurazione di Apache o l'equivalente per altri server web.

- **Aggiornamento delle librerie vulnerabili**: Sostituire o aggiornare le librerie JavaScript vulnerabili presenti sul sito web.
  Azione: Eseguire una scansione completa delle dipendenze del progetto e assicurarsi che tutte le librerie siano aggiornate.

- **Protezione contro gli attacchi Cross-Site Request Forgery (CSRF)**: Implementare token **Anti-CSRF** nelle richieste per proteggere gli utenti autenticati dagli attacchi che eseguono azioni indesiderate senza il loro consenso.
  Azione: Utilizzare framework o middleware che offrono protezione CSRF automatica, oppure implementare manualmente un sistema di token.

- **Rimozione di informazioni di debug o commenti non necessari**: Eliminare **commenti sospetti** o informazioni di debug dalle pagine web che possono fornire dettagli utili agli attaccanti.
  Azione: Eseguire una revisione del codice sorgente e rimuovere commenti o informazioni riservate lasciate per errore.

- **Limitare le informazioni di versione esposte**: Evitare che il server web esponda la versione del software, in quanto queste informazioni possono facilitare gli attacchi mirati.
  Azione: Configurare il server per non includere dettagli sulla versione nei response headers (es. tramite la direttiva `ServerTokens Prod` per Apache).

1.5 Findings Summary

Le vulnerabilità identificate durante il penetration testing sono state classificate in base al loro potenziale impatto sul sistema. Di seguito viene presentata la classificazione per gravità delle vulnerabilità:

- **Alta**: vulnerabilità che richiedono determinati requisiti per poter essere sfruttate e hanno un impatto grave sul sistema. ($\mathbf{CVSS^3} \geq \mathbf{7.5}$)

- **Media**: vulnerabilità non semplici da sfruttare e che hanno un impatto relativamente grave sul sistema. ($6.5 \leq \mathbf{CVSS^3} < 7.5$)

- **Bassa**: vulnerabilità che hanno un impatto poco significativo e che hanno una bassa probabilità di essere sfruttate e, pertanto, non rappresentano, nell'immediato, una minaccia rilevante per il sistema. ($4.5 \leq \mathbf{CVSS^3} < 6.5$)

- **Informativa**: non sono vulnerabilità, ma informazioni su configurazioni di software che nel futuro potrebbero generare delle vulnerabilità. (**CVSS^3 < 4**)

La tabella seguente mostra il numero di vulnerabilità individuate per ciascuna categoria relative all'unico host individuato, ovvero la macchina **Toppo**:

Host	Indirizzo IP	Alta	Media	Bassa	Informativa
TOPPO: 1	10.0.2.5	0	8	3	33

Tabella 1.1: Classificazione delle vulnerabilità

Di seguito sono mostrati un grafico a torta per avere una visione più dettagliata sulla distribuzione delle vulnerabilità presenti e un ortogramma per visualizzarne il conteggio.

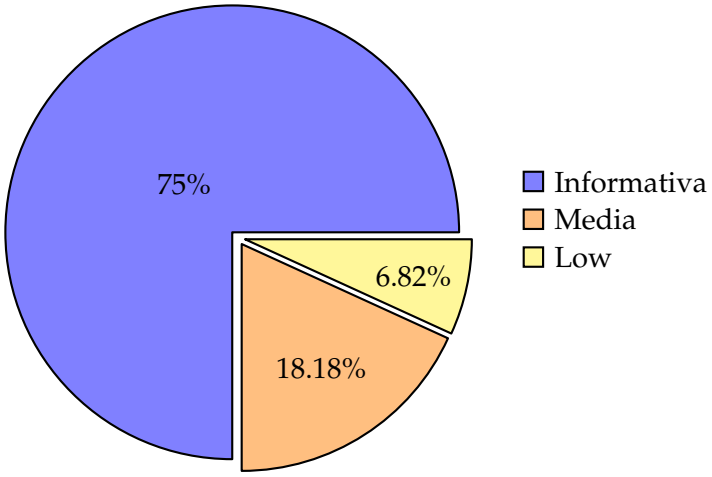

Figura 1.1: Grafico a torta delle vulnerabilità riscontrate

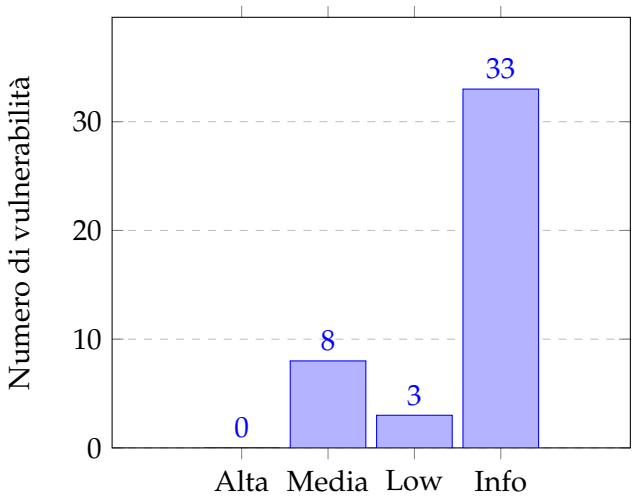

Figura 1.2: Istogramma delle vulnerabilità riscontrate

1.6 Detailed Summary

In questa sezione verranno elencate e descritte tutte le vulnerabilità riscontrate dai vari tool utilizzati.

Titolo:	JQuery 1.2 < 3.5.0 Multiple XSS	**CVE**
	MEDIA	**2020-11022/11023**
Descrizione:		
La versione di JQuery ospitata sul server web remoto è vulnerabile a molteplici vulnerabilità di cross-site scripting (XSS).		
Impatto:		
Un utente malintenzionato può sfruttare tali vulnerabilità per eseguire script dannosi nel contesto di sicurezza del browser della vittima.		
Soluzione:		
Aggiornare JQuery alla versione 3.5.0 o successiva.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	SSH Terrapin Prefix Truncation Weakness	**CVE**
	MEDIA	**2023-48795**
Descrizione:		
Il server SSH remoto è vulnerabile a un attacco di troncazione del prefisso man-in-the-middle, che può consentire a un attaccante di bypassare i controlli di integrità e degradare la sicurezza della connessione.		
Impatto:		
Un utente malintenzionato può sfruttare tale vulnerabilità per intercettare o modificare il contenuto della connessione SSH.		
Soluzione:		
Aggiornare il server SSH e configurare protocolli di sicurezza più robusti.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	OpenSSH User Enumeration Weakness	**CVE**
	MEDIA	**CVE-2018-15473**
Descrizione:		
Il server OpenSSH è vulnerabile a un attacco di enumerazione utenti, che consente a un attaccante remoto di scoprire se uno specifico nome utente esiste su un sistema target. Questa vulnerabilità sfrutta la risposta differente che il server fornisce in caso di tentativi di autenticazione con nomi utente corretti o errati. Ciò può agevolare ulteriori attacchi, come tentativi di brute-force o tecniche di social engineering.		
Impatto:		
Un utente malintenzionato può sfruttare tale vulnerabilità per determinare quali utenti sono presenti sul sistema remoto. Questo facilita la creazione di liste di nomi utenti validi per futuri attacchi mirati di brute-force o attacchi basati sull'ingegneria sociale.		
Soluzione:		
Aggiornare il server OpenSSH alla versione più recente, che include patch per prevenire la user enumeration. Inoltre, configurare OpenSSH in modo da rendere uniforme la risposta del server, indipendentemente dalla correttezza dei nomi utente.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Missing Anti-clickjacking Header	**CVE**
	MEDIA	**-**
Descrizione:		
L'host remoto ha una o più condivisioni Windows a cui è possibile accedere tramite la rete con le credenziali fornite. A seconda dei diritti di condivisione, potrebbe consentire a un aggressore di leggere/scrivere dati riservati.		
Impatto:		
Gli utenti potrebbero essere ingannati nel cliccare su elementi nascosti che eseguono azioni dannose a loro insaputa. Questo può portare a compromissioni di sicurezza significative, come la divulgazione di informazioni sensibili o l'esecuzione di azioni non autorizzate.		
Soluzione:		
I browser Web moderni supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurati che una di queste sia impostata su tutte le pagine Web restituite dal tuo sito/app. Se ti aspetti che la pagina venga inserita in un frame solo da pagine sul tuo server (ad esempio, fa parte di un FRAMESET), allora vorrai usare SAMEORIGIN, altrimenti se non ti aspetti mai che la pagina venga inserita in un frame, dovresti usare DENY. In alternativa, considera di implementare la direttiva "frame-ancestors" della Content Security Policy.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP e Nikto.		

Titolo:	Content Security Policy (CSP) Header Not Set	**CVE**
	MEDIA	**2018-5164**
Descrizione:		
L'intestazione HTTP Content Security Policy (CSP) non è configurata. CSP è una difesa efficace contro vari tipi di attacchi come XSS (Cross-Site Scripting).		
Impatto:		
L'assenza di CSP permette l'iniezione di script dannosi nel contesto dell'utente, aumentando il rischio di attacchi XSS e di altre minacce alla sicurezza.		
Soluzione:		
Configurare l'intestazione CSP per limitare le fonti di contenuti approvati, riducendo significativamente la superficie di attacco.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP e Nikto.		

Titolo:	Assenza di token anti-CSRF	**CVE**
	MEDIA	**2017-14092**
Descrizione:		
L'applicazione web non implementa token Anti-CSRF (Cross-Site Request Forgery). Questo potrebbe permettere a un attaccante di inviare richieste non autorizzate come se fossero inviate da un utente legittimo.		
Impatto:		
Gli attaccanti potrebbero sfruttare questa vulnerabilità per eseguire azioni indesiderate a nome degli utenti autenticati, compromettendo l'integrità dei dati e la sicurezza dell'utente.		
Soluzione:		
Implementare token Anti-CSRF per tutte le operazioni critiche che modificano lo stato dell'applicazione o dei dati.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Directory Browsing	**CVE**
	MEDIA	**-**
Descrizione:		
È possibile visualizzare l'elenco delle directory. L'elenco delle directory può rivelare script nascosti, includere file, file di origine del backup, ecc. a cui è possibile accedere per leggere informazioni sensibili.		
Impatto:		
Gli attaccanti potrebbero raccogliere informazioni su file e directory, facilitando ulteriori attacchi contro il sistema.		
Soluzione:		
Disabilitare la navigazione delle directory nel file di configurazione del server web.		
Metodo di detection:		
-		

Titolo:	Application Error Disclosure	**CVE**
	MEDIA	**-**
Descrizione:		
L'applicazione web rivela dettagli sugli errori interni tramite messaggi di errore visualizzati all'utente. Questi messaggi possono contenere informazioni sensibili come percorsi del filesystem, query SQL o dettagli del server.		
Impatto:		
Un utente malintenzionato potrebbe sfruttare queste informazioni per ottenere una comprensione più profonda della struttura dell'applicazione e condurre attacchi mirati, come SQL injection o traversal path attacks.		
Soluzione:		
Configurare l'applicazione per non mostrare dettagli sugli errori agli utenti finali. Implementare un messaggio di errore generico per gli utenti e registrare i dettagli tecnici degli errori in un sistema di log sicuro.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Vulnerable JS Library	**CVE**
	MEDIA	**2020-11023/11022/829**
Descrizione:		
Il sito utilizza una libreria JavaScript vulnerabile che può permettere l'esecuzione di codice malevolo o l'esposizione di informazioni sensibili.		
Impatto:		
Un utente malintenzionato potrebbe sfruttare queste vulnerabilità per eseguire codice dannoso nel contesto del browser della vittima, compromettere la sicurezza delle sessioni o accedere a dati sensibili.		
Soluzione:		
Aggiornare tutte le librerie JavaScript vulnerabili alla versione più recente disponibile e garantire che siano regolarmente mantenute e aggiornate.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	ICMP Timestamp Request Remote Date Disclosure	**CVE/CVE**
	BASSA	**-**
Descrizione:		
La macchina target ha risposto ad una richiesta ICMP di timestamp. Tale informazione potrebbe essere sfruttata per violare servizi presenti sulla macchina target.		
Impatto:		
Un utente malintenzionato potrebbe utilizzare le informazioni di timestamp per condurre attacchi basati sul tempo.		
Soluzione:		
Disabilitare le risposte ICMP Timestamp sul sistema.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	X-Content-Type-Options Header Missing	**CVE**
	BASSA	**CVE-2019-19089**
Descrizione:		
L'intestazione Anti-MIME-Sniffing X-Content-Type-Options non è impostata su 'nosniff', permettendo a versioni più vecchie di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta.		
Impatto:		
Questo può permettere attacchi basati sull'interpretazione errata del tipo di contenuto.		
Soluzione:		
Configurare l'intestazione X-Content-Type-Options su 'nosniff' nelle risposte HTTP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Server Leaks Version Information via "Server" HTTP Response Header Field	**CVE**
	BASSA	**-**
Descrizione:		
Il server Web/applicazione perde informazioni sulla versione tramite l'intestazione della risposta HTTP "Server". L'accesso a tali informazioni può facilitare agli aggressori l'identificazione di altre vulnerabilità a cui è soggetto il server web/applicazione.		
Impatto:		
La divulgazione delle informazioni sulla versione del server può facilitare la fase di ricognizione di un attaccante, permettendogli di mirare a vulnerabilità note associate alla versione specifica del server web.		
Soluzione:		
Configurare il server web per non rivelare informazioni sulla versione nel campo dell'intestazione di risposta "Server". Questa pratica può essere realizzata tramite la configurazione del server web o l'uso di moduli di sicurezza.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Apache Banner Linux Distribution Disclosure	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Il banner di Apache su questo sistema Linux rivela la distribuzione in uso. Questa informazione può essere utilizzata da un attaccante per identificare potenziali vulnerabilità specifiche della distribuzione.		
Impatto:		
La divulgazione della distribuzione Linux può facilitare la fase di ricognizione per un attaccante, permettendogli di mirare a vulnerabilità specifiche della distribuzione.		
Soluzione:		
Configurare il server web per non rivelare informazioni sulla distribuzione nel banner di Apache.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Apache HTTP Server Version	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Il server Apache HTTP su questo sistema rivela la versione in uso. Questa informazione può essere utilizzata da un attaccante per identificare potenziali vulnerabilità specifiche della versione.		
Impatto:		
La divulgazione della versione del server Apache HTTP può facilitare la fase di ricognizione per un attaccante, permettendogli di mirare a vulnerabilità specifiche della versione.		
Soluzione:		
Configurare il server web per non rivelare informazioni sulla versione di Apache HTTP nel banner.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Backported Security Patch Detection (WWW)	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Il sistema ha rilevato patch di sicurezza backportate per il server web. Queste patch possono includere correzioni di sicurezza senza modificare il numero di versione del software.		
Impatto:		
Le patch di sicurezza backportate possono aiutare a mantenere la sicurezza del sistema senza dover eseguire aggiornamenti completi del software. Tuttavia, la mancata visibilità delle versioni corrette potrebbe confondere i controlli di sicurezza automatizzati.		
Soluzione:		
Verificare regolarmente la disponibilità di patch di sicurezza e applicarle tempestivamente per garantire la protezione contro le vulnerabilità note.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Common Platform Enumeration (CPE)	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin rileva e segnala le informazioni CPE (Common Platform Enumeration) associate ai software e ai sistemi rilevati durante la scansione.		
Impatto:		
L'utilizzo di CPE consente una gestione più precisa delle risorse IT e delle vulnerabilità associate.		
Soluzione:		
Utilizzare le informazioni CPE per valutare e gestire le vulnerabilità presenti nel sistema, assicurandosi che tutte le patch rilevanti siano applicate.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Device Type	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin rileva il tipo di dispositivo (ad esempio, router, switch, server, ecc.) basato sulle informazioni raccolte durante la scansione.		
Impatto:		
La conoscenza del tipo di dispositivo può aiutare a pianificare attacchi mirati o a gestire meglio le risorse di rete.		
Soluzione:		
Utilizzare le informazioni sul tipo di dispositivo per migliorare la gestione della sicurezza e assicurarsi che tutti i dispositivi siano configurati e protetti correttamente.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Ethernet Card Manufacturer Detection	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin rileva il produttore delle schede di rete Ethernet presenti su un host remoto.		
Impatto:		
Le informazioni sul produttore delle schede di rete possono essere utilizzate per identificare potenziali vulnerabilità specifiche del hardware di rete.		
Soluzione:		
Assicurarsi che i driver e il firmware delle schede di rete siano aggiornati con le ultime patch di sicurezza.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Ethernet MAC Addresses	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin rileva gli indirizzi MAC delle schede di rete presenti su un host remoto.		
Impatto:		
Le informazioni sugli indirizzi MAC possono essere utilizzate per identificare e monitorare dispositivi specifici sulla rete.		
Soluzione:		
Utilizzare le informazioni sugli indirizzi MAC per gestire e monitorare la rete in modo efficace, applicando politiche di sicurezza appropriate.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	HTTP Server Type and Version	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin rileva il tipo e la versione del server HTTP in uso su un host remoto.		
Impatto:		
La conoscenza del tipo e della versione del server HTTP può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note.		
Soluzione:		
Assicurarsi che il server HTTP sia aggiornato con le ultime patch di sicurezza e configurato secondo le migliori pratiche di sicurezza.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	HyperText Transfer Protocol (HTTP) Information	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin raccoglie informazioni sui server HTTP rilevati, inclusi header, cookie e altri dettagli di configurazione.		
Impatto:		
Le informazioni raccolte possono essere utilizzate per identificare potenziali vulnerabilità e migliorare la configurazione di sicurezza del server HTTP.		
Soluzione:		
Utilizzare le informazioni raccolte per configurare il server HTTP in modo sicuro e applicare le patch di sicurezza necessarie.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	JQuery Detection	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin rileva l'uso della libreria JavaScript JQuery su un host remoto. Queste informazioni possono essere utilizzate per identificare potenziali vulnerabilità nella versione di JQuery in uso.		
Impatto:		
La conoscenza dell'uso di JQuery può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note della libreria.		
Soluzione:		
Assicurarsi di utilizzare l'ultima versione stabile di JQuery e mantenere aggiornate le librerie per mitigare i rischi di sicurezza.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Nessus SYN scanner	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin è uno scanner di porte "half-open" SYN. È relativamente veloce anche contro target con firewall. Le scansioni SYN sono meno intrusive rispetto alle scansioni TCP complete, ma possono causare problemi a firewall meno robusti e lasciare connessioni non chiuse sul target remoto se la rete è molto trafficata.		
Impatto:		
La scansione SYN può essere utilizzata per identificare i servizi in esecuzione su un host remoto, che può essere utile per pianificare ulteriori verifiche di sicurezza o attacchi mirati.		
Soluzione:		
Proteggere il target con un filtro IP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Nessus Scan Information	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin raccoglie informazioni dettagliate sulla scansione effettuata con Nessus, inclusi dettagli sugli host scansionati, i plugin utilizzati e i risultati della scansione.		
Impatto:		
Le informazioni sulla scansione possono essere utilizzate per analizzare la sicurezza di un sistema e pianificare miglioramenti basati sui risultati ottenuti.		
Soluzione:		
Utilizzare le informazioni raccolte per migliorare la configurazione di sicurezza del sistema e risolvere le vulnerabilità identificate.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	OS Identification	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin identifica il sistema operativo in uso su un host remoto. Queste informazioni possono essere utilizzate per determinare potenziali vulnerabilità specifiche del sistema operativo identificato.		
Impatto:		
La conoscenza del sistema operativo può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note associate a quel sistema operativo.		
Soluzione:		
Assicurarsi che il sistema operativo sia aggiornato con le ultime patch di sicurezza e configurato secondo le migliori pratiche di sicurezza.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Patch Report	**CVE**
	INFORMATIVA	**-**
Descrizione:		
Questo plugin genera un report sulle patch di sicurezza applicate e mancanti su un host remoto. Questo report può essere utilizzato per valutare la conformità del sistema alle politiche di sicurezza.		
Impatto:		
Un report sulle patch può aiutare a identificare le aree del sistema che richiedono aggiornamenti di sicurezza e a pianificare azioni malevoli.		
Soluzione:		
Installare le patch mancanti.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

CAPITOLO 2

Appendix

Una dimostrazione di come è stata sfruttata le vulnerabilita è documentata nel documento ScarpaEduardo_Metodologia, disponible anche al link:

`https://github.com/eduardoscarpa/Penetration_Testing-Toppo-1`

Figura 2.1: Bandiera ottenuta

Bibliografia

Siti Web consultati

- CVE-1999-0524 – https://nvd.nist.gov/vuln/detail/CVE-1999-0524
- CVE-2020-11022– https://nvd.nist.gov/vuln/detail/CVE-2020-11022
- CVE-2020-11023– https://nvd.nist.gov/vuln/detail/CVE-2020-11023
- CVE-2023-48795– https://nvd.nist.gov/vuln/detail/CVE-2023-48795
- CVE-2019-19089– https://nvd.nist.gov/vuln/detail/CVE-2019-19089
- CVE-2017-14092– https://nvd.nist.gov/vuln/detail/CVE-2017-14092
- CVE-2018-5164– https://nvd.nist.gov/vuln/detail/CVE-2018-5164