Università degli Studi di Salerno

Penetration Testing Report

CASO DI STUDIO: **MONEYBOX 1**

Luigi Vollono | Corso di PTEH | A.A. 2022/2023

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

Capitolo 1

1. Executive Summary

Per il progetto di Penetration Testing è stato scelto di effettuare un processo di penetration testing etico sulla macchina virtuale **MoneyBox: 1**, reperibile sulla piattaforma vulnhub al seguente link:

https://www.vulnhub.com/entry/moneybox-1,653/

Gli obiettivi da raggiungere sono i seguenti:

- Enumerare servizi e vulnerabilità presenti sulla macchina target;
- Prendere possesso della macchina target;
- Prendere possesso del flag *root.txt*;
- Instaurare una back-door.

L'attività di penetration testing sulla macchina target ha avuto inizio il 21/04/2023

Questa tipologia di attacco rientra nella categoria grey box testing, in quanto prima di iniziare il processo avevamo conoscenza soltanto del sistema operativo presente sulla macchina target. Non conoscevamo informazioni importanti come l'indirizzo IP e i vari servizi attivi. Durante la fase di penetration testing si seguirà anche l'ideologia di un white-hat hacker con l'obiettivo di scoprire e contrassegnare vulnerabilità del sistema che attestino la sua fragilità, il tutto fatto in modo etico. Si cercherà poi di fornire soluzioni da adoperare per mitigare i problemi di sicurezza riscontrati.

In questo report verranno illustrate tutte le vulnerabilità che sono state individuate durante il processo di penetration testing.

Capitolo 2

2. Engagement Highlights

L'attività di penetration testing che verrà eseguita ha un fine didattico, pertanto, non è stata fatta nessuna contrattazione con un cliente. Saranno utilizzati i tool che possono risultare più efficienti nella ricerca delle informazioni e nell'esecuzione dei task, senza che questi comportino particolari limitazioni.

L'intero progetto ha seguito le fasi che sono state insegnate durante l'intero corso:

1. Information Gathering & Target Discovery;
2. Enumeration Target & Port Scanning;
3. Vulnerability Mapping;
4. Target Exploitation;
5. Post-Exploitation (privilege escalation);
6. Post-Exploitation (maintaining access).

Nella prima fase è stato utilizzato come tool di riferimento ***nmap***, il cui output è stato messo a confronto con diversi altri tool come ***netdiscover*** e ***p0f***, per reperire diverse informazioni utili nelle fasi successive.

Nella seconda fase sono stati utilizzati come tool ***nmap*** e ***unicornscan*** per analizzare le porte aperte e servizi attivi sulla macchina target.

Nella terza fase è stato utilizzato il tool ***Nessun*** per rilevare automaticamente delle vulnerabilità sulla macchina target, mentre per osservare eventuali directory indicizzate è stato utilizzato il tool ***dirb***.

Nella quarta fase siamo riusciti a connetterci alla macchina target tramite il servizio ftp e, una volta ottenuto l'accesso, abbiamo scaricato una immagine sospetta dalla macchina che è stata analizzata tramite tool ***Steghide***, utilizzato per individuare informazioni nascoste all'interno di file, trovano un indizio utile per la fase successiva.

Nella quinta fase si è riuscito a svolgere il privilege escalation una volta ottenuto l'accesso anche al servizio ssh sfruttando il tool ***Hydra***, che permette di effettuare attacchi di forza bruta per scoprire la password sulla porta. In questo modo, abbiamo ottenuto i pieni privilegi sfruttando il fatto che un utente della macchina potesse eseguire il comando *perl* come utente root.

Infine, nella sesta fase si è riuscito a creare una backdoor tramite il tool ***msfvenom***, ma il tentativo di esecuzione non è riuscito siccome sulla macchina target non era presente il file *rc.local*, che avrebbe dovuto contenere una serie di script che il sistema operativo esegue all'avvio per poi aggiungere a tale file la backdoor, è stato anche provato a creare questo file ma il risultato è fallimentare.

Capitolo 3

3. Vulnerability Report

L’analisi di MoneyBox: 1 ha svelato diversi tipi di vulnerabilità, che saranno successivamente elencate. Tra le vulnerabilità più critiche riscontrate troviamo:

- Presenza di pagine web accessibili da browser che contengono suggerimenti per accedere alla macchina target.
- Presenza di una chiave segreta all’interno del codice sorgente di una pagina web accessibile tramite browser.
- Presenza di file immagine contenente il nome utente e informazione su relativa password.
- Presenza di password molto debole dell’utente, attraverso tecniche di password cracking essa viene facilmente rivelata.
- Presenza di privilegi massimi per un dato utente durante l’esecuzione di comandi Perl.
- Presenza di software obsoleti sulla macchina che espongono la macchina a molte vulnerabilità conosciute o meno e possono portare un eventuale utente a ottenere il controllo remoto della macchina.

Capitolo 4

4. Remediation Report

La macchina MoneyBox: 1 possiede un grado di rischio molto elevato, per cercare di mitigare questo fattore è possibile prendere le seguenti contromisure:

- Esegui l'upgrade ad Apache Log4j versione 2.15.0 o successiva o applicare la mitigazione del fornitore.
- Esegui l'upgrade a Spring Cloud Function versione 3.1.7 o 3.2.3 o successiva.
- Aggiornamento al modulo systeminformation alla versione 5.3.1 o successiva.
- Eliminazione dei vari suggerimenti presenti sulla macchina target.
- Sanificazione dell’immagine contenente il nome utente per accedere alla macchina.
- Cambiare la password dell’utente con una più difficile da crackare.
- Assegnare privilegi minimi all’utente della macchina per eseguire comandi Perl.
- Pianificare periodicamente un controllo della sicurezza al fine di valutare la sicurezza del sistema e la presenza di nuove vulnerabilità.
- Aggiornare continuamente i servizi utilizzati.

Capitolo 5

5. Findings Summary

Durante l'attività di penetration testing sono state individuate numerose vulnerabilità nella macchina target MoneyBox: 1. Le vulnerabilità individuate sono state suddivise in quattro classi in base alla loro gravità:

- CRITICAL: vulnerabilità che possono avere un impatto elevato e che possono consentire ad un utente malintenzionato di ottenere un controllo completo o parziale del sistema.
- HIGH: vulnerabilità che richiedono determinati requisiti per poter essere sfruttate e hanno un impatto relativamente alto sul sistema.
- MEDIUM: vulnerabilità non semplici da sfruttare e che, nella maggior parte dei casi, non hanno un impatto diretto molto significativo.
- LOW: 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.
- INFO: non sono vulnerabilità ma sono informazioni su configurazioni di software che nel futuro potrebbero generare delle vulnerabilità.

La tabella seguente mostra il numero di vulnerabilità individuate per ogni categoria:

	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOT
Vulnerabilità	9	1	0	0	37	40

Tabella 5.1: Classificazione vulnerabilità

Di seguito è mostrato anche un grafico a torta per avere una visione più dettagliata sul numero di vulnerabilità presenti:

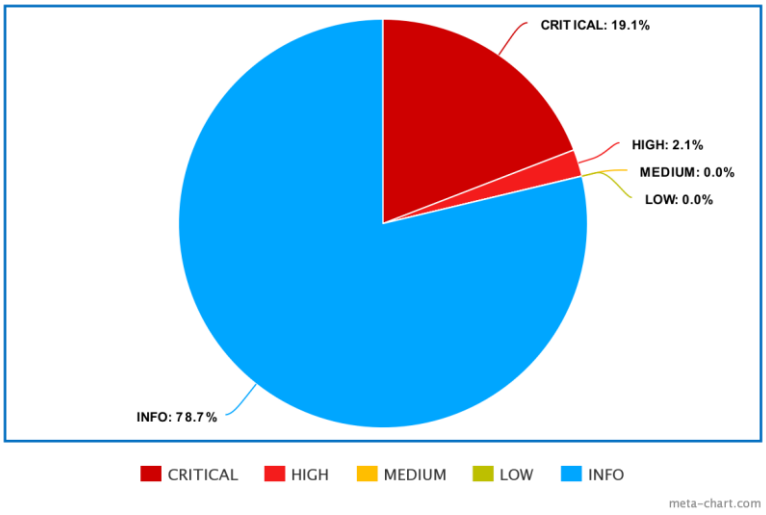

Tabella 5.2: grafico a torta delle vulnerabilità

Capitolo 6

6. Detailed Summary

In questa sezione verranno elencate e descritte tutte le vulnerabilità riscontrate utilizzando il tool Nessus.

6.1 VULNERABILITÀ CLASSIFICATE: CRITICAL

Le vulnerabilità classificate CRITICAL sono:

Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)	**CVE**
	CVE-2021-44228 [1]
Descrizione: Inviando una speciale query NetBIOS, il server potrebbe essere potenzialmente esposto alla vulnerabilità legata all'esecuzione di codice in modalità remota.	
Soluzione: Esegui l'upgrade ad Apache Log4j versione 2.15.0 o successiva o applica la mitigazione del fornitore.	

Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)	**CVE**
	CVE-2021-44228 [1]
Descrizione: Il server Web remoto è affetto da una vulnerabilità legata all'esecuzione di codice in modalità remota tramite un difetto nella libreria Apache Log4j. La vulnerabilità è dovuta all'elaborazione di input non sterilizzati inviati a una funzione di registrazione. Un utente malintenzionato in remoto e non autenticato può sfruttarlo tramite una richiesta Web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.	
Soluzione: Esegui l'upgrade ad Apache Log4j versione 2.15.0 o successiva o applica la mitigazione del fornitore.	

Spring Cloud Function SPEL Expression Injection (direct check)	**CVE**
	CVE-2022-22963[2]
Descrizione: La versione di Spring Cloud Function in esecuzione sull'host remoto è affetta da una vulnerabilità legata all'esecuzione di codice in modalità remota nella funzionalità di routing. Un utente malintenzionato in remoto e non autenticato potrebbe fornire un SpEL appositamente predisposto come routing expression che potrebbe provocare l'esecuzione di codice remoto sull'host.	
Soluzione: Esegui l'upgrade a Spring Cloud Function versione 3.1.7 o 3.2.3 o successiva.	

Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)	**CVE**
	CVE-2021-44228 [1]
Descrizione: Esiste una vulnerabilità legata all'esecuzione di codice in modalità remota in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si tratta di input controllato dall'utente. Un utente malintenzionato in remoto e non autenticato può sfruttarlo tramite una richiesta Web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione. Questo plug-in invia una stringa di test a un insieme di porte aperte sull'host di destinazione.	
Soluzione: Esegui l'upgrade ad Apache Log4j versione 2.15.0 o successiva o applica la mitigazione del fornitore.	

Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)	**CVE**
	CVE-2021-44228 [1]
Descrizione: L'host remoto sembra eseguire SSH. SSH stesso non è vulnerabile a Log4Shell; tuttavia, il server SSH potrebbe essere potenzialmente affetto da vulnerabilità se tenta di registrare i dati tramite una libreria Log4j vulnerabile.	
Soluzione: Esegui l'upgrade ad Apache Log4j versione 2.15.0 o successiva o applica la mitigazione del fornitore.	

Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)	**CVE**
	CVE-2021-44228 [1]
Descrizione: Esiste una vulnerabilità legata all'esecuzione di codice in modalità remota in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si tratta di input controllato dall'utente. Un utente malintenzionato in remoto e non autenticato può sfruttarlo tramite una richiesta Web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.	
Soluzione: Esegui l'upgrade ad Apache Log4j versione 2.15.0 o successiva o applica la mitigazione del fornitore.	

Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution	**CVE**
	CVE-2021-45046 [3]
Descrizione: Esiste una vulnerabilità legata all'esecuzione di codice in modalità remota in Apache Log4j < 2.16.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si tratta di input controllato dall'utente. Un utente malintenzionato in remoto e non autenticato può sfruttarlo tramite una richiesta Web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione. Si noti che questo bypass richiede una configurazione non predefinita. Solo i layout di pattern con una ricerca del contesto (ad esempio, $${ctx:loginId}) sono vulnerabili a questo.	
Soluzione: Esegui l'upgrade ad Apache Log4j versione 2.16.0 o successiva o applica la mitigazione del fornitore.	

6.2 VULNERABILITÀ CLASSIFICATE: HIGH

Le vulnerabilità classificate HIGH sono:

NodeJS System Information Library Command Injection	**CVE**
	CVE-2021-21315 [4]
Descrizione: L'host remoto contiene un modulo npm systeminformation affetto da una vulnerabilità di command injection. La System Information Library per Node.JS (pacchetto npm 'systeminformation') è una raccolta open source di funzioni per recuperare informazioni dettagliate su hardware, sistema e sistema operativo. Nelle informazioni di sistema precedenti alla versione 5.3.1 è presente una vulnerabilità di command injection.	
Soluzione: Aggiornamento al modulo systeminformation alla versione 5.3.1 o successiva.	

6.2 VULNERABILITÀ CLASSIFICATE: INFO

Le vulnerabilità classificate INFO sono:

HTTP Methods Allowed (per directory)	**CVE**
	-
Descrizione: Chiamando il metodo OPTIONS, è possibile determinare quali metodi HTTP sono consentiti su ciascuna directory. I seguenti metodi HTTP sono considerati non sicuri: PUT, DELETE, CONNECT, TRACE, HEAD. Molti framework e linguaggi trattano "HEAD" come una richiesta "GET", anche se senza alcun corpo nella risposta. Se un vincolo di sicurezza è stato impostato sulle richieste 'GET' in modo tale che solo 'authenticatedUsers' possa accedere alle richieste GET per un particolare servlet o risorsa, verrebbe ignorato per la versione 'HEAD'. Ciò consentiva l'invio cieco non autorizzato di qualsiasi richiesta GET privilegiata. Poiché questo elenco potrebbe essere incompleto, il plug-in testa anche - se 'Test approfonditi' sono abilitati o 'Abilita test applicazioni web' è impostato su 'sì' nel criterio di scansione - vari metodi HTTP noti su ogni directory e li considera come non supportati se riceve un codice di risposta di 400, 403, 405 o 501. Si noti che l'output del plug-in è solo informativo e non indica necessariamente la presenza di eventuali vulnerabilità di sicurezza.	

HTTP Server Type and Version	**CVE**
	-
Descrizione: Questo plug-in tenta di determinare il tipo e la versione del server Web remoto.	

HyperText Transfer Protocol (HTTP) Information	**CVE**
	-
Descrizione: Questo test fornisce alcune informazioni sul protocollo HTTP remoto: la versione utilizzata, se HTTP Keep-Alive e il pipelining HTTP sono abilitati, ecc... Questo test è solo informativo e non denota alcun problema di sicurezza.	

Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	**CVE**
	-
Descrizione: Il server Web remoto in alcune risposte imposta un'intestazione di risposta frame-ancestors Content-Security-Policy (CSP) permissiva o non ne imposta affatto. L'intestazione CSP frame-ancestors è stata proposta dal W3C Web Application Security Working Group come un modo per mitigare gli attacchi cross-site scripting e clickjacking.	
Soluzione: Impostare un'intestazione frame-ancestors Content-Security-Policy non permissiva per tutte le risorse richieste.	

Missing or Permissive X-Frame-Options HTTP Response Header	**CVE**
	-
Descrizione: Il server Web remoto in alcune risposte imposta un'intestazione di risposta X-Frame-Options permissiva o non ne imposta affatto una. L'intestazione X-Frame-Options è stata proposta da Microsoft come un modo per mitigare gli attacchi di clickjacking ed è attualmente supportata da tutti i principali fornitori di browser.	
Soluzione: Impostare un'intestazione X-Frame-Options correttamente configurata per tutte le risorse richieste.	

SSH Algorithms and Languages Supported	**CVE**
	-
Descrizione: Questo script rileva quali algoritmi e linguaggi sono supportati dal servizio remoto per la crittografia delle comunicazioni.	

SSH SHA-1 HMAC Algorithms Enabled	**CVE**
	-
Descrizione: Il server SSH remoto è configurato per abilitare gli algoritmi HMAC SHA-1. Sebbene il NIST abbia formalmente deprecato l'uso di SHA-1 per le firme digitali, SHA-1 è ancora considerato sicuro per HMAC poiché la sicurezza di HMAC non si basa sulla resistenza alla collisione della funzione hash sottostante. Si noti che questo plug-in controlla solo le opzioni del server SSH remoto.	

SSH Password Authentication Accepted	**CVE**
	-
Descrizione: Il server SSH sull'host remoto accetta l'autenticazione della password.	

SSH Server Type and Version Information	**CVE**
	-
Descrizione: È possibile ottenere informazioni sul server SSH remoto inviando una richiesta di autenticazione vuota.	

Nessus SYN scanner	**CVE**
	-
Descrizione: Questo plugin è un port scanner SYN 'semiaperto'. Sarà ragionevolmente veloce anche contro un host target protetto da firewall. Si noti che le scansioni SYN sono meno intrusive delle scansioni TCP contro servizi interrotti, ma potrebbero causare problemi per firewall meno robusti e anche lasciare connessioni non chiuse sulla destinazione remota, se la rete è carica.	
Soluzione: Proteggere l'host con un filtro IP.	

Service Detection	**CVE**
	-
Descrizione: Nessus è stato in grado di identificare il servizio remoto tramite il suo banner o guardando il messaggio di errore che invia quando riceve una richiesta HTTP.	

Apache HTTP Server Version	**CVE**
Descrizione: L'host remoto esegue Apache HTTP Server, un server Web open source. Era possibile leggere il numero di versione dal banner.	

Backported Security Patch Detection (FTP)	**CVE**
	-
Descrizione: Le patch di sicurezza potrebbero essere state trasferite al server FTP remoto senza modificarne il numero di versione. I controlli basati su banner sono stati disabilitati per evitare falsi positivi.	

Backported Security Patch Detection (WWW)	**CVE**
	-
Descrizione: Le patch di sicurezza potrebbero essere state trasferite al server HTTP remoto senza modificarne il numero di versione. I controlli basati su banner sono stati disabilitati per evitare falsi positivi.	

Common Platform Enumeration (CPE)	**CVE**
	-
Descrizione: Utilizzando le informazioni ottenute da una scansione Nessus, questo plug-in segnala le corrispondenze CPE (Common Platform Enumeration) per vari prodotti hardware e software trovati su un host.	

Deprecated SSLv2 Connection Attempts	**CVE**
	-
Descrizione: Questo plug-in enumera e segnala tutte le connessioni SSLv2 che sono state tentate come parte di una scansione. Questo protocollo è stato ritenuto proibito dal 2011 a causa di vulnerabilità di sicurezza e la maggior parte delle principali librerie ssl come openssl, nss, mbed e wolfssl non forniscono questa funzionalità nelle loro versioni più recenti. Questo protocollo è stato deprecato in Nessus 8.9 e versioni successive.	

Device Type	**CVE**
	-
Descrizione: In base al sistema operativo remoto, è possibile determinare qual è il tipo di sistema remoto (ad esempio: una stampante, un router, un computer generico, ecc.).	

Ethernet Card Manufacturer Detection	**CVE**
	-
Descrizione: Ogni indirizzo MAC Ethernet inizia con un identificatore univoco organizzativo (OUI) a 24 bit. Questi OUI sono registrati da IEEE.	

Ethernet MAC Addresses	**CVE**
	-
Descrizione: Questo plug-in raccoglie gli indirizzi MAC scoperti sia dal sondaggio remoto dell'host (ad esempio SNMP e Netbios) sia dall'esecuzione di controlli locali (ad esempio ifconfig). Quindi consolida gli indirizzi MAC in un elenco unico, univoco e uniforme.	

FTP Server Detection	**CVE**
	-
Descrizione: È possibile ottenere il banner del server FTP remoto collegandosi ad una porta remota.	

ICMP Timestamp Request Remote Date Disclosure	**CVE**
	CVE-1999-0524 [5]
Descrizione: L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina mirata, che può aiutare un utente malintenzionato in remoto e non autenticato a raggirare i protocolli di autenticazione basati sul tempo.	
Soluzione: Filtrare le richieste timestamp ICMP (13) e le risposte timestamp ICMP in uscita (14).	

IP Protocols Scan	**CVE**
	-
Descrizione: Questo plugin rileva i protocolli compresi dallo stack IP remoto.	

Nessus Scan Information	**CVE**
	-
Descrizione: Questo plugin mostra, per ogni host testato, informazioni sulla scansione stessa: - La versione del set di plugin. - Il tipo di scanner (Nessus o Nessus Home). - La versione del Nessus Engine. - Il/i port scanner utilizzato/i. - L'intervallo di porte scansionato. - Se sono possibili controlli di gestione delle patch con credenziali o di terze parti. - Se la visualizzazione delle patch sostituite è abilitata - La data della scansione e la durata della scansione. - Il numero di host analizzati in parallelo. - Il numero di controlli eseguiti in parallelo.	

OS Identification	**CVE**
	-
Descrizione: Utilizzando una combinazione di sonde remote (ad esempio, TCP/IP, SMB, HTTP, NTP, SNMP, ecc.), è possibile indovinare il nome del sistema operativo remoto in uso. A volte è anche possibile indovinare la versione del sistema operativo.	

OS Security Patch Assessment Not Available	**CVE**
	-
Descrizione: OS Security Patch Assessment non è disponibile sull'host remoto. Ciò non indica necessariamente un problema con la scansione. Le credenziali potrebbero non essere state fornite, la valutazione della patch di sicurezza del sistema operativo potrebbe non essere supportata per la destinazione, la destinazione potrebbe non essere stata identificata o potrebbe essersi verificato un altro problema che ha impedito la disponibilità della valutazione della patch di sicurezza del sistema operativo.	

Patch Report	**CVE**
	-
Descrizione: Nell'host remoto mancano una o più patch di sicurezza. Questo plugin elenca la versione più recente di ciascuna patch da installare per assicurarsi che l'host remoto sia aggiornato.	
Soluzione: Installa le patch elencate di seguito.	

SSH Protocol Versions Supported	**CVE**
	-
Descrizione: Un server SSH è in esecuzione sull'host remoto.	
Soluzione: Questo plugin determina le versioni del protocollo SSH supportate dal daemon SSH remoto.	

Target Credential Status by Authentication Protocol - No Credentials Provided	**CVE**
	-
Descrizione: Nessus non è stato in grado di eseguire correttamente l'autenticazione direttamente alla destinazione remota su un protocollo di autenticazione disponibile. Nessus è stato in grado di connettersi alla porta remota e identificare che il servizio in esecuzione sulla porta supporta un protocollo di autenticazione, ma Nessus non è riuscito ad autenticarsi al servizio remoto utilizzando le credenziali fornite. Potrebbe essersi verificato un errore del protocollo che ha impedito il tentativo di autenticazione oppure tutte le credenziali fornite per il protocollo di autenticazione potrebbero non essere valide.	

TCP/IP Timestamps Supported	**CVE**
	-
Descrizione: L'host remoto implementa i timestamp TCP, come definito da RFC1323. Un effetto collaterale di questa funzione è che a volte è possibile calcolare il tempo di attività dell'host remoto.	

Traceroute Information	**CVE**
	-
Descrizione: Crea un traceroute verso l'host remoto.	

vsftpd Detection	**CVE**
	-
Descrizione: L'host remoto esegue vsftpd, un server FTP per sistemi simili a UNIX scritto in C.	

Web Application Sitemap	**CVE**
	-
Descrizione: Il server Web remoto contiene contenuti collegabili che possono essere utilizzati per raccogliere informazioni su un obiettivo.	

Web Server Directory Enumeration	**CVE**
	-
Descrizione: Questo plug-in tenta di determinare la presenza di varie directory comuni sul server Web remoto. Inviando una richiesta per una directory, il codice di risposta del server Web indica se si tratta di una directory valida o meno.	

References

[1]. CVE-2021-44228 Detail: https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[2]. CVE-2022-22963 Detail: https://nvd.nist.gov/vuln/detail/CVE-2022-22963
[3]. CVE-2021-45046 Detail: https://nvd.nist.gov/vuln/detail/CVE-2021-45046
[4]. CVE-2021-21315 Detail: https://nvd.nist.gov/vuln/detail/CVE-2021-21315
[5]. CVE-1999-0524 Detail: https://nvd.nist.gov/vuln/detail/CVE-1999-0524