

Penetration Testing Report

CENGBOX 2

Alfredo Cannavaro

Prof. Arcangelo CASTIGLIONE
Corso di Penetration Testing

Novembre 2024

1 Executive Summary

Per il progetto di Penetration Testing è stato scelto di effettuare un processo di *penetration testing* etico sulla macchina virtuale CENGBOX 2, reperibile sulla piattaforma VulnHub al seguente link:

<https://www.vulnhub.com/entry/cengbox-2,486/>.

Questa macchina consente agli utenti di esercitarsi su attacchi di brute-force su credenziali di accesso ai servizi, come l'accesso via SSH o il login su una pagina web. Si utilizzano strumenti come Hydra per forzare le password su login HTTP o servizi SSH. Inoltre, offre l'opportunità di praticare l'*escalation dei privilegi* tentare di ottenere privilegi di root utilizzando tecniche come la modifica del file `/etc/passwd` o sfruttando binari SUID presenti sulla macchina.

Gli obiettivi da raggiungere sono i seguenti:

- Enumerare i servizi e le vulnerabilità presenti sulla macchina target;
- Ottenere l'accesso alla macchina target come *root*;
- Prendere possesso del flag `root.txt` e leggere il contenuto;

L'attività di penetration testing sulla macchina target è iniziata il 15/07/2024. Questo tipo di *testing* rientra nella categoria del *grey box testing*, poiché avevamo conoscenza del sistema operativo presente sulla macchina target, ma non avevamo informazioni cruciali come l'indirizzo IP e i servizi attivi.

Durante la fase di penetration testing, abbiamo seguito i principi etici di un *white-hat hacker*, con l'obiettivo di identificare e documentare le vulnerabilità del sistema in modo etico, fornendo soluzioni per mitigare i problemi di sicurezza rilevati.

Questo report illustrerà tutte le vulnerabilità individuate durante il processo di penetration testing. In particolare, le vulnerabilità riscontrate possono permettere a un attaccante di ottenere il pieno controllo del sistema e assumere i privilegi di amministratore. Inoltre, un attaccante potrebbe potenzialmente rubare dati sensibili degli utenti del sito web.

Attualmente, il livello di rischio complessivo associato all'asset risulta essere critico. Tuttavia, attraverso l'adozione di misure quali la rimozione dei dati sensibili dalle risorse pubbliche e l'implementazione di controlli di sicurezza, è possibile ridurre sensibilmente il livello di rischio.

2 Engagement Highlights

L'attività di penetration testing che verrà eseguita ha scopi didattici e, pertanto, non è stata stipulata alcuna contrattazione con un cliente. Saranno utilizzati gli strumenti più efficienti per la ricerca delle informazioni e l'esecuzione dei task, senza 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);

3 Strumenti utilizzati

Gli strumenti utilizzati includono:

- Netdiscover
- Nmap
- Dirb
- Gobuster
- Wfuzz
- Hydra
- Nessus
- OWASP ZAP
- Nikto
- Metasploit

- Msfvenom
- PSPY
- Openssl

4 Vulnerability Report

Durante il processo di Penetration Testing sono state identificate numerose vulnerabilità che potrebbero essere sfruttate per compromettere diversi aspetti del sistema. Di seguito riportiamo le principali vulnerabilità riscontrate.

- **[Severity: Alta] Accesso FTP anonimo senza autenticazione:** Il server FTP consente l'accesso anonimo, permettendo a utenti non autenticati di leggere file sensibili presenti nel filesystem.
- **[Severity: Alta] Credenziali deboli su interfaccia di amministrazione web:** Le credenziali predefinite non sono state modificate, consentendo attacchi di brute-force per ottenere l'accesso all'interfaccia di amministrazione.
- **[Severity: Media] Versione obsoleta di Apache HTTPD:** Il server web Apache utilizza una versione obsoleta (2.4.18), potenzialmente vulnerabile a diversi exploit noti.
- **[Severity: Media] Mancanza di X-Content-Type-Options e X-Frame-Options Header:** L'assenza di questi header espone il sito web ad attacchi di clickjacking e cross-site scripting (XSS).
- **[Severity: Media] Directory listing abilitato:** È possibile navigare tra le directory del server web tramite browser, permettendo la visualizzazione di file sensibili non protetti.
- **[Severity: Bassa] Informazioni sulla versione del server esposte:** Le risposte HTTP contengono dettagli sulla versione del server, facilitando la ricognizione da parte di attaccanti.
- **[Severity: Bassa] Dati di sessione non protetti da crittografia:** I dati di sessione trasmessi tra client e server non sono cifrati, il che potrebbe permettere l'intercettazione delle comunicazioni da parte di attaccanti.

5 Remediation Report

Per eliminare le vulnerabilità riscontrate e ridurre i rischi associati al sistema, si consiglia di seguire le azioni correttive descritte di seguito:

- **Rimozione dell'accesso anonimo al server FTP:** Configurare il server FTP in modo da richiedere sempre l'autenticazione per accedere ai file. Limitare l'accesso solo agli utenti autorizzati per evitare il rischio di esposizione di dati sensibili.
- **Modifica delle credenziali predefinite sul portale di amministrazione web:** Cambiare immediatamente le credenziali predefinite per il portale di amministrazione web e implementare politiche di password forti. Abilitare l'autenticazione a due fattori, se disponibile.
- **Aggiornamento del server Apache alla versione più recente:** Installare l'ultima versione stabile di Apache per correggere le vulnerabilità legate alla versione obsoleta 2.4.18 e garantire la sicurezza delle connessioni web.
- **Abilitazione degli header di sicurezza mancanti:** Aggiungere gli header di sicurezza `X-Content-Type-Options` e `X-Frame-Options` per prevenire attacchi di clickjacking e cross-site scripting (XSS).
- **Disabilitazione del directory listing:** Configurare il server web per disabilitare la visualizzazione delle directory tramite browser, garantendo che i file non siano accessibili pubblicamente senza autorizzazione.
- **Rimozione delle informazioni sulla versione del server dalle risposte HTTP:** Configurare il server web per nascondere l'intestazione `Server` nelle risposte HTTP, riducendo così le possibilità che un attaccante sfrutti vulnerabilità specifiche della versione.
- **Implementazione della cifratura per le sessioni e i dati trasmessi:** Configurare il server web e FTP per garantire che tutte le sessioni e i dati sensibili siano trasmessi attraverso connessioni cifrate, come HTTPS e FTPS, per prevenire attacchi di tipo man-in-the-middle.

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. ($CVSS \geq 7.5$)
- **Media:** vulnerabilità non semplici da sfruttare e che hanno un impatto relativamente grave sul sistema. ($6.5 \leq CVSS < 7.5$)
- **Bassa:** vulnerabilità che hanno un impatto poco significativo e che hanno una bassa probabilità di essere sfruttate, pertanto non rappresentano nell'immediato una minaccia rilevante per il sistema. ($4.5 \leq CVSS < 6.5$)
- **Informativa:** non sono vulnerabilità, ma informazioni su configurazioni di software che nel futuro potrebbero generare delle vulnerabilità. ($CVSS < 4$)

La tabella seguente mostra il numero di vulnerabilità individuate per ciascuna categoria relative all'host **CengBox2**:

Host	Indirizzo IP	Alta	Media	Bassa	Informativa
CengBox2	10.0.2.4	2	7	1	29

Table 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.

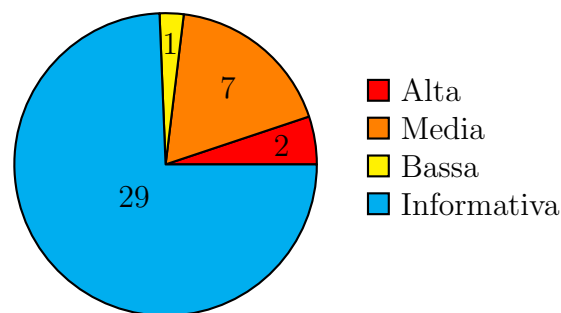


Figure 1: Aerogramma delle vulnerabilità riscontrate

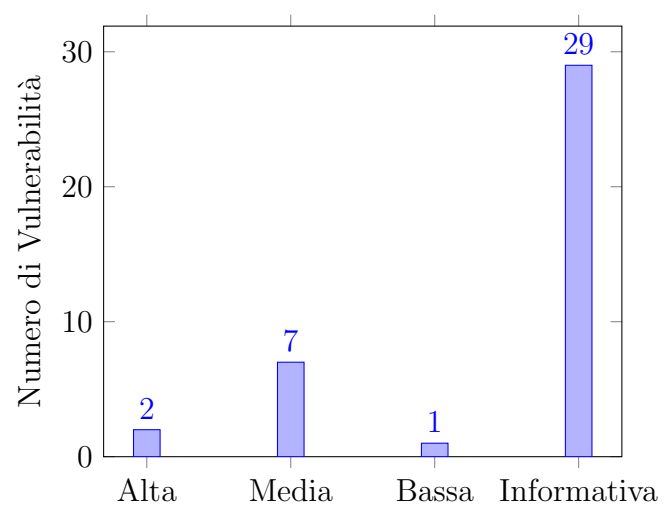


Figure 2: Ortogramma delle vulnerabilità riscontrate

Detailed Summary

Vulnerabilità	CVE	Rischio
Accesso FTP anonimo senza autenticazione	CVE-1999-0497	
ALTA		
Descrizione:	Il server FTP consente l'accesso anonimo, permettendo a utenti non autenticati di leggere file sensibili presenti nel filesystem.	
Impatto:	Questa vulnerabilità permette a un attaccante di accedere a file sensibili senza autenticazione, aumentando il rischio di esfiltrazione di dati o modifica non autorizzata.	
Soluzione:	Disabilitare l'accesso anonimo e richiedere l'autenticazione per ogni connessione al server FTP. Aggiornare le configurazioni di sicurezza del server per prevenire accessi non autorizzati.	
Metodo di detection:	Vulnerabilità individuata tramite scansione iniziale con Nmap.	

Table 2: Vulnerabilità di accesso FTP anonimo senza autenticazione

Vulnerabilità	CVE	Rischio
Modifica delle credenziali predefinite sul portale di amministrazione web	CVE-2019-1653	
ALTA		
Descrizione:	Il portale di amministrazione web utilizza credenziali predefinite che devono essere cambiate immediatamente per prevenire accessi non autorizzati. Implementare politiche di password forti e, se possibile, abilitare l'autenticazione a due fattori.	
Impatto:	Questa vulnerabilità permette a un attaccante di accedere al portale di amministrazione con credenziali predefinite, compromettendo l'intero sistema e aumentando il rischio di modifiche non autorizzate o accessi malevoli.	
Soluzione:	Cambiare immediatamente le credenziali predefinite e implementare politiche di password forti. Abilitare l'autenticazione a due fattori, se disponibile, per aumentare la sicurezza.	
Metodo di detection:	Vulnerabilità individuata tramite attacco di forza bruta con Hydra.	

Table 3: Modifica delle credenziali predefinite sul portale di amministrazione web

Vulnerabilità	CVE	Rischio
Versione obsoleta di Apache HTTPD	CVE-2017-3167	
MEDIA		
Descrizione:	Il server web Apache utilizza una versione obsoleta (2.4.18), che è potenzialmente vulnerabile a diversi exploit noti, mettendo a rischio la sicurezza del sistema.	
Impatto:	Questa vulnerabilità permette a un attaccante di sfruttare le falle conosciute nella versione obsoleta di Apache per compromettere il server web, con conseguenze sulla disponibilità, integrità e riservatezza dei dati.	
Soluzione:	Aggiornare Apache HTTPD all'ultima versione disponibile e applicare patch di sicurezza. Verificare periodicamente gli aggiornamenti per ridurre la superficie di attacco.	
Metodo di detection:	Vulnerabilità rilevata tramite scanner automatico Nessus e confermata con test manuale.	

Table 4: Versione obsoleta di Apache HTTPD

Vulnerabilità	CVE	Rischio
Mancanza di X-Content-Type-Options e X-Frame-Options Header	CVE-2015-2080	
MEDIA		
Descrizione:	L'assenza degli header di sicurezza X-Content-Type-Options e X-Frame-Options espone il sito web ad attacchi di clickjacking e cross-site scripting (XSS).	
Impatto:	Gli attacchi di clickjacking permettono agli attaccanti di sovrapporre contenuti dannosi sulle pagine del sito, mentre la mancanza di X-Content-Type-Options può portare a interpretazioni errate dei contenuti e potenziali attacchi XSS.	
Soluzione:	Abilitare l'header X-Content-Type-Options e X-Frame-Options per prevenire attacchi di XSS e clickjacking. Controllare regolarmente la configurazione della sicurezza del sito.	
Metodo di detection:	Vulnerabilità rilevata tramite OWASP ZAP e confermata tramite test manuale.	

Table 5: Mancanza di X-Content-Type-Options e X-Frame-Options Header

Vulnerabilità	CVE	Rischio
Directory Listing Abilitato	CVE-2000-0354	
MEDIA		
Descrizione:	Il server web ha il "Directory Listing" abilitato, consentendo agli utenti di navigare tra le directory del server tramite browser, esponendo potenzialmente file sensibili non protetti.	
Impatto:	Gli attaccanti potrebbero visualizzare directory e file sensibili, raccogliendo informazioni utili per compromettere il sistema o esfiltrare dati riservati.	
Soluzione:	Disabilitare il Directory Listing nel file di configurazione del server web.	
Metodo di detection:	Vulnerabilità rilevata tramite un test manuale di accesso alle directory tramite browser.	

Table 6: Directory Listing Abilitato

Vulnerabilità	CVE	Rischio
Rimozione delle informazioni sulla versione del server dalle risposte HTTP	CVE-2006-4380	
MEDIA		
Descrizione:	Il server web include l'intestazione "Server" nelle risposte HTTP, esponendo informazioni sulla versione del server che potrebbero essere sfruttate da un attaccante per identificare vulnerabilità specifiche della versione.	
Impatto:	Un attaccante potrebbe utilizzare queste informazioni per lanciare attacchi mirati sfruttando vulnerabilità conosciute della specifica versione del server web.	
Soluzione:	Configurare il server web per nascondere l'intestazione "Server" nelle risposte HTTP. In Apache, questo può essere fatto tramite la direttiva 'ServerTokens' e 'ServerSignature'.	
Metodo di detection:	La vulnerabilità è stata identificata tramite l'analisi delle risposte HTTP usando un tool di scanning automatizzato o un test manuale.	

Table 7: Rimozione delle informazioni sulla versione del server dalle risposte HTTP

Vulnerabilità	CVE	Rischio
Implementazione della cifratura per le sessioni e i dati trasmessi	CVE-2016-2183	
MEDIA		
Descrizione:	Le sessioni e i dati sensibili trasmessi dal server FTP e web non sono cifrati, esponendo potenzialmente le informazioni a intercettazioni da parte di attaccanti tramite attacchi man-in-the-middle.	
Impatto:	Un attaccante potrebbe intercettare dati sensibili o alterare le comunicazioni non cifrate, compromettendo l'integrità delle informazioni trasmesse.	
Soluzione:	Configurare il server web per utilizzare HTTPS e il server FTP per utilizzare FTPS o SFTP, garantendo la cifratura delle sessioni e dei dati trasmessi. Implementare anche certificati validi per migliorare la sicurezza.	
Metodo di detection:	La vulnerabilità è stata identificata tramite un'analisi manuale della configurazione del server e delle connessioni utilizzate per la trasmissione dei dati.	

Table 8: Implementazione della cifratura per le sessioni e i dati trasmessi

Vulnerabilità	CVE	Rischio
SSH Terrapin Prefix Truncation Weakness	CVE-2023-48795	Media
MEDIA		
Descrizione:	Una vulnerabilità nel protocollo SSH che consente a un attaccante di sfruttare le debolezze nel troncamento dei prefissi, potenzialmente portando a attacchi di negazione del servizio o interruzione della comunicazione.	
Impatto:	Può causare disconnessioni di sessioni o l'esposizione dei canali di comunicazione a possibili sfruttamenti da parte di un attaccante.	
Soluzione:	Aggiornare il server alla versione più recente di SSH che risolve questo problema o configurare metodi di comunicazione più sicuri.	
Metodo di detection:	La vulnerabilità è stata identificata tramite Nessus o strumenti simili di scansione delle vulnerabilità.	

Table 9: SSH Terrapin Prefix Truncation Weakness

Vulnerabilità	CVE	Rischio
Content Security Policy (CSP) Header Not Set	CVE-2018-12386	
MEDIO		
Descrizione:	L’header Content Security Policy (CSP) non è configurato, esponendo l’applicazione a potenziali attacchi di Cross-Site Scripting (XSS) e altri attacchi che sfruttano l’iniezione di codice.	
Impatto:	Senza un header CSP, gli attaccanti potrebbero eseguire codice dannoso nel contesto del browser della vittima, compromettendo la sicurezza dell’applicazione e dei dati degli utenti.	
Soluzione:	Configurare correttamente l’header CSP per limitare le fonti di contenuti che il browser può caricare e eseguire. Assicurarsi che le policy siano sufficientemente restrittive per mitigare rischi di XSS e iniezioni di codice.	
Metodo di detection:	La vulnerabilità è stata identificata tramite OWASP ZAP, che ha rilevato l’assenza dell’header nelle risposte HTTP.	

Table 10: Content Security Policy (CSP) Header Not Set

Vulnerabilità	CVE	Rischio
ICMP Timestamp Request Remote Date Disclosure	N/A	Basso
BASSO		
Descrizione:	Permette agli attaccanti di raccogliere informazioni sull'uptime del sistema tramite richieste ICMP timestamp, facilitando attacchi basati sul tempo.	
Impatto:	Anche se non è direttamente dannosa, queste informazioni potrebbero aiutare un attaccante a lanciare attacchi più mirati, comprendendo quando il sistema è stato riavviato per l'ultima volta.	
Soluzione:	Bloccare le richieste ICMP timestamp nella configurazione del firewall.	
Metodo di detection:	La vulnerabilità è stata identificata tramite scanner di vulnerabilità come Nessus.	

Table 11: ICMP Timestamp Request Remote Date Disclosure

Vulnerabilità	CVE	Rischio	
Apache Banner Linux Distribution Disclosure		-	
INFORMATIVA			
Descrizione:	Il server web espone informazioni relative alla distribuzione Linux e alla versione di Apache utilizzata tramite l'intestazione "Server" nelle risposte HTTP.		
Impatto:	Queste informazioni possono essere utilizzate dagli attaccanti per identificare vulnerabilità specifiche legate alla versione di Linux o di Apache, facilitando attacchi mirati.		
Soluzione:	Configurare il server per nascondere o modificare l'intestazione "Server" nelle risposte HTTP, riducendo l'esposizione di informazioni sensibili.		
Metodo di detection:	Questa vulnerabilità è stata rilevata tramite l'analisi manuale delle intestazioni HTTP e scanner di vulnerabilità come Nikto.		

Table 12: Apache Banner Linux Distribution Disclosure

Vulnerabilità	CVE	Rischio	
Apache HTTP Server Version		-	
INFORMATIVA			
Descrizione:	Il server Apache HTTP espone la versione corrente nelle intestazioni HTTP, rendendo visibile agli attaccanti la versione esatta del software in uso.		
Impatto:	La conoscenza della versione specifica di Apache utilizzata potrebbe consentire agli attaccanti di sfruttare vulnerabilità note associate a quella versione.		
Soluzione:	Configurare Apache per nascondere le informazioni di versione dalle intestazioni HTTP, oppure aggiornare regolarmente il server all'ultima versione sicura.		
Metodo di detection:	Questa vulnerabilità è stata rilevata tramite scanner di vulnerabilità come Nikto o OWASP ZAP, analizzando le intestazioni HTTP inviate dal server.		

Table 13: Apache HTTP Server Version

Vulnerabilità	CVE	Rischio	
Backported Security Patch Detection (FTP)		-	
INFORMATIVA			
Descrizione:	La vulnerabilità riguarda l'FTP server, che potrebbe avere patch di sicurezza applicate retroattivamente. Tuttavia, il software esposto potrebbe mostrare versioni vulnerabili, nonostante le patch siano presenti.		
Impatto:	Gli attaccanti potrebbero confondere la versione esposta del server FTP come vulnerabile, tentando di sfruttare vulnerabilità già corrette tramite patch di sicurezza retroattive.		
Soluzione:	Rendere più chiaro, attraverso documentazione o configurazioni, l'uso di versioni patchate retroattivamente e aggiornare le versioni esposte per evitare confusione.		
Metodo di detection:	Rilevata attraverso uno scanner di vulnerabilità come Nessus, che identifica potenziali problemi con versioni di software apparentemente obsolete.		

Table 14: Backported Security Patch Detection (FTP)

Vulnerabilità	CVE	Rischio	
Backported Security Patch Detection (SSH)	-		
INFORMATIVA			
Descrizione:	Questa vulnerabilità riguarda la rilevazione di patch di sicurezza retroattive sul server SSH. Anche se il software SSH può mostrare una versione vulnerabile, le patch di sicurezza potrebbero essere state applicate retroattivamente per correggere le falle.		
Impatto:	Gli attaccanti potrebbero tentare di sfruttare vulnerabilità note basandosi sulla versione esposta di SSH, ignorando che le patch di sicurezza sono state applicate. Questo potrebbe indurre a tentativi di sfruttamento infruttuosi.		
Soluzione:	Aggiornare la versione del software SSH visibile o documentare chiaramente le patch retroattive applicate per ridurre confusione e tentativi di sfruttamento.		
Metodo di detection:	Rilevata tramite Nessus o strumenti simili che individuano versioni apparentemente vulnerabili di SSH nonostante le patch retroattive.		

Table 15: Backported Security Patch Detection (SSH)

Vulnerabilità	CVE	Rischio	
Backported Security Patch Detection (WWW)		-	
INFORMATIVO			
Descrizione:	Questa vulnerabilità riguarda la rilevazione di patch di sicurezza retroattive applicate al server web (WWW). Anche se il software del server web può mostrare una versione vulnerabile, le patch potrebbero essere state applicate retroattivamente per mitigare i rischi.		
Impatto:	Nonostante le patch di sicurezza siano state applicate, l'esposizione della versione del server può indurre attaccanti a tentare di sfruttare vulnerabilità obsolete, sebbene tali tentativi siano destinati a fallire.		
Soluzione:	Aggiornare la versione visibile del server web per riflettere l'applicazione delle patch di sicurezza o disabilitare l'esposizione della versione del server.		
Metodo di detection:	Rilevata tramite scanner di vulnerabilità come Nessus o strumenti simili.		

Table 16: Backported Security Patch Detection (WWW)

Vulnerabilità	CVE	Rischio	
Common Platform Enumeration (CPE)		-	
INFORMATIVO			
Descrizione:	L'utilizzo del Common Platform Enumeration (CPE) permette di identificare piattaforme software e hardware con versioni specifiche, utile per la gestione degli asset e l'identificazione delle vulnerabilità correlate.		
Impatto:	Questo dato non costituisce un rischio diretto ma è utilizzato per abbinare le vulnerabilità note alle piattaforme individuate, fornendo indicazioni su potenziali problemi di sicurezza.		
Soluzione:	Assicurarsi che i sistemi siano aggiornati con le ultime patch di sicurezza per ridurre le vulnerabilità note associate alle versioni specifiche dei software o delle piattaforme hardware.		
Metodo di detection:	Rilevato tramite scanner di vulnerabilità o strumenti di gestione degli asset come Nessus o OpenVAS.		

Table 17: Common Platform Enumeration (CPE)

Vulnerabilità	CVE	Rischio	
Device Type		-	
INFORMATIVO			
Descrizione:	Il dispositivo ha rivelato informazioni relative al suo tipo, che possono essere utilizzate per identificare ulteriori vulnerabilità specifiche del dispositivo stesso.		
Impatto:	L'identificazione del tipo di dispositivo può facilitare un attaccante nella ricerca di vulnerabilità note associate a quel particolare tipo di hardware o software.		
Soluzione:	Assicurarsi che le informazioni sul tipo di dispositivo siano mascherate o minimizzate, se possibile, per evitare di fornire dati utili agli attaccanti.		
Metodo di detection:	Identificato tramite la scansione del dispositivo con strumenti di analisi come Nessus o Nmap.		

Table 18: Device Type

Vulnerabilità	CVE	Rischio	
Ethernet Card Manufacturer Detection		-	
INFORMATIVO			
Descrizione:	Le informazioni sul produttore della scheda Ethernet sono visibili e possono fornire dati sull'hardware del dispositivo.		
Impatto:	Conoscere il produttore della scheda Ethernet può aiutare un attaccante a identificare potenziali vulnerabilità associate a quel tipo di hardware.		
Soluzione:	Configurare il dispositivo per mascherare o limitare la divulgazione di informazioni relative all'hardware del dispositivo.		
Metodo di detection:	Identificato tramite la scansione della rete e dei dispositivi utilizzando strumenti come Nessus.		

Table 19: Ethernet Card Manufacturer Detection

Vulnerabilità	CVE	Rischio	
Ethernet MAC Addresses		-	
INFORMATIVO			
Descrizione:	Gli indirizzi MAC della scheda di rete sono visibili e possono fornire informazioni sul dispositivo in uso.		
Impatto:	Un attaccante potrebbe utilizzare gli indirizzi MAC per filtrare o monitorare il traffico della rete, o persino per tentare attacchi di spoofing.		
Soluzione:	Utilizzare filtri di rete o tecniche di randomizzazione degli indirizzi MAC per nascondere o proteggere queste informazioni.		
Metodo di detection:	Identificato tramite la scansione della rete e dei dispositivi, utilizzando strumenti come Nessus.		

Table 20: Ethernet MAC Addresses

Vulnerabilità	CVE	Rischio	
FTP Server Detection		-	
INFORMATIVO			
Descrizione:	Il server FTP è stato rilevato con dettagli sulla versione e configurazione corrente.		
Impatto:	Questa informazione può essere utile per riconoscizioni e può aiutare un attaccante a identificare eventuali vulnerabilità associate alla versione rilevata del server FTP.		
Soluzione:	Verificare la configurazione del server FTP e aggiornare a una versione più recente, se disponibile. Nascondere le informazioni del banner FTP per limitare la quantità di dettagli disponibili agli attaccanti.		
Metodo di detection:	Identificato tramite la scansione con strumenti come Nessus o simili, che rilevano il tipo di server e le informazioni di versione.		

Table 21: FTP Server Detection

Vulnerabilità	CVE	Rischio	
HTTP Methods Allowed (per directory)		-	
INFORMATIVO			
Descrizione:	Questa vulnerabilità fornisce un elenco di metodi HTTP consentiti per ogni directory del server web.		
Impatto:	Questa informazione può essere sfruttata per capire quali operazioni possono essere eseguite sulle directory, inclusi metodi come GET, POST, PUT, DELETE, che potrebbero esporre ulteriori superfici di attacco.		
Soluzione:	Verificare che solo i metodi HTTP necessari siano abilitati. Limitare i metodi consentiti per ridurre l'esposizione a possibili attacchi, come l'upload di file non autorizzati tramite PUT.		
Metodo di detection:	Identificato tramite strumenti di scansione come Nessus o OWASP ZAP, che rilevano i metodi HTTP disponibili per ogni directory.		

Table 22: HTTP Methods Allowed (per directory)

Vulnerabilità	CVE	Rischio	
HTTP Server Type and Version	-		
INFORMATIVO			
Descrizione:	Rileva il tipo e la versione del server HTTP, fornendo informazioni utili per la ricognizione durante una fase di attacco.		
Impatto:	Queste informazioni possono essere utilizzate dagli attaccanti per cercare vulnerabilità note relative al tipo e alla versione specifica del server HTTP in uso.		
Soluzione:	Configurare il server per nascondere l'intestazione che espone il tipo e la versione, limitando le informazioni divulgate agli attaccanti.		
Metodo di detection:	Individuato tramite strumenti di scansione come Nessus o manualmente attraverso richieste HTTP che rivelano le informazioni del server.		

Table 23: HTTP Server Type and Version

Vulnerabilità	CVE	Rischio	
Host Fully Qualified Domain Name (FQDN) Resolution		-	
INFORMATIVO			
Descrizione:	Il nome di dominio completamente qualificato (FQDN) dell'host è stato risolto, fornendo informazioni utili sull'identificazione della macchina nella rete.		
Impatto:	Questa informazione può essere utilizzata per identificare la struttura del dominio e raccogliere dettagli aggiuntivi durante una fase di ricognizione.		
Soluzione:	Non è necessaria alcuna azione specifica, ma può essere utile nascondere queste informazioni per limitare i dati divulgati agli attaccanti.		
Metodo di detection:	Rilevato tramite strumenti di scansione della rete o strumenti manuali di risoluzione DNS come 'nslookup' o 'dig'.		

Table 24: Host Fully Qualified Domain Name (FQDN) Resolution

Vulnerabilità	CVE	Rischio
HyperText Transfer Protocol (HTTP) Information	-	
INFORMATIVO		
Descrizione:	Raccolta di informazioni su protocolli HTTP utilizzati per la comunicazione web tra client e server.	
Impatto:	Queste informazioni possono essere utilizzate durante la fase di ricognizione per comprendere la struttura del server web e il tipo di comunicazione HTTP in uso.	
Soluzione:	Non è necessaria una soluzione immediata, ma si consiglia di limitare la divulgazione di informazioni tramite header HTTP non necessari.	
Metodo di detection:	Identificato tramite strumenti di scansione di rete come Nessus o manualmente con ‘curl’ o ‘wget’ per analizzare gli header HTTP.	

Table 25: HyperText Transfer Protocol (HTTP) Information

Vulnerabilità	CVE	Rischio	
Inconsistent Hostname and IP Address		-	
INFORMATIVO			
Descrizione:	La configurazione dell'hostname e dell'indirizzo IP non corrispondenti potrebbe indicare un'errata configurazione del DNS o un'errata configurazione della rete.		
Impatto:	Potrebbe causare problemi di risoluzione DNS e difficoltà di connettività tra dispositivi o applicazioni, pur non rappresentando un rischio di sicurezza diretto.		
Soluzione:	Verificare la corretta configurazione del DNS e allineare l'hostname con l'indirizzo IP della macchina.		
Metodo di detection:	Identificato tramite strumenti di rete come 'nslookup' o 'dig' per verificare la risoluzione degli hostname e la corrispondenza con l'IP.		

Table 26: Inconsistent Hostname and IP Address

Vulnerabilità	CVE	Rischio	
Nessus SYN Scanner		-	
INFORMATIVO			
Descrizione:	Il Nessus SYN Scanner rileva le porte aperte su un host remoto inviando pacchetti SYN TCP per determinare quali porte rispondono, senza stabilire una connessione completa.		
Impatto:	Non c'è un impatto diretto sulla sicurezza, ma la scansione SYN può rivelare informazioni sulle porte aperte e sui servizi in esecuzione, che potrebbero essere sfruttati da attaccanti.		
Soluzione:	Non è richiesta alcuna azione diretta, ma è consigliabile monitorare attentamente i log del firewall per eventuali scansioni sospette e configurare regole per limitare gli accessi non autorizzati.		
Metodo di detection:	Rilevato tramite scansioni SYN automatiche effettuate da Nessus per determinare lo stato delle porte.		

Table 27: Nessus SYN Scanner

Vulnerabilità	CVE	Rischio	
OS Identification		-	
INFORMATIVO			
Descrizione:	Rilevamento del sistema operativo remoto tramite fingerprinting di pacchetti di rete. Viene dedotto il tipo di sistema operativo basato sulle risposte TCP/IP.		
Impatto:	Non è dannoso di per sé, ma fornisce agli attaccanti informazioni utili per selezionare exploit mirati basati sul sistema operativo identificato.		
Soluzione:	Offuscare le risposte del sistema per evitare il rilevamento dell'OS, utilizzando tecniche di security through obscurity come IP obfuscation o firewall configurati correttamente.		
Metodo di detection:	Rilevato tramite strumenti di fingerprinting di rete come Nessus o Nmap che analizzano le risposte dei pacchetti TCP/IP.		

Table 28: OS Identification

Vulnerabilità	CVE	Rischio	
OS Security Patch Assessment Not Available		-	
INFORMATIVO			
Descrizione:	Il sistema operativo non ha fornito informazioni riguardanti lo stato delle patch di sicurezza applicate, rendendo difficile valutare se siano stati applicati aggiornamenti critici.		
Impatto:	Non è direttamente dannoso, ma l'assenza di informazioni sulle patch potrebbe indicare vulnerabilità non risolte che un attaccante potrebbe sfruttare.		
Soluzione:	Assicurarsi che il sistema operativo e i relativi pacchetti software siano aggiornati con le patch di sicurezza più recenti. Verificare manualmente l'aggiornamento delle patch se necessario.		
Metodo di detection:	Identificato tramite strumenti di vulnerability scanning come Nessus, che non ha ricevuto risposte chiare riguardanti lo stato delle patch di sicurezza del sistema operativo.		

Table 29: OS Security Patch Assessment Not Available

Vulnerabilità	CVE	Rischio	
OpenSSH Detection		-	
INFORMATIVO			
Descrizione:	Il servizio SSH identificato utilizza OpenSSH, uno dei software più comuni per connessioni sicure remote, indicando che il sistema supporta la comunicazione criptata.		
Impatto:	Non ci sono rischi diretti associati, ma le versioni obsolete o mal configurate di OpenSSH potrebbero essere vulnerabili ad attacchi di brute force o a sfruttamenti delle vulnerabilità del protocollo.		
Soluzione:	Assicurarsi di aggiornare OpenSSH all'ultima versione disponibile e configurarlo correttamente per prevenire potenziali attacchi. Implementare autenticazione a due fattori e limitare gli accessi non necessari.		
Metodo di detection:	Rilevato tramite Nessus o altri strumenti di scanning che analizzano i servizi attivi e le loro versioni.		

Table 30: OpenSSH Detection

Vulnerabilità	CVE	Rischio	
Patch Report	-		
INFORMATIVO			
Descrizione:	Il report fornisce informazioni sulle patch di sicurezza applicate o non applicate al sistema in esame, rilevando eventuali aggiornamenti mancanti o vecchie patch.		
Impatto:	L'assenza di patch aggiornate potrebbe esporre il sistema a vulnerabilità conosciute che sono già state risolte nelle versioni più recenti.		
Soluzione:	Assicurarsi che tutte le patch di sicurezza siano applicate tempestivamente, mantenendo il sistema aggiornato. Verificare periodicamente la disponibilità di nuovi aggiornamenti di sicurezza.		
Metodo di detection:	Rilevato tramite uno scanner di vulnerabilità come Nessus che identifica le patch mancanti o obsolete.		

Table 31: Patch Report

Vulnerabilità	CVE	Rischio
SSH Algorithms and Languages Supported	-	
INFORMATIVO		
Descrizione:	Elenca gli algoritmi di crittografia e i linguaggi di autenticazione supportati dal server SSH. Questo include algoritmi di cifratura, hashing e chiavi usati per stabilire connessioni sicure.	
Impatto:	Queste informazioni aiutano a determinare se il server SSH utilizza algoritmi deboli o obsoleti, che potrebbero essere vulnerabili ad attacchi di forza bruta o crittografici.	
Soluzione:	Aggiornare la configurazione SSH per utilizzare solo algoritmi moderni e sicuri, evitando quelli considerati deboli o vulnerabili.	
Metodo di detection:	Rilevato tramite scanner di vulnerabilità come Nessus o strumenti di configurazione del server SSH.	

Table 32: SSH Algorithms and Languages Supported

Vulnerabilità	CVE	Rischio	
SSH Password Authentication Accepted		-	
INFORMATIVO			
Descrizione:	Il server SSH accetta l'autenticazione tramite password, che può essere meno sicura rispetto ad altri metodi come l'autenticazione tramite chiave pubblica.		
Impatto:	L'autenticazione tramite password è suscettibile ad attacchi di brute force, aumentando il rischio di compromissione del server se le password non sono sufficientemente forti.		
Soluzione:	Si consiglia di disabilitare l'autenticazione tramite password nel file di configurazione SSH e abilitare l'autenticazione tramite chiave pubblica per migliorare la sicurezza.		
Metodo di detection:	Rilevato tramite la configurazione del server SSH o tramite uno scanner di vulnerabilità come Nessus.		

Table 33: SSH Password Authentication Accepted

Vulnerabilità	CVE	Rischio
SSH Protocol Versions Supported	-	
INFORMATIVO		
Descrizione:	Il server SSH supporta diverse versioni del protocollo SSH. Alcune versioni più vecchie del protocollo SSH potrebbero essere vulnerabili a diversi tipi di attacchi.	
Impatto:	Se il server supporta versioni obsolete del protocollo, potrebbe essere più suscettibile ad attacchi di tipo man-in-the-middle o attacchi di downgrade.	
Soluzione:	Aggiornare il server SSH per supportare solo le versioni più recenti e sicure del protocollo SSH, come SSHv2. Configurare il server per rifiutare automaticamente le connessioni che utilizzano versioni precedenti.	
Metodo di detection:	Rilevato tramite scanner di vulnerabilità come Nessus o un’analisi manuale della configurazione del server SSH.	

Table 34: SSH Protocol Versions Supported

Vulnerabilità	CVE	Rischio	
SSH SHA-1 HMAC Algorithms Enabled		-	
INFORMATIVO			
Descrizione:	Il server SSH consente l'utilizzo di algoritmi HMAC basati su SHA-1. Questo algoritmo è considerato debole e vulnerabile a collisioni crittografiche.		
Impatto:	L'uso di SHA-1 potrebbe facilitare attacchi crittografici, compromettendo la sicurezza delle sessioni SSH.		
Soluzione:	Configurare il server SSH per disabilitare gli algoritmi HMAC basati su SHA-1 e utilizzare algoritmi più sicuri come SHA-256 o SHA-512.		
Metodo di detection:	Rilevato tramite strumenti di scansione delle vulnerabilità come Nessus o OpenVAS, o tramite revisione manuale della configurazione SSH.		

Table 35: SSH SHA-1 HMAC Algorithms Enabled

Vulnerabilità	CVE	Rischio
SSH Server Type and Version Information	-	
INFORMATIVO		
Descrizione:	Il server SSH fornisce informazioni sul tipo e sulla versione, esponendo dettagli che potrebbero essere utilizzati per condurre attacchi mirati sfruttando vulnerabilità specifiche della versione.	
Impatto:	Gli attaccanti possono sfruttare le informazioni sulla versione del server SSH per identificare vulnerabilità specifiche e condurre attacchi mirati.	
Soluzione:	Configurare il server SSH per nascondere le informazioni sulla versione o utilizzare banner personalizzati.	
Metodo di detection:	Rilevato tramite strumenti di scansione delle vulnerabilità o una semplice analisi manuale della risposta del server SSH.	

Table 36: SSH Server Type and Version Information

Vulnerabilità	CVE	Rischio	
TCP/IP Timestamps Supported	-		
INFORMATIVO			
Descrizione:	Il sistema supporta i timestamp TCP/IP, che possono essere utilizzati dagli attaccanti per raccogliere informazioni sul tempo di attività del sistema e per facilitare attacchi di tipo TCP sequence prediction.		
Impatto:	Anche se non rappresenta un rischio diretto, queste informazioni possono essere sfruttate per condurre attacchi mirati, come la previsione della sequenza TCP.		
Soluzione:	Disabilitare il supporto per i timestamp TCP/IP a livello di configurazione del kernel o delle impostazioni del firewall.		
Metodo di detection:	Rilevato tramite strumenti di scansione delle vulnerabilità come Nessus o analisi manuale del traffico di rete.		

Table 37: TCP/IP Timestamps Supported

Vulnerabilità	CVE	Rischio
Target Credential Status by Authentication Protocol - No Credentials Provided	-	
INFORMATIVO		
Descrizione:	Nessuna credenziale è stata fornita durante l'autenticazione al protocollo di destinazione, il che può indicare l'uso di metodi non autenticati per l'accesso al sistema.	
Impatto:	Anche se non immediatamente pericoloso, questo comportamento potrebbe evidenziare una mancanza di sicurezza nelle politiche di accesso e potrebbe essere sfruttato da attaccanti non autenticati.	
Soluzione:	Verificare la configurazione del protocollo di autenticazione e garantire che vengano utilizzate credenziali sicure per l'accesso a tutti i servizi di destinazione.	
Metodo di detection:	Identificato tramite scanner di vulnerabilità come Nessus che rilevano protocolli senza credenziali associate.	

Table 38: Target Credential Status by Authentication Protocol - No Credentials Provided

Vulnerabilità	CVE	Rischio	
Traceroute Information		-	
INFORMATIVO			
Descrizione:	L'output del comando traceroute fornisce dettagli sui router intermediari attraversati dai pacchetti verso il server di destinazione, mostrando informazioni dettagliate sui nodi di rete.		
Impatto:	Non direttamente pericoloso, ma un attaccante può usare queste informazioni per mappare la rete e identificare punti di potenziale attacco o debolezze nei dispositivi di rete intermedi.		
Soluzione:	Bloccare i comandi traceroute in uscita o limitare l'uso del protocollo ICMP per evitare che informazioni sensibili sui nodi di rete siano facilmente ottenibili.		
Metodo di detection:	Identificato tramite strumenti di rete come traceroute, che tracciano il percorso dei pacchetti verso una destinazione specifica.		

Table 39: Traceroute Information

Vulnerabilità	CVE	Rischio	
vsftpd Detection		-	
INFORMATIVO			
Descrizione:	Il server FTP rilevato utilizza vsftpd, un server FTP veloce e sicuro utilizzato comunemente in ambienti Linux.		
Impatto:	L'informazione sulla versione del server può essere usata da un attaccante per identificare vulnerabilità note associate alla versione specifica di vsftpd.		
Soluzione:	Assicurarsi che la versione di vsftpd utilizzata sia aggiornata e che non ci siano vulnerabilità conosciute. Implementare misure di sicurezza, come disabilitare l'accesso anonimo e abilitare l'uso di FTPS.		
Metodo di detection:	La vulnerabilità è stata rilevata attraverso uno scanner di vulnerabilità come Nessus o altri strumenti di scansione della rete.		


Table 40: vsftpd Detection

6 Appendix

Una dimostrazione di come è stata sfruttata la vulnerabilità è documentata nel documento *PenetrationTesting Metodologie*, disponibile anche al link:

<https://github.com/AlfCan-dev/CengBox2-PenetrationTesting>

```
mitnick@cengbox:~$ ls -la /bin/nano  
-rwsr-xr-x 1 root root 208480 Feb 15 2017 /bin/nano  
mitnick@cengbox:~$ nano /etc/passwd  
mitnick@cengbox:~$ su aleq  
Password:  
root@cengbox:/home/mitnick# ls  
user.txt  
root@cengbox:/home/mitnick# cd /root  
root@cengbox:~# ls  
root.txt  
root@cengbox:~# cat root.txt
```



I would be grateful for your any feedback. Feel free to contact me on Twitter @arslanblcn_

de89782fe4e8bf2198a022ae7f50613e
root@cengbox:~#

Figure 3: Lettura del file `root.txt`

7 References

- CVE-2023-48795: <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
- CVE-1999-0497 <https://nvd.nist.gov/vuln/detail/CVE-1999-0497>
- CVE-2019-1653 <https://nvd.nist.gov/vuln/detail/CVE-2019-1653>
- CVE-2017-3167 <https://nvd.nist.gov/vuln/detail/CVE-2017-3167>
- CVE-2015-2080 <https://nvd.nist.gov/vuln/detail/CVE-2015-2080>
- CVE-2000-0354 <https://nvd.nist.gov/vuln/detail/CVE-2000-0354>
- CVE-2006-4380 <https://nvd.nist.gov/vuln/detail/CVE-2006-4380>

- CVE-2016-2183 <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
- CVE-2018-12386 <https://nvd.nist.gov/vuln/detail/CVE-2018-12386>