UNIVERSITÀ DEGLI STUDI DI SALERNO

Penetration Testing Report

MHZ_CXF: C1F

Antonio Baldi | Corso di PTEH | A.A. 2022/2023

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA
DIPARTIMENTO DI ECCELLENZA

Sommario

1 Executive Summary

L'attività progettuale svolta per il corso di *Penetration Testing & Ethical Hacking* prevede l'esecuzione di un penetration test sulla macchina target **MHZ_CXF: C1F**. L'obiettivo quest'attività è analizzare la sicurezza della macchina target ed evidenziare eventuali contromisure da adottare per le vulnerabilità riscontrate. È stato utilizzato un approccio di tipo *Black Box* in quanto non si hanno informazioni rilevanti relative alla macchina target e alla struttura di rete. Il test è stato eseguito trovandosi sulla stessa rete locale della macchina da analizzare ed è stato emulato il comportamento di un attaccante con accesso a tale rete. Le vulnerabilità rilevate potrebbero consentire a un utente malintenzionato di ottenere pieno controllo della macchina causando gravi danni al sistema e agli utenti che usufruiscono dei servizi erogati da questa macchina. Questo potrebbe compromettere *la disponibilità*, *l'integrità* e *la confidenzialità* del sistema. Dunque si può affermare che il **livello di sicurezza** della macchina è **BASSO** mentre il **rischio di compromissione** risulta essere **ALTO**; è necessario quindi intervenire modificando il sistema ed eliminando le vulnerabilità riscontrate, in questo modo il rischio verrà riportato a livelli accettabili.

Tutte le vulnerabilità comprese di relative contromisure da adottare verranno elencate e dettagliatamente descritte nelle sezioni di questo documento

2 Engagement Highlights

Le regole di ingaggio, in questo caso, non sono state contestualizzate facendo questo parte di un attività progettuale di tipo accademica e quindi non soggetta ad accordi di non divulgazione (**NDA**). In particolare non sono stati presentati limiti riguardo agli strumenti e alle tecniche consentite a patto di non sconfinare la rete **NAT** creata appositamente per l'analisi di questa macchina. Di seguito riportate le sezioni delle regole d'ingaggio comuni. Usualmente tutto ciò che non viene definito non è consentito, in questo caso non vengono apposti limiti e l'analista ha dichiarato le tecniche e gli strumenti nell'apposito documento nella sezione **Strumenti utilizzati**.

2.1 Accordo di non divulgazione

Non sono stati siglati accordi di non divulgazione avente parte il docente del corso o l'ente dell'università degli studi di Salerno pertanto l'analisi è libera da accordi che ne vietino la divulgazione.

2.2 Consegna stimata

È stato stimato un tempo di completamento di 30 giorni lavorativi per poter effettuare l'analisi e la stesura dei documenti riguardanti gli strumenti e le metodologie utilizzate e il *Penetration Testing Report*.

2.3 Tecniche e strumenti consentiti

L'analisi non è caratterizzata da vincoli riguardo gli strumenti e le tecniche da utilizzare quindi è stata data libera scelta allo studente. Sono state definite le responsabilità legali qualora l'analisi

possa compromettere macchine o servizi esterni alla macchina target o alla rete **NAT**, definita per l'attività di analisi.

2.4 Ambito d'applicazione

L'ambito d'applicazione è legato alla sola analisi della macchina target, pertanto è vietato il recupero di informazioni tramite le forme di **Intelligence**: Human Intelligence e Signal Intelligence. Il processo di analisi non deve includere persone terze come potrebbe essere il creatore della macchina.

2.5 Processo di Analisi

Durante il processo di Analisi non verranno segnalate le vulnerabilità gravi riscontrate. Queste verranno rese note al termine dell'analisi, essendo uno strumento di esercitazione didattico, effettuato su una macchina vulnerabile by design, questa non ha servizi pubblicamente accessibili pertanto non necessità di una segnalazione repentina delle vulnerabilità più gravi.

3 Vulnerability Report

Da un'analisi della macchina sono emerse alcune vulnerabilità che la espongono ad attacchi da parte di utenti maliziosi:

- Alcune credenziali d'accesso sono presenti in chiaro, all'interno di file presenti nel web server esposto dalla macchina analizzata. Tali credenziali consentono l'accesso tramite OpenSSH come utente *first_stage* da cui è possibile accedere ai file presenti sul sistema.
- Il web server permette la navigazione e la visualizzazione di file che non dovrebbero essere accessibili a tutti gli utenti perché non fanno parte della parte funzionale del sito web ma spesso sono file di configurazione o simili utili al funzionamento.
- Sono presenti ulteriori credenziali d'accesso all'interno di file di tipo immagine mediante tecniche di steganografia, cioè informazioni nascoste in un file. Queste non sono protette da password, fornendo delle credenziali di un utente del sistema.
- l'utente al quale si fa riferimento nelle credenziali estratte dall'immagine mediante la steganografia fa parte della lista di **SUDOERS**, cioè, in un sistema UNIX, vuol dire che ha i permessi per diventare amministratore.

4 Remediation Report

Date le problematiche di sicurezza riscontrate durante l'attività di penetration testing dovrebbero essere messe in atto le seguenti strategie al fine di migliorare la sicurezza del sistema:

- Eliminare tutti i dati sensibili non cifrati presenti nei file.

- Gestire l'accesso ai file e le directory relativi al web server e autorizzare la navigazione ai file agli utenti solo nel caso in cui la progettazione del web server prevede che un utente possa visualizzare determinati tipi di file.
- Non utilizzare tecniche di occultamento delle informazioni all'interno di altri file.
- Se necessario utilizzare tecniche di steganografia, utilizzare password per la lettura del contenuto molto robuste, in modo che un attacco a dizionario non abbia successo. Quindi utilizzare password lunghe più di 16 caratteri, alfanumeriche, con caratteri speciali e non utilizzare passowrd con nomi comuni o di breve lunghezza.
- Effettuare un Security Audit in modo frequente e programmato
- Programmare un Penetration testing, come quello effettuato, fissando un numero di volte per il quale effettuarlo durante l'anno.

Si consiglia di risolvere tutte le vulnerabilità presentate in questo documento seguendo un ordine decrescente in base alla gravità: è consigliato dunque risolvere tempestivamente le vulnerabilità critiche e procedere successivamente alla correzione delle vulnerabilità con criticità più bassa.

5 Findings Summary

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

Severity	Info	Low	Medium	High	Critical
# Vulnerabilità	25	2	2	2	2

Il grafico seguente mostra la distribuzione delle vulnerabilità per categoria:

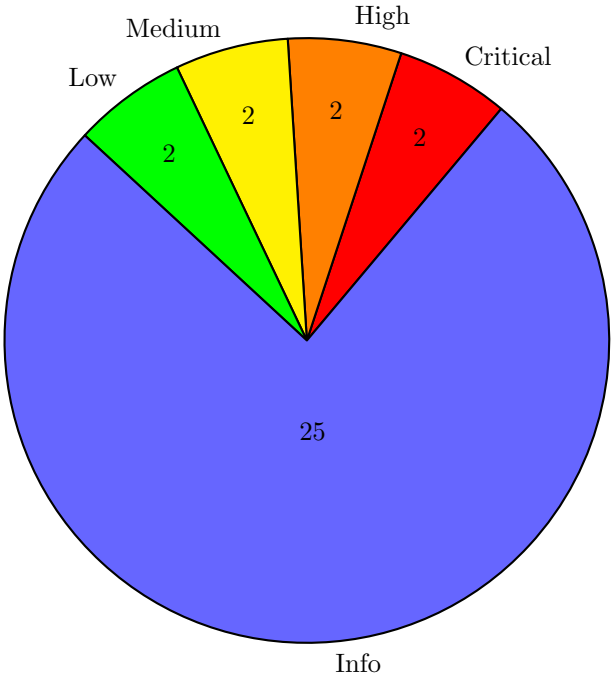

Figure 1: Grafico a torta delle vulnerabilità

6 Detailed Summary

Di seguito verranno riportate e descritte dettagliatamente le vulnerabilità individuate, partendo da quelle più critiche fino a quelle meno critiche. Inoltre per ognuna di essa verranno fornite alcune raccomandazioni su come mitigarle.

6.1 Critical

Credenziali presenti all'interno di file in chiaro

Descrizione

All'interno di un file navigabile dal web server sono presenti le credenziali dell'utente di sistema [1]

Impatto

Sfruttando questa password è possibile accedere all'utente che esegue il web server.

Soluzione

Rimuovere la password in chiaro dal file, rimuovere il file oppure mitigare le debolezze di *full path disclosure, directory listing, information leakage*.

Password Deboli

Descrizione

L'utente first_stage utilizza una password facilmente calcolabile con un attacco del dizionario [2]

Impatto

Questa password permette di avere accesso remoto alla macchina tramite connessione SSH

Soluzione

Aumentare la complessità delle password utilizzate, quindi utilizzare password lunghe, alfanumeriche, con caratteri speciali e assicurarsi che non facciano parte di dizionari comuni di password.

6.2 High

Limitazione non corretta di un percorso a un file o una directory limitata.
Path Traversal

Descrizione

Il web server espone file e directory a utenti non esplicitamente autorizzati ad accedervi ma non prevede protezioni [3].

Impatto

Sfruttando questa debolezza si può accedere a file e directory del web server e, in questo caso, trovare alcune credenziali di sistema.

Soluzione

Convalidare gli input, quando si convalidano nomi di file o percorsi, utilizzare liste consentite e, se possibile, non consentire mai la sequenza ".." per evitare **Relative Path Traversal** [4] ed escludere "/" per evitare **Absolute Path Traversal** [5]

Esposizione di informazioni attraverso **Directory Listing**

Descrizione

Il directory listing fornisce a un utente malintenzionato l'indice completo di tutte le risorse che si trovano all'interno della directory. I rischi e le conseguenze specifici variano a seconda dei file elencati e accessibili [6]

Impatto

Sfruttando questa debolezza si può accedere a file e directory del web server e a seconda dei file trovati è più o meno grave l'impatto.

Soluzione

Le raccomandazioni includono la limitazione dell'accesso a directory o file importanti, adottando un requisito di necessità di conoscenza sia per il documento che per la radice del server, e la disattivazione di funzioni come l'elenco automatico delle directory che potrebbero esporre file privati e fornire informazioni che potrebbero essere utilizzate da un aggressore quando formula o conduce un attacco.

6.3 Medium

Apache server-status enabled

Descrizione

Apache server-status visualizza informazioni sullo stato del servizio Apache [7].

Impatto

Un utente malintenzionato potrebbe utilizzare questa debolezza per recuperare informazioni sullo stato di Apache [8].

Soluzione

Disattivare questa funzionalità se non è necessaria. Commentare la sezione da "*httpd.conf*.

Apache server-info enabled

Descrizione

Apache server-status visualizza informazioni sulla configurazione del servizio Apache [9].

Impatto

Un utente malintenzionato potrebbe utilizzare questa debolezza per recuperare informazioni sulla configurazione di Apache [8].

Soluzione

Disattivare questa funzionalità se non è necessaria. Commentare la sezione da "*httpd.conf*.

6.4 Low

TCP timestamps

Descrizione

L'host remoto implementa i timestamp TCP e quindi consente di calcolare il tempo di attività.

Impatto

Un effetto collaterale di questa funzionalità è che il tempo di attività dell'host remoto può talvolta essere calcolato.

Soluzione

Disabilitare i TCP timestamps all'interno del sistema: aggiungere la riga "net.ipv4.tcp_timestamps=0" in /etc/sysctl.conf. Lanciare successivamente il comando sysctl -p

ICMP Timestamp Reply Information Disclosure

Descrizione

Il Timestamp Reply è un messaggio ICMP che risponde a un messaggio di Timestamp. È composto dal timestamp di origine inviato dal mittente del Timestamp, nonché da un timestamp di ricezione e da un timestamp di trasmissione.

Impatto

Queste informazioni potrebbero teoricamente essere utilizzate per sfruttare i generatori di numeri casuali deboli basati sul tempo in altri servizi.

Soluzione

Disattivare completamente il supporto per il timestamp ICMP sull'host remoto. Proteggere l'host remoto con un firewall e bloccare i pacchetti ICMP che passano attraverso il firewall in entrambe le direzioni (completamente o solo per le reti non attendibili).

6.5 Informative

Le vulnerabilità informative sono quelle individuate in maggioranza dagli strumenti di scansione automatica delle vulnerabilità, tuttavia non sono state riportate dato che non hanno rilevanza nei confronti di potenziali attaccanti. Queste fanno riferimento per lo più al fatto che si possono recuperare le versioni dei servizi esposti come la versione di Apache, la versione di HTTP e altro ancora.

References

[1] *Plaintext Storage of a Password*. URL: `https://cwe.mitre.org/data/definitions/256.html`.

[2] *Use of Weak Credentials*. URL: `https://cwe.mitre.org/data/definitions/1391.html`.

[3] *Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*. URL: `https://cwe.mitre.org/data/definitions/22.html`.

[4] *Relative Path Traversal*. URL: `https://cwe.mitre.org/data/definitions/23.html`.

[5] *Absolute Path Traversal*. URL: `https://cwe.mitre.org/data/definitions/36.html`.

[6] *Exposure of Information Through Directory Listing*. URL: `https://cwe.mitre.org/data/definitions/548.html`.

[7] *Apache server-status enabled*. URL: `https://www.acunetix.com/vulnerabilities/web/apache-server-status-enabled/`.

[8] *Exposure of Sensitive Information to an Unauthorized Actor*. URL: https://cwe.mitre.org/data/definitions/200.html.

[9] *Apache server-info enabled*. URL: https://www.acunetix.com/vulnerabilities/web/apache-server-info-enabled/.