Università degli
Studi di Salerno

Penetration Testing Report

CASO DI STUDIO: POTATO

Eduardo Autore | Corso di PTEH | A.A. 2023/2024

PROFESSORE

ARCANGELO CASTIGLIONE

STUDENTE

EDUARDO AUTORE

MATR: 0522501549

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

1. NON-DISCLOSURE AGREEMENT (NDA)

Questo documento è di esclusiva proprietà di **PenTest Solutions (PTS)** e di **CyberGuard Corp. (CGC)**. Il presente documento contiene informazioni di natura proprietaria e confidenziale.

La duplicazione, redistribuzione, uso parziale o totale, in qualsiasi forma, richiede il consenso di TUTTE le parti definite nel documento. Qualsiasi illecito sarà perseguibile a norma di legge.

PenTest Solutions (PTS) ha la piena possibilità di condividere questo documento con auditors o terze parti, rispettando gli accordi di non divulgazione e proteggendo la privacy dei dati secondo le regole della **G.D.P.R.**, ai fini di mostrare esempi di report a futuri clienti o auditors.

2. DISCLAIMER

Un “Penetration Test” è considerabile come uno “screenshot” dello stato di sicurezza degli asset analizzati, in un determinato lasso di tempo definito. Tutti i ritrovamenti, raccomandazioni o rimedi esposti in questo documento sono da considerarsi esclusivamente relativi al periodo di tempo specificato per il processo di Penetration Testing.

In caso di test effettuati su basi di tempo limitate, vengono ricercati e sfruttati gli anelli più deboli degli asset scelti, simulando quello che un ipotetico attaccante avrebbe potuto fare in un periodo di tempo ristretto.

PenTest Solutions (PTS) raccomanda di condurre valutazioni di sicurezza su base trimestrale, quadrimestrale, semestrale o annuale da parte di auditors appartenenti all’azienda proprietaria degli asset o da auditors di terze parti.

3. EXECUTIVE SUMMARY

L'attività di penetration testing ha avuto inizio il 25/06/2024 sulla macchina Potato:1[1], reperita da vulnhub e consultabile al seguente link: https://www.vulnhub.com/entry/potato-1,529/.

L'obiettivo è stato quello di individuare ed analizzare quante più vulnerabilità possibili sulla macchina target al fine di potervi accedere e mantenere l'accesso permanente mediante backdoor.

Il penetration testing è stato caratterizzato da una metodologia **grey box** in quanto si era già a conoscenza di alcuni dettagli della macchina come il Sistema operativo.

I risultati ottenuti hanno mostrato numerose vulnerabilità all'interno della macchina che potrebbero essere sfruttate per accedere ad essa come la "**Local File Inclusion (LFI)**" e la "**FTP Anonymous login**", ma anche per provocare altre tipologie di danni mediante **sql injection,** a causa della mancanza di controlli adeguati sull'URL encoding.

Questo report fornisce un'analisi dettagliata delle vulnerabilità individuate, insieme a raccomandazioni sulle contromisure da adottare per mitigare la maggior parte di queste.

4. ENGAGEMENT HIGHLIGHTS

Non sono state stabilite alcune particolari regole d'ingaggio in quanto il penetration testing è stato conseguito a fini didattici su macchine hostate in ambienti sicuri (virtual machine) e reperite da vulnhub. Gli autori delle macchine presenti su vulnhub infatti le mettono a disposizioni proprio per studi di questo genere.L'intero processo ha seguito le fasi studiate durante il corso e raccolte nel Framework

Generale per il Penetration Testing (FGPT), ovvero:

- Information Gathering
- Target Discovery
- Enumerating target & port scanning
- Vulnerability Mapping
- Target Exploitation
- Post-Exploitation (Privilege Escalation & Maintaining Access)

La fase iniziale di target scoping è stata omessa in quanto non vi è stata nessuna collaborazione diretta col cliente.

Gli strumenti utilizzati sono stati molteplici:

- Zenmap, Nmap e Unicornscan per le attività di target discovery, enumerating target e vulnerability mapping
- Exploit-db e Cve-details come basi di dati da cui attingere informazioni in maniera manuale sulle possibili vulnerabilità.
- Nessus, OpenVas e Nikto per l'individuazione automatica delle vulnerabilità
- Burp Suite, Dirb, Gobuster e John the Ripper password cracker per le fasi di exploitation
- Cymothoa per la fase di post-exploitation

5. VULNERABILITY REPORT

Come detto precedentemente, tramite Nessus, OpenVas e basi di dati da cui attingere informazioni sulle vulnerabilità. La scansione di Nessus è stata effettuata il 1 luglio ed ha impiegato. Sono state effettuate 2 scansione automatiche e dettagliate sulla macchina target con l'obiettivo di rilevare più vulnerabilità possibili.

- La scansione con **OpenVAS** è stata effettuata il 01/07/2024, è iniziata alle 16:45:14 ed è terminata alle 17:01:03 , durando 15 minuti e 49 secondi. I risultati della scansione con OpenVAS ci hanno dato su una scala di valore massimo 10:

    - 3 vulnerabilità di livello Medio (6.4, 4.8, 4.8)
    - 3 vulnerabilità basse(2.6, 2.6, 2.1)

- La scansione con **Nessus** è stata effettuata il 01/07/2024, è iniziata alle 16:55:50 ed è terminata alle 17:02:58, durando 7 minuti e 8 secondi. I risultati della scansione con Nessus hanno riportato, su una scala di valore massimo 10:

    - 1 vulnerabilità di livello alto (8.3)
    - 2 vulnerabilità di livello medio (5.9, 4.3)
    - 3 vulnerabilità di livello basso (2.6, 2.1, N/A)

Durante l'attività di analisi, sono state riscontrate diverse vulnerabilità nei servizi offerti dalla macchina. I servizi web erano forniti esclusivamente tramite protocollo **HTTP**, rendendo alcune risorse vulnerabili ad attacchi man-in-the-middle. Le informazioni trasmesse tra le pagine HTTP, infatti, viaggiavano in chiaro e potevano essere intercettate da un attaccante in grado di operare in questa modalità.

Ulteriori debolezze nei servizi web riguardavano l'organizzazione degli URL. Formattando opportunamente gli URL, è stato possibile visualizzare risorse della macchina e ottenere accesso a essa. In particolare, una cattiva gestione della pagina dei log nella homepage dell'utente admin ha permesso di ottenere credenziali di accesso SSH alla macchina.

Anche altri servizi presentavano vulnerabilità: il servizio **FTP** consentiva l'accesso in modalità anonima, permettendo l'accesso ai file ospitati. Inoltre, le comunicazioni di questo servizio non erano cifrate, rendendo possibile l'intercettazione da parte di un attaccante in modalità man-in-the-middle. Infine, è stata trovata una vulnerabilità in un'area di **codice PHP** che, a causa di un errato utilizzo dei confronti flessibili e della funzione **strcmp** su una variabile manipolabile da un aggressore, poteva permettere la manomissione della variabile stessa.

Tutte queste vulnerabilità hanno un impatto significativo sulla sicurezza della macchina e verranno analizzate nel dettaglio nel paragrafo "Detailed Summary".

6. REMEDIATION REPORT

Diverse soluzioni possono essere attuate per migliorare la sicurezza:

- **Implementare HTTPS**: Utilizzare esclusivamente il protocollo HTTPS per tutti i servizi web offerti, limitando così le possibilità di attacchi man-in-the-middle.
- Includere l'intestazione **HTTP X-Frame-Options o Content-Security-Policy** (con la direttiva **frame-ancestors**) nelle risposte delle pagine per prevenire attacchi di clickjacking.
- Fortemente raccomandato di modificare gli **script CGI** interessati in modo che escano correttamente gli argomenti ed evitare possibili attacchi di SQL Injections.
- **Utilizzare Comparazioni Rigorose**: Adottare metodi di comparazione rigorosi come "===" invece di "==" in strcmp per azioni sensibili come il login nei file .php. Questo riduce la vulnerabilità alla manipolazione dei parametri, che ha permesso l'accesso all'account admin del servizio web mediante la manipolazione del parametro $pass.
- **Aggiornare i Software**: Aggiornare il software Apache alla versione più recente. (2.4.61) oppure almeno alla versione 2.4.54 per ridurre le vulnerabilità.
- Aggiornare FTP alle versioni più recenti(3.67.1) per ridurre le vulnerabilità.
- Aggiornare SSH alle versioni più recenti (9.8) per ridurre le vulnerabilità.
- Disattivare **l'accesso anonimo** nel servizio FTP.
- **Aggiornare il Sistema Operativo**: Garantire che il sistema operativo sia sempre aggiornato per beneficiare delle ultime patch di sicurezza.
- **Implementare Firewall e Filtri**: Integrare firewall e meccanismi di filtraggio delle porte per aumentare la protezione contro accessi non autorizzati e attacchi.

7. FINDINGS SUMMARY

Di seguito vengono mostrate le vulnerabilità riscontrate, con il rispettivo impatto sulla sicurezza classificato secondo i seguenti parametri (in accordo con Nessus e OpenVAS):

• Basso: Vulnerabilità che possono essere sistemate anche in un secondo momento. Un attaccante, sfruttandole, non sarebbe in grado di danneggiare significativamente il sistema e otterrebbe pochissime informazioni su di esso.

• Medio: Vulnerabilità che richiedono condizioni specifiche e meccanismi particolari per essere sfruttate. Queste vanno risolte, ma non rappresentano un'urgenza immediata.

• Alto: Vulnerabilità che devono essere risolte nel breve termine. Sebbene non siano critiche, potrebbero essere sfruttate per ottenere accesso alle macchine e causare danni significativi.

•Critico: Vulnerabilità che necessitano di una risoluzione immediata, poiché potrebbero portare a danni irreparabili al sistema o alla sua totale compromissione.

RIPARTIZIONE VULNERABILITA' (NESSUS)						
S#	**IP Address**	**Hostname**	**Critical**	**High**	**Medium**	**Low**
1	10.0.2.11	Potato:1	0	1	2	3

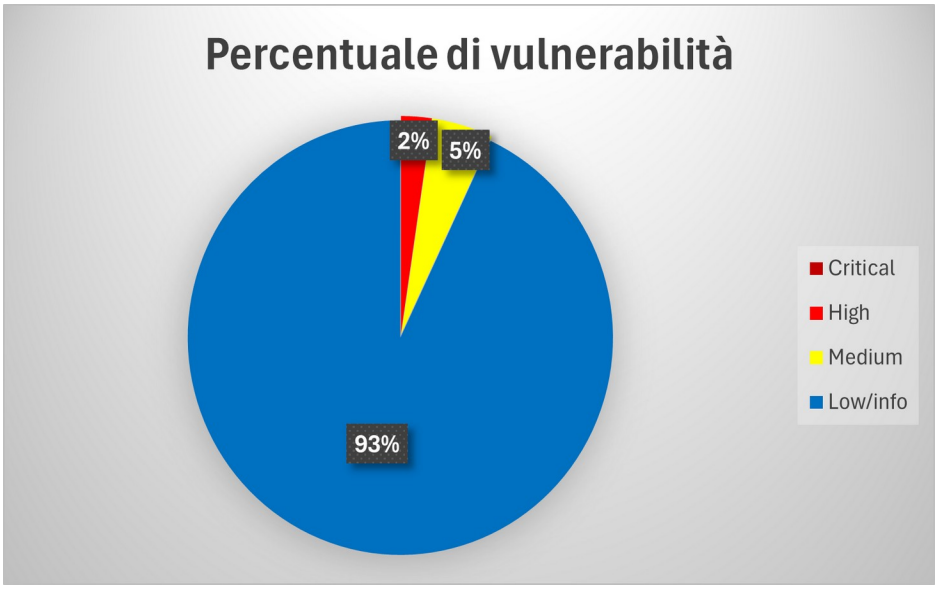

Figura 1 - Grafico Vulnerabilità Nessus

RIPARTIZIONE VULNERABILITA' (OPENVAS)						
S#	IP Address	Hostname	Critical	High	Medium	Low
1	10.0.2.11	Potato:1	0	0	3	3

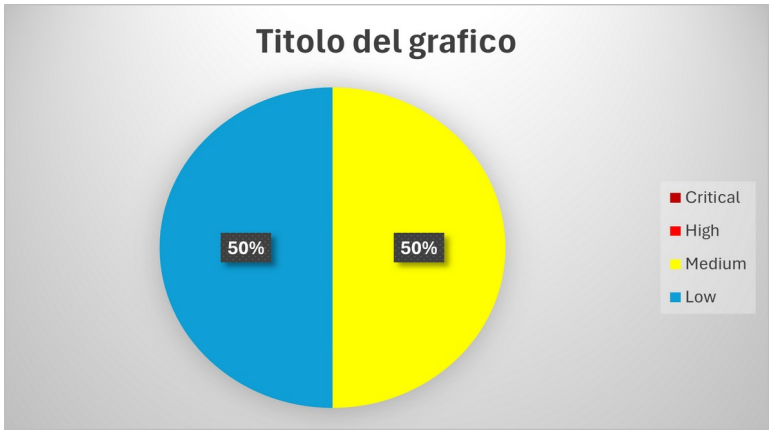

Figura 2 - Grafico Vulnerabilità OpenVAS

8. DETAILED SUMMARY

In questo paragrafo verranno illustrate in dettaglio tutte le vulnerabilità rilevate, insieme ai relativi punteggi CVE e alle misure di mitigazione disponibili.

8.1 NESSUS

E1 - CGI Generic SQL Injection blind (Punteggio CVE: 8.3)

Sinossi
Un'applicazione CGI ospitata sul server web remoto è potenzialmente soggetta ad attacchi di SQL injection.

Descrizione
Inviando parametri appositamente creati a uno o più script CGI ospitati sul server web remoto, Nessus è stato in grado di ottenere una risposta molto diversa, suggerendo che potrebbe essere stato possibile modificare il comportamento dell'applicazione e accedere direttamente al database sottostante.

Un attaccante potrebbe sfruttare questo problema per bypassare l'autenticazione, leggere dati riservati, modificare il database remoto o addirittura prendere il controllo del sistema operativo remoto.

Rischio
Alto

Mitigazione
Modificare gli script CGI interessati in modo che eseguano correttamente l'escape degli argomenti.

Punteggio CVSS v3.0 Base

8.3 (CVSS:3.0/AV/AC/PR/UI/S/C/I/A)

E2 - SSH Terrapin Prefix Truncation Weakness (Punteggio CVE: 5.9)

Sinossi

Il server SSH remoto è vulnerabile a un attacco di troncamento del prefisso man-in-the-middle (mitm).

Descrizione

Il server SSH remoto è vulnerabile a una debolezza di troncamento del prefisso mitm nota come Terrapin. Ciò può consentire a un attaccante remoto, man-in-the-middle, di bypassare i controlli di integrità e degradare la sicurezza della connessione. (CVE-2023-48795[2]).

Mitigazione

Contattare il fornitore per un aggiornamento con le contromisure di scambio di chiavi rigorose o disabilitare gli algoritmi interessati.

Rischio

Medio.

Punteggio CVSS v3.0 Base

5.9 (CVSS:3.0/AV/AC/PR/UI/S/C/I/A)

E3 - Web Application Potentially Vulnerable to Clickjacking (Punteggio CVE: 4.3)

Sinossi

Il server web remoto potrebbe non mitigare una classe di vulnerabilità delle applicazioni web.

Descrizione

Il server web remoto non imposta un'intestazione di risposta X-Frame-Options o una Content-Security-Policy 'frame-ancestors' in tutte le risposte di contenuto. Ciò potrebbe potenzialmente esporre il sito a un attacco di clickjacking o di ridefinizione dell'interfaccia utente, in cui un attaccante può indurre un utente a cliccare su un'area della pagina vulnerabile diversa da quella percepita dall'utente. Questo può portare l'utente a eseguire transazioni fraudolente o dannose.

Mitigazione

Restituire l'intestazione HTTP X-Frame-Options o Content-Security-Policy (con la direttiva frame-ancestors) con la risposta della pagina.

Rischio

Medio.

Punteggio CVSS v2.0 Base

4.3 (CVSS2#AV/AC/Au/C/I/A)

E4 - Web Server Transmits Cleartext Credentials (Punteggio CVE: 2.6)

Sinossi

Il server web remoto potrebbe trasmettere credenziali in chiaro.

Descrizione

Il server web remoto contiene diversi campi HTML di tipo 'password' che trasmettono le loro informazioni in chiaro a un server web remoto.

Mitigazione

Assicurarsi che ogni modulo sensibile trasmetta i contenuti tramite HTTPS.

Rischio

Basso: Un attaccante che intercetta il traffico tra il browser web e il server potrebbe ottenere i login e le password degli utenti validi.

Punteggio CVSS v2.0 Base

2.6 (CVSS2#AV/AC/Au/C/I/A)

E5 - ICMP Timestamp Request Remote Date Disclosure (Punteggio CVE: 2.1)

Sinossi

È possibile determinare l'ora esatta impostata sul sistema remoto.

Descrizione

Il sistema remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un attaccante di conoscere la data impostata sulla macchina bersaglio, il che può aiutare un attaccante remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.

Mitigazione

Filtrare le richieste di timestamp ICMP e le risposte di timestamp ICMP in uscita.

Rischio

Basso.

Punteggio CVSS v2.0 Base

2.1 (CVSS2#AV/AC/Au/C/I/A)

E6 - Web Server Allows Password Auto-Completion

Sinossi

Il campo 'autocomplete' non è disabilitato sui campi password.

Descrizione

Il server web remoto contiene almeno un campo HTML di tipo 'password' in cui 'autocomplete' non è impostato su 'off'. Sebbene ciò non rappresenti un rischio per il server web stesso, significa che gli utenti che utilizzano i moduli interessati potrebbero avere le loro credenziali salvate nei loro browser, il che potrebbe portare a una perdita di riservatezza se utilizzano un host condiviso o se il loro computer viene compromesso.

Mitigazione

Aggiungere l'attributo 'autocomplete=off' a questi campi per impedire ai browser di memorizzare le credenziali.

Rischio

Basso.

8.2 OPENVAS

E1 - Anonymous FTP Login Reporting (Punteggio CVE: 6.4)

Sinossi
Il server FTP remoto consente accessi anonimi.

Descrizione
È stato possibile effettuare l'accesso al servizio FTP remoto utilizzando i seguenti account anonimi (CVE-1999-0497[3]):

- `anonymous:anonymous@example.com`
- `ftp:anonymous@example.com`

Ecco i contenuti della lista di directory remota per l'account "anonymous":

```
css
Copia codice
-rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak
-rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg
```

E per l'account "ftp":

```
css
Copia codice
-rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak
-rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg
```

Mitigazione
Se non si desidera condividere file, è necessario disabilitare gli accessi anonimi.

Rischio
Medio: Sulla base dei file accessibili tramite questo accesso FTP anonimo e dei permessi di questo account, un attaccante potrebbe:

- Accedere a file sensibili
- Caricare o eliminare file.

E2 - Cleartext Transmission of Sensitive Information via HTTP (Punteggio CVE: 4.8)

Sinossi
L'host/applicazione trasmette informazioni sensibili (username, password) in testo chiaro via HTTP.

Descrizione
Sono stati identificati i seguenti campi di input (URL: nome input):

- http://potato/admin/:password
- http://potato/admin/?D=A:password

Mitigazione
Imporre la trasmissione di dati sensibili tramite una connessione crittografata SSL/TLS. Assicurarsi inoltre che l'host/applicazione reindirizzi tutti gli utenti alla connessione SSL/TLS prima di permettere l'inserimento di dati sensibili nelle funzioni menzionate.

Rischio
Medio: Un attaccante potrebbe utilizzare questa situazione per compromettere o intercettare la comunicazione HTTP tra il client e il server, ottenendo accesso a dati sensibili come nomi utente o password tramite un attacco man-in-the-middle

---

E3 - FTP Unencrypted Cleartext Login (Punteggio CVE: 4.8)

Sinossi

Il server FTP remoto consente accessi non crittografati in testo chiaro.

Descrizione

Il servizio FTP remoto accetta accessi senza inviare prima il comando 'AUTH TLS'. Risposta del server:

- Sessioni non anonime: `331 Password required for openvasvt`
- Sessioni anonime: `331 Anonymous login ok, send your complete email address as your password`

Mitigazione

Abilitare FTPS o imporre la connessione tramite il comando 'AUTH TLS'. Consultare il manuale del servizio FTP per ulteriori informazioni.

Rischio

Medio: Un attaccante può intercettare nomi utente e password sniffando il traffico verso il servizio FTP.

E4 - TCP Timestamps Information Disclosure (Punteggio CVE: 2.6)

Sinossi

L'host remoto implementa i timestamp TCP, permettendo di calcolare il tempo di attività.

Descrizione

È stato rilevato che l'host implementa RFC1323/RFC7323. I seguenti timestamp sono stati recuperati con un intervallo di 1 secondo tra di loro:

- Pacchetto 1: 680131116
- Pacchetto 2: 680132176

Mitigazione

Per disabilitare i timestamp TCP su Linux, aggiungere la linea `net.ipv4.tcp_timestamps=0` a `/etc/sysctl.conf` ed eseguire `sysctl -p` per applicare le impostazioni. Per disabilitare i timestamp TCP su Windows, eseguire `netsh int tcp set global timestamps=disabled`.

Rischio

Basso. Un effetto collaterale di questa funzione è che a volte è possibile calcolare il tempo di attività dell'host remoto.

E5 - Weak MAC Algorithm(s) Supported (SSH) (Punteggio CVE: 2.6)

Sinossi

Il server SSH remoto è configurato per consentire/supportare algoritmi MAC deboli.

Descrizione

Il server SSH remoto supporta i seguenti algoritmi MAC deboli client-to-server:

umac-64-etm@openssh.com

umac-64@openssh.com

Il server SSH remoto supporta i seguenti algoritmi MAC deboli server-to-client:

umac-64-etm@openssh.com

umac-64@openssh.com

Mitigazione

Disabilitare gli algoritmi MAC deboli riportati.

Rischio

Basso: Gli algoritmi MAC deboli includono quelli basati su MD5, algoritmi a 96-bit, algoritmi a 64-bit e l'algoritmo 'none'.

E6 - ICMP Timestamp Reply Information Disclosure (Punteggio CVE: 2.1)

Sinossi

L'host remoto risponde a una richiesta di timestamp ICMP.

Descrizione

Il pacchetto ICMP seguente è stato ricevuto (CVE-1999-0524):

- Tipo ICMP: 14
- Codice ICMP: 0

Mitigazione

Disabilitare il supporto per il timestamp ICMP sull'host remoto o proteggere l'host remoto tramite un firewall, bloccando i pacchetti ICMP in entrambe le direzioni (completamente o solo per le reti non fidate).

Rischio

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

REFERENCES

[1] Macchina target Potato:1:
https://www.vulnhub.com/entry/potato-1,529/

[2] CVE-2023-48795; SSH Terrapin Prefix Truncation Weakness:
https://nvd.nist.gov/vuln/detail/CVE-2023-48795

[3] CVE-1999-0497; Anonymous FTP is enabled:
https://nvd.nist.gov/vuln/detail/CVE-1999-0497

[4] Consultazione vulnerabilità su CVE-DETAILS:
https://www.cvedetails.com/

[5] Consultazione vulnerabilità su Nessus:
https://www.tenable.com/

[6] Consultazione vulnerabilità su Greenbone(OpenVAS):
https://www.greenbone.net/en/