Università degli Studi di Salerno

# Penetration Testing Report

FUNBOX: LUNCHBREAKER

Raffaella Calò mat. 0522501436 | Corso di PTEH | A.A. 2023/2024

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

# Sommario

# Executive Summary

Nell'ambito del progetto del corso di **Penetration Testing and Ethical Hacking**, è stata scelta come target la macchina virtuale ***Funbox: Lunchbreaker*** **[1]**, reperibile sulla piattaforma VulnHub all'indirizzo *https://www.vulnhub.com/entry/funbox-lunchbreaker,700/*.

Non avendo a disposizione alcuna conoscenza riguardo la VM da analizzare, eccezion fatta per il sistema operativo in essa installato, è stato utilizzato un approccio di tipo *grey box testing*. Inoltre, come metodologia di riferimento, si è adoperato il **Framework Generale per il Penetration Testing (FGPT)**.

Le varie attività sono state svolte seguendo l'ideologia di un *white-hat hacker* con l'obiettivo di stabilire il livello di sicurezza dell'asset, scoprendo, verificando e notificando eventuali vulnerabilità presenti al suo interno. Sulla VM in questione sono state individuate 2 vulnerabilità di livello medio e 2 di livello basso.

In questo report sono state riportate tutte le vulnerabilità riscontrate, seguite da un'analisi e una serie di contromisure da adottare per eliminarle o, quantomeno, mitigarle.

# Engagement Highlights

L'attività di Penetration Testing qui riportata è stata svolta nell'ambito di un progetto universitario; non c'è stata, quindi, alcuna interazione con un possibile cliente.

Per quanto riguarda metodologia e strumenti, è stato fornito libero arbitrio così come per le tempistiche di consegna.

L'analisi e l'opportuna documentazione del caso studio *Funbox: Lunchbreaker* sono state svolte seguendo le fasi studiate durante il corso, ovvero:

- Information gatering & Target discovery;
- Enumeration target & Port scanning;
- Vulnerability mapping;
- Exploitation;
- Post-Exploitation.

# Vulnerability Report

Durante l'analisi della macchina target, sono state individuate alcune vulnerabilità in grado di esporre la VM ad attacchi da parte di utenti malevoli.

La data presente sulla macchina target è accessibile a tutti, permettendo anche ad un eventuale hacker di sfruttare questa informazione per superare i protocolli di autenticazione di tipo *time-based*.

È stato scoperto che il server SSH è in grado di supportare algoritmi *weak* (SHA1/MD5/96-bit), i quali metterebbero l'attaccante nella condizione di decifrare la comunicazione e stilare un attacco Man-in-the-Middle.

Le credenziali degli utenti potrebbero essere trasmesse in chiaro; la loro conoscenza da parte dell'attaccante gli consentirebbe di impersonificare il relativo user.

Inoltre, è stato riscontrato che gli utenti, pur non avendo a disposizione dei propri username e password, possono comunque accedere al server FTP con credenziali comuni quali *anonymous* o *ftp*.

# Remediation Report

La macchina virtuale *Funbox: Lunchbreaker* possiede un grado di rischio medio-basso; per poter mitigare le varie vulnerabilità individuate, è possibile adottare le seguenti contromisure:

- Aggiornare il sistema operativo e gli applicativi installati sulla macchina a delle versioni più recenti;
- Disabilitare i login anonimi;
- Effettuare un cambio di server, passando da FTP a SFTP (parte della suite SSH) o a FTPS (FTP su SSL/TSL);
- Disabilitare l'opzione **Timestamp Extension for High Performance**;
- Disabilitare gli algoritmi MAC di tipo *weak;*
- Filtrare le richieste che le risposte ICMP timestamp.

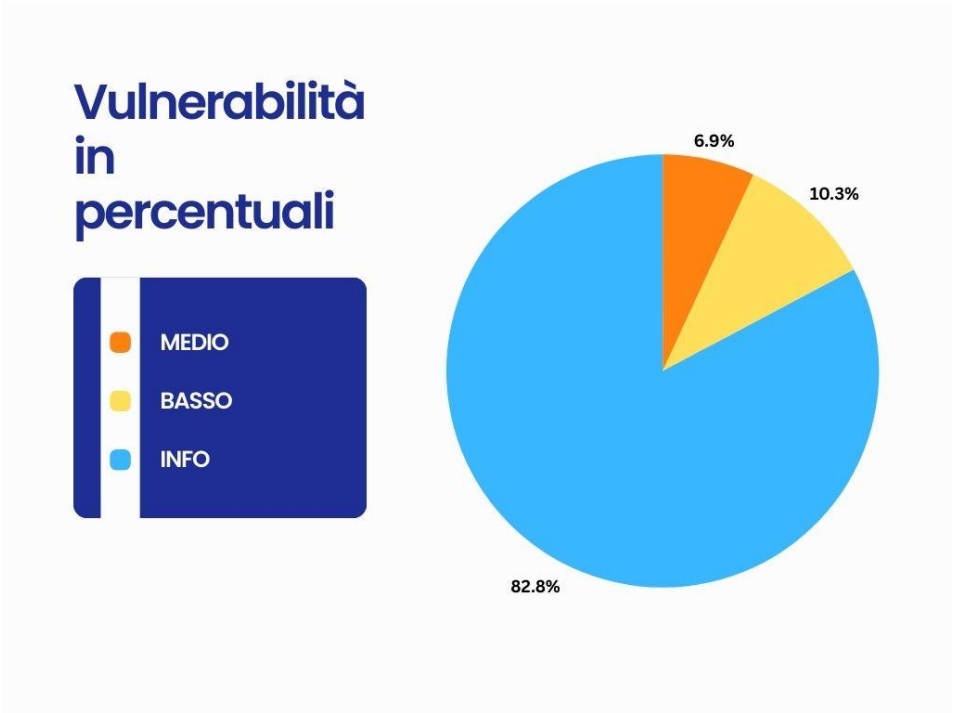
# Findings Summary

Durante l'attività di Penetration Testing, sono state riscontrate diverse vulnerabilità divisibili in base al loro livello di rischio. In particolare, in questo caso sono stati individuati tre diverse *severity:*

- Medio. Vulnerabilità di questo tipo non sono molto semplici da sfruttare che richiedono tecniche di Social engineering o simili; nella maggior parte dei casi non hanno un impatto diretto significativo
- Basso. Queste vulnerabilità mettono a disposizione dell'utente malintenzionato pochissime informazioni e potrebbero non rappresentare una reale minaccia
- Info. Non sono vulnerabilità ma informazioni su configurazioni di software che nel futuro potrebbero generare vulnerabilità.

La seguente tabella mostra il numero di vulnerabilità individuate nella macchina target, raggruppate per livello di minaccia.

| | MEDIO | BASSO | INFO | TOTALE |
|---|---|---|---|---|
| #Vulnerabilità | 2 | 3 | 24 | 29 |



# Detailed Summary

## ICMP Timestamp Reply Information Disclosure

**Summary:**
L'host remoto ha risposto ad una richiesta ICMP timestamp.

**Descrizione:**
Il Timestamp Reply è un messaggio ICMP in risposta ad un messaggio Timestamp. È composto dal timestamp originale inviato dal sender del Timestamp così come da un receive timestamp e un transmit timestamp. Questa informazione potrebbe essere utilizzata per sfruttare generatori deboli di numeri casuali di tipo time-based in altri servizi.

**Soluzione:**
- Disabilitare il supporto per ICMP timestamp sull'host remoto
- Proteggere l'host remoto attraverso un firewall, bloccando il passaggio dei pacchetti ICMP che passano attraverso di esso in entrambe le direzioni

**Rischio:**
Basso

**Riferimenti:**
CVE-1999-0524 [2]

## Weak MAC Algorithm(s) Supported (SSH)

**Summary:**
Il server remoto SSH è configurato per supportare algoritmi MAC deboli.

**Descrizione:**
SSH è configurato per supportare algoritmi MD5 based, 96-bit based e 64-bit based, oltre agli algoritmi 'none'.

**Soluzione:**
Disabilitare gli algoritmi MAC deboli riscontrati.

**Rischio:**
Basso

**Riferimenti:**
https://www.rfc-editor.org/rfc/rfc6668 https://www.rfc-editor.org/rfc/rfc4253#section-6.4

## TCP Timestamps Information Disclosure

**Summary:**
L'host remoto implementa i timestamp TCP e, quindi, permette di computare il tempo di attività.

**Descrizione:**
L'host remoto implementa i timestamp TCP, così come definito da RFC1323/RFC7323. Il periodo di attività dell'host remoto può spesso essere computato.

**Soluzione:**
Per disabilitare i timestamp TCP su Linux bisogna aggiungere la riga 'net.ipv4.tcp_timestamps = 0' al file /etc/sysctl.conf. Successivamente, si esegue 'sysctl -p' per applicare le modifica a runtime.
Per disabilitare i timestamp TCP su Windows si esegue 'netsh int tcp set global timestamps=disabled'. Se si usa Windows Server 2008 e Vista, il timestamp non può essere completamente modificato.

**Rischio:**
Basso

**Riferimenti:**
https://datatracker.ietf.org/doc/html/rfc1323
https://datatracker.ietf.org/doc/html/rfc7323

## FTP Unencrypted Cleartext Login

**Summary:**
L'host remoto sta eseguendo un servizio FTP che permette login cleartext su connessioni non criptate.

**Descrizione:**
L'FTP remoto non crittografa i suoi dati e non controlla le connessioni. Username e password vengono trasmessi in chiaro e potrebbero essere intercettati da un attaccante attraverso un network sniffer o un attacco man-in-the-middle.

**Soluzione:**
Effettua lo switch a FTPS o forza la connessione attraverso il comando 'AUTH TLS'.

**Rischio:**
Medio

**Riferimenti:**
null

## Anonymous FTP Login Reporting

**Summary:**
Il server FTP permette i login anonimi.

**Descrizione:**
Un host che mette a disposizione un servizio FTP potrebbe fornire anche un accesso FTP anonimo; ciò significa che gli utenti non hanno necessariamente bisogno di un account sull'host, ma possono accedervi utilizzando 'anonymous' o 'ftp' come username. In questo caso, un attaccante potrebbe essere in grado di ottenere l'accesso a informazioni sensibili ma anche di caricare o cancellare file.

**Soluzione:**
Disabilitare i login anonimi se non richiesti. Verificare periodicamente il server FTP per avere la certezza che i contenuti sensibili non vengano resi disponibili.

**Rischio:**
Medio

**Riferimenti:**
CVE-1999-0497 [3]

# References

**[1] Funbox:Lunchbreaker** *https://www.vulnhub.com/entry/funbox-lunchbreaker,700/*

**[2] CVE-Details, "Vulnerability details: CVE-1999-0524."** *https://nvd.nist.gov/vuln/detail/CVE-1999-0524*

**[3] CVE-Details, "Vulnerability details: CVE-1999-0497."** *https://nvd.nist.gov/vuln/detail/CVE-1999-0497*