Report Penetration Test

22 Luglio 2025

1. Executive Summary

Questo report riassume i risultati del penetration test condotto sull'infrastruttura aziendale. Sono state identificate diverse vulnerabilità, alcune delle quali critiche, che potrebbero portare a una compromissione completa del sistema. Le vulnerabilità principali includono versioni obsolete di software con backdoor note e configurazioni insicure che espongono il sistema a rischi significativi di esecuzione remota di codice e furto di credenziali.

Riepilogo delle Vulnerabilità

ID	Titolo	Severità	Rischio	CVSS
VULN-001	Obsolete Apache httpd Version with Known Vulnerabilities	Alta	Denial of Service, Cross-Site Scripting (XSS), Remote Code Execution, misconfigurations WebDAV.	8.0
VULN-002	Insecure Telnet Protocol Usage	Media	Intercettazione e furto di credenziali, accesso non autorizzato.	6.0
VULN-003	vsFTPd 2.3.4 Backdoor (Remote Command Execution)	Critica	Esecuzione remota di comandi, compromissione completa del sistema, accesso a dati sensibili.	10.0
VULN-004	Samba smbd 3.0.20-Debian Remote Code Execution and Insecure Configuration	Critica	Esecuzione remota di codice, accesso non autorizzato a condivisioni di rete, compromissione dati.	10.0
VULN-005	Ingreslock Service with Potential Shell Access	Critica	Accesso diretto alla shell, compromissione completa del sistema.	9.8

ID	Titolo	Severità	Rischio	CVSS
VULN-006	UnrealIRCd Backdoor (Remote Command Execution)	Critica	Esecuzione remota di comandi, compromissione completa del sistema.	10.0

2. Reconnaissance

Durante la fase di ricognizione, sono stati identificati i seguenti servizi e le relative versioni, fornendo una panoramica iniziale dell'infrastruttura target:

- **Porta 21 (TCP)**: Servizio FTP, versione vsftpd 2.3.4.
- **Porta 23 (TCP)**: Servizio Telnet, versione Linux telnetd.
- **Porta 80 (TCP)**: Servizio HTTP, versione Apache httpd 2.2.8. Il titolo della pagina web è 'Metasploitable2 - Linux'.
- **Porta 445 (TCP)**: Servizio NetBIOS-SSN, versione Samba smbd 3.0.20-Debian.
- **Porta 1524 (TCP)**: Servizio identificato come ingreslock, versione sconosciuta.
- **Porta 6667 (TCP)**: Servizio IRC, versione UnrealIRCd.

3. Network Scanning

La scansione di rete ha permesso di identificare le porte aperte e i servizi in ascolto sul sistema target, confermando la presenza dei seguenti servizi:

- **Porta 21 (FTP)**: Aperta.
- **Porta 23 (Telnet)**: Aperta.
- **Porta 80 (HTTP)**: Aperta.
- **Porta 445 (SMB/NetBIOS-SSN)**: Aperta.
- **Porta 1524 (Ingreslock)**: Aperta.
- **Porta 6667 (IRC)**: Aperta.

4. Enumeration

La fase di enumerazione ha permesso di raccogliere dettagli specifici sui servizi e le loro configurazioni:

- **Apache httpd 2.2.8**: Versione obsoleta con modulo WebDAV abilitato (DAV/2).
- **Telnet**: Servizio Telnet standard di Linux, trasmette credenziali in chiaro.
- **vsFTPd 2.3.4**: Versione specifica con una backdoor nota.
- **Samba smbd 3.0.20-Debian**: Versione con vulnerabilità critiche, configurato per consentire accesso anonimo e senza firma di sessione.
- **Ingreslock (Porta 1524)**: Il fingerprinting suggerisce la presenza di un prompt di shell, indicando un potenziale accesso diretto.
- **UnrealIRCd**: Versione associata a una backdoor nota.

5. Vulnerability Detection

VULN-001: Obsolete Apache httpd Version with Known Vulnerabilities

Descrizione Tecnica: Il server web Apache httpd, versione 2.2.8, in ascolto sulla porta 80, è una versione obsoleta con molteplici vulnerabilità note. Queste includono potenziali attacchi di denial-of-service, cross-site scripting (XSS) ed esecuzione remota di codice. La presenza di DAV/2 suggerisce inoltre che WebDAV è abilitato, il che può essere una fonte di misconfigurazioni.

Severità: Alta

Rischio: Denial of Service, Cross-Site Scripting (XSS), Remote Code Execution, e potenziali misconfigurazioni dovute a WebDAV.

CVSS Score: 8.0

Evidenze:

```
                Il server web Apache httpd 2.2.8, in ascolto sulla porta 80, è una
versione obsoleta...
                La presenza di DAV/2 suggerisce inoltre che WebDAV è abilitato...
                Server Web: Apache versione 2.2.8, con il modulo WebDAV abilitato.
                Porta 80 (TCP): Servizio HTTP, versione Apache httpd 2.2.8. Il tito
lo della pagina web è 'Metasploitable2 - Linux'.
```

Proof of Concept: Il documento indica che è "sfruttabile", ma non sono dettagliati passaggi specifici o comandi per questa vulnerabilità.

Raccomandazione Tecnica per Mitigazione: Aggiornare Apache httpd alla versione più recente e supportata. Disabilitare o configurare correttamente WebDAV se non strettamente necessario. Implementare un Web Application Firewall (WAF) per mitigare attacchi noti.

Riferimenti: Non esplicitamente forniti (es. CVE specifici per Apache 2.2.8).

VULN-002: Insecure Telnet Protocol Usage

Descrizione Tecnica: Il servizio Telnet, in ascolto sulla porta 23, utilizza un protocollo insicuro che trasmette i dati, incluse le credenziali, in chiaro. Questo lo rende vulnerabile all'intercettazione e al furto di credenziali.

Severità: Media

Rischio: Intercettazione e furto di credenziali, che porta ad accesso non autorizzato.

CVSS Score: 6.0

Evidenze:

```
                Il servizio Telnet, sulla porta 23, utilizza un protocollo insicuro
che trasmette i dati, incluse le credenziali, in chiaro.
                Porta 23 (TCP): Servizio Telnet, versione Linux telnetd.
```

Proof of Concept: Il documento indica che è "sfruttabile", implicando che le credenziali possono essere intercettate, ma non sono dettagliati passaggi specifici o comandi.

Raccomandazione Tecnica per Mitigazione: Disabilitare il servizio Telnet. Utilizzare protocolli sicuri come SSH per l'accesso remoto, che crittografano tutte le comunicazioni, incluse le credenziali.

Riferimenti: Non esplicitamente forniti.

VULN-003: vsFTPd 2.3.4 Backdoor (Remote Command Execution)

Descrizione Tecnica: Il servizio FTP, in ascolto sulla porta 21, sta eseguendo vsFTPd versione 2.3.4, che contiene una backdoor nota che consente l'esecuzione remota di comandi.

Severità: Critica

Rischio: Esecuzione remota di comandi, che porta a una compromissione completa del sistema e accesso a dati sensibili.

CVSS Score: 10.0

Evidenze:

```
                Sul servizio FTP, in ascolto sulla porta 21, è stata rilevata una v
ersione di vsFTPd (2.3.4) contenente una backdoor che permette l'esecuzione remota
di comandi.
                Porta 21 (TCP): Servizio FTP, versione vsftpd 2.3.4.
```

Proof of Concept: Dettagliato nella sezione "Exploitation".

Raccomandazione Tecnica per Mitigazione: Aggiornare vsFTPd alla versione più recente e sicura. Disabilitare il servizio FTP se non è strettamente necessario o limitare l'accesso solo a indirizzi IP autorizzati. Implementare un firewall per limitare l'accesso alla porta 21.

Riferimenti: CVE-2011-2523

VULN-004: Samba smbd 3.0.20-Debian Remote Code Execution and Insecure Configuration

Descrizione Tecnica: Il servizio Samba (smbd 3.0.20-Debian), in ascolto sulla porta 445, presenta vulnerabilità critiche di esecuzione remota di codice. Inoltre, è consentito l'accesso anonimo e non è richiesta la firma della sessione, aumentando significativamente il rischio.

Severità: Critica

Rischio: Esecuzione remota di codice, accesso non autorizzato a condivisioni di rete e potenziale compromissione dei dati a causa dell'accesso anonimo e della mancanza di firma della sessione.

CVSS Score: 10.0

Evidenze:

```
                Il servizio Samba (smbd 3.0.20-Debian), sulla porta 445, presenta v
ulnerabilità critiche di esecuzione remota di codice.
                Inoltre, è consentito l'accesso anonimo e non è richiesta la firma
della sessione, aumentando significativamente il rischio.
                Porta 445 (TCP): Servizio NetBIOS-SSN, versione Samba smbd 3.0.20-D
ebian.
```

Proof of Concept: Il documento indica che è "sfruttabile", ma non sono dettagliati passaggi specifici o comandi per questa vulnerabilità.

Raccomandazione Tecnica per Mitigazione: Aggiornare Samba alla versione più recente e sicura. Disabilitare l'accesso anonimo. Abilitare la firma della sessione (session signing) per tutte le connessioni. Limitare l'accesso alle condivisioni di rete solo agli utenti e ai gruppi autorizzati.

Riferimenti: Non esplicitamente forniti.

VULN-005: Ingreslock Service with Potential Shell Access

Descrizione Tecnica: Un servizio identificato come "ingreslock" è in esecuzione sulla porta 1524, con potenziale accesso diretto alla shell. Questa è una vulnerabilità critica che indica una possibile misconfigurazione o una backdoor.

Severità: Critica

Rischio: Accesso diretto alla shell, che porta a una compromissione completa del sistema.

CVSS Score: 9.8

Evidenze:

```
                Sulla porta 1524 è stato identificato un servizio "ingreslock" con
potenziale accesso alla shell.
                Questa è una vulnerabilità critica che indica una possibile configu
razione errata o una backdoor, ed è sfruttabile.
```

```
                Porta 1524 (TCP): Servizio identificato come ingreslock, ma la vers
ione è sconosciuta. È importante notare che le stringhe di fingerprint suggeriscono
la presenza di un prompt di shell, indicando un potenziale accesso diretto.
```

Proof of Concept: Il documento indica che è "sfruttabile", ma non sono dettagliati passaggi specifici o comandi per questa vulnerabilità.

Raccomandazione Tecnica per Mitigazione: Identificare e disabilitare il servizio `ingreslock` sulla porta 1524 se non è un servizio legittimo e necessario. Se è legittimo, assicurarsi che non offra accesso diretto alla shell e che sia adeguatamente autenticato e autorizzato. Implementare regole di firewall per bloccare l'accesso a questa porta dall'esterno.

Riferimenti: Non esplicitamente forniti.

VULN-006: UnrealIRCd Backdoor (Remote Command Execution)

Descrizione Tecnica: Il servizio IRC, in ascolto sulla porta 6667, è associato a una versione di UnrealIRCd che contiene una backdoor che consente l'esecuzione remota di comandi.

Severità: Critica

Rischio: Esecuzione remota di comandi, che porta a una compromissione completa del sistema.

CVSS Score: 10.0

Evidenze:

```
                Il servizio IRC, sulla porta 6667, è associato a una versione di Un
realIRCd che contiene una backdoor per l'esecuzione remota di comandi.
                Porta 6667 (TCP): Servizio IRC, versione UnrealIRCd.
```

Proof of Concept: Il documento indica che è "sfruttabile", ma non sono dettagliati passaggi specifici o comandi per questa vulnerabilità.

Raccomandazione Tecnica per Mitigazione: Aggiornare UnrealIRCd alla versione più recente e sicura. Disabilitare il servizio IRC se non è strettamente necessario o limitare l'accesso solo a indirizzi IP autorizzati. Implementare un firewall per limitare l'accesso alla porta 6667.

Riferimenti: Non esplicitamente forniti.

6. Exploitation

Durante la fase di exploitation, è stata eseguita con successo la seguente compromissione:

VULN-003: vsFTPd 2.3.4 Backdoor (Remote Command Execution)

Metodologia: L'exploit è stato eseguito con successo sfruttando la backdoor presente nella versione 2.3.4 di vsFTPd, identificata come CVE-2011-2523.

Strumento Utilizzato: Metasploit Framework.

Outcome: È stato ottenuto un accesso immediato alla shell con privilegi di root, senza la necessità di ulteriori escalation di privilegi. Il sistema è stato compromesso, confermando l'accesso alle credenziali di sistema e ai file utente.

Dettagli Post-Exploitation:

- **Persistenza:** È stata stabilita la persistenza aggiungendo un nuovo utente ('backdooruser' con password 'password123').
- **Raccolta Dati:** Sono stati raccolti e simulati l'esfiltrazione di dati sensibili, inclusi:
  - Contenuto di `/etc/shadow` (hash delle password).
  - Versione del kernel: `5.15.0-113-generic`.
  - Contenuto della directory `/home`.
- **Pulizia Log:** I log relativi all'attività (`/var/log/vsftpd.log` e log generali) sono stati puliti per coprire le tracce.

Comandi Eseguiti (Esempio):

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS [TARGET_IP]
exploit
# Una volta ottenuta la shell:
whoami
cat /etc/shadow
uname -a
ls -la /home
history -c && echo > /var/log/vsftpd.log && echo > /var/log/auth.log
```

7. Recommendations

Di seguito sono riportate le raccomandazioni tecniche dettagliate per mitigare le vulnerabilità identificate e migliorare la postura di sicurezza complessiva del sistema:

- **Aggiornamento Software:** Aggiornare tutti i servizi e i sistemi operativi alla versione più recente e supportata. Questo include Apache httpd, vsFTPd, Samba e UnrealIRCd. Gli aggiornamenti spesso contengono patch per vulnerabilità note.
- **Disabilitazione Servizi Non Necessari:** Disabilitare i servizi non essenziali, come Telnet e IRC, se non sono strettamente richiesti per le operazioni aziendali. Meno servizi esposti significano meno superfici di attacco.
- **Sostituzione Protocolli Insecure:** Sostituire l'uso di protocolli insicuri come Telnet con alternative crittografate come SSH per l'accesso remoto e SFTP/FTPS per il trasferimento di file.
- **Hardening delle Configurazioni:**
    - **Samba:** Disabilitare l'accesso anonimo e abilitare la firma della sessione (session signing) per prevenire attacchi man-in-the-middle e garantire l'integrità delle comunicazioni. Limitare l'accesso alle condivisioni di rete solo agli utenti e ai gruppi autorizzati.
    - **Apache httpd:** Disabilitare il modulo WebDAV se non è strettamente necessario. Se WebDAV è richiesto, configurarlo con autenticazione robusta e autorizzazioni granulari.
    - **Ingreslock (Porta 1524):** Indagare l'origine del servizio "ingreslock". Se non è un servizio legittimo, disabilitarlo immediatamente. Se è legittimo, assicurarsi che non offra accesso diretto alla shell e che sia adeguatamente protetto con autenticazione e autorizzazione.
- **Implementazione Firewall:** Configurare regole di firewall per limitare l'accesso alle porte dei servizi solo dagli indirizzi IP e dalle reti autorizzate. Questo riduce l'esposizione a potenziali attaccanti esterni.
- **Monitoraggio e Logging:** Implementare un robusto sistema di monitoraggio e logging per rilevare attività sospette e anomalie. Assicurarsi che i log siano centralizzati, protetti da manomissioni e regolarmente revisionati.
- **Gestione delle Patch:** Stabilire un processo rigoroso di gestione delle patch per garantire che tutti i sistemi e le applicazioni siano tempestivamente aggiornati con le ultime patch di sicurezza.
- **Principio del Minimo Privilegio:** Assicurarsi che tutti i servizi e gli utenti operino con il minimo privilegio necessario per svolgere le loro funzioni.