Security Assessment Report

Analisi delle Debolezze di Autenticazione su Servizi SSH e FTP

Ardelean Pop Catalin
Master in Cyber Security Specialist – Epicode

16 gennaio 2026

Indice

Executive Summary

Il presente report documenta un'attività di Security Assessment svolta su un singolo sistema Linux in ambiente di laboratorio controllato. L'obiettivo dell'analisi è stato valutare la robustezza dei meccanismi di autenticazione dei servizi SSH e FTP.

Durante il test sono state individuate vulnerabilità legate all'utilizzo di password deboli, all'assenza di adeguati controlli contro attacchi a dizionario e al riutilizzo delle stesse credenziali su più servizi esposti. Attraverso l'utilizzo dello strumento Hydra è stato possibile individuare credenziali valide e dimostrare la possibilità di accessi non autorizzati.

1 Scope e Contesto

Le attività descritte sono state eseguite esclusivamente su un sistema di laboratorio autorizzato e configurato a scopo didattico. Il test è stato condotto interamente sulla stessa macchina, utilizzata sia come sistema target sia come ambiente di test.

Non sono stati coinvolti sistemi di produzione o infrastrutture di terze parti.

2 Ambiente di Test

L'ambiente utilizzato per il test presenta le seguenti caratteristiche:

- Sistema Operativo: Kali Linux
- Kernel: Linux 6.12.x
- Indirizzo IP locale: 192.168.50.100

I servizi analizzati durante l'attività sono:

- SSH – OpenSSH 10.0p2 (22/TCP)
- FTP – vsFTPd 3.0.5 (21/TCP)

3 Preparazione dell'Ambiente

Per simulare uno scenario realistico di autenticazione vulnerabile, è stato creato un utente dedicato al testing, al quale è stata assegnata una password debole, "testpass", successivamente utilizzata durante le attività di test.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

Figura 1: Creazione nuovo utente di test

Il servizio SSH è stato avviato manualmente:

```
sudo service ssh start
```

4 Verifica dell'Accesso Legittimo

Prima di eseguire qualsiasi test offensivo, è stato verificato il corretto funzionamento del servizio SSH mediante accesso legittimo.

Al primo tentativo è stata accettata la chiave host del sistema e l'accesso è avvenuto correttamente, confermando la validità delle credenziali.

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:VqetCngv6qBu5iWbA/WIsBjx5RGMlSmnQb717naOkEU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) x86_64
```

Figura 2: Accesso legittimo al servizio SSH

5 Installazione degli Strumenti

Per l'esecuzione degli attacchi a dizionario è stato installato il pacchetto SecLists e le wordlist fornite sono state utilizzate come base per la creazione di liste personalizzate.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1352
  Download size: 545 MB
  Space needed: 1,935 MB / 51.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
Ign:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
Fetched 415 MB in 1min 5s (6,390 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 420995 files and directories currently installed.)
Preparing to unpack .../seclists_2025.3-0kali1_all.deb ...
Unpacking seclists (2025.3-0kali1) ...
Setting up seclists (2025.3-0kali1) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for wordlists (2023.2.0) ...
```

Figura 3: Installazione del pacchetto SecLists

6 Preparazione delle Wordlist

Per l'esecuzione degli attacchi a dizionario è stata utilizzata la collezione di wordlist **SecLists**, considerata uno standard di riferimento nel contesto delle attività di security testing.

A partire dalla wordlist contenente milioni di possibili nomi utente, è stata effettuata un'operazione di filtraggio per individuare esclusivamente voci contenenti il pattern `test`. Questa scelta è stata effettuata per simulare uno scenario realistico in cui account di test o di servizio presentano denominazioni facilmente individuabili.

```
┌──(kali㉿kali)-[/]
└─$ sudo cat usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > home/kali/xato-usernames.txt
[sudo] password for kali:
```

Figura 4: Estrazione dei potenziali nomi utente dalla wordlist SecLists

Il processo di filtraggio ha permesso di ridurre significativamente la dimensione della wordlist originale, limitando il numero di tentativi e rendendo l'attacco più mirato ed efficiente.

In modo analogo, è stata creata una wordlist contenente possibili password, selezionando esclusivamente le voci che includono il pattern `test`. Questa operazione riflette uno scenario comune in cui password deboli o di test vengono utilizzate durante fasi di configurazione o sviluppo.

Figura 5: Creazione della wordlist di password filtrata

Successivamente, entrambe le wordlist sono state ulteriormente analizzate e ridotte, al fine di eliminare voci non rilevanti e contenere il numero complessivo di combinazioni testate. Questa fase ha consentito di migliorare l'efficienza del test, riducendo il rumore e minimizzando i falsi negativi durante l'esecuzione degli attacchi a dizionario.

7 Enumerazione dei Servizi

È stata eseguita una scansione dei servizi attivi per confermare l'esposizione delle porte. La scansione ha confermato la presenza del servizio SSH; successivamente è stato verificato anche il servizio FTP.

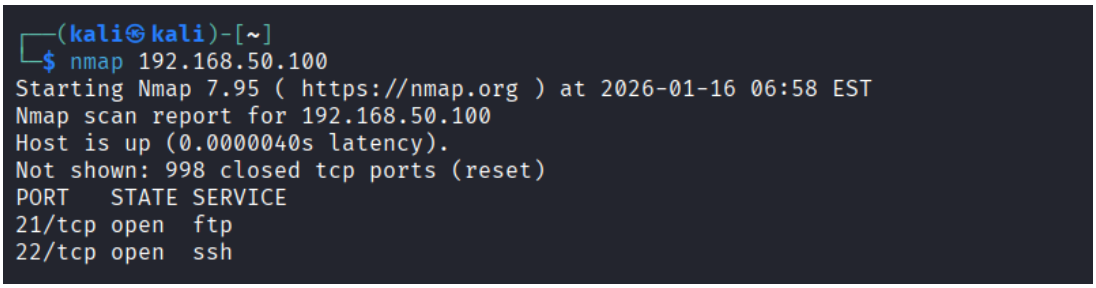

Figura 6: Scansione delle porte con Nmap

8 Attacco a Dizionario su SSH

L'attacco a dizionario contro il servizio SSH è stato condotto utilizzando lo strumento **Hydra**, con l'obiettivo di valutare la resistenza del meccanismo di autenticazione password-based.

L'attività è stata inizialmente eseguita utilizzando un numero elevato di tentativi e differenti livelli di parallelizzazione, al fine di osservare il comportamento del servizio sotto carico. Durante le prime esecuzioni, l'utilizzo di un numero elevato di task paralleli ha causato errori di connessione e l'interruzione dei processi di attacco, indicando la presenza di limiti tecnici nella gestione delle connessioni SSH.

A seguito di queste osservazioni, i parametri di esecuzione sono stati adattati riducendo progressivamente il numero di task paralleli. Questa modifica ha consentito di stabilizzare la comunicazione con il servizio e di proseguire il test in modo controllato e riproducibile.

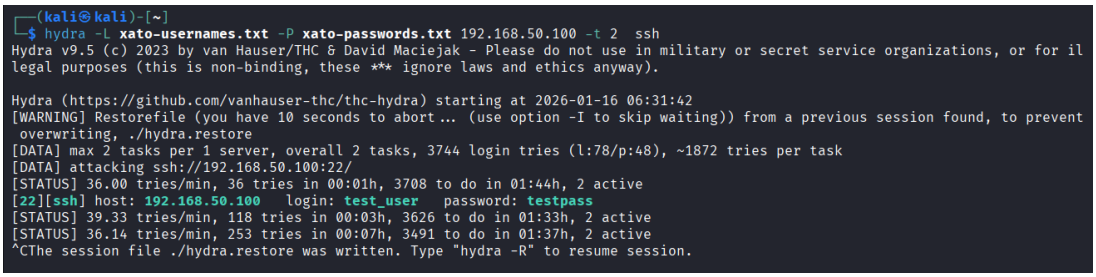

Figura 7: Esecuzione dell'attacco a dizionario con Hydra sul servizio SSH

Con l'utilizzo di una parallelizzazione ridotta, Hydra è riuscito a individuare una coppia di credenziali valide. Il risultato conferma che il servizio SSH consente un numero sufficiente di tentativi di autenticazione falliti senza attivare meccanismi di protezione efficaci, come il blocco dell'account o il rate limiting avanzato.

L'esito dell'attacco dimostra che, in presenza di password deboli e di configurazioni non adeguatamente protette, un attaccante potrebbe ottenere accesso remoto non autorizzato al sistema.

9 Installazione e Test del Servizio FTP

Per ampliare la superficie di analisi e valutare il comportamento di un ulteriore servizio di rete, è stato installato il servizio FTP utilizzando il demone **vsFTPd**.

L'installazione del servizio è stata eseguita manualmente tramite il gestore di pacchetti del sistema e il servizio è stato successivamente avviato per consentire le connessioni in ingresso.

Una volta avviato il servizio, è stata effettuata una verifica manuale dell'accesso FTP, utilizzando le stesse credenziali dell'utente di sistema creato in precedenza. L'accesso è risultato possibile, confermando che il servizio FTP utilizza le credenziali dell'utente locale senza ulteriori meccanismi di protezione o segregazione.

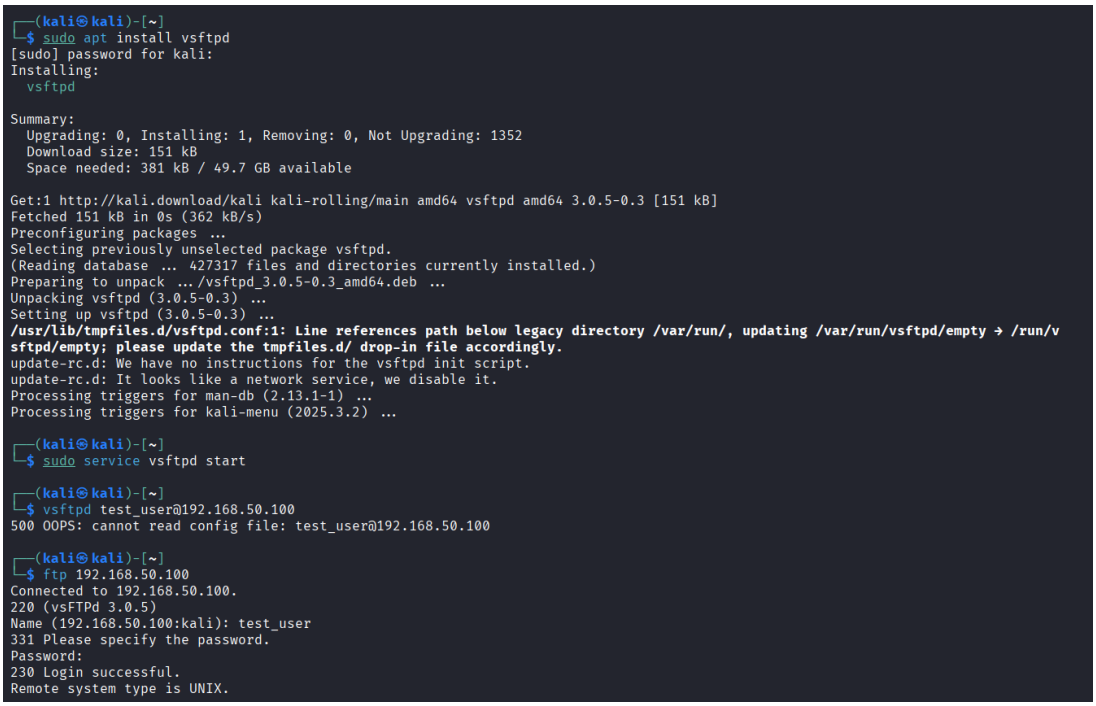

Figura 8: Verifica dell'accesso FTP con credenziali valide

Questa configurazione evidenzia come l'esposizione di più servizi basati sulle stesse credenziali possa aumentare significativamente la superficie di attacco del sistema.

10 Attacco a Dizionario su FTP

A seguito della verifica dell'accesso legittimo, l'attacco a dizionario è stato replicato sul servizio FTP utilizzando lo strumento Hydra e le stesse wordlist preparate in precedenza.

L'obiettivo del test è stato valutare se il servizio FTP presentasse le medesime debolezze di autenticazione già osservate sul servizio SSH.

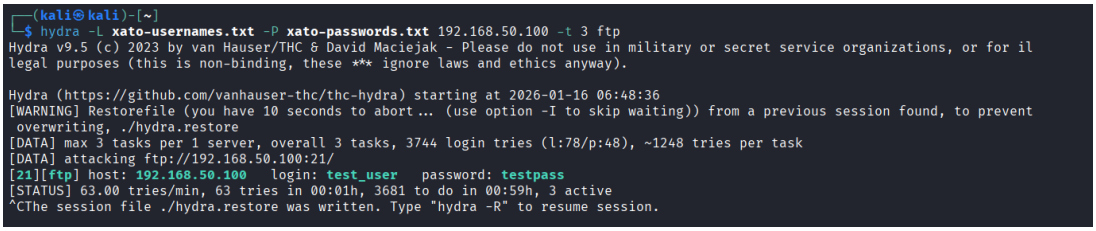

Figura 9: Esecuzione dell'attacco a dizionario con Hydra sul servizio FTP

Anche in questo caso, Hydra è riuscito a individuare una coppia di credenziali valide. L'esito del test conferma che il servizio FTP consente un numero sufficiente di tentativi di autenticazione falliti senza attivare meccanismi di protezione efficaci.

11 Password Reuse

È stato riscontrato il riutilizzo delle stesse credenziali per l'accesso ai servizi SSH e FTP. Questa configurazione incrementa significativamente il rischio complessivo, poiché la compromissione di un singolo servizio consente l'accesso immediato ad altri servizi esposti.

12 Raccomandazioni

Sulla base delle evidenze raccolte durante l'attività di Security Assessment, si raccomanda l'adozione delle seguenti misure correttive al fine di ridurre il rischio di accessi non autorizzati e migliorare la postura di sicurezza complessiva del sistema.

- Disabilitare l'autenticazione basata su password per il servizio SSH, privilegiando l'utilizzo di chiavi crittografiche e limitando l'accesso agli utenti strettamente necessari.
- Implementare policy di gestione delle credenziali che prevedano l'utilizzo di password robuste, uniche per ciascun servizio e soggette a rotazione periodica.
- Abilitare meccanismi di protezione contro attacchi a forza bruta, come il rate limiting, il blocco temporaneo degli account e l'utilizzo di strumenti quali `fail2ban`.
- Evitare il riutilizzo delle stesse credenziali su servizi differenti, riducendo l'impatto di una possibile compromissione di un singolo servizio.
- Limitare l'esposizione dei servizi di rete non strettamente necessari e monitorare costantemente i tentativi di autenticazione sospetti tramite log e sistemi di alerting.

13 Conclusioni

L'attività di Security Assessment ha evidenziato come configurazioni di autenticazione deboli e l'assenza di adeguati controlli di sicurezza possano rendere un sistema vulnerabile ad attacchi di tipo dictionary attack, anche in ambienti di laboratorio o contesti apparentemente controllati.

I test condotti hanno dimostrato che il riutilizzo delle stesse credenziali su più servizi esposti amplifica significativamente il rischio complessivo, consentendo a un attaccante di ottenere accesso remoto non autorizzato con un impatto elevato.

L'adozione delle contromisure suggerite rappresenta un passo fondamentale per rafforzare la sicurezza del sistema, ridurre la superficie di attacco e prevenire compromissioni future. Questo assessment conferma l'importanza di integrare pratiche di hardening e monitoraggio continuo come parte integrante della gestione della sicurezza dei sistemi.