INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: l' esercizio analizza il comportamento di un servizio di rete esposto quando viene configurato con credenziali deboli e facilmente prevedibili.
Attraverso l'attivazione e la pubblicazione di un servizio di accesso remoto e di trasferimento file, viene osservato come un sistema correttamente funzionante possa diventare vulnerabile esclusivamente a causa della scelta delle credenziali di autenticazione.
L'attività mette in evidenza il rapporto diretto tra configurazione del servizio, qualità delle credenziali e livello reale di protezione dell'accesso.

OBIETTIVO: dimostrare in modo operativo che un servizio autenticato, pur essendo tecnicamente funzionante e correttamente avviato, può essere compromesso quando utilizza username e password presenti in dizionari comuni.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
     Active: active (running) since Mon 2026-01-12 10:46:44 EST; 9min ago
 Invocation: 73adcab1891f4448a99bacc61ea8abd3
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 774 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 781 (sshd)
      Tasks: 1 (limit: 13518)
     Memory: 4.8M (peak: 25.2M)
        CPU: 412ms
     CGroup: /system.slice/ssh.service
             └─781 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 12 10:49:00 kali sshd-session[2172]: Failed password for test from 192.168.50.100 port 55886 ssh2
Jan 12 10:49:36 kali sshd-session[2172]: pam_winbind(sshd:auth): getting password (0x00000388)
Jan 12 10:49:36 kali sshd-session[2172]: pam_winbind(sshd:auth): pam_get_item returned a password
Jan 12 10:49:36 kali sshd-session[2172]: pam_winbind(sshd:auth): request wbcLogonUser failed: WBC_ERR_WINBIND_NOT_AVAILABLE, PAM error: PAM_AUTHINFO_UNAVAIL (9)!
Jan 12 10:49:36 kali sshd-session[2172]: pam_winbind(sshd:auth): internal module error (retval = PAM_AUTHINFO_UNAVAIL(9), user = 'test')
Jan 12 10:49:38 kali sshd-session[2172]: Failed password for test from 192.168.50.100 port 55886 ssh2
Jan 12 10:49:39 kali sshd-session[2172]: Connection closed by authenticating user test 192.168.50.100 port 55886 [preauth]
Jan 12 10:49:39 kali sshd-session[2172]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.100  user=test
Jan 12 10:50:16 kali sshd-session[2952]: Accepted password for test from 192.168.50.100 port 52404 ssh2
Jan 12 10:50:16 kali sshd-session[2952]: pam_unix(sshd:session): session opened for user test(uid=1001) by test(uid=0)

┌──(kali㉿kali)-[~]
└─$ ssh test@192.168.50.100

test@192.168.50.100's password:
Linux kali 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 12 10:50:16 2026 from 192.168.50.100
┌──(test㉿kali)-[~]
└─$
```

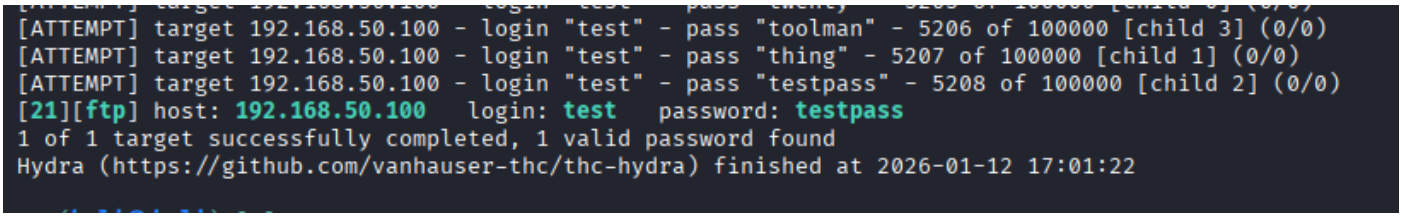
Il laboratorio è iniziato con l'attivazione del servizio di accesso remoto basato su SSH, configurato per accettare connessioni in ingresso tramite autenticazione a password.
Una volta avviato il demone di servizio, ne è stato verificato il corretto funzionamento controllando che fosse effettivamente in esecuzione e in ascolto sulle interfacce di rete del sistema.
La presenza di tentativi di autenticazione registrati e, successivamente, di un accesso riuscito ha confermato che il servizio era operativo e raggiungibile.
A questo punto è stata stabilita una connessione interattiva utilizzando l'utente creato appositamente per l'esercizio. L'accesso riuscito ha dimostrato che il meccanismo di autenticazione basato su username e password era correttamente configurato e funzionante.

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

┌──(kali㉿kali)-[~]
└─$ ls /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt
/usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt

┌──(kali㉿kali)-[~]
└─$
```

Successivamente è stata verificata la disponibilità delle liste di credenziali utilizzate per l'analisi.
In questa fase il sistema è stato controllato per assicurarsi che i dizionari di username e password previsti dall'esercizio fossero presenti e accessibili nei percorsi di sistema; la presenza dei file contenenti gli elenchi di nomi utente e password comuni ha garantito che le successive prove di autenticazione sarebbero state eseguite utilizzando un insieme di credenziali ampio e realistico, rappresentativo di quelle tipicamente impiegate in ambienti operativi.
Questo passaggio ha consentito di allineare l'attività alle condizioni previste dall'esercizio, assicurando che i tentativi di accesso fossero basati su dati effettivi e non su valori inseriti manualmente, rendendo così l'analisi della resistenza del servizio coerente e riproducibile.



Il processo di verifica è stato avviato eseguendo un comando che ha istruito il sistema a utilizzare un elenco di password comuni per tentare l'accesso all'account **test** sul servizio di trasferimento file attivo sull'indirizzo configurato.
Attraverso questo comando, è stato indicato il dizionario da cui prelevare le possibili password e l'endpoint di rete verso cui indirizzare i tentativi di autenticazione, consentendo l'esecuzione di più prove in parallelo per accelerare l'analisi.
Una volta avviato, il sistema ha iniziato a inviare in modo automatico una sequenza di richieste di login, ognuna contenente una diversa password estratta dal dizionario, simulando migliaia di tentativi di accesso reali.
Ogni risposta del servizio è stata valutata per determinare se l'autenticazione fosse stata accettata o rifiutata, fino a quando una combinazione ha prodotto un esito positivo; il processo si è concluso nel momento in cui è stata individuata la coppia di credenziali valida, corrispondente all'utente **test** e alla password **testpass**, dimostrando che il servizio era configurato con una password presente in elenchi di uso comune e quindi facilmente individuabile.

CONCLUSIONE

L’esercizio ha dimostrato in modo concreto come un servizio di rete, pur essendo correttamente installato e operativo, possa risultare vulnerabile quando viene configurato con credenziali semplici e facilmente prevedibili.
L’attivazione dei servizi e la successiva esposizione dell’autenticazione hanno permesso di osservare come un insieme di password comunemente utilizzate sia sufficiente a individuare un accesso valido in tempi contenuti, rendendo il sistema effettivamente compromettibile.
L’ottenimento delle credenziali corrette e la verifica dell’accesso hanno evidenziato che la sicurezza di un servizio non dipende solo dal suo funzionamento tecnico, ma in larga parte dalla qualità delle credenziali con cui viene protetto. In questo contesto, l’esercizio ha messo in luce l’importanza di configurazioni di autenticazione robuste e non standard, poiché anche un servizio stabile e regolarmente avviato può essere esposto a rischi significativi se le credenziali utilizzate rientrano in insiemi facilmente individuabili.