REPORT TECNICO S6/L5: AUTHENTICATION CRACKING

1. Informazioni Generali

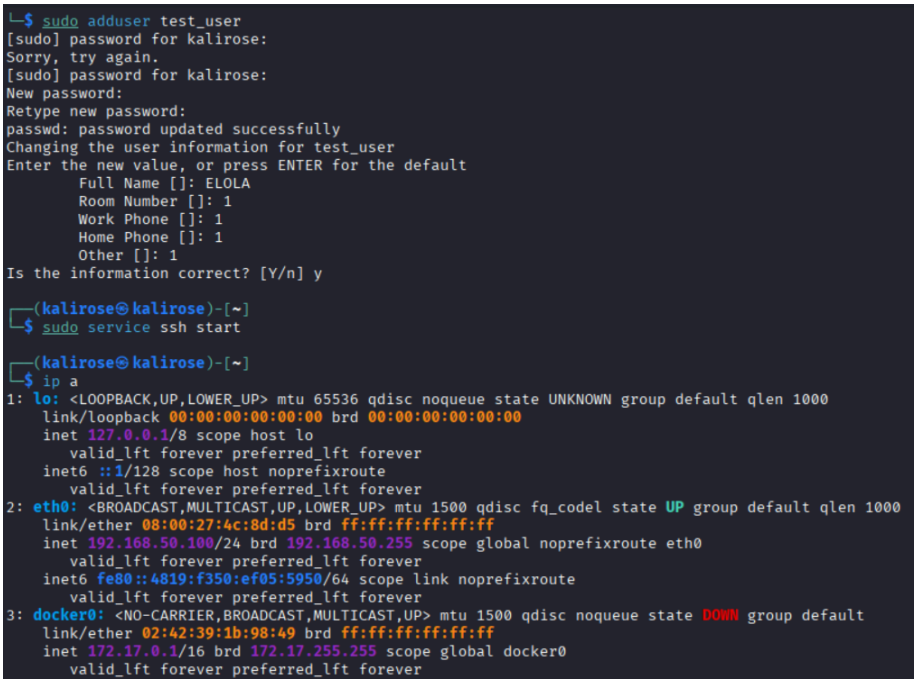
- **Studente:** Victor Rosati
- **Data:** 16 Gennaio 2026
- **Obiettivo:** Effettuare un test di sicurezza sulle procedure di autenticazione dei servizi SSH e FTP della macchina target.
- **Target IP:** `192.168.50.100`.

---

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.



---

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**.

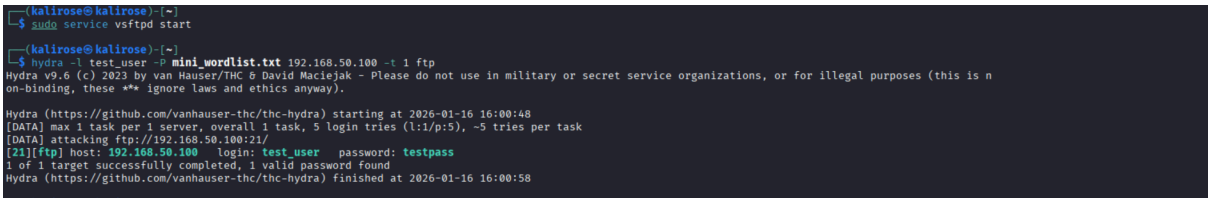
- **Comando utilizzato:** `hydra -l test_user -P mini_wordlist.txt 192.168.50.100 -t 1 ssh`.
- **Risultato:** Le credenziali sono state identificate con successo in meno di 15 secondi.
- **Severità: CRITICAL** (CVSS v3.0: 9.8).

---

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).



---

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.