1. Introduzione

Il presente report documenta le attività di configurazione, messa in sicurezza e successivo auditing offensivo condotte su servizi di rete essenziali. L'obiettivo primario è stato analizzare la resilienza dei protocolli **SSH** e **FTP** contro attacchi di forza bruta (Dictionary Attack).

Le attività sono state suddivise in due fasi operative:

1. **Fase 1:** Configurazione del demone SSH e compromissione tramite Hydra (esercizio guidato).
2. **Fase 2:** Implementazione del servizio FTP e reiterazione dell'attacco per verifica trasversale.

I test hanno evidenziato criticità critiche legate alla gestione delle credenziali utente, confermando la vulnerabilità dei servizi standard di fronte all'utilizzo di password deboli presenti in wordlist pubbliche.

---

2. Fase 1: Analisi del Servizio SSH (Secure Shell)

La prima fase ha riguardato la predisposizione del servizio SSH, standard de facto per l'amministrazione remota sicura, e il successivo tentativo di intrusione.

2.1 Configurazione del Target

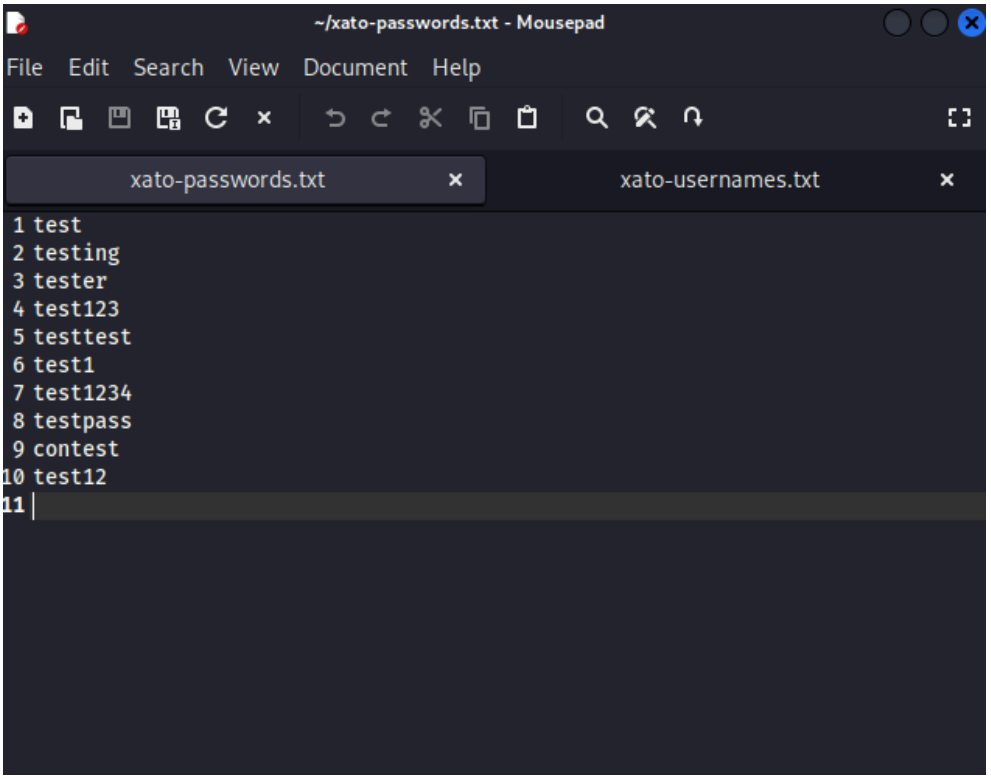
Per simulare uno scenario realistico, è stato creato un account utente dedicato sulla macchina target:

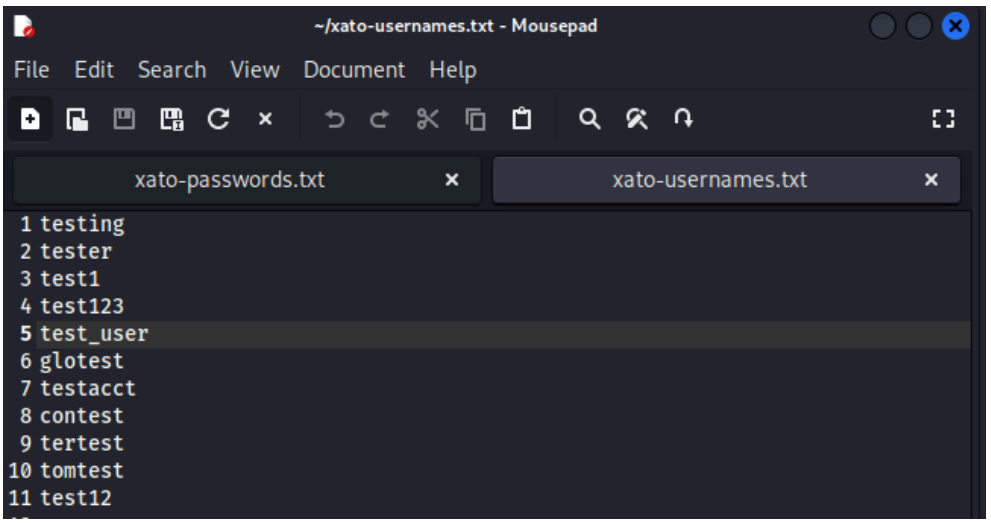
- **Utente:** `test_user`
- **Password:** `testpass` (deliberatamente debole per fini didattici).
- **Gestione Servizio:** Il demone SSH è stato avviato tramite il comando `sudo service ssh start`.
- **Verifica:** È stata testata la connettività tramite `ssh test_user@192.168.50.11`, confermando l'operatività sulla porta TCP/22.

2.2 Esecuzione dell'Attacco (Hydra)

È stato condotto un attacco a dizionario utilizzando il tool **Hydra**, configurato per testare liste multiple di username e password.

Per motivi di tempo e praticità, le liste sono state ridotte come segue:



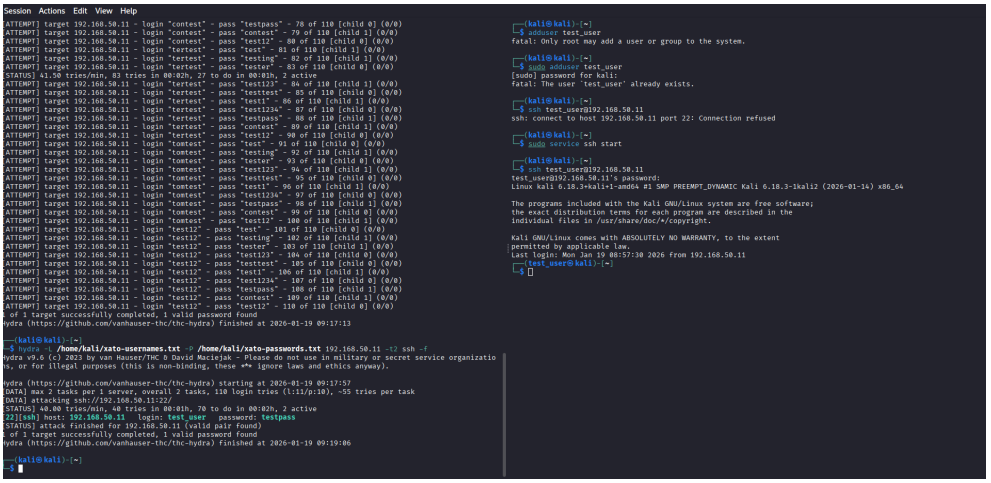


Comando eseguito:

hydra -L /home/kali/xato-usernames.txt -P /home/kali/xato-passwords.txt 192.168.50.11 -t2 ssh -f

Analisi tecnica dei parametri:

- `192.168.50.11`: Indirizzo IP del target identificato.
- `-L / -P`: Utilizzo di liste massive (SecLists) invece di singoli input, simulando una condizione "Blackbox".
- `-t2`: Limitazione a 2 thread paralleli per mantenere la stabilità della connessione SSH.
- `-f`: Interruzione immediata al rilevamento della prima credenziale valida.



- **Credenziali recuperate:** Login: `test_user` / Password: `testpass`.
- **Tasso di successo:** 1 target completato su 1.

---

3. Fase 2: Analisi del Servizio FTP (File Transfer Protocol)

In conformità con le specifiche di progetto per la "Fase 2", è stato selezionato un servizio addizionale per verificare se le vulnerabilità identificate fossero replicabili su protocolli differenti.

3.1 Configurazione del Servizio FTP

È stato scelto il servizio **vsftpd** (Very Secure FTP Daemon).

Procedure di Provisioning:

1. Installazione del pacchetto: `sudo apt install vsftpd`.
2. Avvio del servizio: `sudo service vsftpd start`.

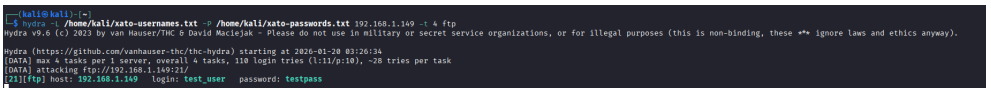
3. Verifica Socket: Conferma dell'ascolto sulla porta TCP/21.

3.2 Reiterazione dell'Attacco

Utilizzando la medesima metodologia della Fase 1, Hydra è stato riconfigurato per targettizzare il protocollo FTP.

Comando eseguito:

hydra -L /home/kali/xato-usernames.txt -P /home/kali/xato-passwords.txt 192.168.50.11 -t 4 ftp



Risultato: Nonostante il cambio di protocollo, l'utilizzo delle medesime credenziali di sistema (`test_user`/`testpass`) ha permesso a Hydra di violare l'accesso FTP in tempi ridotti (< 2 minuti), sfruttando le stesse wordlist utilizzate per SSH.

---

4. Valutazione dei Rischi e Contromisure

L'esercitazione ha dimostrato che la robustezza crittografica di un protocollo (come SSH) è vanificata dall'utilizzo di credenziali deboli.

4.1 Vulnerabilità Identificate

- **Weak Passwords:** La password `testpass` è presente nelle wordlist più comuni (Top 1000 common passwords).
- **Credential Reuse:** La compromissione dell'account di sistema ha esposto simultaneamente sia il servizio SSH che FTP.
- **Configurazione Default:** I servizi sono stati lasciati con configurazioni standard che permettono tentativi di login illimitati o poco controllati.

---

5. Conclusioni

L'attività ha raggiunto pienamente gli scopi didattici prefissati: prendere confidenza con la configurazione dei servizi di rete e dimostrare praticamente l'efficacia degli attacchi a dizionario. Si certifica che il sistema target è stato ripristinato e i servizi di test disattivati al termine della sessione.