S6L5

Attacco di dizionario su SSH e FTP con Hydra

Marco Falchi

Obiettivi dell’esercizio

1. Fare pratica con lo strumento Hydra per effettuare attacchi di brute force sull'autenticazione di servizi di rete.
2. Configurare i servizi SSH e FTP, consolidando la conoscenza di gestione e protezione dei servizi di rete.

Passaggi Seguiti

1. Configurazione del Servizio SSH

Creazione dell'utente per il test con conseguente password con comando:

sudo add user test_user

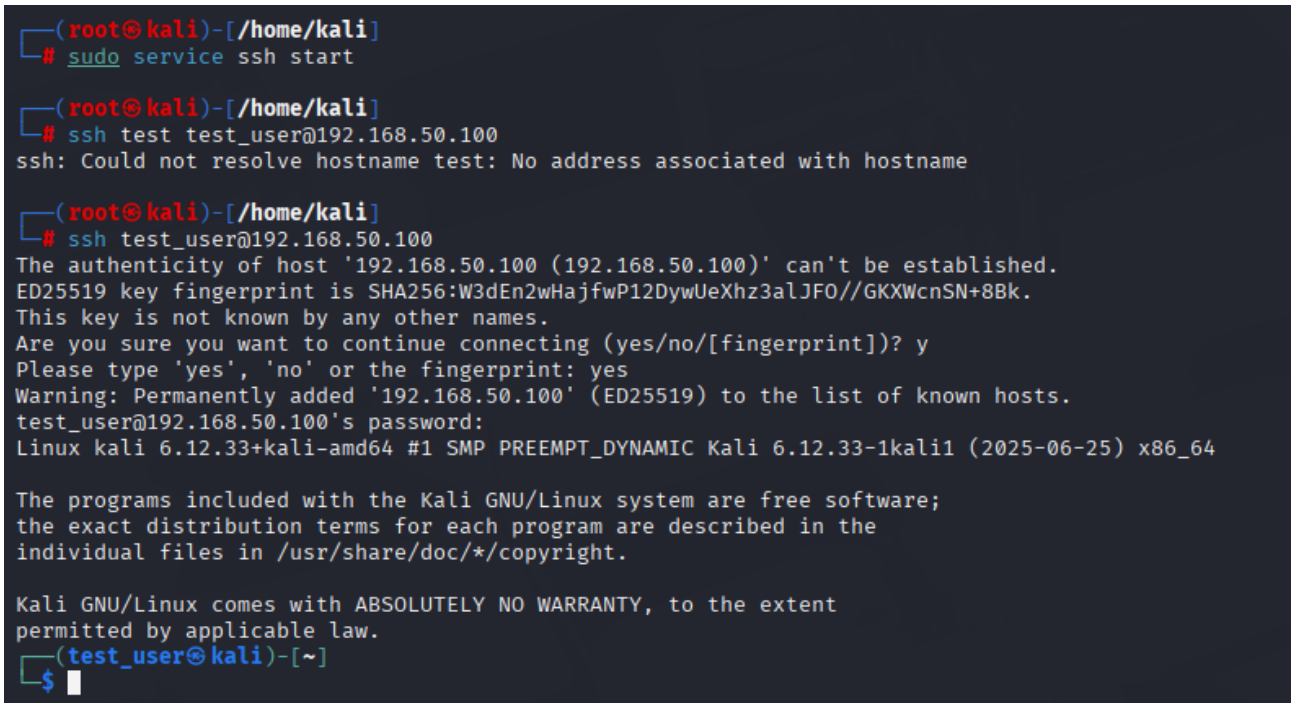
- Nome utente: **test_user**
- Password: **testpass**

---

2. Attivazione del servizio SSH

Per attivare il servizio SSH è stato usato il seguente comando:

sudo service ssh start



Configurazione del file di configurazione servizio SSH (scelta personale)

Ho deciso di configurare il file config del servizio SSH per aggiungere una maggiore personalizzazione e ho eseguito i seguenti comandi:

sudo nano /etc/ssh/sshd_config

Questo primo comando mi mostra il percorso file del config SSH

Una volta nel file config ho modificato i seguenti parametri:

PermitRootLogin yes

MaxStartups 10:30:60

Questi due parametri sono fondamentali, infatti il primo consente all'utente root di connettersi direttamente tramite SSH mentre il secondo protegge da eventuali attacchi Ddos o Dos, infatti limita il numero di connessione non autenticate

10 (start): indica il numero di connessione non autenticate che possono essere stabilite prima che il “demone” inizi a rifiutarle

30 (rate) indica la percentuale di probabilità con cui il “demone” rifiuterà le nuove connessione una volta raggiunto il numero di connessioni start, ossia il 10

60 (full) indica il numero massimo di connessioni non autenticate possibili, una volta raggiunto ogni nuova connessione verrà rifiutata.

---

3. Verifica servizio SSH

Recupero dell'indirizzo IP con comando:

ifconfig

Test della connessione con comando:

ssh test_user@192.168.500.100

---

4. Creazione delle wordlist personalizzate

Per il primo cracking della password ho creato delle wordlist personalizzate per simulare un attacco mirato con un range di parole predefinito, ho quindi creato due liste, una che si occupa dei possibili username e uno delle password e ho usato i seguenti comandi:

Creazione Wordlist delle password:

echo -e "password\n123456\nadmin123\ntestpass\nqwerty\nletmein\npassword1\nwelcome\n12345678\nchangeme\nroot123\ntoor\niloveyou\nsecurepass\npassword123" > passwords.txt

Creazione Wordlist degli username:

echo -e "test_user\nadmin\nroot\nuser1\nguest\noperator\nsupport\nmanager\ndeveloper\nservice\nbackup\ntester\naccount\nsuperuser\nsysadmin" > usernames.txt

5. Utilizzo di Hydra su SSH

Ho usato Hydra per effettuare il "brute force" sul servizio SSH avviato in precedenza

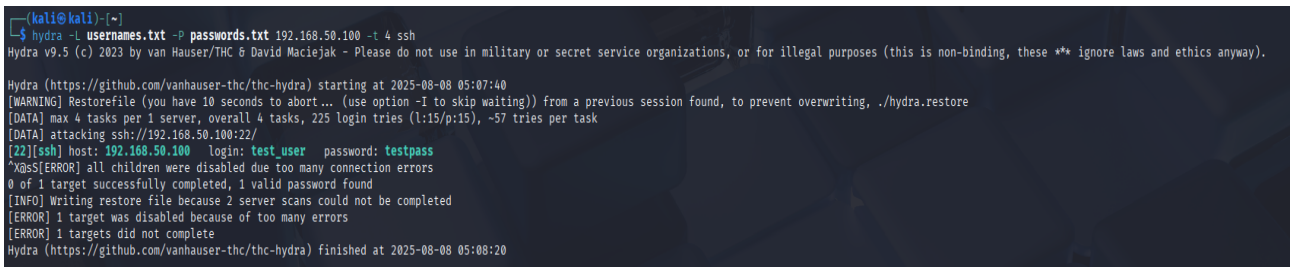
Comando per Hydra:

hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 1 ssh

Spiegazione comando:

- -L usernames.txt: Specifica il file delle wordlist per i nomi utente.
- -P passwords.txt: Specifica il file delle wordlist per le password.
- 192.168.50.100: Indica il server SSH (localhost).
- -t 4: Esegue 4 thread alla volta per fare prima.

NB: In casistiche semplici come questa basterebbe anche un t1 e quindi un thread per volta in quanto avere tanti thread potrebbe creare errori di connessione.



Vediamo quindi come abbiamo trovato sia la password che l'username evidenziati di verde grazie a hydra.

6. Configurazione del Servizio FTP

Ho installato inizialmente il server FTP con il comando:

sudo apt-get install vsftpd -y

Ho poi avviato il servizio con il comando:

sudo service vsftpd start

Ho successivamente creato un nuovo utente e una nuova password anche per il servizio FTP con il comando:

sudo adduser ftp_user

- Nome utente: **ftp_user**
- Password: **ftp_pass**

7. Creazione wordlist personalizzate su servizio FTP

Ho quindi creato una nuova wordlist personalizzata sia per gli username che per le password

Creazione Wordlist degli username:

echo -e "ftp_user\nadmin\nroot\nguest\nuser1\dottorrampino\callcenter\arena breakout\libro\libero\misentite" > ftp_usernames.txt

Creazione Wordlist delle password:

echo -e "123456\npassword\nftp_pass\nadmin123\nwelcome\carino\simone marchica\consegnoalle18" > ftp_passwords.txt

8. Utilizzo di Hydra su FTP

Ho usato Hydra per effettuare il “brute force” sul servizio FTP avviato in precedenza

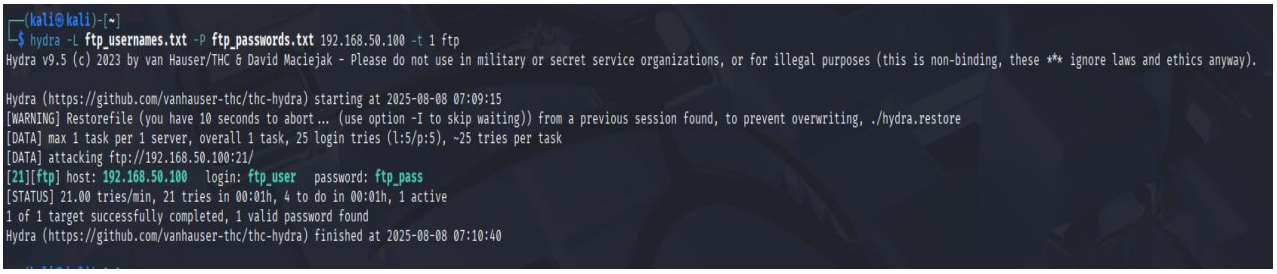
Comando per Hydra:

hydra -L ftp_usernames.txt -P ftp_passwords.txt 192.168.50.100 -t 1 ftp

Spiegazione comando:

- -L usernames.txt: Specifica il file delle wordlist per i nomi utente.
- -P passwords.txt: Specifica il file delle wordlist per le password.
- 192.168.50.100: Indica il server FTP (localhost).
- -t 4: Esegue 4 thread alla volta per fare prima.

NB: In casistiche semplici come questa basterebbe anche un t1 e quindi un thread per volta in quanto avere tanti thread potrebbe creare errori di connessione.



Vediamo quindi come anche in questo caso abbiamo trovato sia la password che l’username evidenziati di verde grazie a hydra.

Conclusioni e Considerazioni

L'esercizio ha dimostrato l'efficacia degli attacchi con dizionari mirati e ha messo in risalto degli aspetti fondamentali come la necessità di proteggere i servizi di rete configurando correttamente il file di configurazione e implementando sistemi di rilevamento.