Authentication cracking con Hydra

Introduzione

L'esercizio odierno si articola in due fasi principali con un duplice obiettivo: praticare l'uso di Hydra per craccare l'autenticazione dei servizi di rete e consolidare le conoscenze sulla configurazione di tali servizi.

Le fasi sono:

1) Abilitazione di un servizio SSH e successiva sessione di cracking dell'autenticazione tramite Hydra.
2) Configurazione e cracking di un servizio di rete a scelta (es. FTP, RDP, Telnet, autenticazione HTTP) in autonomia.

Lista dei Comandi Utilizzati

Configurazione e cracking del servizio SSH

1. **sudo adduser test_user**
   Crea un nuovo utente chiamato test_user sul sistema, che verrà utilizzato per testare l'autenticazione SSH.
2. **sudo service ssh start**
   Avvia il servizio SSH sul sistema.
3. **sudo systemctl status ssh**
   Verifica lo stato del servizio SSH, confermandone il corretto avvio e funzionamento.
4. **ip a**
   Mostra gli indirizzi IP assegnati alle interfacce di rete, utile per identificare l'IP della macchina su cui è attivo il servizio SSH.
5. **ssh test_user@192.168.50.100**
   Tenta di connettersi al servizio SSH sull'indirizzo IP 192.168.50.100 utilizzando l'utente test_user.
6. **nano username_list.txt –** creazione del file di testo contente gli username.
7. **nano password_list.txt –** creazione del file di testo contente le password.
8. **hydra -L /home/test_user/username_list.txt -P /home/test_user/password_list.txt 192.168.50.100 ssh -V -t 1**
   Esegue un attacco di forza bruta sul servizio SSH utilizzando Hydra, con una lista di username e password.

Configurazione e cracking di un altro servizio di rete (ftp)

1. **hydra -L username_list.txt -P password_list.txt 192.168.50.100 ftp -V**
   Esegue un attacco di forza bruta sul servizio FTP utilizzando Hydra, con una lista di username e password.

Esecuzione dell'esercizio

Configurazione e cracking del servizio SSH

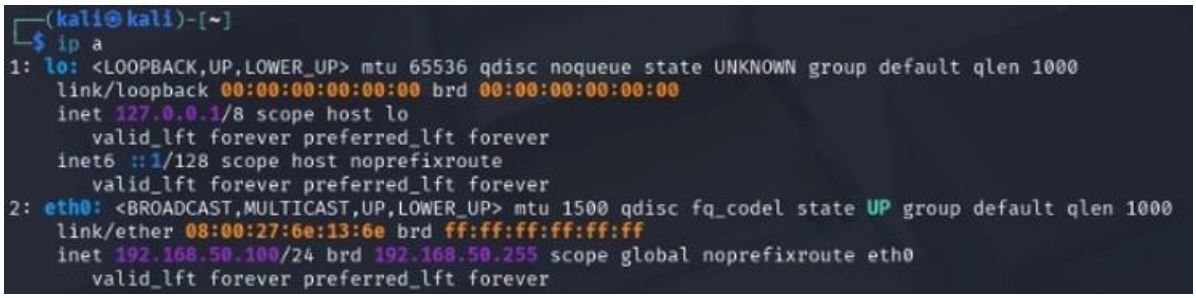
1. Tramite il terminale di Kali, utilizzando il comando **sudo adduser test_user** creiamo un nuovo utente.

L'utente creato avrà come username: **test_user** e come password: **testpass**

2. Avviamo il servizio SSH con: **sudo service ssh start**

3. Successivamente ci accertiamo che il servizio SSH sia attivo con: **sudo systemctl status ssh**

4. Con il comando **ip a** andremo a individuare l'indirizzo IP della macchina su cui è attivo il servizio SSH.

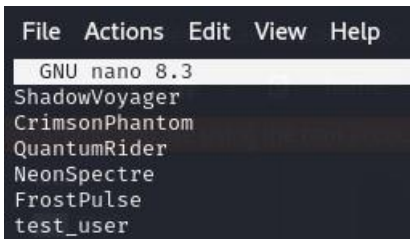


L'indirizzo IP è: **192.168.50.100**

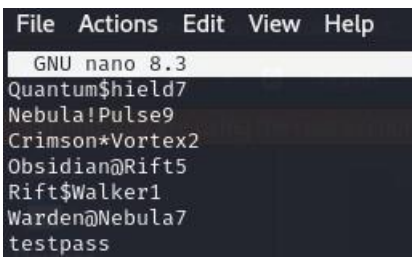
5. Ottenuto l'indirizzo IP, testiamo la connessione con il comando: **ssh** test_user@192.168.50.100

6. Successivamente con i comandi: **nano username_list.txt** e **nano password_list.txt** andremo a creare dei file di testo contenenti vari username e varie password.

Nel file di testo **username_list.txt** aggiungeremo **test_user**

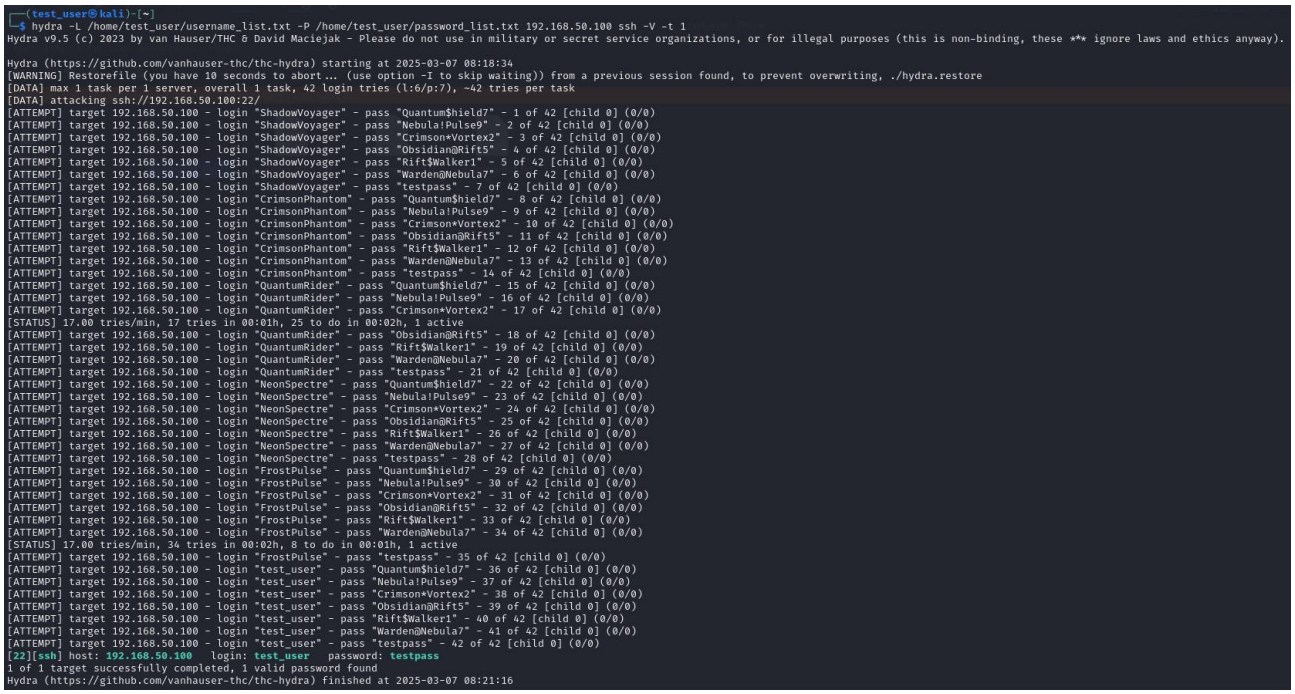


Nel file di testo **password_list.txt** aggiungeremo **testpass**



7. Salvato i file di testo, eseguiremo il seguente comando: **hydra -L /home/test_user/username_list.txt -P /home/test_user/password_list.txt 192.168.50.100 ssh -V -t 1**).

   L'opzione **-V** abilita la modalità verbose, significa che mostrerà più dettagli mentre sta lavorando. L'opzione **-t 1** limita il numero di tentativi paralleli a 1, in altre parole Hydra proverà una combinazione di username e password alla volta, invece di provarne molte insieme. Questo rende l'attacco più lento ma è utile per evitare di sovraccaricare il servizio o essere rilevati.



Questo comando eseguirà un attacco di forza bruta sul servizio SSH utilizzando Hydra insieme ai file di testo visti in precedenza così da farci trovare **l'host**: 192.168.50.100 **login**: test_user e la **password**: testpass

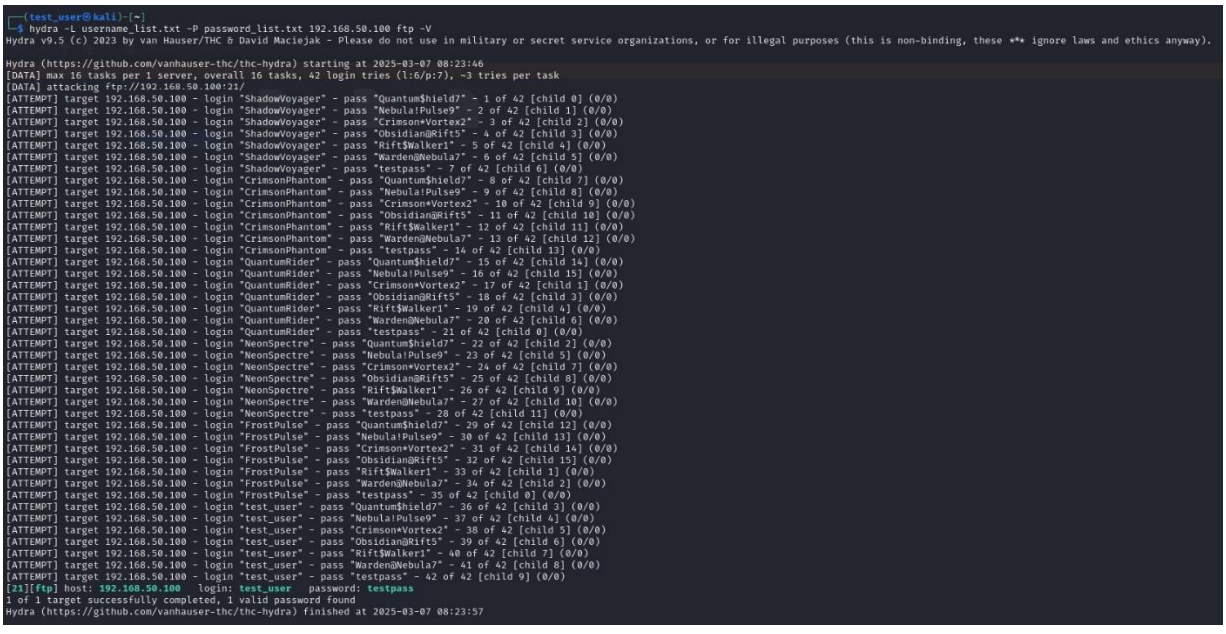
Configurazione e cracking di un altro servizio di rete (ftp)

Per questo esercizio il servizio di rete scelto su cui è stato eseguito l'attacco brute force è il **FTP.**

1. Installiamo il servizio dal terminale Kali con il seguente comando: **sudo apt install vsftpd**

2. Terminata l'installazione, avviamo il servizio con il comando: **sudo service vsftpd start**

3. Utilizziamo Hydra per eseguire un attacco di forza bruta sul servizio ftp con il seguente comando: **hydra -L username_list.txt -P password_list.txt 192.168.50.100 ftp -V**



Questo attacco ci consentirà di trovare **l'host**: 192.168.50.100 **login:** test_user **password:** testpass

Conclusioni

In conclusione, è fondamentale proteggere le proprie password utilizzando combinazioni sicure e complesse, evitando errori comuni come l'uso di password deboli o facilmente indovinabili. Gli attacchi di brute force permettono di ottenere le credenziali con relativa facilità, rendendo ancora più importante adottare misure di sicurezza adeguate a salvaguardare i propri account e dati personali.