Report sull'esercizio di cracking SSH con Hydra

**Obiettivo:**

Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete.

**Procedura:**

L'esercizio è stato svolto in due fasi principali: configurazione del servizio SSH e utilizzo di Hydra per il brute forcing delle credenziali di accesso.

**Fase 1:** Configurazione del servizio SSH

**1. Creazione di un nuovo utente:**

- È stato creato un nuovo utente chiamato “test\_user” con la password “testpass” su Kali Linux.

**Comando:**

“

sudo adduser test\_user

“

**2. Attivazione del servizio SSH:**

È stato attivato il servizio SSH sulla macchina.

**Comando:**

“

sudo service ssh start

“

**3. Test della connessione SSH:**

- È stata testata la connessione SSH all'indirizzo IP della macchina Kali.

**Comando:**

“

ssh test\_user@192.168.1.2

“

**Fase 2**: Utilizzo di Hydra per il brute forcing delle credenziali SSH

**1. Preparazione delle wordlist:**

- Sono andato a creare due wordlist, una per gli username (“username\_list.txt”) e una per le password (“password\_list.txt”).

```

**2. Esecuzione di Hydra per l'attacco brute force:**

Il comando Hydra utilizzato per attaccare il servizio SSH è stato il seguente:

“

hydra -L username\_list.txt -P password\_list.txt 192.168.1.2 ssh -t 4 -V

“

**- Parametri del comando:**

- **“-L username\_list.txt”:** Specifica la lista di username.

- **“-P password\_list.txt”**: Specifica la lista di password.

- **“192.168.1.2”**: Indirizzo IP della macchina Kali.

- **“ssh”**: Specifica che il servizio da attaccare è SSH.

- **“-t 4”**: Numero di task simultanei (4).

**- “-V”**: Modalità verbosa per vedere ogni tentativo.

**4. Risultato dell'attacco Hydra:**

Hydra ha trovato le credenziali valide per l'accesso SSH:

- Username: “test\_user”

- Password: “testpass”

**- Output di Hydra:**

“

[22][ssh] host: 192.168.1.2 login: test\_user password: testpass

“

**Conclusioni:**

La configurazione del servizio SSH e l'utilizzo di Hydra per il brute forcing delle credenziali sono stati completati con successo.

L'accesso SSH con le credenziali “test\_user” e “testpass” è stato verificato e confermato da Hydra.

Immagine che contiene schermata, testo, tipografia, design

Descrizione generata automaticamente

**Report sull'esercizio di cracking Telnet con Hydra**

**Obiettivo:**

Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete, in questo caso il servizio Telnet.

**Procedura:**

L'esercizio è stato svolto in due fasi principali: configurazione del servizio Telnet e utilizzo di Hydra per il brute forcing delle credenziali di accesso.

**Fase 1**: Configurazione del servizio Telnet

**1. Installazione e configurazione del servizio Telnet:**

È stato installato e configurato “telnetd” per permettere l'accesso Telnet alla macchina.

**Comandi:**

“

sudo apt-get update

sudo apt-get install telnetd xinetd

“

**2. Creazione del file di configurazione per Telnet in “xinetd”:**

- È stato creato e modificato il file di configurazione “/etc/xinetd.d/telnet” con il seguente contenuto:

“

service telnet

{

flags = REUSE

socket\_type = stream

wait = no

user = root

server = /usr/sbin/telnetd

log\_on\_failure += USERID

disable = no

}

“

**Spiegazione della configurazione:**

- flags = REUSE: Permette di riutilizzare la connessione per migliorare l'efficienza.

- socket\_type = stream: Imposta il tipo di socket su "stream", che è il tipo di socket utilizzato per i flussi di dati TCP.

- wait = no: Indica che il servizio non deve attendere per completare prima di accettare nuove connessioni.

- user = root: Specifica che il servizio Telnet verrà eseguito come utente root.

- server = /usr/sbin/telnetd: Indica il percorso dell'eseguibile del server Telnet.

- log\_on\_failure += USERID: Aggiunge un'azione di log per registrare il nome utente in caso di fallimento della connessione.

- disable = no: Abilita il servizio. Se impostato su "yes", il servizio sarebbe disabilitato.

**3. Attivazione e verifica del servizio Telnet:**

- È stato avviato “xinetd” e verificato che il servizio Telnet fosse in esecuzione.

- Comandi:

“

sudo service xinetd start

sudo service xinetd status

“

**4. Test della connessione Telnet:**

- È stata testata la connessione Telnet all'indirizzo IP della macchina Kali.

- Comando:

“

telnet 192.168.1.2

“

Le credenziali utilizzate per l'accesso erano:

- Username: “telnet\_user”

- Password: “telnetpass”

**Fase 2:** Utilizzo di Hydra per il brute forcing delle credenziali Telnet

**1. Preparazione delle wordlist:**

Sono andato a creare due wordlist, una per gli username (`telnet\_username\_list.txt`) e una per le password (`telnet\_password\_list.txt`).

**2. Esecuzione di Hydra per l'attacco brute force:**

Il comando Hydra utilizzato per attaccare il servizio Telnet è stato il seguente:

“

hydra -L telnet\_username\_list.txt -P telnet\_password\_list.txt 192.168.1.2 telnet -t 8 -V -d

“

**Parametri del comando:**

- **“-L telnet\_username\_list.txt”:** Specifica la lista di username.

- **“-P telnet\_password\_list.txt”:** Specifica la lista di password.

- **“192.168.1.2”**: Indirizzo IP della macchina Kali.

- **“telnet”:** Specifica che il servizio da attaccare è Telnet.

- **“-t 8”:** Numero di task simultanei (8).

- **“-V”:** Modalità verbosa per vedere ogni tentativo.

- **“-d”:** Modalità debug per avere maggiori dettagli sui tentativi.

**3. Risultato dell'attacco Hydra:**

Hydra ha trovato le credenziali valide per l'accesso Telnet:

- Username: “telnet\_user”

- Password: “telnetpass”

**- Output di Hydra:**

“

[23][telnet] host: 192.168.1.2 login: telnet\_user password: telnetpass

[COMPLETED] target 192.168.1.2 - login "telnet\_user" - pass "telnetpass" - child 0 - 44 of 100

“

Immagine che contiene testo, schermata

Descrizione generata automaticamente

**Conclusioni:**

La configurazione del servizio Telnet e l'utilizzo di Hydra per il brute forcing delle credenziali sono stati completati con successo.

L'accesso Telnet con le credenziali “telnet\_user” e “telnetpass” è stato verificato e confermato da Hydra.