How to login to the task

I was in Macquarie University so I didn't need to log to the Macquarie VPN

Connection:

Go to terminal and use ssh

Port: 8080

Username:45731365

Ip address: 10.46.225.199

ssh -D 8080 45731365@10.46.225.199

password: lumpysugar82

Use Nmap to scan for flags

nmap 172.31.0.0/24

45731365@ctf4:~/flags$ nmap 172.31.0.0/24

Starting Nmap 7.60 (https://nmap.org) at 2020-06-23 03:03 UTC

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 3: open failed: connect failed: Connection refused

channel 5: open failed: connect failed: Name or service not known

channel 5: open failed: connect failed: Name or service not known

Nmap scan report for 45731365_test.1130_45731365_back (172.31.0.10)

Host is up (0.000038s latency).

Not shown: 999 closed ports

PORT   STATE SERVICE

80/tcp open http

MAC Address: 02:42:D8:D9:05:0A (Unknown)

Nmap scan report for 45731365_flag1.1130_45731365_back (172.31.0.20)

Host is up (0.000040s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 02:42:43:AC:DA:C6 (Unknown)

Nmap scan report for 45731365_flag2.1130_45731365_back (172.31.0.30)

Host is up (0.000040s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

21/tcp open ftp

MAC Address: 02:42:F5:F5:0A:9E (Unknown)

Nmap scan report for 45731365_flag3.1130_45731365_back (172.31.0.40)

Host is up (0.000039s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

80/tcp open http

MAC Address: 02:42:F5:F5:54:64 (Unknown)

Nmap scan report for 45731365_flag4.1130_45731365_back (172.31.0.50)

Host is up (0.000039s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

80/tcp open http

MAC Address: 02:42:97:70:87:85 (Unknown)

Nmap scan report for 45731365_flag5.1130_45731365_back (172.31.0.60)

Host is up (0.000041s latency).

Not shown: 999 closed ports

PORT   STATE SERVICE

22/tcp open ssh

MAC Address: 02:42:A5:EE:94:A0 (Unknown)

Nmap scan report for 45731365_flag6.1130_45731365_back (172.31.0.70)

Host is up (0.000039s latency).

All 1000 scanned ports on 45731365_flag6.1130_45731365_back (172.31.0.70) are closed

MAC Address: 02:42:5B:47:85:BB (Unknown)

Nmap scan report for ctf4 (172.31.0.199)

Host is up (0.0000080s latency).

Not shown: 999 closed ports

PORT   STATE SERVICE

22/tcp open ssh

Also, gobuster was used to access the webservers:

http://172.31.0.40/

http://172.31.0.50/

those are the websites needed for the web ctf

Flag 2 FTP: Nmap scan report for 45731365_flag2.1130_45731365_back (172.31.0.30)

Type ftp 172.31.0.30

Then when requested for username: Type Anonymous

Password:

Then type dir (directory)

You could see flag.txt

Type mget flag.txt

It is saved in the server

Quit the ftp

Type ls -a to reveal the flag.txt

Type cat flag.txt and the flag is revealed

a1abed3b639a5ba34863aea64f025256

Flag 1: master of domain

Nmap scan report for 45731365_flag1.1130_45731365_back (172.31.0.20)

ssh 172.31.0.20

type domainname and the flag is revealed

Flag4 (Hidden in plain sight)

This is a web-based flag

Log in to the address 172.31.0.40/index.html

Accessing the page source reveals

</body>

</html>

<!-- Hahaha you'll never find my admin page! -->

It has to do with login in to the admin page.

I turned on the foxy proxy so burp suite could intercept the packets

In the proxy I changed connection to open and forward it to repeater

In the repeater I also changed the connection to open and clicked send, but I couldn’t get the flags

Flag 6 Name: What's my config?

This is a network ctf

This task Is all about getting the configuration of the server

I used the dig command to get the information

Dig axfr @172.31.0.40 flag6.txt

I got a permission restriction.

I couldn’t get this flag

Flag 5