

- Meow - VeryEasy

Start the openvpn

'Ping ip' to ensure the env is correct

'sudo nmap ip' to scan all the available port

find the only available port is telnet

using 'telnet ip' to connect to the server and login with 'root' (or nc 10.129.231.92 23)



'ls' to see all the file in root

cat flag.txt to see the flag

- Fawn - VeryEasy

Start the openvpn

nmap ip to get the available port 21 which is ftp

ftp ip to connect

Find the target is vsftpd 3.0.3

Login with admin - Failed

Login with anonymous - Successful

Check the info and knowing the server is base on UNIX

Ls to check all file

get flag.txt to get the flag

bye to exit the system

- Dancing - VeryEasy

Nmap and find three available port

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Try to connect port 445 which is SMB (server message block)

'smbclient ip'

```
(venv) chien@chien-VMware20-1:~/ctf$ smbclient -L 10.129.201.138

Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
IPC$           IPC            Remote IPC
WorkShares     Disk
SMB1 disabled -- no workgroup available
```

Found that there are 4 available sharename

connect again by 'smbclient //10.129.201.138/WorkShares -N', -N means without password

Found that there are two dir

Found that the flag is in one of the dir.

- Redeemer - VeryEasy

First attempt, 'nmap id' does not get any available port

change to use 'nmap -p- ip' can scan all the ports (nmap only scan the first 1000 common port)

advance: using 'nmap -p --min-rate 1000 -T5 ip' to setup the minimum speed, and speed up (but T4 or T5 does may loss some info, the default one is T3)

successfully get these port:

PORT STATE SERVICE

6379/tcp open redis

using 'redis-cli -h 10.129.109.152' connect to the redis

using 'info' to check system version

using "keys \*" to list all the keys name

using 'get flag'