**VulnHub – Breakout**

1. A screenshot of a computer screen

   Description automatically generatedUse netdiscover to find devices on the network.
2. A computer screen shot of a computer

   Description automatically generatedNext up, use nmap to determine the available servers and open ports. The scan I have done is a no-ping quick scan. Here there are 4 ports and services available to us.

* 80 – HTTP.
* 139 – Provide access to shared resources (files & printers).
* 445 – SMB (sharing resources on windows).
* 10000 – HTTP Mini-server.
* 20000 – HTTP Mini-server (appeared when I did aggressive scan).

1. Now we have established ports, we know there is HTTP so we can run nikto.

* A screenshot of a computer program

  Description automatically generatedApache is running on this server, v2.4.51.
* Port: 10000 is running MiniServ/1.981.

1. I got stuck and decided that I needed to either perform fuzzing or web-crawling. I decided to use go-buster for this, because of previous CTFs.

* A screen shot of a computer

  Description automatically generatedhowever this reveals nothing.

1. Opening the page source shows this message.

* Looking closer, this string could be something important.



* I then proceeded to go online and find a cipher identifier. The above is most likely the brainfuck cipher.
* Decoded value: .2uqPEfj3D<P'a-3



1. Next, I went into Enum4Linux.

* As seen the username is cyber.
* Now we have the username and password, and we can get into the usermin webpage login (port 20,000).

1. A close up of a blue and black background

   Description automatically generatedNow that we are on the page, we need to set up a shell.

* A screenshot of a computer

  Description automatically generatedNow you can use netcat to establish a reverse-shell.

1. Using the cat command on user.txt will reveal the flag format, but no quite the flag.



1. Upgrade the shell.

* Don’t forget to ‘export TERM=xterm”.

1. Now try and upgrade the shell. Lets check by using ‘sudo -L’, however this command isn’t installed so we need some other escalation means.
2. Since this is a server, there should be content in the ‘/var/’ directory. In this case there is a folder called backups. This contains a hidden file called old\_pass.bak.

* A screen shot of a computer

  Description automatically generatedRemember how there was a tar file in the home directory, an executable? This can be used to compile that backup file and sent it to our machine.
* Since this is now sitting in our directory where we have read permissions we can then use the command tar with flags ‘xf’ to decompress and view the file contents.

A screen shot of a computer screen

Description automatically generated

1. This password could belong to the root user. I tried to switch user to root and I was able to.

A computer screen shot of a computer code

Description automatically generated with medium confidence

1. Try and look for the flag. I think the common place would be root, especially how this is only accessible if you are root.A screenshot of a computer screen

   Description automatically generated Checking there reveals a file called r00t.txt.

* Future Michael, I think you can get this flag if you used the “3mp!r3{“ as a pattern for the find command
  + Something like: “find / -name 3mp!r3 ” (or similar).