Text

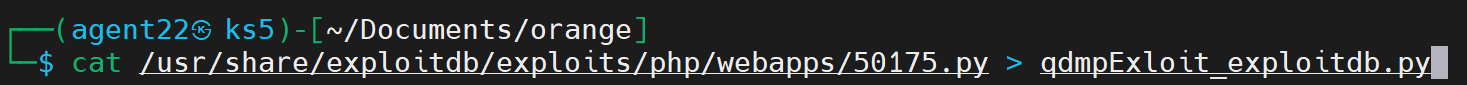
Description automatically generated

The first step I took was to use searchsploit to find exploits that apply to qdpm 9.1.

Text

Description automatically generated

I then located the python scripts actual location in the file system.

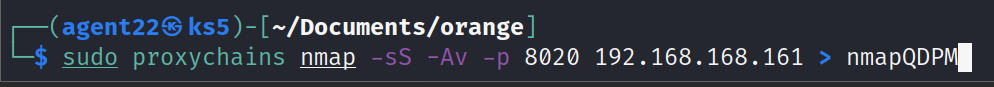


Next I copied the exploit to my folder for this attack path.

Text

Description automatically generated

I then configured the proxychains tool to route traffic through my SOCKS5 proxy connecting to the school network.



Text

Description automatically generated with medium confidence

After configuring proxychains I performed an nmap to make sure I could access the server and get some more info.

Text

Description automatically generated

I then tried to run the code from exploitdb and the code from canvas. The code from exploitdb failed to run correctly. The canvas code worked great. Side note, I really look forward to learning to build these kinds of exploits and tools myself.

Text

Description automatically generated

<http://192.168.168.161:8020//uploads/users/131493-backdoor.php?cmd=whoami>

Using the canvas code I then implanted a backdoor on the qdPM webserver.

Graphical user interface, text

Description automatically generated

Next, I tested and confirmed that the backdoor is working.

Text

Description automatically generated

I then dumped the user accounts on the OS running the webserver.

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Using the backdoor I explored the file system searching for valuable files.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

As directed in the course videos I found the above username and password in the database.yml file. This password is for the database also running in the environment.

A screenshot of a computer

Description automatically generated

I then found the users list for the qdPM server. Next, I attempted to find more open ports using nmap. However, I was getting a lot of connection issues.

Graphical user interface, text, application

Description automatically generated

I therefore used my backdoor to see which ports were open on the server I had access to. The only other service open to me I believe is ssh.

A screenshot of a computer

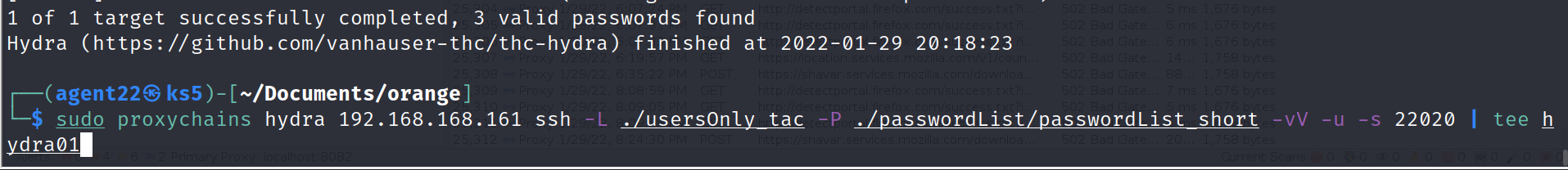
Description automatically generated with medium confidence

Attempted to use hydra to try known and suspected passwords to get into ssh. However, I was not able to connect.

Text

Description automatically generated

Port 22 may or may not be open. However, it doesn’t connect to ssh so I suspect it’s down.



I then remembered the ssh port shown in class. I repeated the hydra request using that port. Before repeating the hydra I added all of the usernames to the password list. The password list also contained all passwords found previously.

Text

Description automatically generated with medium confidence

This resulted in me obtaining three usernames and passwords.