All references to the server, target, etc, refer to the QDPM webserver at 192.168.168.161:8020.

Text

Description automatically generated

The first step I took was to copy the user data from the QDPM web portal to my kali box. I then converted it to a usable format.

Text

Description automatically generated

I then extracted the emails from the user info file.

Text

Description automatically generated

Next, I pulled the usernames from the email file.

Graphical user interface, text, application, email

Description automatically generated

I then performed a password spray using the email list.

Graphical user interface, text, application

Description automatically generated

I also fuzzed the password field. I used my short list of known and suspected passwords. I also used the username file I just generated.

Application

Description automatically generated with medium confidence

This did not yield any new password results.

A screenshot of a computer

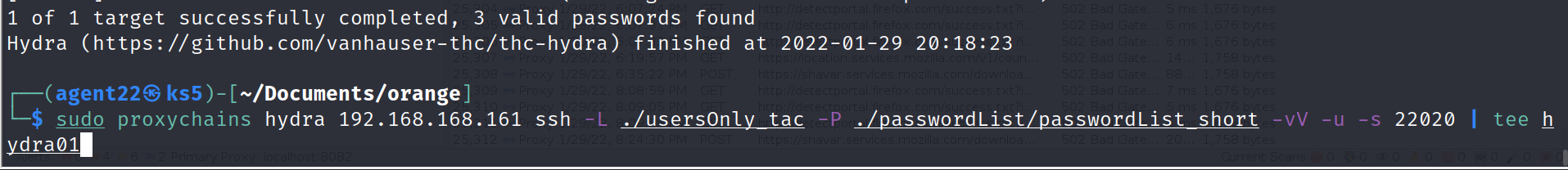
Description automatically generated with medium confidence

Next I attempted to use hydra to try known and suspected passwords to log into the server over SSH. However, I was not able to connect. The default port 22 was not open.

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 found in the passwd file 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 for logging into SSH.

Text

Description automatically generated

I then used the mp username & password to login over SSH to the server.

Text

Description automatically generated

After that I checked the mp account permissions. The mp account can run all commands and perform all actions.

Text

Description automatically generated

Using this access I elevated my access to root.

After gaining access to root I needed to create persistence on the box. I wanted to add a user in the least obvious way possible. In order to learn how to do this I studied the following resources:

<https://attack.mitre.org/techniques/T1564/002/>

<https://askubuntu.com/questions/22006/is-there-a-way-to-create-a-hidden-account>

<https://embracethered.com/blog/posts/2021/linux-user-uid-zero-backdoor/>

<https://askubuntu.com/questions/2471/how-to-hide-users-from-the-gdm-login-screen>

From those resources I took the following notes:

You can have shell users without a home directory:

useradd --no-create-home new\_username

Configure the system to hide users from the login screen

Set userid & group id to an innocuous number under the system default for new users. This is often 1000 or 500. Set the username to look like a system account.

In addition to these ideas generated through research I also had the following thoughts:

Delete malicious user when other users login, then recreate user on logout using built in login and logout scripts. Edit password & shadow files manually instead of using a useradd or adduser command. Make passwd file only available to the admin users so you don’t need to delete your user at every login. Only at the logins of the admin users.

Manually edit the passwd and shadow files to make new user seem less suspicious.

Use an existing system group as the primary group for the new malicious user.

Text

Description automatically generated

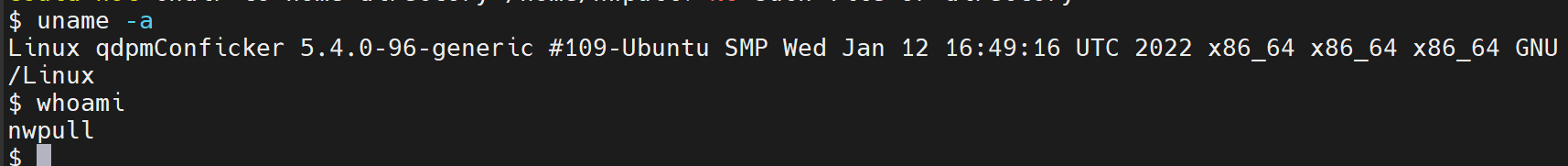
Acting on my research and ideas I created a new user using the above shown useradd command. -l specifies “do not add the user to the lastlog and faillog databases”. -M means do not create a home directory. -N means do not create a group based on the new username. –system means make the user a system user. -g specifies the group id. -u specifies the user id.

I created the account at 7:40pm on 2/2/2022. I then set the password so I could log into the account.

Text

Description automatically generated

I added the account to the news group and designed the name so that it would seem related to the news user.



I then confirmed that I could login over ssh with the nwpull account.

Text

Description automatically generated

I then added nwpull to the sudo group so I could perform any and all actions as nwpull.

Text

Description automatically generated

Text

Description automatically generated

I then modified the /etc/passwd and /etc/shadow files to show the nwpull user in less suspicious locations. I also removed the nwpull home folder from /etc/shadow. I then re-verified that I could login with nwpull.