Password Spraying

The first step I took was to gather some names for username creation. My teammate Arcelia provided a long list of names she gathered from Ensign.edu. If I were to do this attack again in the future, I’d use a python web scraper. I then took that list and converted it to csv format with Excel.

Text

Description automatically generated

I then used the above script provided by the pcn3rd to convert the csv file to a list of possible usernames. I struggled for a while to get this script to work because I didn’t understand the need for -i.

Text

Description automatically generated

Due to my confusion I tried to create a new script as shown above. I then watched the course instructional videos and realized I was missing -i. I then updated the original script to clarify the issue.Text

Description automatically generated

Above is shown the results of using the pcn3rd script correctly.

Text

Description automatically generated

Next, I used the awk command to append the email domain to the usernames.

A computer screen capture

Description automatically generated with medium confidence

I then found a powerful wordlist/password generation tool named cook. Using this tool, I created multiple wordlists meeting the criteria listed in the course instructional video.

Graphical user interface

Description automatically generated

The wordlists are shown above. I then combined and sorted the wordlists into the top two files shown above.

Text

Description automatically generated

Using this combined wordlist and the email list I attempted to fuzz/brute force the login for qdpm. Unfortunately, this fuzz would have taken an excessive amount of time. As you can see in the above screenshot, I generated over five million unique passwords.

Graphical user interface, text

Description automatically generated

Seeing that this first fuzz would take longer than was feasible, I created a much shorter password list. This list was composed of all the ensign and seasonYear based passwords.

Text

Description automatically generated

While this list was significantly shorter, combined with the number of emails to fuzz the password spray would still over 500 thousand requests. I attempted this fuzz, but it was also taking an excessively long time.

Text

Description automatically generated

I then created a password list based on the list used in the video. Using this list and the email list I fuzzed the qdpm website.

Text

Description automatically generated with medium confidence

Using the password spray/fuzz I found a login for qdpm. In an actual penetration test this would have taken much longer, but the correct password was provided in the video.

Graphical user interface, application

Description automatically generated

Using the username and password found in the password spray I successfully logged into the qdpm web portal.

Shape

Description automatically generated with medium confidence