Password Spraying   
(Orange)

Text

Description automatically generated with medium confidence

Password Spray:

According to MITRE ATTACK FRAMEWORK, Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

Using Snov.io tool (a Google Chrome plugin) to derive the emails from the target website “Ensign College”, and using the information college email to make up the list of the password and using Windomain.local for proper domain name.

Text

Description automatically generated

Using the list of popular for college passwords or passphrase to make a proper password spray list.

Text

Description automatically generated

Using fuzz to make the password spray attack, by using the username list and password list I created to use HTTP/HTTP Management Services (80/TCP & 443/TCP) for the attack.

As we scan the website, we can find the POST method which can be used to men-in-the-middle attack as well as password spray. As we can see, /index.php/login is the target address, and it appears the headers that we can implement the payload lists I created.

Graphical user interface, text, application

Description automatically generated with medium confidence

We are targeting the http headers the color highlighted below to to implement the login for username.txr , and password for pw.list

Graphical user interface, application

Description automatically generated

After the result shows in the Size Resp. Header, it has an Outlier bytes with 808 bytes compare to the rest 309 bytes. Meaning the password spray match the result. It is [brailee.ogden@windomain.local](mailto:brailee.ogden@windomain.local) as login, and Winter2022 as password.

Table

Description automatically generated with medium confidence

So we use the credential that we found and try to loging onto the /index/loging.php

Graphical user interface, application

Description automatically generated

As we can see the it login successfully.

Graphical user interface, application

Description automatically generated