**Enumeration**

Results of nmap scan

Text

Description automatically generated

Now I will search for website directories using Dirseach.

Here are the results.

Text

Description automatically generated

**Foothold**

Visiting the website, we are already logged into a user.

Graphical user interface, application, website

Description automatically generated

Clicking on the security SnapShot we can download pcap files.

Opening these files up in Wireshark; we can then look for credentials.

After downloading multi Pcap files, I was then able to find a successful login into FTP.Graphical user interface

Description automatically generated

nathan:Buck3tH4TF0RM3!

After successfully signing into ftp, I was able to retrieve USER.txt.Text

Description automatically generated

We can use the credentials to SSH into the box.

**Privilege Escalate**

User has access to write with Python3. Using the following command to obtain root.

python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md Text

Description automatically generated