Task 1 - Wireshark

In this scenario, Your IT administrator has been bribed and fled the country. He has changed all of the passwords on his way out the door, so we have completely lost all access to our systems. You must break your way back onto the network, and continue securing it.

The "Bait & Tackle Bazzar" is still communicating with HTTP. This protocol is known to have a vulnerability that lets an attacker sniff user id and password. Find a way to exploit this vulnerability by capturing the credentials once entered in the website. Additionally we cannot give you the password to the manager account, as we have lost it. You may be able to capture it as we have detected some automated logins.

Expected Outcome

- Access the remote machine using rdp
    - This will be done with the provided credentials
- Utilize Wireshark to see unencrypted HTTP traffic
- Utilize Wireshark to gather credentials of the manager account
    - What could they use to login? (Some of these are random words)
        - SSH
        - FTP
        - rlogin
        - SFTP
        - FSTPS
        - HTTP
        - Telnet
        - PHD
        - Telephone
        - rsh
- Login to Manager Account