Recon with Wireshark Workout Instructions

Introduction

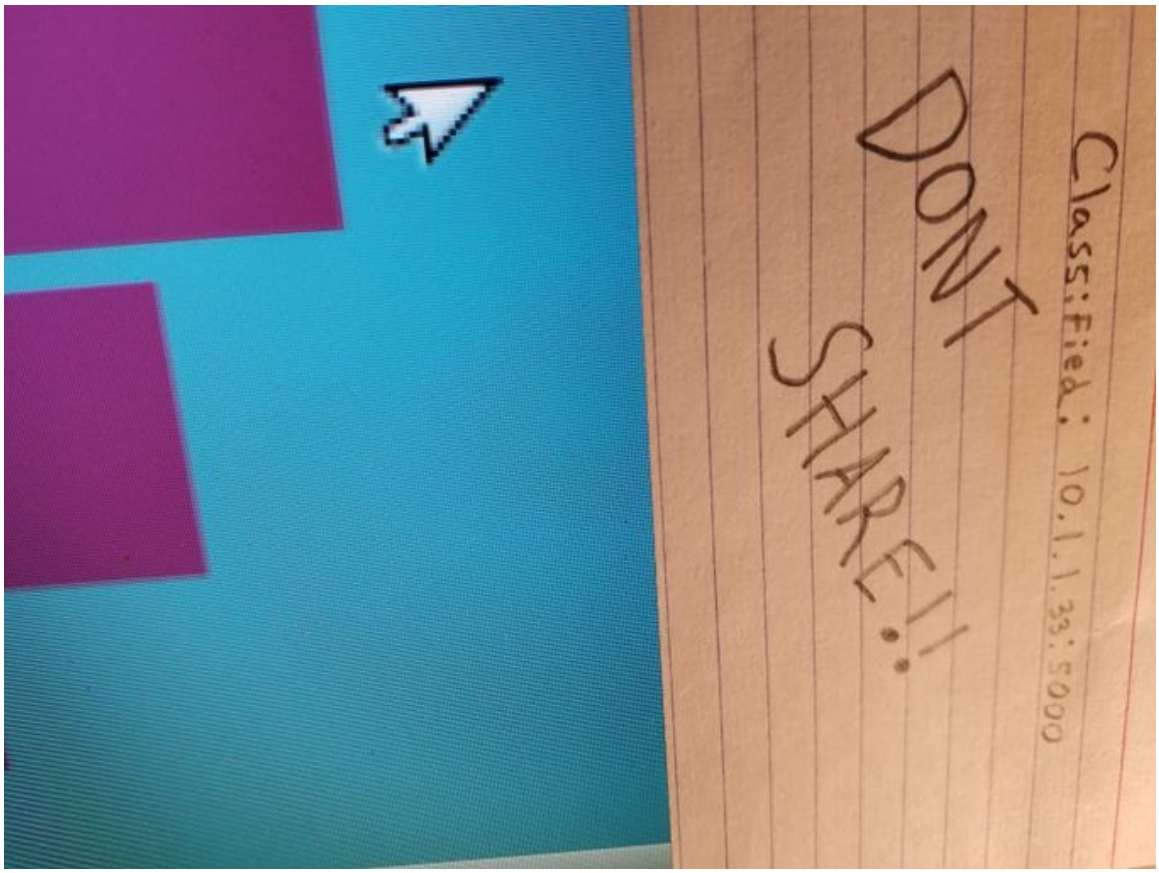
Welcome to your team's *Recon with Wireshark* workout where you will learn how to analyze network packets and understand the inherent insecurity of many network protocols. In this workout, you will perform network traffic analysis against a simulated attack environment. Using Wireshark you will analyze packets originating from the UA Little Rock Classified Web Application to capture its credentials and login to the application.

Logging into your Computer

- Log into the Guacamole web server using *cybergym* and *Let's workout!* as the username and password.
- You may have to refresh the page if a screen does not come up.
- Then, you will log in automatically.

Your Mission

There’s been a lot of talk about a secret classified server from the UA Little Rock Cyber Gym. Word has it that this is where all the security files and important documents are stored. We were able to capture an image of a note from the new receptionist’s computer.



Perhaps the classified server is at http://10.1.1.33:5000 maybe we should investigate. Open Firefox and navigate to the IP address.

If you navigated to the right address you should see what I do. Go ahead and click the green login button.

It looks like we will need the password for the admin. Our analysts told us there was suspicious activity that occurred when you navigated to the classified server. Let's see if you can capture any information and see what's going on. Close your browser and open the Wireshark application from the bottom of the screen, it should be the blue shark fin icon.

With Wireshark, we can capture any packets that occur between you and the classified server. We will need to set a capture filter though. Within the capture filter field type: host 10.1.1.33 and press enter.

This will allow us to capture packets that interact with your computer. Perhaps the password is stored within one of these packet captures. Analyze the packets and find the password, once you have it login to the classified server and report what you find.