Recon with Wireshark Workout Instructions

✓ The Big Idea - Ubiquitous Computing

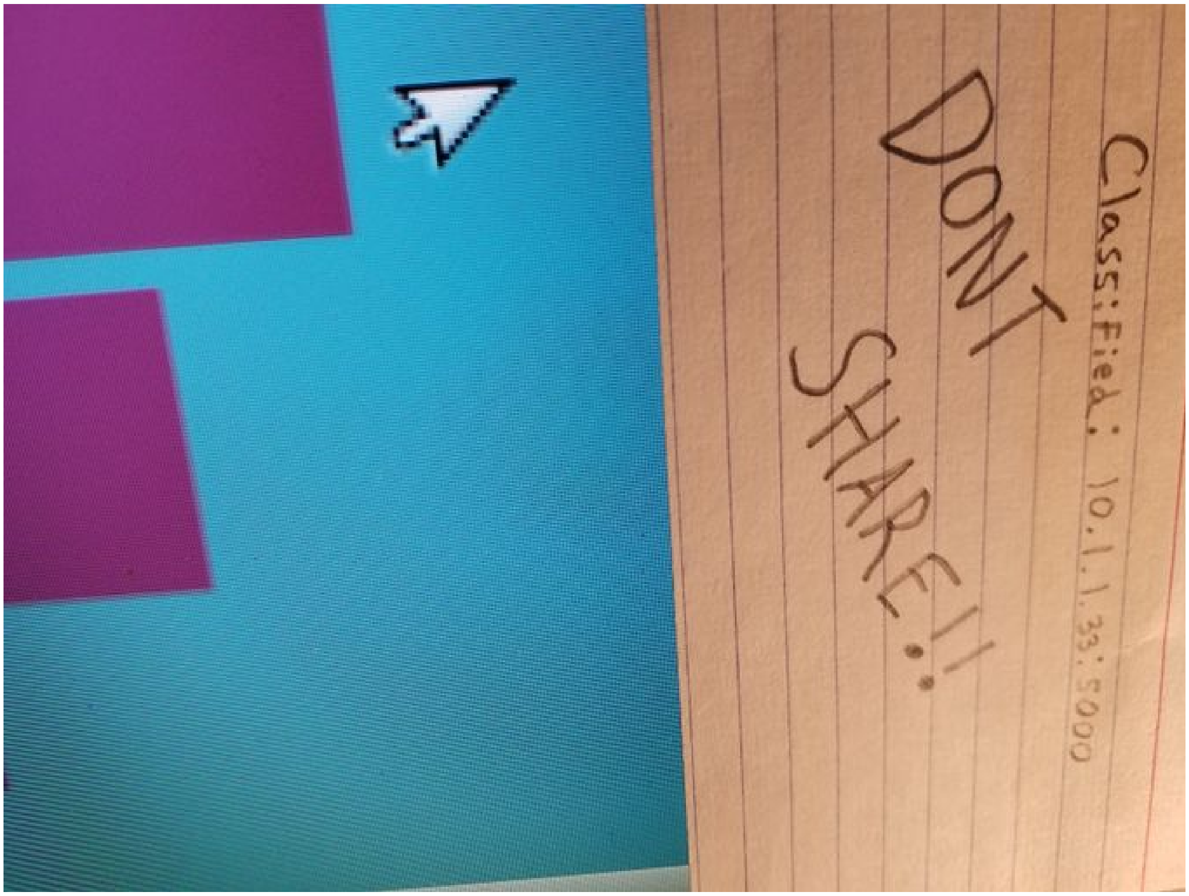
The Internet allows the transmission of data signals to anywhere in the world. The data goes from its source to destination through multiple countries and organizations, and adversaries can easily gain access to this data. Cryptography should be used to protect data as it goes across the Internet, but network protocols may not use cryptography.

This workout explores how an adversary can use reconnaissance tools to obtain sensitive information about a system when systems fail to use cryptographic Internet protocols.

Welcome to the *Recon with Wireshark* workout where you will learn how to analyze network packets and understand the inherent insecurity of many network protocols. You will perform network traffic analysis in this workout 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.

Your Mission

There’s been a lot of talk about a secret classified server from the UA Little Rock Cyber Arena. Word has it that this is where all the security files and essential documents are stored. We captured 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 correct address, go ahead and click the green login button.

It looks like we will need the password for the admin. Our analysts told us suspicious activity occurred when you navigated to the classified server. Let's see if you can capture any information and see what's happening. 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 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 see.