Recon with Wireshark Teacher Instructions

Background

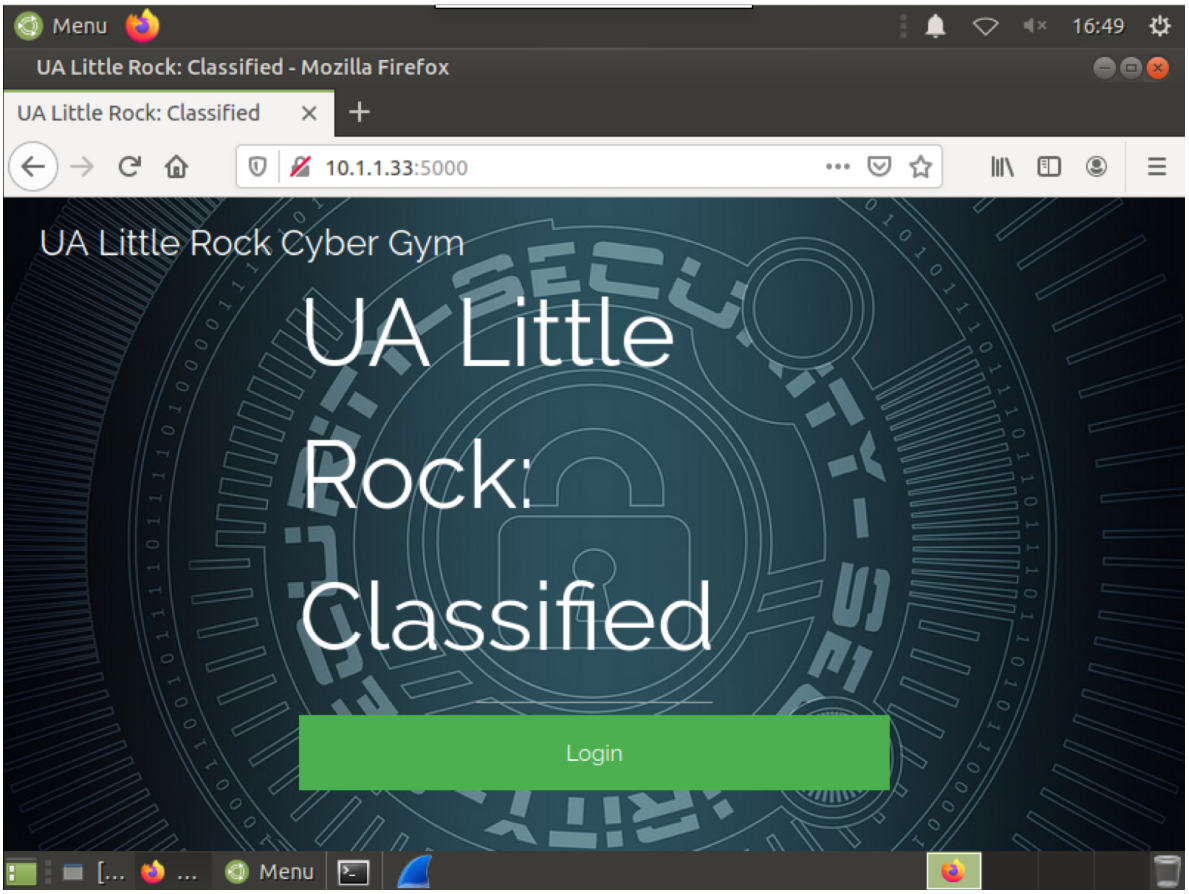
Recon with Wireshark

Wireshark, formerly known as Ethereal, is a popular network analysis tool that captures network packets and displays them at a granular level. Analysis of the packets allows for the detection of network problems and performance of troubleshooting. Although Wireshack can be used to view network traffic for network service quality, it cannot be used for intrusion detection. Learn How to use Wireshack - Wireshack Network Monitor Tutorial and How to use Wireshack Network Protocol Analyzer [Tutorial].

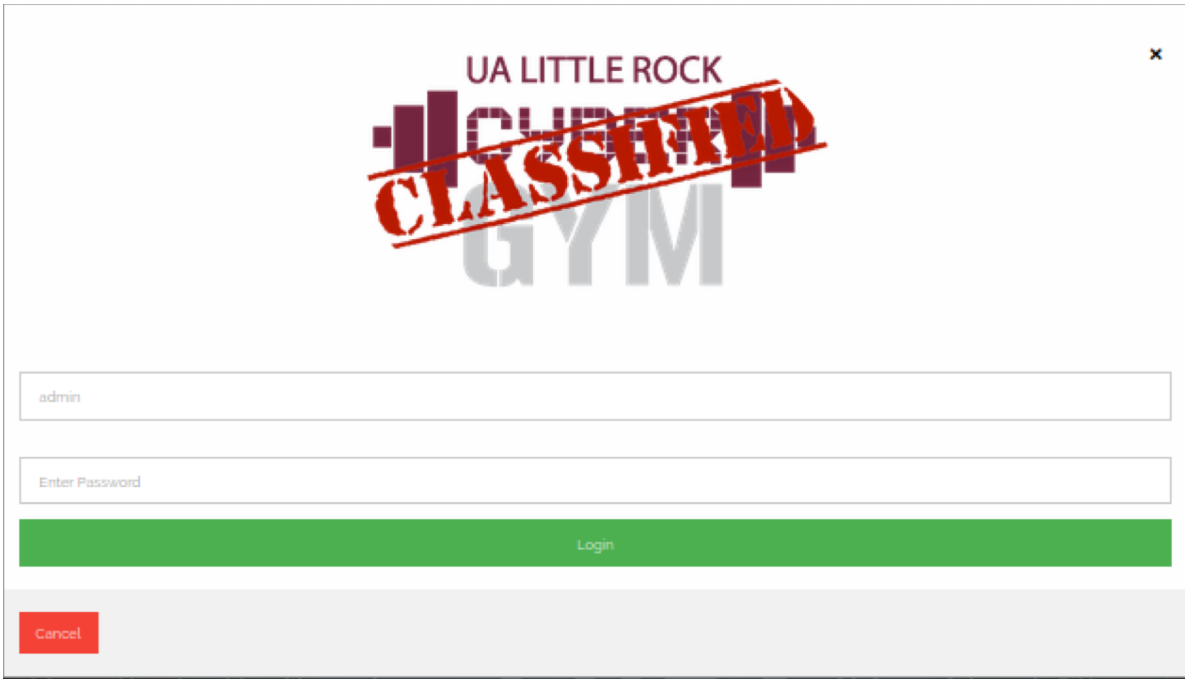
The goal of this workout is to allow students to interact with Wireshark, an open-source packet analyzer, to capture credentials to an intentionally vulnerable web application. Packets are full of user data and control information, and by capturing and analyzing them there is a lot to learn from them. It’s also important to note the security vulnerabilities that occur when transmitted data is not secured.

The Mission

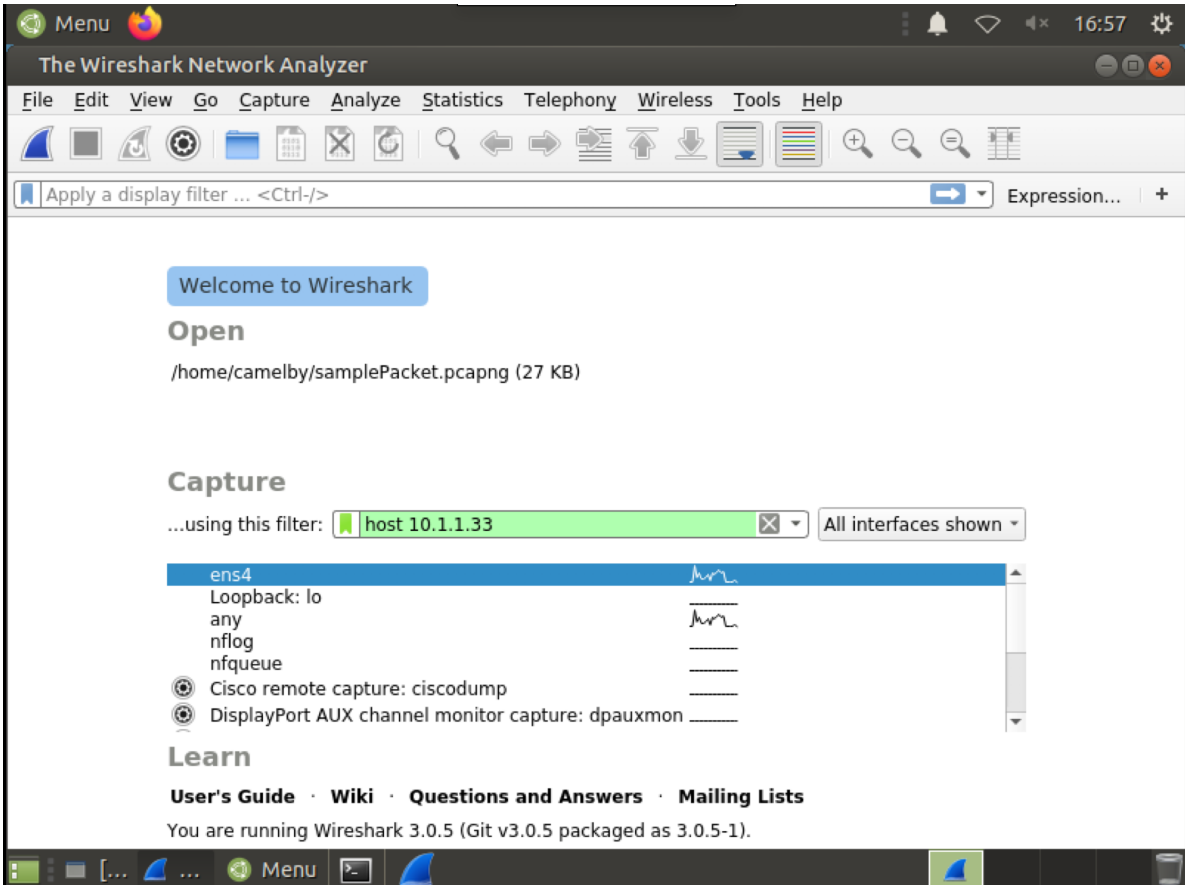
Students are introduced to a scenario that involves a *secret* web application at the IP address http://10.1.1.33:5000. When the students navigate to the web application they will come across a screen that looks like this.



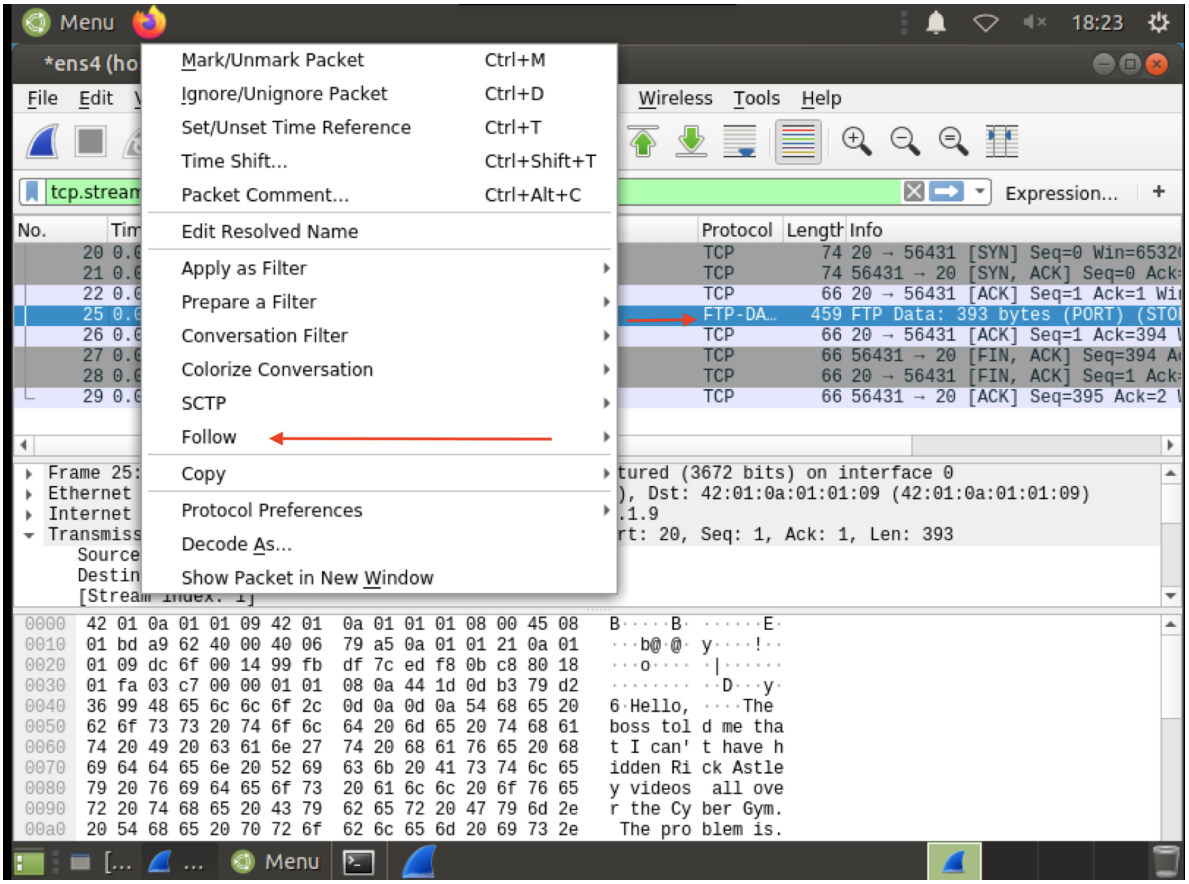
Once the students have reached this screen, they can click the login button. This will take them to a login form that they do not have the credentials to.



The goal of this workout is for the students to discover the credentials themselves. The only information they have is that suspicious activity is originating from the classified server and that they should use Wireshark to capture the packets. You can open Wireshark by clicking the blue shark fin at the bottom of the desktop. Once Wireshark is open, students must enter the capture filter: host 10.1.1.33. This allows the students to capture packets coming to and from their computer and the web application. The capture filter should look like this.



The students can either press ENTER or click the blue shark fin at the top left part of the screen. Students should then start capturing packets of data that contain the credentials of the web application. Data is populated every 15 seconds, so if they don't see anything immediately just wait a few seconds. The packet the students are looking for is under the protocol FTP-DATA that contains the file data of a text file. The text file holds the credentials to the web application and can easily be read by right-clicking the packet and following its TCP stream.



Once the students capture and analyze this packet they will have the credentials to log into the web application. Mission accomplished!

Questions for reflection

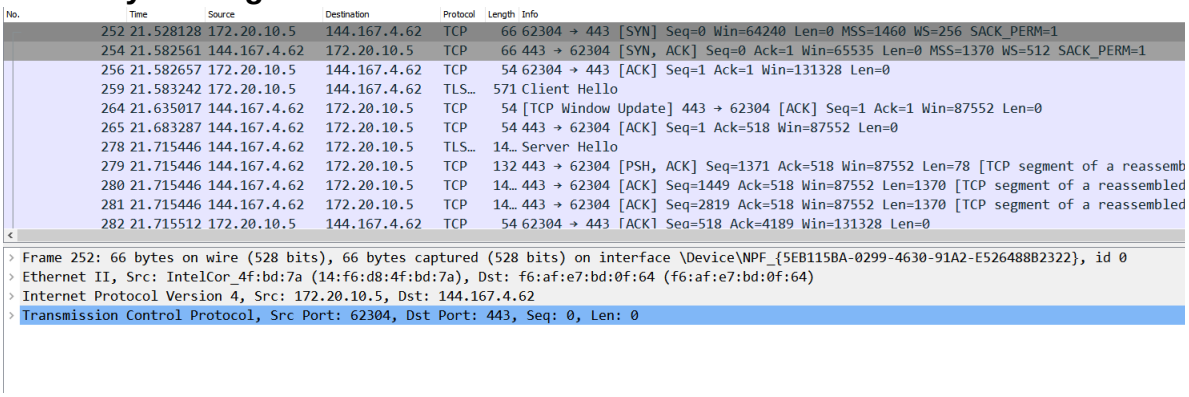
Question: What was the networking vulnerability you exploited to identify the website password?

Answer: The vulnerability was the use of network protocols that do not encrypt the application data. The data going across in plaintext allows adversaries with access to the network to eavesdrop on interactions between the hosts.

Question: What would you change about the system to prevent this type of reconnaissance from occuring while still providing a way to send messages back and forth?

Answer: Use encrypted protocols such as SFTP or SCP to ensure data does not go across the network unencrypted.

Question: Use the following packet capture to answer the next few questions. This capture includes a short https session. It's encrypted, which means you won't see the application traffic, but there are several other artifacts revealed by this capture. First, using arin.net, what is the handle for the entity owning the website?



Answer: UAALR-Z

Question: What can you find out about the client IP address communicating with the web server?

Answer: This is a private IP address for a local network

Question: Ethernet is used for the data link layer. From the MAC address of the client, who manufactured the network card?

Answer: Intel

Question: The destination router device is an Apple iPhone hotspot, which uses MAC address randomization (https://support.apple.com/en-us/HT211227). How might this improve user privacy?

Answer: This prevents correlating MAC address traffic across multiple locations. For example, the MAC Address could be used to track an individual as they connect to different wireless hotspots.