Familiarity With Wireshark

This lab aims to give Wireshark a basic familiarity and utilize its graphical interface to perform traffic captures. We will spend time using capture and display filters and getting used to the different outputs shown by the tool.

A user has brought their laptop to the helpdesk complaining of unusually long load times when they try to surf the web. They said it is almost as if the network is bogged down and the computer is making many different connections. We have been tasked with validating the pc is functioning correctly. To do so, we connect it to the network and start a packet capture while surfing the web. Analyze what can be seen in the output to determine if something is amiss. We only care about the laptop in question at this time, so filter out any traffic not destined to or sourcing from it.

ⓘ If you wish to take a more exploratory approach to this lab, I have posted the overall tasks to accomplish. For a more detailed walkthrough of how to complete each step, look below each task in the solution bubble.

Tasks

Task #1

`Validate Wireshark is installed, then open Wireshark and familiarize yourself with the GUI windows and toolbars.`

Take a minute and explore the Wireshark GUI. Ensure we know what options reside under which tabs in the command menus. Please pay special attention to the Capture tab and what resides within it.

Task #2

`Select an interface to run a capture on and create a capture filter to show only traffic to and from your host IP.`

Choose your active interface (eth0, or your Wifi card) to capture from.

▶ **Click to show answer**

Task #3

`Create a capture filter.`

Next, we want to create a capture filter to only show us traffic sourcing from or destined to our IP address and apply it.

▶ **Click to show answer**

Task #4

`Navigate to a webpage to generate some traffic.`

Open a web browser and navigate to pepsi.com. Repeat this step for http://apache.org. While the page is loading, switch back to the Wireshark window. We should see traffic flowing through our capture window. Once the page has loaded, stop the capture by clicking on the red square labeled Stop in the action bar.

Task #5

`Use the capture results to answer the following questions.`

Are multiple sessions being established between the machine and the webserver? How can you tell?

Cheat Sheet

Resources

Table of Contents

Introduction

- Network Traffic Analysis
- Networking Primer - Layers 1-4
- Networking Primer - Layers 5-7

Analysis

- The Analysis Process
- Analysis in Practice

Tcpdump

- Tcpdump Fundamentals
- Capturing With Tcpdump (Fundamentals Labs)
- Tcpdump Packet Filtering
- Interrogating Network Traffic With Capture and Display Filters

Wireshark

- Analysis with Wireshark
- Familiarity With Wireshark
- Wireshark Advanced Usage
- Packet Inception, Dissecting Network Traffic With Wireshark
- Guided Lab: Traffic Analysis Workflow
- Decrypting RDP connections

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

What application-level protocols are displayed in the results?

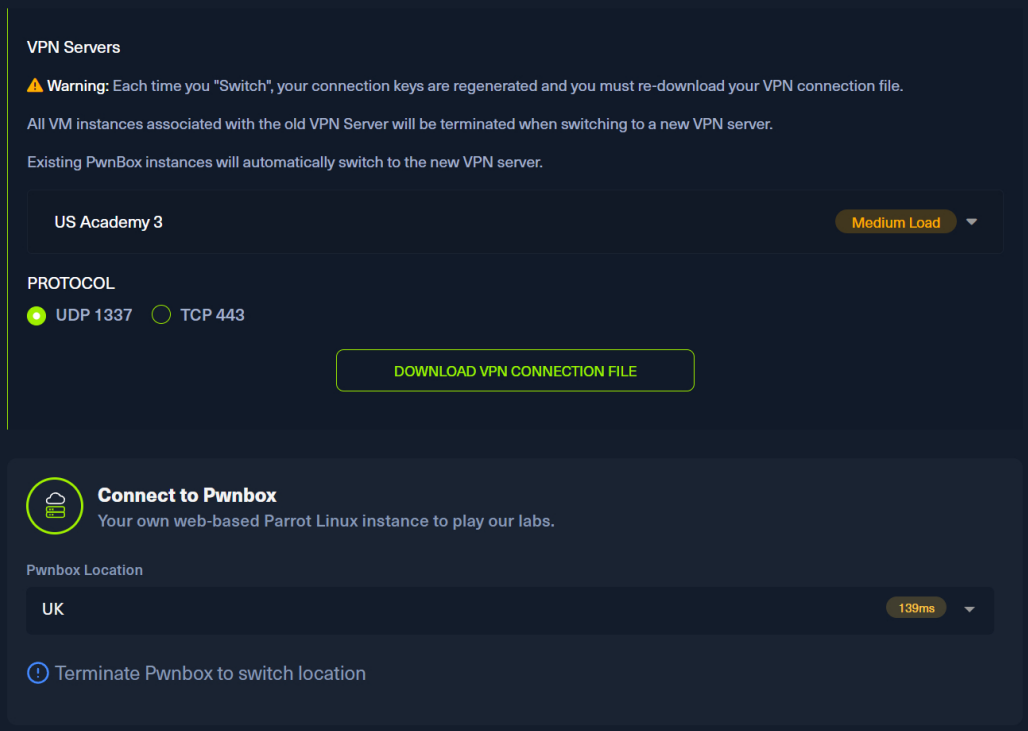
Can we discern anything in clear text? What was it?

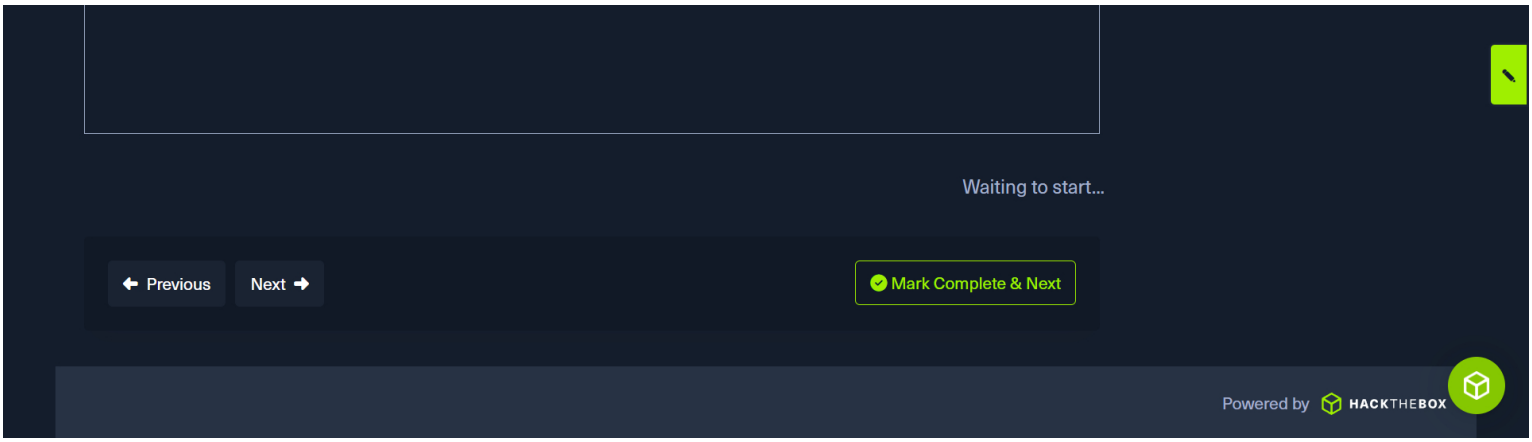
▶ **Click to show answer**

Don't stop here. Take some time to familiarize ourselves with the output Wireshark provides and how we can transform our view. We can also utilize the sample PCAP files found at https://wiki.wireshark.org/SampleCaptures to analyze different protocols and even things like ICS SCADA traffic and viruses. If you are connected to the Academy network to perform this lab, take some time to capture traffic on the interface provided. Some interesting network traffic can be found if one looks hard enough.

Summary

By the end of this lab, we should be familiar with Wireshark and how the GUI looks and operates. We have familiarized ourselves with the command bar and action bar and what resides within each respective tab. One should understand how to select an interface to capture with and successfully start a capture with a filter applied. Experiment with a few filters of your own design to see what different combinations can be used and how it shapes the results.




Waiting to start...
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX