

Wireshark Lab 4

ITSC 200: Network Protocols and Security

Table of Contents

[Lab Outcome(s) 2](#_Toc465173395)

[Reading 2](#_Toc465173396)

[Introduction 2](#_Toc465173397)

1. [Using Wireshark](#_Toc465173398)
2. [Capture network traffic with Wireshark](#_Toc465173398)
3. [Do basic analysis of Wireshark traffic 3](#_Toc465173398)

[References 4](#_Toc465173400)

Lab Outcome(s)

* Gain familiarity with Wireshark and basic network traffic analysis.

Reading

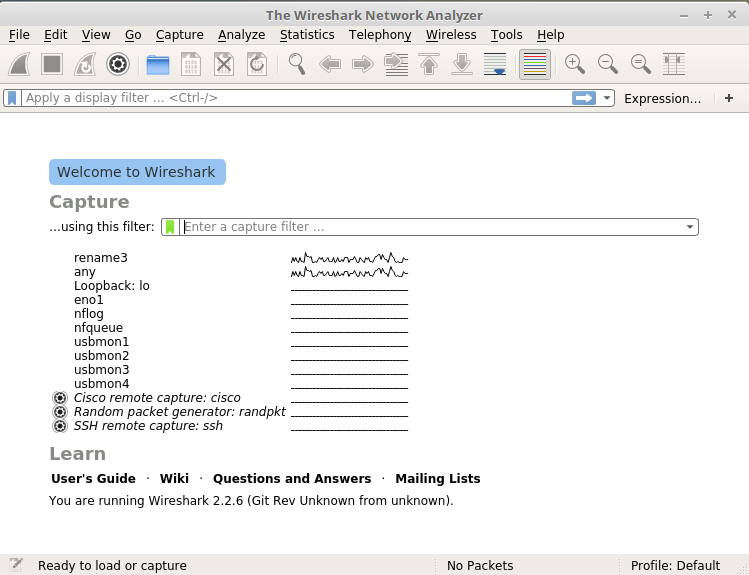
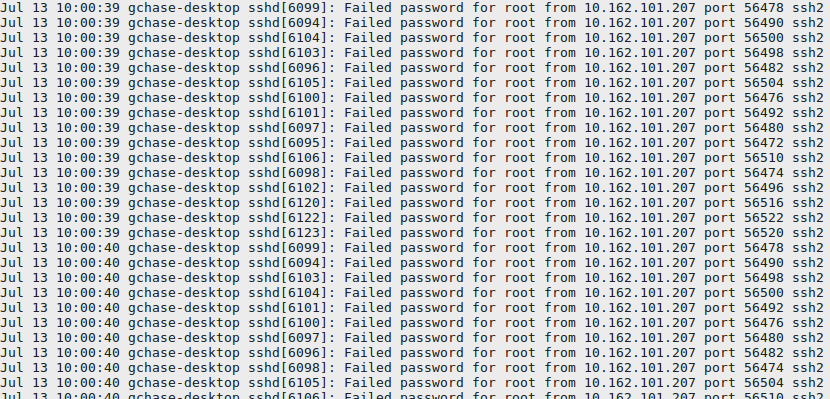
* None

Introduction

This lab is to familiarize you with using Wireshark to capture network traffic. You will learn the benefits and limitations of using Wireshark on a switched network. You will learn how to identify some common types of network traffic.

**Lab Submission :**

Use the pages below to answer the questions about the live Wireshark capture and the various Wireshark capture files that you have been given. Input your answers next to the questions and submit the completed document using the OS Lab 4 link in D2L (Brightspace).

1. Using Wireshark  
   1. Start Wireshark and note that it is not capturing traffic.
   2. Open the “interfaces” list and note the interfaces that are available. What are they ? (note: the screenshot below was done on a Linux computer so your display may be slightly different.)  
        
        
      
   3. What interfaces are actually registering traffic ? (since we haven’t started capturing traffic yet, the traffic can be seen as a line graph but is not actually being captured yet)
   4. Note that it is possible to capture USB traffic as well, although we won’t be doing that in this course.
2. Capturing Traffic with Wireshark  
   1. Note that we can apply a filter to restrict the traffic that we are capturing. We don’t normally do that as we can filter the traffic once we have captured it, however it can be useful on a very busy network where Wireshark has trouble keeping up with the amount of traffic.
   2. Close any web browsers or SSH sessions that you have open and double click on the interface that is “hearing” traffic. We could select the “any” interface here but why is that not the best way to capture traffic ?
   3. Don’t do anything on your computer, just capture traffic for about 15 seconds.  
      1. How many frames did you capture ?
      2. What protocol is the most common ?
      3. Which IP address is generating the most traffic ?
      4. Which transport layer protocol is the most common (UDP or TCP) ?
      5. Which “conversations” are creating the most traffic ?
      6. What is the one thing that might cause us to not trust the above information ?
3. Analyzing Traffic with Wireshark  
   1. Download the capture files for the lab if you haven’t done so already. Open the file student\_assign1\_who\_am\_I.pcapng in Wireshark.  
      1. What is the IP address of the computer that is doing the capture ?
      2. How can you be sure ?
      3. Can you determine an identifier for the Cisco switch that it is connected to?
      4. How many frames were collected in what amount of time ?
   2. Open student\_assign3.pcapng in Wireshark  
      1. What is the IP address of the computer doing the capture ?
      2. What can you learn from frame 299 ?
      3. What is happening in frames 308, 309, and 310 ?
      4. What is happening in frame 499 ?
      5. What is happening in frame 533 ?
   3. Open student\_assign4.pcapng in Wireshark  
      1. What is happening in this capture ?
      2. How do you know ?
      3. Who is doing it ?
   4. Open student\_assign5.pcapng in Wireshark  
      1. What is happening in this capture ?
      2. How do you know ?
      3. Who is doing it ?
   5. Open student\_assign6.pcapng in Wireshark
      1. What is happening in this capture ?
      2. How do you know ?
      3. Here is a screen capture of the /var/log/auth.log file ?  
           
         
   6. It is not always obvious what is going on in a capture but practice asking yourself some key questions.  
      1. Who is doing the capturing ?
      2. Can I see all the traffic ?
      3. Is this “normal” traffic ?
      4. Can I trust the source IP addresses ?

References

Linux\_cheatsheet\_1

Blank page if necessary to make pages an even number

**DO NOT DELETE THE SECTION BREAK BELOW. DELETING IT MAY IMPACT THE FORMATTING IN THIS DOCUMENT.**