With Support from National
Science Foundation &
National Security Agency
(Award# H98230-22-1-0098)

GenCyber 2023 Tennessee Tech

Hide and Seek

Student's Guide

Hide and Seek

Student Guide

Primary Concepts: Confidentiality, Think Like an Adversary

Table of Contents

Table of Contents 1

Overview 2

Learning Objectives 2

Summary 2

Definitions 2

Instructions 4

Step 1: Open PCAP File 4

Step 2: Find Information 4

Step 3: Extract PCAP Files 5

File 1 - Browsing Habits 6

File 2 - Grab the JPEG (webdl.pcap) 7

File 3 - Why not SFTP? 8

Rewards 9

Points to Ponder 9

Relationship with First Cybersecurity Principles 9

CERIAS Cybersecurity Education, Research and Outreach Center

Overview

This lesson demonstrates the basic concepts of information hiding and digital forensics.

Learning Objectives

After Completing this lesson, the student will be able to:

- Understand the basics of network traffic analysis (Understand)
- Examine information which might indicate unexpected activity on a network. (Analyze)
- Appraise detailed data from TCP data streams to support digital forensics investigations. (Evaluate)
- Investigate network traffic and extract useful information from a PCAP file. (Create)
- Critique which information can and cannot be sent in plaintext over the web, and why. (Evaluate)

Summary

You have accidentally come across a flash-drive dropped inconspicuously at CEROC. Succumbing to your curiosity, you have decided to investigate the contents of the drive. After scanning to be sure it contains no viruses or worms, you discover a collection of network capture files.

In this lesson, we will explore a variety of network packet capture files using Wireshark. Wireshark is a network protocol analyzer which allows for an in-depth review of packet captures from a variety of tools. The tool will allow us to visually inspect and filter the packets to discover interesting patterns.

In practice, these capture files allow security professionals to take in depth looks at network activity attempting to identify anomalous traffic patterns, patterns that might indicate malicious activity. These files can also be used to perform basic forensics

Don't be afraid to ask your teacher for help here. This is a difficult activity and will test how quickly you can adapt to new technology.

Definitions

- **Computer forensics** - The process and techniques used to analyze digital evidence and detect cyber crime
- **Capture the Flag** - Information security competition based upon the classic strategy game; common forms include Jeopardy, Attack-Defense, or mixed
- **pcap** - A packet capture which consists of variety of application programming libraries (APIs) for capturing various types network traffic
- **Network traffic analysis** - A process of acquiring meaningful information through network packet inspection and filtering
- **SSH** - Secure shell protocol that allows a secure remote login and other network services over an unsecured network
- **SFTP** - SSH file transfer protocol (or secure file transfer protocol) that provides means of file management and transfer over a secure channel
- **Wireshark** - Originally named Ethereal, a free and open source packet analyzer used for network troubleshooting, analysis, software and communications protocol development, and education
- **IP Address** - A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network
- **TCP –** Stands for Transmission Control Protocol, and is a connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network
- **FTP –** Stands for File Transfer Protocol, and is a set of rules that computers follow for the transferring of files from one system to another over the internet
- **Static IP –** An address that does NOT change
- **Dynamic IP –** A temporary address for devices connected to a network that continually changed over time
- **Error 404 –** The error code that is returned from a server when a file does not exist that matches the request made

Instructions

Step 1: Open PCAP File

More information about Wireshark can be found at https://www.wireshark.org/. As mentioned in the definitions section, a pcap file is a network packet capture file containing raw network packet data captured using one of several tools using a common application programming interface (API). In the Linux/Unix operating system, this is commonly implemented using **libpcap** shared library. For the Microsoft Windows operating system, the library is called **WinPcap**. These capture files allow us to simulate capturing packets on a live network or "sniffing" by replaying the pcap data file. In the following exercises we will use pcap files to perform our network traffic analysis.

1. Open the Wireshark application on your system.

2. In the Wireshark application, go to File → Open and then navigate to and select **capture.cap** (in Desktop → PCAP-files) as show in Figure 1.

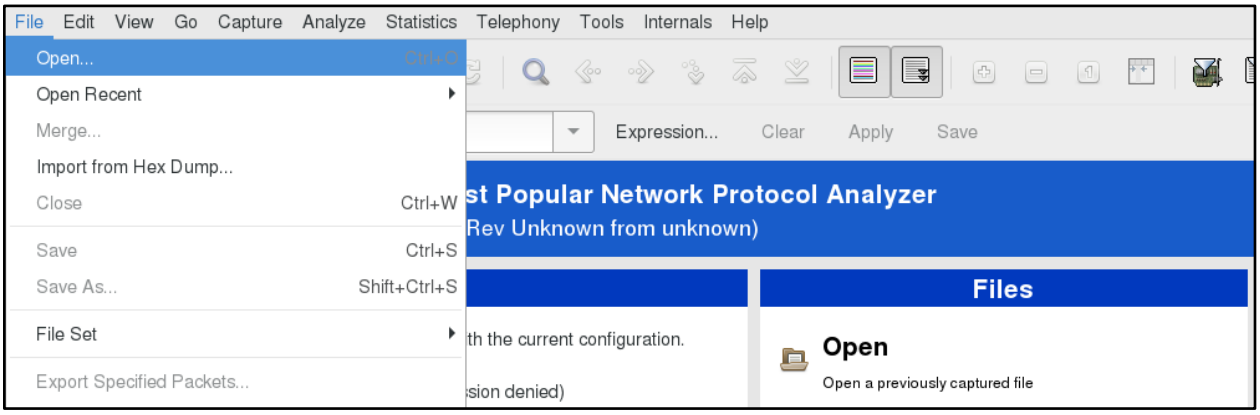


***Figure 1** - Opening capture file in Wireshark*

Step 2: Find Information

Once the file **capture.cap** has been loaded into Wireshark, review the data to determine the existence of any actionable information. **Note**: This activity is not an exact science and will require some working with Wireshark's filter system to improve the view of the data. The data will be "noisy" meaning there will be a lot of data which is not useful for our investigation. The noise can be reduced by adding a filter. For example, it is possible to apply an "**ip.addr**" filter which only shows packets going to or from a specific IP address. You can do the same for protocol. If you only want to see TCP traffic, you can filter that as well using the keyword "**tcp**". Try to weed out some of the info. As long as you can read some basic packets, you'll do fine. If not, ask a chaperone for assistance.

A. What are the names of the two parties in this communication? What are their IP addresses? (Hint: Try exploring the Statistics Tab)

B. What application (User-Agent) did the parties use to send messages (data) to each other?

C. What type of data (content type) has been transmitted?

D. Can you determine where one of the parties will be booking a flight to based on the content found in their messages?

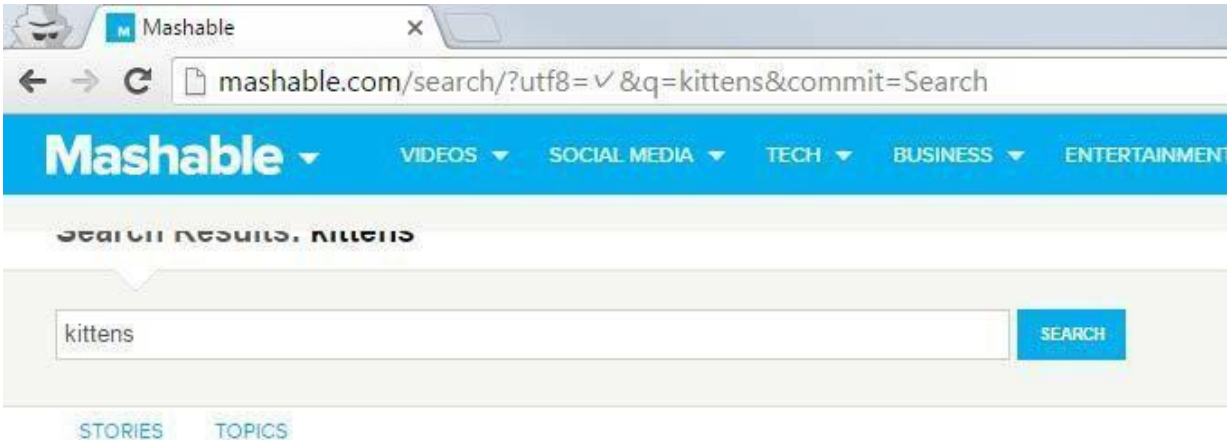
Step 3: Extract PCAP Files

Now that you have been given an example of how to extract information from a PCAP file, it is time to change up the types of data presented. The next few examples will present questions to be answered along with each accompanying PCAP file. Many of these are from past Capture the Flag competitions and represent the diverse applications encountered during these competitions.

File 1 - Browsing Habits

A friend interested in investigating the vulnerability of their network used Wireshark to create a PCAP file containing some of their local traffic. You were told that they visited Mashable.com; however, you wanted to see what else could be discovered in the file. This is a website, so you should check for web traffic. There is a specific protocol for this that you may know. There is some noise as well - things that aren't just Mashable.com. Explore and see what you can learn about scanning web traffic in the "**browsing-habits.pcapng**" file. (When looking for specific strings in certain protocol, you can use ***contains***. Example: **http contains "http://www.google.com"**)

A. What search engine (such as "Google.com") is used to find Mashable.com?



B. What search terms are used on Mashable.com? (Hint: filter using **http contains "mashable.com/search/?utf8=%E2%9C%93"** Also, try using the term **"/search**" in the find box after following a stream.)

C. List the URL of the article that your friend reads while on the site. (Hint: You can mark packets by clicking one and then pressing Ctrl+M. This can help you keep track of a packet when looking at the following ones.) (Hint: The article relates to the previous search terms)

Challenge Question

D. Other than the sites covered so far, name three additional websites visited in the PCAP file. (Hint: You can exclude packets by putting ***not*** in front of the desired filter. Example**: not http contains "http://www.google.com"**)

File 2 - Grab the JPEG (webdl.pcap)

To test the security of their web server, another friend sent you a PCAP file with a brief interchange between their computer and the server. Open and explore the "**webdl.pcap**" file to answers the questions below. (Hint: Try filtering by http traffic)

A. What files are downloaded? (Hint: Consider the definitions provided previously)

B. What three files are not downloaded? Why are the files not downloaded? (Hint: What error is being produced?)

File 3 - Why not SFTP?

Your friend from the previous question decided to also setup a Secure File Transfer Protocol (SFTP) server on their file server. They have decided to evaluate the security of the protocol by capturing traffic over a few days and sending the PCAP file to you. Start by opening the **"why-notsftp.pcap"** file. To deal with this file, you should try filtering to only see FTP traffic. Once this is done, you can find the answer to the first two questions.

A. What is a valid set of credentials for the SFTP server that was used to login?
   a. Username:

   b. Password:

B. What file is downloaded after the valid login?

Now, utilize the "**Follow > TCP Stream**" function in Wireshark by right clicking on any TCP packet that allows it (**Hint:** ACK stands for acknowledgement that some data has been transmitted successfully). Once you do this, you will notice a "**Save As**" button. If you have found the correct TCP stream from during the transfer, change the data type from ASCII to raw, and then you can use "Save As" along with the filetype from Question B. This can be done by adding ".zip" to the end of your filename. This will allow you to download the file itself and check it on your device, basically intercepting the traffic that was on the wire! From this you can find the answer to Question C. Question D can be answered by simply exploring packets and following streams

C. Open the file and describe what is contained within. (Hint: Be sure to extract this file from its zipped folder)

Challenge Question

D. Name one website visited by users other than the SFTP server (Hint: Recall what was used earlier when looking at website traffic to help narrow it down.)



Points to Ponder

Wireshark Analysis

Each of these exercises demonstrate the wealth of diagnostic information that can be derived from network packet capture files. Analysis of PCAP files using tools such as Wireshark allows security professionals to see events such as (not limited to)

- Identification of network-attached devices generating errant network traffic leading to a lack of availability of network resources
- Identification of the sources of denial-of-service attacks
- Identification of anomalous network traffic created by compromised systems such as bot traffic
- Identification of anomalous network traffic created by malware
- Discovery of activity timeline for network-attached devices disabled by internal and external attacks

Relationship with First Cybersecurity Principles

Cybersecurity has a specialized field for analysis and forensics. Analysis involves breaking data into more details like the Pcap files we used here, and then finding information that would otherwise be hidden. In forensics we piece together the information found in analysis to gain a better understanding of the overall situation. Here you analyzed several packets of information, found specific details, and then compiled it to understand what occurred at the time the Pcap files were recorded...

When we sniffed the network, we violated the basic concept of Confidentiality. We were able to tell who sent messages, who the messages were going to, and even the content of that message.