Interrogating Network Traffic With Capture and Display Filters

This lab aims to provide some exposure to interrogating network traffic and give everyone some valuable practice implementing packet filters. We will be utilizing filters like `host`, `port`, `protocol`, and more to change our view while digging through a .PCAP file.

Now that we have proven capable of capturing network traffic for the Corporation, management has tasked us with performing a quick analysis of the traffic our team has captured while surveying the network. The goal is to determine what servers are answering DNS and HTTP/S requests in our local network.

> 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

Utilizing `TCPDump-lab-2.zip` in the optional resources, perform the lab to the best of your ability. Finding everything on the first shot is not the goal. Our understanding of the concepts is our primary concern. As we perform these actions repeatedly, it will get easier.

Task #1

`Read a capture from a file without filters implemented.`

To start, let's examine this pcap with no filters applied.

▶ **Click to show answer**

Task #2

`Identify the type of traffic seen.`

Take note of what types of traffic can be seen. (Ports utilized, protocols, any other information you deem relevant.) What filters can we use to make this task easier?

What type of traffic do we see?

Common protocols:

Ports utilized:

▶ **Click to show answers**

Task #3

`Identify conversations.`

We have examined the basics of this traffic, now determine if you notice any patterns with the traffic.
Are you noticing any common connections between a server and host? If so, who?

What are the client and server port numbers used in the first full TCP three-way handshake?

Who are the servers in these conversations? How do we know?

Cheat Sheet
Resources
? Go to Questions

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

Who are the receiving hosts?

▶ **Click to show answer**

Task #4

`Interpret the capture in depth.`

Now that we have some familiarity with the pcap file, let's do some analysis. Utilize whatever syntax necessary to accomplish answering the questions below.

What is the timestamp of the first established conversation in the pcap file?

What is the IP address/s of apache.org from the DNS server responses?

What protocol is being utilized in that first conversation? (name/#)

▶ **Click to show answer**

Task #5

`Filter out traffic.`

It's time to clear some of this data out now. Reload the pcap file and filter out all traffic that is not DNS. What can you see?

Who is the DNS server for this segment?

What domain name/s were requested in the pcap file?

What type of DNS Records could be seen?

▶ **Click to show answer**

Now that we are only seeing DNS traffic and have a better grasp on how the packet appears, try to answer the following questions regarding name resolution in the enterprise: Who requests an A record for apache.org? (hostname or IP)

What information does an A record provide?

Who is the responding DNS server in the pcap? (hostname or IP)

Task #6

`Filter for TCP traffic.`

Now that we have a clear idea of our DNS server let's look for any webservers present. Filter out the view so that we only see the traffic pertaining to HTTP or HTTPS. What web pages were requested?

What are the most common HTTP request methods from this PCAP?

What is the most common HTTP response from this PCAP?

▶ **Click to show answer**

Task #7

`What can you determine about the server in the first conversation.`

Let's take a closer look. What can be determined about the webserver in the first conversation? Does anything stick out? For some clarity, make sure our view includes the Hex and ASCII output for the pcap.

Can we determine what application is running the webserver?

▶ **Click to show answer**

Summary

Through this lab, we expanded our horizons while utilizing TCPDump to analyze PCAP traffic. We learned how to capture and display filters effectively, dissected traffic to determine what protocols were running in the environment, and even gleaned some critical information about our enterprise segments, DNS, and Webservers. Continue to play on your own and see how deep the rabbit hole goes. Can you capture traffic in your home network and answer the same questions?

Tips For Analysis

Below is a list of questions we can ask ourselves during the analysis process to keep on track.

- what type of traffic do you see? (protocol, port, etc.)
- Is there more than one conversation? (how many?)
- How many unique hosts?
- What is the timestamp of the first conversation in the pcap (tcp traffic)
- What traffic can I filter out to clean up my view?
- Who are the servers in the PCAP? (answering on well-known ports, 53, 80, etc.)
- What records were requested or methods used? (GET, POST, DNS A records, etc.)

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 137ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

+ 1 What are the client and server port numbers used in first full TCP three-way handshake? (low number first then high number)

80 43806

Submit Hint

+ 1 Based on the traffic seen in the pcap file, who is the DNS server in this network segment? (ip address)

172.16.146.1

Submit Hint

Previous Next

Mark Complete & Next