Fundamentals Lab

The purpose of this lab is to expose us to tcpdump and give us time to familiarize ourselves with the terminal and utilizing tools within it. We will practice various tcpdump basics such as reading from and writing to files, utilizing basic switches, and locating files in the terminal. While completing these labs, we can explore and practice using different switches and functionality within tcpdump. When comfortable, take some time and try to determine if we can make out any traffic visible to us on the network.

Keep in mind that this type of work is often used to examine specific hosts and servers in more detail and find out who they all interact with. This procedure can also be used to identify so-called backdoors or other potential breaches. This could be used to monitor and log all communication from one server to analyze the packets sent and received. For the analysis itself, we then use various filters and patterns to filter out suspicious packets. We will look at this in another section.

As the new network administrator for the Corporation, we have been tasked with capturing some network traffic to help baseline and validate the Corporation's network. As a test, we start utilizing tcpdump to get a small capture of our local broadcast domain traffic to ensure our capture device will work to accomplish this task. We need to ensure the tools and dependencies required are installed and test our ability to read traffic and capture it to a file.

> 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 Tcpdump is installed on our machine.`

Before we can get started, ensure we have tcpdump installed. What command do we use to determine if tcpdump is installed on Linux?

▸ **Click to show answer**

Task #2

`Start a capture.`

Once we know tcpdump is installed, we are ready to start our first capture. If we are unsure of what interfaces we have to listen from, we can utilize a built-in switch to list them all for us.

Which tcpdump switch is used to show us all possible interfaces we can listen to?

▸ **Click to show answer**

Task #3

`Utilize Basic Capture Filters.`

Now that we can capture traffic, let us modify how that information is presented to us. We will accomplish this by adding verbosity to our output and displaying contents in ASCII and Hex. Once we complete this task, attempt it again using other switches.

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

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left

Disable name resolution and display relative sequence numbers for another challenge.

▶ **Click to show answer**

Task #4

`Save a Capture to a .PCAP file.`

Now it is up to us how we wish to capture and see the output. Remember, when utilizing capture filters, it will modify what we get. Grab our first full capture from the wire, and save it to a PCAP file. This will be a sample to baseline the enterprise network.

▶ **Click to show answer**

Task #5

`Read the Capture from a .PCAP file.`

Our team members have given us a PCAP they captured while surveying another section of the enterprise, read the PCAP file into tcpdump, and modify our view of the PCAP to help us determine what is happening. We can disable hostname and port resolution for simplicity and ensure we see any TCP sequence and acknowledgment numbers in absolute values. For the sake of the lab, utilize the PCAP file we created in the previous step for this task.

▶ **Click to show answer**

When done with the tasks above, please answer the questions at the bottom of the section to test our understanding.

Questions

Cheat Sheet

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

+ 0 What TCPDump switch will allow us to pipe the contents of a pcap file out to another function such as 'grep'?

-l

Submit Hint

+ 0 True or False: The filter "port" looks at source and destination traffic.

True

Submit Hint

+ 0 If we wished to filter out ICMP traffic from our capture, what filter could we use? (word only, not symbol please.)

not icmp

Submit Hint

+ 0 What command will show you where / if TCPDump is installed?

which tcpdump

Submit Hint

+ 0 How do you start a capture with TCPDump to capture on eth0?

tcpdump -i eth0

Submit Hint

+ 0 What switch will provide more verbosity in your output?

-v

Submit Hint

+ 0 What switch will write your capture output to a .pcap file?

-w

Submit Hint

+ 0 What switch will read a capture from a .pcap file?

-r

Submit Hint

+ 0 What switch will show the contents of a capture in Hex and ASCII?

-X

Submit Hint

Previous Next

Mark Complete & Next