Tools Used In The Analysis

Manpreet Parmar
April 13, 2023

Tools **3**
Suricata 3
Wireshark 3
Scripts **3**
combine.sh 3
csv.sh 3
ip_finder.sh 4
proc_logs.sh 4
suricata.sh 4

Tools

Suricata

Suricata is an open-source intrusion detection and prevention system that uses signature-based, anomaly based, and network-based detection methods to identify and prevent potential security threats. In regards to how it was used for analysis of the networks that were sniffed, I mainly used it to find specific signatures in the capture files of the two directories /ec2 and /log-server. Two rules were set up, which will be explained in the report, in order to create alerts on areas which I wanted to look into for any kinds of abnormal traffic. These logs were then saved for later use in cross referencing with IP addresses where areas of concern were placed.

Wireshark

Wireshark was mainly used when I wanted to dive deeper into a specific packet capture to look at areas of interest where there might have been some sort of malicious traffic going on. Using this tool allowed for a dissection of packets where I believed there was malicious traffic, which allowed me to find out more about the information regarding the packet.

Scripts

combine.sh

This script iterates over each of the pcapng files of a specified folder and runs the command "tshark -r <filename> -qz conv,tcp >> <outputfile>". This command gets all of the conversations in a pcapng file along with information like the amount of packets/bytes sent and received and outputs each conversation to an output.txt file.

csv.sh

This script takes in the output.txt file created by the script "combine.sh" and turns the columns of each conversation into columns of a csv file. Each row is a conversation and the columns are made up of all of the columns created by the output.txt file. This script was made so that I am able to sort the vast amount of conversations by things like the total amount of bytes sent in descending order, for conversations with the most data being sent.

ip_finder.sh

This script will return a pcapng file of a specified folder that has conversations that include a specified IP address. The purpose of this script is to find where in the capture files certain IP addresses that I wish to further investigate are, so that I can open up their pcapng files and look into the traffic surrounding them.

proc_logs.sh

This script goes through a specified log folder and searches for any logs in the log files that pertain to a specific IP address. If the address is not found in any of the files of the current directory, all other subdirectories are also recursively parsed in order to check the log files inside of them as well. If a line does contain the IP address listed, it will be outputted to a .txt file with the name of the log file from which it came from.

suricata.sh

This script allows me to iterate over a folder of pcapng files and use the suricata IDS to check for any alerts created by a pcapng file. To figure out which pcap file an alert came from, I have the contents of the log file catted to the console, so if I want to figure out where an alert was made from all I would have to do is find the first entry of it being catted and look at the name of the file that was echoed to the console.