Assignment 2

The purpose of this Assignment is to explore forming Malformed packets, their impact on some Target and writing a Script to Analyse the same

Assignment is in two parts, Part A

PartA

Forming Malformed Packets

Craft a TCP packet or set of TCP packets (using a tool or a piece of code) to send to a target (Target could be a firewall, WebServer etc), then observe the target's response with a packet capturing tool or view the results of those packet attacks in the log files on the target.

For example, you might alter a TCP SYN packet with information that is not usually found in the packet in order to see the response of your target to the malformed packet.

Show 2 such attacks and target's response. If you are successful in breaching the target, show the exploit (extra marks for this 😊).

<u>What to Submit</u>

What packets did you form and why? Snapshot of the same.

What was the observed response. Snapshot

Your Analysis

Part B Anomaly Detection

In this part, you will programmatically analyze trace data to detect port scanning activity. Port scanning can be used offensively to locate vulnerable systems in preparation for an attack, or defensively for research or network administration.

Example : In one port scan technique, known as a SYN scan, the scanner sends TCP SYN packets (the first step in the TCP handshake) and watches for hosts that respond with SYN+ACK packets (the second step). Since most hosts are not prepared to receive connections on any given port, typically, during a port scan, a much smaller number of hosts will respond with SYN+ACK packets than originally received SYN packets. By observing this effect in a network trace, you can identify source addresses that may be attempting a port scan.

Your task is to develop a Python program that analyzes a PCAP file in order to detect possible port scans. You MUST use dpkt Python library for packet manipulation and dissection.

The program can be for SYN scan or any other port scan

For more information about dpkt: • PyDoc documentation - pydoc dpkt • official website - https://github.com/kbandla/dpkt

You may also find this tutorial helpful: https://jon.oberheide.org/blog/2008/10/15/dpkt-tutorial-2-parsing-a-pcap-file Specifications

• Your program MUST take one argument, the name of the PCAP file to be analyzed: ex) python2.7 4.2.1.py capture.pcap

• Your program MUST print out the set of IP addresses which are possibly attacking (one per line). For the example of SYN print IP addreses that sent more than 3 times as many SYN packets as the number of SYN+ACK packets they received. For the purpose of this assignment, this rule applies even if the number of packets is very small.

For example, following cases are all considered as attacks: SYN=4 ACK+SYN=1 or SYN=4 ACK+SYN=0 or SYN=1 ACK+SYN=0

• Each IP address MUST be printed only once.

• Your program MUST silently ignore packets that are malformed or that are not using Ethernet, IP, and TCP.

Part B is disconnected from A. You need not use packets of Part A for analysis. Its your choice to choose a PCAP file.

What to submit:

1. What port scan you are analyzing, a Python program that accomplishes the task specified above. You MAY use standard Python system libraries, but your program SHOULD otherwise be self-contained.

2. Instructions on How to execute your program , sample input and output you received.

Reference : https://www.netscantools.com/nstpro_packet_generator_tcp.html

https://github.com/kbandla/dpkt/issues/232

https://jon.oberheide.org/blog/2008/10/15/dpkt-tutorial-2-parsing-a-pcap-file/

https://gendignoux.com/blog/2017/05/30/dpkt-parsing-http2.html