John Marinelli, Dillon Shaver

CSCI 5742

Homework 2

**Port Scanner and Port Scanner Detector**

This program includes a port scanner, PortScanner, and a port scanning detector, PortScanDetector. It demonstrates detection of port scanning using fan-out rate.

**PorScanner information:**

Using the Scapy library, this port scanner takes a target IP, start port, end port and wait time between connections and attempts a TCP connection with each port sequentially.

**PortScanDetector information:**

The port scanning detector listens in on network traffic, also using Scapy, in order to store and analyze first connections in a hash table. When those first connections cross one of three fan-out rate thresholds, port scanning is declared to the user.

**LAN setup:**

This program was tested on two Kali Linux virtual machines connected through a host-only virtual network.

**Discussion:**

The program works as intended, scanning and picking up traffic based on fan-out rate. In terms of scanning for TCP and picking up TCP and UDP traffic, it works well.

Some pitfalls in detection include not being able to pick up other, more complex, forms of port scanning. Due to the high volume of traffic that port scanning creates, the information complexity of detection is high, making performance an issue.

Much like other port-scanning detectors, when the interval between connections is longer, this program fails to pick up scanning.

Flaws in the scanning program include not being able to distinguish between closed ports and filtered traffic.

PortScanDetector picking up traffic from PortScanner:

Text

Description automatically generated

The scan from PortScanner that was picked up:

A computer screen capture

Description automatically generated with medium confidence