**Intrusion Detection System**

Adam Sin: 322453689

Eliyahu Fridman: 211691159

**Contents:**

1) Introduction

2-7) Structure

2) Docker, Attacker.py

3) Sniffer.py, Analyzer.py

4) TCP tests

5) UDP,DNS,ICMP tests

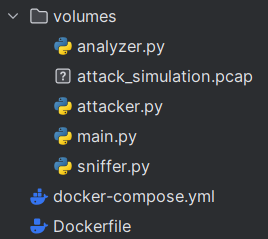
6) HTTP tests

7) TLS tests, Main.py

8) Summery

**Introduction:**

Our goal was to build an IDS focusing on packets suspicious of data exfiltration, looking only into the structure of the packets. The system will sniff traffic on an interface, test each packet, and add to the list of sniffed packets the general information of the packet, a flag of whether the packet failed a test, and the reason why it failed.

**Structure:  
**

**Docker-compose.yml & Dockerfile:**

We would like to run the IDS inside a docker container for a main reason:

**Isolation** - When we start to sniff the traffic, random packets that go through the traffic will get sniffed and tested, which is the point of the IDS, but when testing the system using TCP replay we don’t want any other packets to interfere with the process.

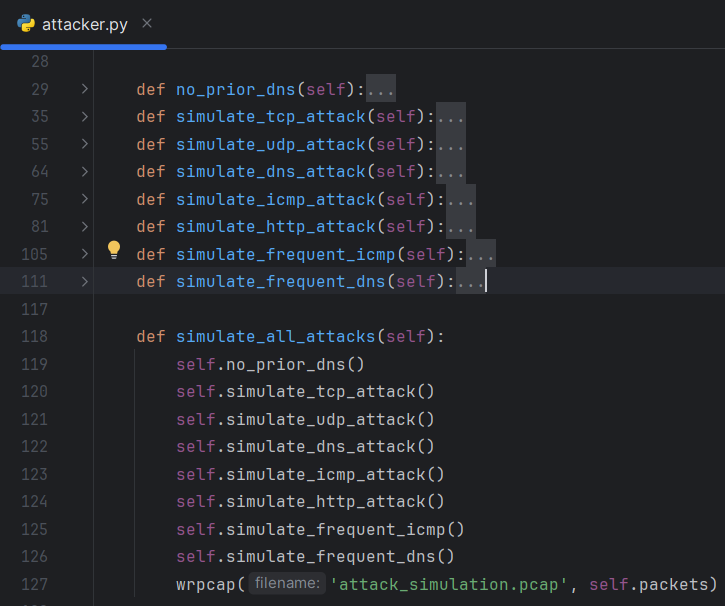
Docker-compose.yml will set up the container and Dockerfile contains the interfaces we want to install to run the IDS like tkinter, pyshark and more.

**Attacker.py:**

This script’s only purpose is to create “attack\_simulation.pcap” which is used for the TCP replay testing each and every test the analyzer conducts on the packets.

The script creates a list with 132 packets, most of them meant to be suspicious of data exfiltration while a small amount are valid and their purpose will be explained later. The list is them used to create the pcap file using scapy’s wrpcap function.

All of the packets are outgoing, meaning they are sent from our company’s internal IPs to unknown external IPs. Because internal traffic shouldn’t cause data exfiltration unless we have a physical mole, external traffic has nothing to do with our company, and the assignment says to not test ingoing packets (from outside in).



**Sniffer.py:**

The class that will be later used in the main IDS script, is responsible for sniffing and storing every packet coming through the traffic using pyshark’s LiveCapture function.

The sniffer has a Queue which is the buffer, this buffer is later used by the analyzer to test the packets.

It also has a flag that determines whether to keep sniffing the traffic or stop.



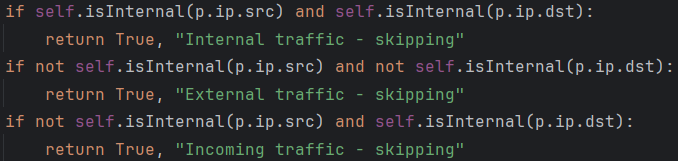
**Analyzer.py:**

Here we conduct all the tests on the packets, to look and flag the suspicious packets.

Validate will go through the buffer for as long as the sniffer runs and there are packets to validate.

isValid returns for each packet whether the packet is valid or not using the functions we’ll expand on



Like said earlier, packets that are not outgoing don’t interest us:  


**tcp\_handle:**

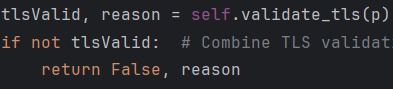
Checks for usual tcp packet ports for secure traffic. Unusual ports may indicate tries to leak data unnoticed. More secure ports can and should be added.



Tests for HTTPS packets on TCP protocol



A https packet must pass security tests, which is its purpose (tls tests are explained later)



https packets sized more than 1460 bytes is unusual, we won’t allow sending so much data.

תמונה שמכילה טקסט, גופן, צילום מסך, גרפיקה

התיאור נוצר באופן אוטומטי

Unusually large TCP size might be a sign to leaked data in the payload



If

תמונה שמכילה טקסט, גופן, צילום מסך, גרפיקה

התיאור נוצר באופן אוטומטי

PSH flag means packets that should be processed by the receiver before any other given packets in the buffer. A packet too big of that importance might indicate a try to process and get the data fast.

תמונה שמכילה טקסט, גופן, צילום מסך

התיאור נוצר באופן אוטומטי

URG flag means packets with some important info that should be processed by the receiver before any other given packets in the buffer. A packet too big of that importance might indicate a try to process and get the data fast.

תמונה שמכילה טקסט, גופן, צילום מסך

התיאור נוצר באופן אוטומטי

**udp\_handle:**

If the udp packet has an unusual port



If



**dns\_handle:**

If



if



if

תמונה שמכילה טקסט, גופן, צילום מסך, טיפוגרפיה

התיאור נוצר באופן אוטומטי

if



if



if

תמונה שמכילה טקסט, צילום מסך, גופן

התיאור נוצר באופן אוטומטי

if

תמונה שמכילה טקסט, גופן, צילום מסך

התיאור נוצר באופן אוטומטי

**icmp\_handle:**

if



if



**http\_handle:**

if



if

תמונה שמכילה טקסט, גופן, צילום מסך, קו

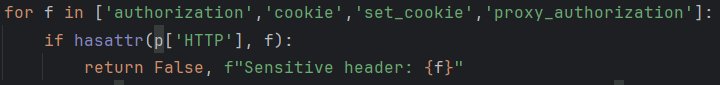
התיאור נוצר באופן אוטומטי

if

תמונה שמכילה טקסט, גופן, צילום מסך, גרפיקה

התיאור נוצר באופן אוטומטי

if



if



if



if

תמונה שמכילה טקסט, צילום מסך, גופן

התיאור נוצר באופן אוטומטי

if



**validate\_tls:**

if



if

תמונה שמכילה טקסט, גופן, צילום מסך, טיפוגרפיה

התיאור נוצר באופן אוטומטי

if



if



if



**Main.py:**

Combines the scripts to work together in order to simulate the IDS sniffing, analyzing,statistics and testing stages.

