Lab X – Intrusion Detection

Assistants

Johannes Blaser
Nicole Dolot
Tom Kersten
Frederick Kreuk
Kyrian Maat
Jullian Verweij
Lu Zhang

Ask questions during the labs. No labs left? Create a question on TicketVise.

Lab dates

Thursday October 8th, and Friday October 9th 2020

Deadline

Friday the 9th of October 2020 23:59

Total points

5 bonus points

This lab is done in pairs.

1. Lab X

This lab is called Lab X because it is a bonus mystery assignment. Lab X does not count towards the minimum required points to pass the practical part of NNS. Instead, we provide you the opportunity to freely explore some network attacks, and earn some free points while doing so.

2. Abstract

In this lab you will receive **three** PCAP files. These files will contain network-based attacks. Your task in this assignment is to write code to detect this attack and classify the type thereof. The attacks are all different types of DDoS attacks. Your perspective is that of the network engineer, trying to protect their network against these DDoS attacks. Ideally you want to classify attacks so that you can create filters to omit malevolent traffic. This is your task in this assignment.

3. Submission

IMPORTANT: Make sure your code is PEP8 compliant.
IMPORTANT: Make sure your code works on GNU/Linux
IMPORTANT: Make sure your code is well-documented!

You can check your code by installing a PEP8 linter, or using an online checker. Points will be subtracted (up to not being graded) for bad formatting, style, and/or lack of comments.

Submit your working code in an archive called `labX-<group_number>.zip` (or `tar.gz`). For example, labX-03.zip. It should contain at the very least the following files:

- **Python script:**
  - Naming convention: `derive_attack.py`.
- **Output file:**
  - Naming convention: `attack.md`.
- **Feedback file:**
  - Naming convention: `feedback.md`.

IMPORTANT: Please make sure you strictly follow the format for the contents.

4. Assignment Description

Along with this assignment you will find some PCAP files containing an attack. The attacks can be of different types. Your task is to classify the type of attack, and derive an *attack fingerprint* from the PCAP files.

a. SYN flood

The first PCAP file (`easy.pcap`) we supply is simple, and will contain a straightforward SYN flood attack. In this attack an attacker keeps sending SYN packages, but never replies to the returned SYN ACK with another ACK. This leaves connections in a sort of *limbo*. Think about what the unique characteristics and patterns are of such a SYN flood attack, and write code to detect this.

b. DNS based attacks

The second PCAP file (`medium.pcap`) contains a DNS based amplification attack. This is the more advanced part of this assignment, so be creative in what makes a DNS amplification attack unique, and how you could detect this. Then, write code to detect this attack.

c. Fragmentation attack

Another attack vector is exploiting fragmentation. The last PCAP file (`hard.pcap`) that contains an attack that exploits fragmentation of packets. Think about how fragmentation can be used to launch a DDoS attack, and how you can detect it in code. Write that code.

d. Percentage of traffic

Your last task is to "apply" your filter. You don't have to do any actual filtering though. Instead, just imagine your filter has been applied. To do this all traffic that matched the fingerprint you have generated will be omitted.

Now, your task is to deduce how effective your filter has been. To do this you have to determine how much of the traffic of **each PCAP file** would be filtered, if your filter would be applied. You have to determine **the percentage of the total traffic** your fingerprint filtered, as well as **the percentage of source IP addresses** your fingerprint filtered (i.e. that matched your fingerprint).

5. Submission Format

Your code should produce an *attack fingerprint.* Submit your working Python script with the following naming convention: `derive_attack.py`. The output attack fingerprint should have the following format:

```
Attack type: SYN-FLOOD/DNS-AMP/FRAG
Victim IP: X
Source: IP.port
Percentage traffic: X%
Percentage IPs: X%
```

You should also submit a Markdown file (.md) containing your findings. Your code needn't generate this file automatically. This file should have the following structure:

```
# PCAP 1
Attack type: SYN-FLOOD/DNS-AMP/FRAG
Victim IP: X
Source: IP:port
Percentage traffic: X%
Percentage IPs: X%

# PCAP 2
Attack type: SYN-FLOOD/DNS-AMP/FRAG
Victim IP: X
Source: IP:port
Percentage traffic: X%
Percentage IPs: X%

#PCAP 3
Attack type: SYN-FLOOD/DNS-AMP/FRAG
Victim IP: X
Source: IP:port
Percentage traffic: X%
Percentage IPs: X%
```

Lastly, your submission should contain a Markdown feedback file (feedback.md) where you can let us know what you thought of this assignment. You do not **have** to submit feedback, but we'd very much appreciate it!