An introduction to Intrusion Detection Systems

Intrusion Detection Systems (IDS) are a first line of defense in enterprise networks. These systems monitor a network or systems for malicious activity or policy violations. Their operation relies on filtering the network traffic against a predefined ruleset. This ruleset usually consists of known malicious traffic patterns, which can be a clear indication of intrusion. The key idea of IDS/IPS is to capture and mitigate malware and exploitation attempts on the network level, before reaching the end (vulnerable) device or application. Moreover, such systems can detect and mitigate the propagation of malware in an infrastructure and execute mitigation strategies.

In this assignment you will get familiar with Snort IDS/IPS (https://www.snort.org/). Snort is one of the most popular IDS/IPS solutions that is also supported by a large user community which offers open-source signatures and rulesets. The goal is to write different rules that will produce an alert when the scanned traffic matches them. You can find Snort and installation guidelines in the following github repository (https://github.com/snort3/snort3.git).

Steps

1. Download and install Snort from github by following the instructions.
    a. Make sure to also install the dependencies required.
    b. You can also download Snort from linux repositories, however it is preferable to also read about the various components which comprise the functionality of Snort
2. Test the installation by running Snort in packet parsing mode, you can use the pcap file provided in Assignment 4
   `$ snort -r test_pcap_5mins.pcap`

Setting up the rules:

For the assignment you need to implement and run the following set of simple rules and report their output in your report, you can find the documentation for the rule syntax in the following link (https://docs.snort.org/rules/)

- Report any icmp connection attempt in **test_pcap_5mins.pcap**
- Find all packets which contain “hello” string in **test_pcap_5mins.pcap**
- Report all traffic between non root ports (port number > 1024)
- Create a rule that will detect ssh brute force attacks in **sshguess.pcap** file
    - A brute force attempt can be realized as 10 attempts within 10 minutes
- Setup the community rules (run snort with associated snort.conf) and report any clear indicator of malicious traffic in **test_pcap_5mins.pcap**
    - Some community rules clearly state the exploit detected

Notes

1. You are provided with a sample packet capture to test your program. Its duration is 5 minutes. You are also provided with a pcap trace containing ssh key guessing attacks.
2. You need to create a README with your name, your AM short descriptions of the rules and their results
3. You must submit the following files: README and simple.rules.
4. You should place all these files in a folder named <AM>_assign6 and then compress it as a .zip file. For example, if your login is 2020123456 the folder should be named 2020123456_assign5 you should submit 2020123456_assign5.zip.
5. Use the tab “Συζήτηση” in courses for questions.