EE6042/ET4028 Host & Network Security
Intrusion Detection Systems Assignment

1. Task

In this assignment you are asked to use Snort to perform intrusion detection. Each student must undertake their own assignment – any duplicate solutions will receive 0 marks.

Proceed as follows:

- Setup a test environment with a victim machine, an IDS machine (Snort) and an attacker machine. Note the following:
  - Victim and IDS can be the same machine.
  - If different machines are used, make sure that IDS will see all traffic directed at victim. You most likely need to put your IDS's NIC into promiscuous mode, if using a switch (virtual or physical) you may need to use a spanning/mirror port - cf. https://community.cisco.com/t5/network-architecture-documents/how-to-configure-port-monitoring-span-on-a-catalyst-2940-2950/ta-p/3132032 and https://en.wikipedia.org/wiki/Port_mirroring.
- Mount at least three different (types of) attack from attacker against victim (make sure that these are truly different attacks, for example all types of port scan count as same type of attack - see note below). I recommend to utilize tools such as NMap, Metasploit or others to mount these attacks.
- Note: you **cannot use any of the rules discussed in the lecture notes**!
- Make sure that Snort is detecting your attacks (either change attack or adjust/add snort rules).
- Also, reduce the number of rules active in your snort configuration to minimize your log file. It is ok if the log file contains several other entries, but its size should be manageable (at most KB, preferable small KB)
- For each attack record and submit:
  - Your snort log file (it can be a single log file containing detection of all three attacks) – make sure it is at most KB in size, preferably small KB.
  - Identification of the location in the log file where your attack has been detected (line number when opened in text editor). Do not convert the log file – please submit in original Snort format to ensure detection is present in log file.
  - Identification of the snort rule (included in your snort.conf file) that is responsible for detecting the attack.
  - A description of all the components/options of the rule that detected the attack. Make sure that the following options are used at least once among your rules:
    - content
    - pcre
    - flow
    - itype

Note on "different (types) of attack": The idea here is to use different detection mechanisms - thus, all port scans count as the same type of attack. On the other hand, buffer overflow attacks against different services/applications would count as different types of attack (even though they are buffer overflows (same kind), their detection is pretty much unrelated (different type)).

2. Deliverables

The following needs to be submitted for this assignment:

- Snort log file (or multiple log files) that contain(s) information about the detection.
- Snort configuration file (snort.conf) that contains your used detection rules (make sure that your rules are visible in this file – if you use include statements, make sure to also submit the included file and indicate file/line number for each rule).
- Report (only MS Word (.doc/.docx), Rich Text Format (.rtf), plain text (.txt) and Portable Document Format (.pdf) are accepted) that contains the following:
    - Short description of each mounted attack.
    - Identification of line number in log file where your attacks are located (if not provided, I assume **log file does not contain** this information).
    - Identification of line number in snort.conf where your detection rules are located (if not provided, I assume configuration **file does not contain rules**).
    - Description of all the components/options of your used detection rules (make sure that options content, pcre, flow and itype are used at least once among your rules).

These deliverables need to be submitted as individual files. Do not use any archiving software such as zip or rar to combine or compress your files.

3. Deadline and Marking

Deadline for submission of your solution is **17:00h (Irish Time!) on Friday, 9th April**. Where I have concerns about the originality of the submitted work, I reserve the right to conduct interviews (via Skype, Zoom or similar) with students, where marks will be adjusted correspondingly.

Marks are distributed as follows:

Description	**Marks**
Description of mounted attacks (3x1)	3
Snort Log File contains detection information (3x1)	3
Snort.conf contains rule according to attacks (3x1)	3
Description of components of each used rule (3x2):	6
Penalties: • No content option used • No pcre option used • No flow option used • No itype option used	 -15% -15% -15% -15%
Total:	**15**