ENPM685 Homework #6 – Intrusion Detection

Version 1.3 – April 1st 2022

Estimated time to complete this assignment: 2 hours.

The packet capture files can be downloaded from ELMS or the class Google Drive share

Part 1

Download **homework6.pcap**, review it and complete the 2 steps below. This is a packet capture of a successful SQL injection attempt.

You are an analyst that was given this packet capture to analyze. You quickly detected that it was a SQL injection attempt and appears to have been successful as packet #34 shows some data from a database being send back to the attacker. You also detected that the SQL injection attempt was done with a tool called sqlmap. You have been asked to write 2 snort rules to help detect this kind of activity on your network specifically targeting web servers listening on port 80.

1. Write a rule to detect a generic SQL injection attempt using a UNION query.
2. Write a rule to detect the use of sqlmap.

You can use the **homework6.pcap** packet capture to help ensure your rules work as intended.

Remember the basic snort rule format:

```
action protocol src_ip src_port -> dest_ip dest_port
(msg:"description"; insert-rule-options-here; sid:100001;)
```

Part 2

Mike is a young SOC analyst who was reading about SQL injection after discovering the following link: https://en.wikipedia.org/wiki/SQL_injection

He quickly developed the following rule:

```
alert tcp any any -> any any (msg:"SQL injection discovered!";
content:"' OR 1=1"; sid:100002;)
```

While this rule works it could use some improvement. What advice would you give Mike to help improve his rule?

Deliverables:

Part 1: Both of your rules
Part 2: Your recommendations on how to improve Mike's rule.