**QUESTION 1**

1. You will use your SecurityOnion VM to complete the homework questions in this assignment.  The lecture slides will tell you how to access your VM via RADISH.  If you missed class, make sure to perform the in-class labs in the lecture slides prior to starting the homework.

During the lecture we replayed the Crimeboss pcap\_a file into the eth1 interface to feed that data to the IDS just like it happened in real-time (slides 86-87).

\*\*Note:  I would also recommend deleting the sguil events from the in-class lab before starting this question.  You can click on the top event and hold down F8 to clear them.  Then replay pcap b.

For this question, you will need to replay the pcap\_b.pcap file and then use Sguil, Squert, Snorby, and ELSA to analyze what happened from the pcap\_b traffic.  Keep in mind that it may take a minute or two for the pcap b data to appear in the tools.  If it does not appear, you may need to replay the pcap again.  Free free to use additional tools contained in SecurityOnion if you would like.  You will answer this question by submitting a report documenting your findings.  The report must contain paragraphs explaining what happened overall in the pcap and must contain the following information:

1.  What hosts, URLs, or IPs from the victim and any malicious traffic are involved?

2.  What malicious traffic occurred and what does it mean?

3.  What malicious files were downloaded by the victim and what do you think their functionality was?

4.  What are the main malicious snort rules/events that fired based on traffic or downloads?

5.  Provide at least one screenshot from your VM's Squil, Squert, Snorby, and ELSA with each screenshot relevant to the pcap\_b data.

**QUESTION 2**

1. Write your own new local Snort rule that detects and reports something that happened in pcap\_b.pcap from the prior question.  (It cannot be a rule that already fired from Snort that you viewed in Sguil.)   Slides 115-132 will help you.

Your rule could detect something in the packet payload with the "content" field (like we did in the in-class snort rule with the "content" field or you can try to detect something else).  You don't have to detect something malicious, it can really be anything.  I just want you to write a rule that detects something inpcap\_a, replay pcap\_a, and then show the fired rule in Sguil.  The "msg" portion of your rule must contain your full name in it.  The full snort documentation for creating rules can be found at the below link:

http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html

If you would like to become fluent at writing snort rules, I would recommending becoming familiar with all of the information in the prior link.  You could also just read each "Quick Reference" section and then select any rules you are interested in to read more about them.

After you write your rule, you will need to reload the rules and then replay the pcap file to see if Sguil detects your new rule as mentioned above.  Remember that sometimes it takes a few minutes for the replay data to appear in the tools.  If your rule doesn't show up after a few minutes then you might need to replay the packet again.  If you see "Fail" after reloading the rules, you most likely have a typo or syntax error.

To answer this question, upload a document that contains your Snort rule and shows a screenshot of it firing in Sguil.  Remember, the "msg" portion of your rule must contain your full name in it to receive credit.

**QUESTION 3**

1. Extra credit:

Follow the same tasks as homework question 1 but this time replay and analyze pcap\_c.pcap.  Upload your finished report here.

* 1. Attach File

**QUESTION 4**

1. This is just a reminder that your individual project slides and video are due April 11, before class at 5:30pm.  You will upload them in the "Project Info" folder in Blackboard in a zip file to the "Individual Project" assignment.

Answer "True" below to acknowledge that you have read this.

 True

 False