**Edumanichukwu Nwachukwu**

**CYBR 445 - Advanced Incident Detection and Response  
Module 5 Lab – Advanced Network Intrusion Detection-Prevention**

* **Given the information you examined on the dashboards, what is some of the useful information generated by Suricata and stored in Elasticsearch?**

I like the fact that I can see all different sorts of alert types. I do like the SN-ALERT-Eventslist because the overview information on the IP addresses affected by threats.

* **Examine the rule. Given your study of Snort/Suricata rules this week, what is the rule looking for?**

**I’ll be looking out for the “alert tcp $HOME\_NET 445 -> any any” which triggers an alert when a TCP traffic originally coming from the defined “$HOME\_NET” on port 445 is detected.**

****

* **Paste a screenshot of your triggered rule below.**

**My rule was not triggered. I tried to check if I made any mistakes when typing out the rule but yet nothing worked.**

A screenshot of a computer

Description automatically generated with medium confidence

* Paste your rule

A screenshot of a computer

Description automatically generated with low confidence

* How many exact packets does this packet capture have?

4156081

* **Were you able to find anything suspicious in the Wireshark packets shown?**

I did see some flagged TCP and DNS requests traffics that is suspicious.

* Paste screenshots of the information in each file below

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

* What kind of information do find in each file?

conn.log - contains incoming connection logs.

dns.log - contains recently logged DNS requests.

files.log – contains file requests.

ssl.log – contains recent socket layer connections.

x509.log – contains TLS connections.

weird.log – contain usual activities.

* Is this information easier to process than raw packet captures in Wireshark?

It is not easier. It’s very complex to read. Raw packets captured in Wireshark can be easily analyzed using built-in tools provided in Wireshark.

* Examine the Beacons table and then the Beacons FQDN tab. Which single FQDN is probably hosting a C2 server?

alpha.saintjameschurch.org

* How man separate connections have been made to the FQDN?

20054

* What is the Beacon Score? The score ranges from 0 to 1 with 1 representing the highest beacon score.

1.0

* Examine the DNS tab. Which base domain name is probably being used for DNS exfiltration or C2?

r-1x.com

* How many unique records (subdomain count) have been requested from this domain?

62468

* How much higher is this than the next most requested domain?

There is a difference of “2” from the most requested domain.

* Click on the Long Connection tab. How many different IP addresses have suspiciously long connections (connections over 1000 seconds in duration)? List the IP addresses below. Note there are a number of duplicates.

10.55.100.100

10.55.100.103

10.55.100.104

10.55.100.105

10.55.100.106

10.55.100.107

10.55.100.108

10.55.100.109

10.55.100.110

10.55.100.111

* Click on the User Agents tab. User Agents are a browsers self-report identity included in web requests. Which single User Agent is suspicious? Why?

The “Empty user agent string” is the most suspicious user agent. It has a high number of times used and it’s not properly named. It seems odds from the others.