Lab 06 – Security Onion

In this lab, you will use Bro logs to look at information collected from a traffic capture and derive conclusions about the traffic.

Use the server at https://ctf.eh200.xyz:8443/app/kibana to complete this lab.

The credentials to login are dsu/Password1!

Answer the following questions below with both the **answer AND a screenshot** showing how you got your results.

Add a filter for 192.168.19.225.
Change time to all time.

1. What are the two most common destination ports for this IP, by total bytes transferred?
2. What destination connection did 192.168.19.255 talk to most, in terms of bytes?
    a. Can you figure out what this IP is?
3. What destination IP did 192.168.19.225 talk to most, in terms of number of connections?
    a. Can you figure out what this IP is?
4. How many DNS requests did 192.168.19.225 make? What server was it using?
5. What domain did 192.168.19.225 request most often?
6. What username was used to log in to the FTP server?
7. What two file names were downloaded from the FTP server?
8. What system was browsing to the FTP server? That is, what IP address is the client at?
9. When browsing to a website, 192.168.19.225 got an HTTP 301 Moved Permanently response. Which IP address provided this response?
10. Bro found quite a bit of traffic that it categorized as weird. What were they? Conduct a bit of research – would you say this traffic is weird? Would you say it is malicious? Explain the various types found.