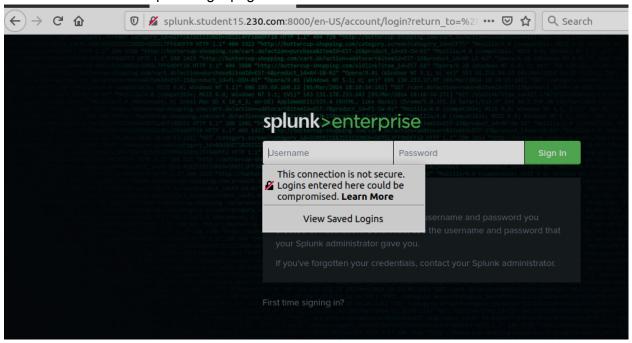
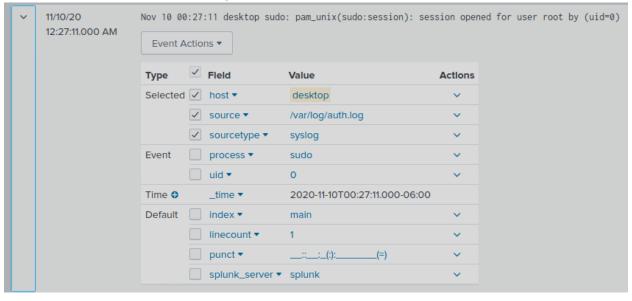
1. Screenshot of splunk DNS query resolving

cpre230@ubuntuserver:~\$ dig splunk.student15.230.com +noall +answer splunk.student15.230.com. 7186 IN A 192.168.1.208 cpre230@ubuntuserver:~\$

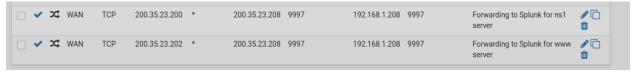
2. Screenshot of Splunk login page



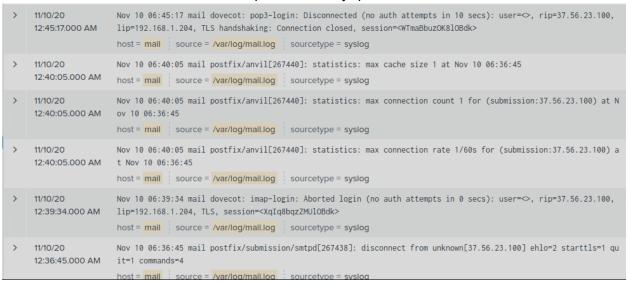
3. Screenshot of pam opening a session for a sudo-user



- 4. Screenshot of pfSense NAT forwarding rules required for ns1 and www splunkforwarding
 - Remember, only these two boxes should be allowed to communicate with the Splunk server



5. Screenshot and answers to suspicious activity question



a. What is going on?

On my mail server, there seems to be numerous connection/login attempts through imap, smtp, and pop3.

b. Is this dangerous?

Potentially, I think the attacker is probably attempting to brute force their way onto the mail server, so gaining control of this server gives them a gateway onto the private network behind the DMZ. It would be dangerous for them to be able to freely access services on this network like the Idap and www2 server.

c. Where is it originating?

It seems to be coming from the IP 37.56.23.100

d. How might you prevent this, if you were so inclined?

One idea could be to block connections from that IP address in pfsense, but then they can just use/spoof a different IP.

6. Screenshot and observations of "ET SCAN" or "ET POLICY" entry (Looking at the very first entry going to Morocco)



a. When did the event take place?

2020-11-10 at 6:54:41

b. Which IP initiated the traffic?

The 37.56.23.100 IP

c. Where was the traffic directed at?

It is directing traffic at the 105.148.172.206 device

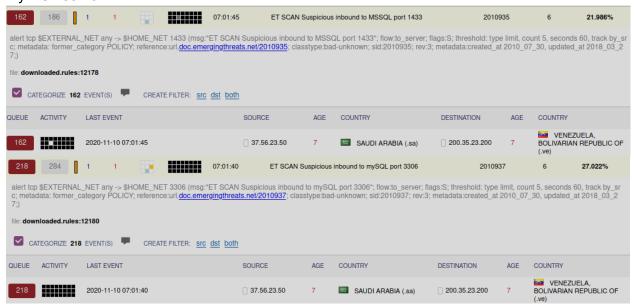
d. What service was involved? (ssh, ftp, smtp, etc.)

The traffic is scanning SSH

7.

- 8. Screenshots and details of three hosts being attacked
 - Pick and report on three hosts these scans are being directed at.
 (I just took shots of all my servers that I could find in the squert)

My NS1 server:



My www Server:



My Mail Server:



My www2 server:



b. Who is initiating these attacks?

There are three IPs coming from either Saudi Arabia or France that are attacking my servers. These are 37.56.23.50 and 37.56.23.100 from Saudi Arabia and 162.88.94.199 from France. They seem to be scanning for MSSQL, mySQL, SSH, and IMAP services running on the machines.