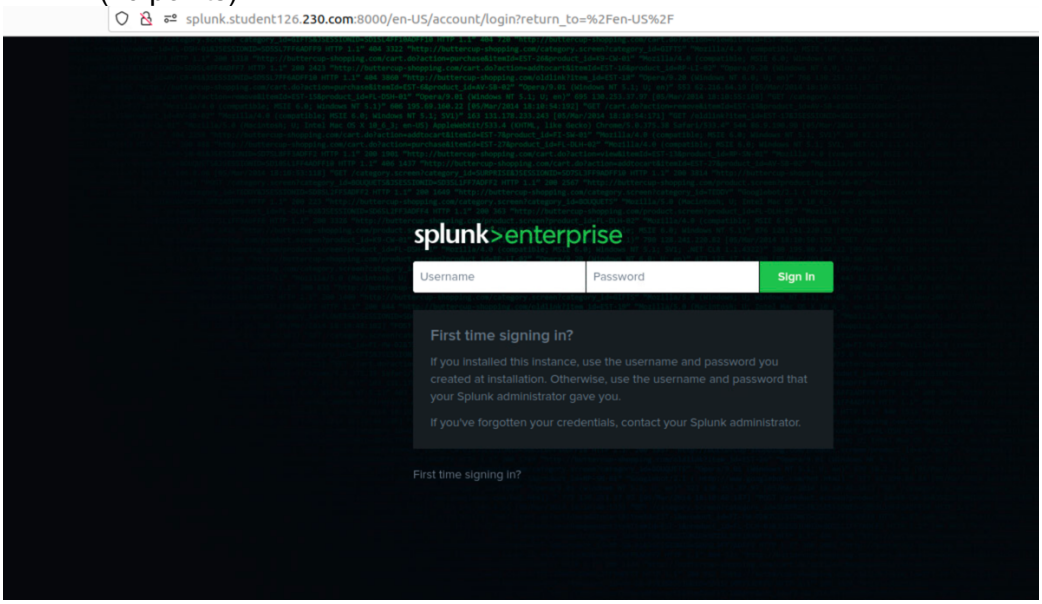
Lab 11 Template

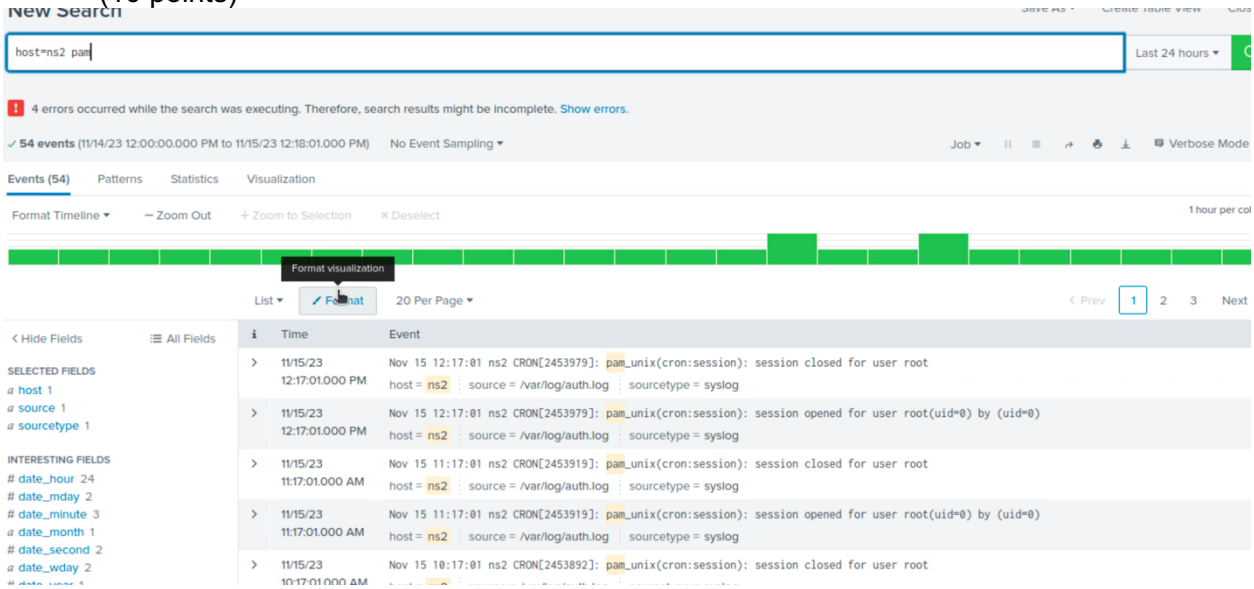
1. **Screenshot of splunk DNS query against ns2 resolving**
   (10 points)

```
root@splunk:/home/cpre230# dig splunk.student126.230.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> splunk.student126.230.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24819
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;splunk.student126.230.com.     IN      A

;; ANSWER SECTION:
splunk.student126.230.com. 1693 IN      A       192.168.1.208

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Nov 09 16:11:23 UTC 2023
;; MSG SIZE  rcvd: 70
```

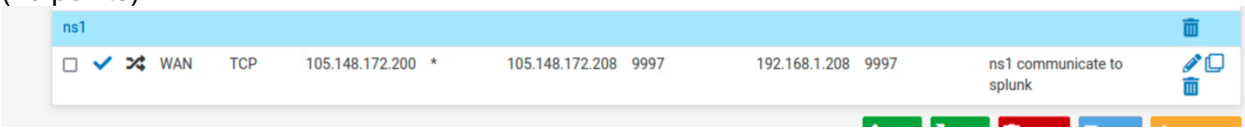
2. **Screenshot of Splunk login page**
   (10 points)



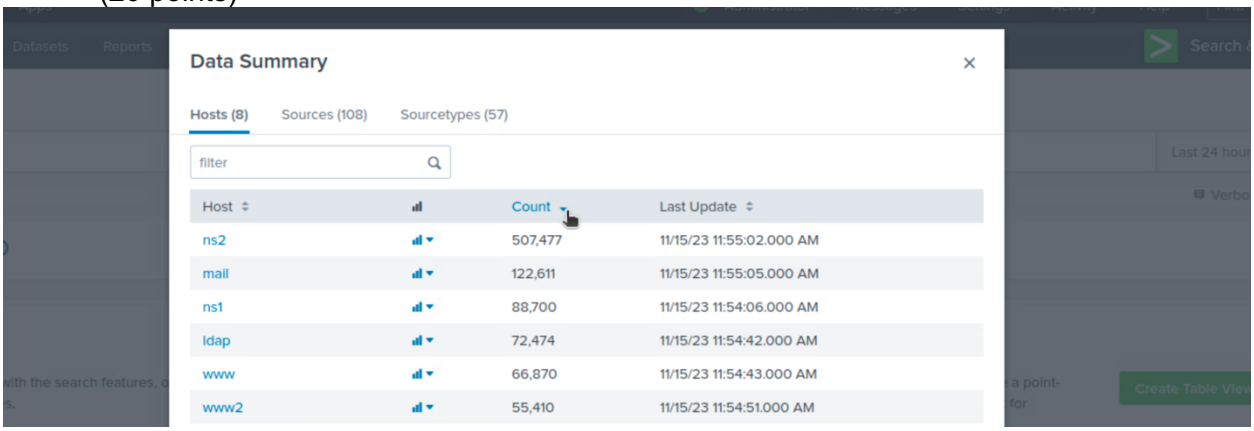
3. Screenshot of pam opening a session for a sudo-user
(10 points)



4. Screenshot of pfSense NAT forwarding rules required for ns1.
Remember, only ns1 should be allowed to communicate with the Splunk server
(10 points)



5. Screenshot of Data Summary page with all servers listed.
(20 points)



6. Screenshots from Splunk and answers to suspicious activity questions

a. [Suspicious Activity 1]

(10 points)

i. What is going on?

1. We do not recognize the source or destination IP so they are coming from outside world.

ii. Is this dangerous?

1. This is dangerous because the outside attacker is receiving information from my pfsense

iii. Where is it originating?

1.

iv. How might you prevent this, if you were so inclined? Or can you prevent this?

1. You could prevent this by making your encoder much more complex so if you were to look on wireshark they would not be able to access info more easily.

b. [Suspicious Activity 2]

(10 points)

i. What is going on?

ii. Is this dangerous?

iii. Where is it originating?

iv. How might you prevent this, if you were so inclined? Or can you prevent this?

c. [Suspicious Activity 3]

(10 points)

i. What is going on?

ii. Is this dangerous?

iii. Where is it originating?

iv. How might you prevent this, if you were so inclined? Or can you prevent this?

7.

(10 points)

Name	Where is it implemented	Alert decisions
Snort	Network based	Signature based
OSSEC	Host based	Both

Security Onion	Network based	Signature based
Zeek	Network based	Both