Lab 11 Template

1. **Screenshot of splunk DNS query against ns2 resolving**

(10 points)

A computer screen with white text

Description automatically generated

1. **Screenshot of Splunk login page**

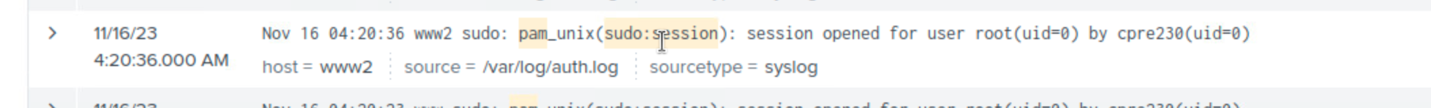
(10 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of pam opening a session for a sudo-user**

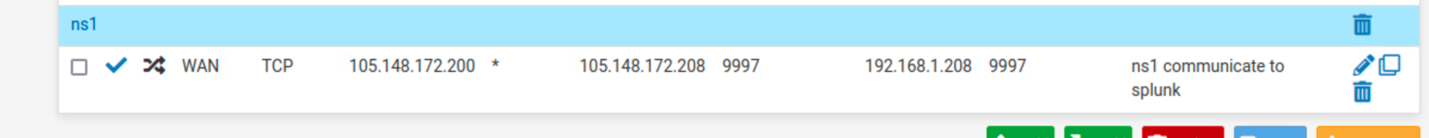
(10 points)



1. **Screenshot of pfSense NAT forwarding rules required for ns1.**

Remember, only ns1 should be allowed to communicate with the Splunk server

(10 points)



1. **Screenshot of Data Summary page with all servers listed.**

(20 points)

A screenshot of a computer

Description automatically generated

1. **Screenshots from Splunk and answers to suspicious activity questions**
   1. **[ Suspicious Activity 1 ]**

(10 points)

A screenshot of a computer

Description automatically generated

1. What is going on?
   1. Outside attacker is attempting to gain access into my www2
2. Is this dangerous?
   1. This is dangerous because the attack would be able to have access to my server anytime.
3. Where is it originating?
   1. 88.203.23.150 port 40238
4. How might you prevent this, if you were so inclined?  Or can you prevent this?
   1. We could prevent this by changing our ports to unfamiliar ports
5. **[ Suspicious Activity 2 ]**

(10 points)



1. What is going on?
   1. The outside attacker is network mapping by sending packets and analyzing data
2. Is this dangerous?
   1. This is dangerous because attackers can gain huge amount of information that does not want to be leaked
3. Where is it originating?
   1. 88.203.23.150
4. How might you prevent this, if you were so inclined?  Or can you prevent this?
   1. If we did not have a firewall at first, then I would implement a firewall to block all incoming connections with imap so Nmap will not return any data to the attacker.

1. **[ Suspicious Activity 3 ]**

(10 points)

1. What is going on?
2. Is this dangerous?
3. Where is it originating?
4. How might you prevent this, if you were so inclined?  Or can you prevent this?



(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 | Anomaly based |