LAB-11

1. **In a cybersecurity lab environment, a team is tasked with implementing and testing an Intrusion Prevention and Detection System (IDS) using Snort. The team's objectives include configuring Snort for optimal performance, conducting rigorous testing to ensure its effectiveness, and developing custom Snort rules tailored to specific security requirements. Additionally, the team aims to simulate real-world attack scenarios using Kali Linux to detect and mitigate potential threats effectively.**

Ensure Ubuntu and Kali linux virtual machines are up and running.
Go to Ubuntu VM…
sudo apt-get install snort
Configure the interface correctly. Choose the interface by running /sbin/route –n in another terminal.
Set the correct interface and click on ok.
Get the IP address of Ubuntu machine.
Go to snort folder
cd /etc/snort
sudo vi snort.conf---(configuration file)
cd rules
vi local.rules -- (Custom rules will be defined here)
vi icmp.rules---(icmp rules defined here)
To test the configuration file:
sudo snort -T -c /etc/snort/snort.conf
To start snort and system is listening to packet processing
sudo snort –A console -c /etc/snort/snort.conf
Go to Kali Linux VM
nmap 192.128.111.133(Ubuntu machine IP)
when the scanning is going here, in the Ubuntu snort terminal. You can go and see the snort. It will able to detect the packets..one of the rule is triggered and it is displaying SNMP request tcp..
So attempt of reconnaissance is detected and captured.
Lie this any attack can be detected.
Even in kali linux machine.. even if you ping from kali linux to Ubuntu.. even ping is captured and display—(ICMP ping)
Customized snort rules.
Go to Ubuntu machine..
cd /etc/snort/rules
vi local.rules
add below rules
Add the below rules in the path
cd /etc/snort/rules/
vi local.rules
#If any ICMP ping is happening --Unique id and name is added
alert icmp $EXTERNAL_NET any -> HOME_NET any (msg:”Shubha”;sid:5889; rev:1;)
#FTP attempt
alert tcp any any -> $HOME_NET 21 (msg:”FTP attempted”; sid:60001; rev:1;)
SSH attempt

alert tcp any any -> $HOME_NET 22 (msg:”SSh attempted”; sid:600022; rev:1;)
Once the rules are added check the snort configuration.
sudo snort -T -c /etc/snort/snort.conf

if there are no issuses with rules..
Then start the snort
sudo snort –A console -c /etc/snort/snort.conf
Now go to Kali linux
1. ping 192.168.111.133
now go check in Ubuntu VM.. shubha msg is detected and displayed while pinging
2. ftp 192.168.111.133
now go check in Ubuntu vm.. FTP attempted msg is detected and displayed performing FTP connection
3. ssh ubuntu@192.168.111.133
now go check in Ubuntu VM.. SSH attempted msg is detected and displayed performing SSH Connection.