LAB ASSIGNMENT No. 11

Aim: Installing snort, configuring it in Intrusion Detection mode and writing rules for detecting pinging activity.

Lab Outcome Attained: LO6

Theory:

Steps to Install snort and configure it in Intrusion Detection Mode.

1. Check the name of the interface using command ifconfig.
2. Install snort in ubuntu machine using command *sudo apt-get install snort*
3. While installing the snort, name of the interface will be asked on which snort is supposed to listen. Enter the interface name observed in step 1.
4. Run the command *sudo gedit /etc/snort/snort.conf* . This opens snort configuration file.
5. Make following changes to configuration file.
    a. ipvar HOME_NET **192.168.44.0/24 (in section 1)**
6. Open new terminal. Open ftp.rule file in it by typing the command *sudo gedit /etc/snort/rules/ftp.rules (optional)*
7. Open new terminal and type the command *sudo snort -T -c /etc/snort/snort.conf -i **ens33*** to validate that all rules are there.
   We use the
   -T flag to test the configuration file,
   -c flag to tell Snort which configuration file to use, and
   -i to specify the interface that Snort will listen on.

8. Type the command *sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33* (to start snort in NIDS mode)
   We use the
   -A console The ‘console’ option prints fast mode alerts to stdout

-q Quiet mode. Don’t show banner and status report.

-u snort Run Snort as the following user after startup

-g snort Run Snort as the following group after startup

-c /etc/snort/snort.conf The path to our snort.conf file

-i ens33 The interface to listen on (change to your interface if different)

9. Now go to kali linux machine.
10. Type command *nmap 192.168.44.128* on it to start port scanning of ubuntu machine and observe the output in terminal where snort is started in detection environment.

    When you execute this command, you will not initially see any output. Snort is running, and is processing all packets that arrive on eth0 (or whichever interface you specified with the -i flag). Snort compares each packet to the rules it has loaded (in this case our single ICMP Ping rule), and will then print an alert to the console when a packet matches our rule.

11. Then try pinging ubuntu machine by typing the command *ping 192.168.44.128* and observe the output in terminal where snort is started in detection mode.

---

12. Adding rule for detecting ping activity performed by another machine:

---

a. In ubuntu machine, type the following command to create a file called local.rules : ***sudo gedit /etc/snort/rules/local.rules***
b. Write the following rule in it: ***alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)***
c. Save the local.rules file.
d. Comment the following lines in configuration file (snort.conf) of snort: icmp.rules and icmp-info.rules
e. Add the local.rules file in section 7 of configuration file of snort by writing: ***include $RULE_PATH local.rules***
f. Validate the changes made in snort.conf file by writing the command in terminal: ***sudo snort -T -c /etc/snort/snort.conf -i ens33***
g. Set the snort in Intrusion Detection Mode by typing the command: ***sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33***
h. Now from kali machine ping the ubuntu machine and see the alert generated.
i. Observe the difference between the alerts generated when icmp.rules and icmp-info.rules are used and when local.rules is used to detect the ping activity.

Reference Link for Demo: https://www.youtube.com/watch?v=iBsGSsbDMyw

---