Roll No 06

Name- Prasad Sunil Arote

Date- 25-08-2023

Lab Assignment 11

Aim: Installing snort, setting in Intrusion Detection Mode and writing rules for Intrusion Detection.

LO6: Demonstrate the network security system using open source tools.

Theory:

What is Intrusion Detection System?

1. A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations.
2. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration.
3. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.
4. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

What are different modes in which Snort works?

Snort operates in three primary modes:

1. Sniffer Mode:

   In this mode, Snort acts as a packet sniffer, analyzing network traffic and displaying the captured packets on the console. It doesn't perform any active intrusion detection or prevention; instead, it's used for network analysis and troubleshooting purposes.

2. Packet Logger Mode:

   In packet logger mode, Snort captures and logs network traffic that matches defined rules to log files. This mode is useful for creating a record of network activity for later analysis.

3. Network Intrusion Detection System (NIDS) Mode:

   This is the main mode of Snort, where it functions as a network intrusion detection system (NIDS). Snort examines network traffic against a set of predefined rules to identify and alert on potential intrusion attempts, malicious activities, or suspicious patterns. When a rule matches, Snort generates alerts that can be sent to various destinations, such as log files, syslog servers, or email.

In addition to these primary modes, Snort also offers inline capabilities through its IPS (Intrusion Prevention System) mode:

4. Network Intrusion Prevention System (IPS) Mode:

   When operating as an IPS, Snort not only detects suspicious activity but can also take active measures to prevent or block potential threats. In this mode, Snort can drop or modify packets that match specific rules, effectively preventing malicious traffic from reaching its intended target.

Write the commands used for installing snort, editing its configuration file and configuring it in Intrusion Detection Mode?

1.Check the name of the interface using command ifconfig.

Installing Snort

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

Editing Configuration File (snort.conf):

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.rulefile 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.

8. Type the command sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -iens33

9. In ubuntu machine, type the following command to create a file called local.rules: sudo gedit /etc/snort/rules/local.rules

10. 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;)

11. Add the local.rules file in section7 of configuration file of snort by writing: include $RULE_PATH local.rules

12. Validate the changes made in snort.conf file by writing the command in terminal: sudo snort -T -c /etc/snort/snort.conf -iens33

13. 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 -iens33

CONCLUSION

The installation and configuration of Snort as an Intrusion Detection System (IDS) play a vital role in enhancing network security. Snort offers multiple modes of operation, including Sniffer Mode for packet analysis, Packet Logger Mode for capturing and logging traffic, and its primary Network Intrusion Detection System (NIDS) Mode for actively monitoring and alerting on potential intrusion attempts.

Configuring Snort involves installing the software, editing the snort.conf configuration file to tailor its behavior to specific network requirements, and then starting the Snort service. While Snort is set to operate in intrusion detection mode by default, its flexibility allows for customization to suit various security needs.