Roll No: 09
Name: Shreya Bagade
Date: 25/08/2023

LAB ASSIGNMENT NO:11

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

Lab Outcome Attained: Demonstrate the network security system using open source tools.

Theory:

> What is Intrusion Detection System?

An Intrusion Detection System (IDS) is a security technology used to monitor network traffic or system activities in order to identify and respond to unauthorized or malicious activities. The primary purpose of an IDS is to detect potential security breaches, intrusions, or attacks on computer systems, networks, and applications. It does this by analyzing patterns, behaviors, and anomalies in network traffic or system logs.

There are two main types of IDS:

Network-based IDS (NIDS): NIDS monitors network traffic in real-time, looking for suspicious patterns or signatures that match known attack patterns. It operates at the network level and can detect activities such as port scanning, malware communication, and unusual data transfers. NIDS can be deployed at key points within a network to monitor all traffic passing through those points.

Host-based IDS (HIDS): HIDS operates on individual computer systems or hosts. It monitors activities and events on the host itself, such as system logins, file changes, and application activities. HIDS can detect attacks that may not be visible at the network level, such as local privilege escalation or unauthorized access attempts.

IDS uses various techniques for detection:

Signature-based detection: This involves comparing network traffic or system events against a database of known attack patterns or signatures. If a match is found, the IDS generates an alert.

Anomaly-based detection: This approach establishes a baseline of normal network or system behavior and alerts when deviations from this baseline are detected. It's effective at identifying novel attacks or activities that don't match known signatures.

Heuristic-based detection: Heuristic techniques involve looking for behaviors or patterns that are indicative of attacks. These techniques are often used in conjunction with other detection methods.

Statistical-based detection: Statistical methods analyze patterns of events over time to identify deviations from expected behavior.

When the IDS detects suspicious activity, it can take various actions, including generating alerts for security personnel to investigate, logging the event, or even initiating automated responses to mitigate the threat.

> What are different modes in which Snort works? (refer user mannual on snort.org for this)

1.Sniffer Mode: Sniffer mode helps with your IDS objectives in the following instances if:

You only need to print out data: ./snort -v

There is a need to see the data in transit and also check the IP and TCP/ICMP/UDP headers: ./snort -vd

You need slightly elaborate information about data packets: ./snort -vde

To list the command lines exclusively: ./snort -d -v -e

2.Logging Mode: Just like the term ‘logging’ implies, when you need to log/record the data packets you may designate a logging directory. Understandably, the data packets are recorded in the directory.

Here’s the line that logs the data in an assumption that you have created a directory called ‘log’ : ./snort -dev -l ./log -h 192.168.1.0/24

3.Network Intrusion Detection System (NIDS) Mode: When you/ or your network administrator is specific about logging a specific kind of data packet/s, you may run Snort in NIDS mode. You may also define the action you want to take upon detection of malicious data packets while you write the rule.

Roll No: 09
Name: Shreya Bagade
Date: 25/08/2023

> Write the commands used for installing snort, editing its configuration file and configuring it in intrusion detection mode.

1. Install Snort: sudo apt-get install snort
2. Edit Configuration File: sudo gedit /etc/snort/snort.conf . This opens snort configuration file.

   Make following changes to configuration file.

   a. ipvar HOME_NET 192.168.44.0/24

   b. Open new terminal. Open ftp.rule file in it by typing the command

      sudo gedit /etc/snort/rules/ftp.rules (optional)

   c. Open new terminal and type the command sudo snort -T -c/etc/snort/snort.conf -i ens33 to validate that all rules are there.

3. Configure Snort in Intrusion Detection Mode:

   Type the command sudo snort -A console -q -u snort -g snort -c

   /etc/snort/snort.conf -i ens33

   sudo gedit /etc/snort/rules/ftp.rules

   sudo snort -T -c /etc/snort/snort.conf -i ens33

   sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

Conclusion: This experiment highlighted the importance of properly configuring and deploying intrusion detection systems like Snort to bolster network security. By installing Snort, setting it to operate in IDS mode, and crafting custom rules, the experiment aimed to showcase the practical aspects of enhancing network monitoring and threat detection capabilities. This hands-on experience equipped participants with valuable insights into real-world network security challenges and solutions.