Assignment No 4

Group B (Network Security)

Aim: Use the snort intrusion detection package to analyze traffic and create a signature to identify problem traffic.

Objectives:

1. To learn various client/server environments to use application layer protocols.
2. To understand the network security by using public key cryptography algorithms.

Theory:

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1 Network Intrusion Detection System (NIDS):

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

2 Host Intrusion Detection System (HIDS):

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to

the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

3 Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4 Application Protocol-based Intrusion Detection System (APIDS):

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5 Hybrid Intrusion Detection System:

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1 Signature-based Method:

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2 Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn’t signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

What is Snort?

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

SNORT is a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. SNORT uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity.

Using SNORT, network admins can spot denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks, Common Gateway Interface (CGI) attacks, buffer overflows, and stealth port scans. SNORT creates a series of rules that define malicious network activity, identify malicious packets, and send alerts to users.

SNORT is a free-to-use open-source piece of software that can be deployed by individuals and organizations. The SNORT rule language determines which network traffic should be collected and what should happen when it detects malicious packets. This snorting meaning can be used in the same way as sniffers and network intrusion detection systems to discover malicious packets or as a full network IPS solution that monitors network activity and detects and blocks potential attack vectors.

What Are the Features of SNORT?

There are various features that make SNORT useful for network admins to monitor their systems and detect malicious activity. These include:

1 Real-time Traffic Monitor

SNORT can be used to monitor the traffic that goes in and out of a network. It will monitor traffic in real time and issue alerts to users when it discovers potentially malicious packets or threats on Internet Protocol (IP) networks.

2 Packet Logging

SNORT enables packet logging through its packet logger mode, which means it logs packets to the disk. In this mode, SNORT collects every packet and logs it in a hierarchical directory based on the host network's IP address.

3 Analysis of Protocol

SNORT can perform protocol analysis, which is a network sniffing process that captures data in protocol layers for additional analysis. This enables the network admin to further examine potentially malicious data packets, which is crucial in, for example, Transmission Control Protocol/IP (TCP/IP) stack protocol specification.

4 Content Matching

SNORT collates rules by the protocol, such as IP and TCP, then by ports, and then by those with content and those without. Rules that do have content use a multi-pattern matcher that increases performance, especially when it comes to protocols like the Hypertext Transfer Protocol (HTTP). Rules that do not have content are always evaluated, which negatively affects performance.

5 OS Fingerprinting

Operating system (OS) fingerprinting uses the concept that all platforms have a unique TCP/IP stack. Through this process, SNORT can be used to determine the OS platform being used by a system that accesses a network.

6 Can Be Installed in Any Network Environment

SNORT can be deployed on all operating systems, including Linux and Windows, and as part of all network environments.

7 Open Source

As a piece of open-source software, SNORT is free and available for anyone who wants to use an IDS or IPS to monitor and protect their network.

8 Rules Are Easy to Implement

SNORT rules are easy to implement and get network monitoring and protection up and running. Its rule language is also very flexible, and creating new rules is pretty simple, enabling network admins to differentiate regular internet activity from anomalous or malicious activity.

What Are the Different SNORT Modes?

There are three different modes that SNORT can be run in, which will be dependent on the flags used in the SNORT command.

1 Packet Sniffer

SNORT's packet sniffer mode means the software will read IP packets then display them to the user on its console.

2 Packet Logger

In packet logger mode, SNORT will log all IP packets that visit the network. The network admin can then see who has visited their network and gain insight into the OS and protocols they were using.

3 NIPDS (Network Intrusion and Prevention Detection System)

In NIPDS mode, SNORT will only log packets that are considered malicious. It does this using the preset characteristics of malicious packets, which are defined in its rules. The action that SNORT takes is also defined in the rules the network admin sets out.

Installation Steps:

1. wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
2. wget https://www.snort.org/downloads/snort/snort-2.9.19.tar.gz
3. tar xvzf daq-2.0.7.tar.gz

4. cd daq-2.0.7
5. ./configure && make && sudo make install
6. cd ..
7. tar xvzf snort-2.9.19.tar.gz
8. cd snort-2.9.19
9. ./configure --enable-sourcefire && make && sudo make install