Final Project Report

## Intrusion Detection System Setup and Tuning

What is an intrusion detection system? This is a device or software application that monitors a network for malicious activity or policy violations. This activity is then typically logged or collected using security information and event management systems (Wikipedia IDS). There are many diverse types of IDS software to choose from. They are Snort, Zeek, OSSEC, Security Onion and Suricata are just a few. The types of IDS and how they work and for what they out. Then look at an IDS/IPS snort and how it works.

There are four many types of intrusion detection system. The (Types of Intrusion Detective Systems)first is a Host Intrusion detection system (HIDS) this monitor all host devices and computers within the network perimeter. It has access to all the system networks and internal networks. HIDS identify internal threats, where malicious traffic gets generated from within the host system residing on the network. A Network Intrusion detection system (NIDS) deployed at strategic points within a network, monitoring various network segments in an enterprise. It helps to identify malicious activity for outbound and inbound traffic to and from all host devices within a network. The downside is it cannot always identify internal threats (Types of Intrusion Detective Systems). The third is an Anomaly-based intrusion detection system (AIDS) this works by monitoring and identifying anomalies within the network traffic. This is done by establishing a baseline to determine that is normal for the network in terms of protocols, bandwidth, ports, devices used, etc. (Types of Intrusion Detective Systems) The final type is a Signature-based Intrusion Detection system (SIDS). This works by monitoring and identifying signatures of data packets traversing within the network. The tools compare the data against the database of previously experienced/drawn attacks signatures or known malicious attributes to issues alerts. (Types of Intrusion Detective Systems)

So, let us look at an intrusion detection system like Snort. Snort is the foremost open-source intrusion prevention system in the world. It uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generate alerts for users. Snort can be deployed to inline stop these packets as well. It has three primary uses. The first is a packet sniffer like tcpdump, a packet logger, which helps network traffic debugging and the last is a full-blown network intrusion prevention system. This one source can be configured for personal and business alike. (Snort) Snort can be used with other applications such as pfsense. Snort not only has a community rule set but can also be used to generate new alerts by inserting new alert rules under the local rule configuration. Snort can be set up to look after one system on the network or many systems on the network and send alerts or prevents in real time.

IDS can be designed to identify common types of attacks such as Scanning, Denial of Service attacks, social engineering attacks, malware, exploits, and many more. A scanning attack involves attackers probing your network for vulnerabilities, The IDS detect port scans, vulnerability scans, and network mapping attempts. DOS attacks aim to overwhelm your system with traffic, making it unavailable to the user. IDS detect flooding attacks and SNY floods and UDP floods. A social engineering attack while not directly detectable through network traffic analysis. An IDS can flag anomalies associated with social engineering attempts. Being either phishing emails, triggering downloads, or suspicious data transfer. IDS can identify attempts to download or install malware by looking for known malware signatures or suspicious file transfers. Exploits happen by software vulnerabilities to gain unauthorized access. IDS can detect the exploit attempt by monitoring network traffic for patterns associated with known vulnerabilities. (What are the types of computer attackes detected by IDS)

We now understand how an IDS system can protect a network against malicious activity by monitoring a network’s traffic and patterns. The four types of IDS being HIDS, NIDS, AIDS, and SIDS and what signatures they look for. A type of IDS/IPS snort and the rules and prevent that can be generated in real time to alert to abnormalities happening on a network. To the types of attacks that IDS lookout for on a network be scanning, DOS, malware, or exploits. IDS are a great defense against attackers and should not be mistaken for firewall, since firewall only sit at the network perimeter and IDS/IPS work on the network but also the host level.

# Works Cited

*Snort*. n.d. snort.org. 03 08 2024.

*Types of Intrusion Detective Systems*. n.d. packetlabs.net. 03 08 2024.

*What are the types of computer attackes detected by IDS*. 26 01 2024. stamus-networks.com. 03 08 2024.

*Wikipedia IDS*. 2018. en.m.eikipedia.org. 03 08 2024.