ASSIGNMENT

PRAJJWAL KUMAR

2K18/IT/085

HIDS AND TOOLS

HIDS: HIDS stands for "**host-based intrusion detection system**," an application monitoring a computer or network for suspicious activity, which can include intrusions by external actors as well as misuse of resources or data by internal ones.

WORKING: HIDS tools monitor the log files generated by your applications, creating a historical record of activities and functions allowing you to quickly search them for anomalies and signs an intrusion may have occurred. They also compile your log files and let you keep them organized in ways aligning with the directory structure of your log file server, making it easy to search or sort the files by application, date, or other metrics.
The key function of HIDS tools is automated detection, which saves you the need to sort through the log files for unusual behaviour once they're organized and compiled. HIDSs use rules and policies—some of which are preset but can usually be modified and updated to suit your organization's specific needs—to search your log files, flagging those with events or activity the rules have determined could be indicative of potentially malicious behaviour.

TOOLS:

1. **SOLARWINDS SECURITY EVENT MANAGER :**
   SolarWinds Security Event Manager (SEM) is a HIDS with a robust lineup of automated threat remediation tools—which, if you've been paying attention to the acronyms, technically makes this option an IPS. It also comes with a toolset of useful log management features. **Security Event Manager makes it easy to constantly monitor, forward, back up, or archive log files, and includes built-in transit and storage encryption.** This tool includes the option for **running manual checks on data integrity**. It also uses a **centralized log analysis system to detect potential APT activity**. Pulling and analyzing data from systems across

the network, the software creates a cohesive monitoring environment to track down the signs of APT cyberattacks to root them out.

2. OSSEC:

OSSEC **organizes and sorts your log files and uses anomaly-based detection strategies and policies**. Because it's an open-source application, you can also download predefined threat intelligence rule sets from the community of other users who have OSSEC installed. If you need technical support, help from the active user community is free to access, and Trend Micro—which produces OSSEC—also offers a professional support package for a cost. OSSEC can be installed on a wide variety of operating systems, including **Windows, Linux, Unix, and Mac OS**. The tool monitors event logs and the registry for Windows systems, and on the other operating systems, it'll guard the root account. OSSEC offers compliance reporting functions as well, and its log file detection methods scan for unusual behaviour or unauthorized changes that could specifically cause compliance issues.

3. SOLARWINDS PAPERTRAIL:

Papertrail™ is another SolarWinds product, and it's a little different than your **typical HIDS** or **NIDS**. This cloud-based management service aggregates your log files and stores them, so you don't have to worry about volumes of log data eating up storage on your systems. **By centralizing log file storage, Papertrail provides easy access and rapid search functions for your entire data archive.**

The tool uses both anomaly- and signature-based detection strategies can manage a variety of file types (including Windows event logs, firewall notifications, and more), and sends out threat intelligence policy updates with new information learned from cyberattacks attempted on other users.

4. MANAGE ENGINE EVENT ANALYZER:

ManageEngine EventLog Analyzer is a comprehensive security application with **both HIDS and NIDS capabilities.** It also centralizes your log files and metadata in one location, and if it detects log files have been altered inappropriately, you can automatically restore your log files from backups. Similar to Papertrail, EventLog Analyzer protects log files with encryption and compression protocols and requires user authentication to access the data. EventLog Analyzer can be installed on Windows or Linux and easily integrates with ManageEngine

infrastructure management tools, which give you greater control and monitoring over your network's performance and functionality. As far as pricing goes, your first five devices are free to monitor—a nice advantage if you're running a network at home or for a very small business. Those managing larger networks can request a quote on the ManageEngine website.

5. **SPLUNK:**

There are several versions of Splunk available, ranging from the free baseline application—which is an excellent anomaly-based HIDS—to paid options with a variety of NIDS features. **The paid versions of Splunk, which include cloud-based options, offer automated features to respond immediately to detected threats, giving them IPS capabilities.** Splunk also boasts an excellent user interface and dashboard with useful visualizations.

All versions of Splunk can be installed on **Windows, Linux, and Mac** operating systems, and each includes a strong data analyzer for easy sorting and searching through your log data. Different free trial periods are available for the different tiers of Splunk, allowing you to try before you buy.

6. **SAGAN:**

Sagan is another free option using both **anomaly- and signature-based detection strategies.** Sagan is customizable and allows you to define automatic actions for the application to take when an intrusion contingency is triggered. It has a number of tools other HIDSs don't offer, **including an IP geolocation feature to create alerts if activity from multiple IP addresses appears to be stemming from the same geographical location.** Sagan also allows for script execution, which means it can function more like an IPS.

Sagan was written to easily integrate with Snort, a NIDS (see below), and when paired together, they create a powerful, open-source HIDS and NIDS combo.

7. **SNORT:**

   Snort is an excellent **open-source NIDS application chock-full of features**. Not only does it work as a robust intrusion detection tool, but it also includes packet sniffing and logging functionality.

   Similar to how OSSEC allows you to download rules and policies from the user community, predefined rules for Snort are available on the website, with options to sign up for subscriptions to make sure your threat intelligence policies are kept up to date. Snort's rules can also be customized to suit your specifications, but the basic set of policies is a good place to start. The events these policies detect include buffer overflow attacks, CGI attacks, OS fingerprinting, and stealth port scans. **The rule set includes both anomaly- and signature-based policies, making the application's scope fairly broad and inclusive**. And, as mentioned above, Snort can be seamlessly combined with Sagan for a more comprehensive open-source monitoring solution.

8. **SAMHAIN:**

   Another free HIDS option, Samhain offers file security functions like integrity checks, monitoring, and analysis. Perhaps its most unique feature is its stealth **mode monitoring, which essentially allows it to run without a hacker noticing**. In many cases of cyberattacks, the intruders can identify and stop detection processes, but their proprietary cryptographic function prevents hackers from noticing it's active and performing sweeps. The tool uses a PGP key to protect central log files and backups, as well.

   Other features include the ability to perform rootkit detection and port monitoring and to detect hidden processes running on your devices. It can manage multiple systems—even if they're running different operating systems—from a centralized interface. Samhain can be installed on **Linux, Unix, and Mac operating systems, and on Windows through Cygwin**.