Experiment 10

Chinmay Parikh A059

Questions

1. Explain the need for IDPS?
2. Explain detection mechanism is used by snort IPS?
3. What the limitations are of snort IPS?

Answers

1.
   - To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system.
   - To detect attacks and other security violations that are not prevented by other security measures.
   - To detect and deal with the preambles to attacks (commonly experienced as network probes and other "doorknob rattling" activities).
   - To document the existing threat to an organization.
   - To act as quality control for security design and administration, especially in large and complex enterprises.
   - To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.
2. Network Intrusion Detection System (NIDS) is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. It monitors traffic on a network looking for suspicious activity, which could be an attack or unauthorized activity. A large NIDS server can be set up on a backbone network, to monitor all traffic; or smaller systems can be set up to monitor traffic for a particular server, switch, gateway, or router. In addition to monitoring incoming and outgoing network traffic, a NIDS server can also scan system files looking for unauthorized activity and to maintain data and file integrity. The NIDS server can also detect changes in the server core components. In addition to traffic monitoring, a NIDS server can also scan server log files and look for suspicious traffic or usage patterns that match a typical network compromise or a remote hacking attempt. The NIDS server can also server a proactive role instead of a protective or reactive function. Possible uses include scanning local firewalls or network servers for potential exploits, or for scanning live

traffic to see what is actually going on. Keep in mind that a NIDS server does not replace primary security such as firewalls, encryption, and other authentication methods. The NIDS server is a backup network integrity device. Neither system (primary or security and NIDS server) should replace common precaution (building physical security, corporate security policy, etc.)

3. Limitations of SNORT

- It is not possible to send error page to client as SNORT does not work on HTTP(S).
- It is not possible just to write rule on outbound traffic. Rule can be written either for both (inbound/outbound) or inbound traffic.
- Snort does have some limited shortfalls when it comes to anomaly detection. The system was not designed for this type of operation, but some pre-processor modules attempt to add this functionality. Currently these modules are not considered effective in detection. There is also concern about how efficient the detection engine actually is in terms of processing performance. The base engine is considered quite efficient, but there is speculation as to how efficient the system becomes when used with the pre-processor modules. The added functionality is good, but what price do you have to pay for that functionality.
- Not an IDPS.