HIDs and HIPs

HIDS

- Host Intrusion Detection or HIDs, typically monitors hosts
- Intrusion may be unnoticed if NIDS is not looking internally
- HIDs can serve several purposes:
    - Monitor files or directories for changes
    - Monitor system activity
    - Monitor system logs
    - Report on patterns that may be seen as malicious

HIDS

- The two most commonly known open-source packages are:
  - AIDE – Advanced Intrusion Detection Engine
    - Used mainly for integrity checking
  - OSSEC – Open-Source Intrusion Detection System
    - Used for host systems in a number of ways

OSSEC - 1

- OSSEC is a very powerful Host Intrustion Detection System
- OSSEC Server runs on Linux, however it can have agents that report in from different sources such as other Linux systems, Windows, and Mac
- Logs from OSSEC are hashed so they cannot be tampered

OSSEC - 2

- OSSEC has four basic components:
  - File Integrity Checking: AIDE can only run on a manual basis
  - Log Monitoring: OSSEC reports to a central server
  - Rootkit Detection: OSSEC agents check for rootkits on a system every 2 hours by default
  - Active Response: Responses are configurable

HIDS Advantages and Disadvantages

- Advantages of using HIDS:
  - HIDS is a simple way of ensuring the integrity of a client remains intact
  - Can be configured to alert key personnel in the event of abnormal activity on a system
  - Relatively easy administration
  - Meets compliance standards for PCI systems
- Disadvantages of using HIDS:
  - Installation and setup can be cumbersome in the beginning
  - Files are changed quite frequently and the alerts produced by HIDS can be overwhelming