Page No.
Date

Assignment: 05

Ques: Discuss various types of IDs in brief?

Ans: Intrusion detection systems can be categorized in 3 different ways depending on the environment and type of intrusion to be detected. These three categories are:

- Network based ID systems.
- Host based ID systems.
- Misuse and anomaly detection systems.

- Network based ID systems

Network based intrusion detection systems (NIDS) are devices intelligently distributed within networks that passively inspect traffic traversing the devices on which they sit.

- Domain 7. Eric conrad.
- Local area network security.
- Embedded security.
- Guarding Against Network intrusions.

- Host based ID systems

A host based IDs (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing systems as well as the network packets on its network interfaces

similar to the way a network based intrusion detection system (NIDS) operates. This was the first type of intrusion detection software to have been designed, with the originally target system being the mainframe computer where outside interaction was infrequent.

→ Misuse and Anomaly Detection System.
Misuse detection within network-based IDS involves checking for illegal types of network traffic
Detection of anomalous activity relies on the system knowing what is "regular" network traffic and this what isn't. Anomalous traffic to a host based IDS might be interactive accesses outside of normal office hours.

Que 2 (i) Explain Deployment of HIDS?
Ans (i) HIDS differ from NIDS in two ways. HIDS protects only the best host system on which it resides and its network card operates in nonpromiscuous mode. Nonpromiscuous mode of operation can be an advantage in some cases, because not all NICs are capable of promiscuous mode. In addition, promiscuous mode can be CPU intensive for a slow

host machine. HIDS can be run directly on the firewall as well, to help keep the firewall secure.

Another advantage of HIDS is the ability to tailor the ruleset to a specific need. For example, there is no need to interrogate multiple rules designed to detect DNS exploits on a host that is not running Domain Name Services. Consequently, the reduction in the number of pertinent rules enhances performance and reduces processor overhead.