ASSIGNMENT #02

BASIL ALI KHAN
20K-0477

Q#01) Based on these videos define how HIDS and NIDS is implemented.

Host Based Intrusion detection (HIDS) and Network Based intrusion detection system (NIDS) are integral components of a comprehensive security infastructure, serving distinct purposes in identifying and mitigating potential security threats

⇒ HOST BASED INTRUSION DETECTION SYSTEM (HIDS):

HIDS monitors and analyzes activities within individual hosts or endpoints, such as servers, workstations, or devices. It focuses on internal hosts activities and detects suspicious or malicious behaviour that could indicate an intrusion or security breach software agents are installed directly on individual hosts or endpoints. These ~~endpoints~~ agents continously monitor and analyze various system activities including file integrity, system logs, registry changes, process activities and user actions. HIDS agents compares observed behaviour against predefined rules or signatures, flagging any deviations or anomalies as potential security threats. It generates alerts or notification when it detects unauthorized or abnormal activities that could indicate a security incident.

HIDS functions autonomously on each hosts providing granular insight into host specific activities. It's capable of detecting both known and unknown threads by analyzing host level behaviours and deviation from normal pattern. It helps in identification and containment of intrusions or security incidonts at the host level. providing valuable insights into affected systems

⇒NETWORK BASIED INTRUSION DETECTION SYSTEM (NIDS):

NIDS is designed to monitor and analyze network traffic for signs of malicious activities or security threads. It operates at the network, analyzing packets traversing the network in realtime.

Deployed at strategic points within network infastructure, typically at network gateways or within segmet of network.

Uses sensor or appliances to capture and analyze network packets applying various detection techniques like signature based detection, anomaly detection, and behaviour analysis

Inspects network traffic, including protocols, packet headers payloads and traffic patterns to identify suspicious behaviour or known attack signatures

Monitors incoming and outgoing network traffic, flagging any unusual or potentially threating activities. It identifies patterns or signature associated with known attack type abnormal traffic behavior or unauthorized access attempts

NIDS generates alerts or alarms when it detects network based threats, allowing security teams to investigate and respond promptly

HIDS and NIDS are critical components of layered security approach each focusing on different aspects of security monitoring While HIDS focuse on monitoring individual host activities NIDS concentrates on analyzing network traffic to identify potential threats.

Q#02) How is this related to techniques outline in textbook chapter # 8 IDS section 8.4 and 8.5.

The video discuss HIDS involving in monitoring and analyzing activities on individual endpoints or hosts to detect suspicious activity. This relates with Section 8.4 that elaborates on purpose, implementation, and data sources used in HIDS.

IMPLEMENTATION SIMILARITIES:

Use of small traces, audit log records, file integrety checksums and registry access as data sources for HIDS which relates to data sources outline in 8.4.

ANOMALY DETECTION IN HIDS:

Emphasized analysis of system calls traces to detect abnormal behaviour relates with section 8.4 explanation of anomaly based detection using system call traces on UNIX / LINUX systems.

WINDOWS BASED HIDS:

Challenges with anomaly based HIDS on Windows due to DLL usage with corresponds to difficulties mentioned in section 8.4 regarding system calles traces on windows platform. Also new approaches using DLL function call traces which parallels section 8.4 exploration of alternative data sources for window HIDS.

Date:

The video discuss NIDS which involves monitoring network traffic for intrusion pattern match concept outlined in section 8.5

NIDS SENSOR DEPLOYMENT:

Deployment of sensor both inline and passive aligns with section 8.5 explanation of inline and passive sensors used in network traffic monitoring.

INTRUSION DETECTION TECHNIQUES:

Both sources covered signature based and anomaly based detection techniques based NIDS similar to examples discussed in section 8.5.

Anomaly detection techniques like DDOS attacks, scanning and worms, reflecting the anomaly detection examples mentioned in section 8.5.

LOGGING ALERTS

Emphasize on logging of alerts and relevant information when potential violation are detected by NIDS sensors.