Evasion

Chapter 17

Intrusion Detection System (IDS)

- **Detects malicious activity in computer systems**
  - Identifies and stops attacks in progress
  - Conducts forensic analysis once attack is over

The Value of IDS

- Monitors network resources to detect intrusions and attacks that were not stopped by preventative techniques (firewalls, packet-filtering routers, proxy servers)
- Compares traffic to signature files that recognize specific known types of attack
- Expands available options to manage risk from threats and vulnerabilities

Difficulties with IDS

- **IDS must correctly identify intrusions and attacks**
  - True positives
  - True negatives
- **False negatives**
  - IDS missed an attack
- **False positives**
  - Benign activity reported as malicious

Handling False Negatives and Positives

- **False negatives**
  - Obtain more coverage by using a combination of network-based and host-based IDS
  - Deploy NIDS at multiple strategic locations in the network
- **False positives**
  - Reduce number using the tuning process

Types of IDS

- **Network-based IDS (NIDS)**
  - Monitors network traffic
  - Provides early warning system for attacks
- **Host-based IDS (HIDS)**
  - Monitors activity on host machine
  - Able to stop compromises while they are in progress

NIDS

- Uses a dedicated platform for purpose of monitoring network activity
- Analyzes all passing traffic
- Sensors have two network connections
  - One operates in promiscuous mode to sniff passing traffic.
  - An administrative NIC sends data such as alerts to a centralized management system.
- Most commonly employed form of IDS

NIDS Architecture

- **Place IDS sensors strategically to defend most valuable assets**
- **Typical locations of IDS sensors**
  - Just inside the firewall
  - On the DMZ
  - On any subnets containing mission-critical servers

NIDS Signature Types

- **Signature-based IDS**
  - Looks for patterns in packet payloads that indicate a possible attack
- **Port signature**
  - Watches for connection attempts to a known or frequently attacked port
- **Header signatures**
  - Watch for dangerous or illogical combinations in packet headers

NIDS Reactions

- TCP resets
- IP session logging
- Shunning or blocking

Host-Based IDS (HIDS)

- Primarily used to protect only critical servers
- Software agent resides on the protected system
- Detects intrusions by analyzing logs of operating systems and applications, resource utilization, and other system activity
- Use of resources can have impact on system performance

HIDS Method of Operation

- Auditing logs (system logs, event logs, security logs, syslog)
- Monitoring file checksums to identify changes
- Elementary network-based signature techniques including port activity
- Intercepting and evaluating requests by applications for system resources before they are processed
- Monitoring of system processes for suspicious activity

HIDS Active Monitoring Capabilities

- Log the event.
- Alert the administrator.
- Terminate the user login.
- Disable the user account.

Passive Detection Systems

- Can take passive action (logging and alerting) when an attack is identified
- Cannot take active actions to stop an attack in progress

Active Detection Systems

- Have logging, alerting, and recording features of passive IDS, with additional ability to take action against offending traffic
- Options
  - IDS shunning or blocking
  - TCP reset
- Used in networks where IDS administrator has carefully tuned the sensor's behavior to minimize number of false positive alarms

Signature and Anomaly-Based IDS

- **Signature detections**
  - Also known as misuse detection
  - IDS analyzes information it gathers and compares it to a database of known attacks, which are identified by their individual signatures
- **Anomaly detection**
  - Creates a model of normal use and looks for activity that does not conform to that model

Honeypots

- False systems that lure intruders and that gather information on methods and techniques they use to penetrate networks—by purposely becoming victims of their attacks
- Simulate unsecured network services
- Make forensic process easy for investigators

Honeypot Deployment Goals

- **Goal**
  - Gather information on hacker techniques, methodology, and tools
- **Deployed for**
  - Conducting research into hacker methods
  - Detecting attacker inside organization’s network perimeter

Commercial Honeypots

- ManTrap
- Specter
- Smoke Detector
- NetFacade

Honeypot Deployment Options

- **For research purposes**
  - Directly connect a honeypot to the Internet, allowing the owner to collect the most data
- **For organizational security**
  - Deploy inside the network where it can serve to detect attackers and alert security administrators to their presence

Honeypot Design

- Must attract, and avoid tipping off, the attacker
- Must not become a staging ground for attacking other hosts inside or outside the firewall

Summary

- Explained intrusion detection systems and identified some of the major characteristics of intrusion detection products
- Detailed the differences between host-based and network-based intrusion detection
- Identified active detection and passive detection features of both host- and network-based IDS products
- Explained honeypots and how they are employed to increase network security
- Outlined the proper response to an attack