Intrusion Detection System (IDS)

Introduction

What is intrusion?
- type of attack on information assets in which instigator attempts to gain entry into or disrupt system with harmful intent
- when a user of an information system takes an action that user was not legally allowed to take
- can be both from inside and outside

Principles of Intrusion Detection

Characteristics of systems not under attack
- Users, process actions conform to statistically predictable pattern
- Users, process actions do not include sequences of actions that subvert the security policy
- Process actions correspond to a set of specifications describing what the processes are allowed to do

Systems under attack do not meet at least one of these

Example

Goal: insert a back door into a system
- Intruder will modify system configuration file or program
- Requires privilege; attacker enters system as an unprivileged user and must acquire privilege
- Nonprivileged user may not normally acquire privilege (violates #1)
- Attacker may break in using sequence of commands that violate security policy (violates #2)
- Attacker may cause program to act in ways that violate program’s specification

Introduction (continued)

Intrusion detection: consists of procedures and systems created and operated to detect system intrusions

Related works
- Intrusion tolerance
- Intrusion prevention
- Intrusion reaction
- Intrusion correction activities

Scary Statics

- Just over 90% of interconnected networks that were running IDS detected computer security breaches in the last 12 months. The fraction of several implemented firewall protections that were installed
- Computer Security Institute, 4/7/02 reported that 80% reported financial losses in excess of $455M was caused by intrusion and malicious acts thereafter
- Millions of jobs have been affected because of intrusion
- Only 0.1% of companies are spending the appropriate budget on IDS
- IDS are mostly misunderstood and are thought of as a firewall product or a substitute
- If you use an antivirus then should also consider adding an IDS as a complimentary product to your security strategy. Most organizations using antivirus software do not use IDS
Intrusion Detection Systems (IDSs)

- Detects a violation of its configuration and activates alarm
- Where should the alarm be sent?
  - Notify administrators directly of trouble via e-mail or pages
  - Notify an external security service organization

Why Use an IDS?

- Prevent problem behaviors by increasing the perceived risk of discovery and punishment
- Detect attacks and other security violations
- Detect and deal with precursors to attacks
- Document existing threat to an organization
- Act as quality control for security design and administration, especially of large and complex enterprises
- Provide useful information about intrusions that take place

IDS Terminology

- Alert or alarm
- False negative
- False positive
- False attack stimulus
- Noise
- True attack stimulus
- Confidence value
- Alarm filtering

Intrusion Detection Methods

- Signature-based
- Statistical anomaly-based

Signature-Based IDS

- Characterize known ways to penetrate a system
  - Pattern/signature
- Examine data traffic in search of patterns that match known signatures
- Widely used because many attacks have clear and distinct signatures
- Problem with this approach?

Statistical Anomaly-Based IDS

- Define and characterize: correct static form and/or acceptable dynamic behavior of the system.
- When measured activity is outside baseline parameters or clipping level, IDS will trigger an alert
- IDS can detect new types of attacks
- Requires much more overhead and processing capacity than signature-based
- May generate many false positives
Types of IDSs

- IDSs operate as
  - network-based
  - host-based
  - application-based

Network-Based IDS (NIDS)

- Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
- When examining packets, a NIDS looks for attack patterns
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment

NIDS Signature Matching

- To detect an attack, NIDSs look for attack patterns
- Done by using special implementation of TCP/IP stack:
  - In process of protocol stack verification, NIDSs look for invalid data packets
  - In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use

Advantages and Disadvantages of NIDSs

- Good network design and placement of NIDS can enable organization to use a few devices to monitor large network
- NIDSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- NIDSs not usually susceptible to direct attack and may not be detectable by attackers

Advantages and Disadvantages of NIDSs (continued)

- Can become overwhelmed by network volume and fail to recognize attacks
- Requires access to all traffic to be monitored
  - Having problems with router switches
  - Cannot analyze encrypted packets
- Cannot reliably ascertain if attack was successful or not
- Some forms of attack are not easily discerned by NIDSs; specifically those involving fragmented packets
**Host-Based IDS**

- Host-based
- Detects when intruder creates, modifies, or deletes key system files or log files
- Most HIDSs work on the principle of configuration or change management
- Advantage over NIDS can usually be installed so that it can access information encrypted when traveling over network

**Advantages of HIDSs**

- Can detect local events on host systems and detect attacks that may elude a network-based IDS
- Functions on host systems, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

**Disadvantages of HIDSs**

- Pose more management issues
- Vulnerable both to direct attacks and attacks against host operating system
- Does not detect multi-host scanning or scanning of non-host network devices
- Susceptible to some denial-of-service attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

**Application-Based IDS**

- Application-based IDS (AppIDS) examines application (database management systems, content management systems, accounting systems, etc.) for abnormal events
- AppIDS may be configured to intercept requests:
  - File System
  - Network
  - Configuration
  - Execution Space

**Advantages and Disadvantages of AppIDSs**

- Advantages
  - Aware of specific users; can observe interaction between application and user
  - Able to operate even when incoming data is encrypted
- Disadvantages
  - More susceptible to attack
  - Less capable of detecting software tampering

**Log File Monitors**

- Log file monitor (LFM) similar to NIDS
- Reviews log files generated by servers, network devices, and even other IDSs for patterns and signatures
- Patterns that signify attack may be much easier to identify when entire network and its systems are viewed holistically
- Requires allocation of considerable resources since it will involve the collection, movement, storage, and analysis of large quantities of log data
Deploying Network-Based IDSs

- NIST recommends four locations for NIDS sensors
  - Location 1: behind each external firewall in the network DMZ
  - Location 2: outside an external firewall
  - Location 3: on major network backbones
  - Location 4: on critical subsets

Deploying Host-Based IDSs

- Proper implementation of HIDSs can be painstaking and time-consuming task
- Deployment begins with implementing most critical systems first
- Installation continues until either all systems are installed or the organization reaches planned degree of coverage it is willing to live with

Active Intrusion Prevention

- Some organizations implement active countermeasures to stop attacks
- LaBrea: takes up unused IP address space

Scanning and Analysis Tools

- Typically used to collect information attacker would need to launch successful attack
- Attack protocol is series of steps or processes used by attacker, in a logical sequence, to launch attack against a target system or network
- Footprinting: first step of attack; find out the IP addresses of the target organization
  - Web reconnaissance: samspade.org
  - Whois information: whois.net
  - Network reconnaissance: ping sweep

Learn From Attackers
Fingerprinting: systematic survey of all of target organization’s Internet addresses collected during the footprinting phase

Fingerprinting reveals useful information about internal structure and operational nature of target system or network for anticipated attack

These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability.

Port Scanners

Tools used by both attackers and defenders to identify computers active on a network and other useful information

Can scan for specific types of computers, protocols, or resources, or their scans can be generic

The more specific the scanner is, the better it can give attackers and defenders useful information

Example software: nmap

Firewall Analysis Tools

Several tools automate remote discovery of firewall rules and assist the administrator in analyzing the rules

Although mostly design to facilitate network administrator’s work, can be used by attackers

Operating System Detection Tools

Detecting a target computer’s operating system (OS) very valuable to an attacker

There are many tools that use networking protocols to determine a remote computer’s OS

- RemOS
- XProbe

RemOS
Vulnerability Scanners

- Active vulnerability scanners scan networks for highly detailed information, initiate traffic to determine holes.
- Passive vulnerability scanners listen in on network and determines vulnerable versions of both server and client software.
- Passive vulnerability scanners have ability to find client-side vulnerabilities typically not found in active scanners.

Attack Toolkit
Packet Sniffers

- Network tool that collects copies of packets from network and analyzes them
- Can provide network administrator with valuable information for diagnosing and resolving networking issues
- In the wrong hands, a sniffer can be used to eavesdrop on network traffic
- To use a packet sniffer legally, an administrator must
  - be on network that organization owns
  - be under direct authorization of owner of network
  - have knowledge and consent of the content creators