Intrusion Detection Systems and Practices

Chapter 13

Lecturer: Pei-yih Ting

Overview

- Intrusion Detection Concepts
- Dealing with Intruders
- Detecting Intruders
- Principles of Intrusions and IDS
- The IDS Taxonomy
- Using Rules and Thresholds for Detectiong
- Snore
- Network-based vs. Host-based IDS
- Security Auditing with an IDS

Intrusion Detection Terms and Concepts

- An intrusion is any use or attempted use of a system that exceeds authentication limits
- Intrusions are similar to incidents
  - An incident does not necessarily involve an active system or network device, an intrusion does
- An intrusion detection system (IDS) is software/hardware that monitors activities on the system or network
  - And delivers an alert if it notices suspicious activity

Intrusion Detection Terms and Concepts (cont'd)

- Security policies are either prohibitive or permissive
- An IDS is sensitive to configuration
  - To achieve the goals of your security policy, you must be able to configure appropriately
- There are three basic types of IDS errors
  - False positives
  - False negatives
  - Subversion error

Dealing with Intruders

- Intruders can be external or internal
  - External intruders are hackers or crackers
  - Internal intruders are more common and very dangerous
- An organizational security policy should state what steps will be taken to handle intrusions
- Block and ignore
  - Simplest tactic for handling intrusions
  - Block the intruder and address the vulnerability
  - Don't take any further action

Dealing with Intruders (cont'd)

- Block and investigate
  - Block the intruder and address the vulnerability
  - Collect evidence and try to determine the intruder's identity
  - Although this may result in finding and stopping the intruder, it can be costly and time-consuming
- Honeypot (bait the intruder)
  - Allow the intruder to access a part of your network
  - Try to catch the intruder while he/she explores
  - This is a potentially dangerous approach
    - The intruder does have at least partial access
    - Crackers may become interested in your site

Detecting Intruders

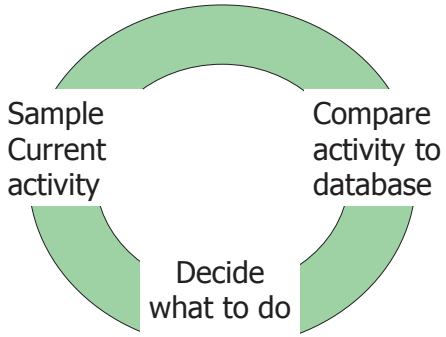
- An IDS monitors system activity in some way
  - When it detects suspicious activity, it performs an action
- The action is usually an alert of some type
  - E-mail, cell phone, audible alert, etc. to a person or process
  - For highly sensitive systems, consider an out-of-band channel that does not depend on the potentially compromised system
- All IDS systems continuously sample system activity and compare the samples to a database

Principles of IDS

- An IDS must run unattended for extended periods of time
- The IDS must stay active and secure
- The IDS must be able to recognize unusual activity
- The IDS must operate without unduly affecting the system's activity
- The IDS must be configurable

Principles of IDS (cont'd)

Figure 13.1 Standard Sample-Compare-Decide IDS cycle



The IDS Taxonomy

- Two basic types of intrusions
  - Misuse intrusion: an attack against a known vulnerability
    - Relatively easy to detect because the actions required for the exploit are known (called the attack signature)
  - Anomaly intrusion: an attack against a new vulnerability or one using an unknown set of actions
    - Relatively difficult to detect, must compare current system activity with some normal baseline of activity
- Two types of IDS that correspond to the two intrusion types
  - Signature based
  - Knowledge based

The IDS Taxonomy (cont'd)

- Signature-based IDS
  - Detects misuse intrusions
  - Maintains a database of attack signatures
  - Compares current activity to database
  - Database must be current and complete to be effective
- Knowledge-based IDS
  - Detects anomaly intrusions
  - Builds a profile of "normal" system activity over time
  - Produces more false positives and requires more administration
  - Requires careful initial configuration

Using Rules and Setting Thresholds for Detection

- A rule tells the IDS which packets to examine and what action to take
  - Similar to a firewall rule
  - Alert tcp any any -> 192.168.1.0/24 111
    (content:"|00 01 86 a5|";msg:"mountd access";)
    - Alert specifies the action to take
    - Tcp specifies the protocol
    - Any any 192…. specifies the source and destination within the given subnet
    - 111 specifies the port
    - Content specifies the value of a payload
    - msg specifies the alert message to send

Using Rules and Setting Thresholds for Detection (cont'd)

- A threshold is a value that represents the boundary of normal activity
- For example, if the login failure threshold is three, the IDS takes some action after the third failed attempt
  - Action might be to lock the account and notify an administrator
- Other thresholds include file I/O, network activity, administrator logins and actions

Exploring a Typical IDS

- **Snort** is an example of an IDS
  - Freely available www.snort.org
  - Current version 2.4.1 (2005-09-26)
  - Originally written for UNIX, but now available for Windows also (since 2.3 2005-01)
- Basically a highly configurable packet sniffer, Snort analyzes network traffic in real time

Exploring a Typical IDS (cont'd)

- Snort sniffs a packet from the network
  - Preprocessor looks at the packet header and decides whether to analyze it further
  - If so, the detection engine compares pattern from rules to the packet payload
  - If the payload matches, the appropriate action is taken
- Snort can be used in a plain packet sniffer mode or in full IDS mode
- Snort has numerous options that are used to configure its activity

Exploring a Typical IDS (cont'd)

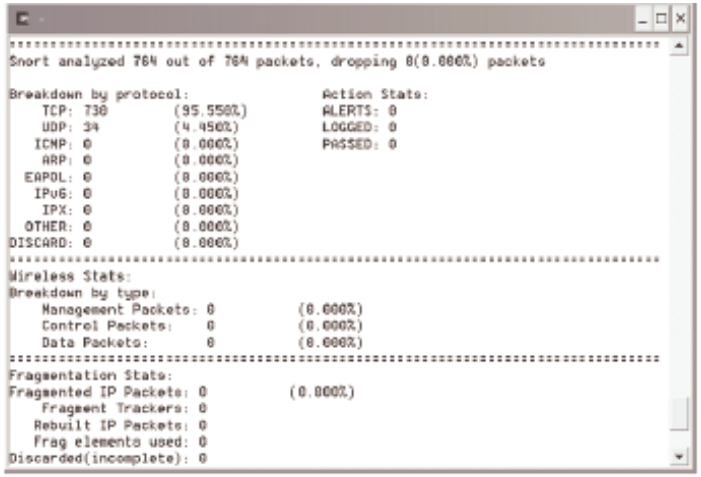


Figure 13.2 Sample Snort packet sniffing summary

Exploring a Typical IDS (cont'd)

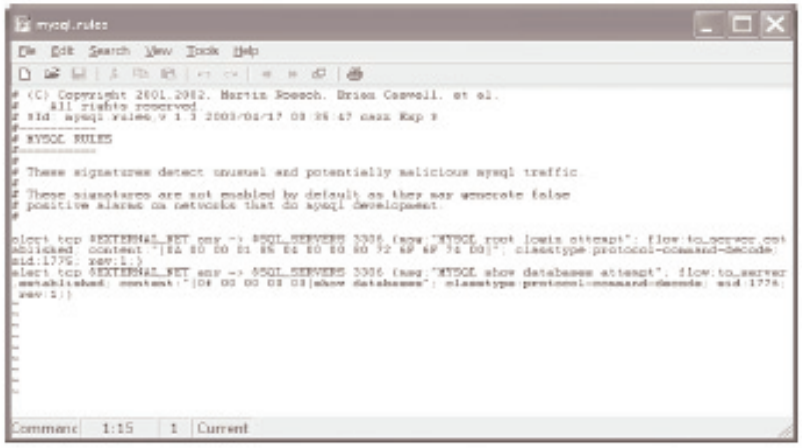


Figure 13.3 Contents of the mysql.rules file

Exploring a Typical IDS (cont'd)

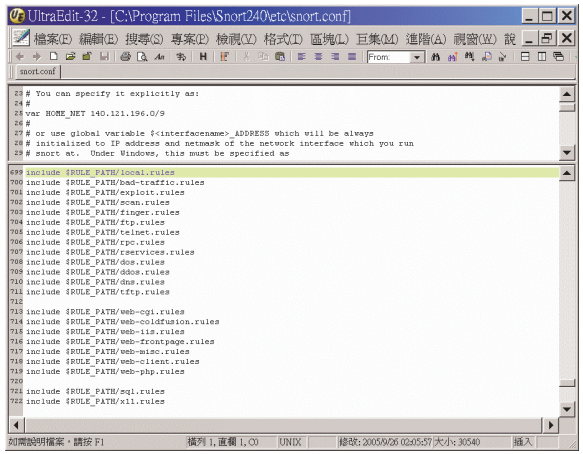


Figure 13.4 Partial contents of snort.conf file

Network-Based IDS

- IDS systems are also classified by their intended locations
- A network-based IDS monitors all traffic on a network segment
  - Can detect intrusions that cross a specific network segment
  - Administrators sometimes place one inside and one outside of a firewall
  - The IDS placed outside of a firewall will not see traffic that passes between LAN computers

A Network-Based IDS

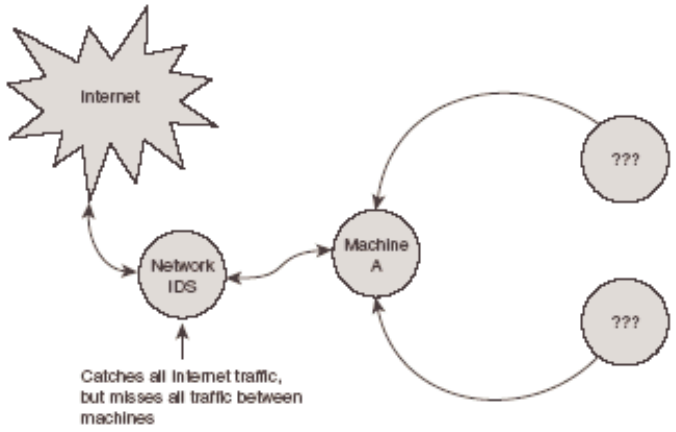


Figure 13.5 A network-based IDS

Host-Based IDS

- A host-based IDS examines all traffic received and activity for a particular machine
  - Can examine system log files as well as inbound and outbound packets
  - Each system requires its own IDS
- If resources are available, the best choice is to use both network-based and host-based IDS in your organization
- Many firewalls provide some IDS functionality, eg. BlackICE

Choosing an Appropriate IDS

- The first step in choosing an IDS is to determine what your organization's security needs are
- Research the different IDS packages available
  - These change frequently
- For medium to large organizations, it is common to use both network-based and host-based IDS
- Make sure you get a product you have confidence in

Security Auditing with an IDS

- Every organization should have periodic security audits
  - Sometimes mandated by law or by corporate structure
- An IDS can contribute to a complete audit
- Many host-based IDS can scan and analyze system log files
  - They can act as a filter for various behaviors
- A port-sniffing IDS can help to profile network activity
  - Providing a picture of system activity over time

Summary

- An intrusion is the use of a system without authorization
- An intrusion detection system (IDS) is hardware or software that monitors system activity, and looks for and responds to suspicious behavior
- Intruders can be external or internal
  - Responses to intruders are block and ignore, block and investigate, and honeypot
- A set of five principles should be applied to the selection of an IDS

Summary (cont'd)

- Two basic types of intrusions are misuse intrusion and anomaly intrusion
- Corresponding IDS types are signature-based and knowledge-based
- A signature-based IDS compares attack signatures to a signature database
- A knowledge-based IDS compares threshold values to current activity
- Snort is a typical, freely available, IDS

Summary (cont'd)

- A network-based IDS monitors all traffic on a network segment
- A host-based IDS monitors activity on a particular machine
- The choice of an IDS should be based on the organization's security needs and its resources
- It is common to implement both network-based and host-based IDS in medium and large organizations
- Auditors can use IDS capabilities to assist in completing a thorough audit

Assignments

- Reading: Chapter 13
- Practice 13.10 Challenge Questions

- Group Assignment: Turn in Challenge Exercise 13.2 with a three pages discussions next week