Auditing

Dr. Ahmad Almulhem

Computer Engineering Department, KFUPM

Spring 2008
Outline

1 Overview
   • Auditing
   • Uses
   • Challenges

2 Structure
   • Logger
   • Analyzer
   • Notifier
Auditing

- Tracing security violations
- Security-relevant actions should be logged
- Accountability
- Logs should be protected
What is Auditing?

**Definition (Logging)**

*Recording* events or statistics to provide information about system use and performance

**Definition (Auditing)**

*Analysis* of log records to present information about the system in a clear, understandable manner
Auditing Uses

- Describe security state (security policy)
  - Determine if system enters unauthorized state
- Evaluate effectiveness of protection mechanisms
  - Determine which mechanisms are appropriate and working
- Deter attacks because of presence of record
  - Abuses are being watched!
Auditing Challenges

- What do you log?
  - Hint: looking for violations of a policy, so record at least what will show such violations
  - Examples: packets, system calls
  - How about logging everything?

- What do you audit?
  - Need not audit everything
  - Key: what is the policy involved?
Audit System Structure

1. **Logger**
   - Records information, usually controlled by parameters

2. **Analyzer**
   - Analyzes logged information looking for something

3. **Notifier**
   - Reports results of analysis
Type, quantity of information recorded controlled by system or program configuration parameters

- sequential/chronological

- May be human-readable or binary

- If binary, viewing tools supplied
Logger Example: Windows XP

- Different logs for different types of events:
  - **System** event logs record system crashes, component failures, and other system events
  - **Application** event logs record events that applications request be recorded
  - **Security** event log records security-critical events such as logging in and out, system file accesses, and other events

- Logs are binary; use event viewer to see them
- If log full, can have system shut down, logging disabled, or logs overwritten
Logger Example: Windows XP

![Event Properties Window](image)

**Event Properties**

- **Event**
- **Date:** 17/05/2008
- **Source:** DCOM
- **Time:** 18:36:06
- **Category:** None
- **Type:** Error
- **Event ID:** 10035
- **User:** NT AUTHORITY\SYSTEM
- **Computer:** VM08

**Description:**

DCOM got error "The service cannot be started in Safe Mode." attempting to start the service EventSystem with arguments "" in order to run the server: (1BE1F766-5536-11D1-B726-00C04FB925AF)

For more information, see Help and Support Center at [http://go.microsoft.com/fwlink/events.asp](http://go.microsoft.com/fwlink/events.asp)
Logger Example: Unix

- Client/Server (syslog - RFC 3164)
- logs are in plain text (most read by root)
- Stored under `/var/log`
- Different logs for different types of events:
  - **Kernel** event logs from kernel
  - **Application** event logs from applications
  - **Daemons** event logs from daemons
Analyzes one or more logs
- Logs may come from multiple systems, or a single system
- May lead to changes in logging
- May lead to a report of an event
Analyzer Examples

- Text-based: Using **swatch** to find instances of telnet logs:
  `/telnet/&!/localhost/&!/*.site.com/`

- GUI: Octopussy
Notifier

- Informs analyst, other entities of results of analysis
  - email, pager, sms message, ... etc.
- May reconfigure logging and/or analysis on basis of results
Notifer Examples

- Using **swatch** to notify root:
  
  /telnet/&!/localhost/&!/*.site.com/ mail root

- Example: Three failed logins attempts:
  
  - **logger** records the attempts
  - **analyzer** checks the number of failed attempts
  - **notifier** disable account and notify admin (when the number reaches 3)