Security Audit Principles and Practices

Chapter 11

Lecturer: Pei-yih Ting

Logging and auditing are two of the most unpleasant chores facing information security professionals.

tedious, time-consuming, boring

Overview

- Configuring Logging
  - What should be logged
  - How long logs must be maintained
  - Configuring Alerts
  - Windows Logging / UNIX Logging
- Analyzing Log Data
  - Profiling Normal Behavior
  - Detecting Anomalies
  - Data Reduction
- Maintaining Secure Logs
- Conducting a Security Audit

Configuring Logging

- To configure logging, you should be prepared to answer the questions
  - What activities/events should be logged?
  - How long should logs be maintained?
  - What events should trigger immediate notifications to security administrators?
- Logging must be configured to the needs of the organization

What Should Be Logged?

- You can't log everything
  - Unless you have a lot of time and resources
  - Someone must review logs
  - Logging has a negative effect on system performance
  - Critical events may be overwritten
- A prudent approach is to strike a balance between logging important events but not everything
- What is an important event is defined by the environment to some degree and should be given careful consideration

What Should Be Logged?

- A government intelligence agency protects highly sensitive classified information. He would want to log every access to files that contain the identify of undercover agents.
- A popular news Web site should protect the integrity of data and try its best maintaining the availability of the Web site.

Determining How Long Logs Must Be Maintained

- Most operating systems allow you to overwrite log files based on time or file size
  - This choice may be determined by policy, e.g., log files must be kept for a certain amount of time
- Log files can be archived
  - You may need to maintain a (semi-) permanent record of system activity
  - Back up log files before they are overwritten
  - A common method is to alternate two log files, backing up one file while the other is active

Configuring Alerts

- With modern operating systems, you can set up alerts that notify administrators when specific events occur
  - For example, immediate notification if a hard drive is full
- Alert options include
  - E-mail, pagers, Short Message Service (SMS), instant messaging, pop-up windows, and cell phones
- Typically alerts can be configured differently depending on the severity of the event and the time
  - Only very severe events should trigger a cell phone call in the middle of the night, for example

Windows Logging

- Windows uses the Event Viewer as its primary logging mechanism
  - Found in Administrative Tools
- Event Viewer log files
  - Security log
    - Records security-related events
    - Controlled by a system administrator: types of events, overwrite policy, user …
    - Typical information includes failed logon attempts and attempts to exceed privileges

Windows Logging (cont'd)

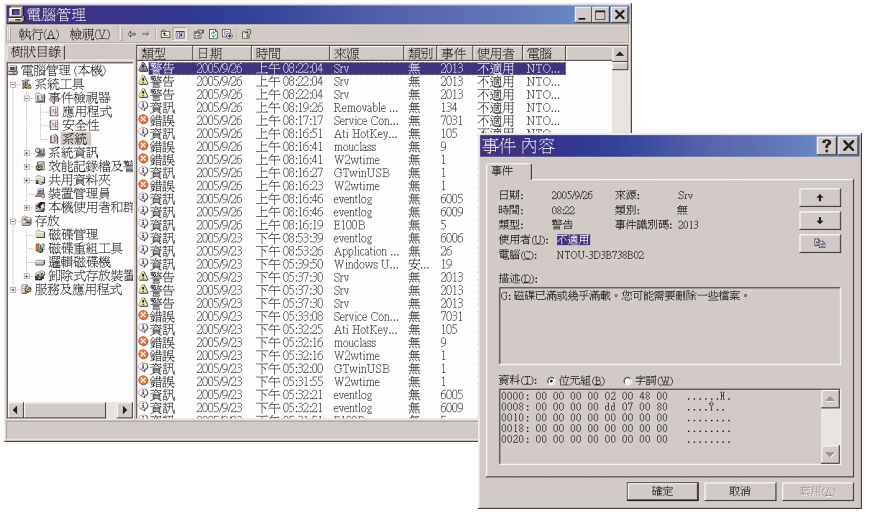
- Event Viewer log files (cont'd)
  - Application log
    - Records events triggered by application software
    - System administrators have control over what events to store
  - System log
    - Contains events recorded by the operating system
    - The system administrator generally has no control over this log
    - Typical events include hardware/software problems: driver failures, harddisk full…
  - Other specialized log files include the directory service log, the file replication service log, and the DNS server log

Windows Logging (cont'd)

- Four types of events are stored in Event Viewer logs
  - Error events are created when a serious problem occurs (corruption of a file system)
  - Warning events are created to alert administrators to potential problems (a disk nearing full)
  - Information events are details of some activities that are not indications of a problem (starting or stopping a service)
  - Success/failure auditing events are administrator-defined events that can be logged when they succeed, when they fail, or both (unsuccessful logon attempts)

Windows Logging (cont'd)

Windows 2000 Professional System log



UNIX Logging

- The primary log facility in UNIX is syslog
  - Very flexible, many options for notification and priority
  - Can write to a remote log file allowing the use of dedicated syslog servers to track all activity on a network
- Syslog implements eight priority levels
  - LOG_EMERG (emergency), LOG_ALERT (require immediate intervention), LOG_CRIT (critical system events), LOG_ERR (error), LOG_WARNING (warn of potential errors), LOG_NOTICE (information, no error), LOG_INFO (future use), LOG_DEBUG (developers use for debugging)

Analyzing Log Data

- Log data is used to monitor your environment
- Two main activities
  - Profiling normal behavior to understand typical system behavior at different times and in different parts of your business cycle
  - Detecting anomalies when system activity significantly deviates from the normal behavior you have documented

Profiling Normal Behavior

- A "snapshot" of typical system behavior is called a baseline
- Baselines can be obtained at the network, system, user, and process level
- Baselines detail consumption of system resources
- Baselines will vary significantly based on time of day or business cycle
- It is the administrator's responsibility to determine the baseline studies appropriate for an organization
  - These will change over time

Detecting Anomalies

- Define anomalies based on thresholds
- The following questions must be answered
  - How much of a deviation from the norm represents an anomaly?
  - How long must the deviation occur before registering an anomaly?
  - What anomalies should trigger immediate alerts?
- Anomalies can occur at any level
  - For example, if a user's behavior deviates from normal, it may indicate a serious security event

Data Reduction

- When possible, limit the scope of logging activities to that which can reasonably be analyzed
  - However, regulations or policies may stipulate that aggressive logging is necessary
- Data reduction tools are useful when more data is collected than can be reviewed
  - Often built into security tools that create log files
  - For example, CheckPoint's Firewall-1 allows you to view log files filtered by inbound TCP traffic to a specific port on a specific date

Maintaining Secure Logs

- Logs themselves must be protected from tampering and corruption
- Common techniques to secure logs include
  - Remote logging uses a centralized, highly protected, storage location
  - Printer logging creates a paper trail by immediately printing logged activity
  - Cryptographic technology digitally signs log files to ensure that changes can be detected, though the files are vulnerable until they are finalized

Conducting a Security Audit

- Security professionals examine the policies and implementation of the organization's security posture
  - Identify deficiencies and recommend changes
- The audit team should be well trained and knowledgeable
  - The team may be multidisciplinary including accountants, managers, administrators, and technical professionals
  - Choose a team based on your organization's needs

Checklists

- Checklists provide a systematic and consistent approach to completing various tasks in an audit
  - Audit checklists provide
    - a high-level overview of the overall audit process
    - stepwise processes for auditing different classes of systems
  - Configuration checklists contain specific configuration settings
  - Vulnerability checklists contain lists of critical vulnerabilities for each operating system in use
  - MS http://www.microsoft.com/technet/security/chklist/default.mspx

IP/Port Scanners

- IP/Port scanners are used by both crackers and system administrators
  - Use brute-force probing of IP addresses to identify open ports running services that may be vulnerable
  - Administrators can use this information to find rogue systems and services
    - Often set up by legitimate users who want to bypass the red tape of going through administration
  - Rogue systems and services are usually either removed or brought under administrative control

Vulnerability Scanners

- Vulnerability scanners are software applications that analyze systems for known vulnerabilities and create reports and suggestions
  - First vulnerability scanner was SATAN in the early 1990s
  - Newer scanners include
    - SARA – a descendant of SATAN (UNIX)
    - SAINT – a commercially supported scanner (UNIX)
    - Nessus – provides a scripting language for writing and sharing security tests (UNIX)
    - Microsoft Baseline Security Analyzer (MBSA) – free from Microsoft, downloads the most recent vulnerability database (Windows)

Integrity Checking

- Integrity checking
  - Maintains cryptographic signatures of all protected files to catch tampering
  - Tripwire is the most common tool for file integrity assurance
    - http://sourceforge.net/projects/tripwire/ free for UNIX
    - http://www.tripwire.com/ 30 days trial for Windows
  - Typically used to protect static Web sites and other systems that store critical data that is infrequently changed

Penetration Testing

- Penetration testing is a proactive approach used by security auditors
- The auditor tries to break into the system to find vulnerabilities
- Many security teams bring in professionals to conduct penetration testing
  - Called "white hat" hackers
  - Malicious hackers are called "black hat" hackers
- Be sure you have proper permission before conducting any type of penetration testing

Audit Results

- The job does not end with the audit
- Common post-audit tasks include
  - Reporting results
  - Prioritizing deficiencies that were found
  - Developing action plans for deficiencies
  - Implementing action plans based on priority and complexity
  - Conducting ongoing monitoring
  - Repeating the audit on a periodic basis

Summary

- Logging is the recording and analysis of system events to determine both normal system activity and anomalies in system activity
- You should strive for balance in determining what events should be logged
- Most logging software provides for considerable functionality and flexibility in configuring alerts
  - Be circumspect in how alerts are used
- The primary Windows logging tool is Event Viewer
- The primary UNIX logging facility is syslog

Summary (cont'd)

- A profile of normal system activity is called a baseline
- An anomaly is a significant deviation from a baseline, as determined by thresholds set by the administrator
- Logs files must be secured to avoid tampering
- Security auditing is used to identify problems in an organization's security policies and controls
- A number of tools are available to auditors to assist in finding problems and making recommendations

Assignments

- Reading: Chapter 11
- Practice 11.7 Challenge Questions

- Turn in Challenge Exercise 11.2 and 11.4 next week