

IT 4823

Information Security Administration

Security Auditing and Audit Controls



Notice: This session is
being recorded.

Assignment 5

1. Explain why blocking pings at edge router is ineffective.
2. Should Active Directory server go in DMZ?
3. Distinguish among packet filtering, stateful inspection, and proxy firewalls. Which kind protects against drive-by downloads?
4. Why block packets to broadcast address?
5. Why block outgoing packets with source addresses not in address space.

Security Auditing

The ability to determine:

- What happened
- When it happened
- Who did it.

Logging preserves this information.

Sources of Log Data in Health Care

Firewall logs	83%
Application logs	72
Server logs	70
Intrusion detection	60
Network devices	64
Storage devices	45

HIMSS Annual Survey: 2010 data

Growth of Log Data Volume

- 15-20% growth in annual volume (SANS Institute.)
 - More log sources
 - Increased regulation
 - Application log data

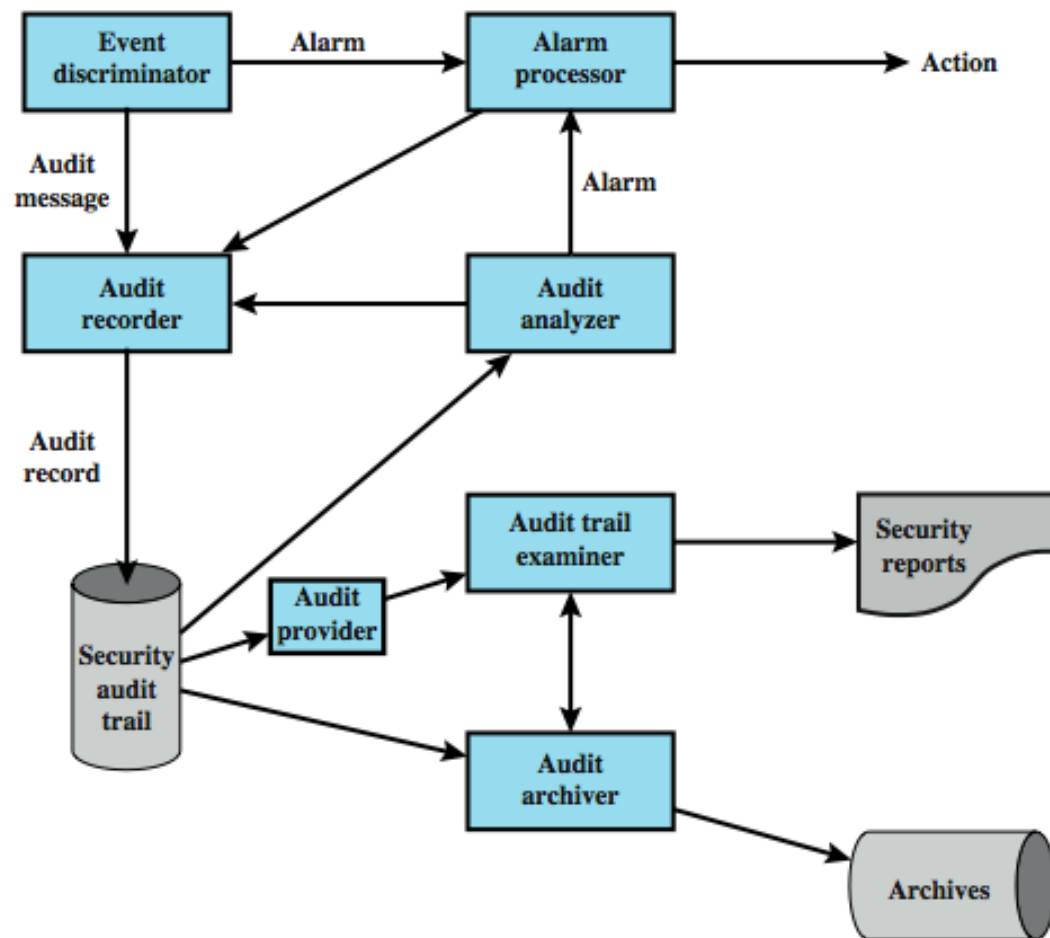
Collection and Use of Audit Data

- Detecting unauthorized access or abuse of authorized access.
- Regulatory requirements
- Financial audit requirements
- Problem determination (troubleshooting)

Problems

- Use of logging is mostly reactive
- Log files from multiple sources are in different, incompatible formats
- Log processing software not yet mature

Security Audit Architecture



Event Definition

- We must define (by policy) what are auditable events
- The Common Criteria suggest:
 - introduction of objects
 - deletion of objects
 - distribution or revocation of access rights or capabilities
 - changes to subject or object security attributes
 - policy checks performed by the security software
 - use of access rights to bypass a policy check
 - use of identification and authentication functions;
 - security-related actions taken by an operator/user
 - import/export of data from/to removable media

Other Audit Requirements

- Event detection hooks in software and monitoring software to capture activity
- Event recording function with secure storage
- Event and audit trail analysis software, tools, and interfaces
- Security of the auditing function itself
- Minimal effect on functionality

Implementation Requirements

1. Management agrees on requirements
2. Scope of checks agreed and controlled
3. Checks limited to read-only access to s/w and data
4. Other access only for isolated copies of system files, then erased or given appropriate protection
5. Resources for performing the checks should be explicitly identified and made available
6. Identify / agree on special requirements
7. All access should be monitored and logged
8. Document procedures, requirements, responsibilities
9. Person(s) doing audit should be independent of activities being audited.

What to Collect

- Issue: amount of data generated
 - tradeoff quantity vs. efficiency
- Data items captured may include:
 - auditing software use
 - use of system security mechanisms
 - events from IDS and firewall systems
 - system management / operation events
 - operating system access (system calls)
 - access to selected applications
 - remote access

Sources of Audit Data

- Operating system
- Application software
- User interaction
- Physical controls

Operating System Audit Data

- Are generally used to monitor and optimize system performance, but...
- Can also serve a security audit function
- Captures logins, device use, O/S functions, *e.g.*

Jan 27 17:18:38 host1 login: ROOT LOGIN console

Jan 27 17:19:37 host1 reboot: rebooted by root

Jan 28 09:46:53 host1 su: 'su root' succeeded for
user1 on /dev/tty0

Jan 28 09:47:35 host1 shutdown: reboot by user1

Application Software Audit Data

- To detect security violations within an application
- To detect flaws in application's system interaction
- For critical / sensitive applications, *e.g.* email, DB
- Record appropriate security related details, *e.g.*

Apr 911:20:22 host1 AA06370: from=<user2@host2>,
size=3355, class=0

Apr 911:20:23 host1 AA06370: to=<user1@host1>,
delay=00:00:02,stat=Sent

Apr 911:59:51 host1 AA06436: from=<user4@host3>,
size=1424, class=0

Apr 911:59:52 host1 AA06436: to=<user1@host1>,
delay=00:00:02, stat=Sent

User Interaction Audit Data

- Trace activity of individual users over time
 - To hold user accountable for actions taken
 - As input to an analysis program that attempts to define normal versus anomalous behavior
- May capture
 - User interactions with system, *e.g.* commands issued
 - Identification and authentication attempts
 - Files and resources accessed.
 - Use of applications

Physical Control Audit Data

- Generated by physical access controls, *e.g.* card-key systems, alarm systems
- Sent to central host for analysis / storage
- Can log
 - Date/time/location/user of access attempt
 - Both valid and invalid access attempts
 - Attempts to change access privileges
 - May send violation messages to personnel

Implementing Logging

- The foundation of security auditing facility is the initial capture of the audit data
- Software must include hooks (capture points) that trigger data collection and storage as preselected events occur
- Logging is operating system / application dependent
 - system-level logging can use existing means
 - review Windows Event Log & UNIX Syslog

Windows Event Log

- Each event is an entity that describes some interesting occurrence and
 - each event record contains: numeric id, set of attributes, optional user data
 - presented as XML or binary data
- Three types of event logs:
 - system - system related apps & drivers
 - application - user-level apps
 - security - Windows Local Security Authority (LSA)

Windows Event Log Example

Event Type: Success Audit
Event Source: Security Event
Category: (1)
Event ID: 517
Date: 3/6/2006
Time: 2:56:40 PM
User: NT AUTHORITY\SYSTEM
Computer: KENT
Description: The audit log was cleared
Primary User Name: SYSTEM
Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7)
Client User Name: userk
Client Domain: KENT
Client Logon ID: (0x0,0x28BFD)

Windows Event Categories

- account logon events
- account management
- directory service access
- object access
- policy changes
- privilege use
- process tracking
- system events

UNIX Syslog

- UNIX's general-purpose logging mechanism
 - found on all UNIX / Linux variants
 - but with variants in facility and log format
- Elements:
 - syslog() API
 - logger command utility
 - /etc/syslog.conf configuration file
 - syslogd daemon to receive/route log events

Syslog Service

- Basic service provides:
 - a means of capturing relevant events
 - a storage facility
 - a protocol for transmitting syslog messages from other hosts to a central syslog server
- Extra features may include:
 - robust filtering, log analysis, event response, alternative message formats, log file encryption, database storage, rate limiting

Syslog Protocol

- A transport allowing hosts to send IP event notification messages to syslog servers
 - provides a very general message format
 - allowing processes / apps to use suitable conventions for their logged events
- Common BSD (RFC3164) version has:
 - PRI: facility and severity code
 - header - timestamp & hostname/IP address
 - message - program name and content

Syslog Examples

```
Mar 1 06:25:43 server1 sshd[23170]: Accepted  
publickey for server2 from 172.30.128.115 port  
21011 ssh2
```

```
Mar 1 07:16:42 server1 sshd[9326]: Accepted password  
for murugiah from 10.20.30.108 port 1070 ssh2
```

```
Mar 1 07:16:53 server1 sshd[22938]: reverse mapping  
checking getaddrinfo for ip10.165.nist.gov failed  
- POSSIBLE BREAKIN ATTEMPT!
```

```
Mar 1 07:26:28 server1 sshd[22572]: Accepted  
publickey for server2 from 172.30.128.115 port  
30606 ssh2
```

```
Mar 1 07:28:33 server1 su: BAD SU kkent to root on  
/dev/tty2
```

```
Mar 1 07:28:41 server1 su: kkent to root on  
/dev/tty2
```

Syslog Facility and Severity

- Facility identifies application / system component that generates the message:
 - user kern mail daemon auth lpr news uucp cron local0-7 mark
- Severity (message level) indicates the relative Severity of the message
 - can be used for some rudimentary filtering
 - emerg alert crit err warning notice info debug

Audit Trail Storage Alternatives

- Read/write file on host
 - Easy, least resource use, fast access
 - Vulnerable to attack by intruder
- Write-once device (*e.g.* CD/DVD-ROM)
 - More secure but less convenient
 - Need media supply and have delayed access
- Write-only device (*e.g.* printer)
 - Provides paper-trail but impractical for analysis
- Must protect both integrity and confidentiality using encryption, digital signatures, access controls

Logging at Application Level

- Privileged applications have security issues
 - which system or user audit data may not see
 - And account for a large percentage of reported vulnerabilities
 - *e.g.* failure to adequately check input data, application logic errors
- Hence there is a need to capture detailed behavior
- Applications can be written to create audit data
- Applications can sometimes be retrofitted to generate log data.

Audit Trail Analysis

- Analysis programs/procedures vary widely
 - *cf.* NIST SP 800-92
- Must understand context of log entries
 - relevant info in same / other logs, config
 - possibility of unreliable entries
- Audit file formats are a mix of plain text / codes
 - hence must decipher manually / automatically
- Ideally, one would regularly review entries to gain understanding of baseline operations

Types of Audit Trail Analysis

- Audit trails can be used in multiple ways
- This depends in part on when done
- Possibilities include:
 - audit trail review after an event: triggered by event to diagnose cause and remediate
 - periodic review of audit trail data: review bulk data to identify problems and characterize behavior
 - real-time audit analysis as part of an intrusion detection function

Audit Review

- Audit review capability provides system administrators with information from selected audit records:
 - actions of one or more users
 - actions on a specific object or resource
 - all or a specified set of audited exceptions
 - actions on a specific system / security attribute
- May be filtered by time / source / freq etc.
- Used to provide system activity baseline
- And to gauge level of security related activity

Approaches to Data Analysis

- Basic alerting: indication that an interesting type of event has occurred
- Baselineing
 - define normal vs. unusual events / patterns
 - compare with new data to detect changes
- Windowing: identification of events within a given set of parameters
- Correlation: seeking relationships among events

“Artificial Stupidity”

- Identify those items in log files that are *not* interesting; filter them out.
- Everything else is either:
 - Interesting; examine further.
 - Not interesting: add to filter list.

Suggested by Marcus Ranum

Integrated Approaches

- Volume of audit data means manual analysis and baselining is impractical
- Instead, use a Security Information and Event Management (SIEM) system
 - a centralized logging and analysis package
 - agentless or agent-based
 - normalizes a variety of log formats
 - analyzes combined data
 - correlates events among the log entries
 - identifies and prioritizes significant events
 - can initiate responses

Security Compliance

- Conduct audits to review security processes
- Verify compliance with security plan
- Use internal or external personnel
- Usually based on checklists; verify that:
 - suitable policies and plans were created
 - suitable controls were chosen
 - that they are maintained and used correctly
- Often as part of wider general audit, *e.g.* an annual financial audit.

Questions

