Evaluating Running Systems

- Evaluating system security requires knowing what's going on
- Many steps are necessary for a full evaluation
- We'll concentrate on two important elements:
  - Logging and auditing

Logging

- No system's security is perfect
- Are my system's imperfections being exploited?
- You need to understand what's going on to tell
- Logging is the tool for that:
  - ***Keeping track of important system information for later examination***

The Basics of Logging

- OS and applications record messages about their activities
  - In pre-defined places in the file system
- These messages record important events
- And unexpected events
- Many attacks leave traces in the logs

Access Logs

- One example of what might be logged for security purposes
- Listing of which users accessed which objects
  - And when and for how long
- Especially important to log failures

Other Typical Logging Actions

- Logging failed login attempts
  - Can help detect intrusions or password crackers
- Logging changes in program permissions
  - A common action by intruders
- Logging scans of ports known to be dangerous

Problems With Logging

- Dealing with large volumes of data
- Separating the wheat from the chaff
  - Unless the log is very short, auditing it can be laborious
- System overheads and costs

Log Security

- If you use logs to detect intruders, smart intruders will try to attack logs
  - Concealing their traces by erasing or modifying the log entries
- Append-only access control helps a lot here
- Or logging to hard copy
- Or logging to a remote machine

Local Logging vs. Remote Logging

- Should you log just on the machine where the event occurs?
- Or log it just at a central site?
- Or both?

Local Logging

- Only gives you the local picture
- More likely to be compromised by attacker
- Must share resources with everything else machine does
- Inherently distributed
  - Which has its good points and bad points

Remote Logging

- On centralized machine or through some hierarchical arrangement
- Can give combined view of what's happening in entire installation
- Machine storing logs can be specialized for that purpose
- But what if it's down or unreachable?
- A goldmine for an attacker, if he can break in

Desirable Characteristics of a Logging Machine

- Devoted to that purpose
  - Don't run anything else on it
- Highly secure
  - Control logins
  - Limit all other forms of access
- Reasonably well provisioned
  - Especially with disk

Network Logging

- Log information as it crosses your network
- Analyze log for various purposes
  - Security and otherwise
- Can be used to detect various problems
- Or diagnose them later

Logging and Privacy

- Anything that gets logged must be considered for privacy
- Am I logging private information?
- If so, is the log an alternate way to access it?
- If so, is the log copy as well protected as the real copy?

An Example

- Network logs usually don't keep payload
  - Only some header information
- You can tell who talked to whom
- And what protocol they used
- And how long and much they talked
- But not what they said

Auditing

- Security mechanisms are great
  - If you have proper policies to use them
- Security policies are great
  - If you follow them
- For practical systems, proper policies and consistent use are a major security problem

Auditing

- A formal (or semi-formal) process of verifying system security
- "You may not do what I expect, but you will do what I inspect."
- A requirement if you really want your systems to run securely

Auditing Requirements

- Knowledge
  - Of the installation and general security issues
- Independence
- Trustworthiness
- Ideally, big organizations should have their own auditors

When Should You Audit?

- Periodically
- Shortly after making major system changes
  - Especially those with security implications
- When problems arise
  - Internally or externally

Auditing and Logs

- Logs are a major audit tool
- Some examination can be done automatically
- But part of the purpose is to detect things that automatic methods miss
  - So some logs should be audited by hand

What Does an Audit Cover?

- Conformance to policy
- Review of control structures
- Examination of audit trail (logs)
- User awareness of security
- Physical controls
- Software licensing and intellectual property issues

Does Auditing Really Occur?

- To some extent, yes
- 2008 CSI/FBI report says more than 64% of responding organizations did audits
- Doesn't say much about the quality of the audits
- It's easy to do a bad audit

Conclusion

- Don't assume your security is perfect
- Either at design time or run time
- Using security evaluation tools can help improve your security
- Necessary at all points in the life cycle:
  - From earliest design until the system stops operating