

## Real-World Scenario 13-3: Auditing Files

**Scenario:** You've analyzed packets, checked Syslogs, and checked for vulnerabilities on the firewall. As a final precaution you want to make sure that no one is accessing your file server and compromising the integrity of your data files.

You decide to enable auditing on the server. What steps are involved in accomplishing this?

## Real-World Scenario 13-3 Solution

Auditing is an excellent way to check for data integrity issues, check for breach of permissions, or simply make sure your files are being accessed exactly the way you want.

For example, you can enable auditing on a Windows Server and review who tried to access what, and whether they succeeded or failed. What you are most interested in is the attempted deletion or modification of data. The basic steps involved with auditing include enabling auditing in a policy, turning on auditing for a data folder (or other resource) in question, and reviewing the security log often.

**Video Solution:** Watch the video solution “13-3: Auditing Files.”