Why we audit user activity

Have you ever wondered if your employer is keeping a record of when you log into company systems?
Well, they are, if they're implementing the third and final function of the authentication, authorization, and accounting framework.

Accounting is the practice of monitoring the access logs of a system.
These logs contain information like who accessed the system, and when they accessed it, and what resources they used.

Security analysts use access logs a lot.
The data they contain is a helpful way to identify trends, like failed login attempts.
They're also used to uncover hackers who have gained access to a system, and for detecting an incident, like a data breach.

In this field, access logs are essential.
Oftentimes, analyzing them is the first procedure you'll follow when investigating a security event.
So, how do access logs compile all this useful information?
Let's examine this more closely.

Anytime a user accesses a system, they initiate what's called a session.
A session is a sequence of network HTTP basic auth requests and responses associated with the same user, like when you visit a website.
Access logs are essentially records of sessions that capture the moment a user enters a system until the moment they leave it.

Two actions are triggered when the session begins.
The first is the creation of a session ID.
A session ID is a unique token that identifies a user and their device while accessing the system.
Session IDs are attached to the user until they either close their browser or the session times out.

The second action that takes place at the start of a session is an exchange of session cookies between a server and a user's device.
A session cookie is a token that websites use to validate a session and determine how long that session should last.
When cookies are exchanged between your computer and a server, your session ID is read to determine what information the website should show you.

Cookies make web sessions safer and more efficient.
The exchange of tokens means that no sensitive information, like usernames and passwords, are shared.
Session cookies prevent attackers from obtaining sensitive data.
However, there's other damage that they can do.

With a stolen cookie, an attacker can impersonate a user using their session token.
This kind of attack is known as session hijacking.

Session hijacking is an event when attackers obtain a legitimate user's session ID.
During these kinds of attacks, cyber criminals impersonate the user, causing all sorts of harm.
Money or private data can be stolen.
If, for example, hijackers obtain a single sign-on credential from stolen cookies, they can even gain access to additional systems that otherwise seem secure.

This is one reason why accounting and monitoring session logs is so important.
Unusual activity on access logs can be an indication that information has been improperly accessed or stolen.
At the end of the day, accounting is how we gain valuable insight that makes information safer.

Revision #1
Created 2023-07-27 16:44:33 UTC by naruzkurai
Updated 2023-08-15 18:44:12 UTC by naruzkurai