JULETTE ANTHONY PEQUE

ACTIVITY 44

INFORMATION ASSURANCE AND SECURITY 1 - IT 3

PROFESSOR: FULGENCIO D. DUCUT

WHAT IS AUDIT LOG?

An audit log is a record of events as they happen within a computer system. A system of log-keeping and records becomes an audit trail where anyone investigating actions within a system can trace the actions of users, access to given files, or other activities like the execution of files under root or administrator permissions or changes to OS-wide security and access settings.

ACTIVITY 44

DESCRIBE THE ROLE OF AUDIT LOG AS PART OF THE DETECTION MODULE OF THE COMPUTER SECURITY OPERATIONAL MODEL

Audit logs capture details about system configuration changes and access events, with details to identify who was responsible for the activity, when and where the activity took place, and what the outcome of the activity was. Automated log analysis supports near real-time detection of suspicious behavior. Potential incidents are escalated to the appropriate security response team for further investigation.

JULETTE ANTHONY PEQUE

THANK YOU!

PROFESSOR: FULGENCIO D. DUCUT