A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

2. Project 3 – terminal after dragging .dmg file

1. Project 3 – terminal with command

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

4. Project 4 – console.app

3. Project 3 – terminal output

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

6. Project 4 – Console search through search box

5. Project 4 – Consol Errors and Faults

A computer screen shot of a computer

Description automatically generated

7. Project 4 – Console Reports

A screenshot of a computer

Description automatically generated

8. Project 4 – System Log File

A screenshot of a computer

Description automatically generated

9. Project 4 – System Log File filtered search

A screenshot of a computer

Description automatically generated

10. Project 4 – Copied System log

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

12. Project 4 – System Log revealed in finder

11. Project 4 – System log pasted into text file

**Project 5**

National Institute of Standards and Technology (NIST) Special Publication (SP) [800-171](https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Rev.2

<https://github.com/usnistgov/macos_security/blob/main/baselines/800-171.yaml>

The macOS security baseline outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Revision 2, provides comprehensive guidelines for nonfederal systems and organizations to protect Controlled Unclassified Information (CUI). The recommendations cover essential aspects such as access control, audit and accountability, configuration management, incident response, security assessment, security training, system and communications protection, and system and information integrity. By emphasizing principles like least privilege, secure configurations, and incident response readiness, organizations can enhance the security posture of their macOS systems, ensuring the confidentiality, integrity, and availability of sensitive information while aligning with broader cybersecurity goals.

**Project Thought Questions**

1. Will these security logs track failed logon attempts? From remote machines too?

Yes, security logs can track failed logon attempts, including those from remote machines.

1. Will it track security events other than just logon/ logoff events?

Yes, security logs can capture a variety of security events beyond logon/logoff activities. These events may include system and network-related events, policy changes, and other security-relevant occurrences.

1. Can you use Event Viewer or Mac Console to view other logs?

Yes, you can use Event Viewer on Windows and Console on macOS to view various logs, including system logs, application logs, and security logs. These tools allow users to inspect and analyze logged events for troubleshooting, security monitoring, and auditing purposes.

1. Why is there a log that tracks which Microsoft office programs you use and how long you use them?

This log is likely for auditing and productivity monitoring purposes.

1. How could a top-notch hacker keep you from knowing which files were changed?

A top-notch hacker might employ advanced techniques like fileless attacks or manipulation of log entries to avoid detection of file changes.

1. Can you calculate a hash for a single file?

Yes, you can calculate a hash for a single file using hashing algorithms like MD5, SHA-256, or others. This hash serves as a unique identifier for the file based on its content.

1. From the hash could you tell what was changed in the file?

While you can verify if a file has been changed by comparing its current hash with the original hash, the hash itself does not reveal what specific changes were made in the file.

1. Can you use the longest hash possible? How long is good enough?

The length of the hash depends on the hashing algorithm used. For example, SHA-256 produces a 256-bit hash, which is longer and more secure than, say, MD5 (128-bit). Generally, longer hashes provide better security against collision attacks, where two different inputs produce the same hash.