

File Audit Report

September 21st, 2025

CIS 4670 - Network Security
Dr. Brown



Jessica Setiadhi

Yuri Hyder

Elke Zak

Safa Alasady

Matthew Garcia

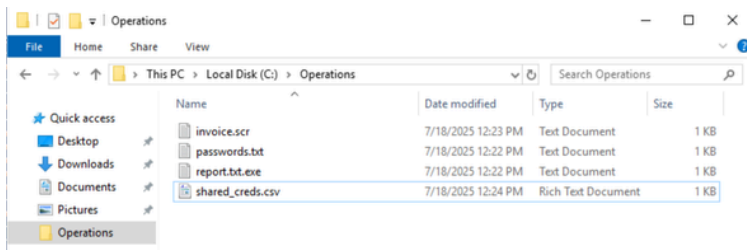
Executive Summary

SWIT was granted access to a Windows 2019 Server for a file audit. During the assessment, several critical vulnerabilities were discovered:

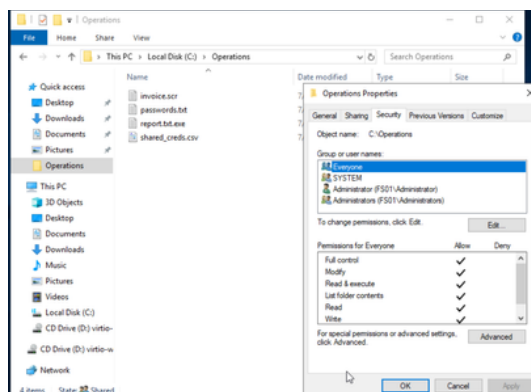
- Unencrypted plaintext credentials.
- Files disguised as unencrypted plaintext credentials that may contain malware.
- Exposed account references to both the privileged and guest users.

These critical vulnerabilities increase the risk of data leakage, unauthorized access, and a fully compromised system. Immediate remediation is recommended for the protection of the system's essential assets.

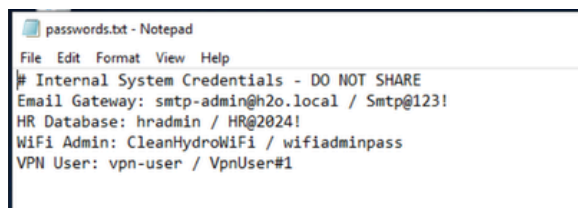
Screenshot 1: A critical vulnerability of unprotected sensitive file exposure. A folder with plain text files which indicates exactly what is stored inside (e.g. passwords.txt).



Screenshot 2: Another critical vulnerability of overly permissive permissions. Every user has access with all permissions enabled.

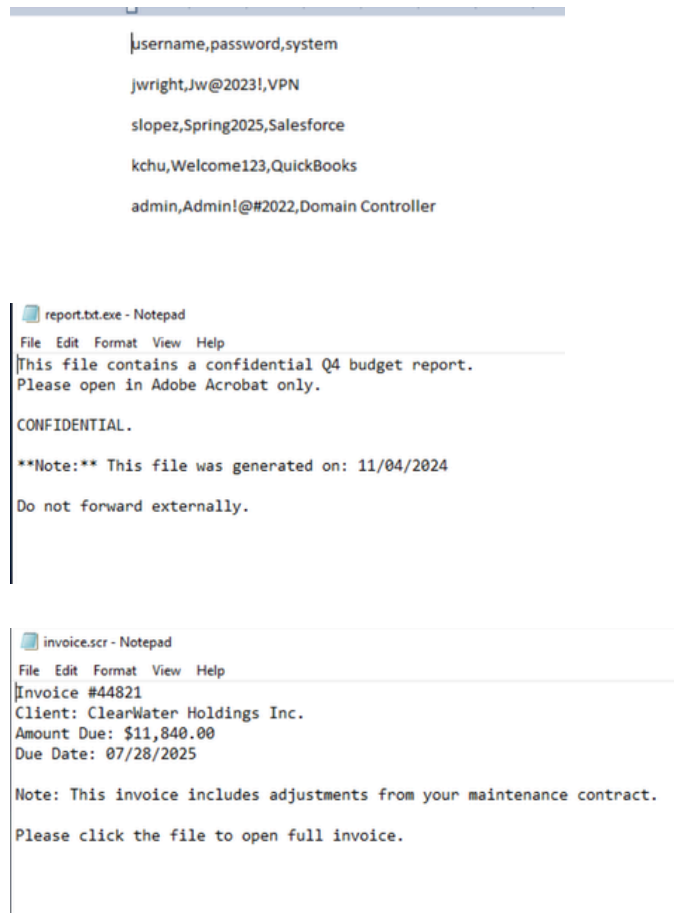


Screenshot 3: Additional critical vulnerability of improper storage of sensitive information. Internal system credentials are stored in an unencrypted plaintext file.



Appendix

Screenshot 4 - 6: Additional examples of the critical vulnerability of improper storage of sensitive information, all in unencrypted, plain text files.



Mitigation Steps

For the best security practices, this server is recommended to follow a formed security plan in order to mitigate their vulnerabilities:

1. Immediate removal of malicious files in order to avoid:
 - a. Causing general damage to the system.
 - b. Data harvesting and exfiltration.
 - c. Potential financial loss.
2. Changing vulnerable credentials to prevent unauthorized access.
3. Implementation of least-privilege access controls to minimize any internal misuse of the system.
4. Encryption of sensitive data to protect against data leaks.
5. Enabling monitoring/logging for future anomalies.