

Iterative Security Test Report

Version: 4

Project Name: Cybersecurity Capstone One Project

Test Completed on: October 31, 2021

Team Members: Riley Dorough, Kayla Echols, Julia Wilkins, Brett Wolff

BLUF Statement: Project is on schedule, there are currently no issues blocking progress.

Vulnerability

Level

● Low ● High ● Untested
● Medium ● Critical

Progress

Key:

In Progress | Completed | Untested

Executive Summary

As the team moves forward, we will be conducting more security tests as well as reviewing the project requirements. We will continue to monitor the many Common Vulnerability Exposures (CVEs) that apply to the various software's including SQL Server, openHistorian, and Grafana as well as the operating systems that our team is using. The team is aware of these and is collecting tools that can be utilized to test for any potential risks as well as preparing a mitigation plan for already known risks. The team will also begin planning ways to test the security of our virtual network to ensure a safe flow of data.

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 1. Vulnerability Metrics. Retrieved from <https://nvd.nist.gov/vuln-metrics/cvss>.

CONFIDENTIAL

OWASP Top 10 Findings

There are a handful of risks which are applicable to the current status of the project. These are the Man in the Middle (MITM), Denial of Service/Distributed Denial of Service (DoS/DDoS), social engineering, Remote Desktop Protocol (RDP), unencrypted communication, and personal identifiable information (PII) leakage. Most of these risks threaten the network layer and thusly, are not evaluated using the manual source code review. These risks, other than social engineering, will be evaluated in the iterative testing cycle, once penetration testing and attempts to break the software begin.

For descriptions of security test cases and their associated risks and security requirements, see Appendices B and C.

Risk	Test Cases (See Appendix C – Security test Cases)	Status
Man in the Middle Attack (MITM)	TC-PT-001: Pen Test: Man in the Middle <ul style="list-style-type: none">SR-AUTN-001SR-AUTN-002SR-AUTN-003	Not Tested
DoS/DDoS (Denial of Service and Distributed Denial of Service)	TC-PT-003: Pen Test: DOS/DDOS <ul style="list-style-type: none">No related security requirements, but DOS/DDOS attacks are a risk that need to be assessed.Both Host and Public Website	Not Tested
Social Engineering	Attempts to gain sensitive information <ul style="list-style-type: none">PhishingPII Leakage	In Progress
Windows Remote Desktop Protocol (RDP)	Attempts to gain access to the desktop remotely to gain control and access information	Completed
Unencrypted Communications	Data in transit could be vulnerable <ul style="list-style-type: none">If unencrypted, someone could intercept informationCould also be under MITM	Not Tested
Unfamiliar/ Insecure Protocols	OPTO devices utilize memory map protocol (MMP). Testing needs to be done to ensure its security. <ul style="list-style-type: none">None/ minimal embedded securityEasy to crack encryption methodsMITM capabilities	In Progress

CVE's

After review of the different technologies being used in this product, we decided to research different CVE's that may be applicable. While there is a handful of CVEs that are applicable to our project, most of them can be resolved simply by updating the software being used. So rather than spending time talking about such software, the focus will be on CVE's that are not so easily resolved.


This also applies to products that will be designed in house as proprietary products. They should hopefully not have any inherent CVE or vulnerabilities, but they will be tested as if they have them, both alone and integrated with the system. Some CVEs will likely exist for the platforms that the software will be built on, however this is not the focus of the software that will be developed/integrated. Namely, the data historian or the database.

CVE	Test Cases	Status
<ul style="list-style-type: none">CVE-2021-040444	Force all systems to comply with updates to Microsoft Defender detection build 1.349.22.0. Backup: ensuring all Word files are opened only in safe mode. Workaround: Disable ActiveX controls via Group Policy	Completed

Manual Code Review Findings

The purpose of the Manual Source Code Review is to determine areas of interest for the iterative testing cycle, as well as document and communicate the initial security posture of the project's software. Beginning code review/ research returned large amounts of CVEs for non-open-source applications and systems.

For descriptions of security test cases and their associated risks and security requirements, see Appendices B and C.

Test Cases & Associated Risks and Requirements	Discovered Vulnerabilities & Impact Summary	Assigned To:	Type:	Status
[Kayla Echols] Windows 10 21h1: <ul style="list-style-type: none"> CVEs to be listed here 	None at this time to be tested. Standing LNG infrastructure to be accessible first.	N/A	N/A	

Automated Code Review Findings

The team is in the process of researching different tools to review the source code for the various programs that we are using for this project including openHistorian and SQL. We anticipate having further code to review as we begin working on the .NET framework and when we begin writing in SQL to construct our databases.

For descriptions of security test cases and their associated risks and security requirements, see Appendices B and C.

Test Cases & Associated Risks and Requirements	Discovered Vulnerabilities & Impact Summary	Assigned To:	Type:	Status
[Kayla Echols] SQL: <ul style="list-style-type: none"> CVEs to be listed here 	None at this time to be tested. Standing LNG infrastructure to be accessible first.	N/A	N/A	In Progress

Stride Threat Model

Spoofing: Opportunities for spoofing attacks are being investigated

Tampering: The possibility for tampering in source and service code is being examined

Repudiation: Allowing attackers to complete malicious actions on the network or hosts without leaving any trace of their identity.

Information Disclosure: Analysis of unwanted information disclosure such as service information is being tested

Denial of Service: The possibility of some services being vulnerable to denial-of-service attacks are being explored

Elevation of Privilege: Avenues of privilege escalation are being explored, specifically in regards to kernel exploitation and sudo version vulnerabilities. Testing was done to determine CentOS 7 vulnerabilities specifically Sudo Baron Samedit and Dirty Cow exploits were tested.

Lateral Movement: Avenues of that allow for pivoting from unprivileged to privileged users are being explored.

Use Case Testing Categories

Test Cases & Associated Risks and Requirements	Associated Use Cases	Type	Status
Authentication	Log into Linux and Windows Server as Admin Log into Linux and Windows Server as Standard User Users can view data in the proper format	Functionality	Completed
Availability	Log into Linux and Windows Server as Admin Log into Linux and Windows Server as Standard User Test the change data functionality as the admin account	User Interface	Completed
Functionality of Code	Manual testing of the code functionality Automated testing of the code	Unit	In Progress
Functionality after Integration	Checks communication between the various programs	Integration	In Progress
Performance	Tests the software for speed, response time, stability, scalability, and resource usage	Performance	In Progress
Confidentiality	Test permissions for the user account Tests the privileges for the admin account	Security	In Progress
Data integrity	Database assessment	Database	In Progress
Functionality	Test new users interactions with the software	Usability	In Progress

Automated Dynamic Testing Findings

Automated dynamic testing involves checking the response of the system to the application being run. It observes the behavior of the software system, memory usage, CPU usage, and overall performance of the system. The main goal of automated dynamic testing is to ensure that the finalized product is in a correct working state that does not overexert the machine to unstable levels. Automated dynamic testing can be conducted using unit testing, integration testing, and system testing. We have determined that this type of testing is not

CONFIDENTIAL

within the scope of the customer's goals for the project. At this time automated dynamic testing will not be applicable. As machine learning is incorporated into the CVALNG project, automated testing becomes much more feasible.

CONFIDENTIAL

Penetration Testing Findings

The purpose of the penetration test is to simulate ways in which an adversary attacking a network running the software would interact with and attack the software. Due to the large number of test cases in the penetration test, it will be split across multiple iterative tests to allow each case to be fully and carefully tested.

For descriptions of security test cases and their associated risks and security requirements, see Appendices B and C.

Test Cases & Associated Risks and Requirements	Discovered Vulnerabilities & Impact Summary	Assigned To:	Type:	Status:
TC-PT-001: Man in the Middle <ul style="list-style-type: none">SR-AUTN-001SR-AUTN-002SR-AUTN-003	The testing and development network is not configured in a manner that allows network traffic from one machine to be collected and viewed by another. This makes it difficult to test Man in the Middle attack testing. The action item related to this test case for the upcoming week is to see if the testing environment can be reconfigured to allow collection of network traffic.			
TC-PT-002: DNS Hijacking	The .NET framework deals with DNS resolution using a class titled System.Net which contains functions such as Resolve (resolves a DNS host name or IP address) and GetHostByName (gets the DNS information for the specified DNS host name). After review of the code, multiple source code files were found to contain the System.Net class. However, none of the source code use any of the functions dealing with DNS.			
TC-PT-003: DOS/DDOS <ul style="list-style-type: none">SR-ATEN-001SR-ATEN-005	The .NET framework contains the CompressedStack class and is defined within the CompressedStack.cs file. The CompressedStack class represents the code access security information containing a Deny action (CompressedStack Class, n.d.). The CodeAccessPermission.Deny Method to prevent callers higher in the call stack from using the code (CodeAccessPermission.Deny Method, n.d.).			

<p>TC-PT-004: API Auth Bypass</p> <ul style="list-style-type: none"> SR-IDEN-002 	<p>After inspecting the source code, the team has decided to ask the client before testing the API. Because the API may be a production service, we'd rather not attack it without express permission and further information from the client.</p> <p>Per the client meeting on 10/11/19, we will not be given access to the API to preform testing. API Authentication security recommendations will be documented and delivered to the client. This test case will be marked as resolved once the client receives the security recommendations.</p>			
<p>TC-PT-005: Malicious Binary Delivery</p> <ul style="list-style-type: none"> SR-INTG-001 SR-INTG-002 SR-INTG-003 SR-IMMU-001 SR-SYSM-002 	<p>After review of the source code, it has been determined that the best way to conduct malicious binary injection is to create a malicious package to be installed and run by the application. Another possibility is to modify an existing package before installation. However, this will be difficult without prior knowledge on how the packages are structured. According to the file 'AgentUtilities.cs' a package is downloaded using the function 'DownloadPackageVersion' from http://.... and saved as a .zip file in</p>			
<p>TC-PT-006: Privilege Escalation</p> <ul style="list-style-type: none"> SR-IMMU-002 SR-IMMU-003 SR-SURV-001 SR-SYSM-002 SR-AUTR-001 SR-AUTR-002 	<p>The System agent code takes advantage of the System.ServiceBase class. This class utilizes "ServiceProcessInstaller" which is responsible for installing the service onto the system.</p> <p>"ServiceProcessInstaller also specifies which account is going to be used to install the service on the system. In "ProjectInstaller.cs" there is a function "InitializeComponent" which specifies that the LocalSystem account will be used to install and start the process contained in the package fed into the agent. The LocalSystem account has full access to the resources on the machine (source). If a malicious package is able to be fed into the agent, we could use the LocalSystem account to our advantage.</p>			

TC-PT-007: COM Hijacking <ul style="list-style-type: none"> SR-AUTN-002 SR-IMMU-002 SR-IMMU-003 	COM is not used by the code within the scope of the project. If we end up working with the software engineering team on their package that interacts with applications, COM Hijacking will become an area of interest.			
TC-PT-008: Back Doors <ul style="list-style-type: none"> SR-IDEN-002 	At this time, the risk of backdoors in the code has been assessed through a manual code review. Based on the safeguards built-in to Velocity's source code, the risk of backdoors is at a low level, and therefore is not at a high priority for testing. However, penetration tests to ascertain the risk of backdoors in the code will be performed in the future.			

Summary Graphs

Listed CVEs Per Host Version - 2021

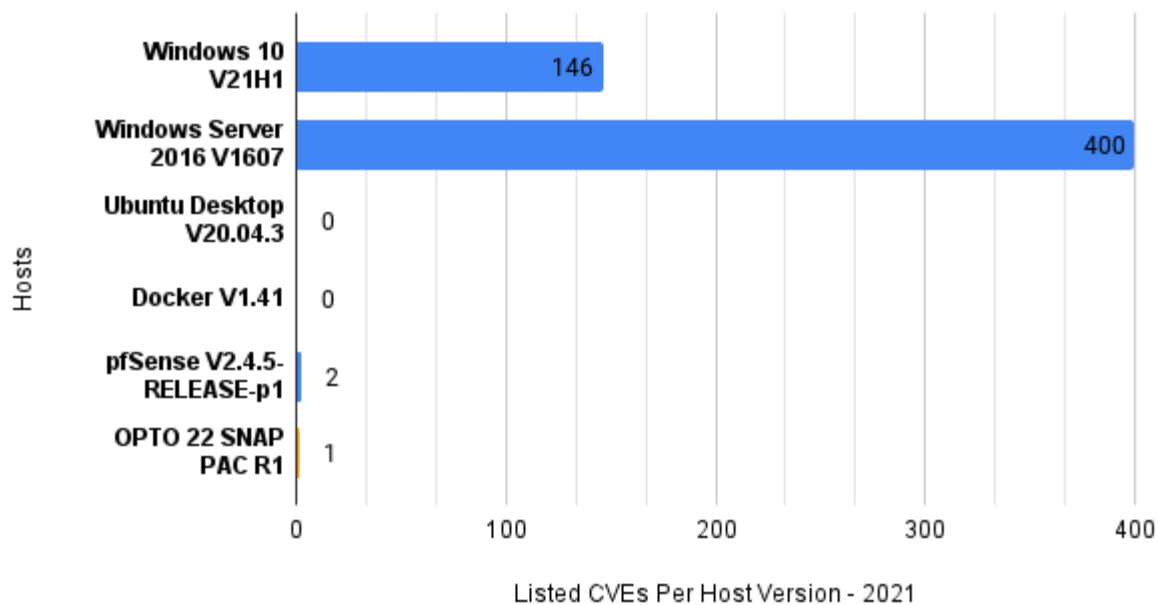
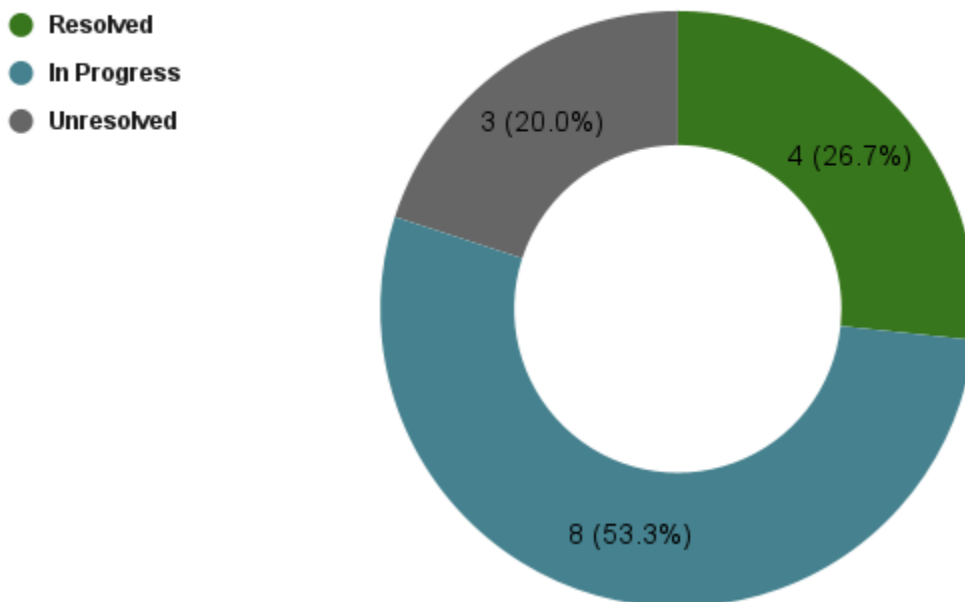


Figure 9.1 Total list of known CVEs per host version in 2021. Data Retrieved from: <https://www.cvedetails.com/>.

Security Points of Interest



ADVERSARY:

Advanced Persistent Threat
Insider Threat
Hacktivists



INFRASTRUCTURE:

SCADA
Industrial Control Systems
Business Office Environment
Database



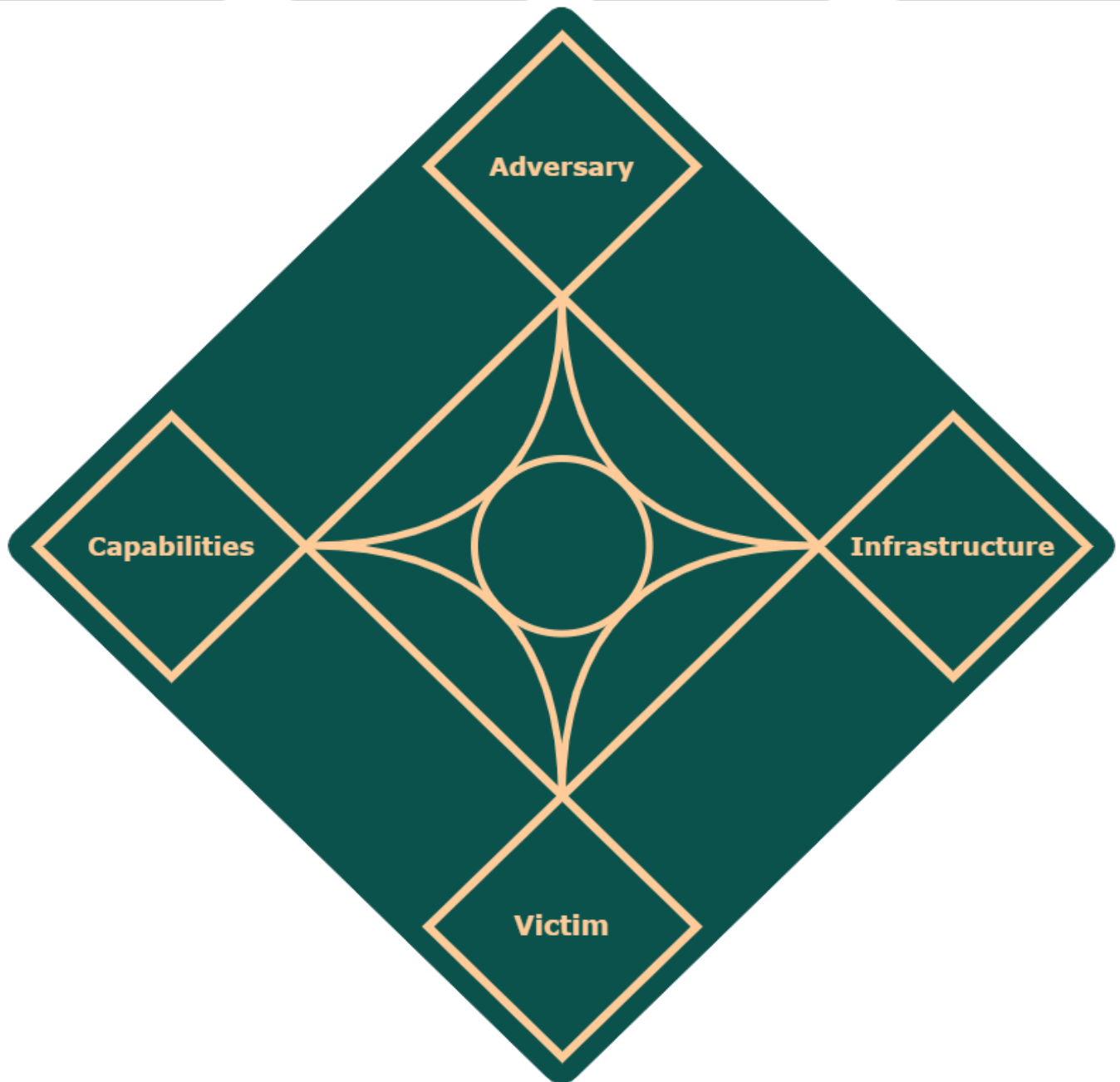
VICTIM:

Clients / Customers
Business / Organization
Shareholders
DEVOPS Team



CAPABILITIES:

TTPs
Exploitation
SQL Injection
Social Engineering



Action Items & Areas of Interest

As we wrap up building and move into testing it is important to take note of any potential issues we might have. After reviewing CVE's as well as surface level code reviews, we have yet to find any major issues in our system. However, this is only a surface level review. Over the next 7 weeks we will be digging more into the system to ensure that we are being thorough in our review. Below is a list of areas we are aware of and will be looking into.

- **API Authentication Bypass:**
 - Discover and investigate the local API.
 - From these discoveries, recommendations for securing these functions will be created.
- **Privilege Escalation:**
 - Perform testing and analysis to better understand the usage and delivery method of the packages that get run by the agent.
 - Further investigate the differences between the system agent and the user agent. Questions to answer include:
 - Which ones handle specific networking functions? Is there segmentation implemented?
 - If so, how and why?
 - Which one runs with elevated permissions, and what does it interface with?
- **Logging:**
 - Research and examine the implementation of a more robust system of logging and investigate the creation of a patch to apply these changes. Currently, the system of logging is decently secure, but gaps remain, and more security is feasible and within scope.
 - Currently documenting logging improvements to be discussed at the next client interaction.
- **Man in the Middle:**
 - Modify the testing environment to allow collection of network traffic.
- **Hijacking**
 - Continue to check if there is any possibility of gaining admin rights on the user system in order to redirect DNS traffic.
- **Malicious Binary Delivery**
 - Determine whether the installer code can be injected into, or if a different mode of injection is used to gain access to a modified installer.
- **SQL Injection**
 - Determine if any applications developed using .NET as well as open historian are susceptible to SQL injection.

API Development Progress

The API that we are currently working on is the development of the openHistorian which uses the OPTO22 software that contains the data from the OPTO22 hardware to communicate to a database and is read into the openHistorian. The purpose of the openHistorian is to organize the data from the OPTO22 hardware into a format that is easily readable by users. The openHistorian offers an open-source visual analytics and interactive web application which allows users to view charts, graphs, and various alerts called Grafana. We plan to gain a better understanding of Grafana as it would be helpful in allowing the information from the openHistorian to be more easily accessible and visually appealing for the users.

Security Recommendations

At this time the team is working on gathering CVE's and other potential risks. The goal at this time is awareness so that when it comes time to harden the systems the team will have sufficient knowledge to formulate a systematic approach. The recommendations at this time is to keep up with an developer updates and keep building our environment with security in mind. We also recommend moving forward in planning ways to test our system that we have in an effort to build upon them with security in mind.

Acronym Definitions

OWASP – Open Web Application Security Project

CVALNG- Central Virginia Liquefied Natural Gas

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

MITM – Man in the Middle Attack

DOS/DDOS – Denial of Service / Distributed Denial of Service

MSCR – Manual Source Code Review

ASCR – Automated Source Code Review

PT – Penetration Test, Pentest

TC – Test Case

SR – Security Requirement

LNG – Liquid Natural Gas

MMP – Memory Map Protocol

DTM – Diamond Threat Model

References

NIST. (n.d.). *NIST CVE details* . NVD. Retrieved October 16, 2021, from <https://nvd.nist.gov/vuln/detail/CVE-2021-26701>.

Security vulnerabilities. CVE security vulnerability database. (n.d.). Retrieved October 13, 2021, from <https://www.cvedetails.com/vulnerability-list>.

Appendices
