CSS300-2203A-02

Vulnerability Assessment and Management

Vulnerability Assessment Project Document Shell

Student Name: Joshua Powell

27 May 2022

Table of Contents

Intrusion Tools and Techniques

INTRUSION DETECTION

In today's world of connectivity there are many possibilities when it comes to malicious activity and what they/or it can do to a company's/business's network. There are two types of systems that are used to detect and prevent network systems from being exploited and used maliciously. They are an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS). They work systematically within a network to help prevent in and outgoing unwanted and warranted activity. The IDS and the IPS work together to help protect a business and its many assets.

One of the ways to keep an unwanted intrusion from happening is through what is called an IDS. In an IDS the main goal is to scan the network traffic for dangerous activity and anything that violates policy guidelines. Then reports it to the system administrator or stores in what is called a System Information and Event Management System (SIEM). It is in an IDS that a business can detect harmful vulnerabilities within a network to prevent them from being exploited. There are five distinct types of IDSs depending on the network and the setup being used. One is the Network Intrusion Detection System (NIDS). In a NIDS kind of setup, it would be installed on the subnet where the Firewall is located to make sure the Firewall is not being broken through. The second is a Host Intrusion Detection System (HIDS). With a HIDS type of setup, it is like it sounds. It protects the individual host or device on the network. The third type of detection system is a Protocol-based Intrusion Detection System (PIDS). Here we have a

system that would preside at the front end of a server and its goal is to secure the web server by monitoring the HTTPS stream and accepting it. The fourth type of IDS is an Application Protocol-based Detection System (APIDS). The main purpose of this type of detection system is to monitor the network traffic flow within a group of servers. The Fifth type is called a Hybrid Intrusion Detection System. This system is made up of a combination of two or more types of detection systems and is used to provide an overall health report of the network. There are also two types of IDS detection methods called Signature-based Method used to detect known malicious activity, and an Anomaly-based Method, which uses machine learning to compare to a model to detect suspicious activity.

With an IDS comes an Intrusion Prevention System. In an IPS the major function like the IDS is to detect malicious/unwanted activity, report it and unlike IDS try to prevent it. The IPS are categorized into four types. One type is a Network-based Intrusion Prevention System (NIPS), which monitors the whole network for unwanted activity and protocol violations. The second is Wireless Intrusion Prevention System (WIPS), which means it works on the wireless network. The third type of prevention system is what is called a Network Behavior Analysis (NBA). This type monitors the network for specific traffic flows to notice such things as a Denial of Service (DOS) attack. Fourth is a Host-based Intrusion Prevention System (HIPS), of course, used to monitor and prevent the individual host or device from being part of an attack or violations (1).

We have seen the types and for what each system is used. They are like ways of detection to better understand what is going on in the network and different in the way they are used to prevent attacks.

AUDITING

Data Auditing is a crucial part of ensuring that a business is making sound decisions based on the integrity of the data. We can contest all day between what one employee witnessed versus another, but with the right/correct and complete data, a business can decide based on facts rather than misguided information based on contested world views. Auditing data is a way from which a business can cut out the ifs and buts of information, to make sure that the data in front of the Board of Executives can base their future endeavors on real/concrete data. Therefore, collecting data and keeping it secure is vital to an effective business model.

Audit Data is stored in two ways. One is called a Database audit trail through what is known as a data dictionary table. A data dictionary table metadata is used to help better understand the aspects of the data to make better concrete decisions based on the rules and characteristics of the data (2). The second form of audit data storage is in the operating system files called an "Operating system audit trail." This form of audit trail helps to ensure data integrity on an operating system. This will help to allow for a more in-depth view of an operating system's coherence.

AUDIT DATA REVIEW

For the business world Audit Data is crucial in maintaining a Business of today. Reviewing the data that is part of making these sound decisions is also a vital part of ensuring that you are doing the necessary actions needed to ensure trust. Like one would trust their doctor, we are in the day in age that we need to trust what is in front of us in the data world as well. With things such as Artificial integrity and Autonomous Cars, one

cannot walk out the door without trusting the computer in their hands. So, making sure your Audit Data is secure as well is indispensable when it comes to trust.

A business needs to consider that their Business relies on sound data to make the most of their business. One way of securing your audit data is making sure you have a policy in place that states who will have access to this data, along with when it should be reviewed. In either aspect, the client's/business involvement is crucial at each stage of the audit process. A policy for Audit Review is necessary for ensuring that the data being managed is still secure and sound or if a violation occurs. This way you can make sure the data audit conducted is sound and just with what was done.

Common Vulnerabilities and Exposures

DEFINITION OF CVE

CVE plays a vital role in the security realm. CVE's first showing was in 1999 and is supported by the nonprofit organization MITRE. They have maintained CVE as a publicly open-source registry for known security flaws and is an international standard. It is a type of registry that Security researchers can use to produce efficient and well-placed designs and features to counteract known problems. Security research relies on such data to better prepare businesses and to produce reports so a business can make sound decisions when it comes to its security. This type of program does not do assessments of any kind to neutralize known issues. Its main use is to be aware of what is going on with a system, its version, what happens, and the form of attack being done (3). The only thing is that with this they are only publicly disclosed security flaws in a CVE Registry, this

means that with each system one needs to make sure they also do their research on any system before implementing. This way, you can make sure your system runs now and well into the future.

CALCULATION OF CVSS

A Common Vulnerability Scoring System (CVSS) was first introduced in 2005 by NIAC, but the international forum for Incident Response and Security Teams (FIRST) no owns and manages it. It remains a publicly available tool and is used to grade the severity of security vulnerabilities in Software, Hardware, and Firmware (4). In combination with a CVE registry, one can put their data to use with a CVSS to make the necessary adjustments and calls to protect their business. A CVSS is comprised of three metric groups and is rated from zero to ten, with ten being the worst. The first group is called the Base Metric Group. It is here that the common attributes that are shared over time and across users are evaluated. The Second is the Temporal Metric Group. It is here that the vulnerabilities that change over time are checked and added to the rating from the Base Metric Group. The third group to be rated is the Environmental Metric Group. It is here that the vulnerabilities specific to the user's environment are assessed and added to the now the overall score (5). This score is then used in combination with CVE in some cases so a customer going for a system can either correct the issue with their current system or find a better way around the issue. A CVSS is a universal language and is used by businesses to assess the risk, as well as, how to mitigate that risk. So, the business can continue to operate without the worry of the next attack or crash due to a system vulnerability (5).

THE USE OF THE NVD

NVD is the National Vulnerability Database and is a government repository of standards-based on vulnerability management data represented using the Security Content Automation Protocol (SCAP). The NVD includes security checklists, security flaws, product names, and impact matrices (6). In the NVD you can bring up CVE docs with the CVSS rating on them to get real-time threats and vulnerabilities that could exist in the organization. I will give a brief overview of three said vulnerabilities that could put your organization at risk. One such vulnerability is CVE-2021-40161. This is a Memory Corruption vulnerability that may lead to code execution through maliciously crafted DLL files through PDFTron earlier than the 9.0.7 version which is used in conjunction with CAD and some Microsoft Office capabilities (7). Another vulnerability with a high rating to keep in mind is one that was found in the ZOOM client for meetings. The case number for this vulnerability is CVE-2022-22782. The CVSS was high on this and intel a vulnerability that made the user vulnerable to an escalation issue during the installation process that a malicious actor could apply to potentially delete system files. A third vulnerability is with cisco routers RV340 and RV345 case #: CVE-2022-20799. The vulnerability is due to insufficient validation of supplied user input that a malicious outside user can use to inject and send superficial commands (8).

Attack Methods

A DISCUSSION ABOUT VARIOUS ATTACK MECHANISMS AND VECTORS, INCLUDING:

Authenticated and Unauthenticated:

- ***Authenticated Attacks***: this is a type of attack that is geared toward the access portion of a website. What that means is let's say you have a password such as 1234 which you should not, but for clarification let's say you do. An attacker then knowing your username can run a brute-force attack with known passwords, "1234" being one of them. Then within minutes said attacker now how must access your website/application without your knowledge and is authenticated. This is one of the main reasons the two- and three-part verification when logging in is so detrimental to our security today. Another example of an authentication attack would be what is known as an "Insufficient Authentication". This type of attack is done through a flaw in the software where with a little know-how and a phrase someone gains access to admin privileges on a server that should not have admin privileges. This is a serious problem as it is a flaw in the security of the software and makes for a real pain if an attacker were to exploit this vulnerability (9).
- ***Unauthenticated Attack:*** In this type of attack, the attacker gains access to the system unknowingly disguised as a user and outwits the security of a network system by exploiting a vulnerability or flaw in that system that does not contain any form of authentication. There are times when such exploits are possible. With

a programmer/programmer writing lines and lines of code, along with them having their checks and balances bugs slip through the cracks as we see from time to time. We need to make sure that if such a bug exists and we find it, we make sure we report it accordingly. A titled example of such an attack is a Spam Attack. This type of attack is where someone gains access to your GameStop account, purchased some stuff, and then floods your email with emails to keep you from noticing the GameStop purchase. Another example of an unauthenticated attack is Phishing. This type of attack I know we have all seen if not at least heard of someone seeing such attacks. In an attack such as this, the attacker has made up a version of the business's email makeup and sent it to you to make it look like your bank so to say. Then they tell you that your account is in restricted status, and you need to click on the link to log on and verify your payments. When, you click on the link that the attacker created and it will prompt you to type in your credentials once you hit submit you may get an error message, but you have given them your login username and password to your bank. It is very serious and is not to be taken lightly (9).

Active and Passive:

- ***Active attack***: This is where the attacker attempts to alter system resources, to make changes to the data en route to the earmark or directly on the earmark.
  - **Example 1**: What is known as a Replay Attack: the objective here is for the attacker to save a copy of the data and later use it to replay hash to gain access to the network (10). A real-world example error code for this is KRB_AP_ERR_REPEAT which is a windows-based error code for such an attack

where the attacker attacks the network directly (11). This can also be an error code for a repeated message or faulty router so one can see the possible vulnerability here

- **Example 2**: Denial of Service Attack: this type of attack can be detrimental to a company and keep customers from being able to do anything with the company's website (10). A vulnerability within windows such as MAX_PATH if written within in an application code it can create a denial-of-service routine inherently prohibiting disk space usage. This can be a big problem when other applications are trying to run (12).
- **Example 3**: Modification of messages: In this type of attack the assailant's main goal is to gain access to the data but use it to spoof the data and flood the network with fake data.

❖ ***Passive Attack:*** This is where the alleged attacker is trying to listen in to the messages/conversation but does not alter it, they are just listening in.

- **Example 1:** Release of Message Content: this type of attack is keen on damaging a company/business integrity by leaking sensitive information to the public. This means that any project that might have been in the works could cause stakeholder problems if such information leaked out that should not have in the first place (10).
- **Example 2:** Traffic Analysis: this type of attack is mainly used to see what is going on and who or what is sending the information. This does not necessarily mean they can see what is being said or done, but they can tell who is sending the message (10).

- Discussion: With these attacks, it is to be noted that they tie into each other. Authenticated attacks are those where the assailant gains access to a data asset and manipulates it in some form such as an active attack in a modification of a message where the attacker actively gains authenticated access to a message to in turn alter it. An unauthenticated attack is much like a passive attack where the attacker gains access to sensitive information through traffic analysis and then releases that sensitive information to the public (10)

Intrusion Detection System Policies

POLICIES

Policy Definition

In a policy, you can address the aspects of what is to be done in situations or how to react to a threat. There are many reasons to have a policy in place. From describing how someone should professionally act in a workplace. To what should not be brought to work. Another aspect would be who you should talk to about certain issues in the workplace that involve a manager or someone you work with directly. This could be something such as a Sexual Harassment/Assault Response and Prevention (S.H.A.R.P.) representative. This person is someone who you can go to, so you can report inappropriate sexual problems within the army work environment (13). In terms of this class, another thing to think about is the difference between secret and top secret. If a file is supposed to be top secret but is labeled secret can result in some serious violations and

unauthorized access to pertinent information that someone should not have access to.

This is a breach using unauthorized disclosure and is not to be taken lightly (14).

Sample policy

Intrusion Tools and Techniques

Purpose

The purpose of the Freightliner Intrusion Tools and Techniques is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

Audience

The Freightliner Intrusion Tools and Techniques apply to individuals who are responsible for **Information Resource** management.

Contents

Policy

Endpoint Protection (Anti-Virus & Malware)

- All Freightliner owned and/or managed **Information/Transport Resources** must use the Freightliner IT management approved software and protection when connecting to the vehicles.
- All non-Freightliner-owned workstations and laptops must use Freightliner IT management-approved OEM Software before any connection to a Freightliner **Information/Transport Resource**.
- The OEM software must not be altered, bypassed, or disabled.
- Each email gateway must utilize Freightliner Helion management-approved email virus protection software and must adhere to the Freightliner rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails and Vehicles.
- Policies in form of enforcement to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must not be used unless approved before use.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to Freightliner Helion Support.

Logging & Alerting

- Documented baseline configurations for **Information Resources** must include log settings to record actions that may affect or are relevant to, information security.
- Event logs must be produced based on the Freightliner Logging Standard and sent to a central log management solution.
- A review of log files must be conducted periodically.
- All exceptions and anomalies identified during the log file reviews must be documented and reviewed.
- Freightliner will use file integrity monitoring or change-detection software on logs and critical files to alert personnel to unauthorized modification.
- Log files must be protected from tampering or unauthorized access.
- All servers and network equipment must retrieve time information from a single reference time source regularly so that timestamps in logs are consistent.
- All log files must be maintained for at least one year.

Patch Management

- The Freightliner IT team maintains overall responsibility for patch management implementation, operations, and procedures.
- All **Information Resources** must be scanned regularly to identify missing updates.
- All missing software updates must be evaluated according to the risk they pose to Freightliner.
- Missing software updates that pose an unacceptable risk to Freightliner **Information Resources** must be implemented within a time that is commensurate with the risk as determined by the Freightliner Vulnerability Management Standard.
- Software updates and configuration changes applied to **Information Resources** must be tested before widespread implementation and must be implemented by the Freightliner Change Control Policy.
- Verification of successful software update deployment will be conducted within a reasonable time as defined in the Freightliner Vulnerability Management Standard.

Penetration Testing

- **Penetration testing** of the internal network, external network, and hosted applications must be conducted at least annually or after any significant changes to the environment.
- Any exploitable vulnerabilities found during a **penetration test** will be corrected and re-tested to verify the vulnerability was corrected.

Vulnerability Scanning

- **Vulnerability scans** of the internal and external network must be conducted at least quarterly or after any significant change to the network.
- Failed **vulnerability scan** results rated as Critical, or High will be remediated and re-scanned until all Critical and High risks are resolved.
- Any evidence of a compromised or exploited **Information Resource** found during **vulnerability scanning** must be reported to the Freightliner Information Security Officer and Helion IT support.
- Upon identification of new vulnerability issues, configuration standards will be updated accordingly.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 12, 18
- NIST CSF: PR.IP, PR.PT, DE.AE, DE.CM, RS.MI
- Incident Management Policy
- Change Control Policy
- Logging Standard
- Vulnerability Management Standard

Waivers

Waivers from certain policy provisions may be sought following the Freightliner Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of the contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	June 2022		FRSecure	Document Origination

End of sample Reference (16)

Protective Measures

VULNERABILITY ASSESSMENT

In the grand scheme of things these days there are a lot of things one can do to check the vulnerabilities of a lot of systems. When it comes to such things as the j1939 network in vehicles, not a lot of people know that there can be exploitable issues when it comes to heavy vehicles such as class 8's. With them becoming part of the IoT you cannot be too careful when protecting not only data assets but physical ones as well.

Some go through life with a false sense of security and find themselves wondering why they ended up in the circumstances in which they are currently. I for one wish I could instill in others the severity of the issue we face today. For instance, let's say that one was to gain access to a company's fleet and take down their ability to get product places, it can inadvertently place the company in a crisis. This can lead to a lot of underlying problems than just this company. The reason being is that the logistics around America are geared towards our network of strong individual groups of people to make sure things such as this never happen.

So let us say for instance that a company supplies vaccines to a health facility. This company is located somewhere on the east coast and the health facility that needs them is over a thousand miles away in the Midwest. A trucker is driving down the road and finds themselves shut off on the side of the road with no way to move and is waiting

on a tow truck. Then not long after that truck shut down another truck shut down from the same company trying to deliver these vaccines. It was not long after these trucks shut down that the whole fleet of 15 trucks was rendered useless until diagnosis was able to be done.

The tech team was sure that it was due to mechanical malfunction for causes such as oil not being changed properly or battery failure. It was not until they started digging into this problem that they could not find a problem that was due to any mechanical failure they thought it might have been at the time. The only failure code they got was j1939 communication failure that they were able to read through the diagnostic software. It was with that they brought the truck to the electronics guy in the shop, who I latent terms did things under the resources available to him, which was not OEM. They realized that the problem could not be solved in the mechanic shop on the premises. The company then proceeded to get the dealership involved from where they got their trucks from.

The dealership got the trucks in and immediately started digging into the problem. They went through the troubleshooting procedures for the code that was showing through the diagnostic software and found that everything they checked, would check out ok. So, the dealership went through it again at least twice to make sure they were not wrong. It was then they filed a complaint with the OEM, now keep in mind the trucks have been down, for now, 12 days overall. Consumers have been without vaccines for almost half a month. This is not only bad for business, but for the consumers as well. So, the dealership gets feedback from the OEM who then proceeds to make sure they covered all the initial basis on the troubleshooting procedures. This then throws up a red flag to not only the dealership but to the OEM.

The OEM sends down their engineers to check out the situation and do their own analysis. They do their analysis, and they are stumped as to why these trucks will not start. So, the OEM called their head systems engineer, and they came down to check the issue out. The engineer checked everything from the 9-pin connector to each ecu. It was then the engineer found some very interesting things embedded in the firmware on one of the electronic control units (ECU). This one ECU was used to control not only the engine but also the chassis. The issue was dug into further by the engineer who found that the embedded firmware was adjusted in such a way that communication between the ECU and power would be cut off after 100 hours of operation. This was not done by any update the OEM had put out. After about another 10 days the OEM was finally able to change the ECU out and updated the firewall on the 9-pin connector (16). They updated it by putting in a gateway of sorts between the connector and the ecus on the truck. The reason being was as it was later concluded that the ECU's firmware had been infected by an outside source, such as a diagnostic compatible device that was already infected with it.

Therefore, your companies must think about more than just their data assets and start thinking about all their assets. You never know where you are vulnerable until it's too late unless you take the right precautionary measures to make sure that such things do not happen. We must develop teams and trust with companies that can assess such vulnerabilities to make sure we can stay strong and effective as a nation.

References

References

1. GeeksforGeeks. (2022a, January 17). *Intrusion Detection System (IDS)*. Retrieved May 25, 2022, from https://www.geeksforgeeks.org/intrusion-detection-system-ids/?ref=gcse
2. *What Is a Data Dictionary? | UC Merced Library*. (2022). UCmerced.Retrieved May 25, 2022, from https://library.ucmerced.edu/data-dictionaries
3. *What is Common Vulnerabilities & Exposures (CVE)*. (2020, February 18). [Video]. YouTube. https://www.youtube.com/watch?v=qfpnJyTl1To
4. Bacon, M. (2020, December 15). *CVSS (Common Vulnerability Scoring System)*. SearchSecurity. Retrieved 2022, from https://www.techtarget.com/searchsecurity/definition/CVSS-Common-Vulnerability-Scoring-System
5. F5. (2020, March 3). *What is Common Vulnerability Scoring System (CVSS)* [Video]. YouTube. https://www.youtube.com/watch?v=rR63F_lfKf0
6. *NVD - Home*. (2022). NIST. Retrieved 2022, from https://nvd.nist.gov/
7. *NVD - CVE-2021-40161*. (2022). NIST. Retrieved 2022, from https://nvd.nist.gov/vuln/detail/CVE-2021-40161
8. *NVD - CVE-2022-20799*. (2022, May 4). NIST. Retrieved 2022, from https://nvd.nist.gov/vuln/detail/CVE-2022-20799

9. Whitehat Security. (2022). *Insufficient Authentication*. WhiteHat Security Glossary. https://www.whitehatsec.com/glossary/content/insufficient-authentication#:%7E:text=Insufficient%20authentication%20occurs%20when%20an%20application%20permits%20an,the%20%2Fadmin%20directory%20without%20having%20to%20log%20in.
10. GeeksforGeeks. (2021, December 24). *Active and Passive attacks in Information Security*. Retrieved 2022, from https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/
11. D. (2021a, October 29). *4649(S) A replay attack was detected. (Windows 10) - Windows security*. Microsoft Docs. Retrieved 2022, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4649
12. L. (2021c, December 15). *Denial of Service - Windows drivers*. Microsoft Docs. Retrieved 2022, from https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/denial-of-service
13. MWR. (2022). *SHARP*. Army MWR. Retrieved 2022, from https://www.armymwr.com/programs-and-services/resources/sharp#:%7E:text=The%20Army's%20Sexual%20Harassment%2FAssault,no%20place%20in%20the%20Army.
14. *Overview of the Privacy Act: 2020 Edition*. (2021, February 16). DOD. Retrieved 2022, from https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties

15. F. (2021, August 11). *Vulnerability Management Policy Template*. FRSecure. Retrieved 2022, from https://frsecure.com/vulnerability-management-policy-template/
16. CSS Electronics. (2021, November 1). *J1939 Explained - A Simple Intro [2021]*. Retrieved 2022, from https://www.csselectronics.com/pages/j1939-explained-simple-intro-tutorial