VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

AUDIT REPORT

CSE3502 - Information Security

Management Digital Assignment 2

Prepared by:

Alokam Nikhitha

19BCE2555

TABLE OF CONTENTS

1.1 Purpose and Scope

The purpose and scope of this document is to investigate and document a security assessment of a multi-national commodities and service supplier that is involved in numerous aspects of the energy sector. The document's goal is to discover any security flaws or loopholes that may exist in such a commodity's security, and then present advice and solutions to help them protect and fine-tune their security channels.

1.2 Objective

- To research our commodity's network design, topology, and configurations.
- Examine the company's security aspects at the design and implementation levels.
- Examining the security procedures of databases, application servers, and other application supporting components, modules, or third-party components integrated into the programme.
- Keeping track of all system flaws that could pose a hazard or be a single point of data leak.
- Ensuring the security of all design management and storage servers.
- Examining the security measures in place to avoid injection attacks.
- Providing a set of recommendations and solutions to improve system, network, and information security.
- To Verify if the authentications and authorization controls are implemented properly in the application.

1.3 Constraints

- Getting satellite monitoring system's administrative privileges.
- Technology tools constraints.
- Network security constraints
- Multi-variate OS information
- Third party access constraints
- Data breaches (Data security for electronic and physical data)
- Application penetration testing
- Scope of Audit Engagement.

1.4 Components and Definitions

The terms system, malware, network, security, testing, information security, vulnerability, and penetration are used frequently in this document. The following definitions are supplied for a better understanding of this document:

Malware – Malware is a type of intrusive software that aims to harm and destroy computers and computer systems. The term "malware" is an abbreviation for "malicious software." Viruses, worms, Trojan horses, spyware, adware, and ransomware are all examples of prevalent malware. It is any software that is intentionally designed to cause a computer, server, client, or computer network to malfunction, leak private information, gain unauthorised access to information or systems, deny users access to information, or inadvertently compromise the user's computer security and privacy.

Information Security - Information security refers to the methods and methodologies used to secure confidential, private, and sensitive information or data in print, electronic, or any other form against unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

Data breaches- A data breach occurs when sensitive, protected, or confidential information is copied, communicated, viewed, stolen, or utilised by someone who is not allowed to do so. [1] Unintentional information disclosure, data leak, information leakage, and data spill are other words. Individuals who hack for personal gain or malice (black hats), organised crime, political activists, or national governments have all been involved in incidents ranging from poorly designed system security to reckless disposal of used computer equipment or data storage media. Leaked material might range from national security concerns to information on actions that a government or official views humiliating and wishes to keep hidden. A deliberate data breach by someone with access to the information, usually for political reasons, is referred to as a "leak."

Network – A network is made up of two or more computers that are connected to share resources like prints and CDs, exchange files, and allow electronic communication. Cables, telephone lines, radio waves, satellites, and infrared light beams can all be used to connect computers on a network.

System – A system is any of the following:

- Computer System (e.g., minicomputer, mainframe computer)
- Network Security (e.g., Local Area Network)
- Network Domain
- Host (e.g., a computer system)
- Network nodes, routers, switches and firewalls

- Network and/or computer application on each computer system.

Penetration Testing – A network penetration test is the process or act of purposely employing various malicious tactics to evaluate the network's security, or lack thereof, by detecting and recording security vulnerabilities in applications, systems, and topologies.

Security – It is the quality or state of being safe, such as the absence of danger, fear or anxiety, or the threat of being laid off. In computer science, the term "security" refers to the state of information, network resources, or messages. The term "network security" encompasses a variety of technologies, devices, and procedures. It is a set of rules and configurations that use both software and hardware technologies to protect the integrity, confidentiality, and accessibility of computer networks and data in its most basic form.

Testing – The purpose of network testing is to provide stakeholders with information about the quality of the product or service being tested. Network testing can also give the organisation an objective, unbiased picture of the network, allowing them to grasp and comprehend the risks associated with network installation. In general, testing is the process of determining how well something performs. In the case of humans, testing determines the level of knowledge or skill attained.

Vulnerability – Vulnerability is a flaw or weakness in software, hardware, or organisational processes that can lead to a security breach if exploited by a hacker. Physical or non-physical network vulnerabilities exist. Anything relating to data and software is often referred to as non-physical network vulnerabilities. If the IT department fails to upgrade a vulnerable operating system, the entire system becomes vulnerable to threat actors. If a virus or malware

infects the Operating System, it has the ability to infect the entire system. Physical network vulnerabilities include activities such as keeping an on-site server in a rank closet and locking it, or demanding a code to reach a secure point of entry.

1.5 Auditing phases

The audit approach is as follows:

- **Selection Phase -** Using a risk-based approach, audit activities are chosen. During the preparation of the yearly audit plan, internal audit meets with leadership and management to examine risks and potential roadblocks to accomplishing objectives. This plan is approached by the Board of Trustees' Executive and Audit Committee, so basically, here we outline all of the tests and systems that we will be reviewing and finalise them with the commodity's concerned authority. In our situation, it will be a commodity in the energy sector, so we will be defining all of these aspects with the Network Head or Manager. The transactional database, energy production logs, satellite trajectories and record logs, internal network design of the tower, and OS permission details will all be scrutinised.

- **Planning -** Every audit necessitates planning, from defining the scope and goal to establishing audit stages to achieve the goal. Internal audit meets with management at the start of the audit to review the audit's purpose, risk factors, and other logistics. The planning phase includes management, and the specifics are recorded in the planning and scoping memo. As a result, we interact with our commodity's management team and discuss why we need to do this audit in order to acquire a picture of expected outcomes. We also go over all of the risk factors that they should be expecting at the end of this audit report with them.

In our scenario, we'd be concentrating on network strength, defence against outside attacks, internal attack risk, risk of satellite breach, energy outsource specifics, and so on.

- **Field work-** Auditors carry out the actions indicated in the planning process during the field work phase. Interviews, studying laws, regulations, and best practises, confirming sample transactions, analysing data sets, and conducting surveys are all common steps. Through monthly status meetings, clients are constantly updated about the audit process. We list all of the steps we'll take to file the audit report in this section. The following are some examples of test steps:

  - Conducting interviews with employees to learn about their responsibilities in the firm and administrative privileges in order to assess the risk of internal attacks.
  - Examining energy logs to see whether there is any inaccurate information about energy output.
  - Analyzing network topology and firewall configurations in order to have a better understanding of network security.
  - Researching advanced security methods such as routers, firewalls, and placement to determine the best defence against external threats.
  - Satellite path coverage, path access details, administrative access details, and so on, in order to assess the risk of a satellite being compromised.

- **Reporting -** At the completion of the fieldwork, auditors meet with management for an exit meeting to review the audit's findings, particular recommendations, and other observations. Auditors send an audit observation memo to management with these

findings and ask for a response with a corrective action plan. As a result, we'll hand over our audit report to the commodity and ask for their feedback. Following the submission of our report, we will inquire about all network changes and permission evaluations. We'll also provide them certain industry-standard laws and best practices to follow.

- **Follow-up-** To ensure that plans are implemented, all audit recommendations and management corrective action plans are followed up on. Annually, the president and the Executive and Audit Committee are informed of any corrective action plans that do not appear to be progressing.

1.6 Auditing Tasks

1) **Virus Detectors:** Anti-virus software must be installed on each host system to reduce the risk of system harm caused by external software. Malware detection and eradication tools must be integrated at the application level. Firewalls can also be configured to operate as semi-antiviruses, preventing any death-of-ping or malicious packets from entering our system. We should also set up the system in such a way that any anomalies that arise are promptly identified and reported. If the anti-virus detects a serious data breach or network imbalance, the system should automatically isolate its vital resources.

2) **Vulnerability Scanning:** Tools should be set up to detect security flaws and vulnerabilities in systems and software that can be exploited by attackers. It's a lot like figuring out how secure a network is. We can get the majority of a system's

possible vulnerabilities by examining network security. Any outside invader will be able to find the key break-in points to the system here. We'd also look into data leaks that could be utilised for eavesdropping by an outsider or an insider. We'd also look into the data transfer encryption and decryption mechanisms to check if the data transfer is vulnerable to confidentiality risks.

3) **Network Strength:** Procedures must be created to locate active network devices by utilizing network protocol capabilities to signal devices and wait for a response. This is used to assess the security of a network. We'd utilize a variety of ICMP ping and ICMP echo commands to look for ICMP vulnerabilities and perhaps zombie systems. We can also use ping commands to determine the real network configuration and identify any deviations from the company's usual standards. In addition, we will need to adjust the firewalls and understand their filtering algorithms in order to assess the network's strength. We'd need to see if they're working on "allow everything that isn't explicitly forbidden" or "deny everything that isn't explicitly allowed" procedures.

4) **Session Management:** Passwords must be used to validate each user session. Session information, such as the time of log-in, log-out, IP address, and host information, must be saved in log files for future verification. We may not have session logs of users because our commodity is not normally a service provider, but we can use the session logs of their staff to understand any danger from internal attacks. Firewalls and other networking devices must monitor and log these sessions at the network level. These facts can reveal any information that

an employee should not have access to, as well as any database schema that should not be accessed by any particular group of employees.

5) **Log Review-** All components that provide logging must have security auditing enabled. Logs give enough information to conduct thorough audits to determine the efficacy and compliance of current security rules. As previously said, we will be looking at the satellite's path, record logs, and energy logs to see if there are any discrepancies. These details will be utilized to investigate the risk factors associated with various network components in our commodity, such as satellite functionality and data leakages, which will aid in identifying vulnerabilities.

1.7 Auditing Methods

- **Document Review:** All of the organization's security and technological documents are properly examined in order to fully comprehend their document policies and the ethics of our commodity. This will also assist us in determining whether our commodity's system's policy design contains any essential weaknesses.

- **OS permission Details:** Because our commodity runs on a variety of operating systems, we need to know their admin level and all of the files they have access to. Our commodity runs on a variety of operating systems, including Windows NT, Open

VMN, UNIX, and Novel. We already know that UNIX systems are secure and are commonly utilised in high-security systems.

- **Interviews:** We interviewed seated employees to determine the privileges they have access to. In addition, where human intervention was required, the appropriate personnel was interviewed according to the criteria. This was done to have a better knowledge of the functions of a few network components. This is exclusively for the purpose of extracting data and ensuring compliance. The transcripts and statements from the interviews are recorded and saved for future study and reference.

- **Transaction Assessments:** The revenue transactions were examined in order to gain a better understanding of the transaction query languages that our commodity employs. We can learn if the organisation uses ACID database attributes in this section. The terms that make up these attributes are as follows:
    - A – Atomicity: The complete transaction occurs at the same time or not at all.
    - C – Consistency: Before and after the transaction, the database must be consistent.
    - I – Isolation: Multiple transactions occur in a non-interfering manner.
    - D – Durability: A successful transaction can still happen even if the system fails.
- **Security Design review:** All of the organization's security and technological documents are properly examined in order to fully comprehend their document policies and the ethics of our commodity. This will also assist us in determining whether our commodity's system's policy design contains any essential weaknesses.

1.8 AUDIT REPORT

Network Strength

S.NO	Check	Findings
1.	Perform network message transmissions to understand the network topology and connected information.	Amongst the IP address that were active, the network topology of system design seemed to resemble that of BUS network with devices attached why single ethernet cable.
2.	Assess the activity of network devices such as routers, proxies to ensure network security.	The log reports and configuration details for each networking device was appropriate and no unusual activity was detected.
3.	Perform periodic network scans to verify each device found is registered in the network. Ensure configuration details of the same are updated in the technical document.	Some IPs which were connected to the network have not been registered. On further inspection, these were found to be devices used for testing purposes.
4.	Checking firewall configurations and their locations.	It has been verified that along with the basic firewall functionalities, information from the outside world is filtered and kept segregated well.

Vulnerability Scanning

S.NO	Check	Findings
1.	Checking if all devices are connected to network while test is being performed.	A few laptops were missed out and upon connecting them, the network was fully functional. No devices were left while being scanned for vulnerabilities.
2.	Finding Zombie Devices or compromised systems	All the systems seemed to be independently working and none of them were infected for DDoS attack.
3.	Verifying security against ICMP sweep attack using ICMP echo commands and noting their response down.	There were only a few systems which were not configured properly for ICMP attacks. They were configured in such a way that they don't respond to further echo commands unless the source stands verified.
4.	Checking that all data inputs are validated and they are not vulnerable to common XML attacks and XML or SQL injection attacks like query tempering and XML external entity attacks.	All database queries and XML requests are validated with parameterized queries and hence is secure.
5.	Checking authentication systems and compromised	At the time of scanning, no visible vulnerability was

	by malicious user to pose threat to original users.	found which could indicate weak authentication.

Log Review

S. NO	Check	Findings
1.	Verify user identification and the types of events preformed by them in the log entries.	All users who perform activities are verified and authorized. No unusual user activity detected.
2.	Verify the originating of events and success and failure indication in the log entries compilation.	All event origination is true and unsuspicious. No attack has been detected from event origination logs.
3.	Verify that the security logs are aggregated and protected from illegal or unauthorized access and modification.	The logs data is integrated and stored on a centralized server. Log injection can be attempted and might possibly be successful.

Session Management

S.NO	Check	Findings
1.	Verifying session times of each employee with respect to their job profile.	The system was not under any internal attack as users have similar use time as their job profiles expected them to have.
2.	Verifying Session invalidation after session log-out.	When the users navigate away from their browser/device without

		logging out properly, exploitation of the established user session might happen.
3.	Verifying if the session cookies are recorded optimally.	All the session activities were logged in console as expected. Even the warnings and exceptions were recorded optimally.
4.	Verifying that session IDs are unique and long.	Once a user has logged on to a system, they are granted a unique session ID that allows for secure communication between the user and web app for the valid session.
5.	Verify the session ID and timeout after specified period of inactivity.	Some session hijacking to log in to the users account is possible and hence we need to improve upon this vulnerability.

Virus Detector

S.NO	Check	Findings
1.	Checking if the system has employed necessary software recommendations to counter cyber-attacks.	The system had necessary software in-place to combat mediocre cyber-attacks.
2.	Checking that software targets critical system	Their anti-virus software ensures that there are no active threats by checking

	areas to detect and remove active malware.	running processes and important registry and disk sections. It also checks for malicious browsers plug-ns and rootkits.
3.	Checking that application detects virus over POP3, HTTP, SMTP, IMAP and FTP protocols.	A full antivirus uses a scanning engine and virus signature database to protect against virus infected over protocols.
4.	Checking firewall configurations.	Firewalls were all configured properly and were filtering traffic packets precisely.
5.	Checking physical device positions and firewall locations.	The firewall although was configured properly, it could have been better placed to increase the security of our system.

2.Summary
2.1 Conclusion

We have documented the necessary network security aspects of our commodity in this report. We examined their network design, documents, policies, log reports, session management, employee interactions, information security concerns, and device configurations.

Our commodity's network security was well-placed and well-protected, while the system may use a few updates to help prepare for future problems. The system required a few topological changes to guarantee that it is fault resilient and has no single point of failure.

The vulnerability scanning revealed that the system is, on the whole, secure. Again, a few systems could be targeted for compromise, but their configurations can readily be modified to prevent this.

Sessions are being handled prudently, and records are being maintained optimally to facilitate clear and precise revival of them, according to the session management.

The virus detectors were in place and working properly, but they needed to be repositioned. The firewalls were only loosely installed at our system's entry and exit points; they must be configured at a different location to prevent servers from being attacked.

As a result, a thorough audit of data integration was conducted in order to extract hidden information for this report. To uncover all conceivable scenarios that could lead to security vulnerabilities, relevant techniques such as network scanning, log analysis and correlation, virus/malware scanning, port scanning, and session managements were used. The important checks and findings have also been listed based on this audit. Based on the findings of this audit, the business can take the required steps to address existing security weaknesses and improve the overall security and reliability of its infrastructure.

2.2 Recommendations and Solutions

❖ Password Controls

Password Controls Ensure that suitable logical access restrictions are applied correctly to all systems and that the system enforces them to prevent unauthorised access via password guessing. Despite the fact that the network's password policies require complex passwords to be entered, that they must be changed every 90 days, and that the user account is locked out after three failed password attempts, the password length is currently set to six characters and only six previous passwords are kept. Unauthorized users are more likely to obtain access to the network if robust password protections are not implemented.

Recommendation:
Management should improve the present password policies for the Corporate Network and for best practises in all council apps, according to the recommendation. This should impose an eight-character minimum password length requirement and limit the number of previously used passwords to thirteen.

❖ Firewall Configuration:

Firewalls were found to be operational and configured correctly, but their location was incorrect.

Recommendation: We'll need to set up a De-Militarized Zone (DMZ) to safeguard our servers against network threats. This would also safely separate our servers in the event that our system was breached. In a DMZ, we need to set up two firewalls, one at the network's entrance and the other near data-logs or server rooms to block access to them.

❖ Use of Emails – Monitoring

A periodic review will ensure that the council's email system is used in accordance with its stated policy, namely that it is not used for anything other than council business. Although email filters for appropriate email usage are in place, there is no compliance check on acceptable email usage. Monitoring of email usage is only done when a service manager requests it. There is a possibility that the email system will be used for non-council purposes, which could have an impact on service delivery.

Recommendation:

We recommend that the use of the Council's email systems be monitored and compliance checks undertaken on a regular basis to identify any instances of possible inappropriate usage during core working hours. This information should be routinely reported to management for information purposes