Statement and Confirmation of Own Work

***A signed copy of this form must be submitted with every assignment.***

***If the statement is missing your work may not be marked.***

**Student Declaration**

I confirm the following details:

|  |  |
| --- | --- |
| **Candidate Name:** | SHIHAB MIRZA |
| **Candidate ID Number:** | P00190603 |
| **Qualification:** | NCC L5DC |
| **Unit:** | Network Security and Cryptography (NSC) (20 Credit) |
| **Centre:** | ZCAS University |
| I have read and understood both NCC Education’s *Academic Misconduct Policy* and the *Referencing and Bibliographies* document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.  I confirm that this is my own work and that I have not colluded or plagiarised any part of it. | |
| **Candidate Signature:** |  |
| **Date:** | 05/10/2022 |



**OPS020\_Candidate Statement of Own Work**

**Contents**

**3…………………… Task 1**

**5……………………. Task 2**

**8………………………Task 3**

**10………………………Task 4**

**11………………………. Task 5**

**12…………………………. REFERENCES**

**TASK—1-**

1. The five (5) most important electronically held assets for Video Zone.

* User Information:

Obviously, one of the most important pieces of data that the company will hold is; User data. This could be anything the user uses to create an account. From first name, Last name, to emails, passwords and so on. This information is what drives the company income, because without the user’s information, we won’t know who is subscribed and who isn’t and there will be confusion and loss of user interest in the company.

* Employee information and records;

Employee records are also important to the company specifically the HR dept., because we can track how much work employees are putting in by checking their attendance records and give salaries accordingly. And sometimes, for legal reasons too.

* Credentials to sensitive platforms like the Company’s social media accounts, DBMS, AWS and API Keys etc.

This is the most critical information asset to the company, because it uses these pieces of information to run the infrastructure properly. If by any chance, the security to these is compromised, such as and API key is leaked somehow, very unpleasant things can happen like malicious hackers can take advantage of that to steal other pieces of information.

* The films and series themselves.

This data can be considered as the company’s main product. The thing they are selling to consumers. The product, obviously is important to the company, because it drives income, hence should be stored in a safe place like a warehouse. In this case, a data warehouse or data center.

* Critical emails.

Emails are important to the company because they can reveal a lot of information about a certain thing. If they fall into the wrong hands, they can cause chaos.

**b c and d) The Threats and likelihood table for each asset.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset** | **Threat** | **CIA?** | **Likelihood** | **Impact** | **Risk** |
| User Information | User Data Theft | C | Low | Medium | Low |
| Employee Information | Employee Impersonation  Server failure to query info about employee | I  A | Medium  Low | Medium  Low | Medium  Very low |
| Important Credentials | Credential Theft | C | Low | High | Medium |
| The films and series | Pirating of films or series  Streaming is slow and low quality | C  A | Medium  High | Low  Medium | Low  High |
| Emails | Phishing  Spam | C  A | Medium  Medium | High  Medium | High  Medium |

**TASK—2-**

1. **Discussing the threats mentioned, their security implementations and alternative countermeasures.**

User data theft:

Many bad things can happen as a result of this. For example, the hacker can be doing undesired things on the users account, like purchasing unwanted subscriptions, changing email or password etc.

We can implement security features such as hashing and salting the passwords using a strong hashing algorithm, keeping (2FA 2 Factor Authentication) for logging into an account etc. Hashing is simply converting a string of characters into a junk/unreadable fix length string for security reasons. And obviously, having SSL is a must.

The alternative countermeasure to include is to only allow strong password when creating an account.

Employee impersonation and failure of server to identify employees:

Employee impersonation is when a hacker enters the system and sends fictitious emails claiming to be from a high-ranking officer or even just another regular employee, with the intention of persuading employees to perform tasks they shouldn't. To pull this off, the hacker must have somehow gained access to employee information on a website or in employee records etc. Another way the hacker could have got in, is if the server has vulnerabilities like SQL injection or it has race conditions that occur in the DBMS on each query which halt the server for some time causing availability issues which the hacker can leverage to gain unauthorized access to an employee account or perform a DDOS attack.

The security feature to implement to avoid impersonation is to have a hashed and signed email each time it sent to someone in the company and to have access control setup. And to avoid the server exploits, we need to make sure the backed code is setup properly and uses ORMs (Object Relational Mappers) etc.

The alternative countermeasure is to prevent leaking important personal email addresses or employee information and to write the backend and setup the DBMS correctly and securely in the first place.

Credential theft:

This is when important company credentials such as Public, Private and API keys, Social Media account credentials, AWS credentials etc. Fall into the wrong hands. The hacker can then use these to do all sorts of things such as; post unwanted things on the companies’ social media, use the API keys to get other sensitive info. Make use of AWS resources for free etc.

The only way to avoid this from happening is to first, keep strong password and username, and secondly, most importantly avoid any leaking of sensitive keys. Usernames and passwords in emails and public platforms like WhatsApp etc.

Pirating of films and series and other platforms making use of our server to stream for free:

Pirating is an issue, because users who are subscribed, make use of the platform to download and stream series elsewhere for free, or even for money.

To avoid this, we should only allow users to have downloaded series or films not more than 10 at a time. And once a user deletes their account, the films and series should also get deleted from their account.

Another issue is when users use the services that video zone provides to, in turn stream on their own websites, so that other non-subscribed users can watch for free.

This is an issue because it will cause the server to slow down and if we are using AWS then more resources will be consumed than necessary.

To avoid this, we should keep CORS Policy (Cross origin resource sharing) to be set to only the videos zones website. So that any other requests that are not coming from video zones domain are ignored. Firewalls can also be useful.

Email phishing and spamming:

Phishing is a kind of online scam in which criminals pretend to be legitimate organizations through emails, text messages, advertisements, or other means to steal sensitive information, like user credentials.

Also, let us not forget the fact that the company uses an unencrypted smtp server which may be vulnerable to a data breach. It is best to encrypt emails before they are sent.

There are some phishing prevention software’s that can be installed on the client’s machine to help in avoiding phishing. Also, we could sign the email before sending to ensure integrity.

Unwanted and unsolicited junk email is sent in large quantities to a random recipient list. Spam is typically sent for commercial reasons. Botnets, or networks of infected computers, have the ability to send it in huge quantities. This in our case will affect our company’s employees.

To avoid spam emails, never publish or disclose your email address to the public unnecessarily.

1. Vulnerabilities and attacks

I) 3 attacks the public facing blog is vulnerable to.

* The WordPress version including its plugins mentioned may be vulnerable to many attacks. The SUPSYSTIC contact form 1.7.5 plugin mentioned may be vulnerable to stored XSS (Cross site scripting) attacks. Client-side scripts can be injected into web pages viewed by other users through XSS attacks. An attacker could use a cross-site scripting vulnerability to get around access controls like the same-origin policy. [reference](https://www.exploit-db.com/exploits/49544)
* The WordPress plugin SUPSYSTIC digital publications 1.6.9 may be vulnerable to Directory Path Traversal. An attacker can gain access to files on your web server that they shouldn't be able to access using a path traversal vulnerability. [reference](https://www.exploit-db.com/exploits/49542)
* The blog entirely may be vulnerable to a [DDOS](https://www.rapid7.com/fundamentals/denial-of-service-attacks/) attack if no rate limiting is put in place.

ii) strategies to detect and prevent the above vulnerabilities.

* XSS can be detected by doing manual testing, code reviews and using a vulnerability scanner.

It can be prevented by using secure coding practices,

Filtering user inputs and using escape techniques.

* Directory path traversal can be detected by carefully analyzing the parts of backend code where a webpage is returned on a get request.

To prevent this, the website or application should be able to validate user input before processing it, then the application ought to append the validated input to the base directory and canonicalize the path by utilizing a platform filesystem API.

* Network traffic monitoring and analysis is the most effective method for identifying a DDoS attack. Through the use of an intrusion detection system or firewall, network traffic can be monitored. DDOS attacks can be prevented by putting in place a [rate limiting](https://www.cloudflare.com/en-in/learning/bots/what-is-rate-limiting/) mechanism.

**TASK—3-**

1. **VPN**

The term "virtual private network" refers to the possibility of establishing a secure network connection while utilizing public networks. VPNs conceal your online identity and encrypt your internet traffic. Third parties will have a harder time tracking your online activities and stealing data as a result of this.

Some Key feature of a VPN:

* Your IP address is hidden by a VPN.
* Secure connection by encryption
* It disguises you location
* Open access to region locked content
* data transfer is secure.

A VPN could be applied in the scenario given by implementing a secure remote access VPN for the Employees that are connecting to the businesses network remotely. Because there is a risk that the traffic that is being sent “nakedly” via the internet can be spoofed and misused.

The type of VPN recommended is Remote Access VPN, because it will allow mobile workers and telecommuters to take advantage of broadband connectivity. Encrypts connections between mobile or remote users and their corporate networks. The remote user can make a local call to an ISP rather than a long-distance call to the corporate remote access server.

1. **Firewalls and DMZ**

A network's first line of defense is a firewall. The goal of a firewall is to prevent outsiders from accessing your network. A firewall is usually placed at the perimeter of the network, and protects the network from internet threats.

There are hardware and software firewalls. In our case we are going to make use of both,

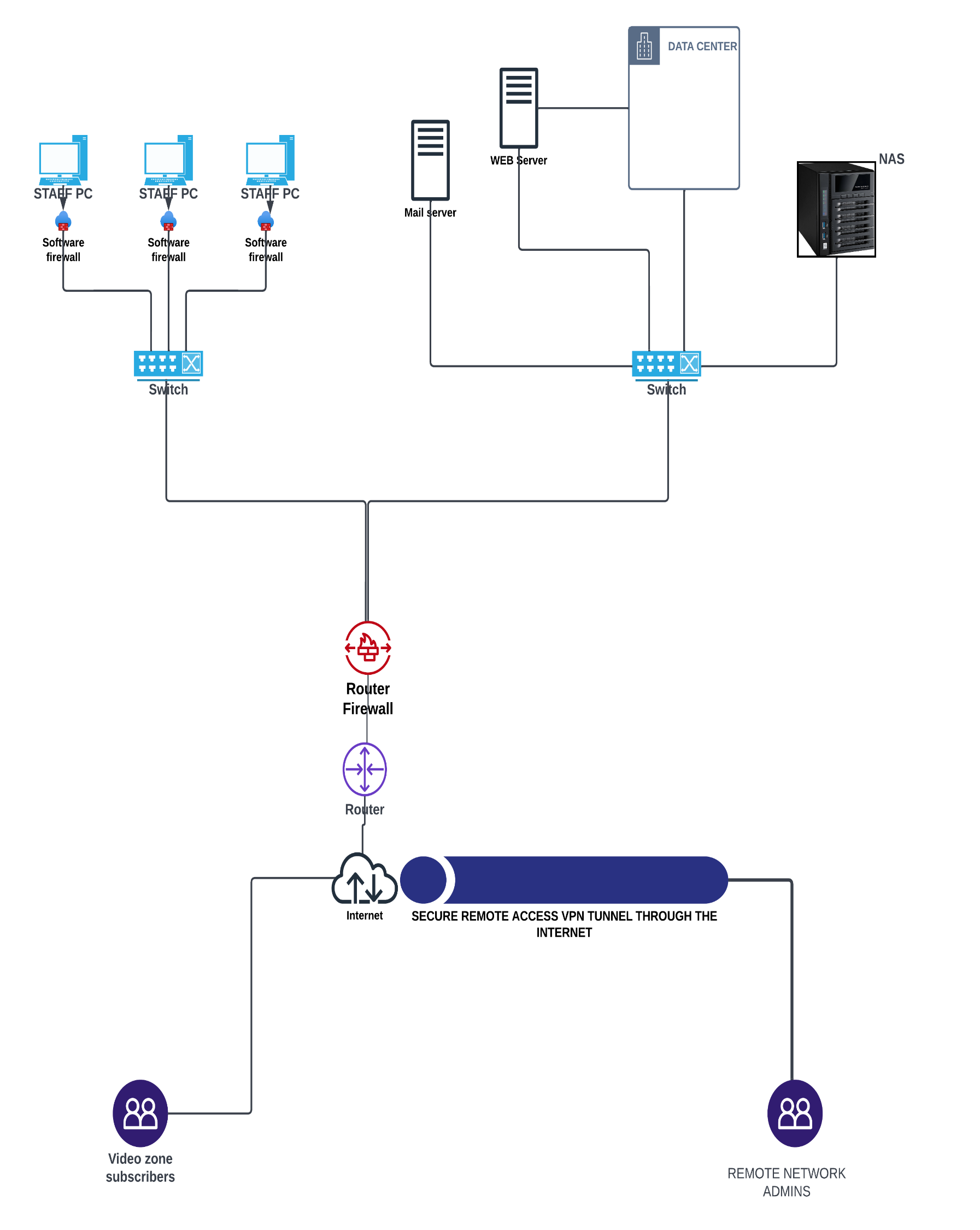
The software firewall will be installed on the staff computers.

The hardware/router firewall will sit right behind the router to analyze and filter incoming traffic.

We can also make use of a DMZ (Demilitarized zone) for more internal network security. A DMZ is separate from the rest of the internal network but still a part of it.

The DMZ in our case will separate the staff computers from all other components in the network (The web server, smtp server, NAS and Datacenter).

**Updated Network Diagram:**

****

1. **Discussion on improving the security on mail server and NAS.**

The internal smtp server transmits non-encrypted traffic which could be vulnerable to attacks. To improve security on this server, we can use SSL and TLS to encrypt POP3 and IMAP authentication. Configuration of the mail relay: By not specifying the domains and IP addresses for which your mail server will relay messages, you can avoid being a spammer's open relay. Port 25 can be blocked and port 587 can be used. Digitally signing the email by using OpenPGP.

To secure the NAS (Network attached storage) device, we can:

Change the default username and password, use 2 factor authentication, enable SSL/TLS, install a firewall, change the default ports, update the software to the latest version, installing antivirus and enabling network access protection.

**TASK—4-**

The main advice given to maintain security, is to be vigilant at al times. Think before you click any link. Check the email first before opening them. Scan any suspicious files that are sent to you via email. Do not respond to unknown and irrelated emails. Do not disclose any sensitive company information to customers. Beware of phishing and pharming attacks. If there are any spam emails. Immediately report to the technical staff.

The finance department should also follow the above advice along with one other type of attack called vishing or (voice phishing) that they should be careful of. This is when a cybercriminal calls an employee using social engineering tactics to sound legitimate in order to chase a payment of an invoice. So, it is always best to double check and verify, before executing such orders.

The social engineering course could help the employees train to identify such scams by making them practically partake in them.

**TASK—5-**

Description and analysis (the what and so what?)

The assignment brought upon a scenario of a company that had many flaws in their corporate network infrastructure by default. I found it easy to identify these loopholes and vulnerabilities because of the way the questions were structured. The smtp server was unencrypted, the remote admins were not making use of a VPN to connect to the network. The public facing blog was built on outdated WordPress software that could potentially have severe vulnerabilities like XSS, SQL injections and directory traversal.

I go to learn about these vulnerabilities through this assignment.

I learnt that vulnerabilities could be in any form, hardware or software. One other thing that the assignment taught me is that access control is very important in a corporate network. The way anyone of the staff could access the NAS, way a bit unsecure. We could only give permissions to some staff who are at a higher tier than others and are trusted, access to that room.

All in all, there were many other security flaws that the scenario brought along with it, its just that the word limit in this assignment never gave me the chance to express them fully.

Future plan (now what?)

I will strive to understand more ways in which the security of a corporate network can be compromised. I will learn more about web-based vulnerabilities that are often overlooked such as: XSS, SQL Injection etc. I will learn how best to write backed code to avoid these types of vulnerabilities. I will also master how to restrict network access and setup access control in a network.

WORD COUNT: APPROX 1900.

**REFERENCES:**

<https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

Accessed on: 07/10/2022

<https://www.indusface.com/blog/what-is-a-website-vulnerability-and-how-can-it-be-exploited/#:~:text=A%20website%20vulnerability%20is%20a,critical%20assets%20of%20the%20organization>.

Accessed on: 07/10/2022

<https://www.fortinet.com/resources/cyberglossary/what-is-dmz>

Accessed on: 08/10/2022

<https://www.webroot.com/us/en/resources/tips-articles/spam-vs-phishing>

Accessed on: 08/10/2022

<https://iosafe.com/data-protection-topics/what-is-a-nas-device/>

Accessed on: 08/10/2022

<https://www.privy.com/blog/what-is-a-hashed-email-and-why-should-marketers-care>

Accessed on: 06/10/2022