

**NETWORK SECURITY AND CRYPTOGRAPHY**

**Module Title NETWORK SECURITY AND CRYPTOGRAPHY**

**EcoMart Digital Marketplace**

**Assignment Title**

**Autumn 2024**

**Examination Cycle**

**THIHANNAING**

**Candidate Name**

**189889**

**Candidate No**

**KMD Computer Centre (Yangon)**

**Centre Name**

**12 June, 2024**

**Submission Date:**

**Important Notes:**

* Please refer to the Assignment Presentation Requirements for advice on how to set out your

assignment. These can be found on the NCC Education *Campus*. Scroll down the left hand

side of the screen until you reach Personal Support. Click on this, and then on Policies and

Advice. You will find the Assignment Presentation Requirements under the Advice section.

* You must familiarize yourself with the NCC Education Academic Dishonesty and Plagiarism

Policy and ensure that you acknowledge all the sources which you use in your work. The

policy is available on *Campus*. Follow the instructions above, but click on Policies rather

than Advice.

* You must complete the **‘Statement and Confirmation of Own Work’**. The form is

available on the Policies section of *Campus*. Scroll down the left-hand side until you reach

Personal Support. Click on this and then click on Policies and Advice.

* Please make a note of the recommended word count. You could lose marks if you write 10%

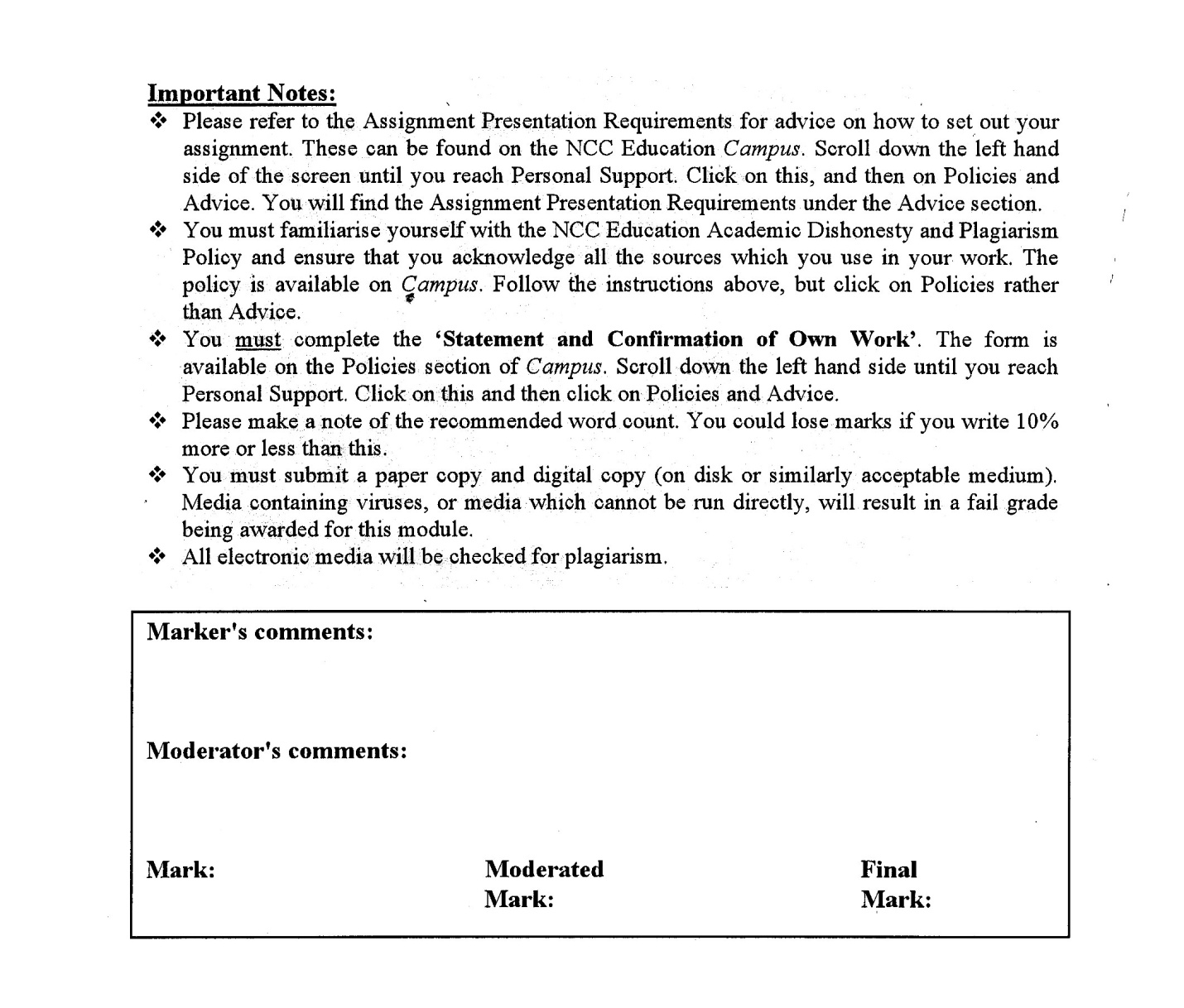
more or less than this.

* You must submit a paper copy and digital copy (on disk or similarly acceptable medium).

Media containing viruses, or media which cannot be run directly, will result in a fail grade

being awarded for this module.

* All electronic media will be checked for plagiarism.





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.

For Level 7 assignments, please use the separate Level 7 Candidate Statement of Own Work form instead of this one.

Student Declaration

I confirm the following details:

|  |  |
| --- | --- |
| **Candidate Name:** | THIHANNAING |
| **Candidate ID Number:** | 189889 |
| **Qualification:** | **Level (5) Diploma in Computing (L5DC)** |
| **Unit:** | **NETWORK SECURITY AND CRYPTOGRAPHY** |
| **Centre:** | **KMD Computer Centre (Yangon)** |
| **Word Count:** | 1981 Words |
| 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 I have not exceeded the stipulated word limit by more than 10%.  I confirm that this is my own work and that I have not colluded or plagiarised any part of it. | |
| **Candidate Signature:** | Thihannaing |
| **Date:** | 12 June, 2024 |

**Table of Contents**

Contents

[**Task 1** 4](#_Toc171614981)

[**Risk Assessment Word Count- (250) Words** 4](#_Toc171614982)

[Risk Assessment 5](#_Toc171614983)

[1.1 Customer data 5](#_Toc171614984)

[1.2 Digital product data 5](#_Toc171614985)

[1.3 E-commerce website data 5](#_Toc171614986)

[1.4 Email data 5](#_Toc171614987)

[1.5 NAS device data 5](#_Toc171614988)

[1.6 Risk Assessment Matrix 5](#_Toc171614989)

[**Task 2** 7](#_Toc171614990)

[**Controlling the risks** 7](#_Toc171614991)

[**a)** **Threats Explanation** 8](#_Toc171614992)

[**b)** **Software and Network Vulnerabilities** 9](#_Toc171614993)

[**Task 3** 11](#_Toc171614994)

[**Securing the network** 11](#_Toc171614995)

[**a)** **Key Features of VPN** 12](#_Toc171614996)

[**b)** **Use of firewall and Demilitarized Zone (DMZ)** 13](#_Toc171614997)

[**c)** **Improving network services** 14](#_Toc171614998)

[**Task 4** 15](#_Toc171614999)

[**Maintaining Security** 15](#_Toc171615000)

[**Maintaining and Monitoring Security Strategies** 16](#_Toc171615001)

[**Task 5** 17](#_Toc171615002)

[**Reflective commentary** 17](#_Toc171615003)

[References 19](#_Toc171615004)

[Candidate Checklist 21](#_Toc171615005)

# **Introduction**

This assignment includes about security necessary factors for EcoMart Digital Marketplace. The main tasks that are included in this assignment are Risk Assessment in Task 1, Controlling the risks in Task 2, Securing the network in Task 3, Maintaining Security in Task 4, and Reflective commentary in Task 5. By following the factors described in this assignment may be able to help EcoMart Digital Marketplace’s security.

# 

# **Task 1**

# **Risk Assessment Word Count- (267) Words**

## Risk Assessment

### 1.1 Customer data

Customer data includes customer profiles, order data, payment histories, email addresses and customers’ personal information. These data needed to be safeguard and maintaining integrity of these data is crucial for customer trust. While developing the system, complying with data privacy regulations is important and will help with data security. (proofprint, n.d.)

### 1.2 Digital product data

This includes all the products sold by EcoMart that are e-books, audiobooks, digital artwork, stock photos, royalty-free images, video clips, and music tracks. Improving security and availability of these data will increase the reputation and company’s revenue. Additionally, improving the security of goods sold and their transaction history is essential too. (Thompson, 2024)

### 1.3 E-commerce website data

Their website is built on PrestaShop CMS which is crucial for their operations. It contains product listings, reviews, and transaction records. Using latest versions of PrestaShop might be essential to improve security and maintainability of the website. Adding new features while ensuring website remains operational, secure, up to date and smoother for user experiences will be needed. (Thompson, 2024)

### 1.4 Email data

Email data includes customer communication records, customer purchasing product records, marketing information. Other business information are also sent via email. Maintaining regulatory compliance related to email data and communications are crucial for customer support, marketing strategies, and company’s image. (proofprint, n.d.)

### 1.5 NAS device data

All e-commerce website’ database including digital product data and order histories, employee payroll information, tax records and payment detail information are backup with NAS devices. These devices ensure data redundancy and business continuity in case of system failures. Protecting and monitoring these devices will be crucial and regular backup plans are also necessary. (Arel, 2022)

### 1.6 Risk Assessment Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset** | **Threat** | **CIA?** | **Likelihood** | **Impact** | **Risk** |
| Customer Data | Social engineering | C | Medium | Low | Low |
| Data Leakage | I | Low | High | High |
| Digital Product Data | Insider threats | C | Low | High | Medium |
| System failures | A | Low | Medium | Low |
| E-commerce website data | DDoS attacks | A | High | Low | Medium |
| XSS attacks | I | Medium | Medium | Medium |
| Email data | Phishing | C | High | Medium | Low |
| Malware attachments | A | Medium | Medium | Medium |
| NAS device data | Unauthorized access | C | Medium | High | High |
| Natural disasters | A | Low | High | Medium |

(Imperva, n.d.)(Cynet, 2024)

# **Task 2**

# **Controlling the risks**

**Word Count- (843) Words**

## **Threats Explanation**

Threats are always existing in any kind of environment including networking security. Threats must to be predicted and prevented and also have counter-measurements and below includes definition, prevention, and counter-measurement for threats that can occur for EcoMart.

**Threats**

Social Engineering: This involves manipulating customers and hack data. This can happen through online communication and in physical.

**Unauthorized Access:** Insider or outsider comes through the server or important rooms to get illegal access. This can be from internet or in physical. (Pryimenko, n.d.)

**Data Leakage:** This can occur due to insecure data storage, misconfigurations or improper data handling. This can happen when the system is attacked or data are leaked by insider. (fortinet, fortinet, n.d.)

**Natural Disasters:** Include fire, water float, earthquakes, tornados (wind disasters), etc.

**Malware Attachment:** Attaching virus files that will destroy data or steal data through files sent by email or shared through external devices. (fortinet, fortinet, n.d.)

**XSS Attacks:** Using malicious scripts into web pages, or inject scripts to database to take user data. (fortinet, fortinet, n.d.)

**DDoS Attacks:** Attacking servers with many devices to stop their services. (fortinet, fortinet, n.d.)

**Insider Threats:** Misusing their access to exploit company’s data, for different purposes. (fortinet, fortinet, n.d.)

**System Failures:** Can occur due to using bad maintenance like using old devices.

**Phishing:** Cloning like an official one and letting user input their information. (fortinet, fortinet, n.d.)

**Preventions**

To prevent Social Engineering, Phishing, and Malware Attachment, educating users, using multi-factors authentications, forcing to use strong passwords, and letting user use email filters and antivirus software can help. (eccouncil, n.d.)

Having non-disclosure agreement with employees, partner companies and third parties, saving data separately, using data centers’ services can prevent Data Leakage and Insider Threats. (Pryimenko, n.d.)

Data encryption, access control, using VPNs, input validations and using secure server protocols can prevent Data Leakage, Unauthorized Access, and XSS attacks. (IPA)

Having backup servers, standbys, cloud servers, regular maintenance, backups and updating devices can prevent System Failures, and DDoS Attacks. (IPA)

Using redundant data center, diverse network routes, backup power supplies and standbys can prevent Natural Disasters. (IPA)

**Counter measurements**

Migration plans, recovery plans, notifying to public can counter measure Natural Disasters, System Failures, and DDoS Attacks. (scale, n.d.)

Having service provider, changing password immediately, use more database design and system, having services or victims may counter measure XSS Attacks, Phishing, Social Engineering. (scale, n.d.)

Using antivirus software, awareness training, data encryption, and improving data integrity can able to counter measure Malware Attachment, and Unauthorized access. (scale, n.d.)

Suing, or firing or publishing if it is needed may able to counter measure Insider Threats. (scale, n.d.)

## **Software and Network Vulnerabilities**

**Vulnerabilities**

Current system has many vulnerabilities such as using old software versions for example, PrestaShop version 1.8.2, using weak network services like FTP, and weak security for physical access.

**Common vulnerabilities and exposures (CVE)**

**Old versions**

current running version of PrestaShop version 1.8.2 is known for security vulnerabilities. For example, SQL injection is common in versions between 1.4.0 and 1.8.2 due to their lack of input sanitization. CVE-2023-28839 highlights issues for this. (CVE, n.d.)

Current running NAS devices' firmware versions QTS 5.0.1 and QuTS hero h5.0.1 for their weak security. Attackers can inject illegal codes remotely. Attackers can gain unauthorized access and disrupt service or data. CVE example of this firmware versions can be seen on CVE-2023-23362, CVE-2022-27596 and CVE-2021-44051. (CVE , n.d.)

**Network services**

FTP transmits data in plain text without having encryption. This can be intercepted by attackers and gain information. Attackers may make Denial of Service attacks, abusing user information, gaining unauthorized access through FTP. CVE example for using FTP services are described in CVE-2024-4425 and CVE-2021-23336. (CVE, n.d.)

Similar to FTP, Telnet also transmits data with plain text which may easy to get data for remote attackers. They can gain unauthorized access though remote attacks. For example, CVE-2024-21785 and CVE-2024-21785 list provide attacks and vulnerabilities of Telnet. (CVE, n.d.)

**Physical vulnerabilities**

Current infrastructure has no access control for NAS devices. All the staff members are accessible increasing the risk of unauthorized access. Leaking important information of the company or customer data leakages can be occur which can be considered as common vulnerability.

**Fixing**

For current software and firmware, doing update to latest versions and continuing regular updates can fix the vulnerabilities.

Using FTPs or SFTP (secure version of FTP) and SSH (secure shell) as replacements for FTP and Telnet will secure for data transfer and remote management. (Glass, 2024)

Implementing role-based access control, monitoring devices and using multi-factor authentication will reduce the vulnerabilities of physical access including NAS devices. (Arel, 2022)

**Email risks**

1. Phishing

Phishing is common method of security risks can happen by sending links. Attackers may trick customers by sending fraudulent emails and let customers enter their information. Sometime attackers attach malicious files to customers. Educating customers, using email authentication protocols, filtering and using anti-virus software can prevent this risk. (Anderson, 2023)

1. Link interceptions

Download links via email can be intercepted and letting attackers get information or unauthorized access to the digital products. To fix this problem, using time limited email or expire download link will be needed. Also adding customer authentication before gaining access of the digital product can fix this problem.

# **Task 3**

# **Securing the network**

**Word Count- (472) Words**

## **Key Features of VPN**

Key features –

1. Encryption: encrypt the transmitted data, ensuring the information remains secure and private.
2. Remote Access: enables secure remote access to employees to work from anywhere while ensuring security and privacy.
3. Authentication: requires authentication, validate that data was sent from authenticated user.
4. Data Integrity: ensures the transmitted data remain unaltered or tampered.
5. Anonymity: masking the user’s IP address while using the IP address given by the server, making user’s location and identity secure and private.

**Application**

EcoMart’s network administrators can use VPN to secure remote access to e-commerce website and NAS devices since services FTP and Telnet are vulnerable. This can reduce risks like unauthorized access, data branches and ensure data integrity.

**Suitable type of VPNs**

**Site-to-site VPN**: connects EcoMart’s multiple offices locations securely ensuring data transferred is encrypted and protected.

**Remote Access VPN**: allows users to connect to EcoMart’s network from different locations allowing to manage NAS devices and use e-commerce website remotely.

(symlex vpn, 2024) (paloaltonetworks, n.d.) (geeksforgeeks, 2023)

## **Use of firewall and Demilitarized Zone (DMZ)**

**Firewall**: it is used to prevent unauthorized access and protect computers from unwanted traffic or going out. They are used for authentication and improve access control. (fortinet, fortinet, n.d.)

**DMZ**: it adds extra layer of security by letting other people able to use the company’s network. The organization’s staff will use another network protected by firewall. (barracuda, n.d.)

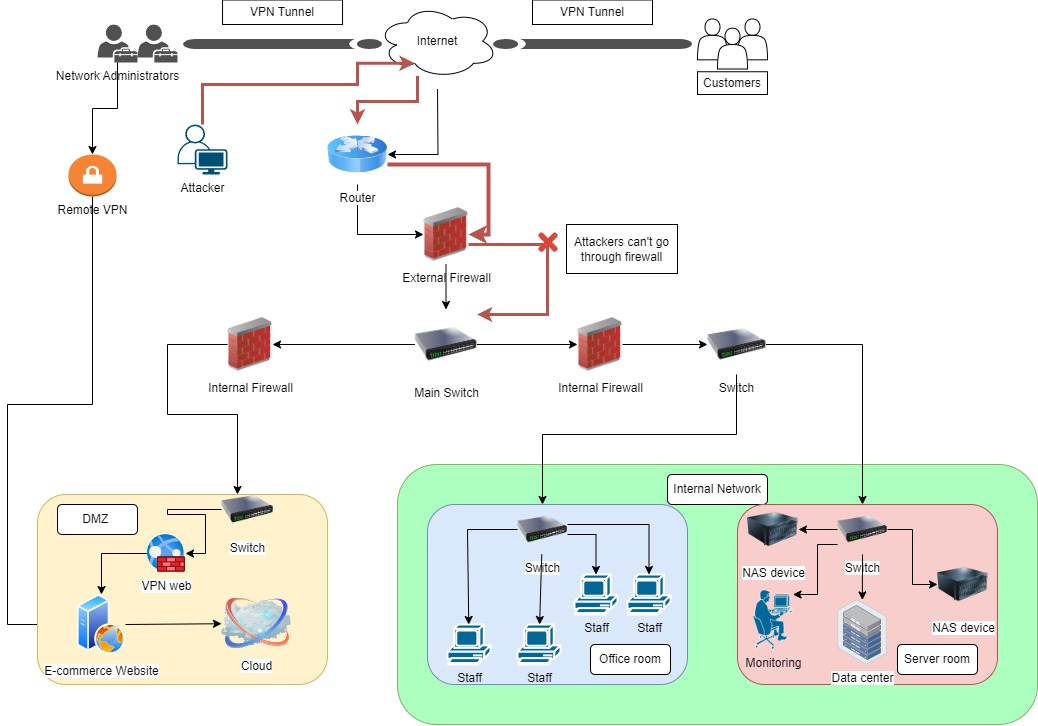


Figure 1 New EcoMart's Network Diagram

**New components**

1. Firewalls –firewalls for better controlling and security
2. Attackers – to show that they cannot attack the system
3. VPN – to use e-commerce website securely
4. Cloud – to backup data
5. DMZ – allows everyone to use website
6. Office room – for staffs
7. Staffs – do inside jobs
8. Monitoring – to monitor the sever room
9. Server room – include important devices

(researchgate, n.d.) (semanticscholar, n.d.) (Google, n.d.)

## **Improving network services**

**Using FTPS (FTP secure)**

While using adds a security layer by using SSL/TLS to provide secure file transfer by encryption. Configure NAS devices to support FTPS. It includes enabling strong certificates and regular updates. (Glass, 2024)

**Implement VPN**

Use company VPN and remote VPNs for data traffic and encryption. Internal VPN for accessing company’s main data and remote VPNs for using e-commerce website data will prevent against unauthorized access. (universityofsandiego, n.d.)

**Access Control**

Using multi-factor authentication will ensure verification and reduce risk of unauthorized access. Physical and internet monitoring internal data will also be needed for safety.

**Enable Firewall**

This is necessary for incoming and outgoing data traffic. These firewalls will protect network from unauthorized access and threats. There will be external and internal firewalls for better defense. (universityofsandiego, n.d.)

**Regular update**

Regular update for NAS devices and other software like e-commerce website, and other associated software are updated which are also necessary for PrestaShop.

(precisely, n.d.)

# **Task 4**

# **Maintaining Security**

**Word Count- (161) Words**

## **Maintaining and Monitoring Security Strategies**

**FTPs:** using strong encryption protocols, auditing on configurations, and regular renewal of SSL/TLS certificates is needed for maintaining. Monitoring logs, having penetrating testing for monitoring. (amazonwebservices, n.d.) (Glass, 2024)

**VPN:** regular updating the software, managing user accounts can be used for maintaining. Tracking bandwidth, and setting access alerts for monitoring. (universityofsandiego, n.d.)

**Access Control:** Training employees, reviewing user access, and having non-disclosure agreements for maintenance. Monitoring access logs, having audits for monitoring of access control. (amazonwebservices, n.d.)

**Firewalls:** Updating firewall and its rules, applying patches and back up configurations can be done for maintaining of firewalls. Monitoring traffic and configuring alerts can be done for monitoring. (universityofsandiego, n.d.)

**Regular Updates:** Implementing patch management policy, test updates, continuously educating employees and training will be needed. For the backup having incident response plan, recovery plan will be needed. (amazonwebservices, n.d.)

Consistently maintaining and monitoring these security strategies can reduce risks, policy violations security incidents, and ensure the CIA of the information and system.

# **Task 5**

# **Reflective commentary**

**Word Count- (171) Words**

**Reflective commentary**

One of the major challenges during this assignment was about understanding CVEs. Researching and understanding of how CVEs work was overwhelming. Learning new networking security words, understanding network security implementations, and creating new network infrastructure was also difficult. Time management was also a little of problem during this assignment.

To solve the CVE problem, I repeatedly use the websites by learning details and information described on the website. And for the new networking words, I used YouTube and other platforms to understand those. For the network implementation and infrastructure, I researched many data and also consult with experienced people and those who are currently working in networking field. For the time management, I had to over worked including sleeping time.

In the future to avoid those problem, will need continuous learning of networking and use those in real life. And will learn also about monitoring and maintenance natures too. Last but not least will need to increase time management skills and have time-plans even before the assignment is given.

**References:**

# References

(n.d.). Retrieved from paloaltonetworks: https://www.paloaltonetworks.com/cyberpedia/types-of-vpn

(n.d.). Retrieved from researchgate: https://www.researchgate.net/figure/A-real-network-infrastructure-used-in-testing\_fig4\_349048832

(n.d.). Retrieved from semanticscholar: https://www.semanticscholar.org/paper/Architecture-for-programmable-network-Barbette/cf1f95596c4ee837c641ffc20777fac51c9052f7

(n.d.). Retrieved from Google: https://www.google.com/search?q=network+infrastructure+reference&sca\_esv=74df811e3a5c80f0&sca\_upv=1&udm=2&biw=1707&bih=825&sxsrf=ADLYWIJ2Nv\_-L7thdufwwduh6VcZPxr6\_A%3A1720698770974&ei=ksePZruYO8eL4-EP\_eKzuA0&ved=0ahUKEwi7qYm49p6HAxXHxTgGHX3xDNcQ4dUDCBA&oq=

(n.d.). Retrieved from precisely: https://www.precisely.com/glossary/ftps#:~:text=FTPS%20(File%20Transfer%20Protocol%20Secure,Secure%20Sockets%20Layer%20(SSL).

(n.d.). Retrieved from amazonwebservices: https://aws.amazon.com/what-is/ssl-certificate/

( 2023, Jan 24). Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/

(2024, May 16). Retrieved from Cynet: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

Anderson, T. (2023, December 5). Retrieved from https://www.bluehost.com/blog/phishing-how-to-protect-yourself-when-working-remotely/?utm\_campaign=dsa\_blog\_PPC&utm\_source=googleads&utm\_medium=genericsearch&utm\_affiliate=bluehost\_PPC&irpid=101&clickid=P61C101S570N0B5578A2D4499E0000V135&channelid=P61C101

Arel, R. (2022, September 19). Retrieved from Tech Target: https://www.techtarget.com/searchstorage/tip/Consider-the-advantages-and-disadvantages-of-NAS

barracuda. (n.d.). *barracuda*. Retrieved from https://www.barracuda.com/support/glossary/dmz-network#:~:text=The%20goal%20of%20a%20DMZ,is%20safe%20behind%20a%20firewall.

*CVE*. (n.d.). Retrieved from CVE: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2023-28839

*CVE*. (n.d.). Retrieved from CVE: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=FTP%20attack

*CVE*. (n.d.). Retrieved from CVE: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Telnet

*CVE* . (n.d.). Retrieved from CVE : https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=QNAP+NAS++devices+running+firmware+versions+QTS+5.0.1+and+QuTS+hero+h5.0.1+

eccouncil. (n.d.). *eccouncil*. Retrieved from https://www.eccouncil.org/cybersecurity-exchange/network-security/how-to-prevent-network-security-attacks/

fortinet. (n.d.). *fortinet*. Retrieved from fortinet: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

fortinet. (n.d.). *fortinet*. Retrieved from https://www.fortinet.com/resources/cyberglossary/what-does-a-firewall-do

Glass, V. (2024, May 18). *jscaape*. Retrieved from https://www.jscape.com/blog/understanding-key-differences-between-ftp-ftps-and-sftp#:~:text=FTP%2C%20FTPS%2C%20and%20SFTP%20differ,data%20exchange%20and%20firewall%20needs.

Imperva. (n.d.). Retrieved from Imperva: https://www.imperva.com/learn/application-security/network-security/

IPA. (n.d.). *Fundamental Information Technology Engineer Examination.*

proofprint. (n.d.). *proofprint*. Retrieved from https://www.proofpoint.com/us/threat-reference/email-security

Pryimenko, L. (n.d.). *ekran*. Retrieved from https://www.ekransystem.com/en/blog/detecting-and-responding-to-unauthorized-access

scale, f. (n.d.). *full scale*. Retrieved from full scale: https://fullscale.io/blog/software-security-threats/

Spasojevic, A. (n.d.). *phoenixNap*. Retrieved from https://phoenixnap.com/blog/network-security-threats

*symlex vpn*. (2024, March 24). Retrieved from linkedin: https://www.linkedin.com/pulse/11-important-features-look-vpn-symlex-vpn-for-all-qygdc

Thompson, K. (2024, March 13). *fortra*. Retrieved from https://www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself

universityofsandiego. (n.d.). *universityofsandiego*. Retrieved from https://onlinedegrees.sandiego.edu/network-security-solutions/

# Candidate Checklist



Please use the following checklist to ensure that your work is ready for submission.

Have you read the NCC Education documents 'What is Academic Misconduct? Guidance for Candidates' and 'Avoiding Plagiarism and Collusion: Guidance for Candidates' and ensured that you have acknowledge all the sources that you have used in your work?



Have you completed the 'Statement and Confirmation of Own Work' form and attached it to your assignment? **You must do this**.



Have you ensured that your work has not gone over or under the recommended word count by more than 10%?



Have you ensured that your work does not contain viruses and can be run directly?