2024

# DNCT703 Network and Cloud Security (DANCT7124C-E/OL)

ASSIGNMENT 1

MURACHI, TAKASHI

ID# 850000605 | DANCT7124C-E

Diploma in Applied Network and Cloud Technology (Level 7)

**Cover Sheet and Student Declaration**

This sheet must be signed by the student and attached to the submitted assessment.

| | | | |
|---|---|---|---|
| **Course Title:** | **DNCT703 Network and Cloud Security** | **Course code:** | **DNCT703** |
| **Student Name:** | **Takashi Murachi** | **Student ID:** | 850000605 |
| **Assessment No & Type:** | **Assessment 1 – report** | **Cohort:** | DANCT7124C-E/OL |
| **Due Date:** | 30/6/2024 | **Date Submitted:** | 30/6/2024 |
| **Tutor's Name:** | **Chirath De Alwis** | | |
| **Assessment Weighting** | 30% | | |
| **Total Marks** | 100 | | |

**Student Declaration:**

I declare that:

I have read the New Zealand School of Education Ltd policies and regulations on assessments and understand what plagiarism is.

I am aware of the penalties for cheating and plagiarism as laid down by the New Zealand School of Education Ltd.

This is an original assessment and is entirely my own work.

Where I have quoted or made use of the ideas of other writers, I have acknowledged the source.

This assessment has been prepared exclusively for this course and has not been or will not be submitted as assessed work in any other course.

It has been explained to me that this assessment may be used by NZSE Ltd, for internal and/or external moderation.

If I am late in handing in this assessment without prior approval (see student regulations in handbook), marks will be deducted, to a maximum of 50%.

**Student signature:**

**Date: 7/5/2024**

| | | |
|---|---|---|
| **Tutor only to complete** | | |
| **Assessment result:** | **Mark /100** | **Grade** |

# Table of Contents

## Requirement 1:

### a)

**Hardware specifications:**
The 48-port 10/100 Mbps switch designed for home or small offices in the Network Equipment and Setup exhibits sluggish performance and may fail to satisfy contemporary network requirements for the increased of online customer(Andriukaitis, 2023). We suggest considering upgrading to a switch with a higher data transfer rate of 10/100/1000 Mbps or faster.

2.Machine-Desktop (10) and Laptop (10):
Machine: Laptop and laptop machines have ended service on 31st of December for Intel® CoreTM i3-2120 processors (end of service:31st of December 2019) and DDR3 RAM (stop production at the end of 2023), with low storage capacity compared to current DDR4 or 5. To optimise work productivity, it is advisable to upgrade to a more advanced processor, such as an Intel Core i5 or i7, and a higher-speed SSD.

**Software specifications:** 1.
Windows Servers: The server(DC, Web and Database) are running on OS Windows Server 2008 R2 with web server: Internet Information Services (IIS)IIS 7.5 in web server was ended of service:14th of January 2020(GitHub-Name, n.d.-a). Database SQL 2005 server in database server was also ended the service on 12th of April 2016(GitHub-Name, n.d.-b). We suggest upgrading to SQL Server 2017 or a newer version to improve data security and streamline operations. Upgrade to Windows Server 2019 or 2022 can mitigate security risks.

2.Machines-both desktop (10), laptop(10) -Windows 10 pro version will be ending on 14th of October 2025 next year due to the lifecycle policy(GitHub-Name, n.d.-c), so after that, no longer support the latest version of operation systems. Both users of front and back end of windows 10 pro in the Auckland head office are affecting to customer self-services on the negative impact after the expiry date. As a justification, both servers and machine related risks are identified total 46,068 entries as of 4th of Jun 2024 from the website "exploit database" as a risk because of expiry of service(*OffSec's Exploit Database Archive*, n.d.).

**Wireless local area network:**
WEP, a deprecated encryption technique, is susceptible to unauthorised access, and contemporary networks should choose WPA2 or WPA3 for robust wireless encryption(Al-Mejibli & Alharbe, 2020). The company allows employees to use their personal devices and connect to its WLAN network. Connecting personal devices to corporate networks increases security vulnerabilities, while merging employee personal information with corporate data may give rise to privacy concerns.

i)

**b)** Due to the staff PC's poor performance despite solid specifications, the log categorized a significant number of tickets as either malware or antivirus issues, which resulted in a high volume of attached customer emails as abnormal behaviour.

**c)** To prevent virus attacks, it's essential to install anti-virus scans like Qualys (*Enterprise Cyber Risk & Security Platform | Qualys*, 2024) and perform regular scans. Regular updates and backups through automated patch management systems are crucial for the smooth operation of antivirus software. Some software automatically updates itself, while others notify users. To protect critical healthcare data from unpredictable events, backups and a comprehensive recovery strategy must be implemented in a cloud computing platform for prompt retrieval(Javaid et al., 2023).

ii)

**b)** Cyberattacks have repeatedly targeted the company's e-commerce site, leading to unauthorised access, email theft, and vendor bank account compromise. These incidents have damaged customer trust in the company's security measures. We attributed the sudden slowdown to a high volume of malicious attack traffic, which prevented the website from accessing WLAN and possibly caused DNS spoofing.

**c)** The combination of firewalls, encryption, an intrusion detection system (IDS), and an intrusion prevention system (IPS) provides a safer and more optimised network environment for users. IDS sends network alerts for suspicious activity, while IPS detects and prevents such activities. VPNs manage network security, ensuring remote access to VLAN network IP addresses within internal departments. Encryption prevents unauthorized access to data packets, ensuring the confidentiality of employee personal information and customer databases(Mohamad Rosman et al., 2023).

iii)

**b)** The attacker used a wireless man-in-the-middle attack to interfere with the company's WLAN network, causing the e-commerce site hosted on the company's web server to experience unstable networking conditions.

**C)** Introducing both WLAN, and VLAN with WPA3 can enhance the wireless service security. After assigning different service set identifier (SSID) names in WLAN networks, VLAN 10 (guest), VLAN 20 (employee), and VLAN 99 (management) can be separated in the network of different SSID group, therefore the system administrator can enhance security in the organisation, so it can be establishing Wi-Fi connection with a long and randomly generated character sequence and upgrading to WPA3. This version allows for continuous monitoring and simplifies the identification of illegal access by various user categories. (121 words)

### iv)

**b)** Over the past year, numerous web-application attacks have targeted the guestbook page of an e-commerce site, causing various issues and inconvenience. These attacks can lead to recurring symptoms such as website attacks, unavailability, content changes, slow loading, malicious content, and slow downloads. These symptoms indicate a compromised server, enabling attackers to alter the website's appearance and download malicious content.

**c)** Install WAF and the encryption approach improves the security of data files, log files, and backups by employing robust encryption and decryption techniques. This approach guarantees transparency for users and executes real-time input, output, or transmission across connections. We recommend using stronger encryption methods, one-way hashing techniques, and transparent database restrictions at the individual cell level to enhance the system's overall protection against data loss (Maurya et al., 2019).
(130 words)

### v)

**b)** Unauthorised individuals gained access to a vendor's bank account details, leading to the theft of client email addresses. This, in turn, resulted in fraudulent transactions and the use of fake postal addresses. Consequently, the organisation has suffered a reduction in client trust and financial losses.

**c)** By validating inputs, the SEA WAF solution enhances web application security by detecting and preventing SQL injection attacks. Secure data transmission, strict access control measures, and encryption are critical to preventing database attacks. Continuous audits and encryption are also essential. The WPA3 protocol targets the IEEE 802.11 Access Point protocol, protecting access points from denial-of-service attacks. Robust cryptography and continuous audits are essential for effective security.
(Ιωάννης, n.d.).

## Requirement 2

### a)

**Current network Strengths**: To improve troubleshooting abilities, 30 Auckland staff members are enhancing their networking infrastructure and administration skills. They plan to pursue further studies and use their current knowledge for future cloud platform implementations. On its e-commerce platform, the organization has 5,000 registered online clients. They have implemented DHCP, DNS, and Active Directory and plan to upgrade the outdated Windows 2008 RS. This will streamline cloud adoption and enable staff to develop a strategic plan for transitioning to the cloud(Kabrilyants et al., 2021).

**Resource Weakness**: The organisation has been operating with outdated infrastructure, which can present challenges and vulnerabilities. This may result in the discovery of obsolete servers or applications that either lack support or have reached the end of their lifecycle. The cost of updating and maintaining this outdated infrastructure can be significant, and it may be more cost-effective to transition directly to a cloud provider's product. Limited network bandwidth can affect the performance and reliability of legacy applications, which is the end of service. Identifying these applications and recommending a migration to the cloud can improve their performance and reliability. A lack of cloud expertise can also pose a challenge, as the technical team may not be technically ready to transition to the cloud. Data governance and compliance requirements can also pose a significant challenge.

**Opportunities:** A load balancer is a versatile technology that monitors network traffic to determine the server's capacity for potential online shopping customers. A load balancer triggers a new server to evenly distribute traffic when the capacity exceeds a certain limit, ensuring resource availability. This technique streamlines procedures, reduces service disruptions, and enhances customer contentment. Load balancers are highly efficient in cloud environments because they can accurately determine the maximum traffic limit for servers without the need for additional equipment. Configuring them doesn't require additional time and costs for materials and labour, nor does it raise concerns about cloud compatibility. In the event of ongoing traffic, the load balancer evenly distributes it, thereby reducing equipment downtime and improving resource allocation efficiency (Nazir et al., 2021).

**Threats**: Vendor lock-in can impede the process of transitioning to alternative service providers, particularly for small private organisations. This is because providers need to make substantial initial investments, unlike public clouds such as AWS, Azure, and Google Cloud. Private clouds may also have restrictions, resulting in inactivity and difficulty transitioning. Furthermore, there may be a pre-established timeframe for resource allocation at a specific time.

### b)

We recommend that the organisation adopt a hybrid cloud. This will enable compliance, security, and performance. By initially investing in a small private cloud provider that offers Platform as a Service (PaaS), the organisation can upgrade to the latest version of all installed devices managed by the cloud vendor. This is because the current software, hardware, and security within the organisation are all out of service, resulting in higher costs associated with purchasing and configuring new physical hardware for each device and installing software on a regular basis. Microsoft Azure will likely have lower prices and a larger customer base. It enables the conversion of a Web server (IIS 7.5) to a Microsoft Azure server, providing adaptability in the cloud service without any compatibility issue. Furthermore, we recommend switching to the Azure SQL Database due to the database server's end-of-service state (SQL 2005). We suggest using this hybrid transition based on the client computers' strong hardware requirements, which are only a year old.

**Security and compliance:** Keeping sensitive data on-site in a data centre, such as client information like birth and credit card details, effectively protects e-commerce enterprises in New Zealand. This is due to the widespread use of third-party payment gateways for payments, some of which do not adhere to New Zealand regulations, leaving personal identifiable information susceptible to data leakage risks. As a result, we currently do not recommend using both public and private cloud computing. Organizations should secure WPA3, and refrain from using personal devices, leaving all laptops in the office. However, Microsoft has announced its intention to construct a data centre in New Zealand by 2025. In 2025, the organisation has the option of keeping client data in a New Zealand data centre, as offered by Microsoft. Then they may shift to Software as a Service (SaaS).

**Flexible business approach:**
The success of e-commerce retail revenues is dependent on discount campaigns, holiday sales, and weather conditions. Initially, organisations start with a private cloud to have full control over their security protocol at every layer. However, in the long term, a private cloud is more costly compared to a public cloud, which offers pay-as-you go. Therefore, migrating data from a private to a public cloud, specifically virtual machines in Microsoft Azure, can help reduce expenses and manage the risks associated with scaling up or down based on fluctuating business conditions in a short period of elastic business demand.

## Requirement 3

### i) Infrastructure security

a) **Analysis**
Organisations should be aware of the possibility of insider threats, which can emerge from dissatisfied employees who may hack or disclose confidential information. Supply chain attacks exploit vulnerabilities in the supply chain of goods or services, presenting a significant security threat.

i) Infrastructure security
b) Suggest and Justification
To address and detect insider threats, organisations should implement measures such as conducting employee training and implementing surveillance to monitor any suspicious behaviour. Disseminating a software update to multiple organisations has the potential to expose a malevolent individual. To mitigate supply chain attacks, organisations should authenticate software updates using the CIS benchmark list, which serves as the minimum-security standard. This allows for benchmark security assessment and the establishment of effective patch management protocols. Both threats require organisations to maintain a constant state of watchfulness and take proactive steps to ensure their security.

### ii) Data security

a) Analysis
Cloud computing has emerged as a crucial component of business operations, necessitating strong data security protocols to guarantee confidentiality, integrity, and accessibility. However, if data is not adequately secured while being sent or stored, it is more likely to be intercepted or accessed by people who have no right to it(*Cloud Security 02.Pptx: DNCT703 Network and Cloud Security (DANCT7124C-E/OL)*, n.d., p. 4).

b) Suggest and Justification
To address this issue, cloud service providers must incorporate robust security measures, including data encryption, access controls, and intrusion detection and prevention systems. Data encryption is the process of converting plaintext data into ciphertext using an encryption algorithm and a key. This ensures that only authorised individuals can access the data(*Cloud Security 02.Pptx: DNCT703 Network and Cloud Security (DANCT7124C-E/OL)*, n.d., p. 11).

### iii) Access Management

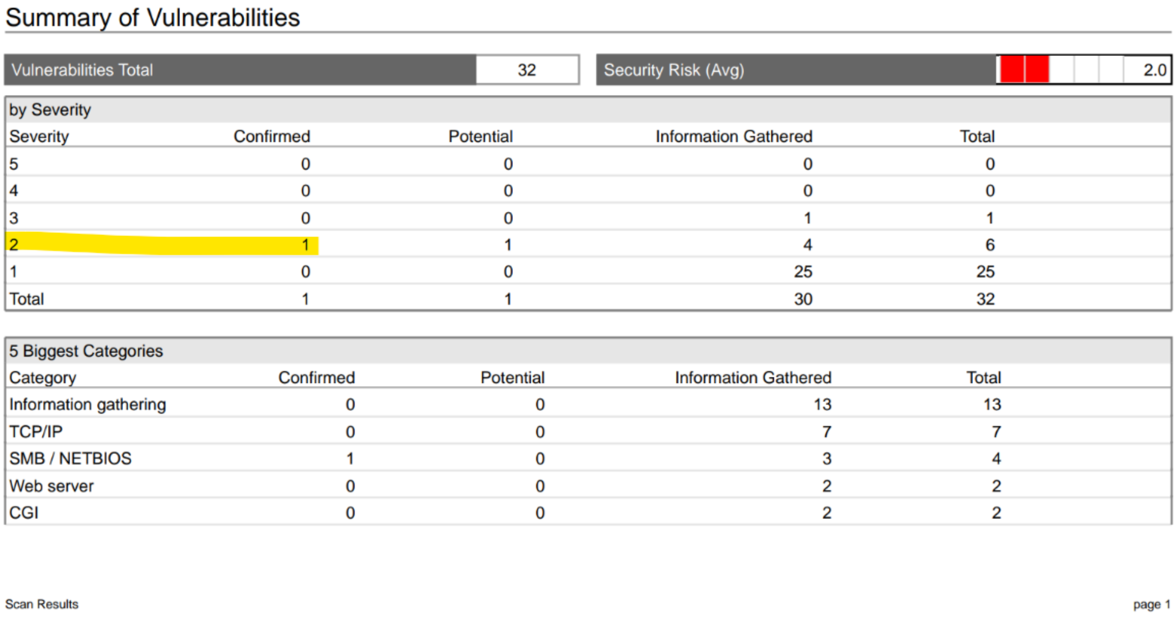
a) Analysis
Unauthorised people can get to private cloud resources or data if the security systems aren't strong enough or the access rules aren't set up right. Cloud computing, a self-service Internet infrastructure, allows more and more people to access and change data saved on faraway computers from any device that can connect to the Internet. However, data security remains a significant issue due to its global storage, necessitating robust defences(Akhtar et al., 2021).

b) Suggest and Justification
Multi-factor authentication is suggested as a one solution, because global administrator can set permission to access the Azure portal by giving the authority so only authorised people can access the cloud, because Businesses place a high priority on data protection, with 94% expressing varying degrees of concern. With a fully secure data flow system, multi-layer security, encryption, IAM, IDAAS, AAAS, MFA, and SAML can stop unauthorized entry and storage that isn't safe. This method allows for biometric security, multi-factor authentication, and key sharing among co-admins(Akhtar et al., 2021).

### c)

**Quantitative Analysis**
This article suggests a complete way to constantly check for hacking risks in smart grid systems that use the Internet of Things. To figure out how dangerous a system is, the method uses attack defence trees and derived risk characteristics. It enables to conduct risk-sensitivity studies and find the best security methods to reduce risks(Rios et al., 2020).

Qualys risk management (**Qualitative Analysis)**
Businesses utilize Qualys, Rapid7, and Tenable to monitor security vulnerabilities. These tools are expensive and only reveal the problem's size when they discuss prioritization. Qualys uses a seven-point scale, whereas Rapid7 uses a scale from 1 to 1000(Walkowski et al., 2021).



## Summary of Vulnerabilities

| Vulnerabilities Total | 32 | Security Risk (Avg) | 🟥🟥⬜⬜⬜ 2.0 |
|---|---|---|---|

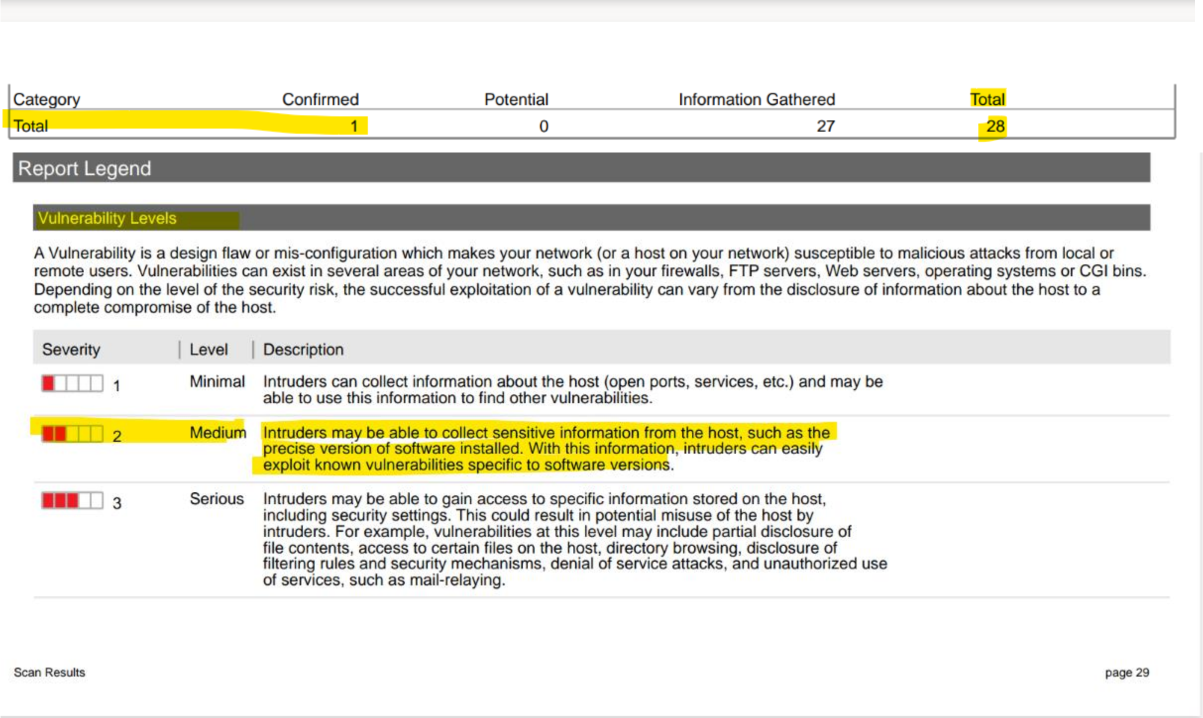
by Severity

| Severity | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| 5 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 1 | 1 |
| 2 | 1 | 1 | 4 | 6 |
| 1 | 0 | 0 | 25 | 25 |
| Total | 1 | 1 | 30 | 32 |

5 Biggest Categories

| Category | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| Information gathering | 0 | 0 | 13 | 13 |
| TCP/IP | 0 | 0 | 7 | 7 |
| SMB / NETBIOS | 1 | 0 | 3 | 4 |
| Web server | 0 | 0 | 2 | 2 |
| CGI | 0 | 0 | 2 | 2 |

Scan Results page 1



| Category | Confirmed | Potential | Information Gathered | Total |
|---|---|---|---|---|
| Total | 1 | 0 | 27 | 28 |

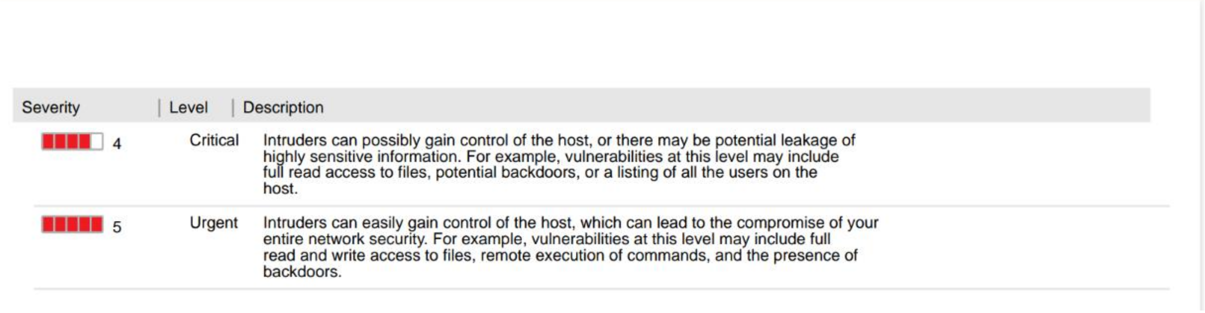
### Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

| Severity | Level | Description |
|---|---|---|
| 🟥⬜⬜⬜⬜ 1 | Minimal | Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. |
| 🟥🟥⬜⬜⬜ 2 | Medium | Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. |
| 🟥🟥🟥⬜⬜ 3 | Serious | Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. |

Scan Results page 29



| Severity | Level | Description |
|---|---|---|
| 🟥🟥🟥🟥⬜ 4 | Critical | Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. |
| 🟥🟥🟥🟥🟥 5 | Urgent | Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. |

# Reference list:

Akhtar, Dr. N., Kerim, B., Perwej, Dr. Y., Tiwari, A., & Praveen, Dr. S. (2021). A Comprehensive Overview of Privacy and Data Security for Cloud Storage. *International Journal of Scientific Research in Science Engineering and Technology*. https://doi.org/10.32628/IJSRSET21852

Al-Mejibli, I. S., & Alharbe, D. N. R. (2020). ANALYZING AND EVALUATING THE SECURITY STANDARDS IN WIRELESS NETWORK: A REVIEW STUDY. *Iraqi Journal for Computers and Informatics*, *46*(1), 32–39. https://doi.org/10.25195/ijci.v46i1.248

Andriukaitis, E. (2023). *MODERNIZATION OF COMPUTER NETWORK IN A COMPANY*. 66.

*Cloud Security 02.pptx: DNCT703 Network and Cloud Security (DANCT7124C-E/OL)*. (n.d.). Retrieved 30 June 2024, from https://nzseg.instructure.com/courses/1111/files/220690?module_item_id=54667

*Enterprise Cyber Risk & Security Platform | Qualys*. (2024, May 31). https://www.qualys.com/

GitHub-Name. (n.d.-a). *Internet Information Services (IIS)—Microsoft Lifecycle*. Retrieved 23 May 2024, from https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis

GitHub-Name. (n.d.-b). *Microsoft SQL Server 2005—Microsoft Lifecycle*. Retrieved 23 May 2024, from https://learn.microsoft.com/en-us/lifecycle/products/microsoft-sql-server-2005

GitHub-Name. (n.d.-c). *Windows 10 Home and Pro—Microsoft Lifecycle*. Retrieved 23 May 2024, from https://learn.microsoft.com/en-us/lifecycle/products/windows-10-home-and-pro

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

Kabrilyants, R., Obeidat, B. Y., Alshurideh, M., & Masa'deh, R. (2021). The role of organizational capabilities on e-business successful implementation. *International Journal of Data and Network Science*, 417–432. https://doi.org/10.5267/j.ijdns.2021.5.002

Maurya, A. K., Singh, A., Dubey, U., & Nath Tripathi, S. P. and U. (2019). Protection of Data Stored in Transparent Database System using Encryption. *Journal of Computer and Mathematical Sciences*, *10*(1), 190–196. https://doi.org/10.29055/jcms/992

Mohamad Rosman, M. R., Arshad, I., Abdullah, N., Abd Aziz, N. E., Osman, G., Shukry, A., Alias, N. R., Rosli, N., Fadzil, F., Md Saleh, M. S., Mohd Zawawi, M. Z., & Rachmawati, M. (2023). *Proceedings of Glocal Symposium on Information and Social Sciences (GSISS) 2023*. https://doi.org/10.5281/zenodo.8201436

Nazir, J., Iqbal, M. W., Alyas, T., Hamid, D., Saleem, M., Malik, S., & Tabassum, N. (2021). Load Balancing Framework for Cross-Region Tasks in Cloud Computing. *Computers, Materials and Continua*, *70*, 1479–1490. https://doi.org/10.32604/cmc.2022.019344

*OffSec's Exploit Database Archive*. (n.d.). Retrieved 4 June 2024, from https://www.exploit-db.com/

Rios, E., Rego, A., Iturbe, E., Higuero, M., & Larrucea, X. (2020). Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees. *Sensors*, *20*(16), Article 16. https://doi.org/10.3390/s20164404

Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability Management Models Using a Common Vulnerability Scoring System. *Applied Sciences*, *11*(18), Article 18. https://doi.org/10.3390/app11188735

Ιωάννης, Δ. (n.d.). *Wireless local area network security and modern cryptographic protocols: WEP & WPA1/2/3*.