

**Group Assignment Cover Sheet**

*You must keep a photocopy or electronic copy of your assignment.*

|  |  |
| --- | --- |
| Unit name: | Introduction to Cyber Security / UG |
| Unit code: | 11906 |
| Lecturer/Tutor’s Name: | Yibe Alem |
| Group Number: | Group 65 |

**I declare that this assignment is solely my own work, except where due acknowledgements are made. I acknowledge that the assessor of this assignment may provide a copy of this assignment to another member of the University, and/or to a plagiarism checking service whilst assessing this assignment. I have read and understood the University Policies in respect of Student Academic Honesty.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Student ID: | u | 3 | 2 | 6 | 3 | 3 | 9 | 6 |
| Student ID: | u | 3 | 2 | 5 | 3 | 0 | 7 | 2 |
| Student ID: | u | 3 | 2 | 6 | 6 | 9 | 4 | 7 |
| Student ID: | u | 3 | 2 | 8 | 4 | 5 | 1 | 3 |

Date: 24/04/2025

# Task 1 - Desktop Severs and Helpdesk

## Uniformity

As the name suggests, “automation for uniformity” is when you use automated processes to ensure a system configuration is consistent across all devices. It greatly reduces the chances of any outliers being present. Certain repetitive tasks are best left automated, as it ensures consistency. When humans are left with repetitive tasks, it increases the possibility of errors. For example, if we manually load Operating Systems (OS) in a computer, there is a high chance that some computers or most will be misconfigured. As a result, diagnosing will be difficult as some computers may have unique problems. (Cameron, n.d.)

If you were to use automation, it would significantly improve productivity, ensure consistency and save time. However, since there aren’t many computers, it might be better to opt for a partially automated system for the scenario mentioned. This is only because there aren’t too many computers, and the cost of the automation might not be worth the time saved.

## Server Technologies

There are many technologies that are essential for servers to boost availability, performance and reliability. Listed below are a few technologies that are beneficial to servers:

**Data backups**- servers contain critical data, and there must be backup servers in case one shutdowns. These backup servers are usually stored in different regions or locations. There is always a chance that natural disasters can affect uptime, so having a server in a different geographical location is vital.

**N+1 Redundancy and Full** – N + 1 redundancy means the system will still be operational if a particular component fails. An example could be a RAID disk. Some RAID systems are still functional even if a disk has failed. Fully redundant systems are when one system runs, and the other is idle. When the second system notices that the first system has failed, the second system is then activated. (Limoncelli 2016, Chapter 2 Page 15)

**Remote Administration access**

Traditionally, old servers had consolers, which could only be operated if you were physically there. Various tasks were performed on the consoles and took up room. In an emergency, a console could be problematic as it may require driving a long distance to solve a minor problem. With remote administration access, you can perform tasks on the server virtually anywhere, thus saving time and being more cost-effective. (Limoncelli 2016, Chapter 2 Page 9)

**Hot-swap components** – Hot swap components refer to the ability of an element to be swapped whilst the system is still operating. Servers cannot afford to power off for long periods as this could cause heavy interruptions. (Limoncelli 2016, Chapter 2 Page 15)

**Redundant Power supplies** – Another fail-prone server component is the power supply. In regard to servers, having a redundant power supply doesn’t just mean having 2 power supplies, but it means if 1 power supply doesn’t work the system will still be working. Usually, each power supply should be on its power socket. (Limoncelli 2016, Chapter 2 Page 14)

## Helpdesks

**Defined processes for staff** – For a helpdesk to operate efficiently, it needs to have well documented protocols on what staff members should follow. It’s not as important for smaller companies, but for larger companies, it is essential. Large businesses use “scripts” for their training. Every type of service request has a set of procedures that need to be followed. For example, a password reset might require users to provide identification or evidence of the account, then the password reset can be accomplished. (Limoncelli 2016, Page 5)

**An Escalation Process**- Escalation processes are the act of moving up a enquiry to a person with more expertise. Typically, the first line of staff should be able to handle 80-90% of queries. The remaining queries should be escalated to the second line of staff, who usually have more experience. If a large portion of calls are escalated to the second line of staff, it could indicate that the first line of staff may require more training or experience. Escalation processes are also suitable for dealing with frustrated customers who want to talk to someone higher up. (Limoncelli 2016, Page 8)

**Help Desk Software –** Helpdesk also need software to help control service requests or tickets. Traditionally, writing notes on a piece of paper was an alternative, but as a business grows, it will certainly not be an efficient way of responding to service requests. Using software helps track and manage service tickets. (Limoncelli 2016, Page 9)

# Task 2 - Cryptography

## Importance of trusted certificate authority

A certificate authority’s (CA) are essential for establishing secure connections over the internet. Whenever you are interacting with websites online, it can occasionally be difficult to verify the authenticity of websites. Some sites could specialise in masquerading as real websites to steal your personal data. The role of CAs is to verify the websites or organisations you are interacting with by issuing the website with an SSL/TLS certificate, or in other words, a “digital certificate” (Awati, 2021).

These types of certificates ensure that connections between both parties are encrypted. With a valid certificate, you will have confidence that your personal data is safe and cannot be intercepted. For university institutes, it is vital that the IT department ensures that students are securely and safely connected to authenticated websites. A trusted CA ensures that students’ data are protected online, establishes secure connections with hosts and prevents a middleman from creating attacks. Signatures are a type of way that a person uses to confirm and authenticate their identity.

## Ensuring authenticity of announcement’s

The IT department must first obtain a digital certificate from a trusted authority. A digital certificate can only be issued by a trusted CA. When the IT department receives a digital certificate, this will establish and verify their identity. A digital certificate is crucial because it determines whether announcements come from a legitimate source. Having a digital certificate will ensure that there is trust between the IT department and the students. A digital certificate also helps prevent spoofing or impersonation of the IT departments because only trusted entities can withhold a digital certificate. A digital certificate will also ensure that messages sent keep their integrity. If the IT department were to send a message and it happens to be modified, the signature will not be verified. This is important as it prevents any message from being tampered with, sent with, or changed.

Once the IT department obtains a digital certificate, the students will need to verify the digital signature from the IT department using the public key from the IT department’s digital certificate. This step is crucial because it will allow students to check whether the IT department’s signature is valid using the public key.

The public key also plays a pivotal role in ensuring students are safe. The public key is there to prove that the message actually came from the source that sent the message (IT department). It is a way of preventing spoofing or fake announcements. The public key will also verify the signature of the IT department. If it has been tampered with or changed, the verification process will fail, thus ensuring the authenticity of the announcements made to the students.

When the IT department receives all the necessary safety measures, including digital certificates, public keys and private keys, the students can fully trust that the announcements made are safe and properly authenticated. All the measures listed above are put in place to ensure authenticity, integrity and safety are all met. In the real world, providing you only communicate with trusted entities is vital. With the rapid advancements in technology, scenarios like this can help us verify who we can actually trust.

## Hands on

1. This command on the terminal will generate a 2048-bit RSA private key.

ITPUB.key is the private key file name

## 

This command will take the public key from the previous private key (ITPUB.key) file that was just made. This command pretty much reads the private key file and tells us where we want to output the public key. It will generate the right public key, by using the files from the private key



1. This command will create a self-signed certificate.

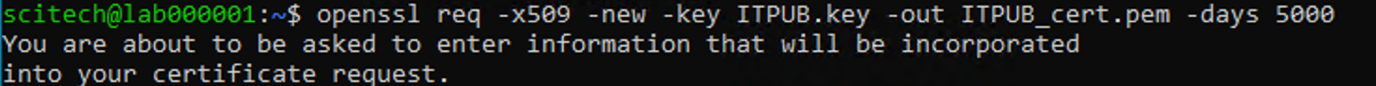
Req- command to generate certificate

New- a new certificate request

Days- how many days the certificate will be active for

X509- tells openssl to generate self-signed certificate

Private key and public key are also specified



1. Creates a text file so we can verify the announcements made by the IT department



1. The IT department can sign the ‘.txt’ file and store it. Uses the private key to sign it



1. Students use the IT departments public key to validate the signature on the announcements. If the signature is valid it will return: Verified OK. If not, it will return: Verification Failure



# Task 3 - DoS and Firewall



### Explanation:

These components were placed strategically to accommodate security reasons and requirements.

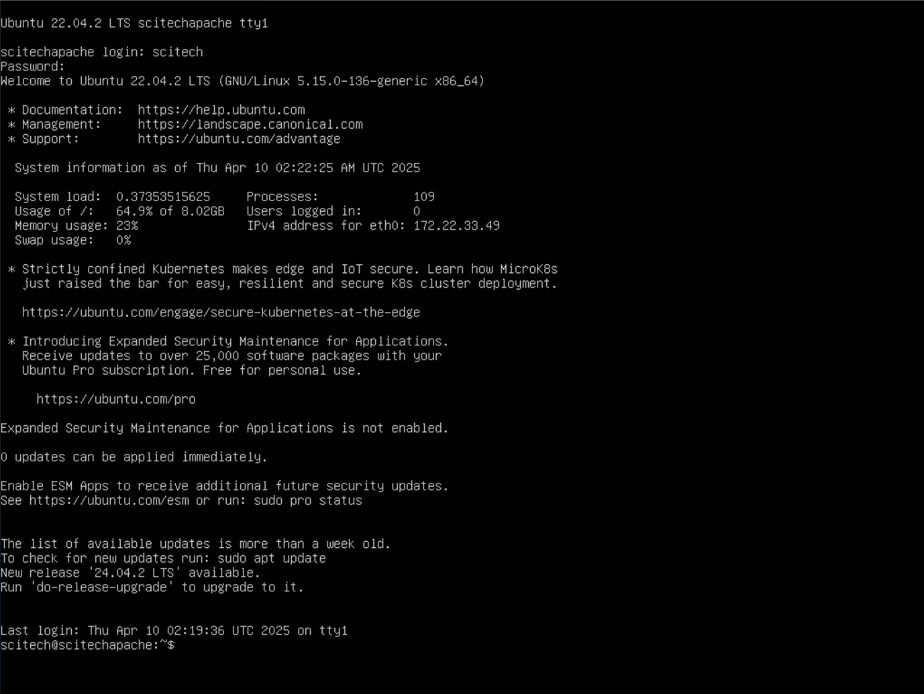
The border router sits at the internet edge as a first line of filtering for public and private addresses before the traffic hits the external firewall. It is primarily responsible for NAT and basic ACL filtering.

The external firewall sits between the internal and DMZ to ensure that it explicitly permits services to reach externally facing servers and blocks everything else. It is primarily responsible for protecting the DMZ, allowing only a specific number of ports (SMTP 25 for the email server, HTTP/HTTPS 80/443 for the Web Server.).

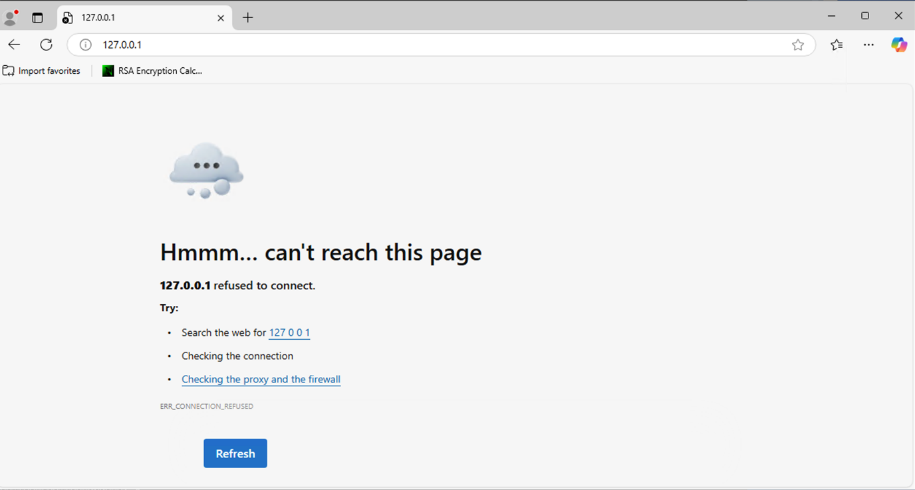
The DMZ (Demilitarised Zone) is responsible for accepting incoming internet connections and isolating them in the area where they are placed so that if compromised, the attacker does not immediately gain access to the internal LAN. The DMZ contains the Email and Web servers, which are exposed externally.

Additionally, the internal firewall surrounding the internal LAN enforces no inbound connection from the internet or DMZ, allows inbound internet access for the desktops and printers, and allows DMZ-LAN only on strictly monitored/needed management ports.

Lastly, the internal LAN area contains desktops and printers. The desktops can initiate outbound traffic, such as email and web browsing, but cannot accept inbound flows. The printer is a shared resource that only communicates between internal desktops when needed. The placement of internal LANs ensures that end-user machines and printers are being used in a trusted segment where policies such as antivirus patching are applied.



*(Apache Server Homepage)*



*(Failed Attempt)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **action** | **ourhost** | **port** | **theirhost** | **port** | **comment** |
| block | 10.0.2.180 | 80 | any | any | Allowing incoming HTTP Traffic |

# Task 4 – Software & System Security

## Buffer overflow and its consequences

Buffer overflow refers to an error in a software’s code which can be exploited by malicious actors to gain access to a system (Fortinet, 2025). The word “buffer” refers to the region of computer memory where data is stored when it is processed within the computer. This is mainly used to regulate the difference between data being received and data being processed (Geeksforgeeks, 2020). When a buffer overflow occurs, the system might attempt to overwrite the incoming data in adjacent memory regions (Imperva, 2020).

The consequences of a buffer overflow issue can be but not limited to a program crashing of being put in an infinite loop, that is executing a series of command infinite time, or the attacker gaining access to the system to execute malicious code content (OWASP, 2021).

## Preventing buffer overflow issues

To prevent or mitigate buffer overflow issues, developers can apply some of the following programming techniques:

* Upgrading the code base to a memory safe language. Although this is a costly endeavour, moving the code base from a legacy language like C to a language like Python will help with memory management without relying on user verification (CISA, 2025).
* Use unit tests with toolchains such as AddressSanitizer and MemorySanitizer along with the source code to identify memory related issues (CISA, 2025).
* Apply new security patches to their codebase or languages.

## Rectifying problems in applications

The first step to rectifying the problem is understanding the problem itself. According to the database provided by NIST, the issues outlined described the vulnerability in the Firefox browser where attackers can execute arbitrary code when specific plugins are used or through certain known and unknown vectors (National Vulnerability Database, 2015).

To rectify this problem, the following actions are recommended:

* Immediately update or patch the currently installed Firefox browser on any system to mitigate potential impact.
* Use advanced monitoring tools to monitor for potential unknown traffic coming into the system (TrueFort, 2025).
* Disable autoplay for media files in browser according to CVE-2015-0813.
* Educate users to avoid opening suspicious links.
* Adopt a zero-trust practice.

## Addressing the problems

Adhering to the “one, some and many” principle, the following steps of action should be taken:

* One computer:
  + Install the latest Firefox update package for the operating system and integrate rules such as disabling autoplay and advanced monitoring tools mentioned above.
* Some computers:
  + Identify some systems using the old version of the Firefox browser without any security measure implemented above, implement them and test if the security measures are implemented correctly.
* Many computers:
  + Once it has been verified that the security measures have been implemented correctly, push the Firefox browser update along with the security measures to all system connected to the network using the update software.

## Summary

Due to the significant threats detailed in the identified CVEs regarding the Firefox browser, installing the Firefox browser is not a recommended course of action due to the nature of a server computer. This computer can store critical data, which is essential for the company’s function, and installing a web browser with a critical level of CVE is not recommended. If the browser is not regularly updated for security patches, malicious attackers could exploit these vulnerabilities and gain unauthorized access to these critical data and potentially cause even more damage to the server, at worst damaging the entire system.

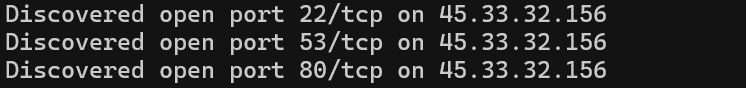
## Hands on practices

Summary: “nmap” Security Report

The following command was run on a Linux distribution:



And the following results were produced (first few lines):



The security scan was done to identify any potential vulnerabilities on the website “nmap.scanme.org”. The scan detected the following:

* Open port 22 which concerns SSH connection
* Open port 53 which concerns DNS or a domain resolver for requested IP addresses of a domain
* Open port 80 which concerns HTTP connection

These ports being opened means that they will respond to connection requests. This is dangerous because threat actors can exploit these open ports to carry out attacks. Some common attacks that can be carried out using these open ports are:

* Port 22: If the SSH authentication protocol is not enforced correctly, the SSH key can be easily acquired which enables attackers to gain remote access into the system without using credentials and is also vulnerable to brute force attacks.
* Port 53: The DNS port translate human-readable domain name into actual IP addresses to process requests. This port is vulnerable to DDoS attack which can disrupt service with a high volume of packets.
* Port 80: This port is responsible for HTTP protocols to connect to web pages. An open port is a target for threat actors to target with attacks such as cross-site scripting, SQL injection and more (Schrader, 2024).

Additionally, the security scan also yields some notable security risks:

* A list of critical CVE exploits on port 22 along with a list of username/password keypairs used for SSH brute-forcing
* A site map of the website on port 80 which contains some of the website’s source files along with a potential vulnerability to Slowloris, and a list of critical vulnerabilities
* Authentication risks for DNS ports, exposed services used on the website and potential implementation flaws

Failure to mitigate these risks could result in:

* Attackers exploiting vulnerabilities in port 22 to gain remote access to the system, which will enable them to execute malicious code on the system.
* The website is vulnerable to DDoS attack which will impact availability, service and could be costly financially.
* Threat actors can insert malicious malware using the system using vulnerabilities identified on port 80 to cause steal critical information from the website and gain complete control of the website.

To mitigate the first issue from the scan result, which concerns SSH, the following steps can be taken:

* Consider turning off port 22 and directing the traffic into any port above 1024 to limit unauthorized access to the server (IBM, 2025).
* Use firewall rules to restrict access from any unrecognized IP addresses
* Disable root login capability and enable SSH keys instead of password (James, 2025).

# Conclusion

Having open ports can pose a significant security risk, especially with the standard ports listed above and their vulnerabilities. Specific recommendations have been outlined above to mitigate the issues on port 22, such as using firewall rules and secure login methods. Following the recommended steps should improve the security measures on port 22. However, additional security measures such as monitoring and regular audits are still recommended to ensure that the system is not vulnerable to remote access attempts.

# References

1. Awati, R. (2021). *What is a certificate authority (CA)?* [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/certificate-authority.
2. Fortinet 2025, *What Is Buffer Overflow? Attacks, Types & Vulnerabilities*, Fortinet.
3. geeksforgeeks 2020, *Buffering in Computer Network*, GeeksforGeeks.
4. IBM 2025, *Aspera FASP Proxy*, Ibm.com.
5. Imperva 2020, *What is a Buffer Overflow | Attack Types and Prevention Methods | Imperva*, imperva.
6. James, H 2025, *SSH Security: Protecting Your Linux Server from Threats*, LinuxBlog.io.
7. *NVD - CVE-2015-0815* 2015, Nist.gov.
8. OWASP 2021, *Buffer Overflow | OWASP*, owasp.org.
9. Schrader, D 2024, *Identifying Common Open Port Vulnerabilities in Your Network*, Netwrix.com, viewed 24 April 2025, <https://blog.netwrix.com/open-ports-vulnerability-list#Port\_22\_Vulnerabilities\_SSH.>.
10. Stergiopoulos, G, Gritzalis, DA & Limnaios, E 2020, ‘Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns’, *IEEE Access*, vol. 8, pp. 128440–128475.
11. Team, SI 2025, *Managing Critical Firefox Vulnerabilities • TrueFort*, TrueFort.