ICT287 ASSIGNMENT1

LEE JIHU (34061648)

Table of Contents

[**Executive summary 2**](#_Toc74539857)

[**Attack Surface Analysis 2**](#_Toc74539858)

[**Network attacks 2**](#_Toc74539859)

[**physical attacks 6**](#_Toc74539860)

[**Summary and prioritization of issues 7**](#_Toc74539861)

[**Recommendations 7**](#_Toc74539862)

[**Reference 8**](#_Toc74539863)

# Executive summary

The ‘Planet of the Grapes’ is an organization that has three stores operated independently by wine and spirit merchants. Due to the faster-than-expected expansion, there is unintentionally no shared data between the stores. This organization has so far not employed IT security staff and has set up systems on their own. However, as the risk to cybersecurity grew, they contracted computer security consulting firms to identify network vulnerabilities and seek advice on the fixes needed to strengthen the network.

There are a total of 10 full-time employees who handle backlogs, salaries, personnel, and schedules. He also often works as a front counter or cashier when requested. There are many casual employees but their turnover is very high. Full-time and general staff work in the same place, so it is easy to access places such as public facilities and offices for employees.  
  
The company's computer systems are connected via Cisco Small Business Series asymmetric digital subscriber line (ADSL) routers, and some computers can be accessed via remote access services without direct manipulation. In addition, all employees are logging in locally to every computer by sharing only two accounts. This allows all employees to access all files that exist on the network. While clients run Windows 7 for office applications, the server runs Ubuntu Linux to host it as an online status check, print server, and file server.

Network level attacks are attacks that violate basic network protocols. You can get sensitive data about the system and use it to attack the system. In these cyberattacks, attackers are usually the first to search for open ports in the system. The first line of defense is the network to prevent such infringement. Vulnerability scanning must be performed to detect open ports and vulnerabilities. This points to potential avenues of security vulnerabilities in the network. (Atul, 2003, p. 11)

# Attack Surface Analysis

## **Network attacks**

|  |  |
| --- | --- |
| Name | SSL/TLS MITM vulnerability (CCS Injection) |
| Port | 25/tcp |
| CVE | CVE-2010-4344 |
| State | Vulnerable |
| Risk Factor | High |
| CVSS Score | 9.3 |
| Description | SSL before 0.9.8za, 1.0.0 before 1.0.0 and 1.0.1h before 1.0.1h. Intermediate attackers trigger certain OpenSSL-to-OpenSSL communication to use a zero-length master key and do not properly restrict the processing of ChangeCipherSpec messages that can be intercepted or obtained through a crafted TLS handshake called "CCS Injection"(Matthew&Jennifer, 2020, p.171). |
| Impact | The vulnerability allows an attacker to remotely execute arbitrary code without direct contact with hardware, which can be executed through an SMTP session resulting in improper denial logging. Consequently, it allows unauthorized disclosure of information and amendments and allows discontinuation of services. |
| Solution | This vulnerability occurs against Exim prior to Exim version 4.69 and can be addressed by upgrading Exim to the latest version. |



|  |  |
| --- | --- |
| Name | Sweet32 |
| Port | 25/tcp, 443/tcp, 631/tcp |
| CVE | CVE-2016-2183 |
| State | Vulnerable |
| Risk Factor | Medium |
| CVSS Score | 5 |
| Description | It is a vulnerability caused by using only medium-intensity password encryption. The medium-intensity password is 64 to 112 bits long, so when enough traffic is sent, it can cause crashes and recover things like session cookies. |
| Impact | A birthday attack on an encrypted session over a long period of time makes it easy to obtain clear textual data. |
| Solution | It can be solved by updating with a stronger password. |

|  |  |
| --- | --- |
| Name | Transport Layer Security (TLS) Protocol DHE\_EXPORT Ciphers Downgrade MitM (LogJam) |
| Port | 25/tcp |
| CVE | CVE-2015-4000 |
| State | Vulnerable |
| Risk Factor | Medium |
| CVSS Score | 4.3 |
| Description | A flaw is present in the Transport Layer Security (TLS) protocol that is triggered when processing the Diffle-Hellman key exchange defined by the DHE\_EXPORT password. This could allow an attacker to undermine the security of TLS sessions to 512-bit export class encryption, which significantly reduces the performance of encryption (Paulino, 2017, p.153). |
| Impact | The vulnerability can easily be exploited by attackers to penetrate encryption barriers and observe or open or open encrypted streams. |
| Solution | User must update the operating system when it is available. User should check the update configuration to ensure that compatibility issues are not encountered. |



|  |  |
| --- | --- |
| Name | ETag Incode Information Leakage |
| Port | 80/tcp, 443/tcp |
| CVE | CVE-2003-1418 |
| State | Vulnerable |
| Risk Factor | Medium |
| CVSS Score | 4.3 |
| Description | Apache is a type of HTTP web server software. Software that retrieves information from the web server itself and then provides information to clients to enable users to access websites over the Internet (Domantas, 2020, p. 1). Apache must be secured, but versions 1.3.22 to 1.3.27 are affected by information disclosure vulnerabilities. This occurs because the entity tag (ETAG) in the HTTP header holds sensitive information, such as the index number of the file. (Yoshiki, 2019, p.75) |
| Impact | The vulnerability is only available to obtain information about files, such as the source, inode (index) number, file size, and when they were last modified. |
| Solution | The remedy for this vulnerability is to remove all file inodes from the ETag header calculation. |



|  |  |
| --- | --- |
| Name | ssl-heartbleed |
| Port | 25/tcp |
| CVE | CVE-2014-0160 |
| State | Vulnerable |
| Risk Factor | High |
| CVSS Score | 5 |
| Description | This is a serious vulnerability in the Open SSL encryption software library that leaves large amounts of personal data on the Internet. |
| Impact | The vulnerability could allow an attacker to steal information that needs to be protected with SSL/TLS encryption. |
| Solution | OpenSSL 1.0.1g has been released and keys generated with vulnerable versions of OpenSSL should be considered affected. Therefore, after applying the patch, you must recreate and distribute the key. It is also recommended that your system administrator consider implementing forward confidentiality to avoid future private keys being compromised. You can also recompile OpenSSL by adding the "OPENSSL\_NO\_HEARTBEATS" to the Code Compilation Time option (Perry, 2019). |



|  |  |
| --- | --- |
| Name | SSL POODLE information leak |
| Port | 25/tcp, 443/tcp |
| CVE | CVE-2014-3566 |
| State | Vulnerable |
| Risk Factor | Medium |
| CVSS Score | 6.8 |
| Description | It paddes block passwords for SSL 3.0, an outdated encryption program that is not detected in the protocol. Thus, an attacker can repeatedly extract prior data using arbitrary data as padding and decrypt them by one byte. |
| Impact | The vulnerability could allow for middleman attacks that could allow SS3.0 connections to obtain plain text data. |
| Solution | It is likely to occur if SSL 3.0 is being used regardless of the product version. Therefore, SSL 3.0 must be completely deactivated on the server. |



|  |  |
| --- | --- |
| Name | Slowloris DOS attack |
| Port | 80/tcp, 443/tcp |
| CVE | CVE-2007-6750 |
| State | Likely vulnerable |
| Risk Factor | Medium |
| CVSS Score | 5.3 |
| Description | Slowloris opens a connection to the destination web server and sends partial requests, keeping connections to the destination web server open. It then empties resources on the http server causing a denial of service. |
| Impact | The vulnerability attacks the threaded web server by sending multiple incomplete HTTP requests. Each request occupying each thread creates a bottleneck to the connection to the server, invading its availability |
| Solution | Slowloris DoS attack techniques are attacks that violate availability by continuously maintaining connections, which can be solved by setting a short duration of connectivity. Applying signature-based filtering through security equipment such as IDS provides additional defense. |



|  |  |
| --- | --- |
| Name | Open ipp |
| Port | 631/tcp |
| CVE | CVE-2014-3704 |
| State | Likely vulnerable - script execution failed |
| Risk Factor | Medium |
| CVSS Score | 7.5 |
| Description | The vulnerability causes the argument extension function in the database to incomplete prepared statements. |
| Impact | This allows remote attackers to carry out attacks via SQL injection. Before using SQL queries, you can use your browser to attack users because you do not recognize whether this is user input data. |
| Solution | Since the attack is mainly via Drupal, it can be prevented by patching or upgrading from Drupal. |



|  |  |
| --- | --- |
| Name | Open mysql |
| Port | 3306/tcp |
| CVE | CVE-2012-2122 |
| State | Likely vulnerable - script execution failed |
| Risk Factor | Medium |
| CVSS Score | 7.5 |
| Description | With a specific implementation of memcp features, a security bug in MySQL allows an attacker to bypass authentication by repeatedly authenticating with the same invalid password that MySQL considers equivalent. This may result in a later incorrect return value resolution. |
| Impact | The vulnerability could allow an attacker to repeated connection attempts to penetrate the system with a password as long as the username is known. This allows you to modify or abort information without permission. |
| Solution | user can restrict access to the local system by modifying the my.cnf file. The user must set the bind-address parameter to 127.0.0.1. |



|  |  |
| --- | --- |
| Name | SMBLost |
| Port | 6001/tcp |
| CVE | CVE-2010-4344 |
| State | Vulnerable |
| Risk Factor | High |
| CVSS Score | 7.5 |
| Description | Two prerequisites are needed. First, you must have user credentials to connect to a remote shared folder. The second is that partitions should be shared on servers such as "c:\", "d:\", etc. The vulnerability could allow an attacker to execute remote code (Miroslav, 2015, p.53). |
| Impact | Attacker can collect Microsoft Server Message (SMB) packets and send them to the system. |
| Solution | All systems for patching should be updated to improve system security. |

## **physical attacks**

1. High turnover of casual employees

There is a possibility that company data and access rights will be shared to external parties without handing over data to the relevant department before the deadline.

1. Public Login User ID and Password

All computers can be accessed with only two user accounts, which severely lacks security. Even important data can be accessed by all staff. In the event of a problem, the tracking of the person in charge becomes difficult due to a common account

1. Employees have remote access to corporate data

Cisco Small Business Series ADSL routers are being used by Telstra, which does not have a centralized authentication server. This allows all parties to access data remotely, and even creates the possibility of outsiders accessing employee information.

# Summary and prioritization of issues

In summary, the vulnerabilities listed above are the most fatal vulnerabilities applied to the system of 'Planet of the Grapes'. The system is vulnerable, which means it is more likely to be attacked, and that it is just as powerless when attacked. And once hit, it's very difficult to recover from that data loss. This regards the urgent need to address the problems that the present system of ‘Planet of the Grapes’ has.

It is impossible to solve the above listed vulnerabilities all at once, and the order in which they should be addressed must be determined first. This should be solved based on the Risk Factor and CVSS Score written in the analysis above. First, the risk factor should be sorted in the order of high, then the CVSS Score should be solved in the order of high. Nevertheless, for vulnerabilities of similar importance, depending on the solution, vulnerabilities that can be resolved faster will need to be addressed first.

# Recommendations

As a basic prerequisite, it is recommended to follow the solutions provided above. As a result, most of the currently identified problems can be dealt with.

In addition, for physical attacks, it is recommended to open a centralized authentication server so that all employees have separate accounts. This raises the basic access barrier, which is believed to reduce information exposure.

The above vulnerabilities are often associated with buffer overflows, and regular testing, ongoing detection, and security practices for buffer processing are critical to prevent such attacks. One of the key strategies is to use other languages that do not allow such actions. The buffer overflow vulnerability is not affected because languages other than some, such as C or C++, which are primarily used for buffer overflow attacks, do not share the characteristics of buffer overflow. (Jason, 2005, p.17)

And it is recommended switching to another vendor that can provide a safer cyber environment for the company.

# Reference

Atul Kahate. (2003). Cryptography and Network Security. Tata McGraw-Hill

Matthew Hickey&Jennifer Arcuri. (2020). Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming. WILEY

Paulino Calderon. (2017). Nmap: Network Exploration and Security Auditing Cookbook. Packt

Domantas, G. (2020). What is Apache? An In-Depth Overview of Apache Web Server. Retrieved 15 April, 2020, from <https://www.hostinger.com/tutorials/what-is-apache>

Yoshiki Shibukawa. (2019). Real World HTTP: rekishi to kōdo ni manabu intānetto to uebu gijutsu. O’REILLY

Perry Carpenter. (2019). Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors. WILEY

Miroslav Vitula. (2015). Learning zANTI2 for Android Pentesting. Packt

Jason Deckard. (2005). Buffer Overflow Attacks: Detect, Exploit, Prevent. Syngress