Penetration test report

Ethical hacking

01 March 2023

Confidential

Content page

Executive summary **2**

Summary of results **2**

Vulnerability findings **3**

CWE-1391: Reusing passwords and usernames 3

Attack narrative

CVE-2017-0143: SMB Eternal blue shell access 4

Attack narrative

CWE-521: Weak passwords 6

Attack narrative

CWE-1392: Use of Default Credentials 8

Attack narrative

CWE-770: Misconfigured security systems 10

Attack narrative

Conclusion **13**

References **14**

Executive summary

I could conduct this penetration test through the authorisation from Frozen Yogurt LTD. This test was authorised to access the company's system security. Frozen Yogurt only provided me with a Windows machine for this test.

There are three main goals/outcomes provided in this report listed below:

- The methodology that was used for assessing.
- The vulnerability and weaknesses found.
- Recommendations for improving security

These goals are outlined to make sure we can improve overall security.

This report is based on the national vulnerability database's scoring for risk assessment and severity level. The main factors affecting these scores will be integrity, confidentiality, and accessibility.

(https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, the website where the scoring was conducted for the weaknesses)

Summary of the tests

Vulnerability	Risk/cvss
Reusing passwords and usernames	8.6
SMB Eternal blue shell access	8.1
Weak passwords	8.1
Use of Default Credentials	7.6
Misconfigured security systems	7.6

High

- Reusing credentials allows for easy brute force and cracking
- Using a reverse shell attack to gain access to the shell of the system
- The ability to crack the passwords on the system
- Not changing default credentials for a root account
- Not having the greatest configured settings for application or security software

Vulnerability findings

CWE-1391: Reusing passwords and usernames		
Risk/CVSS	high	8.6
Tools	Metasploit Framework 6.3, Jack the ripper 1.9.0, hashcat v6.2.6	
Description	This weakness is the process of a person or application reusing a password that could be guessed since they have been used before	
Impact	Since it is being reused on a system, it can allow an attacker to access your information, which may lead to data leaks and the ability to make more attacks from your computers/devices. The potential to be keylogger and gain more account/access since they can sit quietly on your computer while you are using it, monitoring what you are doing.	
Recommendation	Make sure your employees know that when using a different system, they do not use the same passwords they use on anything else to avoid potential cross-over, especially for higher authority accounts.	

Attack Narrative

Before I started the penetration test on Windows, I did one on Linux (figure 9). As you can see, the password is “frozenyougert”. This is important because after I cracked the Windows passwords (figure %), you can see the password for the “frozen” account is the same as “frozenyougert”. This is an issue because the Linux machine does not have an admin/sudo account. However, the one on Windows is an admin account. If someone has the passwords, they could simply brute force them into the Windows account, which can perform a lot more malicious activities since it is a more authorised account.

Figure 9 - the password that is duplicated from Linux

CVE-2017-0143: SMB Eternal blue shell access		
Risk/CSVV	high	8.1
Tools	Nmap v7.93, Metasploit Framework 6.3, Eternalblue 2017-03-14	
Description	The SMBv1 on a Windows system server can be exploited, allowing someone to use arbitrary code to access a shell	
Impact	This vulnerability allows access to a root account on the systems. Attackers can then gain access to everything by extracting passwords and gaining access to all accounts on the system. Letting them install potential malicious programs/applications would let them gain more information from stuff like season tokens or data stored in the RAM.	
Recommendation	An update was released in March 2017: the MS17-010 is designed to fix these flaws. If you can disable SMB for the time being, it will be fixed. possibly implement a more consistent update scheme that allows you to be up-to-date.	

Attack Narrative

I will start by scanning the ports on my IP range to see what is currently active on the network. I did this using Nmap; this service allows me to get network ports and services that are currently running with details on if they are open. This led me to discover that there are many different network ports and services running and open: these were msrpc, netbios-ssn, and Microsoft-ds (figure 1). After this, I ran a vulnerability script using Nmap which led me to find a vulnerability through Smb; after some research, this led me to see that I could use Eternal Blue to access the system's shell (figure 2). (Figure 3) shows me access to the shell.

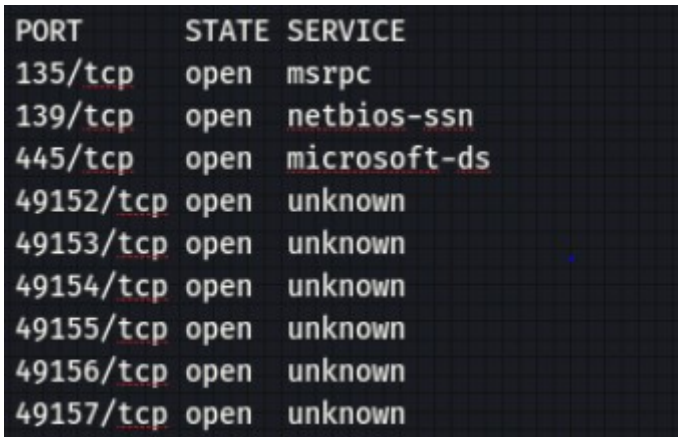

Figure 1 – The result of the Nmap scan

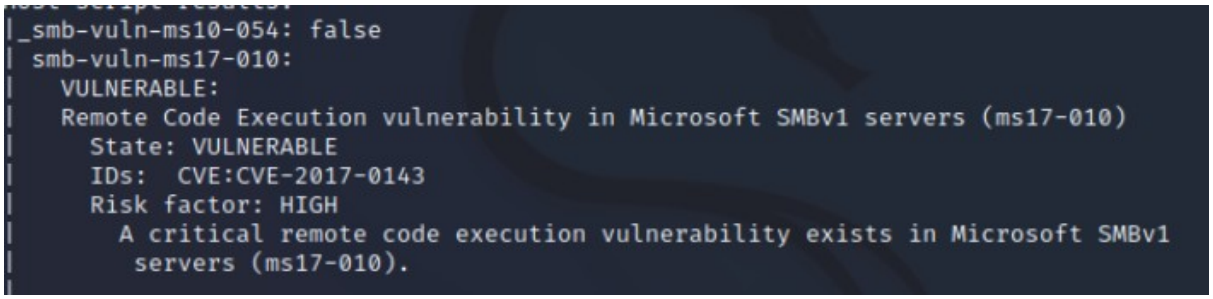

Figure 2 – results of the vulnerability script ran through Nmap

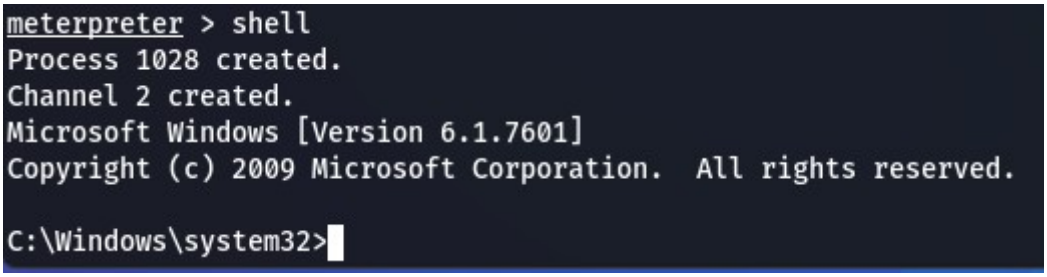

Figure 3 - getting shell access

CWE-521: Weak passwords		
Risk/CSVV	high	8.1
Tools	John the Ripper 1.9.0	
Description	This weakness occurs when the system allows the application of weak passwords, which malicious attackers could easily guess and brute-force.	
Impact	Unauthorised access could allow an attacker to get access to an admin account, which could lead to more accounts and data theft from the system, or it could allow them to implement applications that they could use to exploit your system's long-term.	
Recommendation	Enforce a more assertive password policy that makes it mandatory to have strong passwords on the system. Again, ensure these passwords are unique to accounts and have the usual ideal password methodology.	

Attack Narrative

After getting into the system with Eternal Blue and gaining access to the running shell on the system. In (figure 4) you can see I have gone and done a hash dump for the system, which has given me access to all the password hashes on the system. I then put all of these files into a text document and downloaded “rockyou.txt”. Afterwards, I cracked these passwords using John the ripper, which gave me access to one of the admin accounts and another one (figure 5).

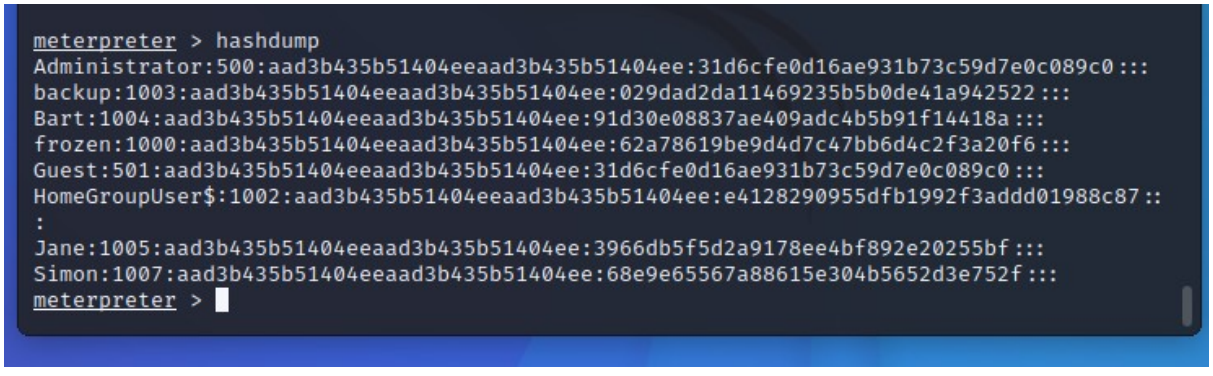

Figure 4 – hash dump of all passwords for user accounts on the system

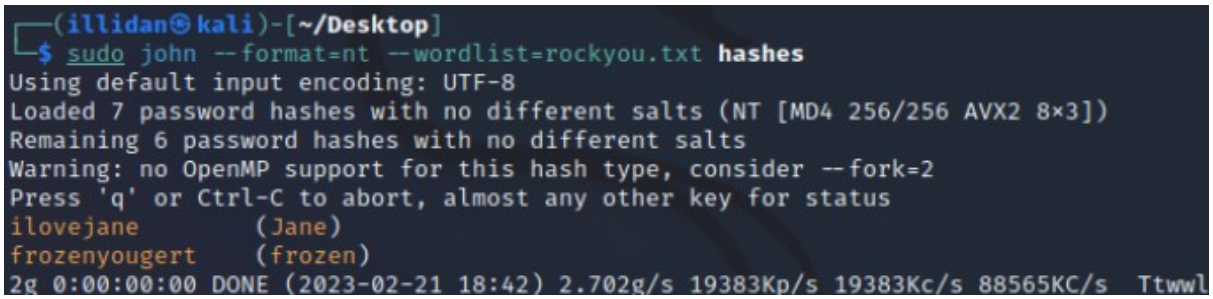

Figure 5 - the result of using John on the hashes

CWE-1392: Use of Default Credentials		
Risk/CVSS	high	7.6
Tools	Metasploit Framework 6.3	
Description	This weakness is the use of default credentials (passwords/usernames) after the installation	
Impact	This can be used to gain unauthorised access to high-functioning accounts on your system, leading to potential data theft or malicious activity that involves the ability to break and monitor activity done by people on the network.	
Recommendation	Always change the default credentials for any system. Hopefully, after just installing it, make sure to use strong and unique passwords. Make sure to delete any text document that could potentially hold important data regarding your accounts.	

Attack Narrative

After accessing the shell (figure 3), I looked around in the users' folders and looked into "Jane". I went through some of the user and application files to see what was attached to see if anything was "exploitable", but I noticed a file in the xampp folder called passwords. This folder shows the user account for phpadmin "root" and the "Password: "(figure 7), meaning there was no password to their root account on the phpadmin web server. This allowed me to log into the phpadmin website and do whatever I wanted, even with their SQL database (figure 8).

Figure 6 - the password file

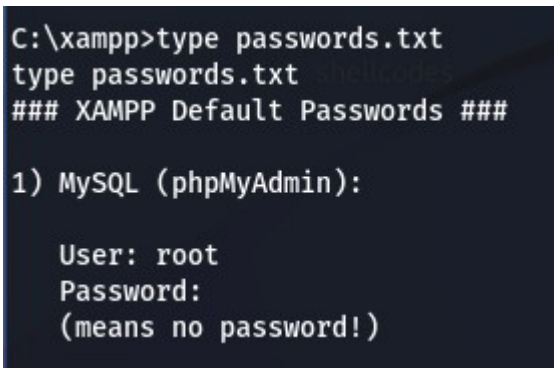

Figure 7 - The content of the password file

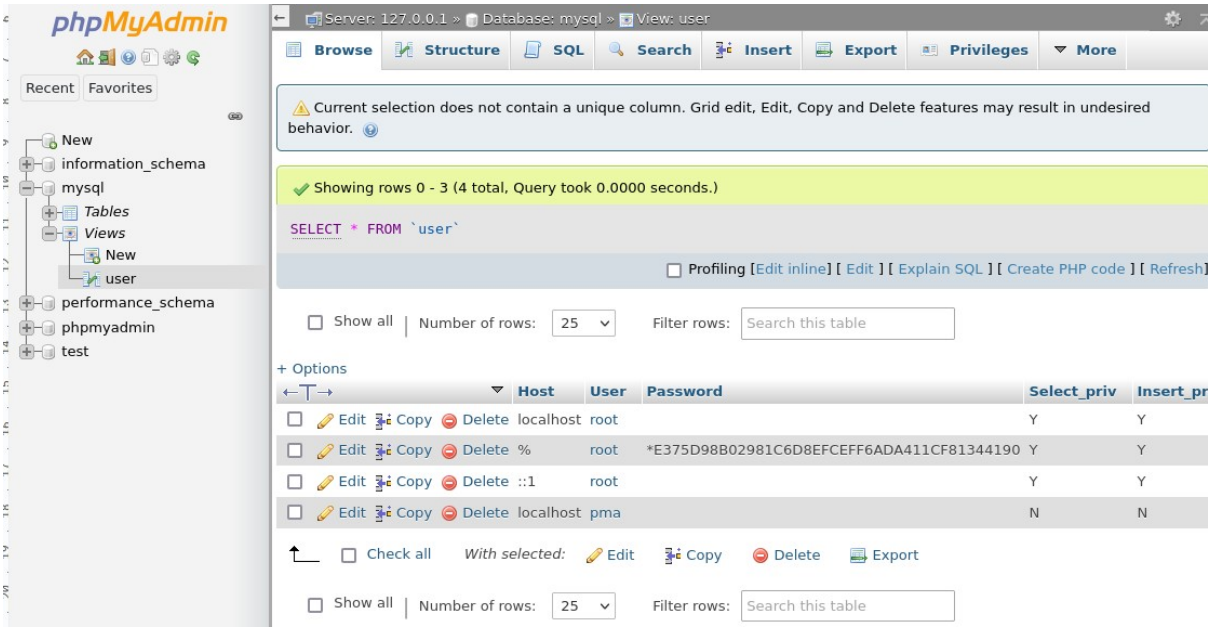

Figure 8 - access to the php admin website

CWE-770: Misconfigured security systems		
Risk/CVSS	high	7.6
Tools	Metasploit 6.3, python3, Any browser, msfvenom	
Description	This is where the system has misconfigured security features.	
Impact	This weakness allows an attacker to bypass security features. This can allow an attacker to monitor what the infected system is doing and lay little traps that they could use to keep an eye on the website you are going to and what you are typing.	
Recommendation	Implement a more industry-standard security process for all your security applications, and ensure you are using more up-to-date security applications and processes.	

Attack Narrative

This attack stems from having a misconfigured firewall/network (figure 10), which could also lead to an upgrade in the operating system. I could use Msfvenom (figure 11) for this attack to create an executable payload. I then put that in a folder on my Kali desktop. I ran an HTTP server inside this folder through Python (figure 12). This created an accessible server from any of the systems on the network. After this, I ran a Metasploit exploit that would make it so that if someone ran this executable, I could gain a reverse shell. (Figure 13) You must get someone to run the website with simple social engineering. This should be possible. After running the executable, which the firewall only warned me for once and executed gave me a reverse_tcp session (figure 14). Running this executable would not be impossible if the firewall were correctly configured.

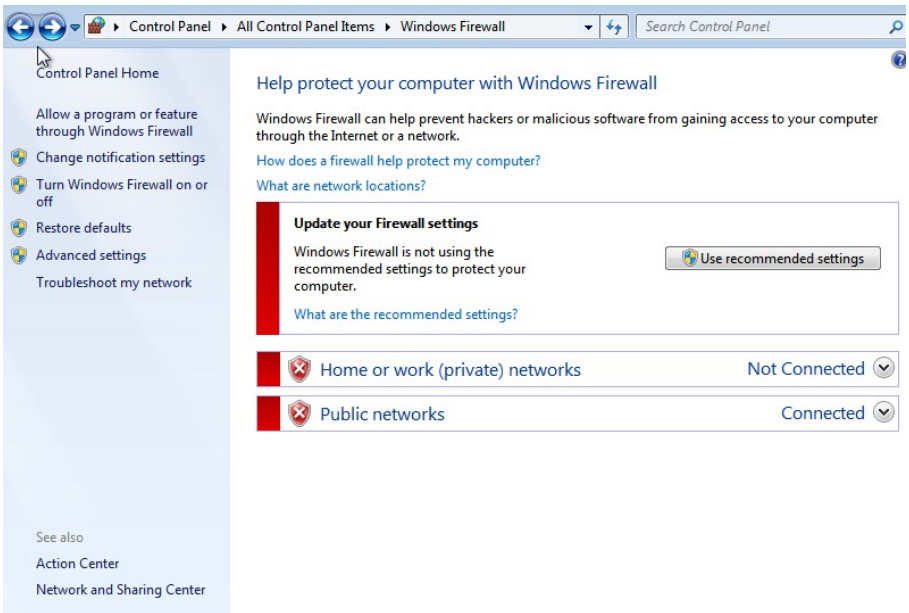

Figure 10 - firewall not up to date

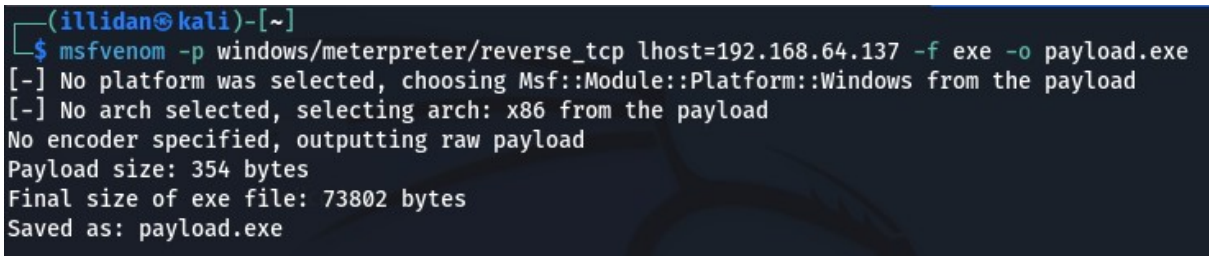

Figure 11 - msfvenom payload

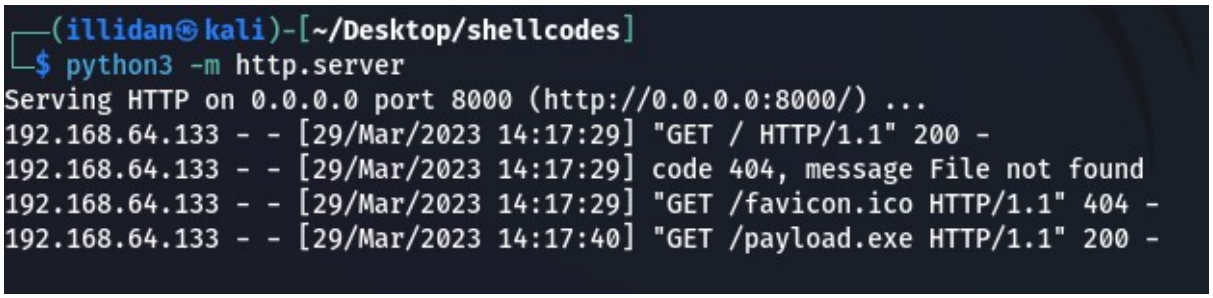

Figure 12 - python HTTP server

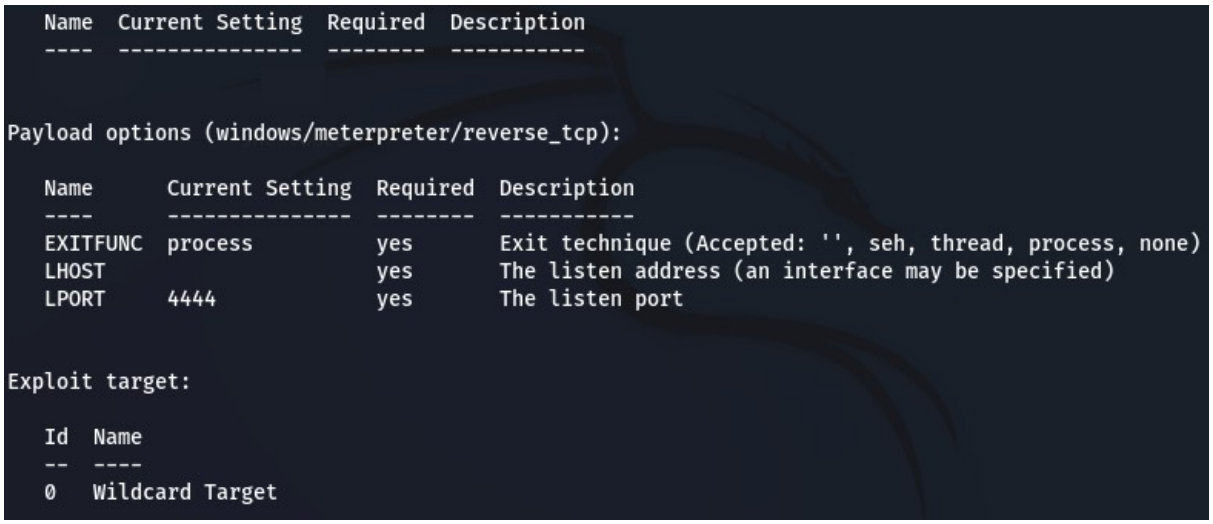

Figure 12 - Metasploit exploit being used

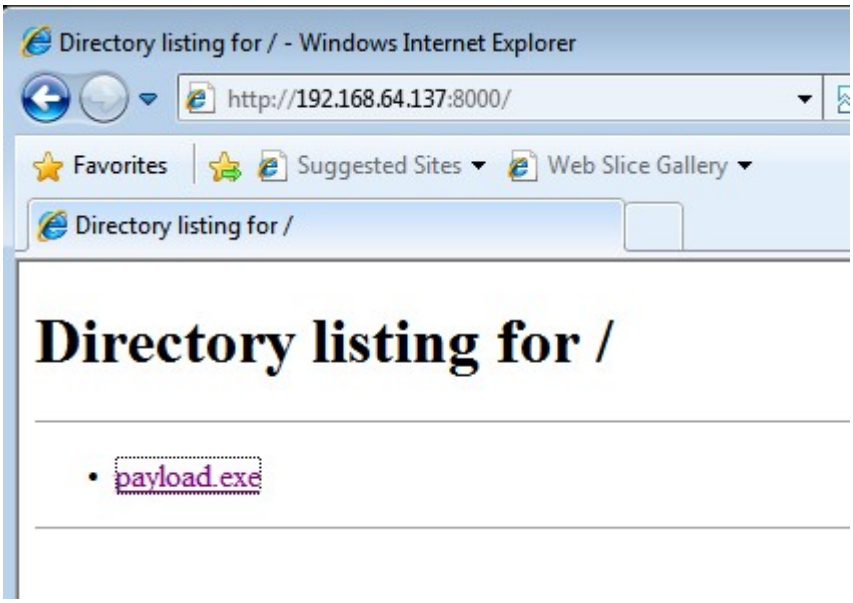

Figure 13 - the HTTP server running

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.64.137:4444
[*] Sending stage (175686 bytes) to 192.168.64.133
[*] Meterpreter session 3 opened (192.168.64.137:4444 -> 192.168.64.133:49168) at 2023-03-29 14:36:02 +0100

meterpreter >
```

Figure 14 - the reverse shell being established

Conclusion/Recommendation

Frozen Yoghurt permitted me to demonstrate that there could be security flaws in their Windows server. There are a variety of system issues, but I found only a few considered to be high, and that is all I could find in the time given.

I have some recommendations on what should be done to make sure the system is secure;

- Patching: Make sure all system applications are patched to the highest standard
- Securing Passwords: Make sure to implement passwords that are unique and long in character length to ensure they are not easily cracked
- Configure security application: Make sure all applications/security software is up to date and configured correctly
- Consult employees: keep employees up-to-date with security issues that could possibly affect them.

Having the company implement these security measures will allow the system to be the most secure it can be; if they keep it this way, the system will constantly be at its most secure. this would make their customers feel a lot more secure with letting you hold there data.

References

CWE - CWE-1391: Use of Weak Credentials (4.9). (n.d.). Cwe.mitre.org. https://cwe.mitre.org/data/definitions/1391.html

NVD - CVE-2017-0143. (n.d.). Nvd.nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2017-0143

CWE - CWE-521: Weak Password Requirements (4.1). (n.d.). Cwe.mitre.org. https://cwe.mitre.org/data/definitions/521.html

CWE - CWE-1392: Use of Default Credentials (4.10). (n.d.). Cwe.mitre.org. https://cwe.mitre.org/data/definitions/1392.html

CWE - CWE-770: Allocation of Resources Without Limits or Throttling (4.8). (n.d.). Cwe.mitre.org. https://cwe.mitre.org/data/definitions/770.html