Frozen Yoghurt Ltd

Penetration Testing Report 2

UP2009045

Table of Contents

[Executive Summary 2](#_Toc101791806)

[Summary of Results 2](#_Toc101791807)

[Attack Narrative 3](#_Toc101791808)

[KDC Enumeration (kerbrute 1.0.3) 4](#_Toc101791809)

[ASREPRoasting (Impacket v0.9.24) 4](#_Toc101791810)

[Accessible credentials 5](#_Toc101791811)

[NTLM dump 6](#_Toc101791812)

[Shell Injection / pass the hash 6](#_Toc101791813)

[Conclusion 7](#_Toc101791814)

[Recommendations 8](#_Toc101791815)

[Appendix 9](#_Toc101791816)

[Vulnerabilities 9](#_Toc101791817)

[Figures 9](#_Toc101791818)

[References 10](#_Toc101791819)

# Executive Summary

I have been contracted by Frozen Yoghurt Ltd to conduct penetration testing on two web servers with the purpose of revealing any vulnerabilities. Actions conducted to collect these results were done so with the aim to replicate a malicious attack on Frozen Yoghurt Ltd. The goals of this investigation include:

* Determining if and how the attacker can penetrate Frozen Yoghurt Ltd’s network.
* Impact of the security breach, i.e., confidentiality and availability of company data

With the focus of this being identification of vulnerabilities and exploitable weaknesses, all attacks were made as if an adversary, i.e., someone who does not have access to the network, were to attempt to attack the client network. Also find that investigation of Frozen Yoghurt Ltd’s web servers were performed within a controlled environment, thus, to limit risk.

## Summary of Results

During the reconnaissance phase of Frozen Yoghurt Ltd’s network, open ports within the network led to the discovery of a misconfigured Key Domain Controller (KDC). This KDC openly provided the local domain name and, further examination using enumeration software and a simple wordlist containing common usernames allowed for the identification of users on the domain. This information was then used to exploit the KDC and gain access to the svc-host password hash which was then decrypted using common password wordlist.

Logging into the backup share on the samba server with these credentials revealed a text document containing credentials for another user. These credentials were stored in the base64 format and required no additional security keys to decrypt. These credentials were then used to retrieve NTLM hashes containing usernames and passwords of all users who have access to the server.

Using one of these NTLM hashes, a shell was injected into the server using administrative credentials. This made it possible to gain administrative access to the web server along with all system contents and complete administrative control.

# Attack Narrative

Frozen Yoghurt Ltd provided a single IP address with no further information, this was to ensure the actions conducted during the investigation strictly imitated those of an adversary with no additional information of the internal network or its systems.

Text

Description automatically generated

Figure 1 – Open ports on system

To understand the network structure, a port scan was conducted, Figure 1, revealing the local domain spookysec.local, several open ports and services indicating a windows server using active directory and Kerberos, further indicating that this could be a KDC.

## KDC Enumeration (kerbrute 1.0.3)

Text

Description automatically generated

Figure 2 – Active Directory Username Enumeration

Following the discovery of Kerberos on the webserver, I used Kerbrute enumeration software, Figure 2, to brute force valid username credentials from the KDC using a basic username wordlist. These results return three notable usernames: administrator, svc-admin, backup.

## ASREPRoasting (Impacket v0.9.24)

Found from the KDC, the svc-admin user can be used to query a ticket from the KDC as it does not require pre-authentication from the server.

Text

Description automatically generated

Figure 3 -Kerberos Pre-Authentication Exploit

Using the impacket toolkit, the ASREP hash for svc-admin was returned after querying the KDC, Figure 3. This hash contains the account password in a format which can be decrypted.

Text

Description automatically generated with medium confidence

Figure 4 – Decrypted hash using John the Ripper

Feeding the hash into a password cracker, e.g., hashcat, svc-admin’s password was decrypted to reveal “management2005”, Figure 4. From here it was possible to gain unauthorised access to the samba server.

## Accessible credentials

Text

Description automatically generated

Figure 5 – User credentials stored in samba share

Listing server shares using the svc-admin account returned the sharenames, further logging into the backup share which matched a valid login username exposed the “backup\_credentials.txt” file, Figure 5.

Graphical user interface, text

Description automatically generated

Figure 6 – Decrypted user credentials

This file contained a base64 hash, when decrypted provided password details to the backup user “backup2517860, Figure 6.

## NTLM dump

A screenshot of a computer

Description automatically generated with medium confidence

Figure 7 – Dumped NTLM hashes

With backup credentials, the account was used to dump NTLM hashes and Kerberos keys from the system, Figure 7. This method gets the domain user list then calls DRSGetNChanges() on the system and replicates user hashes and Kerberos keys.

## Shell Injection / pass the hash

Text

Description automatically generated

Figure 8 – Injected shell substituting password for user hash (pass the hash)

This NTLM hash has already been stored on the system meaning it can be used again for password authentication, Figure 8. PSExec is used to both inject an interactive shell and initiate a pass the hash attack using credentials provided which successfully gave administrative access to the system.

# Conclusion

Frozen Yoghurt Ltd experienced multiple instances where their system failed, and sensitive information was accessed. This led to complete administrative access of the system which would be detrimental if this was a malicious adversary. Vulnerabilities of the system are not helped by the passwords used as they are common and proved to be easy to crack along with credentials being easily accessible and stored using easily crackable formats.

* Determining if and how the attacker can penetrate Frozen Yoghurt Ltd’s network.
* Impact of the security breach, i.e., confidentiality and availability of company data

The original goals of the investigation, stated above, were completed during this investigation. Frozen Yoghurt Ltd’s network was fully enumerated and exploited with the impact of the security breach supplying usernames, password, and complete access to system files, note that most of the access was gained via inadequately secured files.

# Recommendations

The following recommendations are to be made due to the potential impact found from this investigation.

1. Implement and enforce strong password policy across organisation

Frozen Yoghurt Ltd was severely affected by the lack of password security. Following the NIST recommended password guidelines (Poza, 2021) is greatly recommended for creating a company password policy.

1. Safe Storage of Credentials

(Poza, 2021) also details the safe storage of credentials, a main area which lead to complete compromise of the Frozen Yoghurt Ltd web server. Current password hashes stored on the server were stored using simple hashing algorithms, e.g., Base64. It is recommended for the highest level of security hashes be generated with salts stored separately, therefor brute force attacks will prove impractical.

1. Conduct regular vulnerability assessments

To further prevent vulnerabilities being exploited, regular penetration testing is important and should be implemented. This will help monitor the security of the webserver and company’s systems checking that they are not currently vulnerable. Guidelines for risk assessment can be found here: (NIST, 2020; Ross, 2012).

1. Enable Kerberos Pre-Authentication

Enabling Kerberos Pre-Authentication will eliminate the possibility for ASREPRoasting the svc-admin account.

# Appendix

## Vulnerabilities

|  |  |  |
| --- | --- | --- |
| Vulnerability | Explanation | CVE or CWE |
| KDC Enumeration | Brute forcing allows adversaries to enumerate valid usernames from active directory. | (*NVD - CVE-2008-5112*, n.d.) |
| ASREPRoasting | Misconfigured active directory accounts with pre-authentication disabled allowing for the KDC TGT to be retrieved which includes the user password. | (*NVD - CVE-2020-17049*, n.d.) |
| Accessible Credentials | Account credentials, username, and password stored in an easily accessible area of the server. Credentials insufficiently protected, file not encrypted, password stored in base64 hash type. | (CWE-522: Insufficiently Protected Credentials, 2006) |
| NTLM Hash Dump | Unprotected account credentials allowed hash dump for all users on the system. | (*NVD - CVE-2016-3352*, n.d.) |
| Shell Injection / Pass the hash | NTLM hash used in place of a password to gain access to Administrator account. Server compares hashes and does not require password as the hash matches hash on server. | (*CWE - CWE-836: Use of Password Hash Instead of Password for Authentication (4.6)*, n.d.) |

## Figures

[Figure 1 – Open ports on system 3](#_Toc101791834)

[Figure 2 – Active Directory Username Enumeration 4](#_Toc101791835)

[Figure 3 -Kerberos Pre-Authentication Exploit 4](#_Toc101791836)

[Figure 4 – Decrypted hash using John the Ripper 4](#_Toc101791837)

[Figure 5 – User credentials stored in samba share 5](#_Toc101791838)

[Figure 6 – Decrypted user credentials 5](#_Toc101791839)

[Figure 7 – Dumped NTLM hashes 6](#_Toc101791840)

[Figure 8 – Injected shell substituting password for user hash (pass the hash) 6](#_Toc101791841)

# References

*CWE - CWE-836: Use of Password Hash Instead of Password for Authentication (4.6)*. (n.d.). Retrieved April 14, 2022, from https://cwe.mitre.org/data/definitions/836.html

CWE-522: Insufficiently Protected Credentials. (2006). *No Title*. https://cwe.mitre.org/data/definitions/522.html

NIST. (2020). *NIST SP 800-30 | NIST*. https://www.nist.gov/privacy-framework/nist-sp-800-30

*NVD - CVE-2008-5112*. (n.d.). Retrieved April 20, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2008-5112

*NVD - CVE-2016-3352*. (n.d.). Retrieved April 20, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2016-3352

*NVD - CVE-2020-17049*. (n.d.). Retrieved April 20, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2020-17049

Poza, D. (2021). *NIST Password Guidelines and Best Practices for 2020*. January. https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/

Ross, R. S. (2012). Guide for Conducting Risk Assessments. *Special Publication (NIST SP) - 800-30 Rev 1*, *September*, 95. https://doi.org/10.6028/NIST.SP.800-30r1