Logo, company name

Description automatically generated

**Penetration Testing Report**

Ethical Hacking

Company:

**Frozen Yoghurt LTD**

**Date:** 31/03/2023

**Table of Contents:**

**Executive Summary:**

**Summary of Findings:**

**Vulnerability Findings of Linux Server:**

[CVE-2017-7494](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494): Arbitrary shared library load vulnerability.

Attack Narrative

CVE-2009-3548- Exploits default passwords for the admin user.

Attack Narrative

CWE-250: Execution with Unnecessary Privileges allowing Local Privilege Escalation

Attack Narrative

CVE-2015-1328- OverlayFS local Privilege Escalation.

Attack Narrative

CWE-521 ‒ Use of weak passwords

Attack Narrative

**Conclusion:**

**Recommendations:**

**References:**

**Executive Summary:**

This Penetration Test was performed on Frozen Yougert Ltd. The purview of this investigation was restricted to a local machine running their linux OS and its IP address. The Intention of this Penetration Test was to Identify and exploit vulnerabilities within the target system with the aim to access sensitive information.

Each Vulnerability found and exploited was completed in three critical phases: Reconnaissance, Enumeration and Exploitation.

Reconnaissance involves the scanning of each system to recognize open ports and what services are running on each. Enumeration involves finding out more information about these open ports, including the service version of each, which can lead an investigator to known vulnerabilities. And finally, Exploitation involves multiple techniques found in the prior phases that are used to gain access to the system in order to disclose sensitive information.

**Summary of Findings:**

Within the first phase of this Penetration Test, Reconnaissance, many open ports were found with vulnerable services running. Such as Apache Tomcat running on port 8080. The Diagram below shows I managed to exploit a vulnerability within the login manager.

Diagram

Description automatically generated

**Figure 1 –** Phases of Tomcat exploit

This is a similar pattern throughout the entire Penetration process of this Linux target, through a nmap scan it is able to find the Samba daemon running on the linux target, and that is vulnerable to a shared library vulnerability, which gains us access incidental to the whole machine. I discovered several more vulnerabilities within the local target machine, including a file which allows unprivileged users to escalate their privileges, as well as the actual OS version being vulnerable to another privilege escalation and a startup repair vulnerability.

****

**Vulnerabilities Within Windows Machine**

| [**CVE-2017-7494**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494)**:** Arbitrary shared library load vulnerability | | |
| --- | --- | --- |
| **RISK/ CVS:** | **CRITICAL** | **9.8** |
| **TOOLS:** | Metasploit v6, Nmap v7.93 | |
| **Description:** | The Samba is\_known\_pipename() module is vulnerable to an Arbitrary Module Load library attack, which allows an attacker to supply a malicious DLL file that aims to a malicious DLL file. | |
| **Impact:** | This vulnerability can lead to the complete compromise of the system, allowing an unauthenticated attacker to gain root privileges, giving them complete access to all sensitive information within. | |
| **Recommendation:** | Apply the latest Security Patches in which samba have released (v 4.18.0) or disable/restrict access to names pipes. | |

**Attack Narrative:**

After performing a network scan using nmap (**Figure 1),** the service netbios-ssn was found to be open, which is typically found on Windows machines but can be installed on linux machines with the software ‘Samba’, it's used to share and communicate with other Windows machines and commonly printers on a network. Using the ‘Samba is known pipename’ metasploit module, I can get root access into the linux server, allowing me to have complete authority over the system, with all files being compromised.

**Text

Description automatically generated**

**Figure 1 -**  Showing the Service and Version for port 445

**A screenshot of a computer

Description automatically generated**

**Figure 2 -** Linux Machine being exploited using metasploit software.

| **CVE-2009-3548:**  Exploits default passwords for the admin user | | |
| --- | --- | --- |
| **RISK/ CVS:** | **Medium** | **7.5** |
| **TOOLS:** | Metasploit v6, Nmap v7.93, Nikto v2.1.6 | |
| **Description:** | Versions 6.0 - 3.0 use blank default passwords host manager web application for the administrative user which is installed with installed with apache tomcat | |
| **Impact:** | Allows remote attackers to gain privileges and access to underlying system and its information | |
| **Recommendation:** | Change the default passwords for the web application which to meet the requirements of Digital Identity Guidelines (NIST SP 800-63B), or remove the host manager application if it’s not being used. | |

**Attack Narrative:**

Apache Tomcat is a Java based open-source web server, like any installed software which comes with login systems, it often comes with default passwords for users, which can be vulnerable like in this use case. Using Nikto (**Figure 2)**, I was able to enumerate a number of directories under the port 8080 web-server, one of which is a login pop-up. Using the now known username and passwords from this metasploit module, we can take advantage of an exposed /manager/ webpage and execute an arbitrary code payload, we can gain access to a shell.

**Graphical user interface, text, application, chat or text message

Description automatically generated**

**Figure 1 -** Nmap Scan showing port 8080 running Apache tomcat.

**Graphical user interface

Description automatically generated with medium confidence**

**Figure 2 -** A directory scan performed by Nikto shows a ‘/manager/’ webpage.

**Graphical user interface

Description automatically generated**

**Figure 3 -** Login Page under ‘/manager/’

**A screenshot of a computer

Description automatically generated with medium confidence**

**Figure 4 -** A dictionary attack using default credentials of tomcat service performed by a metasploit module.

**Text

Description automatically generated**

**Figure 5 -** Gaining access to a meterpreter shell.

**Text

Description automatically generated**

**Figure 6 -** Proof of shell access; gained access to tomcat user.

| **CWE-250:** Execution with Unnecessary Privileges | | |
| --- | --- | --- |
| **RISK/ CVS:** | **High** | **8.1** |
| **TOOLS:** | HxD v2.5.0, Python v3.9 | |
| **Description:** | The File ‘Process Checker’ has improper privilege management, allowing a user to modify the command within the file, while keeping the SUID bit. | |
| **Impact:** | The entire system is compromised, allowing the attacker to execute any system command. Meaning all system information integrity is compromised. | |
| **Recommendation:** | Delete the ‘Process Checker’ file, and make sure any other files do not allow users with low permissions to complete actions for a SUID bit. | |

**Attack Narrative:**

The ‘Process Checker’ File allowed a user with basic level privileges to execute the file and type in a term in which the file would search for the process if it was being run. When looking at that file in a hex editor (I SCP’d the file out to my host machine with -p to preserve file permissions) I realised the command inside it could be changed, the command originally was ‘**ps aux | grep process name**’. And I changed it to ‘**Python privesc.py**’ where privesc.py is a python file with the command to add the user frozen into the sudoers file (**Figure 2**). The reason I used Python instead to execute a file instead of putting the command directly in the file, is due Python keeping the SUID bit (without using I would get a Lack of Permissions error). After SCP the new process checker (Still with permissions) back onto the frozen account, I made the file executable with ‘chmod +x’ and ran it (**Figure 3)**. After it's finished it has added my account to sudoers giving me complete access to the whole system. (**Figure 4**).

**Text

Description automatically generated**

**Figure 1 -** The Hex View of the ‘Process Checker’ file with the edit made ‘python privecs.py’

**Text

Description automatically generated**

**Figure 2 -** The contents of Privesc.py

**Text

Description automatically generated**

**Figure 3 -** The execution of the new ‘Process Checker’ and sudo privileges on frozen

**A screenshot of a computer

Description automatically generated with medium confidence**

**Figure 4 -** Proof of sudo Privileges on Frozen user account

| [**CVE-201**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494)**5-1328:**  OverlayFS vulnerability allows privilege escalation. | | |
| --- | --- | --- |
| **RISK/  CVS:** | **Medium** | **7.2** |
| **TOOLS:** | Python v3.6, GCC Compiler | |
| **Description:** | Due to overlayfs not properly checking permissions for file creation, allows normal users to gain root access. | |
| **Impact:** | Allows users with no privileges on a system to gain root privileges, meaning all system files and data is compromised | |
| **Recommendation:** | Disable overlayfs within linux or update your linux distribution to any version above 15.04. | |

**Attack Narrative:**

This version of Ubuntu is vulnerable to the overlayfs privilege escalation. This particular exploit allows any user to gain root privileges by running a small bit of C code. The way I got the exploit onto the linux machine was by setting up a Python Web server on my host machine within the directory of the exploit with the command ‘**Python -m http.server [port]** ’ and then downloading the exploit using ‘**wget’** and then the IP address then file path.

After compiling and running ‘./exploit’ I have now gained root privileges, which means files like ‘etc/shadow’ and ‘etc/psswd’ are now privy to being accessed and possibly broken further down the line.

**Text

Description automatically generated**

**Figure 1 -** The Ubuntu Version running on the Linux Version Machine

**Text

Description automatically generated**

**Figure 2 -** Showing the privileges of the user ‘Frozen.’

**Text, chat or text message

Description automatically generated**

**Figure 3 -** Compiling the exploit and running it, then showing the access has changed to root.

| **CWE-521** ‒ Use of weak passwords | | |
| --- | --- | --- |
| **RISK/  CVS:** | **Medium** | **5.5** |
| **TOOLS:** | John The Ripper v1.9.0 | |
| **Description:** | Users of the policy are not required to use secure passwords, which makes it simpler for attackers to access user accounts. | |
| **Impact:** | The acquired hashes are able to be cracked through a dictionary attack, with the first hash being cracked in under 30 seconds. This ultimately leads to sensitive information being accessed. | |
| **Recommendation:** | Make sure all users on the machine change their passwords to meet Digital Identity Guidelines (NIST SP 800-63B) | |

**Attack Narrative:**

These hashes were retrieved from ‘/etc/psswd’ and ‘/etc/shadow’. Using the ‘unshadow’ command I combined both into one file called ‘hashes’. The hashes stored in the shadow file are SHA512, one of the strongest hash types, but it is still susceptible to a dictionary attack. I used the rockyou.txt dictionary which contains over 14,000,000 passwords. Three Passwords were broken out of the possible 5 hashes retrieved from the shadow file. One of which has root privileges (Admin).

**Graphical user interface

Description automatically generated with medium confidence**

**Figure 1 -** Using John the Ripper to crack the hashes.

**Conclusion**

This Penetration test on the Frozen Yougert Linux Machine found numerous dangerous vulnerabilities that endanger the company’s security and data, these include vulnerabilities but are not limited to using default credentials for services which have access to sensitive data, having files with dangerous privilege management and having significantly out of date software versions.

I highly recommend using the following recommendations otherwise a bad actor may exploit these vulnerabilities and have access to your sensitive data.

**Recommendations**

* Make sure the Digital Identity Guidelines (NIST SP 800-63B) format is compulsory for all new users and change all passwords of current users to meet this requirement. Also change all services running which use passwords to fulfill this requirement.
* Update the machine to the newest OS version (Ubuntu 22.04)
* Disable any open ports which are not actively used frequently.
* Follow the NIST Special Publication 800-53 guidelines to ensure privilege management is obeyed.
* Update all versions of software running on this machine to their latest release patch.

**References:**

*Apache Tomcat Manager Authenticated Upload Code Execution*. (n.d.). Rapid7. https://www.rapid7.com/db/modules/exploit/multi/http/tomcat\_mgr\_upload/

*CVE - CVE-2015-1328*. (n.d.). Cve.mitre.org. Retrieved March 24, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1328>

*CVE - CVE-2017-7494*. (n.d.). Cve.mitre.org. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494>

*CVE-2009-3548 : The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a*. (n.d.). Www.cvedetails.com. Retrieved March 24, 2023, from <https://www.cvedetails.com/cve/CVE-2009-3548/>

*CVE-2015-1328 : The overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does no*. (n.d.). Www.cvedetails.com. <https://www.cvedetails.com/cve/CVE-2015-1328/>

*CWE - CWE-250: Execution with Unnecessary Privileges (4.6)*. (n.d.). Cwe.mitre.org. https://cwe.mitre.org/data/definitions/250.html

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

NIST. (2019). *NIST Special Publication 800-63B*. Nist.gov. <https://pages.nist.gov/800-63-3/sp800-63b.html>

NIST. (2020, September 23). *Security and Privacy Controls for Information Systems and Organizations*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

rebel. (2015, June 16). *Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - “overlayfs” Local Privilege Escalation*. Exploit Database. https://www.exploit-db.com/exploits/37292

National Institute of Standards and Technology. (n.d.-b). *NVD - CVSS v3 Calculator*. Nvd.nist.gov. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator