UP891784 Ethical Hacking CW: Frozen Yoghurt Ltd

Frozen Yoghurt Ltd: Penetration Testing Report of Server:

TABLE OF CONTENT:

Server 1:

Executive Summary:

Frozen Yoghurt Ltd requested a penetration test due to the exponentially increasing global risk of weak cyber security within business websites and computer architecture. Many vulnerabilities were found in the attack performed, ranging from low severity to even a severity rating of 8.8/10; due to the amount of vulnerabilities found this report will focus on the top 5 that need to be addressed. Often by fixing the highest level vulnerabilities the low severity risks become obsolete - due to a complete upgrade in operating system/server changing the entire computer architecture environment.

Summary of Results:

Even though the vulnerabilities available on server 1 can lead to privilege escalation and eventually full root access control with all admin permission, they are surprisingly easy to rectify. The main issue with this server is that the software running in every area is largely depreciated and requires updating. Updating all software to its latest form and ensuring it continues to do so will ensure security.

Methodology (Initial Server Information Gathering):

- Ran nmap scan of all ports (0 - 65535)

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-89-57:~# nmap -A -T4 -p- -vvv $ip
```

```
Reason: 65527 resets
PORT      STATE SERVICE     REASON         VERSION
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 23:b1:3a:6a:0b:9e:a7:92:ae:f6:f6:36:35:b8:b8:72 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDQ9jIcIJFFWQxw+VT8FDS1QYYMG01RnSqftXkO1qG7stCoa6EBC+1iSc+7hIsUQrSGOOmGiN/DwvT7iBIMe8AWqPG6Wpws1eGFWrt5tRR5SNOsyDUSRIMDcF7/GjfVgdqTvB8lijo
GfdjVmtaBISq/1GXolQ9wIvzIRtVF2RxyZbAVHzW/CIIvMO0vH4ORFkWqf5QEeOvdCJU4qrPieSzKC2YQjXNHVFxdit2B3KwaXxbfGMm/QjpMFMTdIQqw8EmVR40t2rU1N9ZUNMnV0t1yyx+tyPE/6gf3Tw8I4YJ3vCsx2v5MdaFhBXXS
9dNRN7Psi75aC1oEjNQcQCIp4Q1p
|   256 0b:73:d6:46:f7:9f:ef:18:c8:eb:30:51:5f:3f:d8:87 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHPXcW0wGT/Yh+0wD+zIS/b73dOcEYyVSZgHn7Nj1pnRBpajBL2e9CHJp92tR+g969l91v+PGIOke4GFnA09Kl4=
|   256 be:a3:2a:de:0d:ac:39:fb:4c:01:c0:10:ae:f1:5a:73 (EdDSA)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILbnh6LuQPNKAQqqi0SB1fRRgubnX/H5dUl6FbWi+IUr
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
|_smtp-commands: server, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=server
| Issuer: commonName=server
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-02-24T21:35:52
| Not valid after:  2030-02-21T21:35:52
| MD5:   49ea 9e0a a453 bb35 e4f4 c7e8 1962 15ff
| SHA-1: 9973 eec2 c26a b71c b1e0 1506 9728 11ce 4a98 95f6
| -----BEGIN CERTIFICATE-----
| MIICsjCCAZqgAwIBAgIJAOpXLmPguNPCMA0GCSqGSIb3DQEBCwUAMBExDzANBgNV
```

```
|_ssl-date: TLS randomness does not represent time
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.10.3-P4-Ubuntu
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
110/tcp   open  pop3        syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: TOP CAPA UIDL AUTH-RESP-CODE SASL RESP-CODES PIPELINING
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        syn-ack ttl 64 Dovecot imapd
|_imap-capabilities: SASL-IR more LITERAL+ Pre-login ENABLE capabilities post-login listed IMAP4rev1 IDLE ID LOGINDISABLEDA0001 LOGIN-REFERRALS have OK
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
```

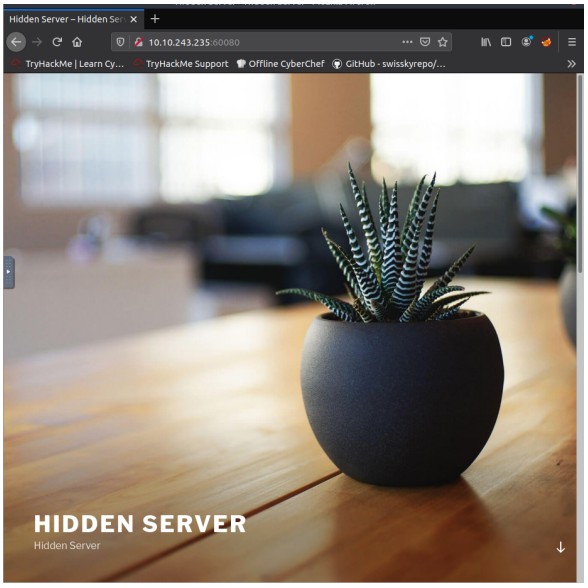
```
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.10.3-P4-Ubuntu
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
110/tcp   open  pop3        syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: TOP CAPA UIDL AUTH-RESP-CODE SASL RESP-CODES PIPELINING
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        syn-ack ttl 64 Dovecot imapd
|_imap-capabilities: SASL-IR more LITERAL+ Pre-login ENABLE capabilities post-login listed IMAP4rev1 IDLE ID LOGINDISABLEDA0001 LOGIN-REFERRALS have OK
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
60080/tcp open  http        syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 5.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Hidden Server &#8211; Hidden Server
MAC Address: 02:33:8C:5E:15:AB (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
```

- discovered open ports [22, 25, 53, 110, 139, 143, 445 and 60080].

- continued to enumerate using enum4linux

```
 ==========================================
|    Share Enumeration on 10.10.243.235    |
 ==========================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (server server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SERVER

[+] Attempting to map shares on 10.10.243.235
//10.10.243.235/print$  Mapping: DENIED, Listing: N/A
//10.10.243.235/IPC$    [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

- nothing interesting was found
- looked into http service on port 60080

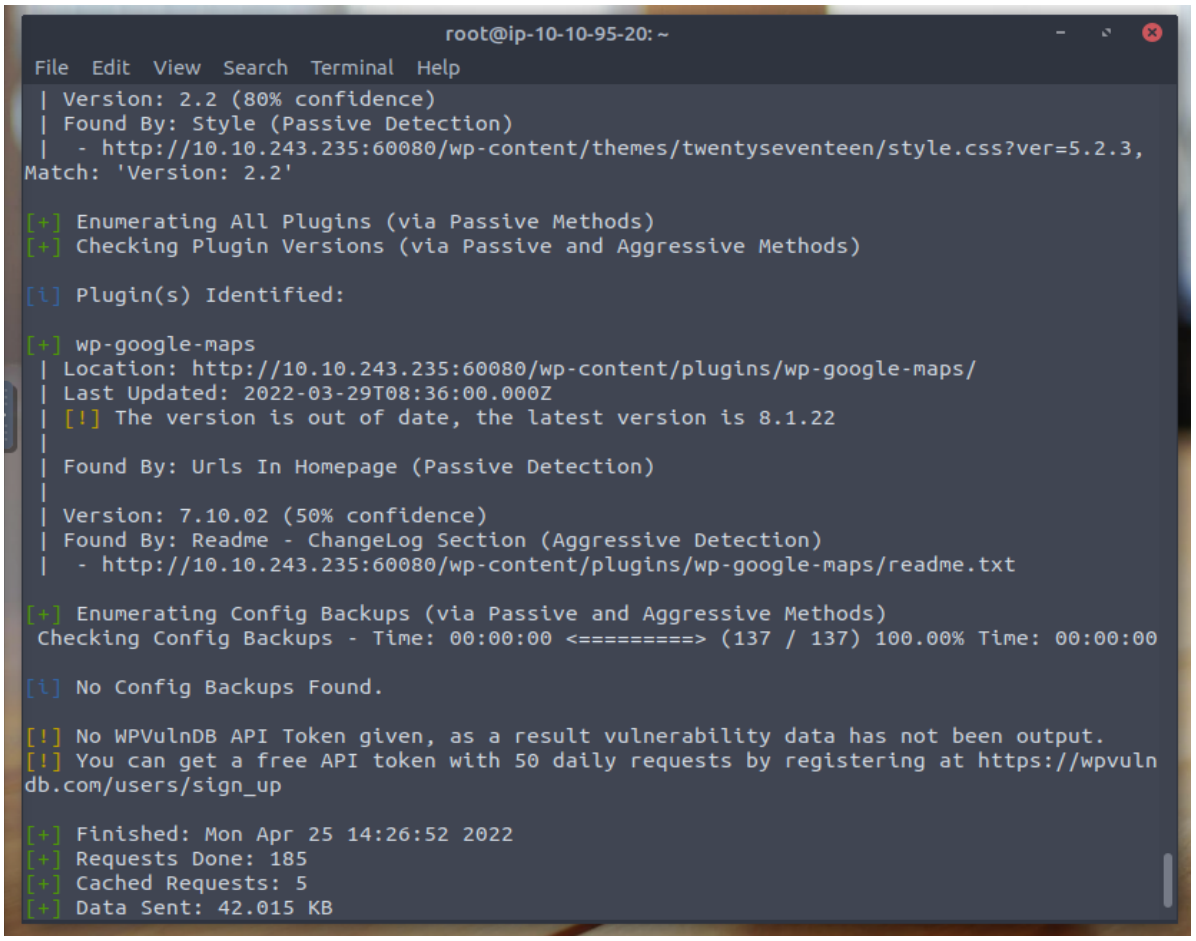


- presented with “hidden server”: a wordpress site

- run a wordpress scan for vulnerabilities [wpscan –url http://ip-address:60080]

```
[+] URL: http://10.10.243.235:60080/ [10.10.243.235]
[+] Started: Mon Apr 25 14:26:46 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.243.235:60080/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://10.10.243.235:60080/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

```
root@ip-10-10-95-20: ~
File  Edit  View  Search  Terminal  Help

[+] WordPress version 5.2.3 identified (Insecure, released on 2019-09-05).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.10.243.235:60080/?feed=rss2, <generator>https://wordpress.org/?v=5.2.3</
generator>
 |  - http://10.10.243.235:60080/?feed=comments-rss2, <generator>https://wordpress.org/?
v=5.2.3</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://10.10.243.235:60080/wp-content/themes/twentyseventeen/
 | Last Updated: 2022-01-25T00:00:00.000Z
 | Readme: http://10.10.243.235:60080/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.243.235:60080/wp-content/themes/twentyseventeen/style.css?ver
=5.2.3
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersiv
e featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.243.235:60080/wp-content/themes/twentyseventeen/style.css?ver=5.2.3,
Match: 'Version: 2.2'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:
```

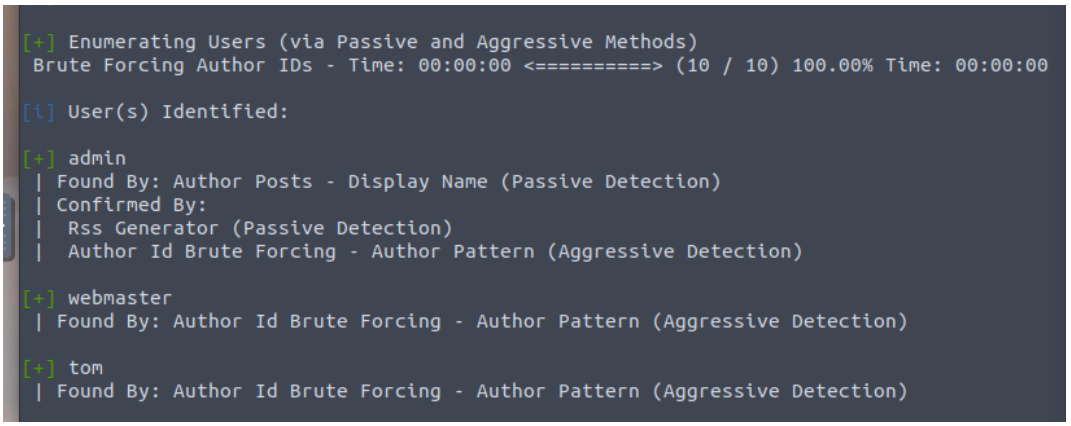


- from this single scan we can uncover various exploitable vulnerabilities!

- gobuster directory scan of the http server uncovered interesting directories:

```
root@ip-10-10-95-20:~# gobuster dir --url http://10.10.243.235:60080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.243.235:60080
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2022/04/25 14:34:35 Starting gobuster
===============================================================
/wp-content (Status: 301)
/wp-includes (Status: 301)
/javascript (Status: 301)
/backup (Status: 301)
/wp-admin (Status: 301)
/phpmyadmin (Status: 301)
/security_wp (Status: 301)
/server-status (Status: 403)
===============================================================
2022/04/25 14:34:52 Finished
===============================================================
```

-running wpscan -e (enumeration tag) –url http://ip-address:60080 outputs users identified on the system



Vulnerabilities:

-V1:
Samba SMB Server running a depreciated version of 4.3.11.

- V2:
Apache 2.4.18 HTTP server found from information gathering exposes the CVE-2019-0211 (https://nvd.nist.gov/vuln/detail/CVE-2019-0211) exploit.

Due to running this depreciated version of Apache, an attacker is able to allow low level child processes to execute arbitrary code with the privileges of the parent process. Therefore an attacker with control over extension modules; which is achievable due to the exposed directories which contain scripting files for the website.

CVE-2019-0211 Severity Rating: 7.8 HIGH

Risk Analysis:
High - due to authentication required to initiate processes, usernames are exposed via wpscan and thus given enough time a password cracker like hydra could eventually gain unauthorised access and then use this exploit to gain root access, since the usernames are exposed via a simple wpscan this is a high risk vulnerability that can be exploited.

Recommendation:
Update Apache to the latest version as outlined in the nist document as these vulnerabilities have been addressed and fixed in updates. You could evasively change the operating system to windows as this CVE only affects Unix systems however updating Apache would be less challenging to install.

- V3:
wp-google-maps is using a deprecated version of 7.10.02 which is highly susceptible to a SQL injection which can expose information from a database and lead to an escalation of privileges if passwords or password hashes are compromised.

https://www.exploit-db.com/exploits/44883

Risk Analysis:
High - Due to usernames and various directories being exposed, an attacker can search through to find the parameters to run a metasploit SQL injection module against the wordpress websites wp-google-maps and expose data that can lead eventually to a root access foothold by the attacker.

- V4:

- V5:
Wordpress 5.2.3 is exposed to a simple URL manipulation in which secret data can be exposed. The relevant NIST article CVE-**2019-17671**. The relevant exploit-db handle https://www.exploit-db.com/exploits/47690.

Due to Wordpress static query being mishandled an attacker can type "?static=1" at the end of a wordpress url to uncover private information such as drafts of pages and even possibly password information.

CVE-2019-17671 Severity Rating: 5.3 MEDIUM

Risk Analysis:
Low due to the information being exposed currently being useless for any privilege escalation that leads to root access.

Recommendations:
Upgrade Wordpress to 5.2.4 or higher where an update has addressed this bug, enable auto-updates for wordpress (https://www.wpbeginner.com/wp-tutorials/how-to-enable-automatic-updates-in-wordpress-for-major-releases/) as in the future as the site develops it may lead to expose secret data than can be exploited for privilege escalation.

- CONCLUSION AND RECOMMENDATIONS:

For the future of Frozen Yoghurt Ltd to progress without any issues in data breaches which can lead to ransom attacks and a loss of reputation and capital for Frozen Yoghurt Ltd it is recommended to upgrade all software specified in the vulnerabilities above.

References:

https://www.exploit-db.com
https://www.wpbeginner.com
https://www.nist.gov/

Server 2:

Executive Summary:

Summary of Results:

Methodology (Initial Server Information Gathering):

Vulnerabilities:
- V1:
- V2:
- V3:
- V4:
- V5:

- SUMMARY

- CONCLUSION AND RECOMMENDATIONS