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/.

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.

Resultados Clave:

Apache 2.4.7: Versión desactualizada con posibles vulnerabilidades conocidas.

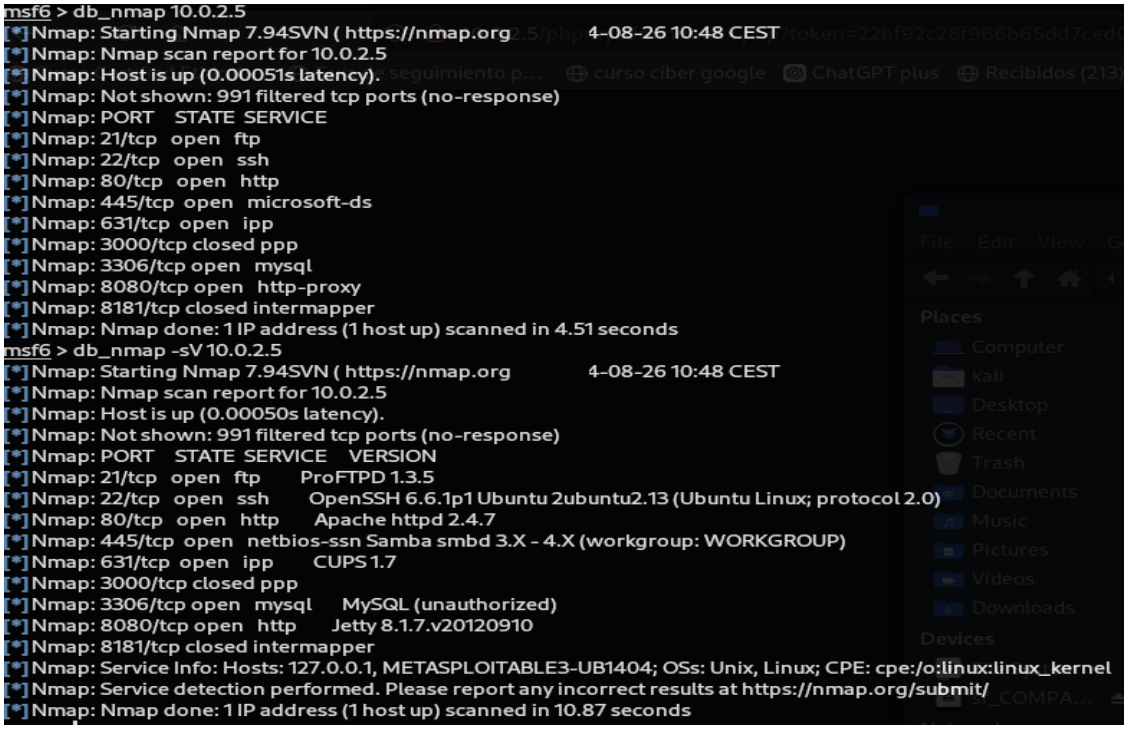
Directory Indexing Enabled: Posible exposición de archivos y directorios no deseados.

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:

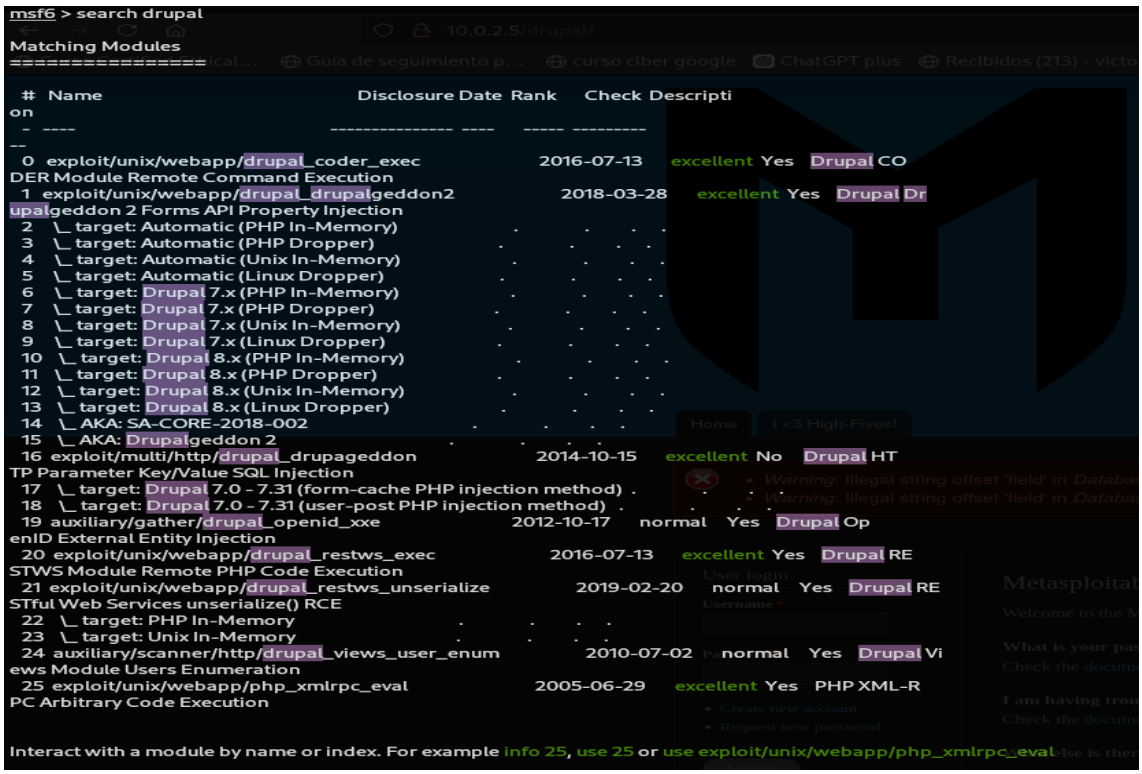


2.- Creación de un Workspace en Metasploit

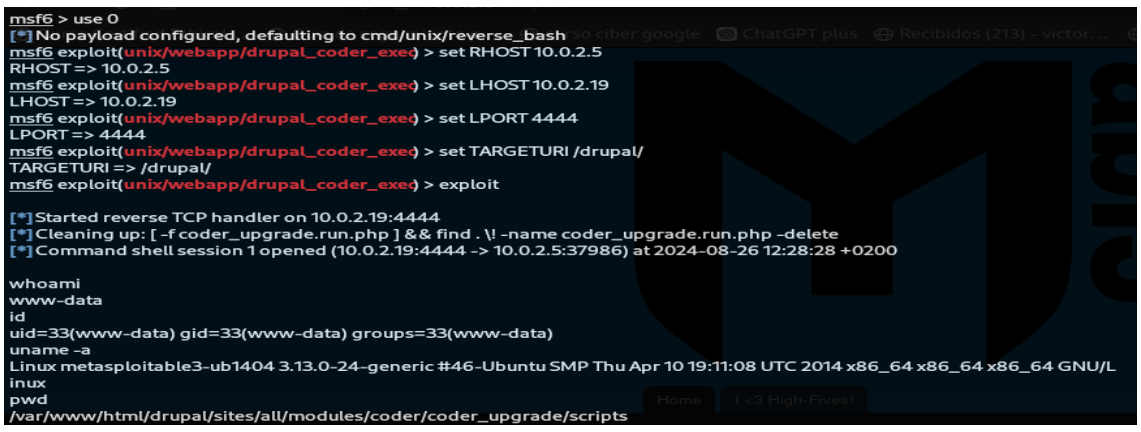
Para una gestión organizada del análisis, se creó un workspace específico en Metasploit llamado *meta3*, para poder centralizar la información y los resultados obtenidos durante las pruebas del objetivo.

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.



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.

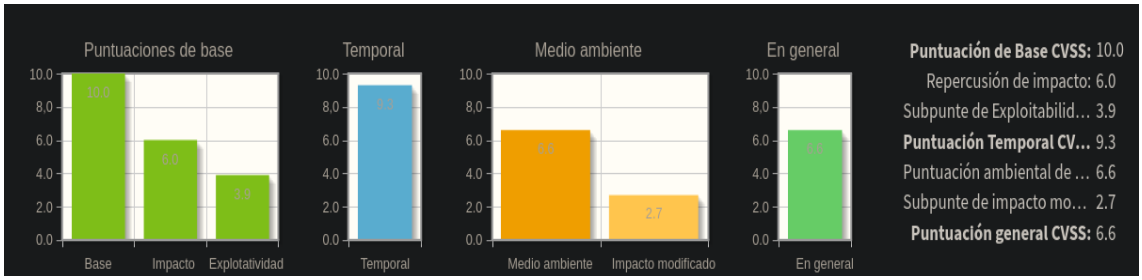


4.- Fase de Post-Explotación

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.