Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 6

Integrantes

Juan Camargo

Diego Castellanos

Profesor

Daniel Esteban Vela Lopez

Bogotá 2024

Resumen Ejecutivo

Juan Camargo y Diego Castellanos evaluamos la máquina "analytics" de Hack the Box mediante pruebas de testeo desde el 27 de febrero hasta el 4 de marzo de 2024. En la siguiente sección, se detallan las vulnerabilidades que descubrimos exitosamente durante la evaluación y además las *flags* que nos pide Hack the box.

Resumen del testeo

Al lograr establecer la conexión exitosa entre la máquina y nuestra instancia de Kali Linux, procedimos a acceder a la página web alojada en la máquina, disponible en http://analytical.htb/. Nuestra primera tarea fue buscar posibles vulnerabilidades que pudieran ser explotadas durante nuestra prueba de penetración.

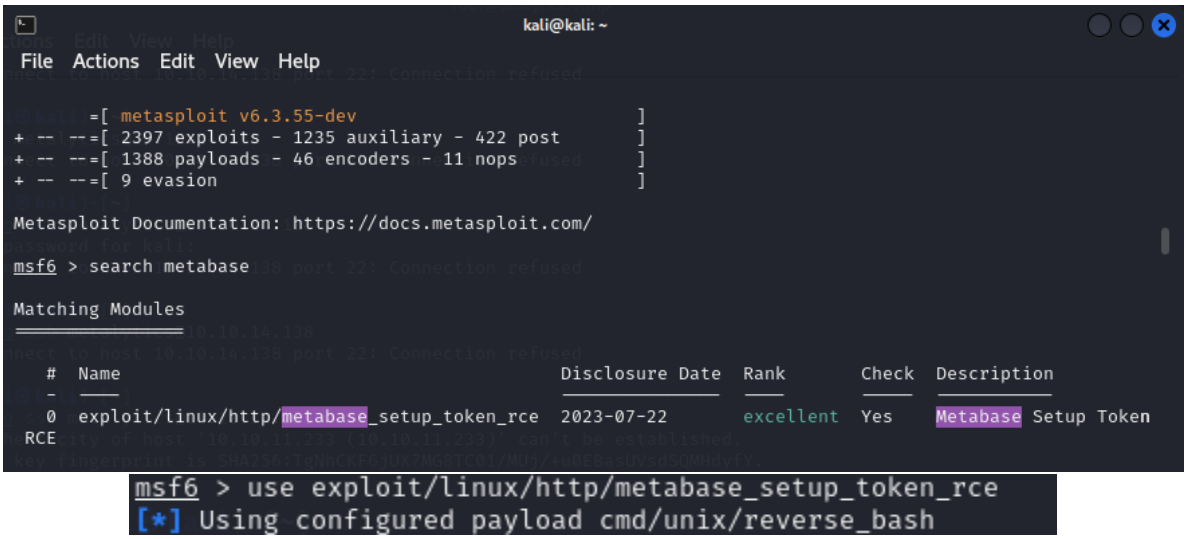
Identificamos una vulnerabilidad relacionada con CVE's asociadas a la plataforma empresarial Metabase, que diseñó el sistema de inicio de sesión. Esta vulnerabilidad, conocida como Pre-auth RCE (Ejecución Remota de Código previo a la autenticación), nos permitió ejecutar o inyectar comandos en la consola del servidor web. La explotación de esta vulnerabilidad se basó en la presencia de un Token (SETUP-TOKEN), generado al crear la instancia del inicio de sesión en la página web. Aunque este token debería eliminarse tras completar la configuración de la instancia, persistía en el sistema. Aprovechando este token, intentamos autenticarnos en un punto final de una API conectada a la base de datos de la empresa para realizar una inyección SQL y obtener credenciales de usuario y contraseña para acceder de forma remota al servidor mediante SSH.

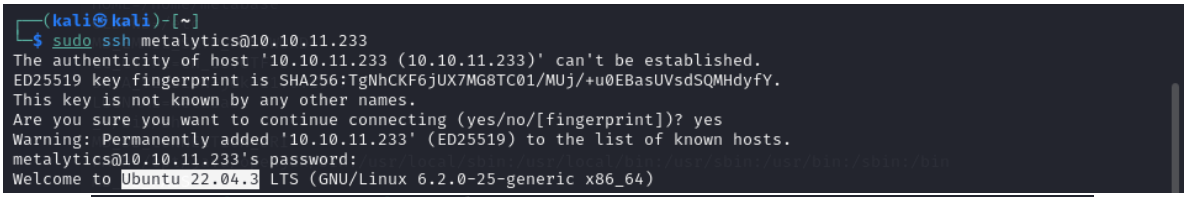
Una vez logrado este paso, localizamos fácilmente la primera bandera de Hack The Box y continuamos explorando posibles vulnerabilidades dentro del servidor. Descubrimos dos vulnerabilidades relacionadas con las CVE's vinculadas al sistema operativo del servidor Ubuntu 22.04.3, específicamente relacionadas con la función OverlayFS, que es una implementación de montaje sindical de sistema de archivos para Linux. Decidimos explotar esta vulnerabilidad, la cual permitía una escalada de privilegios dentro del servidor como si estuviéramos parados desde el root. Utilizamos un exploit previamente desarrollado el cual está diseñado para aprovechar una vulnerabilidad en metabase para lograr la ejecución remota de código en el sistema operativo obteniendo acceso a todos los archivos protegidos por permisos del servidor. Al explorar estos archivos, encontramos la segunda bandera, completando así nuestra prueba de penetración.

Hallazgos técnicos

Pruebas de penetración encontradas (PTF)

PTF-001: Pre-auth RCE (Ejecución Remota de Código previo a la autenticación) CVE-2023-38646





PTF-002: Vulnerabilidad de inyección SQL en el controlador de base de datos H2 (?)

La inyección SQL es una vulnerabilidad grave que puede permitir a los atacantes ejecutar comandos SQL no autorizados en la base de datos para poder exponer datos sensibles.

PTF-003: CVE-2023-2640 y CVE-2023-32629

Aquí se presentan vulnerabilidades de control de acceso inadecuados lo que permite a un usuario sin los permisos necesarios establecer atributos extendidos en los archivos que por lo normal deberían ser reservados para usuarios privilegiados.

Exploit

```
metalytics@analytics:/tmp$ nano exploit.sh
metalytics@analytics:/tmp$ chmod +x exploit.sh
metalytics@analytics:/tmp$ ./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:/tmp# whoiam
whoiam: command not found
root@analytics:/tmp#
root@analytics:/tmp#
root@analytics:/tmp# whoiam
whoiam: command not found
root@analytics:/tmp# cat ../../root/root.txt
53e74dc927e2a6ae64c72f503e4b6b39
```

Remediación

Después de identificar y explotar las vulnerabilidades en la máquina "analytics" de Hack The Box, recomendamos implementar medidas de remediación para mitigar los riesgos de seguridad.

Vulnerabilidad relacionada con Metabase PTF-001:

Refiere a una ejecución remota de código que permite a un atacante ejecutar código de forma remota en un sistema objetivo sin necesidad de autenticarse previamente. Esto significa que un atacante puede aprovechar esta vulnerabilidad para obtener acceso y control sobre el sistema objetivo sin necesidad de tener credenciales válidas pudiendo robar datos, instalar malware y modificar archivos de sistemas lo que tenga graves repercusiones en la seguridad y el funcionamiento del sistema afectado.

Remediación:

Eliminación del Token: Implementar un proceso que asegure que los tokens generados durante la configuración del inicio de sesión en la página web se eliminen correctamente después de completar la configuración.

Actualización de Metabase: La última versión de la configuración de Metabase ya está parchado el problema.

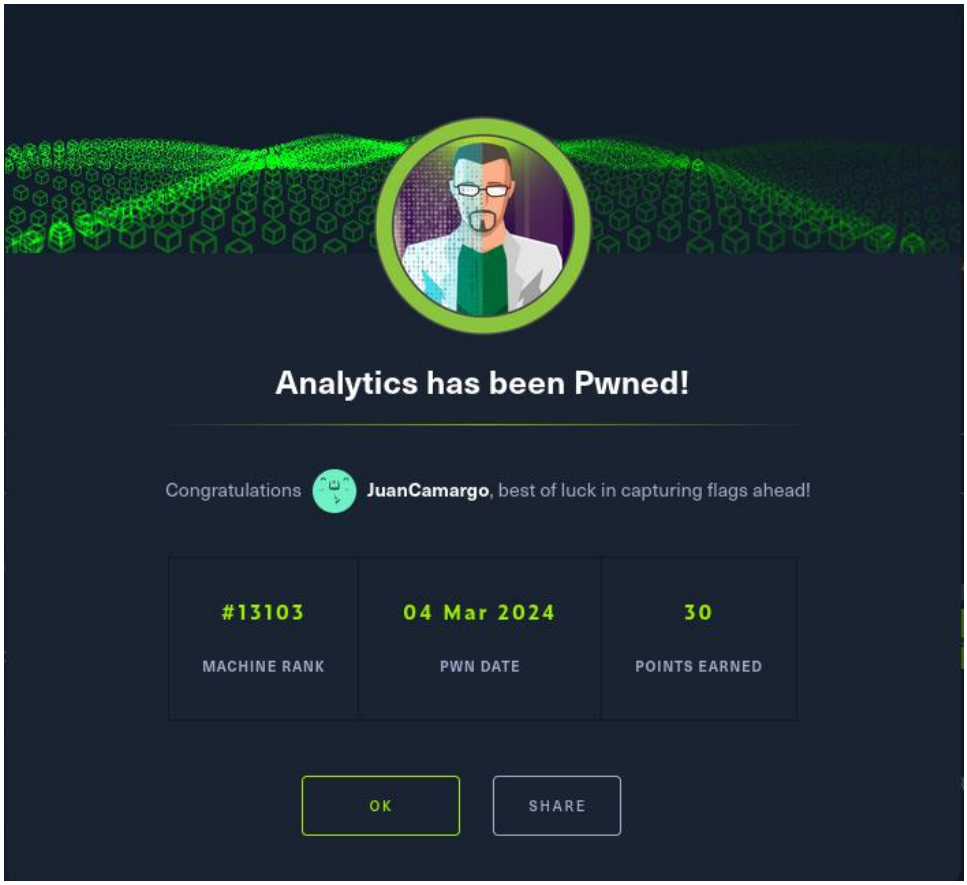
Vulnerabilidades relacionadas con Ubuntu 22.04.3 y OverlayFS PTF-003:

Ubuntu utiliza kernel como núcleo y OverlayFS por lo que todo lo que afecte a kernel afecta al OverlayFS y otros componentes del sistema de archivos.

Remediación:

Parches de Seguridad: Aplicar los últimos parches de seguridad proporcionados por Ubuntu para corregir las vulnerabilidades relacionadas con OverlayFS.

Monitoreo de Actividad del Sistema: Implementar herramientas de monitoreo de seguridad que detecten comportamientos anómalos en el sistema. Un ejemplo es pagar alguna plataforma de seguridad como CrowdStrike, que ya tengan solucionado la vulnerabilidad.



https://www.hackthebox.com/achievement/machine/1861122/569