8-scream

端口

```
nmap -sS -sU -p- --min-rate 8888 192.168.243.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 04:11 GMT
Nmap scan report for 192.168.243.57
Host is up (0.00027s latency).
Not shown: 65534 open|filtered udp ports (no-response), 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
69/udp open  tftp
MAC Address: 00:0C:29:2C:A4:34 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 42.87 seconds
```

服务识别

```
┌──(root㉿kali)-[/etc/network]
└─# nmap -sVC -O 192.168.243.57 -p21,22,23,69

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 04:24 GMT
Nmap scan report for 192.168.243.57
Host is up (0.00032s latency).

PORT   STATE    SERVICE VERSION
21/tcp open     ftp     WAR-FTPD 1.65 (Name Scream XP (SP2) FTP Service)
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp              0 Feb 20 01:30 bin
| drwxr-xr-x 1 ftp ftp              0 Feb 20 01:30 log
|_drwxr-xr-x 1 ftp ftp              0 Feb 20 01:30 root
|_ftp-bounce: bounce working!
22/tcp open     ssh     WeOnlyDo sshd 2.1.3 (protocol 2.0)
| ssh-hostkey:
|   1024 2c:23:77:67:d3:e0:ae:2a:a8:01:a4:9e:54:97:db:2c (DSA)
|_  1024 fa:11:a5:3d:63:95:4a:ae:3e:16:49:2f:bb:4b:f1:de (RSA)
23/tcp open     telnet
```

```
| fingerprint-strings:
|   GenericLines, NCP, RPCCheck, tn3270:
|     Scream Telnet Service
|     login:
|   GetRequest:
|     HTTP/1.0
|     Scream Telnet Service
|     login:
|   Help:
|     HELP
|     Scream Telnet Service
|     login:
|   SIPOptions:
|     OPTIONS sip:nm SIP/2.0
|     Via: SIP/2.0/TCP nm;branch=foo
|     From: <sip:nm@nm>;tag=root
|     <sip:nm2@nm2>
|     Call-ID: 50000
|     CSeq: 42 OPTIONS
|     Max-Forwards: 70
|     Content-Length: 0
|     Contact: <sip:nm@nm>
|     Accept: application/sdp
|     Scream Telnet Service
|_    login:
69/tcp filtered tftp
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port23-TCP:V=7.94SVN%I=7%D=2/20%Time=65D4297A%P=x86_64-pc-linux-gnu%r(N
SF:ULL,12,"\xff\xfb\x01\xff\xfe\"\xff\xfe\0\xff\xfd\x03\xff\xfd\x18\xff\xf
SF:d\x1f")%r(GenericLines,34,"\xff\xfb\x01\xff\xfe\"\xff\xfe\0\xff\xfd\x03
SF:\xff\xfd\x18\xff\xfd\x1f\r\n\r\nScream\x20Telnet\x20Service\r\nlogin:\x
SF:20")%r(tn3270,3C,"\xff\xfb\x01\xff\xfe\"\xff\xfe\0\xff\xfd\x03\xff\xfd\
SF:x18\xff\xfd\x1f\xff\xfc\x18\xff\xfe\x19\xff\xfc\x19\xff\xfb\0Scream\x20
SF:Telnet\x20Service\r\nlogin:\x20")%r(GetRequest,42,"\xff\xfb\x01\xff\xfe
SF:\"\xff\xfe\0\xff\xfd\x03\xff\xfd\x18\xff\xfd\x1fGET\x20/\x20HTTP/1\.0\r
SF:\n\r\nScream\x20Telnet\x20Service\r\nlogin:\x20")%r(RPCCheck,5C,"\xff\x
SF:fb\x01\xff\xfe\"\xff\xfe\0\xff\xfd\x03\xff\xfd\x18\xff\xfd\x1f\x80\0\0\
SF:(r\xfe\x1d\x13\0\0\0\0\0\0\x02\0\x01\x86\xa0\0\x01\x97\|\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0Scream\x20Telnet\x20Service\r\nlogin:\x20")%
SF:r(Help,36,"\xff\xfb\x01\xff\xfe\"\xff\xfe\0\xff\xfd\x03\xff\xfd\x18\xff
SF:\xfd\x1fHELP\r\nScream\x20Telnet\x20Service\r\nlogin:\x20")%r(SIPOption
SF:s,10F,"\xff\xfb\x01\xff\xfe\"\xff\xfe\0\xff\xfd\x03\xff\xfd\x18\xff\xfd
SF:\x1fOPTIONS\x20sip:nm\x20SIP/2\.0\r\nVia:\x20SIP/2\.0/TCP\x20nm;branch=
SF:foo\r\nFrom:\x20<sip:nm@nm>;tag=root\r\nTo:\x20<sip:nm2@nm2>\r\nCall-ID
SF::\x2050000\r\nCSeq:\x2042\x20OPTIONS\r\nMax-Forwards:\x2070\r\nContent-
SF:Length:\x200\r\nContact:\x20<sip:nm@nm>\r\nAccept:\x20application/sdp\r
SF:\n\r\nScream\x20Telnet\x20Service\r\nlogin:\x20")%r(NCP,31,"\xff\xfb\x0
SF:1\xff\xfe\"\xff\xfe\0\xff\xfd\x03\xff\xfd\x18\xff\xfd\x1f\x13Scream\x20
SF:Telnet\x20Service\r\nlogin:\x20");
MAC Address: 00:0C:29:2C:A4:34 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or
Windows Server 2003 SP0 - SP2 (94%), Microsoft Windows 2000 SP4 (94%), Microsoft
Windows XP SP2 (94%), Microsoft Windows XP SP3 (93%), Microsoft Windows 2000
SP0/SP2/SP4 or Windows XP SP0/SP1 (92%), Microsoft Windows 2000 SP1 (92%), Microsoft
Windows 2000 SP2 (92%), Microsoft Windows Millennium Edition (Me) (92%), Microsoft
Windows Server 2003 (91%), Microsoft Windows XP SP2 or SP3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 69.46 seconds
```

利用

```
ftp 192.168.243.57
ftp 可以匿名登录，只有查看权限



tftp 192.168.243.57
tftp 无查看权但能上传目录，上传到root下

http服务访问到的就是root路径下的文件，root下有一个cgi-bin目录，百度得知是一个网络接
口，通常用于该文件夹存储 Perl 或 Python 脚本。所以我们选择上传perl或python的webshell，
然后提权。
```