Using Respond Python Script

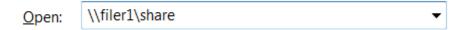
This is a lab for client-side attack. We are approaching with a network traffic monitor type. The purpose is to verify that the company workstation and server are not using a service that has already been announced as vulnerable to password disclosure (**NetBios** and **LLMNR**). The second part of the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

NETBIOS & LLMNR

- 1. Logon to you **Kali**, open *Wireshark*, and start it with the little green button on the top left corner of the interface
- Logon to your <u>Win7</u> VM and create an admin ID with the password <u>Iloveyou2</u>
- 3. On your **Win7**, go to run, type **\\filer1\temp**
- 4. Go to your **Kali**, stop the *Wireshark*. Type **LLMNR** in the filter box and see if you see any traffic of LLMNR protocol. **Take a screenshot** of the LLMNR activities.
- Logon to your <u>Kali</u>, go to <u>/usr/share/responder</u> and edit <u>Responder.conf</u>.
 Make sure SMB is on, and HTTP is on
- 6. In the same directory, execute the command as below. Replace the IP with **your Kali's** IP address

```
/usr/share/responder# ./Responder.py -i 192.168.222.140 -I eth0
```

- 7. Wait for the <u>Python</u> script to run, and **Take a screenshot** of the listening process
- 8. Go to your **Win7** VM, and log on with your admin ID. Go to **Run** and type a non-existed share folder:



9. Go back to your **Kali** to see if it captured the hash. **Take a screenshot** of the hash, ID, and client

```
[*] [NBT-NS] Poisoned answer sent to 192.168.222.145 for name WORKGROUP wser)

[*] [LLMNR] Poisoned answer sent to 192.168.222.1 for name filer1

[SMBv2] NTLMv2-SSP Client : 192.168.222.145

[SMBv2] NTLMv2-SSP Username : WIN-QT1VSHP3IRR\trans

[SMBv2] NTLMv2-SSP Hash trans: LIN-QT1VSHP3IRR:20f1c4a49432adfc:DC2:01010000000000000000653150DE09D201996A1AEC9A0DFCCC000000000002000800530
04E002D00500052004800340039003200520051004100460056000400140053004D0042
```

10. Access the following directory, and see if you have the SMB file created with the discovered hash

/usr/share/responder/logs/SMB*.txt

Open the file and **take a screenshot** of the discovered hash

- 11. Use *John the Ripper* to crack the password stored in the above file
- 12. **Take a screenshot** of the output from *John the Ripper*.
- 13. From your <u>Kali</u>, use <u>rdesktop</u> to logon to your <u>Win7</u> VM with the discovered ID. **Take a** screenshot of your <u>RDP</u> from <u>Kali</u>.