Wireshark – SYN Scan – Packet Spoofing

Outcomes:

a. Refresh Wireshark skills and knowledge of protocol communication, packet data/ transfer.
b. Concepts behind packet spoofing
c. Concepts behind SYN-SCAN and SYN FLOOD

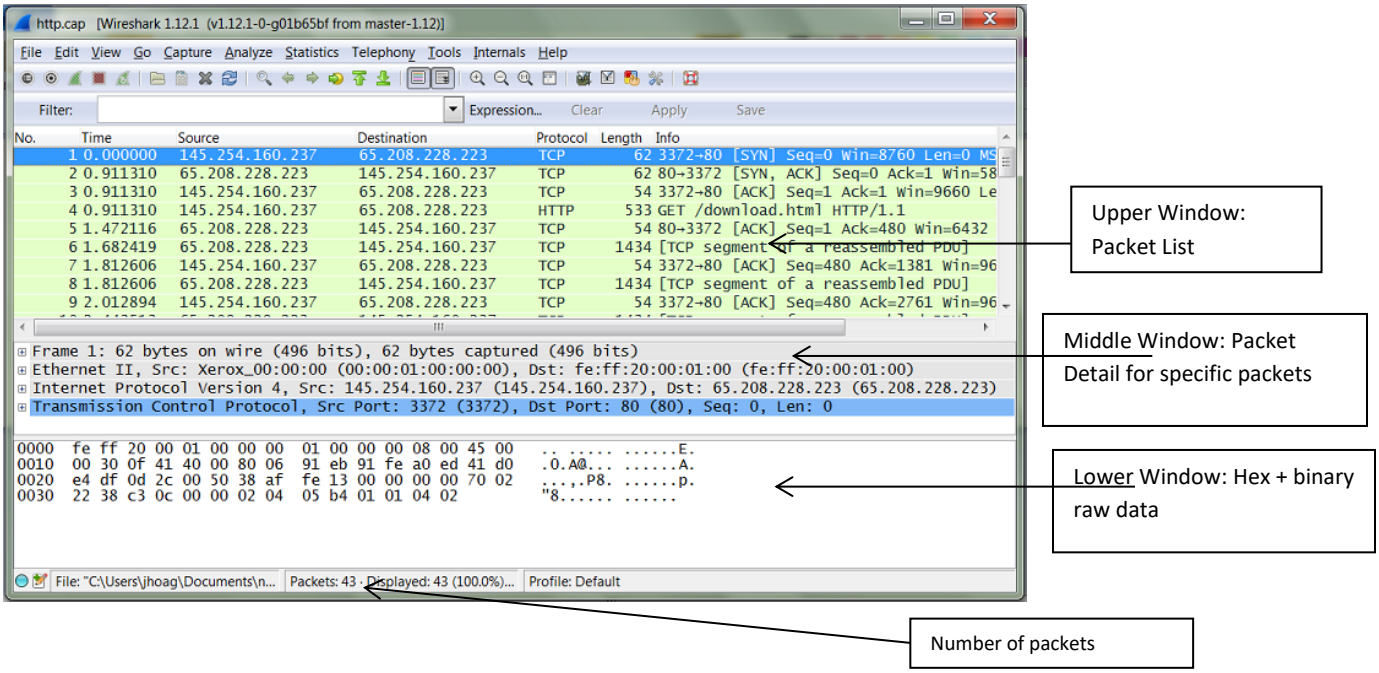
Open your Win10 VM which we have used previously.

Install Wireshark (download 64-bit installer from https://www.wireshark.org)

1a. Wireshark sample

On our canvas page, download http.cap, then open it in Wireshark.

The wireshark display includes 3 main windows/sections, each with a different level of detail:



1b. Exploring Packets

In the first packet, what is the source (browser, or web client) IP address? _____

What is the destination (web server) IP address? _____

What is the length? (value in length Column)? _____

Click in the middle Packet Detail section of the Wireshark window:

- Notice the frame length matches the value you just recorded

In the top Packet List section, right-click on the first packet. Choose the option for Conversation filter (TCP). There are actually 2 TCP conversations in this stream. We want to concentrate on the first one.

Can you find the TCP 3-way handshake?

What packet numbers does it use? _____

What packet does the HTTP protocol show up in? _____

This is the start of the http conversation

After that, there is a series of TCP segments containing the web page data

Packet 38 is the end of the http conversation (HTTP 200 OK)

Packets 40-43 are the TCP FIN sequence to end the connection

What Web Server application is in use here? (Hint: Packet Details) _____

1c. Headers

Let's examine some of the other fields and data in the capture.

Each protocol represents a portion of the entire capture. Each protocol also has a header section that provides information regarding source + destination + what to do with the data. Selecting a particular packet allows you to examine data in the protocol's header fields, as well as the data sent.

In the first packet, click on the Ethernet II header.

What is the source MAC address? _____

What is the destination Mac address? _____

What is the length of this header (Side note: Look in the lower Raw Data window … each pair of hex values in the lower frame is a byte)? _____

Select the IP header

What is the TTL? _____

What is the Total length? _____

What is the Protocol field? (just the protocol, not the number) _____

In the 4th packet (HTTP), click on the TCP header to expand it.

What TCP ports were used in this conversation? _____

What is the size of the TCP header? _____

How much data is sent? _____

1d. Statistics: Now let's explore some statistics of the conversation.

Click on the Statistics tab at the top menu, and select Capture File Properties.

In the bottom of the window, capture statistics are presented regarding the conversation.

Under Capture File Properties, record the following statistics:

Average packets per second (pps) _____

Average packet size (Bytes) _____

1e. Get a baseline of normal traffic.

Start a Wireshark capture, and do normal internet activity for 1-2 minutes. Stop the capture.

Under Statistics/Capture File Properties, record the following statistics:

Packets	
Time spans	
Average pps	
Average packet size, B	
Bytes	
Average bytes/s	
Average bits/s	

Under Statistics/Packet Lengths, what are the 2 most common categories? _____

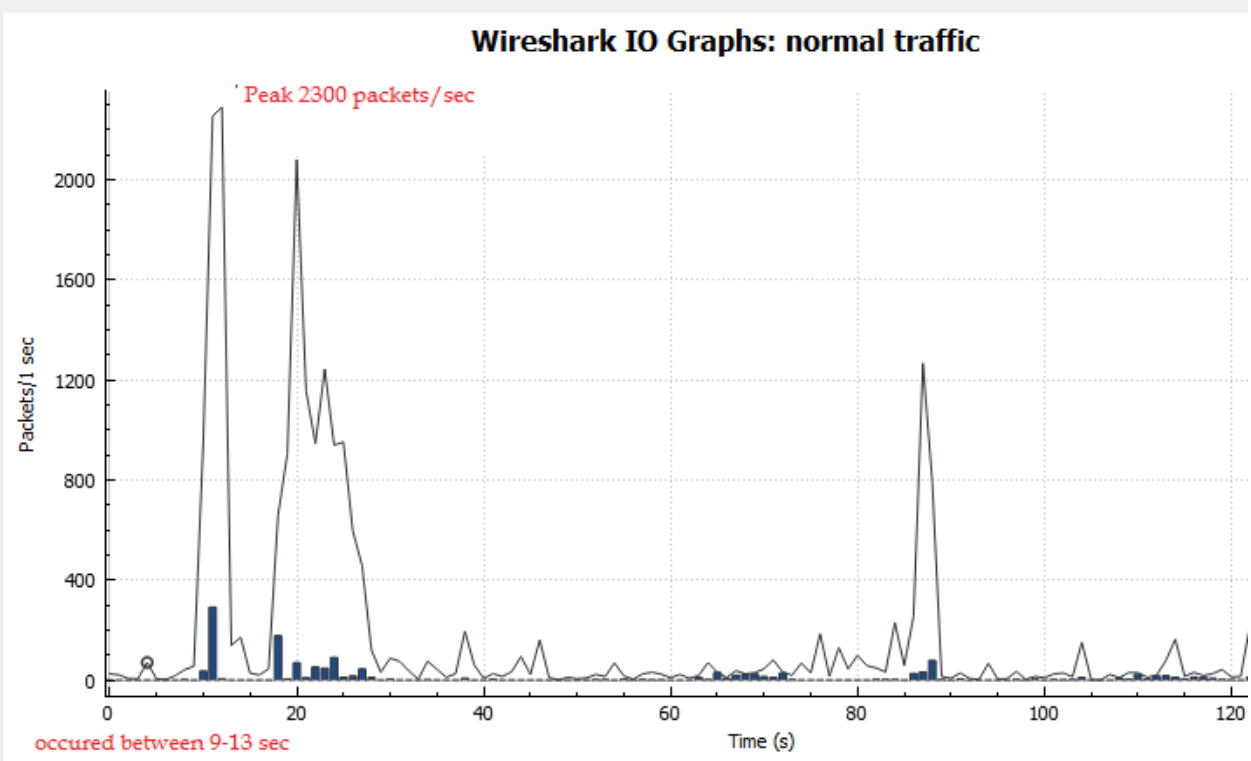
Look at Statistics/I-O graph.

What is the peak value (see example below)? _____

When in the capture did it occur? _____

How long did it last? _____

In this example, you can see the peak occurred from about 9-13 secs and was 2,300 packets/sec.



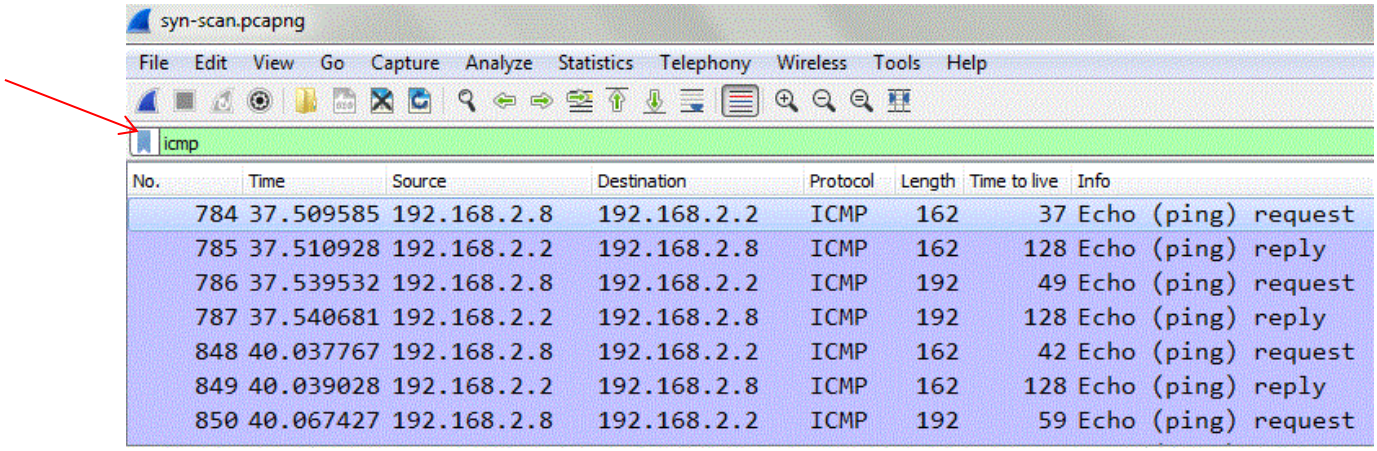
2. IP address spoof:

2a. Use Wireshark to capture a ping communication between your VM and your host.

Ping is an implementation of the Internet Control Message Protocol (ICMP).

In Wireshark, create a filter for ICMP & take a Snip.

The resulting data should look like this:



You should have the 4 ping requests with a matching ping reply.

2b. Spoof

Now you are going to spoof the source IP address. What happens if you say the source is an IP different from your own?

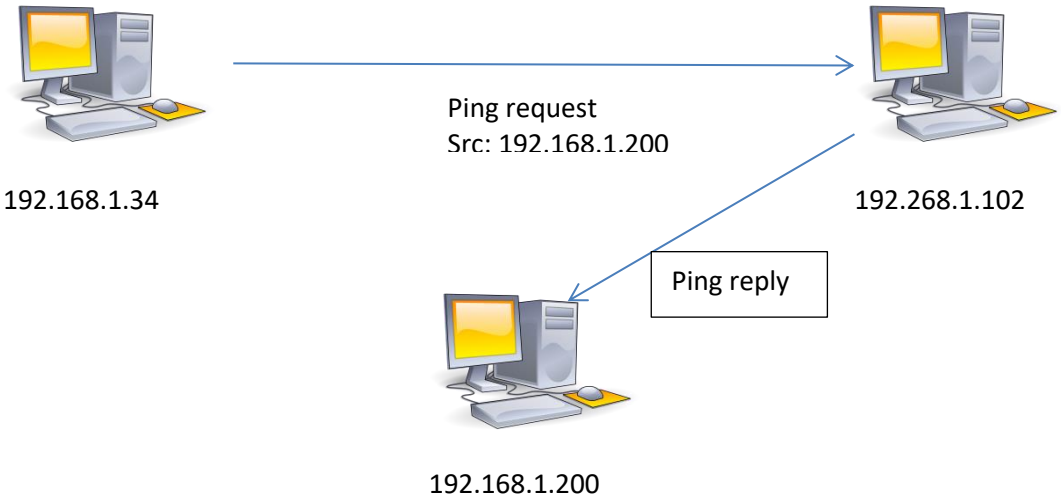
Download nmap on your VM, install it, then open a CMD line window and navigate to the nmap directory. (should be c:\Program Files (x86)\nmap)

nping is a utility that lets you modify the parameters of a ping request.

- Run nping –h to see all the options.
- Run nping neighbor_IP to see what normal output looks like.
- **Snip** your nping's normal output of your neighbor's IP.

Now, you are going to use another live "spoofed" station's IP address as the source IP in a ping to your neighbor. Your neighbor will be running Wireshark to capture the ping requests and responses.

Example:



Target: run Wireshark

Attacker: Run nping –S spoofed_IP target_IP

Target: stop Wireshark capture & then filter by icmp. This should show ICMP replies going to the spoofed system's IP.

The attacker's CMD window should show the ICMP requests, but no replies. Why? _____

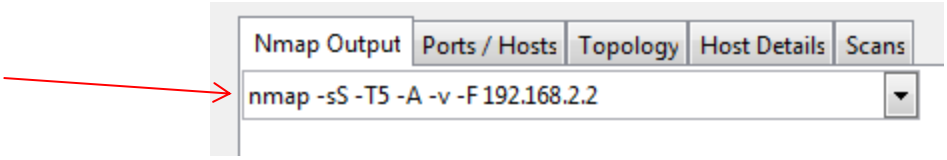
Attacker: Upload a screenshot of the CMD nping window.

Target: **Snip** the Wireshark capture filtered to show only ICMP.

3. SYN-SCAN/FLOOD

A SYN scan uses the 3-way handshake to see what ports are open. A SYN flood uses this same technique to overwhelm a device. A SYN packet is sent. If a port is open, it will send a SYN/ACK back. If the final ACK is never sent, the connection is not opened.

To do this, you'll use nmap. We used Zenmap previously which is the GUI version. You'll recall that Zenmap generated commands based on scan selections



It builds character to use command line, so today you will use nmap from CMD. And you are already in the directory in the CMD window.

- Type nmap –h to see what the possible options are.

Get ready for the scan/attack:

Target: start Wireshark capture

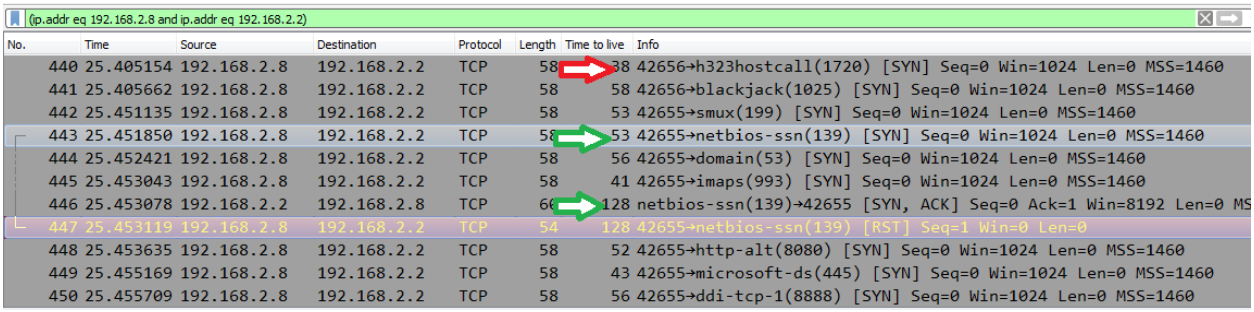
Attacker: run nmap from CMD → nmap –sS –T4 -v target_IP.

*The –sS = a SYN scan, -T4 = speed of packets, -v = verbose output

Target: stop Wireshark

Analyze traffic. You should see a number of SYN requests.

SYN/ACK replies should correspond to the open ports listed in the nmap output.



Maneuver to a set of packets that show both unacknowledged SYNs and SYN/ACKS similar to the image above. **Get a screenshot**.

Attacker: **Snip** nmap output on target.

It might be helpful to know you are being scanned or attacked. An attack in this case would be a more intense number of SYN packets.

Can this action be spotted /identified by the target machine as it is happening?

_____

Find the following data from the Wireshark capture.

Under Capture File Properties, record the following statistics:

Packets	
Time span s	
Average pps	
Average packet size, B	
Bytes	
Average bytes/s	
Average bits/s	

What are the two most common packet lengths? _____

Look at statistics/I-O graph

What is the peak value? _____

When in the capture did it occur? _____

How long did it last? _____

How does this data compare with the normal traffic statistics you obtained earlier? What are the differences that might be able to identify a SYN SCAN/FLOOD? _____