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

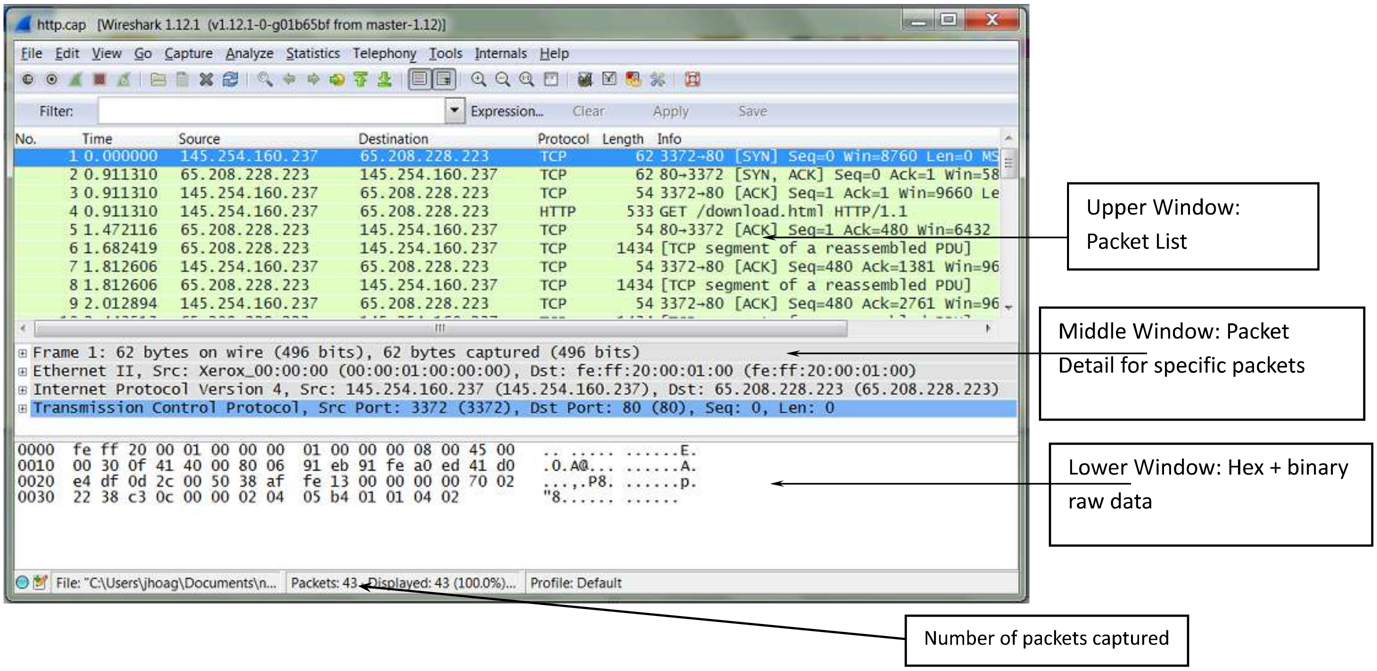
Open your Win10 VM which we have used previously.

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:


http.cap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
File: "C:\Users\jhoag\Documents\n...
Packets: 43 · Displayed: 43 (100.0%)...
Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	62	3372→80 [SYN] Seq=0 Win=8760 Len=0 MS
2	0.911310	65.208.228.223	145.254.160.237	TCP	62	80→3372 [SYN, ACK] Seq=0 Ack=1 Win=58
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372→80 [ACK] Seq=1 Ack=1 Win=9660 Le
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54	80→3372 [ACK] Seq=1 Ack=480 Win=6432
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
7	1.812606	145.254.160.237	65.208.228.223	TCP	54	3372→80 [ACK] Seq=480 Ack=1381 Win=96
8	1.812606	65.208.228.223	145.254.160.237	TCP	1434	[TCP segment of a reassembled PDU]
9	2.012894	145.254.160.237	65.208.228.223	TCP	54	3372→80 [ACK] Seq=480 Ack=2761 Win=96

```
⊞ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
⊞ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
⊞ Transmission Control Protocol, Src Port: 3372 (3372), Dst Port: 80 (80), Seq: 0, Len: 0
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

Upper Window: Packet List

Middle Window: Packet Detail for specific packets

Lower Window: Hex + binary raw data

Number of packets captured

1b. Exploring Packets

In the first packet, what is the source (browser, or web client) IP address?
145.254.160.237

What is the destination (web server) IP address? 65.208.228.223

What is the length? (value in length Column)? 62

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? 1-3

What packet does the HTTP protocol show up in? 4

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) Ethereal

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? 00:00:01:00:00:00

What is the destination Mac address? fe:ff:20:00:01:00

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)? 14

Select the IP header

What is the TTL? 128

What is the Total length? 48

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

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

What TC P ports were used in this conversation? 3372 and 80

What is the size of the TCP header? 20

How much data is sent? 479 bytes of payload, 533 total bytes across the entire packet

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) 1.4 captured, 1.1 displayed

Average packet size (Bytes) 584 captured, 609 displayed

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	1010

Time spans	107.467
Average pps	9.4
Average packet size, B	339
Bytes	342619
Average bytes/s	3188
Average bits/s	25k

Under Statistics/Packet Lengths, what are the 2 most common categories? 40-79 and 80-159

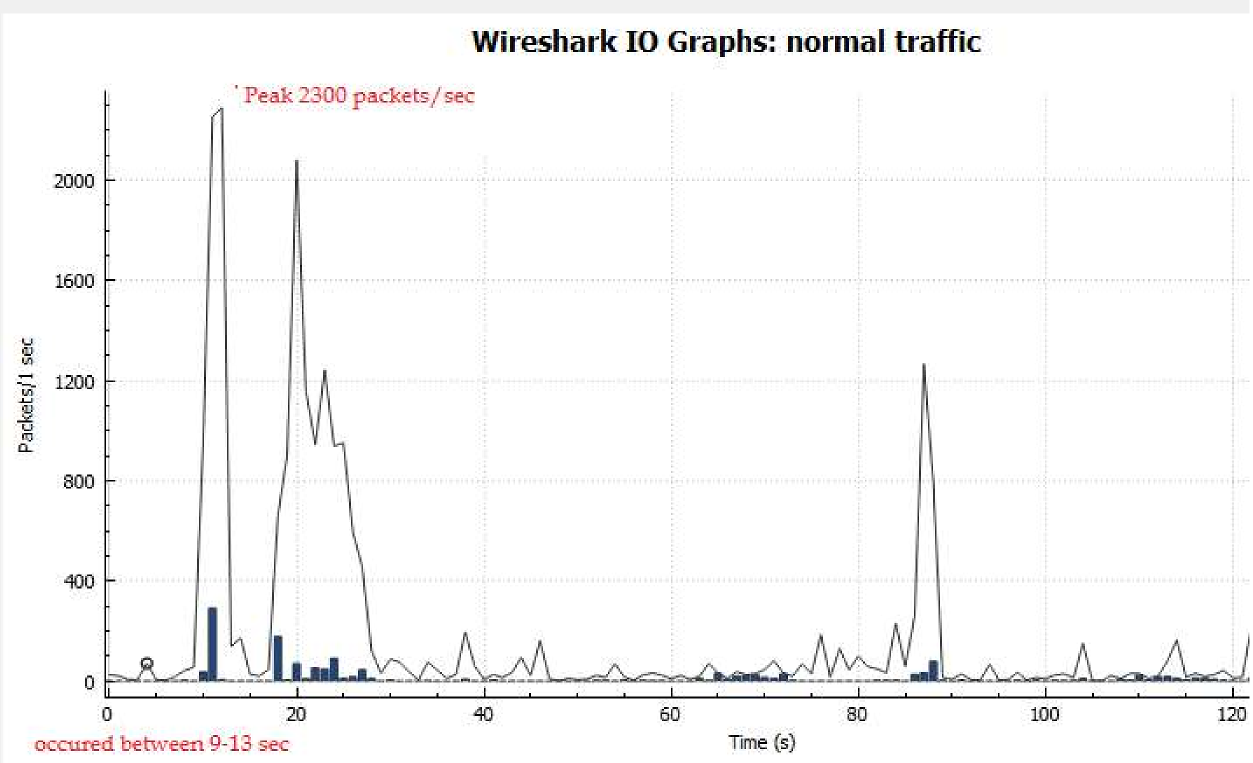
Look at Statistics/I-O graph.

What is the peak value (see example below)? About 225

When in the capture did it occur? 80s

How long did it last? About 1 second

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



Wireshark IO Graphs: normal traffic

Peak 2300 packets/sec

occured between 9-13 sec