## Lab 8a

## Examining Network Traffic

**Introduction**

This week, we will be looking in depth at packet capture files, and the indicators of abnormal traffic. For this lab, we will be using Nmap and Wireshark for network analysis.

## **Learning Outcomes**

After this session you should be able to:

1. Continue to develop skillset with Wireshark
2. Be able to use Wireshark filters efficiently
3. Perform port scanning and be able to interpret scanning activity
4. Be able to pinpoint causes or actions based on network traffic
5. Develop knowledge of how to spot abnormal traffic

**Task 1 – Reconnaissance using Nmap**

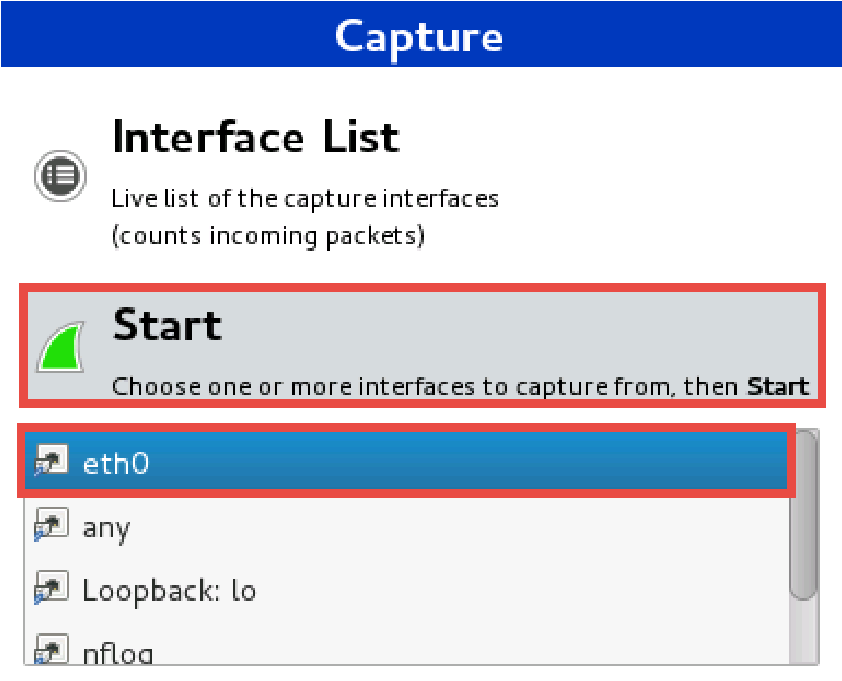
First you need to visit NetLab and schedule a lab session for “NDG Ethical Hacking”.

1. Click on the **Kali** graphic on the topology page.
2. Click anywhere within the Kali console window and press **Enter** to display the login prompt.
3. Enter **root** as the username.
4. Enter **toor** as the password.
5. Open a new terminal by clicking on the **Terminal** icon located on the left panel.
6. Open and review Nmap’s manual by typing the command below followed by pressing Enter.

man nmap

Nmap has many options, including its own scripting engine. Review the man pages to get familiar with the switches and options. Press the **Spacebar** to go to the next page or press **Enter** to go to the next line.

1. Once finished reviewing the man page, press the **Q** character to quit and bring the shell prompt back.
2. Launch Wireshark to observe what happens when a scan is triggered.
3. In the Capture panel, select **eth0** from the list and click **Start**.



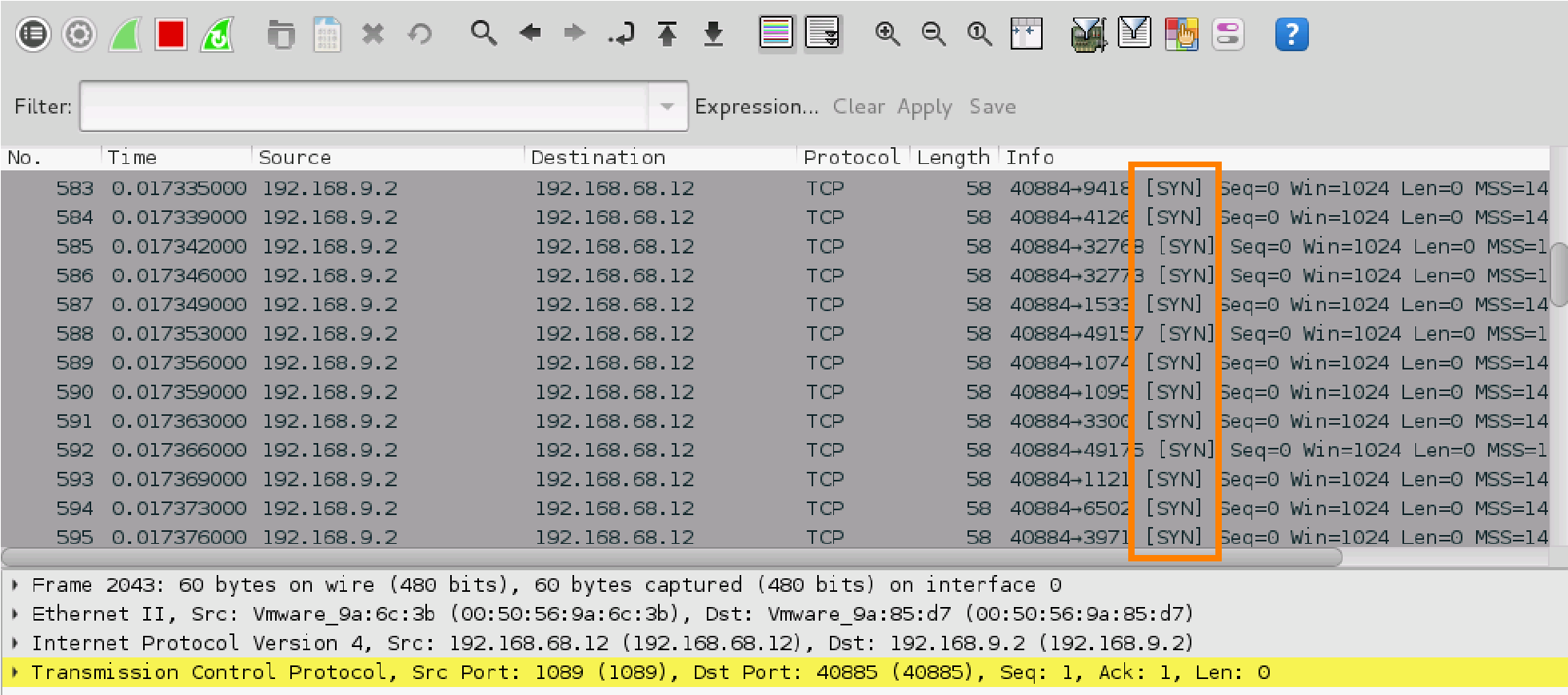
1. In the new Terminal window, initiate a general Nmap scan with no options.

nmap 192.168.68.12

Press **Enter** and wait for the scan to complete.



1. Navigate back to the Wireshark window.
2. Scroll through the Wireshark output and notice how Nmap uses [SYN] flags against all the ports to see if they are open or closed.



1. Save the Wireshark scan results by clicking on the **Capture** menu item followed by clicking on **Stop** and then **File** and **Save as**.
2. What happened here?

**TCP SYN scan - lots of packets send with SYN flag set to different ports**

1. Search for port 22 (SSH) to check whether it is open. Use the filter **tcp.port==22**. Is the port open or closed? How can you tell?

**Open – [SYN, ACK] response**

1. What type of scan is this? How can you tell?

**TCP Half open scan, [SYN]-[SYN, ACK]-[RST] the initiator leaves the communication hanging**

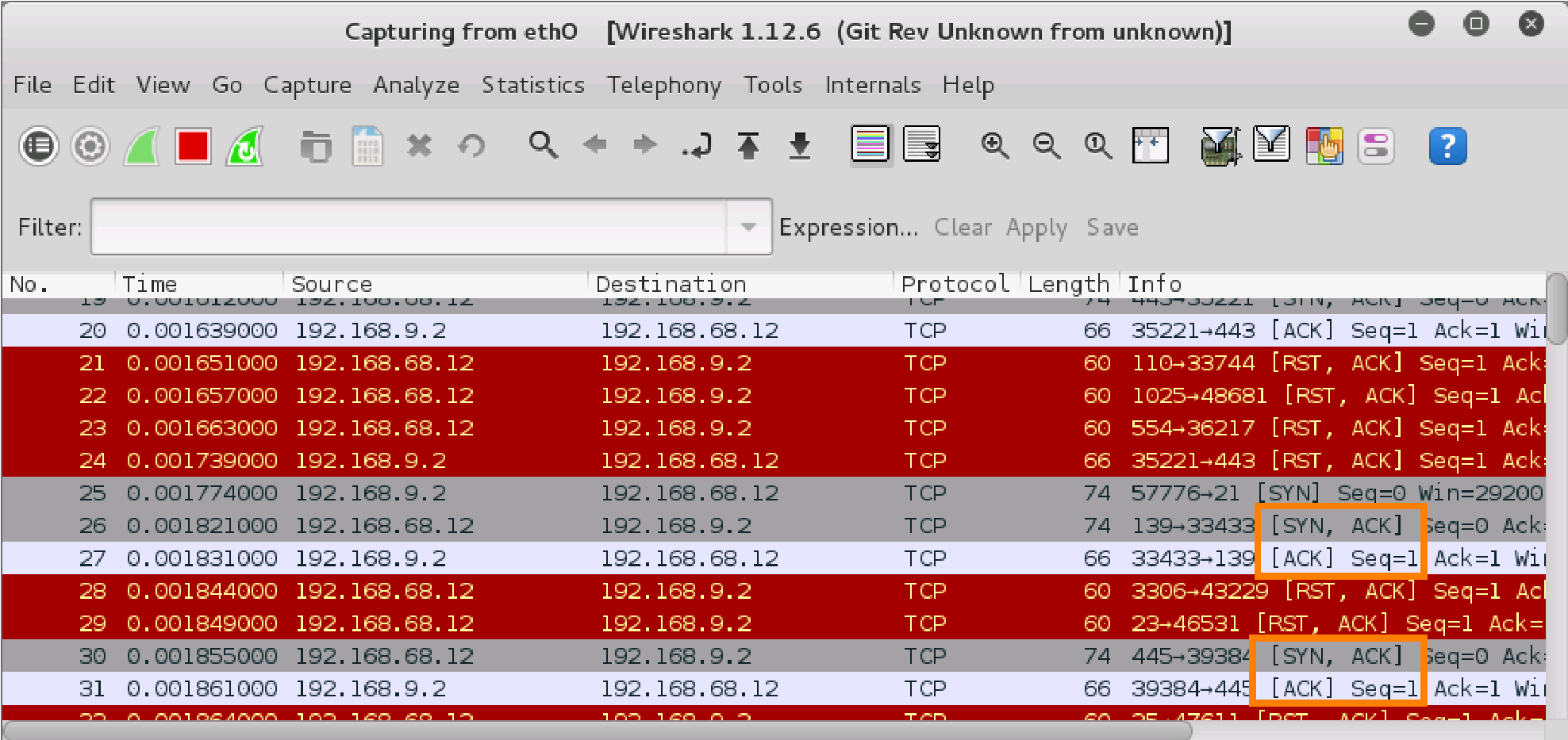
1. Look at the captured packets and try to identify the open ports. Is this consistent with your nmap output?

**22, 80, 139, 143, 443, 445, 5001, 8080, 8081 – Yes it’s consistent**

1. Minimize the Wireshark window and navigate back to the Terminal that the Nmap scan was initiated from.
2. This time, initiate a specific TCP connect scan. Type the command below followed by pressing **Enter**.

nmap -sT 192.168.68.12

1. Once the scan is completed, navigate back to the Wireshark window.
2. In the given Wireshark output, notice a few connections are being attempted using [SYN, ACK] followed by a [SYN].



1. Navigate back to the Terminal that the Nmap scan was initiated from.
2. Nmap scans can be noisy at times with its default port scanning range. Limit Nmap to only scan to the most popular ports by initiating the command below.

nmap -F 192.168.68.12

1. Use Nmap to try to identify versions of software running on the ports. Type the command below followed by pressing **Enter**.

nmap -A 192.168.68.12

1. Notice a lot more information is given about the target machine. Nmap has a set of scripts installed we can use to test for vulnerabilities. Initiate the command below to run a general set of default scripts.

nmap -sC 192.168.68.12

Notice Nmap tries a set of scripts against the target to look for some general vulnerabilities.

**Task 2 – Analysing network traffic**

For this task, go to Home/Downloads and open the “http.pcap” file.

1. What is the first thing that happened and which destination address did it involve? (Hint: Look at the first captured packets)

**TCP 3 way handshake, destination address 65.208.228.223**

1. What packet identifier(s) tell you this and why?

**1-3 – packets were sent with TCP flags for SYN, SYN ACK and then ACK in that order**

1. What is the purpose of the above packet exchange?

**Communication Establishment**

1. Which protocol is being used for the above packet exchange?

**TCP**

1. Which port is being used for the above communication?

**80**

1. Look at packet 17. What was the purpose of the DNS response? Which packet is the response associated to? How can you tell?

**DNS response to packet 13 query - ID 0x0023**

1. Look at packet 17. What does CNAME mean? What other resource records can you find associated with this query/response?

**A stands for IPv4, pagead2.googlesyndication.com was requested; canonical name is pagead2.google.com**

1. Go to packet 38. What does 200 OK mean? What was the browser used for this request? What does GET mean?

**Successful request, Mozilla 5.0, receive content/download file**

1. What is the MAC address for 145.254.160.237?

**00:00:01:00:00:00**

1. How long did the whole activity run for?

**30 Seconds**

**Task 3 – Event recreation**

After gathering all the information you need, you are ready to build a recreation of events and a timeline including:

1. Source and destination addresses and source/destination ports
2. Why the user was using to perform any/all activities, and what protocols might be in use during these activities
3. All the actual activities themselves, and the results of user activity
4. Timestamp everything
5. A list of laws relevant along with a brief explanation as to why it might be relevant

**Task 4 – Reflection**

Nmap is a powerful tool for network exploration and management. How can Nmap help with network security? How can Nmap be used by a threat actor as a nefarious tool?

**Nmap can be used to scan an internal network for specific open ports to identify the extent of a security breach. It can also be used to inventory a network to ensure that all the systems are probably patched against security concerns. On the other hand, nmap can be used for reconnaissance to determine open ports and other information about the network.**