Study Guide

Module 1: Introduction

Lesson 1.1: Introduction
- Instructor: Ken Underhill
- Sniffing is Snooping or Eavesdropping or listening to conversation.

Module 2: Wireshark and TCPDUMP

Lesson 2.1: Wireshark Lab Part 1
- Lab doesn't require login. Lua error on launch can be ignored.
- Capture>> options. Alternatively, Ctrl+K.
- Select the network interface to use.
- Keep the default settings. Promiscuous mode- enabled, Capture Filter box- empty, Display Options- all the boxes are checked,
- Promiscuous mode is a type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode. It is a network security, monitoring and administration technique that enables access to entire network data packets by any configured network adapter on a host system.
- Uncheck all boxes under name resolution and then Start.

Lesson 2.2: Wireshark Lab Part 2
- Generate traffic: with ping x.x.x.x, wget hxxp(s)://url, ssh host, nc host port, etc.
- For the course lab: host: 10.0.10.12 and nc port: 444
- Right click and selecting "Follow TCP Stream", shows the Stream of TCP traffic or what TCP traffic flow was and hence, the completely activity for that traffic flow.

Lesson 2.3: Wireshark Lab Part 3
- Red square button for below the menu ribbon, stops the packet capture.
- Accessing saved pcap: File>>Open>> (location of pcaps)>> Click Open.
- To go to specific packet: Go>> Go to packet>> Type the packet number>> "Jump to".

- Click in a packet, the lower panel gives the details of the packet, for example: Source and Destination IP, Source and Destination ports, Device MACs, packet size, etc.

Lesson 2.4: Packet Sniffing Lab Part 1

- Check in CEH lab for Packet Sniffing lab.
- 5 VMs, so start all of them, to save time.
- Lab VMs have 60 minutes limit, extend the limit by clicking the timer.
- Use lab VM, PLABDM01 (IP: 192.168.0.2) and start Wireshark with adapter as "Ethernet 3".
- Use lab VM, PLABWIN10 and try to login to PLABDC01: 192.168.0.1 with telnet with putty.
- Error indicates telnet connection failure or no active on the destination.
- Login Info for DM01: Administrator|Passw0rd

Lesson 2.5: Packet Sniffing Lab Part 2

- In PLABDM01, stop the packet capture like before.
- In Wireshark, in the filter field, type in telnet, to filter all telnet packets.
- Right Click>> Follow>>TCP stream and the whole telnet transaction should pop-out with the username and password, if not repeat this with a different packet.

Lesson 2.6: Applying Filters to TCPDUMP and Wireshark Lab Part 1

- Search catalogue for the lab: Applying Filters to TCPDUMP and Wireshark and “Launch”.
- Open terminal and navigate to /home/student/Desktop/captures(Command: cd /home/student/Desktop/captures)
- To open a pcap: tcpdump –n –xx tcp –r “file.pcap” | less
- File.pcap can be any existing pcap file.
- Quotes help when the file name has spaces, by treating them as single name and not different parameters.
- “q”+ enter helps us to exit the tcpdump data.
- To filter by port number, the data: tcpdump –n –xx tcp **port 80** –r “file.pcap” | less.
- To filter by port and IP address, the data: tcpdump –n –xx **host 172.16.20.24 and** tcp **port 80** –r “file.pcap” | less.

Lesson 2.7: Applying Filters to TCPDUMP and Wireshark Lab Part 2

- Open Wireshark in the above lab and the go to File>>Open and open the pcap from Desktop.
- Use filter: ip.dst_host contains “xx.xx” and http.
- Using export object feature, we can export individual HTTP/SMB/DICOM packets or a set of transaction/traffic.
- TCP streams can also be saved from Follow>> TCP stream>> Save As and into txt file.
- “!” in filter implies negation or NOT operation. Ex- to exclude TCP traffic, filter:**!tcp**.

Lesson 2.8: TCPDUMP lab

- Lab name is TCPDUMP.
- Directory for capture: /home/student/Desktop/captures.
- To see all interfaces available: sudo tcpdump –D –list-interfaces.
- To start listening: sudo tcpdump –I <interface id>.

Module 3: Conclusion

Lesson 3.1: Capstone Lab Navigation

- Lab name is Introduction to Wireshark.

Lesson 3.2: Conclusion

- 4 labs and 1 Capstone lab for understanding and working out.
- Next courses: PT and EH; NMAP, Kali Fundamentals, BSWJ.

Created by: Arnav Banerjee, TA.