**Lab #4-Using Wireshark-One Kali Linux Tools Used for Network Protocol Analyzer**

**Last Name: \_\_\_\_\_\_\_ First Name: \_\_\_\_\_\_\_**

**Objective:** The aim for this lab is to learn how to analyze a network protocol by using one Kali Linux security tool such as Wireshark. The second aim of this lab is to learn how to select a capture Interface and create a first pcap file. The last aim of this hands-on lab is to learn why Kali Linux is a penetrating and security auditing by using network analysis tools such as wireshark. Wireshark is a wide-open tool that is used for profiling network traffic and analyzing packets. This tool is used to examine the details of traffic at a variety of levels ranging from connection-level information to the bits that made up a single packet. Packet captures provides network administrators with different valid information such as transmit time, source, destination and other valid information.

**Scenarios:** There are many scenarios in which can show an individual can use the wireshark to select a capture Interface and create a first pcap file. Some examples of scenarios would be network administrators using wireshark to analyze the network system or cybersecurity specialist using wireshark to analyze the network to see any vulnerabilities in the network system. While selecting a capture Interface and creating a first pcap file, a PCAP packet sniffer is used to capture these types of files. Then an interface is chosen and identify to be sniffer on. Interface eth0 or wlan0 is chosen if you are using a Kali Linux operating system. An interface can also be selected with the ifconfig command. The individual chooses what type of traffic that wanted to be monitored. Traffic types such as TCP/IP, UCP, UDP, and other types are monitored. Once the filtered traffic is captured, the traffic is analyzed for performance issues. Also, this traffic can be filtered for more targeted analysis by source ports and destination ports to test network elements. This information from the captured packet can be used to solve issues with network performance.

**Background:** Kali Linux is a multiplatform, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains many tools that are fixed on towards different information tasks such as Security Research, Computer Forensics and more. Linux was developed through rewriting of Backtrack by Mati Aharoni and Devon Keams of Offensive Security. Linux contains over six hundred different preinstalled penetration applications that can be discovered. Each program in Kali Linux has its own unique flexibility and case uses. Kali separates these useful utilities into the following categories: Information Gathering, Vulnerability Analysis, Wireless Attacks, Web Applications, Exploitation Tools, Stress Testing, Forensics Tools, Sniffing & Spoofing, Password Attacks, Maintaining Access, Reverse Engineering, Reporting Tools, and Hardware Hacking. Wireshark follows under the sniffing and spoofing category.

Wireshark is a wide-open tool that is used for profiling network traffic and analyzing packets. This tool is used to examine the details of traffic at a variety of levels ranging from connection-level information to the bits that made up a single packet. Packet captures provides network administrators with different valid information such as transmit time, source, destination and other valid information. There are many advantages and disadvantages of packet capturing and PCAP. Some of the advantages are grants visibility, pinpointing the root cause of network issues, monitoring/identify the usage data of applications and devices, and find/resolve performance issues of networks after security breach events. While some of the disadvantages are packet analysis, it allows the individual to monitor network traffic but doesn’t monitor every part of the network, cyberattacks are not launched through network, hackers use encrypted communications to launch attacks on networks and more. PCAP files are files that are created from

sniffing and spoofing software such as Wireshark. These types of files contain packet data of network and are used to analyze a network specific characteristic. The files also help with controlling the network traffic and determining the network status. This type of file creates a record of network data that the individual can view through applications such as wireshark. There are many different types of PCAP that have are used for different capabilities and cases. The names of these types of PACP file are WinPcap, Libpcap, Npcap and PCAPng.

**Goals**

Students will learn these different concepts and terms throughout the various stages of performing this hands-on lab about one of kali Linux security tool (Wireshark) and help to complete the aim of this hands-on lab:

* Learn what Kali Linux is
* Learn what are the different tools that are found in Kali Linux
* Learn how to analyze a network protocol by using one Kali Linux security tool such as Wireshark
* Learn how to select a capture Interface
* Learn how to examine the details of traffic at a variety of levels ranging from connection-level information to the bits that made up a single packet
* Learn to Create a First Pcap file

**Tools**

* Kali Linux Virtual Machine
* Laptop/Desktop

**Task**

**Skip Task #1 if Kali Linux virtual is installed on your device!**

**Task #1: Installing/Preparing/Starting Kali Linux Virtual Machine**

1. Install the VMware with default options from the website (<https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/15>\_0) if you are using a PC or VMware Fusion or Virtual Box if you are using MAC OS operating system.
2. In a search engine, go to <https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/> website where you will click the Kali Linux VMware 64 bit to get the current version of the computer application. Then unzip the download file.
3. Navigate to the Kali VM that was unzipped and start the virtual machine.
4. Log in to Kali with the username kali and password of Kali.

**Task#2: Configuration of Network Settings/Wireshark**

1. In the VMware window with your Kali Linux OS Powered off, highlight the Kali Linux Operating System and click on the edit machine settings selection in the right pane. In the “Network Adapter:” pull down menu select “Bridged Adapter”. This selection will allow your Kali Linux OS to obtain an IP address for its exclusive use instead of using the IP address of the host OS. You will no longer be able to use the wireless connection for any   
   outgoing connections from Kali Linux. Hence, you might want to change the network setting back to “Nat” when you finish this experience.
2. To start WireShark open a ‘Terminal’ and type ‘sudo wireshark’ (you will be prompted to enter   
   the root password).
3. Before you can begin click ‘Ok’ on the pop-up dialog indicating you are running this   
   program as root; it may be hiding behind WireShark.
4. Once WireShark opens click the icon (first icon below ‘file’) to choose a network   
   interface to listen for packets; the dialog below should appear.
5. Choose eth\*, where \* represents a number (your device could be 0 – 9). Make a note of the IP   
   address. We will be using this IP address in Step 4 for interactions with your webserver.
6. Select Start; WireShark will immediately begin intercepting packets.
7. From the top menu, select ‘Capture’ -> ‘Stop’
8. What is the wireshark?

|  |
| --- |
|  |
|  |
|  |

**Task #3: Intercepting, Filtering, Analyze Raw Packets**

1. It is suggested that you close all open internet browsers; if you prefer to keep them on, it may be necessary to comb through more data to complete this section.
2. Select ‘Capture’ -> Start
3. In Kali Linux open Firefox and go to <http://www.famu.edu>   
   After the page completes loading
4. Select ‘Capture’ -> Stop
5. WireShark will continuously report all packets to your machine of all network activity   
   that is not filtered once capturing starts. To avoid being inundated with HTTP/TCP   
   data we stop capturing data at this point to analyze the data.
6. Select ‘Capture’ -> ‘Capture Filters...’
7. Select ‘HTTP TCP port (80)’
8. If this is not shown, choose ‘TCP or UDP port 80 (HTTP)
9. Click ‘Ok’
10. What does HTTP means?

|  |
| --- |
|  |
|  |
|  |

1. What is TCP port (80)?

|  |
| --- |
|  |
|  |
|  |

1. What is UDP port 80?

|  |
| --- |
|  |
|  |
|  |

1. What does TCP mean?

|  |
| --- |
|  |
|  |
|  |

**Task #4: Saving a PCAP File**

1. Save the packet trace in the default format.
2. Click on the **File** menu option and select **Save As**. By default, Wireshark will save the packet trace in libpcap format. This is a filename with a.pcap extension.
3. What is a PACP file?

|  |
| --- |
|  |
|  |
|  |

1. Why is PACP important?

|  |
| --- |
|  |
|  |
|  |

1. List advantages and disadvantages of PACP files?

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

Task 4: **Encrypting Files on a Device**

1. Right-click (or press and hold) file or folder and select Properties.
2. Select the Advanced button and select the encrypted contents to secure the data check box. An “The Advanced Encryption Standard” (AES) is used to encrypt this file.
3. Select Ok to close the Advanced Attributes window, select Apply and then select Ok.
4. . What type of files did you encrypt from this device?

|  |
| --- |
|  |
|  |
|  |

1. What are the vulnerabilities of the encrypting file system?

|  |
| --- |
|  |
|  |
|  |
|  |

1. What are the pros and cons of this encrypting file system?

|  |  |
| --- | --- |
| Pros | Cons |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. What type of AES keys are used to encrypt and decrypt data?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

1. Does AES use symmetric key or asymmetric key algorithms?

|  |
| --- |
|  |
|  |
|  |
|  |

1. Does AES use public or private keys?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

1. In your own words, explain the procedure of encrypting and decrypting a file using the AES method?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |