**Day 17 - Using Wireshark on Kali Linux**

Wireshark is a popular network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network. If you're new to Wireshark and using Kali Linux, this guide will walk you through the basics, from installation to using essential commands.

**Step 1: Install Wireshark on Kali Linux**

Wireshark is pre-installed on Kali Linux. However, if it’s not installed or you want to update it, follow these steps:

1. **Open the Terminal:**
   * You can open the terminal by clicking on the terminal icon or by pressing Ctrl + Alt + T.
2. **Update Your System:**
   * Before installing, it's good to update the system's package list:

sudo apt-get update

1. **Install Wireshark:**
   * If Wireshark is not installed, install it using:

sudo apt-get install wireshark

1. **Grant Permission to Capture Packets:**
   * During installation, you may be prompted to allow non-superusers to capture packets. Choose "Yes".
   * If not prompted, you can manually configure it:

sudo dpkg-reconfigure wireshark-common

sudo usermod -aG wireshark $(whoami)

1. **Reboot or Log Out and Back In:**
   * This ensures the permission changes take effect.

**Step 2: Launching Wireshark**

1. **Open Wireshark:**
   * Type wireshark in the terminal or find it in the application menu under "Sniffing & Spoofing".
2. **Select a Network Interface:**
   * Upon opening Wireshark, you'll see a list of available network interfaces. Choose the one you want to monitor (e.g., eth0 for wired connections or wlan0 for wireless).
3. **Start Capturing Packets:**
   * Double-click the interface or click on it and then click the blue shark fin icon in the toolbar to start capturing packets.

**Step 3: Basic Wireshark Commands and Usage**

1. **Capture Filters vs. Display Filters:**
   * **Capture Filters:** These are set before starting the capture and determine what traffic is captured.
   * **Display Filters:** These filter the captured traffic to display only relevant packets.

**Example Capture Filter:**

* + To capture only HTTP traffic:

port 80

**Example Display Filter:**

* + To display only TCP traffic:

Bash

tcp

1. **Stop Capturing:**
   * Click the red square icon in the toolbar to stop capturing traffic.
2. **Save Captured Data:**
   * You can save the captured data by going to File > Save As, and save it as a .pcap file.

**Step 4: Analyzing Packets**

1. **Inspecting Packets:**
   * Click on any packet in the captured data to view its details. The packet details pane shows the layers of the packet (Ethernet, IP, TCP, etc.).
2. **Follow TCP/UDP Stream:**
   * Right-click on a packet related to a TCP/UDP stream and select "Follow > TCP/UDP Stream". This shows the full conversation in one window.
3. **Filtering by IP Address:**
   * To show traffic from a specific IP:

ip.addr == 192.168.1.1

1. **Filter by Protocol:**
   * To display only HTTP traffic:

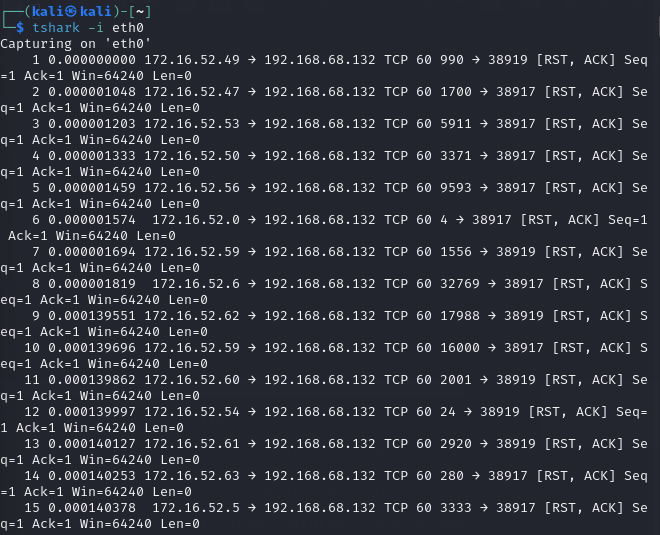
http

**Wireshark Commands**

Wireshark is a network protocol analyzer used for capturing and analyzing network traffic. Unlike Nmap, Wireshark is primarily a GUI tool, but you can use the tshark command-line utility for similar functionality.

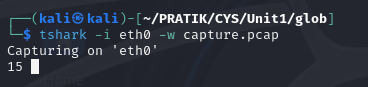
1. **Start Capturing Packets**
   * **Command**: tshark -i [interface]
   * **Description**: Starts capturing packets on the specified network interface.
   * **Example**:

tshark -i eth0



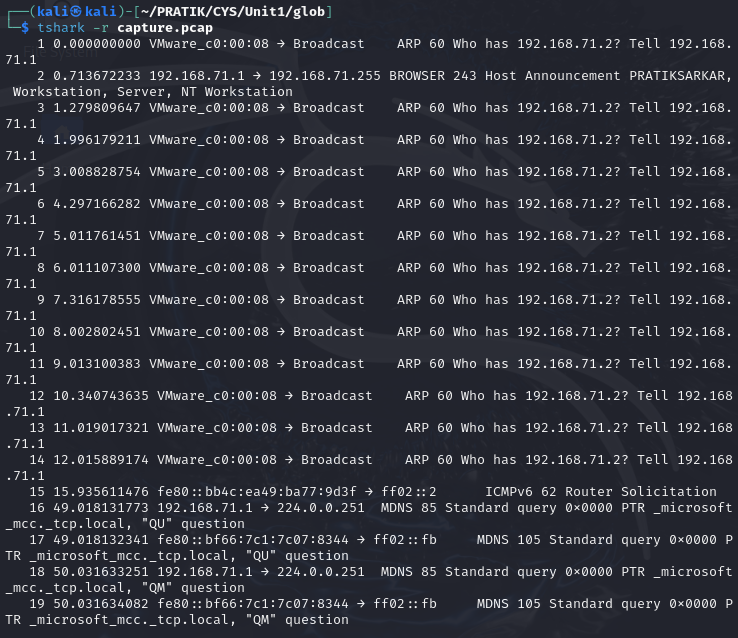
1. **Capture Packets and Save to File**
   * **Command**: tshark -i [interface] -w [filename.pcap]
   * **Description**: Captures packets and saves them to a file.
   * **Example**:

tshark -i eth0 -w capture.pcap



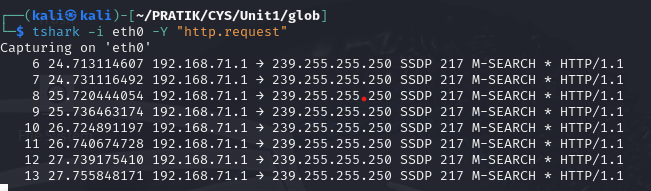
1. **Read Packets from a File**
   * **Command**: tshark -r [filename.pcap]
   * **Description**: Reads and displays packets from a saved file.
   * **Example**:

tshark -r capture.pcap



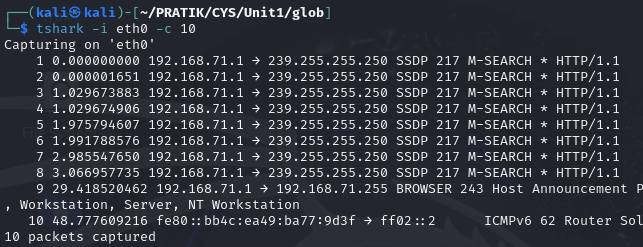
1. **Apply Display Filter**
   * **Command**: tshark -i [interface] -Y [display filter]
   * **Description**: Applies a display filter to the captured packets.
   * **Example**:

tshark -i eth0 -Y "http.request"



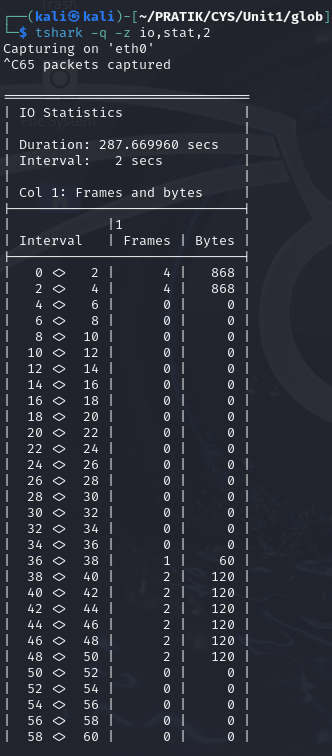
1. **Display Packet Count**
   * **Command**: tshark -i [interface] -c [count]
   * **Description**: Captures a specified number of packets and then stops.
   * **Example**:

tshark -i eth0 -c 100



1. **Show Protocol Hierarchy**
   * **Command**: tshark -q -z io,stat,[interval]
   * **Description**: Displays protocol statistics in intervals.
   * **Example**:

tshark -q -z io,stat,10



1. **Display Packet Details**
   * **Command**: tshark -x -r [filename.pcap]
   * **Description**: Shows detailed packet data in hex and ASCII format.
   * **Example**:

tshark -x -r capture.pcap

