**Exp: no: 2**

Analyse the network traffic using Wireshark tool.

**Aim:**

To analyse the network traffic using Wireshark tool and write the syntax, execute and place the screenshot of all the commands worked on.

a. Explain what is a packet analyzer ?

**Packet Analyzer**

A packet analyzer, also known as a network analyzer, protocol analyzer, or packet sniffer, is a tool used to capture, monitor, and analyze data packets traveling across a network. It allows network administrators, security professionals, and developers to examine the data being transmitted over a network in real-time or from saved packet capture files. By capturing all traffic on a network, a packet analyzer can provide detailed information about each packet, including its source and destination IP addresses, the protocols used, and the data payload. This capability makes packet analyzers indispensable for troubleshooting network issues, ensuring security, and optimizing network performance.

Beyond troubleshooting, packet analyzers are also crucial for security analysis. They can detect and help prevent unauthorized access, monitor for malicious activities, and identify vulnerabilities by examining the flow of data through a network. Additionally, developers use packet analyzers to test and debug network protocols, ensuring that applications interact with the network as intended. Popular tools like Wireshark, tcpdump, and SolarWinds offer varying degrees of functionality, from simple packet capture to advanced network traffic analysis, making packet analyzers versatile tools in both network management and cybersecurity.

**Applications of Packet Analyzers**

* **Network Monitoring and Troubleshooting:** Identifies network bottlenecks, misconfigurations, and connectivity issues.
* **Security Analysis:** Detects unauthorized access, malware, and suspicious activities.
* **Performance Optimization:** Analyzes traffic patterns to improve network performance.
* **Protocol Development and Debugging:** Assists developers in testing and debugging network protocols.

b. Explain the types of packet analyzers.

**Types of Packet Analyzers**

**1. Network Tap Analyzers:**

**Explanation:** Network Tap Analyzers rely on hardware devices called network taps to physically intercept network cables and capture all data passing through. They offer a passive monitoring approach, ensuring that the network's performance and integrity are unaffected during the analysis.

**Example:**

* Garland Technology Network Taps
* NetOptics Bypass Switch
* Datacom Systems TAPs

**2. Software-Based Packet Analyzers:**

**Explanation:** These packet analyzers are software applications installed on computers or servers to capture and examine network traffic on specific segments. They are versatile and widely used for various purposes, including troubleshooting and security monitoring.

**Example:**

* Wireshark
* tcpdump
* Microsoft Network Monitor

**3. Inline Packet Analyzers:**

**Explanation:** Inline packet analyzers are deployed directly within the network path, such as within firewalls or routers. They not only monitor network traffic but also have the capability to block or alter packets based on predefined rules, making them suitable for proactive security measures.

**Example:**

* Cisco Firepower
* Palo Alto Networks Next-Generation Firewall
* Juniper SRX Series Firewalls

**4. Remote Packet Analyzers:**

**Explanation:** Remote packet analyzers allow network administrators to capture and analyze traffic from distant locations without being physically present at the monitoring site. This capability is particularly useful for managing large-scale, distributed networks.

**Example:**

* SolarWinds Network Performance Monitor
* PRTG Network Monitor
* Nagios XI

**5. Protocol-Specific Packet Analyzers:**

**Explanation:** These analyzers focus on capturing and analyzing traffic for specific protocols like HTTP, FTP, or VoIP. They provide in-depth insights into the performance and behavior of specific applications or services on the network.

**Example:**

* SIPp (VoIP)
* Fiddler (HTTP)
* TShark (various protocols)

**6. Capture Appliances:**

**Explanation:** Capture appliances are dedicated hardware devices designed for long-term traffic capture and storage. These devices are optimized for high-speed data capture and are often used in environments where detailed and prolonged traffic analysis is required.

**Example:**

* EndaceProbe
* Riverbed SteelCentral
* VSS Monitoring Distributed Series

c. Dinesh a tech evangelist is interested to learn about packet analyzer tools and decided to use Wireshark. Dinesh trust in you, now your job is help Dinesh in learning Wireshark, now help Dinesh in installing Wireshark tool .

**Step 1:** Visit the official Wireshark website using any web browser. A page with different installers of Wireshark will be shown. Click on ‘Windows x64 Installer’.A screenshot of a computer

Description automatically generated

**Step 2:** Once the download is complete, open it. Setup screen will appear, click on Next.A screenshot of a computer

Description automatically generated

**Step 3:** The next screen will be of License Agreement, click on Noted.A screenshot of a computer

Description automatically generated

**Step 4:** This screen is for choosing components, all components are already marked so don’t change anything just click on the Next button.A screenshot of a computer

Description automatically generated

**Step 5:** This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.A screenshot of a computer program

Description automatically generated

**Step 6:** The next screen will be of installation location so choose the drive which will have sufficient memory space for installation. It needs only a memory space of 261.6 MB.A screenshot of a computer

Description automatically generated

**Step 7:** Next screen has an option to install Npcap which is used with Wireshark to capture packets. pcap means packet capture so the install option is already checked don’t change anything and click the next button.A screenshot of a computer

Description automatically generated

**Step 8:** Next screen is about USB network capturing so it is one’s choice to use it or not, click on Install.

A screenshot of a computer error

Description automatically generated

**Step 9:** After this installation process will start. This installation will prompt for Npcap and USBPcap installation. Agree to everything and click on next.A screenshot of a computer

Description automatically generated

**Step 10:** After the installation process of Wireshark is complete click on the Next button.

A screenshot of a computer

Description automatically generated

**Step 11:** Click on Finish after the installation process of Wireshark is complete. Wireshark is successfully installed on the system and an icon is created on the desktop.A screenshot of a computer

Description automatically generated

**Step 12:** Now run the software and see the interface. At this point, you have successfully installed Wireshark on your windows systemA screenshot of a computer

Description automatically generated

d. Now help Dinesh to understand the overview of Wireshark.

**Overview of Wireshark**

Wireshark is a powerful, widely used network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It is an essential tool for network administrators, security professionals, and developers who need to diagnose network problems, troubleshoot issues, or analyze network traffic for security purposes.

**Key Features of Wireshark:**

* **Packet Capture:** Wireshark captures network packets in real-time, providing detailed information about each packet, including headers, payloads, and metadata. Users can capture traffic from live networks or read from previously saved capture files.
* **Detailed Protocol Analysis:** Wireshark supports a vast array of network protocols, offering detailed analysis and decoding for over a thousand protocols, including TCP/IP, HTTP, DNS, FTP, and many more. This makes it invaluable for understanding how different protocols operate and interact within a network.
* **User-Friendly Interface:** Wireshark's graphical user interface (GUI) is designed to be user-friendly, making it easier to navigate through captured data. The interface allows users to apply filters, search for specific data, and highlight important information.
* **Powerful Filtering Capabilities:** Wireshark provides robust filtering tools, allowing users to focus on specific types of traffic or packets of interest. Display filters, capture filters, and coloring rules can be applied to quickly isolate relevant data.
* **Cross-Platform Availability:** Wireshark is available on multiple platforms, including Windows, macOS, and Linux, making it accessible to a broad range of users.
* **Open-Source and Extensible:** Wireshark is an open-source tool, meaning it is freely available and supported by a large community. Users can extend its functionality by writing custom dissectors or plugins to analyze new or proprietary protocols.

**Common Use Cases:**

* **Network Troubleshooting:** Wireshark helps identify network bottlenecks, latency issues, and misconfigurations by analyzing packet flows and protocol behaviors.
* **Security Analysis:** Security professionals use Wireshark to detect malicious traffic, investigate security incidents, and analyze attacks such as packet sniffing, man-in-the-middle attacks, and more.
* **Protocol Development:** Developers use Wireshark to debug and test network protocols, ensuring they function correctly during communication between devices.
* **Educational Purposes:** Wireshark is a valuable educational tool, helping students and professionals learn about network protocols and their operations by providing a hands-on, interactive experience.

e. While you are explaining the overview of Wireshark Dinesh observed some IP address in the packet capturing window, Dinesh want to extract the information of particular IP address and see where it is going and from where it is receiving the information, help Dinesh to filter particular IP address and its source and destination.

**Step 1: Open Wireshark:** Launch Wireshark and start capturing packets on the desired network interface or open a saved capture file.

**Step 2: Start Packet Capture:** Begin capturing packets or load an existing capture to analyze.

**Step 3: Apply IP Address Filter:**

* Use ip.addr == 192.168.70.99 to filter traffic for a specific IP address.
* For filtering by source or destination, use ip.src == 192.168.70.99

**Step 4: Analyze Filtered Traffic:** Review the source and destination addresses to understand where the traffic is coming from and going to.

* **Time:** Timing of each packet captured during a network session.
* **Source:** The IP address that sent the packet.
* **Destination:** The IP address that received the packet.
* **Protocol:** The protocol used (e.g., TCP, UDP, HTTP).
* **Length:** Size of each packet captured during the network session.
* **Info:** Additional information about the packet, such as the ports used.

**Step 5:** **Examine Packet Details:** Click on any packet to view its detailed information in the packet details pane.

**Step 6: Export Filtered Data:** If needed, export the filtered packets for further analysis.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Result:**

Thus, the network traffic was analysed using Wireshark tool and the commands were executed and verified successfully.