**ASSIGNMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **COURSE** | Deep Packet Inspection | **ASSIGNMENT NO** | Final 1 |
| **MODULE** | DPI | **ASSIGNMENT DATE** | 14/09/2024 |
| **STUDENT NAME** | Konganti Chaithanya kumar | **SUBMISSION DATE** | 14/09/2024 |

**Theory Questions**

------------------------------------------------------------------------------------------------------

1. Which Wireshark filter can be used to monitor outgoing packets from a specific system in the network?
2. How do I use Wireshark to find a password in my network (for both HTTP and HTTPS)?
3. How do I modify Wireshark packets on-the-fly?
4. What exactly does Wireshark do? Explain.
5. How do I create a profile in Wireshark?

------------------------------------------------------------------------------------------------------

**1. Which Wireshark filter can be used to monitor outgoing packets from a specific system in the network?**

**ANS:**

Wireshark filter to monitor outgoing packets: To monitor outgoing packets from a specific system, you can use the filter **ip.src == <IP address>. For E.g**, if the IP address of the system is **192.168.1.5**, the filter would be **ip.src == 192.168.1.5.**

**2. How do I use Wireshark to find a password in my network (for both HTTP and HTTPS)?**

**ANS:**

**Finding a password in your network using Wireshark:**

* HTTP: For HTTP traffic, you can use the filter http.request.method == "POST" to find POST requests, which often contain login credentials. Look for the Authorization header or form data in the packet details.
* HTTPS: HTTPS traffic is encrypted, so you cannot directly see passwords. However, if you have access to the server’s private key, you can use it to decrypt the traffic in Wireshark.

**3.How do I modify Wireshark packets on-the-fly?**

**ANS:**

Modifying Wireshark packets on-the-fly: Wireshark itself does not support modifying packets on-the-fly. For this purpose, you can use tools like Scapy or tcpreplay to modify and replay packets.

**4.What exactly does Wireshark do? Explain.**

**ANS:**

Wireshark is a network protocol analyzer that captures and displays packets in real-time. It allows you to inspect the details of network traffic, troubleshoot network issues, analyze protocols, and monitor network activity. It supports a wide range of protocols and provides powerful filtering and search capabilities.

**5.How do I create a profile in Wireshark?**

**ANS:**

* Creating a profile in Wireshark: To create a profile in Wireshark:
* Go to Edit > Configuration Profiles.
* Click on New to create a new profile.
* Name your profile and click OK.
* Customize the profile by adjusting settings such as display filters, color rules, and column layouts.