# CYBER SECURITY INTERNSHIP

# Task 5: Capture and Analyze Network Traffic Using Wireshark

# **Objective**

The objective of the task was to capture live network packets using Wireshark, analyze them, and identify different network protocols.

### **Tools Used**

- Wireshark (Free and open-source packet analyzer)
- Active Internet Connection

#### **Procedure**

- · Installed and opened Wireshark.
- Selected the active network interface for packet capture.
- Initiated browsing and ping requests to generate traffic.
- Stopped the capture after ~1 minute.
- Applied filters to analyze traffic by protocol (e.g., HTTP, DNS, TCP).
- Identified at least 3 different protocols in the capture.
- Exported the capture as a .pcap file.
- · Documented findings and packet details.

# **Findings**

During the analysis, the following protocols were identified:

DNS Packets	TCP Packets	HTTP Packets
CYBER SECURITY INTERNSHIP Task 5: Capture and Analyze Network Traffic Using Wireshark	CYBER SECURITY INTERNSHIP Task Si Capture and Analyse Network Traffic Using Wireshark	CYBER SECURITY INTERNSHIP Task 5: Capiture and Analyze Network Traffic Using Wireshark
Objective The eligentive of the task was to respitate live network packets using Winselse's analyse their, and analyse different network protocols.	Objective The eliquative of the tests was to register the network perfects using Wiresharks analyze from and analyze different network protocols.	Objective The infigurities of the task was to respitate the network packets using Wireshark, analyse their, and analyze different network protocols.
Tools Used Using Wiresharases and spansanurus pasibel analyses	Tools Used Users Wiresturgers and open-source probet analyzer	Tools Used Living Winnelmore and open-assurer pushed analyzer
Procedure:  I invalidate and supervised Wireselbark.  I invalidate and supervised Wireselbark.  I invalidated biomedical string respirate to generate seaffle.  I initiated biomedical string and pring respirate to generate seaffle.  I invalidated biomedical string respirate to the seaffle.  I invalidated biomedical string string respirate to the seaffle.  I invalidate biomedical string string string string string string string string string.  I interviting all locals 3 affletions (services string seaffleting) string	Procedure:  I. Investigate and opportunit Watendorsk.  I. Investigate and opportunit Watendorsk.  I. Investigate Annual State of the Conference of the globalist Colorbors.  It invisionable themsoning und print, research for generate transport.  It is invisionable themsoning und print, research to generate transport.  It is invisionable themsoning und print or "Invisional".  It is invisionable to the Conference of the Confe	Procedure:  1. Invasion and agreement Wirescharts.  2. Invasion for the procedure of the pr
Findings TEP Paulute HTTP Paulute	Findings TCP Packets HTTP Packets	Findings TEP Paskets HTTP Paskets
Control Control Control	Control of the second s	THE PARTY OF THE P
Chinames  Stocked Cance Capitured and ensistant flow packets.  Stocked Cance Capitured and ensistant flow packets.  Stocked Cance Capitured and ensistant flow packets.  Stocked Capitured	Guissanse  Buccool cance captured and analyzed tine packets,  special cance captured and analyzed tine packets,  specially muriple protects including OND, TOO and EVITO employet.  Handson as segmentare for notwesh transferancing.	Observation of the contract and analyzed the packets, standard mustiple protects including OHA, TOP and ETTP regions. Identified mustiple protects including OHA, TOP and ETTP regions. Hands-un expensions in network translationary.
Rey Convergets Learness   Index-view Guesslans & Antoness   - Products regiment   L. Wards & Microslands cased for P - Products analysis   A packed analysis for the product of the produc	Key Gismenya Lantonad Index view Quantition & Antonomia Lantonomia	Ferg Garanguis Learnand  - Persista requires  - Profession desiriques  - Profession desiriques  - Profession desiriques  - Fattening in Willenstein American desiriques and analysis established access from?  - Fattening in Willenstein  - Estatening in Willenstein  - Fattening in William  - Fatt

#### **Outcome**

- · Successfully captured and analyzed live packets.
- Identified multiple protocols including DNS, TCP, and HTTP.
- Hands-on experience in network troubleshooting and protocol analysis.

## Key Concepts Learned

- Packet Capture
- Protocol Analysis
- TCP/IP Layers
- Filtering in Wireshark
- Network Troubleshooting

#### Interview Questions & Answers

#### Q1 What is Wireshark used for?

A packet analyzer for capturing and inspecting network traffic.

#### Q2 What is a packet?

A small unit of data transmitted over a network.

#### Q3 How to filter packets in

Wireshark? By using filters such as tcp,

http, dns.

#### Q4 Difference between TCP and UDP?

TCP is reliable and connection-oriented, UDP is faster but connectionless.

### Q5 What is a DNS query packet?

A request sent by a client to resolve a domain name to an IP address.

#### Q6 How can packet capture help in troubleshooting?

By identifying issues such as dropped packets or misconfigurations.

### Q7 What is a protocol?

A set of rules governing communication between devices.

## Q8 Can Wireshark decrypt encrypted traffic?

Not directly, unless encryption keys are provided.

# Filter captured packets by protocol (HTTP, DNS, TCP).





