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
		

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.

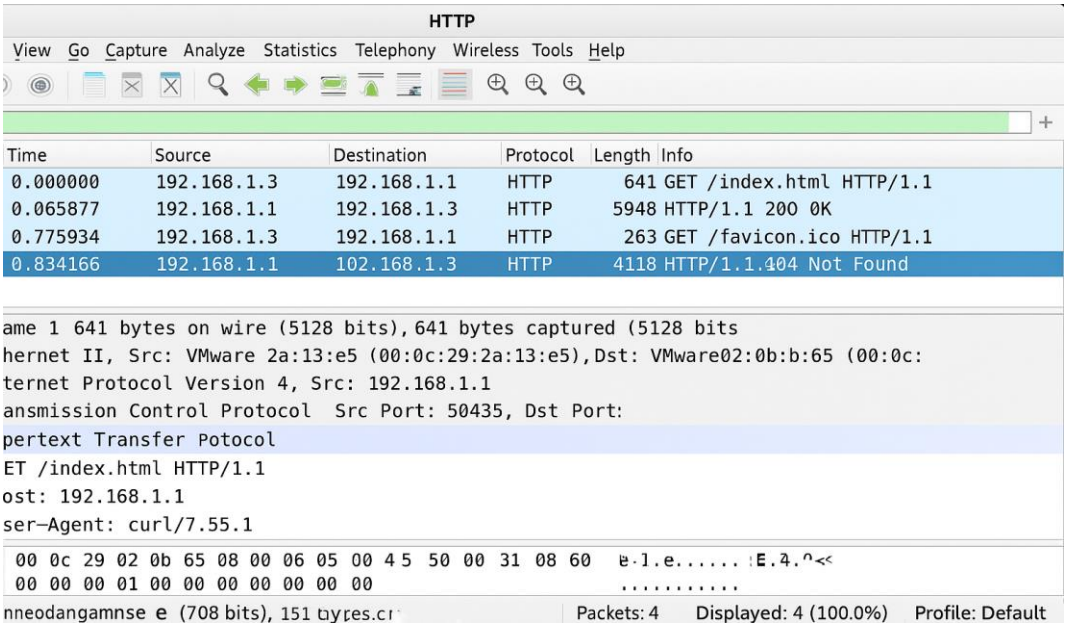
Q5 What is a DNS query packet?
A request sent by a client to resolve a domain name to an IP address.

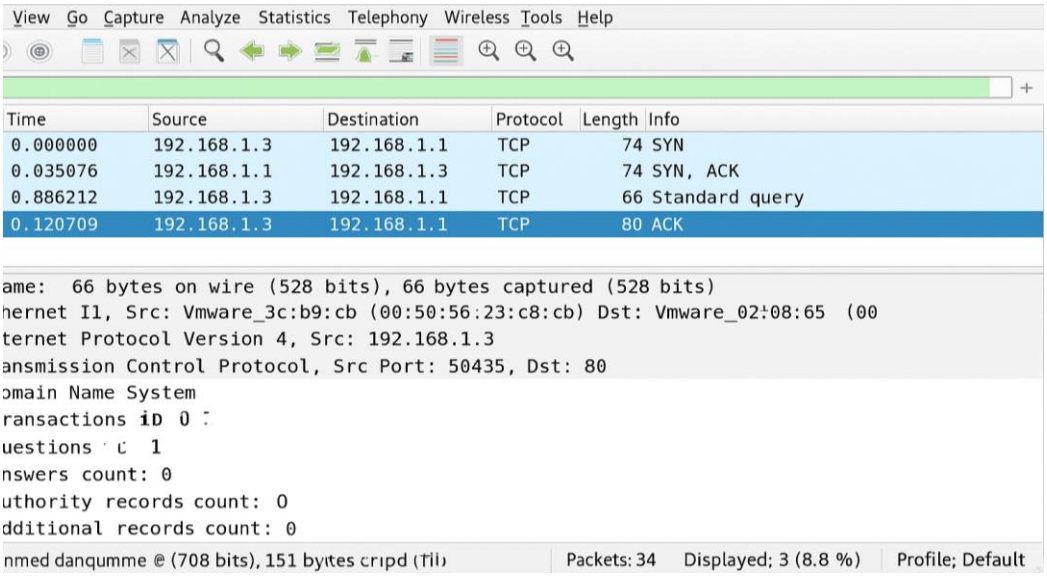
Q6 How can packet capture help in troubleshooting?
By identifying issues such as dropped packets or misconfigurations.

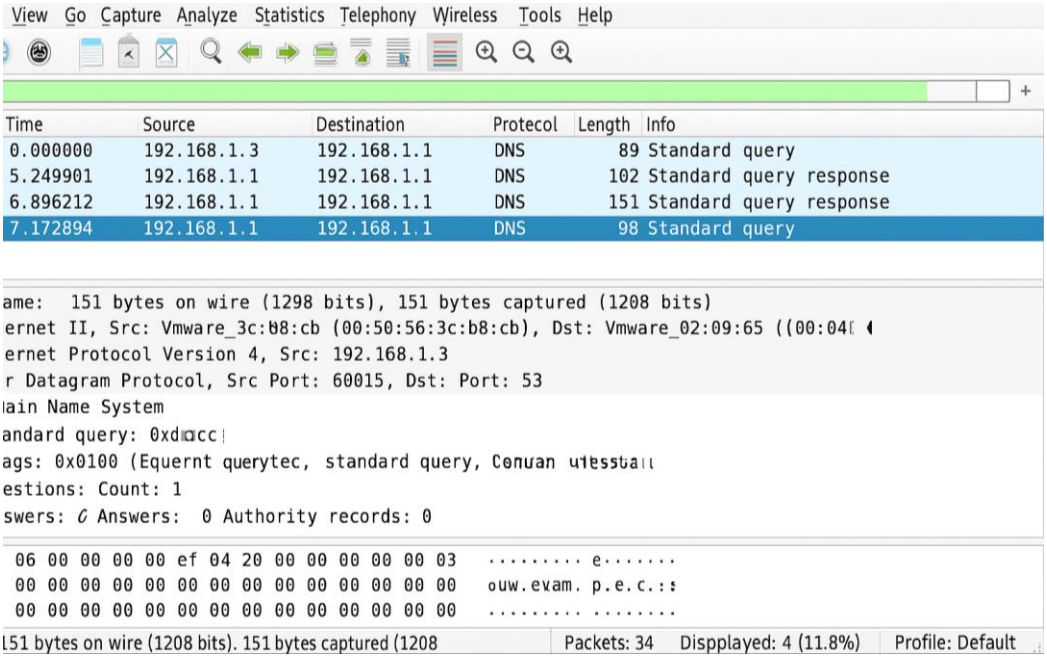
Q7 What is a protocol?
A set of rules governing communication between devices.

Q8 Can Wireshark decrypt encrypted traffic?
Not directly, unless encryption keys are provided.

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




View Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source Destination Protocol Length Info
0.000000 192.168.1.3 192.168.1.1 TCP 74 SYN
0.035076 192.168.1.1 192.168.1.3 TCP 74 SYN, ACK
0.886212 192.168.1.3 192.168.1.1 TCP 66 Standard query
0.120709 192.168.1.3 192.168.1.1 TCP 80 ACK
ame: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
hernet I1, Src: Vmware_3c:b9:cb (00:50:56:23:c8:cb) Dst: Vmware_02:08:65 (00
ternet Protocol Version 4, Src: 192.168.1.3
ansmission Control Protocol, Src Port: 50435, Dst: 80
omain Name System
ransactions ID 0
uestions 1
nswers count: 0
uthority records count: 0
dditional records count: 0
nmed danqumme @ (708 bits), 151 bytes cripd (Tii)
Packets: 34 Displayed; 3 (8.8 %) Profile; Default


View Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source Destination Protocol Length Info
0.000000 192.168.1.3 192.168.1.1 DNS 89 Standard query
5.249901 192.168.1.1 192.168.1.1 DNS 102 Standard query response
6.896212 192.168.1.1 192.168.1.1 DNS 151 Standard query response
7.172894 192.168.1.1 192.168.1.1 DNS 98 Standard query
ame: 151 bytes on wire (1298 bits), 151 bytes captured (1208 bits)
ernet II, Src: Vmware_3c:b8:cb (00:50:56:3c:b8:cb), Dst: Vmware_02:09:65 ((00:04
ernet Protocol Version 4, Src: 192.168.1.3
r Datagram Protocol, Src Port: 60015, Dst: Port: 53
lain Name System
andard query: 0xd
ags: 0x0100 (Equernt querytec, standard query, Conuan
estions: Count: 1
swers: 0 Answers: 0 Authority records: 0
06 00 00 00 00 ef 04 20 00 00 00 00 00 03 ..... e.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 ouw.evam. p.e.c.:s
00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
151 bytes on wire (1208 bits). 151 bytes captured (1208
Packets: 34 Dispplayed: 4 (11.8%) Profile: Default