



PROJECT MODULE
TASK

WIRESHARK PCAP ANALYSIS

CYBERSECURITY & ETHICAL HACKING PROJECT TASKS



PROJECT MODULE

WIRESHARK PCAP ANALYSIS

Background

A PCAP file is a saved copy of captured network traffic. Network engineers and security teams open PCAP files later to find out what happened on a network, without being there at the time.

In this lab you receive a PCAP file taken from a laptop that opened the website microsoft.com. Open it in Wireshark and read the same DNS and TLS information that you found in the live capture lab.

Task

Open the PCAP file Wireshark_Lab2_Microsoft_DNS_v2.pcap in Wireshark on your Windows laptop, then find the six answers below in the packets.

PCAP file: Wireshark_Lab2_Microsoft_DNS_v2.pcap (your instructor will share it with you)

Questions to answer:

1. What is the IP address of the laptop that took this capture?
2. What is the IP address of the DNS server?
3. Which IP addresses did the DNS server return for microsoft.com?
4. Which website name (Server Name) is sent in the TLS Client Hello?
5. Which server port is used for the secure connection?
6. Which TLS version does the website use?

Submit one screenshot of Wireshark showing the DNS answers for microsoft.com, and your answers to the six questions.

Solution

STEP 1

Open Wireshark. Click **File > Open**, select the PCAP file and click **Open**. The packets load in the list. The bottom bar shows how many packets the file has.

STEP 2

Type this in the display filter bar and press Enter:

```
dns.qry.name == "microsoft.com"
```

You should see four packets, two queries and two replies. The first query asks for the IPv4 address (A) and the second asks for the IPv6 address (AAAA).

Click the first query. The Source is the laptop and the Destination is the DNS server.

Answer1: Laptop IP is 192.168.0.105

Answer2: DNS Server IP is 8.8.8.8

STEP 3

Click the first reply (Standard query response A). In the middle pane expand Domain Name System (response), then Answers. Every Address line is an IP address of microsoft.com.

Answer3: The DNS server returned 20.70.246.20, 20.76.201.171, 20.112.250.133, 20.231.239.246 and 20.236.44.162

Tip: The reply to the AAAA query has no answer. You can ignore it.

STEP 4

Use this filter:

```
tls.handshake.type == 1
```

This shows the Client Hello, the first packet of a secure connection. Several websites appear in the list. Click the one that says SNI=microsoft.com. Its Destination is one of the IP addresses from Step 3. Then expand Transport Layer Security > Handshake Protocol: Client Hello > Extension: server_name.

Answer4: Server Name: microsoft.com

Then expand the Transmission Control Protocol line. The Destination Port is the Server port.

Answer5: Server Port is 443

Tip: You will see two Client Hello packets for microsoft.com. Both use the same server IP and port, so you can use either one.

STEP 5

Apply this filter:

```
tls.handshake.type == 2
```

This shows the Server Hello, the reply from the website. Pick the one where the Source is the website IP from Step 4. Look at the Protocol column. It shows the TLS version.

Answer6: TLS version is TLSv1.3



© All Rights are reserved, Networkwalks
Contact us today for your Cybersecurity & Network consultancy or your next training course & certification on
Cisco CCNA, Cybersecurity, Ethical Hacking, Python programming, Linux & AI.

 **+27 766 222 218 | +27 788 220 600**

Leave your feedback at: info@networkwalks.com. Your technical questions, comments & suggestions are always Welcomed.
www.networkwalks.com