



Wireshark

HOW I SOLVED A DNS OUTAGE USING WIRESHARK

A Cybersecurity Network
Analysis Lab





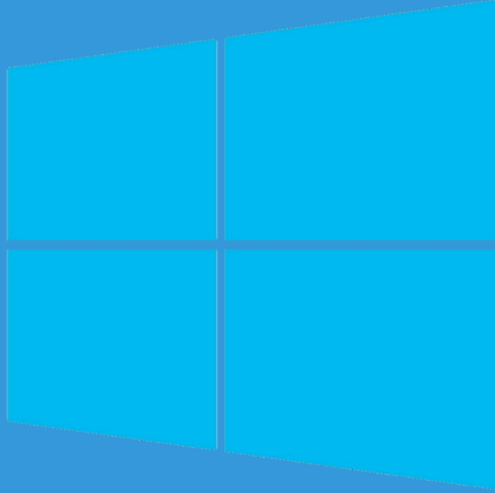
THE PROBLEM

Users reported:

'destination port unreachable'

when trying to access

www.yummyrecipesforme.com



Wireshark

MY TOOLS

1

Wireshark (traffic capture)

2

nslookup (DNS testing)

3

netsh (simulate DNS failure)

MY STEP-BY-STEP INVESTIGATION PROCESS

1

SET FAKE DNS

Changed DNS to 203.0.113.2 using netsh

2

START WIRESHARK CAPTURE

Began recording network traffic

3

TRIGGER DNS QUERY

Ran: nslookup
www.yummyrecipesforme.com

4

STOP CAPTURE

Clicked red square in Wireshark

5

FILTER PACKETS

Applied: dns → then icmp

6

ANALYZE & REPORT

Found no response → DNS failure

KEY INSIGHT

 The DNS service was unreachable — not the website.

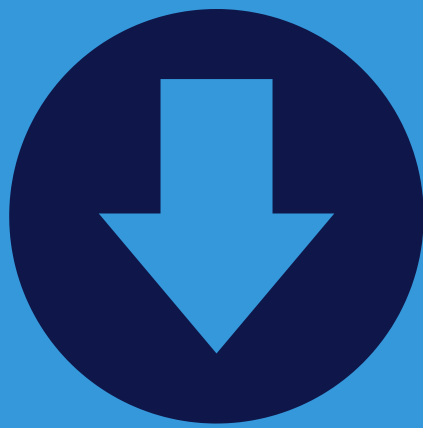
- Protocol affected: **DNS**
- Port: **UDP 53**
- Error type: **ICMP Port Unreachable (expected)**
- Real cause: **Misconfigured or down DNS server**



LESSONS & SKILLS GAINED

- **Packet analysis with Wireshark**
- **Understanding TCP/IP layers**
- **Simulating real-world outages**
- **Cybersecurity troubleshooting**
- **Documentation & reporting**

**CHECK OUT THE
FULL PROJECT
ON GITHUB!**



GITHUBLINK