DAY 3 – TASK 3: NETWORKING BASIC FOR CYBERSECURITY

TOOLS USED:

Wireshark to capture traffics in network

Linux terminal (wsl debian)

Networking concepts covered :

Dns

TCP, UDP, ICMP

HTTP traffic HTTPs not visible coz of encryption

PRACTICAL WORK

USED eth0 network interface to start live capture

Sent packets in bash and verified them in wireshark

Used PING command to generate ICMP traffic

Understood how ICMP echo request-reply packets

Used curl https://example.com to analyse traffic in tcp

Generated http traffic

Applied UDP and DNS display filters used nslookup openai.com 8.8.8.8 to capture dns standard query and response packets

Saved captured traffic as .pcapng file for offline analysis

Key notedowns:

ICMP – ping

TCP – curl UDP/DNS – nslookup