Network Forensics Test

Candidate: Nitin Yadav

Section A – ARP & DNS

1. How many total packets are in the capture?

2. What are the source and destination MAC addresses in the first ARP request packet?

3. Which IP address is being resolved in the initial ARP request/reply exchange?

4. What domain name is queried via DNS, and what IP address does the response resolve it to?

5. What source port does the client use for the DNS query, and what port is the query sent to?

Section B – HTTP

6. Identify the TCP three-way handshake packets for the HTTP connection (list SYN, SYN-ACK, ACK sequence/ack numbers).

7. What resource path is requested in the HTTP GET request, and what is the Host header value?

8. What HTTP status code does the server return, and what Content-Type is specified?

9. What server software is disclosed in the HTTP response headers?

Section C – FTP

10. What username is used to log into the FTP server?

11. What password is sent in cleartext, and in which FTP command?

12. What response code does the FTP server send after a successful login?

13. Why is FTP considered insecure, based on what you observed in this capture?

Section D – ARP Spoofing

14. How many ARP replies claim ownership of 192.168.1.1, and how many distinct MAC addresses are tied to that IP?

15. Which MAC address appears to be spoofing the router's IP, and how can you tell?

16. What could an attacker achieve with this kind of ARP spoofing?

Section E – Port Scan

17. Which source IP is performing a port scan against 192.168.1.20?

18. List all destination ports targeted during the scan.

19. Which ports responded with SYN-ACK (open) and which with RST-ACK (closed)?

20. Based on the SYN flag pattern and lack of completed handshakes, what scanning technique does this traffic represent?