Q1. OSI model

Q2. IDS, IPS – important

Q3. Arp poisoning

Q4. ICMP packet functions

Q5. Server fingerprinting & its features

Q6. Types of enumeration

Q7. Principles of security

Q8. Key function of cryptography principles

Q9. Attack vectors in network security

Q10. TCP & UDP scanning

Q11. WLAN based attacks

Q12. Network pentesting lifecycle

Q13. Application assessments of network pentest.

Q14. Network proxy in detail

Q15. Types of phishing attacks

Q16. Describe war driving with case study.

Q17. Difference between WEP & WPA

Q18. Explain network evidence acquisition process.

Q19. Network forensic investigation methodology

Q20. Difference between threat, vulnerabilities & attcks

Q21. Explain active &passive scanning

Q22. Explain regional internet registries.

Q23. Explain digital signatures.

Q24. What is event log aggregation?

Q25. Explain wlan pentesting

Q26. Network authentication & security flow / flaw case study.

Q27. Asymmetric & symmetric encryption.