Q1. Explain any 5 malware types. (Malware families explain)

Q2. Malware case study (1 or 2)

Q3. Explain 10 assembly commands.

Q4. Explain malware analysis phases (static, dynamic, etc)

Q5. Dependency walker

Q6. Clam AV

Q7. RegShot

Q8. Faking a Network

Q9. Wireshark for Packet analysis

Q10. What is the difference between Snap-Shot & Backup?

Q11. Sandboxing

Q12. Introduction to assembly

Q13. Stack pointer (memory pointer)

Q14. CPU registers

Q15. IDA pro

Q16. Breakpoints

Q17. Exceptions

Q18. Modification of programs (code review)(read the code and tell what the malware is doing)

Q19 DLL

Q20. Window registry commands

Q21. Behaviour of malware.

Q22. Other platform malware (Linux)

Q23. Hex code editor

Q24. Mapping of malware using sysinternals toolkits & wireshark

Q25. file less malware

Q26. Case study – file less malware, Log4j, etc.