1. Cổng SSL with HTTP dùng port gì? UDP 443 hay FTP 8080 hay UDP 8080 FTP 443 (t ko biết chọn gì, ghi lại phương án thôi)
2. Cái nào nhân bản/ không nhân bản: virus, trojan, worm,
3. Tấn công lỗi SQL: SQL Injection
4. Nghe lén: passive
5. Đứng giữa lấy thông tin là kiểu tấn công gì? Man in the middle
6. CIA: confidentiality - itegrility – availability
7. Xác nhận: anthentication
8. Phương thức bảo mật gì đó có liên quan đến mail: hình như là PGP
9. Mấy chữ cái viết tắt éo nhớ là cái gì nữa (nhớ học chứ viết tắt): IMTP, OTS, TC.. gì gì đó
10. Các câu hỏi phân biệt thì phải học các từ tiếng anh (tại biết tiếng việt nó là cái gì mà éo biết tiếng anh là cái gì -> éo chọn đc) : sesion hijacking, spoofing, nhiều nữa
11. Khóa công khai: gửi thông điệp thì dùng khóa công khai của ng nhận
12. Chữ kí số thì dùng khóa bí mật của người gửi
13. Chữ kí số đc dùng khóa của cơ sở hay công ty gì đó, nói chung là cái chỗ đc chứng nhận và chỗ đó dùng khóa bí mật của nó để mã hóa chữ kí số (câu này hàm ý vậy, ko nhớ chính xác nội dung)
14. Mã cesar: cho text, hỏi sau mã hóa thì thành cái gì
15. DDOS: active
16. Cesar: mã hóa thay thế: subsituation gì gì đó
17. Mã chuyển vị là transition
18. 1 câu hỏi kiểu 1 người tấn công vào mạng thì là hacker(?!) ờ thì chắc nó là hacker =,=
19. DES dùng block 64 bit, key 56 bit
20. RSA với DES khác biệt gì? (ko nhớ đáp án) + 1 số câu hỏi kiểu như ưu điểm của cái này so với cái kia
21. Hàm băm thì input tùy ý và output dài bằng nhau hay không ?
22. SSH thì ko có cái gì (éo nhớ phương án) nhưng nói chung câu này hàm ý nó hỏi xem trong 4 cái đáp án đưa ra có 1 cái SSH ko hỗ trợ
23. **Không có các câu tính toán** mã hóa cao siêu gì cả như tính **phi , n , d , e … của RSA**
24. 2 câu về mạng máy tính: Tracert dùng làm gì và liên quan tới cái tính bảo mật gì và 1 câu nữa nhưng ko nhớ nổi

Hiện tại nhớ đc như vậy =,=