1. Forklar følgende begreper – også med eksempel:
   1. Konfidensialitet (confidentiality)
   2. Integritet (integrity)
   3. Tilgjengelighet (availabilit
2. Forklar de 4 måtene vi kan forholde til risiko
3. Hvilke tre hovedelementer angår Attack Surface?
4. Forklar hva vi mener med Social Engineering og gi eksempler
5. Forklar mer inngående følgende:
   1. perimeter security
   2. internal perimete
6. Forklar hvordan er keylogger fungerer
7. Hvordan defineres kryptering og dekryptering?
8. Forklar kort prinsippene med symmetrisk kryptering.
9. Forklar kort prinsippene med asymmetrisk kryptering.
10. Forklar kort hvordan hash fungerer.
11. Hva mener vi med PKI og CA?
12. Forklar kort hva IPsec er og hvilke protokoller som inngår.
13. Hvordan fungerer VPN? Hvilke 4 typer har vi lært om?
14. Hvorfor bør man bruke auditing?
15. Gjør greie for hver av A’ene i AAA
16. Hva er biometri?
17. Hva er to-faktor autentifisering?
18. Hvilke features gir NTFS oss?
19. Hva betyr det å ta ownership til en mappe eller en fil
20. Hva betyr principle of least privilege og hvordan kan vi implementere det?
21. Hvordan hjelper «Account Lockout» oss mot hacking?
22. Hva må være med i et komplekst passord?
23. Forklar :
    1. Packet Filtering Firewall
    2. Circuit Level Firewall
    3. Application Level Firewall
    4. Stateful / Stateless
    5. IDS
    6. IPS
    7. VLAN
    8. DMZ
    9. SSID
24. Hva mener vi med malware?
25. Forklart kort de ulike typene malware :
    1. Virus
    2. Orm
    3. Trojanske Hester
    4. Adware
    5. Spyware
    6. Rootkits
    7. Back Doors
    8. Ransomware
26. Hva er en proxy-server?
27. Hva er spam?
28. Hva er SPF-records?