Aantekeningen Cyber 1

Termen

1. **Isolatie**
2. **Compartimentere**
3. **Beperkingen**
4. **Volldigheid**
5. **Functiesscheiding**
6. **Veilige dafaults**
7. **Open ontwerp**
8. **Ergonomie**
9. **Redudantie**
10. **Diversiteit**
11. **Onderhoud**
12. **Registratie**

Het pentest-practicum wk 1 t/m 4

- Twee computers als VM
  - kunnen werken op je latptop
- Computer 1 Kali linux
- Computer 2 Windows machine

Transpositie

- Transpositie is het verwisselen van volgorde van de symbolen
- De spartanen pasten dit reeds toe in de oudheid "scytale" (*Opm. Bij de scytale is er een transposite van een vaste afstand bv Caeser cypher*)

Substitutie 1: Caesar

- Substitutie is het vervangen van symbolen voor andere symbolen uit het alfabet
- Caesar gebruikte voor codering van militaire berichten een vaste verschuiving (shift)
- De sleutel is de letter waarnaar A wordt geschoven
- Omdat de substitue gelijk is vooe elk symbool spreekt men van mono-alfabetische substitutie

Substitutie 2: S-box

- Substitutie op bassis van een lookup-tabel
- De complete tabel is de sleutel
- Dit is ook een mono-alfabetische

Poly-alfabetische substitutie: Vignère

Substitutie 3: Enigma

-