1. **Introducción a la seguridad**
    - 1.1. Privacidad, anonimato y pseudo anonimato
        - 1.1.1. Mass surveillance
    - 1.2. Seguridad
        - 1.2.1. Assets
        - 1.2.2. Etapas de la seguridad
        - 1.2.3. Modelos de seguridad
    - 1.3. Amenazas
        - 1.3.1. Hackers, crackers,ciber-criminales hacktivistas
        - 1.3.2. Vulnerabilidades, zero days
        - 1.3.3. Malware
        - 1.3.4. Ingenieria Social
            - 1.3.4.1. Phishing, Vishing, Smishing
    - 1.4. Introducción a Operational Security (OPSEC)

2. **Cifrados y esteganografía**
    - 2.1. Cifrado simétrico
    - 2.2. Cifrado asimétrico.
    - 2.3. Funciones Hash
        - 2.3.1. CheckSums
        - 2.3.2. Salt bits, rainbow tables
    - 2.4. Certificado digital y entidades certificadoras
    - 2.5. SSL y TLS
    - 2.6. HTTPS,HPKP,HSTS
        - 2.6.1. Problemas con los certificados
    - 2.7. Esteganografía
    - 2.8. Metadatos
    - 2.9. Contraseñas
        - 2.9.1. Complejidad de contraseñas
        - 2.9.2. Ataques con diccionarios
        - 2.9.3. Manejadores de contraseñas y MFA

3. **Aislamiento y compartimentalización**
    - 3.1. Dominios de Seguridad
    - 3.2. Aislamiento físico
    - 3.3. Aislamiento Virtual
        - 3.3.1. Sandboxes
        - 3.3.2. Máquinas virtuales y ambientes de prueba
    - 3.4. Distribuciones orientadas a seguridad

4. Seguridad y privacidad en redes

- 4.1. Firewalls
  - 4.1.1. Host based
  - 4.1.2. Network based
  - 4.1.3. Evadiendo firewalls
    - 4.1.3.1. Deep packet inspection(DPI)
- 4.2. Seguridad en redes wireless
  - 4.2.1. WEP, WPA, TKIP,CCMP,wpa2,wpa2 enterprise
  - 4.2.2. Debilidades y Hardening
- 4.3. Introducción a syslog
- 4.4. SSH
- 4.5. Navegación privada
  - 4.5.1. Tracking y fingerprinting
  - 4.5.2. Proxys
  - 4.5.3. VPN
  - 4.5.4. Tor
  - 4.5.5. Análisis de tráfico.