# Leeswijzer CS semester 4

Luc van den Acker

Deze documentatie demonstreert mijn kennis en vaardigheden in het domein van Ethical Hacking, Security Engineering, en Risk Consulting. Het doel is om te laten zien dat ik in staat ben om beveiligingsrisico’s te analyseren, beveiligingsmaatregelen te implementeren en te reageren op incidenten op een methodische wijze.

**1. Ethical Hacking en Pentesting**

* **Onderzochte Hackmethodieken**:
  + Path Traversal
  + File Inclusion
  + Command Injection
  + SQL Injection
  + XSS (Cross-Site Scripting)
  + CSRF
* **Bewijslast voor de Basic Hacking and Pentesting Process**:
  + **Pentest Rapport Cubics IT**: Bevat de resultaten van de pentest en de methodologie achter deze resultaten.
  + **Projectplan Pentest Cubics IT**: Documenteert de aanpak en stappen die zijn genomen voor de uitvoering van de pentest.
  + **Ethical Hacker Document**: Beschrijft alle bovenstaande hackmethodieken en de uitgevoerde activiteiten, exclusief de basic hacking en pentesting process.

**2. Security Engineering**

* **Infrastructuur Realisatie**:
  + Aandacht voor functionele en niet-functionele vereisten zoals beveiliging, monitoring, ethiek, compliance en gebruiksvriendelijkheid.
* **Bewijslast**:
  + **Network Separation and Segmentation**: Oprichting van een gesegmenteerd netwerk met diverse subnetten en services.
  + **Firewall Rules**: Documentatie van firewallregels die zijn toegepast op het gesegmenteerde netwerk.
  + **Secure Network Connections**: Uitleg over veilige verbindingen en gebruikte protocollen.
  + **VPN Setup**: Beschrijving van de opzet van een VPN en zijn functionaliteiten.
  + **Identity & Access Management**: Toelichting op de technieken en praktijken binnen IAM.
  + **IT System Hardening**: Identificatie van veelvoorkomende problemen en oplossingen voor systeemverharding.
  + **Veilige Software Oplevering**: Onderzoek naar de vereisten voor het opleveren van veilige software.

**3. Risk Consultant**

* **Risicoanalyse**:
  + Te vinden in het *Pentest Rapport Cubics IT*, hoofdstuk 2, en het *Risk Consultant Document*.
* **Business Continuity & Risk Mitigation**:
  + Uitleg over de begrippen en hun toepassing binnen een organisatie, gedocumenteerd in het *Risk Consultant Document* en mijn *Body of Knowledge*.

**4. Incident Response**

* **Procedurele Respons voor Beveiligingsincidenten**:
  + **Interview Security Incident Management**: Gesprekken met Jean-Paul Sablerolle, Crisismanager bij Cubics IT, over incidentmanagement.
  + **Onderzoek naar Common Vulnerabilities and Exposures (CVE's)**: Inzicht in kwetsbaarheden, met een focus op OV-chipkaarten, gedocumenteerd in mijn *PVI*.

**Conclusie**

Deze leeswijzer biedt een overzicht van mijn relevante vaardigheden, de methodieken die ik heb bestudeerd, en de bewijslast die mijn kennis en ervaring op het gebied van ethical hacking, security engineering, en risicoanalyse onderbouwt. Elk document en rapport fungeert als bewijs van mijn vermogen om te opereren binnen deze complexe en steeds veranderende disciplines.

Deze samenvatting kan dienen als een leidraad voor het presenteren van je vaardigheden en ervaringen in sollicitaties of andere professionele contexten.