# Basic Security

## 2018-2019

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **MODULEBOEK Basic Security** | | | | | | | | |
| **KENMERKEN** | | | | | | | | |
| **Studiepunten: 3** | | | **Studiebelastinguren:** 84  Contacturen:  - Kennisoverdracht: 14  - Begeleide kennisverwerking: 14  Zelfstudie: 56 | | | **Verantwoordelijke lector:   Bram Heyns** | | |
|  | | | | |  | | | |
| **BASISCOMPETENTIES — DOELEN** | | | | | | | | |
| **Algemene competenties**   * Projectmatig werken * Verwerven en verwerken van informatie | | | | | **Algemene beroepsgerichte competenties** | | | |
| **Beroepsspecifieke competenties** | | | | | **Doel** | | | |
| TIN\_R01\_C04 | | De student kan informatiesystemen ontwerpen die tegemoet komen aan de behoeften van de opdrachtgever, die proactief inspelen op de ontwikkelingen en mogelijkheden tot uitbreiding bevatten | | | * De student kan de verschillende basisconcepten van een veilige netwerkconnectie begrijpelijk uitleggen, bv a.d.h.v. het OSI model | | | |
| TIN\_R02\_C01 | | De student kan in een multidisciplinaire omgeving methoden selecteren en toepassen voor softwareontwikkeling en voor het opzetten van computer- en netwerksystemen | | | * De student kan een systeem of netwerk evalueren naar beveiligingsniveau, en eventueel optimalisaties implementeren om tot een veiliger systeem te komen | | | |
| TIN\_R02\_C11 | | De student kan beveiligingsaspecten van een informatiesysteem evalueren en implementeren | | |  | | | |
| TIN\_R04\_C02 | | De student kan teststrategieën opstellen | | |  | | | |
| TIN\_R05\_C03 | | De student kan mondeling en schriftelijk informatie communiceren, presenteren, en toelichten aan leken en aan specialisten rekening houdend met de diversiteit van de betrokkenen | | |  | | | |
| TIN\_R05\_C04 | | De student kan de ontwikkelde toepassingen/systemen overtuigend voorstellen als oplossing voor de behoefte van de klant | | |  | | | |
| TIN\_R05\_C07 | | De student kan gebruik maken van het technisch en commercieel jargon uit de (internationale) IT-wereld | | |  | | | |
|  | | | | |  | | | |
|  | | | | |  | | | |
| **INHOUD** | | | | | | | | |
| De cursus Basic Security bestaat uit 2 delen.  Deel 1 is het cryptografisch gedeelte waar getracht wordt om veilige communicatie op het internet uit te leggen, nml. https (en IPsec). Om deze communicatie te begrijpen worden eerst volgende concepten behandeld: symmetrische en asymmetrische encryptie met hun voor- en nadelen, hashing technieken en digitale handtekeningen, waarvoor dan weer certificaten nodig zijn, die door een PKI worden uitgereikt.  Deel 2 van de cursus is eerder gefocust op systeem- en netwerkbeveiliging. Dit deel bestaat uit een veelvoud van concepten uit de cyber crime wereld, zoals virus, worm, trojan, rootkit, spoofing, DDoS aanvallen, sniffers, poort- en kwetsbaarheidsscanners,… Er wordt getracht om deze concepten vanuit 2 perspectieven te belichten: enerzijds vanuit het standpunt van een hacker, en anderzijds vanuit het standpunt van de verdediging tegen deze hackers. | | | | | | | | |
|  | | | | |  | | | |
| **GEWENSTE BEGINSITUATIE** | | | | | | | | |
| * Voldoen aan de eindcompetenties van Math for IT * Voldoen aan de begincompetenties van .NET Advanced 1 of Java Advanced 1 | | | | | | | | |
|  | | | | |  | | | |
| **STRUCTUUR VAN DE CURSUS** | | | | | | | | |
| 1. Cryptografie    1. Inleiding    2. Geschiedenis    3. Symmetric-key cryptografie       1. 3DES, AES    4. Public key cryptografie       1. RSA, Diffie-Hellman, hashing, digitale handtekening    5. Hybrid cryptografie    6. Public Key Infrastructure       1. PKI componenten, certificaten    7. Beveiliging van het web       1. https met SSL / TLS, IPsec, online betalingen 2. Systeem- en netwerk-beveiliging    1. Virussen/wormen/trojans/rootkits    2. Firewalls    3. Spoofing    4. Port Scanners    5. Vulnerability Scanners    6. Intrusion Detection/Prevention Systems    7. Logging    8. Sniffers    9. (D)DoS attacks    10. Privacy en mythes | | | | | | | | |
|  | | | | |  | | | |
| **STUDIEMATERIAAL** | | | | | | | | |
| * Eigen hand-outs * Pluralsight * Digitaal leerplatform (<http://blackboard.pxl.be>)   + Eigen filmmateriaal (Vimeo/Kaltura) rond cryptografie   + Hierop komt evt ook extra materiaal en aankondigingen | | | | | | | | |
|  | | | | |  | | | |
| **PLANNING** | | | | | | | | |
| WEEK | DATUM | | DOELSTELLINGEN | CONTACTUREN | EVALUATIE | | STUDIETAAK (voorbereiding) | ZELFSTUDIE (voorbereiding) |
| 1+2 |  | | * De belangrijkste doelstelling van de eerste 4 lessen is om inzicht te krijgen over de werking van veilige communicatie op het internet. Daarvoor worden onderstaande aspecten behandeld in w1 * Ontstaan en evolutie van symmetrische encyrptie * Inzicht krijgen over de complexiteit van symmetrische cryptografische functies a.d.h.v. een case, nml. DES encryptie * Nut en verschillende manieren van asymmetrische encryptie bespreken * De voor- en nadelen van symmetrische en asymmetrische cryptografie met elkaar afwegen * Bespreking van hashing technieken | Uitleg over de praktijkopdracht  Uitleg over de belangrijkste topics, 1. a t.e.m. 1. e | Geen | |  |  |
| 3+4+5 |  | | * Inzicht verwerven over hybride cryptografie, nml. de voordelen van symmetrische en asymmetrische cryptografie combineren, gecombineerd met hashing * Security uitleggen adhv het OSI model * Werking en nut van certificaten * Inzicht krijgen over veilige communicatie over het internet a.d.h.v. 2 cases, nml. SSL (https) en SET, betalingen over het internet | Uitleg over de belangrijkste topics, 1.e t.e.m 1.g | Korte mondelinge feedback over de vorderingen van de praktijkopdracht | | * Mededeling van de teamleden (onderling af te spreken)/ * Start maken aan de praktijkopdracht, de basis moet afgewerkt zijn * Knowledge sharing doen tussen de eigen teamleden | Powerpoints (of movies) van Part 1 doornemen   * 1.a t.e.m. 1.e grondig bestuderen, zodat mogelijke vragen kunnen gesteld worden * 1.e. t.e.m. 1.g. al eens doornemen |
| 6+7+8 |  | | Inzicht krijgen in de belangrijkste items rond systeem- en netwerkbeveiliging, bekeken vanuit 2 perspectieven: de aanvaller en de verdediging | Uitleg over de belangrijkste topics, 2.a t.e.m 2. e | Korte mondelinge feedback over de vorderingen van de praktijkopdracht | | * PE opdracht verder afwerken. Het moet al een werkend programma zijn, maar nog niet helemaal gefinetuned * De basis Vulnerability Scans zijn al gebeurd, of er moet al een start zijn voor de infosec policy * Knowledge sharing doen tussen de eigen teamleden | * Powerpoints van Part1 grondig doornemen / bestuderen * Powerpoints van Part2 doornemen: 2.a t.e.m. 2.e. |
| 9+10+11 |  | | Inzicht krijgen in de belangrijkste items rond systeem- en netwerkbeveiliging, bekeken vanuit 2 perspectieven: de aanvaller en de verdediging | Uitleg over de belangrijkste topics, 2.f t.e.m 2.j | Korte mondelinge feedback over de vorderingen van de praktijkopdracht | | * Crypto Program volledig afwerken. * Vulnerability Scan opdracht afwerken / of de security policy * Knowledge sharing binnen het eigen team | * Powerpoints van Part 2 grondig doornemen / bestuderen |
| 12 |  | | Herhalingsles. Alle topics high level nog eens overlopen, en bespreking doen van het voorbeeldexamen. |  | Korte mondelinge feedback over de vorderingen van de praktijkopdracht | | * Ganse PE opdracht afwerken, en verdediging voorbereiden |  |
| 13+14 |  | | PE Evaluatieweken. Ieder team krijgt een timeslot toegewezen om hun mondelinge verdediging te doen van hun PE opdracht |  |  | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **OMSCHRIJVING STUDIETAAK (/TAKEN)**  **PE opdracht bestaat uit 3 aspecten, waarbij het team minstens 2 aspecten moet afwerken, en 1 aspect minstens tot minimaal niveau. Ieder aspect heeft een onderverdeling van basisniveau, minimaal niveau, en extra niveau (zie opdrachtbeschrijving).** | | | |
| **1 — Crypto Program (APPDEV)** | **SBU: 20 (minimaal) – 10 (basis)** | | **Evaluatie: 30% (minimaal) - 10% (basis)** |
| DOEL(EN) | OMSCHRIJVING | | STUDIEMATERIAAL — BRONNEN |
| * De verschillende basisconcepten rond crypto in de praktijk kunnen gebruiken: waarborgen van authenticiteit en integriteit van bestanden (hybrid crypto). | Zie document Opdracht\_BasicSecurity.docx | | * eigen hand-outs * Pluralsight |
|  | |  | |
| **2 — Vulnerability Scan (S&N)** | **SBU: 20 (minimaal) – 10 (basis)** | | **Evaluatie: 30% (minimaal) - 10% (basis)** |
| DOEL(EN) | OMSCHRIJVING | | STUDIEMATERIAAL — BRONNEN |
| * De student kan een systeem of netwerk evalueren naar beveiligingsniveau, en eventueel optimalisaties implementeren om tot een veiliger systeem te komen | Zie document Opdracht\_BasicSecurity.docx | | * eigen hand-outs * Pluralsight |
|  | |  | |
| **3 — Security Policy (IT MGMT)** | **SBU: 20 (minimaal) – 10 (basis)** | | **Evaluatie: 30% (minimaal) - 10% (basis)** |
| DOEL(EN) | OMSCHRIJVING | | STUDIEMATERIAAL — BRONNEN |
| * De student kan een systeem of netwerk evalueren naar beveiligingsniveau, en eventueel optimalisaties implementeren om tot een veiliger systeem te komen | Zie document Opdracht\_BasicSecurity.docx | | * eigen hand-outs * Pluralsight |
|  | |  | |
|  | |  | |
| **BEGELEIDING** | | | |
| * Je verwerkt de theoretische achtergrond van elk onderdeel op zelfstandige basis, en doet aan knowledge sharing binnen je team voor de praktijkopdracht * Tijdens de contacturen zullen de belangrijkste concepten besproken worden. Tevens zal er gewerkt kunnen worden aan, en feedback kunnen gegeven worden over, de praktijkopdracht. | | | |
|  | |  | |
| **EVALUATIE** | | | |
| * + Examen 60%, schriftelijk gesloten boek examen over de theoretische concepten. Kan hernomen worden voor 2de zit   + Permanente evaluatie: 40%, mondelinge (team)verdediging van de praktijkopdracht tijdens de laatste 2 weken van de periode. Kan niet hernomen worden voor 2de zit | | | |
|  | |  | |