HOGESCHOOL ROTTERDAM / CMI / TI

Security Basis

TINSEC03-1

Aantal studiepunten: 2
Cursusbeheerder: A. Scherphof

Cursusbeschrijving

Cursusnaam:	Security Basis
Cursuscode:	TINSEC03-1
Aantal studiepunten en studiebelastinguren:	2 ec Dit studieonderdeel levert de student 2 studiepunten op bij het succesvol afronden van een mondelinge verdediging, overeenkomend met een studielast van 56 uren. Lesuren: 100 minuten * 8 weken = 14 uur Huiswerk maken: 3 uur * 8 weken = 24 uur Voorbereiden verdediging + deelname = 8 uur
Vereiste voorkennis:	Geen
Werkvorm:	Theorie ondersteund practicum van 2 uur
Toetsing:	Online challenges + mondelinge verdediging
Leermiddelen:	● Site https://www.certifiedsecure.com/
Leerdoelen:	1. Je bent in staat als ethical hacker onderzoek te doen naar de veiligheid van computersystemen, netwerken en webapplicaties in **opdracht** van een bedrijf of organisatie. 2. Je bent in staat dit onderzoek in een mondelinge verdediging toe te lichten.
Inhoud:	Online challenges van Certified Secure • Veilig Internet • Veilig Internet+ • Essential Security • Essential Security Specialties • Security Specialist • Security Aware Administrator • Security Aware Programmer • Web Security Specialist • Server Security Specialist • Forensic Specialist
Opmerkingen:	Er wordt gebruikt gemaakt van de Essential Security en Security Specialist trainingspakketten van Certified Secure BV. Deze pakketten worden, bij deelname aan de cursus, door Hogeschool Rotterdam per mail aan je geleverd.
Cursusbeheerder:	A. Scherphof
Datum:	21 juni 2018

1 Algemene omschrijving

Deze cursus levert een bijdrage aan de toenemende behoefte aan goed opgeleide security professionals. De module geeft je een praktische training als basis waarmee je je verder kan ontwikkelen als ethical hacker. De ethical hacker werkt nadrukkelijk in opdracht van bedrijven of instellingen die de veiligheid van hun ICT-voorzieningen nader willen laten onderzoeken.

1.1 Inleiding

Hoe werkt hacking in de praktijk en hoe kun je je ertegen beschermen? Hoe onderzoek je een systeem om een opdrachtgever ervan te overtuigen dat het systeem bestand is tegen de meest voorkomende aanvallen? Een praktische training op de site van ‘Certified Secure’ brengt je dichter bij het antwoord op deze vragen. Certified Secure heeft een trainingswebsite ingericht waar je mág hacken. Op elke andere productieomgeving is dit uiteraard streng verboden. Let er dus op dat je je kennis en vaardigheden die je hierop doet nooit buiten een formele opdracht van een bepaald bedrijf of organisatie toepast op welke productieomgeving dan ook!

Tijdens deze module hanteren wij de IEEE Code of Ethics. Studenten riskeren schorsing wanneer zij deze niet naleven.

1.2 Relatie met andere onderwijseenheden

Binnen ons vakgebied gaat het om de (geautomatiseerde) verwerking van gegevens tot informatie en mogelijk verder tot het verwerven van nieuwe kennis en inzichten. In elk van de onderwijseenheden die aan deze aspecten aandacht geven, is security (het ongestoord en veilig laten plaatsvinden van deze verwerking) een aandachtspunt welke terugkomt in de projecten, stage en het afstuderen.

1.3 Leermiddelen

Er wordt gebruik gemaakt van de training en challenges van ‘Certified Secure’. Om van deze content gebruik te kunnen maken heb je twee licenties (unlock codes) nodig. Deze licenties worden, bij deelname aan deze cursus, door Hogeschool Rotterdam ingekocht en vervolgens per mail aan jou geleverd.

Hieronder de procedure voor het gebruik van de unlock-codes.

Een unlock code kan op 2 manieren worden ingevoerd:

- Nog geen Certified Secure Account

Op de frontpage (https://www.certifiedsecure.com) kan een Certified Secure account worden aangemaakt. De unlock code kan meteen bij het aanmaken van het account in het veld "Unlock code" worden ingevoerd. Het trainingspakket wordt nu meteen automatisch aan de toolbox van het nieuwe account toegevoegd (https://www.certifiedsecure.com/toolbox).

- Reeds in bezit van een Certified Secure Account

Indien er reeds een Certified Secure Account bestaat kan er worden ingelogd. In de toolbox (https://www.certifiedsecure.com/toolbox) bestaat de optie "Unlock Content". Wanneer hierop geklikt wordt verschijnt er een popup waar de unlock code kan worden ingevoerd. Vervolgens wordt het trainingspakket automatisch aan de toolbox van het account toegevoegd.

LET OP:

Als je een account aanmaakt let dan goed op dat je naam e.d. juist is vermeld. Deze gegevens worden later overgenomen op je certificaten.

Iedere code is uniek en kan slechts eenmalig worden geactiveerd. Wanneer een code is ingevoerd kan deze niet nogmaals worden gebruikt. De unlock codes worden slechts eenmalig verstrekt.

Als onderdeel van de training worden een aantal (web) aanvallen uitgevoerd op de trainingswebsites en bijbehorende IP-adressen van Certified Secure. Wanneer gebruik gemaakt wordt van beveiligings-apparaten is het belangrijk om URL's die eindigen op certifiedsecure.com te white-listen voor alle poorten.

Deze module maakt gebruik van de online challenges van Certified Secure waarvoor de student ook certificaten ontvangt. De student moet bij 6 van de volgende 10 challenges 100% scoren om een voldoende te krijgen:

- **Veilig Internet**

Met het Veilig Internet Certificaat weet je zeker dat je de basisvaardigheden beheerst die je nodig hebt om veilig online te zijn, namelijk het up-to-date te houden van je computer en het herkennen en oplossen van veelvoorkomende situaties op het internet.

- **Veilig Internet+**

De volgende stap op het gebied van veilig internetten is de Veilig Internet Plus certificering. Aan de orde komen onderwerpen zoals phishing, downloads en e-mailbijlagen, maar ook het veilig omgaan met wachtwoorden.

- **Essential Security**

Hoe werkt hacking in de praktijk en hoe kun je je ertegen beschermen? De Essential Security certificering geeft je een praktische introductie in de wereld van applicatie- en serverbeveiliging. Alles draait om de kwetsbaarheden SQL Injection en Path Traversal. Het Essential Security Certificaat toont aan dat je deze kwetsbaarheden begrijpt en dat je in het bezit bent van de benodigde hacker mindset.

- **Essential Security Specialties**

De Essential Specialties certificering is het logische vervolg op Essential Security. De challenges vragen het uiterste van je op het gebied van SQL Injection en Path Traversal. Je haalt het certificaat wanneer je de drie examinatie- challenges succesvol hebt afgerond. Om verder te gaan met de Security Specialist certificering is een score van 33% benodigd en hoef je dus slechts één van de examinatie challenges af te ronden.

- **Security Specialist**

De Security Specialist certificering is de volgende stap in server- en applicatiebeveiliging. De challenges op dit niveau zijn een uitdaging voor zelfs de meest gemotiveerde deelnemer. Het certificaat garandeert dat je de werking van de meest voorkomende gevaren voor websites en servers begrijpt, je een poortscan en host probe scan kunt uitvoeren en dat je Cross Site Scripting, geavanceerde SQL Injection en geavanceerde Path Traversal kunt ontdekken en voorkomen. Het Security Specialist Certificaat is een must-have voor iedere securityprofessional.

- **Security Aware Administrator**

Bij de Security Aware Administrator certificering draait alles om secure system administration. Het Security Aware Administrator Certificaat garandeert een gedegen begrip van het updaten van software en het veilig configureren van een firewall. Het certificaat vormt de basis van veilig systeembeheer.

- **Security Aware Programmer**

De Security Aware Programmer certificering gaat dieper in op secure development. De certificering is gericht op de applicatieontwikkelaar en het voorkomen van SQL Injection, Path Traversal en Cross Site Scripting. Het certificaat garandeert een gedegen begrip van authenticatie en invoervalidatie waarmee kwetsbaarheden voorkomen kunnen worden.

- **Web Security Specialist**

De Web Security Specialist certificering duikt in de wereld van geavanceerde webapplicatie kwetsbaarheden. Het Web Security Specialist Certificaat garandeert gedegen begrip van Javascript Authenticatie, Identifier Based Authenticatie, Command Injection, PHP Uploads, Cross Site Request Forgery en Password Guessing. In combinatie met het Server Security Specialist Certificaat vormt het de basis voor iedere securityconsultant.

- **Server Security Specialist**

De Server Security Specialist certificering gaat dieper in op serverbeveiliging. Certified Secure kiest zoals altijd voor een hands-on aanpak. Het Server Security Specialist Certificaat garandeert een gedegen begrip van (UDP) Port Scanning, Mail Relaying, Anonymous Uploading en Password Guessing. In combinatie met de Web Security Specialist certificering vormt het certificaat de basis voor iedere securityconsultant.

- **Forensic Specialist**

De Forensic Specialist certificering biedt een introductie in de wereld van de forensische analyse en richt zich op digitaal sporenonderzoek. Welke sporen blijven achter op een gecompromitteerd systeem? Hoe herken je een aanval en hoe analyseer je netwerkverkeer? Het Forensic Specialist Certificaat garandeert een basisbegrip van netwerkmonitoring en forensische analyse. Alle technieken worden geïllustreerd aan de hand van realistische voorbeelden.

2 Programma

Week	Literatuur/huiswerk	Lesinhoud	Producten
2		Introductie ethical hacking.	Veilig Internet & Veilig Internet+ afronden in de les.
3 t/m 8	Certified Secure Challenges: ● Essential Security ● Essential Security Specialties ● Security Specialist ● Security Aware Administrator ● Security Aware Programmer ● Web Security Specialist ● Server Security Specialist ● Forensic Specialist	Demonstraties en theorie ondersteunend aan de opdrachten van Certified Secure. Mogelijkheid om vragen te stellen over de opdrachten.	Afgeronde opdrachten in de omgeving van Certified Secure.
9, 10	Voorbereiden mondelinge verdediging.	Mondelinge verdediging om aan te tonen dat je de benodige hacking skills onder de knie hebt.	

3 Aanwezigheid

Voor les 1 geldt verplichte aanwezigheid voor alle studenten. Tijdens week 3 t/m 8 worden studenten via Google Classroom op de hoogte gehouden voor welke lessen de verplichte aanwezigheid geldt. Voor week 9 en 10 geldt aanwezigheid op basis van welke week de student zijn mondelinge verdediging heeft.

4 Toetsing en beoordeling

4.1 Procedure

Aan het einde van het kwartaal moet de student 6 van de 10 challenges van Certified Secure behaald hebben met een score van 100%. Wanneer de student hieraan voldoet mag de student deelnemen aan de mondelinge verdediging. De student neemt uitgeprint de behaalde certificaten mee naar de verdediging. Tijdens de verdediging moet elke student individueel aantonen dat de student de benodigde skills beheerst. Als de student de verdediging behaalt met 6 van de 10 challenges krijgt de student een 6 als cijfer. Voor elke challenge met 100% score boven de 6 uit 10 krijgt de student 1 punt extra. Voor de inhoud van de challenges zie §1.3.

Als de student niet voldoet aan de 6 van de 10 challenges met een score van 100% mag deze niet deelnemen aan de verdediging en moet deelnemen aan de herkansing. Ook als de student de verdediging niet behaald moet deze deelnemen aan de herkansing.

Het wordt de student aangeraden om een labjournaal bij te houden met gedetailleerde handelingen welke de student heeft verricht om de challenges te voltooien. De student mag dit labjournal meenemen naar de verdediging. Als de student een labjournal wilt gebruiken moet deze voorafgaand de verdediging ingeleverd worden op Google Classroom en goedgekeurd worden door de docent.

4.2 Herkansing

Voor de herkansing moet de student alsnog voldoen aan een 100% score bij 6 van de 10 challenges en moet over deze challenges aan een mondelinge verdediging deelnemen. Voor de herkansing kan de student maximaal een 7 behalen. Wanneer de student wegens omstandigheden niet deel kan nemen aan de eerste gelegenheid geld het maximale cijfer van een 7 niet. De student word in dat geval wel geacht de docent tijdig op de hoogte te brengen van omstandigheden.

Voor langstudeerders die volgens de conversietabel deze cursus moeten volgen geld dat zij mee moeten doen met het reguliere programma van Security Basis.

Bijlage: toetsmatrijs

Toetsonderdeel	Bloom-niveau	Leerdoelen
Challenges Certified Secure	1, 2, 3, 4	1
Assessment	5	2

Bloom-niveaus:

1. Remember
2. Understand
3. Apply
4. Analyse
5. Evaluate
6. Create