UNIVERSITEIT GENT

Studiefiche

Vanaf academiejaar 2026-2027

Netwerkhacking en -bescherming (E008711)

Cursusomvang *(nominale waarden; effectieve waarden kunnen verschillen per opleiding)*

Studiepunten 6.0 **Studietijd 180 u**

Aanbodsessies in academiejaar 2026-2027

A (semester 1) Engels Gent

Lesgevers in academiejaar 2026-2027

Volckaert, Bruno TW05 Verantwoordelijk lesgever

Aangeboden in onderstaande opleidingen in 2026-2027	stptn	aanbodsessie
Brugprogramma Master of Science in Bioinformatics(afstudeerrichting Engineering)	6	A
Master of Science in Bioinformatics(afstudeerrichting Engineering)	6	A
Master of Science in Computer Science Engineering	6	A
Master of Science in de industriële wetenschappen: informatica	6	A
Master of Science in de informatica	6	A
Master of Science in de ingenieurswetenschappen: computerwetenschappen	6	A
Micro-credential Network Hacking and Protection	6	A
Uitwisselingsprogramma industriële wetenschappen: informatica	6	A
Uitwisselingsprogramma informatica (niveau master)	6	A

Onderwijstalen

Engels

Trefwoorden

Penetratietesten, netwerkverkenning, netwerkbeveiliging, netwerkovernames, veilige vormen van virtualisatie, digitaal forensisch onderzoek, zero trust systemen, incidentafhandeling, intrusiedetectie, red team, blue team, purple team.

Situering

ICT infrastructuur ligt aan de basis van zowel kritische als niet-kritische functionaliteit waar we als maatschappij op steunen. Met de blijvende digitalisatie (vb. slimme toestellen, smartphones, slimme huizen, slimme steden, slimme energienetwerken, cloud-systemen) is het essentieel dat de beveiliging van die infrastructuur de nodige aandacht krijgt.
Het doel van deze cursus is om aan te leren door middel van welke methodes cyber-aanvallers typisch gaan proberen infiltreren in systemen of de normale werking van systemen proberen verstoren, en – als ze eenmaal binnen zijn – hoe ze gaan proberen om controle te verkrijgen over andere systemen in hetzelfde netwerk en mogelijks hun acties proberen verdoezelen. Gewapend met die kennis, wordt het opzetten van correcte netwerkverdedigingen tegen zulke aanvallen besproken.
Deze cursus is complementair met de cursussen van informatiebeveiliging, die focust op cryptografie en implementaties daarvan op een hoog abstractieniveau; en Softwarehacking en -protectie, waarbij het gedrag van het systeem (ofwel deels ofwel volledig) ongekend is door een aanvaller, en het doel van de aanvaller is om het gedrag van het systeem te begrijpen en manipuleren; en Veilige software en systemen, die zich richt op (vaak op afstand) exploiteerbare gebreken en bugs in softwareontwerpen en -implementaties.
Deze cursus bouwt verder op de kennis opgedaan in eerdere cursussen rond computerarchitectuur, besturingssystemen en computernetwerken.

Inhoud

- Netwerkbeveiliging (firewall, DDoS beschermingsdiensten)
- Verkenning (OSINT, kwetsbaarheid/netwerkscans, webapplicatie scans) om doelwitten te identificeren en op te lijsten
- Penetratietesten (MetaSploit a.o.)
- Escalatie van bevoegdheden op afstand
- Lateraal netwerk doorkruisen
- Intrusiedetectie (op basis van handtekeningen / heuristieken)
- Aanvallen gebaseerd op fysieke toegang
- Social engineering aanvallen (dubbelganger domeinen, phishing)
- Draadloze netwerk-overnames
- Jump-servers, Werkstation met geprivilegieerde toegang
- Digitaal forensisch onderzoek na een beveiligingsincident
- Risico modellering (risicofactoren in netwerkbeveiliging, waar moet sleutelinfrastructuur geplaatst worden, gedemilitariseerde zones)
- Veilig IoT design – SCALA – andere netwerktypes
- Veilige virtualisatie-opties: containers, microVMs, sandboxing, etc.
- Zero trust systemen (enclaves, confidentiële containers, gebruik van gehuurde infrastructuur voor sensitieve werklast)
- Incidentmanagement: beheer van geheimen (b.v. in Kubernetes), back-up infrastructuur, fouttolerantie, administratieve toegangspoorten

Begincompetenties

- Programmeren in C en C++, Python
- Kennis van computerarchitectuur
- Kennis van de fundamenten van computernetwerken
- Kennis van besturingssystemen
- Basiskennis van Linux (i.e. Bash)
- Basiskennis van databanken

Eindcompetenties

1 Begrijpen en kunnen gebruiken van de terminologie aangaande offensieve en defensieve netwerkbeveiligingsaspecten (red team, blue team, purple team).
2 Diepgaande kennis omtrent verkenningstechnieken (OSINT, scannen op kwetsbaarheden, etc.).
3 Het vermogen om penetratietesten uit te voeren op netwerkapplicaties en de bekomen resultaten op een professionele manier te documenteren.
4 Het vermogen om ongewenste penetratietesten op te sporen op eigen infrastructuur.
5 Diepgaande kennis omtrent kwetsbaarheden in software toegankelijk via een netwerk, analyse van hun impact en constructie van tegenmaatregelen om ervoor te zorgen dat deze kwetsbaarheden niet uitgebuit kunnen worden.
6 Diepgaande kennis van technieken om gevirtualiseerde werklast te beveiligen.
7 Kennis van de principes van zero trust systemen.
8 Het vermogen om een beveiligd bedrijfsnetwerk te ontwerpen en op te zetten met publiekgerichte applicaties en omgekeerd het vermogen om een onveilig netwerk binnen te dringen.
9 Het vermogen om digitaal forensisch onderzoek uit te voeren op een systeem dat gecompromitteerd werd.
10 Domeinspecifieke kennis op een correcte en duidelijke manier communiceren en presenteren, met de juiste taalvaardigheid, inclusief het gebruik van correcte terminologie.

Creditcontractvoorwaarde

Toelating tot dit opleidingsonderdeel via creditcontract is mogelijk na gunstige beoordeling van de competenties

Examencontractvoorwaarde

Dit opleidingsonderdeel kan niet via examencontract gevolgd worden

Didactische werkvormen

Hoorcollege, Practicum, Zelfstandig werk

Toelichtingen bij de didactische werkvormen

Laptops van studenten moeten x64 virtuele machines kunnen uitvoeren

Studiemateriaal

Type: Slides

Naam: Netwerkbeveiliging
Richtprijs: Gratis of betaald door opleiding
Optioneel: nee
Taal : Engels
Aantal slides : 700
Beschikbaar op Ufora : Ja
Online beschikbaar : Ja
Beschikbaar in de bibliotheek : Nee
Beschikbaar via studentenvereniging : Nee

Referenties

- (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition, Mike Chapple, James Michael Stewart, Darril Gibson, 2021, ISBN: 978-1-119-78623-8
- CompTIA Security+ Study Guide, 7th Edition, Emmett Dulaney, Chuck Easttom, 2017, ISBN: 978-1-119-41690-6
- The Hacker Playbook: Practical Guide to Penetration Testing (vol 1, 2 and 3), Peter Tim, 2014 (1), ISBN 978-1494932633, 2015 (2), ISBN 978-1512214567, 2018 (3): ISBN 978-1980901754

Vakinhoudelijke studiebegeleiding

- Interactieve ondersteuning en coaching door afspraken op het elektronisch leerplatform
- Docent en assistenten zijn beschikbaar voor extra hulp voor en na contacturen, en via e-mail chat en conference calls

Evaluatiemomenten

periodegebonden en niet-periodegebonden evaluatie

Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode

Schriftelijke evaluatie met open vragen

Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Schriftelijke evaluatie met open vragen

Evaluatievormen bij niet-periodegebonden evaluatie

Participatie, Peer en/of self assessment, Werkstuk

Tweede examenkans in geval van niet-periodegebonden evaluatie

Examen in de tweede examenperiode is enkel mogelijk in gewijzigde vorm

Toelichtingen bij de evaluatievormen

- Periodieke evaluatie: schriftelijk examen omtrent theorie, met gesloten boek
- Niet-periodieke evaluatie: verslag opdracht

Eindscoreberekening

- 50% op niet-periodieke evaluatie, 50% op periodieke evaluatie.
- Gebrek aan participatie voor de niet-periodieke evaluatie zonder grondige reden zal resulteren in een 0 voor dat deel.
- Bij groepswerk verkrijgen studenten in een groep dezelfde score normaliter. Enkel als er een duidelijk verschil is in contributieniveau zullen de studenten een verschillende score ontvangen.
- Studenten moeten voor beide onderdelen >= 10/20 scoren om te slagen voor de cursus. Als ze falen voor 1 deel terwijl ze nog altijd >= 10/20 behalen, zal de finale score herleid worden naar 9/20
- Wanneer men niet deelneemt aan de evaluatie van één of meer onderdelen kan men niet meer slagen voor het geheel van het opleidingsonderdeel en wordt het eindcijfer, indien dit hoger ligt dan 7/20, teruggebracht tot het hoogste niet-delibereerbare cijfer (7/20)

Faciliteiten voor werkstudenten

Mogelijkheid om niet te moeten fysiek participeren in labos na overleg met de verantwoordelijke lesgever (elk labo heeft een deadline van minstens een week). Mogelijkheid om feedback te verkrijgen na afspraak gedurende en na de werkuren.