IFBD
Institute for Business Development

2024

Zoek en vind de zwakheden en datalekken in uw beveiliging en wees hackers en cyber-criminelen die ene stap voor!

Denk als een hacker

- Word zelf voor één dag hacker en oefen in een veilig lab.
- Leer de methodes, systemen en tools van de hacker.
- Zoek én vind de zwakheden en data lekken in uw beveiliging.

Onder de deskundige leiding van:

Malik Mesellem
Security Consultant & Trainer
Directeur MME BV

>>> **IFBD.BE** /
informatica training

Waarom dit programma?

CYBERCRIMINELEN RUNNEN DE DERDE GROOTSTE ECONOMIE WERELDWIJD

Volgens de laatste cijfers zal Cybercriminaliteit in 2022 wereldwijd 6 biljoen dollar schade aanrichten. Dit betekent dat cybercriminelen de op twee na grootste economie ter wereld aansturen, na de VS en China. Ondanks deze hallucinante cijfers, zijn vele Belgische bedrijven toch bereid het risico te lopen, deels uit onwetendheid, deels uit onverschilligheid. U kunt de hackers en andere cybercriminelen echter die ene – cruciale - stap voor blijven!

IMPACT VAN CYBERCRIMINALITEIT OP UW ORGANISATIE

De impact die een cyber aanval heeft op de continuïteit én geloofwaardigheid van uw organisatie is immers enorm : beschadiging en vernietiging van data, ongewilde financiële transacties, productiviteitsverlies, diefstal van intellectuele eigendom, diefstal van persoonlijke en financiële data, verstoring tot zelfs stopzetten van de operaties na een aanval en … reputatieschade. Want niemand van uw klanten vindt het fijn dat zijn of haar persoonlijke gegevens te grabbel worden gegooid.

LEER DENKEN ALS EEN HACKER

Deze workshop leert u denken als een hacker. Voor één dag kruipt u in de huid van een hacker en denkt u als een hacker. U krijgt niet alleen inzicht in hoe een hacker uw kwetsbaarheden, data lekken en zwakheden opspeurt, maar evenzeer hoe u zich hiertegen kunt en moet beschermen.

VERLAAT DEZE WORKSHOP MET EEN CONCREET ACTIEPLAN

U leert hoe hackers stapsgewijs de inhoud van sites veranderen, data aanpakken, databases leeg halen en computers en servers overnemen. U leert scannen, testen, hacken maar vooral beveiligen. U krijgt inzicht in de meest gebruikte technieken en tools gebruikt door hackers om websites te hacken, draadloze verbindingen af te tappen en wachtwoorden te kraken. Gedurende deze ene dag bent u zelf hacker en kijkt u hoe u (een demo-web applicatie) kunt aanvallen. Hierdoor keert u terug naar uw werkplek met een duidelijk actieplan bij het optimaal beveiligen van uw eigen data en IT-omgeving.

"Na deze dag bent u in staat om zelf een aanval uit te voeren op uw eigen omgeving en kunt u uw dataomgeving beschermen tegen inbrekers."

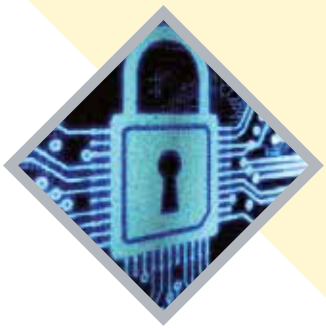
De docent

Malik Mesellem is een zelfstandig security consultant met een grote passie voor penetration testing, ethical hacking, en webapplicatie beveiliging.
In 2010 richtte hij 'MME BV' op: een organisatie gespecialiseerd in security audits, penetration testing, vulnerability assessments, security training en user awareness.
Malik is tevens actief als security trainer en heeft op regelmatige basis 'shocking' trainingen en sessies aan diverse bedrijven en instituten. Zo was Malik in het verleden ook SANS mentor voor België, actief betrokken bij de OWASP organisatie en Microsoft Certified trainer.
Internationaal is Malik bekend met het bWAPP - a buggy web application - web security testing platform. bWAPP is een open-source 'bewust niet-veilige' web applicatie, ontwikkeld door Malik. bWAPP wordt wereldwijd gebruikt door zowel security enthousiastelingen als door security auditors, en heeft ondertussen bijna 1 miljoen downloads.
Als spreker rond dit thema was Malik aanwezig op o.a. Infosecurity Brussels, SANS Orlando, B-Sides Orlando, en het Trusted Digital Identity Symposium.

Leermethodiek van deze dag

Aan de hand van voorbeelden, cases en allerhande materiaal leert u alles over de hacker-methodologie. Allerhande technieken en tools worden toegelicht. U leert alles over het overnemen van servers, het leeghalen van databases en het veranderen van web content.

Programma



DEEL1 – HACKING : METHODES, SYSTEMEN EN TOOLS

- Inleiding tot hacking:
  - Wie zijn de spelers en wat is hun spel?
  - Van nationale aanvallen tot ransomware .
  - Kwetsbaarheden en assessments.
- Welke methodes en technieken en tools passen zij toe om:
  - websites te hacken
  - draadloze verbindingen af te tappen
  - wachtwoorden te kraken
- Penetration Testing en Tools
- System Hacking met Metasploit
- Post-Exploitation en MitM
- Defense-in-Depth Strategieën
- Wachtwoord concepten en aanvallen
- Lateral Movement en Defenses
- Wireless Attacks en Defenses
- Client-Side Attacks en Malware
- Client & Server Hardening
- Introductie tot Web Security
- De OWASP Top 10 risico's
- Web Application Hacking
- Web Server Hardening

INTERMEZZO: ZIN EN ONZIN VAN EEN CYBERVERZEKERING

(korte bijdrage van Vincent Pauwels - Bestuurder WILINK)

> De drie bouwstenen: technische bijstand, rechtsbijstand, schadevergoeding.
> Is "roekeloos" gedrag van medewerkers gedekt?
> Best & worst practices.

DEEL 2 – DEMOLABO : LEER TESTEN, SCANNEN, HACKEN EN BEVEILIGEN

In dit – confronterende en verrassende – demolabo leert u de echte praktijk van het hacken, krijgt u inzicht in hoe hackers beveiligingslekken opsporen en hoe zij informatie verzamelen voor gerichte aanvallen.

Met uw eigen laptop heeft u de mogelijkheid om het 'kwetsbare' netwerk – opgezet door de trainer – aan te vallen.Uw taak bestaat erin om de verschillende besturingssystemen te compromitteren en om uw rechten te escaleren tot u 'eigenaar' wordt van het netwerk…

Ook wordt o.a. het bWAPP web security platform gebruikt. Deze opzettelijk onveilige webapplicatie ontwikkeld door MME heeft meer dan 100 web kwetsbaarheden! Het dekt alle belangrijke web beveiligingsrisico's, inclusief deze uit het OWASP Top 10-project. Op deze manier kunt u de verschillende web kwetsbaarheden - zoals SQL injection - zelf 'uitbuiten', en dit in een veilige omgeving begeleid door de trainer.

DEEL 3 – EN WAT ALS U ALSNOG GEHACKT WORDT

- Te volgen procedure
- Concreet actieplan

Timing cursus

08.30	Ontvangst, registratie met koffie/thee.
09.00	Start van de trainingsdag (met voorstelling docent)
12.30	Lunch
17.00	Einde van de cursusdag.

Zowel in de voor- als namiddag wordt een korte (koffie-)pauze gehouden.

Verhoogde interactiviteit

De deelnemers krijgen uitgebreid de kans om hun eigen problematiek ter sprake te brengen. Om dit te realiseren, vragen wij op voorhand een beknopte beschrijving van de probleemstelling te formuleren. Op die manier kunnen wij de cursus volledig opstellen volgens uw eigen informatiebehoefte.
U kunt hiervoor steeds contact opnemen met **Dirk Spillebeen** op het nummer: **+32 50 38 30 30** (e-mail: **dirk@ifbd.be**).

Denk als een hacker

2024

> **Datum & locatie:** zie hiertoe onze website **www.ifbd.be**
> **Kostprijs: € 795** (excl. BTW)

>>> INSCHRIJVEN

E-mail:
info@ifbd.be

klik hier

Via onze website:
ifbd.be

klik hier

Via QR:

Telefoon:
00 32 50 38 30 30

Voor meer informatie omtrent uw inschrijving ...

>>> INSCHRIJVINGSMODALITEITEN

De deelnameprijs aan dit 1-daagse programma bedraagt **795 Euro** excl. 21% BTW. Dit bedrag is inclusief koude/warme dranken en een uitgebreide lunch tijdens de cursusdag. U ontvangt bovendien een **documentatiemap** die u als naslagwerk kunt raadplegen. Los van de eventuele subsidiëring van de Vlaamse Overheid (zie verder) geeft het IFBD per extra deelnemende collega **5% extra korting** op het **totaalbedrag** met een maximale **korting van 20%** (= 5 deelnemers of meer).
Na ontvangst van uw inschrijving krijgt u een **deelnamebevestiging** en een factuur. Een tweetal weken voor de cursus ontvangt u een **herinnering met nog enige praktische informatie** en een **routebeschrijving**.

DE VLAAMSE OVERHEID INVESTEERT IN OPLEIDING: TOT 30% KORTING!

Het **IFBD** is erkend als **gecertificeerd opleidingsinstituut**. Dit maakt dat u onze trainingen gedeeltelijk kunt betalen met de subsidies toegekend door de Vlaamse Overheid via het systeem van de "KMO-portefeuille". Indien uw bedrijf voldoet aan de vooropgestelde criteria kan u tot 30% besparen op de opleidingskost. Meer informatie omtrent het systeem kan u vinden op de website van de Vlaamse Overheid: **www.kmo-portefeuille.be**.

Annulatie.
We begrijpen dat andere prioriteiten kunnen optreden tussen uw inschrijving en de cursus. Indien wij minstens **2 weken voor de cursus** uw annulatie ontvangen zoeken we samen met u naar de beste oplossing. **Minder dan 2 weken voor de eerste cursusdag** bent u ons het integrale bedrag verschuldigd en wordt mogelijks een administratieve kost (€ 75) aangerekend. Wij zijn uiteraard steeds verheugd een collega te mogen verwelkomen in uw plaats.

HOTELOVERNACHTING OP DE LOCATIE VAN DE TRAINING

U kan op onze diverse trainingslocaties veelal een overnachting boeken om de cursus op een ontspannen manier te kunnen aanvatten en/of af te sluiten. Meer informatie hieromtrent vindt u op onze website of via volgende link: www.ifbd.be/nl/over-ons/algemene-voorwaarden

IFBD-DATABASE & GDPR

We houden u graag op de hoogte van de laatste evoluties binnen uw sector. Daarom hebben we uw gegevens opgenomen in onze database. Uw informatie is voor eigen gebruik, wordt beveiligd en nooit aan derden doorgegeven. Hiertoe nemen we alle nodige maatregelen. Te allen tijde heeft u - overeenkomstig de wet "verwerking persoonsgegevens" van 8/12/1992 en de "AVG-reglementering" van 24/5/2016 - recht op inzage, wijziging of verwijdering van uw gegevens. Meer informatie via onze webpagina www.ifbd.be/nl/GDPR of via e-mail: DPO@ifbd.be.

ALGEMENE VOORWAARDEN

Op onze website op de pagina **ifbd.be/nl/over-ons/algemene-voorwaarden** vindt u al onze modaliteiten terug.