Voorbereiding op de opleiding Ethical Hacker van OptiSec

Welkom alvast. In dit pdfje vind je waar het bij Ethical Hacking om draait, hoe je laptop klaar te zetten, en welke gratis bronnen je nu al kunt pakken om soepel te starten. Pak een koffie, lees rustig door, en kijk of dit jouw vak is.

Na uren puzzelen is het zover, je bent eindelijk binnen!

Het pad van een hacker is niet lineair. Je kunt uren achter je computer puzzelen, en nog geen stap verder komen. Dat is hoe het leven als Ethisch Hacker eruit ziet. Struggelen totdat je de oplossing hebt gevonden, en dan staat de volgende uitdaging al voor je klaar!

Wat een Ethical Hacker écht doet

Een Ethisch Hacker denkt als een aanvaller, maar werkt met toestemming: kwetsbaarheden vinden vóórdat kwaadwillenden dat doen. Je brengt veel tijd door met scannen, enumereren en handmatig testen van systemen: op zoek naar de ene fout die een deur open kan zetten. Elke bevinding werk je uit tot een helder rapport, zodat organisaties hun beveiliging kunnen verbeteren.

Past het bij jou om Ethisch Hacker te worden?

Ben je nieuwsgierig, oplossingsgericht, zelfstandig, en heb je een goede dosis doorzettingsvermogen? Dan is Ethisch Hacken mogelijk wel iets voor jou! De wereld van een Ethisch Hacker staat nooit stil. Je ontwikkelt je voortdurend mee met nieuwe technieken, en geeft niet op als de oplossing niet meteen voorhanden ligt. Dat maakt het werk uitdagend, en daarnaast ook ontzettend leuk!

BIJ OPTISEC

De meeste mensen hier komen binnen zonder IT-achtergrond. Deze gids maakt de start een stuk soepeler.

Zo ziet jouw route naar Ethical Hacker eruit

De volledige opleiding bestaat uit meerdere modules en certificeringen. Je hoeft je daar nu nog niet druk om te maken. Dit document gaat alleen over de voorbereiding. Maar het is goed om te weten waar je naartoe werkt.

JIJ BENT HIER

Voorbereiding

Tools installeren, basis-IT begrippen, beetje Linux ruiken

MODULE 1

IT Fundamentals & ISC2 CC

De volledige IT basis. Hardware, OS, netwerken, en je gaat voor je CC certificaat.

MODULE 2

CPTS Fundamentals

Je leert de eerste basis van het hacken

MODULE 3

CPTS Attacks

Je gaat leren over het aanvallen van computers & netwerken.

MODULE 4

CPTS Web Attacks

Je gaat het web leren aanvallen

MODULE 5

CPTS Privilege Escalation

Leer hoe je meer rechten kan krijgen wanneer je binnen bent!

Join the Red Team!

In de wereld van cybersecurity praten we over een Red Team en een Blue Team. De red teamers zijn de Ethical Hackers, de aanvallers. Het Blue Team is juist de verdediging: de analisten.

Drie stappen om jezelf voor te bereiden

De stappen lopen op in moeilijkheid. Stap 1 is voor iedereen. Stap 2 is heel handig om alvast te doen. Stap 3 is voor wie er klaar voor is. Hoe verder je komt, hoe soepeler je start zal zijn. Geen verplichte stof, geen druk om alles af te krijgen.

1

Kennismaken en installeren

VMware en Kali Linux op je laptop, een notitie-app, en een AI-account voor als je vastloopt. Hier maak je je werkbank klaar.

2

Gratis leer-materiaal

Online bronnen waar je in je eigen tempo de IT basis kunt opbouwen. TryHackMe, Linux Journey, Professor Messer en HTB Academy.

3

Concepten verkennen

Een lijstje begrippen die in de eerste lesweek voorbij komen. Zoek ze één keer op, dan heb je er al een beeld bij als wij ze behandelen.

HOE JE DIT HET BESTE AANPAKT

Lees eerst dit document helemaal door voordat je begint. Niet om alles te onthouden, maar om te zien wat je te wachten staat. Daarna pak je rustig stap 1. Een paar avonden van een uur is meer dan genoeg om er goed doorheen te komen.

01

STAP 1

Kennismaken en installeren

We beginnen met je werkbank klaarzetten. Een virtuele machine voor Kali Linux, een notitie-app, en een AI-account. Niets technisch om je nu zorgen over te maken, gewoon stap voor stap.

Installeer VMware Workstation Pro

Wat is een VM eigenlijk?

Een computer-in-een-computer, een sandbox waarin je veilig kunt klooien.

Een Virtual Machine is een complete nep-computer die binnen je echte computer draait. Eigen besturingssysteem, eigen bestanden, en als je hem stukmaakt gebeurt er niets met je echte laptop. Voor security werk ideaal.

Wat is VMware Workstation Pro?

Het programma waarin je die VM's draait, een huis voor je virtuele computers.

VMware Workstation Pro is sinds kort gratis voor persoonlijk gebruik. Het is beter dan VMware Player of VirtualBox qua performance. Je virtuele Kali Linux loopt er soepel mee.

Zo download je hem

1 **Ga naar de Broadcom site en maak een account aan**

VMware is overgenomen door Broadcom. Je downloadt VMware nu via hun portal. Een gratis account aanmaken is verplicht, kost een paar minuten.

2 **Klik door naar My Downloads en daarna Free Downloads**

Daar vind je VMware Workstation Pro. Klik die aan, en je komt op de downloadpagina met de releases.

3 **Pak de versie 26H1**

Dat is op dit moment de actuele stabiele versie. Oudere versies (zoals 25H2u1) gaan je telkens lastig vallen met update nag screens, dus pak meteen de juiste. Installeer hem zoals elk ander programma op Windows.

LOOP JE VAST?

Geen paniek. Het Broadcom portal is een doolhof, daar struikelt iedereen wel even. Plak je foutmelding in ChatGPT, Claude of Google en kom er zelf even uit. Uitzoeken en onderzoeken is óók onderdeel van de Ethisch Hacker mindset, dus dit is alvast goede oefening.

Installeer Kali Linux

Wat is Linux?

Een ander besturingssysteem dan Windows of macOS vooral populair bij servers.

Linux is gratis, open-source, en heeft duizenden varianten. Vrijwel alle internet-servers draaien er op. Als analist krijg je dagelijks met Linux te maken, en de terminal is een belangrijk gereedschap.

Waarom Kali specifiek?

Kali is een Linux variant met security tools al voorgeïnstalleerd.

Kali is bekend van hacker series en films, in feite een toolkit. Wij gebruiken hem niet om aan te vallen, maar om te begrijpen wat aanvallers doen. We gebruiken Kali ook in de opleiding zelf.

Installatie in vier stappen

1 **Download de Kali VM image**
Ga naar kali.org/get-kali en kies Virtual Machines. Pak de VMware variant. Ongeveer 3,5 GB. Pak uit op een vaste plek, bijvoorbeeld D:\VMs\Kali .

2 **Voeg de VM toe aan VMware**
Open VMware. Menu: File → Open . Navigeer naar de uitgepakte Kali map en kies het bestand met de extensie .vmx . De VM verschijnt in je library links.

3 **Upgrade de hardware compatibility**
Rechts-klik op de VM, ga naar Manage → Change Hardware Compatibility, en zet hem op Workstation 26H1. Hierdoor draait de VM op volle snelheid mee.

4 **Verhoog het RAM (als je laptop dat aankan)**
Open de VM settings en zet Memory van 2 GB naar 4 GB. Heeft je laptop minimaal 8 GB totaal, geen probleem. Daarna kun je de VM starten.

EERSTE LOGIN Gebruiker en wachtwoord zijn beide kali, dat is de standaard fabrieksinstelling van Kali. Veranderen hoeft niet, maar handig om te weten.

Kies een notitie-app en begin nu al

Tijdens de opleiding ga je veel zien, veel proberen, en veel vergeten. Dat is normaal. Iedereen, ook ervaren hackers, werkt met cheat sheets en eigen notities. Begin daar nu al mee. Het hoeft niet mooi, het hoeft niet compleet, het moet voor jou werken.

Een paar goede opties

LEKKER IN DE CLOUD

Notion

Gratis, in de browser, makkelijk te delen. Werkt goed voor zowel tekst als screenshots. Voor de meeste mensen de eenvoudigste keuze.

AANBEVOLEN

Obsidian

Lokaal op je computer, markdown gebaseerd, krachtig met links tussen notities. Iets steilere leercurve, maar wel de favoriet onder Ethical Hackers.

MICROSOFT MENSEN

OneNote

Komt vaak al met Office. Werkt prima, vooral als je toch al in het Microsoft ecosysteem leeft.

HACKER OLD SCHOOL

Cherry Tree

Lokaal, hiërarchisch, populair bij pentesters. Een tikje ouderwets uiterlijk maar doet zijn werk.

TIP Documenteer ook al wat je in deze voorbereiding leert. Dat geeft je meteen een idee welke notitie-app voor jou prettig werkt.

Maak een ChatGPT- of Claude-account aan

Een AI-assistent is geen vervanging voor leren, maar wel een goede sparringpartner. Loop je vast op een concept? Vraag hem het in eigen woorden uit te leggen. Begrijp je een log-regel niet? Plak hem erin en vraag wat het betekent. Het bespaart je veel tijd.

ChatGPT

De bekendste. De gratis variant is meer dan voldoende voor wat je nu nodig hebt.
chat.openai.com

Claude

Goed alternatief, vaak iets nauwkeuriger op technische uitleg. Ook gratis te gebruiken.
claude.ai

Hoe je hem het beste gebruikt

- Vraag om uitleg in eigen woorden, niet alleen om een definitie. "Leg me uit wat nmap is alsof ik vijftien ben" werkt vaak beter dan "Wat is nmap?"
- Plak foutmeldingen er rechtstreeks in. Vraag wat ze betekenen. Niet alleen "wat is het?", ook "waarom zou dit gebeuren?" en "is dit erg?"
- Gebruik hem niet voor antwoorden op opdrachten. Je leert er niets van. Wel om concepten op te helderen, dat is de bedoeling.
- Hij heeft het ook niet altijd bij het rechte eind. Twijfel je over een antwoord, dubbelcheck via een tweede bron.

02

STAP 2

Gratis leermateriaal

Bronnen waarmee je in je eigen tempo de basis kunt opbouwen. Allemaal gratis, allemaal beginner-vriendelijk. Pak één tegelijk, zonder druk om alles af te ronden.

TryHackMe, Pre Security Path

Als je tijd hebt voor één ding, doe dit dan. TryHackMe is een interactieve leeromgeving waar je in je browser oefent met netwerken, Linux, Windows en webfundamentals. Geen lange video's om door te ploegen, je doet het zelf, in stappen.

Pre Security Path
tryhackme.com/path/outline/presecurity

Vier modules: Cyber Security Introduction, Network Fundamentals, How the Web Works, en Linux Fundamentals. Samen ongeveer dertig uur, te doen in een paar avonden of weekenden. Perfect als je echt vanaf nul begint.

Waarom dit zo goed werkt

Je doet het zelf

Geen passief kijken. Elke oefening eindigt met een vraag die je beantwoordt door iets in een terminal te doen of een log te bekijken. Dat plakt veel beter dan een video.

Veilige sandbox

Alles draait in een browser-VM bij hen. Je kunt niets stukmaken, je hoeft niets te installeren. Klik op start, en je zit in een Linux terminal.

Helder opgebouwd

De cursus is gemaakt in de juiste volgorde. Begin gewoon bovenaan, ga één voor één naar beneden. Geen keuzestress.

HOEVEEL TIJD ZOU IK ERIN STEKEN?

Als je hier een uur of dertig in stopt voor de opleiding begint, heb je een enorme voorsprong. Lukt dat niet, doe dan in elk geval de modules Network Fundamentals en Linux Fundamentals. Die twee zijn het belangrijkst.

Linux Journey en Professor Messer

Twee gratis bronnen die je naast TryHackMe kunt gebruiken. Beide leggen de IT basis op een andere manier uit, en herhaling helpt. Als één bron iets niet bij je laat landen, probeert een andere bron het vanuit een net andere hoek.

Linux Journey
linuxjourney.com

Een rustige, tekstuele cursus over Linux. Geen video, geen account nodig. Doe in elk geval alle modules onder Grasshopper. Daar zit de hele basis in: navigeren, bestanden lezen, gebruikersrechten, processen. Reken op een uurtje of zes voor het hele Grasshopper traject.

Professor Messer, CompTIA A+
professormesser.com

Gratis YouTube serie die de absolute IT basis behandelt. Hardware, besturingssystemen, troubleshooting. Engels gesproken, helder uitgelegd. Niet alles is even relevant voor Ethisch Hacken, maar voor wie nog nooit met IT te maken heeft gehad een hele goede start.

WELKE KIES IK?

Hou je van lezen en je eigen tempo? Linux Journey. Wil je liever iemand zien uitleggen op een whiteboard? Professor Messer. Mag allebei. Maar als je TryHackMe Pre Security al doet, heb je in feite het meeste hier al meegepakt.

03

STAP 3

Concepten verkennen

Een lijstje begrippen die je in de eerste lesweken tegenkomt. Je hoeft ze niet uit je hoofd te leren. Zoek ze één keer op, lees twee minuten, en je hebt er al een beeld bij als wij er dieper op in gaan.

Penetration Testing Process

De Ethical Hacking Methodology

Als Ethisch Hackers gaan we niet random ons target aanvallen in de hoop dat één van de aanvallen werkt. We werken gestructureerd en methodologisch aan de hand van 6 stappen. Dit proces is niet lineair. Regelmatig ga je van stap vier of vijf weer terug naar stap twee en blijk je achteraf toch iets over het hoofd te hebben gezien. Juist daarom is het zo belangrijk om wel methodologisch te werk te gaan.

De stappen

Één

Pre-engagement

Voordat we van start gaan maken we eerst duidelijke afspraken over de opdracht. Dat doen we in de pre-engagement fase

Twee

Information Gathering

We gaan informatie verzamelen over ons target.

Drie

Vulnerability Assessment

Op basis van de gevonden informatie gaan we op zoek naar kwetsbaarheden.

Vier

Exploitation

Tijd om in de aanval te gaan. We gaan de gevonden kwetsbaarheden exploiteren.

Vijf

Post-exploitation

Eenmaal binnen gaan we kijken of we onszelf dieper het netwerk in kunnen werken én of we meer rechten kunnen krijgen.

Zes

Rapporting

Gedurende het proces houden we notities bij. Aan het eind maken we hier een mooi rapport van voor onze opdrachtgever.

WAT DOET EEN ETHISCH HACKER OP EEN DAG?

Als Ethisch Hacker ben je de hele dag aan het puzzelen. Je verzamelt informatie, gaat op zoek naar kwetsbaarheden, probeert ze uit en komt in een proces van trial & error steeds verder. Ondertussen houd je je aan de vooraf afgesproken scope en regels, en houd je een uitgebreid rapport bij.

Zoek de volgende begrippen eens op

Je hoeft ze niet direct uit je hoofd te kennen, maar kijk eens wat je over deze begrippen kunt vinden op het internet.

Poort scanning
- Wat is een IP adres?
- Wat zijn TCP/UDP poorten?
- Wat is FTP, SMB, SSH, HTTP, MYSQL?

Payloads
- Wat is een payload?
- Wat is een shell?
- Wat is een reverse shell en een bind shell?

Encryptie
- Wat is encryptie?
- Wat is een hash?

Active Directory (AD)
- Wat is AD?
- Wat is een Domain Controller?
- Wat is Kerberos?

OSI model (networking)
- Wat is het OSI model?
- Uit welke lagen bestaat het OSI model?

Information security
- Wat is de CIA Triad?
- Wat is vishing, whaling, spoofing, DDoS?

Windows en Linux, je ziet ze allebei

De meeste eindgebruikers in een organisatie zitten op Windows. De meeste servers, vooral op het internet, draaien Linux. Als Ethisch Hacker krijg je beide werelden voor je kiezen. Je moet zowel Windows als Linux computers en servers kunnen aanvallen. Dat begint bij goed begrijpen hoe deze operating systemen werken. Goed met Windows en Linux kunnen werken is dus een belangrijke basis.

Windows

Vrijwel alle bedrijfsnetwerken gebruiken Windows computers en servers.

Verdiep je eens in:

- Windows Defender
- Windows PowerShell
- Gebruikersaccounts: groepen, lokale accounts vs. domeinaccounts

Linux

Het besturingssysteem op de meeste servers, vooral richting internet toe.

Verdiep je eens in:

- De Linux terminal/command line → Bash
- Linux gebruikersaccounts, UID/GID, permissies
- De Linux bestandsstructuur (FHS)

Klaar voor de start?
Dat is mooier dan je denkt.

Heb je deze gids doorgenomen en stap 1 gedaan, dan zit je al ruim boven het gemiddelde van wie op dag één binnenkomt. Wij beginnen sowieso bij het begin, dit document maakt jouw begin alleen wat soepeler.

Wat je mag verwachten van ons

Het tempo is stevig en de stof is geregeld pittig, daar zijn we eerlijk over. Daar zetten we persoonlijke begeleiding in kleine groepen tegenover. Vragen mogen altijd, hoe klein ook.

Wat wij van jou verwachten

Nieuwsgierigheid, doorzettingsvermogen op momenten dat iets niet werkt, en bereidheid om vragen te stellen. Verder niets. Geen voorkennis, geen vakdiploma's, geen IT-achtergrond

VRAGEN OVER DEZE GIDS?

ChatGPT, Claude of een nette Google search lossen 90% op. Uitzoeken hoort sowieso bij Ethisch Hacker-werk, zie het als de eerste oefening. Welkom alvast.