- Internet - Veiligheid en bewustwording

Voor beginners

- Internet - Veiligheid en bewustwording

Voor beginners

Marc Huyghebaert

Schrijver: Marc Huyghebaert
Eerste verbetering: Josiana Bossuyt
Tweede verbetering: Peter van Hecke
Front cover: Brave New Books – Nederland
Foto backcover: Gordon de Clerck
ISBN: 9789464356007

Uitgave versie: Eerste druk, versie Mei 2023
Gedrukt door: Brave New Books - Nederland

DISCLAIMER

Alle foto's in dit boek blijven eigendom van hun respectievelijke makers en mogen niet worden gereproduceerd, gekopieerd of gebruikt zonder hun uitdrukkelijke toestemming.

De genoemde merknamen zijn eigendom van hun respectieve bedrijven. We hebben geen banden met deze bedrijven, tenzij uitdrukkelijk vermeld.

Het is belangrijk om te begrijpen dat dit boek bedoeld is als een leidraad en niet als een exacte wetenschap. Hoewel het waardevolle inzichten en informatie biedt over cyberveiligheid, biedt het op zichzelf geen garantie of bescherming tegen mogelijke cyberbedreigingen.

Het is aan de lezer om deze informatie te gebruiken als onderdeel van een bredere strategie voor cyberveiligheid, die regelmatig moet worden geëvalueerd en aangepast om rekening te houden met veranderende bedreigingen en risico's.

We raden lezers dan ook aan om professioneel advies in te winnen en hun eigen onderzoek te doen voordat ze beveiligingsmaatregelen implementeren.

De auteur en de uitgever van dit boek hebben geprobeerd om de informatie in dit boek zo accuraat mogelijk weer te geven op het moment van publicatie. De auteur en de uitgever zijn echter niet verantwoordelijk voor eventuele fouten of weglatingen, of voor eventuele schade die voortvloeit uit het gebruik van de informatie in dit boek.

Voor vragen over de rechten voor publicatie van dit boek of voor meer informatie over de auteur, kunt u contact opnemen via info@ethisch-hacker.be.

DANKWOORD

Graag wil ik mijn dankbaarheid uitspreken aan iedereen die de tijd heeft genomen om mijn teksten na te lezen, tests uit te voeren en mij te inspireren, moed te geven, kracht te bieden en te steunen op momenten waarop ik het gevoel had dat ik niet verder kon. Jullie steun heeft mij geholpen om door te zetten en het beste uit mezelf te halen.

Het is niet altijd gemakkelijk om een project of doel te bereiken en ik ben me ervan bewust dat ik dit niet alleen had kunnen doen. De steun en feedback die ik heb ontvangen hebben mij geholpen om mijn werk te verbeteren en te groeien als persoon.

Ik realiseer me ook dat het niet vanzelfsprekend is dat mensen hun tijd en energie steken in de ondersteuning van anderen. Ik waardeer het daarom des te meer dat er mensen zijn die dat wel doen. Jullie hebben mijn leven verrijkt en ik zal jullie steun nooit vergeten.

Nogmaals, hartelijk dank voor jullie steun en aanmoediging. Ik zal deze ervaring koesteren en als motivatie gebruiken voor toekomstige uitdagingen en doelen die ik wil bereiken.

VOORWOORD

Het doel van dit boek is om u een waardevol instrument en handvat te bieden, waarmee u uw online veiligheid kunt waarborgen en beschermen.

Cybersecurity is een complexe uitdaging en er zijn veel factoren die afzonderlijk of gezamenlijk uw veiligheid in gevaar kunnen brengen. Dit boek biedt inzicht in de belangrijkste bedreigingen en risico's waarmee u online te maken kunt krijgen en geeft praktische adviezen en oplossingen om deze risico's te verminderen.

Om uw cybersecurity verder te verbeteren, bieden wij op maat gemaakte trainingen aan. Onze trainingen zijn gericht op het vergroten van uw bewustzijn van de gevaren van het internet en op het aanleren van effectieve technieken en 'best practices' om uzelf te beschermen. We begrijpen dat elke persoon en elk bedrijf anders is en daarom bieden we trainingen die speciaal zijn afgestemd op uw individuele behoeften en eisen.

Onze toewijding ligt bij het verbeteren van uw online veiligheid en het voorzien van de nodige tools en kennis om veilig te blijven in de digitale wereld. Wij begrijpen dat het belangrijk is om op de hoogte te blijven van de nieuwste technieken en bedreigingen, en daarom bieden wij voortdurend actuele informatie en trainingen aan om u te helpen. Onze missie is om u te ondersteunen bij het creëren van een veilige online omgeving voor uzelf, uw gezin en/of uw bedrijf.

Als men een schoendoos neemt, dan is de grootte ervan bekend. Bij Cybersecurity en hacking is er echter geen grootte of vast einde. Ieder moment van de dag komt er wel iets nieuws bij. Voor mij persoonlijk gaat het erom de computergebruiker bewust te maken van de gevaren van het internet.

Dagelijks horen we in het nieuws over mensen die in de val zijn getrapt. En nu komt iets wat velen niet graag zullen horen, maar meestal is het hun eigen schuld of hebben ze (onbewust) mee bijgedragen aan de oplichting of inbreuk. Onbewust, maar het had voorkomen kunnen worden.

Ik ga dus proberen om zoveel mogelijk technische en juridische zaken uit te leggen. In onze Cybersecurity Awareness Trainingen kunnen wij u effectief laten zien hoe Phishing werkt, hoe men uw pc, gsm, camera of microfoon kan overnemen, enzovoort. Hoe dit precies in zijn werk gaat, hoeft u niet in dit boek te verwachten. Dit is geen handleiding voor aspirant-hackers, laten we dat duidelijk stellen.

Iets leren en kunnen is één ding, het vertellen en tonen gaat nog wel, maar het op papier zetten is totaal iets anders. We gaan dus ons best doen.

Veel leesplezier!

BIO

Mijn naam is Marc Huyghebaert. Ik behaalde mijn eerste certificaat voor ethisch hacken in augustus 2021, gevolgd door mijn Bachelor in Security Management in december van datzelfde jaar.

Een essentieel aspect van Security Management is hacking en ik blijf mezelf voortdurend bijscholen door het volgen van cursussen. Mijn doel is om mensen van alle leeftijden bewust te maken van het belang van cybersecurity en in het bijzonder van hacking. Het internet kan namelijk een gevaarlijke plek zijn en het is belangrijk dat mensen zich bewust zijn van de mogelijke risico's en gevaren.

Als cybersecurity-professional wil ik mensen laten zien hoe criminelen hen kunnen aanvallen en vooral hoe ze zichzelf kunnen beschermen tegen deze bedreigingen. Door het vergroten van het bewustzijn en het delen van mijn kennis en expertise hoop ik bij te dragen aan een veiligere digitale wereld voor ons allemaal.
.

Inhoudstafel

Hacking

1.1 Hacking – Definitie

Wat is Hacking?

Net zoals een inbreker toegang tot uw huis probeert te krijgen, probeert een hacker toegang te krijgen tot uw digitale infrastructuur, of het nu gaat om één enkele computer of telefoon of uw hele netwerk, zowel privé als van uw bedrijf. Een hacker krijgt dus toegang tot uw digitale informatie, uw digitale identiteit, uw digitale leven.

Het openen van een bierflesje met uw telefoon is bijvoorbeeld geen hacking en een vals of nepprofiel op een sociaal media platform is ook geen hacking.

De term hacking wordt de laatste jaren nogal losjes gebruikt. De meest gangbare definitie van hacking is het ongeoorloofd binnendringen in een computersysteem. Met de inbraak is meestal kwaad opzet gemoeid. Maar ook het per ongeluk tot stand brengen van een verbinding en het vrijwillig behouden van die verbinding wordt als hacking beschouwd.

1.2 Type Hackers

Nu we weten wat hacking eigenlijk is, moeten we ook weten dat niet alle hackers dezelfde zijn. Over het algemeen zijn er drie soorten hackers die elk dezelfde kennis en vaardigheden hebben, maar toch sterk van elkaar verschillen.

De Black Hat - Hacker

Dit is de crimineel. Deze persoon of groep personen gebruiken hun kennis met criminele doeleinden, variërend van het platleggen van systemen en het eisen van geld (Malware) tot het wijzigen van gegevens en het buitmaken van geld, enzovoort.

De Gray Hat – Hacker

Dit type hacker doet meestal goede dingen. Hij breekt zonder toestemming in en rapporteert dan zijn bevindingen aan de desbetreffende eigenaar. Als de buit echter te mooi is, dan...

De White Hat – Hacker

Meestal ook wel de Ethische Hacker genoemd. Hij vraagt eerst toestemming of heeft als doel mensen bewust te maken van de problematiek. Grote bedrijven nemen dit type hacker de laatste jaren in dienst om hun eigen systemen voortdurend te testen en te beveiligen zodat de Black Hat Hacker geen kans meer heeft om iets te stelen.