KEUZEDELEN edu actief

VEILIG PROGRAMMEREN

Boom beroepsonderwijs

COLOFON

Boom beroepsonderwijs
info@boomberoepsonderwijs.nl
www.boomberoepsonderwijs.nl

Auteur: Gabriel Sanchez Cano

Eindredactie: Jan Hoeve

Titel: Veilig programmeren

ISBN: 978 90 372 6152 3, maakt deel uit van pakket 978 90 372 6153 0.

Eerste druk/eerste oplage

INHOUDSOPGAVE

1. WERKEN MET DIT KEUZEDEEL 4
2. NETWERKARCHITECTUUR 6
3. PENTESTEN MET KALI LINUX 50
4. SECURITY DEVELOPMENT LIFECYCLE 105
5. UITDAGING 189

1 WERKEN MET DIT KEUZEDEEL

DIGITALE LEEROMGEVING

Bij sommige opdrachten heb je hulpmiddelen nodig. Bijvoorbeeld filmpjes, formulieren of een link naar een website. Deze staan allemaal in de digitale leeromgeving. Dit icoontje verwijst naar de digitale leeromgeving. Om hier te komen ga je naar digitaal.boomonderwijs.nl/beroepsonderwijs.

Eerste keer inloggen in de digitale omgeving
Voordat je de digitale leeromgeving kunt gebruiken moet je je licentie activeren.

- Overleg met je docent welk type account je gebruikt.
- Ga naar www.boomberoepsonderwijs.nl/licentie.
- Bekijk de instructiefilm of lees het stappenplan.
- Volg de stappen.

Daarna kun je aan de slag!

VEILIG PROGRAMMEREN

Het keuzedeel Veilig programmeren gaat in op de beveiligingsaspecten van het ontwikkelen van webapplicaties. In dit keuzedeel doe je specialistische kennis en vaardigheden op om tijdens het ontwikkelen van applicaties voldoende maatregelen te treffen op het gebied van beveiliging. In dit keuzedeel komen specialistische kennis en vaardigheden aan bod rondom het ontwerpen, ontwikkelen, testen en onderhouden van veilige applicaties.

Deze nieuwe versie is volledig geherstructureerd. Het eerste deel is volgens het OSI-model geschreven. Het tweede deel is volgens de SDL-methodiek gestructureerd. Dit gecombineerd met een nieuwe opmaak levert een meer helder en up-to-date boek op.

Voorkennis en ervaring met het bouwen van webapplicaties en MySQL-databases zijn vereist.

Bekijk de film. Deze geeft je een goed beeld waar dit keuzedeel over gaat.

Je kunt de audio in de video automatisch laten ondertitelen in het Nederlands.

LEERDOELEN

1. Je hebt basiskennis van alle lagen van het OSI-model.
2. Je kunt serverscans uitvoeren.
3. Je kunt server-pentesten uitvoeren.
4. Je kunt applicatie-pentesten uitvoeren.
5. Je weet hoe SDL-methodologie toe te passen.
6. Je kunt beveiligingseisen voor een applicatie opstellen.
7. Je weet hoe foutafhandeling binnen een applicatie te ontwerpen.
8. Je kunt zonering toepassen in een applicatie zodat applicatiecode en gegevens zoveel mogelijk worden gescheiden.
9. Je kunt cryptografische technieken toepassen.
10. Je kunt code reviewen van de eigen code en code van anderen.
11. Je kunt rol gebaseerde autorisaties implementeren.
12. Je kunt het OAuth2 framework implementeren

13. Je weet hoe handelingen van gebruikers vast te leggen in een logbestand.
14. Je kunt testplannen opstellen.
15. Je kunt privileges voor services opstellen.
16. Je kunt verifiëren of een applicatie ongewenste functionaliteit(en) bevat en kwetsbaar is voor aanvallen.
17. Je kunt het juiste gebruik van een applicatie controleren en/of achteraf fouten en overtredingen opsporen.

Dit keuzedeel bestaat uit:

- *Theorie, begrippen en opdrachten*
  Hierbij leer je over en oefen je met de praktijk. In sommige opdrachten werk je aan beroepsproducten, deze opdrachten herken je aan . Deze beroepsproducten kun je verzamelen in je portfolio en heb je nodig om de uitdaging aan het einde van dit keuzedeel goed af te ronden.
  De beroepsproducten in dit keuzedeel zijn:
  - *Wireshark-scan*
  - *Metasploit-pentest*
  - *ZAP-pentest*
  - *Risicoanalyse*
  - *Google developersaccount*
  - *OAuth2*
  - *OAuth2 in frameworks*
  - *SSL-certificaat*
  - *OAuth2 in API's*
  - *Pentest-rapport*

- *Test je kennis*
  Hiermee kun je zelf je kennis van de theorie testen.

- *Uitdaging*
  Dit is het eindproduct en de afronding van het keuzedeel. Hier werk je gedurende het hele keuzedeel naartoe. En hier word je op beoordeeld.
  Voor de uitdaging van dit keuzedeel ontwerp, ontwikkel en test je een veilige applicatie.

- *Theorietoets*
  Je docent besluit of je ter afsluiting een theorietoets maakt.

2 NETWERKARCHITECTUUR

Bij het beveiligen van servers en applicaties kun je als analogie denken aan het beveiligen van je eigen huis. Je wilt eerst weten hoeveel deuren en ramen er zijn. Welke deuren en ramen zijn kwetsbaar voor inbrekers? Wat zijn de gewoontes? Laat je de achterdeur soms open? Ligt de sleutel altijd onder de mat? Bij het beveiligen van servers en applicaties gaan we precies hetzelfde doen. In dit hoofdstuk kijken we naar netwerkarchitectuur en in hoofdstuk 4 naar softwarearchitectuur.

Figuur 2.1 Netwerkarchitectuur.

AAN HET EIND VAN DIT HOOFDSTUK

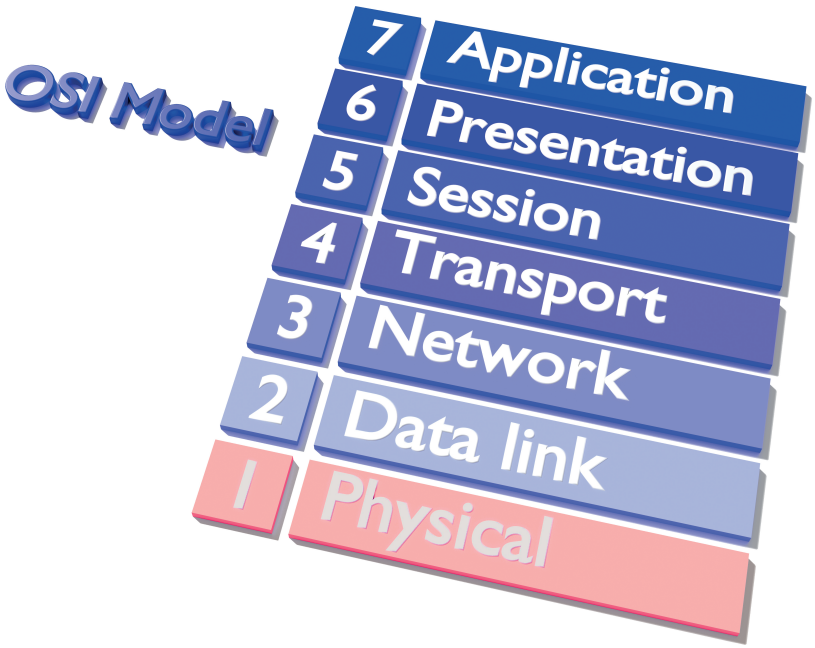
1. heb je basiskennis van het OSI-model
2. heb je basiskennis van de kwetsbaarheden van de lagen in het OSI-model
3. heb je basiskennis van het beschermen van de lagen in het OSI-model
4. kun je netwerkverkeer scannen en analyseren met Wireshark.

THEORIEBRON OSI-MODEL

Netwerkarchitectuur is het design van de fysieke componenten van een netwerk en de procedures en de communicatieprotocollen van deze componenten. Netwerkapplicaties gebruiken protocollen om met andere applicaties in het netwerk te communiceren. Een protocol schrijft voor welke regels uitgevoerd

moeten worden. De programmeur focust meestal op het softwareontwikkelingstraject. Bij het ontwerp van veilige applicaties moet de programmeur ook kennis hebben van de geïmplementeerde protocollen en de kwetsbaarheden verbonden met deze componenten en protocollen.

Het OSI-model beschrijft de verschillende taken in lagen (layers) die nodig zijn voor het verbinden en communiceren met netwerken. Het OSI-model staat voor: Open Systems Interconnection. Het OSI-model is een referentiemodel en beschrijft de functies die op een bepaalde laag uitgevoerd moeten worden. Programmeurs gebruiken het TCP/IP-model om te zien wat voor protocollen hun programma's gaan draaien. Netwerkbeheerders gebruiken het OSI-model voor trouble shooting (netwerkproblemen oplossen). In de volgende figuur is het OSI-model schematisch weergegeven. De application layer is de interface tussen de gebruiker en de applicaties en gebruikt protocollen zoals HTTP, SMTP en DNS. Aan de hand van het OSI-model bestuderen we in dit hoofdstuk de architectuur en de veiligheid en kwetsbaarheden van netwerken. In hoofdstuk 4 kijken we naar de architectuur en de veiligheid en kwetsbaarheden van webapplicaties.



Figuur 2.2 OSI-model.

OSI-Physical layer

Dit is de onderste laag in het Open System Interconnection (OSI)-model. Het bestaat uit verschillende netwerkcomponenten zoals stekkers, connectoren, ontvangers, kabeltypes et cetera. Physical layer stuurt databits van het ene apparaat (zoals een computer) naar het andere apparaat. De physical layer kan coax, fiber of wireless zijn en zorgt voor de dataconnectiviteit.

Figuur 2.3 OSI-Physical layer.

Physical layer kwetsbaarheden

Beveiliging in deze laag is van cruciaal belang. Bijvoorbeeld bij een DoS-aanval moet de kabel losgekoppeld worden van het primaire systeem. Denial of Service oftewel DoS-aanvallen bespreken we in de volgende hoofdstukken. Deze verstoring kan worden veroorzaakt door het fysiek doorknippen van de kabel en door het verstoren van draadloze signalen.

Om deze laag te beschermen, zijn biometrische beveiliging, camerabewaking, sleutelkaarten en andere fysieke bewaking nodig.

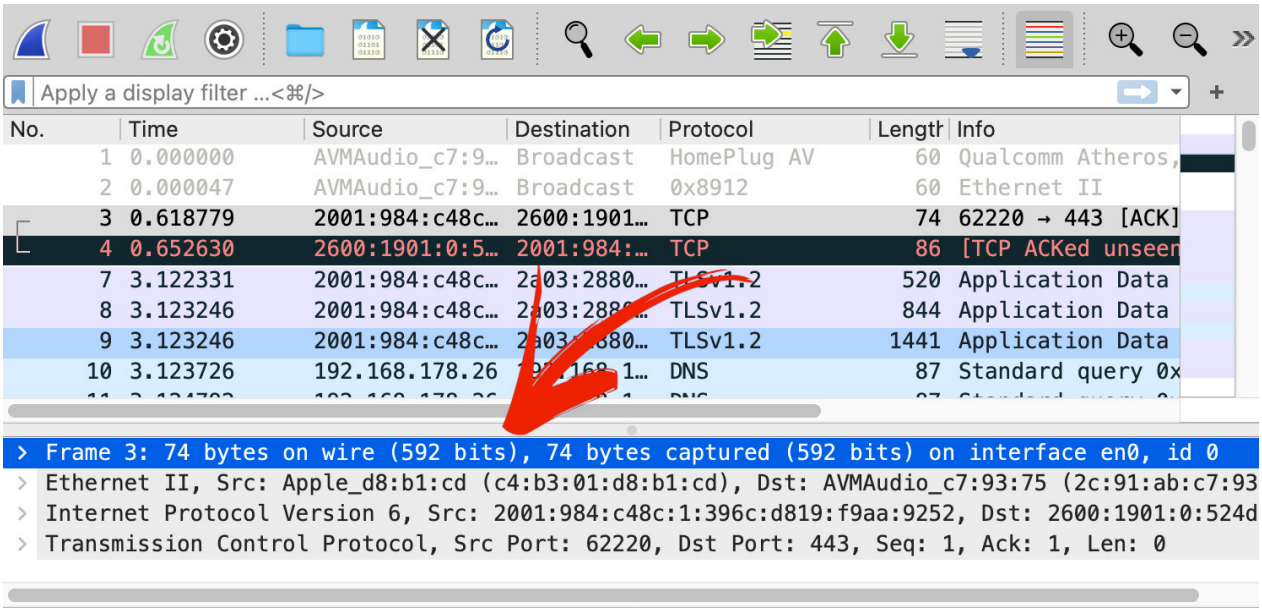
Er zijn geautomatiseerde draadloze hacktools beschikbaar die cybercriminelen gebruiken. Enkele van deze tools zijn:

- AirCrack
- AirSnort
- Cain & Able
- Wireshark
- NetStumbler.

Met deze tools kun je toegang op afstand, schoudersurfen, toegang tot het dashboard van de draadloze router en brute-force-aanvallen uitvoeren om draadloze beveiliging te doorbreken. Een brute-force-aanval is een hackmethode die alle beschikbare inputs in een tabel probeert om wachtwoorden, inloggegevens en coderingssleutels te kraken.

Netwerkscans

Wireshark is een tool die we gaan gebruiken om verkeer tussen netwerken te scannen en analyseren. In de volgende figuur zie je een Wireshark-scan van het verkeer tussen twee netwerken.



Figuur 2.4 Wireshark-netwerkscan van physical layer.

In bovenstaande figuur zie je een Wireshark-scan. Bovenaan hebben we data-packet 3 geselecteerd. Onderaan zien we frame 3 met informatie over de physical layer. Op het eerste gezicht lijkt het allemaal raadselachtig. In de volgende hoofdstukken gaan we deze geheimzinnige codes ontcijferen door een beetje detectivewerk te verrichten. Na het kijken naar deze scan realiseren we ons dat we eerst moeten kennismaken met een aantal basisbegrippen over netwerken zoals:

- netwerkmodellen
- netwerkprotocollen
- data-packets
- headers
- poorten
- IP-adressen.

Netwerkmodellen

Zoals eerder gezegd, om een gebouw te kunnen beveiligen moet je eerst de blauwdruk van het gebouw bestuderen om de kwetsbare punten te kunnen identificeren. Een netwerkblauwdruk noemen we een netwerkmodel.

In de volgende figuur zien we twee netwerkmodellen: het peer-to-peer-model, verkort tot P2P, en het client/server-model.

Figuur 2.5 Netwerkmodellen.

Peer-to-peer

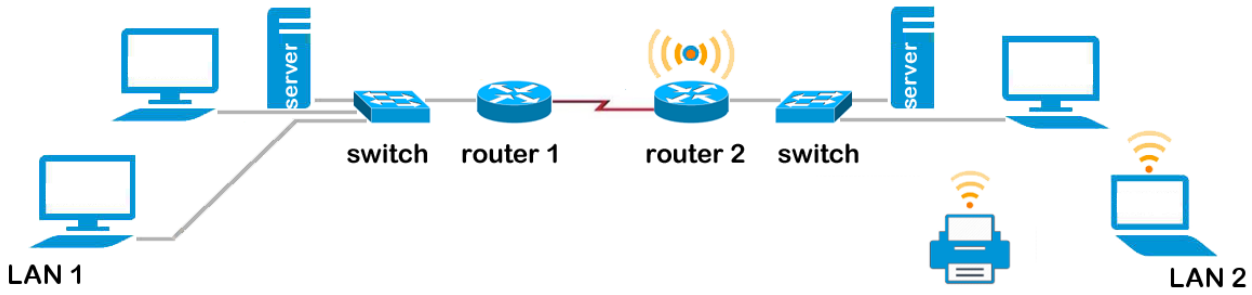
In een peer-to-peer-model hebben we twee computers die bestanden met elkaar delen. Voorbeelden van P2P-netwerken zijn bestanden delen met BitTorrent of instant messaging met WhatsApp. In dit model zijn beide computers servers, want beide computers serveren bestanden.

Client/server

In een client/server-model is één computer de server en de andere zijn clients. De server serveert bestanden en andere data aan de clients. Voorbeelden van client/server-netwerken zijn webwinkels en internetbankieren.

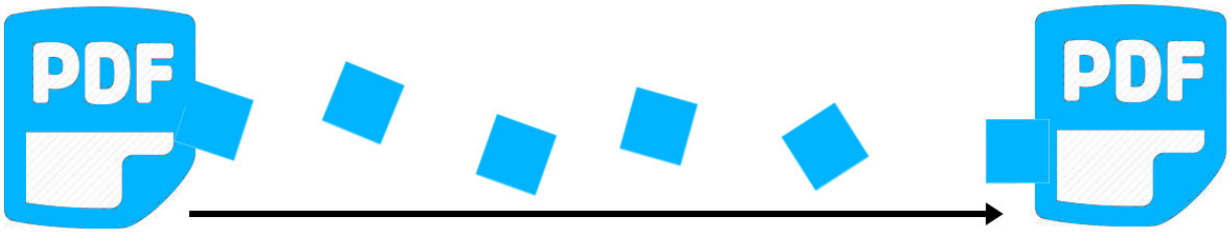
Routers en switches

Met switches kunnen we computers fysiek met elkaar UTP, fiber of wireless verbinden binnen een local area network (LAN). Een router verbindt twee of meer netwerken met elkaar of met het internet. In de volgende figuur zien we een netwerktopologie met netwerk 1 met twee computers verbonden via een router met netwerk 2.



Figuur 2.6 Netwerktopologie.

Een server kan bestanden delen (serveren) met de computers in het eigen netwerk. Maar deze kan ook bestanden serveren via de router naar computers in een ander netwerk. Dit doet de router met behulp van protocollen. Bijvoorbeeld, een protocol zorgt ervoor dat het te delen bestand opgesplitst wordt in data-packets. Een data-packet is een data-eenheid. Deze packets worden via de netwerkverbinding verstuurd naar de ontvangende computer.



Figuur 2.7 Bestand opgesplitst en verstuurd in data-packets.

OPDRACHT 1 Lab: Physical layer

a. In deze lab-opdracht maken we kennis met Wireshark. Wireshark is een tool voor het scannen of 'snuiven' van data-packets in netwerkverkeer en het analyseren van de gebruikte protocollen in netwerkcommunicatie. Download, installeer en start Wireshark. Dubbelklik op *Wi-Fi* om het dataverkeer tussen je pc en het internet te scannen. Maak een scan als volgt:

Stap 1. Typ als filter wireshark.org in.
Stap 2. Selecteer *Wi-Fi* om een scan van het dataverkeer tussen jouw pc en wireshark.org uit te voeren.
Stap 3. Klik op de startscan-knop

Met je browser ga naar de wireshark.org website, je ziet in Wireshark het dataverkeer verschijnen.

Zie volgende figuur.