CySec – les 5

Netwerken, Man in the middle, netwerk beveiliging en wireshark

Nova College

Programma

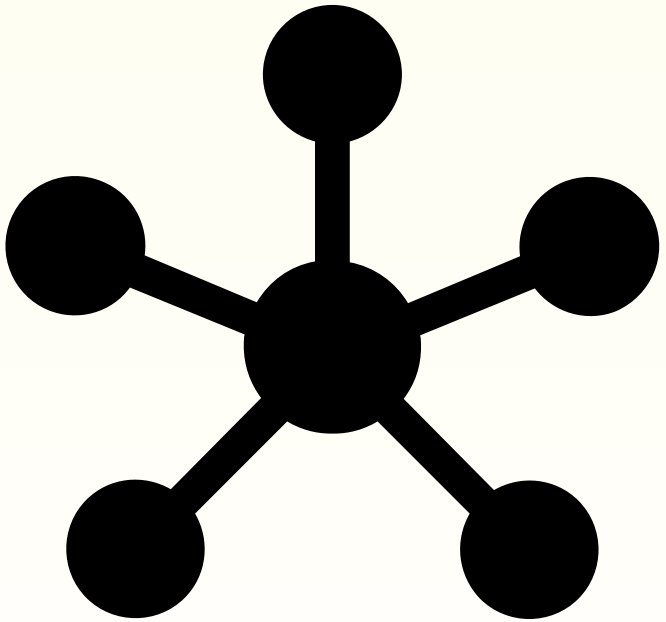
- Terugblik vorige les
- Leerdoelen
- Netwerken
- Man in the middle
- Netwerk beveiliging
- Wireshark en netwerkverkeer
- Volgende week

Wat weten we nog van vorige les?

Leerdoelen

- Aan het einde van de les:
  - Weet je de basis structuur van een netwerk
  - Weet je wat voor soort berichten over een netwerk gaan
  - Weet je hoe een man in de middle werkt
  - Weet je wat te doen om een man in de middle tegen te gaan
  - Weet je wat je kan doen om een netwerk gepast te beveiligen
  - Kan je een Netwerk monitoren en berichten filteren

Netwerken

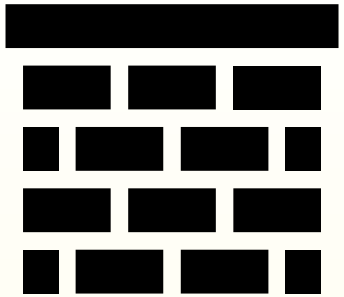


- Een connectie tussen twee of meer computerende apparaten
- 3 kern-types van netwerken
  - Direct pc-pc (Komt bijna niet meer voor)
  - Kabelnetwerk (Ethernet, USB-C)
  - Draadloos (Wifi, 5G)

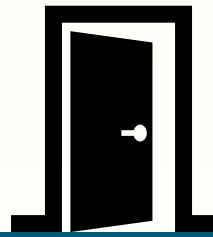
Werkvorm - Netwerken

- 2 paren kiezen een wachtwoord voor ieder paar uit de opties
- 1 persoon is de netwerk runner.
- De twee paren staan op overstaande zijdes van het lokaal met de ruggen naar elkaar toe.
- De verzoeker stuurt berichten met hun wachtwoord
- De ontvanger geeft het correcte bericht terug naar de verzoeker
- Communicatie is blind en via de netwerk runner.

Netwerk aanvallen



- Blokkade/wijgering aanvallen
  - DDOS – Distributed denial of services
    - Het platleggen van een systeem door het netwerk te bombarderen met verzoeken van vele plaatsen
  - Volume bezetting/sturing
    - Een netwerk bezet houden waardoor werkelijke berichten niet erdoorheen komen
  - Malafide geformatteerde pakketten aanvallen
    - Een invoer die de server/service der mate verlangzaamd dat deze niet goed meer kan functioneren
- Toegang aanvallen
  - IP spoofing
    - Maskeer je IP adres om te doen alsof je al op een netwerk zit of hoort om toegang te krijgen.
  - Man in the middle/ packet sniffing
    - Netwerken afluisteren om data te krijgen of om cruciale gegevens te vinden om meer toegang te krijgen.



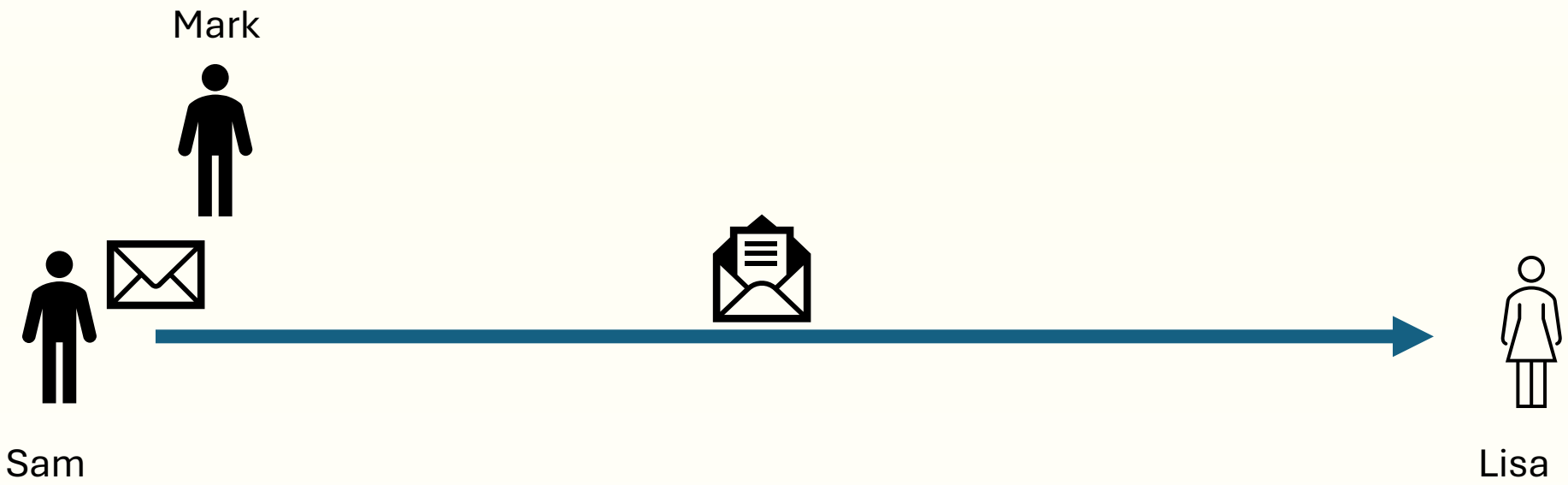
Netwerk aanvallen

- Onderzoekende aanvallen
  - Ping/port sweeping
    - Welke apparaten/ poorten staan open om toegang te verlenen op een netwerk en hoe kan je die benutten om vervolgens verder in het systeem te komen.
- Afluisterende aanvallen
  - IP spoofing
    - Slechte netwerken controleren niet of er een dubbel IP adres actief is op het netwerk. Beide krijgen een kopie van al hun binnenkomende berichten.

Netwerk aanvallen

- Brekende/manipulerende aanvallen
  - Buffer overflow aanvallen
    - Gebruik maken van server zwaktes om errors herhaaldelijk te creeren om zo het systeem’s geheugen aan te tasten. Dit zorgt ervoor dat er een gat ontstaat in de code en die kan een hacker vullen met eigen code

Man in de middle !



Bekende netwerk tactieken en voorbeelden

- De “Wifi in de trein” techniek
- De “Koffieshop” techniek
- Het “IT studentenhuis” fiasco

- Extra: het pride parade schandaal van een groep onderzoekers

Netwerk beveiliging - invalshoeken

- Voorkom connectie
- Voorkom toegang
- Voorkom ongeauthorizeerde data
- Voorkom data extractie

Netwerk beveiliging - thuis

- WPA3 versleuteling
- Splitsing tussen privé en gast netwerk
- Beveiligd netwerk zonder publieke fysieke aansluiting
- Firewalls
- VPN
- Sterke geheime wachtwoorden, dit blokkeert 70% van de privé dreigingen
- Formeel verzoek tot verwijdering data geschiedenis bij internet provider **'recht op vergetelheid'** (artikel 17 AVG)

Spysoftware

- Hackers willen om meerdere redenen spysoftware plaatsen
  - Chantage (blackmail) van personen of bedrijven
  - Bedrijfsgeheimen
  - Zwarte markt voor data
  - Zwaktes ontdekken voor een zwaardere aanval

- Veel van de bekende spysoftware is makkelijk te herkennen

Spysoftware

- Syptomen van spysoftware:
  - Camera’s die aan en uit gaan van apparaten zonder reden
  - Je computer is ineens verlangzaamd zonder reden
  - Je computer wordt veel warmer zonder reden
  - Je muis beweegt zonder dat er input is (Dit is ook control software)
  - Je computer gaat van standby ineens aan zonder reden.

Spysoftware - beveiliging

- Meeste spysoftware is te vinden via de standaard beveiliging
- Mcafee en AVG zijn iets beter maar deels betaald

- Open geen files waarvan je niet weet waar en van wie ze vandaan komen. Een spysoftware kan al in een afbeelding verstopt zitten.
- Klik niet op links van vreemde bronnen of advertenties die te mooi klinken.
- Voorkom inloggen op publieke netwerken

Wireshark

- Wireshark is een soort afluister programma dat in een grijs gebied valt.
- Er is een opdracht beschikbaar voor maar die is **NIET** verplicht.
- **BELANGRIJK**: DOE dit **NIET** op het eduroam netwerk maar op het ICT netwerk. Je IP wordt anders **geblokkeerd.**

Volgende week

- Wetgeving deel 2
  - Nederlandse cyber wetgeving
  - Amerikaanse cyber wetgeving
  - Chineese cyber wetgeving
- Contracten en NDA