Inhoudstabel

LES 1: Introductie cryptografie – Symmetrische cryptografie

Leg uit: Steganografie

- Data verstoppen in of achter andere data
  - Foto
  - Document
  - Folder
  - Audio
  - Video
  - Web based/ websites/ url/ verborgen locatie op een pagina
  - E-mails
  - …
- Vervangt ongebruikte data bits met de verborgen data bits (LSB)
- Heel moeilijk, misschien zelfs onmogelijk om te achterhalen

Leg uit: Caesar 5 Substitutie

= mono-alfabetische substitutie

Bijvraag: 5 is de sleutel

Bij de versleuteling maak je gebruit van twee alfabetten. Een regulier en een met rotatie daarin. Als er bijvoorbeeld een voor een rotatie van 23 (Rot23) wordt gekozen:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

Hierna vervangt men de letters van de onversleutelde tekst door de letter die eronder staat in de tabel. Zodoende wordt de geheime boodschap:

Klare tekst: D I T I S Z E E R G E H E I M

Cijfertekst: A F Q F P W B B O D B E B F J

Leg uit: Vigenère

= poly alfabetische substitutie

Het vervangen van letters aan de hand van verschillende alfabetische reeksen.

Men kiest eerst een geheim sleutelwoord, bijvoorbeeld ZODIAK. Dit schrijft men onder de klare tekst. Vervolgens zoekt men de klare letter op in het verticale alfabet en de letter van het sleutelwoord in het horizontale alfabet. De kruising van beiden is de resulterende codeletter. Zo kunnen we zien dat de kruising van D en Z in de tabel de letter C is.

Klare tekst: D I T I S Z E E R G E H E I M

Sleutelwoord: Z O D I A K Z O D I A K Z O D

\- -

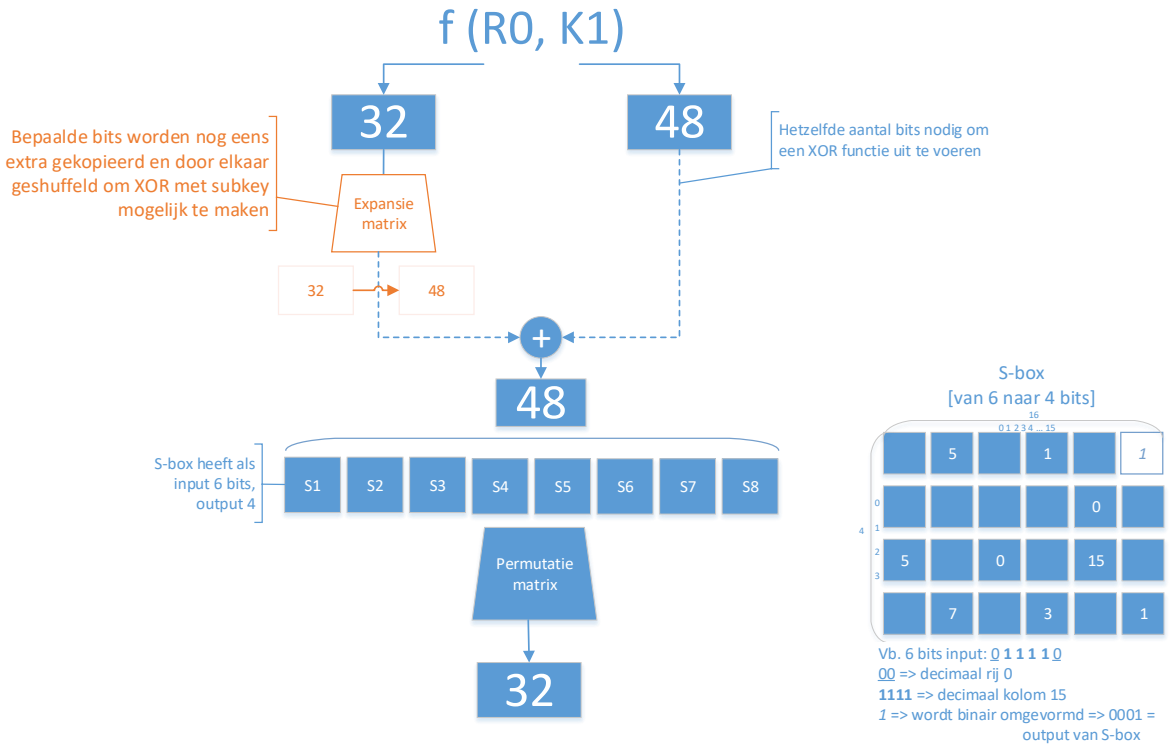
Cijfertekst: C W W Q S J D S U O E R D W P

Geef de voor- en nadelen van DES/AES

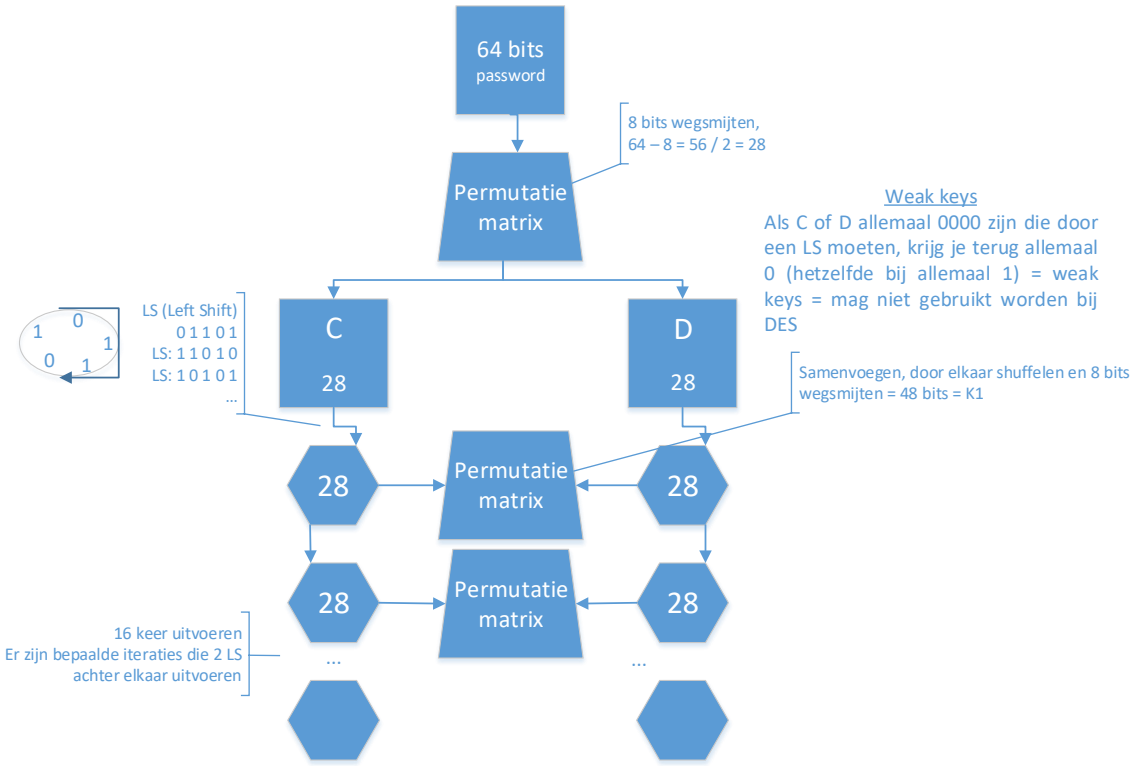
✓ Voordeel:
- Snel (=number crunchers)

- Nadeel:
- Sleutelmanagement, hoe ga je de sleutel veilig van A naar B krijgen (big bad internet)
- Het aantal sleutels, aantal keys stijgt exponentieel met het aantal gebruikers

Leg uit: Fystal functie (figuur)



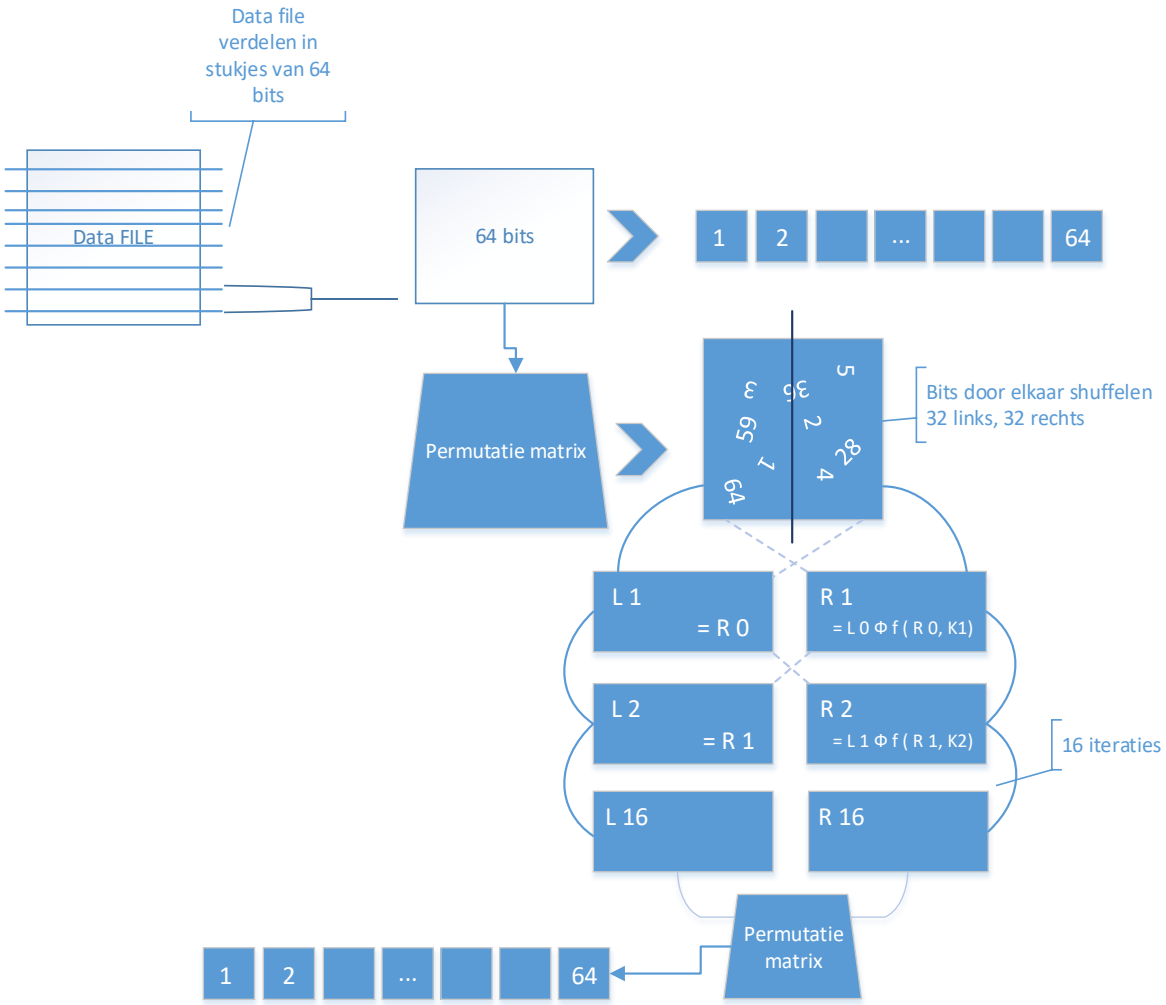
Leg uit: subkey berekening van DES (figuur)



Zie filmpjes Onsophic

Leg uit: algemene structuur van DES + fystal functie

DES werkt met substitutie en transpositie > 16 iteraties (=number cruncher)



Leg uit: Avalanche effect

Wanneer een hacker de file probeert te decrypteren, doet hij een gok naar het paswoord. Stel dat hij maar 1 bit ernaast zit, een kleine fout. De kleine fout zal door de 16 iteraties supergroot worden waardoor het decrypteren onmogelijk zal worden.

Leg uit: Weak Keys

Bij de keyberekening worden de bits geshuffeld door een LS (left shift) uit te voeren. Als er allemaal 0000 of 1111 door een LS moeten, krijg je terug allemaal 0000 of 1111 = weak keys. Mag niet gebruikt worden bij DES

LES 2: Asymmetrische cryptografie, Hashing, Digital Signature

Geef voorbeeld algoritme van asymmetrische cryptografie

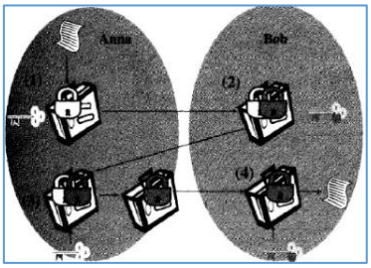
RSA

Voordelen en nadelen van asymmetrische cryptografie

✓ Voordeel:
  - Key management: enkel eigen private key bijhouden en public key staat op het internet

- Nadeel:
  - Traag > veel wiskundige magic

Leg uit: Diffie-helman



Principe: sleutel veilig van A naar B kunnen brengen.

1. A doet slotje op koffer en verstuurt naar B (alleen A kan openen
2. B doet slotje op koffer en verstuurt naar A (alleen B kan openen)
3. A haalt slotje eraf en stuurt naar B
4. B haalt slotje eraf

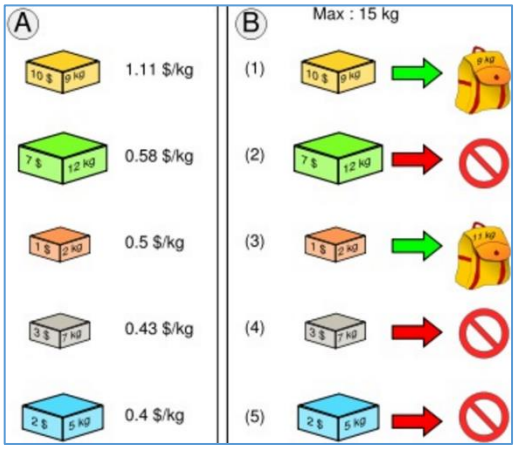
Leg uit: Man in the middle attack

- C stelt zich tussen A en B op
- We krijgen nu communicatie tussen A-C en C-B
- A-C spreken nu sleutel K1 af, en C-B spreken sleutel K2 af
- A en B hebben op die manier niet door dat iemand hun berichten onderschept en eventueel kan veranderen => best authenticatie-methode zoals digitale handtekeningen gebruiken

Leg uit: Knapzak systeem

Enorm grote verzameling objecten met ieder een apart gewicht

- Aantal object worden in de zak gestoken (geheim welke objecten)
- Gewicht wordt bekend gemaakt + de grote lijst van mogelijke objecten
- = ondoenbaar, te veel combi's om uit te rekenen
- Niet meer veilig > achterdeur om private key van public key af te leiden



Leg uit: Hashing

Hashing maakt van data een unieke hash code die niet teruggerekend kan worden (one way function) naar de oorspronkelijke code. Voorbeeld: wachtwoorden worden gehashed opgeslagen. Op het moment dat de identiteit van iemand geverifieerd wordt (identiteitscontrole), wordt de hash van het wachtwoord vergeleken met de hash dat in de database opgeslagen staat. Op deze manier kan men controleren of iemand het juiste wachtwoord ingevoerd heeft zonder dat dat wachtwoord opgeslagen is op een manier die terug te rekenen is naar het oorspronkelijke wachtwoord. + collision free.

Geef voorbeeld algoritmes van hashing

MD5, SHA1, SHA2, …

Leg uit: Rainbow tables

Een rainbow table is een eenvoudige tabel met allerlei mogelijke wachtwoorden en de hashes van deze wachtwoorden. Hij wordt gebruikt om wachtwoorden te testen op veiligheid, of om ze te kraken. Een efficiënte methode om dit tegen te gaan is gebruik van zogezegd zout (salt). Dit is het toevoegen van een willekeurige tekenreeks aan het wachtwoord voordat het gehasht wordt. De salt wordt samen met de hash van het wachtwoord bewaard.

Leg uit: Birthday paradox

- Hoeveel willekeurige mensen moet je verzamelen in een kamer, zodat de kans dat iemand dezelfde verjaardag heeft al u, 50% is? > 253
- Hoeveel willekeurige mensen moet je verzamelen in een kamer, zodat de kans dat 2 willekeurige mensen in de kamer dezelfde verjaardag hebben, 50% is? > 23
- = het vinden van een exacte collision is zeer moeilijk, maar een willekeurige collision iets minder moeilijk, maar toch nog moeilijk
- = omdat het aantal connecties (mappings) tussen de kandidaten exponentieel toeneemt wanneer het aantal kandidaten toeneemt

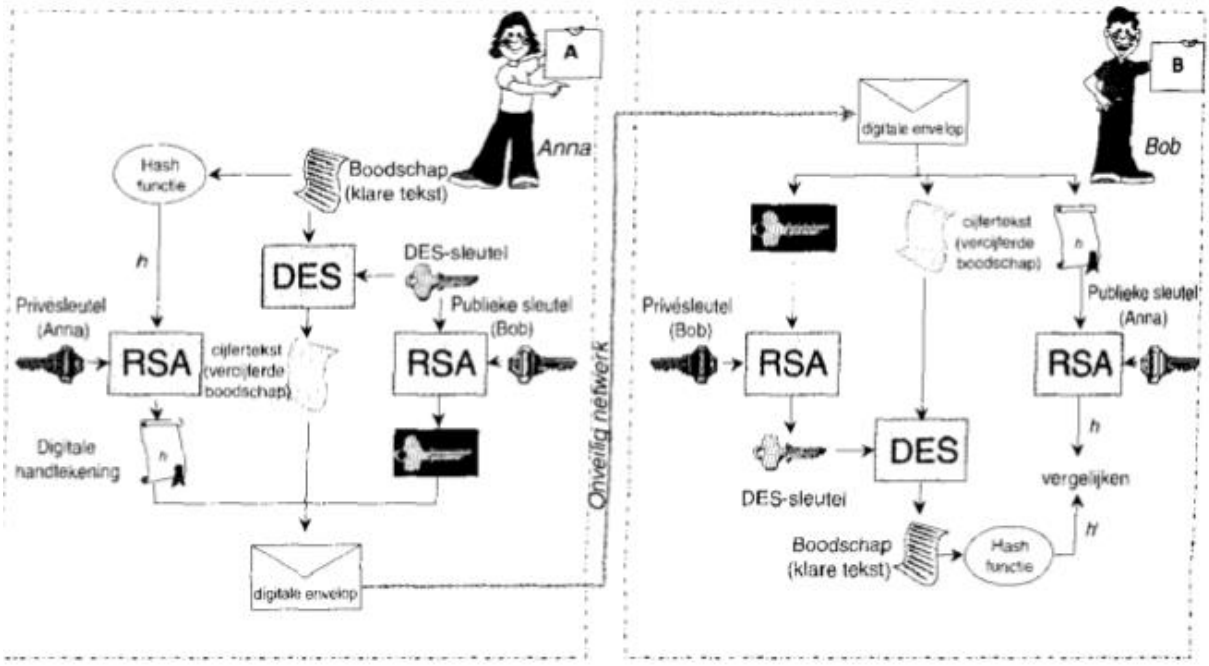
Leg uit: Hybrid cryptografie

Hybride cryptografie is een combinatie van asymmetrische en symmetrische cryptografie. De verbinding wordt eerst asymmetrisch tot stand gebracht met behulp van een combinatie van een publieke en een geheime sleutel. Vervolgens vindt de gegevensoverdracht symmetrisch plaats. Op deze manier wordt zowel van de snelheid van de symmetrische methode als van de veiligheid van de asymmetrische methode geprofiteerd.

Leg uit: Salting

Username	**Hash**	**Salt**
Hannah	Hashen van combinatie van wachtwoord en salt	Random gegenereerd

Leg tekening uit:



1. File wordt geëncrypteerd met DES (symmetrische sleutel)
2. De sleutel wordt geëncrypteerd (RSA) met de publieke sleutel van Bob
3. File wordt gehashed
4. Hash file wordt gesigneerd (RSA) met privé sleutel van Anna

> Bob krijgt een geëncrypteerde file (DES), krijgt een klein bestandje van de AES-sleutel, geëncrypteerd met zijn publieke sleutel en krijgt een hash gesigneerd met de privé sleutel van Anne

1. DES-sleutel eruit halen > terug door RSA sturen met zijn privé sleutel
2. File ontcijferen > file terug door DES sturen met gedecrypteerde sleutel > Hash getal
3. Gesigneerde hash terug door RSA sturen met de publieke sleutel van Anna > Hash getal

Komen overeen? Dan is hij absoluut zeker dat het van A komt

LES 3: PKI-Certificats, -Components, -Architecture, -Process

Leg alle componenten uit van PKI

CA

= Certification Authority

Een CA (= trusted third party) is een entiteit die digitale certificaten verleent aan andere partijen. De bedoeling is dat het digitale certificaat bewijst dat de eigenaar daadwerkelijk degene is die hij beweert te zijn.

De taak van de CA is controle van de identiteit van de aanvrager, zodat gebruikers (partijen die CA vertrouwen) de informatie in de certificaten van de CA kunnen vertrouwen. De gedachte hierbij is: als de gebruiker de CA vertrouwt en de handtekening van de CA kan verifiëren, dan kan de gebruiker erop vertrouwen dat een bepaalde publieke sleutel daadwerkelijk toebehoort aan diegene die wordt vermeld in het certificaat.

Als de CA ondermijnd kan worden, dan is het systeem niet langer veilig. Stel bijvoorbeeld dat een aanvaller, M, een CA een vals certificaat laat uitgeven, waarin A aan een foutieve publieke sleutel gekoppeld wordt. Wanneer B vervolgens de publieke sleutel in het certificaat ontvangt en gebruikt, komt door M de veiligheid van zijn communicatie in het gedrang. B's boodschappen kunnen bijvoorbeeld ontcijferd worden, of hij kan valse handtekeningen accepteren. (= Man-in-the-middle-aanval)

RA

= Registration Authority

Een RA is een autoriteit dat gebruikersaanvragen verifieert voor een certificaat. En geeft dit door aan de CA om te overwegen.

VA

= Validation Authority

Een VA verifieert de geldigheid van een certificaat en of het al dan niet is ingetrokken of opgeschort.

Repository

Een plaats waar certificaten worden opgeslagen.

Identiteiten

Personen vragen certificaten aan en maken een public en private key aan.

CP

= Certificate Policies/ Certificate Practice Statement

Organisatorische en juridische richtlijnen. Gestandaardiseerd document: hoe willen ze uitgifte aanpakken, certificaat formaat-CRL formaat, contractuele bepalingen, …

CPS

De door de CA gevolgde procedures om aan die regels en normen te voldoen.Hoe ze de CP concreet invullen. Door CP en CPS kan gebruiker bepalen hoeveel vertrouwen hij heeft in het certificaat.

CRL

Een CRL is een volledige lijst met ingetrokken certificaten van een bepaalde CA. Omdat deze periodiek wordt uitgegeven en vervolgens gedownload moet worden, kan de informatie gedateerd zijn.

OCSP

= Online Certificate Status Protocol

Er wordt een aanvraag verzonden naar OCSP om een certificaat te controleren en de OCSP-server geeft de huidige status van het certificaat terug (= Online real-time controle van certificaat) in een elektronisch ondertekend bericht: Good=niet op CRL, Revoked=op CRL, Unknown=OCSP kent CA niet.

Leg uit: Key escrow principe

Het principe dat de USA oplegt aan crypto ontwikkelaars om de private key in beheer te geven van een TTP (Trusted Third Party). Op die manier kan de USA via een gerechtelijk bevel aan de private key van iemand komen om zijn secure communication te decrypten.

LES 4: Web security, Email, SSL VPN, SET

Leg uit: 2 modes van VPN

- Transport mode
  Het originele pallet wordt niet geïncapsuleerd in een ander IP-pakket, maar behoudt zijn eigen header.

  Transport mode wordt gebruikt voor end-to-end communicatie, bijvoorbeeld: communicatie tussen een client en een server.

- Tunnel mode:
  Het hele IP pakket is beschermd door IPSec: IPSec pakt het originele pakket in, encrypteert het, voegt er een nieuwe IP header aan toe en verzend het pakket naar de andere kan ven de VPN tunnel.

  Tunnel mode wordt gebruikt om het verkeer tussen secure IPSec gateways te encrypteren, bijvoorbeeld 2 routers geconnecteerd over het internet via IPSec VPN.

Leg uit hoe je secure e-mailt

1. Hybride cryptografie toepassen op email (kunnen tekenen, zie tekening)
2. 2 opties: S/MIME of PGP
   a. S/MIME = Secure Multipurpose Internet Mail Extension
      S/MIME is een standaard voor het beveiligd verzenden van e-mail dat in een MIME-structuur is gevat. Maakt gebruik van PKI X.509v3 certificaten (uitgereikt door CA)
   b. PGP = Pretty Good Privacy
      Gebruikt zelf gemaakte certificaten die vertoruwd worden door een WoT (=Web of Trust) (= niet afhankelijk van een CA).

      WoT: Als x-aantal van uw vrienden een certificaat vertrouwen, dan vertrouw jij dit ook.

Leg uit: SSL

= Secure Socket Layer

Bestaat uit 2 lagen van protocollen:

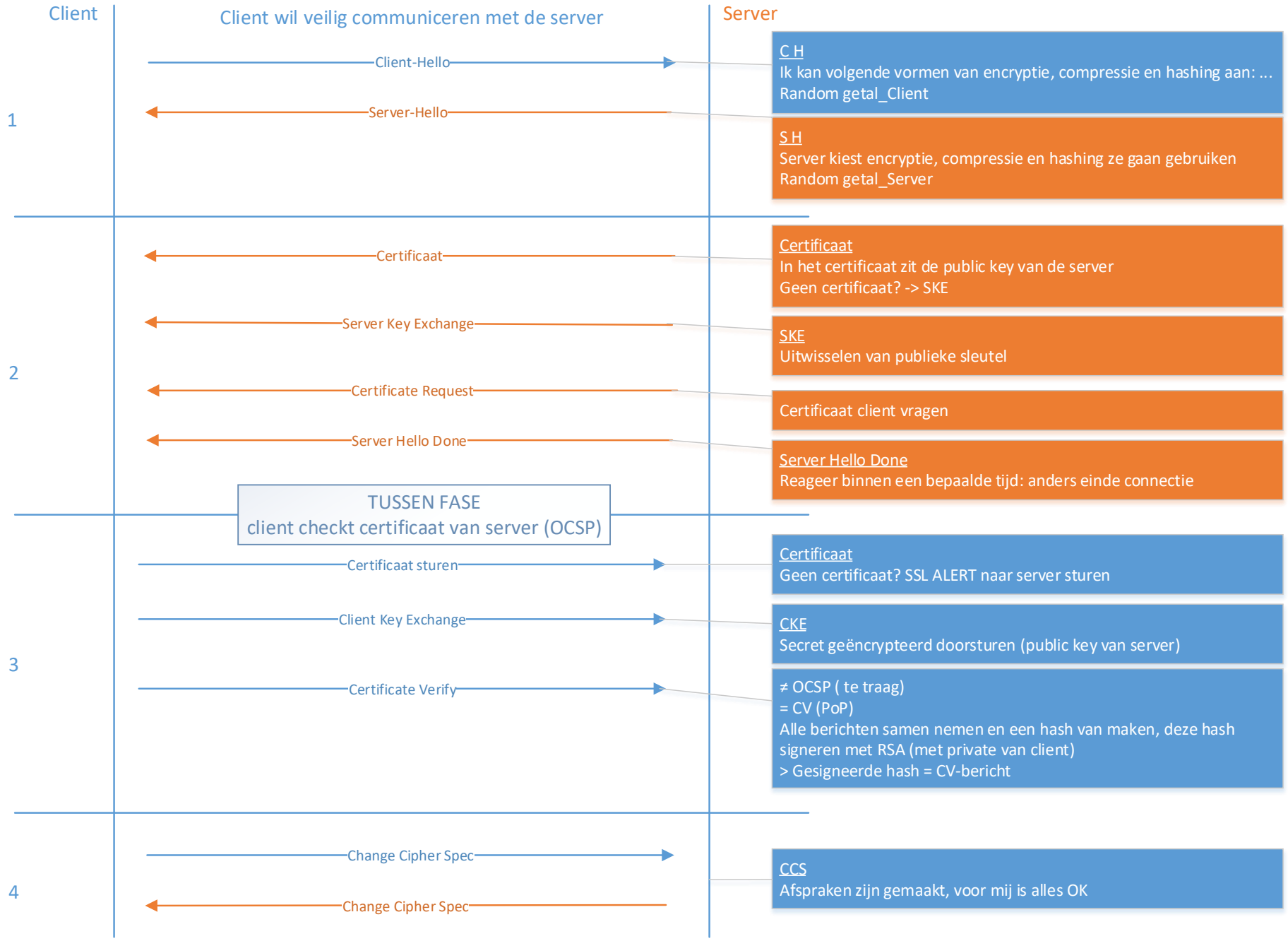
SSL Alert Protocol	SSL Handshake Protocol	SSL Change Cipher Spec
SSL Record protocol		

1. SSL Record Protocol = encryptie van data
   Data komt van laag 7 (browser) en wordt naar laag 4 gestuurd: data in stukjes kappen:
   a. Compressie van data
   b. Controle getal toevoegen: HMAC
   c. Geheel wordt geëncrypteerd
   d. SSL Header aan toevoegen
2. SSL Alert Protocol
3. SSL Change Cipher Spec
4. SSL Handshake Protocol

--- Zie volgende pagina ---

Leg uit: TLS

TLS is gebaseerd op Secure Socket Layer (SSL). Een voordeel van TLS is dat het onafhankelijk is van het applicatieprotocol. Het protocol loopt boven transport protocollen (TCP/IP) en onder applicatieprotocollen zoals HTTP of IMAP. Wanneer er gecommuniceerd wordt tussen server en gebruiker, zorgt TLS ervoor dat de data niet kan worden afgeluisterd of vervalst.


Client
Client wil veilig communiceren met de server
Server
Client-Hello
C H
Ik kan volgende vormen van encryptie, compressie en hashing aan: ...
Random getal_Client
1
Server-Hello
S H
Server kiest encryptie, compressie en hashing ze gaan gebruiken
Random getal_Server
Certificaat
Certificaat
In het certificaat zit de public key van de server
Geen certificaat? -> SKE
Server Key Exchange
SKE
Uitwisselen van publieke sleutel
2
Certificate Request
Certificaat client vragen
Server Hello Done
Server Hello Done
Reageer binnen een bepaalde tijd: anders einde connectie
TUSSEN FASE
client checkt certificaat van server (OCSP)
Certificaat sturen
Certificaat
Geen certificaat? SSL ALERT naar server sturen
Client Key Exchange
CKE
Secret geëncrypteerd doorsturen (public key van server)
3
Certificate Verify
≠ OCSP (te traag)
= CV (PoP)
Alle berichten samen nemen en een hash van maken, deze hash signeren met RSA (met private van client)
> Gesigneerde hash = CV-bericht
Change Cipher Spec
CCS
Afspraken zijn gemaakt, voor mij is alles OK
4
Change Cipher Spec

LES 5: Firewall, Virus, Worm, Trojan RootKit, Sniffer

Leg uit: Laag 5 Firewall | Stateful Packet

- L5 OSI-model
- Meestal minimumvereiste voor een firewall voor een netwerk
- Doet pakketfiltering + houdt sessies en verbindingen bij in tabellen
  - Kijkt dus niet alleen naar de pakketjes op zich, als stand-alone, maar kijkt ook naar de context
  - Speciaal ontworpen tegen DoS attacks

Leg uit: Laag 7 Firewall | ProxyFile

- L7 OSI-model
- Inspecteert het verkeer niet alleen op netwerk- en sessieniveau maar ook nog eens op toepassingsniveau
  - Deep packet inspection
    - HTTP-pakket arriveert > doorgegeven aan http-proxyprocedure
    - FTP-pakket > doorgegeven aan FTP-proxyprocedure
- Proxyfirewall is in principe dus veiliger, want begrijpt ook de toepassingsprotocollen (HTTP, FTP, SMTP, POP, …)
- Problemen:
  - Meestal trager (belangrijk bij zware belasting netwerk)
  - Nieuw protocol wordt uitgevonden > geen procedure voor

Wat is het grootste verschil tussen een worm en een virus

- Worm doet ook aan replicatie, maar manier van hechting is anders dan een virus
  - Virus hecht zich aan legitiem programma
  - Worm verspreidt zich via het netwerken/systemen zonder zich ergens aan te hechten
    - Besmet dus zijn omgeving (OS, of e-mailsysteem) i.p.v. specifieke objecten zoals bestanden
    - Meestal ook geen user interaction nodig
      - Misbruik van lekken in software
      - Snellere verspreiding dan virus > geen user interaction

Leg uit: RAT

Een Remote Access/Administration Tool (RAT) geeft een ICT'er de mogelijkheid om op alle geregistreerde computers in te loggen vanaf één basiscomputer en deze op afstand te beheren. Bij verkeerd gebruik kan een RAT nadelige gevolgen hebben. Een RAT heeft immers een open poort in de firewall nodig, zodat de beheerder erin kan.

Legitiem gebruik: TeamViewer

Illegaal: Back Orifice van Cult of the Dead Cow. Trojan om toegang te krijgen zonder medeweten van het slachtoffer, hacker is in controle van het systeem

Leg uit: Rootkit

Een rootkit is een set softwaretools die wordt gebruikt door een hacker na toegang te hebben verkregen tot een (computer)systeem. De rootkit nestelt zich diep in het besturingssysteem, zodat het besturingssysteem instabiel wordt. De rootkit is bijna niet te verwijderen zonder de functie van het besturingssysteem te beschadigen.

Rootkits kunnen op twee niveaus werken: kernelniveau (Kernel mode) en gebruikersniveau (User mode). Programma's in kernelmodus hebben toegang tot het gehele geheugengebied; toepassingen in gebruikersmodus krijgen specifieke geheugensegmenten toegewezen.

Rootkits hebben de bedoeling om lopende processen, systeemdata of bestanden te lezen, wijzigen of beïnvloeden. Een rootkit helpt de indringer toegang te houden tot het systeem, zonder dat de gebruiker hier iets van merkt.

https://www.youtube.com/watch?v=H23qyUbKuHM

Wat is de meeste gebruikte sniffer?

WIRESHARK
> Al het verkeer dat over het netwerk loopt opslaan en nadien analyses uitvoeren op deze data.

Leg uit: Sniffer

- Basisvereisten voor sniffer:
  - NIC haalt enkel data op bedoeld voor eigen MAC-adres
  - Sniffer zet NIC in overspel modus > alle data opvangen

- 2 grote functies:
  - Black side: Sniffer
    - Bekijkt plain text data: http, FTP, TELNET (> gebruik dus altijd https)
    - Waar? Installeer sniffers dicht bij servers of bij gateways
    - Wat? Sniffers filteren op TCP verkeer, eerste 200 – 300 bytes (meest nuttige informatie ex. login wordt via TCP verstuurd)
  - White side: Protocol Analyzer
    - Defence is moeilijk want een sniffer is passief (= luistert gewoon)
    - Beveiligen op 2 manieren:
      - Detect & Destroy
        > Programma's zoeken naar NIC die in overspel modus staan
        > Hash checken van statische code
      - Protected Data
        > Gebruik nooit plain text > beveilig data d.m.v. encryptie
        > Segmentatie (= toevoegen van extra switches en routers in het netwerk)

LES 6: Spoofing, DDos

Leg uit: TCP Spoofing

1. Stap 1: Authenticatie
   > Authenticatie va target overnemen: Rhosts (= authenticatie op basis van IP-adres)

2. Stap 2
   NON-Blind Spoofing

   = Hacker stuurt TCP-berichtje naar server, hacker forceert dat berichtje van server terug langs hem passeert.

   a) IP Source Routing
      Route bepalen > In header staat een optie waarin je kan definiëren hoe IP-berichtje terug gestuurd moet worden > getallen onderscheppen en berichtje langs u laten komen
   b) ARP Poisoning
      ARP is een tabel in uw NIC waar een mapping in staat met een link tussen MAC en IP.

      Berichtje sturen naar Server: *Als je een berichtje wilt sturen naar deze … IP, dan is dat naar deze MAC (=ARP Respons)* = Man in the Middel Attack

   Bling Spoofing

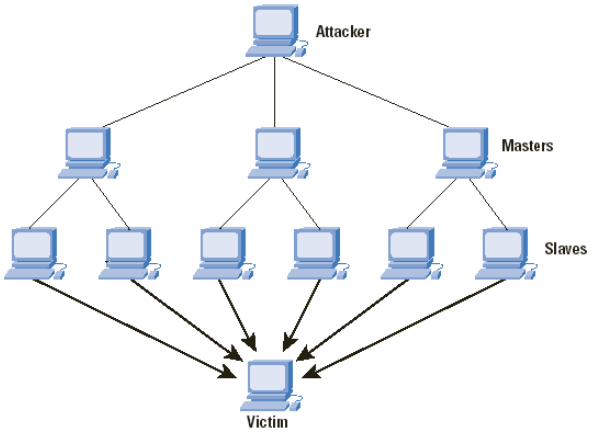
   = Meest voorkomend in de praktijk

   a) Proefdraaien: patroon van psuedo random generators achterhalen
   b) Connectie aanleggen > gokken met welke getallen de server ging antwoorden
   c) Backdoor installeren > onszelf in Rhost file zetten > altijd toegang vanaf nu

3. Stap 3
   Zorgen dat target niet kan reageren op request > zorgen dat target down is > DDoS attack

Wat is de structuur van een DDoS Attack?

- Netwerkverkeer is afkomstig te zijn van heleboel verschillende systemen tegelijkertijd
- Functioneert op basis van Master-Slave (zombie) principe
  - Master is controlerende station: aanvaller definieert daarop zijn doel en methode
  - Slaves zijn externe systemen waarop het aanvalsprogramma is geïnstalleerd
  - Master zegt tegen slaves: 'voer aanval uit', 'stop aanval'
    - Moeilijker tegen te houden omdat het van zoveel verschillende systemen komt
    - Server kan het hoofd niet meer boven water houden -> crash



Leg uit: Smurf Attack

Smurf is een DoS (denial-of-service-aanval) tegen een host. De aanval werkt door pings met een vervalst IP-bronadres naar een broadcastadres binnen een netwerk te sturen. De aangevallen host zal overspoeld worden met de antwoorden op deze verzoeken waardoor legitiem netwerkverkeer in het gedrang raakt.

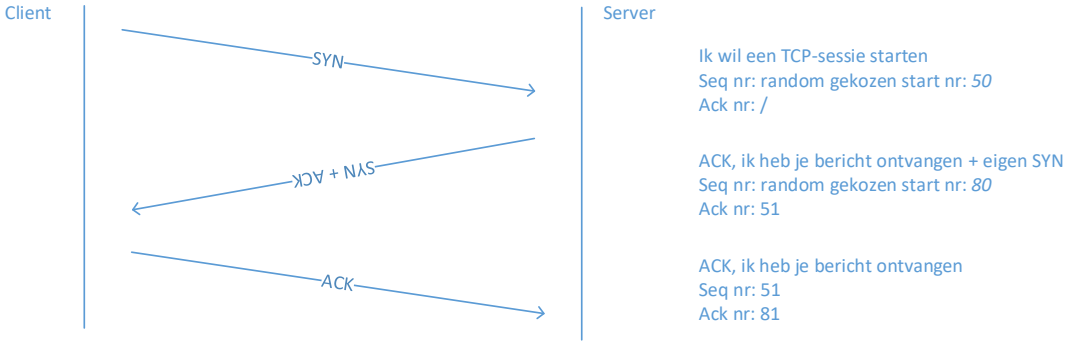
Leg uit: Ping Attack

Een Ping-of-Death (POD) is een DoS-aanval tegen een host op een computernetwerk. Een Ping is normaal 64bytes groot. De maximum grootte van een POD is 65 536bytes. Omdat het illegaal is om zo'n grote ping door te sturen wordt de ping gefragmenteerd. Wanneer de ontvangen fragmenten bij ontvangst opnieuw samengevoegd worden ontstaat een bufferoverloop waardoor de TCP/IP-stack kan crashen.

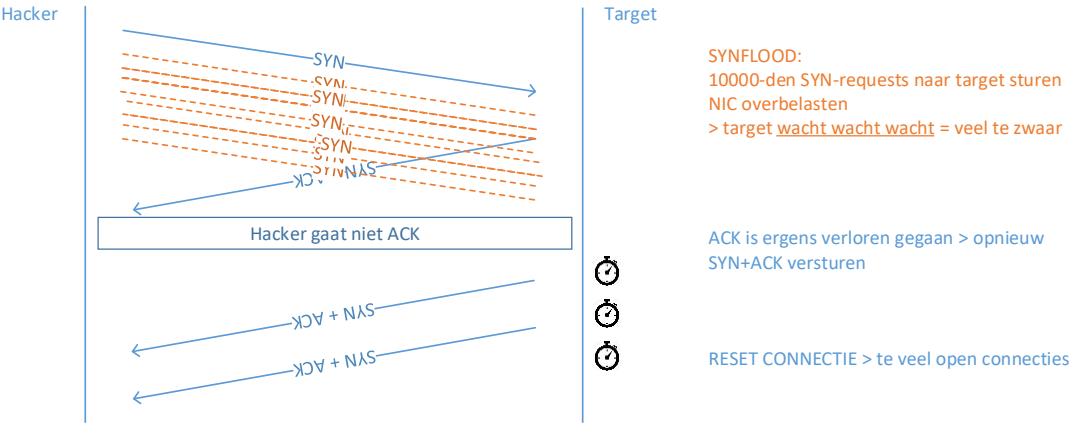
Op welke 3 manieren krijg je een webserver down?

1. SYN-aanval
   = misbruik van 3-way handshake in TCP/IP
2. HTTP–aanval
   Tegelijkertijd HTTP-verbindingen tot stand brengen met webserver, kan het aantal aanvragen niet aan, wordt trager, en valt uiteindelijk uit
3. PHP-scripts
   Script gaat er voor zorgen dat server gegevens gaat opslaan > HD van server is vol

Leg uit: 3 way handshake

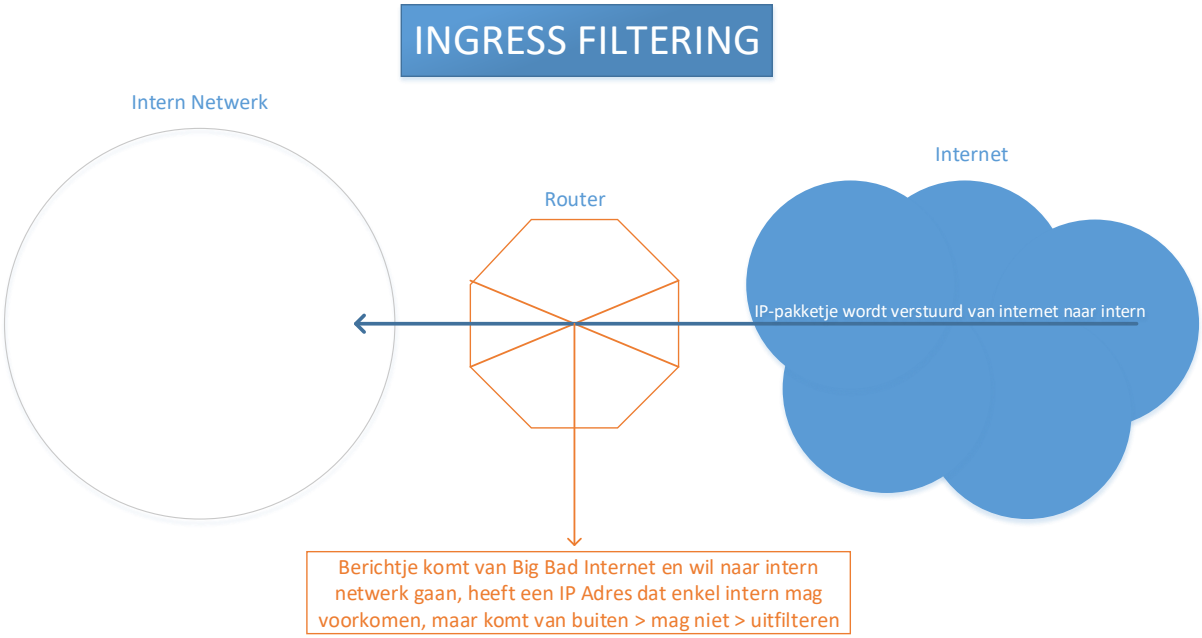


Leg uit: Synflood



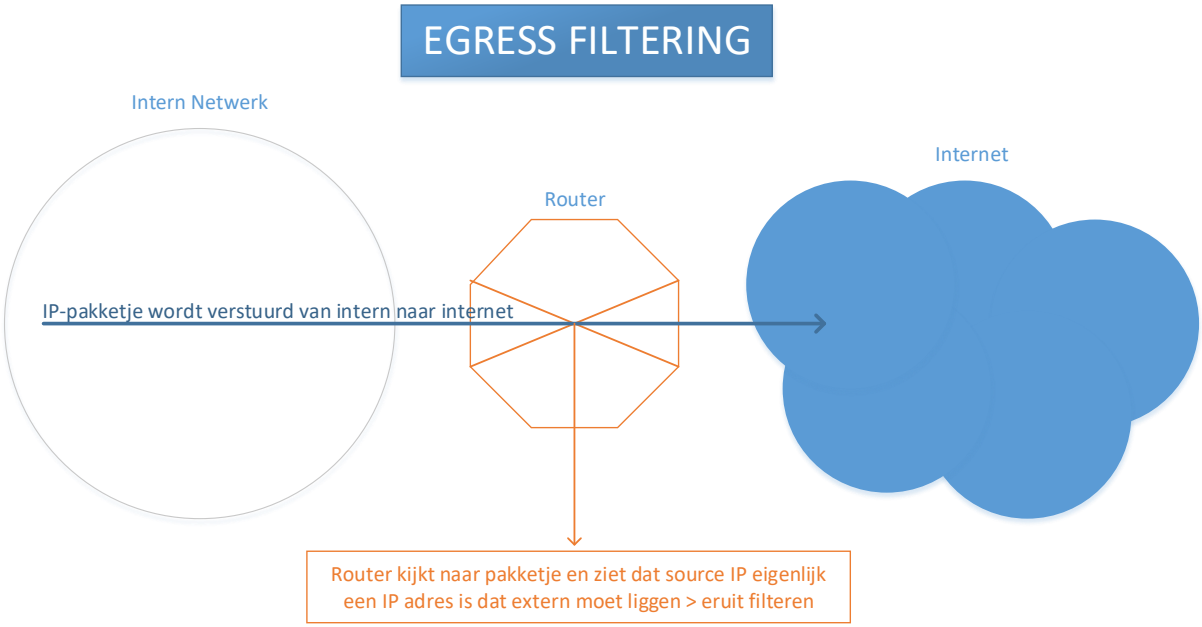
Leg uit: Ingress filtering

= beveiliging tegen spoofing (naast monitoring & logging en sterke authenticatie)



Leg uit: Egress filtering

= beveiliging tegen spoofing (naast monitoring & logging en sterke authenticatie)



LES 7: Poortscanners, Vulnerability Scanners, IDS

Leg uit: Portscanning

Een portscanner is een computerprogramma dat op verschillende manieren probeert te achterhalen welke TCP- en UDP-poorten op een computer bereikbaar zijn.

Wat is de meest gebruikte portscanner?

Nmap

Wat is de meest gebruikte vulnerability scanner?

ISS (=Internet Security Scanner)

SATAN (= Security Administrator Tool for Analyzing Networks)

Leg uit: IDS en IPS

IDS (= Intrusion Detection System)

Is een technologie die vijandige indringers automatisch ontdekt en de beheerders waarschuwt. Het is een soort inbraakalarm.

2 grote groepen IDS:

- Misbruikdetectiemodellen
  - Netwerk-IDS
    SNORT: Sniffers die pakketten parsen en vergelijken met aanvalspatronen
  - Host-IDS
    Tripwire: analyseren van logs en aanmeldingsprocedures. Zoeken naar Trojans en backdoors
- Anomaliedetectiemodellen
  Identificeert items of gebeurtenissen die niet voldoen aan een verwacht patroon.
  = FUZZY LOGIC: maakt gebruik van statische berekeningen, normale verdeling, etc.

IPS (= Intrusion Prevention System)

= IPS inspecteert een binnenkomend packet met duizenden regels waaraan het moet voldoen om het packet te weigeren. (Te vergelijken met een firewall)

Leg uit: SNORT

Snort is een gratis en opensource-beveiligingssoftwarepakket. Het kan worden gebruikt als Intrusion Detection System (IDS) of Intrusion Prevention System (IPS), waardoor pogingen tot inbraak op computers gedetecteerd en verijdeld kunnen worden. Verder kan Snort ook als sniffer ingezet worden, een programma dat het netwerkverkeer afluistert.

Wat is een SIEM server?

= Security Information and Event Management

2 delen

- SIM: Security Information Management
  Log Management specifiek voor security doeleinden (= historische analyse doen)
- SEM: Security Event Management
  Real time monitoring van events (= logs worden gebruikt om attacks in real time te detecteren)

Leg uit: CVE

Common Vulnerabilities and Exposures is een databank met informatie over kwetsbaarheden in computersystemen en netwerken.

CVE en soortgelijke databanken, zoals de Open Source Vulnerability Database (OSVDB) zorgen ervoor, dat als er kwetsbaarheden in systemen gevonden worden, hier openheid van informatie over is. Hierdoor kunnen deze kwetsbaarheden geadresseerd worden voordat ze misbruikt kunnen worden door kwaadwillenden zoals computerkrakers en scriptkiddies.

Leg uit: Actionable rapport

Meedelen wat ze gevonden hebben, zodat er een actie kan ondernomen worden

Classificatie van problemen, dus kan er een false positive of een false negative tussen zitten (confusion matrix)

Leg uit: Confusion Matrix

- Hoe goed is de classificatie (confusion matrix)?
- Het is niet Positive (vulnerable) of Negative (non-vulnerable):
  - Hoe dikwijls zeg je P, en was het ook echt P (true positive)
    - Goed! Vulnerability in het rapport is ook echt een vulnerability
  - Hoe dikwijls zeg je P, en was het eigenlijk N (false positive)
    - Slecht! Vulnerability in het rapport blijkt na veel opzoekingswerk eigenlijk geen vulnerability te zijn
  - Hoe dikwijls zeg je N, en was het ook echt N (true negative)
    - Goed! De Non-vulnerable services in het rapport zijn ook in het echt non-vulnerable
  - Hoe dikwijls zeg je N, en was het eigenlijk P (false negative)
    - Super slecht! Het rapport zegt: service is non-vulnerable, dus ik denk dat ik safe zit, maar het blijkt echter wel een vulnerable service te zijn!

Scanner1		Scanner2		Scanner3		Scanner4			
20	0	10	5	10	10	10	0	TP	FN
0	80	5	80	0	80	10	80	FP	TN

- Scanner1: Dit is de ideale scanner. Haalt alle vulnerabilities eruit, zonder false positives – false negatives
  - In de praktijk is er geen enkele scanner ideaal, daarom bekijken we vooral scanner2-3-4
- Scanner2 – 3 – 4 : allen doen evengoed op vlak van TP en TN, en het zijn degelijke scanners, want ze halen er 10 TP uit, maar:
  - Scanner2:
    - 5 FN: 5 vulnerabilities heeft hij niet gedetecteerd (erg naar security, maar ik moet niet extra onderzoeken of acties ondernemen), en 5 services heeft hij als vulnerable gezet (5 FP), en moet ik onderzoeken, maar die blijken toch safe te zijn (redelijk wat tijd verloren)
  - Scanner3:
    - 10 FN: 10 vulnerabilities heeft hij niet gedetecteerd (erg slecht), maar langs de andere kant moet ik ook niet veel extra opzoekingswerk doen. Het is nog steeds een ‘degelijke’ scanner want hij had 10 TP gevonden, die ik ga fixen
  - Scanner4:
    - 10 FP, en 0 FN: die 10 FP moet ik onderzoeken, maar blijken toch safe te zijn. Heel veel tijd verloren, maar het is een zeer secure scanner.

LES 8: Logging, Monitoring, Privacy, Mythes

Leg uit: Black hats

- Zeer veel ervaring met comp
- Zelden gepakt, doen grondig onderzoek, zeer gerichte aanval
- Je hoort weinig over hun vaardigheden of capaciteiten (ninja's van het internet)

Leg uit: White hats

- Beveiligingsprofessionals die gaten opsporen en dichten
  - 'Pentesting'
- Bedrijven huren hen in om beveiliging te testen
- Meestal zijn ze begonnen als black hat

Leg uit: Script-kiddie

- Grootste groep, meestal onervaren, jong
- Surfen op het web naar utilities, scripts, ...die ervaren aanvallers daar gepost hebben
- Meestal mislukt hun aanval
- Zullen eerder gegevens op kwaadaardige manier beschadigen, dan welk ander type cracker ook
  - Weinig sympathie voor hen, zelfs binnen de crackers community

Leg uit: Cookie

Een cookie is een hoeveelheid data die een server naar de browser stuurt met de bedoeling dat deze opgeslagen wordt en bij een volgend bezoek weer naar de server teruggestuurd wordt. Zo kan de server de browser opnieuw herkennen en bijhouden wat de gebruiker, c.q. de webbrowser, in het verleden heeft gedaan. Een dergelijk historie is bijvoorbeeld voor marketingdoeleinden interessant.

Authenticatie cookie: login gegevens bijhouden, zodat je niet iedere keer opnieuw moet authentiseren

Leg uit: Same Origin Principle

Een script van site X kan enkel die cookies gebruiken die afkomstig zijn van dat domein X.

> Een script dat draait op facebook.com kan niet aan je cookie van google.com

Leg uit: Cross Site Scripting

= Same Origin Principle omzeilen

- Client injecteert onwetend code op een website, bv via een search bar.
  - Bv via een Email met een img in waar een URL aan gelinkt is.
  - In de URL zit een javascript file gelinkt en deze wordt geïnjecteerd
- Website valideert de code niet goed
- Client krijgt bv een error pagina terug, maar hier zit de geïnjecteerde code in
- Code kan nu uw Cookie inlezen

Leg uit: Reflected Scripting

- Soort van witwassen van het script, door het te laten te reflecten door een trusted site aan het target.
- Principe is om Code Injection door de client te laten doen, zonder zijn medeweten:
  - Client misleiden om script code naar een site te sturen (via social engineering truc), naar bv een searchbar
  - Site valideert de code niet goed, en returned zijn antwoord, met die scriptcode in, terug aan de client.
- Op die manier is de script code 'witgewassen'. Komt van trusted site, dus script mag aan de cookies van die site.

Oplossing quizvragen

1. Het Vigenère systeem is een voorbeeld van wat voor type systeem?

   - Steganografie
   - **Substitutie**
   - Transpositie
   - Permutatie

2. Vul aan

   De LSB (Least Significant Bit) gebruiken om daar uw data in te verstoppen, zodat het echt niet opvalt dat er extra data in de file zit, noemt men niet cryptografie, maar **steganografie**.

3. Vul aan

   De 2 basisoperaties van ieder cryptografisch systeem om data onleesbaar te maken, zijn **substitutie** en **transpositie**.

4. Vul aan

   Het DES algoritme gebruikt steeds data blokken van **64** bits.

5. Welke statement kom het best overeen bij een symmetrisch crypto algoritme

   - Het gebruikt slimme wiskundige truckjes, en daarom is het snel
   - **Het gebruikt veel iteraties, die supersnel door de CPU kunnen uitgevoerd worden, en daarom is het snel**
   - Het heeft een goed sleutelmanagement
   - Het is veiliger dan asymmetrische encryptie

6. Om DES te brute forcen, moet een hacker maximaal 2 tot de macht 64 mogelijkheden doorlopen om de key te achterhalen

   - Waar
   - **Niet waar**

7. Vul aan

   Een key pair bij asymmetrische encryptie bestaat uit een **public** key, die iedereen mag kennen. En een **private** key die strikt persoonlijk is, en nooit mag doorgegeven worden aan anderen.

8. RSA is het meest bekende asymmetrische algoritme. RSA steunt op het principe discrete logaritmen met grote priemgetallen om de linking tussen de private en de public key te beveiligen.

   - **Waar**
   - Niet waar

9. Op basis van welke wiskunde principes kan asymmetrisch encryptie werken?

- Feistel functie
- **Elliptische curven**
- **Factorisatie**
- **Discrete logaritmen**
- **Knapzak systeem**
- Avalanche principe

10. Vul aan

Indien 2 verschillende paswoorden toch dezelfde hash uitkomen, noemt men dit een **collision**.

11. Een hash van een file, dient als fingerprint van een file. In principe kan dit dus gebruikt worden om te controleren of het wel de oorspronkelijke file was, want indien er maar iets veranderd was aan de file klopt de fingerprint niet meer. Dit noemt men het controleren van de ...

- Autorisatie
- **Integriteit**
- Authenticiteit

12. Vul aan

Om de database, waarin gehashte paswoorden worden bijgehouden, beter te beveiligen tegen dictionary of rainbow table attacks, gebruikt men het principe van **salting**. Dit wilt zeggen dat er een extra waarde bij het paswoord moet worden gecombineerd, en deze combinatie wordt dan gehashed.

13. De eerste stap in hybrid crypto is om een al dan niet grote file te encrypteren. Daarvoor gebruikt men best een asymmetrisch crypto algoritme (omwille van de snelheid).

- **Niet waar**
- Waar

14. Welke stap in het hybrid crypto proces garandeert dat enkel de ontvanger de boodschap kan lezen?

- **Encryptie met asymmetrische crypto (public key ontvanger)**
- Hashing van de file
- Encryptie met asymmetrische crypto (private key verstuurder)
- Encryptie met symmetrische crypto

15. Kies uit onderstaande opties alle meest optimale en/of secure algorithms om hybrid crypto te kunnen uitvoeren.
    - RSA
    - MD5
    - 3DES
    - DES
    - **AES**
    - **ECC**
    - **SHA256**

16. De reden waarom we een certificaat vertrouwen (en dit is tevens ook de belangrijkste eigenschap van een certificaat) is omdat:

    - Het gesigneerd (geëncrypteerd met private key) is door onszelf
    - Het een officiële standaard is
    - **Het gesigneerd (geëncrypteerd met private key) is door een CA**

17. Een certificaat is de linking tussen welke 2 items?

    - **Identiteit van iemand/entiteit**
    - Asymmetrische crypto
    - **Public key van iemand/entiteit**
    - Betalingsbewijs van iemand/entiteit
    - Private key van iemand/identiteit
    - Symmetrische crypto

18. De officiële standaard van certificaten is:

    - RS 232
    - IEEE 802.16
    - **X. 509 v3**

19. Vul aan

    Ieder PKI bedrijf heeft 2 beleidsdocumenten waarin beschreven staat wat voor soort certificaten ze uitgeven (de level van certificaten, bv military grade), en hoe ze dit ook technische verwezenlijken.

    Het eerste document is higher level, en eerder een management document. Hierin worden de richtlijnen gezet van welke levels van certificaten men nastreeft. Dit document is de **CP** (afkorting).

    Het 2de document is de praktische implementatie van het eerste document. Als bv in het eerste document staat dat ze military grade certificaten nastreven, zal in het 2de document beschreven staan hoe ze die grade nastreven: bv als ID check een DNA scan, als crypto services AES, ECC, SHA256, enz. Dit 2de document noemt met de **CPS** (afkorting).

20. Het belangrijkste deel van de PKI-infrastructuur, het deel dat de certificaten aanmaakt voor de policies, en ook signed, is de...

- Registration Authority
- **Certification Authority (CA)**
- Validation Authority (VA)

21. Het deel van de PKI infrastructuur dat de aanvraag voor een certificaat gaat verwerken, d.w.z. controle doen van de ID, en controle doen op key pair (Proof of Possession), is de:

- Validation Authority
- Certification Authority
- **Registration Authority**

22. Vul aan

Wanneer certificaten vervallen of wanneer ze vermoedelijk gehacked zijn geweest, worden ze op een blacklist geplaatst. Deze blacklist van certificaten noemt men de **CRL** (geef de afkorting).

23. Vul aan

Het protocol om online certificaten te controleren op geldigheid, is het **OCSP** (afkorting) protocol.

24. De RA moet een controle doen dat de user een geldig key pair heeft. Aangezien het PKI bedrijf niet altijd een key pair genereert voor een user, maar dat een user gewoon een public key aan de RA kan geven, moet de user ook bewijzen dat hij de tegenhanger sleutel heeft. Hoe noemt dit principe?

- Authentication Check
- Integrity Check
- **Proof of Possession (PoP)**

25. Vul aan

Het principe dat de USA oplegt aan crypto ontwikkelaars om de private key in beheer te geven van een TTP (Trusted Third Party), noemt men **key escrow** (2 woorden). Op die manier kan de USA via een gerechtelijk bevel aan de private key van iemand komen om zijn secure communication te decrypten.