2 delen : 1e deel 1u30min gesloten boek, 2e deel 1u30min open boek

Vraag 1 : verklaar volgende termen

1. DiGraph crypto
2. Degenerate signed data
3. Dual-homed firewall
4. Metamorfisch virus

Vraag 2 : Enkele waar/niet waar vragen. Leg uit.

1. Is Ephemeral DH veiliger dan traditionale DH
2. Is een metamorphic virus detecteerbaar met emulator

Vraag 3 : SSH

1. Geef de 3 protocollen van SSH en hen functionaliteiten
2. Geef van de volgende of ze al dan niet worden gerealiseerd in SSH en hoe :

Traffic flow confidentiality, authentication, availability, integrity

1. Waarom gebruikt SSH beide RSA en Diffie Hellman
2. geef 3 verschillen die SSH heeft met VPN
3. Als je een ssh connectie wil openen in China maar China blokkeert de ssh poort en filtert al het ssh pakket verkeer. Hoe kan je toch een ssh connectie openen.

Vraag 4 :

Vraag 5 : Malware

1. Geef 5 manieren om malware te verbergen
2. Wat is een bufferoverflow
3. 3 manieren om bufferoverflow te voorkomen

Vraag 6 :

Vraag 7 :

1. Hoe worden transacties bijgehouden
2. Hoe worden nieuwe munten in het systeem gebracht
3. Geef van de volgende of ze al dan niet worden gerealiseerd en hoe :

Authentication, Confidentiality, Availability

1. Naast proof of work bestaat ook nog proof of stake, geef 3 verschillende implementaties  
   en leg ze uit.
2. Als je een gedistribueerde voting toepassing zou willen ontwikkelen met behulp van blockchains, hoe zou je dit aanpakken

Deel 2 :

Vraag 1 : decrpyteren en encrypteren (volgens cbc en modes)

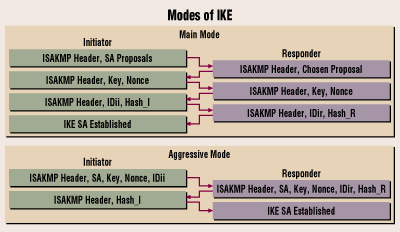
Vraag 2 : geschetste situatie van een webapplicatie die goederen verkoopt waarbij een klant een winkelkarretje heeft en deze kan opvullen. Als de klant een item toevoegt aan zn winkelkarretje wordt dit toegevoegd aan een bestand op de server. Elke klant heeft hierbij een bestand met dus een lijst van zn bestellingen in zn winkelkarretje.

1. Is dit scenario kwetsbaar voor een Denial of Service aanval?

Implementatie van scenario wordt aangepast en de klant houdt een lijst client-side bij en bij klikken op knop “voeg-toe” wordt een verborgen HTML form gestuurd naar de server die de info over het object ophaalt en deze teruggeeft aan de client. Eens de client zn bestelling wil afronden wordt de lijst van zn winkelkarretje doorgestuurd naar de server en deze stuurt het totaal terug met een lijst van producten waarna de client nog een bevestiging van deze bestelling moet geven.

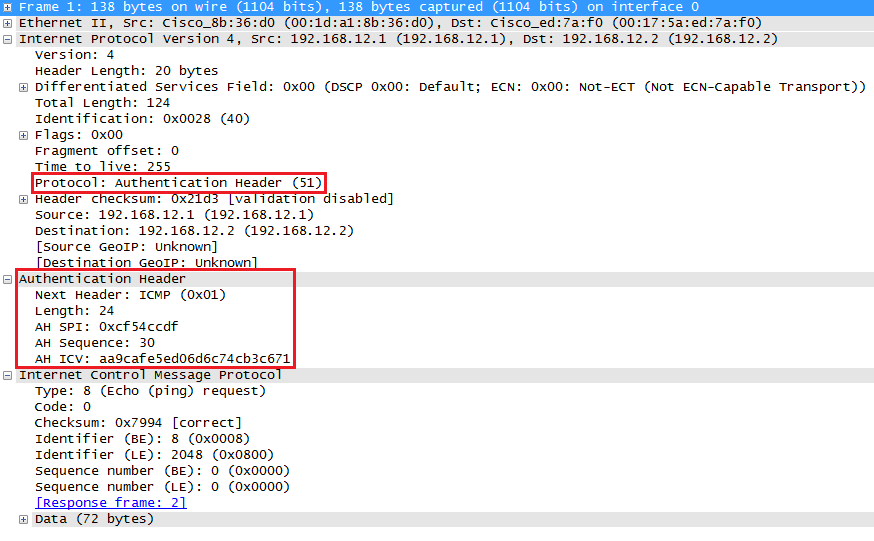
1. Is deze implementatie nog steeds kwetsbaar voor de DOS vanuit de 1e implementatie
2. Zijn er nog andere aanvallen mogelijk? Veronderstel dat er https gebruikt wordt en XSS, CSRF, SQL injection, … dus niet mogelijk zijn.

Vraag 3 : IPsec (gegeven afbeelding berichtverkeer 1e fase : main mode en aggressive mode)



1. Waarom main mode veiliger dan aggressive mode
2. Waarom wordt toch nog soms voorkeur aan aggressive mode gegeven
3. Vanaf welk bericht is het berichtverkeer geëncrypteerd in beide modes
4. Authenticatie gebeurt maar in het 5de en 6de bericht, welke impact heeft dit op de beveiliging?
5. Nadat er een tunnel is gecreeërd na de 1e fase is er nog een 2e fase die dient voor overleg.  
   Voor wat dient deze 2e fase?

(gegeven wireshark bericht van 1e bericht in main mode)



1. Leid af uit afbeelding of het transport of tunnel mode is
2. Waarom geen random waarde bij het eerste bericht
3. Voor wat dient de AH SPI (Security Parameter Index)
4. Voor wat dienen de velden Next header en AH ICV (integrity checksum)