

2016 januari examen

Theorie

Dit examen werd in 2017, 2018 en 2019 getoond als voorbeeldexamen.

Deel 1: meerkeuzevragen

Principe: Per vraag zijn er vier tot 6 stellingen gegeven. Duid telkens aan welke allemaal juist zijn. Het aantal juiste mogelijkheden wordt gegeven. Elke aangeduide mogelijkheid moet juist zijn. Als de juiste antwoorden bv. zijn 'A, F & G' en je duidt 'A, B & G' aan dan is dit volledig fout. De vragen werken ook volgens het principe van eliminatie; er worden ook stellingen over ongeziene stof gegeven en door te elimineren wat je weet van de geziene stof kan je besluiten of de onbekende dingen juist zijn.

1) Welke dingen zijn van toepassing op IPsec transportmode:

- Tussen eindstations
- Unicast
- Enkel payload
- Tussen gateways
- Multicast (Zie tekst over IPsec)
- Hele pakket (Is tunnelmode)

2) Welke twee protocollen zorgen voor confidentialiteit van uitgewisselde data

- SSH
- HTTPS

3) Welk systeem kan aanvallen **inline** tegenhouden. Bv. hacker wilt website defacen via Joomla Exploit.

- IPS (Intrusion Prevention System)
- IDS (Intrusion Detection System)
- Packetfilter
- Stateful Inspection Firewall
- Virusscanner

4) Beweringen over Telnet

- Machines op afstand beheren (e.g. router)

- ~~Telnet is geen protocol~~
- ~~Telnet heeft een beveiligde verbinding~~
- ~~Met Telnet kun je veilig inloggen~~

5) *Iets over access lists*

6) Welke tools om mail te versturen

- Netcat
- Telnet
- POP3 (Lezen)
- ESP (IPsec)
- SSTP (type)

7) *Beweringen over IPsec-verbinding*

- Wanneer client achter NAT-gateway zit dan kan AH niet gebruikt worden.
- IPsec VPN-tunnel die gebruik maakt van AH biedt geen confidentialiteit.
- Gebruiker die via VPN van thuis toegang wil krijgen tot intern bedrijfsnetwerk gebruikt daarvoor best een ESP IPsec verbinding in tunnel mode.

8) ACC's

- Specifiekere ACC's vanboven
- Zelfde trafiek filteren -> meer regels dan Stateful Inspection Firewall

9) *Beweringen over NAT*

- Portforwarding is een soort van NAT (Voorbeeldje met Plex)

10) Iets over diensten die IPsec levert. Mensen struikelden hier over het woordje diensten, want in de lijst stonden implementaties ook.

11) Welke zijn block cyphers? Dit was een kutvraag volgens Swennen. Afleiden door reductie.

12) Alice mailt Bob. Je moet blijkbaar zo'n constructies kunnen begrijpen:

- $K^+ + ^\sim B \sim (K \sim C \sim) + K \sim S \sim ((K^+ - ^\sim A \sim (H(m)) + m))$

13) Applicaties bovenop UDP

- DNS
- SIP

14) *Beweringen over HTTP*

- Body is soms leeg (Bv. Conditional Get)

15) Welke functies noodzakelijk voor IPsec?

- IKE om de SA af te spreken
- Diffie-Helman om shared-secret af te spreken

16) Welk van onderstaande servers ook application gateway

- HTTP-proxy
- SIP-proxy

17) Packet Jitter

- Variatie in delay
- Buffering kan negatieve effecten reduceren
- Jitter buffering zorgt voor algemene vertraging

18) Router die QoS algoritme WFQ samen met ???? kan garantie leveren op

- Delay
- Snelheid
- Packetsize
- Throughput

19) HTTP-conversatie, er stond geen 200 dus dat was sowieso al niet goed

- Server geen idee welke website.

20) Router in welke laag OSI-model? **Hier was Swennen het meest in teleurgesteld!!!**

- Laag 3

21) Beweringen ESP IPsec

- Tunnel mode wordt gebruikt tussen host en security gateway
- Tunnel mode wordt gebruikt tussen 2 security gateways
- Transport mode zal de originele IP header niet versleutelen

22) TCP source ports.

- 20
- 21
- 10000

23) Welke van de volgende zaken worden niet voorzien door TCP (transmission control protocol)?

- Timing

- Security

Deel 2: open vragen

1) In bijlage staat een wiresharkoverzicht van een verbinding.

1a) Hoeveel verbindingen werden er gemaakt? Aan wat zie je dit?

Twee. Dit vind je door SYN, SYNACK, ACK te tellen.

1b) In pakket 8 zien we dat er een HTML-request is. In welk pakket is dit nog zo en waarom zien we dit niet zo als in pakket 8?

Andere is HTTPS.

1c) Hoeveel data (bytes) is er verstuurd in de connectie die op lijn 29 wordt beëindigd.

ACK = 2626 -> seq 2626 = aantal bytes

Ergens was er ook nog een vraag over $(a * b) \bmod n$. Hierbij moest je niet rekenen, is formule die je zo kunt omzetten.

2) Geef een volledig schema over hoe mail van bij Alice die op haar mailclient (Mozilla Thunderbird) zit vanuit een telenetnetwerk tot aan Bob (ucll) geraakt. Volgende zaken moeten minstens voorkomen

DNS records, DNS, TLD, IMAP, SMTP, (nog iets denk ik maar ben het vergeten).

Die lijst met dingen die je moet aanduiden staat er niet voor niets. Die helpt je je antwoord logisch op te bouwen. Zie dat je eerst op kladblad tekent.

Revision #1

Created 17 June 2021 12:06:57 by Jasper G.

Updated 3 December 2021 22:13:08 by Jasper G.