

2012 januari examen

Theorie

1. Analyse van pakketten
 1. Zoek IP-adres van de DNS server
 2. Wat gebeurt er in pakketten x tot y (was de 3-way handshake)
 3. In pakket x wordt een http request gedaan. In welk pakket nog en waarom ziet er dat niet uit zoals in pakket x?
 4. Hoeveel data is verstuurd tijdens de connectie tussen x en y die in pakketten a tot b wordt beëindigd? Kijken naar SYN en ACK bytes
 5. Wat betekent de 301 status code van een http response
2. Je krijgt de uitvoer van netstat te zien
 1. Wat is het IPv4 adres van de server
 2. Is de server een webserver?
 3. Welke poort kan je alleen aanspreken met een IPv4 adres? Kijken naar poorten in tcp en tcp6-output
 4. Is [IPv6-adres local van bovenstaande netstat uitvoer] het IPv6 adres van de server? (Was onwaar omdat de poort erbij stond)
3. Alice wil veilig communiceren met Bob via zijn publieke sleutel. Hoe kan ze zeker zijn dat ze met Bob communiceert en niet met Trudy die de pakketten probeert te onderscheppen. Geef twee manieren hoe de uitwisseling veilig kan gebeuren en leg kort uit.
4. Een IPv6 adres voluit in hexadecimaal uitschrijven
5. Juist of fout + leg uit
 1. Een pakketfilter ontdekt geen virussen
 2. Het Session Initiation Protocol dient om media (audio/video) te versturen
 3. Het IPSEC AH beschermt de gehele IP header
 4. Door de komst van asymmetrische sleutels zijn symmetrische sleutels eigenlijk niet meer nuttig.
6. Geef een voorbeeld van een service die met UDP werkt en leg uit waarom.
7. Verklaar
 1. Ticket (Kerberos)
 2. Onweerlegbaar
 3. ACL (Access Control List)
 4. Peering

Praktijk

- Van elk hoofdstuk zo goed als 1 vraag

- Vragen:

- Toon met alleen netcat, grep en echo de grootte van een foto die op het internet staat. (Oplossing Tom)
- Port-scan met netcat op 1 poort met alleen een handshake. Als de poort open is moet hij "Poort open" tonen, anders niets.
 - if nc -z debbie.vlan77.be 80; then echo "Poort open"; fi
- Toon het e-mailadres van een certificaat
 - openssl x509 -in ABAecom_=sub.__Am._Bankers_Assn.=_Root_CA.crt -email -noout
- Verifieer met gpg enkele files.
 - gpg --import <publickey>
 - find /home/test/gpg/ -type f -name 'tekst*\.txt\.asc' -exec gpg --verify {} \;
- Toon hoeveel woorden beginnen met be en eindigen met en
 - grep -E '^be(.*)en\$' /usr/share/dict/dutch | wc -w

Revision #1

Created 17 June 2021 12:08:56 by Jasper G.

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