Geen giscorrectie.

Alle vragen stonden op 1 punt, tenzij anders vermeld.

Geen deelpunten bij vragen met meerdere antwoorden.

VRAAG 1

Als je bestanden per mail wil versturen, moeten deze bestanden geconverteerd worden naar... (kies 1)

a. ASCII
b. Geen van bovenstaande
c. Binary
d. UTF8

VRAAG 2

Welke van onderstaande beweringen zijn correct over het HTTP protocol? (kies 5)

a. Het HEAD of LINE Blocking probleem in HTTP1.x wordt slechts gedeeltelijk verholpen door het moeilijk te implementeren pipelining. De echte oplossing is het gebruik van HTTP2 dat door multiplexing hier geen last van heeft.
b. HPACK wordt in HTTP1.x gebruikt voor headercompressie.
c. Spriting, inlining, concatenation en sharding zijn technieken om HTTP verbindingen sneller te maken.
d. HTTP headers bevatten veel redundante informatie die telkens terug komt (denk aan cookies, User-Agent,...).
e. Het is niet noodzakelijk om applicaties aan te passen bij de overstap van HTTP1.x naar HTTP2.
f. HTTP2 laat toe om objecten naar de client te pushen, nog voor ze gevraagd worden.
g. In HTTP1.x kan zowel de body als de header gecompresseerd worden.

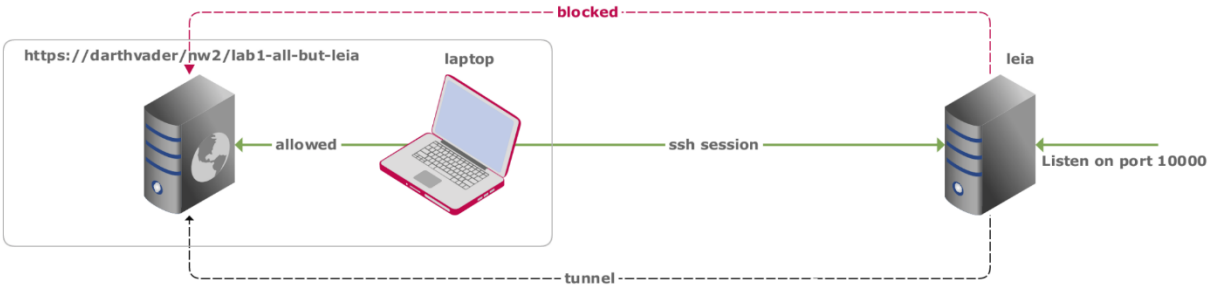
VRAAG 3

Welke van deze protocollen werken met een handshake op applicatieniveau? Ze wisselen dus eerst controle pakketten uit vooraleer er data uitgewisseld wordt. (kies 1)

a. HTTP/2
b. SMTP
c. HTTP/1.1

VRAAG 4

Zoals aangegeven in onderstaande figuur is de website https://darthvader.uclllabs.be/lab1-all-but-leia niet rechtstreeks bereikbaar vanaf leia. Welke variant van ssh port forwarding (tunneling) wordt er hier gebruikt om dit probleem op te omzeilen, zodat Leia toch darth vader kan contacteren? (kies 1)



a. Remote ssh port forwarding.
b. Local ssh port forwarding.
c. Dynamic ssh port forwarding (SOCKS).

VRAAG 5

Welk protocol gebruiken mailservers om te beslissen bij welke next hop (volgende mailserver) ze mail moeten afleveren? (kies 1)

a. DNS
b. SMTP
c. WHOIS
d. IP
e. HTTP

VRAAG 6

Wanneer een VPN een klein aantal eindpunten heeft dan kan de beheerder handmatig de informatie voor de beveiligingsassociatie (encryptie en authenticatie algoritme, sleutels,...) invoeren. Bij een groot aantal eindpunten is deze methode niet werkbaar. Welk protocol wordt er gebruikt om dit proces te automatiseren? (kies 1)

a. IKE
b. PKI
c. TLS
d. ESP

VRAAG 7

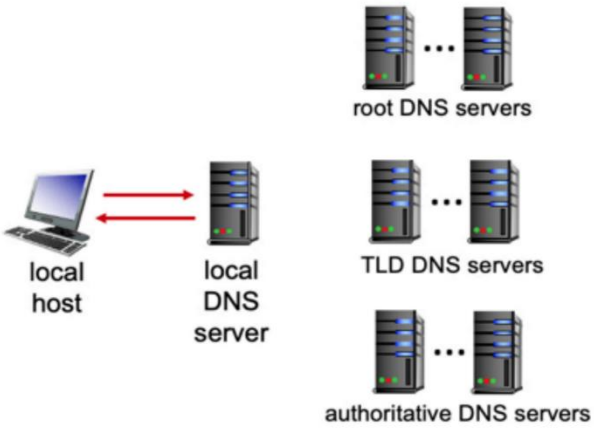
Welke van onderstaande HTTP headers behoren tot groep response headers? (kies 4)

a. Server
b. User-Agent
c. If-Modified-Since
d. ETag
e. Host
f. Last-Modified
g. Set-Cookie

VRAAG 8 (3 punten)

In onderstaande tekening zie je een client die beroep doet op zijn lokale DNS server voor al zijn DNS queries.

- Ga ervan uit dat deze locale DNS server alle binnenkomende informatie van de root, TLD en authoritative DNS servers opslaat in zijn cache gedurende 20 tijdseenheden (minuten, uren, dagen, maakt niet uit). Dus, wanneer de root nameserver de naam en het IP adres van de TLD nameserver voor .be doorstuurt, zal de locale DNS server dit opslagen in zijn cache en zolang deze cache geldig is onthouden dat dit de TLD nameserver is die verantwoordelijk is voor de .be zone.
- Initieel is de cache van de locale DNS server leeg.
- De locale DNS server maakt steeds gebruik van iteratieve queries.
- Eén 'time unit' is nodig voor elke server-to-server of client-to-server request/response. Voor een DNS vraag (request) en bijbehorend DNS antwoord (response) zijn er dus steeds 2 'time units' nodig. Eén voor de vraag en één voor het antwoord.
- Er is slechts één nameserver verantwoordelijk voor de elk TLD domein. Dus één DNS server voor .com, één voor .be, één voor .org, enz...



Bij volgende requests, gestuurd op deze tijdstippen, hoeveel 'time units' nemen deze requests gemaakt door de client in beslag. Gevraagd is de tijd tussen het stellen van de vraag en het ontvangen van het antwoord. Tel dus het totaal aantal pijlen.
Antwoord met een cijfer tussen 0 en 9.

… t=0, resolve jefke.1.cnw2.uclllabs.be

… t=1, resolve icann.org

… t=5, resolve www.kbc.be

… t=10, resolve jefke.1.cnw2.uclllabs.be

… t=11, resolve ucll.be

… t=35, resolve jefke.1.cnw2.uclllabs.be

VRAAG 9

Een malafide hacker heeft een exacte kopie van je website opgezet. Via dns cache poisoning probeert hij gebruikers naar zijn valse website te lokken. Na onderzoek blijkt dat gebruikers geen certificaat waarchuwing krijgen bij het surfen naar de valse website. De verbinding is wel degelijk beveiligd met https. Welke stappen moet je ondernemen om ervoor te zorgen dat toekomstige bezoekers van de valse website wel een certificaatwaarschuwing krijgen? (kies 2)

a. Genereer een nieuwe CSR (Certificate Signing Request) en laat deze ondertekenen door een erkende CA. Je huidige private key laat je op de CRL (Certificate Revocation List) zetten.
b. Genereer een nieuwe CSR (Certificate Signing Request) en laat deze ondertekenen door een erkende CA. Je huidig certificaat en private key vervang je door de nieuwe in de configuratie van je webserver.
c. Het is niet nodig om een nieuwe CSR te maken.
d. Genereer een nieuwe CSR (Certificate Signing Request) en laat deze ondertekenen door een erkende CA. Je huidig certificaat laat je op de CRL (Certificate Revocation List) zetten.

VRAAG 10

Welke beweringen zijn correct m.b.t. de DMZ (gedemilitariseerde zone)? (kies 2)

a. De DMZ wordt minder streng beveiligd dan de meeste andere zones in het bedrijfsnetwerk.
b. Servers die toegankelijk moeten zijn voor zowel interne clients als het gehele internet zet je best in de DMZ.
c. De DMZ is de best beveiligde zone van het gehele bedrijfsnetwerk.
d. Servers die enkel toegankelijk moeten zijn voor de interne clients zet je best in de DMZ.

VRAAG 11

Welke DNS records worden gebruikt voor mail routing? (kies 2)

a. A of AAA
b. SMTP
c. CNAME
d. TXT
e. MX

VRAAG 12

Welke beweringen over het DNS protocol zijn correct? (kies 2)

a. Een DNS request naar 1 van de 13 root DNS servers (A-M, de named authorities) wordt via broadcast gerouteerd naar de dichtstbijzijnde node.
b. DNS maakt soms gebruik van TCP i.p.v UDP, voor grote pakketjes zoals zone transfers.

c. Via UDP source port randomisatie wordt de TXID uitgebreid tot 32bit. DNS cache poisoning via sibling names (1.uclllabs.be, 2.uclllabs.be, 3.uclllabs.be) wordt zo nagenoeg onmogelijk gemaakt.
d. De query ID, ook wel transaction ID (TXID) genoemd waarmee een DNS query gelinkt wordt aan een DNS response zorgt voor een afdoende beveiliging tegen DNS cache poisoning.

VRAAG 13

Uit hoeveel objecten bestaat een webpagina die bestaat uit 5 afbeeldingen en 1 html file? (kies1)

a. 6
b. 5
c. 1
d. Geen van bovenstaande is correct.

VRAAG 14

Welke van onderstaande protocollen zijn stateful? (kies 2)

a. FTP
b. TCP
c. HTTP/1.1
d. DNS
e. UDP

VRAAG 15

De verschillende rfcs (Request For Comments) van het HTTP protocol beschrijven o.a. de structuur en het formaat van de data. De gebruikte term hiervoor is: (kies 1)

a. semantiek
b. protocol
c. syntax

VRAAG 16

Welke beweringen zijn correct over een IDS systeem? (kies 3)

a. Signature based systemen zijn volkomen blind als het gaat over nieuwe aanvallen die nog niet eerder gedetecteerd zijn.
b. Een op anomalieën gebaseerd IDS systeem creëert een profiel van het normale verloop van het gecontroleerde dataverkeer. Vervolgens zoekt het naar packetstreams die statistisch gezien ongebruikelijk zijn.
c. Er zijn ruwweg 2 categorieën van IDS systemen: systemen die werken met handtekeningen (signature based) en systemen die gebaseerd zijn op anomaliedetectie.

d. False positives (valse waarschuwingen) komen nooit voor bij signature based IDS systemen.

VRAAG 17

De meeste van de HTTP-methods kunnen gebruikt worden om een webtoepassing aan te vallen. Hoewel GET en POST bij de meeste aanvallen gebruikt worden, zijn de methoden zelf niet het probleem. Ze zijn noodzakelijk voor de goede werking. Een aantal methoden zoals PUT, DELETE en CONNECT echter zijn typisch niet vereist voor webservers. Waarmee kan je HTTP methods die niet nodig hebt blokkeren? (kies 2)

a. application gateway
b. stateful inspection firewall
c. packet filter
d. proxy server

VRAAG 18

Welke van onderstaande beweringen is correct over SSH tunneling. (kies 2)

a. Bij local portforwarding krijg je een certificaatwaarschuwing bij het surfen naar https websites omdat de common name van het certificaat niet overeenkomt met de hostname.
b. Bij local portforwarding kan je enkel poorten forwarden naar een http of https website. Het is niet mogelijk om een port te forwarden voor andere protocollen.
c. Bij remote portforwarding krijg je een certificaatwaarschuwing bij het surfen naar https websites omdat de common name van het certificaat niet overeenkomt met de hostname.
d. Bij dynamische portforwarding krijg je een certificaatwaarschuwing bij het surfen naar https websites omdat de common name van het certificaat niet overeenkomt met de hostname.

VRAAG 19

DNS is hiërarchisch opgebouwd, met helemaal bovenaan de DNS rootserver(s). Welke beweringen over deze DNS rootserver(s) zijn correct? (kies 2)

a. Door de gedistribueerde opzet is 1 rootserver voldoende.
b. Er zijn 400+ rootservers die beheerd worden door 13 verschillende organisaties.
c. De rootservers zijn elk verantwoordelijk voor een deel van de DNS root zone.
d. Als de DNS rootserver(s) onbeschikbaar zijn/is dan zullen veelgebruikte domeinen nog even blijven werken door caching.
e. Er zijn 13 fysieke rootservers.

VRAAG 20

Wat zit er minstens in een RSA certificaat: (kies 2)

a. Private key

b. Common Name
c. AES SSL key
d. Public key

VRAAG 21

Welke beweringen over packet jitter zijn correct? (kies 3)

a. Jitter is één van de technologieën die gebruikt worden bij VoIP
b. Jitter is de variatie in delay.
c. Buffering kan de negatieve effecten van jitter reduceren
d. Jitter buffering zorgt voor algemene vertraging.
e. Jitter is de variatie in pakketgrootte.
f. Jitter zorgt voor het snel verzenden van data, ook al is de TCP buffer nog niet helemaal gevuld.

VRAAG 22

Welke van onderstaande protocollen maakt gebruik van public key cryptografie? (kies 3)

a. AES
b. RC4
c. https (http1.0)
d. PGP
e. http (H2 - http2)

VRAAG 23

Welk van onderstaande protocollen zijn binair? (kies 2)

a. HTTP/2
b. SPDY
c. FTP
d. HTTP/1.1
e. IMAP
f. SMTP

VRAAG 24

Stel dat een SSL/TLS-sessie gebruik maakt van een blockcipher in de CBC (Cipher Block Chaining) modus, dan verzendt de server de initialisatievector naar de client in onversleutelde vorm. Welke van onderstaande beweringen is correct? (kies 1)

a. Waar, de IV wordt niet versleuteld bij CBC.
b. Een IV wordt niet gebruikt bij blockciphers, wel bij een streamcipher zoals RC4 die de basis vormt van het WEP protocol.
c. Een IV wordt enkel gebruikt ECB modus

VRAAG 25

Welke beweringen over de body van een HTTP response bericht zijn correct? (kies 1)

a. De body is soms leeg.
b. De body is altijd leeg.
c. De body is nooit leeg.
d. HTTP antwoorden hebben geen body.

VRAAG 26

Welke van onderstaande beweringen zijn correct over certificaten? (kies 1)

a. Een certificaat wordt altijd ondertekend door een 3e vertrouwde partij, de CA.
b. Een certificaat is een digitaal document dat het eigenaarschap bewijst van een publieke sleutel.
c. Wanneer de publieke sleutel van het certificaat op straat komt te liggen wordt het certificaat best op de CRL (Certificate Revocation List) gezet.
d. Een certificaat is een digitaal document dat het eigenaarschap bewijst van een privé sleutel.

VRAAG 27

Een ACL (Access Control List, of filterpolicy) entry van een packetfilter kan gebaseerd zijn op het al dan niet ingeschakeld zijn van de TCP ACK bit. (kies 1)

a. Een packetfilter kan enkel filteren op de SYN bit.
b. Een packetfilter zal nooit filteren op basis van TCP flags zoals SYN, ACK, FIN. Enkel stateful packetfilters kunnen dit.
c. Dit is enkel mogelijk bij UDP trafiek.
d. Nee, want een ACL entry kan verkeer pas controleren na de 3-way handshake.
e. Hiermee kan de packetfilter toestaan dat interne clients verbindingen maken met externe servers, en tegelijkertijd verhinderen dat externe clients een verbinding kunnen opzetten met interne servers.

VRAAG 28

Welk van onderstaande beweringen zijn waar voor een IPsec verbinding. (kies 3)

a. Een IPsec VPN tunnel die gebruik maakt van het AH protocol biedt geen confidentialiteit.
b. Een IPsec Security Association is bidirectioneel.
c. Een gebruiker die via VPN van thuis toegang wil krijgen tot het interne bedrijfsnetwerk gebruikt daarvoor best een IPsec verbinding in transport mode.
d. Wanneer de client achter een NAT gateway zit dan kan AH niet gebruikt worden.
e. Een gebruiker die via VPN van thuis toegang wil krijgen tot het interne bedrijfsnetwerk gebruikt daarvoor best een TLS IPsec verbinding in tunnel mode.
f. Een gebruiker die via VPN van thuis toegang wil krijgen tot het interne bedrijfsnetwerk gebruikt daarvoor best een ESP IPsec verbinding in tunnel mode.

g. De 3 protocollen om een IPsec tunnel op te bouwen zijn ESP, TLS en AH.

VRAAG 29

Een bekende bittorrent tracker valt plots uit door een hardware crash. Wat gebeurd er met de lopende bittorrent transfers van zijn gebruikers. (kies 2)

a. De download en upload van chunks die al gestart waren voor de crash loopt gewoon verder.
b. De lopende bittorrent transfers kunnen enkel verder indien de gebruikers een extra (publieke) tracker toevoegen.
c. Indien er voldoende clients zijn met ondersteuning voor DHT is die tracker zelfs niet nodig. Het uitvallen ervan heeft geen invloed.
d. Die stoppen onmiddellijk, en zullen automatisch verder gaan eenmaal de tracker terug beschikbaar is.

VRAAG 30

Namebased en IP based virtual hosts worden gebruikt om meerdere websites te laten draaien op een enkele host. Welke van volgende stellingen is correct? (kies 2)

a. Namebased vhosts kunnen gebruikt worden vanaf HTTP/1.0. Een speciale HTTP header wordt gebruikt om aan te geven welke website de gebruiker wil bekijken.
b. Er is geen ondersteuning binnen het HTTP protocol nodig om name based vhosts te laten werken. Hiervoor bestaat er DNS
c. Namebased vhosts kunnen gebruikt worden vanaf HTTP/1.1. Oudere versie hebben niet de vereiste ondersteuning hiervoor.
d. IP based vhosts kunnen gebruikt worden bij HTTP/2