UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria de Manresa

Final d'Aplicacions i Serveis

20 de juny de 2024 | Enginyeria de Sistemes TIC | 120 MINUTS

COGNOMS:

NOM: SUBGRUP:

Exercici 1 [26 punts]. Responeu cert (C) o fals (F) a les següents frases. Justifiqueu la resposta. Respostes i justificacions contradictòries no compten. Resposta o justificació incorrectes resten 1/2 punt. Les respostes sense justificació sumen o resten la meitat. Si no hi ha resposta (C) o (F) no compten.

a) Quan un servidor de correu fa de smarthost d'altres, cal configurar-lo amb la llista d'adreces IP de les màquines de les que pot rebre missatges de correu. Aquesta llista pot ser tot el rang d'adreces existents.

b) Quan un servidor de correu lliura a un smarthost, aquest servidor s'ha de configurar amb l'adreça IP del smarthost, encara que el smarthost tingui un registre A o AAAA en el servei de DNS.

c) El registre MX del DNS té com a valor l'adreça IP del servidor de correu del domini que es consulta.

d) Si un servidor fa de smarthost comprova el domini del remitent del missatge de correu que li lliuren.

e) Quan el lliurament de correu és a un smarthost el domini del destinari de correu es té en compte per escollir el smarthost.

f) Un missatge de correu pot recórrer molts servidors de correu, però només un d'ells consultarà el registre MX del DNS corresponent a @nom en funció del destinatari del correu.

g) Quan un servidor de correu té definit un àlies d'alguna de les bústies, just en el moment de rebre un missatge comença un nou viatge per a aquest missatge com si s'hagués originat de nou.

h) La llista de dominis locals d'un servidor de correu vol dir que aquest servidor de correu disposa de les bústies d'usuari per a aquests dominis o bé tindrà definits àlies d'aquests usuaris.

i) La codificació MIME serveix per transformar la informació que es vol enviar en un correu en un format de caràcters ASCII de 7 bits i acceptar diferents parts dins d'aquest correu.

j) Existeix algun missatge de petició HTTP que no cal que generi un missatge HTTP de resposta.

k) El servei de DNS està estructurat en forma d'arbre com una base de dades distribuda on cada node està format pels servidors autoritat.

l) Els registres NS ens informen sobre qui es delega un domini.

m) Per a cada servidor Autoritat existeix un servidor Local associat que actua de caché.

n) Els servidors DNS locals accepten normalment consultes iteratives.

o) Quan un servidor DNS accepta una consulta iterativa dóna una resposta final i no parcial.

p) Amb Javascript, sense la creació d'objectes XmlHttpRequest es pot canviar el contingut inicial d'una pàgina web sense que intervingui l'usuari.

q) Les cookies són un mecanisme incorporat a HTTP que permeten implementar el concepte de sessió.

r) El contingut d'un certificat digital es pot transferir per qualsevol tipus de canal ja sigui segur o insegur amb garanties de seguretat.

s) L'atribut action d'un formulari HTML conté la localització del servidor que processarà les dades del formulari en el moment de fer submit.

t) Per poder lliurar diferents continguts segons el nom de domini en un Apache cal utilitzar un *proxy invers*.

u) Tant la directiva *alies* com la *redirect* es poden fer servir per adreçar contingut d'altres servidors.

v) Els sockets de servidor UDP accepten més d'un client en el mateix socket.

w) Els sockets de servidor TCP accepten més d'un client en el mateix socket.

x) Una autoritat de certificació és una entitat de la que es coneix de manera fiable la seva clau pública i per tant confiem en tot el que estigui signat amb la seva clau privada.

y) El mecanisme d'autentificació basat en usuari i contrasenya es pot aplicar sempre amb seguretat.

Exercici 2 [1 punt]. Per quin motiu normalment s'utilitzen conjuntament les directives ProxyPass i ProxyPassReverse.

Exercici 3 [2 punts]. Descriu quina funció té el fitxer /etc/resolv.conf en un sistema Linux. Pot contenir el valor 127.0.0.1? Si és possible, que implica en aquest cas?

Exercici 4 [1 punt]. Quin és l'usuari d'un sistema Linux que executa el servidor apache?

Exercici 5 [1 punt]. Quina és la comanda que serveix per reconfigurar un servei de sistema sense aturar-lo?

Exercici 6 [1 punt]. Quins ports estan reservats pel protocol HTTP, HTTPS, SSH i DNS.

Exercici 7 [10 punts]. Es vol crear una empresa que actuarà com Autoritat Certificadora (CA) per generar certificats digitals per a servidors web. El procediment per obtenir els certificats és el següent:

- L'administrador del servidor web (admin) omple un formulari web de la CA on introdueix el domini del servidor web (name) i la clau pública (K_{pub})
- La CA respon amb 2 nombres arbitraris A i B en format de fitxers de text amb les següents instruccions:
  - El fitxer A s'ha de trobar a la URL: http://name/certificacio/A
  - El fitxer B s'ha de pujar de nou al web de la CA després de ser transformat amb la K_{priv}.
- Un cop fet això, la web de la CA retorna el certificat digital corresponent al servidor web (name).

a) Es pot considerar una signatura del servidor web transformar B amb K_{priv}? Resposta (S) o (N).

b) Es pot considerar una signatura del servidor web transformar B amb una funció de Hash? Resposta (S) o (N).

c) Creus que aquest procediment és valid? Resposta (S) o (N).

d) Justifica el perquè. [2 punts]

e) Seria possible un procediment vàlid on la CA retorna només un valor arbritari A? Resposta (S) o (N).

f) Justifica el perquè. [4 punts]

Exercici 8 [8 punts]. Quan es vol aplicar l'algoritme RSA, tingueu en compte que $p = 3$, $q = 11$ i $e = 7$. El mapa entre lletres i valors és el següent:

A:1, B:2, C:3, D:4, E:5, F:6, G:7, H:8, I:9, J:10, K:11, L:12, M:13, N:14, O:15, P:16, Q:17, R:18, S:19, T:20, U:21, V:22, W:23, X:24, Y:25, Z:26, _:27, Ç:28, Ñ:29, *:30, !:31, ?:32, +:33

a) Quina és la clau pública?

b) Quina és la clau privada?

c) En quina operació recau la fortalesa d'aquest algoritme per aplicar-lo a la seguretat?

d) Troba el valor més petit possible per d.

e) Desxifreu VOMIA. [4 punts]

Exercici 9 [6 punts]. Un estudiant TIC espavilat vol patentar un mecanisme d'autentificació. El mecanisme generarà 6 dígits decimals que tindran una validesa durant 30 segons i serviran per a que B autentifiqui a A. El procediment és el següent:

- Originalment A i B pacten una clau k de manera segura.
- El *Epoch Time* o temps UNIX és el nombre de segons que han passat des de mitjanit de l'1 de gener de 1970. Generalment està codificat als rellotges de les màquines com un enter amb signe de 32 bits. Després de consultar aquest valor a la màquina, es fa una divisió entera per 30 obtenint el valor $t30$.
- La funció de Hash SHA-512, disponible a la majoria de sistemes Linux, genera una sortida de 512 bits. Amb aquesta funció es calcula el Hash del missatge format per la clau k seguida de $t30$. El resultat és el valor v.
- Es considera que v és un enter sense signe de 512 bits. Es calcula el mòdul 10^6 i s'obté el valor vm.
- La representació decimal de vm serà el valor que A envia a B com a contrasenya per poder ser autentificat.

a) Aquest mecanisme es pot considerar adequat per a que B autentifiqui a A? Resposta (S) o (N).

b) Justifica el perquè.

c) Si ho consideres necessari, proposa quines modificacions faries.