Aplicacions i Serveis a Internet

durada 3h

Final - Juny 2017

1. Preguntes cert o fals. Justifiqueu la resposta. Les respostes incorrectes resten. Les respostes sense justificació compten la meitat. (5)

   a) És possible tenir més d'un servidor web en una xarxa privada i que es pugui accedir a ells amb diferents noms de domini només obrint únicament el port 80 de l'encaminador NAT que és l'únic que té l'adreça pública.

   b) Si la clau pública només s'envia a persones de confiança, es millora la seguretat de la privacitat dels missatges xifrats.

   c) Si la clau pública només es rep de persones de confiança, deixen de tenir sentit les autoritats certificadores.

   d) Si una persona genera el parell de claus públic i privat, pot xifrar missatges per ella mateixa i signar missatges per tothom.

   e) Si un client vol autentificar-se amb un servidor generant un parell de claus pública i privada, li ha de proporcionar al servidor la clau pública de manera que cada vegada que es connecti, el servidor pugui comprovar que és ell. En canvi el servidor no cal que generi cap parell de claus.

   f) A i B volen comunicar-se de formar xifrada. A té un certificat digital. B no té. Fins que B no obtingui un certificat o generi un parell de claus (pública - privada), no és possible cap mecanisme de comunicació xifrada entre ells.

   g) Un certificat digital és el resultat de xifrar el valor de la clau pública d'una identitat fent servir la clau privada d'una altra entitat de la que coneixes de manera fiable el valor de la seva clau pública.

   h) Un missatge signat no és fiable si s'ha rebut per un canal que podem assegurar que no és fiable.

   i) El mecanisme més ràpid, mantenint amples de banda, per distribuir el contingut de fitxers entre varis nodes és via peer to peer.

   j) Per a que un navegador web pugui presentar continguts en funció de les dades prèvies enviades, cal mantenir una comunicació http sempre oberta.

   k) Una comunicació http funciona per sobre d'una connexió TCP (generalment en el port 80). Aquesta connexió TCP es crea en cada petició http i es destrueix cada vegada que el navegador ha rebut tot el contingut que desitja mostrar.

   l) El mecanisme de Sockets permet el pas de missatges entre processos de diferents màquines però no entre processos de la pròpia màquina.

   m) Les comunicacions fetes a través d'un proveïdor de Internet oficial (registrat com ISP) sempre són segures.

   n) Quan es compra un domini, el gestor al que li contractes l'únic que fa es demanar al responsable del top level domain una entrada a la seva base de dades amb un registre NS del domini registrat cap a un servidor de DNS autoritatiu gestionat pel propi gestor.

   o) Si algú accedeix a la nostra clau privada, el que s'ha de fer és canviar la contrasenya de la clau immediatament per continuar garantint la seguretat.

   p) Hem de comprovar per quin canal aconseguim el certificat d'un usuari per considerar-lo fiable.

   q) El mecanisme per garantir la restricció d'accés a certes pàgines s'aconsegueix a través de les cookies.

   r) Si accedim a internet a través d'una xarxa insegura, no podem fer res per assegurar les nostres comunicacions.

   s) Es pot simular l'enviament de dades d'un formulari amb un navegador web sense accedir al formulari si el mètode del formulari és GET.

t) Si el mètode d'un formulari és POST, no existeix cap altre manera per enviar les dades que primer accedint al formulari i després polsar el botó enviar. És a dir, no es poden enviar les dades amb una única petició.

u) Un smarthost que accepta ser-ho per qualsevol adreça ip és un servidor potencial de correu spam.

v) El protocol SMTP comprova que els remitents dels missatges siguin els que toca en funció de qui origina el missatge.

2. Actualment gairebé cap operador ofereix adreça IP pública (encara que sigui dinàmica) per a les connexions de dades mòbils (2G, 3G, 4G, etc.). Es vol disposar d'un petit sistema autònom amb bateries que faci de servidor de vídeo amb una webcam. És viable que des d'Internet es pugui accedir a aquest servidor?. Suposeu que el servei de vídeo es troba disponible gràcies a l'aplicació VLC que ofereix un streaming pel port 80. Doneu una solució tècnicament viable, si és possible, per aconseguir-ho. Enumereu els recursos que us calen des del punt de vista de l'assignatura ASI (registrar donimi, servidor a Internet, servidor a casa, tipus de servei instal·lat, etc.) (1)

3. Defineix la diferència entre Alias, Redirect, ProxyPass i ProxyPassReverse. Digues quantes connexions TCP intervenen quan un client accedeix a una URL del tipus http:// on al path intervé cadascuna d'aquestes directives. En cas que hi hagi més d'una connexió TCP, indica si es produeixen en seqüencialment o concurrentment. (1)

4. Quines són les diferències a Apache entre definir-se diferents sites o diferents virtualhosts (1)

5. Proposa una solució al següent problema: Una petita empresa té la seva xarxa amb un adreçament privat. Disposa d'un servidor web amb nom empresa.cat. Els empleats, a vegades estan a dins de la empresa (per tant el servidor web estarà a l'adreça 172.20.0.1) i a vegades es troben a fora de l'empresa amb un accés a Internet. L'encaminador NAT de l'empresa té com adreça pública la 83.5.5.5. Per tant, quan els usuaris obren un navegador amb http://empresa.cat volen veure el servidor estiguin on estiguin. Defineix quins serveis i quina configuració han de tenir per aconseguir això. Si existeix més d'una possibilitat llista-les i justifica quina esculls. (1)

6. Un mecanisme per obtenir un certificat vàlid d'una autoritat certificadora per un servidor web amb nom empresa.cat consisteix en el següent: L'autoritat certificadora disposa d'una web on es rep la petició del certificat. L'autoritat genera un fitxer.txt amb un contingut concret i específic. L'autoritat espera trobar aquest fitxer en el servidor web a la URL (http://empresa.cat/fitxer.txt). Quan l'autoritat de certificació troba el seu fitxer a la URL especificada és quan pot generar el certificat per aquesta web i ofereix un enllaç de descàrrega per obtenir-lo. (1)

   a) Consideres que és un mecanisme vàlid per concedir el certificat? Justifica.

   b) Quins són els punts febles d'aquest mecanisme per tal d'aconseguir el certificat?

   c) Quina és la funció d'un "nonce"? El fitxer.txt fa aquesta funció? Justifica.

   d) Quan es fa la petició del certificat a la web de l'autoritat de certificació, cal adjuntar (enviar) a l'autoritat de certificació alguna cosa extra?