Aplicacions i Serveis a Internet

durada 2h

Final - Juny 2022

1. Responeu cert o fals a les següents frases. Justifiqueu la resposta. Les respostes incorrectes resten. Les respostes sense justificació compten la meitat. (26)

   a) El servei de noms de domini consisteix en generar una base de dades mundial on existeixen registres de diferents tipus on algun d'aquests registres tenen a veure amb l'adreça IP

   b) El DNS està estructurat globalment en forma d'arbre binari

   c) Els servidors autoritat DNS d'un domini sempre han d'estar accessibles per Internet.

   d) Els registres tipus A no poden tenir adreces de tipus privat

   e) El servei de noms de domini pot donar un nom a partir d'una adreça IP

   f) Els servidors de correu receptors poden fer servir alguns registres del servei de noms de domini per confirmar la autenticitat dels servidors de correus emissors de missatges

   g) Un servidor de correu que fa de smarthost verifica els servidors que el fan servir en funció dels dominis per als que fa de smarthost

   h) Un servidor de correu es basa en el domini del destinatari del missatge de correu per enviar els missatges a un smarthost

   i) Un servidor de correu rep missatges des d'Internet d'aquell servidor de correu que estigui a la llista de dominis que accepta

   j) La tecnologia Asynchronous Javascript and XML serveix per a que un navegador web pugui fer peticions peticions GET sense la intervenció de l'usuari i POST amb la seva intervenció

   k) Un script Javascript a part d'interactuar localment amb els recursos del navegador web on s'executa, també pot interactuar amb el servidor web des d'on s'ha descarregat aquest script i només amb ell.

   l) Entre una transacció HTTP i la següent no hi ha cap mena de relació. És a dir, una no depèn de l'altre

   m) Si no ha d'intervenir un tercer C, la signatura digital d'una transacció de A cap a B pot simplificar-se per una autentificació de A per part de B en aquesta transacció

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

   o) Les autoritats de certificació s'encarreguen de generar el certificat digital i han de proporcionar-te la clau privada associada a aquest certificat

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

   q) 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 es coneix de manera fiable el valor de la seva clau pública

   r) Quan unes claus caduquen, els documents signats amb aquestes claus també caduquen

   s) Si canviem la contrasenya de la clau privada, també canviem la clau privada

   t) Quan es compra un domini, el gestor al que li contractes demana 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

   u) Quan acceptem les cookies d'un lloc web, aquest lloc pot conèixer tota l'activitat que hem tingut amb ell

   v) El protocol HTTPS sempre garanteix la confidencialitat de la informació entre client i servidor a més de garantir l'autenticació de servidor però no de client

w) Les aplicacions P2P obliguen a obrir els ports dels encaminadors NAT que tenim a casa

x) En una funció de Hash, el conjunt de valors de sortida és més reduït que el conjunt de valors d'entrada. Per tant 2 entrades poden donar la mateixa sortida.

y) Un Firewall en Linux es pot implementar amb iptables

z) El DNS és un servei de la capa de Xarxa

2. Respon sí o no i justifica si els següents mecanismes serveixen per autentificar múltiples vegades (evitar atac de gravació) a un usuari A davant d'un usuari B. Considereu que si no es diu el contrari, la comunicació no està xifrada. Quan es parla de contrasenya, tant A com B la coneixen. (8)

a) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge H(m) com a prova de la seva identitat, on H(m) és el resultat d'aplicar una funció de hash coneguda.

b) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge H(m1|m2) on m2 és un missatge aleatori generat per A i m1|m2 és la concatenació dels dos missatges. H() és una funció de hash coneguda.

c) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge K(m) que és el resultat d'aplicar una transformació a m on aquesta funció K() de transformació només és coneguda per A i B.

d) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge H(m1|m2) on m2 és un missatge fixe conegut només per A i per B. H() és una funció de hash coneguda.

e) Usuari B espera la recepció d'un missatge c de A, on c és un la contrasenya associada a A.

f) Usuari B espera la recepció d'un missatge m de A, on m = KBp(c) és la contrasenya associada a A xifrada amb la clau pública de B.

g) Usuari B espera la recepció d'un missatge m de A, on m = K(c) és la contrasenya associada a A xifrada amb una clau només coneguda per A i B.

h) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge KBp(m2) on m2 és un missatge aleatori generat per A. La concatenació K = m1|m2 és la clau de sessió d'un algoritme conegut de xifrat simètric. Usuari A envia K(c) a B, on c és la contrasenya associada a A i coneguda per B.

3. Descriu el mecanisme que fa servir Let's Encrypt per validar la identitat del servidor del que es vol obtenir un certificat. (4)

4. Per aconseguir que ssh no demani usuari i contrasenya aprofitant la tecnologia de clau asimètrica, descriu què s'ha de fer tant en el client com en el servidor. (4)

5. Aplicant l'algoritme RSA, desxifreu el següent missatge: *LOYA. Teniu en compte que p=3, q=11 i e=7 (s'ha de trobar el valor correcte de d). (4)

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