Aplicacions i Serveis a Internet

durada 3h

Final - Juny 2015

1. Aplicant l'algoritme RSA, desxifreu el següent missatge: M_IOZOI. Teniu en compte que p=3, q=11 i e=7 (s'ha de trobar el valor correcte de d). (1)

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	

2. Un amic vostre vol començar una aventura com empresari. Aquest amic és molt conscient de la importància que té donar una bona imatge respecte als recursos TIC, per aquest motiu us demana assessorament per muntar una web i unes bústies de correu. Com al començament està malament de diners, decideix utilitzar servidors gratuïts tant per les bústies de correu com per la web. Disposa del compte pepet1234@bustiagratis.com com de la web aprofita.webgratis.com/pepetlleig. En tot cas, el que està disposat a pagar és el domini pepet.cat. El gestor de domini, a més de poder definir qualsevol aspecte sobre el servei de noms, li permet definir qualsevol tipus de configuració sobre un servidor web i un servidor de correu del propi gestor, però no és possible allotjar cap tipus de dada. Aquest amic tampoc es pot permetre la instal·lació d'un servidor propi. Aquest amic us demana poder rebre correus dels comptes info@pepet.cat i comandes@pepet.cat i que la gent accedeixi a la seva web tant amb pepet.cat com www.pepet.cat. És possible satisfer les seves necessitats amb aquestes restriccions? Indiqueu si cal algun recurs extra més. Proposeu de quina manera s'haurien de configurar tant el servei de DNS, el servidor web i el servidor de correu del gestor. Recordeu que en el servei de DNS els principals registres que es poden definir són: NS, A, CNAME, MX. Recordeu que en el servei web algunes de les directives sobre les que s'ha treballar han sigut: VirtualHost, DocumentRoot, ServerName, Location, ProxyPass, ProxyPassReverse, Redirect, Alias, Directory, etc. Recordeu que el servei de correu des del punt de vista de recepció essencialment pot ser: local, dominis locals, com a smarthost. El correu des del punt de vista del lliurament essencialment pot ser: local, cap a smarthost, a internet. (1.5)

3. Quan es compra un domini, sobre quins servidors de domini (local, root, autoritatiu, ...) s'han de fer modificacions als seus fitxers de configuració? Indica les modificacions que s'han de fer en cadascun d'ells. (1)

4. Per molts treballs d'administració de maquines remotes, la manera més habitual de treballar és establir una sessió de shell remota amb ssh. La connexió a un servidor ssh té dues fases. La primera determina el mecanisme per a que tant client com servidor arribin a un acord per establir una clau simètrica de sessió. Un cop establerta aquesta sessió, la segona fase determina la autentificació del client. Aquesta autentificació es pot realitzar de dues maneres: introduint nom d'usuari i contrasenya o bé a través de claus asimètriques. Justifica sempre les respostes a les següents preguntes: (1.5)

   a) Enumera quins són els aspectes que intervenen sota el concepte de seguretat en les comunicacions.

   b) Quin mecanisme d'autentificació consideres més segur?

   c) Quan un client ssh ha establert la sessió amb el servidor, i vol fer servir l'autentificació per claus, qui ha de generar el parell de claus, el client, el servidor o els dos?

   d) La primera vegada que un client connecta a un servidor, surt un missatge d'alerta. Sobre què pot alertar aquest missatge?

   e) Si una entitat disposa de la clau pública d'una altra, de quina manera pot comprovar que l'altra entitat és la que correspon amb aquesta clau pública?

   f) Si una entitat disposa de la clau pública d'una altra, quins són els aspectes relatius a la seguretat que pot satisfer i quins no?

5. Preguntes cert o fals. Justifiqueu la resposta. Les respostes incorrectes resten 0.25 (2.5)

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

   b) 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.

   c) Es pot considerar signatura electrònica simplement el Hash corresponent de qualsevol missatge, sempre i quan aquest Hash provingui de manera fiable de qui ha generat el missatge. Per tant no cal la utilització de claus asimètriques.

   d) 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.

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

   f) Els atacs de denegació de servei es produeixen per una utilització pobre de les claus de xifrat.

   g) El tracker d'una xarxa bittorrent conté el llistat dels fitxers que ell està difonent, per tant els peers es connecten per conèixer el llistat de fitxers compartits

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

   i) Els recursos del sistema que necessiten els Sockets són iguals tant pels UDP com pels TCP, ja que tant un com l'altre permeten l'enviament i recepció del mateix tipus de informació.

   j) Si obro el meu punt d'accés WIFI de casa i instal·lo un programari per capturar els missatges dels possibles clients del meu punt d'accés, puc veure tota la informació que intercanvien sense que ells puguin fer res per aconseguir una comunicació segura. Aquest atac forma part de la família "Man in de middle".

6. Quina utilitat té un Nonce en temes de seguretat? Dóna un exemple. Quins aspectes de seguretat pot protegir? (0.5)

7. Dóna 2 exemples concrets de filtrat que indiquen que un Firewall és amb estat. (1)

8. Es vol dissenyar una pàgina web que inverteixi el text que entra l'usuari i li retorni el resultat. Descriu com dissenyaries aquest sistema (javascript, cgi, PHP, ...). Suposa que en qualsevol llenguatge que utilitzis disposes de la funció reverse(). (1)