Ejercicio-sesion-6.pdf

PruebaAlien

Fundamentos de Redes

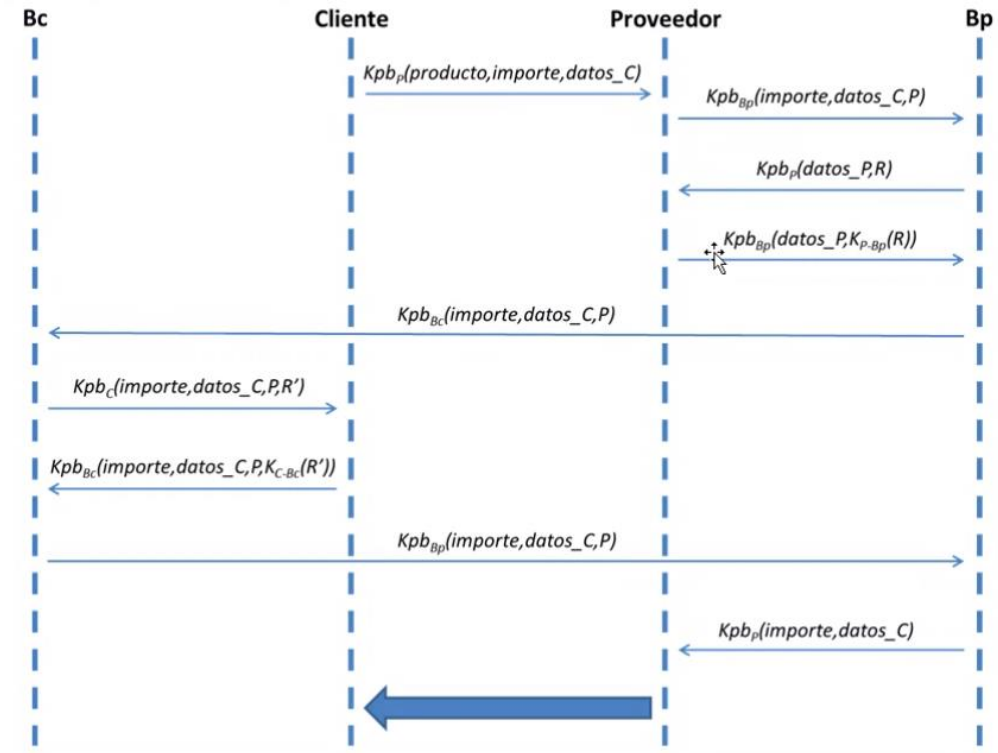
3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación
Universidad de Granada

Ejercicio de seguridad

Mensajes:

- C → Cliente
- P → Proveedor
- kbp_{Bp}
- kbp_p
- kbp_{Bc}
- kbp_c
-



a)

como va todo cifrado, tiene **confidencialidad**, como no hay una función hash, que compruebe los datos, con lo cual no tiene **integridad**, tiene **autenticación parcialmente**, ya que el proveedor se autentifica en su entidad bancaria y lo mismo en el cliente, pero puede haber suplantación en la entidad bancaria, ya que no hace autentificación con el proveedor o cliente, no tiene **no repudio**, porque los mensajes se envía hacia un sentido y el proveedor no puede saber que sea el cliente el que se ha conectado, ya que no tienen firma digital, es decir que el cliente lo encripte con la clave privada y el proveedor lo desencritpa con la clave publica del cliente.

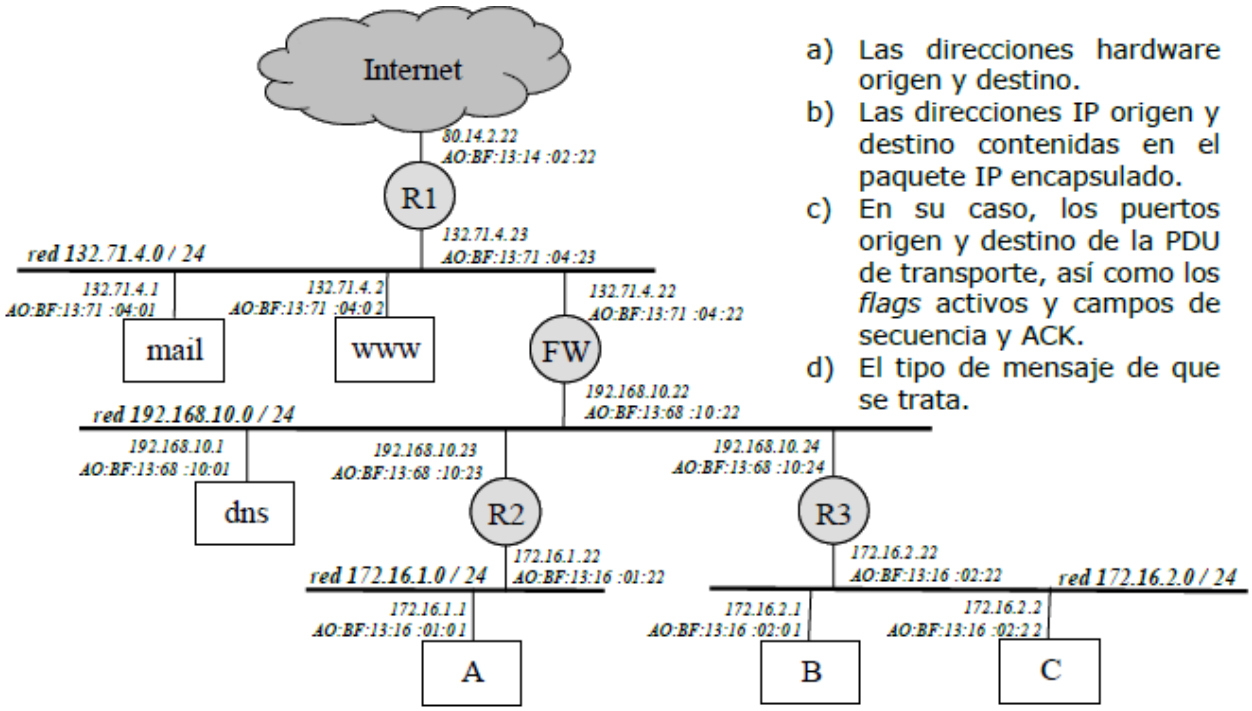
b)

no tiene integridad, para solucionarlo habría que hacer un calculo de hash en todas las transmisiones de datos.

No tiene no repudio, para solucionarlo, ambos (cliente y proveedor) autentificar con un certificado virtual, enviando el cliente una clave encriptada y en el proveedor envia la clave desencriptada

Y podría haber otro paso de autentificación entre cliente y proveedor.

EJERCICIO DE TRAFICO GENERADO Y CAMPOS EN LOS PAQUETES



a) Las direcciones hardware origen y destino.
b) Las direcciones IP origen y destino contenidas en el paquete IP encapsulado.
c) En su caso, los puertos origen y destino de la PDU de transporte, así como los *flags* activos y campos de secuencia y ACK.
d) El tipo de mensaje de que se trata.

NOTA: *suponga todas las tablas ARP son conocidas y, por simplicidad utilice sólo el último de los 6 octetos de las direcciones físicas de las NIC (interfaces o tarjetas de red)*

CONEXIONES:

1. B →DNS
2. DNS → B
3. B → MAIL (HELLOW)
4. MAIL → B (HELLOW)
5. B → MAIL (Cierre de conexión)
6. MAIL → B (Cierre de conexion)

LAS 132 SON PUBLICAS

ETH Origen	ETH Destino	IP Origen	IP Destino	PORT Ori	PORT Des	Flags	MENSAJE	COMENTARIOS

KEEP CALM AND ESTUDIA UN POQUITO

WUOLAH + #QuédateEnCasa

AO:DF:13:16:02:01 (B)	AO:BF:13:16:02:22 (R3)	172.16.2.1 (B)	192.168.10.1 (DNS)	(1*)	53	---	Solicitud DNS, dominio mail	A traves de R3
AO:BF:13:68:10:24 (R3)	AO:BF:13:68:10:01 (DNS)	172.16.2.1 (B)	192.168.10.1 (DNS)	(1*)	53	---	Solicitud DNS, Dominio mail	Retransmitiendo de R3 a DNS
AO:BF:13:68:10:01 (DNS)	AO:BF:13:68:10:24 (R3)	192.168.10.1 (DNS)	172.16.2.1 (B)	53	(2*)	---	Respuesta DNS, IP de email	A TRAVES DE R3
AO:BF:13:16:02:22 (R3)	AO:DF:13:16:02:01 (B)	192.168.10.1 (DNS)	172.16.2.1 (B)	53	(2*)	---	Respuesta DNS, IP de email	Retransmisión a B

(1*) asignación del so (2*) PUERTO ELEGIDO EN (1*)

(1*) y (2*) son el mismo (asignado por el S.O.)

Paso 2: establecimiento conexión TCP

NAT == masquerading, es una traducción de IPs entre subredes.

SMTP sobre TCP en el Puerto 25

ETH ORI	ETH DES	IP ORI	IP DEST	PORT ORI	PORT DES	FLAGS	MENSAJE	COMENTARIOS
04:22 (B)	02:22 (R3)	172.16.2.1 (B)	132.71.4.1 (email)	(1*)	25	SYN X (3*)	Solicitud establecimiento TCP a email	A través de R3
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (email)	(1*)	25	SYN X (3*)	Solicitud establecimiento TCP a email	Retransmision a FW
10:22 (FW)	04:22 (email)	132.71.4.22 (FW)	132.71.4.1 (email)	(5*)	25	SYN X (3*)	Aceptación y establecimiento en otro sentido	MASQUERADIN FW entrega
04:22 (email)	10:22 (FW)	132.71.4.1 (email)	132.71.4.22 (FW)	25	(5*)	SYN, ACK X+1, Y	Aceptación y establecimiento en otro sentido	Mail hacia el firewall
10:22 (FW)	10:24 (R3)	132.71.4.1 (email)	172.16.2.1 (B)	25	(2*)	SYN, ACK X+1, Y	Aceptación y establecimiento en otro sentido	Deshace el masquerading FW retransmisión
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (email)	(1*)	25	SYN X (3*)	Solicitud establecimiento TCP a email	R3 retransmision a FW
04:22 (B)	10:24 (R3)	132.71.4.1 (email)	172.16.2.1 (B)	25	(2*)	SYN, ACK X+1, Y	Aceptación en el otro sentido	R3
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (email)	(1*)	25	SYN X (3*)	Aceptación en el otro sentido	MASQUERADIN
10:22 (FW)	04:22 (email)	132.71.4.22 (FW)	132.71.4.1 (email)	(5*)	25	SYN X (3*)	Aceptación en el otro sentido	A TRAVES DE R3

(2*) puerto elegido en (1*)

(1*) puerto elegido por el S.O.

(3*) numero aleatorio elegido por el emisor

(4*) FW al hacer masquerading mapea

(5*) puerto elegido por FW en (4*)

Una vez establecida la conexión, ya se iniciaría el acceso al correo

SMTP sobre TCP en el puerto 25

NAT == masquerading, es una traducción de IPs entre subredes.

ETH ORI	ETH DES	IP ORI	IP DEST	PORT ORI	PORT DES	FLAGS	MENSAJE	COMENTARIOS
04:22 (B)	02:22 (R3)	172.16.2.1 (B)	132.71.4.1 (email)	(2*)	25	X+1	Helo servidor	Conexión con el servidor
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (email)	(2*)	25	X+1	Helo servidor	Retransmision a FW
10:22 (FW)	04:22 (email)	132.71.4.22 (FW)	132.71.4.1 (email)	(5*)	25	X+1	Helo servidor	MASQUERADIN FW entrega
04:22 (email)	10:22 (FW)	132.71.4.1 (email)	132.71.4.22 (FW)	25	(5*)	ACK X+1+NB(helo), Y+1	Texto respuesta servidor	Mail hacia el firewall
10:22 (FW)	10:24 (R3)	132.71.4.1 (email)	172.16.2.1 (B)	25	(2*)	ACK X+1+NB(helo), Y+1	Texto respuesta servidor	Deshace el masquerading FW retransmisión
10:24 (R3)	10:22 (B)	172.16.2.1 (B)	132.71.4.1 (email)	25	(2*)	ACK X+1+NB(helo), Y+1	Texto respuesta servidor	R3 retransmision a FW