

Caso T8

1) En el siguiente fragmento de XML, que describe al emisor de una factura electrónica, existen 5 errores a nivel léxico y/o sintáctico, independientemente de la existencia o no de un DTD o esquema. El ejercicio consiste en localizarlos, explicar en qué consisten y cómo se solucionarían. Los números de línea no forman parte del XML, solo aparecen para que resulte más fácil referirse a líneas específicas al describir los errores. (Valor por error detectado y analizado correctamente: 10%)

```
1. <SellerParty>
2.   <TaxIdentification>
3.     <PersonTypeCode>J</PersonTypeCode>
4.     <ResidenceTypeCode>R</ResidenceTypeCode>
5.     <TaxIdentificationNumber>A82735122</TaxIdentificationNumber>
6.   </TaxIdentification>
7. <SellerParty>
8.   <LegalEntity>
9.     <CorporateName>Company Comp & Partners SA</CorporateName>
10.    <TradeName>Comp</TradeName>
11.    <RegistrationData>
12.      <Book>1</Book>
13.      <RegisterOfCompaniesLocation>12AP22</RegisterOfCompaniesLocation>
14.      <Sheet>3</Sheet>
15.      <Folio>15</Folio>
16.      <Section>2</Section>
17.      <Volume>12</Volume>
18.      <AdditionalRegistrationData>Sin datos</AdditionalRegistrationData>
19.    </RegistrationData>
20.    <AddressInSpain>
21.      <Address>C/ Mayor 33 15º E</Address>
22.      <PostCode>28001</PostCode>
23.      <Town>Argamasilla de Alba</Town>
24.      <Province>Ciudad Real</Province>
25.      <CountryCode>ESP</>
26.    </AddressInSpain>
27.    <ContactDetails>
28.      <Telephone>917776665</Telephone>
29.      <TeleFax>917776666</TeleFax>
30.      <WebAddress>www.facturae.es</WebAddress>
31.      <ElectronicMail><facturae@mityc.es></ElectronicMail>
32.      <ContactPersons>Fernando</ContactPersons>
33.      <CnoCnae>28000</CnoCnae>
34.      <INETownCode>2134AAB</INETownCode>
35.      <AdditionalContactDetails>Otros datos</AdditionalContactDetails>
36.    </ContactDetails>
37.  </LegalEntity>
38. </SellerParty>
```

Valor de la pregunta: 50% de la nota del caso

2) El kernel del sistema operativo Linux lleva integrado el firewall *iptables*. Para el presente ejercicio se utilizará una versión simplificada del mismo, definida de la siguiente manera:

- Las reglas del firewall se estructuran en cadenas. Una cadena es una sucesión ordenada de reglas, con un nombre y una política (que es la acción que se ejecuta por defecto después de procesar todas las reglas de una cadena si estas no ejecutan una acción **ACCEPT** o **DROP**, que finaliza el procesamiento de la cadena inmediatamente). Existen nombres de cadenas reservados y otros que se pueden crear por el usuario. En este caso, utilizaremos como nombres de cadena reservados únicamente **INPUT** (filtra todos los paquetes que se dirigen al servidor que contiene el firewall), **OUTPUT** (filtra todos los paquetes que se originan en el

servidor que contiene el firewall) y **FORWARD** (filtra todos los paquetes que pasan por el firewall, pero tanto su origen como su destino son equipos diferentes).

- La política de una cadena no definida por el usuario puede ser **ACCEPT** (se acepta el paquete) o **DROP** (se ignora el paquete). Las cadenas definidas por el usuario tienen siempre como política implícita **RETURN** (se devuelve el control a la regla siguiente, esté en la cadena que esté, a la que ha causado que se salte a la cadena actual).
- Cada regla tiene un objetivo, protocolo, origen, destino, puerto origen (si el protocolo es **tcp** o **udp**) y puerto destino (si el protocolo es **tcp** o **udp**). Si los datos del paquete encajan con lo especificado en el protocolo, origen, destino, puerto origen y puerto destino, se ejecuta la acción asociada al objetivo.
- El objetivo puede ser **ACCEPT**, **DROP**, **RETURN** (como las políticas equivalentes) o el nombre de una cadena definida por el usuario (se salta a la primera regla de la cadena especificada, que va procesando todas sus reglas por orden, hasta encontrar una regla que aplique un nuevo objetivo o hasta llegar al final de la cadena, donde se aplicaría su política).
- El protocolo puede ser **all**, **tcp**, **udp** o **icmp**.
- El origen y el destino son la dirección IP de origen y destino del paquete en el formato *dirección[/máscara]*. La dirección IP tiene el formato estándar (p. ej., 10.201.45.67) y la máscara, opcional, puede estar en el formato completo (p. ej., 255.255.255.0), o bien en el formato CIDR, donde se especifica el número de bits "1" consecutivos que tiene la máscara, empezando por la izquierda (p. ej., /24 sería la notación CIDR equivalente a /255.255.255.0). Alternativamente, se puede especificar la palabra **anywhere** para que se acepte cualquier dirección de origen y/o de destino.
- El puerto de origen y de destino son un entero de 16 bits que especifica el número de puerto (0-65535) o bien la palabra **any** para aceptar cualquier puerto.
- Si en el valor del protocolo, origen, destino, puerto origen o puerto destino se especifica en primer lugar el carácter "!", la condición pasa a tener el sentido contrario (operación booleana NOT). Si, por ejemplo, especificamos que el puerto de destino es el 80 (http), el paquete que llegue deberá ir dirigido a ese puerto para cumplir la condición; en cambio, si especificamos como puerto de destino "!80", entonces cumple la condición cualquier valor del puerto de destino excepto el 80.
- Se considera que el firewall tiene una regla implícita de control de conexiones, por lo que las reglas solo se aplican al primer paquete de una conexión. Si se acepta o rechaza el primer paquete de una conexión, el resto de paquetes de la misma conexión son igualmente aceptados o rechazados sin tener que procesar las reglas de las cadenas correspondientes, con lo que solo debemos preocuparnos de definir las reglas en función del paquete inicial.

Las cadenas de iptables para el ejercicio se escribirán en el siguiente formato (la última fila es una regla de ejemplo que corta todo el tráfico TCP dirigido a la IP 80.1.1.5 excepto el que va al puerto 80):

Req.	Cadena:	(nombre)				
(letra0)	Política:	(política)				
	Objetivo	Protocolo	Origen	Destino	Puerto Orig.	Puerto Dest.
(letra1)	(objetivo1)	(protocolo1)	(origen1)	(destino1)	(ptoorig1)	(ptodest1)
(letra2)	(objetivo2)	(protocolo2)	(origen2)	(destino2)	(ptoorig2)	(ptodest2)
...
j	DROP	tcp	anywhere	80.1.1.5	any	!80

Se pide escribir las cadenas de iptables según la definición y el formato anterior para el caso práctico que se planteará a continuación. La columna "Req." no forma parte de las reglas de iptables, pero debe contener, como referencia, la letra que identifica el requerimiento correspondiente por el cual se ha creado una regla o se ha dado un valor a una política.

En nuestro caso práctico, una organización tiene un firewall que protege el perímetro de su red. La organización tiene múltiples subredes privadas dentro del direccionamiento 10.0.0.0/8 y una subred DMZ con direccionamiento público 80.1.1.0/24. Todo el tráfico que entra o sale de la organización atraviesa el firewall. También atraviesa el firewall el tráfico entre la subred privada y la DMZ, pero no el tráfico interno de la subred privada ni el de la DMZ. Para permitir a las subredes privadas acceder a Internet con una IP pública, el firewall incorpora la funcionalidad de SNAT (traducción de direcciones de origen). Así pues, la organización ha decidido implementar en el firewall los siguientes requerimientos de control de acceso a la red:

- El firewall solo puede recibir tráfico dirigido a él si proviene de la red privada y va dirigido al puerto 443/tcp (https). Todo el tráfico de salida originado en él mismo está permitido. El resto del tráfico, el que atraviesa el firewall, se rechazará por defecto mientras no exista un requerimiento que lo permita. (Valor: 10%)
- En las direcciones 80.1.1.16 hasta 80.1.1.31 se encuentran los servidores web, que deben aceptar tráfico hacia los puertos 80/tcp (HTTP) y 443/tcp (HTTPS). (Valor: 10%)
- Las redes internas 10.1.0.0/16, 10.17.5.128/25 y 10.20.40.0/24 tienen permitido acceder a Internet (todas las direcciones públicas excepto la DMZ de la organización), pero el resto de las redes internas, no. (Valor: 10%)
- Ninguno de los equipos de la red interna debe poder acceder a los puertos 25/tcp (SMTP) y 110/tcp (POP3) de la DMZ o de Internet. (Valor: 10%)
- Debe poderse acceder desde la red 10.0.0.0/8 a los servidores 80.1.1.3, 80.1.1.5 y 80.1.1.8 por los puertos 18080/tcp, 28080/tcp y 38080/tcp (servidores de aplicaciones). (Valor: 10%)

Valor de la pregunta: 50% de la nota del caso