

## Cas T8

1) En el següent fragment d'XML, que descriu l'emissor d'una factura electrònica, hi ha 5 errors a nivell lèxic i/o sintàctic, independentment de l'existència o no d'un DTD o esquema. L'exercici consisteix en localitzar-los, explicar en què consisteixen i com se solucionarien. Els nombres de línia no formen part de l'XML, només apareixen perquè resulti més fàcil referir-se a línies específiques en descriure els errors. (Valor per error detectat i analitzat correctament: 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 cas

2) El kernel del sistema operatiu Linux duu integrat el firewall *iptables*. Per al present exercici s'utilitzarà una versió simplificada del mateix, definida de la següent manera:

- Les regles del firewall s'estructuren en cadenes. Una cadena és una successió ordenada de regles, amb un nom i una política (que és l'acció que s'executa per defecte després de processar totes les regles d'una cadena si aquestes no executen una acció **ACCEPT** o **DROP**, que finalitza el processament de la cadena immediatament). Existeixen noms de cadenes reservats i altres que es poden crear per l'usuari. En aquest cas, utilitzarem com a noms de cadena reservats únicament **INPUT** (filtra tots els paquets que es dirigeixen al servidor que conté el firewall), **OUTPUT** (filtra tots els paquets que s'originen al servidor que conté el firewall) i

**FORWARD** (filtra tots els paquets que passen pel firewall, però tant el seu origen com la seva destinació són equips diferents).

- La política d'una cadena no definida per l'usuari pot ser **ACCEPT** (s'accepta el paquet) o **DROP** (s'ignora el paquet). Les cadenes definides per l'usuari tenen sempre com a política implícita **RETURN** (es torna el control a la regla següent, sigui a la cadena que sigui, a la que ha causat que se salti a la cadena actual).
- Cada regla té un objectiu, protocol, origen, destinació, port origen (si el protocol és **tcp** o **udp**) i port destinació (si el protocol és **tcp** o **udp**). Si les dades del paquet encaixen amb l'especificat en el protocol, origen, destinació, port origen i port destinació, s'executa l'acció associada a l'objectiu.
- L'objectiu pot ser **ACCEPT**, **DROP**, **RETURN** (com les polítiques equivalents) o el nom d'una cadena definida per l'usuari (se salta a la primera regla de la cadena especificada, que va processant totes les seves regles per ordre, fins a trobar una regla que apliqui un nou objectiu o fins i tot arribar al final de la cadena, on s'aplicaria la seva política).
- El protocol pot ser **all**, **tcp**, **udp** o **icmp**.
- L'origen i la destinació són l'adreça IP d'origen i destinació del paquet en el format *adreça/màscara*. L'adreça IP té el format estàndard (p. ex., 10.201.45.67) i la màscara, opcional, pot estar en el format complet (p. ex., 255.255.255.0), o bé en el format CIDR, on s'especifica el nombre de bits "1" consecutius que té la màscara, començant per l'esquerra (p. ex., /24 seria la notació CIDR equivalent a /255.255.255.0). Alternativament, es pot especificar la paraula **anywhere** perquè s'accepti qualsevol adreça d'origen i/o de destinació.
- El port d'origen i de destinació són un enter de 16 bits que especifica el nombre de port (0-65535) o bé la paraula **any** per acceptar qualsevol port.
- Si en el valor del protocol, origen, destinació, port origen o port destinació s'especifica en primer lloc el caràcter "!", la condició passa a tenir el sentit contrari (operació booleana NOT). Si, per exemple, especificam que el port de destinació és el 80 (http), el paquet que arribi haurà d'anar dirigit a aquest port per complir la condició; en canvi, si especificam com a port de destinació "!80", llavors compleix la condició qualsevol valor del port de destinació excepte el 80.
- Es considera que el firewall té una regla implícita de control de connexions, per la qual cosa les regles només s'apliquen al primer paquet d'una connexió. Si s'accepta o rebutja el primer paquet d'una connexió, la resta de paquets de la mateixa connexió són igualment acceptats o rebutjats sense haver de processar les regles de les cadenes corresponents, amb la qual cosa només ens hem de preocupar de definir les regles en funció del paquet inicial.

Les cadenes d'iptables per a l'exercici s'escriuran en el següent format (la darrera fila és una regla d'exemple que talla tot el trànsit TCP dirigit a la IP 80.1.1.5 excepte el que va al port 80):

<b>Req.</b>	<b>Cadena:</b>	<i>(nom)</i>				
<i>(lletra0)</i>	<b>Política:</b>	<i>(política)</i>				
	<b>Objectiu</b>	<b>Protocol</b>	<b>Origen</b>	<b>Destinació</b>	<b>Port Origen</b>	<b>Port Destí</b>
<i>(lletra1)</i>	<i>(objectiu1)</i>	<i>(protocol1)</i>	<i>(origen1)</i>	<i>(destí1)</i>	<i>(portorig1)</i>	<i>(portdestí1)</i>
<i>(lletra2)</i>	<i>(objectiu2)</i>	<i>(protocol2)</i>	<i>(origen2)</i>	<i>(destí2)</i>	<i>(portorig2)</i>	<i>(portdestí2)</i>
...	...	...	...	...	...	...
j	DROP	tcp	anywhere	80.1.1.5	any	!80

Es demana escriure les cadenes d'iptables segons la definició i el format anterior per al cas pràctic que es plantejarà a continuació. La columna "Req." no forma part de les regles d'iptables, però ha de contenir, com a referència, la lletra que identifica el requeriment corresponent pel qual s'ha creat una regla o s'ha donat un valor a una política.

En el nostre cas pràctic, una organització té un firewall que protegeix el perímetre de la seva xarxa. L'organització té múltiples subxarxes privades dins del direccionament 10.0.0.0/8 i una subxarxa DMZ amb direccionament públic 80.1.1.0/24. Tot el trànsit que entra o surt de l'organització travessa el firewall. També travessa el firewall el trànsit entre la subxarxa privada i la DMZ, però no el trànsit intern de la subxarxa privada ni el de la DMZ. Per permetre a les subxarxes privades accedir a Internet amb una IP pública, el firewall incorpora la funcionalitat de SNAT (traducció d'adreces d'origen). Així doncs, l'organització ha decidit implementar al firewall els següents requeriments de control d'accés a la xarxa:

- a) El firewall només pot rebre trànsit dirigit a ell si prové de la xarxa privada i va dirigit al port 443/tcp (https). Tot el trànsit de sortida originat en ell mateix està permès. La resta del trànsit, el que travessa el firewall, es rebutjarà per defecte mentre no existeixi un requeriment que ho permeti. *(Valor: 10%)*
- b) En les adreces 80.1.1.16 fins a 80.1.1.31 es troben els servidors web, que han d'acceptar trànsit cap als ports 80/tcp (HTTP) i 443/tcp (HTTPS). *(Valor: 10%)*
- c) Les xarxes internes 10.1.0.0/16, 10.17.5.128/25 i 10.20.40.0/24 tenen permès accedir a Internet (totes les adreces públiques excepte la DMZ de l'organització), però la resta de les xarxes internes, no. *(Valor: 10%)*
- d) Cap dels equips de la xarxa interna no ha de poder accedir als ports 25/tcp (SMTP) i 110/tcp (POP3) de la DMZ o d'Internet. *(Valor: 10%)*
- e) Ha de poder accedir-se des de la xarxa 10.0.0.0/8 als servidors 80.1.1.3, 80.1.1.5 i 80.1.1.8 pels ports 18080/tcp, 28080/tcp i 38080/tcp (servidors d'aplicacions). *(Valor: 10%)*

*Valor de la pregunta: 50% de la nota del cas*