Tecnologies avançades d'Internet
Pràctica 1: *Iptables*

curs 2020-2021

1 Objectius

`Iptables` és l'aplicació encarregada d'interactuar amb el nucli Linux per tractar aspectes relacionats amb paquets IP que es generen, travessen o es manipulen en el sistema operatiu.

L'objectiu d'aquesta pràctica és aprendre el funcionament de la infraestructura utilitzada a `iptables` i entendre com manipular les principals opcions de la mateixa. Aquest coneixement s'haurà d'aplicar per resoldre l'hipotètic cas de gestió explicat a la següent secció.

2 Introducció al CORE

Per realitzar la pràctica utilitzarem un emulador de xarxa anomenat CORE (Common Open Research Emulator). Aquest emulador permetrà tenir múltiples contenidors que es comportaran com a sistemes Linux aïllats entre si. Aquest contenidors, donat que són sistemes Linux, podran ser clients, hosts, routers o hubs, entre d'altres.

El CORE permet realitzar proves i tasques d'administració en els diferents `containers` (o sistemes) d'una manera còmoda i eficaç. A més, els contenidors tot i que són semblants a les màquines virtuals que podríem utilitzar en VMWare són molt més lleugeres reduint així el consum de recursos.

L'emulador es proporciona totalment configurat dintre d'una màquina virtual. D'aquesta manera és podran realitzar les pràctiques tant al laboratori com a qualsevol altre màquina que suporti VMWare.

Un cop inicieu l'emulació, els contenidors de CORE estan accessibles a través del directori de la màquina virtual: */tmp/pycore.xxxx* on *xxxx* és l'identificador de l'emulació actual (pot variar entre emulacions).

Dins d'aquest directori trobarem un directori **.conf* per a cada un dels contenidors. Aques directori **.conf* és el directori *home* del contenidor.

Per exemple el directori */tmp/pycore.xxxx/gateway.conf/* contindrà l'estructura de directoris del `gateway` per a l'emulació `xxxx`.

En el cas de la pràctica només heu de llençar una emulació alhora.

2.1 Aspectes a considerar

Per a la correcta consecució de la pràctica heu de tenir en compte el següent:

- Tots els passos a realitzar s'han de fer des de la línia de comandes, no serà vàlid modificar la configuració del CORE per aconseguir la funcionalitat que us demanem, excepte si s'especifica el contrari.
- Assegureu-vos d'utilitzar sempre l'escenari de CORE adient per cada pràctica.

  Per aquesta primera pràctica el fitxer de l'escenari és el **`p1.imn`**.

  Un cop heu arrencat la màquina virtual que conté el CORE instal.lat cal que us descarregueu aquest escenari. Per a fer-ho, en la màquina virtual, descarregueu-vos el fitxer p1.imn del campus virtual i deixeu-ho a l'escriptori.
- Per a carregar la topologia del fitxer `p1.imn` seguiu les següents passes:

  1. Executeu el `core`.
  2. Carregueu la topologia des d'opció de menú: `file > open > p1.imn`.
  3. Executeu la simulació tot clicant en el botó del play del `core`.
- Una vegada parem l'emulació, tota la configuració així com el contingut dels `containers` s'esborrarà. Així doncs serà important guardar els scripts de manera regular.
- La màquina virtual serà utilitzada per altres grups, enrecordeu-vos de no deixar scripts en aquesta.

3 Enunciat

3.1 Esquema principal

La topologia de xarxa que gestionarem la trobeu a la figura 1. Aquesta topologia està configurada en l'escenari **`p1.imn`**.
En aquest escenari tindrem 4 contenidors que faran les funcions de *gateway*, *workstation* (o client) i de *màquina real*.
Noteu que l'escenari de CORE proposat és molt semblant al que ens podríem trobaren qualsevol configuració d'una petita `LAN`.
A tots els nodes de l'escenari (gateway, WS i màquina real) tindreu accés de **root** amb password: **root** per a que pugueu modificar la configuració de xarxa.
Al node de la `màquina real` no farà falta modificar res.

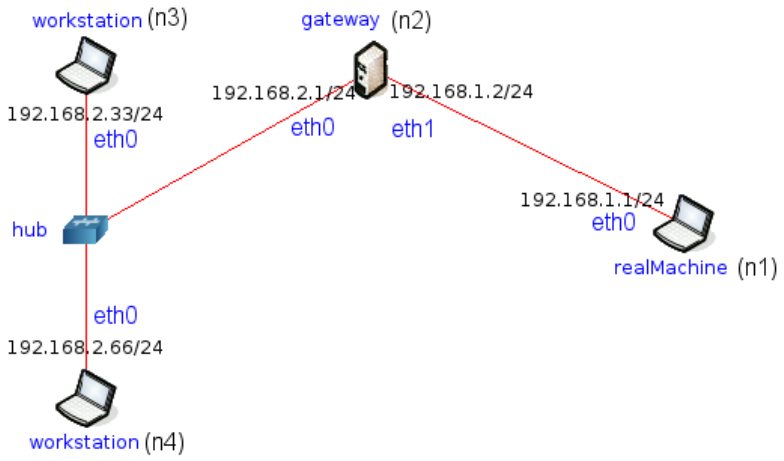

Figura 1: *Esquema principal del muntatge.*

De la topologia noteu els següent detalls:

- L'estació de treball utilitza el *gateway* per encaminar-se a Internet.
- La interfície `eth0` d'aquest gateway està connectada a un *hub* que permet la connexió de les interfícies `eth0` de les estacions de treball a la mateixa subxarxa: la `192.168.2.0/24`.
- Per dirigir els paquets que provenen d'aquesta xarxa cap a Internet, el *gateway* disposa d'una segona interfície, la `eth1`. Aquesta està connectada a

la xarxa `192.168.1.0/24` on, a partir de la interfície `eth0` de la màquina real, s'encaminen els paquets cap a Internet.

- La configuració que us trobareu en el *gateway* és la següent:
  - Les dues interfícies ja tenen assignades les IP corresponents.
  - La taula d'encaminament està configurada per accedir a les dues subxarxes i l'entrada per defecte d'aquesta taula és la IP `192.168.1.1`, corresponent a la interfície `eth0` de la màquina real.

3.2 Configuració de la xarxa

La pràctica consisteix en aplicar una configuració amb `iptables` que permeti el següent:

1. El gateway ha de poder redirigir els paquets provinents de les estacions de treball[1] cap a Internet.
2. S'ha de poder tallar/obrir la connexió a Internet segons l'usuari connectat a l'estació de treball.
3. Heu de configuració el sistema de logs del *gateway* per poder controlar les connexions que realitzen els usuaris. En el logs que genereu he d'especificar:
   - L'usuari que ha generat el datagrama.
   - La IP de l'estació de trebal des d'on l'usuari ha generat el datagrama.
   - La IP de destí del datagrama que ha generat l'usuari.
   - Un timestamp del datagrama que ha generat l'usuari.

3.2.1 Ususaris de les workstations

A les estacions de treball teniu definits els següents usuaris:

Taula 1: *Usuaris de les workstations.*

`login`	`password`	`userID`
root	root	0
user1	user1	999
user2	user2	998

Només farà falta registrar els logs del tràfic generat pels usuaris: `user1` i `user2`.

L'usuari `root` del sistema sempre ha de tenir accés a Internet.

[1] En aquest escenari tenim dues estacions de treball: la `n3` i la `n4`.

3.2.2 Aspectes a tenir en compte a l'hora d'aplicar les configuracions en el CORE

La configuració que heu d'aplicar a l'esquema anterior sempre ha de ser sobre l'escenari de CORE proporcionat **sense alterar cap configuració del emulador**, excepte si s'especifica el contrari.

Hi ha diverses formes de configurar el *gateway* i les estacions de treball per aconseguir els nostres objectius. Qualsevol mètode que funcioni serà vàlid per aprovar la pràctica, però és important que s'entenguin totes les opcions disponibles i que apliqueu la que creieu més adequada i funcional segons els requeriments demanats. La configuració adoptada s'haurà de justificar en l'informe final.

Totes les configuracions s'han de fer de forma dinàmica, és a dir, en cap moment ha de ser necessari parar l'emulació per aplicar les modificacions realitzades. Tot i que en un entorn real hauríem de poder aplicar els canvis necessaris i gravar-los perquè al reiniciar s'apliquessin, en el nostre cas **NO** s'ha de fer així. Recordem que la màquina virtual proporcionada serà utilitzada per tots els alumnes, de forma que si modifiquem algun aspecte del sistema el següent grup es pot trobar amb problemes.

3.3 Passos a realitzar per a la configuració de la xarxa

En aquest apartat donarem una breu descripció dels passos que s'haurien de seguir per aconseguir els nostres objectius.

1. FORWARDING DE DATAGRAMES IP

La distribució Debian GNU/Linux instal·lada als `containers` per defecte no permet redireccionament de paquets IP per qüestions òbvies de seguretat. El primer que haurem de fer és esbrinar on i què hem de modificar per permetre *forwarding* de paquets.

2. EMMASCARAMENT

El *gateway* amb la seva adreça `192.168.1.2` pot accedir a internet.

El gateway ha de poder encaminar els datagrames provinents de la xarxa `192.168.2.0/24` cap a internet.

Noteu que les adreces del rang `192.168.2.0/24` són adreces privades no enrutables.

Així doncs caldrà que el *gateway* faci una traducció d'adreces no enrutables per la seva adreça enrutable.

Això implica que el *gateway* ha de canviar la IP origen dels paquets que redirigeix, per la seva `192.168.1.2`.

3. COMPROVACIÓ

Per comprovar que realment la configuració aplicada fins ara funciona correctament, des del client hauríeu de ser capaços de fer *pings* cap a alguna IP d'Internet, s'han de resoldre noms, s'ha de poder navegar per la web (teniu el navegador en mode text *lynx*), etc.

4. MARCATGE DE PAQUETS

L'única forma de poder tallar/obrir l'accés a Internet des del *gateway* als diferents usuaris és poder marcar els paquets IP de les estacions de treball en funció de l'usuari.

Heu d'esbrinar algun mecanisme de marcatge de paquets i comprovar que realment funciona.

Compteu amb el programa *tcpdump*[2] i *wireshark*[3]. Executeu comandes diferents a ping perquè ping s'executa sempre com a root. Alternativa: Lynx.

[2] Amb l'emulació iniciada, botó dret sobre el container a analitzar, seleccionar tcpdump i clicar sobre la interfície a *snifar*

[3] Amb l'emulació iniciada, obrir el wireshark i seleccionar la interfície del container a *snifar*. Per exemple, per analitzar la eth0 del gateway (n2) al wireshark trobarem aquesta interfície identificada com a veth2.0.x.

5. CONTROL DE CONNEXIONS SEGONS USUARI

Si els paquets es marquen en funció de l'usuari, el *gateway* haurà de ser capaç de poder-los identificar correctament i, per tant, deixar-los passar o no.

6. COMPROVACIÓ

Podeu configurar el gateway per a que deixi passar el tràfic generat per l'usuari `user1` i no deixi passar el tràfit generat per `user2`.

Per comprovar el control per usuari, des de l'estació de treball `n3`, identifiqueu-vos com a `user1` i des de l'estació de treball `n4` identifiqueu-vos com a `user2`. Intenteu accedir a Internet en ambdós casos.

7. CONFIGURACIÓ DEL SISTEMA DE LOGGING

Cal que, en funció de l'usuari, genereu un log de la seva activitat. Aquest log ha de contenir com a mínim la següent informació:

- *Timestamp* del log
- UserID
- Ip i port d'origen
- IP i port de destí

Aquests logs els heu de desar en un fitxer.

4 Part No Obligatòria

La configuració de la xarxa que us hem proposat en les seccions anterior és obligatòria. Ha de funcionar tot. A continuació us proposem una funcionalitat, que no és obligatòria, amb la que podreu obtenir una puntuació de 10 en la pràctica.

4.1 Modificar l'escenari de CORE

Per a poder realitzar correctament la part opcional d'aquesta pràctica, s'ha de configurar el `gateway` a l'escenari de CORE per a que llenci un servidor HTTP
.
Per a fer-ho, amb **l'emulació parada**, s'ha de prémer botó dret sobre el `gateway`, clicar sobre `services` i seleccionar, sota la columna de `Utility`, el servei `HTTP`. La configuració final ha de quedar tal i com es mostra a la figura 2.
Seguidament farà falta prémer `Apply` a les dues finestres prèviament obertes.

Tingueu en compte que quan inicieu l'emulació el CORE triga una mica a arrencar el servidor `HTTP`. És per aquest motiu que el fitxer de configuració de la topologia que utilitzem, **p1.imn**, no té aquest servei ja arrencat.

4.2 Funcionalitat no obligatòria

A continuació us indiquem quina és la funcionalitat no obligatòria que podeu implementar.

4.2.1 Llista negra /llista blanca

Definir dues noves cadenes, chains, de Iptables:

Llista negra: Amb la primera **cadena** heu de crear una *llista negra* de IPs que **no puguin** accedir al servidor HTTP que hi ha instal.lat en el gateway.

Degut a la configuració de xarxa que tenim, els únics hosts als que podem aplicar aquesta restricció son els que pertanyen a la xarxa `192.168.2.0/24`.

Per a provar-ho, des de les workstations us podeu connectar via HTTP cap al `gateway(192.168.1.2)`. Podeu utilitzar com a navegador el `lynx` o bé utilitzar les comandes `wget` o `curl` per descarregar-vos via HTTP l'index.html.

Llista blanca Amb la segona cadena heu de crear una *llista blanca* de IPs que **sí puguin** accedir al servei SSH del gateway.

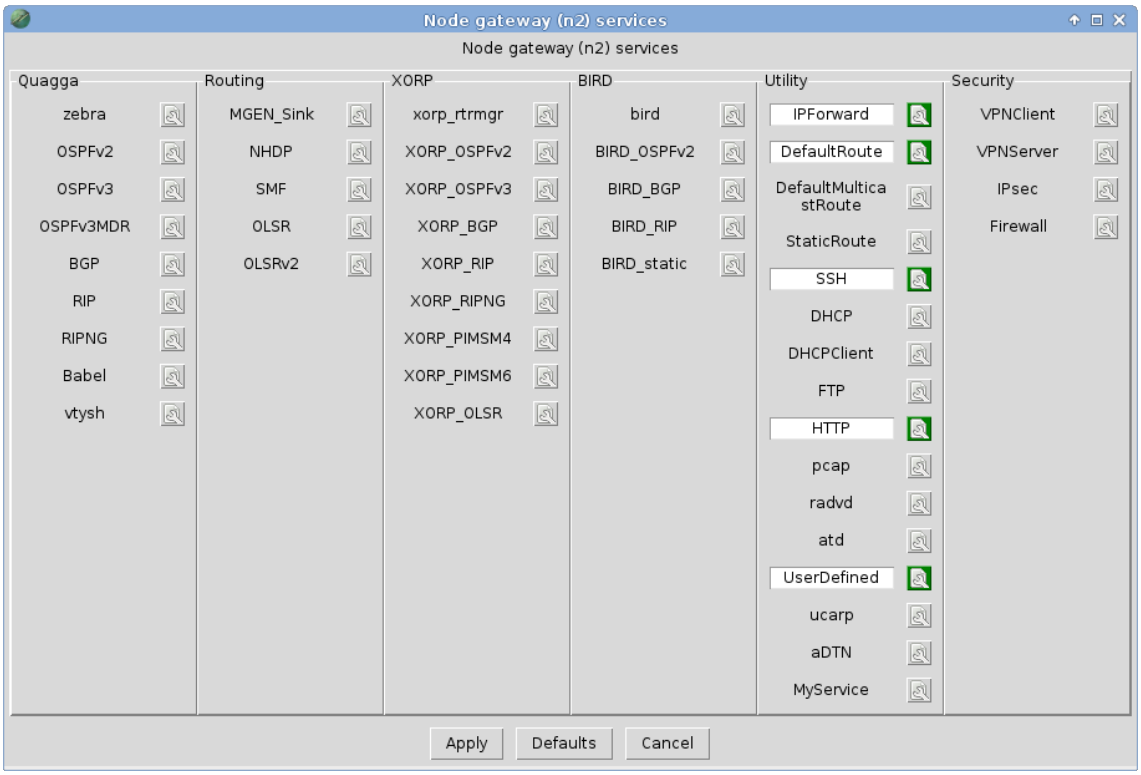

Figura 2: *Serveis activats per a la part no obligatòria.*

Com en el cas anterior, els únics hosts als que podem aplicar aquesta restricció son els que pertanyen a la xarxa `192.168.2.0/24`.

4.2.2 Limitar l'accés a les workstations

Configurar que les workstations **només** es puguin connectar a:

- Qualsevol màquina de la xarxa del deic: `158.109.79.0/24`.
- Al serveri **FTP** de rediris (`ftp.rediris.es`).

4.2.3 Blocar el servei del traceroute del gateway

Heu de configurar el gateway per a que no respongui si rep una petició a algun port del traceroute.
Aquesta configuració només l'heu d'aplicar a les peticions que li arriben al gateway des d'internet.

Degut a la configuració de xarxa que tenim, considereu que la *realMachine* està a Internet.
Així doncs per provar la configuració executeu el *traceroute* des d'aquesta màquina.

5 Entrega i avaluació

- L'avaluació de la pràctica es farà la setmana del **15/03**.
- Caldrà que creeu els fitxers **gateway.sh** i **client.sh** amb les comandes de `iptables` que us calguin per complir amb els requeriments de la pràctica.

  Si us calen més scripts, creeu un fitxer `README.txt` a on expliqueu per a què utilitzeu els scripts.

  Tots aquests fitxers els heu de deixar en el vostre compte de pràctiques, en el directori `entregues/iptables/final`, una hora abans de la sessió de pràctiques i no els heu de borrar després de l'entrega.
- Per la part no obligatòria cal crear els scripts: **llista_negra.sh**, **llista_blanca.sh**, **deic_rediris.sh** i **traceroute.sh**.
- Haureu de desar l'informe final en el directori `entregues/iptables/informe` la setmana del **22/03** una hora abans de la sessió de pràctiques.
- La nota de la pràctica es calcularà a partir de la taula 2:

Taula 2: *Avaluació de la pràctica.*

part	*nota sobre 10 + 1*
Part obligatoria	6.5
Previ(extra)	1
Llistes negra/blanca	1
Restricció d'accés	0.25
Blocar el traceroute	0.25
Informe	2

6 Altres aspectes, recomanacions, ...

- La imatge de la màquina virtual esta al directori:

  `/opt/vmware/Debian-7.x_32-bit`

  Per a iniciar-la, cal que obriu el fitxer `Debian-7.x 32-bit.vmx` des de la línia de comandes:

  ```
  vmplayer Debian-7.x\ 32-bit.vmx &
  ```

- S'ha d'iniciar sessió a la màquina virtual com a `root` on la password és "root".

- El servidor HTTP que hi ha instal.lat en el gateway serveix els fitxers que hi hagin en el directori `/tmp/pycore.xxxx/gateway.conf/var.www` (on `xxxx` serà l'identificador del CORE per a l'emulació actual).

- Tots utilitzareu la mateixa màquina virtual. No us deixeu pràctiques, scripts, ... a les mateixes.

- Recordeu també que quan una emulació es para, tots els fitxers desats en els linux containers dels nodes s'esborren. Us pot servir per a començar la pràctica de nou. **Recordeu-vos però de passar els scripts que vulgueu conservar abans de parar la simulació al vostre compte**.

- La comanda `iptables-save` mostra per pantalla la configuració de totes les taules de `iptables`. Us pot ser d'utilitat.

  Podeu volcar aquesta sortida cap a un fitxer i a posteriori restaurar-ho amb la comanda `iptables-restore`:

  ```
  iptables-save > iptables.conf
  iptables-restore iptables.conf
  ```

  Podeu utilitzar aquestes comandes i el fitxer `iptables.conf` en els scripts de configuració `gateway.sh` i `client.sh`.

- A continuació us indiquem com ho podeu fer per copiar els fitxers del vostre compte de pràctiques cap al **gateway|workstation** i a la inversa. Cal que hagueu iniciat la simulació amb el CORE.

  Noteu que un cop l'emulació està iniciada, en la màquina virtual s'han creat els directoris:

Per al gateway `/tmp/pycore.XXXX/gateway.conf`

Per a les workstations `/tmp/pycore.XXXX/workstation-nX.conf`

- **Per copiar els fitxers que tenim en el nostre compte de pràctiques cap al `gateway|workstation` un cop l'emulació està iniciada**:
  1. Obriu un terminal en la màquina virtual `Debian`.
  2. Executeu la comanda sense les cometes dobles:
     `"scp tai-a1@deic-dc1.uab.cat:iptables/*.sh ."`
  3. Per a transferir aquest fitxer cap al gateway o workstation ho podeu fer de forma visual o per comandes:

     De forma visual (a) Obriu en la màquina virtual el gestor de fitxers. Cliqueu en en 'Systema de Fitxers'. Navegueu fins el directory `/root/`. En aquest directori és a on tindreu els fitxers que heu copiat del vostre comtpe de pràctiques.

     (b) Des de l'emulador, obriu una consola en el `gateway/workstation` amb doble click sobre la icona del node.

     (c) Des de l'aplicació de gestió de fitxers arrossegueu el fitxer que voleu copiar a la consola del `gateway/workstation`. Us apareixerà en la consola la ruta d'origen del fitxer.

     (d) Des de la consola del `gateway/workstation` afegiu a la ruta la comanda per copiar el fitxer en el directori actual:
     `cp /root/XXX.sh .`
     No us oblideu del punt final!

     Per línia de comandes Des del terminal de la màquina virtual a on us heu copiat els fitxers del vostre compte de pràctiques executeu:
     `cp *.sh /tmp/pycore.40397/gateway.conf/`
     i ja està.

- **Per desar la feina que tenim en el `gateway/workstation` cap al vostre compte de pratiques**, directori iptables, fer:
  1. Obriu un terminal en el `gateway/workstation` del CORE.
  2. Executeu la comanda sense les cometes dobles:
     `"scp *.sh tai-a1@deic-dc1.uab.cat:iptables"`

  Si voleu transferir els fitxers cap a la màquina virtual, ho podeu fer visualment amb el gestor de fitxers o bé executant la comanda:

  `cp *.sh /root`

- Si teniu algun problema amb alguna de les màquines virtuals reinicieu la màquina del laboratori.
- Per aplicar les configuracions que us demanem, recordeu que no s'ha de necessitar reinicialitzar la màquina virtual ni cap dels `containers` del CORE en cap moment.
- Quan hagueu acabat de treballar amb la màquina virtual, amb la `Debian`, penseu que cal aturar degudament el seu sistema operatiu. Cal que executeu la seqüència: `Ctr+Alt+Supr`. Quan s'hagi acabat el procés d'aturada del sistema operatiu, abans de que torni a carregar-se, tanqueu l'aplicació *vmplayer*.

Referències

[1] **Manual d'iptables.** Manual del sistema de iptables accessible a partir de la comanda "man 8 iptables".

[2] **Manual de rsyslogd.** Manual del sistema de rsyslog accessible a partir de la comanda "man 8 rsyslogd".

[3] **Iptables Tutorial 1.2.2.** URL: *http://www.frozentux.net/documents/iptables-tutorial/*. Tutorial de Iptables.

[4] **VMWare homepage.** URL: *http://www.vmware.com*. Pàgina web oficial de l'empresa vmware.

[5] **Core homepage** URL: *http://www.nrl.navy.mil/itd/ncs/products/core*. Pàgina web oficial del simulador `CORE`.