Tecnologies Avançades d'Internet

Pràctica 3: *Encapsulament i xifratge d'informació*

curs 2016-2017

1 Objectius

El principal objectiu d'aquesta pràctica és entendre el funcionament de l'encapsulació d'informació mitjançant l'ús de túnels i de quina forma la informació es transmet d'un punt a un altre.

Aquesta pràctica tindrà dues tasques principals a realitzar:

- Encapsulació sense xifratge.
- Encapsulació amb xifratge de les dades a nivell de transport.
- (Opcional) Desxifratge d'un paquet xifrat a partir de la clau privada.

En aquesta pràctica continuarem amb l'ús de `iproute2`[4] ja que és una eina molt versàtil que ens permet fer multitud de tasques, entre elles la creació de túnels. Per a la part de xifratge de les dades s'utilitzarà `IPSEC`[6], concretament les arquitectures de seguretat `AH` i `ESP`.

Serà important, per tant, distingir quines arquitectures haurem d'utilitzar per a aconseguir els objectius establerts (dades xifrades, autèntiques o ambdues).

Aquesta pràctica pretén aprofundir en els coneixements d'encaminament, protecció i validació de la informació encapsulada.

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[1] 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[5] són molt més lleugeres reduint així el consum de recursos.

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

Els contenidors de CORE es podran trobar, sempre que s'hagi iniciat prèviament l'emulació, en el directori de la màquina virtual: */tmp/pycore.xxxx* on *xxxx* serà l'identificació 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 Principals aspectes a considerar

Tingueu en compte els següents aspectes:

- 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 demanada, excepte si s'especifica el contrari.
- Assegureu-vos d'utilitzar sempre l'escenari de CORE adient per cada pràctica, en aquest cas s'anomena **p3.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, obriu un terminal i executeu la comanda:

  `wget http://deic-dc0.uab.cat/tai/tunneling/p3.imn`
- 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

Una empresa ha decidit utilitzar IPv6 per a la seva xarxa local donat la multitud d'avantatges que aporta aquesta versió del protocol enfront de IPv4.

Els caps de l'empresa, han decidit que volen connectar les seus d'Espanya i Anglaterra utilitzant IPv6.

Com s'ha explicat a classe, la transició de IPv4 a IPv6 és molt lenta, així que s'ha decidit utilitzar un mètode d'encapsulament basat en túnels per tal de poder enviar paquets IPv6 entre les dues seus de l'empresa, utilitzant la infraestructura d'Internet existent (IPv4). És a dir, utilitzar IPv6 sobre IPv4.

Com a primer pas els caps de l'empresa volen poder tenir un túnel operatiu (sense xifrar les dades). Per a més endavant poder-hi afegir el xifratge a nivell de transport.

A continuació es presenta l'escenari on es duran a terme les accions d'aquesta pràctica.

3.1 Esquema principal

Tal i com veiem a la figura 1 el muntatge realitzat a l'escenari **p3.imn** consisteix en dues xarxes locals (seus de l'empresa) formades per un ordinador client i un router que es comuniquen mitjançant IPv6. A la vegada, aquests routers tenen una interfície de xarxa IPv4 connectada directament a Internet (routers *dual stack*).

Es representa internet a través dels tres routers (`ISPs`). Podem veure com les IPs d'aquests routers són IPv4.

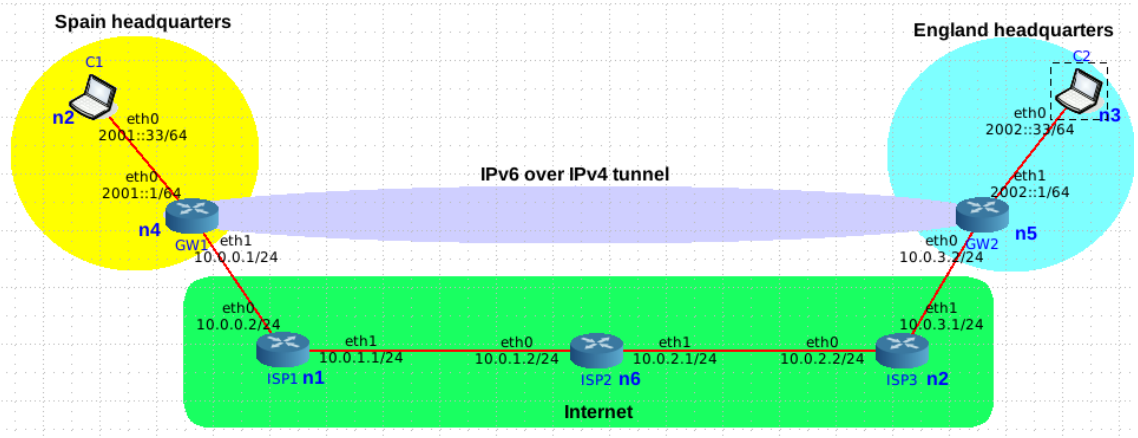

Figura 1: *Escenari de la pràctica.*

3.2 Funcionalitat que hem d'implementar

La pràctica consisteix en realitzar una configuració utilitzant `iproute2` i `IPSEC` que permeti el següent:

1 Crear un túnel (**sense xifrar**) entre els dos routers de cadascuna de les seus, és a dir, entre el `GW1` i `GW2` amb la finalitat que els clients `C1` i `C2` es puguin intercanviar missatges.

2 Analitzar i comentar el format (i les seves diferències) d'un missatge ICMPv6 de `C1` a `C2` interceptat a `GW1 (eth0)` i `ISP2`.

3 Xifrar tot el tràfic a nivell de transport amb origen a `GW1` i destí `GW2` i viceversa. S'ha d'utilitzar l'eina IPSEC[1].

4 Analitzar i comentar el format (i les seves diferències) d'un missatge ICMPv6 de `C1` a `C2` interceptat a `ISP3` i `GW2 (eth1)`.

3.3 Passos a realitzar

És important tenir clar que **no** hem de modificar els fitxers de configuració del sistema ni cap configuració gràfica del CORE; en reiniciar, el sistema perdrà totes les modificacions que haguem realitzat[2].

Els passos que s'haurien d'anar seguint per realitzar correctament la pràctica són:

1. CREAR EL TÚNEL

1. S'ha de crear un túnel **punt a punt** `IPv6 sobre IP` sense xifrat, entre `GW1` i `GW2`. Aquest túnel ha de permetre la comunicació de dades IPv6 utilitzant la infrastructura IPv4 d'Internet.
   Tingueu en compte les següents indicacions i seguiu les següents passes:
   (a) S'ha d'utilitzar l'eina `iproute2` per a crear el túnel:
   Les referències [7] i [8] (secció 3) poden ser-vos de molta utilitat.
   Comanda: `ip t a ...`

   Per comprovar que els tunnels s'han creat correctament podeu utilitzar les comandes:
   `ip t s` (ip tunnel show)
   `ip a s` (p address show)

   Noteu que acabeu de crear un tunnel, que es tracta com a una nova interfíce!
   (b) Reviseu l'estat de la nova interfície:
   Comanda: `ip a s`

   Noteu que la interfície del tunel està `DOWN`. Per poder-la utilitzar cal posar-la a `UP`:
   Comanda: `ip link set ...`

   (c) Cal que especifiqueu una ruta per poder encaminar el tràfic generat en la xarxa `IPV6` de la seu espanyola cap a la xarxa `IPV6` de la seu de UK.

   Us cal modificar la taula d'encaminament per afegir una ruta `IPV6`.
   Comanda: `ip -6 r ...`.

   (d) Per provar que el túnel està ben configurat podeu fer un ping, versió 6, des de `C1` a `C2` i veure que funciona correctament:
   `$ ping6 2002::33`
   No us oblideu de realitzar les proves en les dues direccions!
2. Intercepteu un datagrama generat amb la comanda `ping6`, des de `C1`, en els punts `GW1 (eth0)` i `ISP2 (eth0)`, comproveu les principals diferències entre ambdós.

   NOTA: En l'informe haureu d'explicar les diferències principals entre aquests dos paquets interceptats i el perquè d'aquestes difències.
   Us serà d'utilitat dibuixar l'encapsulació de manera esquemàtica per a utilitzar-la de suport en la vostra explicació.
3. Caldrà que feu els escripts: **`setupTunnelGW1.sh`** i **`setupTunnelGW2.sh`** amb les comandes per crear els tunnels.

[1] Necessitareu instalůlar l'eina IPSEC amb la següent comanda dintre de la màquina virtual: `apt-get install ipsec-tools`.
[2] Si la màquina virtual es queda desconfigurada o porta problemes, reinicieu la màquina **real**: Ctrl Alt F2 i Ctrl Alt Supr

2. CONFIGURACIÓ IPSEC

1. Ara, configurarem IPSEC per a realitzar una **comunicació confidencial** entre `GW1` i `GW2`.

   La configuració d'IPSEC s'especifica, normalment, en el fitxer `/etc/ipsec-tools.conf`.

   Trobareu la informació que necessiteu en la secció 7.1 de [4]. Podeu utilitzar el manual de `setkey`[9] per conéixer més detalls de les comandes que us calen per configurar `IPSEC`.

   Seguiu les següents passes:

   (a) Assegureu-vos que heu instal.lat el paquet `IPSEC`. Per a instal.lar-lo cal que executeu la comanda:
   `apt-get install ipsec-tools`

   (b) Com que els `containers` de CORE comparteixen els arxius de configuració de `/etc`, crearem els fitxers de configuració d'`IPSEC` amb els noms: **`ipsec-GW1.conf`** i **`ipsec-GW2.conf`** al `home` dels *containers* dels routers `GW1` i `GW2` respectivament.

   (c) Inicieu els fitxers de configuració amb les comandes necessàries per eliminar:
   - La `SAD`, *Security Asssociation Database*: `flush;`
   - La `SPD`, *Security Policy Database*: `spdflush;`

   (d) Afegiu en els fitxers de configuració:
   - En en fitxer de configuració de `GW1`, cal que afegiu la comanda per crear la `SA`, *Security Association*, per xifrar el tràfic de `GW1` cap a `GW2`.
     Comanda:
     `add` *`src dest protocol spi`* `-E` *`algorithm encription_key`*`;`
     Els paràmetres en cursiva cal que els canvieu per valors.

     Noteu que en l'altre extem, a `GW2`, en el fitxer de configuració, heu de crear la mateixa *security association*, ja que quan `GW2` llegeixi la capçalera `ESP` del datagrama enviat per `GW1`, allà hi ha el *Security Parameter Index*, *spi*, amb les dades de l'esquema de seguretat per poder desxifrar les dades del datagrama.
   - En el fitxer de configuració de `GW1`, equivalent al que acabem de comentar, cal que afegiu la `SA` que heu creat en `GW2` per xirar el tràfic de `GW2` cap a `GW1`. Així quan rebeu tràfic de `GW2` sapigueu, tot utilitzant el `spi` de la capçalera `ESP`, quines són les dades de l'esquema de seguretat per desxifrar les dades del datagrama.
   - La comanda per indicar al kernel que voleu xifrar les dades de la comunicació entre `GW1` i `GW2`. El kernel sap trobar quina és la `SA`, de les que heu definit, que cal utilitzar.
     Esteu definint la `SP`, *Security Policy*. Assegureu-vos que especifiqueu correctament la *direction*, amb el paràmetre `-P`.
     Comanda:
     `spdadd` *`src_range dest_range protocol_upper_layer`* `-P` *`direction`* `ipsec esp/transport//require;`
   - La comanda per indicar al kernel que no voleu acceptar tràfic de `GW2` que us arribi sense xifrar. Haureu de definir una nova `SP`.
     Haureu d'utilitzar la comanda anterior. Pareu atenció amb el valor del paràmetre `-P`, *direction*.

   Heu de replicar la configuració anterior, amb els canvis necessaris, en els dos gateways.

   (e) Per carregar aquests fitxers de configuració podeu utilitzar la següent comanda:
   `$ setkey -f <script_configuracio.conf>`

   (f) Per provar que el xifratge funciona correctament executeu un `ping`, versió 6, des de `C1` a `C2`. Esnifeu la xarxa, en qualsevol punt intermedi de la comunicació. Hauríeu de veure que hi ha un paquet xifrat i per tant no en podeu conèixer les dades.

2. Intercepteu un datagrama a `GW1 (eth0)` i a `ISP2` generat amb un `ping6` de `C1` a `C2`. Comproveu quines són les diferències principals entre ambdós.
   NOTA: En l'informe haureu d'explicar les diferències principals en aquests dos paquets interceptats i el perquè d'aquest comportament.

3.4 Part Opcional

Per realitzar la part opcional d'aquesta pràctica no és necessari canviar d'escenari. Podem utilitzar el mateix que per a la part obligatòria.

3.4.1 Desxifrar un paquet xifrat tenint la clau privada

Un atacant ha aconseguit obtenir la informació de la clau privada de l'empresa situada a Espanya utilitzada per a xifrar els paquets amb destí la seu d'Anglaterra. Aquestes són les dades de l'esquema de seguretat emprat pel xifrat:

```
$ ip xfrm state

  src 10.0.0.1 dst 10.0.3.2
    proto esp spi 0x00003d55 reqid 0 mode transport
    replay-window 0
    enc cbc(des3_ede) 0x33444553556e636f7665726564506173737776f7264455350
    sel src 0.0.0.0/0 dst 0.0.0.0/0
```

A més, us ha enviat un paquet per a que col·laboreu a extreure'n la informació. La informació per desxifrar és una traça de `Wireshark`. Podreu obrir aquesta traça amb el `Wireshark` i configurar-lo per a desxifrar-ne les dades.

La traça us la podeu descarregar de la URL:
`wget http://deic-dc0.uab.cat/tai/tunneling/interceptedPacket`

Seguiu les següents passes per configurar el `wireshark` per desxifrar el datagrama:

1. Obriu el fitxer amb el datagrama xifrat.
2. Aneu a l'opció de menú: `Edit -> Preferences -> Protocols`.
3. Seleccioneu el protocol `ESP`. Volem configurar certs aspectes d'aquest protocol per ser capaços de desxifrar les dades del datagrama.
4. Afegiu tantes `SA`'s com us calguin per indicar les dades de seguretat necessàries per desxifrar el datagrama.
5. Un cop afegiu les `SA`'s, automàticament, el `wireshark` us mostrarà les capçaleres de transport i les dades, tot desxifrat.

Esbrineu quin era el missatge xifrat.

NOTA: En l'informe haureu de fer una captura de pantalla mostrant les diferents SA's que us han calgut per desxifrar el datagrama, tot comentant tots els camps de cada una d'elles.
Aquesta part opcional està valorada amb **0.75** punts.

3.4.2 Establir una comunicació autèntica i segura

Com ja sabeu, amb IPSEC no només es pot xifrar el missatge per a transmetre-ho d'una manera segura sino que també es pot autenticar per a assegurar-nos que aquest missatge no ha sigut modificat i l'envia aquell que ho diu.

Cal que modifiqueu el fitxer de configiguració de `ipsec`, per afegir el protocol `ah`, a més del `esp` que ja heu configurat.

Heu de seguir les passes de la configuració `IPSEC` afegint les `SA`'s, i modificant les `SP`'s associades al protocol `ah`.

Pel que fa a les `SP`'s no cal que afegiu de noves. Cal que compeleteu la que ja teniu configurada:

```
spdadd src_range dest_range protocol_upper_layer -P direction ipsec
esp/transport//require
ah/transport//require;
```

Aquesta part opcional està valorada amb 0.75 punts.

4 Altres aspectes, recomanacions, ...

- La imatge de la màquina virtual esta a `/opt/vmware/Debian-7.x_32-bit`. Per a iniciar aquesta, cal que obriu el fitxer `Debian-7.x 32-bit.vmx`.
- S'ha d'iniciar sessió a la màquina virtual com a `root` on la password és "root".
- 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 de les 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**.
- Quan hagueu acabat de treballar amb les màquines virtuals, penseu que cal aturar degudament el sistema operatiu que estan executant. 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*.
- Per poder copiar els fitxers als `gateways` del CORE, amb l'emulació iniciada podeu utilitzar *ssh* (*scp* o *sftp*) des del vostre compte de `tai`.

  Exemples per copiar els scripts:

  - Per copiar els fitxers que tenim en el nostre compte de pràctiques cap al `gateway`:
    1. Aneu al directori `GW1.conf` del CORE.
    2. Executeu la comanda sense les cometes dobles:
       `"scp tai-a1@deic-dc1:tunneling/* tunneling/."`.
  - Per desar la feina que tenim en el `gateway` cap la màquina real del laboratori, directori iptables, fer:
    1. Aneu al directori `GW1.conf` del CORE.
    2. Executeu la comanda sense les cometes dobles:
       `"scp tunneling/* tai-a1@deic-dc1:tunneling"`.
- 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.

5 Entrega i avaluació

- L'avaluació de la pràctica es farà la setmana del **29/05**.
- Caldrà que deseu tots els scripts i fitxers de configuració en el vostre compte de pràctiques, en el directori `entregues/tunneling/final` i no els heu de borrar després de l'entrega. Si us calen més scripts, creeu un fitxer `README.txt` a on expliqueu per a què utilitzeu els scripts.
- L'entrega de l'informe serà, per tothom, el dia **5/6**, a les **23:00h**.

  Cal que el deseu en el directori: `entregues/tunneling/informe`
- La nota de la pràctica es calcularà a partir de la taula 1:

Taula 1: *Avaluació de la pràctica.*

part	*nota sobre 10*
Part obligatoria + previ	6
Part opcional 1	0.75
Part opcional 2	0.75
Informe	2.5

Referències

[1] **CORE Homepage.** URL: *http://www.nrl.navy.mil/itd/ncs/products/core*. Pàgina web oficial del CORE..

[2] **IP command reference.** URL: *http://linux-ip.net/gl/ip-cref/ip-cref.html*. Manual de la comanda ip.

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

[4] **Linux Advanced Routing & Traffic Control.** URL: *http://www.lartc.org*. HOWTO de Linux Advanced Routing & Traffic Control utilitzant l'infraestructura de iproute2.

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

[6] **Manual de ipsec** accessible a partir de la comanda "man ipsec".

[7] **http://linux-ip.net/gl/ip-tunnels/ip-tunnels-node4.html**

[8] **Configuring tunnels with iproute2**. URL: *http://www.deepspace6.net/docs/iproute2tunnel-en.html#id2808093*

[9] **Manual del setkey** accessible a partir de la comanda "man setkey".