Xarxes: Pràctica 3, Ànalisi de trànsit

César Fernàndez, Enric Guitart, Carles Mateu

Maig 2020

Enunciat

L'anàlisi de trànsit és una tasca que permet obtenir informació d'una xarxa, detectar problemes actuals i prevenir problemes futurs. Per dur a terme aquesta tasca cal tenir clars els conceptes teòrics sobre els mecanismes de comunicació de la xarxa a analitzar i disposar d'eines que permetin la captura i visualització de trànsit. Per aquesta pràctica s'emprarà com a eina de captura i visualització Wireshak. Whireshark és una eina de captura i visualització, també s'anomenen analitzadors de protocols de xarxa (*Network protocol analyzer*), de lliure distribució que podeu trobar a http://www.wireshark.org/.

Les dades que cal analitzar es proporcionen en un arxiu (CapturaPractica3.pcapng.gz) que trobareu en el campus virtual (Recursos → Practiques → Enunciats). Es tracta d'un arxiu comprimit que conté una part de la captura de trànsit d'una xarxa en producció.

Tasques

1. **Caracterització de la xarxa**

   Determineu les característiques principals de la xarxa on s'han capturat els paquets. Com a mínim cal que especifiqueu:

   - Tipus d'adreçament de la capa de xarxa (classe A, B, C,...)
   - Adreça de xarxa
   - Adreça de broadcast
   - Porta d'enllaç de la xarxa

   Per cada característica de la xarxa cal que justifiqueu la vostra resposta indicant el procediment emprat.

2. **Anàlisi nivells d'enllaç i de xarxa**

   En aquest apartat l'anàlisi se centra en l'entramat de nivell 2 i el protocol que encapsula. Cal que determineu:

   - Els protocols encapsulats en les trames de nivell 2. Per cada protocol cal que especifiqueu el valor del camp `[type]` (si existeix) de la trama de nivell 2 i que aporteu l'estructura de trama del protocol encapsulat.
   - L'adreça IPv4 (si la té) de cada equip que empra el protocol MDNS per IPv6.
   - Les adreces multicast que hi ha en la captura. Per cada adreça doneu el protocol d'aplicació que estan emprant juntament amb una petita descripció de la seva utilitat.
   - Una gràfica de distribució dels protocols de nivell 3 (gràfica de pastís).

3. **Anàlisi nivell de transport**

Abans d'iniciar l'anàlisi del nivell de transport caldrà desestimar els següents paquets i protocols:

- El paquets que tenen com a destí l'adreça broadcast de nivell 2
- Els paquets d'IPv6
- Els paquets de multicast
- Els protocols ARP, DNS i NTP

Del trànsit restant cal que determineu:

- Les comunicacions TCP que no s'han dut a terme, indicant en cada cas el motiu. Doneu una taula amb IP-Origen, Port-Origen, IP-Destí, Port-Destí, Motiu-Fallida.
- Les comunicacions TCP completes que hi ha en la captura, classificades en dos apartats:
  (a) Comunicacions HTTP i HTTPS: Per aquestes comunicacions no s'han de considerar les connexions realitzades per cada element de la pàgina. S'ha de considerar com una única comunicació les connexions des d'un mateix origen (adreça IP) cap al mateix destí (adreça IP) i port 80 ò 443. Aporteu una taula amb els camps IP-Origen i IP-Destí on es mostrin totes aquestes comunicacions.
  (b) Resta de comunicacions: Doneu una taula amb IP-Origen, Port-Origen, MTU-Origen, Finestra-Origen-Inicial, IP-Destí, Port-Destí, MTU-Destí, Finestra-Destí-Inicial
- Les comunicacions UDP que podeu assegurar que no s'han dut a terme. Doneu una taula amb IP-Origen, Port-Origen, IP-Destí, Port-Destí, Motiu-Fallida.
- Les comunicacions UDP que s'han dut a terme en la captura. Doneu una taula amb IP-Origen, Port-Origen, IP-Destí Port-Destí.
- Per les comunicacions TCP:
  (a) 172.16.0.105 $\Leftrightarrow$ 172.16.0.121
  (b) 172.16.0.112 $\Leftrightarrow$ 172.16.0.115
  (c) 172.16.0.117 $\Leftrightarrow$ 172.16.0.124

  determineu:
  - Els paquets, identificats per el número que li assigna Wireshark en la captura inicial, que formen part de l'apertura de la connexió i el tancament.
  - El nombre de bytes d'usuari (aplicació) i totals transmesos en cada sentit de la comunicació.
  - El cabal brut i útil per cada sentit de la comunicació.
  - Les opcions TCP que s'han intercanviat en la fase de connexió i el seu valor. Especifiqueu per cada opció la seva utilitat.
  - El nombre de seqüència inicial real del transmissor i del receptor.
- La gràfica del trànsit en el temps (mesurat en paquets) on figuri el trànsit total i el dels dos protocols de transport de TCP/IP.

Lliurament

- **Documentació**

  Cada alumne ha de confeccionar un informe de la pràctica on es reflecteixin els resultats de les tasques d'anàlisi i les conclusions extretes. Tots els resultats i conclusions han de ser justificats de la manera més clara possible, aportant els procediments emprats i els filtres aplicats.

  Aquest document ha de complir les següents condicions generals:

  - Una bona estructuració.
  - Un format dels elements de text correctes.
  - Un contingut clar i una redacció correcta (no s'acceptaran errades ortogràfiques ni abreviatures o símbols per substituir paraules).

  El document es lliurarà en format PDF per el campus virtual (`cv.udl.es - Activitats -`).

  El nom del document ha de tenir l'estructura:

  XARXES-P3-*Cognom1Cognom2***.pdf**

  IMPORTANT: La documentació que no assoleixi aquests requisits no serà avaluada.

- **Termini**

  El termini per rebre la documentació relacionada amb aquesta pràctica finalitza el 05 de Juny de 2020.