P2-Anàlisis de serveis TCP/IP

INTE – Internet

09/11/2018

Departament d'Enginyeria Telemàtica
Rafael Vidal Ferré

Contingut

1 Introducció

En aquesta segona pràctica, un cop ja sabem con dissenyar i configurar una xarxa TCP/IP, toca entrar en els serveis que podríem proporcionar. Això implica fixar-se en els protocols d'aplicació que fan servir aquests serveis i, de retruc, en els de transport necessaris per a que els d'aplicació puguin fer la seva tasca.

Abans però ens fixarem amb la interacció entre els processos associats a aquest serveis, ja siguin a les màquines que fan de clients com a les que fan de servidors. Així, ens fixarem en els ports i les connexions associades aquests serveis. Ho farem a nivell local i també a nivell remot, fent ús de la tècnica coneguda com escaneig de ports. Després, examinarem el protocol de transport TCP. Primer ens fixarem en com conèixer algun dels paràmetres que controlen el seu funcionament. Seguidament, n'estudiarem els mecanismes d'establiment de connexió, control de flux i control d'errors. Per a fer-ho, generarem trànsit TCP amb aplicacions que també estudiarem. Primer ho farem amb Telnet i FTP, dos protocols de capa d'aplicació amb dues filosofies diferents de com transportar les dades i la informació de control. Finalment, estudiarem la Web i concretament, el protocol HTTP.

2 Objectius

En acabar aquesta pràctica sereu capaços de:

- Identificar els protocols de transport i ports que fan servir les aplicacions/serveis que utilitzem habitualment
- Descobrir els serveis que està corrent un equip mitjançant la tècnica de l'escaneig de ports
- Entendre el funcionament del protocol TCP a nivell d'establiment de connexió, control de flux i control d'errors, identificant paràmetres com ara: flags, nº de seqüència, nº d'ACK, finestra de transmissió o RTO.
- Entendre i identificar els estats pels que passa una connexió TCP
- Entendre el funcionament dels protocols Telnet, FTP i HTTP
- Entendre la interacció entre els protocols Telnet, FTP i HTTP i TCP
- Utilitzar eines bàsiques per obtenir els principals paràmetres de connexions TCP/IP (netstat o ss) i fer un escaneig de ports (nmap)
- Utilitzar eines específiques per analitzar protocols de transport i aplicació (diferents tipus d'estadístiques de Wireshark)

3 Material

Per parelles, utilitzareu el següent material

- 1 router Mikrotik hAP ac lite
- 2 PCs del laboratori (Windows i Linux)
- 1 portàtil amb Wi-Fi (es necessitaran permisos d'administrador)
- 1 smartphone
- Cables UTP (3 per parella)

3.1 Software necessari

PCs del laboratori:

- Cal descarregar-se la imatge de la màquina virtual VM-INTE i guardar-ne una còpia.

Smartphone:

- Cal instal·lar les aplicacions:
    - IP Tools per Android o iOS
    - Network Connections per Android (no he trobat quelcom semblant per iOS)

4 Organització

Treballareu en parelles que mantindreu al llarg de les 3 sessions que dura la pràctica:

- S1-Serveis, ports i connexions: anàlisi en local i escaneig de ports
- S2-Anàlisis dels protocols Telnet i FTP
- S3-Anàlisi del protocol HTTP

Per a cada sessió es publicarà un document a mode de guia anomenat "Pla de treball". En aquest document s'indicaran tan les eines com els passos a realitzar al llarg de la sessió.

5 Avaluació

Al final de cada sessió s'obrirà un qüestionari a atenea que s'ha de respondre individualment. La seva finalitat es permetre-us comprovar si heu entès els conceptes que s'han treballat durant la sessió.

Per a que aquesta qüestionaris siguin útils cal:

- Llegir-los abans de fer la pràctica
- Mentre feu la pràctica, cal que relacioneu les seves preguntes amb el que esteu fent. No us esteu de preguntar si quelcom no us queda clar.
- Contestar-los abans de començar la següent sessió de laboratori
- Anar a consultes si no es veu clara la resposta a alguna de les preguntes.

Important:

- El qüestionari s'ha de lliurar el dia abans de les 21 hores de la sessió de laboratori següent (els que tenen laboratori el dilluns tindran com a límit el diumenge a les 21 hores i els del divendres, dijous a les 21 hores).
- El nom del arxiu a entregar del qüestionari ha de tenir el següent format de nom: P1_SX_NomCognom1_NomCognom2 (X s'ha de canviar per el número de sessió corresponent). El document ha de ser en format PFD.

6 Referències

De manera general, només us farà falta consultar/repassar les transparències de teoria associades a cada pràctica. Per aquesta segona pràctica aquestes transparències són les corresponents als temes:

1. Introducció
4. Lliurament d'informació
5. Serveis

Per a consultes específiques per ampliar coneixements sobre l'equipament i el software que utilitzarem us poden ser útils els següents enllaços:

- Router Mikrotik RB951G-2HnD (especificacions i suport). Enllaç: https://mikrotik.com/product/RB952Ui-5ac2nD
- Wireshark User's Guide. Enllaç: https://www.wireshark.org/docs/wsug_html_chunked/ Informació relativa a estadístiques que utilitzarem en aquesta pràctica:
    - https://www.wireshark.org/docs/wsug_html_chunked/ChStatTCPStreamGraphs.html
    - https://www.wireshark.org/docs/wsug_html_chunked/ChStatFlowGraph.html
    - https://www.wireshark.org/docs/wsug_html_chunked/ChStatHTTP.html