P3-Tallafocs: disseny i configuració de polítiques de seguretat en tallafocs

INTE – Internet

25/11/2018

Departament d'Enginyeria Telemàtica
Rafael Vidal Ferré

Contingut

1 Introducció

En aquesta tercera pràctica, un cop ja sabem con dissenyar i configurar una xarxa TCP/IP i coneixem com funcionen a nivell de comunicació alguns dels serveis, és hora de fixar-nos en la seguretat. Concretament en com limitar les comunicacions per a reduir el risc d'atacs utilitzant tallafocs.

Per a fer-ho, utilitzarem l'escenari de la pràctica 1. A partir del pla d'adreçament que es va fer i dels requeriments de comunicació per a cada xarxa que es proporcionaran, es derivaran les polítiques de filtrat de paquets que després seran configurades als routers de l'escenari, que inclouen la funcionalitat de tallafocs.

2 Objectius

En acabar aquesta pràctica sereu capaços de:

- A partir dels requeriments de comunicació (serveis que es volen permetre o prohibir) identificar els patrons de trànsit (protocol de transport i ports) i les accions a realitzar (permetre o denegar)
- Traslladar aquests patrons i accions a regles compatibles per un tallafocs basat en iptables
- Interpretar la configuració de partida d'un tallafocs com a primer pas per a modificar-la
- Afegir regles a un tallafocs basat en iptables i comprovar-ne el seu funcionament

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

No farà falta cap software específic. Només un navegador per a configurar els routers Mikrotik i una mica d'imaginació (ping, nslookup, Wireshark,...) per a comprovar que la configuració dels tallafocs és la correcta.

4 Organització

Treballareu en parelles que mantindreu al llarg de les 2 sessions que dura la pràctica:

- S1-Disseny de les polítiques de seguretat
- S2-Configuració i test de les polítiques de seguretat

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 per parellas. 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:

2. Adreçament
3. Lliurament de paquets
4. Encaminament
5. Lliurament d’informació
6. Serveis
7. Seguretat

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

- Router Mikrotik Mikrotik hAP ac lite (especificacions i suport). Enllaç: https://mikrotik.com/product/RB952Ui-5ac2nD
    - Informació específica sobre filtrat de paquets https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter