UNIVERSIDAD DE CASTILLA-LA MANCHA
ESCUELA SUPERIOR DE INFORMÁTICA

Topología Segura

Práctica 4

Marcos López Sobrino

Seguridad en Redes
17/01/2019

Introducción

Esta práctica trata del diseño de implementación de una topología de red segura. En este documento, se expone la política de seguridad que se ha decidido seguir.

Para la construcción del escenario se ha usado *Vagrant*, y las máquinas se han aprovisionado con Ansible; dichas máquinas son:

- Un **cliente en la red privada MZ**, con IP assignada por DHCP por el router (el DHCP implementado con *dnsmasq*)
- Un **servidor en la red DMZ**, con IP estática y que proporciona un solo servicio, web, implementado con A*pache*.
- Un **router**, que tiene una interfaz en modo puente, de tal manera que pueda salir a Internet. Este router proporciona los servicios de DHCP, caché DNS, y *firewall* con *iptables*.

Política de seguridad

Se ha seguido una política de descarte por defecto, lo que quiere decir que los paquetes que lleguen y no cumplan con alguna de las reglas, serán descartados.

A continuación, se muestra una lista de las acciones permitidas para la configuración de reglas establecida:

- Ping desde la red MZ a la red DMZ.
- Ping desde la red MZ al exterior (Internet).
- SSH desde la red MZ a la red DMZ.
- Acceso al servidor web ubicado en la red DMZ:
  - Desde la red MZ.
  - Desde el exterior.
- Acceso a Internet desde la MZ.
- Servicio DNS para la red MZ.
- Servicio DHCP para los hosts de la red MZ.

No se permite el acceso desde Internet a la red MZ, pero sí a la DMZ, aunque solamente en el puerto 80 para acceder. Tampoco se permite el acceso por SSH desde la red MZ al exterior o al router, ni la recepción de paquetes ICMP por parte de este.