SCHOOL OF HACKING 2015
Reto Comunicaciones Seguras

INSTRUCCIONES

El reto se establece desde el jueves, 9 de abril, a partir de las 21 horas. Desde ese momento se dispondrá de dos días para su resolución y entrega de las soluciones, que finalizará el 11 de abril a las 24:00 horas.

Hay dos ejercicios que puntuarán para la consecución del reto. Cuando el participante crea haber resuelto estos ejercicios deberá mandar un correo electrónico a la dirección afdiaz@ugr.es conteniendo de forma breve y clara la solución de los ejercicios. Sólo se aceptará una una solución por participante. La puntuación se obtendrá por el orden en el que se remiten las soluciones correctas.

EJERCICIOS

1.- (10 PUNTOS) Tenemos una configuración con una máquina cliente (nodo_a) y queremos acceder a un nodo remoto (nodo_c) a través de un nodo frontend (nodo_b). Para las máquinas nodo_a y nodo_c tenemos privilegios de root, pero para la máquina frontend (nodo_b) NO tenemos privilegios de root y sólo tenemos acceso a esa máquina a través de ssh como un usuario normal.

Es decir, desde nodo_a podemos ejecutar : ssh usuario@nodo_b y desde el nodo_b podemos ejecutar ssh root@nodo_c.

Además, en el frontend (nodo_b) nos han limitado recursos (tunneling, forwarding, ...), en particular en el /etc/ssh/sshd_config del nodo_b:

AllowAgentForwarding No

AllowTcpForwarding No

GatewayPorts No

PermitTunnel No

X11Forwarding No

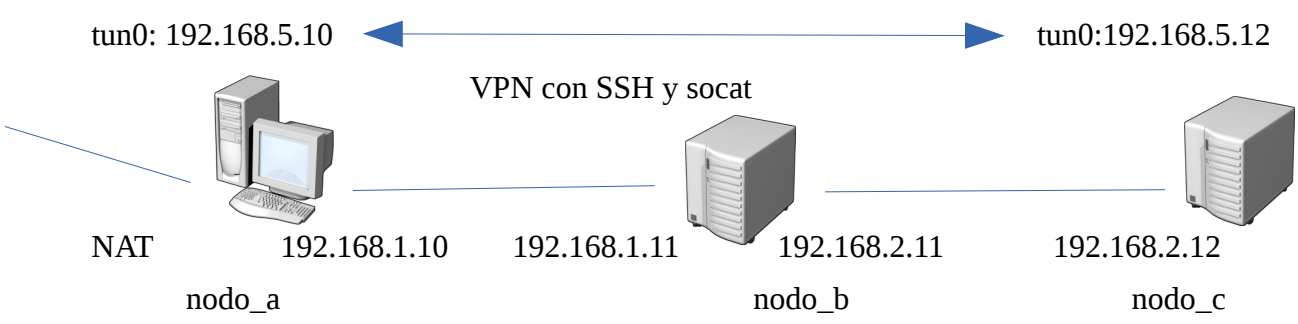
Queremos establecer una VPN mediante ssh y socat que permita poder hacer ping entre los nodos_a (tun0:192.168.5.10) y nodo_c (tun0:192.168.5.12) directamente.

Añadir una ruta por defecto en el nodo_c hacia el nodo_a de forma que el nodo_c pueda acceder a internet a través de la VPN que hemos creado con el nodo_a, por su salida NAT.

nodo_a: eth0 (NAT) , eth1:192.168.1.10

nodo_b: eth0 :192.168.1.11, eth1:192.168.2.11

nodo_c: eth0: 192.168.2.12



2.- (10 PUNTOS) Utilizando el servicio de openport descrito en el taller de comunicaciones seguras (consultar transparencias), crear los scripts o programas (preferentemente en Python) que permitan levantar automáticamente una conexión VPN mediante ssh de dos máquinas nodo_a y nodo_b que están detrás de un NAT no tienen acceso directo entre sí de forma que utilicen algún servicio gratuito en internet para el intercambio del url de acceso.