

Seminario 1 – Guía de trabajo

- Visitar página web http://dtstc.ugr.es/it/gii_fr/
 - Descargar la máquina virtual **FR_tools.ova**
 - Usuario: fr
 - Contraseña: 1819_FR_Inf
 - Descargar introducción a los seminarios
- Descargar e Instalar VirtualBox

VirtualBox

- Instalar en VirtualBox la máquina virtual de la asignatura (*Archivo-Importar servicio virtualizado*).
- Iniciar la máquina (usu: alumno, pass: finisterre).
- Comprobar que están instalados los servicios necesarios:
 - telnet: telnet localhost
 - ssh: ssh localhost
 - wireshark: wireshark
- Apagar la máquina virtual.

REDES NAT

- Crear una Red Nat (*Archivo, preferencias, red, pestaña de Red NAT*).
- Crear Red y dejar su nombre por defecto *NatNetwork*.
- Comprobar que la máquina virtual tiene asignada esa Red Nat. Entrar en su Configuración-Red: Conectado a “Red NAT”, Nombre: “NatNetwork”.
- Iniciar la máquina virtual y comprobar su conectividad a internet (Usar Firefox).
- Apagar máquina.

CREAR RED de MVs

- Clonar la MV “FR”. *Máquina-Clonar o Botón derecho -> Clonar.* (*Reinicio de MACs, clonación enlazada*).
- Crear MV “FR_2” y “FR_3” clonando “FR”.
- Comprobar que las tres MVs tienen el interfaz como tipo “Red NAT” y están en la red “NatNetwork”.
- Arrancar las 3 máquinas.
- Comprobar sus direcciones IP:
 - En Ubuntu, *Icono Conexiones (Menú arriba derecha) - Información de la Conexión.*
 - En una pantalla de Terminal: `ifconfig`
 - Las IPs serán:
 - FR: 10.0.2.4
 - FR_2: 10.0.2.5
 - FR_3: 10.0.2.6
- Comprobar conectividad entre ellas:
 - En Terminal: `ping 10.0.2.4`
`ping 10.0.2.5`
`ping 10.0.2.6`

- Comprobar default gateway (será la máquina que hará el NAT entre las direcciones internas y las direcciones públicas de Internet):
 - `netstat -rn`
 - `route`
- Comprobar conectividad con Internet:
 - Firefox a una página web
 - En Terminal: `ping www.ugr.es`

Wireshark

- Iniciar Wireshark:
 - En Terminal: `wireshark`
- Veremos que no hay interfaces a monitorizar.
- Iniciar Wireshark como superusuario:
 - En Terminal: `sudo wireshark`
- Elegir el interfaz ethernet (`eth0` o `eth1`).
- Empieza la captura.
- Se pueden ver paquetes generados de cuando en cuando (mantenimiento de topología de la red, actualización de DNS).
- Entrar en Firefox en www.ugr.es.
- Se verán muchos paquetes capturados.
- Parar la captura y reiniciarla (elegir de nuevo el interfaz a monitorizar).
- Generar tráfico en un chat:
 - Iniciar en FR_2 el servidor netcat:
 - En Terminal: `nc -l 10000`
 - Iniciar en FR el cliente netcat:
 - En Terminal: `nc 10.0.2.5 10000`
- Escribir en las máquinas y comprobar que el texto sale en la otra.
- Ver las capturas:

<ul style="list-style-type: none"> ◦ Se inicia la comunicación con un paquete SYN ◦ Se responde con SYN-ACK ◦ Se responde de nuevo con ACK y se empieza a transmitir los datos (textos) 	3-way handshaking de TCP
--	--------------------------------
- Revisar el tráfico (source, destination, protocol, info).
- Comprobar cabeceras anidadas (en marco intermedio). *Statistics -> Protocol Hierarchy*.
- Aplicar filtros: *tcp, ip.addr, tcp.port*
- *Analyze -> Display Filters*.
- Se puede salvar una captura y abrirla posteriormente para su análisis.
- Sobre uno de los mensajes del chat: *Botón derecho -> Follow TCP/UDP Stream*
- *Statistics -> Flowgraph*