**UF1 Introduccion a la seguridad informatica:**



**Indice:**

1. Introducción
2. Scripts de bash
3. Instruciones basicas de red en Linux
4. Estructura de protocolos
5. ICMP
6. ARP
7. Ping de la muerte
8. Estructura de la paqueteria
9. Escaneos de red

A lo largo de este curso, aprenderemos algunas técnicas de hacking que tendrán utilidad para la administración de sistemas y para aplicar las políticas de uso. Las pruebas en el laboratorio serán ataques informáticos en redes locales con los que podremos evaluar el daño causado en la red y las consecuencias sobre los usuarios también veremos cómo protegerse de estos mismos.

En esta unidad formativa repasaremos conceptos del curso anterior tanto de redes como de nomenglatura.

**Documentos basicos de seguridad:**

PDF 1: Introduccion a la seguridad 1

<https://elpuig.xeill.net/Members/jordifarrero/2014-15-seguretat-en-xarxes-sm2ab-diurn/uf1-documentacio/pdf-introduccio-seguretat/view>

PDF 2: Introduccion a la seguridad 2

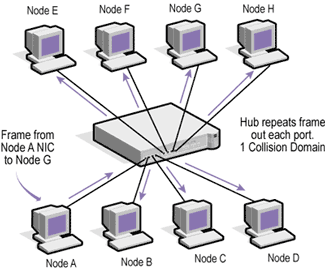
<https://elpuig.xeill.net/Members/jordifarrero/2014-15-seguretat-en-xarxes-sm2ab-diurn/uf1-documentacio/pdf-introduccio-seguretat-2/view>

**Relacion de conceptos asociados a una red de area local**

Cuando una administrador de red diseña una topología para una empresa debe tener en cuenta el funcionamiento básico de sus dispositivos de res.

Los concentradores o dispositivos de la capa de usuario son los repetidores y los puentes.

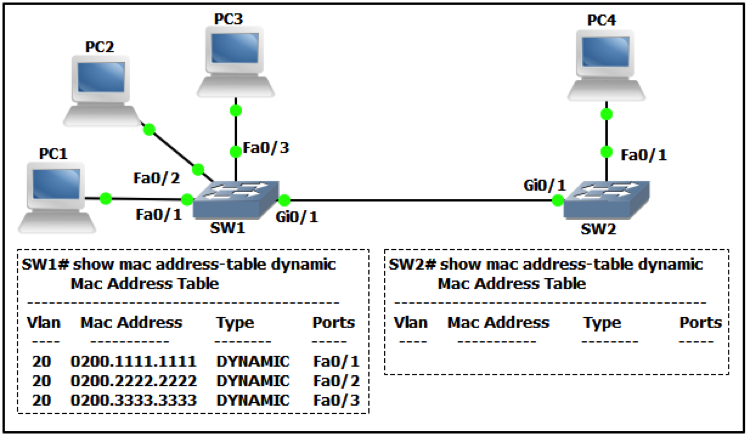
**Repetidores (HUB):**



Como se observa en esta imagen los HOB utilizan un repetidor para comunicarse entre sí , pero este tiene una restricción a nivel de diseño y es que replica toda la paquetería en todos los puertos disponibles. Cuando una red LAN utiliza repetidores suele ser lenta (debido a las colisiones) e insegura. Cuando un usuario envía un paquete a otro usuario de la LAN el paquete lo reciben todos los usuarios y si no va dirigido a ellos lo descartan por lo tanto se llega a la conclusión que un host puede capturar tráfico de el resto de la red.

Los HUB actualmente estan desuso son inseguros y generan colisiones.

**Puentes (Switch):**

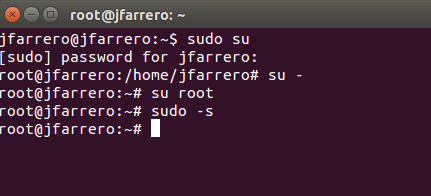


El puente es el dispositivo más común en redes LAN debido a su bajo coste y su buen funcionamiento. El switch es un dispositivo capaç de desencapsular paquetería hasta la capa 2 (ethernet) por lo tanto conoce las direcciones MAC de origen y destino y las guarda en las tablas MAC.

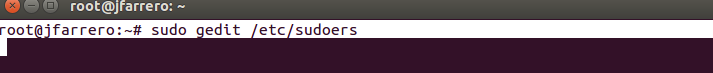
Cuando un host desea enviar un paquete a un destino el switch recibe el paquete lo abre y busca la dirección MAC del destino en su tabla MAC y lo reenvía en el puerto específico por lo tanto solo recive el paquete un destinatario.

Cuando un hacker desea capturar tráfico en una red basada en switch este debe utilizar técnicas o engaños para recibir tráfico no legítimo y a partir de ahí de pueden iniciar otros ataques por ejemplo una suplantación de identidad.

**2- Relacion de comandos basicos de BASH para servicios de red**



La instrucción “sudo” nos permite ejecutar y acceder a los comandos en modo “root” en la mayoría de casos de seguridad requieren “sudo”.

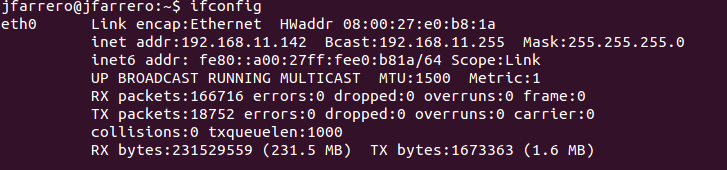


El fichero “sudoers” permite especificar usuarios y grupo que requieren permisos de “root”.

**Comandos basicos de red**

Los comandos de red son imprescindibles en Linux para saber el estado configuración de los discos. Por defecto cualquier interfaz del host se encuentra y se muestra con el comando “ifconfig” y “iwconfig” también “ip link”. A lo largo de este curso utilizaremos las interfaces ethernet para realizar todas las pruebas pero también si fuera necesario se podrían utilizar las interfaces WIFI.

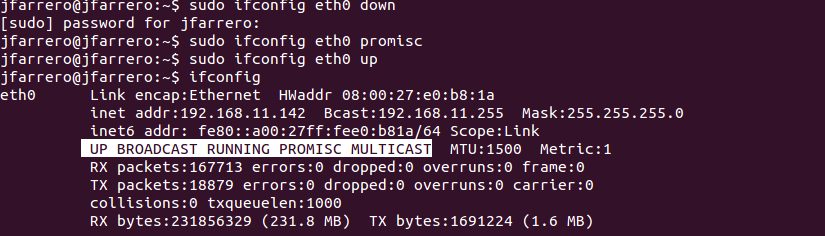
Linux por defecto asigna “eth0” como interfaz 802.3 y le asigna parámetros predeterminados como por ejemplo el MODO MULTICAST, este modo es el método que permite transmitir datagramas a un grupo de receptores y descarta aquellas tramas que no son para el host.



Como se ve en la imagen el MODO MULTICAST esta activo.

**Modo promiscuo:**

Como hemos visto anteriormente por defecto la interfaz de red solo captura las tramas dirigidas al host si se desea capturar tramas de otros usuarios es imprescindible activar el modo promiscuo este modo requiere “sudo”. Todos los sniffers requieren de este modo para capturar tramas.

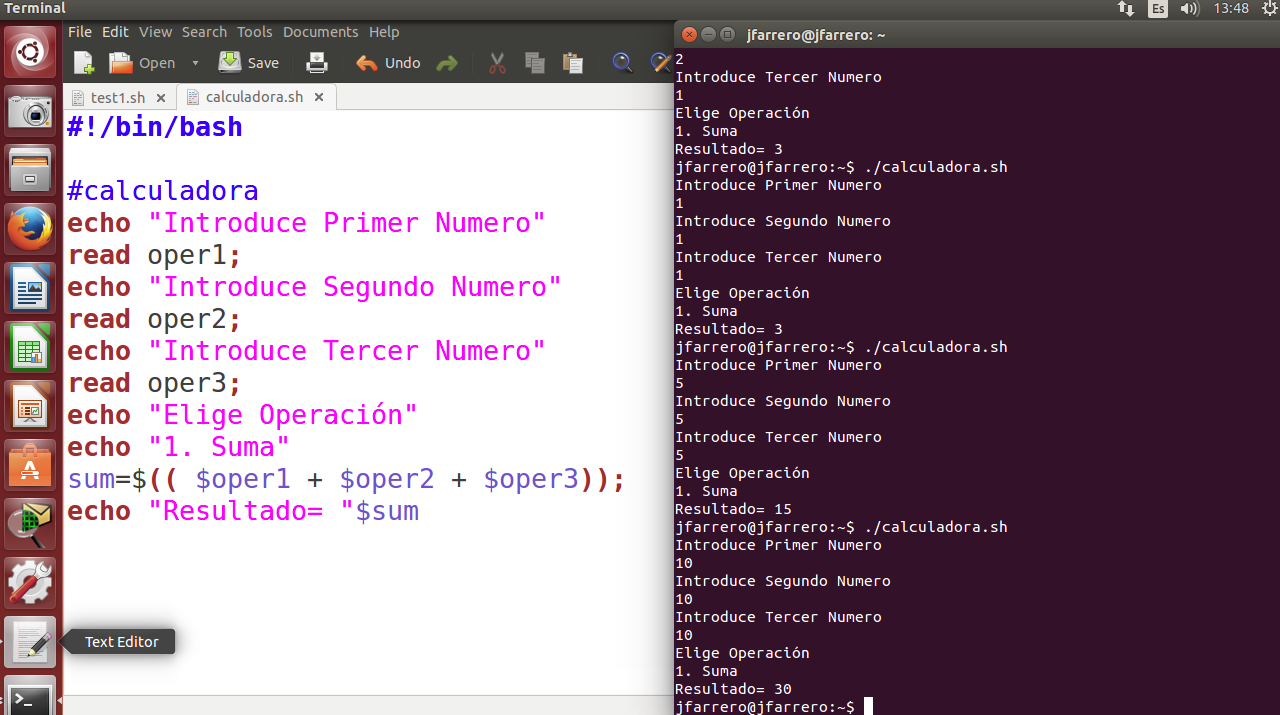


**Creacion de scripts basicos de BASH**

Cualquier administrador de red debe ser capaz de diseñar sus propios scripts para automatizar tareas. En el ámbito de la seguridad también se debe crear scripts para sistemas de menús en el que tareas complejas pueden ser ejecutadas por usuarios no expertos es en este momento donde se debe aprender los conceptos básicos de programación de scripts.

**Ejercicio 1:**

Diseña una calculadora que sume 3 valores y que muestre el resultado.



En el siguiente script podemos diferenciar los siguientes bloques:

1. Inicialmente se debe inicializar las variables por ejemplo: valor1=0
2. Declarar el bloque de codigo principal
3. Finalmente devolver el resultado o efectuar la operacion.

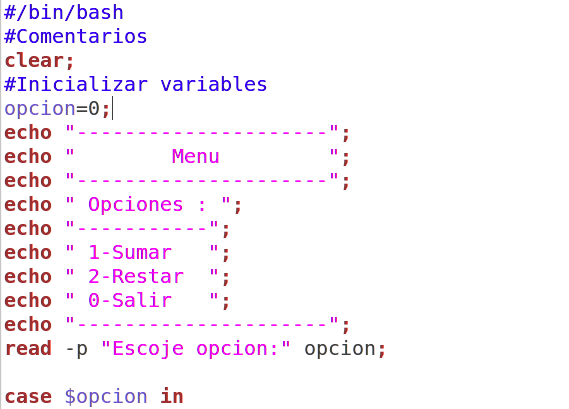
Despues de a ver identificado los bloques es el momento de realizar un pequeño compendio de las instrucciones utilizadas:

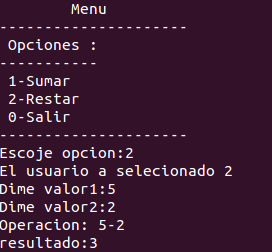
1. echo: Instrucion que devuelve una cadena de caracteres o frase a la salida estandard (monitor).
2. read: La funcion read permite mostrar un mensaje a la salida estandard y despues recojer valor de la entrada estandard (teclado) y lo tira en una variable.
3. let/sum: Por defecto todas las variables contienen cadenas de caracteres esto significa que 1+1=11, si se desea que la variable interprete el valor como entero se debe utilizar la instrucuion “let o sum” por lo tanto 1+1=2.

**Ejercicio 2:**

Realiza un pequeño sistema de menus en el que hay 3 opciones:

1. Realizar una suma
2. Realizar una resta
3. Salir





Como ven en este ejercicio la forma de recojer variable sigue siendo igual con la isntrucion “read” la unica diferencia es que en este script se utiliza la instrucion “case”.

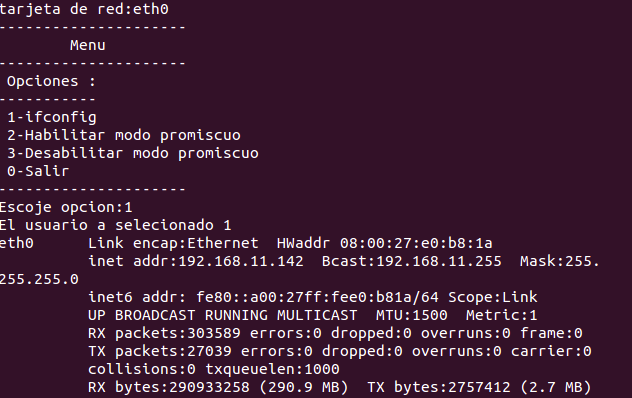
La instrucion “case” nos permite evaluar el contenido de una variable en caso de que el valor de la variable sea el mismo que el valor decidido en la instrucion “case” este ejecutara un bloque de codigo especifico. Si ibservamos el codigo veremos que “case” evalua 3 valores posibles en caso de 0- salir, en caso de 1- sumar, en caso de 2- restar.

**Ejercicio 3:**

Diseña un script que realize las siguientes funciones:

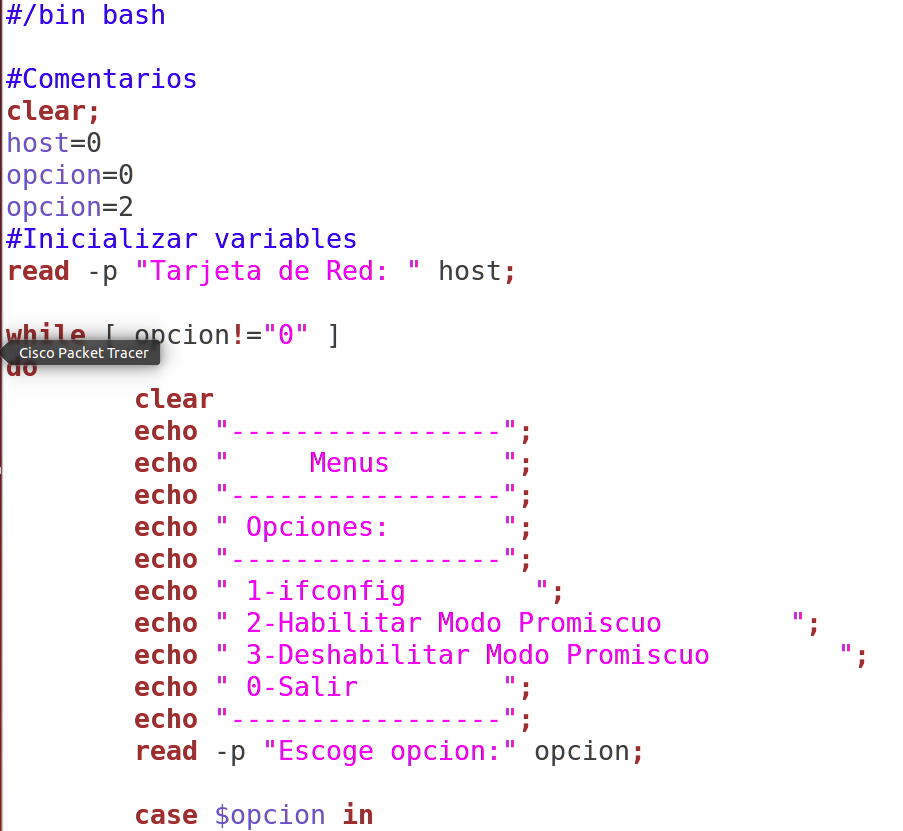
1. Pide el nombre de la interfaz del host
2. Aparece un menú que tiene las siguientes opciones: 1-realizar un “ifconfig”,2- poner la tarjeta declarada en modo promiscuo,3- desabilitar el modo promiscuo, 0- salir

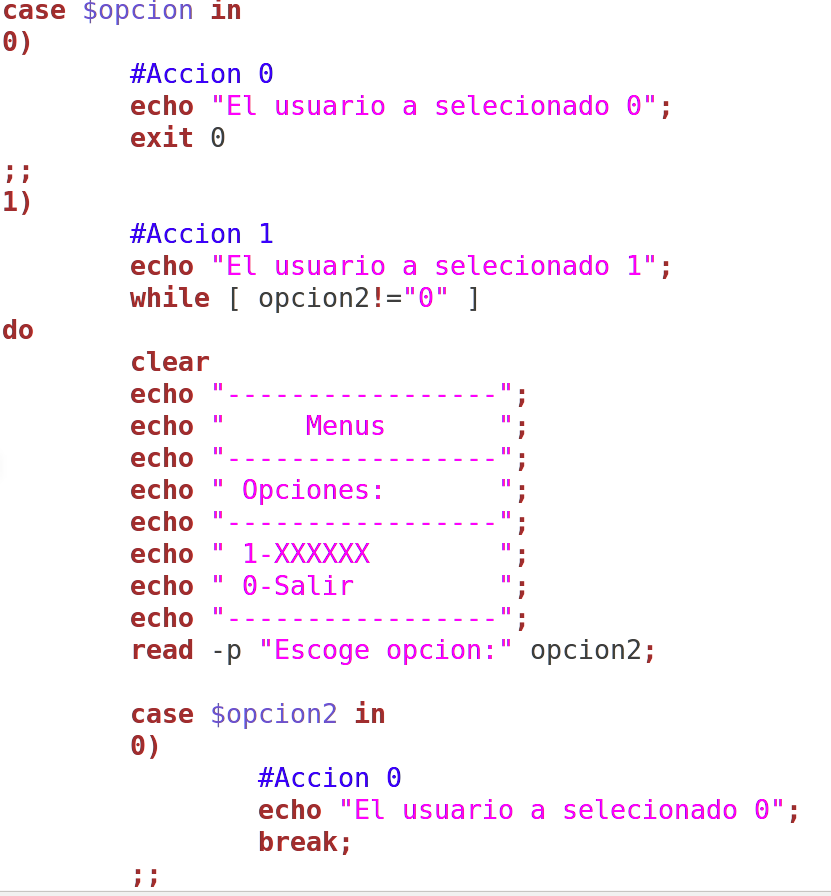


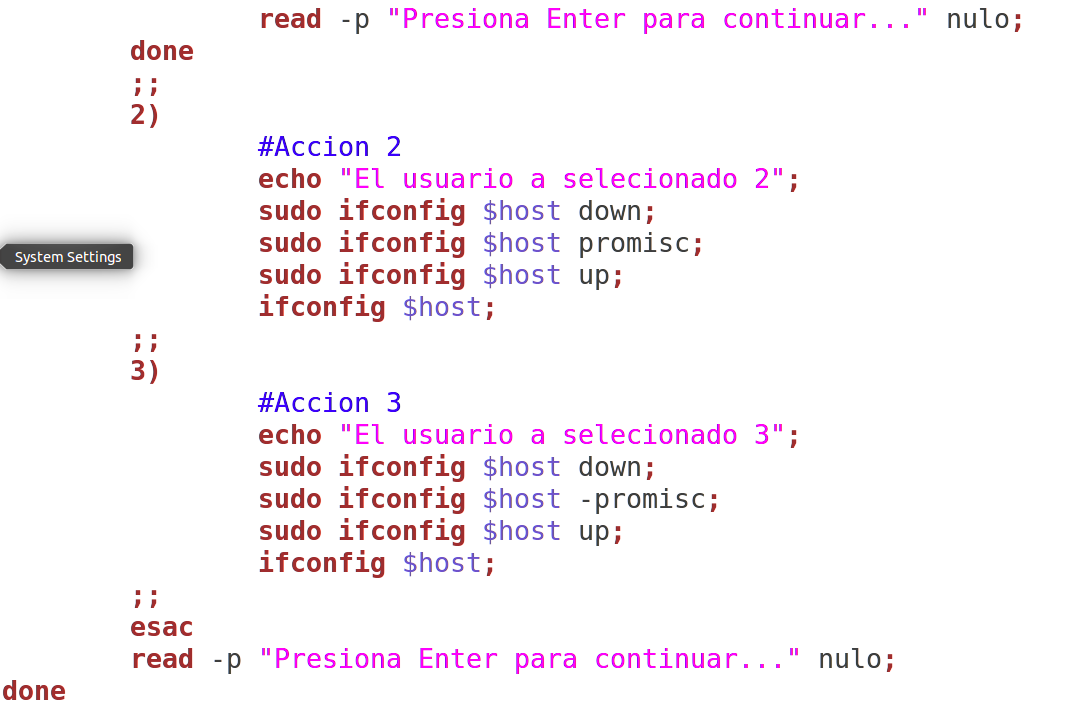


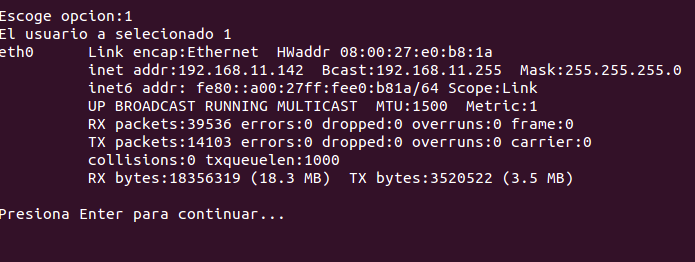
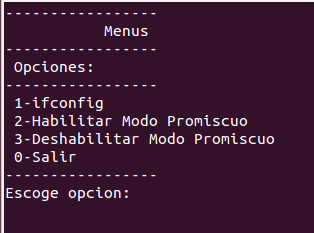
**Ejercicio 4:**

Crear un Submenu:





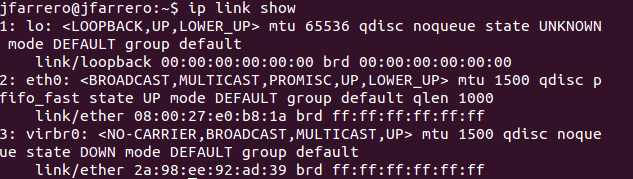


****

Como observamos en la solución del ejercicio los menús anidados no son nada más que una estructura de menús dentro de otra estructura de menús. Si miramos detalladamente el código vemos que dentro de la instrucción en “case” se ha copiado y tabulado otra vez todo el bloque de menú desde el “while” hasta las opciones del “case” obteniendo que cuando el usuario selecciona la opción donde se encuentra el submenú pasa a mostrar toda la estructura del submenú que se encuentra dentro del “case”. Tabular correctamente el código hace que se pueda entender mucho mejor.

**Herramientas de recorte para información de la salida estándar**

Como ya se ha aprendido en el curso anterior existe una relación de herramientas que permiten formatear la información que sale en la pantalla así el usuario puede recibir información fácil y sencilla por ejemplo:

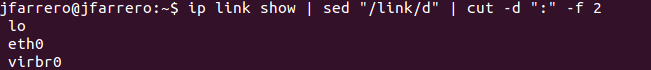


En esta imagen podemos ver un resultado que les sera muy dificil de entender a un usuario no experto es aquí donde entran las instrucciones de recorte.

Las instrucciones “cut”, “sed”, “awk”, son necesarias para reportar la información y mostrar solo lo que un usuario pueda entender.

**Ejercicio 5:**

Recorta la salida estándar de la instrucción “ip link” y que muestre solo la siguiente información:



<https://elpuig.xeill.net/Members/jordifarrero/2014-15-seguretat-en-xarxes-sm2ab-diurn/uf1-scripts-demo/altres-exercicis-cut-sed-awk>

ip link show | sed "/link/d" | cut -d ">" -f 1 | cut -d "<" -f 2

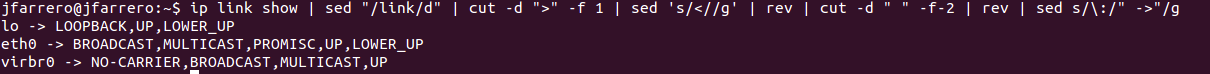
ip link show | sed "/link/d" | cut -d ">" -f 1 | sed 's/<//g' | rev | sed 's/://g'

ip link show | sed "/link/d" | cut -d ">" -f 1 | sed 's/<//g' | rev | sed 's/://g' | cut -d " " -f-2 | rev

ip link show | sed "/link/d" | cut -d ">" -f 1 | sed 's/<//g' | rev | cut -d " " -f-2 | rev | sed /:/s/^/'->'/

ip link show | sed "/link/d" | cut -d ">" -f 1 | sed 's/<//g' | rev | sed 's/://g' | cut -d " " -f-2 | rev | sed /:/s/^/'->'/

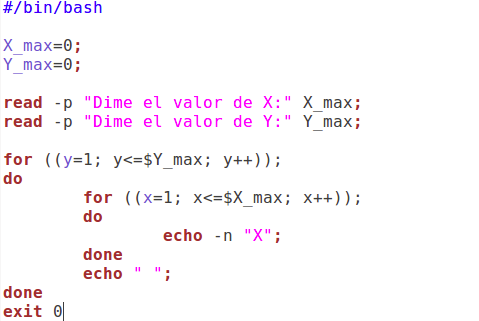
ip link show | sed "/link/d" | cut -d ">" -f 1 | sed 's/<//g' | rev | cut -d " " -f-2 | rev | sed s/\:/" ->"/g

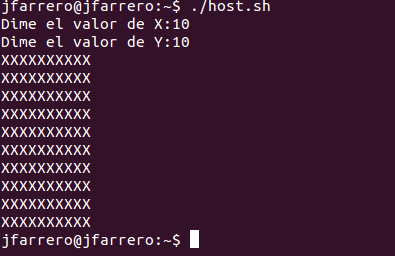


Este comando nos permite crear bloques de formación que un usuario no experto puede entender de una forma intuitiva. Aunque la instrucción es larga debido a que se concatenan una relación de instrucciones de recorte el resultado es óptimo para añadirlo en un sistema de menús de un script de automatización de tareas de red.

**Sentencia de creacion FOR**

Al igual que existe la instrucion “While”tambien existen otras sentencias que pueden repetir un bloque de informacion un numero de veces finitas y aqui es donde interviene la sentencia “for”.

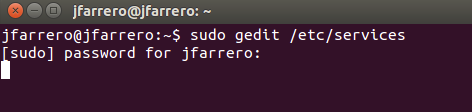




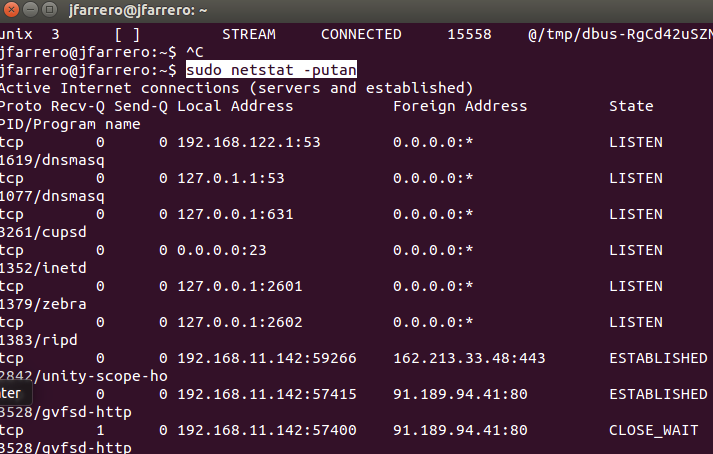
Con este simple ejercicio se puede entender como funciona esta sentencia que itera un número determinado de veces las condiciones que usa esta sentencia son: Valor inicial de la variable/ condición en el caso de ser cierta entra en la zona entre el “do” y el “done” normalmente menor o igual/ incremento por cada iteración (cada vez que da la vuelta se incrementa en una posición)

En este ejercicio hay 2 sentencias for anidadas que conforman el resultado final del dibujo de una matriz de X x Y.

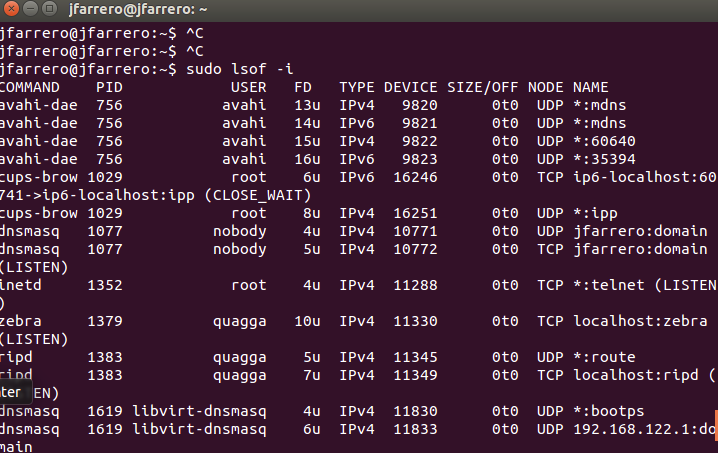
**Relacion de comandos asociados a servicios de red**



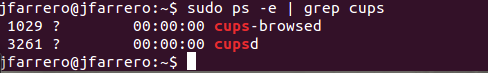
Este comando nos permite ver la relación de nombres de puerto, numero, tipo de protocolo y una breve descripción. Un administrador de red debe recordar algunos números de puerto sobretodo los más utilizados el fichero “services” nos sirve para identificar si es un puerto conocido.



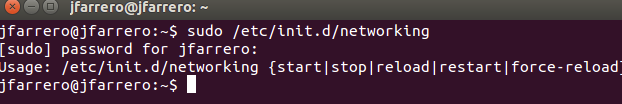
El comando “netstat” es el comando basico para tener control de que servicios y en que estado tiene nuestro host. Podemos observar los puertos que se encuentran abiertos, cerrados y filtrados en caso de encontrar un servicio no deseado la mejor opcion desabilitar el servicio y desinstalar el (demonio).



Otra alternativa al “netstat” “lsof -i” que nos tabula la informacion de una forma distinta al “netstat”.



El comando “ps -e” nos muestra los servicios recurrentes y procesos activos en el host. Debido a que Linux cientos de servicios en una sesión de usuario estándar el comando “ps” suele ir acompañado del “grep” para filtrar por nombre.



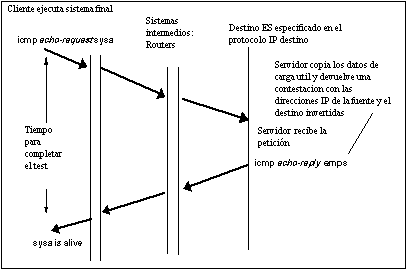
El comando “networking” nos permitirá iniciar o parar los servicios de red de nuestro host. Normalmente será necesario reiniciarlo cuando instalemos un servicio de red nuevo.

**Protocolos basicos de red**

**ICMP**

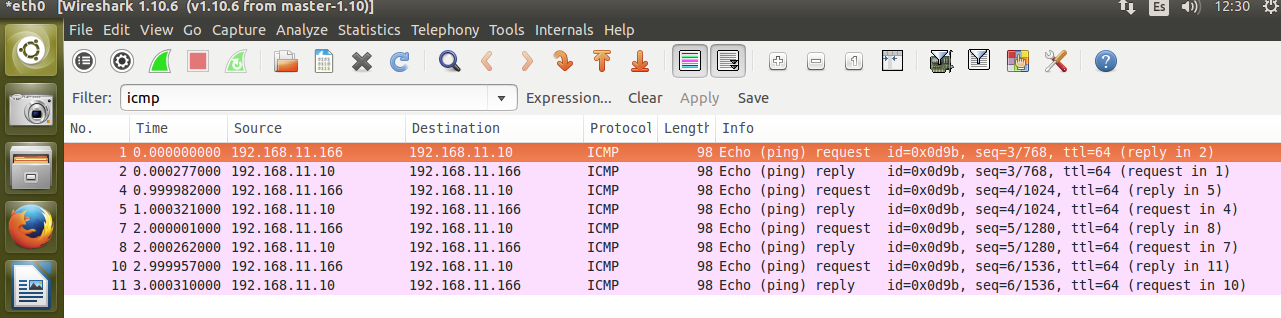
El protocolo “ICMP” protocolo de control entre host muy utilizado para la verificación del estado y conectividad entre host. El 'Protocolo de Mensajes de Control de Internet' es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

El protocolo “ICMP” es un protocolo usado para la verificación y control de redes. En redes LAN se usa para verificar el estado de conexión de host y dispositivos el comando mas utilizado es “ping”.



Este diagrama representa el funcionamiento e intercambio de paquetería de tipo ICMP entre origen y destino (PDU). El método de encapsulamiento de el protocolo es el siguiente:

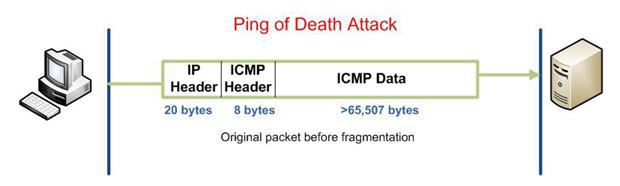
1. El origen monta una trama con la MAC origen y destino.
2. Dentro de la trama hay un paquete con la IP origen destino.
3. Como ICMP es un subprotocolo de la la capa de red el paquete tiene asignado un marcaje de tipo *echo- request* (es una pregunta tipo ICMP).
4. Se envia el paquete al destino.
5. El destino desencapsula y lee la pregunta de tipo ICMP.
6. El destino encapsula un paquete ICMP con marcaje de tipo *echo- reply*.
7. El host origen recive el paquete y muestra el resultado a la salida estàndard.



Como se puede ver en esta captura la instrucción “ping” contra un destino que genera la paqueteria correspondiente al diagrama anterior, podemos observar el “echo request” y el “echo replay”.

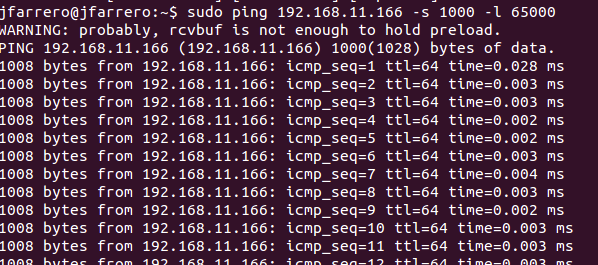
ICMP es un subprotocolo de la capa de red y actualmente no tiene importantes huecos de seguridad pero hace años se encontró un problema de desbordamiento de pila grave que provocaba un error en los servicios de red de Windows 95, 98 y millenium y en Linux kernel 2.0, denominado “ping de la muerte”.

**Ping de la muerte**



Un ping de la muerte es un tipo de ataque en un sistema informático que implica el envío de un ping mal formado o malicioso a una computadora.

Como se puede ver en la imagen se basa en enviar un carga ICMP de tamaño superior a la esperada provocando un desbordamiento en el servicio de red de la computadora. Debido a que el trailer de ICMP tiene longitud superior a 64 bytes y el hacker envía una carta de 65 bytes el servicio de red escribe los bytes sobrantes en una zona reservada por el sistema, por lo tanto cuando el sistema quiere recuperar el dato de la zona sobreescrita por el ping de la muerte falla y genera un kernel panico.



En el ejercicio de verificación de el “ping de la muerte” primero observamos la propia sintaxis del comando que son los siguientes:

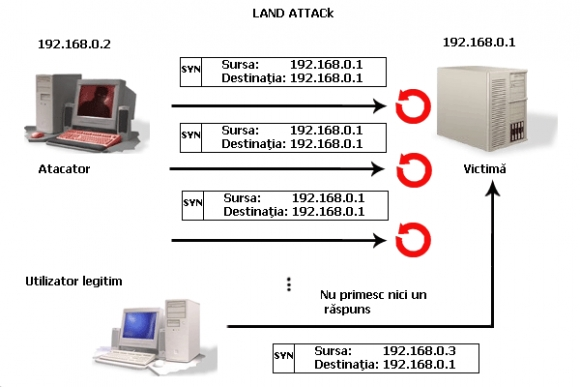
* -l: longitud del payload (carga). El tamaño de la carga del ICMP es de 64 bytes por lo tanto el tamaño del “ping de la muerte” debería ser superior a los 64 bytes.
* -i: a la instrucción “ping” se le puede especificar cuantas veces se encapsula un paquete por segundo en este caso ponemos un valor muy bajo del orden “0,” su funcion sera la de inyectar tantos paquetes como sea posible.

“Ping de la muerte” no es un ataque por inundación por lo tanto no es imprescindible utilizar “-i”, en principio con un solo ICMP corrupto el sistema operativo víctima debería fallar.

Conclusión: el “ping de la muerte” no funciona en las versiones actuales de los sistemas operativos, y como hemos comprobado en clase una inundación de “ping de la muerte” contra un solo host no afecta al sistema operativo ni la latencia de la red.

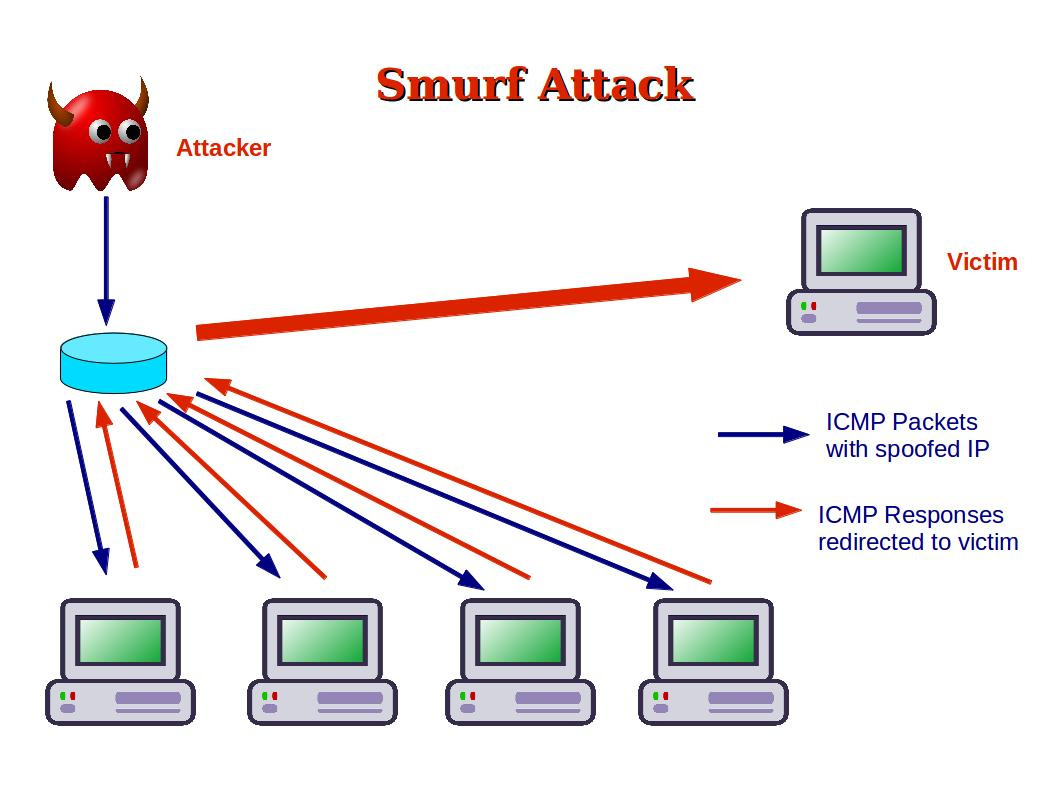
**Ataques actuales basados en ICMP**

1. Ataque LAND



El LAND ATTACK se basa en un ataque contra una arquitectura de red muy completa, el hacker envía paquetería que puede ser de tipo ICMP masivamente en que el origen y el destino del paquete son: la ip pública y la ip privada de la víctima, por lo tanto la víctima entrara en bucle devolviendo las respuestas a su misma interfaz de origen.

1. Ataque SMURF



El ataque “Smurf” se basa en la utilización de host reales de las que los hackers pueden tomar el control. Este ataque es complejo ya que requiere una arquitectura de host o zombies en la red de redes.Cuando el hacker manda una señal a los zombies estos realizaran una acción y esta acción realizar el ataque de tipo SMURF.

En concreto el ataque “Smurf” consiste en montar un paquete ICMP de tipo “echo- request” con el origen de la víctima y destino el zombie el efecto que se desea es que el zombie rebota el mensaje ICMP que sera un “echo- replay” se dirigira hacia la víctima. Si esta acción la repetimos miles de veces de orígenes distintos se puede provocar lentitud de procesos en la víctima.

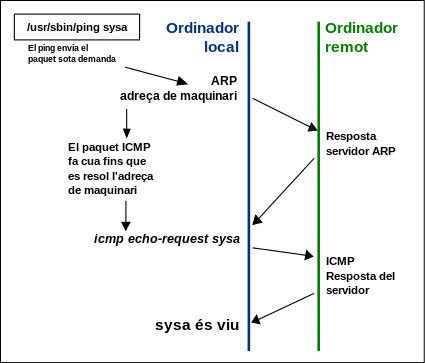
Conclusión: En ningún caso podemos utilizar ICMP como un ataque de flooding válido existen otros métodos más efectivos y más agresivos.

**ARP**

(address resolution protocol) es un **protocolo de comunicaciones** de la capa de enlace, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

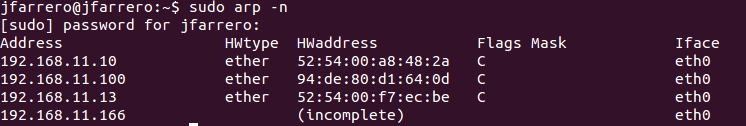
El protocolo ARP se inicia en una red LAN cuando un host tiene la ip de un destino pero le falta la dirección MAC para encapsular el paquete que desea enviar es en este punto donde interviene ARP. ARP contiene una tabla con todos los host con los que nos hemos comunicado alguna vez, en la tabla incluimos la IP del host y su MAC.

El proceso ARP consiste en montar un paquete con el host origen y con la MAC de destino el broadcast (FF:FF:FF:FF:FF:FF) este mensaje llegara al broadcast de la red gracias al switch, solo contestara con otro mensaje ARP de tipo “reply” el host con la IP que estamos buscando este host incluye su MAC en la respuesta y la devuelve al host origen, el host origen apunta en la tabla ARP los datos.



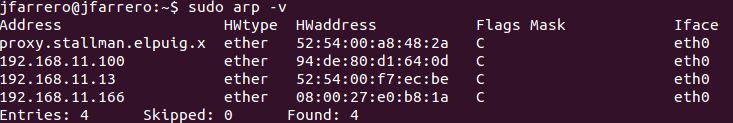
**Ejercicio:** Determina que características tiene cada una de esta opciones:

1. -n:



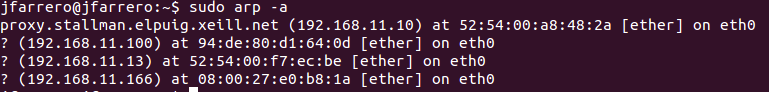
Muestra direcciones numéricas en lugar de tratar de determinar el nombre simbólico de host, puerto o usuario.

1. -v:



Dígale al usuario lo que está pasando siendo prolijo (pequeños detalles).

1. -a:



Utilice un formato de salida de estilo BSD alternativo (sin columnas fijas).

1. -d:



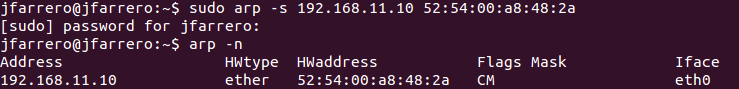
En lugar de un hw\_addr, el argumento dado es el nombre de una interfaz. arp usará la dirección MAC de esa interfaz para la entrada de la tabla. Esta suele ser la mejor opción para configurar una entrada proxy ARP para usted.

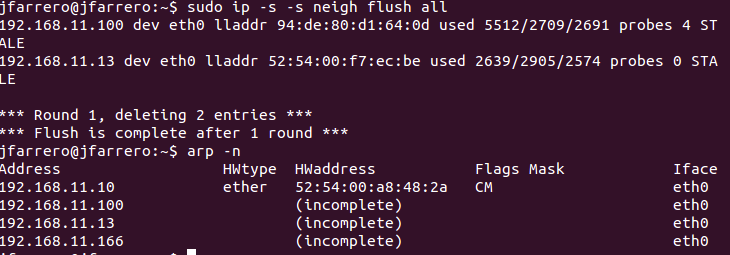
1. -s:

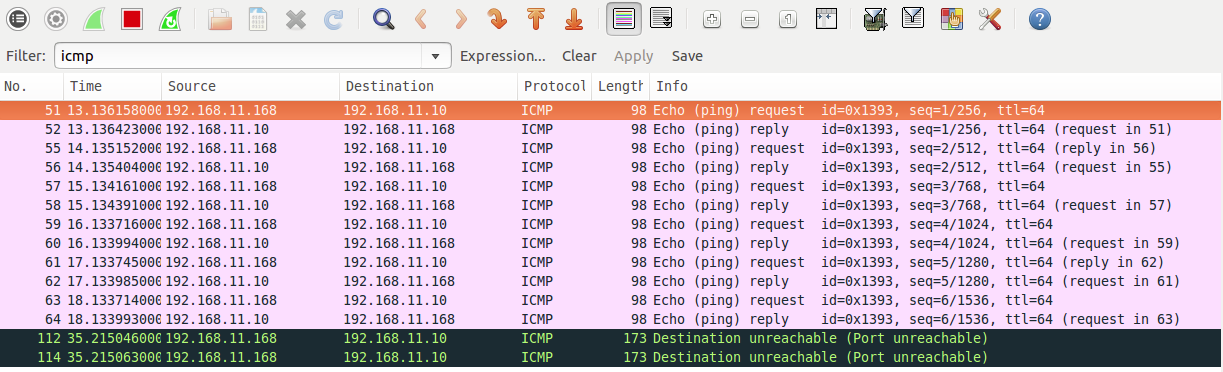


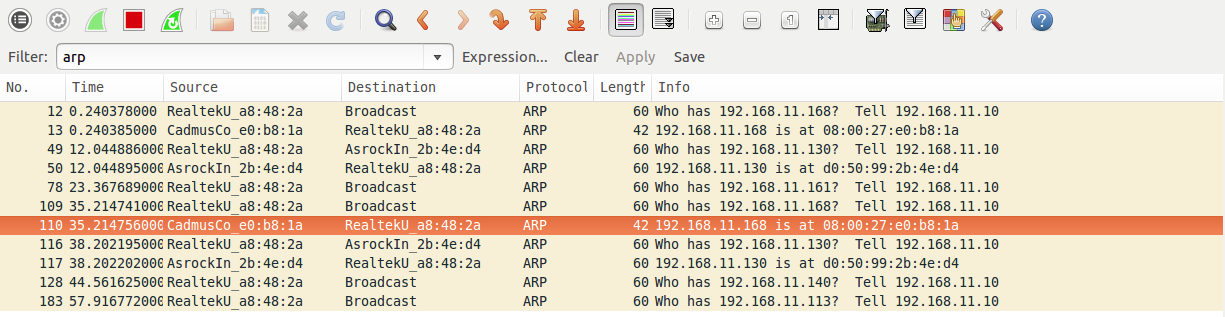
Añade una direccion a la tabla MAC.

El parametro “-s” nos permite realizar entradas estaticas (inamovibles) en la tabla ARP. Por defecto las entradas ARP ordinarias tiene un estado de flag (bandera) de tipo “C” en el momento que introducimos una entrada estática el flag pasa al estado “CM”. El “flag CM” indica al host que aunque reciva ARPs que quieran modificar esa entrada no se aplicaran (esta entrada no se puede modificar).









Debido a la arquitectura del protocolo ARP al igual que ICMP no existe una relacion entre la pregunta y la respuesta (request-replay) por lo tanto puede haber muchos replays sin haber generado ningun request es aqui donde intervienen los ataques o envenenamientos con el protocolo ARP que viene a ser equivalente a una suplantacion de identidad, estos ataques se llaman ARP SPOOFING” o “ARP POISONING” estos ataques los veremos en la siguientes UF’s.

1. Busca una instruccion que borre todas las entradas ARP:

arp -n

De la tabla debes elegir una ruta a eliminar dado que arp elimina de a una sola:

arp -d 192.168.1.1

Este borra la línea referida a la ruta 192.168.1.1.

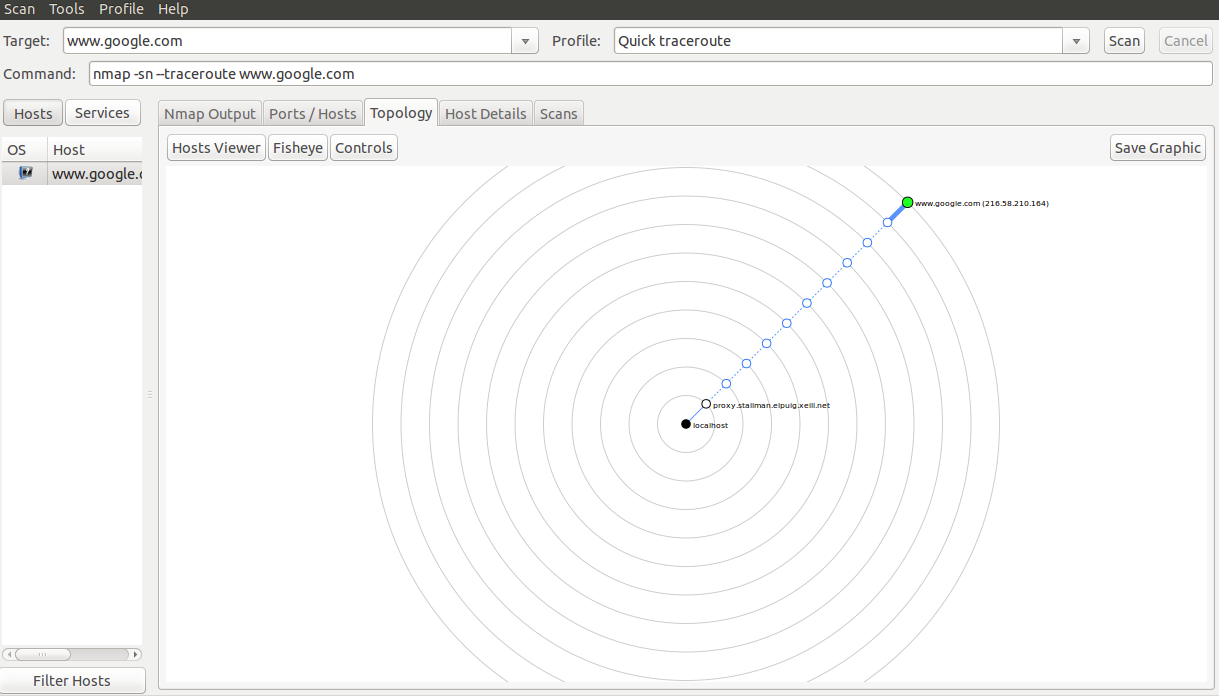
La opción más poderosa para eliminar el cache es:

ip -s -s neigh flush all

Limpia todo el cache en un solo comando.

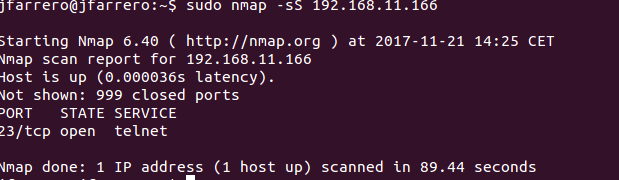
**Herramientas de mapeo e identificacion de host en una LAN**

Cuando un hacker quiere posicionarse o bien entender la topología y la estructura de la red es imprescindible realizar un simple escaneo del broadcast de la red, de este modo el hacker podrá identificar todos los host, dispositivos de red, servidores y otros dispositivos inalámbricos una vez el hacker obtiene la relación de recursos escogerá a la víctima en función de su objetivo.

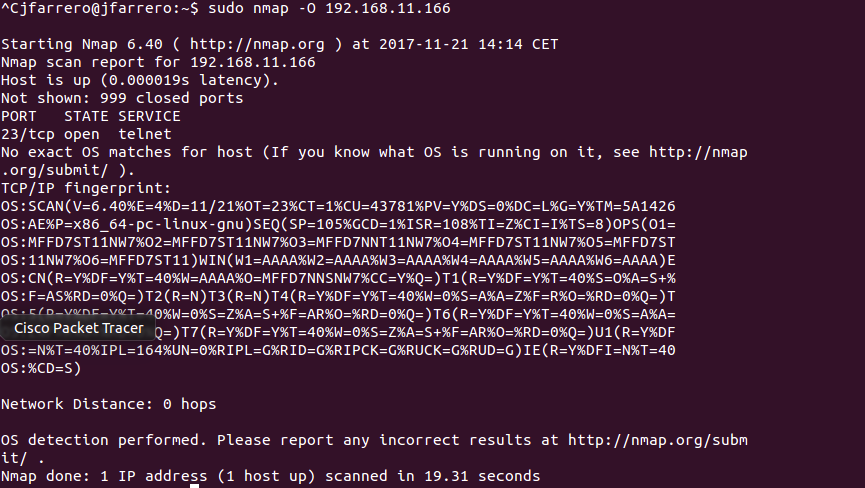


NMAP es una instrucción que soporta múltiples opciones de parámetros, cada usuario escogerá un conjunto de opciones que se adapten a sus necesidades la mayoría de veces los escaneos al BROADCAST suelen ser largos debido al tipo de detalle requerido por ejemplo: Números de puerto y versiones, Identificación de OS, Identificación de fingerprinting, Número de saltos, Tipo de escaneo.

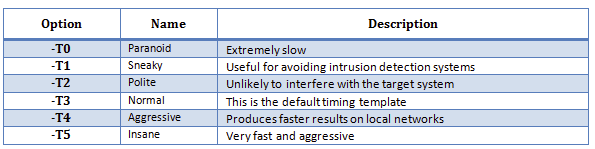
**Ejercicio 1:** Diseña una instrucción con NMAP que nos devuelva el número y tipo de puerto, version y información de tipo del sistema operativo.



**Ejercicio 2:** Identificar la version fingerpriting del SO en un rango de host concreto.

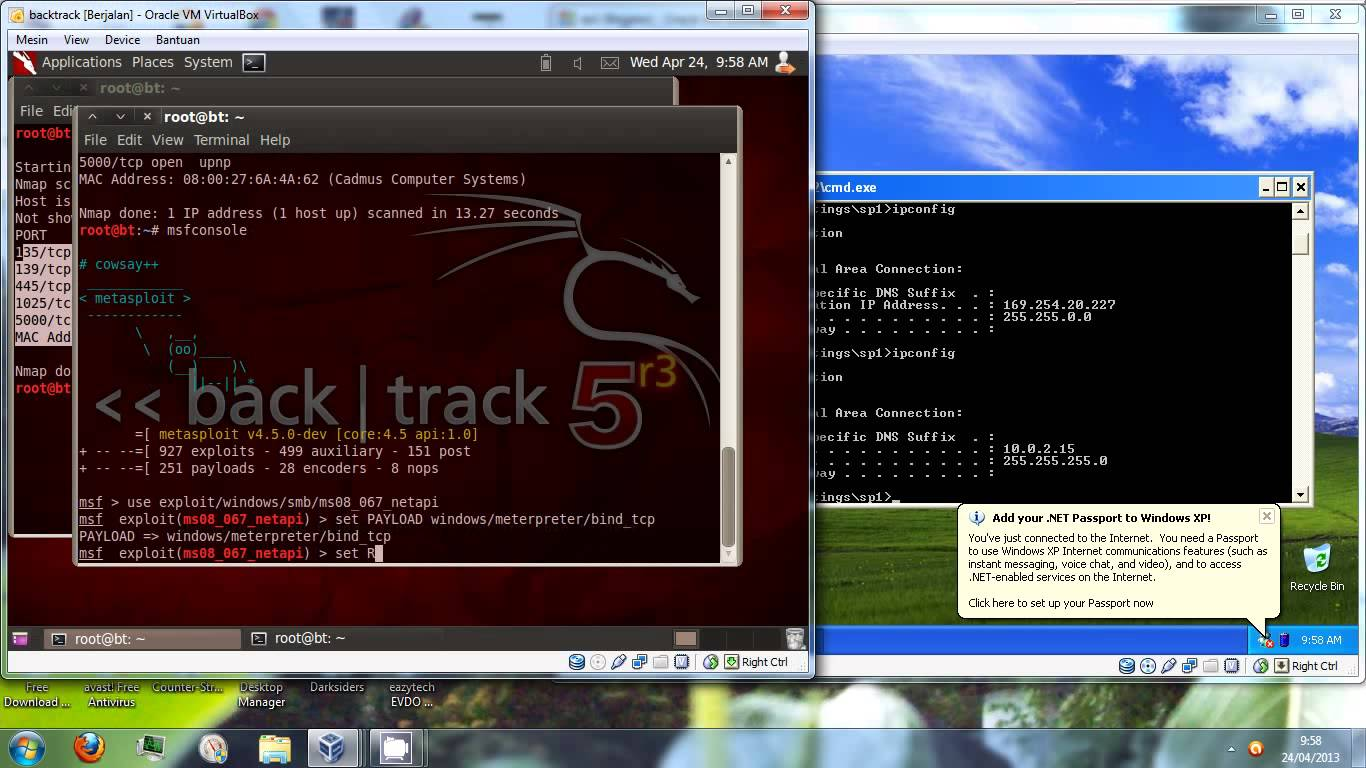


Hemos visto que NMAP es capaz de preguntar los host existentes en un segmento de red y indagar qué puertos y versiones tienen, pero encontramos cierta problemática asociada a este descubrimiento, básicamente NMAP realiza preguntas a la red asociadas a sus puertos o bien para identificar el host. Este tipo de identificación suele utilizar el protocolo ICMP o ARP el resultado se inyectan a la red cientos de paquetes de estos protocolos generando mucho ruido. Si la red está auditada (vigilada) pueden saltar alertas indicando que cierto puesto de trabajo está inyectando paqueteria poco habitual respecto al tráfico inyectado anteriormente.



Como se puede observar en esta tabla NMAP tiene una opción que permite indicar el nivel de sigilo para auditar toda una red estos modos van desde el 0 hasta el 5. El 0 es modo sigiloso muy lento y el modo 5 es el modo rápido ( modo de identificación rápida), conociendo estos niveles de sigilo es importante ajustar correctamente el valor para no ser auditados o identificados.

Los administradores de red deben conocer bien el funcionamiento del NMAP asi podran evitar y controlar su red administrada.



Un buen ejemplo de los hallazgos que se pueden hacer con el NMAP es la de identificar un host con el puerto 135 abierto en el caso que sea en windows xp (obsoleto) podremos aprovechar la vulnerabilidad en este puerto, la herramienta del metasploit que estudiaremos en las siguientes UF’s permite aprovechar esta brecha de seguridad para abrir una sesión de escritorio remoto a la víctima pudiendo manipular a su antojo el sistema operativo de la víctima. Este ataque es muy vistoso pero en realidad el 99% de los ataques no son tan aparatosos como este.

**Tipos de Sniffers**

Un **sniffer** es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

Hasta ahora hemos utilizado el sniffer en modo gráfico en WIRESHARK, pero este programa tiene ciertas restricciones cuando se trata de captura de paquetería en segundo plano es decir si un hacker quiere capturar paqueteria de alguna víctima no es suficiente realizar una captura de 5 minutos si no que lo importante es capturar paqueterias durante días, semanas o meses para así poder crear un perfil de usuario más o menos aceptable. WIRESHARK no nos permite realizar capturas largas ya que tiene restricciones propias del modo gráfico existen otras herramientas como el TCPDUMP que son en modo texto y se puede lanzar en segundo plano.

**Temario Examen UF1**

1. **PDF 2: De la 1 a la 30.**
2. **Funcionamiento y diagrama ICMP, ARP, Ping de la muerte,Ataque LAND, Ataque SMURF**
3. **NMAP: Funcionamiento**
4. **TCPDUMP: Funcionamiento**
5. **Explica los pasos para que realizar la captura de usuario y password de un usuario no cifrado (Telnet)**