Después de crackear la wep…

Obteniendo Información
-Computadoras conectadas
-Servicios y Servidores

Negación de Servicio
-Reiniciar el dispositivo
-Bloquear sitios especificos

Spoofing
-DNS Spoofing
-ARP Poison Redirection

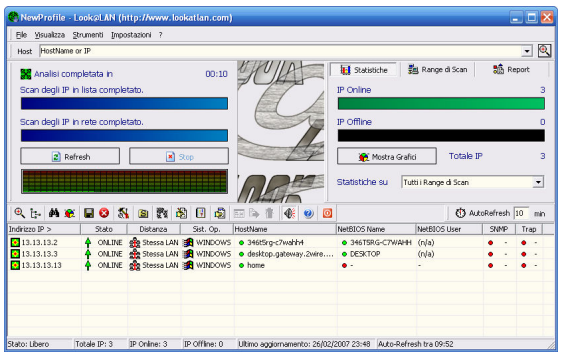
Sniffing
-Data
-Passwords

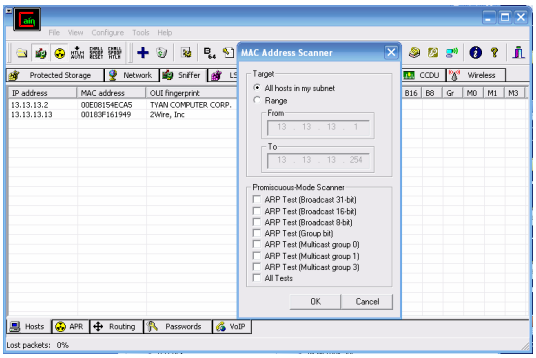
Introducción

Este texto explica algunos ataques que se pueden realizar posteriores a crackear la wep de un ruteador de prodigy. Es una compilación de herramientas y técnicas conocidas.

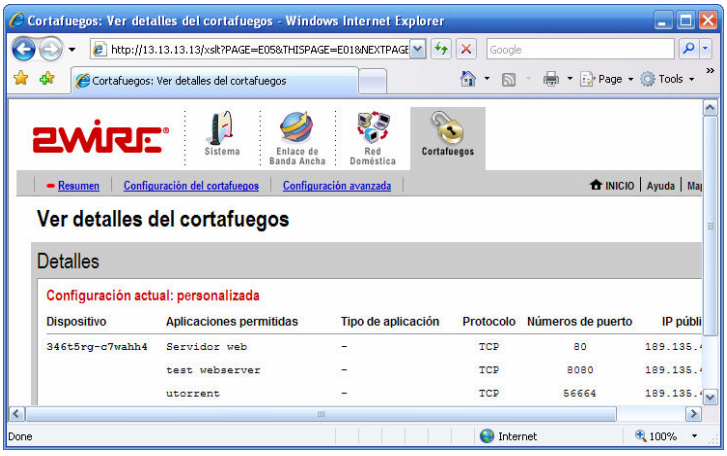
OBTENIENDO INFORMACION

Para obtener las computadoras conectadas a la red podemos entrar en la configuración del ruteador (http://home o el default gateway) y ver en la parte de Home Network las computadoras y su IP. Si no esta disponible el ruteador puedes usar un programa como Look at Lan (http://www.lookatlan.com) o en Cain (http://oxid.it) pueden conocer todos los hosts habilitando el sniffer y luego en el tab de Hosts dentro de Sniffer dan click con el boton derecho del mouse y seleccionan Scan MAC.

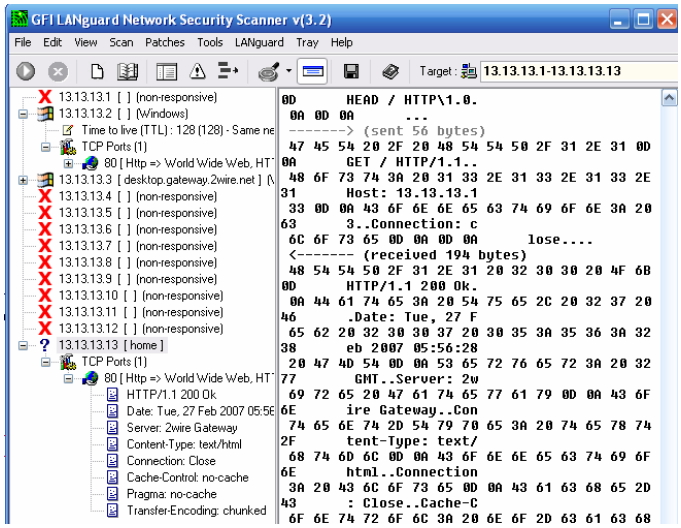


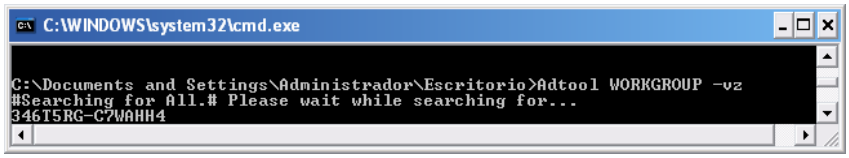


Si se desea conocer los servicios y servidores disponibles podemos ver dentro del portal del ruteador en la seccion del firewall los servidores que tienen puertos exteriores asignados.

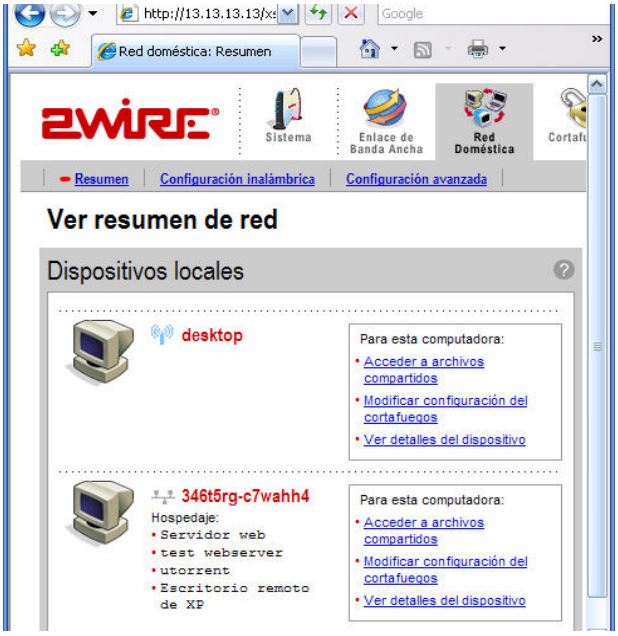


También podemos usar un programa como LAN Guard Network Scanner (http://www.languard.com) para conocer servicios y puertos abiertos de los hosts y utilizar el ADtool (http://www.securitynation.com) de napa.



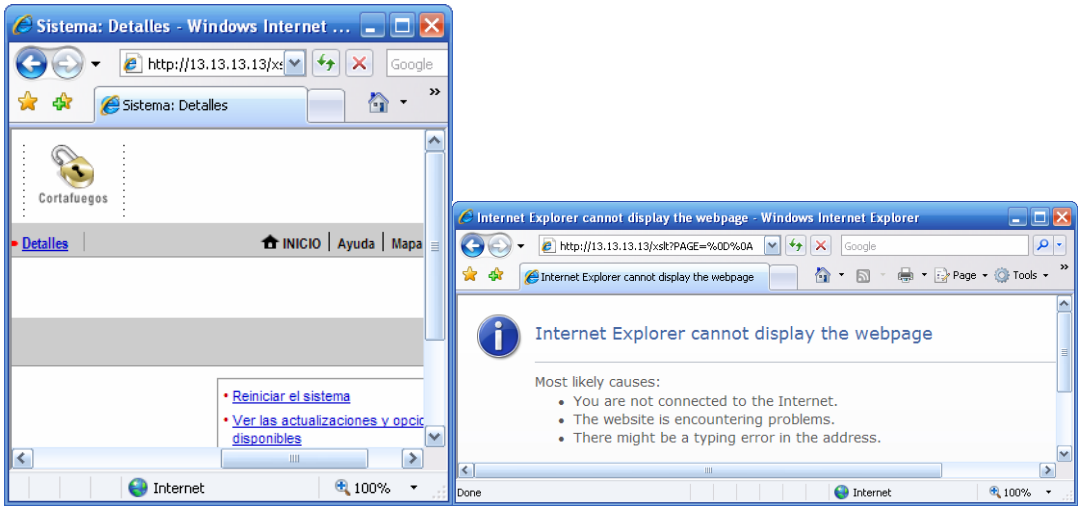


En algunos ruteadores es posible accesar a los recursos compartidos desde la misma interfaz del ruteador en la seccion Home Network.

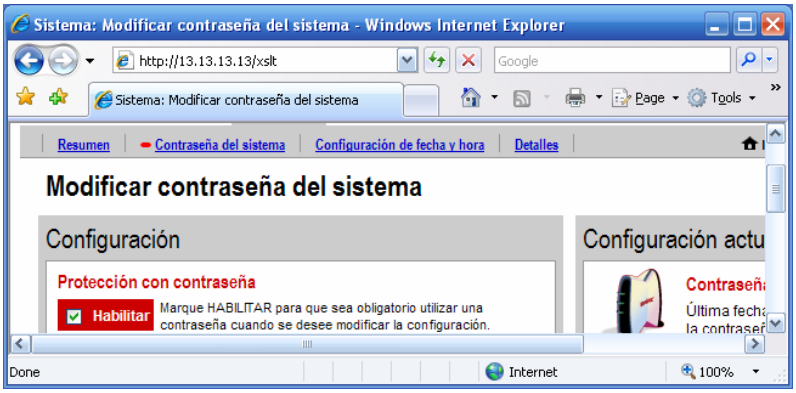


NEGACION DE SERVICIO

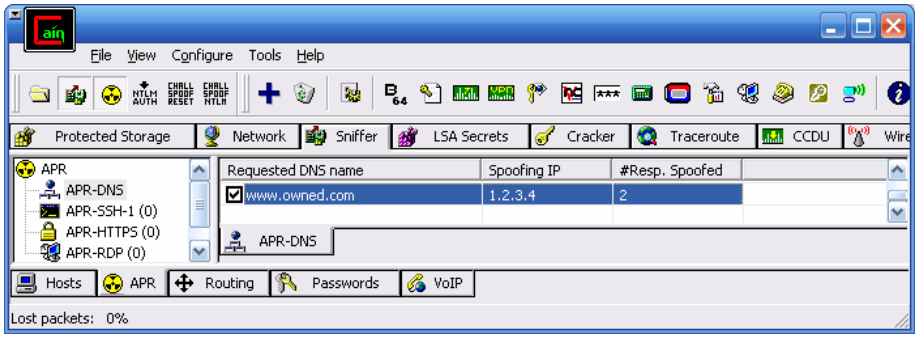
Se puede reiniciar el ruteador por unos minutos para negar el servicio a todos los clientes, desde el portal en la parte de Detalles en Sistema. Si no se cuenta con password para el acceso se puede utilizar una vulnerabilidad publicada por preth (http://www.mexhackteam.org/Publics/Topicos/get.php?id_codigo=2) para reiniciarlos.



También se puede modificar la configuración de DSL o DHCP y ponerle password para dejarlo sin funcionar correctamente mas tiempo.



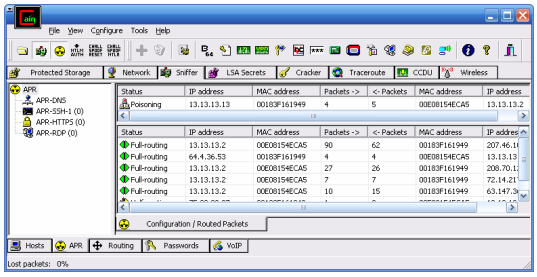
Utilizando Spoofing se puede bloquear al acceso a sitios específicos.

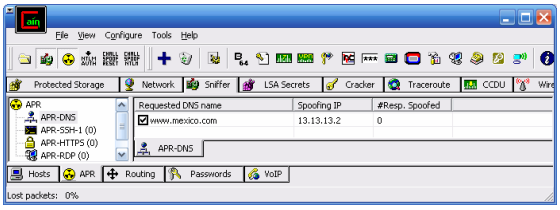


SPOOFING

Podemos instalar un servidor DNS, como Simple DNS (http://www.simpledns.com) y desde el portal del ruteador apuntar a nuestro servidor DNS y crear las entradas correspondientes, en Simple DNS presionar Ctrl-Q y llenar el campo de dominio e IP.

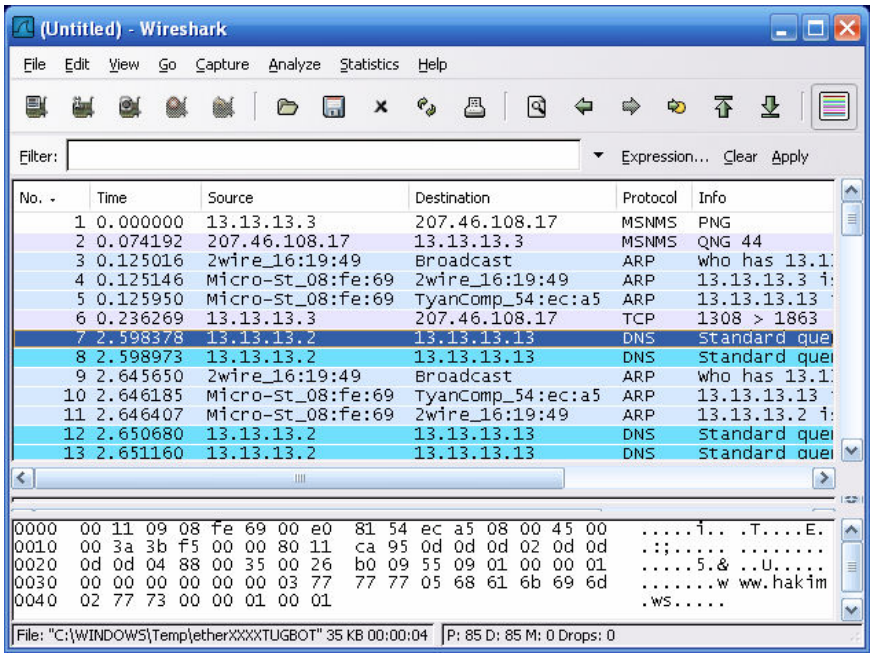
En Cain es sencillo hacer DNS Spoofing, dentro del Sniffer seleccionamos APR y seleccionamos el botón de + para habilitar APR Poison Routing, ahora en APR-DNS podemos agregar al Host e IP al que deseamos redirigir.



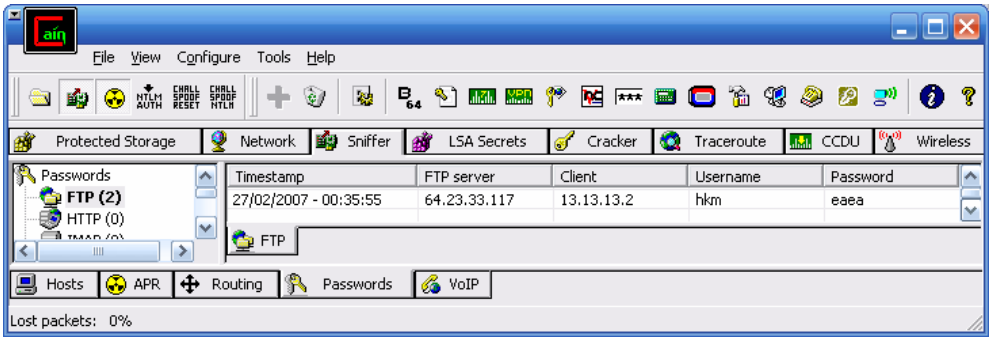


SNIFFING

Al habilitar APR Poison Routing con Cain podemos utilizar el WireShark (http://www.wireshark.com) y ver la comunicación del host que hayamos seleccionado.



También podemos ver los passwords que se envía en la parte de passwords del Cain.



hkm
27/2/7 Martes 12:41am