UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

DEPARTAMENTO DE ELECTRONICA

Seguridad Inalámbrica

Integrantes:
Manuel Ramírez
Carlos Polanco
Bernardo Farías

Profesor:
Agustín J. González

Introducción

WLAN es una amplia red inalámbrica que permite conectar un equipo a la red para acceder a Internet, impresoras y demás servicios sin necesidad de cables. Probablemente la desventaja más grande de las conexiones inalámbricas, es que es de fácil acceso para los hackers detectar éstas señales y obtener su información privada. La transferencia de datos confidenciales sobre una conexión inalámbrica plantea graves riesgos a su identidad como es su información personal, tales como números de tarjetas de crédito y datos bancarios. En la actualidad el tema de la seguridad inalámbrica es en el que más hincapié se está haciendo. El nivel de seguridad actual de estas redes está a años luz del de sus comienzos. Al ser el aire el medio de propagación empleado por las ondas, hace que la información esté expuesta a sufrir distintos tipos de ataques, por lo que es el inconveniente más importante que presentan las WLAN en cuanto a seguridad.

Resumen

Se investiga parte del funcionamiento de las redes inalámbricas, específicamente como está resguardada la información de quienes están conectados a la red. En el caso de Wi-fi esta funciona a base de encriptación de sus datos, en donde para poder saber el encriptado usado en la señal se debe conocer algún usuario y contraseña para así poder recibir correctamente los paquetes enviados desde la red. Es en este punto en donde se enfocan los ataques a las señales inalámbricas, en el lograr conocer de alguna manera el usuario y contraseña de la señal para poder recibir sus paquetes. Para impedir que personas no deseables obtengan tal información es que existen diferentes sistemas de seguridad, tales como el WEP, el WPA, el WPA2 entre otros, los cuales se rigen bajo normas del IEEE (instituto de ingenieros eléctricos y electrónicos) encargada de estandarizar estos protocolos de seguridad, eso si, todos basados en el sistema de usuario/contraseña. Ya logrando ingresar a la red WLAN es posible conocer lo que están descargando los usuarios de la red, logrando así conocer información relevante de estos, tales como contraseñas, números de tarjetas de crédito, información personal, etc. Siendo fundamental la protección de estas señales inalámbricas.

Objetivos

- Analizar las propuestas de seguridad actuales que hay para este tipo de redes.
- Identificar los diferentes tipos de ataques que se pueden encontrar actualmente.

Funcionamiento de la red inalámbrica

Seguridad a nivel de protocolo:

La seguridad a nivel de protocolo es la encargada de que los datos transmitidos por una WLAN no puedan ser descifrados por alguien ajeno a nuestra red. Para ello nuestra red ha de tener un algoritmo de codificación y gestión de claves.

En primer lugar, el IEEE publicó un algoritmo de seguridad opcional en el estándar 802.11 llamado WEP.

WEP:

El protocolo WEP (Wired Equivalent Privacy) es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), para cifrar todos los datos que se intercambian entre los clientes y el punto de acceso. RC4 consiste en generar una clave de forma pseudo-aleatoria que tiene la misma longitud que el texto original. A esta clave y al texto original se le aplica la operación lógica XOR (O exclusiva), obteniendo como resultado un texto cifrado. La clave pseudo-aleatoria se genera utilizando una clave secreta que define el propio usuario con una longitud de 40 o 104 bits y un vector de inicialización (IV) de 24 bits que lo genera aleatoriamente el sistema para cada trama. Pero wep tenia muchos defectos como era la reutilización del vector de inicialización, del cual se derivan ataques estadísticos que permiten recuperar la clave WEP. Por lo tanto la IEEE trabajaba en otro algoritmo más potente, pero la Alianza Wi-Fi lanzó un algoritmo alternativo y más potente que WEP, llamado WPA.

WPA:

WPA (Wifi Protect Access) es el protocolo de seguridad que lanzó la Alianza Wi-Fi para solucionar los problemas de seguridad del protocolo WEP.

Este protocolo implementa las siguientes mejoras:

- Autenticación del usuario mediante el IEEE 802.1x (control de acceso a red basada en puertos).
- Soluciona la debilidad del vector inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits).
- Utiliza el intercambio dinámico de claves mediante el protocolo TKIP (Temporal Key Integrity Protocol).
- El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, pero para comprobar la integridad de los mensajes, se cambió el código de detección de errores CRC-32 por uno nuevo llamado MIC (Message Integrity Code).

Posteriormente el IEEE publicó el estándar 802.11i, también conocido como WPA2.

WPA2:

Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser mucho más seguro. Incluye el intercambio dinámico de la clave, un cifrado mucho más fuerte, y la autenticación de usuario, pero añade las mejoras siguientes:

- Nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque simétrico. Utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes.

Intercepción de paquetes

Ataques activos :

•*Suplantación :* Consiste en la obtención de la identidad de un usuario autorizado por parte del atacante. Este tipo de ataque normalmente incluye otros tipos de ataques activos. Como ejemplos de este tipo de ataques se tiene: Man in the Middle, MAC Spoofing y ARP Poisoning.

•*Reactuación:* Consiste en capturar mensajes legítimos y repetirlos para producir un efecto no deseado, como podría ser por ejemplo repetir ingresos de dinero, envío masivo de de emails, etc.

•*Modificación :* Consiste en capturar mensajes enviados por un usuario autorizado y modificarlos, borrarlos o reordenarlos, para producir un efecto no autorizado, como podría ser por ejemplo capturar un mensaje que diga “Realizar un ingreso en efectivo en la cuenta A”, y modificar el número de cuenta por “B”.

•*Denegación de Servicio* : Consiste en evitar que los clientes legítimos consigan acceder a la red o a un servicio que esta ofrezca. Existen varias formas de hacer que esto sea posible, como por ejemplo: inyectar mucho tráfico a la red para disminuir su rendimiento o colapsarla, saturar a peticiones de autenticación a un Punto de Acceso inalámbrico, etc.

Ataques pasivos :

•*Sniffing* :Consiste en capturar el tráfico de una red para posteriormente poder obtener datos de ellas como por ejemplo direcciones IP, direcciones MAC, direcciones de correo electrónico, etc.

• *Análisis de tráfico :* Consiste en obtener información mediante el análisis del tráfico y sus patrones, como por ejemplo a que hora se encienden ciertos equipos, cuanto tráfico se envía, a que horas hay más tráfico, etc.

En éste informe se centrará en el ataque activo ARP Poisoning.

Ataque ARP Poisoning

Primero se definirá el ARP (Address Resolution Protocol), que es un protocolo de la capa de enlace de datos responsable de encontrar la dirección MAC que corresponde a una determinada dirección IP. Su funcionamiento, radica en enviar un paquete (ARP request) a la dirección de difusión de la red que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.

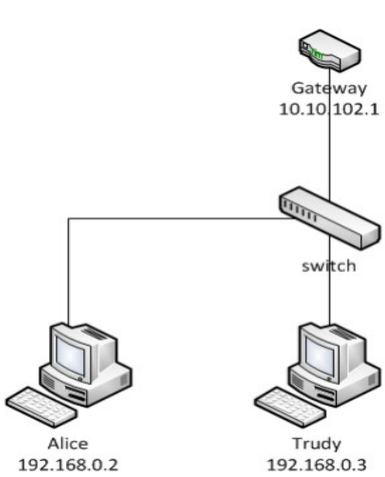
ARP Poisoning:

- Trudy lanza un *ARP request* a la dir. *broadcast* preguntando por la MAC de la IP 192.168.0.1 (*Gateway*)
- El *GW* contesta con *ARP reply* indicando cuál es su dir. MAC.
- Trudy lanza un *ARP request* a la dir. *broadcast* preguntando por la MAC de la IP 192.168.0.2 *(Alice*)
- Alice contesta con su dir. MAC.

Proceso normal

- Trudy envía reiteradamente *ARP reply* falsos, a Alice y al *GW*, asociando la IP de ambos con su propia MAC.
  - A Alice le hace creer que él es el *GW*
  - Al *GW* le hace creer que él es Alice
  - Todo el tráfico que transite entre el *GW* y Alice pasará a través de Trudy

spoof



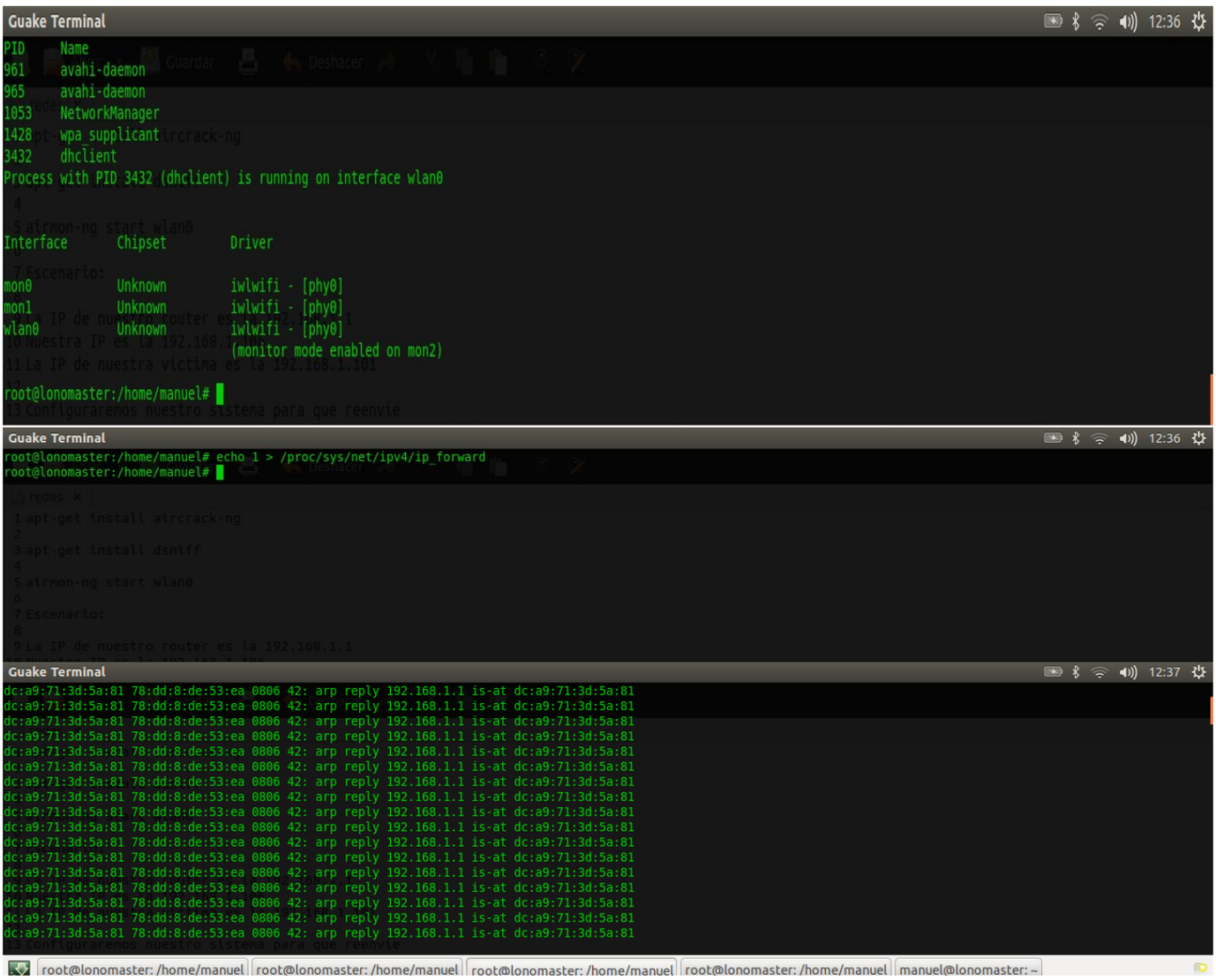
Demostración de ataque ARP

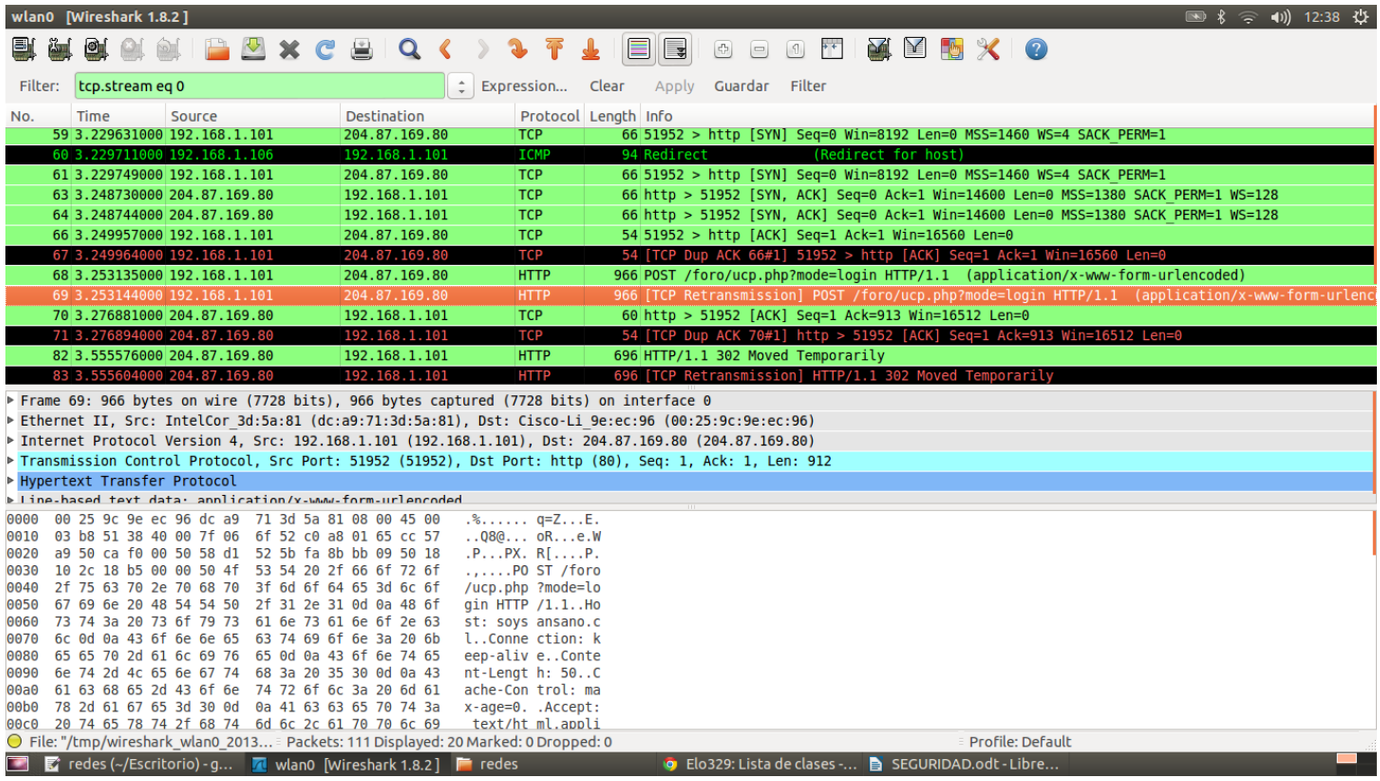
- Herramientas a necesitar: $># apt-get install aircrack-ng && apt-get install dsniff
- Activando nuestra tarjeta de red en modo monitor:$># airmon-ng start wlan0
- Con el escenario siguiente: La IP de nuestro router :192.168.1.1 Nuestra IP :192.168.1.106

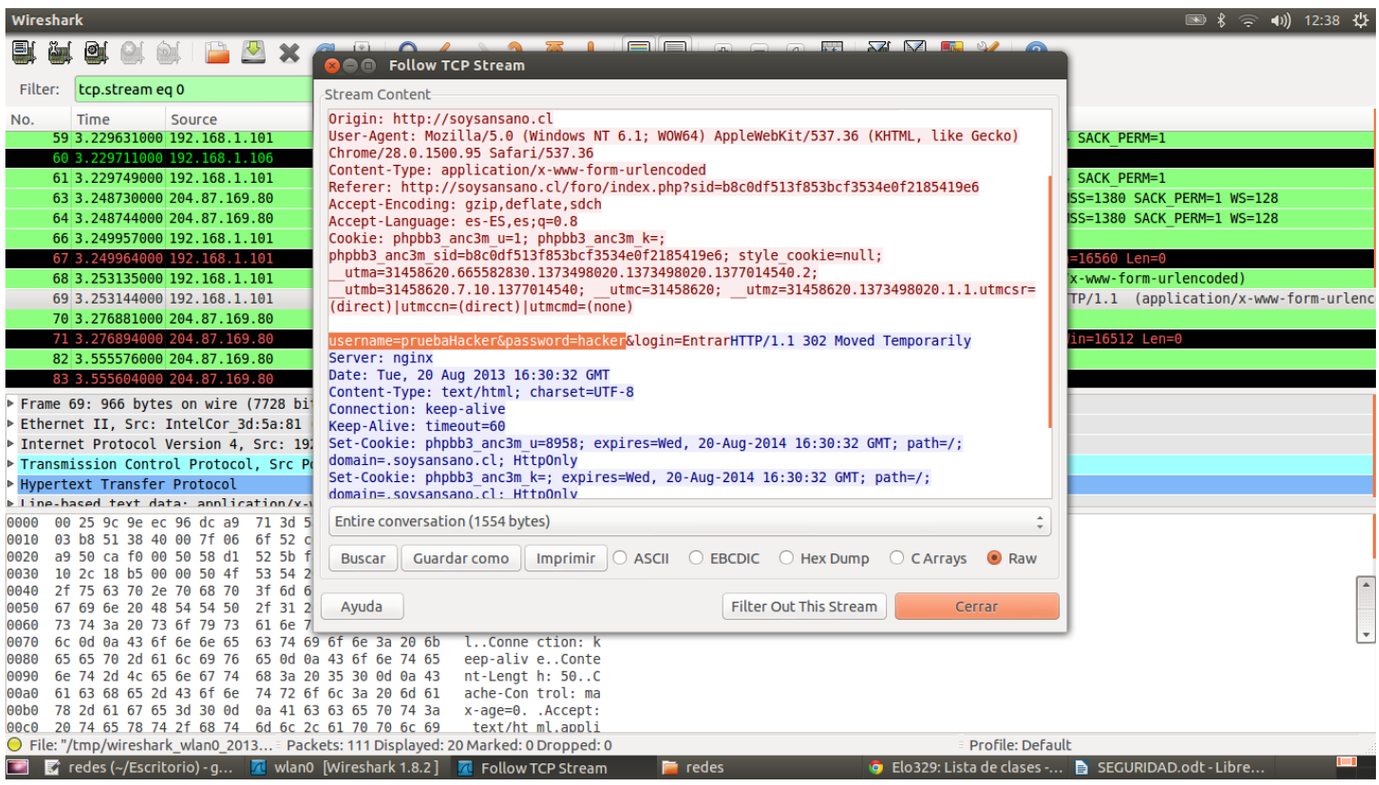
  La IP de nuestra víctima: 192.168.1.101
- Configuraremos nuestro sistema para que reenvíe todos los paquetes a sus verdaderos destinatarios mediante el comando: $># echo 1 > /proc/sys/net/ipv4/ip_forward
- Ahora procedemos a envenenar las tablas: Ponemos cada uno de estos comandos en una consola diferente para indicar que nuestra MAC es la MAC asociada a la IP del router y que también es la MAC asociada a la IP de nuestra víctima:

  $> # arpspoof -i wlan0 -t 192.168.1.1 192.168.1.101

  $> # arpspoof -i wlan0 -t 192.168.1.101 192.168.1.1







- Para terminar nuestra demostración se aprecia los datos capturados de un login y su respectiva password en el sitio http://www.soysansano.cl

Soluciones que se deben implementar para el ataque ARP

Un método para prevenir el **ARP Poisoning**, es el uso de tablas ARP estáticas, es decir añadir entradas estáticas ARP, de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP. Sin embargo, esta no es una solución práctica, sobre todo en redes grandes, debido al enorme esfuerzo necesario para mantener las tablas ARP actualizadas: cada vez que se cambie la dirección IP de un equipo, es necesario actualizar todas las tablas de todos los equipos de la red.

Conclusiones

En el ámbito personal o doméstico, la seguridad que existe actualmente con WPA2 es suficiente, ya que, la importancia de la información que se puede llegar a obtener en este tipo de ámbitos no merece la pena la dedicación de tiempo y recursos para poder obtenerla.

En cambio, en el ámbito empresarial, la cosa es distinta., WPA2 no es suficiente y se debe tener mucha mas seguridad, pero aun así este tipo de redes nunca sera completamente segura.

Referencias

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html>

<http://www.wi-fi.org/>

<http://www.wikipedia.org/>

<http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf>

<http://www.docstoc.com/docs/27566993/Seguridad-en-Redes-Wireless-80211-abg>

<http://www.wifiway.org/>

<http://www.seguridadwireless.net/hwagm/manual-aircrack-ng-castellano.html>