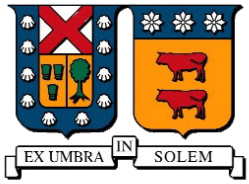


UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Departamento de Electrónica
Universidad Técnica Federíco Santa María

Redes de Computadores

Proyecto final

” Funcionamiento de aplicación LogMeIn Hamachi”

ELO-322

Valparaíso

Alumno		Danilo Ávila Cárcamo	201321032-5
		Patrick Guicharrousse Vargas	201121023-6
		Miguel San Martín Agurto	201121074-3
Fecha	:	20/06/2016	
Profesor	:	Agustín González	

1 Resumen

Este proyecto consiste en la explicación del funcionamiento de la aplicación LogMeIn Hamachi, la cual sirve para crear redes privadas virtual (VPN) e intercomunicar distintos periféricos sin importar en el lugar físico en cual se encuentren. Para esto se analizarán los paquetes enviados mientras se establece la conexión mediante wireshark utilizando una aplicación en concreto la cual corresponde al videojuego "Counter Strike Source", pero también veremos que otras aplicaciones de las cuales se puede sacar provecho.

2 Introducción

Las redes de área local, también conocidas como LAN, nos permiten compartir información y conectar computadores de forma rápida y como dice su nombre local, sin embargo con el auge del Internet es necesario para las empresas, universidades y hasta para usuarios comunes de internet lograr esta mismas conexión LAN entre computadores que estén conectados al Internet y no en una conexión de área local.

Para lograr este objetivo se crearon las Redes Virtuales Privadas también conocidas por sus siglas en ingles VPN, las que logran crear sobre redes publicas conexiones LAN con todas sus funcionalidades y seguridad.

La aplicación LogMeIn Hamachi es un software gratuito que permite crear y gestionar de manera fácil y rápida redes VPN. En este proyecto se estudiará como opera Hamachi para poder crear redes VPN y como es que los computadores se comunican al estar conectados mediante este software, y las principales aplicaciones que se le pueden dar tanto en el ámbito empresarial como en el domestico.

3

3.1 ¿Que es LogMeIn Hamachi y para que sirve?

LogMeIn Hamachi es una aplicación gratuita que configura redes privadas virtuales(VPN) capaz de establecer una conexión a través de Internet y simular una red de área local formada por computadoras remotas.Comúnmente también genera vínculos directos entre computadoras que están bajo firewalls de NAT sin necesitar reconfiguración alguna. Dentro de los posibles usos que se le pueden a estas redes privadas virtuales encontramos las siguientes:

- Acceso a una red de trabajo mientras se está de viaje: Los VPNs se usan con frecuencia para aquellos profesionales que viajan y necesitan entrar en su red de trabajo mientras están lejos. Usar este método permite que los recursos se mantengan seguros porque en están en la nube.
- Acceso a una red del hogar mientras se está de viaje: También se puede usar para entrar al ordenador que hemos dejado en casa, como si estuviésemos usando una LAN (Local Network Area).
- Esconde los datos de navegación: Por ejemplo, si estás usando un Wi-Fi público, de esos que están disponibles sin contraseña en restaurantes y centros comerciales, todo lo que visites que no tenga conexión HTTPS estará visible para cualquiera que sepa dónde mirar. En cambio si tienes un VPN, lo único que podrán ver es la conexión al VPN; todo lo demás será anónimo.
- Entrar en sitios con bloqueo geográfico: Usualmente los problemas de bloqueo de región suelen pedir que estés en Estados Unidos. Esto sucede con Hulu, Pandora o el catalogo de Netflix que es más grande y completo en este país. A veces pasa también en ciertos vídeos de YouTube. Para evitar estas restricciones, sólo hay que usar un VPN que tenga localización de USA.
- Evitar la censura en Internet: Para aquellos gobiernos que deciden censurar ciertos sitios web, un VPN funciona muy bien para acceder a ellos sin problemas.
- Jugar videojuegos en LAN: Muchos videojuegos tienen la opción de poder jugar vía LAN, pero a veces existe el impedimento de poder reunirse en un lugar físico. De esta forma se puede jugar con tus amigos en la comodidad de tu hogar.

3.2 Funcionamiento de Hamachi

Hamachi es un sistema VPN de administración centralizada que consiste en un cluster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios. El software cliente agrega una interfaz de red virtual al ordenador que es utilizada tanto para interceptar el tráfico VPN saliente como para inyectar el tráfico VPN entrante. El tráfico saliente enviado por el sistema operativo a esta interfaz es entregado al software cliente, que lo cifra y lo autentifica y luego lo envía al nodo de destino a través de una conexión UDP. Hamachi se encarga del tunelamiento del tráfico IP, incluido el broadcast y el multicast. Cada cliente establece y mantiene una conexión de control con el Cluster servidor. Cuando la conexión está establecida, el cliente entra en una secuencia de identificación de usuario, seguida de un proceso de descubrimiento y sincronización de estado. El paso de autentificación de usuario autentifica al cliente contra el servidor y viceversa. El descubrimiento es utilizado para determinar la topología de la conexión a Internet del cliente, y más concretamente para detectar la presencia de dispositivos cortafuegos y servidores NAT. El paso de sincronización extrae una vista del cliente de sus redes privadas sincronizadas con los otros miembros de esas redes. Cuando un miembro de una red se conecta o se desconecta, el servidor da instrucciones a los otros nodos de la red para que inicien o detengan túneles con dicho miembro. Cuando se establecen túneles entre los nodos, Hamachi utiliza una técnica de NAT transversal asistido por servidor, similar al "UDP hole punching" ("perforadora de agujeros UDP").

3.3 Direccionamiento

A cada cliente Hamachi se le asigna una dirección IP desde el bloque de direcciones 5.0.0.0/8 cuando inicia una sesión en el sistema por primera vez, y es en adelante asociada con la clave de cifrado pública del cliente. Mientras el cliente retenga esta clave, puede autentificarse en el sistema y utilizar esa dirección IP 5.X.X.X Esta asignación es sin embargo no oficial, como RIPE NCC(Centro de Coordinación de redes IP europeas) tiene los derechos para realizar asignaciones en ese rango. La dirección IP en adelante se asocia con el cliente público con Criptografía asimétrica. Siempre y cuando el cliente conserva su clave, puede conectarse al sistema y utilizar esta dirección IP. La red 5.0.0.0/8 es utilizada para evitar colisiones con redes IP privadas que podrían estar utilizándose en la parte cliente. Específicamente, las redes privadas 10.0.0.0/8, 172.16.0.0/16 y 192.168.0.0/24. Actualmente debido a que RIPE NCC ha aumentado el uso de las direcciones ip 5.X.X.X se ha realizado un cambio en el direccionamiento hecho por hamachi reasignando a los usuarios a direcciones ip 25.X.X.X. Según el comunicado oficial de hamachi, la elección de esta dirección fue hecha ya que rima 25/8 con 5/8 además de que este conglomerado de direcciones esta relacionadas con la agencia gubernamental británica hace dos décadas y afirman que no poseen ningún usuario Hamachi desde este espacio de direcciones, y es muy poco probable que el público en general tendría que acceder a una de estas direcciones IP.

3.4 Compatibilidad

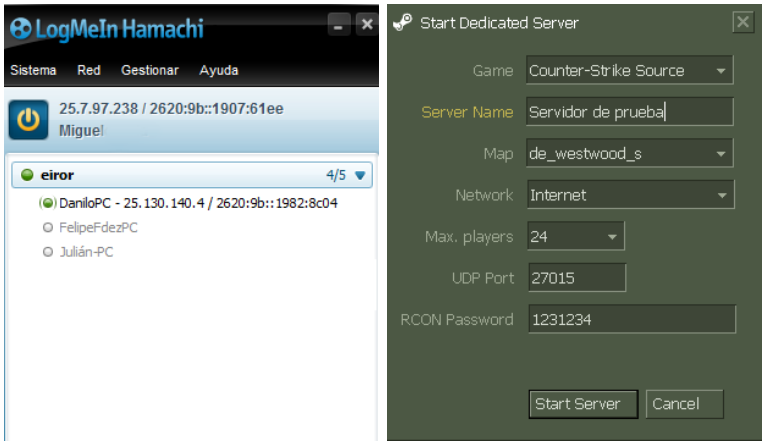
Las generaciones actuales de Hamachi están disponibles para los siguientes sistemas operativos:

- Microsoft Windows 2000, XP, Server 2003, Vista, Windows 7 y Windows 8.
- Mac OS X (beta)
- Linux (beta)

Muchos usuarios de Windows Vista habían experimentado problemas de compatibilidad y conexión mientras se utiliza Hamachi. El 30 de marzo de 2007, el software incluye ahora Vista tweaks, que responde a estos problemas relacionados con el sistema operativo, entre otras soluciones específicas.

3.5 Análisis mediante wireshark

Para realizar este análisis fue necesario escoger una de las tantas aplicaciones que se le puede dar a este software, la seleccionada fue un videojuego de disparo en primera persona llamado "Counter Strike Source" el cual es consiste en el enfrentamiento de terroristas en contra de un grupo de antiterroristas. Comenzamos creando una red en hamachi e invitando a nuestros amigos a unirse a esta VPN, luego creamos el servidor de counter strike donde disponemos la posibilidad de asignar el puerto UDP que queremos utilizar, por defecto el numero de este puerto es 27015,tan solo con estos dos pasos dar inicio a la partida y a comenzar la captura a través de wireshark.



(a) Red de Hamachi (b) Servidor de Counter Strike

Figure 1: Configuración de Hamachi y el servidor

Para esta prueba fueron tres computadores utilizados de los cuales uno actuo como administrador del servidor de Hamachi y el juego

2278	30.9740980	25.7.97.238	25.0.209.219	UDP	123	Source port: 27015	Destination port: 27005
2279	30.9742230	25.7.97.238	25.130.140.4	UDP	115	Source port: 27015	Destination port: 27005
2280	30.9902980	25.0.209.219	25.7.97.238	UDP	110	Source port: 27005	Destination port: 27015
2281	30.9903470	25.0.209.219	25.7.97.238	UDP	102	Source port: 27005	Destination port: 27015
2282	31.0219500	25.130.140.4	25.7.97.238	UDP	108	Source port: 27005	Destination port: 27015
2283	31.0345920	25.7.97.238	25.0.209.219	UDP	126	Source port: 27015	Destination port: 27005
2284	31.0347400	25.7.97.238	25.130.140.4	UDP	116	Source port: 27015	Destination port: 27005
2285	31.0349580	25.0.209.219	25.7.97.238	UDP	92	Source port: 27005	Destination port: 27015
2286	31.0836410	25.0.209.219	25.7.97.238	UDP	90	Source port: 27005	Destination port: 27015
2287	31.0897380	25.130.140.4	25.7.97.238	UDP	104	Source port: 27005	Destination port: 27015
2288	31.0932060	25.7.97.238	25.0.209.219	UDP	146	Source port: 27015	Destination port: 27005
2289	31.0935060	25.7.97.238	25.130.140.4	UDP	139	Source port: 27015	Destination port: 27005
2290	31.1252000	25.7.97.238	25.0.209.219	UDP	148	Source port: 27015	Destination port: 27005
2291	31.1255020	25.7.97.238	25.130.140.4	UDP	119	Source port: 27015	Destination port: 27005
2292	31.1420520	25.0.209.219	25.7.97.238	UDP	102	Source port: 27005	Destination port: 27015
2293	31.1473750	25.130.140.4	25.7.97.238	UDP	102	Source port: 27005	Destination port: 27015
2294	31.1833700	25.7.97.238	25.0.209.219	UDP	146	Source port: 27015	Destination port: 27005
2295	31.1835140	25.7.97.238	25.130.140.4	UDP	117	Source port: 27015	Destination port: 27005

Figure 2: Paquetes capturados durante el juego

906	31.1119390	25.130.140.4	25.7.97.238	UDP	80	Source port: 27005	Destination port: 27015
907	31.1548660	25.7.97.238	25.130.140.4	UDP	76	Source port: 27015	Destination port: 27005
908	31.1719930	25.130.140.4	25.7.97.238	UDP	80	Source port: 27005	Destination port: 27015
909	31.2223980	25.7.97.238	25.130.140.4	UDP	657	Source port: 27015	Destination port: 27005
910	31.2321040	25.130.140.4	25.7.97.238	UDP	80	Source port: 27005	Destination port: 27015
911	31.2385500	25.7.97.238	25.130.140.4	UDP	500	Source port: 27015	Destination port: 27005
912	31.2938530	25.130.140.4	25.7.97.238	UDP	92	Source port: 27005	Destination port: 27015
913	31.3035210	25.7.97.238	25.130.140.4	UDP	480	Source port: 27015	Destination port: 27005
914	31.3538210	25.130.140.4	25.7.97.238	UDP	78	Source port: 27005	Destination port: 27015
915	31.3710670	25.7.97.238	25.130.140.4	UDP	189	Source port: 27015	Destination port: 27005
916	31.3763920	25.7.97.238	25.130.140.4	UDP	150	Source port: 27015	Destination port: 27005
917	31.4123840	25.130.140.4	25.7.97.238	UDP	78	Source port: 27005	Destination port: 27015
918	31.4290500	25.130.140.4	25.255.255.255	UDP	305	Source port: 54915	Destination port: 54915
919	31.4366450	25.7.97.238	25.130.140.4	UDP	177	Source port: 27015	Destination port: 27005

Figure 3: Paquetes capturados durante el juego

Las IPs que se ven en las imágenes corresponden a:

- 25.7.97.238 Administrador
- 25.130.140.4 Usuario 1
- 25.0.209.219 Usuario 2

Cabe mencionar que estas no corresponden a las IPs reales de cada computador sino a las que son asignadas mediante Hamachi.

En las imágenes se puede apreciar que existe una constante comunicación con el puerto asignado a la hora de crear el servidor (27015), este puerto corresponde al administrador del servidor mientras que el puerto 27005 corresponde a los otros usuarios conectados a este. Podemos apreciar en la primera imagen (correspondiente a la captura de paquetes por parte del administrador del servidor) que este realiza conexiones e intercambio de paquetes con ambos de los usuarios conectados al servidor. En cambio en la captura de paquetes de uno de los usuarios se aprecia que este solo realiza conexiones con el administrador, a partir de estos datos asumimos que los dos usuarios no realizan conexiones ni intercambian paquetes de forma directa pese a que estén conectados en la misma vpn, y el administrador del servidor hace de mediador entre estos dos. Hay que destacar que el protocolo utilizado en el envió de los paquetes es UDP y esto es lógico ya que en aplicaciones como streaming, videollamadas o videojuegos no es necesario que se asegure la recepción de cada paquete enviado por que no afecta totalmente la comunicación entre el remitente y destinatario. Además queda explícitamente determinado a la hora de crear el servidor del juego en el campo UDP port. En general si analizamos los paquetes enviados y recibidos durante esta prueba podemos encontrar muchas similitudes en cada uno de ellos, como por ejemplo el tamaño. Cada paquete enviado por cada usuario tiene un tamaño promedio de 68 bytes, y la data de cada uno de estos paquetes no supera los 40 bytes. Como se menciono anteriormente el protocolo utilizado es UDP(17) y cada uno de ellos posee un time to live de 128, también como el paquete es pequeño no es necesario la fragmentación de este por lo que el campo flags se mantiene en 0x00 y por consiguiente fragment offset en cero. Por último el campo de header checksum se mantiene deshabilitado para todo los paquetes. En resumen la única diferencia entre paquetes son las pequeñas variaciones en cuanto el tamaño que se mantienen dentro del promedio como también el campo de destinatario y fuente de quien emite cada paquete.

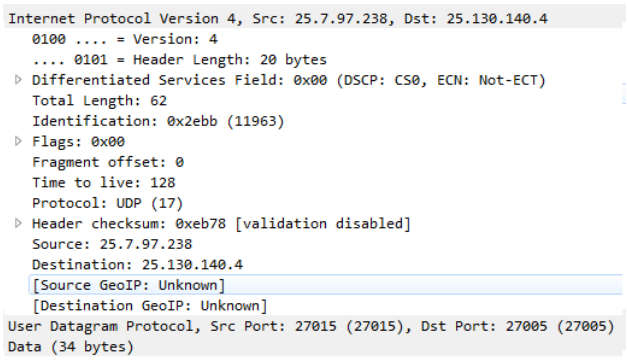


Figure 4: Detalles del paquete

4 Conclusión

A partir de la investigación realizada específicamente al software Hamachi y de las pruebas que se han realizado podemos concluir que si bien existen abundantes documentos que explican como operan las redes privadas virtuales no existe mucha información detallada de como Hamachi opera e integra las VPN, solo explica a grandes rasgos el funcionamiento y direccionamiento por lo que resulto difícil realizar el estudio en detalle sobre la aplicación. A pesar de la alta gama de aplicaciones y funciones que se le pueden dar a este software se escogió la que nos resulto más familiar, la cual corresponde al enfoque de los videojuegos.Durante todas las pruebas realizadas nos propusimos analizar los tipos de paquetes que se enviaban, con el fin de realizar comparaciones y la caracterización de ellos.
Hamachi posee muchos puntos a favor uno de ellos es que no es necesario realizar la compra de este software, ya que solo con la versión gratuita nos basta para hacer pequeñas vpn y comunicarnos con otros periféricos. También puede ser difícil para un usuario sin conocimiento sobre redes la creación de VPN de forma manual debido a la gran cantidad de variables y conceptos técnicos que se deben manejar, por lo que Hamachi facilita bastante el este trabajo. Finalmente, el software Wireshark ha sido de gran utilidad a la hora de capturar paquetes, en este caso en particular como también en el resto de tareas realizadas durante el semestre. El buen uso y manejo de este, puede ser de gran utilidad tanto para este curso como también en otros contextos.

5 Referencias

https://secure.logmein.com/CL/welcome/documentation/ES/pdf/Hamachi/LogMeIn_Hamachi_GettingStarted.pdf

https://secure.logmein.com/welcome/documentation/EN/pdf/Hamachi/LogMeIn_Hamachi_SecurityWhitepaper.pdf

http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

https://community.logmein.com/t5/Hamachi/Hamachi-and-DINSA-Ministry-of-Defense/td-p/87674

https://blog.logmein.com/products/changes-to-hamachi-on-november-19th

6 Anexos

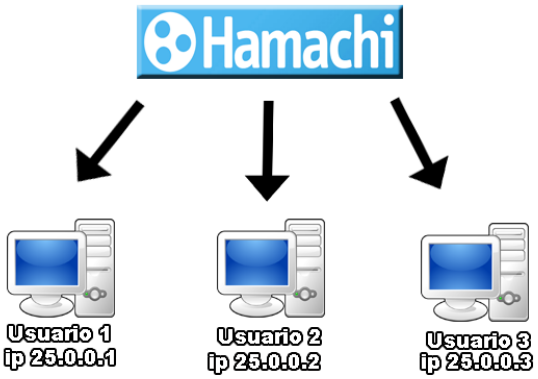


Figure 5: Direccionamiento de Hamachi

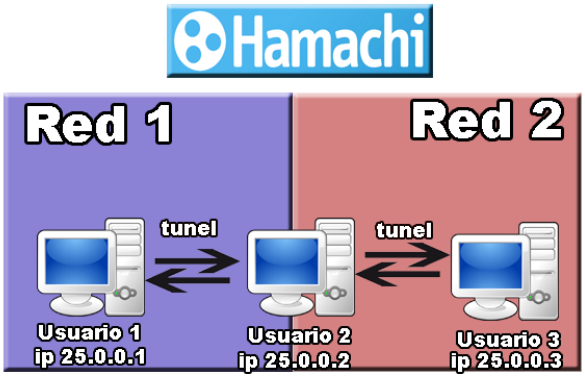


Figure 6: Comunicación entre periféricos