UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

"ANÁLISIS DE LAS TÉCNICAS DE TUNELIZADO POR HTTP PARA EVITAR ATAQUES HACKER"

Estudiante:

Braulio Gustavo Ochoa Clavijo

Tutor:

Ing. Marco Lituma Orellana

Cuenca – Ecuador

Noviembre, 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Ing. Marco Lituma Orellana

Director de Tesis

CERTIFICA:

Que el presente trabajo de investigación **"Análisis de la técnicas de tunelizado por http para evitar ataques hacker"**, realizado por el Sr. Braulio Gustavo Ochoa Clavijo, egresado de la Facultad de Sistemas Informáticos, se ajusta a los requerimientos técnico-metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 7 de Noviembre de 2011

_____

Ing. Marco Lituma Orellana

DIRECTOR DE TESIS

UNIVERSIDAD TECNOLÓGICA "ISRAEL"

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

Los contenidos, argumentos, exposiciones, conclusiones son de responsabilidad del autor. El documento de tesis con título **"Análisis de las técnicas de tunelizado por http para evitar ataques hacker"** ha sido desarrollado por Braulio Gustavo Ochoa Clavijo con C. C. No. 010388570-3, persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Braulio Ochoa Clavijo

UNIVERSIDAD TECNOLÓGICA "ISRAEL"

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

Yo, Braulio Gustavo Ochoa Clavijo, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: "Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad".

Cuenca, 7 de Noviembre del 2011

_____

Braulio Ochoa Clavijo

C.C. No. 010388570-3

DEDICATORIA

La presente tesis la dedico a mis hijos Andrés Sebastián y Mateo Nicolás, quienes son mi apoyo y mi fuerza para seguir adelante. A mis padres que siempre me han apoyado moralmente en todos los momentos de mi vida, y a toda mi familia que de una u otra forma me ayudaron para la culminación de mis estudios superiores.

Braulio Ochoa C.

AGRADECIMIENTO

Un agradecimiento primero a Dios y luego uno muy sincero a todos mis profesores por impartirme los conocimientos que hoy poseo, a la institución que me acogió y a todas las personas que directa o indirectamente colaboraron para mi preparación académica.

Braulio Ochoa C.

RESUMEN

La seguridad en el envío y recepción de información en una red, como por ejemplo Internet, siempre ha sido un inconveniente que durante muchos años se ha venido investigando en este tema, para mejorar la protección de la información que se transmite, ya que terceras personas con malas intenciones como hackers podrían aprovecharse de las vulnerabilidades de una red para captar la información que por ella circulan.

Es por esto que se dio lugar a protocolos que permiten crear un túnel entre computadoras de una red, protegiendo los datos enviados entre estas maquinas y así evitar que terceras personas maliciosas puedan tener acceso a la información que se envía por la red.

Un ejemplo de estos protocolos es el protocolo SSH (Secure SHell) que permite conectarse remotamente a otra computadora y con la capacidad de poder manejar por completo dicha máquina mediante comandos, además este protocolo permite gestionar de manera eficiente claves públicas, así también este protocolo permite pasar datos por un canal tunelizado de forma segura.

Así también explicaremos brevemente otro protocolo criptográfico como lo es el SSL que brinda comunicaciones seguras por Internet.

Y el IPsec un protocolo muy usado en VPN’s e internet ya que brinda seguridades a nivel de IP, cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP en un flujo de datos.

También tomaremos el protocolo PPTP (Point to Point Tunneling Protocol) el cual principalmente se utiliza para la implementación de VPN`s (redes privadas virtuales).

Y finalmente abordaremos al protocolo IEEE 802.1Q que fue creado para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, y con una ventaja grandísima en comunicaciones como lo es que este protocolo permite esta comunicación entre redes pero sin ningún tipo de interferencia entre ella.

Espero que el presente trabajo sirva para dar a conocer de forma clara y breve la utilidad de estos protocolos y sus aplicaciones para comunicaciones seguras.

SUMMARY

Safety in the sending and receiving information over a network such as Internet has always been a problem for many years has been investigating this issue, to improve protection of information transmitted, and that third parties as malicious hackers could exploit the vulnerabilities of a network to capture the information which it circulates.

This is why we are led to protocols that create a tunnel between computers on a network, protect data sent between these machines and thus prevent malicious third parties can access information sent over the network.

An example of these protocols is SSH (Secure SHell) which allows to connect remotely to another computer and the ability to completely manage the machine through commands, in addition this protocol allows to efficiently manage public keys, so this protocol allows a channel to pass data securely tunneled.

So also briefly explain another cryptographic protocol such as SSL that provides secure Internet communications.

And the widely used protocol IPsec VPN's and Internet and providing security at the IP level, whose function is to ensure the IP communications by authenticating and / or encrypting each IP packet in a data stream.

We will also PPTP (Point to Point Tunneling Protocol) which is used to mainly implementing `s VPN (virtual private networks).

And finally board the IEEE 802.1Q protocol was established to develop a mechanism to allow multiple networks transparently share the same physical

environment, and a very great advantage in communications as it is that this protocol allows the communication between networks without any type of interference among them.

I hope this report will serve to make known clearly and briefly the utility of these protocols and applications for secure communications.

TABLA DE CONTENIDOS

CAPITULO I: ANTEPROYECTO 1
1. PLANTEAMIENTO DEL PROBLEMA 1
TEMA DE INVESTIGACIÓN 1
1.1 ANTECEDENTES 1
1.2 DIAGNOSTICO O PLANTEAMIENTO DE LA PROBLEMÁTICA GENERAL 2
1.2.1. CAUSA-EFECTO 2
1.3. PRONÓSTICO Y CONTROL DE PRONÓSTICO 3
1.3.1. PRONÓSTICO 3
1.3.2. CONTROL DE PRONÓSTICO 3
1.4. FORMULACIÓN DE LA PROBLEMÁTICA ESPECÍFICA 4
1.4.1 PROBLEMA PRINCIPAL 4
1.4.2. PROBLEMAS SECUNDARIOS 4
1.5. OBJETIVOS 4
1.5.1. OBJETIVO GENERAL 4
1.5.2. OBJETIVOS ESPECÍFICOS 5
1.6. JUSTIFICACIÓN 5
1.6.1. JUSTIFICACIÓN TEÓRICA 5
1.6.2. JUSTIFICACIÓN METODOLÓGICA 6
1.6.3. JUSTIFICACIÓN PRÁCTICA 6
1.7. MARCO DE REFERENCIA 6
1.7.1. MARCO TEÓRICO 6
1.7.2. MARCO ESPACIAL 9
1.7.3. MARCO TEMPORAL 9
1.8. METODOLOGÍA Y CRONOGRAMA 9
1.8.1. METODOLOGÍA: 9
1.8.2. CRONOGRAMA: 10
CAPITULO II: MARCO DE REFERENCIA 11
2.1 MARCO TEORICO 11
2.1.1 INTERNET 11
2.1.10 PROTOCOLO HTTP 25
2.1.11 HACKER 26

2.1.2 PROTOCOLO 16
2.1.3 PROTOCOLOS DE SEGURIDAD 17
2.1.4 TÚNEL 18
2.1.5 PROTOCOLO SSH 19
2.1.6 PROTOCOLO SSL 20
2.1.7 PROTOCOLO IPSEC 21
2.1.8 PROTOCOLO PPTP 22
2.1.9 PROTOCOLO IEEE 802.1Q 24
2.2 Marco Espacial 27
2.3 Marco Temporal 27
2.4 Marco Legal 27
CAPITULO III: METODOLOGÍA 30
3.1 ENCUESTA 30
3.2 ENTREVISTA 39
CAPITULO IV: DESARROLLO 45
4.1 PROTOCOLO 45
4.1.1 PROTOCOLOS DE SEGURIDAD 45
4.2 TÚNEL 47
4.2.1 PROTOCOLO SSH 50
4.2.2 PROTOCOLO SSL 54
4.2.2.1 ESTÁNDARES 59
4.2.4 PROTOCOLO IPSEC 63
4.2.4 PROTOCOLO PPTP 71
4.2.5 PROTOCOLO IEEE 802.1Q 73
4.3 PROTOCOLO HTTP 75
4.3.2 CÓDIGOS DE HTTP 82
4.3.3 MÉTODOS 85
4.3.4 CABECERAS 88
4.3.4.1 Generales 88
4.3.4.2 De petición 89
4.3.4.3 De respuesta 90
4.3.4.4 Cabeceras de entidad 91
4.4 HACKER 92

4.4.1 Comunidades Hacker 93
4.4.2 Terminologías De Hackers 95
4.5 Crear Una Conexión Segura Mediante Una Tecnica Del Tunelizado 98
4.5.1 Conexión a un servidor remoto usando el protocolo SSH 98
4.6 Cuadro Comparativo Entre Los Principales Protocolos De Tunelizado 101
CAPITULO V: CONCLUSIONES Y RECOMENDACIONES 102
5.1 CONCLUSIONES 102
5.2 RECOMENDACIONES 103
GLOSARIO 105
REFERENCIAS BIBLIOGRÁFICAS: 107
ANEXO 1: ENTREVISTAS 109
ANEXO 2: ENCUESTAS 110

LISTA DE ANEXOS

Anexo 1: Entrevistas 109

Anexo 2: Encuestas 110

LISTA DE CUADROS Y GRÁFICOS

Cuadros:

Cuadro 1: Metodología 9

Cuadro 2: Cronograma 10

Cuadro 3: Cuadro comparativo Protocolos 101

Imagen:

Imagen 1: Gráfico de Internet 11

Imagen 2: Configuración Típica de VPN 16

Imagen 3: Comunicación Segura por Túnel 17

Imagen 4: Ejemplo de Túnel 18

Imagen 5: Ejemplo de Protocolo SSH 19

Imagen 6: Ejemplo de Protocolo SSL 20

Imagen 7: Ejemplo de Protocolo IPsec 21

Imagen 8: Ejemplo de Protocolo PPTP 22

Imagen 9: Foto de Protocolo IEEE 802.1Q 24

Imagen 10: Protocolo HTTP 25

Imagen 11: Foto de Hacker 26

Imagen 12: Ejemplo de protocolo 45

Imagen 13: Protocolo de seguridad 46

Imagen 14: Ejemplo de Túnel 47

Imagen 15: Protocolo SSH 50

Imagen 16: Protocolo SSL 54

Imagen 17: Protocolo IPsec 63

Imagen 18: Protocolo PPTP 71

Imagen 19: Protocolo IEEE 802.1Q 73

Imagen 20: Protocolo HTTP 75

Imagen 21: Logo HTTP 82

Imagen 22: Foto Hacker 92

Gráficos:

Gráfico 1: Que es Internet? 33

Gráfico 2: Que es el protocolo HTTP? 34

Gráfico 3: Que es la técnica del tunelizado? 35

Gráfico 4: Que es el Protocolo SSH? 36

Gráfico 5: Que es el Protocolo SSL? 37

Gráfico 6: Que es el Protocolo IEEE 802? 37

Gráfico 7: Que es el Hacker? 37

Gráfico 8: Uso de Internet 41

Gráfico 9: Uso de HTTP 41

Gráfico 10: Transacciones Comerciales 42

Gráfico 11: Protocolos Seguros 43

Gráfico 12: Que Protocolos Conoce 43

Gráfico 13: Que es un Hacker? 44

CAPITULO I: ANTEPROYECTO

TEMA DE INVESTIGACIÓN

“Análisis de las técnicas de tunelizado por http para evitar ataques hacker”

1. PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES

Internet tiene su fundamento en base a protocolos estándares, sin los cuales no podría funcionar. Si bien el protocolo subyacente es el TCP/IP, para ciertas funciones particulares son necesarios otros protocolos, como en el caso específico de la Web, donde fue necesario crear un protocolo que resolviese los problemas planteados por un sistema hipermedia, y sobre todo distribuido en diferentes puntos de la Red.

Este protocolo se denominó HTTP (HyperText Transfer Protocol, o Protocolo de Transferencia de Hipertexto), y cada vez que se activa cumple con un proceso de cuatro etapas entre el browser y el servidor que consiste en lo siguiente:

Conexión: el browser busca el nombre de dominio o el número IP de la dirección indicada intentando hacer contacto con esa computadora.

Solicitud: el browser envía una petición al servidor (generalmente un documento), incluyendo información sobre el método a utilizar, la versión del protocolo y algunas otras especificaciones.

Respuesta: el servidor envía un mensaje de respuesta acerca de su petición mediante códigos de estado de tres dígitos.

Desconexión: se puede iniciar por parte del usuario 0 por parte del servidor una vez transferido un archivo.

Es entonces que se puede aprovechar este protocolo muy utilizado para la tunelización, un método efectivo de saltear firewalls o IDSs (Sistema de Detección de Intrusos) es tunelizar un protocolo bloqueado a través de uno permitido (por ejemplo SMTP a través de HTTP)

La mayoría de los IDS y firewalls actúan como proxies entre la PC cliente e Internet, solo dejando pasar el tráfico definido como permitido.

La mayoría de las organizaciones permite el tráfico HTTP ya que por lo general contiene tráfico benigno.

Pero a través del tunelizado HTTP, un atacante puede pasar el proxy escondiendo protocolos potencialmente peligrosos. Por ejemplo tunelizar protocolos de mensajería instantánea.

1.2 DIAGNOSTICO O PLANTEAMIENTO DE LA PROBLEMÁTICA GENERAL

1.2.1. CAUSA-EFECTO

El protocolo http al ser un protocolo de uso mundial obligatorio para acceder al Internet, podemos estar vulnerables a ataques mediante el uso de este protocolo.

Usando el protocolo http pueden tener acceso a nuestra red con lo que pudieran manipular e incluso el robo de nuestra información.

Evasión de protecciones de nuestra red, ya que con la técnica de tunelizado se puede evadir protecciones tales como firewall o IDSs.

Otra causa va a ser la desprotección de los datos enviados por internet, ya que terceras personas maliciosas pueden fácilmente ver la información que esta fluyendo por la red de internet.

1.3. PRONÓSTICO Y CONTROL DE PRONÓSTICO

1.3.1 PRONÓSTICO

La utilización del protocolo HTTP es en la actualidad de uso mundial en el ambiente web y por lo tanto las personas así como las organizaciones, confían en el protocolo HTTP, por lo que no tienen claro el potencial peligro que esto puede significar, al estar expuestos a que personas puedan ver la información que viaja por la red mediante este protocolo HTTP.

1.3.2. CONTROL DE PRONÓSTICO

Al estar expuestos a la vulnerabilidad que el protocolo HTTP posee, el presente trabajo explicara la forma de tunelizar este protocolo y así las personas puedan tener un concepto más claro sobre el tema y estén preparados para tomar las medidas correctivas a tiempo para proteger su información.

1.4. FORMULACIÓN DE LA PROBLEMÁTICA ESPECÍFICA

1.4.1. PROBLEMA PRINCIPAL

El protocolo HTTP al ser un protocolo “confiable”, las personas utilizan este protocolo para el acceso a Internet en la mayoría de los sitios web, por lo que pueden ser víctimas de tunelización maliciosa, con lo que terceras personas pueden pasar protocolos potencialmente peligrosos mediante el HTTP y poner en riesgo la información de las empresas, organizaciones o personas.

1.4.2. PROBLEMAS SECUNDARIOS

El protocolo HTTP es un protocolo universal para el acceso a internet por lo que su uso es de forma obligatoria para la mayoría de páginas web.

Es difícil detectar e impedir un tunelizado con la implementación de firewalls o IDSs para proteger nuestra red.

La información de las empresas quedan vulnerables con el ataque de un hacker mediante la técnica del tunelizado por HTTP.

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

Realizar el análisis de las técnicas de tunelizado por medio del protocolo HTTP para demostrar las formas en las que personas maliciosas pueden acceder a una red evadiendo los Firewalls o IDSs existentes en los sistemas informáticos.

1.5.2. OBJETIVOS ESPECÍFICOS

- Explicar en qué consiste la técnica de tunelizado
- Explicar que es el Protocolo HTTP y su utilidad
- Brindar recomendaciones para evitar un ataque hacker.
- Proteger los datos enviados usando la técnica de tunelizado.
- Realizar un cuadro comparativo entre las técnicas de tunelizado más importantes

1.6. JUSTIFICACIÓN

1.6.1. JUSTIFICACIÓN TEÓRICA

El tunelizado es una técnica utilizada para encapsular un protocolo dentro de otro, esta técnica se utiliza un protocolo permitido para transportar un protocolo no permitido por una red.

HTTP es el protocolo usado en cada transacción de la World Wide Web, es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. El protocolo HTTP trabaja de la siguiente manera: el cliente que efectúa la petición (un navegador web o un spider), la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

Es por esto que el protocolo SSH (secure shell) se utiliza con frecuencia para tunelizar tráfico confidencial sobre Internet de una manera segura.

1.6.2. JUSTIFICACIÓN METODOLÓGICA

Se ha elegido este tema porque es un tema que conozco, y además de esto es un tema muy interesante ya que como se ha expuesto anteriormente el protocolo HTTP es usado por todo el mundo en la red Internet, por lo que su interés es muy grande, se utilizará las técnicas y estrategias necesarias para recolectar la mayor cantidad de información sobre el tema planteado y así reforzar la propuesta de esta tesina.

1.6.3. JUSTIFICACIÓN PRÁCTICA

El tema propuesto, podrá aportar de una manera significativa en demostrar técnicas de tunelizado que permitirán a las personas asegurar sus datos enviados por el protocolo HTTP para que no puedan ser interceptados y modificados por otras personas, así mismo ayudará a incrementar el conocimiento del funcionamiento de este protocolo dentro de la Web.

1.7. MARCO DE REFERENCIA

1.7.1. MARCO TEÓRICO

1.7.1.1. INTERNET

“Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.”((RAE, 2011))

El servicio que más se usa en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior y utiliza Internet como medio de transmisión.

1.7.1.2. PROTOCOLO

Un protocolo es un conjunto de reglas, normas o estándares que utilizan las computadoras para comunicarse unas con otras a través de una red informática.

1.7.1.3. TÚNEL

Se conoce como túnel al efecto de la utilización de ciertos protocolos de red que encapsulan a otro protocolo. Así, el protocolo A es encapsulado dentro del protocolo B, de forma que el primero considera al segundo como si estuviera en el nivel de enlace de datos. La técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

1.7.1.4. HYPERTEXT TRANSFER PROTOCOL (HTTP)

Hypertext Transfer Protocol o HTTP (protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

1.7.1.5. TÚNEL SSH

El protocolo SSH (secure shell) se utiliza con frecuencia para tunelizar tráfico confidencial sobre Internet de una manera segura. Por ejemplo, un servidor de ficheros puede compartir archivos usando el protocolo SMB (Server Message Block), cuyos datos no viajan cifrados. Esto permitiría que una tercera parte, que tuviera acceso a la conexión (algo posible si las comunicaciones se realizan en Internet) pudiera examinar a conciencia el contenido de cada fichero trasmitido.

Para poder montar el sistema de archivo de forma segura, se establece una conexión mediante un túnel SSH que encamina todo el tráfico SMB al servidor de archivos dentro de una conexión cifrada SSH. Aunque el protocolo SMB sigue siendo inseguro, al viajar dentro de una conexión cifrada se impide el acceso al mismo.

1.7.2. MARCO ESPACIAL

El presente trabajo al basarse en un ambiente Web es de uso mundial, por lo cual no se puede delimitar su uso, ya que se puede realizar desde cualquier computador y en cualquier parte del mundo.

1.7.3. MARCO TEMPORAL

La investigación durará alrededor de 3 meses, tiempo en el cual se desarrollara el tema planteado tratando de cubrir todos los elementos que van inmersos en dicho tema.

1.8. METODOLOGÍA Y CRONOGRAMA

1.8.1. METODOLOGÍA:

Método	Técnica	Instrumentos
Deductivo/Inductivo	Análisis documental	Fichas para recolectar información Consultas de libros/Internet

	Entrevista	Guía para llevar la entrevista de una manera ordenada y objetiva
	Encuesta	Formularios para realizar la encuesta y luego tabular dichos datos

Cuadro 1: Metodología

1.8.2 CRONOGRAMA:

CRONOGRAMA DE ACTIVIDADES		DISTRIBUCION TEMPORAL										
		SEPTIEMBRE				OCTUBRE				NOVIEMBRE		
	ACTIVIDADES:	SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3
1	Desarrollo de la etapa exploratoria											
2	Determinacion del problema de investigacion											
3	Ubicacion del problema de investigacion en el contexto de su problematica											
4	Elaboracion de la introduccion											
5	Seleccion de los elementos necesarios al Marco teorico											
6	Formulacion de los objetivos											
7	Definicion de la estrategia metodologica											
8	Elaboracion de cada instrumento de investigacion											
9	Aplicacion de los instrumentos(recoleccion de la informacion)											
10	Procesamiento de la informacion											
11	Elaboracion de conclusiones											
12	Elaboracion del borrador del trabajo final de grado											
13	Predefensa del trabajo final de grado											
14	Correcciones de señalamientos											
15	Entrega del trabajo final de grado											

Cuadro 2: Cronograma 1

CAPITULO II: MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

2.1.1 INTERNET

Imagen 1: Gráfico de Internet 1

“Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.

ORTOGR. Escr. t. con may. inicial.”((RAE, 2011))

“Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.”((wikipedia.org, 2011))

El servicio que más se usa en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VoIP), televisión (IPTV)-, los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

Internet se remonta a la década de 1960, dentro de ARPA (hoy DARPA), como respuesta a la necesidad de esta organización de buscar mejores maneras de usar los computadores de ese entonces, pero enfrentados al problema de que los principales investigadores y laboratorios deseaban tener sus propios computadores, lo que no sólo era más costoso, sino que provocaba una duplicación de esfuerzos y recursos. Así nace ARPANet (Advanced Research Projects Agency Network o Red de la Agencia para los Proyectos de Investigación Avanzada de los Estados Unidos), que nos legó el trazado de una red inicial de comunicaciones de alta velocidad a la cual fueron integrándose otras instituciones gubernamentales y redes académicas durante los años 70.

Esto dio lugar a que los investigadores, los científicos, los profesores y los estudiantes se beneficiaron de la comunicación con otras instituciones y

colegas en su rama, así como de la posibilidad de consultar la información disponible en otros centros académicos y de investigación. De igual manera, disfrutaron de la nueva habilidad para publicar y hacer disponible a otros la información generada en sus actividades.

En el año 1961 Leonard Kleinrock publicó el primer documento sobre la teoría de conmutación de paquetes. Leonard Kleinrock convenció a Lawrence Roberts de la factibilidad y las ventaja teórica de las comunicaciones vía paquetes en lugar de circuitos que se usaba hasta entonces, lo cual se convirtió en un gran avance en lo que se refiere a las tecnologías en red. Con este nuevo descubrimiento se logro hacer dialogar a los ordenadores entre sí. Como ejemplo de esto en el año de 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

Estos descubrimientos fueron tan trascendentes que en la actualidad el Internet tiene un impacto muy profundo en el mundo laboral, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Debido al vertiginoso crecimiento del Internet comparado a las enciclopedias y a las bibliotecas tradicionales, ahora con el uso de la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los weblogs, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales

animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

En el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos dos computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería inasequible de otra manera.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna o irrelevante.

Al inicio el Internet tuvo un objetivo claro que era la búsqueda de información y se navegaba en la red solo con ese objetivo, ahora quizás también se lo usa con este fin, pero sin duda alguna hoy es más probable perderse en la red, debido al inmenso abanico de posibilidades que brinda. Hoy en día, la sensación que produce Internet es un ruido, una serie de interferencias, una explosión de ideas distintas, de personas diferentes, de pensamientos distintos de tantas posibilidades que, en ocasiones, puede resultar excesivo. El crecimiento o más bien la incorporación de tantas personas a la red hace que las calles de lo que en principio era una pequeña ciudad llamada Internet se

conviertan en todo un planeta extremadamente conectado entre sí entre todos sus miembros. El hecho de que Internet haya aumentado tanto implica una mayor cantidad de relaciones virtuales entre personas. es posible concluir que cuando una persona tenga una necesidad de conocimiento no escrito en libros, puede recurrir a una fuente más acorde a su necesidad. Como ahora esta fuente es posible en Internet Como toda gran revolución, Internet augura una nueva era de diferentes métodos de resolución de problemas creados a partir de soluciones anteriores. Algunos sienten que Internet produce la sensación que todos han sentido sin duda alguna vez; produce la esperanza que es necesaria cuando se quiere conseguir algo. Es un despertar de intenciones que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios Internet genera una sensación de cercanía, empatía, comprensión y, a la vez, de confusión, discusión, lucha y conflictos que los mismos usuarios consideran la vida misma.

Con la aparición de Internet y de las conexiones de alta velocidad disponibles al público, Internet ha alterado de manera significativa la manera de trabajar de algunas personas al poder hacerlo desde sus respectivos hogares. Internet ha permitido a estas personas mayor flexibilidad en términos de horarios y de localización, contrariamente a la jornada laboral tradicional, que suele ocupar la mañana y parte de la tarde, en la cual los empleados se desplazan al lugar de trabajo.

Un experto contable asentado en un país puede revisar los libros de una compañía en otro país, en un servidor situado en un tercer país que sea mantenido remotamente por los especialistas en un cuarto.

Internet y sobre todo los blogs han dado a los trabajadores un foro en el cual expresar sus opiniones sobre sus empleos, jefes y compañeros, creando una cantidad masiva de información y de datos sobre el trabajo que está siendo recogido actualmente por el colegio de abogados de Harvard.

Internet ha impulsado el fenómeno de la Globalización y junto con la llamada desmaterialización de la economía ha dado lugar al nacimiento de una Nueva Economía caracterizada por la utilización de la red en todos los procesos de incremento de valor de la empresa

2.1.2 PROTOCOLO

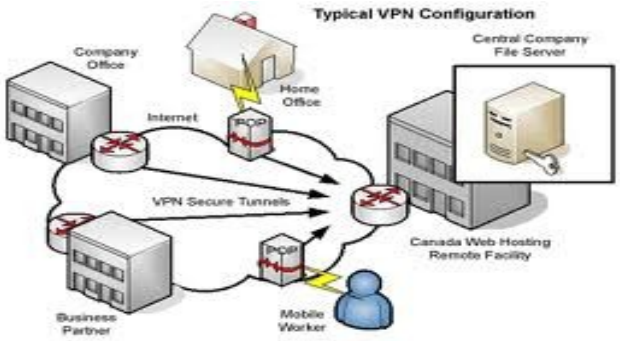


Imagen 2: Configuración Típica de VPN

"Un protocolo es un conjunto de reglas, normas o estándares que utilizan las computadoras para comunicarse unas con otras a través de una red informática.

Así mismo un protocolo es un conjunto de reglas o procedimientos que deben respetarse la sintaxis, semántica y sincronización para el envío y la recepción de datos a través de una red

Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos.”((wikipedia.org, 2011))

De una forma más técnica, podemos decir que un protocolo define el comportamiento de una conexión de hardware.

2.1.3 PROTOCOLOS DE SEGURIDAD

Imagen 3: Comunicación Segura por Túnel

Un protocolo de seguridad define las reglas que gobiernan las comunicaciones entre computadoras, diseñadas para que el sistema pueda soportar ataques de carácter malicioso.

Protegerse contra todos los ataques posibles es generalmente muy costoso, por lo cual los protocolos son diseñados bajo ciertas premisas con respecto a los riesgos a los cuales el sistema está expuesto.

Existen varios protocolos posibles. Las distintas compañías que instalan y administran este tipo de redes elijen unos u otros protocolos. En todos los casos se crean túneles entre origen y destino. Dentro de estos túneles viaja la información, bien por una conexión normal (en este caso no se encriptan los datos) o bien por una conexión VPN. El protocolo IPSec es uno de los más

empleados. Este se basa en GRE que es un protocolo de tunneling. Este protocolo también se utiliza de forma conjunta con otros protocolos como PPTP.

2.1.4 TÚNEL

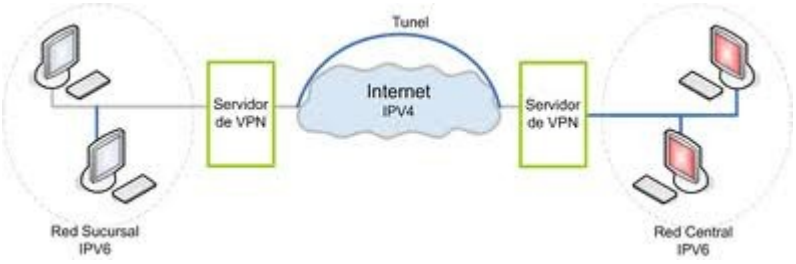


Imagen 4: Ejemplo de túnel

Túnel es la utilización de ciertos protocolos de red que encapsulan (un paquete de datos dentro de otro paquete en un solo protocolo) a otro protocolo para que pueda ser enviado por la red. Es así entonces que podemos encapsular un protocolo que llamaremos A dentro de otro protocolo llamado B, de forma que el primero considerara al segundo como si estuviera en el nivel de enlace de datos.

La técnica de tunelizar protocolos es utilizada para transportar un protocolo en una red que de forma normal no lo podría realizar, es decir, un protocolo A esta deseando ingresar en una red a la que no tiene acceso, entonces la forma de ingreso será que este protocolo A se encapsule a un protocolo B que si tiene acceso a dicha red, y de esta forma podrá ingresar a la red que normalmente no lo permitiría.

Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales, que son redes más seguras usadas para el transporte de información.

2.1.5 PROTOCOLO SSH

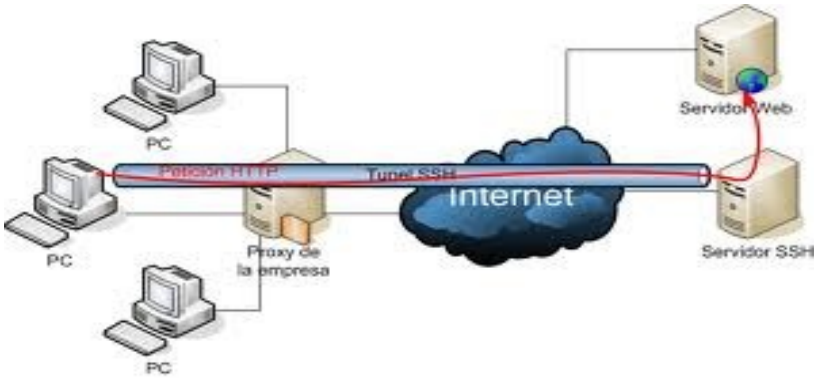


Imagen 5: Ejemplo de Protocolo SSH

SSH (Secure Shell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

2.1.6 PROTOCOLO SSL

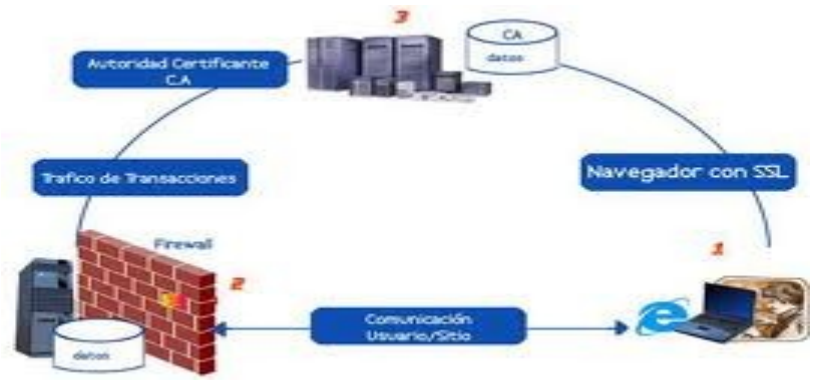


Imagen 6: Ejemplo de Protocolo SSL

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales

- Cifrado del tráfico basado en cifrado simétrico
- Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar.

2.1.7 PROTOCOLO IPSEC

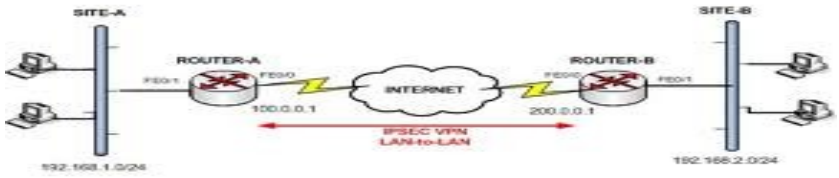


Imagen 7: Ejemplo de Protocolo IPsec

IPsec es el Protocolo de Seguridad de Internet, y es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP en un flujo de datos.

IPsec también incluye protocolos para el establecimiento de claves de cifrado. Este protocolo fue desarrollado para IPv6, que posteriormente también fue utilizado por IPv4

IPsec emplea dos protocolos diferentes AH y ESP, para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo

maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

2.1.8 PROTOCOLO PPTP

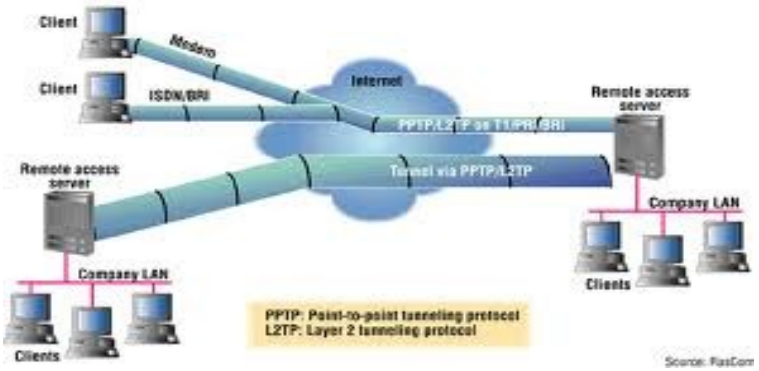


Imagen 8: Ejemplo de Protocolo PPTP

Point-To-Point Tunneling Protocol (PPTP) permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol). La tecnología PPTP encapsula los paquetes ppp en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización. Las compañías "involucradas" en el desarrollo del PPTP son Microsoft, Ascend Communications, 3com / Primary Access, ECI Telematics y US Robotics.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPN`s sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

2.1.9 PROTOCOLO IEEE 802.1Q

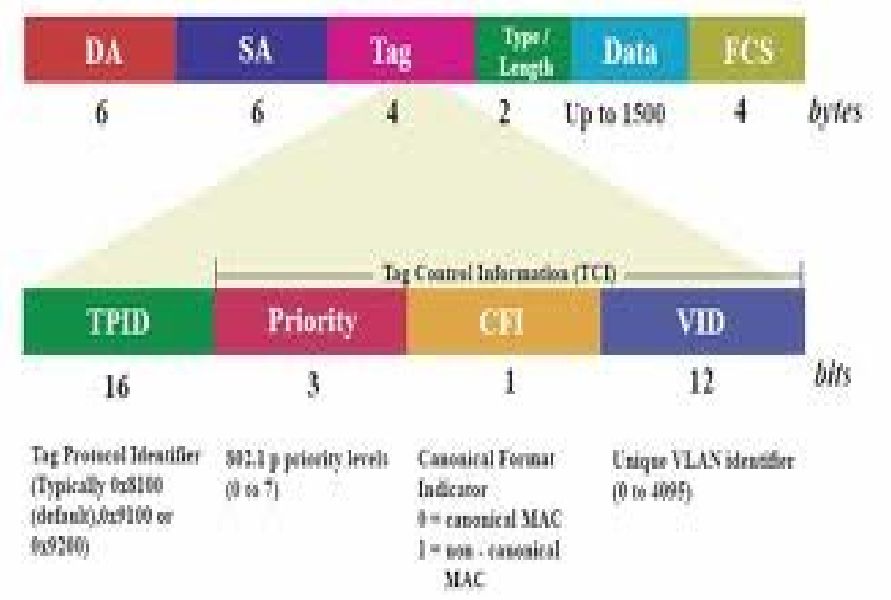


Imagen 9: Foto del Protocolo IEEE 802

El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

El protocolo 802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un recálculo del campo "FCS".

2.1.10 PROTOCOLO HTTP

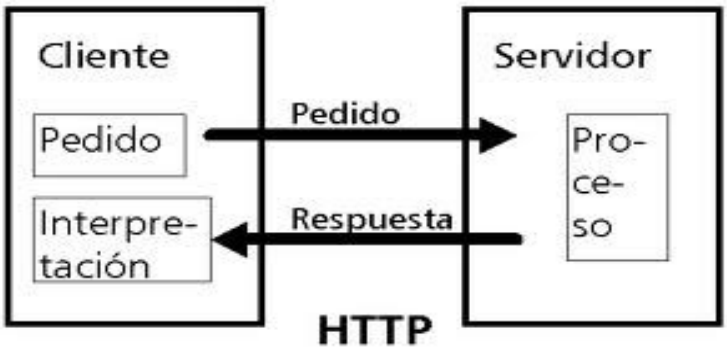


Imagen 10: Protocolo HTTP

El protocolo de transferencia de hipertexto (del inglés Hypertext Transfer Protocol) es el protocolo usado en cada transacción de la Web y define la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse entre si.

HTTP fue desarrollado por el World Wide Web Consortium y la Internet EngineeringTaskForce, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. ((wikipedia.org, 2009))

HTTP es un protocolo de comunicación orientado a transacciones y sigue el esquema petición – respuesta entre un cliente y un servidor. Un cliente (navegador web) efectúa la petición, luego esta información es transmitida, a lo que se le llama recurso y se la identifica mediante un localizador uniforme de recursos (URL), estos recursos pueden archivos, el resultado de una ejecución de un programa, una consulta a una base de datos, la traducción de un documento, etc. y la respuesta que es lo que obtenemos como respuesta de la petición realizada mediante el URL.

2.1.11 HACKER

Imagen 11: Foto de Hacker

Se llama Hacker a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

Un hacker es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes:

- Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

- Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT. Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son

creaciones de hackers. El RFC 13924 amplia este significado como "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas"

2.2 Marco Espacial

El presente trabajo al basarse en un ambiente Web es de uso mundial, por lo cual no se puede delimitar su uso, ya que se puede realizar desde cualquier computador y en cualquier parte del mundo.

2.3 Marco Temporal

La investigación durará alrededor de 3 meses, tiempo en el cual se desarrollara el tema planteado tratando de cubrir todos los elementos que van inmersos en dicha investigación.

2.4 Marco Legal

La realización del presente trabajo se halla enmarcado en la constitución de la República del Ecuador, reformada por la Asamblea Constituyente en el año 2008, en la “LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS”, bajo los siguientes artículos:

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Título I: DE LOS MENSAJES DE DATOS

Capítulo I: PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Título III

DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS.

Capítulo I: DE LOS SERVICIOS ELECTRÓNICOS

Art. 44.- Cumplimiento de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

Título V: DE LAS INFRACCIONES INFORMÁTICAS

Capítulo I

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

CAPITULO III: METODOLOGÍA

Para sustento del presente trabajo, además de la investigación documental que se realizó mayormente en Internet, por ser un tema que no se encuentra mayormente en libros, se han realizado entrevistas y encuestas las cuales se encuentran en los respectivos anexos y cuyo resumen se presenta a continuación:

3.1 ENCUESTA

Modelo:

NOMBRE: _____

FECHA: _____

La siguiente encuesta se realiza para evaluar el nivel de conocimientos que posee las personas sobre el uso de protocolos de internet y de las técnicas de tunelizado existentes.

Se pide la mayor sinceridad posible en sus respuestas ya que de ello dependerá el éxito de esta investigación.

Por favor marque con una X la respuesta correspondiente.

1. Internet es…….

( ) Es una red de ordenadores privados que permite compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales

( ) Es una red interconectada de cobertura mundial que utiliza los protocolos TCP/IP

( ) Ninguna de las anteriores

( ) Desconozco

2. Que es el protocolo HTTP (HyperText Transfer Protocol = protocolo de transferencia de hipertexto)?

( ) Es el protocolo usado en cada transacción de la World Wide Web

( ) Es un protocolo de red para la transferencia de archivos

( ) Es un protocolo usado para crear programas informáticos en la Web

( ) Desconozco

3. Que es la técnica de tunelizado en informática?

( ) Es la técnica mediante la cual se usa la tecnología informática para crear túneles para carreteras de grandes dimensiones

( ) Túnel es la utilización de ciertos protocolos de red que encapsulan (un paquete de datos dentro de otro paquete en un solo protocolo) a otro protocolo para que pueda ser enviado por la red

( ) Túnel es una técnica mediante la cual se puede a acceder a paginas restringidas con contenido para adultos de forma directa

( ) Desconozco

4. Que es el protocolo SSH(Secure Shell = intérprete de órdenes segura)?

( ) Es el nombre de un protocolo que se usa para switchar una red para conectarla a internet

( ) Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red

( ) Es el nombre de un protocolo que sirve para ver la IP de una computadora y de su dirección MAC

( ) Desconozco

5. Que es el protocolo SSL(Secure Sockets Layer = protocolo de capa de conexión segura)

( ) SSL proporciona un servicio de video conferencias seguras por internet

( ) SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía

( ) SSL proporciona servicios de correo electrónico dentro de una LAN

( ) Desconozco

6. Que es la IEEE 802.1Q?

( ) Es un protocolo

( ) The *Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)*

( ) Instituto Ecuatoriano de Estadísticas y Educación

( ) Desconozco

7. Que es un hacker?

( ) Se llama Hacker a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal

( ) Es un sobrenombre que se utiliza para referirse a las personas de medio oriente

( ) Se llama así a las personas peligrosas que roban bancos y comercios con armas sofisticadas

( ) Desconozco

Como se ve en las encuestas se utilizó preguntas simples de conceptos que enmarca al entendimiento de tema planteado, realizando a un número de 40 personas encuestadas con conocimientos medios en informática, estudiantes de Informática y Sistemas, obteniendo los resultados que se exponen a continuación.

Pregunta 1: Internet es….

( ) Es una red de ordenadores privados que permite compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales

( ) Es una red interconectada de cobertura mundial que utiliza los protocolos TCP/IP

( ) Ninguna de las anteriores

( ) Desconozco

Pregunta1. Internet es….	
OP. 1	4
Op. 2	35
Op. 3	1
Op. 4	0

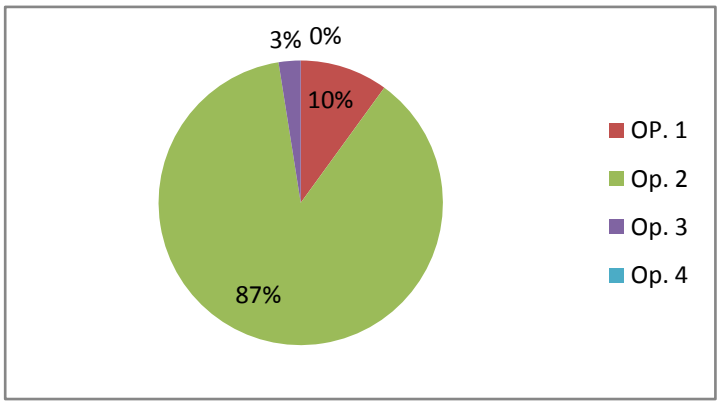


Gráfico 1: Que es Internet?

Interpretación: Pudiendo deducir que el 87% de las personas encuestadas saben de manera precisa que es el Internet, y el restante 13% tiene una idea errónea del concepto de Internet.

Pregunta 2: Que es el protocolo HTTP (HyperText Transfer Protocol = protocolo de transferencia de hipertexto)?

( ) Es el protocolo usado en cada transacción de la World Wide Web

( ) Es un protocolo de red para la transferencia de archivos

( ) Es un protocolo usado para crear programas informáticos en la Web

( ) Desconozco

Pregunta2. Que es el protocolo HTTP	
OP. 1	24
Op. 2	2
Op. 3	1
Op. 4	13

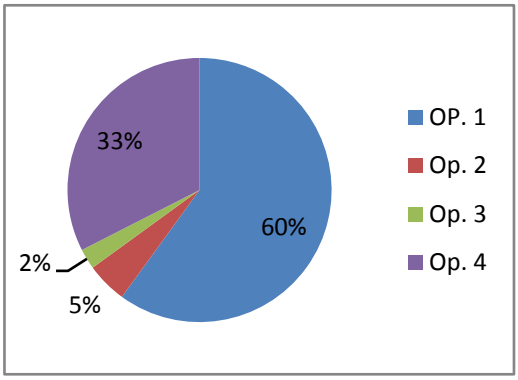


Gráfico 2: Que es el protocolo HTTP?

Interpretación: Según estos resultados se puede deducir que si bien el 60% de los encuestados conocen que es el protocolo HTTP, hay un 33% de personas que desconocen para que sirve este protocolo y un 7% responde erróneamente.

Pregunta 3: Que es la técnica de tunelizado en informática?

( ) Es la técnica mediante la cual se usa la tecnología informática para crear túneles para carreteras de grandes dimensiones

( ) Túnel es la utilización de ciertos protocolos de red que encapsulan (un paquete de datos dentro de otro paquete en un solo protocolo) a otro protocolo para que pueda ser enviado por la red

( ) Túnel es una técnica mediante la cual se puede a acceder a paginas restringidas con contenido para adultos de forma directa

( ) Desconozco

Pregunta3. Que es la técnica de tunelizado	
Op. 1	1
Op. 2	15
Op. 3	11
Op. 4	13

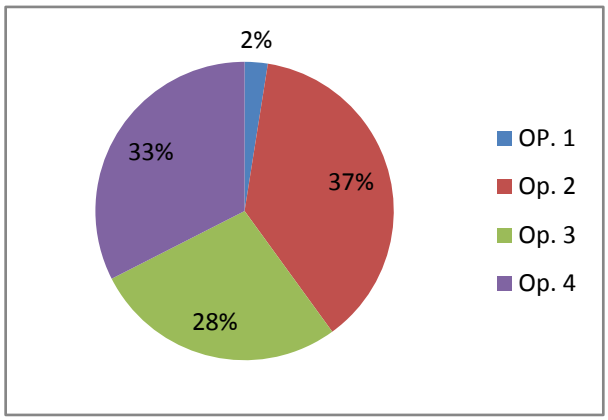


Gráfico 3: Que es técnica de tunelizado? 1

Interpretación: Según los resultados obtenidos se puede deducir que un porcentaje mínimo del 37% conoce lo que es un túnel informático, un 33% desconoce sobre el tema y el 30% selecciona una respuesta errónea.

Pregunta 4: Que es el protocolo SSH (Secure Shell = intérprete de órdenes segura)?

( ) Es el nombre de un protocolo que se usa para switchar una red para conectarla a internet

( ) Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red

( ) Es el nombre de un protocolo que sirve para ver la IP de una computadora y de su dirección MAC

( ) Desconozco

Pregunta4. Que es el protocolo SSH	
OP. 1	4
Op. 2	18
Op. 3	1
Op. 4	17

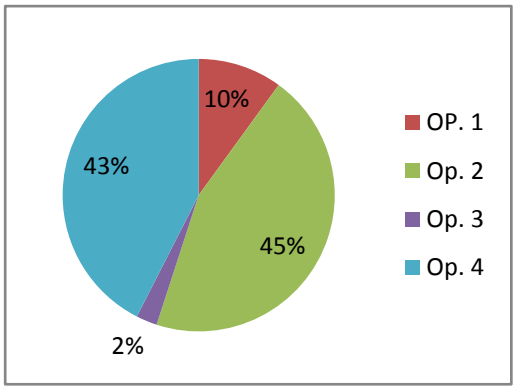


Gráfico 4: Que es el protocolo SSH?

Interpretación: Según los resultados obtenidos se puede deducir que un porcentaje del 45% conoce lo que es un protocolo SSH, un 43% desconoce sobre el tema y el 12% selecciona una respuesta errónea.

Pregunta 5: Que es el protocolo SSL (Secure Sockets Layer = protocolo de capa de conexión segura)

( ) SSL proporciona un servicio de video conferencias seguras por internet

( ) SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía

( ) SSL proporciona servicios de correo electrónico dentro de una LAN

( ) Desconozco

Pregunta5. Que es protocolo SSL	
OP. 1	1
Op. 2	10
Op. 3	10
Op. 4	19

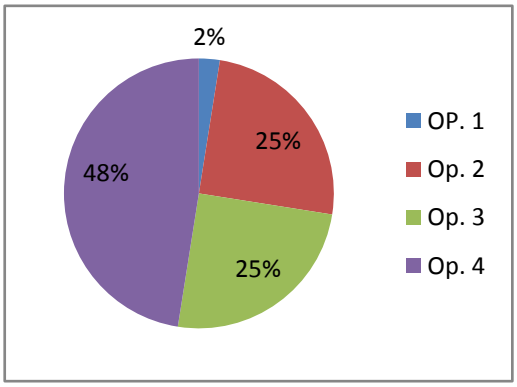


Gráfico 5: Que es el protocolo SSL? 1

Interpretación: Según los resultados obtenidos se puede deducir que lamentablemente un porcentaje mínimo del 25% conoce lo que es un protocolo SSL, y un elevado número del 48% desconoce sobre el tema y el 27% selecciona una respuesta errónea.

Pregunta 6: Que es la IEEE 802.1Q?

( ) Es un protocolo

( ) The *Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)*

( ) Instituto Ecuatoriano de Estadísticas y Educación

( ) Desconozco

Pregunta6. Que es la IEEE	
OP. 1	7
Op. 2	13
Op. 3	7
Op. 4	13

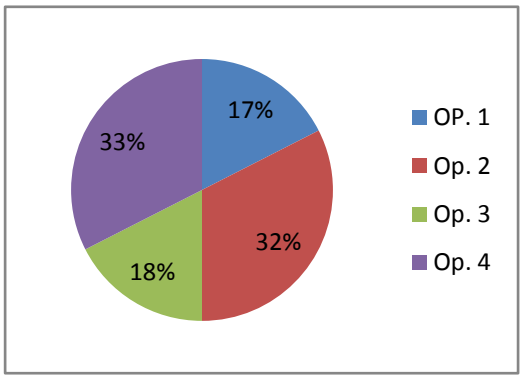


Gráfico 6: Que es la IEEE 802?

Interpretación: Según los resultados obtenidos se puede deducir que solo un porcentaje mínimo del 17% conoce lo que es el protocolo IEEE 802.1Q, y un elevado número del 33% desconoce sobre el tema y el 50% selecciona una respuesta errónea.

Pregunta 7: Que es un hacker?

( ) Se llama Hacker a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal

( ) Es un sobrenombre que se utiliza para referirse a las personas de medio oriente

( ) Se llama así a las personas peligrosas que roban bancos y comercios con armas sofisticadas

( ) Desconozco

Pregunta7. Que es un hacker?	
OP. 1	32
Op. 2	1
Op. 3	0
Op. 4	7

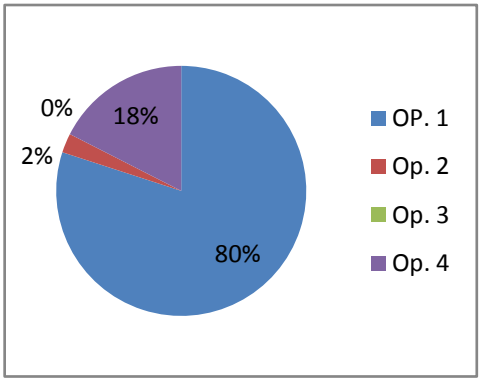


Grafico 7: Que es un Hacker?

Interpretación: Según los resultados obtenidos se puede deducir que un gran porcentaje del 80% conoce lo que es un hacker, y un reducido número del 18% desconoce sobre el tema y un mínimo 2% selecciona una respuesta errónea.

Conclusión:

Por los datos obtenidos en las diferentes preguntas podemos observar que los encuestados en su mayoría saben que es internet y que es un hacker, pero desconocen completamente el tema de los protocolos que se usan para el tunelizado en una red informática por lo que una vez más estas estadísticas abalizan la importancia de esta investigación ya que con este trabajo se pretende aportar al conocimiento de estos protocolos y a los beneficios que estos brindan para proteger la comunicación entre computadoras.

3.2 ENTREVISTA

Modelo:

ENTREVISTA

NOMBRE: _____

FECHA: _____

1. Usted usa internet con qué frecuencia?

( ) Una vez al mes

( ) Una vez a la semana

( ) Todos los días

( ) No usa

2. Sabía que para conectarse a una página en internet debe usar un protocolo llamado HTTP?

( ) SI

( ) NO

( ) Desconozco

3. Realiza transacciones comerciales por internet?

( ) Siempre

( ) A veces

( ) Nunca

4. Conoce usted la existencia de protocolos seguros para la comunicación?

( ) SI

( ) NO

5. Si la respuesta anterior es positiva indique cuales de los siguientes conoce:

( ) SSH

( ) SSL

( ) IEEE 802.1Q

( ) PPTP

( ) Otros _____

6. Para su concepto un hacker es una persona buena o mala?

( ) Buena

( ) Mala

( ) Desconozco

En el desarrollo de las entrevistas se utilizó preguntas simples del uso de Internet y sus protocolos del tema planteado, realizando a un número de 20 personas entrevistadas con conocimientos medios estudiantes de Informática y Sistemas, obteniendo los resultados que se exponen a continuación.

1. Usted usa internet con qué frecuencia?

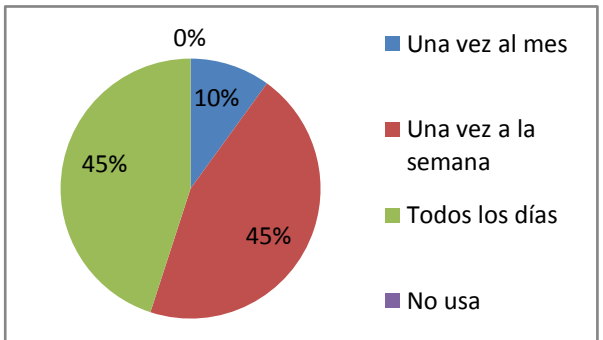
( ) Una vez al mes

( ) Una vez a la semana

( ) Todos los días

( ) No usa

1. CON QUE FRECUENCIA USA EL INTERNET



Una vez al mes	2
Una vez a la semana	9
Todos los días	9
No usa	0

Interpretación: Con los resultados obtenidos sobre la frecuencia de uso del Internet se puede notar que de las personas entrevistadas un 45% usa todos los días, un 45% usa al menos una vez a la semana y un porcentaje del 10% usa internet una vez por mes, pero todos usan Internet ya que hay un 0% que uno usa.

2. Sabía que para conectarse a una página en internet debe usar un protocolo llamado HTTP?

( ) SI

( ) NO

( ) Desconozco

2. Sabía que para conectarse a una página en internet debe usar un protocolo llamado HTTP?	
SI	7
NO	7
DESCONOZCO	6

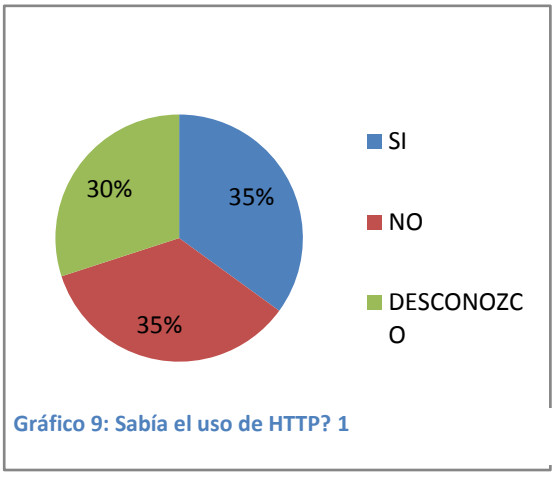


Gráfico 9: Sabía el uso de HTTP? 1

Interpretación: Como se puede observar en los resultados obtenidos, hay un 35% que conocía el uso del protocolo HTTP, pero un 65% no sabían o desconocían esto, lo que es muy preocupante el nivel de desconocimiento de

este protocolo ya que éste al ser un protocolo tan importante para el uso de internet.

3. Realiza transacciones comerciales por internet?

( ) Siempre

( ) A veces

( ) Nunca

3. Realiza transacciones comerciales por internet?	
Siempre	0
A veces	5
Nunca	15

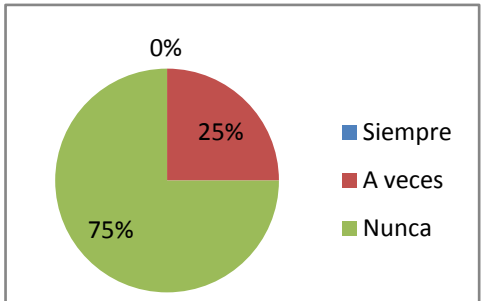


Gráfico 10: Transacciones Comerciales 1

Interpretación: Como se puede observar en el gráfico, un 75% nunca ha realizado una transacción comercial por Internet, lo que justifica de cierta manera el desconocimiento de los protocolos, ya que al usar internet básico es transparente el uso del protocolo HTTP.

4. Conoce usted la existencia de protocolos seguros para la comunicación?

( ) SI

( ) NO

4. Conoce usted la existencia de protocolos seguros para la comunicación?	

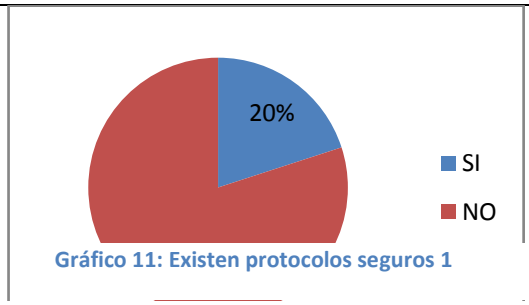


Gráfico 11: Existen protocolos seguros 1

SI	4
NO	16

Interpretación: Lamentablemente los resultados arrojan un 80% de desconocimiento de la existencia de protocolos seguros de comunicación, y solo un 20% conoce sobre el tema, lo cual es preocupante porque la seguridad no le interesa al usuario sino lo deja al sistema.

5. Si la respuesta anterior es positiva indique cuales de los siguientes conoce:

( ) SSH
( ) SSL
( ) IEEE 802.1Q
( ) PPTP
( ) Ninguno

5. Si la respuesta anterior es positiva indique cuales de los siguientes conoce:	
SSH	1
SSL	1
IEEE 102.1Q	1
PPTP	1
NINGUNO	16

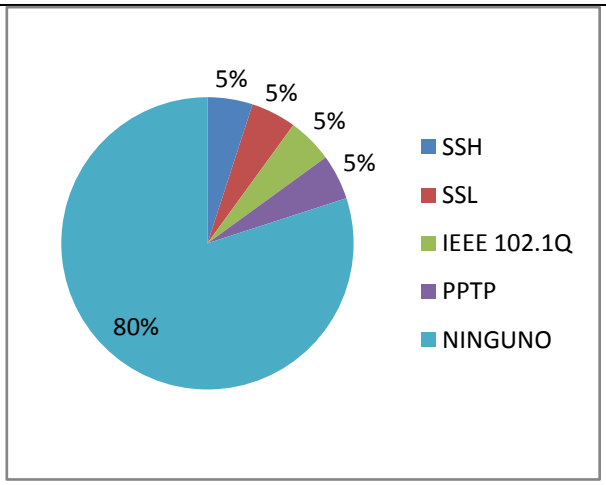


Gráfico 12: Que protocolos conoce? 1

Interpretación: Esta es una pregunta encadenada de la anterior, y como se puede observar las personas consultadas en su mayoría un 80% no conocen los protocolos tunelizados, siendo solo un 20% que conoce al menos uno de los protocolos planteados.

6. Para su concepto un hacker es una persona buena o mala?

( ) Buena

( ) Mala

( ) Desconozco

6. Para su concepto un hacker es una persona buena o mala?	
Buena	2
Mala	8
Desconozco	10

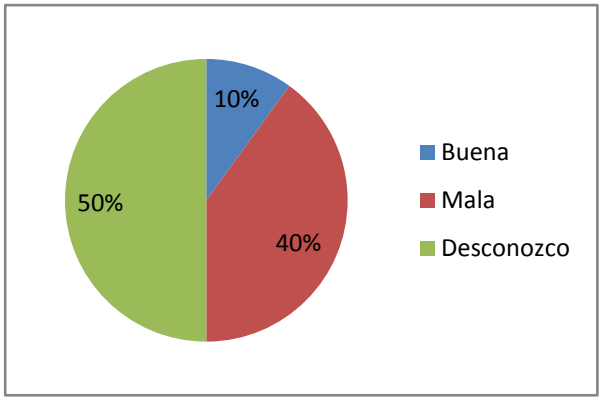


Grafico 13: Que es un hacker? 1

Interpretación: En esta pregunta se puede notar que de las personas entrevistadas un 50% no conocen lo que es un hacker, en un 40% piensan que es una persona mala y tan solo un 10% piensan que es una persona buena.

Conclusión: Luego de tabulado los datos obtenidos en la entrevista podemos notar que si bien las personas usan comúnmente internet, no conocen el uso del protocolo HTTP, peor sobre los protocolos de tunelizado, sin tener ni idea de lo que es un Hacker, lo que nos lleva a la conclusión de que las personas se confían de las aplicaciones informáticas sin averiguar la seguridad o no para hacer como por ejemplo sus transacciones.

CAPITULO IV: DESARROLLO

4.1 PROTOCOLO

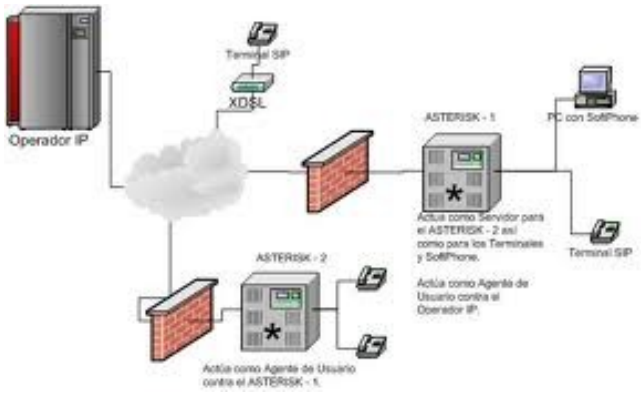


Imagen 12: Ejemplo de Protocolo

"Un protocolo es un conjunto de reglas, normas o estándares que utilizan las computadoras para comunicarse unas con otras a través de una red informática.

Así mismo un protocolo es un conjunto de reglas o procedimientos que deben respetarse la sintaxis, semántica y sincronización para el envío y la recepción de datos a través de una red

Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos." (wikipedia.org, 2011)

Entonces podemos decir que un protocolo informático de una manera más técnica define el comportamiento de una conexión de hardware, es decir la conexión de componentes físicos en lo que llamamos la red.

4.1.1 PROTOCOLOS DE SEGURIDAD

Imagen 13: Ejemplo de Protocolo de Seguridad

Existen protocolos de seguridad en informática que podemos definir como las reglas que gobiernan las comunicaciones entre computadoras, diseñadas para que el sistema pueda soportar ataques de carácter malicioso.

Protegerse contra todos los ataques posibles es generalmente muy costoso, por lo cual los protocolos son diseñados bajo ciertas premisas con respecto a los riesgos a los cuales el sistema está expuesto.

Es entonces que las empresas gastan mucho dinero en cuestión de seguridades tanto físicas como lógicas, y que justamente dieron paso a la aparición de protocolos que regulan o restringen de alguna manera el manejo de la conexión de redes.

Existen varios protocolos posibles para el manejo de redes. Las distintas compañías que instalan y administran este tipo de redes elijen unos u otros protocolos. En todos los casos se crean túneles entre origen y destino. Dentro de estos túneles viaja la información, bien por una conexión normal (en este caso no se encriptan los datos) o bien por una conexión VPN.

4.2 TÚNEL

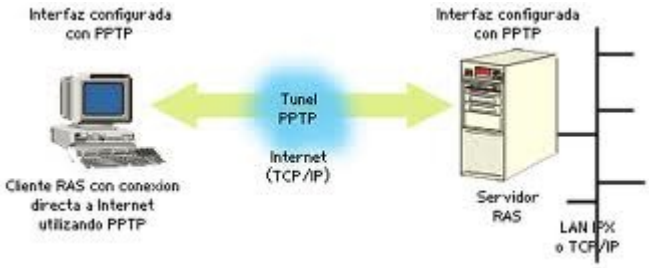


Imagen 14: Ejemplo de Túnel 1

Se denomina túnel en informática a un método que permite conectar a computadoras en red, haciendo uso de una red intermedia para transferir datos de un extremo a otro de la red.

Los paquetes que se transmiten se encapsulan sobre otro encabezado correspondiente al protocolo de túnel, este nuevo encabezado contiene la información necesaria para que el paquete atravesando la red intermedia llegue al destino correspondiente, una vez llegados a destino son desencapsulados y dirigidos al destino final.

Un túnel es un canal virtual, configurado entre dos sistemas remotos que se encuentran en diferentes redes, sobre una conexión real que involucra más de un nodo intermedio.

Entonces podemos decir que túnel es la utilización de ciertos protocolos de red que encapsulan (un paquete de datos dentro de otro paquete en un solo protocolo) a otro protocolo para que pueda ser enviado por la red. Es así entonces que podemos encapsular un protocolo que llamaremos A dentro de otro protocolo llamado B, de forma que el primero considerara al segundo como si estuviera en el nivel de enlace de datos.

Explicado de otra manera, la técnica de tunelizar protocolos es utilizada para transportar un protocolo en una red que de forma normal no lo podría realizar, es decir, un protocolo A esta deseando ingresar en una red a la que no tiene acceso, entonces la forma de ingreso será que este protocolo A se encapsule a un protocolo B que si tiene acceso a dicha red, y de esta forma podrá ingresar a la red que normalmente no lo permitiría.

De esta forma un paquete puede “saltar” la topología de una red. Por ejemplo, un túnel puede ser usado para evitar un firewall (con los peligros consecuentes de esta decisión). Esta es una consideración a tener en cuenta al configurar un túnel.

El túnel es creado encapsulando un protocolo de red dentro de los paquetes del mismo protocolo, que serán llevados por la red real. Adicionalmente, el paquete encapsulado es encriptado por el emisor, en acuerdo con el receptor (el sistema que se encuentra en del otro lado del túnel) de manera que sólo ambos extremos puedan acceder a los datos transportados. Éste tipo de comunicación solo es posible si el protocolo soporta esta facilidad, denominada modo túnel. La otra modalidad posible, modo transporte, provee protección sólo para protocolos de la capa superior.

De esta forma, el túnel es simplemente la ruta que toman los paquetes encapsulados (y encriptados), dentro de un paquete del mismo protocolo, entre las dos redes. Un atacante puede interceptar los mensajes que viajen por el túnel, pero los datos encapsulados están encriptados y solo pueden ser recuperados por el destinatario final. En el sistema de destino, el mensaje

encapsulado es extraído del paquete recibido, desencriptado, y reinyectado en la red a la que pertenece el receptor (en el caso de un Gateway).

Con el uso en modo túnel, el encabezado IP interno (encapsulado) es encriptado, ocultando la identidad del destinatario y del origen del tráfico. Los mismos servicios pueden ofrecerse a un usuario móvil al cual se asigna un IP dinámicamente para una conexión de conexión telefónica: se establece un canal en modo túnel al firewall del ISP funcionando como un gateway de seguridad. En relación con una conexión o canal seguro, cabe introducir un concepto importante: el de Asociación de Seguridad (Security Asociation - SA). Una asociación de seguridad (AS) es una instancia de una política de seguridad junto con componentes claves. Las SAs son identificadas de forma única por una dirección de destino, un protocolo de seguridad y un índice de parámetros de seguridad o SPI (un conjunto de atributos se seguridad).

Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales, que son redes más seguras usadas para el transporte de información.

4.2.1 PROTOCOLO SSH

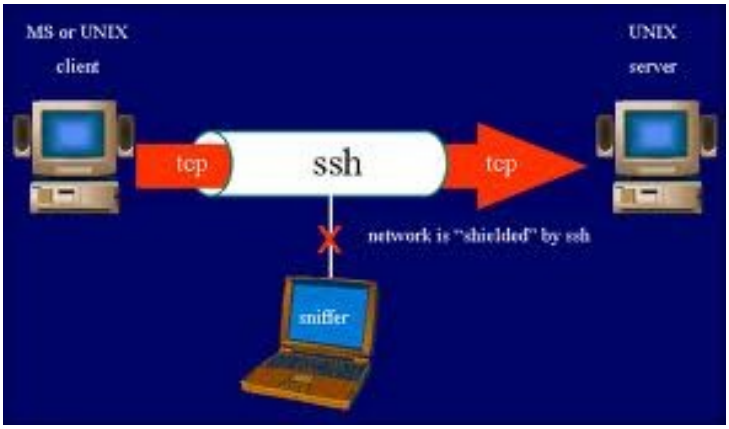


Imagen 15: Protocolo SSH 1

SSH (Secure SHell), que en español significa intérprete de órdenes segura; es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

El protocolo SSH permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

Podemos comparar entre el protocolo SSH que trabaja en forma similar a como lo hace telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de

manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

Al principio sólo existían los r-commands, que eran los basados en el programa rlogin, el cual funciona de una forma similar a telnet.

La primera versión del protocolo y el programa eran libres y los creó un finlandés llamado Tatu Ylönen, pero su licencia fue cambiando y terminó apareciendo la compañía SSH Communications Security, que lo ofrecía gratuitamente para uso doméstico y académico, pero exigía el pago a otras empresas. En el año 1997 (dos años después de que se creara la primera versión) se propuso como borrador en la IETF.

A principios de 1999 se empezó a escribir una versión que se convertiría en la implementación libre por excelencia, la de OpenBSD, llamada OpenSSH.

SSH evita muchos de los ataques más habituales, en los que los datos se ven comprometidos e incluso la seguridad de la red. Uno de los riesgos que evita, es IP spoofing, donde un host remoto envía paquetes que pretenden venir de otro ordenador, el cual es de confianza. Esta suplantación de identidad es bastante peligrosa y SSH nos da una buena protección contra este método.

Aun hoy en día, se suele utilizar el protocolo de conexión entre ordenadores (o servidores), llamado telnet, el cual ha sido extremadamente útil y utilizado en los últimos años. El problema es que el nombre de usuario y la contraseña son enviados en texto claro por la red. Esto significa que si alguien en el medio de

la red (entre tu ordenador y el ordenador destino), captura los datos con un sniffer (herramienta de captura de datos), puede conseguir el usuario y la contraseña para poderlos utilizar en el futuro. SSH encripta estos datos según viajan de una máquina a la otra, por lo que si son capturados, no tendrán ningún sentido para el que ha conseguido esta información.

Características de SSH

SSH es un protocolo para crear conexiones seguras entre dos sistemas usando una arquitectura cliente/servidor.

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de enviar X11 aplicaciones lanzadas desde el intérprete de comandos de la shell. Esta técnica proporciona una interfaz gráfica segura (llamada reenvío por X11), proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un

conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada reenvío por puerto, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

Red Hat Linux contiene el paquete general de OpenSSH (openssh), el servidor de OpenSSH (openssh-server) y los paquetes de clientes (openssh-clients).

Una gran cantidad de programas de cliente y servidor puede usar el protocolo SSH. Muchas aplicaciones SSH cliente están disponibles para casi todos los principales sistemas operativos en uso hoy día.

Los usuario maliciosos tienen a su disposición una variedad de herramientas interceptar y dirigir el tráfico de la red para ganar acceso al sistema. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

Intercepción de la comunicación entre dos sistemas — En este escenario, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información, o puede modificar la información y luego enviarla al recipiente al cual estaba destinada.

Este ataque se puede montar a través del uso de un paquete sniffer — una utilidad de red muy común.

Personificación de un determinado host — con esta estrategia, un sistema interceptor finge ser el recipiente a quien está destinado un mensaje. Si funciona la estrategia, el cliente no se da cuenta del engaño y continúa la

comunicación con el interceptor como si su mensaje hubiese llegado a su destino satisfactoriamente.

Esto se produce con técnicas como el envenenamiento del DNS o spoofing de IP.

Ambas técnicas causan que se intercepte información, posiblemente con propósitos hostiles. El resultado puede ser catastrófico.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar archivos, estas amenazas a la seguridad se pueden disminuir notablemente. Esto es porque el cliente SSH y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptado. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

4.2.2 PROTOCOLO SSL

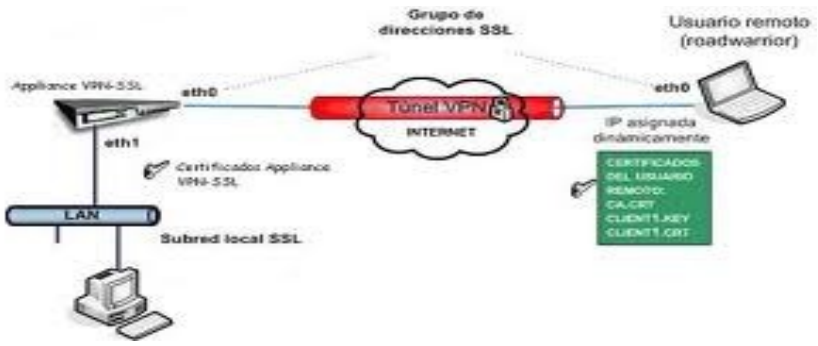


Imagen 16: Protocolo SSL

El protocolo SSL que viene del inglés Secure Sockets Layer que significa “protocolo de capa de conexión segura” y su sucesor TLS que viene del inglés Transport Layer Security que significa “Seguridad de la capa de transporte” son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

El protocolo SSL para su implementación implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard);

- Con funciones hash: MD5 o de la familia SHA.

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autenticación del mensaje (MAC). Cada registro tiene un campo de content_type que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo handshake, que tiene el content_type 22.

El cliente envía y recibe varias estructuras handshake:

Envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados Challenge de Cliente o Reto). Además puede incluir el identificador de la sesión.

Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.

Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.

Cliente y servidor negocian una clave secreta (simétrica) común llamada master secret, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función pseudoaleatoria cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

Numerando todos los registros y usando el número de secuencia en el MAC.

Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Protección contra varios ataques conocidos (incluyendo ataques man-in-the-middle), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.

El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.

La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

Aunque un número creciente de productos clientes y servidores pueden proporcionar SSL de forma nativa, muchos aún no lo permiten. En estos casos, un usuario podría querer usar una aplicación SSL independiente como Stunnel para proporcionar cifrado. No obstante, el Internet Engineering Task Force recomendó en 1997 que los protocolos de aplicación ofrecieran una forma de actualizar a TLS a partir de una conexión sin cifrado (plaintext), en vez de usar un puerto diferente para cifrar las comunicaciones – esto evitaría el uso de envolturas (wrappers) como Stunnel.

SSL también puede ser usado para tunelizar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

Desarrollado por Netscape, SSL versión 3.0 se publicó en 1996, que más tarde sirvió como base para desarrollar TLS versión 1.0, un estándar protocolo IETF definido por primera vez en el RFC 2246. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

SSL opera de una manera modular: sus autores lo diseñaron extensible, con soporte para compatibilidad hacia delante y hacia atrás, y negociación entre las partes (peer-to-peer).

Algunas primeras implementaciones de SSL podían usar claves simétricas con un máximo de sólo 40-bit debido a las restricciones del gobierno de los Estados Unidos sobre la exportación de tecnología criptográfica. Dicho gobierno impuso una clave de 40-bit lo suficientemente pequeña para ser “rota” por un ataque de fuerza bruta por las agencias de seguridad nacional que desearan leer el tráfico cifrado, a la vez que representaban un obstáculo para atacantes con menos medios. Una limitación similar se aplicó a Lotus Notes en versiones para la exportación. Después de varios años de controversia pública, una serie de pleitos, y el reconocimiento del gobierno de Estados Unidos de cambios en la disponibilidad en el mercado de 'mejores' productos criptográficos producidos fuera del país, las autoridades relajaron algunos aspectos de las restricciones de exportación. La limitación de claves de 40-bit en su mayoría ha desaparecido. Las implementaciones modernas usan claves de 128-bit (o más) para claves de cifrado simétricas.

4.2.2.1 ESTÁNDARES

La primera definición de TLS apareció en el RFC 2246: "The TLS Protocol Version 1.0" (El protocolo TLS versión 1.0).

Otros RFC posteriores extendieron TLS:

RFC 2712: "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)". Las familias de cifrados de 40-bit definidas en este memo aparecen

sólo para propósitos de documentación del hecho de que esas familias de códigos de cifrado han sido ya asignadas.

La flexibilidad es una de las principales fortalezas del protocolo TLS. Clientes y servidores pueden negociar suites de cifrado para cumplir con la seguridad específicos y las políticas administrativas. Sin embargo, hasta la fecha, la autenticación de TLS se limita sólo al público las soluciones clave. Como resultado, TLS no es totalmente compatible con las organizaciones con las implementaciones de seguridad heterogéneos que incluyen sistemas de autenticación basados en criptografía simétrica. Kerberos, originalmente desarrollado en el MIT, es basado en un estándar abierto [2] y es la más utilizada del sistema simétrico de autenticación de clave. Este documento propone una nueva opción para la negociación de la autenticación Kerberos en el marco TLS. Con ello se consigue la autenticación mutua y el establecimiento de un secreto maestro con credenciales de Kerberos. Los cambios propuestos son mínimos y, de hecho, no es diferente de la adición de un nuevo algoritmo de clave pública en el marco de TLS.

RFC 2817: "Upgrading to TLS Within HTTP/1.1", explica cómo usar el mecanismo de actualización en HTTP/1.1 para iniciar TLS sobre una conexión TCP existente. Esto permite al tráfico HTTP inseguro y seguro compartir el mismo puerto conocido (en este caso, http: en el 80 en vez de https: en el 443).

TLS, también conocido como SSL (Secure Sockets Layer), establece una organización privada de extremo a extremo de conexión, incluyendo opcionalmente la autenticación mutua fuertes, utilizando una variedad de

sistemas criptográficos. En un principio, una fase de negociación utiliza tres subprotocols crear una capa de registro, autenticación de terminales, los parámetros establecidos, así como los errores del informe. Entonces, existe un protocolo de registro continuo de capas que se encarga de encriptación, compresión, y montaje para el resto de la conexión. Este último está destinado a ser completamente transparente. Por ejemplo, no hay dependencia entre los marcadores de registro TLS y certificados y la codificación HTTP/1.1 's fragmentada o autenticación.

RFC 2818: "HTTP Over TLS", diferencia tráfico seguro de tráfico inseguro mediante el uso de un 'puerto de servidor' diferente.

HTTP [RFC2616] fue originalmente utilizado en el claro de la Internet. Sin embargo, un mayor uso de HTTP para aplicaciones sensibles ha requerido medidas de seguridad. SSL, TLS y su sucesor [RFC2246] se han diseñado para proporcionar canales orientados a la seguridad. Este documento describe cómo usar HTTP sobre TLS.

RFC 3268: "AES Ciphersuites for TLS". Añade la familia de cifrado AES a los cifrados simétricos previamente existentes.

Este documento propone varios conjuntos de cifrado nuevo. En la actualidad, los sistemas de cifrado simétrico con el apoyo de Transport Layer Security (TLS) son RC2, RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES) y DES triple. El protocolo se verá reforzada por la adición de Advanced Encryption Standard (AES) Ciphersuites.

RFC 3546: "Transport Layer Security (TLS) Extensions", añade un mecanismo para negociar extensiones de protocolos durante la inicialización de sesión y define algunas extensiones.

RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", añade tres conjuntos de nuevas familias de cifrados para que el protocolo TLS permita la autenticación basada en claves previamente compartidas.

Por lo general, TLS utiliza certificados de clave pública [TLS] o Kerberos [KERB] para la autenticación. Este documento describe cómo usar las claves simétricas (más tarde llamado claves pre-compartidas o PSKs), compartida por adelantado entre las partes en comunicación, para establecer una conexión TLS.

Básicamente, hay dos razones por las cuales uno puede querer hacer esto:

En primer lugar, utilizando claves pre-compartidas puede, en función del conjunto de cifrado, evitar la necesidad de operaciones de clave pública. Esto es útil si se utiliza TLS en el rendimiento de entornos con limitaciones de potencia de CPU limitado.

En segundo lugar, claves pre-compartidas puede ser más conveniente desde el punto de vista de la gestión de claves. Por ejemplo, en ambientes cerrados donde las conexiones son en su mayoría configurado manualmente con antelación, puede ser más fácil de configurar una PSK de utilizar certificados. Otro caso es cuando las partes ya tienen un mecanismo para la creación de una clave secreta compartida, y que el mecanismo podría ser utilizado para "arrancar" una clave para autenticar una conexión TLS.

4.2.4 PROTOCOLO IPSEC

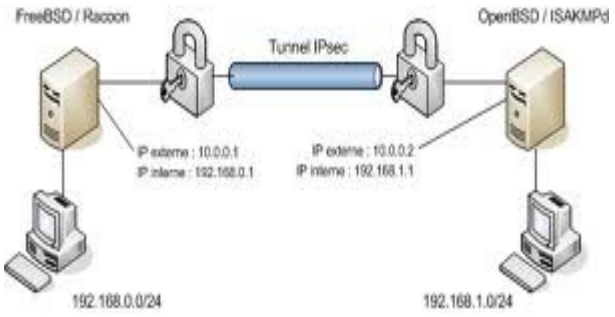


Imagen 17: Protocolo IPsec

IPsec son las abreviaturas de Internet Protocol security, es decir Protocolo de Seguridad de Internet, es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Este protocolo fue desarrollado para IPv6, que posteriormente también fue utilizado por IPv4.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad como base para construir funciones de seguridad en IP, que es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

IPsec emplea dos protocolos diferentes AH y ESP, para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de los datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados

inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases).

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.
- Protocolo IPsec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.
- Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:
- Modo IPsec (túnel o transporte)
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.

- Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales.

Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas

críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves.

Para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

Los protocolos IPsec

La familia de protocolos IPsec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50.

AH - Cabecera de autenticación

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.

La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente

es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bit protege frente a ataques por repetición. Finalmente, los últimos 96 bit almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network address translation - Traducción de direcciones de red, también conocido como Enmascaramiento de direcciones) reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

ESP - Carga de Seguridad Encapsulada

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes.

Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI especifica qué SA emplear para desencapsular el

paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT-Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

El protocolo IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la

SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec.

La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509 (racoon puede realizar esta autenticación incluso mediante Kerberos).

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y

transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido.

Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

4.2.4 PROTOCOLO PPTP

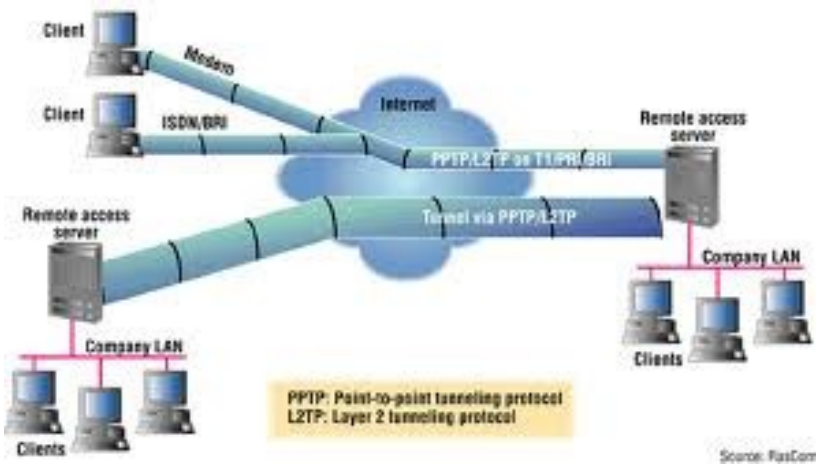


Imagen 18: Protocolo PPTP

El protocolo PPTP que viene del inglés Point to Point Tunneling Protocol que significa Protocolo Tunelizado Punto a Punto, es un protocolo de comunicaciones desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas

colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

Una VPN es una red privada de computadores que usa Internet para conectar todos sus nodos.

El protocolo PPTP permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol). La tecnología PPTP encapsula los paquetes ppp en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización. Las compañías "involucradas" en el desarrollo del PPTP son Microsoft, Ascend Communications, 3com / Primary Access, ECI Telematics y US Robotics.

PPTP y VPN: El protocolo Point-To-Point Tunneling Protocol viene incluido con Windows NT 4.0 Server y Workstation. Los computadores que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red pública como Internet.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPN`s sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad ASLEAP puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo.

4.2.5 PROTOCOLO IEEE 802.1Q

Imagen 19: Protocolo IEEE 802.1Q

El protocolo IEEE 802.1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

IEEE es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

Este protocolo es comúnmente conocido como dot1Q.

Formato de la trama

El protocolo IEEE 802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un recálculo del campo "FCS".

VLAN nativas

El estándar 9 de este protocolo define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLAN nativas. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk. Y en el otro lado, si a un puerto llega una trama sin etiquetar, la trama se considera perteneciente a la VLAN nativa de ese puerto. Este modo de funcionamiento

fue implementado para asegurar la interoperabilidad con antiguos dispositivos que no entendían 802.1Q.

La VLAN nativa es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk. Sólo se puede tener una VLAN nativa por puerto.

4.3 PROTOCOLO HTTP

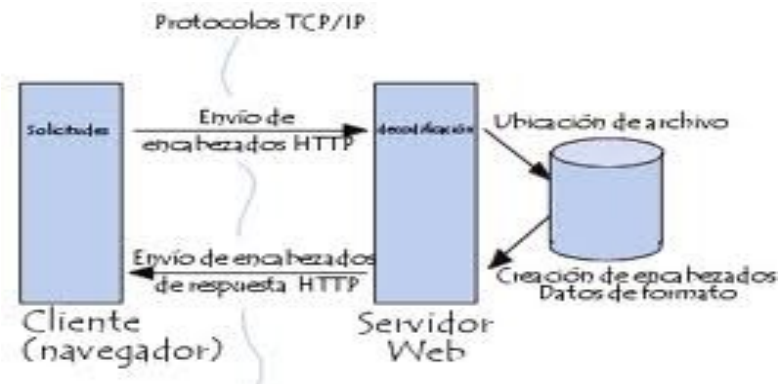


Imagen 20: Protocolo HTTP 1

"El protocolo de transferencia de hipertexto (del inglés Hypertext Transfer Protocol) es el protocolo usado en cada transacción de la Web y define la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse entre sí.

HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1." (wikipedia.org, 2009)

La orientación del uso del protocolo HTTP está orientado a transacciones y sigue el esquema petición – respuesta entre un cliente y un servidor. Un cliente (navegador web) efectúa la petición, luego esta información es transmitida, a lo

que se le llama recurso y se la identifica mediante un localizador uniforme de recursos (URL), estos recursos pueden archivos, el resultado de una ejecución de un programa, una consulta a una base de datos, la traducción de un documento, etc. y la respuesta que es lo que obtenemos como respuesta de la petición realizada mediante el URL.

El protocolo de transferencia de hipertexto es un protocolo del nivel de la capa de aplicación usado para la transferencia de información entre sistemas, de forma clara y rápida. Este protocolo ha sido usado por el World-Wide Web desde 1990.

Este protocolo permite usar una serie de métodos para indicar la finalidad de la petición y se basa en otros conceptos y estándares como Uniform Resource Identifier (URI), Uniform Resource Location (URL) y Uniform Resource Name (URN), para indicar el recurso al que hace referencia la petición. Los mensajes se pasan con un formato similar al usado por el Internet Mail y el Multipurpose Internet Mail Extensions (MIME).

El protocolo HTTP se basa en un paradigma de peticiones y respuestas. Un cliente envía una petición en forma de método, una URI, y una versión de protocolo seguida de los modificadores de la petición de forma parecida a un mensaje MIME, información sobre el cliente y al final un posible contenido. El servidor contesta con una línea de estado que incluye la versión del protocolo y un código que indica éxito o error, seguido de la información del servidor en forma de mensaje MIME y un posible contenido.

Generalmente es el cliente el que inicia la comunicación HTTP y consiste en la petición de un recurso del servidor. Puede hacerse de forma directa al servidor o a través de intermediarios.

Sintaxis de la petición

El esquema “http” se usa para localizar recursos en la red por medio del protocolo http.

La sintaxis de la petición es la siguiente:

“http:” “//"' dirección [“:” puerto] [path]

Donde dirección es el nombre de un dominio de Internet o una dirección IP, el puerto es un número que indica el puerto al que se envía la petición y el path indica el recurso al que se accede.

Si no se indica un número de puerto, por defecto se supone que se accede al puerto 80.

Si no se indica un path, entonces se supone que este es “/”.

4.3.1 Sintaxis de la petición

El esquema “http” se usa para localizar recursos en la red por medio del protocolo http.

La sintaxis de la petición es la siguiente:

“http:” “//"' dirección [“:"' puerto] [path]

Donde dirección es el nombre de un dominio de Internet o una dirección IP, el puerto es un número que indica el puerto al que se envía la petición y el path indica el recurso al que se accede. Si no se indica un número de puerto, por defecto se supone que se accede al puerto 80. Si no se indica un path, entonces se supone que este es ``/''.

4.3.1.1 Mensaje HTTP

Un mensaje http es una petición de un cliente al servidor y en la respuesta que el servidor envía al cliente.

Las peticiones y respuestas pueden ser simples o completas. La diferencia es que en las peticiones y respuestas completas se envían cabeceras y un contenido. Este contenido se pone después de las cabeceras dejando una línea vacía entre las cabeceras y el contenido. En el caso de peticiones simples, sólo se puede usar el método GET y no hay contenido. Si se trata de una respuesta simple, entonces ésta sólo consta de contenido.

Esta diferenciación entre simples y completas se tiene para que el protocolo HTTP/1.0 pueda atender peticiones y enviar respuestas del protocolo HTTP/0.9.

4.3.1.2 Petición

Una petición de un cliente a un servidor incluye el método que se aplica al recurso, el identificador del recurso y la versión del protocolo que usa para realizar la petición.

Para mantener la compatibilidad con el protocolo HTTP/0.9 se permite una petición simple con el formato:

“GET”' SP URI CRLF

Donde SP es un espacio, URI es la URI del recurso al que hace referencia la petición y CRLF es un retorno de carro y nueva línea.

En el caso de que la petición se haga con el protocolo HTTP/1.0 o con el protocolo

HTTP/1.1 la petición sigue el formato:

Línea de petición

*(Cabeceras)

CRLF

[Contenido]

La línea de petición comienza indicando el método, seguido de la URI de la petición y la versión del protocolo, finalizando la línea con CRLF:

En el caso del protocolo HTTP/0.9 sólo se permite el método GET, con el protocolo

HTTP/1.0 GET, POST y HEAD y con el protocolo HTTP/1.1 OPTIONS, GET, HEAD,

POST, PUT, DELETE y TRACE. En caso de que un servidor tenga implementado un método, pero no está permitido para el recurso que se pide,

entonces ha de devolver un código de estado 405 (método no permitido). Si lo que ocurre es que no tiene implementado el método, entonces devuelve un código 501 (no implementado). Los únicos métodos que deben soportar los servidores de forma obligatoria son los métodos GET y HEAD.

En el apartado de cabeceras, éstas pueden ser de tres tipos: cabeceras generales, de petición y de entidad. Las cabeceras generales son las que se aplican tanto a peticiones como a respuestas, pero no al contenido que se transmite. Las cabeceras de petición permiten al cliente pasar información al servidor sobre la petición y sobre el cliente. Las cabeceras de entidad permiten definir información adicional sobre el contenido que se transmite y en caso de que no haya contenido, sobre el recurso al que se quiere acceder con la petición.

El contenido (si está presente) está en un formato con una codificación definida en las cabeceras de entidad.

4.3.1.3 Respuesta

Después de recibir e interpretar una petición, el servidor debe responder con un mensaje HTTP. Este mensaje tiene el siguiente formato:

Línea de estado

*(Cabeceras)

CRLF

[Contenido]

La línea de estado es la primera línea de la respuesta y consiste en la versión de protocolo que se utiliza, seguida de una indicación de estado numérica a la que puede ir asociada una frase explicativa. El formato es el siguiente:

“Versión del protocolo” SP “Código de estado” SP “Frase explicativa” CRLF

El código de estado es un número de 3 dígitos que indica si la petición ha sido atendida satisfactoriamente o no, y en caso de no haber sido atendida, indica la causa. Los códigos se dividen en cinco clases definidas por el primer dígito del código de estado.

Así tenemos:

1xx: Informativo. La petición se recibe y sigue el proceso. Esta familia de respuestas indican una respuesta provisional. Este tipo de respuesta está formada por la línea de estado y las cabeceras. Un servidor envía este tipo de respuesta en casos experimentales.

2xx: Éxito. La acción requerida por la petición ha sido recibida, entendida y aceptada.

3xx: Redirección. Para completar la petición se han de tomar más acciones.

4xx: Error del cliente. La petición no es sintácticamente correcta y no se puede llevar a cabo.

5xx: Error del servidor. El servidor falla al atender la petición que aparentemente es correcta.

4.3.2 CÓDIGOS DE HTTP

Imagen 21: Logo de HTTP

Algunos de los códigos más comúnmente usados y las frases asociadas son:

CÓDIGO	DESCRIPCIÓN
100,	Continuar.
101,	Cambio de protocolo.
200,	Éxito.
201,	Creado.
202,	Información no autoritativa.
203,	
204,	Sin contenido.
205,	Contenido restablecido.
206,	Contenido parcial.
300,	Múltiples elecciones.

301,	Movido permanentemente.
302,	Movido temporalmente.
303,	Ver otros.
304,	No modificado.
305,	Usar proxy.
400,	Petición errónea.
401,	No autorizado.
402,	Pago requerido.
403,	Prohibido.
404,	No encontrado.
405,	Método no permitido.
406,	No se puede aceptar.
407,	Se requiere autentificación proxy.
408,	Límite de tiempo de la petición.
409,	Conflicto.
410,	Gone.
411,	Tamaño requerido.

412,	Falla una precondición.
413,	Contenido de la petición muy largo.
414,	URI de la petición muy largo.
415,	Campo media type requerido.
500,	Error interno del servidor.
501,	No implementado.
502,	Puerta de enlace errónea.
503,	Servicio no disponible.

La frase explicativa, es eso, una frase corta que explica el código de estado enviado al cliente.

Se pueden usar más códigos, pero las aplicaciones HTTP no tienen que conocer todos los códigos definidos y su significado, pero sí están obligadas a conocer su clase y tratar los códigos desconocidos como el primer código de la clase (x00).

En cuanto a las cabeceras de la respuesta, son de tres tipos: las cabeceras generales, las cabeceras de la respuesta y las cabeceras de entidad.

Las cabeceras de respuesta permiten al servidor enviar información adicional al cliente sobre la respuesta. Estos campos dan información sobre el servidor y acceso al recurso pedido.

4.3.3 MÉTODOS

Un método se dice que es seguro si no provocan ninguna otra acción que no sea la de devolver algo (no produce efectos laterales). Estos métodos son el método GET y el método HEAD. Para realizar acciones inseguras (las que afectan a otras acciones) se pueden usar los métodos POST, PUT y DELETE. Aunque esto está definido así, no se puede asegurar que un método seguro no produzca efectos laterales, porque depende de la implementación del servidor.

Un método es idempotente si los efectos laterales para N peticiones son los mismos que para una sola petición. Los métodos idempotentes son los métodos GET, HEAD, PUT y DELETE.

4.3.3.1 Método OPTIONS

Este método representa una petición de información sobre las opciones de comunicación disponibles en la cadena petición-respuesta identificada por la URI de la petición. Esto permite al cliente conocer las opciones y requisitos asociados con un recurso o las capacidades del servidor.

La respuesta sólo debe incluir información sobre las opciones de comunicación.

Si la URI es "*", entonces la petición se aplica al servidor como un conjunto. Es decir, contesta características opcionales definidas por el servidor, extensiones del protocolo, etc.

4.3.3.2 Método GET

El método GET requiere la devolución de información al cliente identificada por la URI. Si la URI se refiere a un proceso que produce información, se devuelve la información y no la fuente del proceso.

El método GET pasa a ser un GET condicional si la petición incluye las cabeceras If-Modified-Since, If-Unmodified-Since, If-Match, If-None-Match o If-Range.

Estas cabeceras hacen que el contenido de la respuesta se transmita sólo si se cumplen unas condiciones determinadas por esas cabeceras. Esto se hico para reducir el tráfico en las redes.

También hay un método GET parcial, con el que se envía sólo parte del contenido del recurso requerido. Esto ocurre cuando la petición tiene una cabecera Range. Al igual que el método GET condicional, el método GET parcial se creó para reducir el tráfico en la red.

4.3.3.3 Método HEAD

El método HEAD es igual que el método GET, salvo que el servidor no tiene que devolver el contenido, sólo las cabeceras. Estas cabeceras que se devuelven en el método HEAD deberían ser las mismas que las que se devolverían si fuese una petición GET.

Este método se puede usar para obtener información sobre el contenido que se va a devolver en respuesta a la petición. Se suele usar también para chequear la validez de links, accesibilidad y modificaciones recientes.

4.3.3.4 Método POST

El método POST se usa para hacer peticiones en las que el servidor destino acepta el contenido de la petición como un nuevo subordinado del recurso pedido. El método

POST se creó para cubrir funciones como la de enviar un mensaje a grupos de usuarios, dar un bloque de datos como resultado de un formulario a un proceso de datos, añadir nuevos datos a una base de datos, etc.

La función llevada a cabo por el método POST está determinada por el servidor y suele depender de la URI de la petición. El resultado de la acción realizada por el método POST puede ser un recurso que no sea identificable mediante una URI.

4.3.3.5 Método PUT

El método PUT permite guardar el contenido de la petición en el servidor bajo la URI de la petición. Si esta URI ya existe, entonces el servidor considera que esta petición proporciona una versión actualizada del recurso. Si la URI indicada no existe y es válida para definir un nuevo recurso, el servidor puede crear el recurso con esa URI. Si se crea un nuevo recurso, debe responder con un código 201 (creado), si se modifica se contesta con un código 200 (OK) o 204 (sin contenido). En caso de que no se pueda crear el recurso se devuelve un mensaje con el código de error apropiado.

La principal diferencia entre POST y PUT se encuentra en el significado de la URI. En el caso del método POST, la URI identifica el recurso que va a manejar en contenido, mientras que en el PUT identifica el contenido.

Un recurso puede tener distintas URI.

4.3.3.6 Método DELETE

Este método se usa para que el servidor borre el recurso indicado por la URI de la petición. No se garantiza al cliente que la operación se lleve a cabo aunque la respuesta sea satisfactoria.

4.3.3.7 Método TRACE

Este método se usa para saber si existe el receptor del mensaje y usar la información para hacer un diagnóstico. En las cabeceras el campo Via sirve para obtener la ruta que sigue el mensaje. Mediante el campo Max-Forwards se limita el número de pasos intermedios que puede tomar. Esto es útil para evitar bucles entre los proxy.

La petición con el método TRACE no tiene contenido.

4.3.4 CABECERAS

4.3.4.1 Generales

Los campos de este tipo de cabeceras se aplican tanto a las peticiones como a las respuestas, pero no al contenido de los mensajes.

Estas cabeceras son:

Cache-Control, son directivas que se han de tener en cuenta a la hora de mantener el contenido en una caché.

Connection, permite especificar opciones requeridas para una conexión.

Date, representa la fecha y la hora a la que se creó el mensaje.

Pragma, usado para incluir directivas de implementación.

Transfer-Encoding, indica la codificación aplicada al contenido.

Upgrade, permite al cliente especificar protocolos que soporta.

Via, usado por pasarelas y proxies para indicar los pasos seguidos.

4.3.4.2 De petición

Este tipo de cabeceras permite al cliente pasar información adicional al servidor sobre la petición y el propio cliente.

Estas cabeceras son las siguientes:

Accept, indican el tipo de respuesta que acepta.

Accept-Charset, indica los conjuntos de caracteres que acepta.

Accept-Encoding, que tipo de codificación acepta.

Accept-Language, tipo de lenguaje de la respuesta que se prefiere.

Authorization, el agente de usuario quiere autentificarse con el servidor.

From, contiene la dirección de correo que controla en agente de usuario.

Host, especifica la máquina y el puerto del recurso pedido.

If-Modified-Since, para el GET condicional.

If-Match, para el GET condicional.

If-None-Match, para el GET condicional.

If-Range, para el GET condicional.

If-Unmodified-Since, para el GET condicional.

Max-Forwards, indica el máximo número de elementos por los que pasa.

Proxy-Authorization, permite que el cliente se identifique a un proxy.

Range, establece un rango de bytes del contenido.

Referer, indica la dirección donde obtuvo la URI de la petición.

User-Agent, información sobre el agente que genera la petición.

4.3.4.3 De respuesta

Permiten al servidor pasar información adicional al cliente sobre la respuesta, el propio servidor y el recurso solicitado.

Son los campos:

Age, estimación del tiempo transcurrido desde que se creó la respuesta.

Location, se usa par a redirigir la petición a otra URI.

Proxy-Authenticate, ante una respuesta con el código 407 (autentificación proxy requerida), indica el esquema de autentificación.

Public, da la lista de métodos soportados por el servidor.

Retry-After, ante un servicio no disponible da una fecha para volver a intentarlo.

Server, información sobre el servidor que maneja las peticiones.

Vary, indica que hay varias respuestas y el servidor ha escogido una.

Warning, usada para aportar información adicional sobre el estado de la respuesta.

WWW-Authenticate, indica el esquema de autentificación y los parámetros aplicables a la URI.

4.3.4.4 Cabeceras de entidad

Como su nombre indica, los campos de este tipo aportan información sobre el contenido del mensaje o si no hay contenido, sobre el recurso al que hace referencia la URI de la petición.

Los campos de este tipo son:

Allow, da los métodos soportados por el recurso designado por la URI.

Content-Base, indica la URI base para resolver las URI relativas.

Content-Encoding, indica una codificación adicional aplicada al contenido (aparte de la aplicada por el tipo).

Content-Language, describe el idioma del contenido.

Content-Length, indica el tamaño del contenido del mensaje.

Content-Location, da información sobre la localización del recurso que da el contenido del mensaje.

Content-MD5, es un resumen en formato MD5 (RFC 1864) para chequear la integridad del contenido.

Content-Range, en un GET parcial, indica la posición del contenido.

Content-Type, indica el tipo de contenido que es.

Etag, define una marca para el contenido asociado.

Expires, indica la fecha a partir de la cual la respuesta deja de ser válida.

Last-Modified, indica la fecha de la última modificación.

4.4 HACKER

Imagen 22: Foto de Hacker

Se llama Hacker a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo, el cual puede o no ser maligno, o legal o ilegal.

La acción de usar sus conocimientos se denomina hacking o hackeo.

4.4.1 Comunidades Hacker

Un hacker es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes:

- **Gente apasionada por la seguridad informática**. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

- **Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta** alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT. Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son creaciones de hackers. El RFC 13924 amplia este significado como "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas"

- **La comunidad de aficionados a la informática doméstica**, centrada en el hardware posterior a los setenta y en el software (juegos de ordenador, crackeo de software) de entre los ochenta/noventa.

En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. A los criminales se les pueden sumar los llamados "script kiddies", gente que invade computadoras, usando

programas escritos por otros, y que tiene muy poco conocimiento sobre cómo funcionan. Este uso parcialmente incorrecto se ha vuelto tan predominante que, en general, un gran segmento de la población no es consciente de que existen diferentes significados.

Mientras que los hackers aficionados reconocen los tres tipos de hackers y los hackers de la seguridad informática aceptan todos los usos del término, los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como "crackers" (analogía de "safecracker", que en español se traduce como "un ladrón de cajas fuertes").

Los términos hacker y hack tienen connotaciones positivas e, irónicamente, también negativas. Los programadores informáticos suelen usar las hacking y hacker para expresar admiración por el trabajo de un desarrollador de software cualificado, pero también se puede utilizar en un sentido negativo para describir una solución rápida pero poco elegante a un problema. Algunos desaprueban el uso del hacking como un sinónimo de cracker, en marcado contraste con el resto del mundo, en el que la palabra hacker se utiliza normalmente para describir a alguien que se infiltra en un sistema informático con el fin de eludir o desactivar las medidas de seguridad.

Desde el año 2002-2003, se ha ido configurando una perspectiva más amplia del hacker, pero con una orientación a su integración al hacktivismo en tanto movimiento. Aparecen espacios autónomos denominados hacklab o hackerspace y los hackmeeting como instancias de diálogo de hackers. Desde

esta perspectiva, se entiende al hacker como una persona que es parte de una conciencia colectiva que promueve la libertad del conocimiento y la justicia social.

En este caso, los roles de un hacker pueden entenderse en cuatro aspectos:

- Apoyar procesos de apropiación social o comunitaria de las tecnologías.
- Poner a disposición del dominio público el manejo técnico y destrezas alcanzadas personal o grupalmente.
- Crear nuevos sistemas, herramientas y aplicaciones técnicas y tecnológicas para ponerlas a disposición del dominio público.
- Realizar acciones de hacktivismo tecnológico con el fin de liberar espacios y defender el conocimiento común, o mancomunal

4.4.2 Terminologías De Hackers

White hat y black hat

Un hacker de sombrero blanco (del inglés, White hat), en jerga informática, se refiere a una ética hacker que se centra en asegurar y proteger los sistemas de Tecnologías de información y comunicación. Estas personas suelen trabajar para empresas de seguridad informática las cuales los denominan, en ocasiones, «zapatillas o equipos tigre»

Por el contrario, un hacker de sombrero negro (del inglés, Black Hat) es el villano o chico malo, especialmente en una película de western, de ahí que en tal carácter se use un sombrero negro, en contraste con el héroe, el de sombrero blanco.

También conocidos como "crackers" muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking.

En los últimos años, los términos sombrero blanco y un sombrero negro han sido aplicados a la industria del posicionamiento en buscadores (Search Engine Optimization, SEO). Las tácticas de posicionamiento en buscadores de los hackers de sombrero negro, también llamada spamdexing, intento de redireccionar los resultados de la búsqueda a páginas de destino particular, son una moda que está en contra de los términos de servicio de los motores de búsqueda, mientras que los hackers de sombrero blanco, utilizan métodos que son generalmente aprobados por los motores de búsqueda.

Samurái

Normalmente es alguien contratado para investigar fallos de seguridad, que investiga casos de derechos de privacidad, esté amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitime acciones semejantes. Los samuráis desdeñan a los crackers y a todo tipo de vándalos electrónicos. También se dedican a hacer y decir cómo saber sobre la seguridad con sistemas en redes

Phreaker

De phone freak ("monstruo telefónico"). Son personas con conocimientos amplios tanto en teléfonos modulares (TM) como en teléfonos móviles.

Wannabe

Generalmente son aquellos a los que les interesa el tema de hacking y/o phreaking pero que por estar empezando no son reconocidos por la elite. Son aquellos que si perseveran aprendiendo y estudiando, pueden llegar a convertirse perfectamente en hackers. No por ser novato es repudiado, al igual que tampoco hay que confundirlo con un lammer.

Lammer o script-kiddies

Es un término coloquial inglés aplicado a una persona falta de madurez, sociabilidad y habilidades técnicas o inteligencia, un incompetente, que por lo general pretenden hacer hacking sin tener conocimientos de informática. Solo se dedican a buscar y descargar programas de hacking para luego ejecutarlos, como resultado de la ejecución de los programas descargados estos pueden terminar colapsando sus sistemas por lo que en general acaban destrozando la plataforma en la que trabajan.

Son aprendices que presumen ser lo que no son, aprovechando los conocimientos del hacker y poniéndolos en práctica, sin saber. En pocas palabras, no saben nada de hacking o roban programas de otros, frecuentemente recién hechos, y dicen que los crearon ellos.

Newbie

Newbie es un término utilizado comúnmente en comunidades en línea para describir a un novato, en esta área, es el que no posee muchos conocimientos en el tema.

4.5 CREAR UNA CONEXIÓN SEGURA MEDIANTE UNA TÉCNICA DEL TUNELIZADO

Con lo expuesto de las ventajas que brindan estos protocolos, podemos resumir por ejemplo que el protocolo SSH protege contra los siguientes tipos de ataques:

• IP Spoofing: un ordenador trata de hacerse pasar por otro ordenador (en el que confiamos) y nos envía paquetes "procedentes" del mismo. SSH es incluso capaz de proteger el sistema contra un ordenador de la propia red que se hace pasar por el router de conexión con el exterior.

• Enrutamiento de la IP de origen: un ordenador puede cambiar la IP de un paquete procedente de otro, para que parezca que viene desde un ordenador en el que se confía.

• DNS spoofing: un atacante compromete los registros del servicio de nombres.

• Intercepción de passwords y datos a través de la red.

• Manipulación de los datos en ordenadores intermediarios.

• Ataques basados en escuchar autentificación contra servidores X-Windows remotos.

4.5.1 Conexión a un servidor remoto usando el protocolo SSH

Para conectarnos con un servidor SSH remoto desde Ubuntu tenemos un cliente por defecto. En Windows no, hay que descargar un cliente (por ejemplo,

el programa Putty). Usar el cliente es muy sencillo: basta con teclear desde una consola o terminal lo siguiente:

$ ssh host_remoto

Donde host_remoto es la IP del servidor SSH o el nombre de este. Eso hará que nos conectemos con nuestro nombre de usuario. Si queremos conectar como un usuario remoto teclearemos:

$ ssh usuario_remoto@host_remoto

Luego nos pide la contraseña del usuario. La primera vez que nos conectemos a un servidor tarda un poco más y nos pide confirmación tecleando "yes" con todas sus letras, las subsiguientes ya no. Sabemos que estamos conectados porque el prompt cambia y aparece en lugar del nombre de nuestro host el nombre del host remoto.

Los comandos, programas y scripts que lancemos tras conectarnos se ejecutarán en la máquina a las que nos hayamos conectado, utilizando los recursos del host remoto (CPU, memoria, disco, etc.). Esta arquitectura puede utilizarse, por ejemplo, para tener un servidor más potente y varios clientes que ejecutan aplicaciones en dicha máquina.

Para ejecutar aplicaciones gráficas en la máquina a la que nos conectamos tenemos dos opciones. La primera consiste en definir la variable $DISPLAY apuntando a la máquina desde la que nos conectamos.

$ export DISPLAY=host_local:0.0

Este mecanismo no se recomienda por motivos de seguridad (el protocolo X11 no se encuentra cifrado) y, además, pueden encontrarse problemas porque cortafuegos intermedios bloqueen ese tráfico (puertos 600x TCP).

Una solución mejor es utilizar un túnel SSH para encapsular el protocolo X11, lo que transmite la información de manera segura y, además, no suele dar problemas con los cortafuegos intermedios.

Para poder ejecutar aplicaciones gráficas en el host remoto de forma segura, necesitamos dos cosas. La primera, que en la configuración del servidor SSH del host remoto (/etc/ssh/sshd_config) se encuentre activada la siguiente opción:

```
X11Forwarding yes
```

Para aprovechar esta característica, hemos de conectarnos usando el parámetro -X, lo que exportará la configuración de la variable $DISPLAY con lo que podremos ejecutar aplicaciones gráficas de forma remota:

```
$ ssh -X usuario_remoto@host_remoto
```

Ahora si ejecutas el programa xclock verás que la ventana sale en tu escritorio:

```
$ xclock
```

4.6 CUADRO COMPARATIVO ENTRE LOS PRINCIPALES PROTOCOLOS DE TUNELIZADO

Protocolo Características	Protocolo SSH	Protocolo SSL
Plataforma	Linux, Unix, Windows(Putty), Mac	Linux, Unix, Windows, Mac
Encriptado	• Cifrado del tráfico basado en cifrado simétrico	• Usa criptografía • Intercambio de claves públicas y autenticación basada en certificados digitales • Cifrado del tráfico basado en cifrado simétrico
Estándares	RFC 4250, RFC 4251, RFC 4252, RFC 4253, RFC 4254, RFC 4255, RFC 4256, RFC 4335, RFC 4344, RFC 4345, RFC 4419, RFC 4432, RFC 4462, RFC 4716, RFC 4819	RFC 2246, RFC 2712, RFC 2817, RFC 2818, RFC 3268, RFC 3546, RFC 4279
Capa del modelo OSI	Capa de Aplicación	Capa de Transporte

Cuadro 3: Cuadro Comparativo Protocolos 1

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Como conclusiones podemos decir que existen protocolos que sirven para tener tráfico seguro en una red, pero por desconocimiento no se los utilizan para este fin y de forma directa entre equipos en una red.

Es así que el protocolo SSH permite crear un túnel directo entre dos maquinas pudiendo administrar la otra máquina de forma remota. Así mismo otro protocolo como el SSL que como se ha visto encripta los datos y permite también enviar datos de forma segura por la red, al igual que el protocolo PPTP que nos brinda un protocolo tunelizado punto a punto tan seguro que se utiliza en las redes privadas virtuales o VPN's y finalmente también desarrollamos sobre el protocolo tunelizado IEEE 802.1Q que es un protocolo que permite comunicar a varias redes de forma transparente, segura y fiable.

Es por esto que el tema desarrollado es muy interesante ya que he aprendido sobre la importancia de estos protocolos y su implementación es muy fácil y muy útil para la casa, la oficina o en una organización, incluso cuando trabajamos como administrador del área de sistemas se puede administrar otra máquina en forma remota, facilitando muchísimo el trabajo y con herramientas sencillas de utilizar como los protocolos objetos de estudio de la presente tesina.

5.2 RECOMENDACIONES

Luego de realizado la descripción de los diferentes elementos que forman parte de un tunelizado y sus diferentes técnicas, podemos recomendar que para evitar un ataque hacker a nuestra información enviada por una red, lo mejor que se puede usar es un protocolo tunelizado, como por ejemplo el protocolo SSH para poder conectarse entre diferentes maquinas de nuestra red, que funciona parecido a Telnet, pero con la diferencia que el protocolo SSH cifra la información para que no pueda ser legible por terceras personas en caso de que este paquete de información pueda ser interceptado, lo que permite proteger nuestra información enviada llegue segura a su destino, ya que no podrá ser legible por otras personas sino únicamente por el origen y destino especificados.

Así mismo podemos recomendar el uso del protocolo SSL para evitar ataques hacker, ya que es muy usado especialmente en Internet, por su encriptación que usa para los dos extremos de la comunicación, protegiendo de una excelente manera la información que se envía por internet, ya que este protocolo uso criptografía para proteger los paquetes, negocia entre las partes que se comunican, intercambian claves publicas y autenticaciones basadas en certificados digitales lo que maximiza la seguridad del envío de información, usando el cifrado simétrico para el manejo de tráfico.

Otro protocolo muy usado es el PPTP que permite también el intercambio seguro de datos, ya que crea una red privada virtual entre el cliente y el

servidor. Lo más notorio de este protocolo es que provee redes privadas gratuitas para una compañía. Al ser una extensión mejorada de la tecnología PPP

Otro protocolo recomendado para este fin es el protocolo IEEE 802.1Q, llamado así porque lo crearon el grupo de trabajo 802 de la IEEE diseñaron un mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, con la ventaja de no tener problemas de interferencia entre estas redes.

5.3 APORTES DE LA INVESTIGACIÓN

- La presente investigación intenta aportar al conocimiento sobre el tema de las técnicas de tunelizado, ya que como se demostró hay un gran desconocimiento sobre este tema.
- Se realizo una socialización sobre este tema a los alumnos de quintos y sextos cursos del Colegio Técnico Nabón en el que soy profesor sobre el tema de mi tesis y sus beneficios.
- Se subió el desarrollo del presente trabajo al internet a la dirección: Braulio.ochoa.blogspot.com para aportar con la comunidad mundial esta investigación.

GLOSARIO

Algoritmo de Encriptación: Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales.

Blowfish: En criptografía, Blowfish es un codificador de bloques simétricos, diseñado por Bruce Schneier en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado.

Criptología: Ciencia que estudia el arte de crear y utilizar sistemas de encriptación.

Delito Informático: Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

Desencriptación: Descifrado. Recuperación del contenido real de una información previamente encriptada o cifrada.

Encriptación: Acción de proteger la información mediante técnicas criptográficas ante modificaciones o utilización no autorizada.

Firewall: Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

Firma Digital: Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación.

Integridad: Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

Paquete: Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial.

Sitio Web: Traducción del inglés Web Site, conjunto de páginas de una institución o persona.

Spam: Se llama Spam, correo basura o SMS basura, a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

Spoofing: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Spyware: Software que se instala en una computadora para recopilar información sobre las actividades realizadas en ella.

REFERENCIAS BIBLIOGRÁFICAS:

ALEGSA. (01 de Febrero de 2011). Recuperado el 01 de Noviembre de 2011, de Sitio Web alegsa.com.ar: http://www.alegsa.com.ar/Dic/protocolo%20tunelizado.php

Alvarez, M. A. (01 de Febrero de 2011). Recuperado el 29 de Octubre de 2011, de Sitio Web desarrolloweb.com: http://www.desarrolloweb.com/articulos/telnet-ssh-protocolo-red.html

Campaña, D. A. (11 de Diciembre de 2088). Recuperado el 23 de Octubre de 2011, de Sitio Web cruzrojainstituto.edu.ec: http://www.cruzrojainstituto.edu.ec/Documentos/Segunda.pdf

Castillo, A. G. (28 de Marzo de 2002). Recuperado el 01 de Noviembre de 2011, de Sitio Web uma.es: http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/http.html

CIVILA.COM y EDUCAR.ORG. (01 de Enero de 2010). Recuperado el 25 de Octubre de 2011, de Sitio Web civila.com: http://www.civila.com/desenredada/que-es.html

Félix, A. d. (01 de Enero de 2000). Recuperado el 25 de Octubre de 2011, de Sitio Web acsblog.es: http://acsblog.es/articulos/trunk/LinuxActual/Apache/html/x49.html

García, J. (25 de Febrero de 2011). Recuperado el 29 de Octubre de 2011, de Sitio Web naguissa.com: http://www.naguissa.com/archivos.php?path=11&accion=descarga&IDarchivo=58

Guglielmetti, M. (11 de Febrero de 2005). Recuperado el 28 de Octubre de 2011, de Sitio web mastermagazine.info: http://www.mastermagazine.info/termino/5204.php

INTERLAB.ES. (29 de Enero de 2010). Recuperado el 29 de Octubre de 2011, de Sitio Web interlab.es: http://www.internetlab.es/post/888/que-significa-el-protocolo-https-y-como-funciona/

Jeff. (16 de Octubre de 2008). Recuperado el 28 de Octubre de 2011, de Sitio Web kioskea.net: http://es.kioskea.net/contents/internet/protocol.php3

MASADELANTE.COM. (30 de Junio de 2011). Recuperado el 27 de Octubre de 2011, de Sitio Web masadelante.com: http://www.masadelante.com/faqs/que-significa-http

Michelena, A. V. (01 de Enero de 2007). Recuperado el 23 de Octubre de 2011, de Sitio Web books.google.com.ec: http://books.google.com.ec/books?id=u0ZeCjcr2S0C&pg=PA141&dq=hacker+definicion&hl=es&ei=1TRiTt3LGcba0QGX5e22Cg&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCkQ6AEwAA#v=onepage&q&f=false

MONOGRAFIAS.COM. (15 de Marzo de 2011). Recuperado el 30 de Octubre de 2011, de Sitio Web monografias.com: http://www.monografias.com/Computacion/Internet/

Otrre, L. (13 de Septiembre de 2009). Recuperado el 30 de Octubre de 2011, de Sitio Web guia-ubuntu.org: http://www.guia-ubuntu.org/index.php?title=rvidor_ssh#Conexi.C3.B3n_a_un_servidor_remoto

RAE, D. (7 de Junio de 2011). Recuperado el 20 de Octubre de 2011, de Sitio Web buscon.rae.es: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=internet

Universidad NUR. (01 de Noviembre de 2008). Recuperado el 23 de Octubre de 2011, de Sitio Web blogspot.es: http://ciined.blogspot.es/img/ejdecronograma.pdf

wikipedia.org. (01 de Junio de 2009). Recuperado el 15 de Octubre de 2011, de Sitio Web es.wikipedia.org: http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol

wikipedia.org. (21 de Octubre de 2011). Recuperado el 25 de Octubre de 2011, de Sitio Web wikipedia.org: http://es.wikipedia.org/wiki/Internet

wikipedia.org. (02 de Noviembre de 2011). Recuperado el 03 de Noviembre de 2011, de Sitio Web wikipedia.org: http://es.wikipedia.org/wiki/Protocolo_(inform%C3%A1tica)

ANEXO 1: ENTREVISTAS

ANEXO 2: ENCUESTAS

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Tannia Mayorga

PARA: Msc. Luis Andrés Chávez Ing.

DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

ASUNTO: Autorización de Empastado

FECHA Quito, 30 de Noviembre del 2011

Por medio de la presente certifico que el pregradista Braulio Gustavo Ochoa Clavijo con CI No.0103885703 ha realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada “Análisis de las técnicas de tunelizado por HTTP para evitar ataques hacker”, del título de ingenieros en sistemas informáticos

Atentamente

_____

Ing. Tannia Mayorga

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Pablo Ochoa

PARA: Msc. Luis Andrés Chávez Ing.

DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

ASUNTO: Autorización de Empastado

FECHA Cuenca, 30 de Noviembre del 2011

Por medio de la presente certifico que el Braulio Gustavo Ochoa Clavijo con CI No.0103885703 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada "Análisis de las técnicas de tunelizado por HTTP para evitar ataques hacker", del título de ingenieros en sistemas informáticos

Atentamente

_____

Ing. Pablo Ochoa

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Juan Perez

PARA: Msc. Luis Andrés Chávez Ing.

DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL

ASUNTO: Autorización de Empastado

FECHA Cuenca, 30 de Noviembre del 2011

Por medio de la presente certifico que el pregradista Braulio Gustavo Ochoa Clavijo con CI No.0103885703 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada "Análisis de las técnicas de tunelizado por HTTP para evitar ataques hacker", del título de ingenieros en sistemas informáticos

Atentamente

_____

Ing. Juan Perez