UNIVERSIDAD CATÓLICA ANDRÉS BELLO.
FACULTAD DE INGENIERÍA.
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES.

ESTUDIO DEL COMPORTAMIENTO DE VULNERABILIDADES DE UNA RED PRIVADA VIRTUAL (VPN)

TRABAJO ESPECIAL DE GRADO

Presentada ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES.

REALIZADO POR: *Br. Hurtado Calvillo, Wilmer Daniel*
C.I- 18.222.574
Br. Ponce Rivas, Sergio Luis
C.I- 19.227.672

TUTOR: *Ing. Wilmer Pereira*
C.I- 5.521.075

FECHA: *Caracas, Agosto de 2013.*

ESTUDIO DEL COMPORTAMIENTO DE VULNERABILIDADES DE UNA RED PRIVADA VIRTUAL (VPN)

Este jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado:

_____

JURADO EXAMINADOR.

Firma: _____ Firma:_____ Firma: _____

Nombre: Wilmer Pereira **Nombre:** Wilfredo Torres **Nombre:** Javier Barrios

REALIZADO POR: *Br. Hurtado Calvillo, Wilmer Daniel*
C.I- 18.222.574
Br. Ponce Rivas, Sergio Luis
C.I- 19.227.672
TUTOR: *Ing. Wilmer Pereira*
C.I- 5.521.075

FECHA: *Caracas, Agosto de 2013.*

UNIVERSIDAD CATÓLICA ANDRÉS BELLO.
FACULTAD DE INGENIERÍA.
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES.

ESTUDIO DEL COMPORTAMIENTO DE VULNERABILIDADES DE UNA RED PRIVADA VIRTUAL (VPN)

Br. Hurtado Calvillo, Wilmer Daniel wdaniel.20.20@gmail.com
Br. Ponce Rivas, Sergio Luis slponcer@gmail.com

Resumen

Este Trabajo Especial de Grado pretende forjar sólidos conocimientos en el área de seguridad de redes mediante el estudio de vulnerabilidades de Redes Privadas Virtuales. A lo largo del proyecto se estudió las propiedades, elementos y beneficios de una VPN, con el fin de comprender su funcionamiento y observar sus posibles debilidades. Investigando precedentes de vulnerabilidad de seguridad y estudiando posibles ataques que pudiesen ser exitosos contra esta y cualquier tipo de red. Se desarrolló entonces una investigación enfocada en seguridad contra actividades que afecten a una VPN, mediante búsqueda documental y la realización de pruebas experimentales controladas. Encontrando los tipos de ataques que más afectan a una VPN y analizando los escenarios para encontrar soluciones o recomendaciones para cada caso. Esperando dar como aporte, a los administradores de red de las empresas o instituciones, información con respecto a la contingencia a seguir en caso de que su red sea invadida y medidas de prevención.

Palabras clave: VPN, seguridad de redes, troyanos, DOS

ÍNDICE GENERAL

CAPÍTULO I. 1
I.1 Planteamiento del Problema 1
I.2 Objetivos 2
I.2.1 Objetivo General: 2
I.2.2 Objetivos específicos: 2
I.3 Alcance y limitaciones 3
I.4 Justificación 4
CAPÍTULO II 5
II.1 Antecedentes 5
II.2 Marco Teórico 6
II.2.1 Redes 6
II.2.1.1 Seguridad de redes 6
II.3 Red Privada Virtual 7
II.3.1 Tipos de VPN 10
II.3.1.1 VPN de Usuario 11
II.3.3.2 VPN de Sitio 12
II.3.2 VPN a través de LAN 12
II.3.3 Características de una VPN 13
II.3.4 Propiedades de una VPN 13
II.3.5 Componentes de un VPN 14
II.3.6 Beneficios de una VPN 16
II.3.7 Elementos de una VPN 17
II.3.8 Funcionamiento de las VPN 19
II.3.9 Sistemas VPN 20
II.4 Túneles 21
II.4.1 Tipos de túneles 21
II.4.2 Tunneling 21
II.5 Protocolos de VPN y Propiedades de estos 22

II.5.1 PPP (Point to Point Protocol) 22
II.5.2 PPTP (Point to Point Tunneling Protocol) 23
II.5.3 L2TP (Layer 2 Tunneling Protocol) 25
II.5.4 IPSec (Internet Protocol Security) 27
II.5.4.1 Protocolo AH 30
II.5.4.2 Protocolo ESP 32
II.5.4.3 IKE: Protocolo de control 37
II.5.4.4 ISKAMP 41
II.5.5 SSH (Secure Shell) 43
II.6. Análisis de herramientas de estudio de redes (Servidores, Sniffers e IDS) 48
II.6.1 Servidores 48
II.6.2 Sniffers 48
II.6.3 IDS (Sistema de Detección de Intrusos) 50
II.6.4 Tipos de Sistemas de Detección de Intrusiones, IDS 51
II6.4.1 IDS basado en anfitrión (Host-based IDS, HIDS) 51
II.6.4.2 IDS basado en red (Network-Based IDS, NIDS) 53
II.6.5 Perfiladores 55
CAPÍTULO III 56
III.1 Fase I: Realizar la revisión bibliográfica, levantamiento de información. 57
III.2 Fase II: Conocer los distintos ataques para VPN 57
III.3 Fase III: Estudiar que herramientas se utilizaran para medir los parámetros de la VPN. 57
III.4 Fase IV: Instalar la red de prueba 58
III.5 Fase V: Instalar la VPN en la red. 58
III.6 Fase VI: Hacer pruebas pertinentes 58
III.7 Fase VII: Analizar y concluir. 58
III.8 Fase VIII: Redacción del libro de tesis. 58
CAPÍTULO IV 59
IV.1 Fase I: Realizar la revisión bibliográfica, levantamiento de información. 59

IV.2 Fase II: Conocer los distintos ataques para VPN 59
IV.3 Fase III: Estudiar que herramientas se utilizaran para medir los parámetros de la VPN. 60
IV.4 Fase IV: Instalar la red de prueba 62
IV.5 Fase V: Instalar la VPN en la red. 62
IV.6 Fase VI: Hacer pruebas pertinentes 64
IV.7 Fase VII: Analizar y concluir. 65
CAPÍTULO V 66
V.1 Fase II: Conocer los distintos ataques para VPN. 66
V.1.1 Ataques de algoritmos criptográficos 68
V.1.2 Ataques de generador de números aleatorios (RNG) 71
V.1.3 Ataques al Protocolo de seguridad de Internet (IPSec) 72
V1.3.1 Ataques de implantación 73
V1.3.2 Ataques de administración de claves 73
V.1.4 Ataques de Protocolo de establecimiento de túneles punto a punto (PPTP) 74
V.1.6 VPN de sitio 77
V.1.7 Ataques de DOS 78
V.1.8 Sniffers 80
V.1.9 Varios 81
V.2 Fase III: Estudiar que herramientas se utilizarán para medir los parámetros de la VPN. 81
V.3 Fase IV: Instalar la red de prueba 82
V.3 Fase V: Instalar la VPN en la red. 89
V.4 Fase VI: Hacer pruebas pertinentes 89
V.4.1 Experimento 1: Análisis en Ambiente Windows VPN (PPTP) 89
V.4.2 Experimento 2: Análisis en Ambiente Debian VPN (SSH) 91
V.4.1.1 Análisis de Wireshark (Perfilador) 92
V.4.1.2 Análisis de Wireshark (Ataques) 93
V.4.1.3 Resultados del perfilador 96

V.4.1.4 Resultados del NIDS. 98
V.4.1.5 Análisis de eventos detectados por el NIDS 100
V.4.3 Experimento 3: Análisis en ambiente Windows VPN (IPSec/L2TP) 111
V.4.2.1 Análisis de Wireshark (Perfilador).....113
V.4.2.2 Análisis de Wireshark.....115
V.4.2.3 Resultados de NIDS 118
CAPÍTULO VI 127
VI.1 Conclusiones 127
VI.2 Recomendaciones.....129
VI.2.1 VPN de usuario.....130
VI.2.2 VPN de sitio 130
VI.2.3 Ataques de algoritmos criptográficos 131
V.2.4 Ataques comunes en algoritmos criptográficos 131
VI.2.4 Ataques comunes en algoritmos criptográficos.....132
VI.2.5 Ataques de generador de números aleatorios (RNG) 132
VI.2.6 Ataques a IPsec.....133
VI.2.7 Ataques a PPTP 133
VI.2.8 Ataques a la autoridad emisora de certificados 134
Bibliografía.....136
ANEXOS.....138

ÍNDICE DE ILUSTRACIONES

ILUSTRACIÓN 1 RED PRIVADA VIRTUAL FUENTE: (FOROUZAN, 2001) 8
ILUSTRACIÓN 2 PROTOCOLOS MÚLTIPLES DE MANEJO DE VPN. FUENTE: (MAIWALD, 2005) 11
ILUSTRACIÓN 3 CONFIGURACIÓN VPN DE USUARIO. FUENTE: (MAIWALD, 2005) 12
ILUSTRACIÓN 4 VPN SITIO A SITIO DE INTERNET. FUENTE: (MAIWALD, 2005) 12
ILUSTRACIÓN 5 ARQUITECTURA DE RED VPN APROPIADA CUANDO EL MURO DE FUEGO ES EL SERVIDOR VPN. 18
ILUSTRACIÓN 6 ARQUITECTURA DE RED VPN APROPIADA PARA UN SERVIDOR VPN ÚNICO. FUENTE: (MAIWALD, 2005) 18
ILUSTRACIÓN 7 PPTP. FUENTE: (MICROSOFT, 2012) 25
ILUSTRACIÓN 8 ESQUEMA L2TP. FUENTE: (FARLEX, 2012)..... 27
ILUSTRACIÓN 9 ESTRUCTURA DE UN DATAGRAMA AH. FUENTE: (IGLESIAS, 2001) 31
ILUSTRACIÓN 10 FUNCIONAMIENTO DEL PROTOCOLO AH. FUENTE: (IGLESIAS, 2001) 32
ILUSTRACIÓN 11 ESTRUCTURA DE UN DATAGRAMA ESP. FUENTE: (IGLESIAS, 2001) 33
ILUSTRACIÓN 12 FUNCIONAMIENTO DEL PROTOCOLO ESP 35
ILUSTRACIÓN 13 MODOS DE FUNCIONAMIENTO TRANSPORTE Y TÚNEL IPSEC (IGLESIAS, 2001)..... 37
ILUSTRACIÓN 14 FUNCIONAMIENTO DEL PROTOCOLO IKE. FUENTE: (IGLESIAS, 2001) 39
ILUSTRACIÓN 15 PKI EN IPSEC. FUENTE: (IGLESIAS, 2001) 41
ILUSTRACIÓN 16 ENCABEZADO BÁSICO DE ISAKMP 43
ILUSTRACIÓN 17 ESQUEMA RESUMEN DE LA METODOLOGÍA 57
ILUSTRACIÓN 18 USO DE UN TROYANO PARA TENER ACCESO A LA RED INTERNA. FUENTE: (MAIWALD, 2005) 77
ILUSTRACIÓN 19 INTERFAZ UDP FLOOD..... 78

ILUSTRACIÓN 20 SOFTWARE DE ATAQUE UDP FLOODER 79
ILUSTRACIÓN 21 INTERFAZ DIVINE INTERVENTION 80
ILUSTRACIÓN 22 INTERFAZ PLAGUEZ FLOODZ 80
ILUSTRACIÓN 23 TOPOLOGÍA DE RED UCAB 83
ILUSTRACIÓN 24 TOPOLOGÍA DE RED, PROTOCOLO SSH. VPN DE SITIO 84
ILUSTRACIÓN 25 TOPOLOGÍA DE RED, PROTOCOLO IPSEC. VPN PUNTO A PUNTO 84
ILUSTRACIÓN 26 RED DE PRUEBA PPTP 90
ILUSTRACIÓN 27 RED DE PRUEBA, AMBIENTE SSH 91
ILUSTRACIÓN 28 PAQUETE DEL CLIENTE AL SERVIDOR (PIPE VIEWER) 92
ILUSTRACIÓN 29 PAQUETE DE RESPUESTA DEL SERVIDOR AL CLIENTE (PIPE VIEWER) 93
ILUSTRACIÓN 30 PAQUETE UDP (EXTREME UDP FLOODER) 93
ILUSTRACIÓN 31 PAQUETE UDP (UDP FLOODER 2.0) 94
ILUSTRACIÓN 32 PAQUETES FRAGMENTADOS. ATAQUE DE FLOODZ. ... 94
ILUSTRACIÓN 33 PAQUETE DE RESPUESTA 95
ILUSTRACIÓN 34 RED NIDS 96
ILUSTRACIÓN 35 SFTP SIN NINGUNA OTRA HERRAMIENTA ACTIVA 96
ILUSTRACIÓN 36 SFTP Y PERFILADOR ACTIVO 97
ILUSTRACIÓN 37 SFTP CON EL PERFILADOR Y EL SNIFFER EN FUNCIONAMIENTO 97
ILUSTRACIÓN 38 TRES MINUTOS DE ATAQUE 97
ILUSTRACIÓN 39 ONCE MINUTOS DE ATAQUE 98
ILUSTRACIÓN 40 ATAQUE DOS EXITOSO 98
ILUSTRACIÓN 41 99
ILUSTRACIÓN 42 ATAQUE DOS PROLONGADO 99
ILUSTRACIÓN 43 CAPTURA DE EVENTOS WARNING 100
ILUSTRACIÓN 44 NOTICE HTTP HEAD REQUEST 105
ILUSTRACIÓN 45 EVENTOS INFORMATION 109
ILUSTRACIÓN 46 RED DE PRUEBA IPSEC 112

ILUSTRACIÓN 47 ATAQUE A IPSEC 112
ILUSTRACIÓN 48 FLUJO DE DATOS DEL PERFILADOR 114
ILUSTRACIÓN 50 FLUJO DE DATOS DEL CLIENTE AL SERVIDOR..... 115
ILUSTRACIÓN 51 INICIO DE CONEXIÓN VPN, CON PROTOCOLO IPSEC. 116
ILUSTRACIÓN 52 PAQUETES ESP..... 117
ILUSTRACIÓN 53 TRAFICO NORMAL..... 118
ILUSTRACIÓN 54 EVENTOS NIDS CON WIRESHARK..... 118
ILUSTRACIÓN 55 NIDS VPN IPSEC CONEXIÓN..... 119
ILUSTRACIÓN 56 PERFILADOR (VELOCIDAD OPTIMA DEL CANAL)..... 120
ILUSTRACIÓN 57 NIDS ESTADO ANTES DEL ATAQUE 120
ILUSTRACIÓN 58 PROGRAMAS DE ATAQUE DOS 121
ILUSTRACIÓN 59 PERFILADOR (DURANTE EL ATAQUE)..... 122
ILUSTRACIÓN 60 CAPTURA NIDS DURANTE EL ATAQUE A VPN IPSEC 122
ILUSTRACIÓN 61 TRANSCURSO Y FINALIZACIÓN DEL ATAQUE 123
ILUSTRACIÓN 62 EVENTOS DE EXPERIENCIA DE ATAQUE A VPN IPSEC 124

INTRODUCCIÓN

En la actualidad el conjunto de redes de comunicación descentralizadas que representan a la Internet, evolucionan cada día por las diversas aplicaciones que se generan y a las nuevas informaciones manejadas por este medio de comunicación. Permitiendo el manejo versátil de cualquier tipo de información, pudiendo ser de índole educativa, recreativa, informativa y confidencial, como informaciones sobre personas particulares, cuentas bancarias, patentes de proyectos de empresas, entre otras. Sabiendo la creciente complejidad del manejo de redes por la visualización de estas informaciones se entiende la importancia de la seguridad de redes y la aplicación de herramientas de transporte de data que provean alta fidelidad. Partiendo de este punto se resalta la aplicación de herramientas que provean confidencialidad, integridad y seguridad de datos, como son las Redes Privadas Virtuales (VPN), capaces de establecer enlaces de transporte de datos y manejar data de forma remota, mediante túneles seguros que atraviesan la Internet.

La aplicación de esta herramienta que establece un enlace virtual de manejo versátil e implantación económica se a extendió comercialmente en las empresas y en uso personal como herramienta de red que provee acceso remoto desde computadores, Tablet y teléfonos móviles. Estableciéndose como herramienta habitual en cualquier equipo comercial con propiedades de conexión a redes. Por ende se establece la importancia de estudiar la seguridad de esta, a modo de generar luces en el área de seguridad de redes, enfocando el estudio en base a las vulnerabilidades que puede tener esta herramienta y como puede comprometer una red habitual en caso de ser comprometida, comprendiendo que posiblemente sus vulnerabilidades pueden ser muchas o pocas, pero pueden ser propias de una red habitual o aplicaciones futuras similares a esta. De esta forma se establece un estudio de los ataques que puede sufrir una VPN y sus vulnerabilidades propias generadas por su estructura estándar.

Comprendiendo la importancia de una VPN en el área de seguridad de redes se establece este Trabajo Especial de Grado que se compromete a realizar un Estudio del Comportamiento de Vulnerabilidades de una Red Privada Virtual, mediante la aplicación de una metodología que inicia con la investigación de las características, propiedades y elementos de una VPN en su primera fase, con el fin de comprender lo que se está estudiando, para luego realizar en las consecuentes fases del proyecto una investigación teórica de los posibles ataques que pueden comprometer a una VPN y los ataques que históricamente han afectado a esta herramienta, en caso de haber precedentes. Como objetivo principal de esta fase de investigación de ataques se obtuvo los ataques practicos que son aplicables para la realización de experimentos controlados, de esta manera, en las siguientes fases se realiza un estudio de las herramientas recomendadas para realizar el análisis de efectos en la seguridad de redes con conexión VPN, con las que consecuentemente se instalo una red de prueba con diferentes tipos de conexión VPN la cual fue comprometida con los ataques estudiados que pudieron ser aplicados. Teniendo al final de las experiencias resultados arrojados por los Sistemas de Detección de Intrusos IDS, los analizadores de protocolos y los test de velocidad de transporte de data, que fueron analizados y se plantearon soluciones o recomendaciones a cada ataque y vulnerabilidad estudiado que afectan a una VPN.

CAPÍTULO I.

Planteamiento del Proyecto

El presente trabajo especial de grado contiene un proyecto de investigación respecto a las VPN (Virtual Private Network), consiste en probar su seguridad y eficacia con respecto a diferentes ataques informáticos, mediante una investigación teórica de ataques trascendentales y experiencias prácticas de ataque a diferentes protocolos VPN bajo un ambiente controlado. El aporte que se espera dar, a los administradores de red de las empresas, es información con respecto a la contingencia a seguir en caso de que su red sea invadida.

I.1 Planteamiento del Problema

En la actualidad trabajar con VPN's (Virtual Private Network) resulta bastante práctico por proporcionar a las personas la posibilidad de interconectarse a una red distante físicamente, intercambiar información y visualizar las operaciones de un computador remoto, de manera segura mediante túneles que unen redes físicamente separadas convirtiéndolas en un solo dominio de red privada.

La seguridad provista por las VPN se debe a que los paquetes de datos son cifrados y viajan en los túneles que proveen su propia seguridad según el protocolo que se use. Adicionalmente la aplicación de autenticación de usuario les permite verificar la identidad de emisor y receptor. A pesar de estas previsiones de seguridad, una VPN puede ser objetivo de un ataque que perjudique la integridad y la confidencialidad de los datos enviados.

Debido a este problema se propone un estudio de las fallas y tipos de ataques que puede sufrir una VPN, mediante la realización de una investigación teórica de ataques trascendentales y experiencias de ataques reales.

I.2 Objetivos

I.2.1 Objetivo General:

Estudio de comportamientos de las vulnerabilidades de seguridad que puede sufrir una Red Privada Virtual (VPN).

I.2.2 Objetivos específicos:

1.- Investigar las características, propiedades, elementos y funciones, de una Red Privada Virtual y las herramientas para hacer un estudio de vulnerabilidades. Adicionalmente analizar qué tipos de VPN es ventajoso de acuerdo al protocolo para desarrollar un estudio concreto.

2.-Instalar una red real que permita mediante software, hacer notable las vulnerabilidades de seguridad de una VPN.

3.-Implantar una VPN que pueda proporcionar integridad, confidencialidad y seguridad de datos. Además de mecanismos de autentificación y certificación de usuarios. Para proporcionar una VPN con seguridad regular, con el fin de tener un estudio valedero.

4.-Realizar pruebas funcionales sobre cada módulo y analizar los diferentes escenarios de ataques, estudiándolos de forma real.

I.3 Alcance y limitaciones

1.- Como ninguna herramienta es totalmente infalible, se puede decir que algunos ataques estudiados pueden llegar a ser inevitables por consiguiente no se darán soluciones o recomendaciones a todos los ataques estudiados. En la gran mayoría solo se dará recomendaciones.

2.- Este Trabajo Especial de Grado demostrará una prueba de carácter experimental.

3.- Los ataques simulados serán clasificados en niveles según su finalidad y no se realizaran ataques de alto nivel considerando la falta de experiencia en Hacking y que algunas técnicas de ataque no son de acceso público o tienen derechos de autor.

4.- Los ataques en contra de la VPN, se efectuarán en un ambiente de red controlado para algunas experiencias.

5.- Algunos ataques no se estudiarán de forma práctica, por la integridad de los componentes de la red. En este caso se dará un enfoque teórico

6.- Las soluciones dadas, serán de índole teórica no serán probadas en la práctica.

I.4 Justificación

La posibilidad de tener una conexión a una Red Privada Virtual totalmente segura es de gran importancia, para empresas que unen redes de dos o más sucursales o separan una red en dos, para tener una con extra de confidencialidad de datos y también para particulares, que pueden manejar un computador remoto que contenga información importante desde cualquier otro computador. Sabiendo que la información con que se trabaja, es cada vez más delicada y herramientas como VPN son tan versátiles para manejar información de forma económica y práctica, generando enlaces seguros para la transferencia de data y control remoto de informaciones. Se establece la necesidad de estudiar y si es posible plantear soluciones para reforzar la seguridad de esta tecnología, entendiendo que en la actualidad la delincuencia informática es un hecho. La idea de este proyecto es ofrecer luces con el tema de seguridad de las redes. El aporte que se espera obtener del proyecto es información sobre que tan eficaces son las VPN frente a ataques, demostrando de esta manera su eficacia y posiblemente reforzarla en cuanto a seguridad, convirtiéndola en una herramienta más fiable en el área de las telecomunicaciones.

CAPÍTULO II

Marco Referencial

En el presente capitulo, se encuentra el desarrollo del marco teórico del proyecto el cual contiene los antecedentes, además de los conceptos prácticos y teóricos de las VPN, temas imprescindibles para el entendimiento del proyecto.

II.1 Antecedentes

Las VPN se han utilizado siempre para proporcionar conectividad de redes con seguridad, es un elemento fundamental en la seguridad de cualquier red y además se utilizan para interconectar de manera segura dos o más redes LAN separadas físicamente. Esta versátil herramienta ha crecido gradualmente en su uso y en su distribución en el mercado de parte de muchas marcas reconocidas que proporcionan software de calidad. Pero a pesar de ser utilizado a menudo como herramienta de seguridad, separando una misma red con el fin de proporcionar seguridad adicional a una sección de esta, se ha demostrado la existencia de problemas en la seguridad de identidades y en los túneles VPN, por lo que se ha tenido que implantar nuevos protocolos más seguros gradualmente.

II.2 Marco Teórico

II.2.1 Redes

Según Forouzan una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. Los enlaces conectados con los dispositivos se denominan a menudo canales de comunicación. (Forouzan, 2001).

Las redes son de gran importancia en el mundo de las telecomunicaciones, dado que son la infraestructura base sobre la cual se colocan todas las nuevas tecnologías de servicio de comunicación. Los elementos básicos que la componen son *routers*, *switches*, *firewall* y otros dispositivos que como computadores que representan el usuario de la conexión de red.

Un *router* o enrutador de paquetes, es un dispositivo que envía y encamina paquetes de una red a otra, es decir subredes. Proveyendo conectividad de nivel de red, siendo la capa tres del modelo OSI.

Los conmutadores o *switch*, son los encargados de interconectar las redes de computadoras, es decir une dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo a la dirección destino de las tramas en la red. Este dispositivo generalmente se conectan a un firewall, el cual verifica los paquetes entrantes y salientes, para proveer seguridad, mediante el uso de puertas de enlace y un dispositivo que filtra, que en un diseño hardware sería un enrutador.

II.2.1.1 Seguridad de redes

Antes de comenzar a estudiar y entender las VPN es necesario comprender las nociones de la seguridad en redes.

De acuerdo con Brown el término seguridad de redes abarca tantos aspectos de una organización que será más adecuado usar el término seguridad de la información. La seguridad de la información abarca la seguridad de red, la seguridad de las computadoras, la seguridad de acceso y la seguridad física. La tecnología VPN esta implementada en los niveles más bajos de la pila OSI (Físico, Enlace de datos y Red), esto crea un beneficio y un problema potencial. Tener esta tecnología tan abajo como sea posible en la pila ayuda a eliminar muchos de los ataques que podrían suceder si estuviera más arriba, es decir, mientras más bajo se encuentre la VPN en el modelo habrá un menor número de ataque sobre ellas. (Brown, 2000)

Como identificar los ataques

Lo que normalmente sucede con los ataques es que se reciben avisos de que alguien se ha intentado introducir y no tuvo éxito o se introdujo, cuando esto sucede es necesario rastrear la intrusión y ver si los archivos de registro puede identificar de donde vino el intruso, cuales su dirección IP. Esto es monitorear para luego auditar.

El monitoreo es la vista en tiempo real de los paquetes conforme pasan el límite entre la red interna de la empresa y una infraestructura pública. Este monitoreo viene de una política bien establecida que consiste en definir qué tipo de trafico permite entrar, que tipo de tráfico permite salir y que servicios están permitidos. El monitoreo en tiempo real es la única forma efectiva de observar las desviaciones contra la política de seguridad establecida.

II.3 Red Privada Virtual

Según Tanenbaum una *Virtual Private Network* o VPN como se le conoce en inglés, es un término genérico que abarca el uso de redes públicas o privadas para crear grupos de usuarios que estén separados de otros usuarios de la red y que puedan comunicarse entre ellos como si estuviesen en una red privada. (Tanenbaum, 2003).

En el campo de trabajo del área de transmisión de datos, cuando se monta una red para una organización, se puede establecer redes privadas con enlaces exclusivos entre los distintos dispositivos de conexión, pero dado a que es muy costoso establecer enlaces de manera física, se utilizan enlaces que atraviesen la red de internet, pero dado a que este es un ambiente hostil es necesario proteger los datos transmitidos, y una herramienta que da solución a este problema son las VPN, estas ofrecen seguridad a muy bajo costo y enlaces virtuales. Para lograr comprender este concepto de manera gráfica ver la figura 1. Aquí se ilustra una Intranet corporativa, conectada de manera segura a un acceso remoto y a unas sucursales además se puede observar, una VPN articula un túnel virtual, simulando una conexión directa entre las distintas redes, entonces las redes pasan a ser parte de un solo dominio.

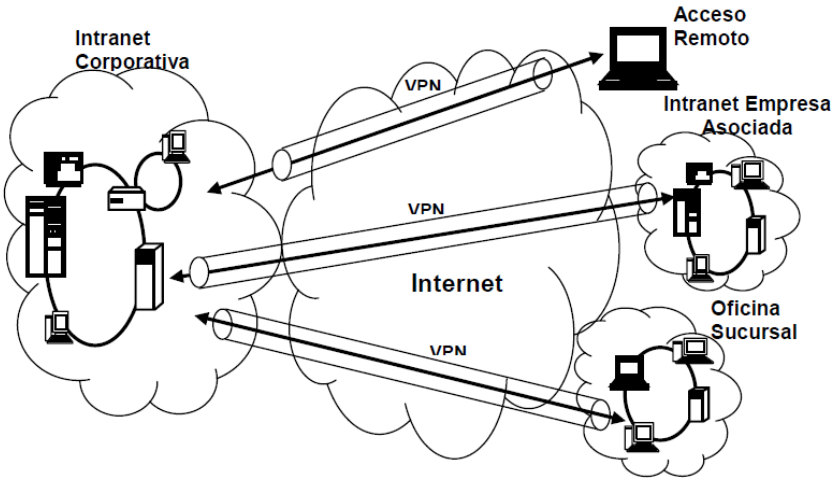


Ilustración 1 Red Privada Virtual Fuente: (Forouzan, 2001)

Los paquetes de datos de una VPN viajan por medio de un túnel definido en la red pública. El túnel es la conexión definida entre dos puntos en modo similar a como lo hacen los circuitos en una topología WAN basada en paquetes. A diferencia de los protocolos orientados a paquetes, capaces d enviar los datos a través de una variedad de rutas antes de alcanzar el destino final, un túnel representa un circuito virtual dedicado entre dos puntos. Para crear el túnel es preciso que un producto

especial que encapsule cada paquete origen en uno nuevo que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel.

Requisitos para la seguridad en las VPN

Según Brown estos requisitos fueron propuestos por el centro de coordinación CERT, este es una organización dedicada a ayudar a las empresas a mantenerse al día con las más recientes violaciones a la seguridad y ofrecer asistencia técnica para las compañías. Las compañías envían reportes sobre incidentes ocurridos y el CERT con esta información ayuda a mejorar las políticas de seguridad de las empresas o compañías. Teniendo lo expuesto anteriormente claro, CERT propuso que los requisitos de la seguridad incluyen el cifrado, los dispositivos que establezcan la VPN, la autenticación, el no repudio, el cifrado punto a punto y la administración centralizada de la seguridad. (Brown, 2000)

- Cifrado: La meta es del cifrado es permitir que sólo la persona a la que se le envía lo convierta en un texto legible.

- Dispositivos que establecen la VPN: Las VPN pueden implementarse en plataformas UNIX y LINUX, enrutadores y switches capa 3. Estos tienen la ventaja de ser muy fáciles de mantener y manejar por un personal bien capacitado en materia de comunicaciones.

- Autenticación: Lo ideal en este requisito, autenticación de usuario, es que los usuarios tengan varias contraseñas distintas para los diferentes servidores, y que estas no deben escribirse y decirse a nadie, ahora el problema radica en que por lo general si escriben las contraseñas y generan contraseñas muy fáciles de recordar y es aquí donde radica el problema de protección con contraseñas. De hecho uno de los ataques más exitosos son los “ataque de diccionario”, un simple ataque de conjetura.

- No repudio: CERT propone que debe existir alguna manera de en que una parte esté completamente segura de quela otra parte ya envió el mensaje.

- Cifrado punto a punto: Los túneles cifrados aseguran la integridad de los datos conforme pasan por una red pública. Por lo general se utilizan dos términos cifrado y encapsulamiento (estudiados más adelante). Por ahora lo que hay que entender es que el cifrado solo codifica los datos y el encapsulamiento de datos hace un paquete de datos del paquete original, lo envuelve en su propio paquete y después lo codifica. Dependiendo de la tecnología que se emplee, los datos pueden permanecer cifrados hasta su destino final. También una vez que el paquete este en el interior de la red, se puede descifrar y almacenar en un servidor.

- Administración de seguridad centralizada: Si existen distintas aplicaciones en un modelo cliente/servidor, corriendo en varios servidores que soportan distintos clientes en redes diferentes, sería muy engorroso manejar este tipo de topología. En este caso si una aplicación de seguridad se actualiza o se modifica puede afectar a toda la red y puede pasar mucho tiempo antes de que todo el personal que maneje la red pueda darse cuenta.

II.3.1 Tipos de VPN

Los tipos de VPN se estructuran y diferencian según las necesidades de los usuarios y organizaciones. De igual forma en la capa de aplicación estas son construidas para aceptar protocolos diferentes, como se observa en la ilustración 2.

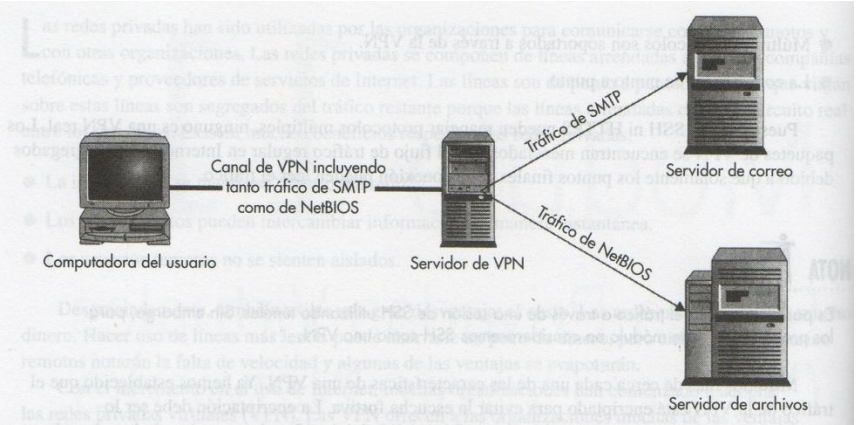


Ilustración 2 Protocolos múltiples de manejo de VPN. Fuente: (Maiwald, 2005)

Las VPN generalmente se encuentran separadas en dos tipos: VPN de usuario y VPN de sitio. La diferencia entre ellas es la manera en que los dos tipos son utilizados, y no debido a la manera en que el tráfico es segregado para cada tipo. Se analizará cada tipo de VPN con detalle.

II.3.1.1 VPN de Usuario

Las VPN de usuario o de acceso remoto, son redes privadas virtuales entre la máquina de un usuario individual y la red de un sitio de una organización. El servidor VPN puede ser el firewall de la organización o puede ser un servidor VPN por separado. El sitio de la organización solicita autenticación del usuario y permite acceso a la red interna de la organización como si dicho usuario estuviera físicamente en la red, pero la velocidad de la red será más lenta debido al factor limitante de la conexión a internet.

Aunque el usuario tiene una VPN hacia la red interna de la organización, también tiene una conexión a internet y puede navegar en la web como un usuario normal. La VPN es manejada mediante una aplicación en la computadora del usuario. Ver la ilustración 3.

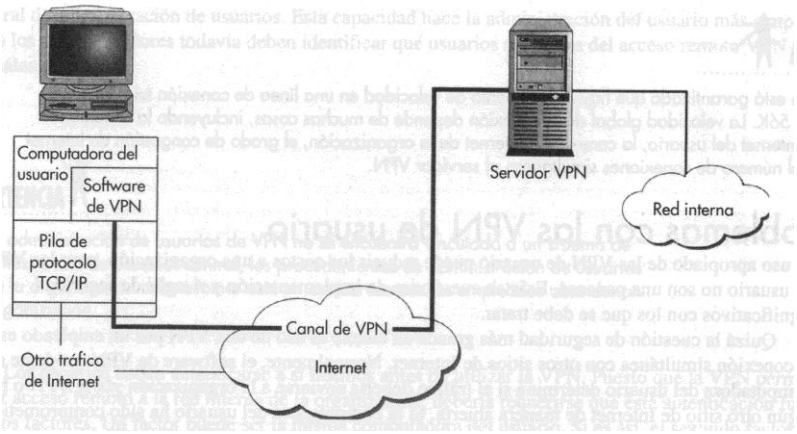


Ilustración 3 Configuración VPN de usuario. Fuente: (Maiwald, 2005)

II.3.3.2 VPN de Sitio

Conocidas en el mercado como de punto a punto, este tipo de VPN son empleadas por las organizaciones para conectar redes de sucursales separadas físicamente, sin necesidad de costosas líneas arrendadas. Generalmente, la VPN conecta un firewall o un enrutador limítrofe con otro muro de fuego o enrutador limítrofe, como se observa en la ilustración 4. Para iniciar la conexión, un sitio intenta enviar tráfico hacia el otro. Los dos extremos negociarán los parámetros de la conexión dependiendo de las políticas de los dos sitios. Los dos sitios se autenticaran entre si utilizando algún secreto compartido que haya sido configurado previamente, o bien mediante un certificado de clave pública.

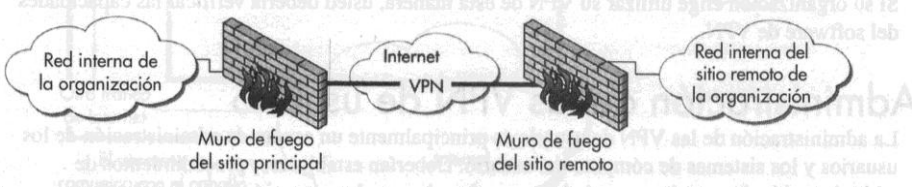


Ilustración 4 VPN sitio a sitio de internet. Fuente: (Maiwald, 2005)

II.3.2 VPN a través de LAN

Esta no utiliza Internet como vínculo, si no la misma red de área local (LAN) en donde se emplea. Su finalidad va hacia aislar zonas y servicios de la misma red

interna de una organización, con el fin de aplicar una mejor seguridad al separar los servicios privados de una sucursal de los de acceso público.

II.3.3 Características de una VPN

Al conectar dos o más sucursales de una empresa usando internet, o al acceder a un equipo remoto es necesario hacerlo de una manera segura y con enlaces virtuales para minimizar los costos, de allí la necesidad de las VPN. Para conseguir esto es necesario que el medio de trasmisión garantice autentificación, integridad y confidencialidad de toda la comunicación.

- Autentificación y autorización: Emisor y receptor son capaces de determinar de forma inequívoca sus identidades, de tal manera que no exista duda sobre las mismas. Esto puede conseguirse mediante firmas digitales o aplicando mecanismos desafío-respuesta.

- Integridad: Es la garantía de los datos enviados no han sido alterados es decir, los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Para esto se pueden utilizar firmas digitales.

- Confidencialidad: Es la manera de conseguir la privacidad de los datos, de modo que no pueda ser interceptada y leída, en los túneles creados por la VPN en la red de internet. La manera de conseguir esto es mediante la encriptación.

II.3.4 Propiedades de una VPN

Según Maiwald las propiedades de una VPN se dividen en encapsulación, autenticación y cifrado de datos.

- Encapsulación: Las VPN encapsulan datos privados con un encabezado que les permite atravesar la red pública.

- Autentificación: Con esta propiedad el servidor VPN autentifica el cliente VPN que desea conectarse y al mismo tiempo verifica que tenga los permisos adecuados debido a que la autentificación entre ellos es mutua. La autenticación en una red privada virtual consiste en la autenticación de datos y usuarios.

- Cifrado de datos: Esta propiedad permite convertir algún texto legible en un texto ilegible, logrando de esta manera que solo la persona a la que se le envía lo convierta en un texto legible (Maiwald, 2005).

II.3.5 Componentes de un VPN

Las VPN consisten en hardware y software además de otro conjunto de componentes. Según Brown estos componentes son simples requisitos que garantizan que la VPN sea segura, este disponible y sea fácil de mantener. Son los siguientes:

- Disponibilidad: Esta se aplica tanto al tiempo de actualización como al de acceso. A parte de tener acceso a los servicios que maneja la VPN también es necesario tener acceso a la red.

- Control: Es ventajoso que el control de la VPN lo tenga los servicios administradores que proveen el servicio debido a que ellos tienen capacitación, experiencia, supervisión meticulosa y funciones de alerta.

- Seguridad: La seguridad lo es todo en una RPV, nunca será suficiente hacer hincapié en este componente. La seguridad de una VPN abarca desde el proceso de cifrado que se implementan, los servicios de autenticación, las firmas digitales y las autoridades emisoras de

certificados que utiliza. También abarca el software que implementa los algoritmos de cifrado en la VPN.

- Autenticación de datos y usuarios: La autenticación de datos reafirma que el mensaje que ha sido enviado completamente y que no ha sido alterado de ninguna manera. La autenticación de usuarios es un proceso que permite que el usuario tenga acceso a la red.

- Sobrecarga de tráfico: En cualquier tipo de tecnologías existen tráficos velocidad contra desempeño, seguridad contra flexibilidad. Las VPN caen en la misma característica. Si una VPN cifra cada paquete que sale de los adaptadores de red, entonces el procesamiento de las máquinas debe ser alto. Si la VPN encapsula cada paquete, puede incrementar el tamaño del paquete y por lo tanto afectar la utilización del ancho de banda. IPsec añade una sobrecarga a cada paquete en busca de más seguridad. Ahora experimentará cuellos de botella en los enlaces, para evitar esto se debe decidir qué tipo de tráfico proteger. Las transmisiones generales, las transmisiones múltiples y el tráfico similar no necesita cifrarse pero necesitan autenticarse. Las VPN pueden agregar autenticaciones a estos paquetes (autenticación de paquetes) sin la sobre carga asociada al incremento del tamaño del paquete y el receptor puede estar seguro de que los datos no fueron modificados.

- Mantenimiento: La actualización en la seguridad debe ser tan primordial como es la revisión del software en busca de virus. El mantenimiento lo pueden hacer un proveedor de este servicio o personalmente.

- Sin repudio: Es el proceso de identificar positivamente al emisor de tal manera que no pueda negarlo. (Brown, 2000)

II.3.6 Beneficios de una VPN

Entre las utilidades potenciales en la implementación de la tecnología VPN podemos señalar:

- Seguridad: Una VPN tiene una alta seguridad. Una VPN requiere el estableciendo de un túnel en la red corporativa y la encriptación de los datos entre la PC del usuario y los servidores corporativos. Utilizan protocolos estándar de autenticación y encriptación que permiten ocultar los datos en entornos inseguros de internet, pero que son accesibles a los usuarios corporativos mediante una VPN. (Ñacato Gualotuña, 2007)

- Transparencia: El usuario de la VPN tiene total control del proceso de transferencia de la información, una vez que este ha sido autenticado por el servidor VPN.

- Flexibilidad: Una VPN ofrece una variedad de métodos de acceso mucho mayor que la de una red WAN convencional. Cada empresa dispone de un abanico de opciones de ancho de banda.

- Facilidad de instalación y uso: Este servicio usa software estándar de cliente, lo cual el sistema sea amigable y de fácil uso.

- Ahorro en los costos: Un VPN no necesita de enlaces dedicados, puesto que utiliza los recursos ya existentes en la red mundial, internet, para establecer canales virtuales y temporales conocidos como túneles.

Dentro de los beneficios que tienen las VPN hay que tomar en cuenta cuando es benéfica para una organización en aras de satisfacer las necesidades en ciertas áreas y aplicaciones como las siguientes:

1) Acceso remoto de usuarios

2) Sitios internacionales
3) Base de usuarios geográficamente diversa
4) Expansión barata del mercado
5) Requisitos razonables de ancho de banda
6) Necesidad de un enlace global de bajo costo
7) Acceso a servicios externos

También existen algunas áreas donde las VPN pueden no ser recomendables:

1) Donde el desempeño es apremiante
2) Donde el estado latente es inaceptable

II.3.7 Elementos de una VPN

Existen 4 componentes clave de una VPN:

- El servidor VPN
- Los algoritmos de encriptación
- El sistema de autenticación o validación
- El protocolo VPN

Según Maiwald con estos 4 componentes se satisfacen los requerimientos de seguridad, rendimiento e interoperabilidad de la VPN (Maiwald, 2005).

- Servidor VPN

Este sistema de cómputo actúa como extremo para la VPN. Este debe ser adaptado para procesar la carga esperada. La DMZ de VPN debería estar protegida por el conjunto de reglas del firewall y solamente permitir el tráfico que sea requerido por la VPN. Una DMZ (Demilitarized Zone) es referida a una parte de una red que no es de confianza, la DMZ proporciona un lugar en la red para dividir sistemas a los que tiene acceso personas en internet de aquellos a los que solamente tienen acceso los empleados.

El servidor VPN también debe ser colocado en la red; el servidor puede ser el firewall o un enrutador limítrofe, ver la ilustración 5. Que haga fácil la colocación del servidor VPN.

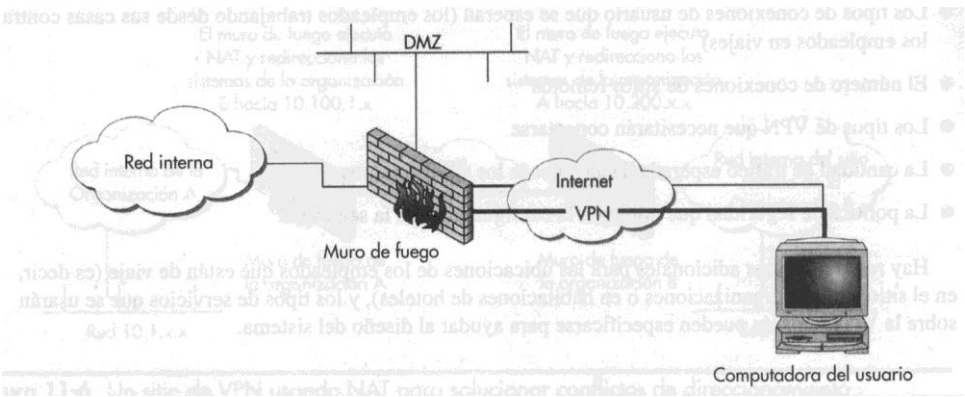


Ilustración 5 Arquitectura de red VPN apropiada cuando el muro de fuego es el servidor VPN.

Cuando el servidor es un sistema autónomo, ver ilustración 6. Idealmente, la DMZ de VPN solamente sostendrá el servidor de VPN y estará separada de la red DMZ de internet. En este caso el servidor VPN permite el acceso a sistemas internos por parte de los usuarios autorizados.

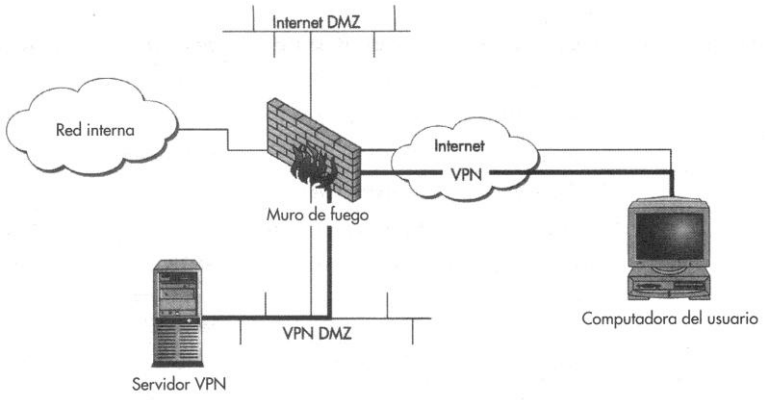


Ilustración 6 Arquitectura de red VPN apropiada para un servidor VPN único. Fuente: (Maiwald, 2005)

- Algoritmos de encriptación

El algoritmo de encriptación utilizado en la VPN debe ser robusto y bien conocido. Idealmente todos los algoritmos robustos y bien conocidos pueden utilizarse de una manera eficiente en una VPN.

- Sistema de autenticación

Esta característica se refiere a que el sitio remoto debe ser autenticado. Esto puede requerir que algunos usuarios sean autenticados o validados ante un servidor central, o puede requerir que ambos extremos de la VPN se autentiquen entre si. Para una validación mutua, se requiere que ambos sitios demuestren el conocimiento de un secreto compartido que se haya configurado anteriormente.

- Protocolo de VPN

El protocolo determina como un sistema VPN interactuará con otros sistema en Internet y también cómo será resguardado el tráfico. El protocolo VPN es una parte que tendrá efecto global sobre la seguridad global del sistema, debido a que el protocolo será utilizado para intercambiar claves de encriptación entre los dos extremos (Maiwald, 2005).

II.3.8 Funcionamiento de las VPN

Primeramente el usuario del cliente VPN se pone en contacto con un servidor VPN designado como propiedad de la empresa u organización a través de internet e inicia el proceso de autentificación. Seguidamente el usuario ingresa el ID y el *password* es autenticado y se proporcionan los datos de seguridad.

El servidor VPN proporciona una nueva dirección del protocolo internet IP al equipo cliente, al que se ordena enviar el tráfico de red adicional con esa dirección a través del servidor VPN. Todos los paquetes de red son encriptados completamente mientras se intercambian.

II.3.9 Sistemas VPN

En este punto se comentará acerca de la implementación real de una VPN dentro de una LAN. Según Maiwald cada administrador de red debe discutir el tipo de sistema es mejor de acuerdo a sus necesidades. Existen tres tipos principales de sistema de VPN:

- Sistemas de hardware

Estos sistemas incluyen un dispositivo de hardware para ser utilizado como el servidor VPN. Este dispositivo ejecuta el software del fabricante y por lo general se requiere que dicho software se instale en el sistema de usuario remoto para implementar la VPN. Los beneficios de un sistema VPN de hardware son velocidad y seguridad. En cuanto a la velocidad, esta ventaja se debe a que el hardware esta optimizado para soportar la VPN, a diferencia de un hardware que maneje propósitos generales. Esto trae como consecuencia que se puedan manejar un mayor número de conexiones VPN simultáneas. Por otra parte en referencia a la seguridad, es ofrecida debido a que todos los procesos y software ajenos son removidos del sistema, esto se traduce en una mayor seguridad al sistema

- Sistemas de software

Estas son caracterizadas por el hecho de que son cargadas en un sistema de cómputo de uso general. Pueden ser instaladas en un sistema dedicado a la VPN o pueden ser instaladas en conjunto con algún otro software como lo puede ser un firewall.

- Sistemas basado en web

El usuario utiliza una navegador web para conectarse a la VPN mediante el protocolo SSL. SSL se encarga de la encriptación del tráfico y la autenticación podría estar incrustada en el sistema para validar el usuario (Maiwald, 2005).

II.4 Túneles

El túnel es un camino lógico a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando una trama encapsulada llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red.

II.4.1 Tipos de túneles

- Túneles voluntarios: Un túnel voluntario ocurre cuando una estación de trabajo o un servidor de enrutamiento utiliza el software del cliente del túnel para crear una conexión virtual al servidor del túnel objetivo. Para lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente. Los túneles voluntarios requieren una conexión IP.

- Túneles obligatorios: Varios proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora o el dispositivo de red proporciona el túnel para la computadora del cliente es conocida de varias maneras: Procesador frontal (FEP) en PPTP, un concentrador de acceso a L2TP (LAC) en L2TP o un Gateway de seguridad IP en el IPSec.

II.4.2 Tunneling

El proceso conocido como *Tunneling* es la técnica utilizada para generar una infraestructura entre redes que permita transferir datos de una red a otra, transfiriendo la carga como tramas de otro protocolo. Los protocolos *tunneling* encapsulan las tramas con una cabecera adicional que proporciona información de *routing* para hacerla capaz de atravesar la red intermedia, de modo que las tramas son encapsuladas y enrutadas a través de un camino lógico o túnel, donde los paquetes encapsulados viajan de un punto a otro de la red intermedia. Cuando una trama encapsulada llega a su destino dentro de la red intermedia, se desencapsula y se envía

a su destino final dentro de la red. En definitiva el proceso de *Tunneling* abarca los procesos de encapsulado, desencapsulado y la transmisión de las tramas.

Tecnologías de *Tunneling* usadas regularmente:

1) DLSW – Data Link Switching (SNA over IP)
2) IPX for Novell Netware over IP
3) GRE – Generic Routing Encapsulation (RFC 1701/2)
4) ATMP – Ascend Tunnel Management Protocol
5) Mobile IP – For Mobile Users
6) IPSec – Internet Protocol Security Tunnel Mode
7) PPTP – Point to Point Tunneling Protocol
8) L2F Layer 2 Forwarding
9) L2TP – Layer 2 Tunneling Protocol

II.5 Protocolos de VPN y Propiedades de estos

II.5.1 PPP (Point to Point Protocol)

Según el RFC 1661 cuando se realiza una conexión por linea alquilada entre routers se requiere un protocolo punto a punto, que maneje la capa de enlace de datos y sus funciones. Este protocolo tiene como función la de proporcionar un método estandarizado para el transporte de paquetes Multiprotocolo. Este transporte se realiza entre dos pares que están a ambos extremos de la conexión. Los mismos nos proveen de operación bidireccional y full-duplex, asumiendo que los paquetes serán entregados en orden. (RFC1661, 1994)

Según Brown el protocolo PPP tiene tres componentes básicos.

1. Un mecanismo para encapsular paquetes multiprotocolo y manejar la detección de errores.

2. Un protocolo de control de enlace Link Control Protocol (LCP), el cual se usa para configurar automáticamente diferentes opciones de formatos de encapsulación, límites de manipulación de tamaño de paquetes, detección de enlaces con ciclos, errores por mala configuración y la terminación de enlace. Además provee adicionalmente la autentificación de la identidad de los pares del enlace.

3. Una familia de protocolos de control de red *Network Control Protocols* (NCP) para establecer y configurar los distintos protocolos de nivel de red.

La comunicación de datos PPP es la comunicación inicial que necesita el equipo para conectarse al PSI. El cliente remoto habilitado para PPTP se conecta al PSI utilizando datagramas PPTP cifrados y autentica al usuario. (Brown, 2000)

II.5.2 PPTP (Point to Point Tunneling Protocol)

El RFC 1701 establece que la función de este protocolo es crear un túnel dentro de una red IP pública o privada, utilizando el protocolo *Generic Routing Encapsulation* (GRE), mecanismo que proporciona el flujo controlado de los paquetes o datagramas de servicio, para aplicar encapsulación y transporte de los paquetes PPP. (RFC1701, 1994)|

De esta manera el protocolo PPTP encapsula tramas PPP en datagramas IP para su transmisión sobre una red. Permitiendo la creación de un vínculo virtual de comunicación entre dos equipos a través de cualquier red IP, función no posible solo con el Protocolo Punto a Punto PPP.

Según Brown el protocolo punto a punto PPTP se diseñó para permitir que los usuarios remotos marcaran a su proveedor de internet local y establecieran un túnel al servidor de la compañía. PPTP utiliza la infraestructura de protocolos existente para permitir una conexión por marcación, llamada PPP. Luego toma estos paquetes PPP y los encapsula dentro de un encabezado con encapsulamiento para

enrutamiento genérico. PPTP utiliza algoritmos de cifrado tales como PAP y CHAP para proporcionar el cifrado, además del cifrado punto a punto de Microsoft (MPPE). PPTP viene en dos configuraciones Modo Obligatorio y Modo Voluntario. En modo obligatorio utiliza los servicios de un PSI (Proveedor de Servicio de Internet) junto con un procesador frontal PPTP, no se necesita ningún software específico en el cliente. El protocolo PPP maneja cualquier problema de comunicación en una conexión por marcación al PSI, por ende cualquier problema en el equipo puede deberse a la configuración de marcación a la red. El modo obligatorio se crea sin el conocimiento del usuario y también restringen el acceso de los usuarios a otras partes de internet.

Por otra parte en el modo voluntario los clientes establecen una conexión PPTP directa con el servidor PPTP en el otro extremo de la red para crear un túnel, en este caso el PSI no está involucrado. (Brown, 2000)

Ahora bien para el establecimiento de túneles PPTP de datos, el protocolo en cuestión forma los paquetes PPP que tienen paquetes PPTP cifrados y los envía al servidor PPTP. Entonces, dicho servidor descifra estos paquetes y los envía a los paquetes respectivos. Las comunicaciones PPTP dependen del tipo de modo que se emplee, ya sea voluntario u obligatorio. En el modo obligatorio el (FEP) procesador frontal del PSI maneja las comunicaciones PPTP por otra parte en el caso de modo voluntario, el mismo equipo maneja los mensajes de control. PPTP maneja los siguientes pasos típicos para manejar las comunicaciones:

1) El equipo crea una cuenta PPP de marcación a un PSI
2) El FEP podría enviarle una señal al servidor PPTP con una *PPTP_Start_Session_Request*, y el servidor podría responder con una *PPTP_Start_Session_Reply*
3) El FEP hace una solicitud al servidor PPTP
4) El servidor envía la respuesta al FEP

5) Comienza la comunicación de datos
6) Finalmente, se envía un *PPTP_Stop_Session_Request* y se recibe un *PPTP_Stop_Session_Reply*.

En la ilustración 7 se puede observar de manera simplificada el esquema de trabajo de PPTP, se puede ver el servidor PPTP y los clientes

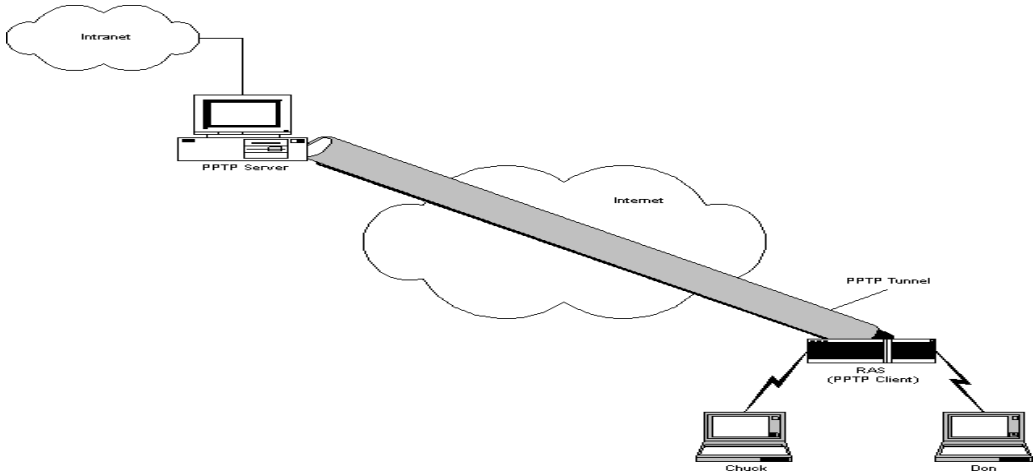


Ilustración 7 PPTP. Fuente: (microsoft, 2012)

En resumidas cuentas el protocolo punto a punto se utiliza para asegurar las conexiones PPP a través de TCP/IP, esto se logra estableciendo una conexión VPN del cliente al servidor. PPTP encapsula los paquetes PPP, los cuales a su vez son encapsulados en paquetes de Encapsulamiento de enrutamiento genérico (GRE). PPTP crea una instalación de conexión y controla el canal al servidor PPTP sobre el puerto 1723.

II.5.3 L2TP (Layer 2 Tunneling Protocol)

Este protocolo es considerado la evolución del protocolo PPTP, porque provee la creación de múltiples túneles en redes IP, teniendo cado uno su propio Contrato de Calidad de Servicio. Basandose en las especificaciones de reenvío de capa 2 Layer Two Forwarding (L2F) y del protocolo punto a punto PPTP, encapsula las tramas

PPP que encapsulan a su vez los protocolos IP, permitiendo a los usuarios ejecutar aplicaciones de forma remota aunque dependan de protocolos específicos.

Se puede entender L2TP como una combinación de L2F y PPTP, L2TP se apoya en PPP para establecer una conexión por marcación,pero a diferencia de PPTP, define su propio protocolo para establecer túneles. Utiliza PPP (PAP y CHAP) para autenticar usuarios, y dado que es un protocolo de nivel 2 del modelo OSI permite el transporte sobre protocolos que no son IP.

La configuración de una VPN con L2TP es muy parecida que en PPTP es decir el paquete de datos incluye la comunicación PPP inicial y PPP puede utilizarse para paquetes cifrados. L2TP es independiente del medio, L2TP define los siguientes tipo de mensajes para el establecimiento de la comunicación:

1) Start-Control-Connection-Request (Inicia la sesión)
2) Start-Control-Connection-Reply (Responde la solicitud)
3) Start-Control-Connection-Connected (Responde la réplica, termina el reconocimiento en el establecimiento del túnel)
4) Start-Control-Connection-Notification (Cierra la conexión de control)
5) Hello tunnel (Esta activo)

L2TP maneja dos tipos de mensajes de control y de datos, el primero se encarga la configuración, la terminación, la administración de la sesión y el estado del túnel y también se emplean para mantener las características dentro del túnel. Por otra parte los mensajes de datos son paquetes PPP sin la información de tramas. L2TP utiliza los mismos modos que PPTP (Voluntario y obligatorio) y tiene su propia lista de control como la definida anteriormente, además L2TP utiliza una terminología especial para definir los puntos donde se inicia y termina la comunicación. Un concentrador de acceso (LAC) L2TP se comunica con un servidor de red (LNS) L2TP para controlar las conexiones. (Brown, 2000). En la ilustración 8 se puede apreciar una VPN con L2TP con los componentes explicados anteriormente.

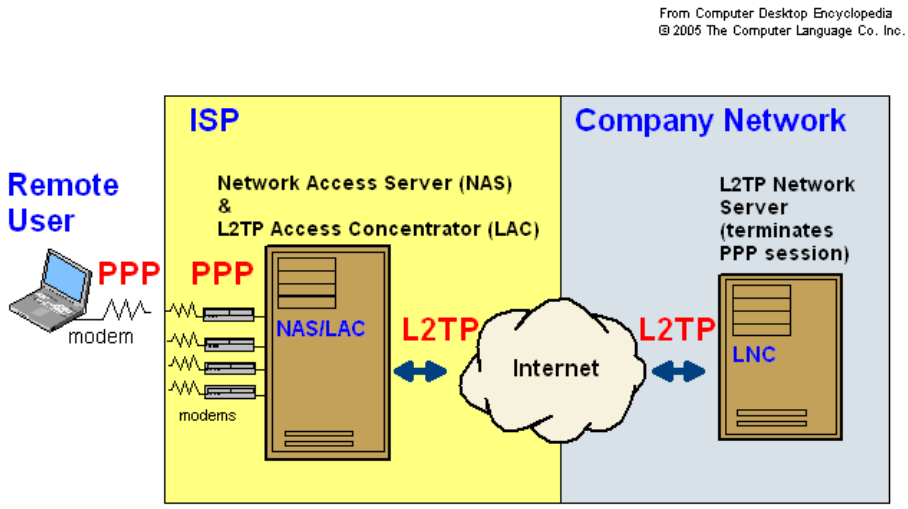


Ilustración 8 Esquema L2TP. Fuente: (farlex, 2012)

II.5.4 IPSec (Internet Protocol Security)

De acuerdo la página de Microsoft®, IPSec se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una dirección IP de origen hasta una dirección IP de destino. La dirección IP en sí no se considera necesariamente una identidad, sino que el sistema que hay tras la dirección IP tiene una identidad que se valida a través de un proceso de autenticación. Los únicos equipos que deben conocer que el tráfico está protegido son los equipos remitente y receptor. Cada equipo trata la seguridad en su extremo respectivo y supone que el medio a través del cual tiene lugar la comunicación no es seguro. Los equipos que se limitan a enrutar datos desde el origen hasta el destino no necesitan ser compatibles con IPSec, salvo en el caso de que se filtren paquetes de tipo servidor de seguridad o se traduzcan direcciones de red entre los dos equipos. (Microsoft, 2003)

IPSec establece que antes de que ocurra cualquier comunicación, se negociará una Asociación de Seguridad (SA) entre los dos nodos o compuertas de la VPN. La SA establece toda la información necesaria para asegurar las comunicaciones

entre los dos host, es decir maneja aspectos como el trasporte y los servicios a nivel de aplicación, autenticación y carga cifrada. La SA especifica el cifrado de punto terminal y los protocolos de autenticación, como por ejemplo DES para cifrado y MD5 para autenticación asimismo determina las claves utilizadas en estos algoritmos y otros tipos de datos.

La SA específica se identifica por un número de 32 bits llamado índice de parámetros de seguridad (SPI). IPSec se subdivide posteriormente en dos tipos de transformaciones de datos para la seguridad de los paquetes IP: el encabezado de autenticación (AH) y la carga de seguridad encapsulada (ESP). AH proporciona autenticación en el encabezado IP, AH puede utilizarse en los modos de túnel y transporte. En el modo transporte se inserta después del encabezado IP original y protege a los protocolos de nivel superior. En el modo túnel, se inserte antes del encabezado original y se introduce un nuevo encabezado IP. AH proporciona autenticación de datos al calcular un valor de verificación de integridad.

Por otra parte el ESP proporciona confianza, autenticación, integridad sin conexión y servicios contra repeticiones, este conjunto de servicios en ESP se instala durante el establecimiento de la asociación de seguridad. ESP al igual que AH puede emplearse en dos modos de transporte o túnel. (Brown, 2000)

De acuerdo con Iglesias, IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros). La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual. (Iglesias, 2001)

Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogénea para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la

versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6. Una característica destacable de IPSec es su carácter de estándar abierto.

Entre los beneficios que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.

- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación.

- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.

- Ofrece al tele trabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

Iglesias en una descripción del IPSec establece que es un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), además de tecnologías de clave pública (RSA), algoritmos de *hash* (MD5, SHA-1) y certificados digitales. No obstante se ha definido ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, igual que MD5 y SHA-1, para funciones de *hash*. Es posible usar otros algoritmos que se consideren mejor adaptados a las

necesidades que se tengan en un ambiente de red especifico, como por ejemplo un algoritmo de cifrado de calve simétrica IDEA, Blowfish y AES (Iglesias, 2001).

Siguiendo con la descripción, dentro de IPSec se distinguen dos componentes:

- Dos protocolos de seguridad: *IP Authentication Header* (AH) e *IP Encapsulating Security Payload* (ESP) que proporcionan mecanismos de seguridad para proteger tráfico IP.

- Un protocolo de gestión de claves *Internet Key Exchange* (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

II.5.4.1 Protocolo AH

El protocolo AH, según Iglesias, es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar y los datos transportados. Ver la ilustración 9.

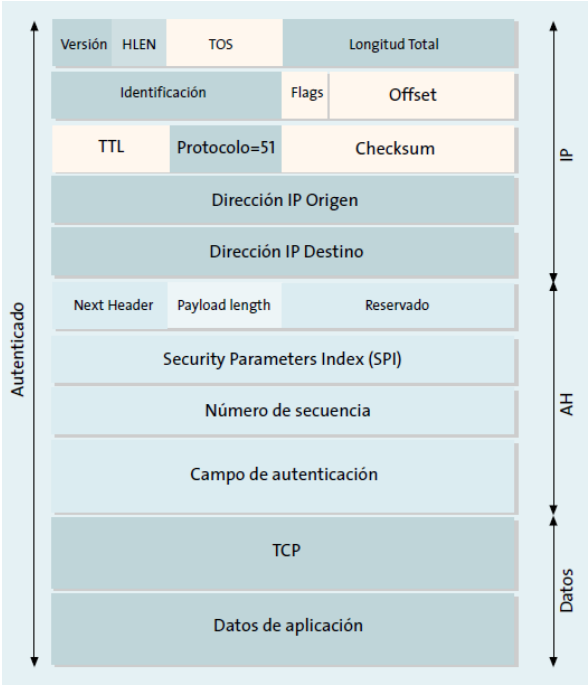


Ilustración 9 Estructura de un datagrama AH. Fuente: (Iglesias, 2001)

La IANA le asignó el número de protocolo el decimal 51, esto quiere decir que el campo Protocolo de la cabecera IP tiene el valor de 51, en lugar de 6 ó 17 asociados TCP y UDP respectivamente, esto se puede observar en la figura. (Numbers, 2013).

De acuerdo con Krawczyk es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables TOS, TTL, *flags, offset y checksum*. El funcionamiento de AH se basa en un algoritmo código se autenticación de mensajes HMAC (*Keyed-Hashing for Message Authentication*). Dicho algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que se denomina extracto, este tiene la propiedad de que funciona como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que esta es la única que conoce la clave.

En la ilustración 10 se muestra el modo en que funciona AH. El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete. Hecho esto si son iguales, el receptor puede tener la certeza de que el paquete IP no fue modificado y que procede del origen esperado. (H. KRAWCZYK, 1997)

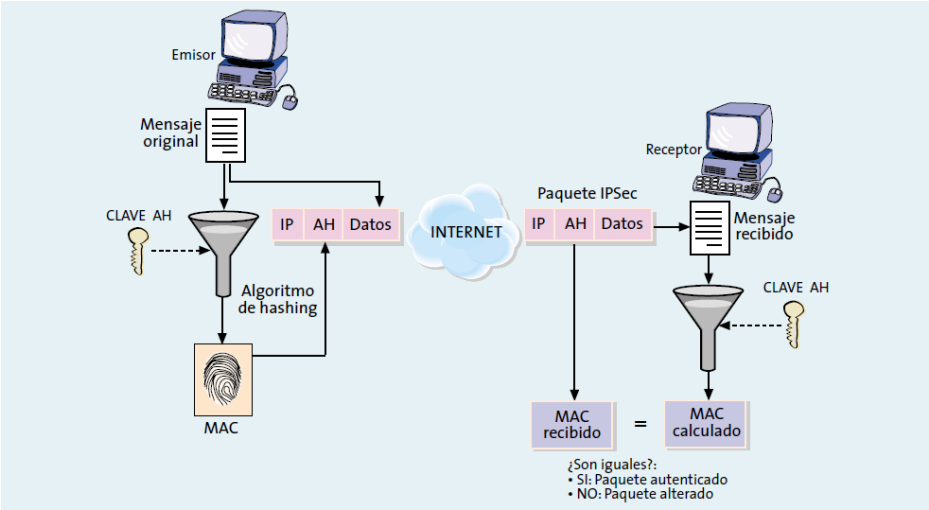


Ilustración 10 Funcionamiento del protocolo AH. Fuente: (Iglesias, 2001)

Si se analiza con detalle el protocolo AH, se puede concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave y que dicha clave sólo la debe conocer el emisor y el receptor, observar la ilustración 8 se observa que los datos junto con la clave se les realiza la función hash.

II.5.4.2 Protocolo ESP

Según Atkinson el objetivo principal del protocolo ESP (*Encapsulating Security Payload*) es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH. (ATKINSON, 1998).

La cabecera de ESP es más compleja que la de AH, este consta de una cabecera y una cola que idean los datos transportados. Dichos datos pueden ser cualquier protocolo IP. En la ilustración 9 se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrada.

Describiendo el protocolo ESP, la carga útil y el campo protocolo está cifrado, entonces en caso de darse un ataque el agresor que intercepta el paquete no podrá saber si el contenido es TCP o UDP; con esto se logra ocultar información. Pasando a otro punto la función de cifrado en este protocolo es dado por un algoritmo de clave simétrica. Normalmente su usan algoritmos de cifrado de bloque, de modo que la longitud de los datos a cifrar tiene que ser múltiplo del tamaño del bloque (8 ó 16 Bytes). Por esta razón existe un campo de relleno que tiene una función adicional que permite añadir caracteres de relleno al campo de datos para ocultar así la longitud real y así también las características del tráfico ver la ilustración 11.

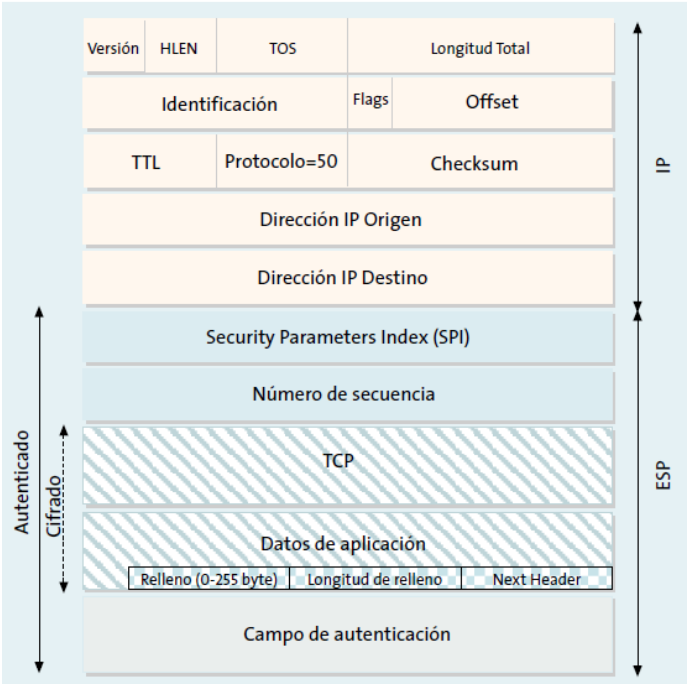


Ilustración 11 Estructura de un datagrama ESP. Fuente: (Iglesias, 2001)

La IANA (*Internet Assigned Numbers Authority*) ha asignado al protocolo ESP el número decimal 50. Esto implica que el campo protocolo de la cabecera IP tendrá el valor 50, mientras que dentro del mensaje ESP e indica la naturaleza de los datos. (Numbers, 2013).

De acuerdo con Iglesias un atacante puede deducir cierta información a partir del análisis de ciertos parámetros de la comunicaciones, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar estos ataques (Iglesias, 2001).

En la ilustración 12 se presenta como el protocolo ESP permite enviar datos de forma confidencial. Y funciona de la manera siguiente el emisor toma el mensaje original lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

Para Iglesias está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor (Iglesias, 2001).

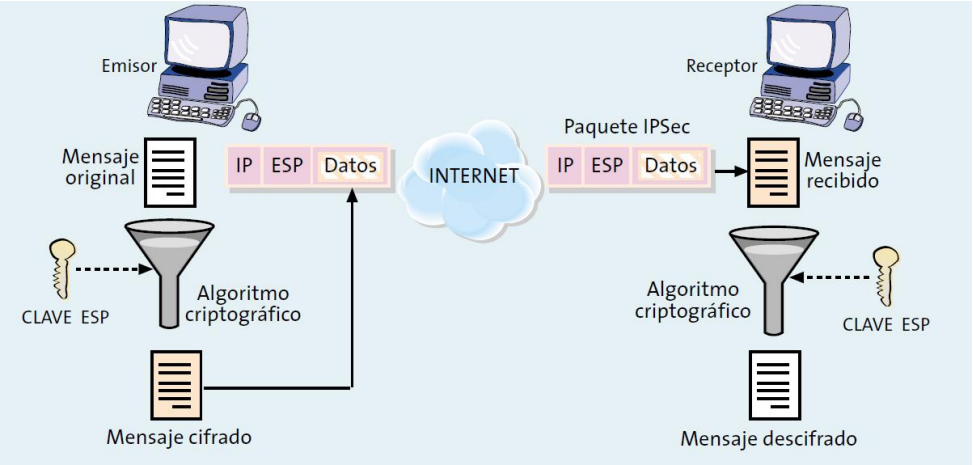


Ilustración 12 Funcionamiento del protocolo ESP

Llegado a este punto, se concluye que la distribución de claves de forma segura es un requisito esencial para el funcionamiento de ESP y también de AH. ES fundamental que tanto el emisor y el receptor estén de acuerdo tanto del algoritmo de cifrado o de *hash* como el resto de otros parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control llamado IKE (*Internet Key Exchange*).

Antes de explicar el protocolo IKE es necesario explicar los dos modos de funcionamiento de IPSec. Según Iglesias tanto ESP como AH proporcionan dos métodos de uso:

- Modo transporte: Este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

- Modo túnel: En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones (Iglesias, 2001).

El modo túnel es empleado normalmente cuando se utiliza ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto en ESP como en AH, es poder establecer VPN a través de redes públicas. IPSec puede ser implementado bien en un host o bien en un equipo dedicado, tal como como un *router* o un *firewall* que cuando realiza estas funciones se denomina *Gateway* IPSec. En la ilustración 13 se puede observar los dos modos de funcionamiento, en la parte de arriba se tiene dos *hosts* que entienden IPSec y que se comunican de forma segura. Esta comunicación es realizada en modo transporte, por tanto la información que se protege es únicamente la del protocolo TCP o UDP, así como los datos de la aplicación. En la parte de abajo se muestran dos redes que utilizan para conectarse dos *gateways* IPSec y, por tanto, emplean una implementación en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los *gateways* IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales. Sin embargo ambos PCs envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración. (Iglesias, 2001)

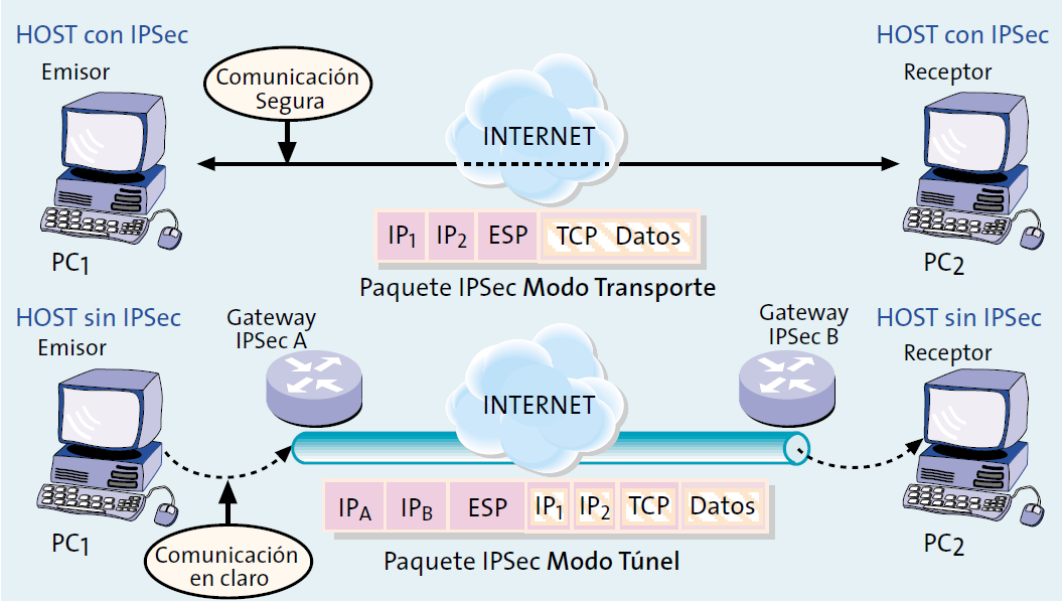


Ilustración 13 Modos de funcionamiento transporte y túnel IPSec (Iglesias, 2001)

II.5.4.3 IKE: Protocolo de control

Un concepto esencial en IPSec es el de asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Como se expuso anteriormente es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios. A esta operación se le llama negociación de SAs (Iglesias, 2001).

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes.
Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF. (D. HARKINS and D. CARREL, 1998)

Iglesias establece que IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley. ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo de IKE es la de establecer una conexión cifrada y autenticada entre dos entidades, a través del cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación de efectúa en dos fases:

1) El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales. En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de

forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública).

2) En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

En la ilustración 14 se representa de forma esquemática el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH. (Iglesias, 2001).

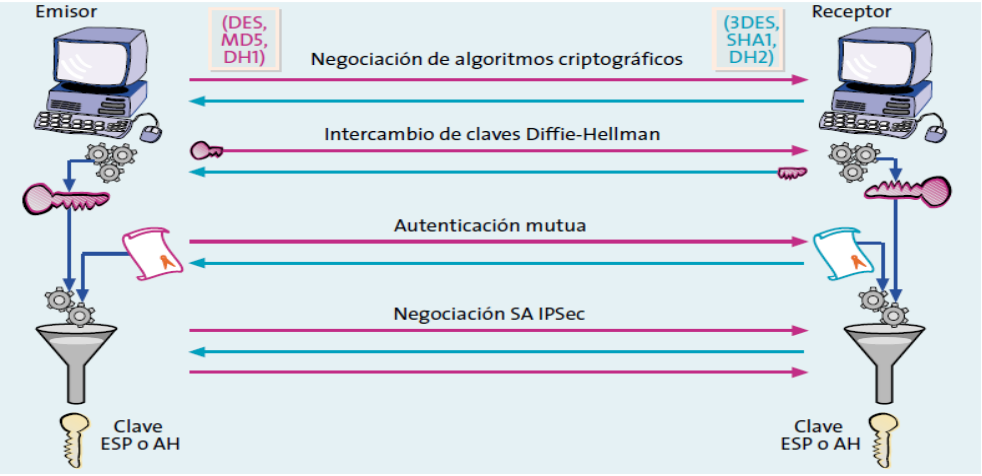


Ilustración 14 Funcionamiento del protocolo IKE. Fuente: (Iglesias, 2001)

El uso de PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. Se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (en adelante CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA. En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI.

De acuerdo con Iglesias la manera en que funciona PKI es la siguiente, en la ilustración 15 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL (Iglesias, 2001).

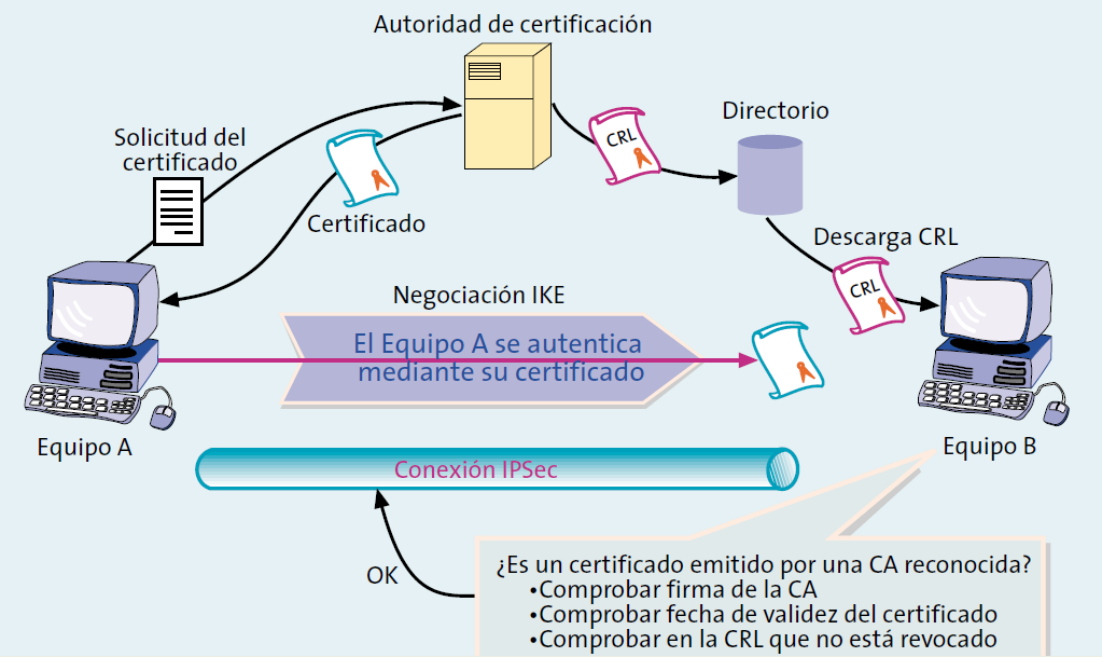


Ilustración 15 PKI en IPSec. Fuente: (Iglesias, 2001)

II.5.4.4 ISKAMP

Como se mencionó anteriormente IKE describe un protocolo híbrido cuyo propósito es negociar y proveer el material de claves para desarrollar una asociación de seguridad de manera protegida.

Según Corlleti, IKE define tres elementos fundamentales:

1) OAKLEY: Este define una serie de modos de intercambio de claves detallando los servicios que provee cada uno, está definido en el RFC 2412.

2) SKEME (*Secure Key Exchange Mechanism for Internet*): Describe una técnica de intercambio de claves muy versátil que provee anonimato, repudio y rápido refresco de claves.

3) ISAKMP (*Internet Security Association and Key Management Protocol*): Provee un entorno para autenticación e intercambio de claves, pero no los define, sólo se limita a establecer las fases a seguir:

   3.1) Modo Principal (Obligatorio): Solo se emplea en la fase uno de ISAKMP. Es una instancia de ISAKMP para proteger el intercambio.

   3.2) Modo agresivo (Optativo): Sólo se emplea en la fase uno de ISAKMP. Es también una instancia de ISAKMP, y funciona de acuerdo a la siguiente explicación: Aquí se destaca que también existe un modo rápido (Solo empleada en la fase dos de ISAKMP) para refrescar las claves y SA, el cual no es un intercambio completo, pero es usado como parte de los procesos anteriores (Corletti).

Además dentro de lo que se desea explicar tanto en modo principal o agresivo se permiten estos métodos de autenticación:

- Firma Digital
- Dos métodos de clave pública
- Secreto precompartido

ISAKMP combina los conceptos de seguridad de las asociaciones de autenticación, gestión de claves, y la seguridad de establecer la seguridad necesaria para las comunicaciones privadas en Internet.

"La Asociación de Seguridad de Internet y el protocolo de administración de claves (ISAKMP) define los procedimientos y formatos de paquetes para establecer, negociar, modificar y eliminar asociaciones de seguridad (SA). SA contiene toda la información necesaria para la ejecución de servicios de seguridad en diversas redes, tales como los servicios de la capa IP (como cabecera la autenticación y la

encapsulación de carga útil), el transporte o servicios de la capa de aplicación o de autoprotección del tráfico de negociación. ISAKMP define cargas útiles para el intercambio de generación de claves y autenticación datos. Estos formatos proporcionan un marco coherente para la transferencia de clave y los datos de autenticación, que es independiente de la técnica de generación de clave y el algoritmo de cifrado y el mecanismo de autenticación". (M.Schneider, 1998).

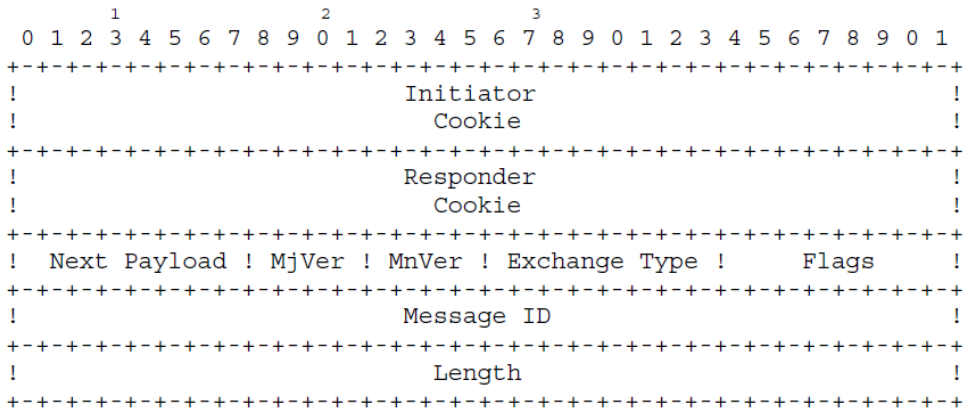


Ilustración 16 Encabezado básico de ISAKMP

Entre las aplicaciones prácticas de IPSec se tiene: Interconexión de redes locales (LAN), acceso seguro de usuarios remotos, interconexión de sucursales, entre otros.

Para finalizar la descripción de IPSec, se concluye que este protocolo es flexible y potente y que gracias a esto se pueden utilizar las redes para aplicaciones críticas como transacciones comerciales entre empresas. Ofrece una solución ideal para aquellos escenarios en que se requiera seguridad, independientemente de la aplicación. Se considera una tecnología bastante madura para ser implementada en todos aquellos escenarios en los que la seguridad es un requisito prioritario.

II.5.5 SSH (Secure Shell)

"SSH™ (o *S*ecure *SH*ell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los

usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas." (Red Hat, 2005)

De acuerdo con la página oficial Red Hat, entre las características de SSH se tiene:

- 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 sesión 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 reenviar aplicaciones X11 desde el servidor. Esta técnica, llamada reenvío por X11, proporciona un medio seguro para usar aplicaciones gráficas sobre una red. X11 se refiere al sistema de visión por ventanas.

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 puertos. Al utilizar SSH para inicios de sesión remota y para copiar archivos, se disminuyen la probabilidad de amenazas, debido a que el cliente y el servidor usan firmas digitales para su identidad.

La secuencia de eventos de una conexión SSH para proteger la integridad de la comunicación es la siguiente:

1) Se lleva a cabo un '*handshake*' (apretón de manos) encriptado para que el cliente pueda verificar que se está comunicando con el servidor correcto.
2) La capa de transporte de la conexión entre el cliente y la máquina remota es encriptada mediante un código simétrico.
3) El cliente se autentica ante el servidor.
4) El cliente remoto interactúa con la máquina remota sobre la conexión encriptada.

Para continuar con el desarrollo explicativo de SSH es necesario recordar que el cifrado lo hace SSH con la capa de transporte, reforzada con SSL (que es en realidad un plug-in) esto con el fin de facilitar una comunicación segura entre los dos hosts durante la autenticación y la subsecuente comunicación. En la capa de transporte se lleva esto a cabo manejando la encriptación y decodificación de datos y proporcionando protección de integridad de los paquetes de datos mientras son enviados y recibidos gracias a la labor de SSL. Además, la capa de transporte proporciona compresión de datos, lo que acelera la transmisión de información.

Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de transporte correctamente. Durante el intercambio, según Red Hat Enterprise, se producen los siguientes pasos:

1) Intercambio de claves
2) Se determina el algoritmo de encriptación de la clave pública
3) Se determina el algoritmo de la encriptación simétrica
4) Se determina el algoritmo autenticación de mensajes
5) Se determina el algoritmo de hash que hay que usar

El servidor se identifica ante el cliente con una *llave de host* única durante el intercambio de llaves. Si este cliente nunca se había comunicado antes con este determinado servidor, la llave del servidor le resultará desconocida al cliente y no lo conectará.

SSH fue ideado para funcionar con casi cualquier tipo de algoritmo de clave pública o formato de codificación. Después del intercambio de claves inicial se crea un valor *hash* usado para el intercambio y un valor compartido secreto, los dos sistemas empiezan inmediatamente a calcular claves y algoritmos nuevos para proteger la autenticación y los datos que se enviarán a través de la conexión en el futuro (Red Hat, 2005).

Después que una cierta cantidad de datos haya sido transmitida con un determinado algoritmo y clave (la cantidad exacta depende de la implementación de SSH), ocurre otro intercambio de claves, el cual genera otro conjunto de valores de hash y un nuevo valor secreto compartido. De esta manera aunque un agresor lograse determinar los valores de hash y de secreto compartido, esta información sólo será válida por un período de tiempo limitado.

La autenticación en SSH se lleva a cabo cuando la capa de transporte haya construido un túnel seguro para transmitir información entre los dos sistemas, el servidor le dirá al cliente de los diferentes métodos de autenticación soportados, tales como el uso de firmas privadas codificadas con claves o la inserción de una contraseña. El cliente entonces intentará autenticarse ante el servidor mediante el uso de cualquiera de los métodos soportados.

Los servidores y clientes SSH se pueden configurar para que permitan varios tipos de autenticación, lo cual le concede a cada lado la cantidad óptima de control. Luego el servidor podrá decidir qué métodos de encriptación soportará basado en su pauta de seguridad, y el cliente puede elegir el orden en que intentará utilizar los métodos de autenticación entre las opciones a disposición.

Luego de una autenticación exitosa sobre la capa de transporte SSH, se abren múltiples *canales* a través de la multiplexación. Cada uno de estos canales maneja la conexión para diferentes sesiones de terminal y para sesiones de reenvío X11.

Los clientes y servidores pueden crear un canal nuevo. Luego se le asigna un número diferente a cada canal en cada punta de la conexión. Cuando el cliente intenta abrir un nuevo canal, los clientes envían el número del canal junto con la petición. Esta información es almacenada por el servidor y usada para dirigir la comunicación a ese canal. Esto es hecho para que diferentes tipos de sesión no afecten una a la otra y así cuando una sesión termine, su canal pueda ser cerrado sin interrumpir la conexión SSH primaria.

Los canales también soportan el *control de flujo*, el cual les permite enviar y recibir datos ordenadamente. De esta manera, los datos no se envían a través del canal sino hasta que el host haya recibido un mensaje avisando que el canal está abierto y puede recibirlos.

El cliente y el servidor negocian las características de cada canal automáticamente, dependiendo del tipo de servicio que el cliente solicita y la forma en que el usuario está conectado a la red. Esto otorga una gran flexibilidad en el manejo de diferentes tipos de conexiones remotas sin tener que cambiar la infraestructura básica del protocolo.

Con SSH puede asegurar los protocolos TCP/IP a través del reenvío de puertos. Cuando use esta técnica, el servidor SSH se convierte en un conducto encriptado para el cliente SSH. El reenvío de puertos funciona mediante el mapeado de un puerto local en el cliente a un puerto remoto en el servidor. SSH le permite mapear cualquier puerto desde el servidor a cualquier puerto en el cliente; y los números de puerto no necesitan coincidir para que esto funcione (Red Hat, 2005).

II.6. Análisis de herramientas de estudio de redes (Servidores, Sniffers e IDS)

II.6.1 Servidores

"Un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente. Un servidor dedicado, es aquel que dedica todos sus recursos a atender solicitudes de los equipos cliente. Un servidor compartido es aquel que no dedica todos sus recursos a servir las peticiones de los clientes, sino que también es utilizado por un usuario para trabajar de forma local". (Sistemas, 2012)

Existe diferentes tipos de servidor entre los más destacados se tienen:

- Servidor de archivos.
- Servidor de Directorio Activo/Dominio.
- Servidor de Correo.
- Servidor Proxy.
- Servidor Web.
- Servidor de base de datos.
- Servidor DNS.
- Servidor DHCP.

II.6.2 Sniffers

Ahora se procederá a estudiar *los sniffers* empezando por su definición y utilidad.

Según CISCO® un *sniffer* es un programa de captura de las tramas de red. Es algo común que, el medio de transmisión sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el *sniffer* le dice a la computadora que deje de ignorar todo el tráfico no destinado al equipo y le ponga atención, esto es conocido como poner en estado "promiscuo" a la NIC (*Network*

Interface Card) (CISCO, 2009). En el caso de este estudio se utilizará un HUB para lograr dicho fin.

Una vez que la NIC está en este estado se necesitarán los privilegios administrativos o de *root*, de ésta manera la computadora será capaz de ver todos los datos transmitidos. Es entonces cuando el programa comienza a hacer una lectura de toda la información entrante al PC por la tarjeta de red. Con esto el *sniffer* conseguirá observar el equipo de origen, el equipo de destino, número de puerto, entre otras cosas, en resumen puede ver la información intercambiada entre dos computadoras.

De acuerdo con CISCO® uno de los principales usos que se le pueden dar son:

- Captura de contraseñas enviadas sin cifrar y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por atacantes para corromper sistemas de red.
- Análisis de fallos para descubrir problemas en la red,
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- Para los desarrolladores, en aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red. (CISCO, 2009)

Algunos *sniffers* más utilizados se tienen los siguientes:

- Wireshark®, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.
- Ettercap.
- Kismet.
- TCPDUMP, “es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario

> capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado". (CISCO, 2009)

Un *sniffer* puede ser de gran utilidad en la administración de una red, con fines de seguridad y funcionalidad, pero hay que tomar en cuenta de que es una herramienta que puede ser de doble filo, ya que algún usuario puede utilizarla con un fin adecuado y pueda tomar ventaja de esto.

II.6.3 IDS (Sistema de Detección de Intrusos)

Según Maiwald los sistemas de detección de intrusiones son otra herramienta utilizada por el personal de seguridad informática de una organización para protegerse, mediante la identificación de hackers que intentan una penetración. De manera ideal, un sistema así solamente dará la alarma cuando se efectúe un ataque exitoso. La detección de intrusiones también puede ayudar a la identificación proactiva de las amenazas activas, proporcionando indicaciones y advertencias de que una amenaza está reuniendo información para un ataque. (Maiwald, 2005)

Los sistemas de detección de intrusiones (IDS, *Intrusion Detection Systems*) han sido basados en métodos antiguos de seguridad como perros guardianes y centinelas. En el caso del perro guardián se provee en el sistema un identificador de agresores y un mecanismo de respuesta disuasoria que ahuyenta a los posibles atacantes. El centinela presenta relativamente los mismos propósitos, aunque este provee una respuesta más contundente contra el atacante, como ejemplificación sería equivalente en la vida cotidiana a que el centinela puede accionar su arma o llamar a las autoridades.

"Otra analogía más cercana a los IDS, corresponde a alarmas antirrobo diseñadas para detectar cualquier intento de entrada al interior de un área protegida cuando esta se encuentra desocupada. Cabe destacar que el área protegida o perímetro de seguridad estaría delimitado conceptualmente en el mundo computacional, como todos los sistemas de cómputo o red, pudiendo estar definidos por corta fuegos,

módems, computadores, entre otros dispositivos de red. Siendo estos monitorizados por un IDS, que está diseñado para diferenciar entre una entrada autorizada y una intrusión malintencionada. Definiendo cuales eventos constituyen una violación del perímetro de seguridad, realizando las preguntas; ¿Es un evento la identificación de sistemas vivos? Y ¿Qué hay acerca del uso de un ataque conocido en contra de un sistema en la red? En la medida que estas preguntas sean respondidas, queda claro que las respuestas no pueden darse en un esquema en blanco y negro. Más bien, de otros eventos y del estado del sistema objetivo." (Maiwald, 2005)

II.6.4 Tipos de Sistemas de Detección de Intrusiones, IDS

En el mercado existen dos tipos principales de IDS, uno basado en modo de anfitrión (HIDS) y el otro basado en la red (NIDS). El HIDS reside en un anfitrión particular y busca indicaciones de ataques en ese anfitrión, en cambio un NIDS reside en un sistema separado que vigila el tráfico de la red, buscando indicios de ataques que atraviesen esa parte de la red.

II6.4.1 IDS basado en anfitrión (Host-based IDS, HIDS)

Los HIDS son un sistema de sensores que se encuentran ubicados en varios servidores dentro de una organización y son controlados por algún administrador central. Estos sensores son capaces de examinar varios tipos de eventos asociados con el servidor donde están cargados y tomar acciones en un servidor particular según lo que se requiera o enviar una notificación. Por consiguiente un sensor HIDS es capaz de determinar si un ataque tuvo éxito o no, dentro del servidor donde se encuentra.

Existen diferentes tipos de HIDS que tienen una ejecución particular según las necesidades de una organización, acotando la importancia de determinar qué tipo de sensor HIDS es apropiado para cada servidor. Se considera que cada servidor debe tener una licencia del sensor, un gran número de sensores provoca que el sistema complejo cueste más, a pesar de que por unidad es más económico. Por lo que es

importante delimitar el tipo de HIDS, con el fin de intentar usar pocas unidades de sensores. Existen, según Maiwald, cinco tipos básicos de sensores HIDS:

Analizadores de Bitácoras.

Este analizador vigila los archivos de bitácora apropiados en el sistema cuando se ejecuta un proceso. Generalmente estos analizadores están bien configurados para buscar entradas de registro que puedan señalar un evento de seguridad, pero adicionalmente el administrador del sistema puede definir nuevas entradas de registro que le sean de interés. Estos se adaptan para evitar ataques internos, pero cabe destacar que son sistemas reactivos que reaccionan luego de que el sistema ya ha sido comprometido.

Sensores Basados en Firmas

Los sistemas basados en firmas tienen la capacidad de ver los ataques a medida que llegan al sistema, mediante la comparación del tráfico entrante de la red con el conjunto de firmas de eventos de seguridad con que ya viene integrado, siendo capaz de realizar alguna notificación adicional de los ataques. Al igual a los analizadores de bitácoras da seguimiento a usuarios autorizados, pero se diferencia en que este si analiza el trafico entrante.

Analizadores de llamadas al sistema

Los analizadores de llamadas al sistema analizan las llamadas entre las aplicaciones y el sistema operativo, identificando eventos de seguridad, mediante una base de datos de firmas de tipos de comportamientos que pueden significar un ataque o un evento relevante para el administrador del IDS. A diferencia de los anteriores este es capaz de evitar que una acción ocurra.

Analizadores del Comportamiento de la Aplicación

Los analizadores de comportamiento, trabajando como una calza de software entre aplicaciones y el sistema operativo, examinan la llamada para determinar si la

aplicación tiene permisos para realizar una acción en lugar de examinar la llamada para determinar si parece un ataque, a diferencia de los analizadores de llamadas.

Verificadores de la Integridad de los Archivos

Los verificadores de la integridad de los archivos vigilan los cambios realizados en los archivos, mediante el uso de una suma de verificación criptográfica o firma digital del archivo. La firma resultante se modificara si cambia cualquier bit en el archivo original (esto puede incluir atributos como fecha de creación o el tamaño de archivo). Los algoritmos utilizados para este proceso fueron desarrollados para hacer extremadamente difícil que se hicieran cambios que permitieran dejar la misma firma. (Maiwald, 2005)

Inicialmente el sensor IDS será configurado con los archivos que se deseen monitorear, calculando sus respectivas firmas y almacenando estas en una ubicación segura. Periódicamente se calculara las firmas de los archivos y se comparara con la almacenada, a fin de comprobar si han sufrido modificaciones. Si bien esta verificación de integridad no proporciona ninguna indicación de ataque, en su lugar, expone en detalle los resultados del ataque.

II.6.4.2 IDS basado en red (Network-Based IDS, NIDS)

De acuerdo con Maiwald un NIDS existe como un proceso de software en un sistema de hardware dedicado. El NIDS pone la tarjeta de interfaz de la red en el sistema en modo promiscuo, lo que significa que la tarjeta pasa todo el tráfico en la red hacia el software NIDS, más que exclusivamente el tráfico destinado para ese sistema. Entonces se analiza el tráfico de acuerdo a un conjunto de reglas y firmas de ataque para determinar si el tráfico es de interés.

Los sistemas NIDS están basados principalmente en firmas de ataque que son punto de comparación para detectar eventos en el tráfico en línea. Estos también pueden especificar el tráfico de interés sobre la base de la dirección fuente, dirección destino,

puerto fuente o puerto destino, permitiendo a las organizaciones definir el tráfico para vigilar lo que esté fuera de las firmas de ataque.

Considerando el caso de ataques que no se encuentren en los archivos de firmas, los cuales el NIDS no descubrirá, existen en el mercado un NIDS basado en anomalías que puede al menos saltar un alerta por pequeñas varianzas en el tráfico normal.

La configuración más común para un NIDS es utilizar dos tarjetas de interfaz de red, donde una tarjeta se utiliza para monitorear una red, estando la tarjeta en modo furtivo con el fin de que no tenga dirección IP y no responda a conexiones de entrada. En cambio la segunda tarjeta es utilizada para comunicarse con el sistema de administración de IDS y para emitir alarmas. A su vez se encuentra adscrita a una red interna que no es visible para la red que está siendo monitoreada (Maiwald, 2005).

Las ventajas de un NIDS se resumen en las siguientes afirmaciones:

- El NIDS puede estar completamente oculto en la red de modo que un atacante no sabrá que está siendo monitoreado.
- Se puede emplear un NIDS simple para monitorear el tráfico en un gran número de sistemas objetivo potenciales.
- El NIDS puede capturar el contenido de todos los paquetes que viajan hacia un sistema objetivo.

Las desventajas a considerar son:

- El sistema NIDS solo puede dar la alarma si el tráfico coincide con las reglas o firmas previamente configuradas.
- El NIDS puede perder tráfico de interés debido a la utilización de un ancho de banda elevado o rutas alternas.
- El NIDS no puede determinar si el ataque tuvo éxito.
- El NIDS no puede examinar el tráfico que está encriptado.

- Las redes conmutadas (en oposición a las redes de medios compartidos) requieren configuraciones especiales para que el NIDS pueda examinar todo el tráfico.

II.6.5 Perfiladores

Para determinar el estado de la VPN antes y durante el ataque, es necesario conocer el progreso de los datos que fluyen a través del túnel. Según Wood un perfilador se inserta en dicho túnel para dar indicación visual, ya sea por consola o con alguna interfaz gráfica, de la velocidad de los datos, el tiempo que ha tomado y una estimación del ancho de banda del canal (Wood, 2010).

En la investigación realizada se consiguieron dos modelos de perfiladores el primero Pipe Viewer para el protocolo SSH y el segundo Jperf para el protocolo de VPN IPsec teniendo este una interfaz gráfica. El funcionamiento de estos se explica en los resultados.

CAPÍTULO III

Marco Metodológico

En el presente capitulo se muestra la sistemática utilizada al realizar el presente proyecto de grado, exponiendo en cada fase de esta, el plan a efectuar para lograr los objetivos del proyecto. A su vez se entenderá claramente la elección de los procedimientos y métodos usados.

La metodología presentada corresponde a las exigencias de investigación del trabajo especial de grado que tiene como objetivo principal conocer el comportamiento de una Red Privada Virtual frente a ataques reales, con el fin de obtener la información lo más exacta posible sobre la vulnerabilidad de esta herramienta. Para esto se procedió a levantar información para encontrar y analizar opciones disponibles de herramientas especializadas en realizar un estudio de este tipo, planteando como base la construcción de una red de prueba. La cual una vez en funcionamiento será provista de conexiones VPN y mecanismos de ataque de redes, que permitirán realizar el estudio deseado, trayendo como resultado una lista de vulnerabilidades de red, especializada en debilidades de Redes Privadas Virtuales donde se planteara en cada caso su respectiva solución o recomendación. Teniendo en cuenta que algunos resultados serán obtenidos mediante investigación teórica. De esta manera se provee un esquema de soluciones sobre ataques a red y adicionalmente una metodología aplicable para el estudio de otras herramientas de redes.

Para lograr el estudio teórico y práctico se desarrolló la siguiente metodología planteada en el esquema, que se desenvuelve en las fases que lograra cumplir con el proyecto establecido.

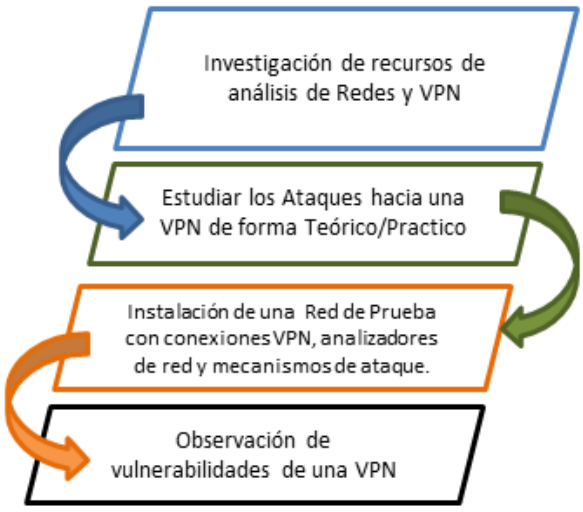


Ilustración 17 Esquema Resumen de la Metodología

III.1 Fase I: Realizar la revisión bibliográfica, levantamiento de información.

Se investiga y estudian los diferentes métodos, técnicas y software que se emplean del área de seguridad en redes para tener enlaces confiables mediante VPN. Entendiendo la necesidad de conocer lo que se está investigando en este caso las VPN.

III.2 Fase II: Conocer los distintos ataques para VPN

Se estudia los distintos ataques hacia una Red Privada Virtual de forma directa e indirecta, analizando cuál de estos serán aplicables en la parte práctica del proyecto. Esto con el fin de encontrar las vulnerabilidades de una VPN

III.3 Fase III: Estudiar que herramientas se utilizaran para medir los parámetros de la VPN.

Se procede a estudiar la conveniencia de las herramientas a utilizar, para hacer un estudio lo más detallado posible de las vulnerabilidades de las VPN.

III.4 Fase IV: Instalar la red de prueba

Se procede a montar una red física con herramientas de análisis de red y mecanismos de ataque de redes.

III.5 Fase V: Instalar la VPN en la red.

Se implantó redes privadas virtuales en la red de prueba, por métodos distintos para probar su calidad y su correcto funcionamiento. De tal manera que se pueda realizar adicionalmente una comparación entre los tipos de configuración de VPN más resaltantes.

III.6 Fase VI: Hacer pruebas pertinentes

Se aplica de manera práctica los ataques estudiados en forma teórica anteriormente, en la VPN instalada en la red montada.

III.7 Fase VII: Analizar y concluir.

Documentación de los resultados arrojados por las herramientas que se usaron para el estudio de la VPN. Proponiendo luego soluciones inmediatas a estas vulnerabilidades encontradas.

III.8 Fase VIII: Redacción del libro de tesis.

Documentación y definición de conclusiones de los ataques estudiados, proponiendo soluciones o recomendaciones.

CAPÍTULO IV

Desarrollo

El capítulo muestra el procedimiento utilizado para cumplir con los objetivos del proyecto, desarrollando en orden cronológico las siguientes fases.

IV.1 Fase I: Realizar la revisión bibliográfica, levantamiento de información.

En esta fase se contaron con recursos bibliográficos desde libros hasta fuentes electrónicas aplicando el levantamiento de la información para cumplir con el primer objetivo específico. Todo esto para investigar y estudiar los diferentes métodos, técnicas, protocolos y software que se emplean en el área de seguridad en redes para tener enlaces confiables mediante VPN.

IV.2 Fase II: Conocer los distintos ataques para VPN

Se estudió inicialmente de manera teórica los tipos de ataques a redes pueden afectar a una Red Privada Virtual, para luego analizar cuáles son posibles de efectuar en las pruebas prácticas. Considerando no descartar ataques importantes cuya aplicación no sea realizable por excesivo riesgo a la integridad de los dispositivos de prueba, o por imposibilidad de acceso a su fuente.

En esta fase se encontraron dificultades debido a la desinformación con respecto a ataques hacia las VPN, mostrada por pocas respuestas de parte de personas capacitadas en seguridad de redes y fuentes de la Web, debido a lo específico del tema. Para solucionar esto se decidió investigar ataques históricamente trascendentales y otros que pudieran ser indirectamente dirigidos a una VPN por funcionar contra redes convencionales. Adicionalmente se investigó en la web en lugares con tendencia en promover conocimientos en el área del hacking. Al hacer esto se encontró que debido a la naturaleza de la investigación las páginas web

consultadas eran de dudoso origen, no obstante, no se corrió riesgo al navegar en ese tipo de páginas. Algunas páginas ofrecían ataques básicos no directamente a la VPN pero si a los elementos que la constituyen como por ejemplo ataque a los servidores y puertos usados por protocolos específicos, teniendo más relevancia los ataques de inundación ICMP y UDP.

Se probaron varios ataques de inundación y muchos no tenían efecto alguno en el rendimiento de la VPN, no obstante se encontraron otros que sí y fueron seleccionados para hacer los experimentos planteados de las siguientes fases. Estos programas de ataque fueron *Net Tools (UDP flood), UDP Flooder 2.00 y Divine Intervention (Plagez Floodz*), ataques de denegación de servicio.

Otros ataques de VPN considerados para el estudio además de los que afectan al servidor VPN como los anteriores, son aquellos que afectan la autenticación mediante suplantación de usuarios y alteración de los datos transmitidos al túnel VPN. Entre estos se encuentran ataques como el troyano conocido como SUBSEVEN que utiliza VPN para controlar *hosts* remotos y programas como MSCHAP V.2 famoso por suplantar al usuario VPN con conexión PPTP, los cuales fueron mencionados en resultados como ataques históricos por su trascendencia en el área de hacking contra las VPN y las redes en general. Adicionalmente se estudiaron de forma teórica algunos otros ataques que no pudieron ser probados de forma práctica, pero investigando se espera como resultado lograr conseguir soluciones a estos.

IV.3 Fase III: Estudiar que herramientas se utilizaran para medir los parámetros de la VPN.

Se procedió a analizar distintos prototipos de herramientas para formar una red de prueba que permitiera capturar y analizar los datos de la red referentes al desempeño de la Red Privada Virtual que se pruebe. En el proceso se obtuvo, mediante la

investigación diversos mecanismos de análisis de red, siendo algunos de alta efectividad.

Una herramienta de monitoreo de red que poseen bases de datos de ataques que son actualizadas con periodicidad, por su uso potencial en seguridad de redes de empresas y otros entes, son los sistemas de detección de intrusos en siglas en ingles conocido como NIDS. El NIDS provee información de lo que se quiere estudiar, como las tendencias del flujo de información de la red mediante gráficas, además de la descripción y clasificación exacta de los eventos detectados en la red de estudio. Se estudiaron muchos NIDS, se presentó el inconveniente de que la gran mayoría que poseen base de datos actualizadas son de pago, para solucionar esto se trabajó con un NIDS muy completo con versión de prueba, llamado $SAX\ 2^{®}$ de la empresa Ax3soft Corporation. Este mecanismo de captura en conjunto con herramientas como los analizadores de protocolos, que permiten capturar los datos en las interfaces de red involucradas en el estudio, en este caso por su versatilidad se escogió Wireshark®. Esto junto con el NIDS forma el sistema de análisis de la red, al cual se le añadió un elemento más para medir la velocidad de transferencia en el túnel VPN, que es un perfilador.

Cabe destacar que un camino fallido en el proyecto fue el montaje de una red trampa conocida como HoneyNet, que posee en teoría las características de captura y análisis, enfocadas en estudios de atacantes y vulnerabilidades, usada habitualmente como una red vulnerable a atacantes que atrae a hackers y esconde sus herramientas de captura con el fin de estudiar el comportamiento de los agresores. Teniendo de esta manera un herramienta perfectamente acorde con el proyecto, pero en la práctica durante su instalación se descubrió que sus bases de datos de ataques, paquetes de análisis, entre otros elementos estaban desactualizados porque había sido desatendida por sus creadores, debido a que esta había sido desplazada por otros sistemas de seguridad como los IDS, por su alto costo de montaje y compleja configuración. En

consecuencia se solventó para el estudio desplegar la red de prueba con las herramientas antes mencionadas.

IV.4 Fase IV: Instalar la red de prueba

Mediante los mecanismos de análisis de red estudiados en la fase anterior se construyó una red de prueba, en donde se coloca un host atacante que posee las herramientas para realizar los ataques de prueba. Con la finalidad de dar un estudio extenso se procedió a estudiar las vulnerabilidades de las VPN en dos ambientes (Windows® O.S. y Debian®O.S.) utilizando dos distintas arquitecturas de red, además de utilizar distintos protocolos de VPN.

En Windows®O.S. se desplegó una topología de red LAN compuesta por cuatro *host*, en donde solo dos se conectarían por VPN siendo uno servidor y otro cliente, mientras uno realizaría la captura y análisis de todo lo ocurrido en la red con el NIDS SAX2®y el *sniffer* Wireshark®, siendo el último *host* el atacante. De esta manera se instaló una red de prueba para VPN de usuario.

La arquitectura utilizada para el ambiente en Debian® O.S. fue emular una VPN de sitio en donde se unirían dos redes LAN separadas por su *proxy* respectivo, mediante una conexión VPN entre ellos. Para lo cual se implementó dos servidores proxy *squid*, con la ayuda de la aplicación *Webmin* que provee un entorno grafico para la configuración de dicho servidor.

IV.5 Fase V: Instalar la VPN en la red.

Antes de hacer las pruebas pertinentes se instaló tres distintos tipos de VPN en la topología de red desarrollada en la fase anterior, para realizar en total tres experimentos.

De esta manera para la primera experiencia se instaló una VPN de usuario en Windows® O.S. cómo se describió antes, con el protocolo de seguridad VPN PPTP, configurando un *host* como servidor aceptando conexiones entrantes de clientes VPN pre-configurados, por consiguiente estableciendo un *host* con conexión VPN a la IP del servidor y con seguridad PPTP. Siempre utilizando el software de configuración VPN inherente en el sistema operativo. Cabe destacar que en esta primera prueba la red se encontraba aislada por motivos de integridad y seguridad, para evitar daños catastróficos extendidos, pudiendo así comprobar si los ataques utilizados en las próximas pruebas pudiesen ser ejecutadas en un ambiente real.

En el ambiente Debian® O.S. la VPN, de los *proxys squid*, pasa por una red pública, en este caso la red de la UCAB, esto con el fin de tener un ambiente de estudio más realista. Primero se comprobó con la experiencia anterior que los ataques encontrados cumplían su objetivo sin afectar ningún otro elemento de la red, y luego se procedió a ejecutar la instalación de la red de prueba con VPN de sitio descrita en la fase anterior, con el protocolo SSH, configurando un proxy como cliente y otro como servidor VPN SSH y aplicando los requerimientos de autenticación de usuario para la conexión, que permitirá a los *host* separados por su respectivo proxy establecer comunicación.

Para la última prueba se instala una VPN de usuario con el protocolo IPSec, dejando esta como última prueba para tener precedentes con otros protocolos de seguridad, con el fin de generar una clara comparación, considerando su relevancia por su actual importancia en la aplicación de seguridad en el protocolo IPv6. De esta manera fue montada una VPN de usuario entre dos equipos con sistema operativo Windows®, para lo cual se escribió copias de certificados IPSec de autenticación de clave compartida en cada máquina y se estableció un servidor y un cliente VPN con la herramienta del sistema operativo configurando la conexión con seguridad L2TP/IPSec. Teniendo de esta manera la conexión VPN con seguridad IPSec

establecida, la cual fue utilizada para configurar una conexión por escritorio remoto entre servidor y clientes, para observar los efectos de la prueba con claridad.

IV.6 Fase VI: Hacer pruebas pertinentes

Con todos los elementos para las pruebas en funcionamiento se realizan los principales tres experimentos con expectativas de resultados satisfactorios para la investigación.

En el primer experimento teniendo la red de prueba con una VPN de usuario con seguridad PPTP, como se comentó anteriormente y con la conexión VPN en funcionamiento se inicia los ataques a la VPN con los programas de ataques conseguidos, destacándose aquellos que realizan Denegación de Servicio, utilizando como datos para poder efectuar el ataque la IP del servidor VPN y en algunos el puerto pre-configurado donde se establece el túnel. Mientras el analizador de protocolos *sniffer* y el NIDS, realizan la captura de la data para el posterior análisis. De esta manera se probó cada programa de ataque encontrado y se referencia en los resultados solo aquellos de valor significativo. Obteniendo para las siguientes pruebas los programas de ataques más factibles y seguros para la integridad de los equipos de prueba. Cabe destacar que en esta experiencia con la red aislada se destacó como funcional no solo los ataques de DOS, sino también el troyano SubSeven uno de los ataques trascendentales.

En el segundo experimento se realizaron las pruebas pertinentes en la red de prueba manejada por *proxys* conectados entre sí por la conexión VPN SSH, como se dijo en las anteriores fases, en la cual se aplicó la misma modalidad del anterior experimento solo que se empleó únicamente los ataques funcionales, que fueron de Denegación de Servicio. Con el ataque en curso se realizó descargas de archivos del servidor al cliente VPN, con el fin de observar las consecuencias del ataque.

Para el último experimento en el cual se aplica la misma red que en el primero pero estando conectado a una red pública, se realiza los ataques de Denegación de Servicio, capturando todo el tráfico, los paquetes en curso y se además calcula la velocidad de transferencia de la conexión al igual que las anteriores experiencias. Pero se aplica una conexión de escritorio remoto que permite ver de manera más grafica lo que observa una víctima durante un ataque.

De esta manera con todos los datos obtenidos de las experiencias se realiza un análisis detallado generando conclusiones y recomendaciones sobre la seguridad de una VPN y las redes en general.

IV.7 Fase VII: Analizar y concluir.

Los resultados obtenidos de las pruebas fueron analizados y clasificados, a fin de obtener en lo posible soluciones o recomendaciones, para cada ataque efectuado y en caso de los tipos de ataques que no se llevaron a la práctica por su respectiva causa se discutió la posible solución de forma teórica.

CAPÍTULO V

Resultados

En respuesta a la metodología seguida y objetivos se plantean los resultados de acuerdo al orden en que se expusieron. Las fases I, II y III surgen para dar cumplimiento al primer objetivo, como resultado se tiene el conocimiento de los elementos principales, propiedades que conforman una VPN, todo descrito en el marco teórico, conociendo esto se puede pasar a destacar en que puntos son vulnerables las VPN de acuerdo al protocolo utilizado, con esto se da la fase I por cumplida. Cabe destacar que los ataques encontrados no son directos a la VPN, sino a los elementos que la comprometen, debido a que actualmente no se cuenta con hardware suficientemente poderoso como para descifrar fácilmente el flujo de datos VPN, estas son virtualmente casi imposibles de descifrar.

El primer objetivo plantea conocer lo vulnerable que puede ser una VPN a ataques y determinar cuáles herramientas son eficientes para hacer el estudio práctico. Teniendo puntualizado el camino principal de la investigación se procede a dar los resultados encontrados organizados por fase.

V.1 Fase II: Conocer los distintos ataques para VPN.

Los ataques se estudian de manera teórica, y se desarrollan experimentalmente aquellos ataques que permitan hacer pruebas de significativo valor, sin comprometer catastróficamente los equipos usados para la prueba. Primeramente es necesario considerar si existe algo como un ataque a una VPN especifica o si es vulnerable a cualquier ataque. Entre los ataques estudiados se encuentran aquellos que eventualmente pueden conducir a la VPN a revelar los datos manejados, también si los agresores rompen el algoritmo se trata de un ataque VPN, si entran al servidor y leen sus claves también es un ataque. Estos son ataques a algoritmos criptográficos, ataque de generador de números aleatorios; en consecuencia ataques a IPSec y ataques a PPTP, entre otros protocolos de seguridad usados en VPN.

Con la finalidad de tener acceso exitoso a la información trasmitida sobre la VPN un atacante debe:

- Capturar toda la sesión, lo que significa que debe situarse un rastreador entre los extremos en una ubicación por donde deba pasar todo el tráfico de la VPN
- Utilizar una cantidad sustancial de poder de cómputo y tiempo para obtener la clave mediante fuera bruta y descifrar el código.

Ataques a la seguridad de una VPN

Según Brown, existen dos protocolos de VPN importantes: IPSec y PPTP, se pasará a estudiar los puntos débiles de estos, ya que cada uno de ellos es un marco de referencia para lograr una VPN segura. Hay que acotar que tanto IPSec como PPTP no hacen cifrado y tampoco ofrecen seguridad en paquetes de datos, con esto claro si llegara a ocurrir un ataque se llevaría a cabo en base a estos marcos de referencia. Pero acotando el hecho de que si bien IPSec no da seguridad por sí solo, utilizando el encabezado (AH) provee autenticación y la carga de seguridad encapsulada (ESP) consigue cifrar. (Brown, 2000).

Antes de comenzar a estudiar los ataques es necesario acotar que se encontró que la mayoría de las fallas de seguridad, no vienen de fuerza bruta sino de derivar la clave secreta de la pública. Por ejemplo una computadora potente puede forzar un criptosistema de clave pública de un módulo de 256 bits y algunas universidades y gobiernos pueden forzar claves de 318 y 512 bits. Aun las claves con módulos de 768 y 1024 bits son seguras. Esto demuestra que no está lejos de la realidad el hecho de quebrantar cualquier clave privada, pero para este estudio no se dará mayor importancia a este tipo de ataque porque es inalcanzable poseer un hardware con capacidad de procesamiento suficiente para realizar este tipo de tareas.

Es necesario ponerse a pensar si existe algo como un ataque específicamente contra VPN o si una VPN es vulnerable a cualquier ataque. Pero los siguientes ataques no se

dirigen expresamente a VPN, sin embargo la comprometieron. Estos son ataques a algoritmos criptográficos, ataque de generador de números aleatorios; ataques a IPSec y ataques a PPTP:

V.1.1 Ataques de algoritmos criptográficos

Los algoritmos criptográficos son vulnerables y están sujetos a ataques del mismo modo que cualquier otra pieza de software o hardware y por lo general existen tres formas de atacar a un algoritmo criptográfico: ataques contra el protocolo, ataques contra el algoritmo y ataques contra la implementación

1. Ataques contra el protocolo: Un sistema criptográfico es tan sólido como los algoritmos de cifrado y las funciones de transformación del código en los que se basa. Aspectos tales como no usar los generadores de números aleatorios correctos, reutilización de valores dañan la integridad de todo el diseño. Se debe seleccionar una semilla segura para no destruir la integridad de los algoritmos de cifrado y los protocolo de intercambios de claves.

   1.1 Ataques contra el algoritmo: El uso de claves débiles, el uso de una cantidad insuficiente del tamaño de datos a la alteración de las funciones de transformación del código contribuyen al debilitamiento del sistema.

   1.2 Ataques contra la implementación: Algunas veces al momento de implementar una VPN, los que hacen dicha labor dejan archivos temporales, mensajes en texto simple y datos almacenados en la memoria intermedia cuyo acceso es muy fácil. Hay que tener en cuenta que entre más claves haya en el sistema será más seguro, no obstante al combinar claves débiles con las fuertes estas quedan comprometidas amenazando a todo el sistema.

1.3 Ataques comunes en algoritmos criptográficos: Uno de los principales problemas con los ataques criptográficos es que es posible que la VPN sea atacada y los usuarios no sean conscientes de ello. Al igual que los ataques contra otros sistemas los algoritmos criptográficos son sujetos a los siguientes ataques típicos.

1.3.1 Ataque de texto simple conocido: En este ataque el agresor conoce parte del documento en texto simple o puede hacer conjeturas con cierta base sobre el mismo también puede tener acceso a alguna parte del texto simple con su correspondiente cifrado. Un texto simple puede adivinarse debido a que es posible que sea un saludo, encabezado o sinopsis estándar. Entonces debido a que el atacante tiene el texto cifrado, o también noción de este, puede utilizar el texto simple para decodificar el resto del texto.

1.3.2 Ataque de texto simple seleccionado: En este tipo de ataques el agresor toma algún texto y lo cifra con la clave desconocida. El atacante intenta adivinar la clave utilizada para este cifrado. En estos tipos de ataques el agresor tiene la capacidad de encontrar el texto cifrado que corresponde a un mensaje de texto simple arbitrario de su elección.

1.3.3 Ataque de intermediario: Este escenario se desarrolla al momento en que dos partes intercambian sus claves para comunicaciones posteriores. El intermediario secuestra las claves del emisor y el receptor, y las sustituye con las propias, por lo cual obtiene la capacidad de interceptar todas las comunicaciones futuras sin que el emisor y el receptor lo sepan. La manera de impedir esto es

mediante el uso de firmas digitales y con el mecanismo de claves secretas compartidas.

1.3.4 Ataque de sincronización: Este se basa en la medida de los tiempos de ejecución de una operación de exponenciación modular que se utiliza en los algoritmos criptográficos. Los criptosistemas toman cantidades de tiempo ligeramente diferentes para procesar entradas distintas, cuando el CPU ejecuta rutinas de optimización, ramificaciones, ciclos, instrucciones condicionales y demás se utilizan distintas cantidades de ciclos de una máquina. Los atacantes pueden explotar las medidas de tiempo o de sincronización en sistemas vulnerables para encontrar la clave secreta completa. Este tipo de ataque no es caro y a menudo requiere el conocimiento del texto cifrado. Se puede utilizar en algoritmos RSA y Difiie-Hellman.

1.3.5 Ataque de fuerza bruta: Es básicamente intentar recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

1.3.6 Solidez de los algoritmos criptográficos: No se puede probar que un algoritmo criptográfico no es seguro, excepto mediante el proceso de prueba y error. En teoría, cualquier algoritmo criptográfico puede romperse al probar todas las claves posibles en secuencia, pero el numero de pasos requeridos para los ataques de fuerza bruta crece en forma exponencial con la longitud de la clave. A continuación en la tabla 1 se puede apreciar la cantidad de pasos requeridos para cada tamaño de clave:

Tabla 1 Pasos requeridos para romper una clave. Fuente (Brown, 2000)

Longitud de la clave (bits)	Pasos requeridos
32	2^{32}
40	2^{40}
56	2^{56}
64	2^{64}
80	2^{80}
128	2^{128}
160	2^{160}

Las claves de 120 bits y 160 bits son seguras por ahora, las de menor longitud se pueden comprometer si se dispone de computadoras de alto rendimiento, como por ejemplo las de gobierno o de universidades.

Por lo general en los sistemas de clave pública, la mayoría de las fallas en seguridad no vienen del método de fuerza bruta sino de derivar la clave secreta de la clave pública, es decir que con una computadora potente se puede forzar un criptosistema de clave pública de un módulo de 256 bits con relativa facilidad; las universidades y gobiernos pueden forzar claves de módulos de 318 y 512 bits. (Brown, 2000)

V.1.2 Ataques de generador de números aleatorios (RNG)

Un RNG es un dispositivo que selecciona un número al azar. Los únicos números aleatorios están en la naturaleza, el hombre se apoya de un Generador de números pseudoaleatorios (PRNG) para generar números supuestamente aleatorios. El PRNG recopila la aleatoriedad supuesta desde varios flujos de entrada de baja entropía e intenta generar entradas que en la práctica no se pueden distinguir de los flujos verdaderamente aleatorios. La razón de dar una breve explicación de lo que un RNG es el hecho de que esta es común denominador en muchas funciones criptográficas, por ende si sus algoritmos no están diseñados correctamente puede ser un punto débil. Entonces también se presentan ataques RNG, estos son:

1.2.1 Ataque de entrada: Ocurren cuando el agresor puede tener conocimiento sobre la entrada de PRNG con el fin de producir algunas salidas del PRNG. Este ataque ocurre cuando las entradas son en cierta medida predecible.

1.2.2 Ataques de sincronización: Es parecido al ataque en las funciones criptográficas. Se cree que el agresor puede determinar cuando ocurren ciertas operaciones booleanas. Las adiciones referentes a los bits pueden detectarse al contar los ciclos de máquina. Después, al determinar el número total de adiciones en lo que respecta a bits y la longitud del tiempo de ejecución de máquina, el agresor puede ser capaz de predecir el número de ceros en los otros bytes, revelando información.

1.2.3 Confidencialidad adelantada perfecta: La confidencialidad adelantada perfecta es un mecanismo mediante el cual si una clave se roba en algún momento del futuro no se puede revelar ninguna comunicación que se ha conducido en el pasado. La desventaja es que si bien es una buena medida de seguridad, su implementación consume muchos recursos, ya que cada paquete requiere una clave nueva.

V.1.3 Ataques al Protocolo de seguridad de Internet (IPSec)

Antes de comenzar a estudiar los ataques a IPSec, se debe tener conocimiento de lo que es IKE (Intercambio de claves de Internet). Los principales componentes de los procesos de seguridad siempre han sido las claves. La generación, la distribución y el manejo de estas claves caen dentro de lo que se conoce como administración de claves. La creación, el intercambio y el mantenimiento de estas claves no existen en IPSec. No obstante el protocolo

de intercambio de claves de Internet (IKE) es una norma de un protocolo de administración de claves usado por IPSec. El sistemas IKE permite que IPSec ofrezca funciones tales como: Especificar un tiempo de vida útil para la asociación de seguridad IPSec, permitir que se actualicen las claves cifradas durante las sesiones IPSec, permitir que IPSec proporcione servicios contra repeticiones y permitir el soporte de la autoridad emisora de certificados. (Brown, 2000). Ahora los ataques comunes a IPSec a estudiar son los ataques de implementación, ataques de administración de claves, ataques de recuperación de claves/leyes de exportación, ataques de administrador y de comodín, además se hará un estudio de los puntos débiles de IPSec.

V1.3.1 Ataques de implantación

La norma IPSec sólo requiere de un algoritmo de cifrado (DES-CBC) y dos modos de autenticación (HMAC-MD5 y HMAC-SHA-1); sin embargo requiere los algoritmos "NULL" adicionales ya que AH o ESP pueden ser opcionales. Entonces lo que se debe interpretar es que incluso si un extremo de la comunicación utiliza DES-CBC, el otro extremo aún debería ser capaz de utilizar NULL o de no utilizar ningún algoritmo y así todavía comunicarse. El RFC de IPSec permite que tanto el cifrado como la autenticación se ajusten algoritmo NULL, pero no al mismo tiempo. En el componente IKE ambos extremos del canal de comunicaciones deciden qué tan a menudo se deben cambiar las claves de cifrado. Las claves establecidas en un principio fueron de 56 bits, lo cual pueden forzarse en 3 días.

V1.3.2 Ataques de administración de claves

Según expone Brown este ataque es un problema relacionado al protocolo IKE, particularmente en el manejo de claves criptográficas en IPSec. Puntualmente el protocolo IKE determina como deberían intercambiarse las claves, pero generalmente se refiere al inicio de la comunicación y no al final de ella. Bajo la especificación IKE, cualquiera de las dos partes podría

terminar una sesión, pero no hay forma de que el otro extremo sepa que la sesión se ha terminado; el extremo emisor seguirá enviando datos (Brown, 2000).

V.1.4 Ataques de Protocolo de establecimiento de túneles punto a punto (PPTP)

Según Brown la VPN de PPTP está formada por varios componentes y de manera similar a IPSec, PPTP es un marco de referencia. Y no se le exige algoritmos de cifrado y autenticación, esto se deja a los otros protocolos, como PAP, CHAP y MS-CHAP. Los protocolos involucrados aquí son: GRE (protocolo de encapsulamiento de enrutamiento genérico), PPP es un protocolo de red punto a punto utilizado para proporcionar servicios de conexiones TCP/IP sobre líneas de conexión serial, PPTP que utiliza GRE para establecer un túnel PPP y añade una instalación de conexiones y un protocolo de control, MS-CHAP es la versión de microsoft® de CHAP y es responsable de autenticación de respuesta de pruebas y por último MPPE que es un protocolo de cifrado punto a punto de Microsoft y es el encargado de generar una clave y cifrar las sesión (Brown, 2000).

Un punto vulnerable de PPTP es que se basa en PPP, es decir que antes de cualquier comunicación dicho protocolo, establece e inicializa los parámetros de comunicación y debido a que no tiene autenticación contra estos paquetes, pueden ocurrir ataques como los de intermediario y de falsificación.

Los ataques clásicos para PPTP son ataques al GRE.

Ataques al GRE: Los paquetes, como se dijo anteriormente, se encapsulan dentro de un GRE y se envían por los túneles a través de IP hacia su destino. Los paquetes GRE pueden transportar un número de secuencia y un número de reconocimiento y pueden utilizar una ventana deslizable para evitar la congestión. Esto significa que si se desea probar los paquetes PP encapsulado

en GRE, simplemente se necesita desincronizar el canal de GRE. Esto se puede evitar con el número de secuencia. El GRE no tiene forma de que el anfitrión final reaccione ante un número de secuencia duplicado o erróneo.

Otro ataque que se puede dar en el establecimiento de VPN, es a la autoridad emisora de certificados (CA), debido a que una CA no es diferente a cualquier otro dispositivo de terceras partes validadas. Si existe un ataque a una CA, los agresores pueden hacerse pasar por quien desea unir cualquier clave de su elección al nombre de otro usuario, y utilizar a la CA para verificarla. Sólo se requiere una CA insegura para comprometer a la cadena entera, a continuación se pasará a describir de manera teórica la manera en que una autoridad emisora de certificados podría ser atacada estos son, entre otros, ataques de sello fechado, ataque de hardware y ataques débiles.

- Ataques de sello fechado: Este ataque es provocado por la carencia de un sello fechado en un certificado. Si el atacante es capaz de comprometer la clave de un certificado, pero la CA ya no usa esa clave. El atacante podría crear una clave, firmar con la clave pública de alguien más, generar una clave de CA de certificado comprometida y ponerle una fecha anterior a algún momento en el pasado cuando el certificado era válido. Para protegerse contra esto, se insertan sellos en el certificado que indican cuando se hizo válido.

- Ataque de hardware: Si un atacante puede tener acceso al dispositivo en el cual reside la CA, su clave privada puede descubrirse mediante ingeniería inversa , es decir obtener dicha clave a partir de los certificados que emite para determinar cómo las hace, sobre el dispositivo. Entonces al momento de comprometer la CA, también se compromete cada certificado. Cabe acotar aquí que existen muchas diferencias en las medidas de protección de cada SA.

- Ataques débiles: La CA debe conocer la identidad de aquel que solicita la certificación; toda CA que sea confiable debe tener precauciones con la siguiente situación: Supóngase que se solicita una un certificado con una clave pública, la CA no sabe a quién se la está emitiendo, por ende una persona puede suplantar la identidad de otra. Entonces se puede crear un certificado falsificado con el nombre alguien más y hacer ataques en nombre de esta persona. Para evitar este ataque muchas CA necesitan de dos o más personas para generar certificados, deben tomar medidas para detener este tipo de ataque.

Con la finalidad de seguir conociendo las vulnerabilidades, se encontraron algunas en las VPN de usuario y las VPN de sitio las cuales se pasarán a describir seguidamente empezando por el despliegue de VPN de usuario.

V.1.5 VPN de usuario

En este tipo de despliegue existen cuestiones de implementación y riesgos de seguridad significativos con los que hay que lidiar. La cuestión de seguridad más grande, tratándose de este tipo de implementación es la conexión simultánea con otros sitios de internet. Si la computadora ha sido comprometida con un caballo de troya, puede ser posible que algún usuario externo no autorizado utilice la computadora del empleado para conectarse a la red interna. Para entender esto de manera gráfica ver la ilustración 18.

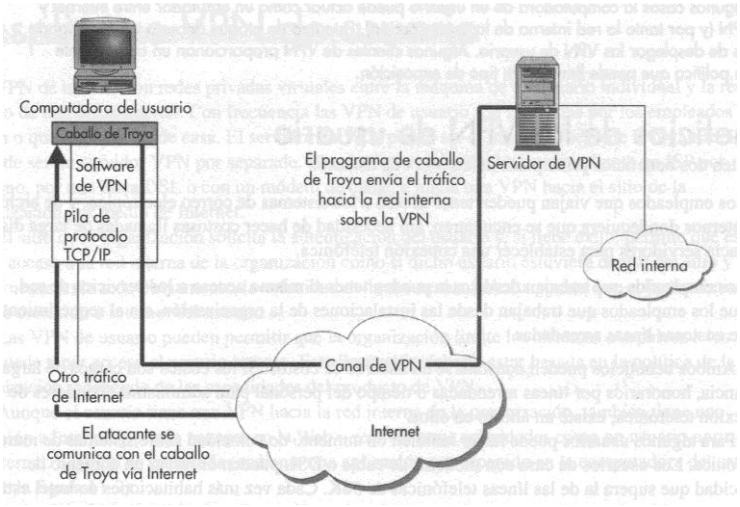


Ilustración 18 Uso de un troyano para tener acceso a la red interna. Fuente: (Maiwald, 2005)

V.1.6 VPN de sitio

En este caso si la seguridad en el sitio remoto es débil, la VPN puede permitir que un intruso obtenga acceso al sitio central o a otras partes de la red interna. Es un ataque similar al despliegue de VPN de usuario.

No se efectúan todos los ataques teóricos dado a que no se va implementar una VPN en la red de internet, como es el caso de los ataques débiles, además de que algunos requieren de software y hardware muy especializado.

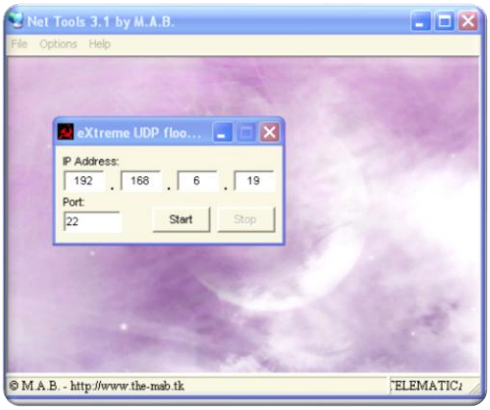
Otro resultado obtenido de la investigación fue la conclusión de Rik Farrow ya que según él una VPN puede ser un camino por el cual un atacante puede acceder a una red interna. En la actualidad existen muchos troyanos (uno de ellos es SubSeven) para Windows que pueden lograr este objetivo, se puede lograr un ataque desde internet a través del servidor de seguridad mediante el túnel VPN; el atacante puede configurar el troyano para que pueda transmitir el tráfico a través del sistema remoto. Dicho tráfico tiene la misma dirección IP de origen como el sistema remoto, utilizando el mismo túnel VPN. También acota que las VPN no protegen al servidor web de ataques y tampoco a la red interna.

Se va proceder a estudiar los ataques de manera práctica, se clasificaran de acuerdo a lo que hacen, los ataque encontrados son de DOS, de *sniffer*, y de diccionario, este último se descartó para ataques prácticos.

V.1.7 Ataques de DOS

Los ataques de Denegación de Servicio aplicables para las experiencias son:

- Net Tools (UDP flood): Este ataque consiste en inundar un puerto con paquetes UDP, para lograr saturar el puerto con flujo de información haciendo que se sobrecargue y no pueda prestar el servicio.



- UDP Flooder 2.00: Al igual que el anterior ataque descrito, permite enviar mucho flujo de informacion a un puerto especifico; una de las caracteristicas principales de este software es el control de transmision que permite escoger el tiempo de duracion del ataque, la cantidad de paquetes que se envían y la velocidad de transmision de estos en paquetes sobre segundos. Además nos permite controlar la data que se envía al puerto como mandar texto plano o de un archivo en especifico y por ultimo escoger el tamaño de los paquetes que se envían en un rango escogido. Este software permite visualizar cuantos paquetes se envian y el tiempo transcurrido del ataque.

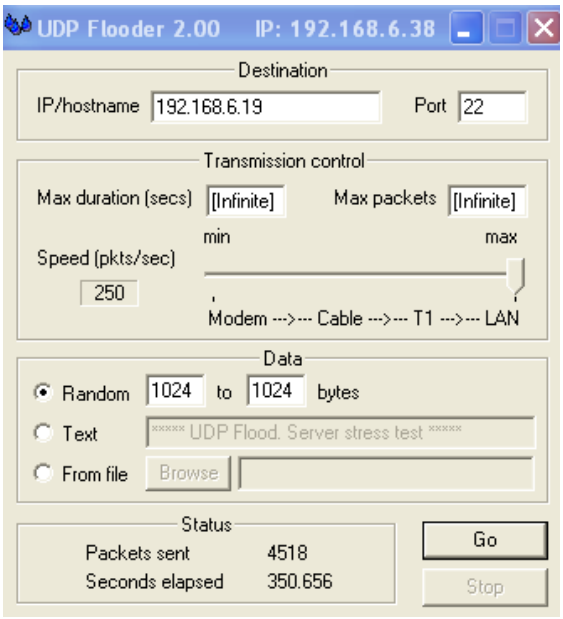


Ilustración 20 Software de Ataque UDP Flooder

- Divine Intervention: Es un programa que contiene varios ataques, se probaron todos los que ofrecia pero fue escogido FLOODz, debido a que si afecta el rendimiento de la VPN gracias a que permite escoger el tamaño del paquete ICMP, ahora bien un ataque comun con paquetes ICMP no afecta el rendimiento de la VPN, no obstante, este programa permite aumentar la cantidad de hilos del ataque ICMP esto lo hace muy eficaz. La cantidad maxima de hilos que ofrece es de 50 y el tamaño de los paquetes 32767 bytes obligando fragmentar el paquete para su procesamiento.

Ilustración 21 Interfaz Divine Intervention

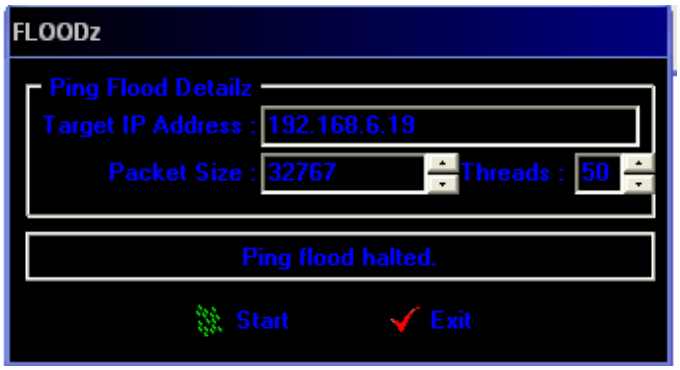


Ilustración 22 Interfaz Plaguez Floodz

- SuperKod v 1.0: Envía paquetes IGMP para que la máquina, lleve su rendimiento al máximo y niegue al servicio.
- Reset: Envía comandos a una máquina para que se reinicie.
- Sequito de Ataque: Es un programa que dispone de varias utilidades para distintos tipos de ataque de DOS.
- CISCO Bomb V.6: Es un programa DOS que envía paquetes a un puerto hasta tirar la conexión.

V.1.8 Sniffers

- Spynet: Este programa espía puertos de internet e intercepta claves y nombres de usuarios. Dispone de dos herramientas CaptureNet (Captura los datos) y PeepNet (Interpretación de los datos capturados).

V.1.9 Varios

Lestat: Es una herramienta para el análisis estadístico de frecuencia literal en el descifrado del texto encriptado

También en la investigación se encontró un programa que ofrece una posible defensa contra aquellos ataques hacia algoritmos criptográficos específicamente en uno de solo texto cifrado:

- Anti Sniff v1.0: Es un programa que permite protegerse de los *sniffers*.

V.2 Fase III: Estudiar que herramientas se utilizarán para medir los parámetros de la VPN.

Al implementar la Honeynet, se consiguió en la página principal que el software de captura de datos estaba obsoleto, es decir requería un condigo MD5 para activarse pero al momento de buscar dicho código el servidor no lo tenía. Por esto y por las razones expuestas en el capítulo III se descartó el uso de esta herramienta.

Por recomendación del tutor y tras analizar los resultados obtenidos de las anteriores fases se determinó que lo mejor para estudiar las VPN es la utilización un *sniffer* y un IDS, para analizar el tráfico. El IDS escogido fue SAX2®, por proveer de una buena base de datos de ataques en modo de versión de prueba. Mientras el *sniffer* elegido como analizador de protocolos fue Wireshark®debido que ya se tiene experiencia en la manipulación de este *sniffer*, y es reconocido como uno de los analizadores de red más recomendados en el área de Sistemas. Para la primera experiencia con el fin de "husmear" en los paquetes se utilizará un HUB como se dijo anteriormente, conectando la máquina con el Wireshark® instalado en ese dispositivo de red, esto para evitar colocar la tarjeta de red de la máquina en modo promiscuo y el puerto de un *switch* en modo espejo, gracias a las características del HUB esto facilitara e trabajo de observación. Siguiendo lo expresado anteriormente

Wireshark® es una herramienta que permitirá ver el flujo de datos consecuencia de los protocolos que usa la VPN, y de allí inferir si fue comprometida su integridad, además de permitir analizar fallos en la red, de allí la razón de su uso.

A parte del HUB, otras herramientas utilizadas son 4 PCs, dos para formar los extremos de la VPN, otra donde se instalará el Wireshark® y otra de donde implantará los ataques prácticos.

V.3 Fase IV: Instalar la red de prueba

Al utilizar los recursos descritos anteriormente para conformar una red de prueba, esta se implementó sin ningún contratiempo. Dando como resultado tres redes de prueba diferenciadas por su topología, que serán capaces de analizar todo lo que ocurre en la red. Estando la primera compuesta por computadores unidos a un *hub* utilizando IPs estáticas, sin ningún servicio de red adicional, mientras las otras redes de prueba se encuentran dentro de la topología de red de la UCAB descrita más adelante, que les proporciona conexión a Internet.

La arquitectura de red de la UCAB, sigue una topología del tipo árbol y de acuerdo a la información dada por el personal de la UCAB se tiene lo descrito en la ilustración 23.

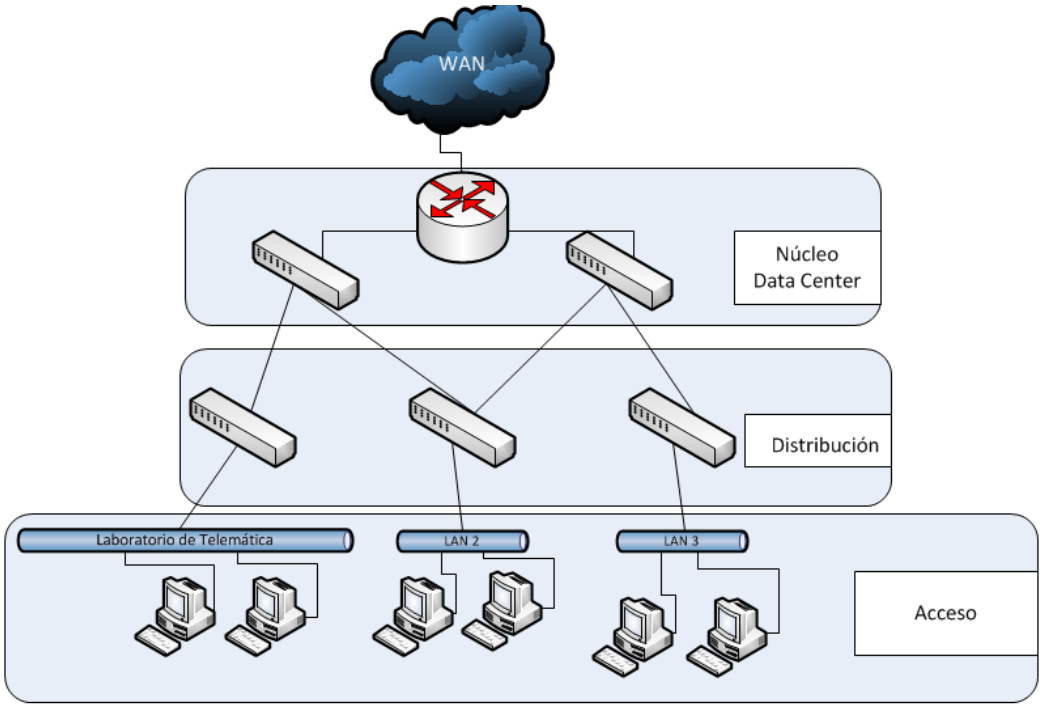


Ilustración 23 Topología de Red UCAB

En la ilustración 24 se observa la LAN del experimento dos sobre Debian®OS, donde la línea verde indica la conexión VPN en la LAN, estando dicha red conectada a un Switch de acceso con una puerta de enlace predeterminada 192.168.6.1, al igual que en el experimento tres de VPN IPSec mostrado en la ilustración 25.

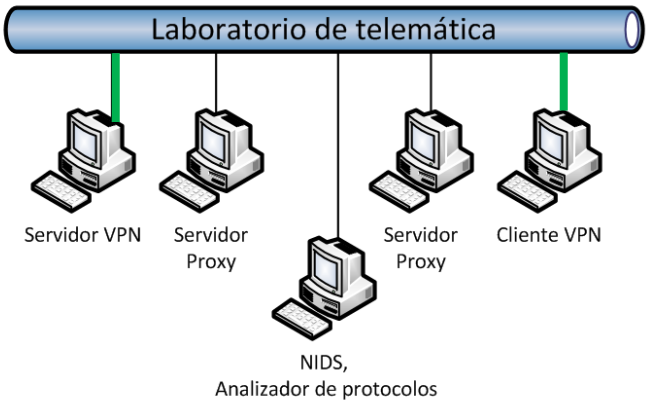


Ilustración 24 topología de red, protocolo SSH. VPN de Sitio

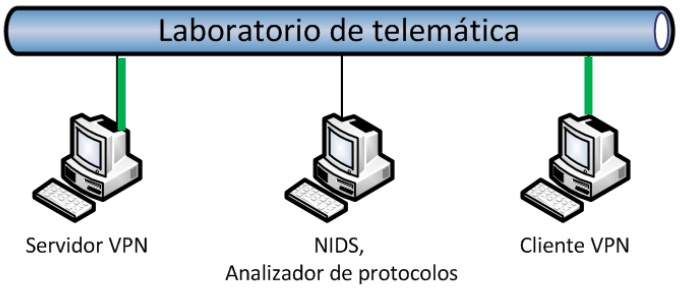


Ilustración 25 Topología de red, protocolo IPSec. VPN punto a punto

A continuación se presentan todas las especificaciones técnicas de la red de pruebas, de acuerdo a lo implantado en la red y a lo que se logró capturar en el analizador de protocolos.

1 Hardware de la LAN

1.1 Adaptadores de red

Es una interface hardware entre la plataforma o sistema informático y el medio de trasmisión físico por el que transporta la información de un lugar a otro.

1.2 Servidores de red

Son nodos de la red especializados en brindar servicios al resto de los nodos de la red. Entre los servicios que hicieron vida en la red de prueba son los servidores VPN para los protocolos SSH, PPTP e IPSec, además de los servidores proxy.

2 Software de la LAN

2.1 Controladores de los adaptadores de red

Los adaptadores de red necesitan de un software controlador que conduzca sus operaciones desde el sistema operativo. Estos controladores en el caso de esta red conducen sus operaciones desde los sistemas operativos *Windows XP* y *Debian.*

2.2 Sistemas de redes cliente / servidor

Algunos nodos de red tienen definidas funciones de cliente y servidor, esto se debe a que los clientes VPN se conectan a un servidor VPN. De igual manera el proxy squid hace funciones de servidor y las máquinas de los usuarios de clientes.

2.3 Sistemas operativos

Windows XP OS, Debian OS, CISCO OS.

3 Protocolos de redes

3.1 Familia de protocolos TCP/IP

El énfasis de esta descripción está dirigida a en los del tipo IP en el nivel de red y el protocolo TCP en la capa de transporte, debido a que estos fueron los protocolos predominantes en la red de prueba.

3.1.1 Protocolo IP

IP (*Internet Protocol*) es el protocolo de nivel de res de ARPANET, el sistema de comunicaciones utilizado en sistemas UNIX. Es un protocolo no orientado a conexión que carece de seguridad en la entrega de paquetes. IP fue diseñado para conducir paquetes a través de distintas redes interconectadas.

3.1.2 Protocolo DHCP

Este protocolo ayuda al administrador a automatizar las asignaciones de las direcciones IP. El servidor DHCP asigna una dirección IP a cada nodo que lo solicita. Este protocolo hizo vida en la red de prueba para asignar las direcciones IP de los hosts cuando se levantó la VPN.

3.1.3 Protocolo TCP

TCP (*Transmition Control Protocol*) fue diseñado para realizar conexiones en redes inseguras, es un protocolo de capa de transporte adecuado para interactuar contra el protocolo IP en el nivel de red. Dicho protocolo fue detectado en el analizador de protocolos, claramente debido a que este es el que controla la comunicación en la red LAN del laboratorio de telemática.

3.2 UDP (*User Datagram Protocol*)

UDP no admite numeración de los datagramas, este protocolo es utilizado cuando el orden en que se reciben los mismos no es un factor fundamental, o también cuando se requiere enviar información de poco tamaño que cabe en un único datagrama. Este protocolo hace su papel dado a que en la red de pruebas al momento de levantar la VPN con el protocolo IPSec, la comunicación se realiza a través de este. Además se realizó dos ataques de inundación de paquetes UDP.

3.3 Protocolo ICMP

Protocolo de mensajes de control de internet es de características similares al UDP. Es un protocolo que encapsula en un único paquete IP algún

evento que se produce en la red. En la red de pruebas se utiliza este protocolo para verificar la conexión entre dos hosts y además se realizó un ataque enviando paquetes ICMP más grandes de lo habitual para saturar la red de paquetes fragmentados.

3.4 ARP (*Address Resolution Protocol*)

ARP es el protocolo encargado de realizar las conversiones de direcciones correspondientes (direcciones MAC y direcciones IP) a cada host. Este protocolo es parte fundamental para el encaminamiento de los paquetes, se puede notar su efecto en la red gracias al NIDS.

3.5 Routing

Es el proceso que permite a los paquetes llegar a su destino final. La red LAN sigue la tecnología *Ethernet* y protocolos de internet TCP/IP. Las tareas de *routing* son implantadas por el protocolo IP sin que los protocolos de nivel superior tengan constancia de ello. Cuando se requiere enviar información a un ordenador, el protocolo IP comprueba si el ordenador de destino se encuentra en la misma red local que el ordenador origen. Si es así se envía el datagrama de forma directa, la cabecera IP contendrá el valor de la dirección Internet del ordenador destino y la cabecera *Ethernet* contendrá el valor de la dirección de la red *Ethernet* que corresponde a este mismo ordenador. Este es el caso de la red de pruebas, no hizo falta un enrutador para encaminar los datos de la VPN, todo el tráfico de enrutamiento fue trabajo del protocolo IP y no de ningún protocolo de enrutamiento.

3.6 Sistema de nombres por dominio

DNS (*Domain Name System*) es una forma alternativa de identificar una maquina conectada a Internet. Este protocolo es utilizado para referirse a un ordenador en la red, además de proporcionar una idea del propósito y localización del mismo. En la captura del analizador de protocolos se observan todos los DNS utilizados por los hosts.

4 Protocolos detectados en la red de pruebas

4.1 Inter Switch Link (ISL)

Es un protocolo propietario de CISCO que mantiene información sobre VLANs en el tráfico entre *routers* y *switches.* Debido al uso de VPN y a la existencia de enrutadores CISCO en la red de la UCAB, este protocolo está presente en la red de pruebas.

4.2 Dynamic Trunk Protocol

Es un protocolo propietario de CISCO que opera entre *switches* CISCO, el cual automatiza la configuración de *trunking* (etiquetado de tramas de diferentes VLANs con ISL) en enlaces *Ethernet.* El origen mostrado es de un *switch* Cisco_2f:16:82, como sucede con el ISL se hace presente en la red de pruebas bajo las mismas condiciones.

4.3 Spanning Tree Protocol

La fuente de este protocolo es del mismo *Switch* CISCO detectado en DTP, este protocolo tiene como función la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. Debido a los enlaces redundantes observados en la ilustración 22 este protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma de garantizar la eliminación de bucles.

4.4 Online Certificate Status Protocol

Es un método para determinar el estado de revocación de un certificado digital. Este protocolo hace su aparición dado a que se implanta en VPN de administración de claves públicas, utilizada por los servidores VPN.

V.3 Fase V: Instalar la VPN en la red.

Se instaló diferentes VPNs para realizar las pruebas pertinentes lo más completo posible. De esta manera se montó una VPN con protocolo PPTP en Windows® O.S., una VPN con protocolo SSH en Debian® O.S. y por ultimo una VPN con protocolo L2TP/IPSec en Windows®.

V.4 Fase VI: Hacer pruebas pertinentes

Como se expuso en el desarrollo se realiza diferentes pruebas experimentales con el fin de probar la vulnerabilidad de una VPN de forma práctica con la generación de una red de prueba con una conexión VPN. La cual es atacada por algunos de los ataques documentados anteriormente, mientras todo el tráfico de datos de las interfaces relevantes es capturado por un NIDS ($SAX2$®) y un analizador de protocolos (Wireshark®).

V.4.1 Experimento 1: Análisis en Ambiente Windows VPN (PPTP)

Esta experiencia se realizó con el fin de estudiar completamente las características de los ataques, debido a la naturaleza maliciosa de estas, hay que estar seguros de que solamente hacen lo que deben hacer y no otras cosas como instalar un troyano en la PC que los descarga.

Antes de hacer las experiencias de prueba con IPSec y SSH, se montó una red de prueba en respuesta a lo expuesto en el apartado anterior, cabe destacar que esta red se hizo con un HUB para leer todo el tráfico y además es una red que se desenvuelve en un entorno cerrado dado como resultado una red aislada de la red de la UCAB, por último los ataques se descargaron en una máquina virtual para dar la protección máxima a la red, dando como resultado lo explicado seguidamente.

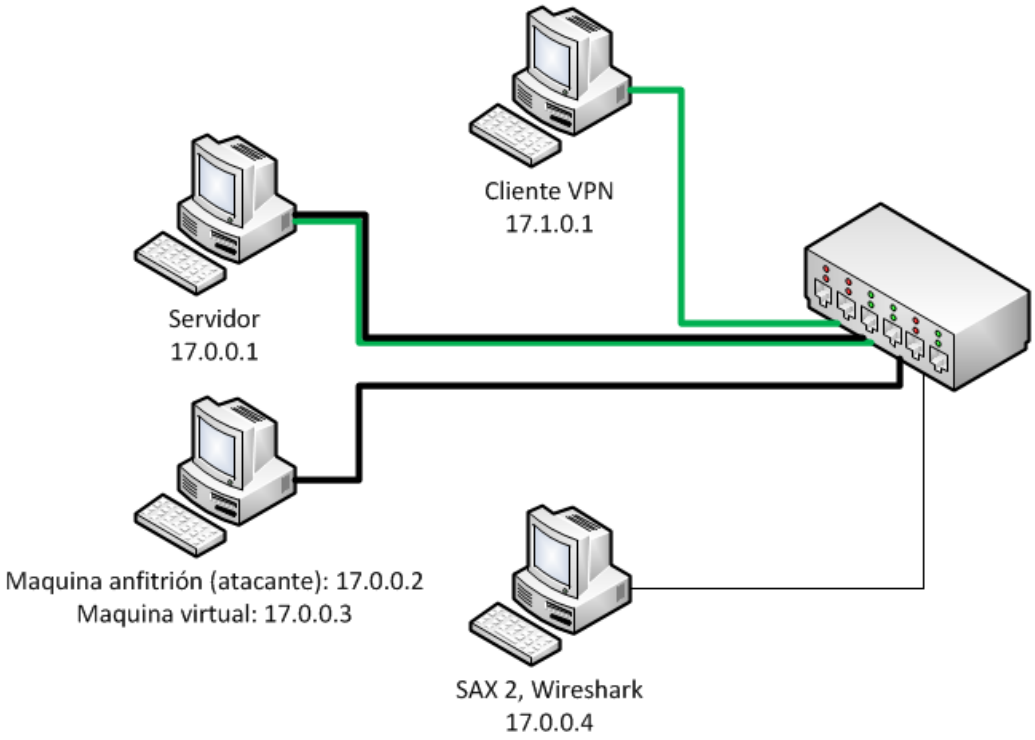


Ilustración 26 Red de prueba PPTP

La línea oscura muestra el recorrido de los ataques, y la otra muestra la conexión VPN. Cabe acotar que las direcciones IP cambian debido a que esta experiencia se realizó varias veces para obtener los mejores resultados.

Las vulnerabilidades de PPTP se presenta debido a que durante el proceso de autenticación PPP (MS-CHAP v2) no ofrece ninguna garantía de cifrado, esto abre la posibilidad de un ataque de hombre en el medio (MITM) *Man In The Middle*.

El ataque se realiza mediante una aplicación llamada *aeslap* y *Ettercap*, existe un programa llamado *Backtrack* que contiene ambas aplicaciones. El proceso de autenticación de MS-CHAP v2, la manera en que se ejecuta el ataque y las experiencias prácticas que se hizo con PPTP en el laboratorio está en el anexo del CD.

V.4.2 Experimento 2: Análisis en Ambiente Debian VPN (SSH)

Como se explicó en la fase IV, se ensamblan dos redes LAN separas por sus *proxys*, que se unirán mediante VPN, con el fin de simular la aplicación de una VPN de sitio usada habitualmente para unir redes de sucursales de instituciones. De esta manera se realizan las pruebas con una VPN con protocolo SSH en el ambiente Debian® O.S, teniendo la topología que se observa en la ilustración 27.

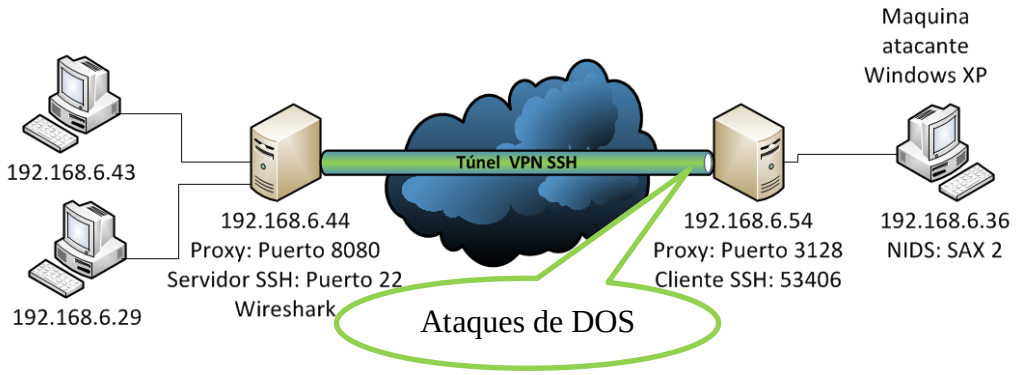


Ilustración 27 Red de prueba, ambiente SSH

Como se puede notar en la ilustración, el ataque consiste en mandar un ataque de DOS desde una maquina con Windows®O.S a través del proxy donde se ubica el cliente SSH pasando por la VPN hasta llegar al otro proxy del servidor SSH. La idea de esta prueba es ejecutar un ataque de DOS mientras esta activo el servicio SFTP (*SSH File Transfer Protocol*). Para medir el desempeño de la VPN, se utilizó adicionalmente el perfilador *Pipe Viewer* para observar el rendimiento del túnel, en lo referente a velocidad de transferencia y flujo de datos. Mientras lo expuesto anteriormente se desarrolla, se utilizó un NIDS para observar el desempeño de la red, además de Wireshark® para analizar mediante la captura de paquetes los ataques y el rendimiento de la VPN. La manera en que se conectó la VPN con el protocolo SSH y la manera en la que se configuró el proxy están en el anexo del CD.

A continuación se presenta los resultados en el siguiente orden: Análisis de los paquetes de los distintos elementos que conforman el estudio es decir el Perfilador *(Pipe Viewer*) y los ataques. Y segundo se presentaran los resultados del NIDS, cabe acotar que por cuestiones de tiempo la duración de los ataques fueron de varios minutos, aun así es suficiente para dar un estudio acertado, luego se dejó correr el estudio 20 min para complementar el estudio.

V.4.1.1 Análisis de Wireshark (Perfilador)

Se puede observar en la ilustración 28 los paquetes que utiliza el *Pipe Viewer* para estimar la velocidad de túnel, este utiliza el RTT *Round Trip Time* (tiempo de ida y vuelta) de un paquete enviado por el cliente para tal fin. IP servidor: 192.168.6.18, IP cliente: 192.168.6.39.

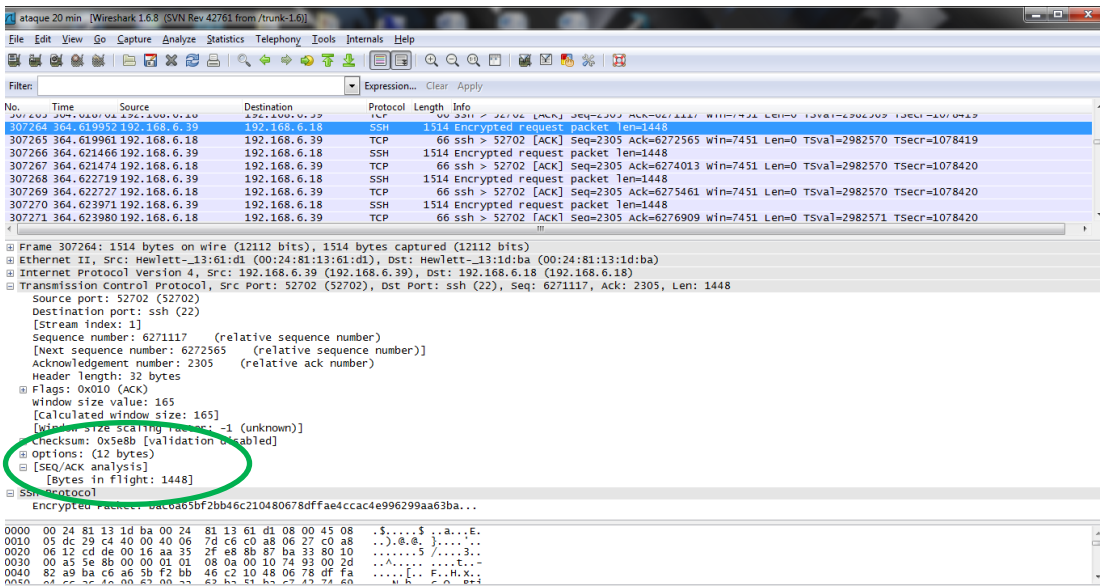


Ilustración 28 Paquete del cliente al Servidor (Pipe Viewer)

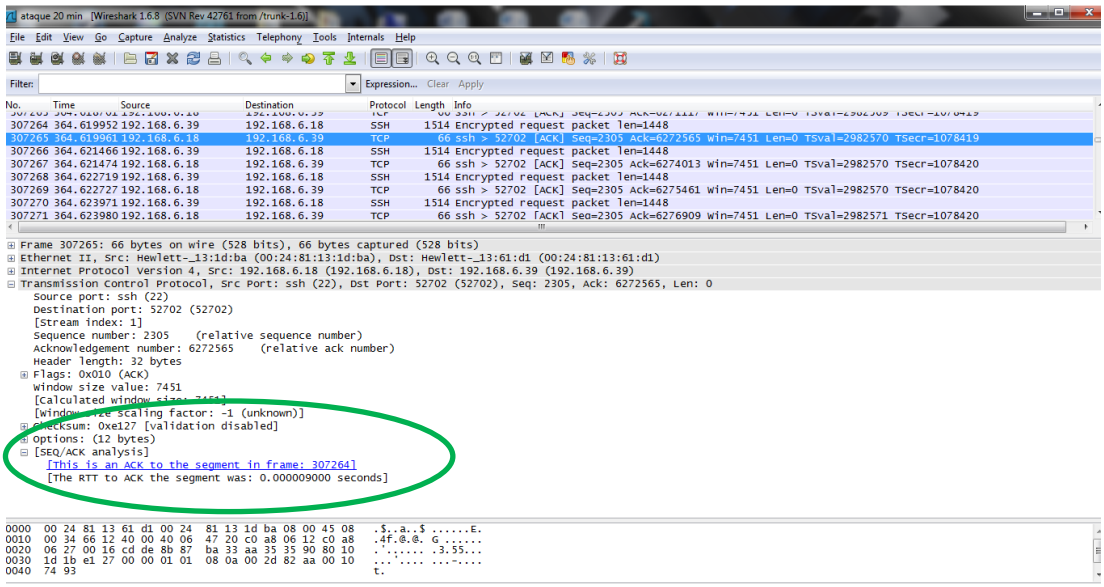


Ilustración 29 Paquete de respuesta del servidor al cliente (Pipe Viewer)

V.4.1.2 Análisis de Wireshark (Ataques)

La ilustración 30 muestra un paquete correspondiente al ataque correspondiente al programa Extreme UDP flooder

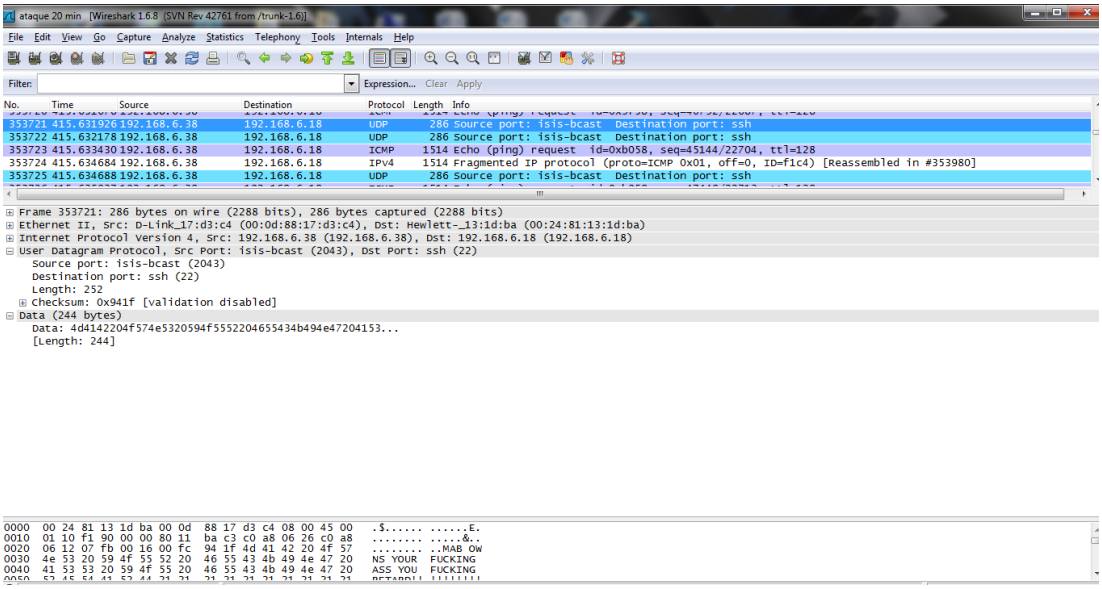


Ilustración 30 Paquete UDP (Extreme UDP flooder)

Ahora se muestra un paquete de UDP flooder 2.0

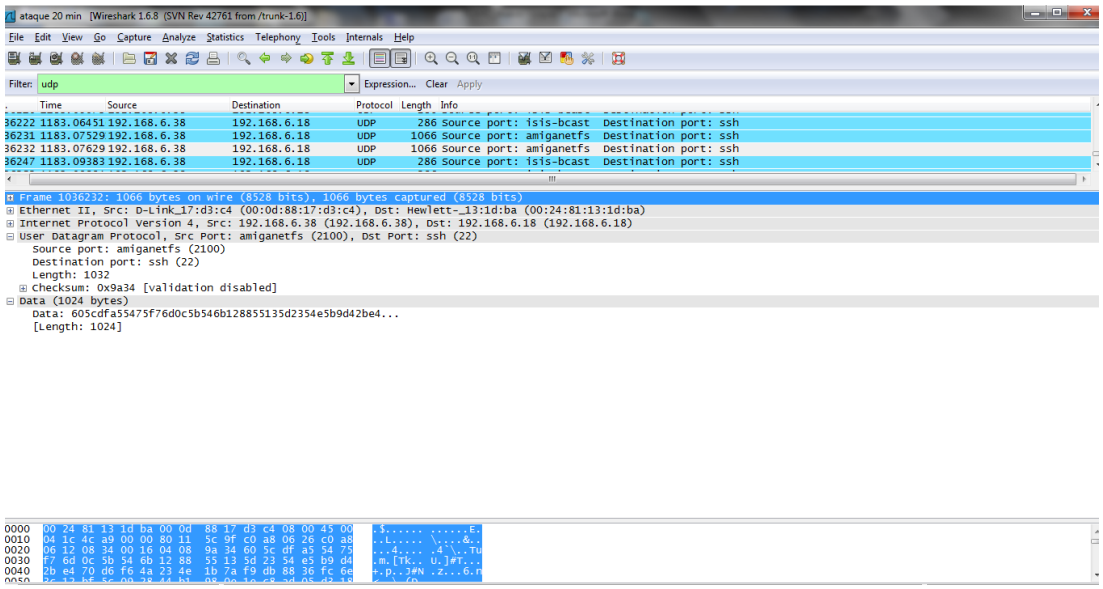


Ilustración 31 Paquete UDP (UDP flooder 2.0)

Ahora se muestra ilustración 32 un ataque correspondiente a FLOODz, este ataque utiliza el protocolo ICMP mandando paquetes muy grandes para procesar en la red (32767 bytes), obligando a fragmentar los paquetes e inundar la red con paquetes fragmentados.

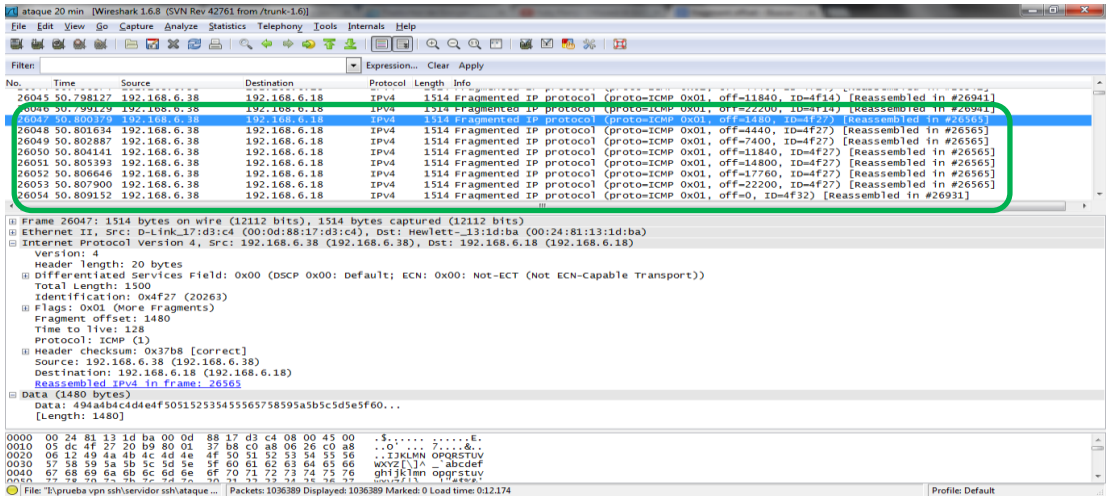


Ilustración 32 Paquetes fragmentados. Ataque de FLOODz.

En la muestra observada en la ilustración 32 se pueden observar la IP de la maquina fuente (192.168.6.38) y la IP destino (192.168.6.18) correspondiente al servidor SSH, la longitud del paquete es de 1514 (el máximo permitido en la red) y se puede notar el ID del paquete, como es el caso del paquete cuyo ID es 4f27, el cual posee el *fragment offset* activo y se muestra que en la línea número 26565, será reemsamblado dando como resultado el *ping* de respuesta, hay que recordar que el ataque consiste en un paquete ICMP de gran tamaño. Y así como existe este paquete existen más paquetes que serán fragmentados y reemsamblados, dando como resultado una inundación de paquetes fragmentados en la red, afectando el rendimiento de la VPN en lo referente a velocidad de transferencia de datos.

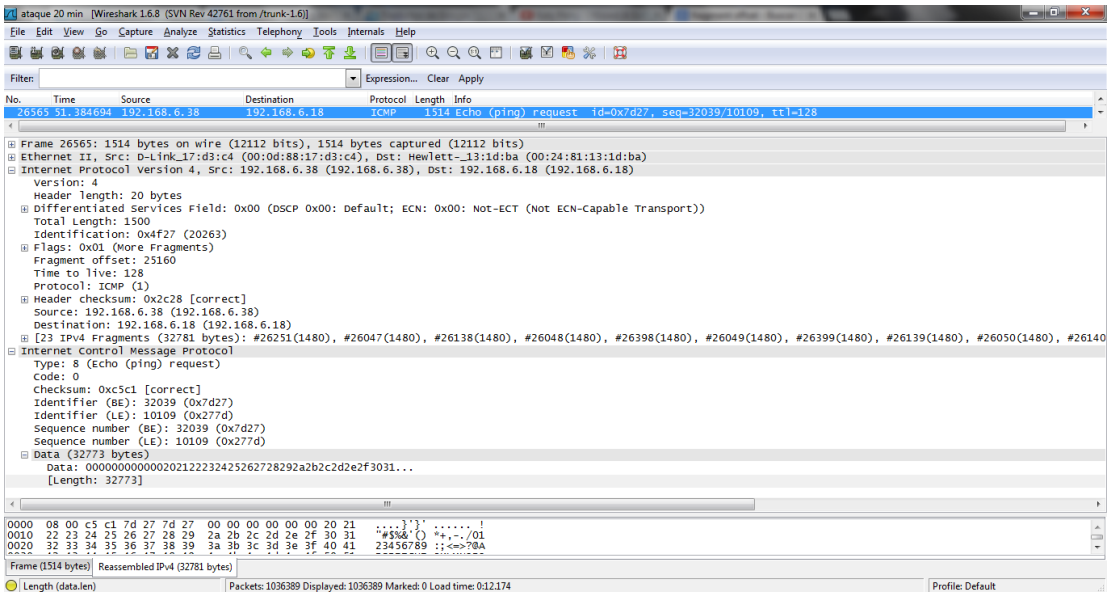


Ilustración 33 Paquete de respuesta

Ahora se dará un análisis de NIDS, en esta oportunidad, debido a que en la primera oportunidad el NIDS se colgó y por cuestiones de tiempo, se probó nuevamente los ataques pero las direcciones IP de todos los componentes cambiaron debido a la

configuración de las direcciones IP (DHCP). El funcionamiento de la red y su arquitectura es exactamente igual que la experiencia anterior.

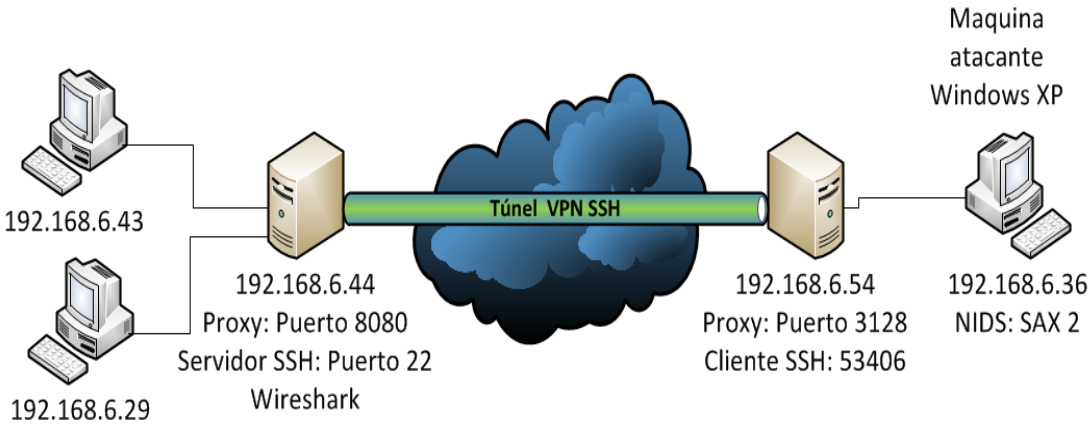


Ilustración 34 Red NIDS

V.4.1.3 Resultados del perfilador

Primero se muestra al perfilador, solo con SFTP activo, sin el *sniffer*, sin el NIDS y sin los ataques activados, mostrando lo destacado en la ilustración 35:

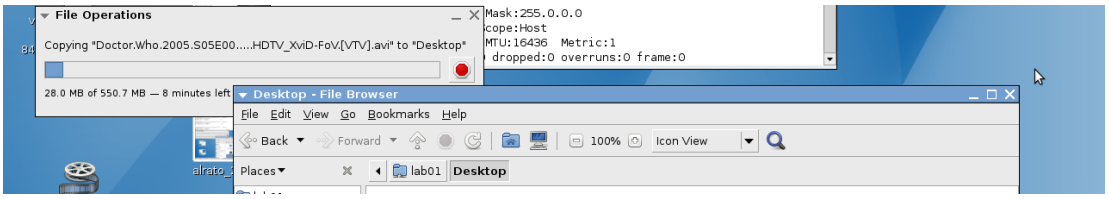


Ilustración 35 SFTP sin ninguna otra herramienta activa

Se observa que el archivo se terminará de transferir en aproximadamente 8 minutos.

Seguidamente se puede observar en la ilustración 36, el SFTP y el perfilador en acción, se puede observar que dado a la acción de este sobre el canal, el archivo extiende su descarga a 1 hora y 24 minutos aproximadamente pero la capacidad del canal no se ve afectada.

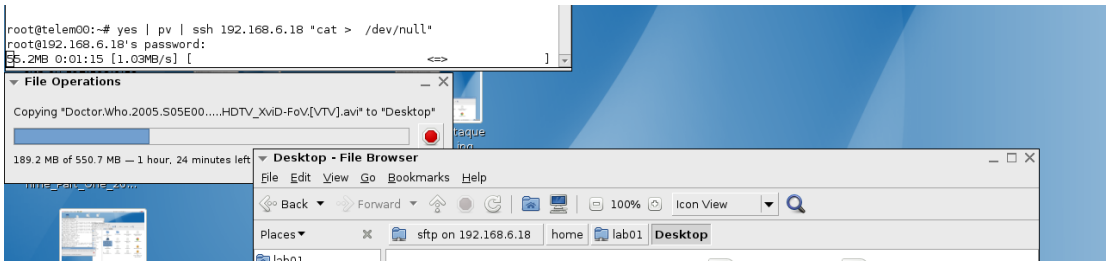


Ilustración 36 SFTP y perfilador activo

Ahora se muestra en la ilustración 37 el SFTP con el perfilador y el *sniffer* activos y se puede notar que gracias a la acción de estas dos herramientas, el tiempo de descarga del archivo se elevó a 14 horas aproximadamente.

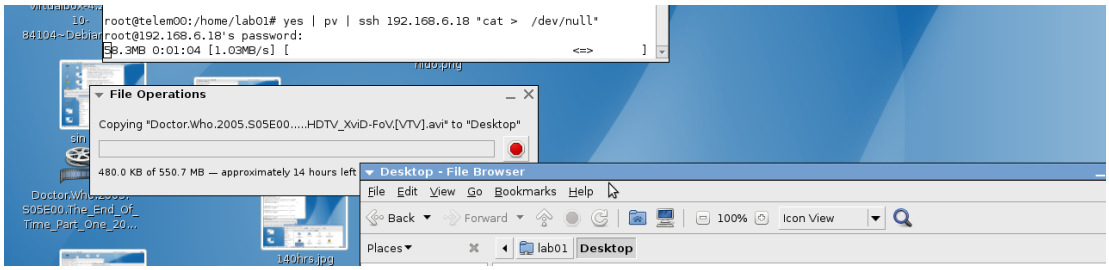


Ilustración 37 SFTP con el perfilador y el sniffer en funcionamiento

Por último se hizo el experimento con el *sniffer*, el perfilador, el SFTP y los ataques activos mostrando lo siguiente:

A los tres minutos de iniciar el ataque, se observa en la ilustración 38 que el tiempo de descarga aumenta a 28 horas,

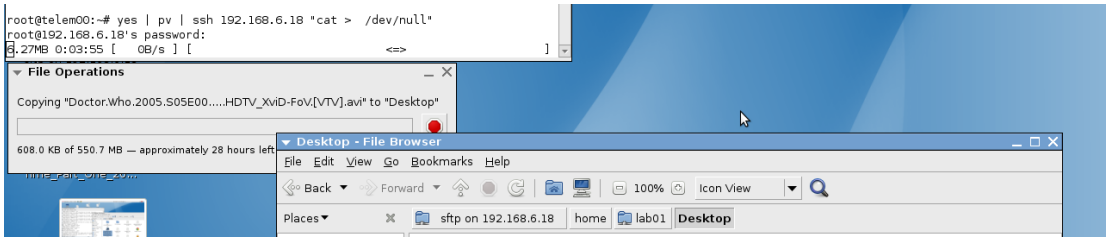


Ilustración 38 Tres minutos de ataque

En la ilustración 39, a los once minutos de ataque el tiempo asciende a 140 horas, durante este tiempo el perfilador mostró en algunas ocasiones ciertas velocidades de transferencia pero eran demasiado esporádicas y no duraban más de un segundo mostrada en pantalla.

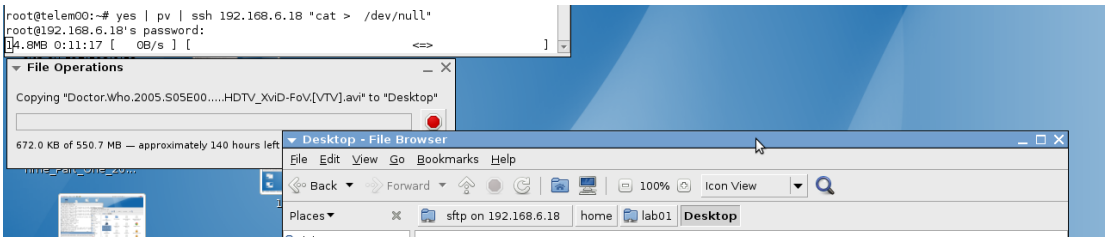


Ilustración 39 Once minutos de ataque

Se dejó continuar el ataque aproximadamente diez minutos más y se observa que el tiempo de descarga se mantiene en 140 horas, además que la velocidad de transferencia de la VPN es de 0B/s. Con esto se da como resultado, el ataque de DOS completado, observar la ilustración 40.

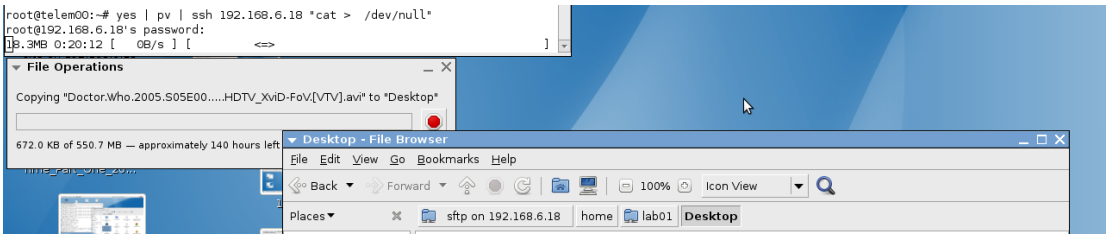


Ilustración 40 Ataque DOS exitoso

V.4.1.4 Resultados del NIDS.

En la ilustración 41 se observa una gráfica de curva de eventos y tráfico, donde en la primera se observa un aumento significativo de la curva durante el tiempo que dura el ataque y al finalizar, mostrando el decrecimiento en la curva de eventos. En la siguiente grafica se tiene que antes de iniciar el ataque se tenía una trafico promedio de 1500 Bytes/segundo en el eje vertical y las 12:22, momento en que se inicia el ataque el tráfico se eleva a una tasa de 1.181.206 Bytes/segundo. Cabe destacar que luego de detener el ataque aproximadamente a las 12:23 la curva de eventos comienza a decrecer y la curva de tráfico muestra que a pesar de que se detuvo el ataque aun la red está inundada de paquetes que quieren llegar a su destino, es decir que aun trasciende los efectos del ataque.

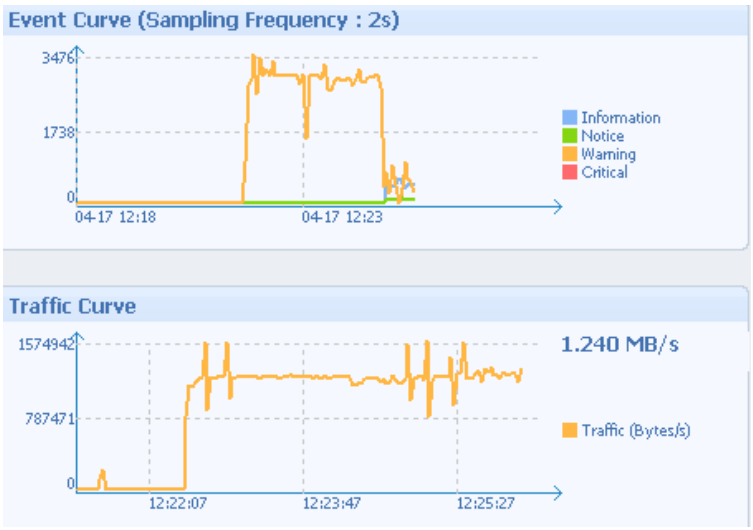


Ilustración 41

A diferencia de la experiencia anterior se dejó el ataque un periodo, más prolongado, para tener un estudio más asertivo de los eventos mostrados en NIDS. Ver figura 42.

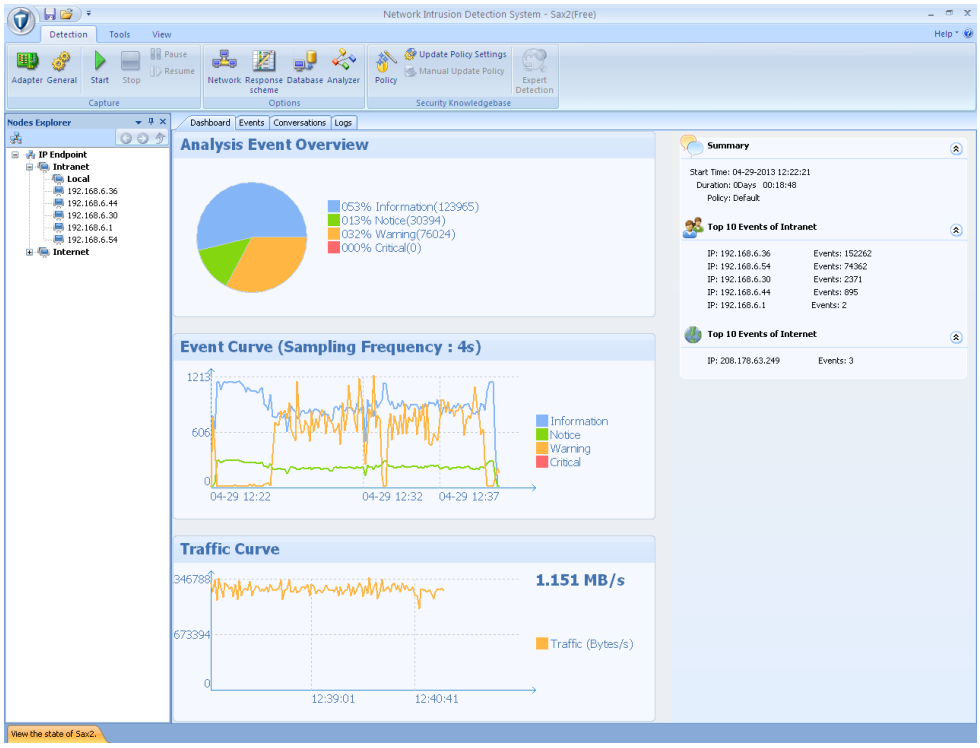


Ilustración 42 Ataque DOS prolongado

A continuación se presentan los eventos del detectados por el NIDS, *SAX2*®, que clasifica los eventos en 4 (*Information, Notice, Warning y Critical*) y cada evento nos muestra a detalle de manera cuantificada lo que sucede en la red, obteniendo una descripción del evento y el impacto que puede tener en elementos de la red, además de una posible acción correctiva.

V.4.1.5 Análisis de eventos detectados por el NIDS

En la figura 43 se muestra los eventos de tipo *Warning* capturados por el NIDS, el cual provee de una breve descripción del evento detectado y el destino en donde fue encontrado en algunos casos, es decir entre que direcciones detecto el evento.

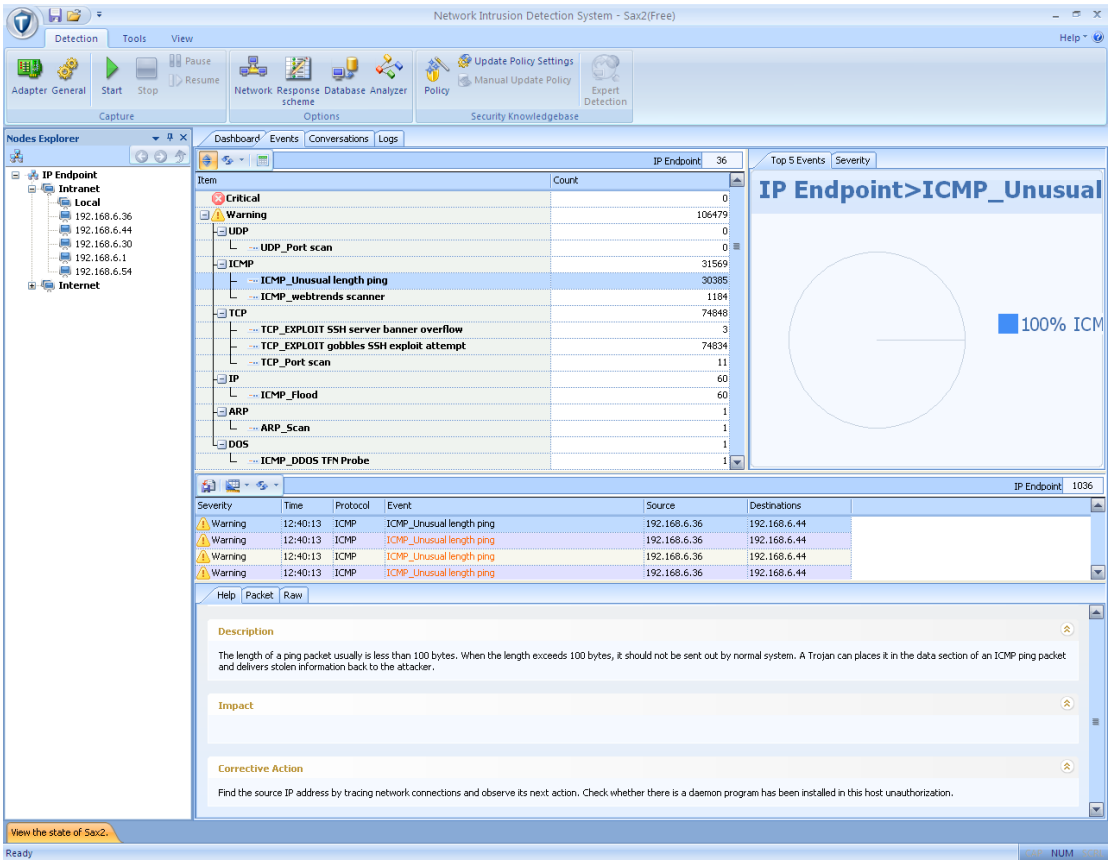


Ilustración 43 Captura de eventos Warning

Como se observa en la captura de eventos *Warning* el primer evento es un UDP *Port Scan*, el cual no muestra ningún evento capturado pero aparece debido a que el NIDS

analiza la probabilidad de que ocurra este evento por el escenario observado y lo clasifica como un evento UDP posible. Se pasa a explicar cada uno de los eventos detectados según su clasificación.

1) Eventos *Warning*

1.1) ICMP

1.1.1) *ICMP_Unusual_length ping*:

Descripción: El NIDS muestra que la longitud de un paquete ping es de menos de 100 bytes. Cuando excede los 100 bytes no es enviado por un sistema normal. Explica que un troyano puede utilizar estos paquetes para ofrecer información robada al atacante.

Acción correctiva: Se debe encontrar la dirección IP de origen mediante un trazado de las conexiones de red como por ejemplo mediante el comando *tracert* si se trabaja en Windows® y *trace route* si se trabaja en Debian®. Y luego observar su próxima acción.

1.1.2) ICMP_Webtrends Scanner

Descripción: Este evento es generado cuando el software *Webtrends Security Scanner* genera un eco ICMP. Los ecos ICMP se utilizan para determinar si un host está funcionando en una dirección IP específica. Un atacante remoto puede utilizar una gran cantidad de peticiones de ecos ICMP para determinar los equipos que están funcionando en la red.

Acción correctiva: Para evitar la recopilación de información, se recomienda configurar el firewall para bloquear los mensajes de petición ICMP entrante tipo 8 (petición) y código 0 (la respuesta de eco). Al momento de comprobar el estado de

la conexión, puede traer inconvenientes debido a que no se encontrara respuesta a la solicitud.

1.2) TCP

1.2.1) *TCP_EXPLOIT SSH server banner overflow*

Descripción: Este evento es generado cuando se hace un intento de aprovechar una vulnerabilidad de seguridad (en esta caso SSH), para conseguir un comportamiento no deseado del mismo (ataque tipo exploit). Esto se debe a que el ataque al túnel es de DOS.

Acción correctiva*:* Mantener actualizada la versión de software SSH, que no sea afectada por el atacante. En este caso detener el ataque DOS.

1.2.2) *Exploit gobbles SSH exploit attempt*

Severity	Time	Protocol	Event	Source	Destinations
Warning	12:40:40	TCP	TCP_EXPLOIT gobbles SSH exploit attempt	192.168.6.54	192.168.6.44

Descripción: Existe la posibilidad de que una atacante ejecute un código arbitrario con privilegios de usuario que ejecuta el *daemon* SSH o una posible denegación de servicio DOS. Se observa que la dirección IP fuente es de 192.168.6.54 (Cliente SSH y Proxy de la maquina Hacking) y no de la máquina de donde provienen los ataques (192.168.6.36). Como resultado este evento se interpreta como un ataque de DOS detectado.

Acción correctiva: El NIDS recomienda actualizar el software SSH a una versión que no sea afectada por este ataque. Lo más recomendable es rastrear el host en este caso el proxy, de donde viene el ataque y tomar acciones.

1.2.3) *TCP_Port scan*

Descripción: Tal vez los ataques de gusanos o scanner de un equipo local o remoto está escaneando los puertos TCP abiertos. En esta oportunidad lo que detecta el NIDS es la acción del Wireshark® con sus características de *sniffer*.

Acción correctiva: Comprobar la dirección de origen, y poner atención a lo que se intenta escanear, y configurar el firewall para prohibir la comunicación con dicha dirección IP.

1.3) IP

1.3.1) *ICMP_Flood*

Severity	Time	Protocol	Event	Source	Destinations
Warning	12:40:19	IP	ICMP_Flood	192.168.6.36	192.168.6.44
Warning	12:40:33	IP	ICMP_Flood	192.168.6.36	192.168.6.44

escripción: Un atacante remoto puede estar tratando de bloquear el sistema mediante el envío de una gran cantidad de paquetes ICMP en un corto periodo de tiempo. En efecto es así, la maquina hacking (192.168.6.36) está atacando con una inundación de paquetes ICMP (Intervención Divina).

Acción correctiva: El NIDS nos muestra la fuente del ataque y con esto se puede localizar el host que está enviando los paquetes. Cabe destacar que como es un ataque DOS este trabajo es fácil. Ahora bien si es DDOS hay que hacer un trabajo más exhaustivo para esto.

1.4) ARP

1.4.1) *ARP_Scan*

Descripción: Existe un protocolo ARP en la red, el NIDS da como posibilidades, primero que el protocolo ARP está siendo ejecutado por un host infectado o que un host necesita enviar un paquete a otro host de la misma red utilizando ARP para tal fin.

Acción correctiva: Utilizar un antivirus para descartar la posibilidad de un ataque proveniente de un software malintencionado. Encontrar cual host está utilizando el protocolo ARP y tomar las acciones correspondientes.

1.5) DOS

1.5.1) *ICMP_DDOS TFN Probe*

Descripción: Este evento es generado cuando un host intenta comunicarse con un cliente DDoS que da acceso a una *Tribal Flood Network* (TFN), que permite al atacante realizar inundaciones a través de agentes de otros sistemas comprometidos. La TFN (*Tribe Flood Network*) está compuesta por un conjunto determinado de programas que hacen vida en una PC, que llevan a cabo ataques de DDOS como inundación con paquetes ICMP y UDP. La hipótesis que se tiene es que debido a la similitud entre la forma de trabajo de los experimentos (ataques de inundación) y la manera en que trabaja una TFN, el NIDS lo detectó como tal, pensando que el *host* atacante realiza estas acciones porque está comprometida por una TFN que le obliga a realizar ataques de inundación automáticos, en vez de detectar un simple ataque DOS.

Acción correctiva: Realizar un análisis forense sobre el Host sospechoso que intenta hacer conexión con el cliente TFN y para futuros ataques realizar identificación de IDs de paquetes ICMP con

algún sistema de seguridad, pero que realice la inspección no solo de los ID por default sino también los personalizados, porque estos últimos suelen ser malévolos.

2) Eventos *Notice*

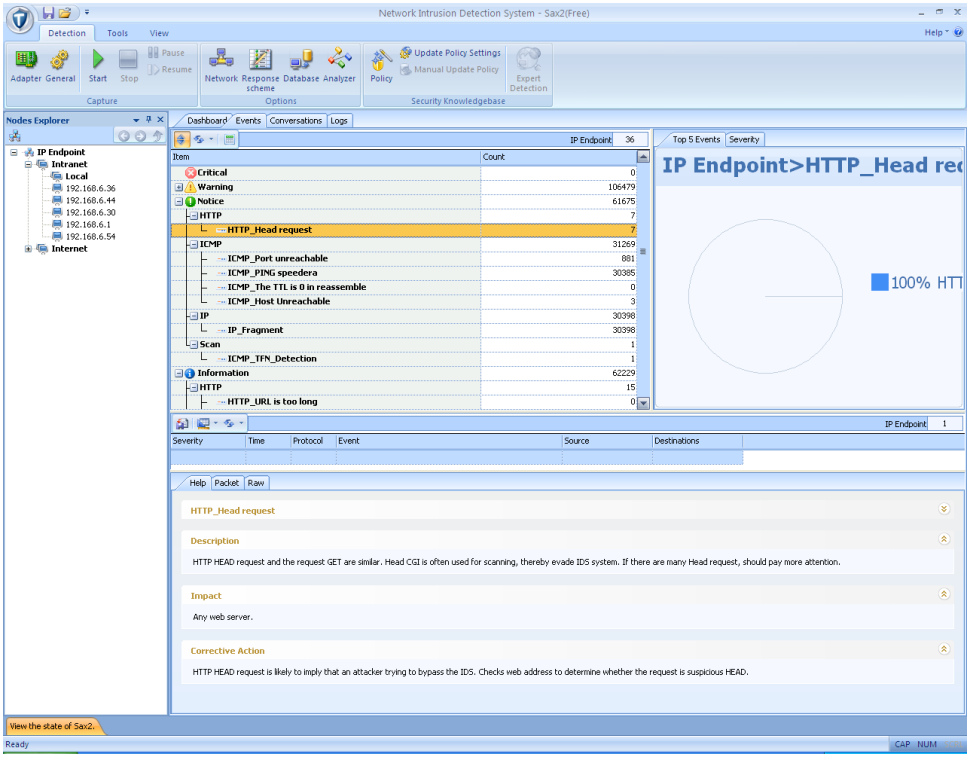


Ilustración 44 Notice HTTP Head request

2.1) HTTP

2.1.1)*HTTP Head request*

Descripción: Petición similar a *GET request*, que puede significar que un atacante quiera ocultarse del NIDS, con una cabeza CGI que se utiliza a menudo para escaneo, haciendo capaz de evadir el sistema IDS dependiendo de la efectividad de este.

Acción correctiva: Pudiendo encontrar este tipo de solicitud en cualquier servidor web se recomienda verificar la cabecera y verificar si es sospechosa.

2.2) ICMP

2.2.1) *ICMP Port Unreachable*

Descripción: Una estación recibe un mensaje ICMP de un puerto no alcanzable.

Acción correctiva: Ninguna necesaria.

2.2.2) *ICMP Port speedera http://www.snort.org/search/sid/480*

Severity	Time	Protocol	Event	Source	Destinations
Notice	12:40:13	ICMP	ICMP_PING speedera	192.168.6.36	192.168.6.44
Notice	12:40:13	ICMP	ICMP_PING speedera	192.168.6.36	192.168.6.44

Descripción: Este evento se genera cuando se detecta un *ping* benévolo utilizado por SpeedEra.net (una Red de Entrega de Contenido o CND). Después de visitar ciertos sitios de este CND, varios pings serán recibidos por el anfitrión. Estos *pings* se envían para que Speedera pueda encontrar el chache más cercano al host.

Acción correctiva: Ninguna necesaria, porque la norma de encontrar el chache más cercano al host tiene por objeto distinguir los *pings* benévolos de los *pings* normales, posiblemente malévolos.

2.2.3) *ICMP The TTL is 0 in reassemble*

Descripción: Este evento muestra que un paquete ICMP ha excedido su tiempo de vida TTL, por lo que es enviado a la fuente del datagrama para ser ensamblado.

Acción correctiva: Se requiere analizar la red para determinar porque el paquete no llego a su destino. Cabe destacar que esto se debe a efectos del ataque DOS realizado, pero no se registra un evento porque el NIDS determino la posibilidad de este evento pero el ataque no pudo afectar lo suficiente para exceder el TTL de algún ICMP.

2.2.4) *ICMP Host Unreachable*

Descripción: Una estación recibe un mensaje ICMP de un Host no alcanzable.

Acción correctiva: Ninguna necesaria.

2.3) IP

2.3.1) *IP Fragment*

Descripción: La fragmentación es una característica del Protocolo de Internet (IP) que permite a los paquetes que se dividirse en unidades más pequeñas para ser transferidos a través de redes que no soportan MTUs (Unidades de transferencia de mensajes) más grandes. En el destino el paquete IP que se divide en varios fragmentos, se vuelve a montar para formar un paquete IP completo. Algunos *routers* o *firewalls* sólo analizan el primer fragmento de una serie para determinar si debe o no pasar. Los subsiguientes fragmentos restantes serán pasados a ciegas. Fragmentos posteriores que se sustituye el primer fragmento podría llegar a un destino que el *router* o *firewall* tiene la intención de bloquear.

Mediante el uso de la fragmentación de esta manera, un atacante puede ejecutar un ataque más allá de los módulos de control de filtro o de acceso implementados en los enrutadores o servidores de seguridad de filtrado de paquetes. Siéndole a este posible construir fragmentos individuales de un paquete IP para que los paquetes posteriores se superpongan. Como resultado de ello, los fragmentos pueden sobrescribir partes de la cabecera TCP cuando

se vuelven a montar en el destino. En este caso, un router de filtrado intermedio puede ser engañado en la creencia de que el paquete está destinado a un servicio permitido, cuando en lugar del paquete está destinado a un servicio de filtrado.

Acción correctiva: Asegurarse de que está utilizando las últimas versiones disponibles para sus *routers* y *firewalls*. Ponerse en contacto con los proveedores para la actualización o información de parche. Consultar la documentación de los enrutadores y servidores de seguridad para obtener más información sobre cómo manejar la fragmentación.

2.4) Scan

2.4.1) *ICMP TFN Detection*

Descripción: Este evento indica un escaneo generado por una red de ataque DDoS de tipo Tribal Flood Network, programa maestro que posee sistemas comprometidos capaces de realizar ataques de inundación ICMP. Cabe destacar que las redes TFN a diferencia de la redes DDoS como Trinoo no son capaces de suplantar la dirección origen de los agentes atacantes

Acción correctiva: Conocer medidas de protección contra los paquetes ICMP TFN. Contra el *scaning* de TFN solo es aplicable sistemas de seguridad anti-scaning.

3) Eventos Information

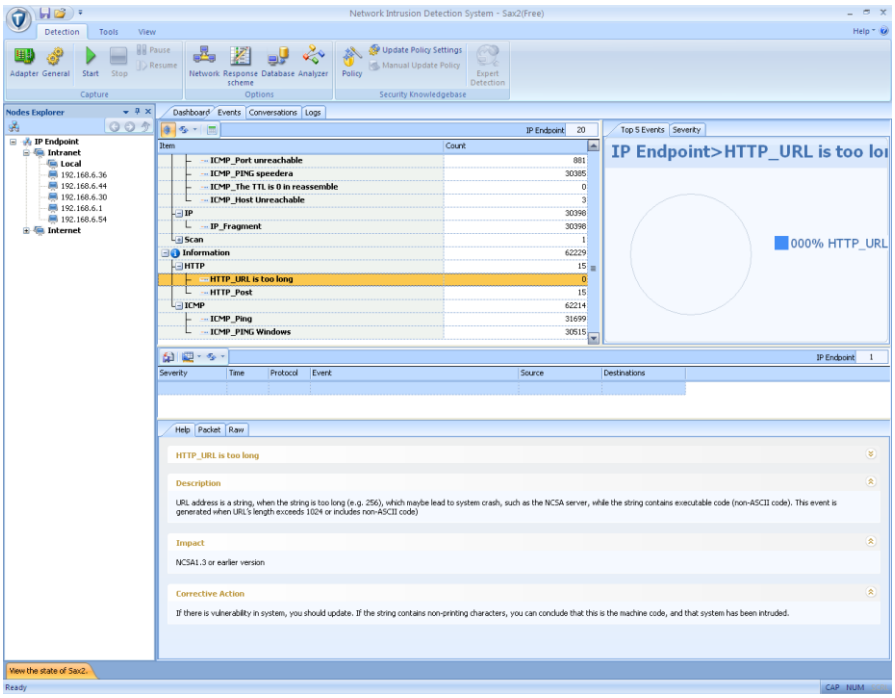


Ilustración 45 Eventos Information

3.1) HTTP

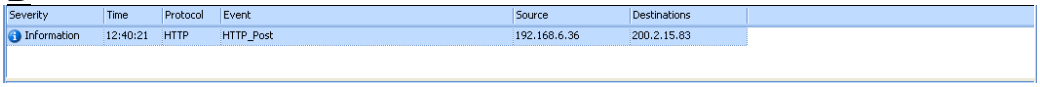
3.1.1) *HTTP URL is too long*

Descripción: La cadena de una dirección URL, en caso de ser demasiado larga puede conducir a un fallo del sistema, como en un servidor básico NCSA, mientras que la cadena contiene código ejecutable (código no ACII). Este evento se genera cuando la longitud URL excede 1024 o incluye código no ACII

Acción correctiva: Si existe una vulnerabilidad en el sistema, se debe actualizar. Si la cadena de caracteres de la dirección URL contiene algunos no imprimibles, se puede concluir que este es el código de la máquina y el sistema se ha inmiscuido.

3.1.2) *HTTP Post*

D



s

cripción: Una solicitud HTTP POST es un paquete de información que un navegador web intenta enviar a un servidor web. Esta información es propensa a intrusos ya que puede contener nombres de empleados de una empresa, números de teléfonos e incluso un número de tarjeta de crédito. Este tipo de peticiones también envían información que el usuario no ve, como por ejemplo la dirección IP del ordenador.

Acción correctiva: Se puede prohibir la solicitud HTTP POST mediante la configuración del *firewall* para denegar el servicio.

3.2 ICMP

3.2.1 ICMP_Ping

D

Descripción: El ping de ICMP es un protocolo que se utiliza para consultar si un host esta en linea, ademas permite obtener la direccion IP de este y otra información.

Acción correctiva: Se debe prestar atencion a este tipo de actividades y observar la dirección IP de origen para tomar acciones respectivas.

3.2.2 *ICMP_PING Windows*

Severity	Time	Protocol	Event	Source	Destinations
Information	12:40:13	ICMP	ICMP_PING Windows	192.168.6.36	192.168.6.44
Information	12:40:13	ICMP	ICMP_PING Windows	192.168.6.36	192.168.6.44
Information	12:40:13	ICMP	ICMP_PING Windows	192.168.6.36	192.168.6.44
Information	12:40:13	ICMP	ICMP_PING Windows	192.168.6.36	192.168.6.44

Descripción: Este evento es generado cuando una solicitud de *echo ICMP* es hecho desde un host Windows. Se observa que el contador de este evento muestra cantidad semejante con ICMP_PING, esto se debe a que muchos paquetes *ICMP request* se pierden, exactamente 1184, debido a la inundación de paquetes.

Acción correctiva: Se debe bloquear las solicitudes de *echo ICMP* entrantes, considerando la fuente de la solicitud.

V.4.3 Experimento 3: Análisis en ambiente Windows VPN (IPSec/L2TP)

Con el fin de cumplir el objetivo de realizar todas las pruebas pertinentes se desarrolla una prueba de vulnerabilidad sobre una VPN con protocolo IPSec, considerada una de las más seguras debido a la aplicación de certificados y aplicación de sistemas de cifrado robustos, que logra superar las deficiencias del protocolo PPTP.

Para el experimento se utiliza la aplicación de montaje de VPN inherente en el sistema operativo Windows XP, configurando el protocolo de seguridad como L2TP/IPSec y usando una clave previamente compartida en vez de solicitar un certificado a una entidad emisora (CA), para tener un certificado de autentificación que no requiera renovación y pago. De esta manera se realiza una conexión L2TP/IPSEC entre una maquina servidor y un solo cliente, teniendo ambos activos una copia del certificado que especifica sus IPs y la autenticación de clave compartida. A su vez entre las maquinas se activara un perfilador para medir la

velocidad de transferencia y un *sniffer Wireshark®* para capturar los protocolos de IPSec y los generados por el ataque. En la siguiente ilustración se muestra la conexión VPN realizada.

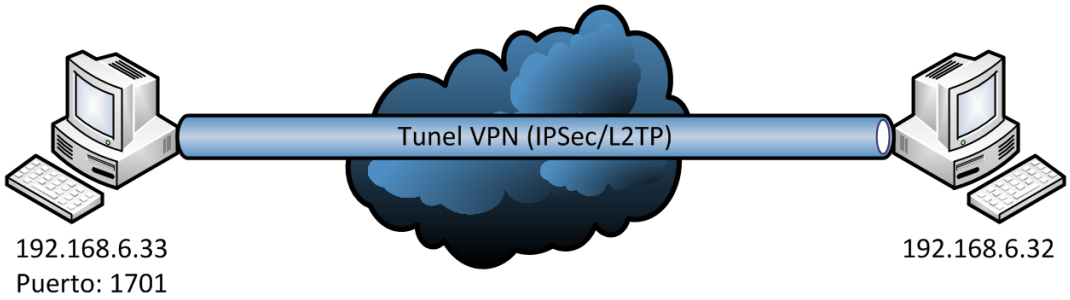


Ilustración 46 Red de Prueba IPSec

Estas dos máquinas Windows XP conectadas por VPN, se encuentran en un dominio público o red pública, donde una maquina monitorizara la conexión mediante el NIDS Sax V.2 y otra máquina realizara los ataques de Denegación de Servicio contra el servidor VPN, como se observa en la Ilustración 47.

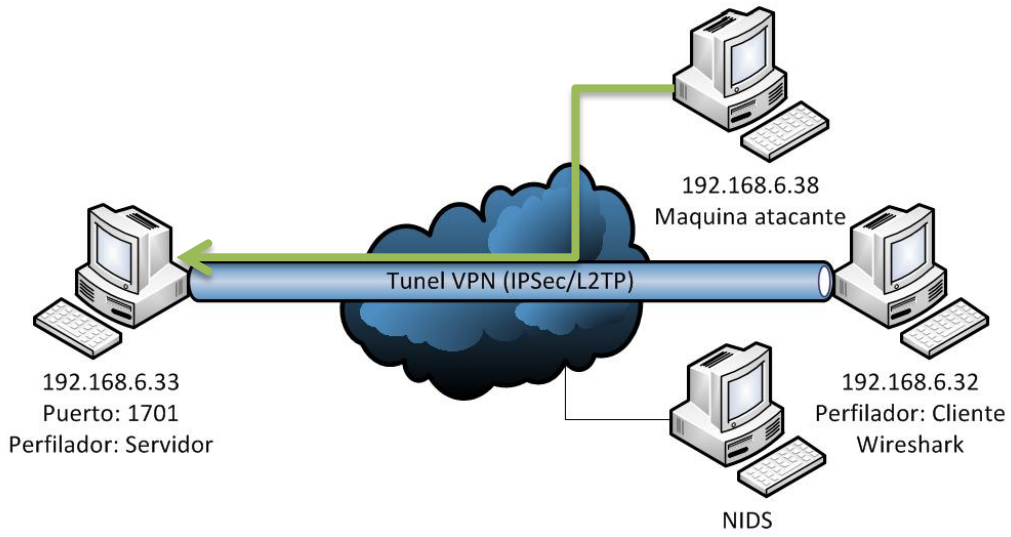


Ilustración 47 Ataque a IPSec

Al inicio del experimento el NIDS captura el tráfico de paquetes en estado normal y luego se efectúa el inicio de la conexión VPN L2TP/IPSEC desde el cliente configurado antes en las conexiones entrantes del servidor VPN, mientras el Wireshark® captura los primeros paquetes de cifrado ESP pertenecientes al protocolo IPSec y los paquetes generados por el perfilador de velocidad de transferencia.

Como se hizo en la experiencia en Debian® los resultados se exponen en el siguiente orden primero se analizan los paquetes que forman parte del perfilador (en este caso *JPerf*) y debido a que se utilizaron los mismos ataques y estos fueron explicados anteriormente, no se dará detalle de estos en lo referente al resultado de Wireshark®. El análisis llevado a cabo con el Wireshark® estará centrado en el perfilador y en aquellos paquetes de la VPN. Segundo se presenta los resultados del NIDS.

V.4.2.1 Análisis de Wireshark (Perfilador)

Este perfilador funciona de la siguiente manera, manda tráfico de un extremo del túnel a otro, esto se puede hacer de manera simultánea o en una dirección al vez, al hacerlo del segundo (Modo *Dual*) el ancho de banda disponible se redujo a la mitad, se decide entonces hacerlo del primer modo (Modo *Trade*) así el ancho de banda no se compromete. Al observar la figura el perfilador manda paquetes del servidor al cliente por eso aparece el mismo proceso una y otra vez pero siempre alternando la dirección IP de destino y la de fuente. Para aplicar el análisis se estudia el caso en el que el perfilador manda datos del cliente 192.168.6.32 al servidor 192.168.6.33.

En la ilustración 48 se expone los paquetes enviados y recibidos del cliente

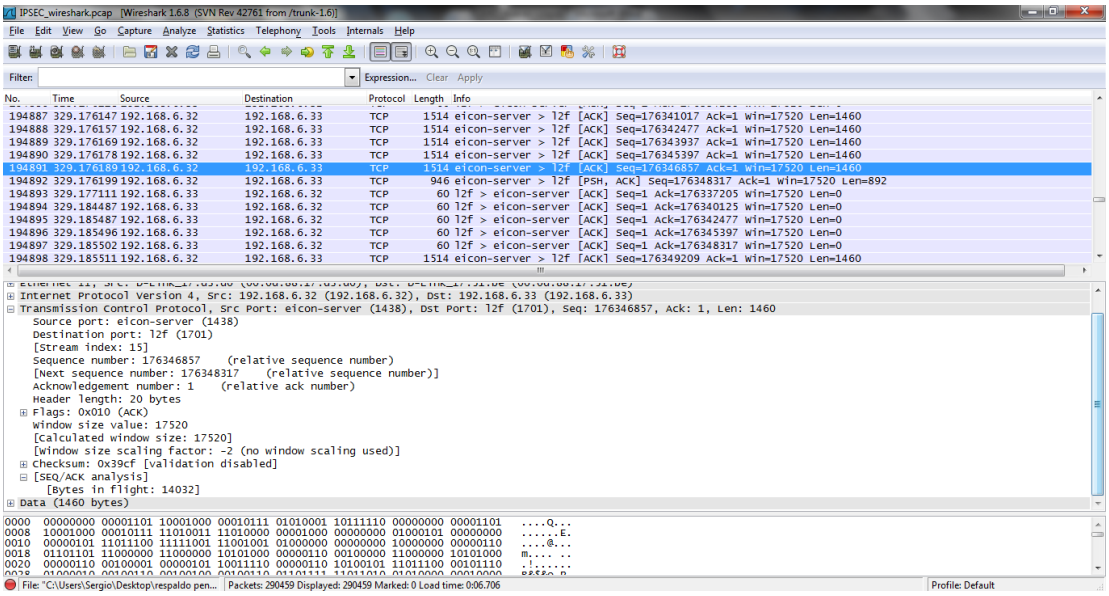


Ilustración 48 Flujo de datos del perfilador

El servidor manda una respuesta por cada paquete enviado desde el cliente en este caso fueron 5 paquetes, esta vez se puso la atención en la trama 194891. Observar ilustración 48 y la respuesta de la trama en la ilustración 49.

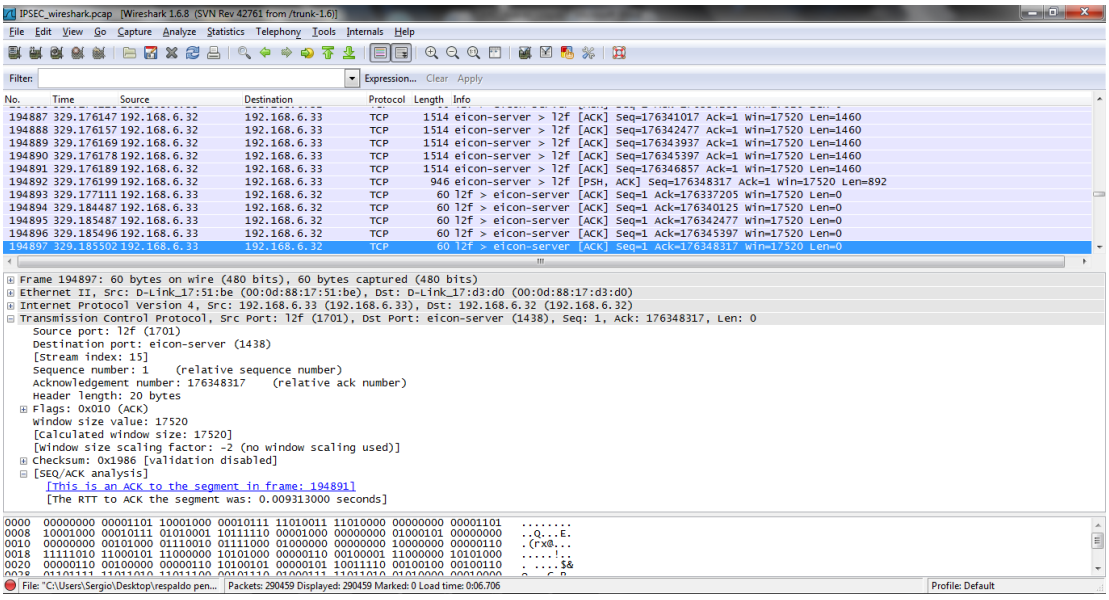


Ilustración 49 Respuesta de la trama

Como se puede observar el perfilador manda una cantidad determinada de paquetes de un extremo del túnel a otro, y por cada uno recibe un ACK y mediante el análisis del RTT perfila la VPN cada segundo. Como se observa en la ilustración 50 se observa cómo se repite el proceso pero ahora el flujo de datos proviene del cliente, y como recibe un ACK específicamente en la trama 194914.

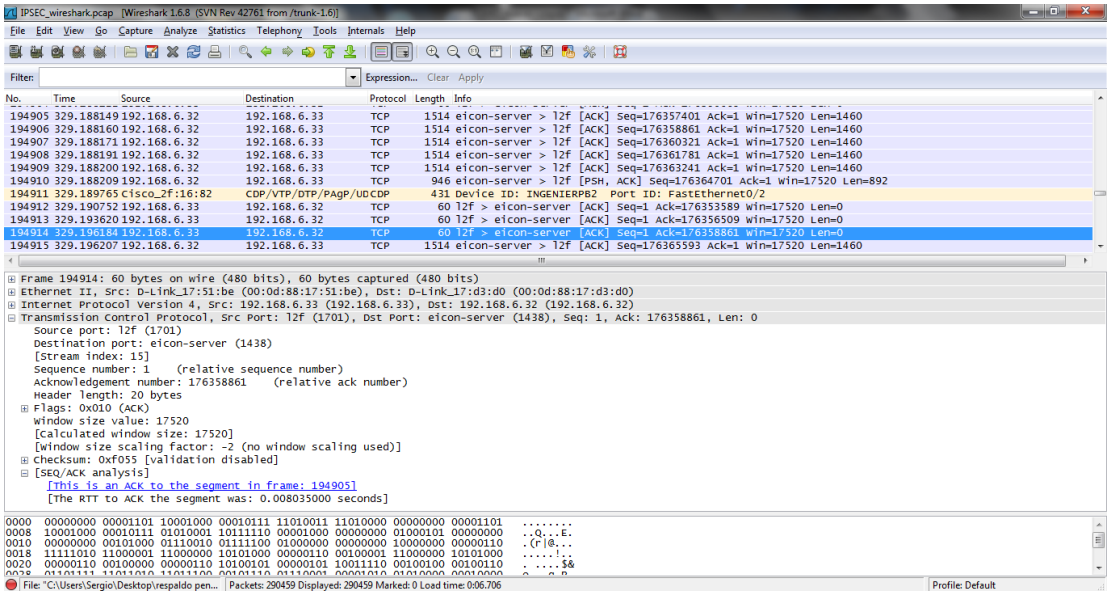


Ilustración 49 Flujo de datos del cliente al servidor

V.4.2.2 Análisis de Wireshark

Con el *sniffer* Wireshark® funcionando en el cliente VPN, considerando que todas las máquinas de la red de prueba están conectadas al mismo *switch*, se logra capturar todos los protocolos que circulan por la LAN. Teniendo configurado los usuarios autorizados en el servidor VPN, además de los permisos para conexiones de escritorio remoto y los duplicados de certificados IPSec de clave compartida en el cliente y servidor VPN, se inicia la conexión VPN desde el cliente, autenticándose este son capturados por el Wireshark® los primeros paquetes IPSec. Ver ilustración 51.

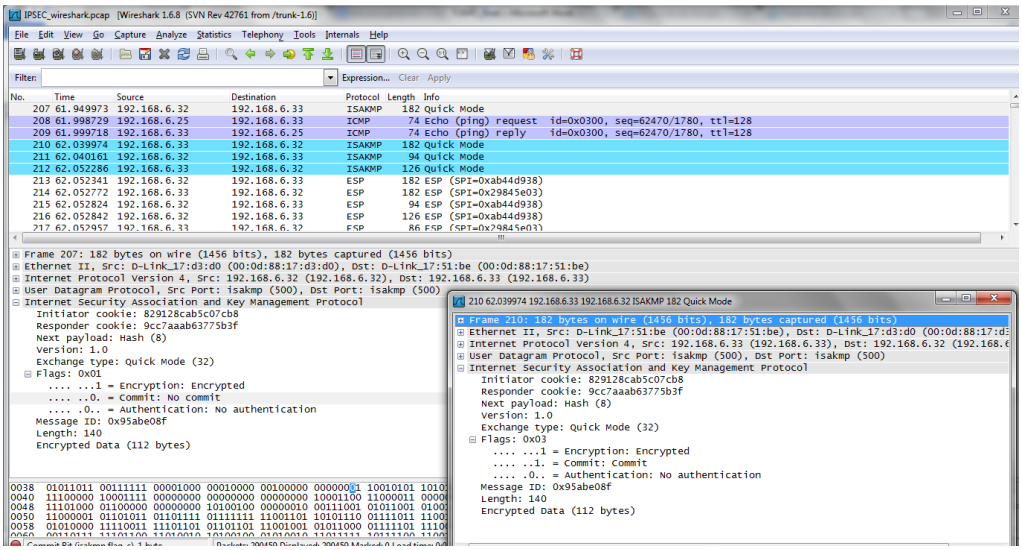


Ilustración 50 Inicio de conexión VPN, con protocolo IPSec

Como se observa en la imagen el cliente VPN con IP 192.168.6.32 inicia la conexión con un paquete ISAKMP de 128 bytes y este primer protocolo IPSec indica que una cookie de la entidad, inicio el establecimiento de *Security Associations* y una respuesta a la autoridad SA. Además establece el tipo de carga útil utilizada en este caso el Hash y activa el modo *Quick Mode* para refrescar las claves y SA, razón de la aparición del *responder cookie*. En cuanto a las banderas se observa que la data es encriptada, pero no existe compromiso hasta que se realiza la respuesta del servidor VPN, con el segundo paquete ISAKMP de 128 bytes, en el cual se levanta el *flag* de compromiso. Luego de un refrescamiento de las claves realizado con otra petición y respuesta ISAKMP se establece definitivamente la conexión VPN y se generan los paquetes ESP.

Los primeros paquetes ESP se generan del cliente al servidor como se observa en la siguiente ilustración 52 indicando que se está utilizando ESP en modo transporte, porque no se oculta la dirección de los host en comunicación y adicionalmente se sabe que ambas maquinas entienden IPSec, debido a como se configuro la conexión VPN al escribir certificados IPSec. Sin embargo el paquete ESP mostrado no muestra

que protocolo IP es enviado y tampoco el puerto especificado para la conexión, que fue el puerto UDP 1701, esto se debe a que fue cifrado junto con los datos enviados. Adicionalmente se observa otros parámetros propios de ESP como SPI (Índice de Parámetros de Seguridad), valor arbitrario de 32 bits que combinado con la IP destino y el protocolo ESP, identifica la Asociación de Seguridad SA del datagrama enviado.

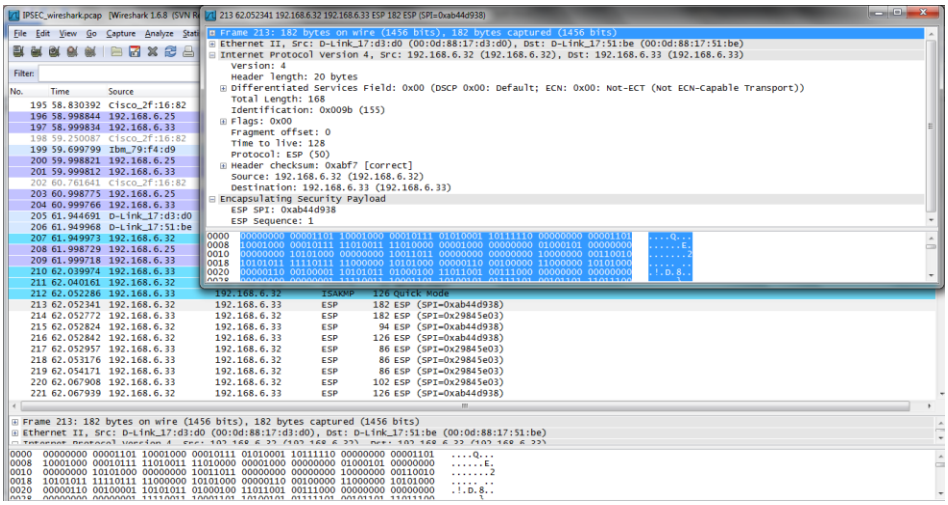


Ilustración 51 Paquetes ESP

Por lo visto el protocolo ESP propio de IPSec es bastante eficiente en cuanto a su robustez de cifrado y por su capacidad de ocultar el tipo de protocolo IP y los puertos usados. Si bien en el experimento el ataque de denegación de servicio ira dirigido al puerto correcto, en la realidad el atacante no podría saber que puerto es usado para la conexión VPN, por lo que tendría que inundar solo el puerto 80 y si quisiera tomar control de la máquina de la víctima a través de los puertos de conexión VPN abiertos, como lo hace SubSeven a modo de escritorio remoto, tendría que realizar un escaneo de puertos sobre la víctima. En definitiva IPSec es un protocolo muy eficiente para realizar conexiones remotas seguras a diferencia de sus antecesores como el protocolo PPTP que si delata los puertos usados.

V.4.2.3 Resultados de NIDS

Ahora se pasa a analizar los resultados del NIDS en las diferentes fases del experimento. Primero se captura el estado normal de la red de prueba capturando el tráfico y los eventos en curso, como se observa en la ilustración 53. Donde la IP 192.168.6.25 que pertenece a la maquina NIDS solo detecta pocos eventos de tipo Información.

Ilustración 52 Trafico Normal

En estas condiciones se enciende la captura de protocolos con el Wireshark® que incrementa el tráfico a 594 Bytes/seg y se registra más eventos no problemáticos como se muestra a continuación en la ilustración 54.

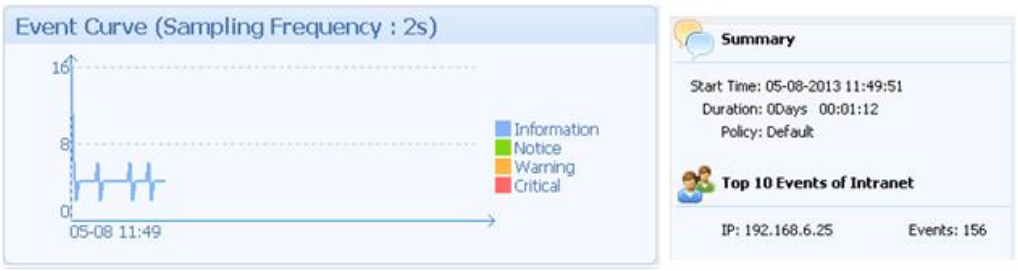


Ilustración 53 Eventos NIDS con Wireshark

Ahora se inicia la conexión VPN y el NIDS detecta un pico en la curva de tráfico y de eventos por el intercambio de claves de inicio de conexión del protocolo IPSec. Ver Ilustración 55.

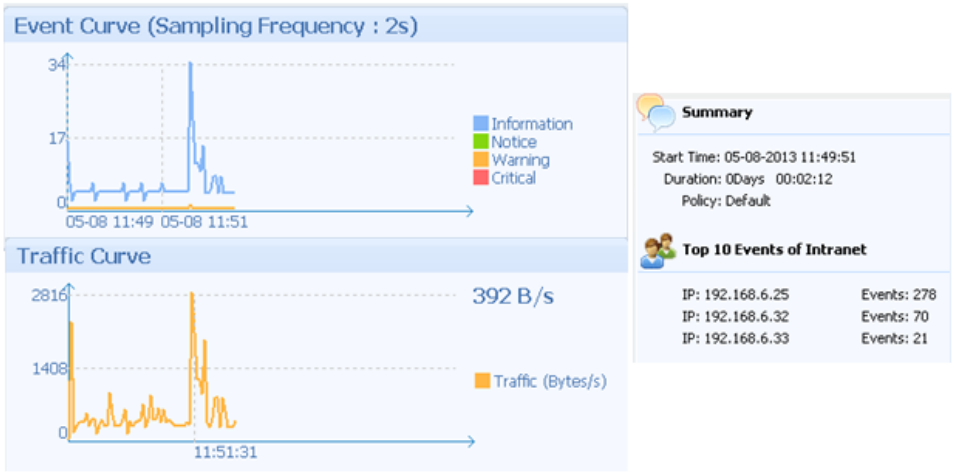


Ilustración 54 NIDS VPN IPSec conexión

Como se observa el tráfico generado por el Wireshark® empezaba a bajar cuando a las 11:51:31 se inicia la conexión VPN L2TP/IPSec, aumentando el tráfico en un pico a más de 2816 B/s y generando eventos registrados por el NIDS entre el servidor y cliente VPN. Además se genera un *Warning* pero no es considerado relevante porque es un UDP *Port scan*, el cual se activa por la acción de *sniffer* que realiza el Wireshark®. Ahora que la conexión VPN está activa se mide con el perfilador ya mencionado la capacidad de transferencia del canal, codificando en este el puerto UDP 1701 (puerto elegido para la conexión VPN).Ver figura 56.

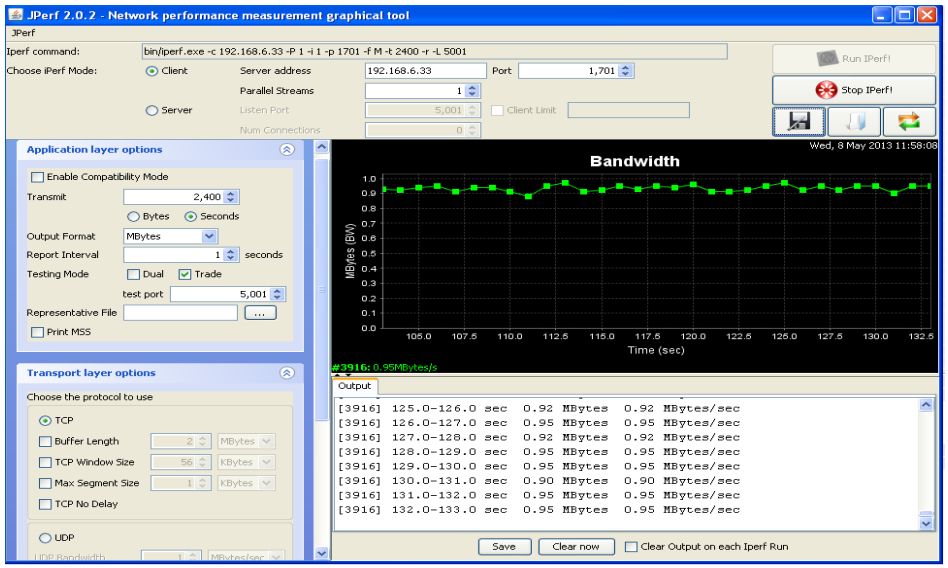


Ilustración 55 Perfilador (Velocidad optima del canal)

Como se explicó antes *JPerf* envía paquetes entre el servidor y el cliente VPN, para calcular la capacidad de transferencia del canal y como se observa en la ilustración 57 este incrementa sustancialmente el tráfico del canal a más de 1 MB/s, pero no genera eventos *warning* y tampoco picos de eventos *informations*.

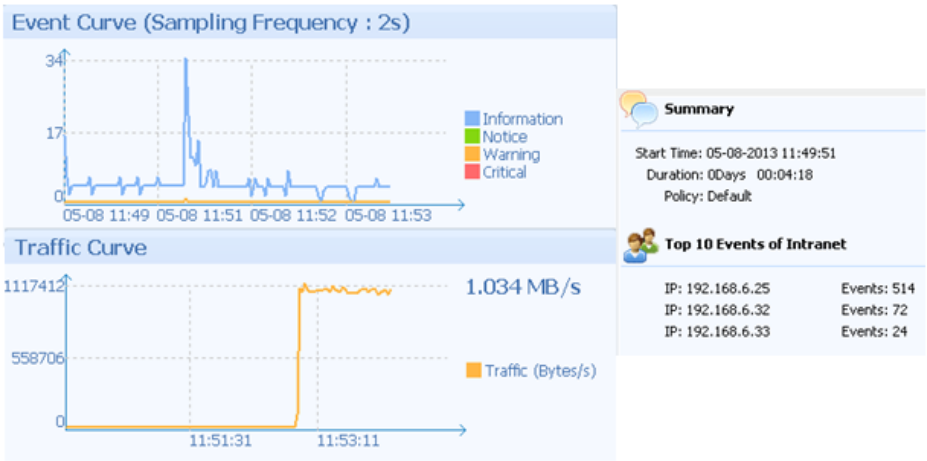


Ilustración 56 NIDS Estado antes del ataque

Con la red de prueba en funcionamiento se dispone a realizar el ataque al servidor VPN con IP 192.168.6.33, desde la maquina perteneciente a la LAN con IP: 192.168.6.38, usando los programas de ataque antes utilizados para las pruebas con las VPNs PPTP y SSH. Ver ilustración 58.

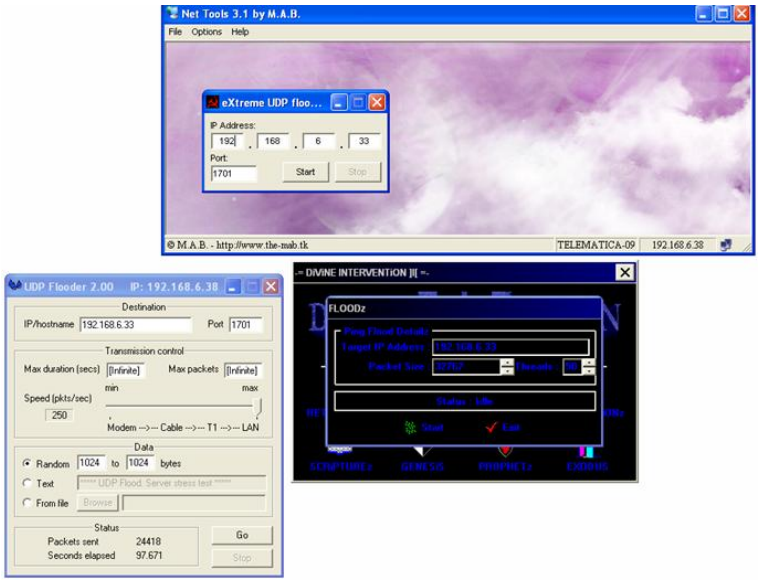


Ilustración 57 Programas de ataque DOS

Con la inundación accionada por el ataque DOS, el canal se satura y el perfilador *JPerf* realiza su última muestra de capacidad de transferencia del canal antes de detenerse, por la espera indefinida sus paquetes *request* de análisis. Ver ilustración 41. Mientras el NIDS SAX2® captura todo lo ocurrido. Tomando en cuenta que la experiencia es similar a las pruebas anteriores, los resultados del NIDS en cuanto a los eventos capturados, solo son importantes los eventos nuevos. Ver ilustración 61.

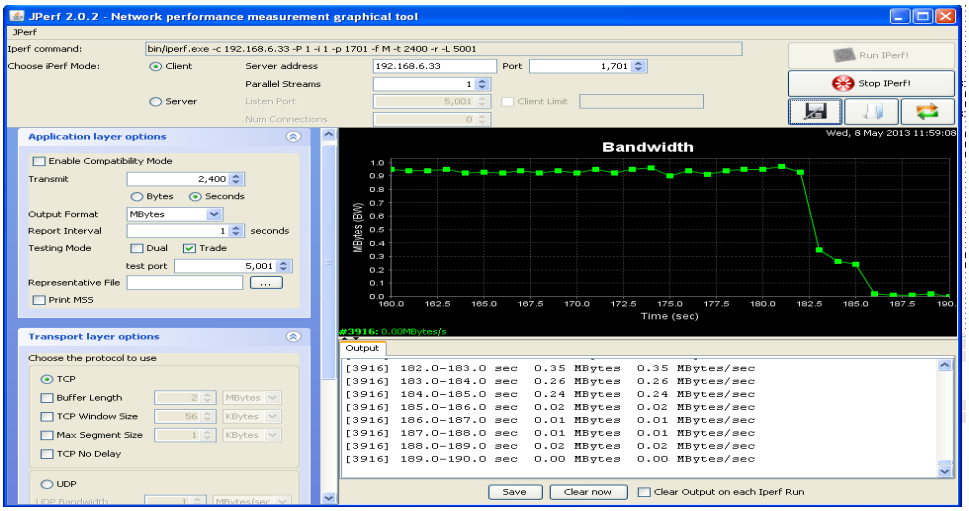


Ilustración 58 Perfilador (Durante el ataque)

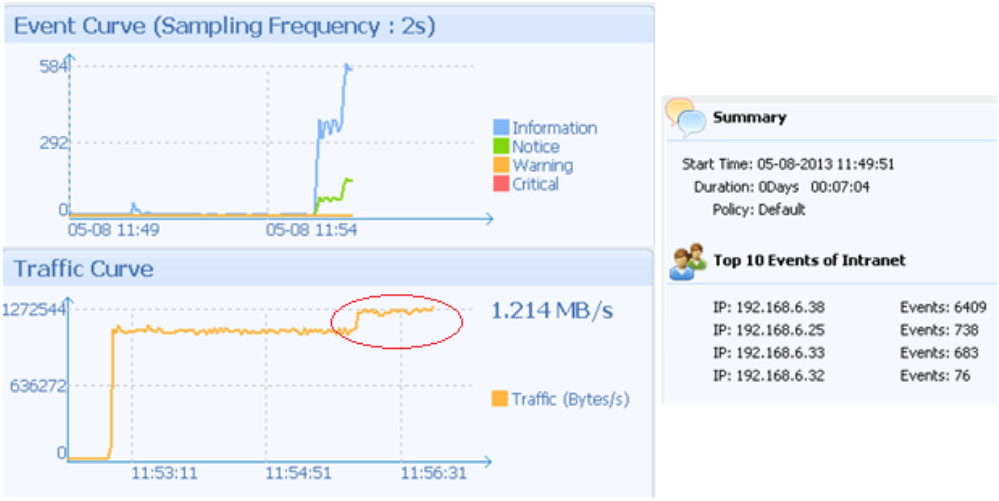


Ilustración 59 Captura NIDS durante el ataque a VPN IPSec

La curva del tráfico de la ilustración 60 indica un aumento del tráfico de 0.180MB/s con respecto al tráfico estable de 1MB/s, pero se debe considerar que el perfilador usado se para por completo por la acción del ataque, evitando que envíe mensajes para calcular la velocidad de transferencia. Por lo que, el tráfico generado por el ataque es de 1.214MB/s menos el trafico normal de la conexión VPN que se encuentra alrededor de 392B/s. Cabe destacar que el efecto del ataque sobre el perfilador no estaba previsto. Durante el ataque la conexión VPN de IPSec se vio

interrumpida al igual que las otras experiencias, hasta que se detiene por orden de la maquina atacante y se observa en la ilustración 61 como el tráfico se normaliza luego del ataque.

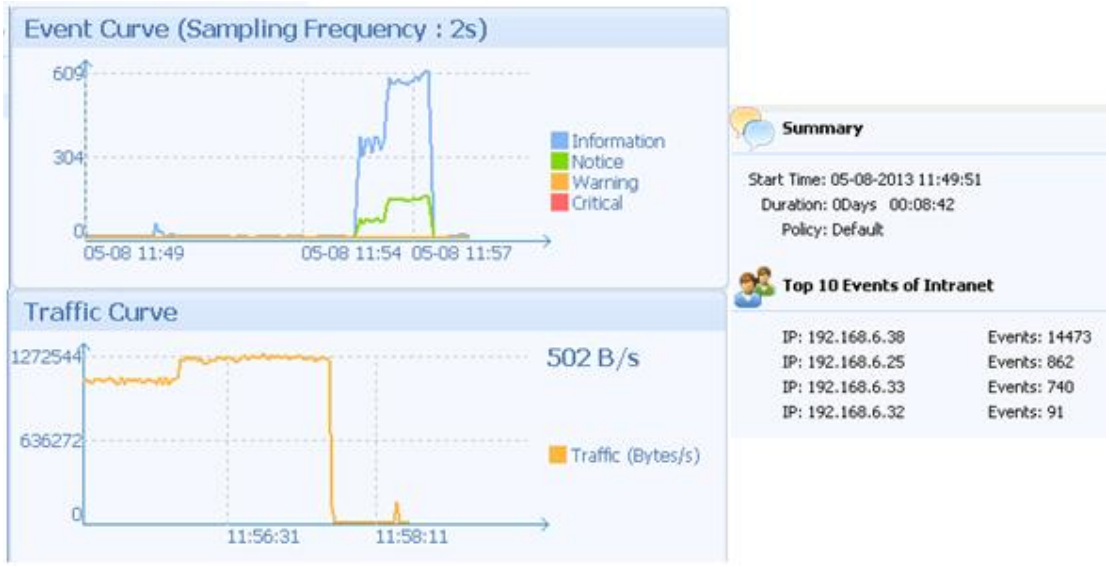


Ilustración 60 Transcurso y Finalización del ataque

La estabilización del tráfico de la conexión VPN es prácticamente inmediata como se observa, pero en otra prueba práctica utilizando esta conexión se realizó una conexión de escritorio remoto, donde el cliente VPN toma control del servidor y opera está. Luego el ataque es efectuado y la ventana del escritorio remoto vista desde el cliente se detiene por completo y solicita reiniciar la conexión o esperar, mientras la conexión VPN no muestra estar desconectada, pero lo está porque IPSec no verifica si la conexión se mantiene, pero luego de un minuto de detenido el ataque si no se reinicia la conexión del escritorio remoto, esta se normaliza con lentitud y en el analizador de protocolos se observa la llegada abrupta de todos los paquetes ESP que se encontraban en espera, de esta manera se normaliza el tráfico.

De la experiencia se toma registro de los eventos capturados por el NIDS, los cuales su mayoría son iguales a los obtenidos con la experiencia de la VPN con protocolo

SSH. Ahora se muestra la ilustración 62 que contiene una tabla de eventos generados por el ataque:

Item	Count
Critical	0
Warning	2890
ICMP	2883
ICMP_L3retriever Ping	2
ICMP_Unusual length ping	2881
HTTP	0
WEB_FRONTPAGE /_vti_bin/ access	0
WEB_MISC WebDAV search access	0
UDP	0
UDP_Port scan	0
ARP	0
ARP_Scan	0
IP	6
ICMP_Flood	6
DOS	1
UDP_DOS ISAKMP invalid identification payload...	1
Notice	6676
HTTP	0
HTTP_Head request	0
ICMP	2955
ICMP_Port unreachable	0
ICMP_PING speedera	2881
ICMP_The TTL is 0 in reassemble	74
IP	3721
IP_Unknown protocol	121
IP_Fragment	3600
Information	6892
HTTP	4
HTTP_URL is too long	0
HTTP_Post	4
ICMP	6888
ICMP_PING Windows	3443
ICMP_Ping	3445

Ilustración 61 Eventos de experiencia de ataque a VPN IPSec

Considerando solo los eventos nuevos se tiene el siguiente análisis de eventos:

1) Eventos *Warning*

1.1) *ICMP_L3retriever Ping*

Descripción: Evento es generado por una solicitud de eco ICMP, realizado por un *host* que ejecuta el escáner de seguridad L3 "*Retriever 1.5*", con el fin de

determinar los *hosts* de una red que están activos. Un escenario de ataque que puede platearse es el escaneo en busca de *hosts* vivos de una red, de parte de un atacante antes de realizar un ataque.

Acción correctiva: la solución es bloquear petición de eco ICMP entrante.

1.2) *WEB_FRONTPAGE /_vti_bin/ access*

Descripción: este evento se genera cuando se hace un intento de comprometer un host que ejecute extensiones de servidor de Microsoft FrontPage, en este caso se refiere al servidor de conexiones entrantes VPN. Siendo el impacto la recopilación de información al explorar una vulnerabilidad de un servidor Web, mediante la ejecución de código arbitrario de ataque, que podría ser Denegación de Servicio.

Acción correctiva: la solución planteada por Sax2 y el NIDS Snort, es mantener actualizado el sistema.

1.3) *WEB_MISC WebDAV search access*

Descripción: evento generado por el intento de iniciar una búsqueda WebDAV en el servidor web. Siendo WebDAV (*Web based Distributed Authoring and Versioning*), extensiones que permiten a los usuarios crear, editar o mover documentos en un servidor web. Acarreando como posible impacto la búsqueda de estas extensiones de parte de un atacante, el cual con la información obtenido potencialmente podrá realizar un ataque de Denegación de Servicio.

Acción correctiva: para solucionar se plantea la comprobación de signos de compromiso con *hosts*. Actualización hacia las últimas versiones del software, con los parches suministrados por proveedores y bloqueo de acceso a WebDAV en el servidor, para las fuentes externas de la red protegida.

1.4) *UDP_DOS ISAKMP invalid identification payload attempt*

Descripción: este evento se genera cuando se hace un intento de explotar una Denegación de Servicio (DoS) en un *host* que ejecuta TCPDUMP, herramienta de línea de comandos cuya utilidad principal es analizar el tráfico de la red capturando los paquetes transmitidos y recibidos. Aprovechando la vulnerabilidad en el análisis de ISAKMP protocolo de intercambio de claves de IPSec mediante TCPDUMP, afectando de tal manera que el análisis del paquete ISAKMP en el puerto UDP 500, permite a un atacante forzar TCPDUMP con un bucle infinito al recibir un paquete especialmente diseñado, generando en TCPDUMP interrupción en el servicio por la interpretación constante de paquetes ISAKMP malformados.

Acción correctiva: actualizar a la última versión del software que no afecte esta vulnerabilidad, más específicamente a versiones de ISAKMP superiores a 3.6 y 3.7.1.

1.5) *IP_Unknown protocol*

Descripción: considerando que hay un solo byte en la cabecera IP encargado de identificar el tipo de protocolo de capa superior. Siendo por lo general el código de protocolo para (ICMP) 1, para (TCP) 2 y (UDP) 17. El evento indica la incógnita sobre la identificación del protocolo capturado, pudiendo ser este concebido por un atacante o un homeserver que suelen establecer la comunicación a través de protocolos no estándar. Pero claramente es ilegal por lo que indica un ataque.

Acción correctiva: localizar el *host* y eliminar el proceso malicioso según la dirección IP en el registro.

CAPÍTULO VI

Conclusiones y Recomendaciones

VI.1 Conclusiones

- Tanto SSH como IPsec son propensos a ataques DOS y DDOS, no obstante SSH fue probado mediante la aplicación de SFTP e IPSec con escritorio remoto por ende no se puede concluir cual es mejor dado que fueron probados en ambientes de prueba distintos.

- El protocolo SFTP, que usa por debajo SSH, es mucho más eficiente a la hora de transferir datos en aplicaciones en tiempo real como videos debido al trabajo que realiza. Pero se debe tomar en cuenta que IPSec, oculta el puerto donde trabaja entre otras informaciones, por ende es más seguro en este sentido frente a un atacante.

- EL uso de elementos de estudio de red como Wireshark® y perfiladores de VPN, afectan de manera negativa la conexión debido al ancho de banda que utilizan para recopilar información.

- SSH actúa en la capa de aplicación, esto hace que este optimizado para trabajar con aplicaciones como *SFTP* y http, SSH asegura los protocolos TCP/IP a través del reenvío de puertos permitiendo crear un túnel para otras aplicaciones, por otra parte IPSec proporciona seguridad en la capa de red y no se integra a niveles superiores este protocolo es utilizado en modelos cliente servidor, en *routers*, equipos de VPN y servidores de seguridad. Cabe destacar que no existe interoperabilidad entre SSH e IPSec debido a que estos están diseñados para diferentes usos, pero son aplicables a las VPN.

- IPSec soporta una gran cantidad de algoritmos de cifrado entre los que se encuentran *3DES, IDEA. Blowfish, Twofish* y *Cast* además es fácil de instalar. Entre los beneficios que tiene este protocolo es que es posible hacer un túnel TCP basado en aplicaciones a través de SSH como correo electrónico, herramientas de programación y aplicaciones empresariales. Entre las limitaciones de SSH se tiene que no está diseñado para utilizarse es *Gateways* como *routers* o firewalls, debe estar conectado a la cuenta de usuario para utilizar la capa de transporte y el problema más grave que tiene es que en la actualidad existen diversas aplicaciones que manejan distintos protocolos y SSH no provee interoperabilidad.

- Con IPSec se puede lograr una total transparencia con respecto al usuario. Y se asegura cada paquete sin importar que sea UDP, TCP u otro. Para escoger un modo de trabajo de IPsec es decir operar en AH (modo transporte o túnel) o ESP (modo transporte o túnel), es necesario conocer que tipo de requerimientos encajan en las soluciones de red ofrecidas. Entre los beneficios que ofrece IPSec es que proporciona seguridad directamente en la capa de red y asegurar los datos en los niveles superiores de dicha capa. Se ha demostrado que este protocolo es un método seguro y fiable para proteger los datos, además permite crear túneles anidados, es decir, si un usuario debe pasar por dos o más *Gateways* de los túneles puede estar doblemente encriptado. Entre las limitaciones que se pueden encontrar es que es más difícil de implementar y requiere una mayor atención por parte de los usuarios en referente a los equipos a utilizar. A pesar de que IPsec garantiza la interoperabilidad entre diferentes implementaciones existen algunas que no siempre siguen el estándar.

- Para seleccionar una solución VPN para un entorno específico se deben conocer las limitaciones y diferencias de los protocolos, ya que ninguno es

adecuado para todos los escenarios. Es necesario entender que es lo que se quiere lograr.

- El tiempo de recuperación del servicio después de culminado un ataque DOS es directamente proporcional al tiempo que duró este.

VI.2 Recomendaciones

- No utilizar PPTP

- Para acceder de manera segura a un servidor y para transferir archivos SFTP ofrece la solución más simple.

- Para problemas empresariales como la necesidad de conectarse a un equipo remoto dentro de una empresa, lo mejor es conectarse a través de IPSec, con esto se logra pertenecer a la misma red de la empresa y obtener el mismo acceso. Para la comunicación entre diferentes dispositivos como servidores proxy y enrutadores lo mejor es usar este protocolo debido a que no requiere autenticación constante por parte de usuarios, debido a que la autenticación del origen de los datos es suficiente.

- Para hacer frente a un ataque de inundación se recomienda utilizar IPS (*Intrusion Prevention System)* o sistemas de prevención y detección de intrusiones, estos equipos están dedicados a la prevención de intrusiones a partir de la identificación y bloqueo de patrones específicos de ataques. Identifican la actividad maliciosa, la registra, intentan bloquear la actividad y por ultimo genera un informe de actividades.

  Entre los equipos IPS dedicados específicamente a esta solución o *routers* con esta funcionalidad incluida, se recomienda el Cisco *ASA 5500 IPS Solution Series*, ver anexo 1. Como también equipos similares de otras marcas.

Para los *routers* con funcionalidad IPS se puede utilizar Cisco *2911 Integrated Services Route*r que tiene incluido CISCO IOS IPS para ver el equipo recomendado ver el anexo2

Los equipos IPS contienen un software llamado Cisco *IPS Manager Express,* que ofrece una interfaz gráfica para el administrador de la red (ver anexos 3 y 4).

Las soluciones para los ataques estudiados de manera individual se muestran a continuación.

VI.2.1 VPN de usuario

Se deben establecer procedimientos de administración de usuarios apropiados y seguirse durante la separación de un usuario. Los usuarios deben autentificarse a si mismos antes de usar la VPN, con el fin de evitar que otra persona no autorizada la use. Deben cargarse las versiones y las configuraciones apropiadas de software VPN en las computadoras de los usuarios. Un aspecto clave para reducir la probabilidad de un ataque es la de instalar un buen paquete de antivirus en la computadora del usuario y mantener su licencia al día.

Se recomienda para las VPN de usuario combinar políticas a fin de protegerla, esto se logra mediante el uso de software antivirus y firewall personales.

VI.2.2 VPN de sitio

Para evitar un ataque a la red interna se deben hacer funciones de auditoria y políticas robustas para asegurar la seguridad de dicha red. Las organizaciones involucradas en la VPN deben definir que se permite y que no se permite a través de esta para establecer sus políticas de firewall de acuerdo con eso. Es recomendable intercambiar secretos compartidos para establecer la conexión, pero se aconseja no utilizar el mismo secreto en dos VPNs. Si se manejan

certificados de clave pública, se deben crear procedimientos para manejar y establecer la caducidad de los mismos.

Una recomendación que se debe tomar en cuenta son los algoritmos secretos o sin publicar, es la de ser precavidos con esto. Ya que ningún algoritmo en que depende de la confiabilidad del mismo es seguro.

VI.2.3 Ataques de algoritmos criptográficos

Ataques contra el protocolo

Se recomienda utilizar encarecidamente los generadores de números aleatorios correctos, no reutilizar valores (semillas). Al seleccionar una semilla fuerte la integridad del protocolo no se verá comprometida.

Ataques contra el algoritmo

No usar claves débiles, y tampoco limitar mucho el tamaño de esta. Otra recomendación importante es no alterar las funciones de transformación del código, ya que de hacerlo se contribuye al debilitamiento del sistema.

Ataques contra la implementación

Evitar que las implementaciones dejen archivos temporales, mensajes en texto simple y datos almacenados en una memoria intermedia. Utilizar siempre claves fuertes, y no combinar nunca con claves débiles.

V.2.4 Ataques comunes en algoritmos criptográficos

Ataque de texto simple conocido

Se debe ser muy precavido al momento de una fuga de información. Dar solo la información necesaria a personas realmente involucradas en un proceso en específico, que utilice una VPN

Ataque de texto simple seleccionado

La imponencia de este tipo de ataque depende de la habilidad del agresor de inferir un texto claro de una clave desconocida. No se puede evitar que una persona dedique sus esfuerzos a esto.

Ataque de texto cifrado seleccionado

Depende de la fortaleza del algoritmo, existen algunos creados pensado en este tipo de ataque, mientras que otros no lo toman en cuenta.

Ataque de intermediario

La única manera de evita esto es con el uso de firmas digitales y con el mecanismo de claves secretas compartidas.

VI.2.4 Ataques comunes en algoritmos criptográficos

Ataque de sincronización

Mantener confidencial el lenguaje de programación utilizado por el software del algoritmo de cifrado, para que se desconozca los ciclos de maquina requeridos por instrucción para generar el texto cifrado.

Ataque de fuerza bruta

Se recomienda usar claves de 128 y 160 bits ya que por ahora son claves seguras.

VI.2.5 Ataques de generador de números aleatorios (RNG)

Ataque de entrada

Evitar el uso de entradas predecibles. O evitar dar a conocer las entradas del PRNG para evitar que el agresor sepa conocer algunas salidas de este.

Ataques de sincronización

Mantener confidencial el lenguaje de programación utilizado por el software RNG, para que se desconozca los ciclos de maquina requeridos por instrucción para realizar el proceso.

Confidencialidad adelantada perfecta

Una buena medida a implementar seria que cada paquete tuviese una clave nueva, pero hay que tener presente que esto consume muchos recursos. Es necesario conocer que la mayoría de los algoritmos criptográficos utiliza una clave de sesión en cada paquete que se deriva de una clave secreta compartida.

VI.2.6 Ataques a IPsec

Ataques de implantación

Los proveedores de este servicio deben decidir previamente como implementar la opción NULL, incluyendo saber cuales sistemas son compatibles con este algoritmo. Otra recomendación es que ambos extremos deben ponerse de acuerdo para decidir que tan a menudo se deben cambiar las claves de cifrado, mientras más a menudo las cambien mejor.

Ataques de administración de claves

Como el protocolo IKE de IPSec establece el intercambio de claves inicial pero no verifica si el usuario receptor cierra sesión, entonces tiene como consecuencia que se sigan enviando datos que pueden ser capturados por un agresor. Siendo esto un problema del protocolo IPSec se recomienda a los creadores actualizar el protocolo con un paquete hello para verificación de conexión.

VI.2.7 Ataques a PPTP

Ataques al GRE

Este ataque puede evitarse con el número de secuencia, la especificación original del GRE no lleva esta implementación por ende hay que solicitarla. No utilizar este protocolo debido a que su seguridad fue totalmente quebrantada.

VI.2.8 Ataques a la autoridad emisora de certificados

Ataque de sello fechado

Para evitar esto se insertan sellos en el certificado que indican cuándo este se hizo válido.

Ataque de hardware

Limitar estrictamente el acceso a este dispositivo, para evitar que un intruso aplique la ingeniería inversa. Si se va hacer uso de una AC, visitarla personalmente para conocer que medidas de protección se toman.

Ataques débiles

La única manera de evitar este ataque es contar con personal suficiente calificado para emitir los certificados. Los CA deben tomar todas las precauciones para detener estos ataques.

Pasando a otras recomendaciones al dar respuesta a la conclusión de Rik Farrow, asesor y consultor de seguridad de UNIX e internet, se determinó que anteriormente se debe configurar el firewall, si es el punto final de VPN, para permitir sólo el tráfico seguro a través del túnel VPN. Los sistemas remotos deben ser tratados como sistemas locales, contar con protección de firewall, antivirus y firmas lo más actualizadas posibles. No obstante Rik Farrow expone lo anterior como una fantasía, dado a que según la experiencia que tiene, las personas hacen caso omiso de la seguridad en general. Una solución propuesta es la creación de un software que podría obligar a cumplir las políticas. Las distintas LAN conectadas deben tener las mismas políticas de seguridad y mantenerla al mismo nivel. El cifrado es una herramienta que debe ser usada correctamente para que cumpla los fines eficazmente.

La encriptación puede proteger los datos de la escucha furtiva, pero para garantizar dicha protección los puntos extremos no deben proporcionar una vía fácil para que un intruso aprenda ya sea acerca de los datos o la clave.

El hecho de que un sistema de hardware para VPN sea utilizado para la implementación de una VPN, no significa que el sistema nunca será vulnerable a un ataque. Como recomendación se tiene que se mantenga actualizado con la ayuda de las correcciones o actualizaciones del vendedor. Por otra parte cuando la implementación es por software se debe asegurar que el sistema se encuentre configurado apropiadamente y que todas las vulnerabilidades sean corregidas, además de que debe contarse con suficiente potencia de procesamiento para soportar el uso proyectado de la VPN.

- Se recomienda usar protocolos estándar (IPSec) al momento de desplegar una VPN que conecte varias LAN, por otra parte al momento de desplegar una VPN para uso interno se recomienda se pueden usar protocolo propietarios ya que en este caso no es muy importante que sea interfuncional

- Si una organización depende de contraseñas para el sistema de autenticación estas deben ser robustas y cambiarse con regularidad.

- Posibles investigaciones futuras

Se recomienda para estudios futuros desarrollar una aplicación que fuerce al usuario a seguir medidas de seguridad como mantener actualizada la base de datos de los antivirus y el firewall correctamente configurado, todo esto antes de levantar la VPN.

Se recomienda a los desarrolladores de aplicaciones que establecen conexiones VPN, agregar un método de confirmación rutinaria de conexión al código mediante paquetes *hello*.

Para acciones futuras contra ataques DOS y DDOS, se recomienda el desarrollo de aplicaciones o configuraciones de firewall que filtre la inundación de paquetes UDP y ICMP, provenientes de uno o varios *hosts* desconocidos o sospechosos dentro de la LAN, mediante el establecimiento de una cantidad máxima de paquetes recibidos de un *host* y la verificación del ID de algunos paquetes.

Bibliografía

ATKINSON, S. K. (1998). *IP Encapsulating Security Payload (ESP). RFC 2406.*

Brown, S. (2000). *Implementación de redes pirivadas virtuales (RPV).* USA: Mc Graw Hill.

CISCO, M. (2009, Agosto). *www.mundocisco.com*. Retrieved Octubre 2012, from http://www.mundocisco.com/2009/08/que-es-un-sniffer.html

Cobo, Á., Gómez, P., Pérez, D., & Rocha, R. (2005). *PHP y MySQL Tecnologías para el desarrollo de aplicaciones web.* España: Ediciones Diaz de Santos.

Colobran Huguet, M., & Galindo, E. M. (2008). *Administración de sistemas operativos en red.* UOC.

Corletti, A. (s.f.). Protocolo IPSec (ISKAMP). *Congreso Nacional de Seguridad y Criptografía.* Madrid.

D. HARKINS and D. CARREL, R. 2. (1998). *The Internet Key Exchange.*

farlex, t. f. (2012). *http://encyclopedia2.thefreedictionary.com/*. Retrieved Octubre 2012, from http://encyclopedia2.thefreedictionary.com/L2TP

Forouzan, B. A. (2001). *Transmisión de Datos y Redes de Comunicaciones.* Mc Graw Hill.

H. KRAWCZYK, M. B. (1997). *HMAC: Keyed-Hashing for Message Authentication, RFC 2104.*

Iglesias, S. P. (2001). Analisis del protocolo IPSec: el estándar de seguridad en IP. *Comunicaciones de Telefonica I+D*, 51-63.

M.Schneider, J. T. (1998). *ISKAMP(Internet Security Association and Key Management Protocol). RFC 2408.*

Maiwald, E. (2005). *Fundamentos de seguridad de redes.* Mc Graw Hill.

Microsoft. (2003). *Microsoft TechNet*. Retrieved julio 2012, from http://technet.microsoft.com/es-es/library/cc757786(v=ws.10)

microsoft. (2012). *http://technet.microsoft.com*. Retrieved Octubre 2012, from TechNet: http://technet.microsoft.com/en-us/library/cc768083.aspx

Numbers, P. (2013, Febrero 17). *http://www.iana.org/assignments/protocol-numbers*. Retrieved Febrero 2013, from www.iana.org.

Ñacato Gualotuña, M. A. (2007, enero). *Escuela Politécnica Nacional de Quito.* Retrieved Julio 24, 2012, from Repositorio Digital EPN: http://bibdigital.epn.edu.ec/handle/15000/1309

Red Hat, I. (2005). *Red Hat Enterprise Linux, manual de referencia.*

RFC1661. (1994, julio). *The Point-to-Point Protocol (PPP) (RFC 1661 - IETF*. Retrieved julio 2012, from http://www.ietf.org/rfc/rfc1661.txt

RFC1701. (1994, octubre). *RFC 1701 - Generic Routing Encapsulation (GRE)*. Retrieved julio 2012, from http://tools.ietf.org/html/rfc1701

Sistemas, a. D. (2012, Diciembre). *www.anerdata.com*. Retrieved from http://www.anerdata.com/que-es-un-servidor.html

Tanenbaum, A. S. (2003). *Redes de Computadoras.* México: Pearson Educación.

Wood, A. (2010). *http://www.ivarch.com/*. Retrieved Diciembre 9, 2012, from http://www.ivarch.com/programs/quickref/pv.shtml

ANEXOS

Anexo 1 Cisco ASA 5500 IPS Solution Series

Anexo2 Cisco 2911 Integrated Services Router

Anexo 3 Cisco IPS Manager Express

Anexo 4 Cisco IPS Manager Express