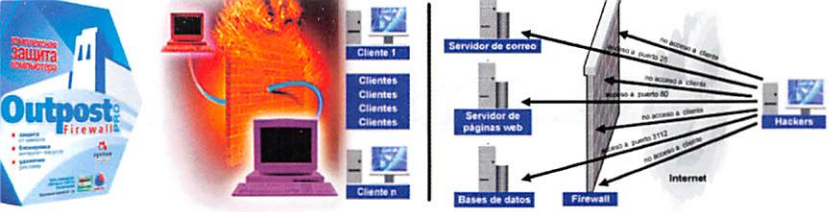

Red de datos con protección de capa de dos modelos TCO/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales en las distintas entidades o empresas del Ecuador

Carlos Gordón
Ingeniero Electrónico,
Docente de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, UTA

RESUMEN

La Tecnología va evolucionando progresivamente de acuerdo a las exigencias de la sociedad y requiere de una adecuación continua a dichos requerimientos. Cada día aparecen nuevas propuestas para mejorar el servicio de las empresas, por lo que son considerados primordiales los cambios que ocurren por mejorar la vida de los seres humanos.

Brindar mejor servicio a los clientes es el objetivo primordial del las Empresas Públicas, para lo cual debe realizar su proceso de trabajo con la mayor eficiencia y los mejores elementos. Como referencia, la empresa seleccionada es el Ilustre Municipio de Pelileo (IMP) escogida por mi afinidad ya que vivo en la ciudad de Pelileo. Es muy importante indicar que el estudio se lo ha realizado netamente en la Universidad Técnica de Ambato y no ha sido necesaria información confidencial del Municipio de Pelileo por lo que nombre se ha utilizado únicamente por Referencia. Públicamente manifiesto que no se ha atentado contra la integridad del Ilustre Municipio de Pelileo y me libero de todas las responsabilidades del manejo de información.

Se considera que la comunicación entre las Sucursales la Empresa Pública es el elemento fundamental y por ello se requiere aportar para que la comunicación tenga una seguridad muy efectiva que es el objetivo primordial de nuestra investigación.

SUMMARY

Technology is developing progressively in agreement to the existences in the society and requires a continuous acceptance to their requirements. Every day appear new proposes to improve the service of the companies, for this reason they are considered fundamental to changes that take place to improve the life of human beings.

Giving the best service to the clients is the fundamental objective of the public companies, for this reason it is necessary to do the process of work with the most efficiency and with the best elements. As a reference the selected company is the illustrate town council of Pelileo (IMP) selected for my affinity because I live in the city of Pelileo. It is very important to mention that the study has been done specifically in the Technical University of Ambato and there is not necessary confidential information of the Illustrate Town Council of Pelileo because I only use the name for reference. Publically express that there is not attempt against the Illustrate Town Council of Pelileo and I liberate of all the responsibilities of managing information.

It is considered that the communication between branch offices of the public company is the fundamental element and for reason is required to contribute to the communication has a security very effective that is the fundamental objectives of our investigation.

INTRODUCCIÓN

El término seguridad proviene del latín "securitas" que se refiere a la ausencia de riesgo o también a la confianza en algo o alguien. La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

Cuando una entidad realiza sus actividades de forma segura todos sus servicios son eficientes y brinda satisfacción a sus clientes. Ante esta realidad se considera como objetivo primordial mejorar la seguridad de la comunicación de las Sucursales la Empresa Pública pero considerando mejorarlo en varios aspectos, así se tiene.

Reducir los costos económicos y brindar un servicio de seguridad muy confiable es la prioridad de la presente investigación, por ello se considera la necesidad de la utilización de software libre que no requiere de recursos económicos para su implementación.

El sistema operativo utilizado para el proyecto de investigación es IPCop que es un firewall muy efectivo y con la combinación de Zerina permite implementar un túnel virtual muy confiable y seguro para la comunicación de las sucursales del Ilustre Municipio de Pelileo.
Finalmente es necesario indicar que a más de crear el túnel virtual se realizan pruebas de Hackeo para verificar el grado de confiabilidad de la propuesta. Las pruebas realizadas se relacionan a la identificación de puertos abiertos Port Scan para realizar ataques, Password Sniffing o rastreo de claves, ARP poisoning o envenenamiento ARP y Denial of Service o denegación de servicio, las cuales luego de ser ejecutadas proporcionan resultados muy halagadores y permitieron determinar que el túnel virtual sí provee una seguridad muy confiable en la comunicación de las sucursales del Ilustre Municipio de Pelileo.

METODOLOGÍA

Enfoque
La investigación se ha fundamentado en el Paradigma Cualitativo porque el problema requiere investigación interna, interesa la interpretación de el efecto que se consiga con el estudio de un sistema de prevención de ataques, sus objetivos plantean acciones inmediatas que se las debe tomar para corregir lo más pronto las falencias existentes en la red de datos del Ilustre Municipio de Pelileo debido al ataque de intrusos y virus , determina una hipótesis lógica que busca un fin específico, requiere de un trabajo de campo con todos los empleados del IMP y el jefe de sistemas, además sus resultados no son generalizables ya que el estudio va a ser particularizado solo para mejorar la seguridad en la Red de Datos del Ilustre Municipio de Pelileo.

Objetivos
General:

- Elaborar el diseño y simulación de la Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP utilizando software libre para mejorar la seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo.

Específicos:

- Analizar la infraestructura de Red de datos con la que cuenta el Ilustre Municipio de Pelileo.
- Realizar un diagnóstico sobre las características fundamentales de la protección a nivel de protocolos de capa dos del modelo TCP/IP, en el IMP.
- Proponer el diseño y simulación de una Red de datos con protección a nivel de protocolos de capa dos del modelo TCP/IP, que brinde seguridad en el enlace de las sucursales del Ilustre Municipio de Pelileo

MATERIALES

Un elemento muy importante para implementar la comunicación segura entre las sucursales del Municipio de Pelileo es la utilización de un Firewall conocido como IPCop.

Distribución IPCop
IPCop es una distribución Linux que implementa un cortafuegos (o *firewall*) y proporciona una simple interfaz web de administración basándose en una computadora personal. Originalmente nació como una extensión de la distribución SmoothWall cuyo desarrollo había estado congelado bastante tiempo.
IPCop
Parte de la familia GNU/Linux Cortafuegos

Figura 1: Logo IPCop

IPCop tiene como objetivos ser un cortafuegos administrado a través de una interfaz web, con funcionalidades

básicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. IPCop se actualiza desde el Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel.

User Datagram Protocol (UDP)

Es un protocolo mínimo de nivel de transporte orientado a mensajes documentado en el RFC 768. En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y la carga útil. Cualquier tipo de garantías para la transmisión de la información deben ser implementadas en capas superiores.

El protocolo UDP se utiliza por ejemplo cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

Puertos de Comunicación

UDP utiliza puertos para permitir la comunicación entre aplicaciones. El campo de puerto tiene una longitud de 16 bits, por lo que el rango de valores válidos va de 0 a 65.535. El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta.

- Los puertos 1 a 1023 se llaman puertos "bien conocidos" y en sistemas operativos tipo Unix enlazar con uno de estos puertos requiere acceso como superusuario.
- Los puertos 1024 a 49.151 son puertos registrados.
- Los puertos 49.152 a 65.535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.

Seguridad Mediante Cifrado

Cifrado Simétrico

La criptografía simétrica se basa en la utilización de la misma clave para el cifrado y para el descifrado, es decir, la robustez de un algoritmo de cifrado simétrico recae en el conocimiento de dicha clave. Sus ventajas son la sencillez de implementación, su rapidez y la robustez que provee; sin embargo, se encuentra un problema difícil de atajar: la distribución de claves: como la clave debe ser secreta para garantizar plenamente la confidencialidad de los datos cifrados, ¿cómo y a quién se distribuyen las claves para permitir una comunicación bidireccional?.

ESTRUCTURA DE LA RED DE DATOS DEL ILUSTRE MUNICIPIO DE PELILEO

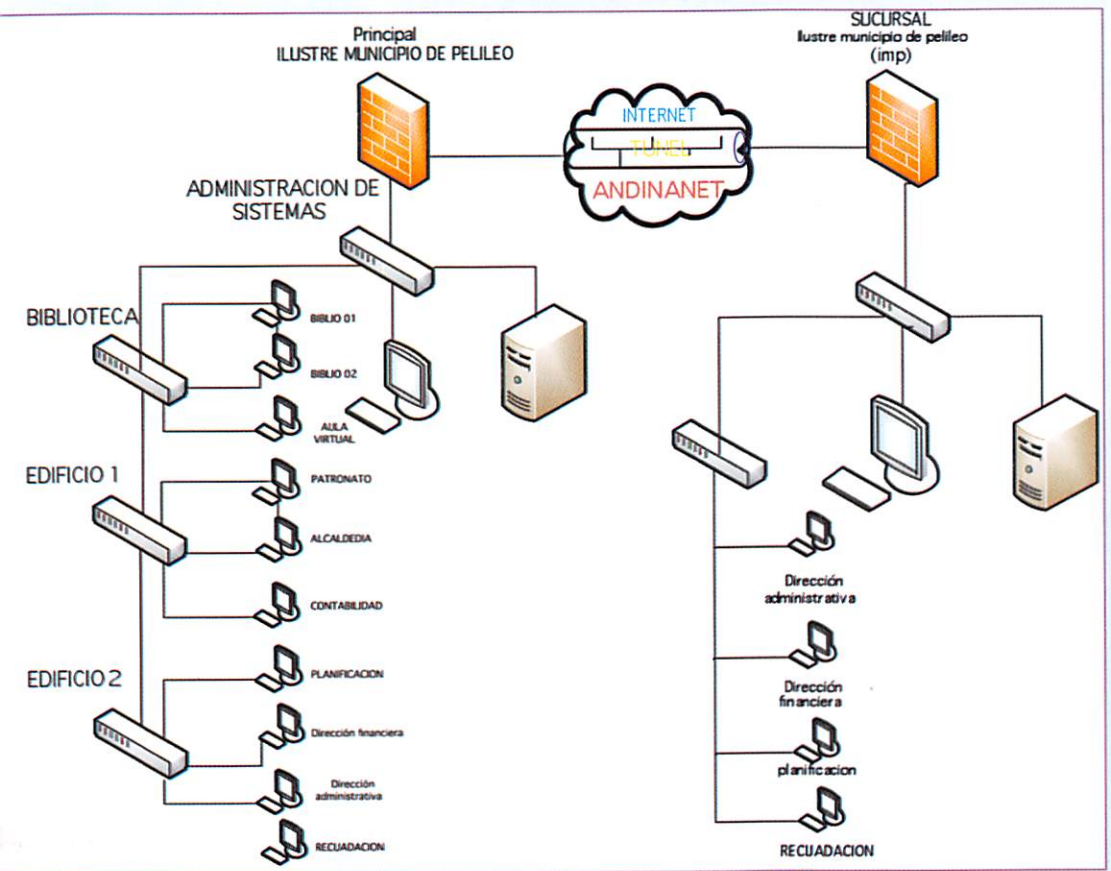

Figura 2: Túnel Virtual que Interconecta las Sucursales en el Municipio de Pelileo

CONFIGURACION DE EQUIPOS

A continuación se despliegan las imágenes en secuencia de los pasos más importantes en la configuración de los equipos

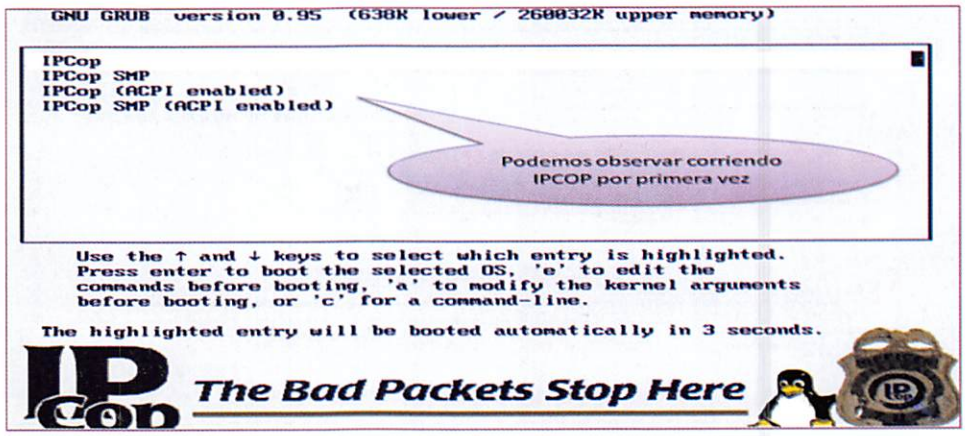

Figura 3: Arranque de IPCop por primera vez.

Es necesario crear los correspondientes certificados, para ello presionar sobre el botón **"Generar certificados de Raíz/Anfitrión"**, y aparece la siguiente imagen:

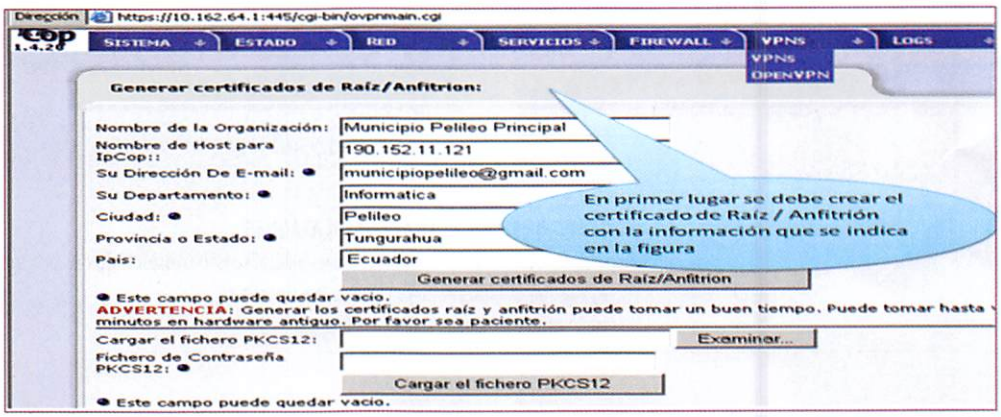

Figura 4: Autoridades Certificadoras

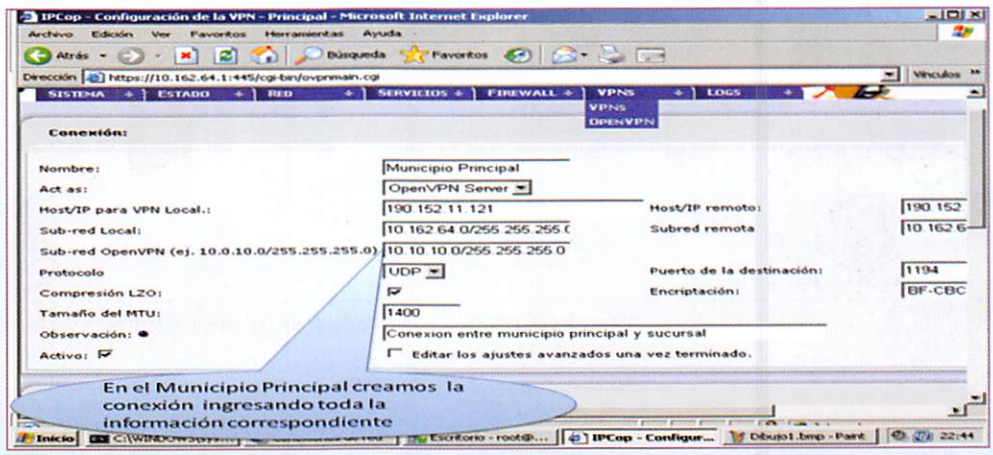

Figura 5: Información de Conexión Municipio Principal (a) .

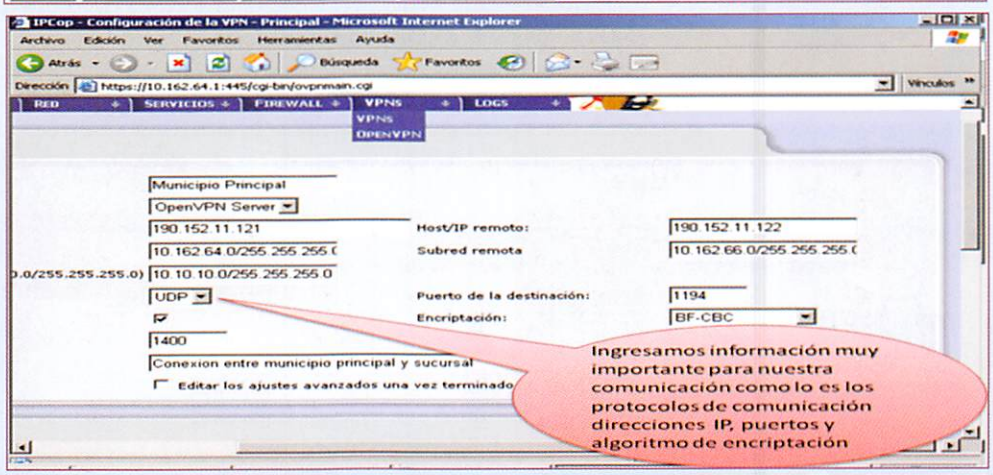

Figura 6: Información de Conexión Municipio Principal (b).

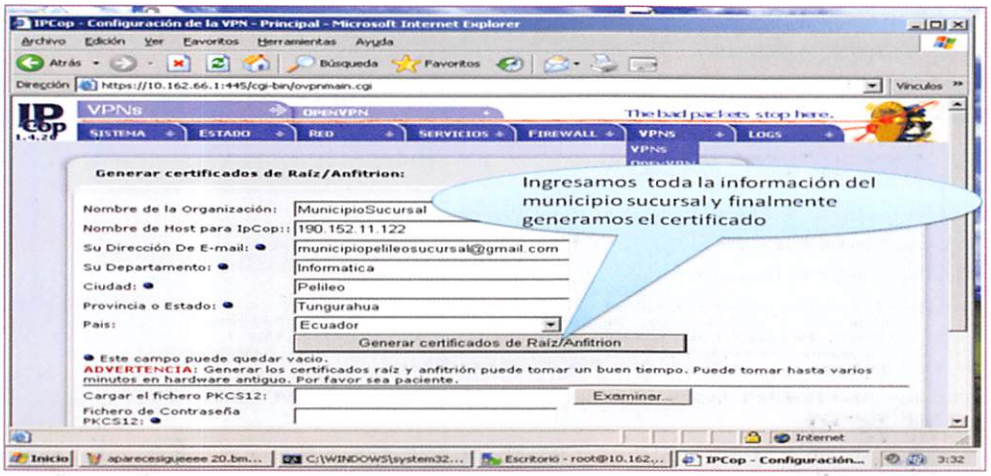

Figura 7: Información Certificado Raíz / Anfitrión en el Municipio Sucursal.

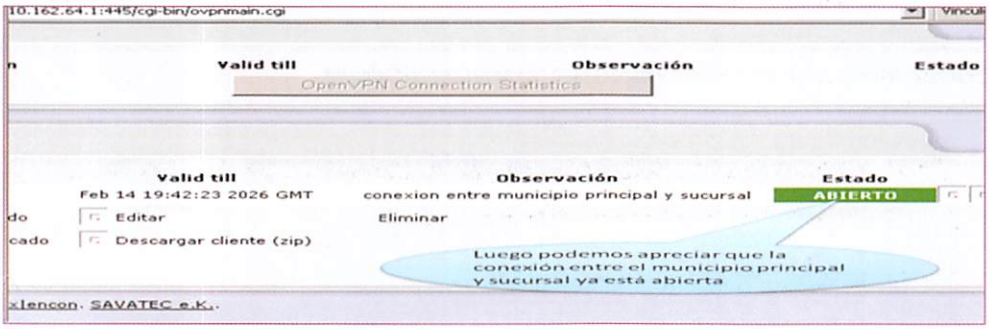

Figura 8: Estado Abierto del Túnel Virtual.

PRUEBAS DE SEGURIDAD FRENTE A ATAQUES

Para la realización de Hackeo en el túnel virtual se han considerado dos puntos de ataque primordiales así se tiene:

a) Ataque del hacker en la red Pública (Internet)

b) Ataque del Hacker en la LAN Interna

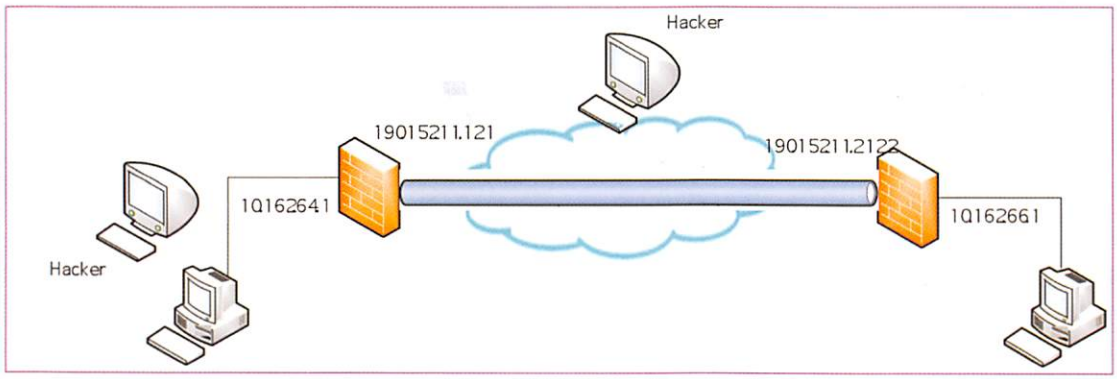

Figura 9: Hackers en el IMP.

Los ataques que se llevaron a cabo desde los dos puntos estratégicos son los siguientes:

Escaneo de puertos (PORT SCAN)

El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuego.

Existen varios programas escaneadores de puertos. Así tenemos Port Scan, Nmap, etc. Para este caso se utiliza Port Scan y se lo aprecia en ejecución a continuación.

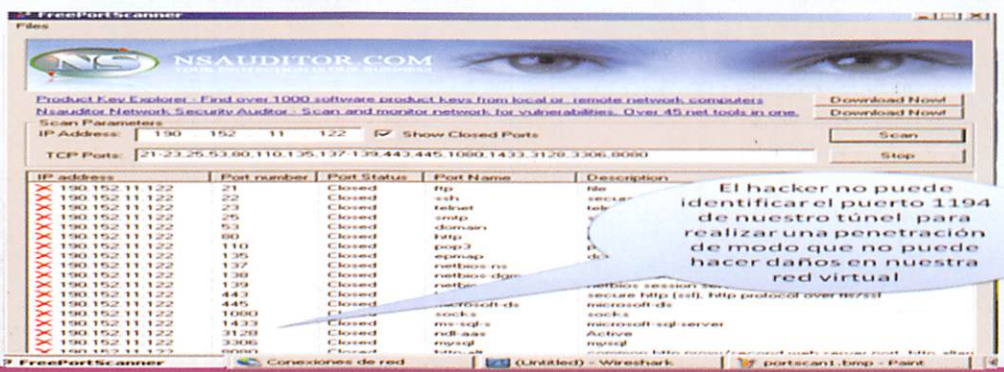

Figura. 10: Port Scanner no identifica el puerto 1194

La ejecución del programa Port Scan indica varios puertos, pero no revela el puerto por el cual se ha creado el tunel de conexión entre el Municipio Principal y Sucursal que es el puerto 1194.

Búsqueda de Claves (PASSWORD SNIFFING)

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

Existen varios programas para obtener las claves de ingreso así se tiene, Wireshark, Ettercap. En las siguientes gráficas se puede ver la ejecución de Wireshark.

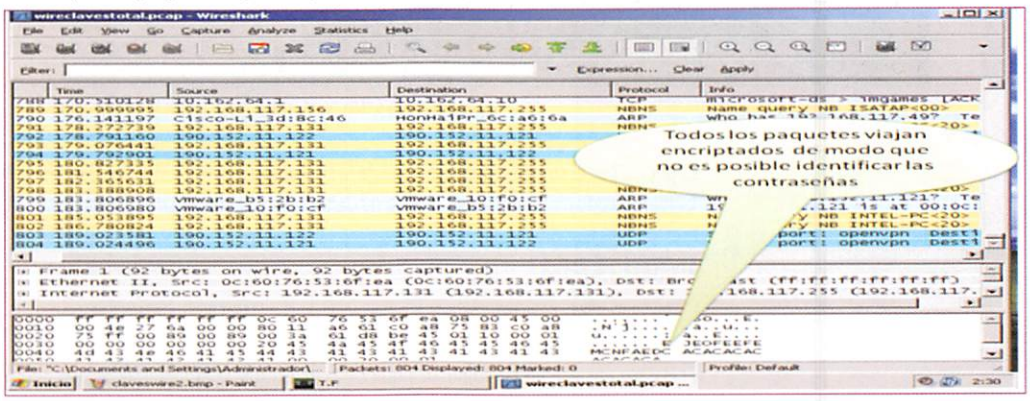

Figura 11: No se identifica la Clave.

Se aprecia que las claves no pueden ser obtenidas ya que la comunicación se realiza con paquetes que utilizan un eficiente algoritmo de encriptación de modo que es difícil desencriptarlo.

Envenenamiento ARP (ARP SPOOFING)

El objetivo es envenenar la comunicación que se produce en el protocolo de comunicación de paquetes ARP, que es el protocolo de resolución de direcciones responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas (MAC). Así pues, este breve trabajo explica básicamente el funcionamiento del protocolo ARP, para centrarnos en donde puede afectar a la seguridad de la red, para luego definir el problema y el punto débil, finalmente se aprecia la potencia de la herramienta Ettercap que es capaz de explotar satisfactoriamente la vulnerabilidad a la que nos referimos.

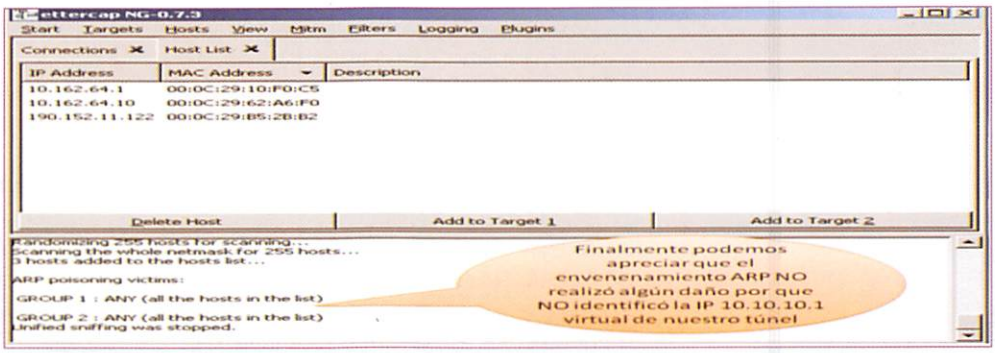

Figura 12: El envenenamiento no identificó la dirección IP virtual

Finalmente es importante manifestar que el procedimiento de comunicación se realiza en el túnel creado con un nivel de encriptación muy alto, y no se revelan las direcciones IP que conectan el túnel de modo que no es posible envenenar los paquetes ARP.

Denegación de Servicio (DENIAL OF SERVICE)

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Hay varias herramientas para realizar la denegación de servicio entre ellas se puede citar Thunderflood que se analiza a continuación.

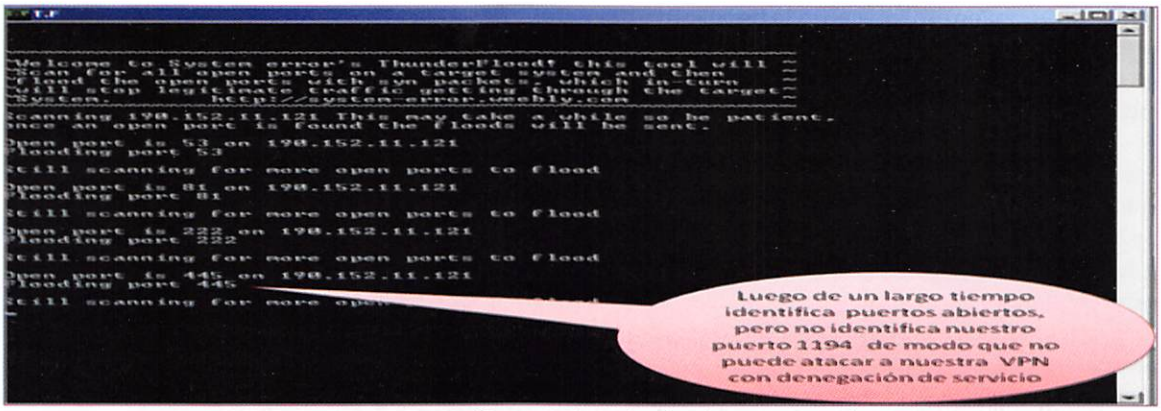

Figura 13: No se identifica el Puerto y no puede Atacar

El puerto por el cual se genera el túnel de la comunicación entre el Municipio de Pelileo Principal y la Sucursal no es identificado de modo que el ataque de denegación de servicio no genera efecto alguno en la comunicación.

RESULTADOS

Análisis del Hacker ubicado en la red Pública (Internet)

El Hacker ubicado en la red pública no puede identificar la dirección IP virtual del túnel, ni el número de puerto. Esto representa un grado de seguridad muy confiable ya que el hacker no puede fácilmente penetrar en la red y hacer daño. Además se tiene la facilidad de cambiar periódicamente la dirección IP virtual y el número de puerto de modo que será muy difícil que el hacker pueda identificar estos parámetros para hacer daños en la red.

Análisis del Hacker ubicado en la red LAN Interna (Municipio)

Para este caso se puede indicar que ocurre la misma situación que al estar ubicado en la red pública. Pero es importante indicar que un hacker ubicado en la Red Interna puede hacer mayor daño, porque es más fácil acceder y obtener claves para destruir el sistema, y ante esto se debe implementar excelentes políticas de seguridad en los administradores de la red del Ilustre municipio de Pelileo.

DISCUSIÓN

Conclusiones.

- ✔ Un túnel virtual brinda un nivel de seguridad muy efectivo ya que todos los paquetes viajan encriptados con potentes algoritmos de encriptación y protección a nivel de protocolos que evitan ser fácilmente manipulados por personas sin escrúpulos que navegan en la red pública.
- ✔ Una red con seguridad a nivel de protocolos posee una característica fundamental que es la de crear una red virtual con direcciones IP que difícilmente son identificadas en el internet y que solo lo conoce la persona que creó el túnel virtual.
- ✔ Cuando se crea el túnel virtual se generan certificados encriptados con información muy importante de la empresa, que solo lo comparten los Firewalls / Routers que están interconectados entre sí generando el túnel virtual. Esto provee el nivel de seguridad muy aceptable en la red del ilustre Municipio de Pelileo.
- ✔ Analizando el comportamiento del túnel virtual en la simulación se puede determinar que presenta una seguridad muy elevada ante el ataque de diversos hackers ya que no da a conocer el puerto de comunicación ni las direcciones IP virtuales que se utiliza en la comunicación.
- ✔ La creación de un túnel virtual a través del internet utilizando software libre y específicamente IPCop representa la manera más económica y eficiente de crear una red con seguridad a nivel de protocolos porque no se debe comprar ningún tipo de software debido a que todo es gratuito.

Recomendaciones.

- ✔ Es necesario considerar que si bien es cierto el túnel virtual brinda un nivel de seguridad muy efectivo, pero no representa un sistema 100% seguro, puesto que conocemos que ningún sistema es perfecto. Ante esto debemos establecer políticas de seguridad que nos proveerán de una seguridad más confiable.
- ✔ El protocolo a utilizar para brindar la seguridad es recomendable que sea UDP porque es un protocolo no orientado a la conexión y no necesita del reenvío de paquetes para que sean fácilmente interceptados por los hackers.
- ✔ Es recomendable la utilización de clave de encriptación simétrica porque constituye una sola clave y va ha

ser compartida entre las dos sucursales mediante un certificado de autenticación lo cual permite implementar una seguridad muy confiable con la utilización de políticas de seguridad efectivas.

- ✔ Es necesario recomendar que el número de puerto y la dirección virtual se la cambie periódicamente, pues si bien es cierto, las pruebas de Hackeo no pueden revelarlos, pero habrá un momento que pueda ser descubierto por otro hacker y se perdería la seguridad.
- ✔ Es muy primordial recomendar que el software libre si bien no tiene costo, pero si demanda de investigación adicional y es necesario que se esté actualizando con nuevas versiones de IPCop y Zerina o también desarrollar una manera para mejorar dicho software libre.

REFERENCIAS

Internet:

- ✓ DICCIONARIO INFORMATICO. (10 de junio de 2009) , www. alegsa. com. ar/Dic /sistema %20 informatico.php
- ✓ MARTINEZ, David. (10 de junio de 2009). Seguridad en redes. http://exa. unne.edu.ar /depar/areas /informatica
- ✓ SAHAGÚN, Marco (10 de junio de 2009). Seguridad Informática. http://www. monografias.com /trabajos/hackers/hackers.shtml
- ✓ UNIVERSIDAD DE CHILE. (10 de junio de 2009). Seguridad en las redes de Datos. http://www.ing.puc.cl/esp/infgeneral
- ✓ CARDOSO, Luis. (10 de junio de 2009) .Las Normas de Seguridad. http://www3. gartner.com /5_about/press_releases/pr11june2003c.jsp
- ✓ REDES DE DATOS. (10 de octubre de 2009) http: //www .geocities .com /v.iniestra /apuntes/redes/
- ✓ RED DE COMPUTADORAS. (10 de octubre de 2009) http://es. wikipedia.org /wiki/Red _ de_computadoras

ANEXOS

Tablas:

INFORMACIÓN GENERAL	
Modelo de desarrollo	Software Libre
Última versión estable	1.4.20 24 de julio de 2008
Tipo de núcleo	Monolítico
Interfaz gráfica por defecto	Interfaz web
Licencia	GPL / AGPL/ BSD
Estado actual	En desarrollo
Idiomas	Español / Inglés

Tabla 1: Información General IPCop

User Datagram Protocol (UDP)		
Familia:	Familia de protocolos de Internet	
Función:	Intercambio de datagramas a través de una red.	
Ubicación en la pila de protocolos		
	Aplicación	DNS, DHCP, NTP, ...
	Transporte	UDP
	Red	IP
	Enlace	Ethernet, Token Ring, FDDI, ...
	Estándares:	RFC 768 (1980)

Tabla 2: Protocolo UDP

993/tcp	IMAP**4 sobre** SSL (E-mail)
995/tcp	POP3 sobre SSL (E-mail)
1080/tcp	SOCKS Proxy
1337/tcp	suele usarse en máquinas comprometidas o infectadas
1352/tcp	IBM Lotus Notes/Domino RCP

Tabla 3: Puertos de Utilización preestablecida