TESIS USS

UNIVERSIDAD SEÑOR DE SIPÁN

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

TÉCNICAS DE ENCRIPTACIÓN PARA MEJORAR LA SEGURIDAD EN LA TRANSFERENCIA DE ARCHIVOS EN UN ENTORNO FIABLE

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:
Bach. Sánchez Vallejos Jhonny Moisés

Asesor:
Ing. Coronado Navarro Alex Franklin

Línea de Investigación:
Tecnologías de la Información

Pimentel – Perú
2017

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Telef: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

TÉCNICAS DE ENCRIPTACIÓN PARA MEJORAR LA SEGURIDAD EN LA TRANSFERENCIA DE ARCHIVOS EN UN ENTORNO FIABLE

Aprobación de la Tesis

Mg. Carrión Barco Gilberto

Presidente del jurado de tesis

Mg. Bravo Ruiz Jaime Arturo

Secretario del jurado de tesis

Ing. Ocampo Moreno Rosa Liliana

Vocal del jurado de tesis

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Índice

Resumen. …… vii

Introducción…… 10

CAPITULO I: PROBLEMA DE INVESTIGACION…… 11

1.2. Situación Problemática 11

1.3. Formulación del problema..... 13

1.4. Delimitación de la Investigación..... 13

1.5. Justificación e Importancia..... 13

1.6. Limitaciones de la Investigación 13

1.7. Objetivos de la Investigación 14

1.7.1. Objetivo general 15

1.7.2. Objetivos específicos 15

CAPITULO II: MARCO TEÓRICO……16

2.1. Antecedentes de la Investigación..... 16

2.2. Estado del Arte. 22

2.3. Bases Teórico Científicas..... 29

2.3.1. Criptografia o Técnicas de Cifrado..... 29

2.3.1.1 Criptografia Simétrica..... 31

2.3.1.2 Criptografia Asimétrica 32

2.3.2. Técnicas de Ataque..... 34

2.3.3. Características de los Servicios de Transferencia de Archivos ..... …..38

2.3.3.1 Seguridad e Integridad en la Transferencia de datos 40

2.3.3.1.1 Servicios NFS..... 41

2.3.3.1.2 Servicios CIFS/SMB..... 42

2.3.3.1.3 SAMBA 43

2.3.3.1.4 SFTP (SSH File Tranfer Protocol)..... 43

2.3.3.1.5 TFTP..... 44

2.3.3.1.6 FXP..... 45

2.3.3.2. Algoritmos Criptograficos 46

2.3.3.2.1 Algoritmos de criptografia de clave Secreta..... 46

2.3.3.2.2 Algoritmos de criptografia de clave Pública 49

2.3.3.2.3 Algoritmos Híbridos 51

2.4. Definición de términos básicos..... 52

CAPITULO III: MARCO METODOLÓGICO 56

3.1. Tipo y Diseño de la Investigación..... 56

3.1.1 Tipo de Investigación..... 56

3.1.2 Diseño de Investigación 56

3.2. Población y Muestra 56

3.2.1. Población. 56

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

3.2.2. Muestra. 56
3.3. Hipótesis 56
3.4. Variables 57
3.4.1. Variable dependiente 57
3.4.2. Variable independiente 57
3.5. Operacionalización 57
3.6. Abordaje Metodológico, técnicas e instrumentos de recolección de datos 588
3.6.1 Abordaje Metodológico 588
3.6.2 Técnicas de Recolección de datos 58
3.6.3 Instrumentos de Recolección de datos 59
3.7. Procedimiento para la recolección de datos 59
3.8. Análisis estadístico e interpretación de los datos 60
3.9. Principios éticos 611
3.10. Criterios de Rigor Científico 611
CAPITULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS 62
4.1. Resultados en Tablas y Gráficos…..... 62
4.1.1 Tiempo de Procesamiento, Longitud de Clave…..…….... 62
4.1.2. Margen de Error en la Transmisión 63
4.2. Discusión de los Resultados 67
CAPITULO V: PROPUESTA DE INVESTIGACIÓN……..69
CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES……115
6.1. Conclusiones 115
6.2. Recomendaciones 116

Referencias……117
Anexos……...……..121

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Índice de Figuras

Figura 1 Factores que pueden comprometer la privacidad del usuario 12
Figura 2 Tipos de Cifrado Moderno 30
Figura 3 Esquema de un Criptosistema..... 31
Figura 4 Algoritmos de cifrado simétrico mas comunes 32
Figura 5 Criptografía Asimétrica 33
Figura 6 Algoritmos de cifrado Asimétricos más utilizados 34
Figura 7 Winpcap herramienta Sniffer 35
Figura 8 Caín herramienta Sniffer 36
Figura 9 Etthercap herramienta sniffer 37
Figura 10 Analizador de Protocolos Wireshark……38
Figura 11 Protocolo FXP …….……45
Figura 12 Algoritmo DES…….……47
Figura 13 Matriz Estado AES…….……49

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Índice de Tablas

Tabla N° 1 Tiempo de Procesamiento, Longitud de Clave de Técnica1…….63
Tabla N° 2 Tiempo de Procesamiento, Longitud de Clave de Técnica2……..63
Tabla N° 3 Tiempo de Procesamiento Escenario sin ninguna Técnica……..…..64
Tabla N° 4 Margen de Error en la Transmisión de Técnica 1……..……..64
Tabla N° 5 Margen de Error en la Transmisión de Técnica 2……....65
Tabla N° 6 Margen de Error en la Transmisión Escenario sin ninguna Técnica……....66
Tabla N° 7 Protocolos de Seguridad de Transferencia de Archivos……70
Tabla N° 8 Algoritmos de Tecnología Simétrica……...71
Tabla N° 9 Algoritmos de Tecnología Asimétrica……73
Tabla N° 10 Comparación entre AES, 3DES, DES……...……...74
Tabla N° 11 Análisis Comparativo de Algoritmos Asimétricos……74
Tabla N° 12 Revisión de la Seguridad en los ServiciosIPV6……75

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Resumen

La transferencia de los archivos mediante una red no es segura, ya que el canal por el que viajan los datos no es seguro, y resulta una amenaza para la empresa si estos datos que pueden ser confidenciales son interceptados por un pirata informático. La gran mayoría de los datos que pasan por una red no han sido cifrados por tal motivo pueden ser capturados por un tercero que logre infiltrarse en nuestra red. Hoy en día existe una gran variedad de programas que me permiten capturar y observar todo lo que circula por una red informática, estos programas se denominan packet Sniffer que son husmeadores de la red capturando todo el tráfico que pasa a través de ella. Por tanto, se realizó un análisis de técnicas de encriptación de datos, siendo estos probados en la red, a través de un analizador de paquetes que es el Wireshark, estas pruebas se han llevado a cabo en máquinas virtuales bajo plataforma Linux, donde establecemos una conexión cliente - servidor, y luego se procedió a hacer las pruebas de transferencias de archivos en distintos escenarios. Finalmente, se pudo definir un escenario eficiente que contribuyó a mejorar en cuestiones de seguridad las transferencias de archivos en un entorno para que sea fiable, y luego se determinó que técnica de encriptación de los datos resultó más eficiente, siendo el criptosistema RSA de 2048 bits con cifrado AES de 256 bits, el que ha proporcionado mejores resultados en cuestiones de seguridad de los datos, minimizando el riesgo que corren los datos cuando se están siendo transmitidos en una red informática, puedan estos ser vulnerados por un tercero y además contribuyo a reducir el impacto negativo de provocar un ataque o introducción de un virus a la red informática, cuando no se toman las medidas necesarias cuando se están siendo transmitidos datos a través de ella. Se analizó 3 escenarios, de los cuales 2 se implementaron las técnicas de encriptación asimétrica y simétrica conjuntamente, ya que para que estas trabajen de manera eficiente necesitaron de ambas características, dando como resultados, en el 1 escenario la técnica RSA de 2048 bits con cifrado AES de 256 bits, nos ha devuelto todos los datos encriptados, sin poderle capturar en el trayecto de la transmisión ningún dato, siendo capaz de ser un escenario eficiente, y por último en el 3 escenario, donde se analizó la técnica de encriptación RSA de 1024 bits con cifrado AES de 128 bits, se ha determinado que es un escenario eficiente al no dejar pasar ningún dato en texto plano, y se llegó a la conclusión que el 1 escenario es más avanzado que el tercer escenario, ya que las claves del 1 escenario de 2048 bits generan el doble de

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

seguridad de encriptación a comparación de las de 1024 bits del 3 escenario, lo que incluso generó mayor velocidad de transmisión de los datos para aquellos escenarios de más recursos a administrar o mayor dimensión de los datos a ser transmitidos.

Palabras Claves

Técnicas de Encriptación, Seguridad Informática, Protocolos de Seguridad, algoritmos de cifrado de datos, ataque informático.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Abstract

The transfer of files through a network is not secure, since the channel through which the data travels is not secure, and is a threat to the company if these data that can be confidential are intercepted by a hacker. The vast majority of data that passes through a network has not been encrypted for that reason can be captured by a third party that can infiltrate our network. Nowadays there is a great variety of programs that allow me to capture and observe everything that circulates by a computer network, these programs are denominated packet Sniffer that are sniffers of the net capturing all the traffic that passes through her. Therefore, an analysis of data encryption techniques was performed, being tested in the network, through a package analyzer that is the Wireshark, these tests have been carried out in virtual machines under Linux platform, where we establish a client - server connection, and then proceeded to do file transfer tests in different scenarios. Finally, it was possible to define an efficient scenario that contributed to improve in security issues the transfer of files in an environment to be reliable, and then it was determined that the technique of encryption of the data was more efficient, being the RSA crypt system 2048 bits with 256-bit AES encryption, which has provided better results in data security, minimizing the risk of data being transmitted in a computer network, can be violated by a third party and also contribute to reduce the negative impact of causing an attack or introduction of a virus to the computer network, when the necessary measures are not taken when data is being transmitted through it. We analyzed 3 scenarios, of which 2 were implemented the asymmetric and symmetric encryption techniques together, since in order for these to work efficiently they needed both characteristics, giving as results, in the 1 scenario the 2048-bit RSA technique with encryption AES 256 bits, we have returned all the encrypted data, without being able to capture in the transmission path any data, being able to be an efficient scenario, and finally in scenario 3, where we analyzed the RSA encryption technique of 1024 bits with AES encryption, it has been determined that it is an efficient scenario by not passing any data in plain text, and it was concluded that the scenario is more advanced than the third scenario, since the keys of the scenario 1 2048 bits generate twice the encryption security compared to the 1024 bits of the 3 scenario, which even generated a higher speed of data transmission for that the scenarios of more resources to manage or larger dimension of the data to be transmitted.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Key Words: Encryption techniques, IT Security, security protocols, data encryption algorithms, computer attack.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Introducción

Según (Escrivá, Romero & Ramada, 2013*)."Seguridad informática".* Uno de los recursos más valiosos de una empresa es la información que ésta contiene, siendo estos datos confidenciales o no, si cayeren en manos equivocadas la empresa generaría muchos gastos de dinero lo que generaría su ruina. La seguridad de la información es un conjunto de normas y técnicas a tomar en cuenta, que permiten salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Según (Jean, 2004). "*Seguridad en la Informática de empresa. Riesgos, amenazas, prevención y soluciones".* La transferencia de los archivos mediante una red no es segura, ya que el canal por el que viajan los datos no es seguro, y resulta una amenaza para la empresa si estos datos que pueden ser confidenciales son interceptados por un pirata o delincuente informático. La gran mayoría de los datos que pasan por una red no han sido cifrados por tal motivo pueden ser capturados por un tercero que logre infiltrarse en nuestra red. Hoy en día existe una gran variedad de programas que me permiten capturar y observar todo lo que circula por una red informática, estos programas se denominan packet Sniffer que son husmeadores de la red capturando todo el tráfico que pasa a través de ella. Estos programas "husmeadores de la red", permiten capturar todo tipo de tráfico como: contraseñas introducidas, las páginas web consultadas, los documentos o archivos transmitidos, e-mails enviados. Por ello se implementó, ciertas técnicas de encriptación de los datos, provocando cuando estos datos fueron transmitidos han sido ilegibles ante observadores no autorizados a nuestra red, con el fin de mitigar posibles ataques informáticos o la exposición de un virus en nuestro sistema. Finalmente, la implementación de dichas técnicas de Encriptación permitió el incremento de la seguridad en la transferencia de archivos en un entorno de Red para que sea confiable.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

CAPITULO I: PROBLEMA DE INVESTIGACION

1.2. Situación Problemática

Según (Escrivá et al, 2013*)."Seguridad informática".* Uno de los recursos más valiosos de una empresa es la información que ésta contiene, siendo estos datos confidenciales o no, si cayeren en manos equivocadas la empresa generaría muchos gastos de dinero lo que generaría su ruina. La seguridad de la información es un conjunto de normas y técnicas a tomar en cuenta, que permiten salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Necesitamos adentrarnos en el tema seguridad de la información, que no es más, que evitar vulnerabilidades a nuestro Sistema de información, para mantenernos seguros de cualquier infiltración que podría producirse en nuestra Red Computacional. Según (Gonzáles & Fuentes, 2014). *Sistemas Seguros de Acceso y Transmisión de Datos*. "La seguridad de la información tiene como objetivo el establecimiento de medidas que controlen, mitiguen y prevengan distintos problemas de seguridad de un sistema, como pueden ser el acceso de datos no autorizados o la recepción de datos maliciosamente modificados" (p.17).

Por ello debemos saber salvaguardar los principales activos de una empresa que es la información, adecuándolos a normas, políticas que hagan del conocimiento asignado el usufructo de lo establecido en ellas para adecuarlas a nuestra Empresa o Negocio.

Según (Blanco Galicia, 2010)**. "***Análisis de Algoritmos Criptográficos y su Aplicación al cifrado de archivos".* Cuando se envía información para luego ser usada o simplemente esta se almacene, se corre el riesgo de que esta información sea vulnerada, perdiendo su integridad de la misma, posteriormente esta pierda su valor, generando un gran déficit empresarial en una organización, por ello se necesita que dicha información sea segura, para ello se puede hacer uso de técnicas de cifrado de los datos, sin embargo es

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

necesario que estas técnicas sean probadas para su posterior utilización y provea la seguridad pertinente al sistema de información.

Según (Villegas Gómez, 2009). *"Comparativa de Seguridad de Algoritmos de cifrado Asimétrico".* La información en una organización tiene vital importancia para que esta continúe en su desarrollo socioeconómico, y requiere de un trato muy cuidadoso, para que estos datos no caigan en manos equivocadas, lo cual provocaría un gran riesgo para la organización. Por ello se necesita brindar confidencialidad a dicha información, de esta manera evitar fugas de la misma, una forma de brindar dicha confidencialidad a la información es a través de técnicas de encriptación de los datos, dichas técnicas simétricas y asimétricas proveen características distintas de su funcionamiento y capacidades, ya que las combinaciones de ambas permiten obtener mejores resultados aprovechando las ventajas de cada una.

A continuación, detallaremos a través de un cuadro un resumen de estudio, hecha por la empresa ESET Latinoamérica, acerca de los factores que provocan surjan algunas amenazas de seguridad, así como también las implementaciones o soluciones de tecnologías posible para ser Considerado por las empresas para mejorar en cuestiones de seguridad en la transferencia de información a través de su Sistema de Información en una Red que sea Fiable.

Figura N° 1. Factores que pueden comprometer la privacidad del usuario. ESET, Latinoamérica (2014). *Tendencias 2014 El desafío de la privacidad en internet*. Recuperado de http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Según (Marc Jean, R., 2004). *Seguridad en la Informática de empresa. Riesgos, amenazas, prevención y soluciones*. La transferencia de los archivos mediante una red no es segura, ya que el canal por el que viajan los datos no es seguro, y resulta una amenaza para la empresa si estos datos que pueden ser confidenciales son interceptados por un pirata o delincuente informático. La gran mayoría de los datos que pasan por una red no han sido cifrados por tal motivo pueden ser capturados por un tercero que logre infiltrarse en nuestra red. Hoy en día existe una gran variedad de programas que me permiten capturar y observar todo lo que circula por una red informática, estos programas se denominan packet Sniffer que son husmeadores de la red capturando todo el tráfico que pasa a través de ella. Estos programas "husmeadores de la red", permiten capturar todo tipo de tráfico como: contraseñas introducidas, las páginas web consultadas, los documentos o archivos transmitidos, e-mails enviados, etc. (p. #23).

1.3. Formulación del problema

¿Cómo mejorar la seguridad en la transferencia de archivos en un Entorno de Red para que sea Fiable?

1.4. Delimitación de la Investigación

a) La presente investigación se implementará geográficamente en un laboratorio de la escuela de Ingeniería de Sistemas de la Universidad Señor de Sipán.
b) Se realiza durante el año 2016.
c) Abarca el rubro de Redes de Telecomunicaciones y seguridad Informática.

1.5. Justificación e Importancia

La presente investigación es de impacto de Seguridad Informática ya que pretende dar a conocer en la implementación de Algoritmos de Encriptación de datos en una red local que sea fiable para el usuario, permitiendo de esta forma que la transferencia de archivos sea de forma cifrada e ilegible para cualquier observador ilegal a la red, conforme a esta se cumplirá ciertos niveles o principios de Seguridad Informática: Integridad y Privacidad de la Información.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Según (Marc Jean, R., 2004). Seguridad en la Informática de empresa. Riesgos, amenazas, prevención y soluciones. Es necesario saber que deben existir medidas de seguridad en la Red Computacional para proteger los datos durante su transmisión y garantizar que éstos sean auténticos. La herramienta automática más importante para la seguridad en la Red y la comunicación es el cifrado de los datos. Para ello es necesario conocer y analizar algoritmos de cifrado de datos que permitan que los datos no sean expuestos en la Red, que algún malintencionado o delincuente informático como lo es un cracker, intente acceder de manera ilegal a nuestra información permitiendo así la exposición de un virus o ataque informático en la Red Computacional, derivándose así un gran riesgo para la empresa o Negocio lo que generaría: robo o pérdida de información, suplantación de identidades, interrupción del servicio, etc. Finalizando la pérdida de dinero y valor del Servicio de una Empresa o Negocio. (p. #86).

Para ello implementaremos un conjunto de técnicas empleadas para proteger los datos en tránsito de manera que no sean legibles frente a observadores no autorizados, a las cuales se les denomina algoritmos de encriptación de los datos en un entorno de Red para que sea Fiable.

1.6. Limitaciones de la Investigación

a) Escasa información referente a protocolos de seguridad en la transferencia de archivos.
b) En este proyecto solo se probarán los métodos o técnicas de encriptación referente a la seguridad en la transferencia de archivos (Encriptación Simétrica y Encriptación Asimétrica).

1.7. Objetivos de la Investigación

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

1.7.1. Objetivo general

Implementar Técnicas de Encriptación, para mejorar la Seguridad en la transferencia de archivos en un Entorno Fiable.

1.7.2. Objetivos específicos

a) Analizar Protocolos de cifrado y algoritmos de Encriptación con respecto a la seguridad en la transferencia de archivos.
b) Implementar la topología contextual, física y lógica para una red segura en la capa de aplicación con referencia a la transferencia de archivos.
c) Implementar un prototipo del diseño realizado con referencia a la transferencia de archivos segura.
d) Evaluar la Implementación del Prototipo con el Sniffer para verificar la transferencia de archivos segura.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

CAPITULO II: MARCO TEÓRICO

2.1. Antecedentes de la Investigación

Según (Velasco, 2015). *"Análisis de los Mecanismos de Encriptación para la Seguridad de la Información en Redes de Comunicaciones".* Esta tesis de maestría tiene como objetivo analizar los mecanismos de encriptación en redes de comunicaciones. Esta investigación analiza los trabajos relacionados con temas de seguridad informática, criptografía, normas y estándares internacionales, para ser recomendados, de acuerdo a las características y requerimientos, el mecanismo idóneo a ser aplicado en una red de telemedicina. En las redes de comunicaciones, la información está expuesta a un sin número de eventos que pueden ser provocados por quienes buscan apropiarse y conocer la información que se transmite. La seguridad de la información es la que va a permitir que muchas empresas sigan existiendo, por ello es necesario considerar diferentes mecanismos para proteger la información que circula a través de la red. Una vez analizados los diferentes parámetros de los algoritmos de criptografía asimétrica, se determinó que el algoritmo criptográfico de Curvas Elípticas (ECC), cumple con los parámetros de robustez y seguridad, dejando atrás al algoritmo RSA, que a pesar de ser el más popular de esta criptografía no cumple con las expectativas que la tecnología actual requiere.

La implementación de seguridad en una red de telemedicina, debe cubrir las dimensiones de seguridad de la recomendación X.805 dela UIT-T. Debido a la información que se va a manejar en los centros hospitalarios y considerado el tipo de amenazas a las que se expone una red de telemedicina se debe diseñar los mecanismos de seguridad que permitan: control de acceso, autenticación, no repudio, confidencialidad, seguridad de la comunicación, integridad, disponibilidad y privacidad. Por este motivo, se debe considerar algunas recomendaciones en función de los requerimientos para implementar los mecanismos de seguridad que permitan alcanzar niveles de seguridad adecuados en una red de este tipo. Evaluando parámetros como velocidad de

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

proceso, tiempo de ejecución, robustez, tamaño de clave, se recomienda que para los procesos de encriptación de los diferentes mecanismos en base al análisis de velocidad de encriptación se determinó que los algoritmos AES de criptografía simétrica y el de curvas Elípticas ECC de criptografía asimétrica, son idóneos para utilizarlos como algoritmos de encriptación de seguridad en redes de comunicaciones de este tipo. El algoritmo asimétrico de Curvas Elípticas posee características altamente seguras en robustez y tamaño de clave. Sin embargo, no ha sido difundido adecuadamente por lo que existen muy pocas aplicaciones que lo utilizan. Además de los tiempos de procesamientos más bajos que otros algoritmos y un significativo ancho de banda requerido.

Según (Paguay, 2015)*." Análisis de Algoritmos Matemáticos de Criptografía Pública para mejorar el Aprendizaje de la materia de Criptografía en la Carrera de Ingeniería En Sistemas de la ESPOCH".* El objetivo de esta tesis de maestría es analizar algoritmos de criptografía Pública, entre ellos RSA, Diffie Hellman, EL Rabin, Elgamal, desde el punto de vista de cómo están compuesto matemáticamente en su criptosistema, como los métodos o fórmulas que utilizan, los pasos que tienen cada algoritmo para cifrar y descifrar la información, así como también los conceptos por los que están compuestos sean de fácil asimilación por los estudiantes que necesiten comprender el funcionamiento de cada algoritmo de encriptación de llave pública. Estos algoritmos criptográficos pueden ser analizados de distintos ámbitos: la informática, la matemática, por su propia teoría de algoritmos e incluso por la dificultad para su criptoanálisis, el objetivo de un estudiante no es crear algoritmos, pero si emplearlos de forma adecuada para su aplicabilidad, ya que la deficiente asimilación de estos algoritmos criptográficos acarreará en un futuro problemas en la creación de sistemas informáticos, aplicaciones y desarrollo de software inseguro, por lo que es necesario hacer este análisis comparativo de los algoritmos criptográficos con la finalidad de optimizar la asimilación de estos conceptos, para su posterior utilización en un ámbito de competencia profesional. Los resultados obtenidos muestran a RSA como un

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

algoritmo con menor número de pasos para cifrar y descifrar la información, además posee conceptos matemáticos básicos como la aritmética modular y estructuras algebraicas, así como también de fácil comprensión, estas características permiten que el funcionamiento de RSA sea de fácil asimilación por ente el principio de la criptografía también.

Según (Díaz, 2012). *"Algoritmo de Encripción Híbrido: Cifrado Simétrico AES (Advanced Encryption Standar) en Combinación con curva Elíptica".* El objetivo de esta tesis de maestría es construir un algoritmo híbrido. Este consiste en la combinación de dos cifrados, uno simétrico y el otro asimétrico. El cifrado simétrico es el AES (advanced Encryption Standar) y el asimétrico es el conocido como ECC (Encriptación de curva Elíptica). Trabajar con una curva elíptica para cifrado, implica utilizar un campo finito lo suficientemente grande para ser considerado seguro, también el manejo de números de más de cincuenta dígitos, esto conlleva a una complejidad computacional adicional. Para poder manejar este tipo de información, en la implementación del cifrador de curva elíptica se utilizó el lenguaje de programación C, sobre software libre. La seguridad se encuentra basada, en el problema de logaritmo discreto elíptico, el cual implica en su solución un tiempo exponencial, por lo que se puede utilizar llaves de longitud más pequeñas que las que utiliza RSA, ya que RSA se encuentra basado en el problema de factorización de enteros, el cual tiene un tiempo de solución sub - exponencial. La utilización de estos algoritmos de encriptación de curva elíptica viene siendo dadas las desventajas de RSA de utilizar longitudes de llaves muy grandes, ya que por medio de estas longitudes radica su seguridad, considerado seguro (2048 bits), lo que en el futuro se necesitará mayor longitudes claves debido al avance de las tecnologías de las computadoras, lo que hará a RSA impráctico. Es por ello, se ha visto el campo de la curva elíptica un área de más interés por las ventajas que ofrece, tales como la flexibilidad en la implementación sobre diferentes variantes de cifrado. Su uso empieza a tener aplicaciones tales como el cifrado, autenticación, firma digital, entre otros. Sin embargo, no hay la suficiente penetración, esto es por la fuerza que tiene actualmente RSA, ya que es el

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

algoritmo con más uso en cifradores asimétricos. En cuanto al cifrado simétrico, se ha utilizado el estándar AES (Advanced Encryption Standar) con una longitud de llave de 128 bits. El cifrador asimétrico con curva elíptica, se utiliza un esquema basado en ELGamal, así también se hace uso del protocolo DIffie-Hellman para el intercambio seguro de la clave pública. Los resultados obtenidos son congruentes con lo planteado en la teoría, pues una implementación de cifrado con curva elíptica requiere mayor tiempo de procesamiento que el cifrador de cifrado simétrico. La implementación no es sencilla, haciendo un balance entre las ventajas en cuanto a flexibilidad, así como a la seguridad ofrecida por el espacio de puntos de la curva elíptica utilizada, considero que el balance es positivo. Los resultados nos indican que el criptosistema tiene un buen desempeño en tiempo de ejecución, no así en consumo de recursos del equipo. Se implementó el criptosistema utilizando el lenguaje C, el cual nos permite utilizar el código sobre diversos sistemas operativos, como son Windows y Linux, ofreciendo mayor flexibilidad a la implementación realizada. Finalmente, se ha creado un criptosistema que puede tener aplicaciones prácticas, concretamente para el cifrado de archivos de texto, las pruebas fueron realizadas hasta con archivos de 15 MB, sin embargo, la flexibilidad del programa generado permite archivos más grandes.

Según (Blanco Galicia, 2010)**. "***Análisis de Algoritmos Criptográficos y su Aplicación al cifrado de archivos".* Esta tesis se basa en el estudio de cuatro algoritmos conocidos en el campo de la Criptografía que serán puestos a prueba con el objetivo de encontrar el más seguro y eficiente para cubrir la necesidad de enviar información o simplemente almacenarla para su posterior uso, evitando que ésta sea robada, copiada o modificada por lo que no se puede confiar en los medios de transmisión, por lo tanto se requiere que la información sea segura por si mima, y por ello se necesita emplear estas técnicas o métodos de cifrado de los datos. Se implementará este algoritmo elegido bajo el lenguaje de Programación Java, habiéndole antes modificado su código fuente para lograr que incrementen más su seguridad, esta aplicación sea multiplataforma. Los parámetros o criterios de selección para llegar a

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

destinar la implementación de tal Algoritmo criptográficos serán: Tiempo de procesamiento, Complejidad de los Algoritmos, Ataques a los que es vulnerable, Tipos de Algoritmo, Dependencia de factores externos.

Los algoritmos de Encriptación investigados en esta tesis son: DES, RSA, RC4, AES, después de una serie de estudios y pruebas de vulnerabilidades hechas a cada uno de ellos analizando cuidadosamente cada opción, se ha decidido trabajar con el algoritmo de Encriptación simétrico AES que permite una mayor flexibilidad a cambios sin alterar su estabilidad, siendo que no es necesario mantener una misma secuencia en las etapas de cifrado, y se puede alterar el tamaño del bloque de la clave o de mensaje a diferencia de DES que no cumple esta característica siendo también un algoritmo de encriptación con buenas prestación de seguridad y en tanto a las pruebas a las que se le se les ha sometido, resaltando por encima de RSA, RC4, pero no de AES (Advanced Encryption Standar). Los algoritmos analizados a pesar de mostrar debilidades reales o teóricas, no significan que por ello dejan de ser útiles, eso dependerá del tipo de aplicación y el nivel de seguridad que se requiera, ya que no siempre se necesita seguridad máxima, aunque siempre es lo deseado. Conforme avanza la tecnología se requiere incrementar la complejidad de los algoritmos criptográficos ya que surgen nuevos ataques reflejándose en nuevas amenazas para los algoritmos de encriptación incluyendo DES.

Según (Franchi, 2012). "Algoritmos de Encriptación de Clave Asimétrica". Esta tesis tiene como objetivo analizar los principales algoritmos de criptografía pública RSA, DSA/Diffie Hellman, ECDSA de curva Elíptica, en lo que respecta al tamaño de la clave, nivel de seguridad, uso y velocidad o tiempo de procesamiento que tiene estos algoritmos. Además, también se comparan algoritmos simétricos como AES, DES; en cuanto a características de seguridad que ofrecen ante los algoritmos asimétricos. Para comunicaciones del tipo almacenamiento y reenvío como el correo electrónico, es más eficiente realizar el cifrado de datos con algoritmos simétricos. La clave simétrica se cifra con la clave pública del receptor. Este manejo de claves se puede implementar

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

con RSA o con Diffie Hellman en modo “half-static” donde se usa una clave de largo plazo y otra de corto plazo. Para las operaciones de cifrado/descifrado, Diffie Hellman es comparable con ECDH sobre GF(p) y RSA es más lento para descifrar y mucho más rápido para cifrar. Las diferencias aparecen con RSA, que tiene un proceso de verificación de firma muy rápido, lo cual es muy útil en sistemas basados en certificados, donde la operación más común es la verificación de una firma. También se pudo determinar en tiempos de ejecución o tiempos de procesamiento se determinó que AES es más veloz que RSA, este último por ser un algoritmo asimétrico.

La única forma de hoy y en el futuro de salvaguardar la información es por medio del cifrado de datos, donde debemos asumir el costo de la sobrecarga de cómputo, que puede llegar a comprometer la viabilidad de muchos sistemas. Los algoritmos de cifrado confían en la tremenda dificultad de resolver ciertos problemas matemáticos, no obstante, estos algoritmos que alguna vez fueron efectivos van cayendo ante el aumento de la potencia de cálculo y de los avances en el criptoanálisis. Para contrarrestar esta circunstancia, es necesario aumentar el largo de la clave a fin de mantener el mismo nivel de seguridad, la otra solución es encontrar algoritmos de mayor complejidad algebraica. A cerca de la complementariedad de los algoritmos de clave privada y de clave pública, estos últimos son más nuevos y más versátiles que los primeros, esto no implica que los algoritmos simétricos vayan a ser reemplazados, ya que cada uno tiene sus ventajas relativas. Los algoritmos de clave privada establecen su predominio a la hora de cifrar grandes cantidades de datos. Por otro lado, los algoritmos de clave asimétrica prevalecen al momento de implementar el intercambio de claves, las firmas digitales y garantizar el no repudio. En cuanto a la conveniencia de utilización de un algoritmo de clave pública sobre otro, es fundamental evaluar el tipo de aplicación en la que va a utilizarse el algoritmo. Finalmente, no hay que dejar de lado la cuestión de la velocidad para el cifrado/descifrado que, dependiendo de la aplicación, puede ocupar un lugar más relevante.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Según (Gallegos García, 2011). *"Diseño de protocolos criptográficos para votación electrónica".* Esta tesis doctoral tiene como objetivo diseñar protocolos criptográficos para votación electrónica que dejen en la fase del conteo de los votos en manos de "n" autoridades, ciudadanos y candidatos a elegir. Todo esto mediante el uso de primitivas criptográficas de cifrado, firma funciones hash y secreto compartido, con la finalidad de que los protocolos propuestos puedan ser utilizados dentro de un sistema de información que desarrolle en las cuatro etapas de un proceso de votación electrónica. Proponiendo tres protocolos criptográficos, lo cual su vez serán analizados en distintos niveles para cumplir de manera incremental con ciertos requisitos de seguridad: privacidad, precisión, equidad, elegibilidad, robustez e in-coercibilidad necesarios en un proceso de votación electrónica, evaluándoseles a fin de encontrarles un óptimo rendimiento en función de los requisitos de seguridad necesarios y un mejor desempeño.

Se analizaron estos protocolos criptográficos propuestos para votación electrónica como basados en emparejamientos bilineales, criptografía de umbral basado en identidad sin GLP y esquema de firma ciega y el tercer protocolo con esquema de cifrado y esquema de firma ciega basados en identidad.

Los resultados obtenidos del análisis de cada protocolo criptográficos muestran que tanto los tres protocolos cumplen con los requisitos de seguridad establecidos para votación electrónica.

Finalmente, el protocolo propuesto mejora las propuestas anteriores desde el punto de vista de las premisas de seguridad que tiene el hecho de trabajar con esquemas que basen su funcionamiento en emparejamientos bilineales.

2.2. Estado del arte

Según (Molina, Mendoza & Melgar, 2016)."*Aplicación de Algoritmos de llave Pública para certificar la sobrevivencia de pensionados en el extranjero de el Salvador*". La comprobación de la supervivencia de salvadoreños residentes en el extranjero se realiza de forma manual, lo que implica el traslado de la

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

información impresa en papel, de cierto país a EL Salvador, expuesta a la modificación o al acceso no autorizado por parte de terceros. En esta investigación se propone un protocolo que certifica la comprobación de supervivencia y garantiza que tanto la generación, el envío y la verificación de la documentación digitalizada sea protegida usando algoritmos criptográficos como las firmas digitales, funciones hashing (funciones picadillo), timestamping (marca de tiempo o estampa de tiempo). De tal manera que la información pueda ser transmitida vía correo electrónico y que la parte receptora tenga los mismos mecanismos de seguridad para confirmar la fiabilidad de la información recibida.

Se propone un protocolo que permite el envío de la declaración jurada de manera digital, protegida con un estampa o marca de tiempo como la propuesta de Adams et. al (2001) que se encuentra firmada digitalmente, con lo cual el notario público del Consulado correspondiente certifica la sobrevivencia. Ambas técnicas están basadas en el algoritmo de llave pública RSA. El protocolo propuesto considera únicamente la generación digital de la declaración jurada que previamente fue realizada de manera convencional por el notario, considerando por supuesto la transmisión de la declaración jurada, ya que es estrictamente necesario que el pensionado o su representante legal asista al consulado. De tal manera, la aseguradora puede recibir y verificar el documento de forma electrónica, haciendo el proceso mucho más eficiente y seguro. La digitalización de la declaración jurada y el anexo de la estampa de tiempo son certificados a través de la firma digital RSA generada por el Cónsul o Notario Público “autorizado” con lo cual se protege la integridad de la información y se autentica la identidad del certificador.

Según (Medina & Miranda, 2015) ."*Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES".* En esta investigación se centra en una comparación equitativa de tres algoritmos de criptografía de clave simétrica más comunes: DES, AES y 3DES. En Términos de seguridad y rendimiento, DES fue diseñado para funcionar mejor en hardware que en software, a pesar

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

de esta característica DES, actualmente, es vulnerable a ataques de fuerza bruta. Es por ello que DES no es apropiado para la seguridad. La solución rápida a esto es introducir 3DES, que es lo suficientemente seguro para la mayoría de propósitos hoy en día. 3DES es una construcción de DES, tres veces en secuencia, con tres llaves diferentes, una longitud de clave efectiva de 168 bits. Otra variación es DES con solo 2 claves, reduciendo el tamaño de clave en 112 bits, que es menos segura. Comparándolo con su predecesor 3DES toma tres veces más potencia en cuestiones de rendimiento.

Sin embargo, AES supera a 3DES, tanto en software como en hardware, este algoritmo Rijndael ha sido seleccionado como Advanced Encryption Standar para reemplazar a 3DES. Bajo los criterios de seguridad, rendimiento en software como en hardware, idoneidad en entornos de espacios restringido, resistencia al análisis del poder y otros ataques de implementación. AES, utiliza 128 bits y el tamaño de bloque fijo para claves de 128, 192 y 256 bits. AES es el reemplazo para 3DES, según NIST ambas cifras coexistirán hasta el año 2030, permitiendo una transición gradual a AES. A pesar de que AES tiene ventaja teórica sobre 3DES para la velocidad y la eficiencia de alguna implementación de hardware 3DES puede ser más rápido algunas veces.

Finalmente, el estudio comparativo entre DES, 3DES y AES donde se presentaron doce factores, que son longitud de la clave, el tipo de cifrado, tamaño de bloque, desarrollado, resistencia criptoanálisis, la seguridad, la clave posibilidad, posible ASCII teclas de caracteres imprimibles, el tiempo necesario para marque todas las claves posibles en 50 mil millones segundos, éstos demostraron que AES es mejor que DES y 3DES.

Según (Mejia, 2014) "*Implementación de Protocolo SSL, TLS, SSH*". Actualmente existen diferentes protocolos del modelo OSI, cada uno con funcionalidades distintas para lo que fueron diseñados. En esta sección tomaremos interés esencial en 3 protocolos, cada uno que trabaja con diferentes algoritmos de encriptación.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

SSL(Secure Socket Layer) Capa de Conexión Segura, fue creado para que cierta información sea transmitida de forma segura, empleando maneras de cifrado y descifrado, de esta forma se conoce que este protocolo nos ofrece autenticación y privacidad a la hora de logearnos al servidor, pactando en primera instancia el cliente y servidor que algoritmos se van a emplear, además de una serie de normas y estándares que se necesitan cumplir para que se realice la comunicación.

El protocolo SSH (Secure Shell), nos permite transferencias seguras entre sistemas empleando una conexión cliente-servidor, trabajando con conexiones remotas, siendo un procedimiento seguro que se pueda descifrar las claves encriptadas, permite un modo seguro para aplicaciones graficas en la red.

Protocolo TLS (Transport Layer Security) es la versión desarrollada del protocolo SSL; este protocolo nos permite transferencias seguras a través de un túnel cifrado entre un cliente y servidor, lo que provoca un intercambio de información libre de posibles atentados de seguridad.

Estos protocolos evitan el espionaje telemático (eavesdropping), previniendo adulterar la identidad del emisor sosteniendo la integridad de la información en una conexión cliente- servidor. El objetivo de estos protocolos es usar técnicas de encriptación que usan algoritmos de cifrado de los datos, estos con sus correspondientes fortalezas y debilidades, que estos se condicionan a distintos escenarios donde el cliente determine trabajar.

La aplicación en el uso de protocolos TLS junto con otras técnicas de encriptación como IPSec, cifrado RPC, etc., nos ayudan a mantener la confidencialidad e integridad de los datos durante la comunicación, protegiendo así datos confidenciales como números de tarjetas de crédito en las diferentes transacciones de comercio electrónico, envió de información privada, en una intranet o a través de Internet, de una organización, etc.

Aunque no hay que olvidar que los ataques pueden ser múltiples y cada vez más sofisticados, lo que obliga a una permanente investigación de mejora de

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

los diferentes protocolos de seguridad, se puede decir que un uso correcto de estos protocolos nos proporciona hoy en día un nivel de seguridad "bastante aceptable".

Según (Vera, López & Manta, 2014). *"Modelo test-bed de Simulación y Evaluación de criptografía de curva elíptica en redes IPv6 de próxima generación".* En la actualidad las redes móviles e inalámbricas de nueva generación, tales como las redes de área personal IPv6 de baja potencia (6LoWPAN), redes de sensores inalámbricos sobre IPv6 y redes móviles IPv6 jerárquicas se encuentran bajo rigurosa investigación y desarrollo, pues representan el paso por seguir en la evolución de las redes Machine-to-Machine (M2M), al tiempo que apoyan el acceso de banda ancha de próxima generación de tecnologías y sistemas inteligentes sobre Internet futuro.

Estas redes de nueva generación imponen restricciones de cuanto al poder de procesamiento, ancho de banda y recursos de energía, lo que representa un gran límite en la implementación de mecanismos de seguridad. En este sentido, en los últimos años han surgido diversas propuestas para la administración de claves, procedimientos de firma digital y cifrado de datos basados en curvas elípticas e híper-elípticas, que logran niveles de seguridad equivalentes a los algoritmos Diffie-Hellman y Rivest-Shamir-Adleman (RSA), pero que reducen la longitud de clave y, por ende, los recursos computacionales y de red asociados.

En esta investigación examina los algoritmos basados en criptografía de curvas elípticas (ECC) y su aplicación a redes móviles e inalámbricas de nueva generación habilitadas para IPv6. Así mismo, describe un modelo de simulación para la evaluación de ECC, donde se comparan los recursos computacionales necesarios y las limitaciones en mecanismos ligeros de seguridad.

Los avances de la ciencia de la tecnología, la matemática aplicada, criptografía de Curva Elíptica e Hiperelíptica han permitido a lo largo de los últimos años el desarrollo y estandarización de novedosos protocolos de seguridad y marcos de referencia (Balde et al., 2005; Cohen et al., 2006). La criptografía de Curva

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Elíptica se puede convertir en un elemento para la próxima generación de comunicaciones inalámbricas habilitadas con soporte a IPv6.

Según (Bareño, Navarro & Cárdenas, 2015). "*Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV6*". Día a día los Sistemas de transmisión a través de diferentes redes internas o externas son cada vez más inseguras, debido a la facilidad de analizar el tráfico por parte de diversos atacantes. El presente artículo busca mitigar los posibles ataques o problemas en el proceso de autenticación, integridad y confidencialidad de usuarios locales o remotos a través de diversas redes con resultados de implementación confiable y seguros. Se hace utilidad el protocolo nativo IPSEC en IPV6 de host a host en lugar de punto a punto como se hace en IPV4. El encabezado de autenticación AH se utiliza para garantizar la integridad y ataques de no repudio, ESP (Carga de Seguridad Encapsulada) para la confidencialidad e integridad. Para el escenario de las pruebas se ha determinado realizarlo en máquinas virtuales y un analizador de paquetes o Sniffer como Wireshark, para el fin de determinar en cuestiones de seguridad de los datos en cuanto a confidencialidad, integridad, autenticación y no repudio.

Finalmente, la implementación y revisión de la seguridad de los servicios analizados en entornos integrados bajo IPV6 será un proceso continuo en el que diariamente aparecen nuevas vulnerabilidades y riesgos de seguridad. Es importante, por ello, mantener una buena formación en los protocolos utilizados, porque hacia el futuro existirán nuevos riesgos en medida de seguridad, cuando se incremente la utilización del protocolo IPV6.

Según (kaschel & Alvarado, 2014*). "Criptografía de Curva Elíptica aplicada a Seguridad para Redes WBAN bajo la norma IEEE 802.15.6".* Esta investigación tiene como objetivo presentar un sistema de Seguridad basado en Criptografía de Curva Elíptica aplicado a Redes de Área Corporal Inalámbricas (WBAN: Wireless Body Area Network) fundamento en la norma IEEE 802.15.6. Donde

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

se hace un análisis comparativo de los sistemas asimétricos RSA y ECC, donde se exponen las ventajas de cada una de estas tecnologías de encriptación como una solución de seguridad aplicada a este tipo de Redes Área Corporal Inalámbricas denominado WBAN.

WBAN tiene una amplia gama de aplicaciones de vigilancia de la salud, incluyendo respuesta médica de emergencia. Sin embargo, presentan muchas vulnerabilidades que las vuelven propensas a ataques que ponen en peligro su seguridad y privacidad. Un aspecto importante en una WBAN radica en una variedad de requisitos de seguridad y privacidad bastante estrictos que el despliegue de aplicaciones de estas redes debe satisfacer, ya que al transportar datos de los signos vitales de las personas, las amenazas de seguridad (como el robo o alteración de información) puede llevar a un paciente a una situación peligrosa, incluso la muerte. Sin embargo, la integración de un mecanismo de seguridad de alto nivel en un sensor limitado de recursos y de bajo consumo, aumenta los costos de cómputo, comunicación y gestión. En una WBAN, la seguridad y el rendimiento son igualmente importantes, por lo tanto, el desarrollo de métodos de seguridad es un reto fundamental para los diseñadores.

En WBAN los nodos sensores se comunican a través de enlaces de comunicación inalámbricos, la seguridad de la red se pone en peligro debido al medio utilizado (ondas de radio) pero también por las vulnerabilidades específicas de las redes de sensores inalámbricos, éstas pueden ser hackeadas (“pirateadas”) e invadidas. Por otro lado, todos los protocolos de seguridad tienen que limitar el número de mensajes necesarios para su propio funcionamiento, ya que la comunicación entre los sensores es la principal fuente de consumo de energía en la red de sensores inalámbricos, donde el procesamiento del algoritmo de seguridad involucra un cierto porcentaje en el consumo de energía.

Los requerimientos de seguridad, que exige una WBAN son confidencialidad, integridad, autenticación, disponibilidad, actualización de datos, no repudio y

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

autorización. Por tal motivo, se hace un análisis de técnicas de encriptación enfocadas en estos requerimientos de seguridad, adoptando la mejor medida, pero todavía en una investigación concreta por resolver, se ha tomado en cuenta a la criptografía de Curva Elíptica como una de las mejores técnicas a emplear para suplir los retos de seguridad en WBAN. Comparándolo, con otros métodos como AES y RSA, los tamaños de clave más pequeños de ECC son aptos para dispositivos computacionalmente menos capaces. ECC optimiza y reduce los tiempos de procesamiento matemático ofreciendo un mismo nivel de seguridad con menos cálculos. Además, es relativamente sencillo teniendo en cuenta que se aprovecha la complejidad en los caculos inversos. Permite cubrir varios requerimientos de seguridad WBAN como autenticidad, confiabilidad, integridad y no repudio. A todo ello se suma que es la sugerida en la normativa IEE 802.15.6, correspondiente a WBAN.

Finalmente, se recomienda desarrollar un Sistema de Seguridad aplicado a WBAN que se base en técnicas de Criptografía de Curva Elíptica, siguiendo las sugerencias de largo de clave de la última publicación de la norma NIST (National Institute of Standards and Technology).

2.3. Bases Teórico Científicas

2.3.1. Criptografía o Técnicas de Cifrado

Según (Jara & Pacheco, 2011). Actualmente hay dos tipos de cifrado, cifrado por bloques y cifrado por flujo, en esta sección nos concentraremos en el cifrado por bloques, por razones de implementación. Para salvaguardar la información a través de técnicas criptográficas, es necesario tomar en cuenta cuatro principios básicos de la seguridad de la información, siendo estos: **confidencialidad**, **integridad**, **autenticidad** y **no repudio**.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

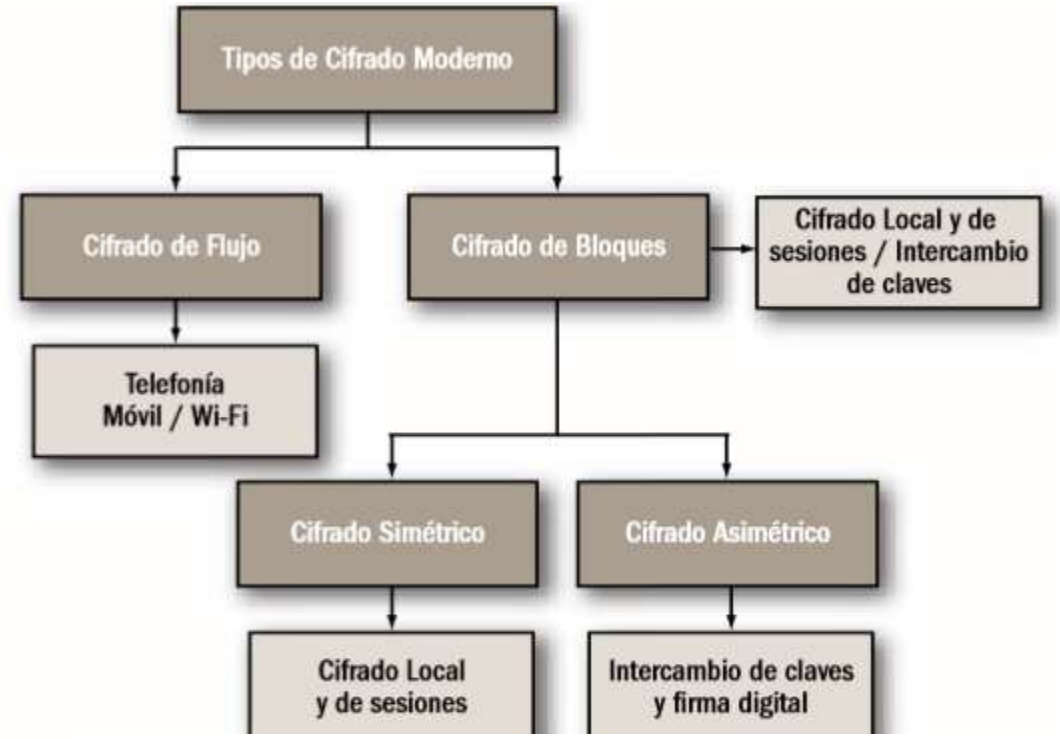


Figura N° 2. Tipos de Cifrado Moderno. Fuente: (Jara & Pacheco, 2011).

El primer paso es conocer que un sistema que ponga en práctica la criptografía (criptosistema), mantendrá un proceso similar al de la **Figura 3**. En cada situación, tendremos un mensaje en texto plano (**M**), que es la información que queremos almacenar o transferir; la clave (**K**), que teniendo en cuenta el tipo de algoritmo pueden ser dos, una para cifrar; y otra para descifrar; el algoritmo de cifrado, responsable de llevar a cabo los procesos de cifrado y descifrado; y finalmente, un mensaje cifrado (**C**), que es la información en texto sin cifrar después de haber culminado el progreso de cifrado.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

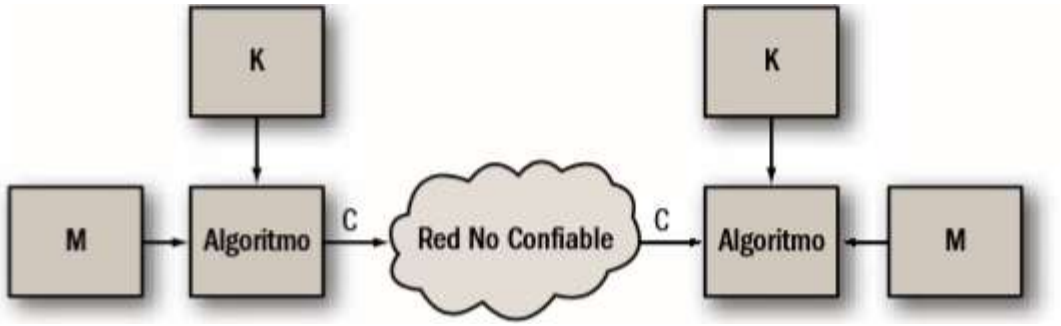


Figura N° 3. Criptosistema genérico, donde actúan un emisor y receptor en ubicaciones diferentes. Fuente: (Jara & Pacheco, 2011).

En una situación de transmisión entre dos puntos, una vez que el receptor ha aceptado el mensaje o la información que ha sido transmitida, se genera el proceso inverso obteniendo, el mensaje o la información en texto claro.

2.3.1.1 Criptografía Simétrica

La fundamental particularidad de la criptografía simétrica es emplear una única clave para cifrar y descifrar los mensajes semejantes a la **figura 3**, tanto la llave K usadas a la hora de cifrar como la utilizada al descifrar son las mismas.

Por este motivo la clave K se le acostumbra a denominar clave simétrica o clave secreta (**Ks**). De esta manera, preservamos la **confidencialidad**; después que la información está cifrada, ninguna persona ajena (es decir, que no tenga la llave K) accederá a ella en texto claro. Por lo tanto, aseguramos que uno de los principios de la seguridad de la información se siga sin impedimento alguno.

Una de características favorables de este tipo de algoritmo es que son muy veloces para cifrar y descifrar la información.

Un atributo considerable son las longitudes de claves que abarcan desde 128 hasta 256 bits, obteniendo categorías de cifrado de alta calidad, complicadas de romper si empleamos contraseñas fuertes. Estos algoritmos son débiles a la fuerza bruta, ya que con tiempo y medios disponibles es probable recorrer todo el espacio de llaves; el empleo de llaves de cifrado robustas es un factor

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

importante de apreciar. Por lo tanto, truncar una llave de longitud estándar cifrada con el algoritmo AES-256, retrasaríamos cientos de miles de años en alcanzar la llave indicada, o todavía, millones, sometiéndose a la capacidad de análisis que se necesite ejecutar.

El principal problema de estos algoritmos es no tener un proceso de intercambio de claves, por tal motivo, para que se cumplan los cuatro principios básicos de la seguridad de la información propuestos al comienzo, no son suficientes los algoritmos simétricos de clave secreta al poner en marcha un criptosistema.

Algoritmo	Tamaño de Claves (Bits)	Tamaño de Bloque (Bits)	Número de Etapas	Aplicaciones
DES	56	64	16	SET Kerberos
3DES	112 o 168	64	48	PGP, S/MIME
AES	128, 192 o 256	128	10, 12 o 14	
IDEA	128	64	8	PGP
Blowfish	Variable hasta 448	64	16	Varias
RC5	Variable hasta 2048	64	Variable hasta 256	Varias

Figura N° 4. Algoritmos de cifrado simétrico más conocidos. Fuente: (Jara & Pacheco, 2011).

2.3.1.2. Criptografía Asimétrica

En confrontación con la criptografía simétrica que empleaba una o más claves obedeciendo al algoritmo de cifrado, y este empleaba una única clave para cifrar y descifrar, familiarizada por el emisor y el receptor, llamada clave secreta o simétrica. A diferencia los algoritmos asimétricos de clave pública emplean **dos llaves**, una **pública** y una **privada**. La llave púbica puede saberla cualquiera sin algún peligro, mientras que la privada debe saberla únicamente su dueño. Consideremos que cuando ciframos con una, luego procedemos a descifrar con la otra.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Estos algoritmos, cubren conceptualmente tres requerimientos (confidencialidad, autenticidad y no repudio), son muy lentos en el proceso de cifrado de la información. Por tal motivo, necesitan trabajar en conjunto con algoritmos simétricos, que serán los responsables de cifrar los datos por transferir, así, asegurar la confidencialidad del mensaje o la información transferida.

Debido a la lentitud de los algoritmos de llave pública, solamente pueden cifrar limitadas cantidades de información; un ejemplo, sería AES que tiene una longitud de llave de 128 o 256 bits. De esta manera, el receptor aceptará la llave simétrica y, a partir de allí, ambos lados tendrán la capacidad de cifrar los datos con dicha llave (Ks), conservando la confidencialidad del mensaje. En la **Figura 5** observamos el proceso de intercambio de llaves entre un emisor A y un receptor B, ambos con sus llaves públicas y privadas.

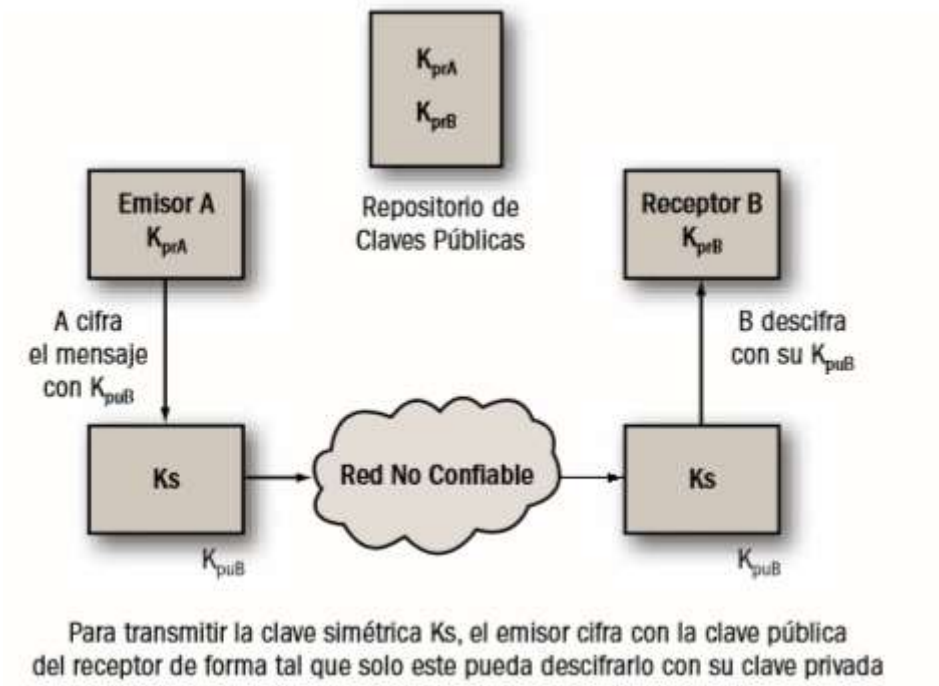


Figura N° 5. Proceso de cifrado Asimétrico Fuente: (Jara & Pacheco, 2011).

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Algoritmo	Cifrado/Descifrado	Firma Digital	Intercambio de clave
RSA	Sí	Sí	Sí
Diffie Hellman	No	No	Sí
Curva elíptica	Sí	Sí	Sí

Figura N° 6. Algoritmos de cifrado Asimétrico más conocidos**.** Fuente: (Jara & Pacheco, 2011).

Por motivos de implementación debido a los requerimientos de seguridad establecidos y que se tomarán sólo en cuenta la integridad y confidencialidad de la información, más no la autenticación y el no repudio, ya que en la transferencia de archivos en una red solo es necesario los primeros, por tal medida se ha llegado a la conclusión de utilizar algoritmos asimétricos juntos con algoritmos simétricos, siendo necesario las características de ambos. En conjunto éstos llevarán a cabo medidas de seguridad eficaces a la hora de transferir archivos en un entorno de red que sea fiable. (p. #254-264).

2.3.2 Técnicas de Ataque

Según (Jara & Pacheco, 2011). **Envenenamiento de la red: Poisoning**

Se basa en volver a trasmitir el tránsito de clientes auténticos a sitios administrados por un ciber criminal. Dicha técnica se logra al llevar a cabo la utilización de los protocolos ARP y DNS.

Un ataque ARP de este tipo también se le denomina ARP **spoofing**, que produce solicitudes y contestaciones ARP alteradas con el propósito de acoplar la dirección MAC del ciber criminal con la dirección IP de la puerta de enlace. De esta forma, la totalidad del tránsito de esta sección la tomará el ciber criminal que tendrá la oportunidad conocer los datos y al final volver a transmitir hacia

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

otro destino. Una manera conocida frente a esta técnica es empleando listas **ARP Estáticas**.

Análisis de protocolos: Sniffing

Es un examinador de protocolos o también denominado sniffer, dicha herramienta es empleada para **supervisar** y **examinar** el tránsito en una red, capturando todo el tránsito para luego analizarlo de acuerdo con los protocolos compatibles, empleando filtros avanzados. Al inicio ha sido creado para encontrar desaciertos y/o conflictos en los esquemas de diversas redes.

Con este modelo de herramientas es dable coger los datos para luego plasmarlos en texto claro. Por lo mismo, si un protocolo que transmita los datos sin cifrar, esta apto a ser víctima de un sniffer. Es compatible con: **HTTP**, **SMTP**, **POP3**, **IMAP**, **Telnet**, **FTP, etc.**

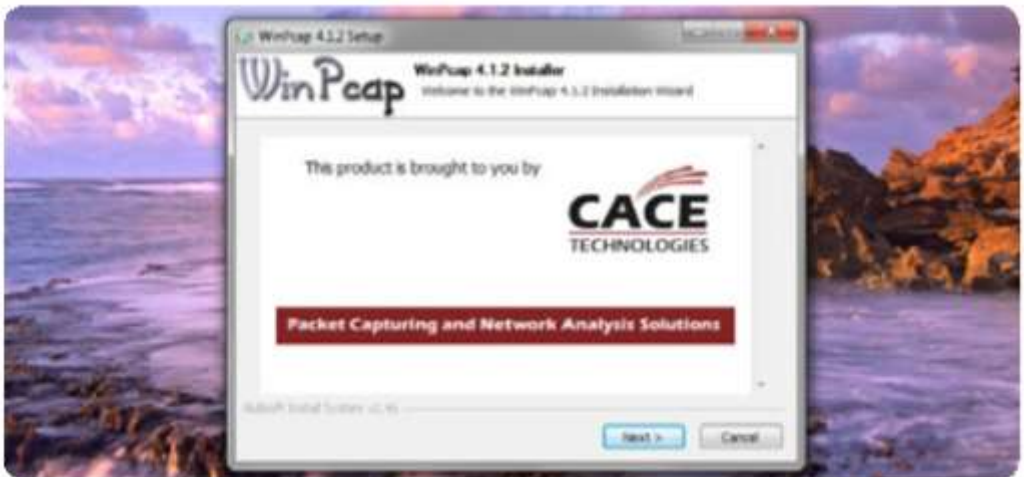


Figura N° 7. Herramienta Winpcap, sniffer empleado para ingresar a la capa de enlace de Windows. Fuente: (Jara & Pacheco, 2011).

Cuando en una red se emplean switches, existe una mayor facilidad de utilizar un **ARP poisoning,** ya que el switch es el que reenvía todos los paquetes de destino. Algunos sniffer pueden enviar paquetes particularmente generados, además de hacer la captura del tránsito necesario. Esto es muy beneficioso, en una red que ha sido segmentada por switches, haciendo posible un atentado ARP poisoning, así truncar las restricciones impuesta por estos mecanismos.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

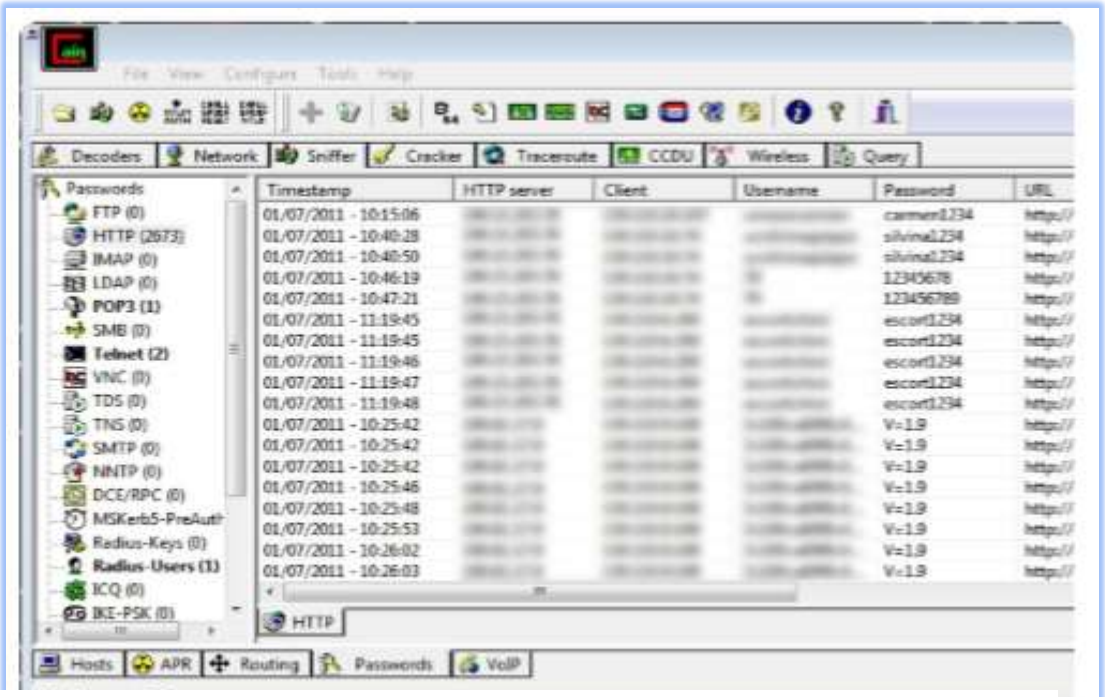


Figura N° 8. Herramienta **Caín**; en la sección contraseñas se visualizan algunas. Fuente: (Jara & Pacheco, 2011).

Entre las habilidades que poseen algunas herramientas de este tipo que las hace distintas entre ellas son: el arte de distinguir y categorizar protocolos inseguros acoplados con sus respectivas claves, la facultad de ejecutar atentados ARP poisoning, crear licencias digitales contra el protocolo SSL. Podríamos mencionar a **Caín** para entorno Windows, para entorno Linux **Ettercap.**

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

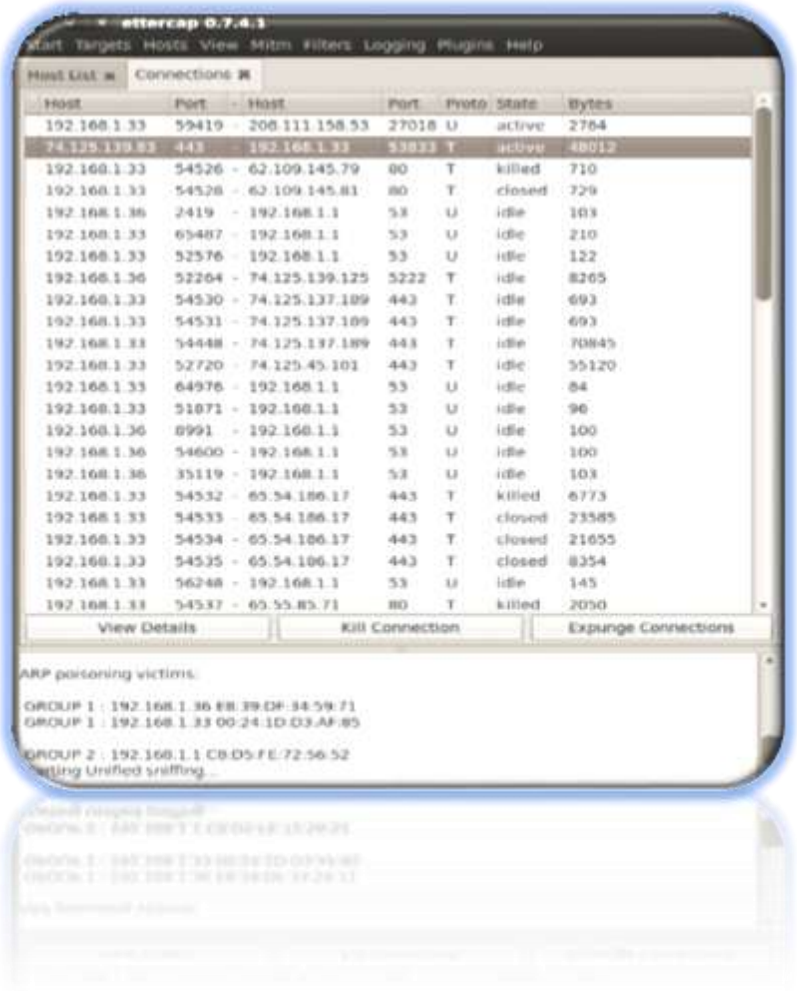


Figura N° 9. Herramienta **Ettercap**. Se visualizan las conexiones realizadas por el cliente. Fuente: (Jara & Pacheco, 2011).

De los sniffers más sobresalientes esta **Wireshark**, antes denominada **Ethereal**. Empleado, continuamente para examinar y encontrar fallos en redes de telecomunicaciones, además como un programa instructivo para examinar los diversos protocolos del modelo OSI, en tiempo vivo. Una de las características principales de esta herramienta es que tiene licencia GPL, interfaz dinámica y habilidades de filtros avanzados. Además, es compatible con archivos **tcpdump,** posee la habilidad de corregir sesiones TCP, siendo multiplataforma (p. #233-240).

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

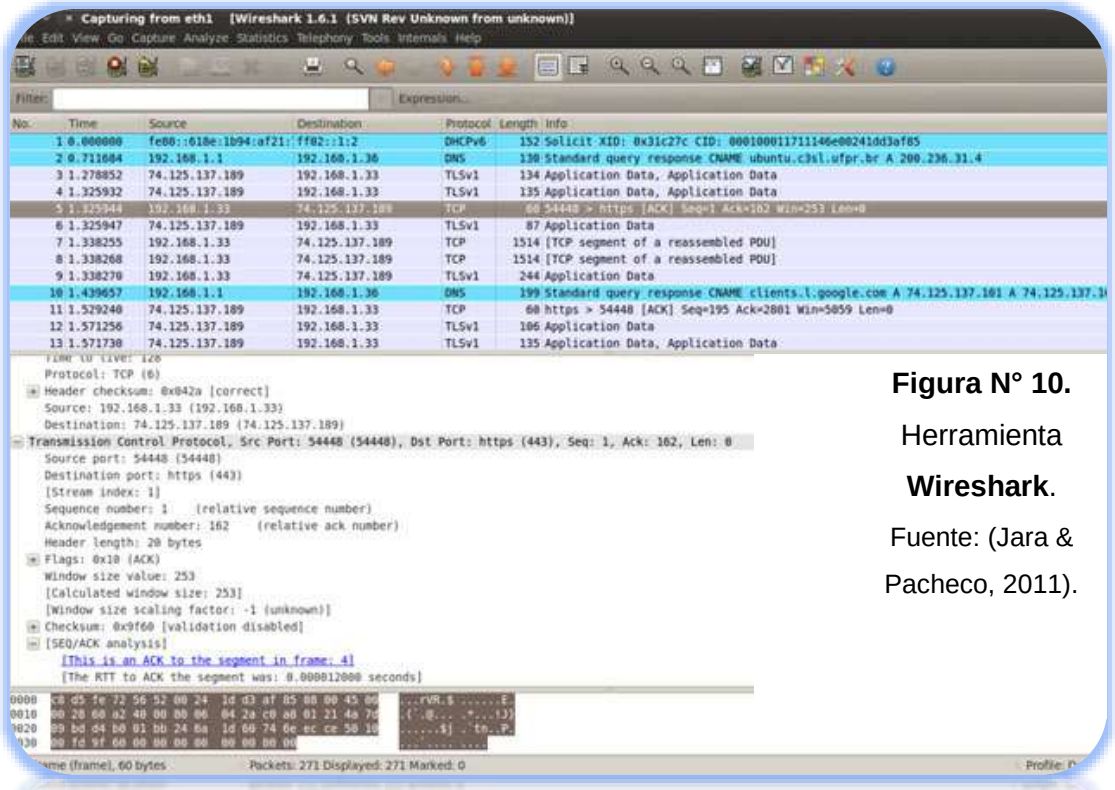


Figura N° 10. Herramienta **Wireshark**. Fuente: (Jara & Pacheco, 2011).

2.3.3 Características de los Servicios de Transferencia de archivos

Según (Montero, 2000). Existen diferentes mecanismos de transferencia de ficheros en la red. La elección de un sistema u otro vendrá determinada por las características del servicio que se desea proporcionar. Algunos factores que incluirán dicha elección son los siguientes:

Costes: el presupuesto disponible ha de tenerse siempre en cuenta en la planificación de la implantación de un servicio de transferencia de archivos. El presupuesto de una implantación lo componen principalmente tres conceptos:

a) **Hardware:** El hardware necesario para dicha implantación vendrá determinado por el mecanismo de transferencia seleccionado, así como por algunos otros factores enumerados en los siguientes puntos.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

b) **Software:** Costes relacionados con la adquisición de licencias y contratación de soporte por parte del proveedor.
c) **Gastos del Personal:** Ha de planificarse el número de horas de trabajo necesarias para llevar a cabo la implantación, el esfuerzo necesario para el mantenimiento diario de estos servicios o la formación requerida para los administradores de la plataforma o para los usuarios finales.

Número de Usuario: Estimación de la medida de usuarios habituales y el máximo número de usuarios hasta el que podría evolucionar el servicio. En relación a este factor, también ha de tenerse en cuenta el número de usuarios concurrentes que podrían hacer uso del servicio en mismo momento.

Tipos de Acceso: Se podrá dar servicio únicamente a los equipos ubicados dentro de una red privada o estar expuesto al acceso desde cualquier punto de Internet.

Multiplataforma: Entre los mecanismos y protocolos de transferencia existentes, algunos se caracterizan por estar orientados a proporcionar servicio a cualquier dispositivo independiente del sistema operativo utilizado. Algunos otros tienen su origen en sistemas propietarios, lo que, aunque dificulta el servicio multiplataforma, en la actualidad no supone una gran barrera para que los usen otros sistemas operativos distinto de aquellos para los que fueron diseñaos en un principio.

Ancho de banda: El ancho de banda necesario para proporcionar un servicio fiable variará dependiendo del mecanismo de transferencia seleccionado. El ancho de banda también se verá afectado por otros factores, como por ejemplo, el número de usuarios concurrentes o el nivel de seguridad requerida.

Seguridad, privacidad y auditoría: Existen algunos mecanismos y protocolos especialmente orientados a proporcionar una mayor seguridad en la transferencia de datos, identificando a los usuarios, asegurando la privacidad de los mismos e impidiendo que las tramas de datos sean capturadas por terceros no deseados.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Así pues, no debemos olvidar aspectos legales como la Ley Orgánica de Protección de Datos (LOPD), que nos obligará a auditar qué usuarios han accedido a la información sensible almacenada en el sistema o el obligado cumplimiento a respetar los derechos del autor fijados sobre determinados contenidos digitales.

Seguridad e integridad: Otra variante incluida en el concepto de seguridad es el asegurar que los archivos transferidos llegan íntegramente a su destino, es decir, que no se produzcan pérdidas de información que puedan dañar el archivo.

Alta Disponibilidad: Si se trata de un Servicio crítico que tenga que estar activo en todo momento, sin que se produzcan desfallecimientos del mismo. Este factor puede influir no solo en la elección del mecanismo de transferencia, sino también en la infraestructura que lo rodea. Por ejemplo, se pueden disponer de máquinas (hardware) duplicadas, para que en el caso de que se caiga un servidor, este puede ser sustituido inmediatamente por una copia del mismo. Otras técnicas relacionadas con la alta disponibilidad son la posibilidad del balanceo de la carga (peticiones del servicio) entre varias máquinas iguales, asegurando de este modo un nivel de servicio aceptable, independientemente del número de usuarios concurrentes.

2.3.3.1 Seguridad e Integridad en la Transferencia de datos

Una carencia del protocolo encargado en la transferencia de archivos en una red local (protocolo FTP), es la total ausencia de un mecanismo de seguridad que evite que terceras personas puedan capturar y leer los datos transferidos al servidor. El protocolo FTP envía incluso el usuario y contraseña de inicio de sesión de forma descubierta, sin ningún tipo de encriptación o cifrado.

Para solventar estas carencias, se implementó el denominado protocolo de transferencia segura FTPS, que trabaja con seguridad basada en SSL/TLS.

La capa de seguridad SSL es un sistema muy extendido en Internet, se aplica en numerosos protocolos, como por ejemplo, HTTP, SMTP u otros mecanismos

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

basados en la capa de transporte TCP, SSL proporciona seguridad en tres sentidos:

Confidencialidad: Permite encriptar los datos enviados de forma que solo puedan ser desencriptados por el destinatario de la transmisión.

Verificación de los actores: Un usuario tendrá la certeza de estar enviando los datos al servidor correcto, sin posibilidad de suplantación de identidad, que es un ataque muy conocido realizado por un pirata informático.

Integridad del mensaje: Asegura que un mensaje recibido no ha sido interceptado y modificado por terceros.

La seguridad SSL se consigue gracias a certificados digitales controlados por agencias de certificación debidamente homologadas.

FTPS puede encriptar tanto el canal de control o comandos como el canal de datos, aunque generalmente, con cifrar el canal de control es suficiente para asegurar la comunicación.

2.3.3.1.1 Servicios NFS

NFS es protocolo de la capa de aplicación que permite compartir archivos a través de una red TCP/IP. NFS fue creado por Sun MicroSystems en los años 80, extendiéndose rápidamente por la mayoría de sistemas operativos Unix y Linux. NFS permite trabajar de forma transparente para el usuario, con archivos o directorios remotos como si de elementos locales se tratasen. Algunas ventajas son:

a. Las estaciones locales de trabajo no requerirán de discos duros con grandes capacidades ya que delegarán parte de su almacenamiento a los sistemas remotos.
b. Un mismo directorio remoto puede ser compartido por varios usuarios.
c. Ayuda a la centralización de la información y el conocimiento dentro de una organización.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

d. Los usuarios no necesitarán conocer comandos específicos para usar este protocolo, al contrario de lo que sucede con FTP. Al encontrarse representadas las carpetas remotas como directorios locales, los comandos para acceder a ellas serán los del propio sistema operativo.

Cuando hablamos del protocolo NFS pensamos en una arquitectura cliente-servidor, donde el cliente "mapeará" carpetas remotas y el servidor, generalmente Unix/Linux, pondrá en marcha una serie de servicios especiales que le permitirán compartir sus directorios en red.
Un Servidor NFS utilizará el control de acceso al sistema de archivos propio de Unix/Linux. Por lo tanto, los clientes deberán estar dados de alta como usuarios de la máquina que contiene los servicios NFS. Cuando un usuario se conecta, el servidor examinará la petición para comprobar si el usuario dispone de la autorización necesaria para acceder al recurso. Una vez verificada la autorización, el servidor retornará al cliente un identificador (magic cookie) que deberá usar en sus futuros accesos.

2.3.3.1.2 Servicios CIFS/SMB

SMB/CIFS es el protocolo en el que se basan la mayoría de redes locales Windows. Entre otras muchas funcionalidades, permite compartir ficheros y otros recursos (como impresoras), entre los terminales de la red.

Podemos afirmar que se trata de un protocolo de tipo cliente-servidor, donde cualquiera de los nodos de la red puede actuar como cliente, en el caso de que este quiera acceder a recursos remotos, o como servidor, si publica información accesible por otros equipos de la red.

SMB es un protocolo basado en comandos que pertenecen al nivel de aplicación del modelo de capas de red TCP/IP, abarcando también la capa de presentación del modelo OSI.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Además de establecer la encriptación de los datos que viajen por la red, también se pueden establecer permisos de acceso a los recursos compartidos mediante los siguientes mecanismos:

a. User level security: se gestionan directamente los usuarios que tienen acceso al recurso compartido, otorgando permisos de lectura, escritura.
b. Share level security: Consiste en proteger un recurso bajo una contraseña. Donde los clientes deberán conocer dicha contraseña establecida por el servidor, para consumir dicho recurso.

2.3.3.1.3 SAMBA: Accediendo a Redes CIFS/SMB desde LINUX/UNIX

SAMBA es una implementación libre de los protocolos CIFS/SMB para sistemas operativos UNIX, mediante la cual cualquier sistema operativo podrá adherirse a una red Windows y compartir o consumir recursos de la misma.

SAMBA fue implementado originalmente para UNIX por Andrew Tridgell, quien tuvo que descifrar los paquetes de información que viajaban en una red Windows para llevar a cabo su proyecto, ya que el protocolo CIFS es un protocolo propietario y su implementación no es pública.

SAMBA está compuesta por un conjunto de aplicaciones y servicios que, entre otras, nos ofrecen las siguientes funcionalidades:

a. Compartir o consumir archivos y carpetas.
b. Compartir o utilizar impresoras en red.
c. Visualizar y navegar a través de los equipos de la red.
d. Autenticación en el dominio de Windows.
e. Resolución de nombres.

2.3.3.1.4 SFTP (SSH File Transfer Protocol)

Es un protocolo de nivel aplicación que permite una transferencia fiable de ficheros en un entorno cliente – servidor. Aunque su funcionalidad se asemeja

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

a la de los protocolos FTP o FTPS, no es exactamente igual, ya que se trata de un protocolo independiente al que se le añadieron características del FTP.

Tiene como predecesor al protocolo SCP (Secure Copy) y generalmente opera en el puerto 22 usando un único canal para la comunicación (al contrario que el FTP, que usaba dos). Como Seguridad y encriptación utiliza SSH (Secure Shell), intérprete de comandos seguro con gran aceptación entre los sistemas Unix/Linux. Se considera un protocolo mucho más seguro que el FTPS mencionado previamente. Al igual que en FTP, usa clientes específicos (clientes gráficos o basados en comandos) para acceder a los servicios SFTP.

Tanto el protocolo SFTP como el FTPS utilizan un algoritmo de Encriptación Asimétrico (RSA, DSA), un algoritmo simétrico (AES) y un algoritmo de intercambio de claves. Para la autenticación, FTPS, utiliza certificados X.509, mientras que SFTP utiliza las claves SSH.

Técnicamente **SFTP** es más avanzado que **FTPS**, sin embargo, algunos dispositivos pueden no ser compatibles con SFTP (como los móviles, consolas, etc.), en cambio con FTPS sí lo son ya que es una extensión de FTP.

2.3.3.1.5 TFTP

TFTP (Trivial File Transfer Protocol) es un protocolo de la capa de aplicación basado en FTP pero mucho más simplificado. Suele ser utilizado para transferir pequeños ficheros en una red. Podemos encontrar este protocolo en mecanismos de actualización de firmware de routers y switches o en mecanismos de arranque remoto de terminales sin requerir el uso de discos duros locales.

TFTP es un protocolo de transferencia muy básico y limitado. En total solo existen cinco tipos de paquetes a transmitir u operaciones que puede realizar:

a. Petición de lectura (Read request [RRQ]).
b. Petición de escritura (Write request [WRQ]).
c. Transferencia de datos (DATA)
d. Reconocimiento o respuesta de conformación (ACK).

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

e. Error (ERROR).

2.3.3.1.6 FXP

FXP (File eXchange Protocol) es un protocolo que permite la transferencia directa de datos entre dos servidores FTP, siendo simplemente administrada por un cliente. Se trata de una extensión de FTP que nos ayudará a administrar nuestros servidores.

Tal y como se muestra en la figura 11, utilizando el protocolo FXP la transferencia entre los dos servidores será directa y la velocidad de la misma dependerá del ancho de banda de la conexión entre los servidores, independientemente del ancho de banda del cliente.

Muchos servidores FTP disponen de opciones para habilitar el protocolo FXP, ya que por defecto esta opción suele encontrarse deshabilitada por ser conocido que puede provocar problemas o agujeros de seguridad. También encontraremos clientes gráficos que facilitan la transferencia FXP entre servidores. (p. #14-31).

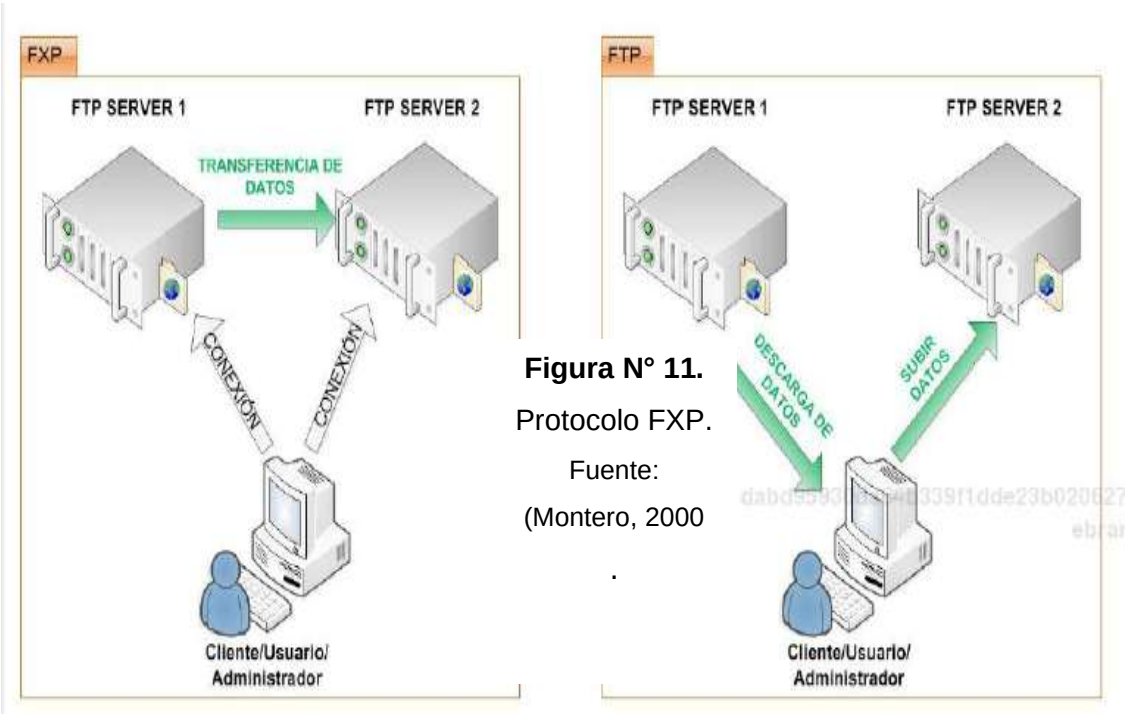


Figura N° 11.
Protocolo FXP.
Fuente:
(Montero, 2000
.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

2.3.3.2 Algoritmos Criptográficos más frecuentemente utilizados

Según (Gonzáles & Fuentes, 2014). Numerosos son los algoritmos existentes tanto en la criptografía de clave privada como de clave pública. De los primeros es posible destacar: DES, Triple DES, AES, IDEA y Blowfish. Por otro lado, entre los algoritmos de clave pública cabe destacar a RSA y el Gamal. Sin embargo, dadas las debilidades y fortalezas de la criptografía pública y privada, otro tipo de algoritmos (conocidos como híbridos) son frecuentemente utilizados.

2.3.3.2.1 Algoritmos de criptografía de clave secreta

Data Encryption Estándar (DES)

Este algoritmo es uno de los más utilizados. Fue adoptado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) en 1997. Sin embargo, en 1998 DES fue atascado en 56 horas en un primer momento y en 22 horas posteriormente (DES cracker), surgiendo la necesidad de crear un algoritmo más robusto. En 2001 este algoritmo es sustituido por AES.

El algoritmo DES se basa en un cifrador de bloque en el que la clave es de 64 bits, dividiendo el mensaje en bloques de igual tamaño a la clave. En cuanto a la base matemática que lo soporta, esta consiste en sustituciones, lineales y no lineales, y en permutaciones. En concreto, el algoritmo presentado en la Figura 17, se puede dividir en los siguientes pasos:

1. El mensaje a cifrar se divide en bloques.
2. Se Selecciona un bloque y se descompone en 64 bits.
3. Sobre el bloque se realiza una permutación inicial (IP), la cual consiste en cambiar de orden todos los bits en base a unos criterios establecidos.
4. Por cada bloque permutado se producen un total de 16 rondas, en cada una de las cuales se realizan los siguientes pasos:
    a. El bloque se divide en dos partes, izquierda (L_o) y derecha (R_o), cada una de ellas de 32 bits.
    b. A R_o se le introduce en una caja E, en donde se realiza una permutación y una expansión, obteniendo como resultado un bloque de 48 bits.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

c. A la salida de la caja E se le aplica una operación OR exclusivo (XOR) con una clave de ronda de 48 bits.
d. El resultado de la operación anterior se introduce en las Cajas S. Estas cajas, un total de ocho, se corresponden con un conjunto de ocho matrices, donde cada una de ellas toma como entrada un conjunto de seis bits consecutivos y produce 4 bits de salida.
e. Tras la salida de las Cajas S, a los 32 bits resultantes se les ejecuta una permutación final.
f. Para terminar, la ronda finaliza con un XOR entre los bits permutados y L_o, obteniendo R_1 (es decir, el bloque derecho de la siguiente ronda) y considerando que en la siguiente ronda el bloque izquierdo (L_1) será R_o.

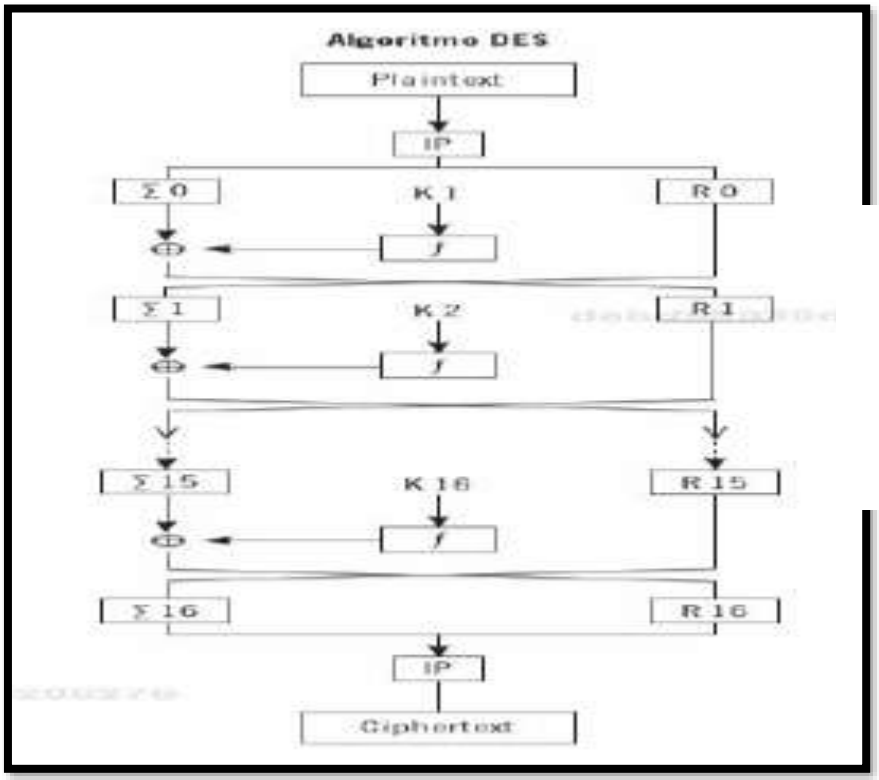


Figura N° 12. Algoritmo Asimétrico DES. Fuente: (Gonzáles & Fuentes, 2014)

.

Triple DES

En 1999 se crea Triple DES, que consiste en el encadenamiento de tres funciones DES. Particularmente, su forma más común está basada en el uso

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

de dos claves, de forma que se cifran con la primera, el resultado se descifra con la segunda y a su vez el resultado se cifra con la tercera.

International Data Encryption Algorithm (IDEA)

IDEA, creado en 1991, tenía como objetivo reemplazar el algoritmo DES. Es un cifrador de bloque que opera sobre bloques de 64 bits, claves de 128 bits y un total de 8 rondas. Además este algoritmo fue utilizado en las primeras versiones de PGP, uno delos programas de cifrado más comúnmente utilizados en los últimos tiempos.

El proceso de funcionamiento de IDEA se basa en ejecutar operaciones algebraicas no conmutativas de grupos algebraicos diferentes (XOR, sumas y multiplicaciones) sobre bloques y las subclaves utilizadas.

Blowfish

Se desarrolló en 1993 con el objetivo de reemplazar al algoritmo DES o IDEA pero no llegó a convertirse en estándar. Actualmente Blowfish es un algoritmo público que está a disposición de los usuarios.

Blowfish es un cifrador de bloque que opera sobre bloques de 64 bits con unos tamaños de claves desde 32 a 448 bits. Su funcionamiento consiste en la ejecución de 16 rondas, aplicando el cifrador de Feistel, en las que se hace uso de claves dependientes de las Cajas S (igual a DES).

Advanced Encryption Estándar (AES)

Como mejora de DES y Triple DES se propone AES, basado en el algoritmo Rijndael. Este algoritmo fue escogido en 2001 por el NIST como el nuevo estándar para comunicaciones gubernamentales, transferencias de fondos bancarios, comunicaciones por satélite y software libre.

Es un cifrador de bloque que opera sobre bloques de 128 bits y claves de 120, 192 o 256 bits con subclaves de 128 bits. Este algoritmo es rápido tanto a nivel hardware como software, fácil de implementar y requiere poca memoria. Matemáticamente está basado en cuatro funciones invertibles que se aplican a

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

los bytes de una matriz llamada **Estado**, durante un número determinado de rondas. A grandes rasgos, el algoritmo funciona del siguiente modo:

1. El mensaje a cifrar se divide en bloques.
2. La matriz **Estado** se carga inicialmente con el XOR de los bytes del bloque de entrada y la primera de las subclaves generadas.
3. Para cada bloque y por un conjunto N de rondas, a la matriz **Estado** se le pasa consecutivamente por las siguientes funciones:
    a. SubBytes: función no lineal realizada a través de una caja S (S-box).
    b. ShiftRows: función que desplaza bloques de un byte hacia la izquierda módulo columna dentro de una fila. Por ejemplo, suponiendo una matriz 4x4, la fila 0 no se desplazaría, la fila 1 se desplazaría un byte, la fila 2 se desplaza 2 bytes y la fila 3 se desplaza 3 bytes:

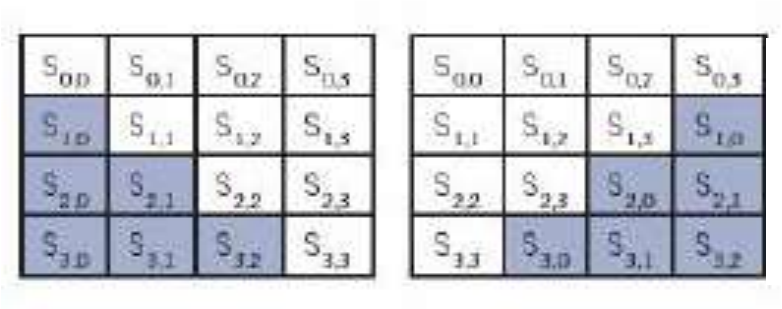


Figura N° 13. Matriz Estado AES. Fuente: (Gonzáles & Fuentes, 2014)

    c. MixColumns: función matemática compleja. Simplificando su descripción, está función multiplica columnas por un polinomio fijo.
    d. AddRoundKey: función que, en la primera ronda y al final de cada ronda, aplica un XOR entre el bloque implicado y la clave de ronda.

2.3.3.2.2 Algoritmos de criptografía de clave pública

Los algoritmos más conocidos son el algoritmo RSA, basado en el problema de la factorización, y el algoritmo EL Gamal, basado en el problema del logaritmo discreto.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

RSA

Este algoritmo fue creado en 1978 por Rivest, Shamir y Adleman, de donde proviene el nombre RSA, y destaca por ser el primer algoritmo efectivo de clave pública. Otros algoritmos fueron creados y todos ellos fueron rotos, permaneciendo este.

A diferencia de El Gamal, RSA utiliza el mismo algoritmo tanto para el cifrado como para la firma electrónica. En ambos casos, el proceso utiliza la clave pública para una operación (envío de mensajes cifrados / verificación de la firma) y la privada para la contraria (descifrado de mensajes / realización de una firma).

Es preciso señalar los dos conceptos básicos sobre los que se desarrolla RSA. En primer lugar, la operación módulo (que aparece en la ya citada aritmética modular). El segundo concepto es el indicador de Euler para un determinado número n, que se representa como ø (n). Se define como la cantidad de números naturales menores o iguales a n cuyo máximo común divisor (m.c.d) con n es exactamente 1. Los números que cumplen esta propiedad se denominan **primos relativos**.

Utilizando ambos conceptos es posible comprender el proceso seguido por RSA. Considérese el caso de cifrado de la información. Suponiendo que A quiere mandar un mensaje cifrado a B, el proceso de ejecución es el siguiente:

1. A escoge dos números primos muy grandes y no públicos, p y q, de modo que obtiene n=p.q.
   A escoge un número entero e que sea primo relativo con ø (n).
   A escoge un número d tal que e.d=1mod (ø (n)).
   La clave pública de A es (e,n), mientras que la clave privada es (d,n).
   A distribuye su clave pública utilizando cualquiera de los mecanismos de distribución de claves públicas.
2. B envía un mensaje cifrado (que llamaremos M) a A, $C = M^e \bmod(n)$.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Esta operación se realiza primero, multiplicando el mensaje por sí mismo tantas veces como indique “e” y, posteriormente, se obtiene el resto de dividir el resultado por el número “n”. Es importante resaltar que el mensaje M tiene que ser numérico, por lo que si fuese un texto será necesario representarlo como número.

3. A descifra el mensaje haciendo uso de la clave privada, $M = C^d \bmod(n)$.

ElGamal

Es un algoritmo basado en el protocolo de intercambio de claves Diffie-Hellman. Fue creado en 1984 y es utilizado en versiones recientes del programa de ordenador PGP.

El Gamal se basa en el problema del logaritmo discreto y puede utilizarse tanto para cifrar como para firmar, aunque los algoritmos son distintos. La principal diferencia frente a RSA radica en que en El Gamal cada operación de cifrado sobre el mismo dato produce un resultado distinto, lo que complica el criptoanálisis.

2.3.3.2.3 Algoritmos Híbridos

La criptografía de clave secreta y pública tiene ventajas y desventajas opuestas. Es posible destacar que la criptografía de clave secreta, en contraposición con la de clave pública, es rápida pero necesita de la existencia de un canal seguro para los intercambios de la claves y, además, la gestión de un elevado número de claves es un proceso complejo. Por tanto, haciendo uso de la ventajas de la criptografía de clave pública y privada simultáneamente, se desarrollan los criptosistemas híbridos. Estos algoritmos están basados en la aplicación de un algoritmo de clave pública y otro de clave privada.

Asumiendo que se desea enviar un mensaje desde A a B, el proceso de ejecución consiste en los siguientes pasos:

a. A cifra un mensaje utilizando un algoritmo de cifrado de clave privada, como por ejemplo DES.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

b. La clave utilizada en el paso anterior (representada por k_S) se cifra utilizando un algoritmo de clave pública (como RSA) usando la clave pública de B.

c. A envía el resultado de ambas operaciones a B.

d. B descifra primero la clave simétrica k_S haciendo uso de su clave privada. Posteriormente, utiliza k_S para descifrar el mensaje. (p. #41-48).

2.4. Definición de términos básicos

Amenaza: Es la probabilidad de que ocurra un evento no deseado, situación o evento con el que se puede provocar daños en un sistema.

Auténtico: Debe cumplir las siguientes características de integridad, Autenticación, no repudio, y válido:

Integridad: Los activos informáticos y la información transmitida puede ser modificado solo por las partes autorizadas. Las modificaciones incluyen la escritura, el cambio de estado, la eliminación o repetición de mensajes.

Autenticación: Se refiere a que el origen del mensaje sea correctamente identificado con la seguridad de que la identidad no es falsa.

No repudio: Se refiere a que ni el emisor ni el receptor de un mensaje pueden negar posteriormente el haber efectuado la transmisión, como así también su recepción (previamente validada por el sistema).

Válido: La validez del contenido del mensaje está dada por las conciliaciones y controles administrativos.

Caballo de Troya (o troyano): Programa informático de aspecto inofensivo que oculta en su interior un código que permite abrir una “puerta trasera” en el sistema en el que se ejecuta.

Capacidad de Conexión Segura (SSL): Protocolo que permite transmitir, cifrada y segura la información a través de la red

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Confidencialidad: Requisito de seguridad que indica que el acceso a los recursos del sistema debe estar limitado exclusivamente a los usuarios con acceso autorizado.

Clave Pública: Es la clave que se distribuye a todas las personas que vayan a tener contacto con el destinatario, con ella se hará el cifrado del mensaje.

Clave Privada: Clave que sólo será conocida por el destinatario y está servirá para desencriptar el mensaje cifrado con la clave pública correspondiente.

Cracker: Es considerado un vándalo virtual que utiliza sus conocimientos para invadir sistemas, descifrar claves, contraseñas de programas, algoritmos de encriptación, etc.

Cracker de Sistemas: Término designado a programadores y decoders que alteran el contenido de un determinado programa, por ejemplo, alterando fechas de expiración de un determinado programa para hacerlo funcionar como si se tratara de una copia legítima.

Cracker de Criptografía: Término usado para aquellos que se dedican a la ruptura de criptografía (cracking codes).

Cifrado por bloques: División del mensaje de una longitud fija que pasará al proceso de cifrado uno a uno.

Criptografía: El estudio de técnicas para cifrar información de tal manera que no sea legible para personas a las que no vaya destinado, esto por medio de técnicas que normalmente se basan en procesos matemáticos.

Criptoanálisis: Estudio complementario de la criptografía, con el propósito de demostrar la seguridad de un algoritmo o sistema criptográfico, consiguiendo la información legible sin la necesidad de respetar claves o procesos establecidos del algoritmo o sistema.

Cyberpunk: Son los vándalos de páginas web o sistemas informatizados. Destruyen el trabajo ajeno

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Decodificación: Volver al texto original para ser leído.

Encriptación: Método de codificar o encriptar datos para evitar que usuarios no autorizados puedan leerlos o alterarlos. Solo los usuarios con acceso a una contraseña o una clave podrán desencriptar y utilizar los datos. Estos datos pueden ser mensajes, archivos, carpetas o discos.

Estenografía: Arte de transmitir información de modo que la presencia de la mismo pase inadvertida. Se suele hacer camuflando los datos en el interior de un texto, imagen o fichero multimedia.

Fraude: Manipular la información con el fin de obtener un beneficio propio.

Hardening: Herramienta indispensable que tiene como objetivo prevenir incidentes. Adapta los sistemas de forma segura y personalizada. Proceso de reducción de posibles vulnerabilidades de un sistema.

Medida de Seguridad: Proceso, procedimiento, técnica o función destinada a mitigar los efectos del riesgo. Las medidas de seguridad rara vez eliminan el riesgo, sino que lo reducen a un nivel aceptable.

Phreaker: Cracker especializado en telefonía. Tiene conocimiento para hacer llamadas gratuitas, reprogramar centrales telefónicas, grabar conversaciones de otros teléfonos para luego escuchar la conversación en su propio teléfono, etc.

Puerta trasera: Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta.

Riesgo: Amenaza que explota una vulnerabilidad que puede causar daño a uno o más activos.

Servicios de Seguridad: Servicios de administración de seguridad, supervisión y respuesta que permiten a las organizaciones beneficiarse del saber de los expertos en seguridad de Internet para proteger el valor de sus activos y sus infraestructuras de red.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Virus: Programa malicioso con el objetivo de demostrar intelectualidad respecto al programador o hacker y otras veces con fines de sabotaje o fraude.

Virus Encriptado: Virus que utiliza la encriptación para ocultarse de los escáneres de virus. Es decir, el virus encriptado altera el código de programa para que no se pueda detectar.

Vulnerabilidad: Una vulnerabilidad (universal) es un estado en un sistema informático (o conjunto de sistemas) que:

- Permite a un atacante ejecutar comandos como otro usuario.
- Permite a un atacante acceder a los datos en contra de las restricciones de acceso especificadas para esos datos.
- Permite a un atacante hacerse pasar por otra entidad.
- Permite a un atacante realizar una navegación de servicio.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

CAPITULO III: MARCO METODOLÓGICO

3.1. Tipo y Diseño de la Investigación

3.1.1. Tipo de Investigación

La presente investigación es del tipo cuantitativo, porque dirige a una respuesta final y reducen las direcciones posibles que la investigación pueda tomar.

3.1.2. Diseño de Investigación

Su diseño es Cuasi-Experimental, porque se elegirá los datos y el escenario a utilizar.

3.2. Población y Muestra

3.2.1. Población.

Se ha determinado realizarse 5 pruebas de transferencias de archivos, en cada prueba se transferirá 20 archivos, en base a la investigación de (Bareño, Navarro & Cárdenas, 2015)."*Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV6*". Donde se ha realizado 4 pruebas de implementación de servicios corporativos como FTP y SSH, en 4 sistemas operativos diferentes: Windows Server 2008 y server 2012 R2, además Linux debían y Ubuntu server, utilizando máquinas virtuales como el VirtualBox y el análisis de tráfico se realizó con la herramienta Wireshark, finalmente las implementaciones sobre Linux permitieron un nivel de seguridad mayor en autenticación, confidencialidad e integridad.

3.2.2. Muestra.

La muestra en este caso es poblacional debido a la naturaleza de la investigación ya que es necesario contar con la mayor cantidad de archivos en la red, es decir 5 pruebas de 20 transferencias de archivos.

3.3. Hipótesis

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

La aplicación de técnicas de Encriptación de los datos mejorará la seguridad en la transferencia de archivos en un entorno de red para que sea Fiable.

3.4. Variables

3.4.1. Variable dependiente

Seguridad en la transferencia de archivos.

3.4.2. Variable independiente

Las técnicas de Encriptación.

3.5. Operacionalización

Variable Dependiente	Dimensiones	Indicadores	Fórmula	Instrumentos de recolección de datos
Seguridad en la transferencia de archivos	Medidas de rendimiento	Cantidad Archivos encriptados	$\sum n = (n1 + n2 + n3 + .. + n)$	Sniffer, observación, ficha técnica
		Cantidad Archivos desencriptados	$\sum n = (n1 + n2 + n3 + .. + n)$	
		Cantidad Archivos Encapsulados	$\sum n = (n1 + n2 + n3 + .. + n)$	
		Cantidad Archivos Desencapsulados	$\sum n = (n1 + n2 + n3 + .. + n)$	

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Variable Independiente	Dimensiones	Indicadores	Fórmula	Instrumentos de recolección de datos
Técnicas de Encriptación	Encriptación simétrica	Tiempo de Procesamiento	$\dot{X} = \frac{X1 + X2 + X3 + \cdots + Xn}{N}$	Sniffer, observación, ficha técnica
		Margen Error - en la transmisión	$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{N}}$	
	Encriptación Asimétrica	Longitud de Clave	N° bits	Sniffer, observación, ficha técnica

3.6. Abordaje Metodológico, técnicas e instrumentos de recolección de datos

3.6.1 Abordaje Metodológico

El abordaje metodológico es Cuasi-Experimental, porque se elegirá los datos y el escenario a utilizar.

3.6.2 Técnicas de Recolección de datos

a) Observación

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Se observarán todos los eventos a lo largo de la investigación. Nos enfocaremos en el análisis de la topología de la red que se diseñará a partir de un esquema físico y lógico de una red local, luego se procederá a la configuración de la topología y posteriormente se evaluará la misma a través de una simulación o prueba de la topología de la red.

3.6.3 Instrumentos de Recolección de datos

a) Técnicas: Registro de Observaciones

Se usan para recopilar los datos de las pruebas. Registrando cada prueba realizada al esquema de la topología de la red. En Particular los datos arrojados por el analizador de paquetes se registrarán.

b) Sniffer

Software de captura de paquetes. Se procederá a instalar el analizador de paquetes de la red, para las pruebas pertinentes del tráfico de la red. Se realizará mediante la puesta en ejecución de las técnicas usadas para evaluar el desempeño de cada una de ellas de acuerdo con los indicadores que se han establecido.

3.7. Procedimiento para la recolección de datos

El desarrollo de la siguiente investigación se ha basado en la utilización de técnicas o instrumentos de recopilación de datos:

a) Observación

1. Análisis de la topología: Esquema del prototipo de la red.
2. Diseño de la topología: Esquema lógico y físico de la red.
3. Configuración de la topología: Implementación de la topología de la red.
4. Prueba de la topología: Simulación del Prototipo de red.

b) Registro de las Observaciones

1. Registro de las Configuraciones: Implementación de la topología propuesta.
2. Registro de las Pruebas: El testeo correspondiente de las técnicas

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

utilizadas.

c) Sniffer

1. Instalación de analizador de paquetes del tráfico de la red: Implementación de analizador de paquetes de la red.
2. Configuración de analizador de paquetes: Determinación de las opciones predeterminadas, para analizar la red.
3. Prueba de analizador de paquetes: Puesta en marcha del Programa de análisis de paquetes de la red.

3.8. Análisis estadístico e interpretación de los datos

a) Tabulación de datos

Uso de tablas estadísticas

Uso de gráficos estadísticos como producto del procesamiento de los datos obtenidos de las pruebas realizadas y procesadas.

b) Análisis de datos

Interpretación de indicadores de acuerdo con las pruebas que se realizaran.

Sumatorias: Llamada también notación Sigma, es una operación matemática que se emplea para calcular la suma de muchos o infinitos sumandos, su sintaxis es la siguiente: $\sum n = (\mathrm{n1} + \mathrm{n2} + \mathrm{n3} + .. + \mathrm{n})$

Media Aritmética: La media aritmética es el valor obtenido al sumar todos los datos y dividir el resultado entre el número total de datos. Su sintaxis es la siguiente: $\dot{X} = \frac{X1 + X2 + X3 + \cdots + Xn}{N}$

Donde: X1= T1; T1=TF-TI

X1: Prueba 1; T1: Tiempo 1 para la prueba 1.

TF: Intervalo final. TI: Intervalo inicial.

Desviación Estándar: Esta fórmula se utilizará para la determinar el margen de error en la seguridad de la transmisión de los datos.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_n - \bar{x})^2}{N}}$$

Veamos: Digamos que tenemos el tiempo de procesamiento de cada prueba que se ha analizado en diferentes escenarios, para ello tenemos: 8 pruebas con sus respectivos tiempos de procesamiento.

9, 3, 8, 8, 9, 8, 9, 18

$$\dot{X} = \frac{9+3+8+8+9+8+9+18}{8} = 9$$

$$\frac{\sqrt{(9-9)^2 + (3-9)^2 + (8-9)^2 + (8-9)^2 + (9-9)^2 + (8-9)^2 + (9-9)^2 + (18-9)^2}}{8}$$

$$= 3.87\%$$

En este caso la desviación estándar para el margen de error ha dado como resultado, 3.87%, que determina que existe un mínimo de margen de error posible en la transmisión de los datos.

3.9. Principios éticos

a) **Objetividad:** El análisis de la situación encontrada se basará en criterios técnicos imparciales

b) **Confidencialidad:** Se asegurará que los registros usados para la prueba que son de un ámbito privado no se hagan públicos.

c) **Veracidad:** La información mostrada será verdadera

d) Integridad: La información utilizada no sufrirá modificaciones a lo largo de la investigación.

3.10. Criterios de Rigor Científico

a) **Validación:** Se validarán los instrumentos de recolección de datos

b) Contrastación: Se contrastará la hipótesis a través de métodos estadísticos debido al diseño cuasi experimental.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1. Resultados en Tablas y Gráficos

4.1.1 Tiempo de Procesamiento, Longitud de Clave

Tabla Nª 1: Tiempo de Procesamiento, Longitud de Clave de Técnica 1

1º Técnica de Encriptación	Tiempo Procesamiento				
	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5
RSA de 2048 bits de clave, con cifrado AES de 256 bits	99, 443 seg	36, 507 seg	19, 848 seg	44, 133 seg	25, 341 seg
Tiempo Procesamiento Total	**45, 0544 seg**				
Transferencias	20	20	20	20	20
Total Transferencias	100				
Paquetes	1 452	1 516	1 256	1 494	1 470
Longitud de Clave	2048 bits				

Tabla Nª 2: Tiempo de Procesamiento, Longitud de Clave de Técnica 2

2º Técnicas de Encriptación	Tiempo Procesamiento				
	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5
RSA de 1024 bits de clave, con cifrado AES de 128 bits	329, 995 seg	335, 715 seg	323, 095 seg	305, 452 seg	307, 178 seg

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Tiempo Procesamiento Total	**320, 287 seg**				
Transferencias	20	20	20	20	20
Total Transferencias	100				
Paquetes	210	208	204	203	210
Longitud de Clave	1024 bits				

Tabla Nª 3: Tiempo de Procesamiento - Escenario sin ninguna Técnica

Transferencia FTP	**Tiempo Procesamiento**				
	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5
Texto Plano	300, 168 seg	300, 196 seg	300, 199 seg	300, 194 seg	300, 259 seg
Tiempo Procesamiento Total	**300, 2032 seg**				
Transferencias	20	20	20	20	20
Total Transferencias	100				
Paquetes	154	150	152	152	154

4.1.2 Margen de Error en la transmisión

Tabla Nª 4: Margen de Error en la transmisión de Técnica 1

1º Técnica de Encriptación	**Tiempo Procesamiento**				
	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

RSA de 2048 bits de clave, con cifrado AES de 256 bits	99, 443 seg	36 ,507 seg	19, 848 seg	44, 133 seg	25, 341 seg
Margen Error- en la transmisión	**28. 48%**				
Transferencias	20	20	20	20	20
Total Transferencias	100				
Paquetes	1 452	1 516	1 256	1 494	1 470

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_n - \bar{x})^2}{N}}$$

$$\dot{X} = \frac{99{,}443 + 36{,}507 + 19{,}848 + 44{,}133 + 25{,}341}{5} = \mathbf{45{,}054}$$

$$\frac{\sqrt{(99{,}443 - X)^2 + (36{,}507 - X)^2 + (19{,}848 - X)^2 + (44{,}133 - X)^2 + (25{,}341 - X)^2}}{5}$$

$$\frac{\sqrt{(54{,}389)^2 + (-8{,}547)^2 + (-25{,}206)^2 + (-0{,}921)^2 + (-19{,}713)^2}}{5}$$

$$\sqrt{811{,}2015152}$$

$$= 28{,}48\%$$

Tabla Nª 5: Margen de Error en la transmisión de Técnica 2

2º Técnicas de Encriptación	**Tiempo Procesamiento**				
	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5
RSA de 1024 bits de clave,	329, 995 seg	335, 715 seg	323, 095 seg	305, 452 seg	307, 178 seg

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

con cifrado AES de 128 bits					
Margen Error- en la transmisión	$\mathbf{27,01\%}$				
Transferencias	20	20	20	20	20
Total Transferencias	100				
Paquetes	210	208	204	203	210

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_n - \bar{x})^2}{N}}$$

$$\dot{X} = \frac{329{,}995+335{,}715+323{,}095+305{,}452+307{,}178}{5} = \mathbf{320{,}287}$$

$$\frac{\sqrt{(329{,}995 - X)^2 + (335{,}715 - X)^2 + (323{,}095 - X)^2 + (305{,}452 - X)^2 + (307{,}178 - X)^2}}{5}$$

$$\frac{\sqrt{(9{,}708)^2 + (15{,}428)^2 + (2{,}808)^2 + (-14{,}835)^2 + (-13{,}109)^2}}{5}$$

$$\sqrt{732{,}076418}$$

$$= 27{,}01\%$$

Tabla Nª 6: Margen de Error en la transmisión - Escenario sin ninguna Técnica

Transferencia FTP	**Tiempo Procesamiento**				
	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5
Texto Plano	300, 168 seg	300, 196 seg	300, 199 seg	300, 194 seg	300, 259 seg

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Margen Error- en la transmisión	$\mathbf{0,03\%}$				
Transferencias	20	20	20	20	20
Total Transferencias	100				
Paquetes	154	150	152	152	154

$$\dot{X}= \frac{300,168+300,196+300,199+300,194+300,259}{5}=\mathbf{300,203}$$

$$\frac{\sqrt{(300,168-X)^2+(300,196-X)^2+(300,199-X)^2+(300,194-X)^2+(300,259-X)^2}}{5}$$

$$\frac{\sqrt{(-0,035)^2+(-0,007)^2+(-0,004)^2+(-0,009)^2+(0,056)^2}}{5}$$

$$\frac{\sqrt{0.0009014}}{} = 0.03\%$$

De esta forma tenemos en cuenta que con la implementación de estas técnicas mejoramos la seguridad con respecto a la transferencia de archivos en un entorno para que sea fiable.

Hemos verificado que la técnica 1: RSA de 2048 bits de clave con cifrado AES de 256 bits, respecto a la técnica 2: RSA de 1024 bits de clave con cifrado AES de 128 bits; ha quedado demostrado a través del tiempo de procesamiento obtenido es más avanzada, por lo tanto, es más rápida en la encriptación de los datos, siendo el Tiempo de Procesamiento menor de la Técnica 1, en comparación del Tiempo de Procesamiento de la Técnica 2.

Para el margen de error, nos ha dado como resultado que para la técnica más efectiva que es el RSA de 2048 bits de clave ha dado 28,4% en comparación con la técnica 2 del último escenario RSA de 1024 bits de clave ha dado 27%, esto nos dice que la técnica 1 a pesar de ser muy rápido en comparación con la última tiene un pequeño margen de error al transmitir grandes cantidades de

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

información con la posibilidad de pérdida de algún paquete cuando se transmite en una red informática grandes cantidades de información.

4.2. Discusión de los Resultados

Para que las técnicas de encriptación funcionen con alto nivel de eficiencia, se necesitan que ambas se unan para adoptar las características de ambas para un buen rendimiento, la primera técnica RSA de 2048 bits de clave, siendo un algoritmo asimétrico de clave pública que trabaja en este caso con un algoritmo de cifrado AES de 256 bits de clave privada o simétrica, ha dado un resultado satisfactorio en cuando a velocidad de tiempo de procesamiento de encriptación de los datos transmitidos, siendo mayor en características de velocidad a comparación de la técnica 2 del último escenario que trabaja con RSA de 1024 bits de clave, un algoritmo de Asimétrico de clave pública, y con un algoritmo de cifrado AES de 128 bits de clave privada o simétrica.

Aunque estas técnicas en la verificación de los indicadores margen de error de tiempo en la transmisión, nos ha dado un pequeño margen de 28 % y 27 % para la primera y segunda técnica, esto no deja de ser algoritmos fuertemente compuestos en su criptosistema, difícil de vulnerar, ya que el principal objetivo de esta investigación, ha sido determinar aspectos de seguridad de vulnerabilidad de los datos en la no infiltración de un atacante para corromper y capturar los paquetes en nuestra red, lo cual ha sido verificado con el sniffer, dando satisfactorias las pruebas realizadas, siendo de alta implicancia la implementación de técnicas de encriptación para mejorar la transferencia de archivos en un entorno de red para que sea fiable.

En cuanto a las limitaciones obtenidas en esta investigación ha quedado determinada por el indicador margen de error en la transmisión de los datos cuando se trasmiten grandes cantidades de información en un escenario donde los recursos a administrar son mayores. Siendo los porcentajes alcanzados respecto a este indicador mínimos, donde finalmente en las pruebas obtenidas

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

no se ve afectado la transmisión de los datos en ningún escenario donde se aplicaron estas técnicas.

Las Evidencias registradas están en el Anexo N°1.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN

En este capítulo se detalla las técnicas de encriptación para la seguridad en la transferencia de archivos, así como también las distintas pruebas realizadas a cada algoritmo de encriptación de los datos que hemos tomado para un análisis; con el fin de determinar que técnica de encriptación es la más apropiada y además, pueden estos trabajar conjuntamente de forma eficaz, para que finalmente se logre determinar una comunicación segura entre un emisor y receptor mediante el envío de archivos que estos a su vez pueden ser confidenciales o no, estos estén siendo transmitidos; con esta solución se logre mitigar los posibles ataques o robos informáticos de cuantiosos, valiosos datos que se trasmiten a través de una red informática en una organización.

Tabla Nº 7: *Protocolos de Seguridad de Transferencia de Archivos***.**

Protocolos de Seguridad de Transferencia de Archivos	Características Principales
NFS	Permite compartir archivos en una red TCP/IP. Permite trabajar con Directorios Remotos. No hace uso de Protocolos propios, Es multiplataforma.
CIFS/SMB	Protocolo que trabaja como Cliente-Servidor. Basado en comandos de Nivel de Aplicación del Modelo de Capas de Red TCP/IP y Presentación del Modelo OSI. Trabaja en la mayoría de las redes locales Windows.
SAMBA	Implementación libre de Protocolos CIFS/SMB para Sistemas Operativos UNIX. Permite compartir ficheros con una Red Windows y consumir sus recursos.
SFTP	Transferencia fiable de ficheros en un entorno cliente-servidor.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

	Utiliza SSH (Secure Shell), interprete de comandos seguro con gran aceptación en los Sistemas UNIX. Utiliza sus propios comandos, usa clientes específicos (gráficos o basados en comandos).
FTPS	Versión segura de FTP (Protocolo de transferencia de ficheros) Trabaja con los mismos comandos que FTP. Presenta mayor compatibilidad con dispositivos de hardware como son móviles, consolas, etc.

Nota. Recuperado de http://site.ebrary.com/lib/bibsipansp/reader.action?docID=11046103&ppg=14#. Ra-Ma Editorial. (Montero, 2000). Administración de servicios de transferencia de archivos y contenidos multimedia.

A continuación detallaremos los algoritmos más utilizados frecuentemente por su tecnología robusta, por sus antecedentes registrando como atributo la seguridad de que sería muy difícil romper dichos sistemas o criptosistemas con un algún criptoanálisis (se realiza mediante el uso de ordenadores de grandes capacidades con el fin de encontrar debilidades en estos sistemas, rompiendo su seguridad, para encontrar las claves de encriptación y desencriptación que se crearon con estos algoritmos), y así descubrir su integridad de los archivos.

Tabla Nº 8: *Algoritmos de Tecnología Simétrica.*

Algoritmos de Tecnología Simétrica	Principales Características
DES	Se basa en un cifrador de bloques en el que la clave es de 64 bits. La base matemática que lo soporta consiste en Sustituciones Lineales y no lineales y en Permutaciones.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

TRIPLE DES	Consiste en el encadenamiento de tres funciones DES. Basado en el uso de dos claves, que se cifran con la primera, el resultado con la segunda y a su vez el resultado se cifra con la tercera.
IDEA	Se basa en un cifrador de bloque de 64 bits, claves de 128 bits y un total de 8 rondas. Ejecuta operaciones Algebraicas no conmutativas de grupos algebraicos diferentes (XOR, sumas, multiplicaciones) sobre bloques y las subclaves utilizadas.
BLOWFISH	Se basa en un cifrador de bloque de 64 bits con tamaños de claves desde 32 a 448 bits. Consiste en la ejecución de 16 rondas, aplicando el cifrador Feistel, que hace uso de claves dependientes de la Caja S igual a DES.
AES	Se basa en un cifrador de bloques de 128 bits y claves de 120, 192 o 256 bits con subclaves de 128 bits. Algoritmo rápido tanto a nivel de hardware como software. Requiere poca memoria para su implementación. Matemáticamente basado en cuatro funciones invertibles que se aplican a los bytes de una matriz llamada Estado, durante un número determinado de rondas. Que son varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloques de 16 bytes, por lo que se llama blockcipher (cifrado por bloques).

Nota. Recuperado de http://site.ebrary.com/lib/bibsipansp/reader.action?docID=11126449&ppg=10. IC Editorial. (1 Edición). Málaga. (Gonzáles & Fuentes, 2014). *Sistemas seguros de acceso y transmisión de datos*.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Tabla Nº 9: *Algoritmos de Tecnología Asimétrica.*

Algoritmos de Tecnología Asimétrica	Principales Características
RSA	Primer algoritmo efectivo de clave Pública. Se basa matemáticamente, en primer lugar: la operación módulo, y segundo lugar: el indicador de Euler. Se compone en la factorización de números compuestos como productos de primos, basándose su seguridad en que no existe una manera rápida y sencilla de factorizar cantidades que son producto de dos números primos largos
GAMAL	Basado en el protocolo de intercambio de claves de Diffie-Helman. Su seguridad se basa en el problema de logaritmo discreto. Radica en la dificultad de no haber sido demostrado de calcular logaritmos discretos sobre un cuerpo finito. Lo principal diferencia frente a RSA radica en que el GAMAL cada operación de cifrado sobre el mismo dato produce un resultado distinto, lo que complica el criptoanálisis.

Nota. Recuperado de http://site.ebrary.com/lib/bibsipansp/reader.action?docID=11126449&ppg=10. IC Editorial. (1 Edición). Málaga. (Gonzáles & Fuentes, 2014). *Sistemas seguros de acceso y transmisión de datos*.

A continuación, detallaremos una comparación o contraste de los algoritmos tanto de Criptografía Simétrica como Asimétrica, así también de los protocolos más utilizados de transferencia segura de archivos.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Tabla 10: Comparación de Algoritmos Simétricos entre AES, 3DES, DES.

Factores	AES	3DES	DES
Longitud de la clave	128, 192 Y 256 bits	K1, k2 y k3 168 bits (k1 y k2 168 bits (k1 y k2 es mismo)112 bits)	56 bits
Tipo de Cifras	Simétrica bloques de cifrado	Simétrica bloques de cifrado	Simétrica bloques de cifrado
Tamaño de Bloque	128,192 ó 256 bits.	64 bits	64 bits
Desarrollo	2000	1978	1977
Resistencia Criptoanálisis	Diferencial en Contra de Fuerte, Truncado Diferencial e Interpolación Lineal y Plazas de Ataques.	Vulnerable al Diferencial de Fuerza Bruta Atacante Podría ser analizada en texto plano con criptoanálisis Diferencial.	Vulnerables a Diferencial y Lineal Criptoanálisis. Las tablas de Sustitución Débiles.
Seguridad	Considerado Seguro	Sólo uno débil. Que es salir en DES.	Resultado Insuficiente.
Posibles Claves	2”, 2” y 95”	2’”, y 2’”	2”
Posible Tecla de Caracteres ASCCII Imprimir	95”, 95” y 95”	95”, y 95”	95’
Imprimible Revisión toda la Llave en 50 Mil Millones de Claves	Para una clave de 128 Bits 5x10 Años.	Para una clave de 112 Bits 800 Días	Para una clave de 56 Bits 400 Días
Ronda	10(128 bits), 12(192 bits), 14(256 bits)	48	16
Rendimiento (Encriptación Desencriptación)	4.174/6.452	3.45/5.665	4.01/6347
Clave	Solo	Sola (dividida en 3 partes)	sola

Nota. Recuperado de:

https://dialnet.unirioja.es/servlet/articulo?codigo=5286657. (Medina & Miranda, 2015). *Comparación de Algoritmos basados en la Criptografía Simétrica DES, AES y 3DES*.

Tabla 11: Resumen de Análisis Comparativo de Algoritmos criptográficos Asimétricos.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

INDICADORES	ÍNDICES	ALGORITMOS CRIPTOGRÁFICOS			
		RSA	Diffie-Hellman	El Rabín	El Gamal
1. Datos de Entrada	1. Números de Datos de Entrada	5	4	4	3
	2. Dificultad para la preparación de los Datos de Entrada.	5	5	3	1
2. Algoritmo de Cifrado	3. Número de Pasos del Algoritmo	5	0	2	1
	4. Dificultad de los Pasos	5	0	5	1
	5. Orden de Complejidad	5	0	3	5
3. Algoritmo de Decifrado	6. Número de Pasos del Algoritmo.	5	3	3	1
	7. Dificultad de los Pasos	5	3	1	5
	8. Orden de Complejidad	5	5	1	5
4. Conceptos Matemáticos	9. Cantidad de Definiciones Matemáticas Empleadas	5	5	3	3
	10. Importancia de los Conceptos Matemáticos	5	5	1	1
TOTALES		50/50	30/50	26/50	24/50

Nota. Recuperado de:

http://dspace.espoch.edu.ec/bitstream/123456789/4431/1/20T00643.pdf. (Paguay.,2015) Análisis De Algoritmos Matemáticos De Criptografía Pública Para Mejorar El Aprendizaje De La Materia De Criptografía En La Carrera De Ingeniería En Sistemas De La ESPOCH.

Tabla 12: Revisión de la Seguridad en los Servicios IPV6

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

	Server Windows 2008		Server Windows 2012 R2		Server Linux Debian		Server Ubuntu	
Servicios	FTPS	SSH	FTPS	SSH	FTPS	SSH	FTPS	SSH
Soporta IPV6	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Parámetros de Configuración (Nivel de dificultad)	Baja	Baja	Baja	Baja	Alta	Alta	Media	Media
Soporta IPsec	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
VPN	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Autenticación clave Compartida y certificado Digital	RSA /DSA	RSA /DSA	RSA /DSA	RSA /DSA	RSA/ DSA/ PSK	RSA/ DSA/ PSK	RSA/ DSA/ PSK	RSA/ DSA/ PSK
Confidencialidad entre 56 y 128 bits	DES	DES	3DES	3DES	3DES / AES	3DES / AES	3DES/ AES	3DES/ AES
Integridad	MD5	MD5	MD5	MD5	MD5/ SHA	MD5/ SHA	MD5/ SHA	MD5/ SHA

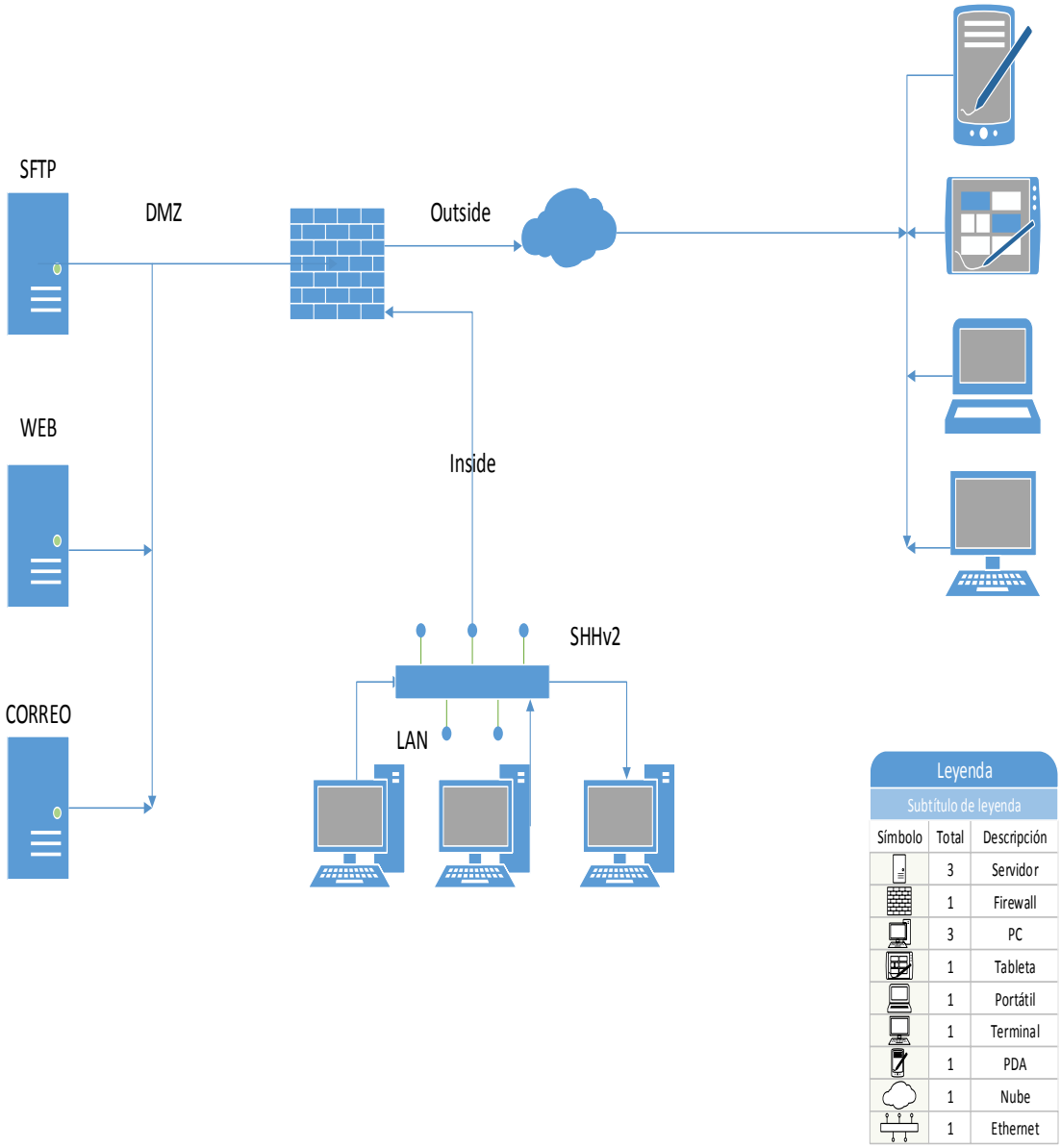
Nota. Recuperado de:

https://dialnet.unirioja.es/descarga/articulo/6041589.pdf. (Bareño et al., 2015). *Análisis de la Seguridad en la Implementación de Servicios Corporativos sobre el protocolo IPV6*.

Posteriormente, se determinará la topología contextual, física y lógica para una red (LAN) pueda funcionar de forma segura, adicionando ciertos niveles o principios de seguridad informática: integridad, confidencialidad de la información; con el fin de lograr un buen desempeño o incremento de la seguridad con respecto a la transferencia de ficheros en una red informática.

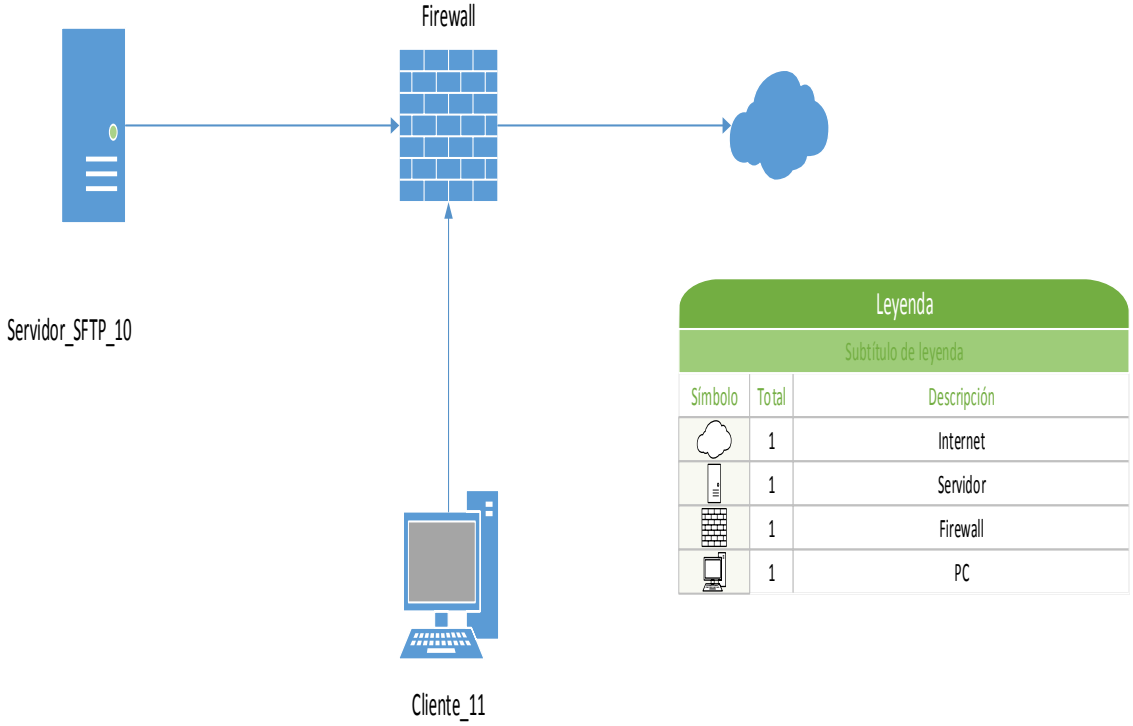
1. Diseño de la Topología Contextual de la Red

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

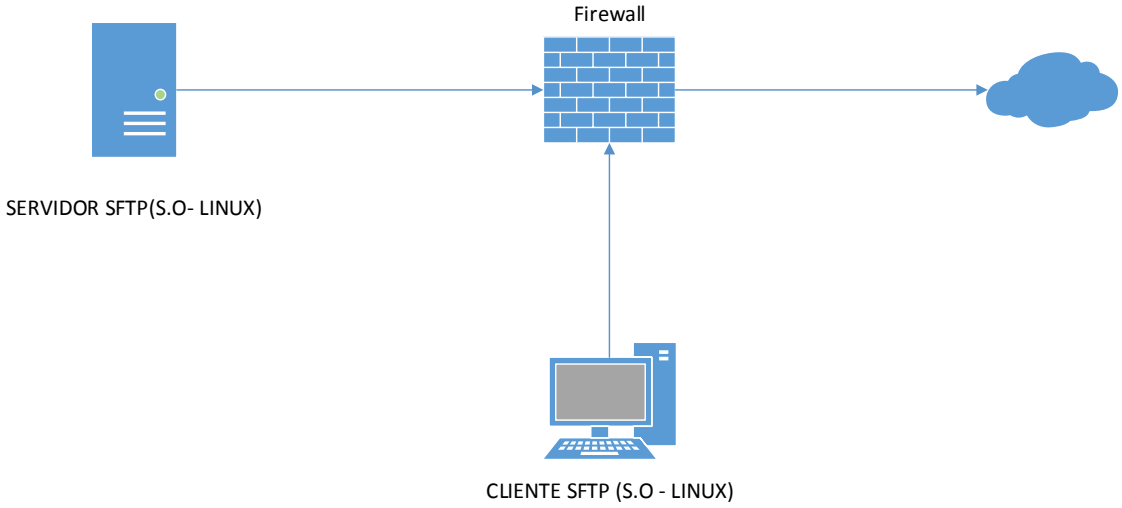


2. Diseño Físico de la Red

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



3. Diseño Lógico de la Red

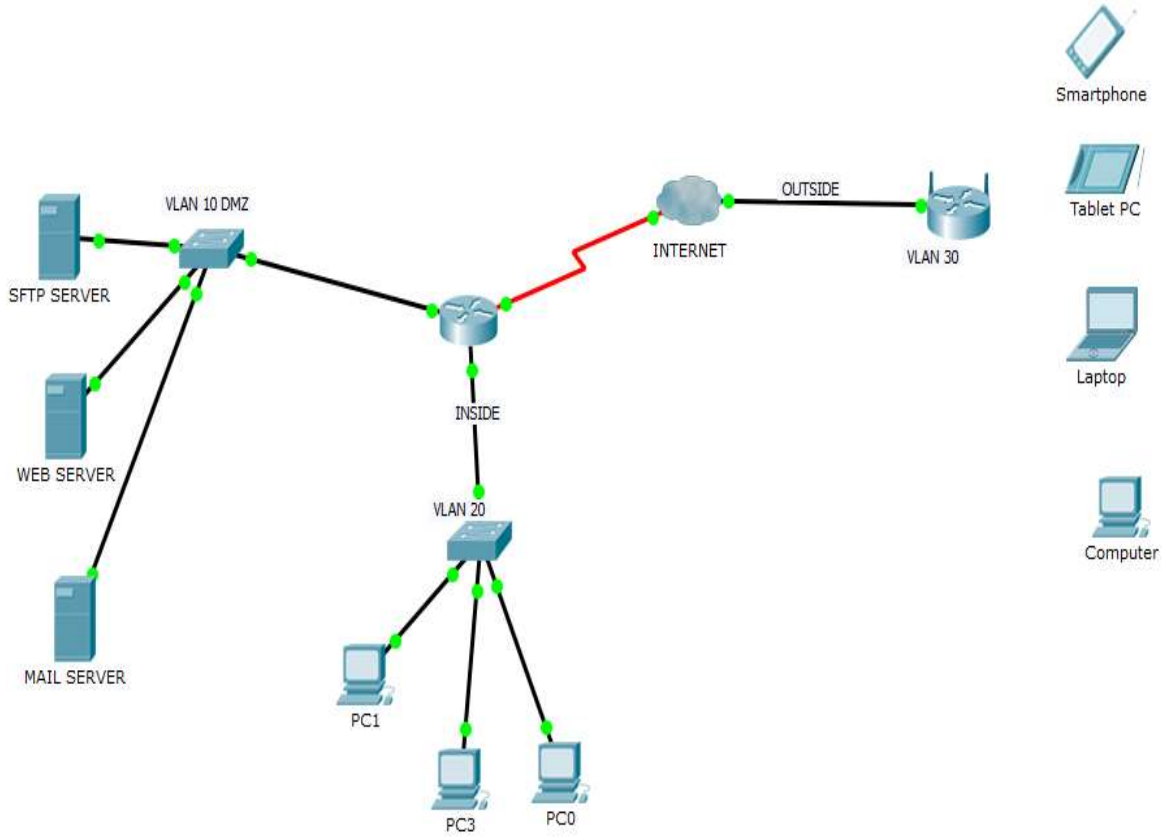


Servidor Sftp: Se ejecuta sobre el Sistema Operativo Linux, distribución de Ubuntu, versión: Ubuntu Server 16.04.1 LTS - xenial xerus.

Clientes Sftp: Se ejecutan sobre el Sistema Operativo Linux, distribución de Ubuntu, versión: Ubuntu 12.04.5 LTS – precise pangolín.

4. Topología de Red: Estrella Extendida

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



192.168.10.10/24 ---> Vlan 10 ---> DMZ

192.168.20.20/24 ---> Vlan 20 ---> Inside (Red Local)

192.168.30.30/24 ---> Vlan 30 ---> OutSide (Red Wifi)

En este apartado se ha definido un prototipo de Red, la cual se ha montado sobre la Plataforma Linux, distribución de Ubuntu, realizando una conexión Cliente - Servidor, para lo cual se ha necesito levantar un Servidor en Linux, Ubuntu versión 16.04.1 LTS Xenial Xerus, y el cliente en una distribución de Linux, Ubuntu 12.045 LTS precise pangolín, a continuación, se definirá el prototipo montado en Linux:

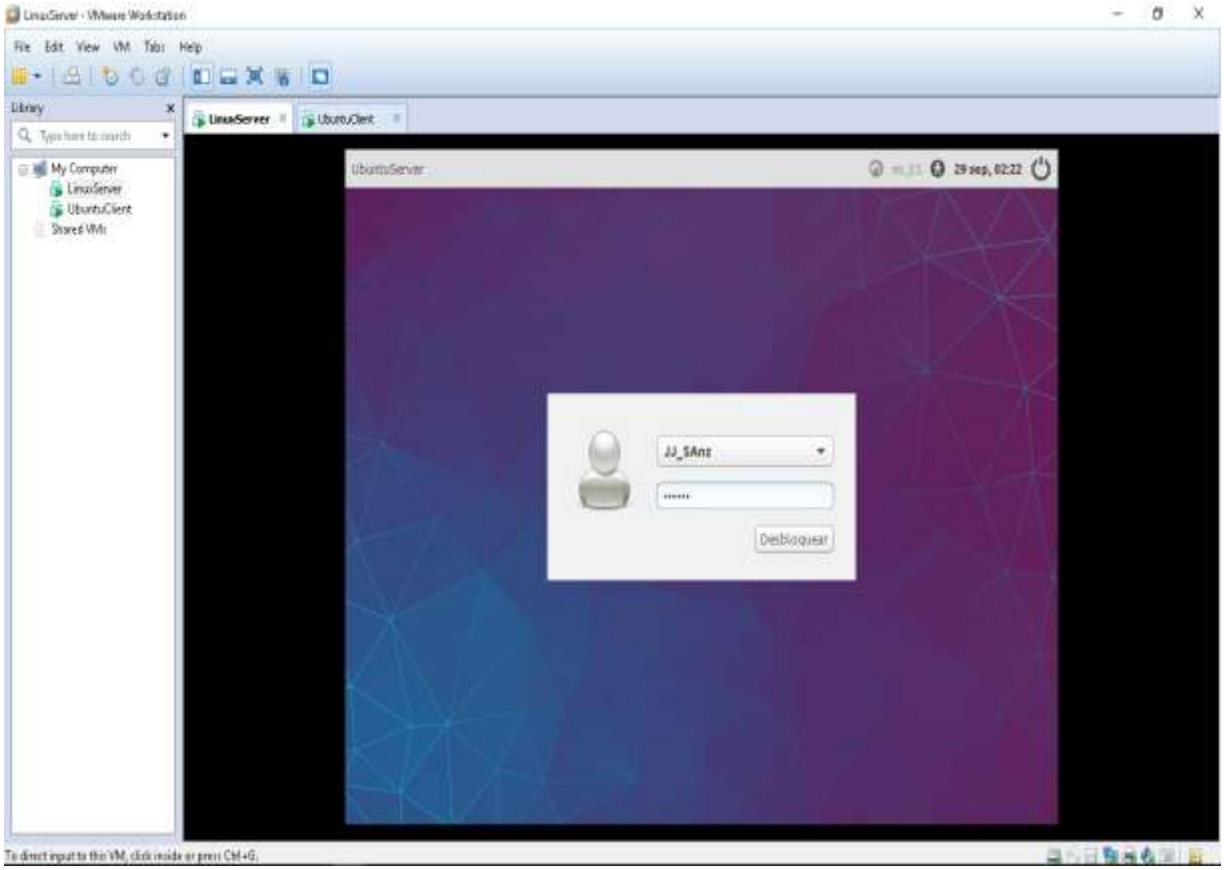
En el servidor hemos instalado un modo gráfico, ya que como se sabe las versiones de Servidor, vienen en modo Texto; lo que permite que el sistema sea muy ligero, y consume pocos recursos de memoria y procesador, ya que un servidor tiene que ahorrar mucho costo de procesamiento y ancho de banda para ejecutar ciertos

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

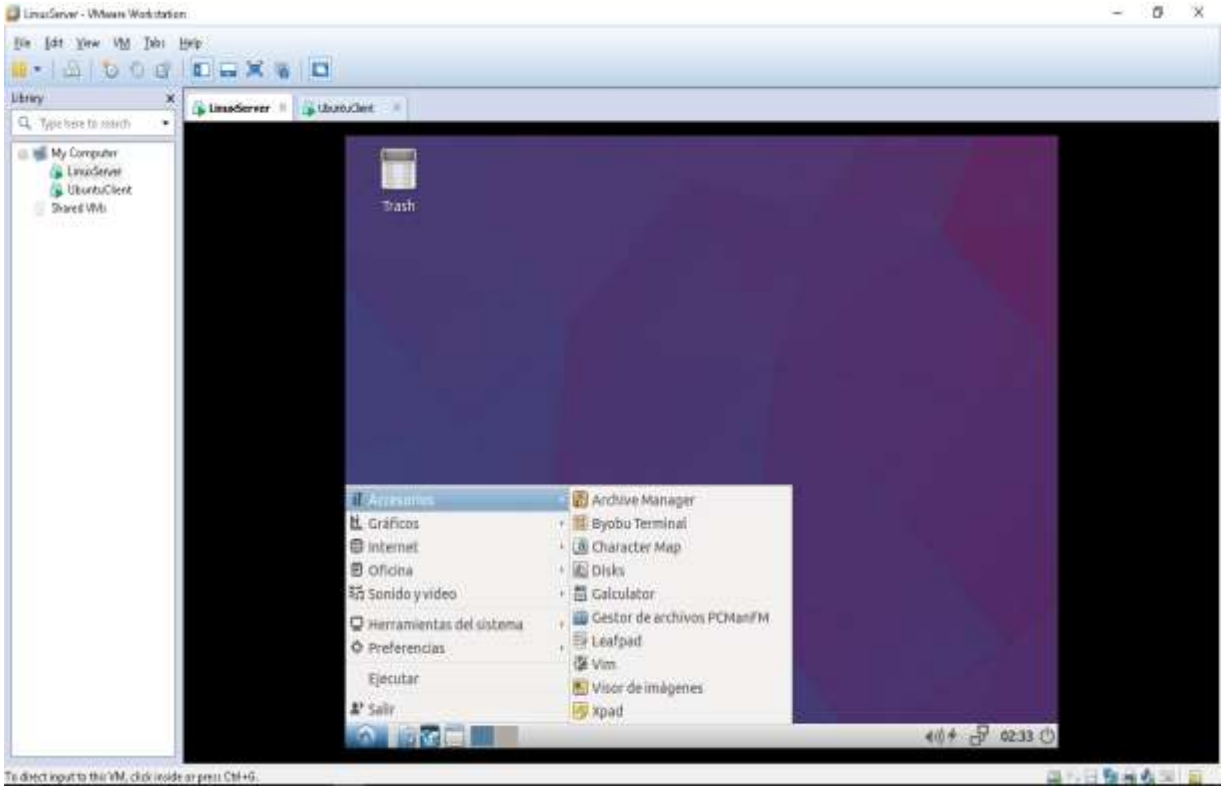
servicios en una red informática, a continuación, para ello abrimos la terminal con lo siguientes atajos, ctrl+ alt+ t y digitamos lo siguientes comandos:

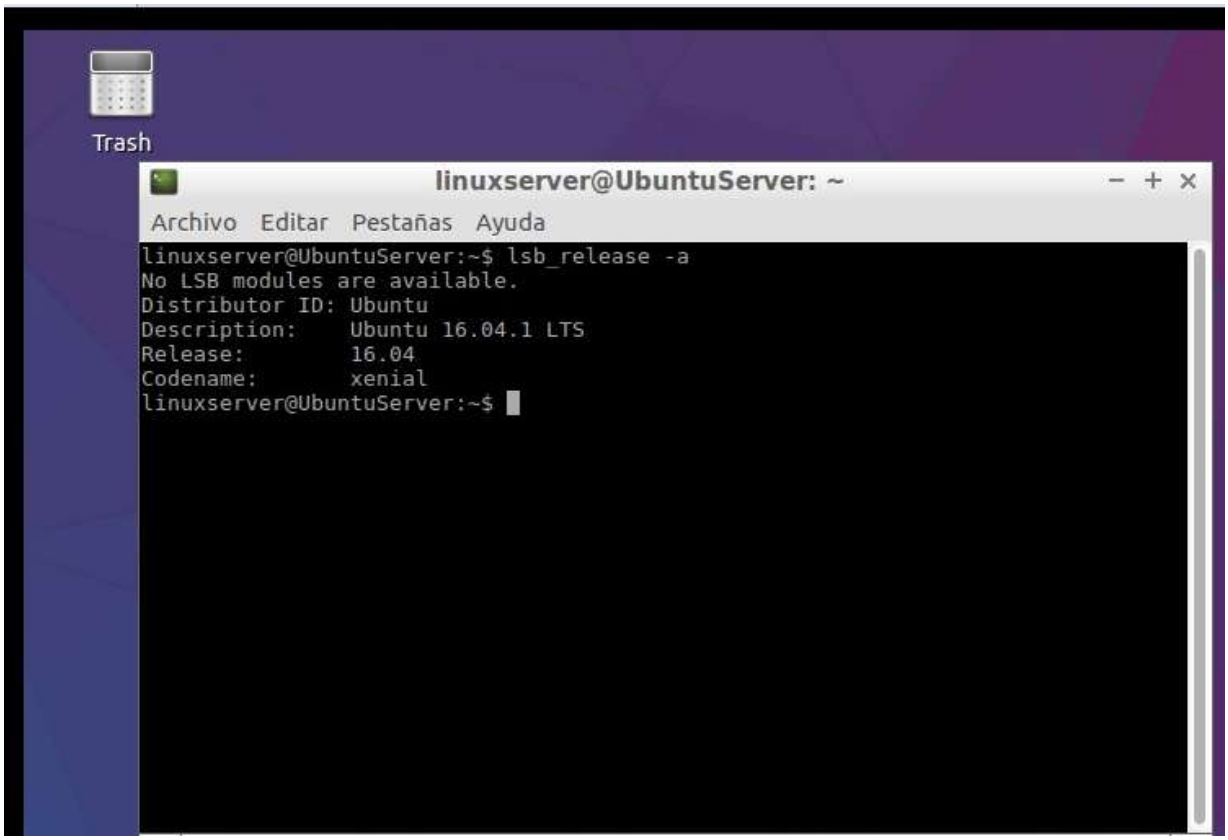
sudo apt-get update, sudo apt-get upgrade.

sudo apt-get install --no-install-recommends lubuntu-desktop



Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis





Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Para continuar definiendo nuestro prototipo necesitamos actualizar algunos paquetes, para que nuestro servidor queda listo para las pruebas pertinentes a esta investigación: sudo apt-get update, sudo apt-get upgrade.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

```
linuxserver@UbuntuServer: ~
Archivo  Editar  Pestañas  Ayuda
linuxserver@UbuntuServer:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.1 LTS
Release:        16.04
Codename:       xenial
linuxserver@UbuntuServer:~$ sudo apt-get update
[sudo] password for linuxserver:
Des:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [94,5 kB]
Obj:2 http://pe.archive.ubuntu.com/ubuntu xenial InRelease
Des:3 http://pe.archive.ubuntu.com/ubuntu xenial-updates InRelease [95,7 kB]
Des:4 http://pe.archive.ubuntu.com/ubuntu xenial-backports InRelease [92,2 kB]
Descargados 282 kB en 3s (91,8 kB/s)
```

```
linuxserver@UbuntuServer: ~
Archivo  Editar  Pestañas  Ayuda
Se actualizarán los siguientes paquetes:
  accountsservice grub-legacy-ec2 gtk2-engines-murrine ifupdown
  isc-dhcp-client isc-dhcp-common libaccountsservice0 libegl1-mesa libgbm1
  libgl1-mesa-dri libgl1-mesa-glx libglapi-mesa libnm0 libnma-common libnma0
  libp11-kit0 libpam-systemd libpython3.5 libpython3.5-minimal
  libpython3.5-stdlib libsystemd0 libudev1 libwayland-egl1-mesa libxatracker2
  mtools network-manager network-manager-gnome p11-kit p11-kit-modules
  python3.5 python3.5-minimal snapd systemd systemd-sysv ubuntu-drivers-common
  udev
36 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 26,4 MB de archivos.
Se utilizarán 1.027 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://pe.archive.ubuntu.com/ubuntu xenial-updates/main i386 systemd-sysv
i386 229-4ubuntu8 [13,9 kB]
Des:2 http://pe.archive.ubuntu.com/ubuntu xenial-updates/main i386 libpam-system
d i386 229-4ubuntu8 [123 kB]
Des:3 http://pe.archive.ubuntu.com/ubuntu xenial-updates/main i386 libsystemd0 i
386 229-4ubuntu8 [224 kB]
Des:4 http://pe.archive.ubuntu.com/ubuntu xenial-updates/main i386 ifupdown i386
 0.8.10ubuntu1.1 [55,0 kB]
Des:5 http://pe.archive.ubuntu.com/ubuntu xenial-updates/main i386 systemd i386
229-4ubuntu8 [3.678 kB]
12% [5 systemd 2.752 kB/3.678 kB 75%]                        213 kB/s 1min 49s
```

Luego procederemos a arrancar nuestro servidor, en la consola o terminal digitamos:

Sudo apt-get install openssh-server

Sudo apt-get –f install --> instala algún paquete posiblemente roto.

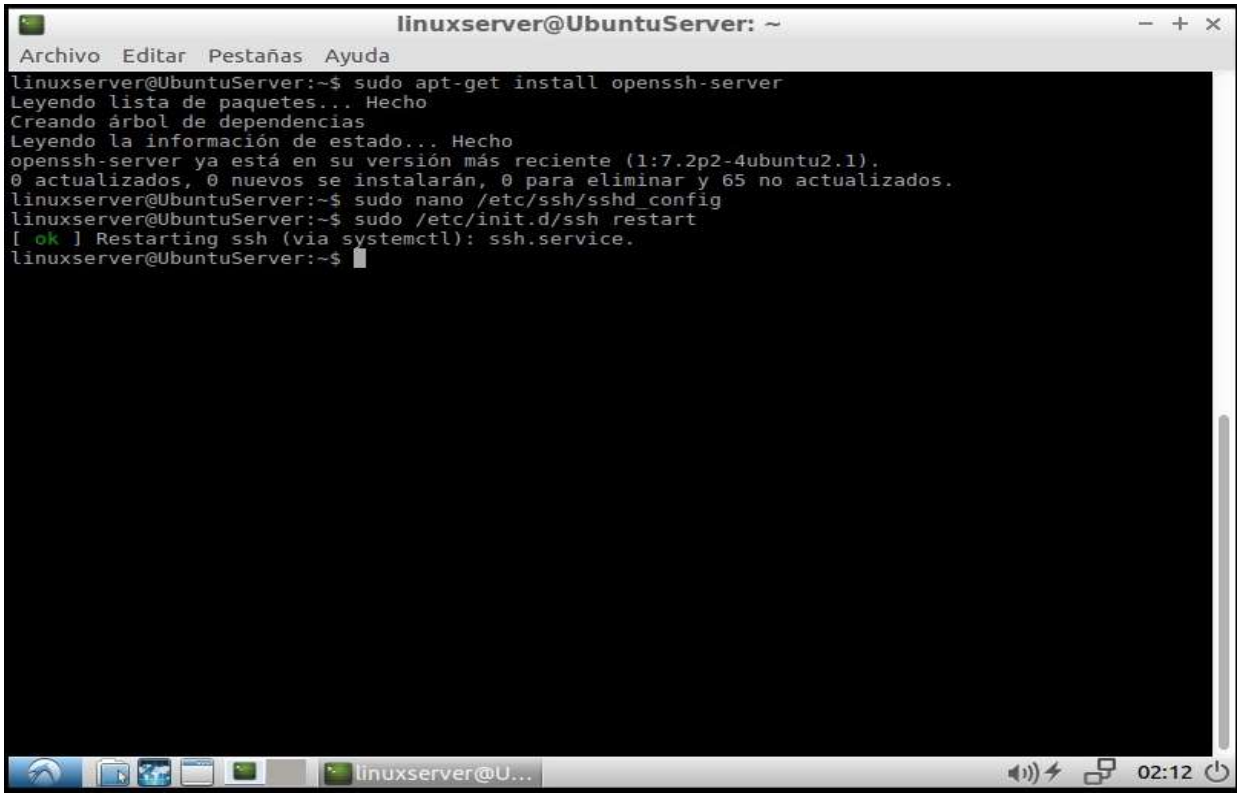
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Seguido de esto, necesitamos configurar nuestro servidor, para ello en la consola:

Sudo nano/etc/ssh/sshd_config

Verificamos que arranque en el puerto 22, y también añadimos lo siguiente, para permitir que usuarios se conecten de forma remota, guardamos todo, salimos y reiniciamos el servicio:

AllowUsers racy



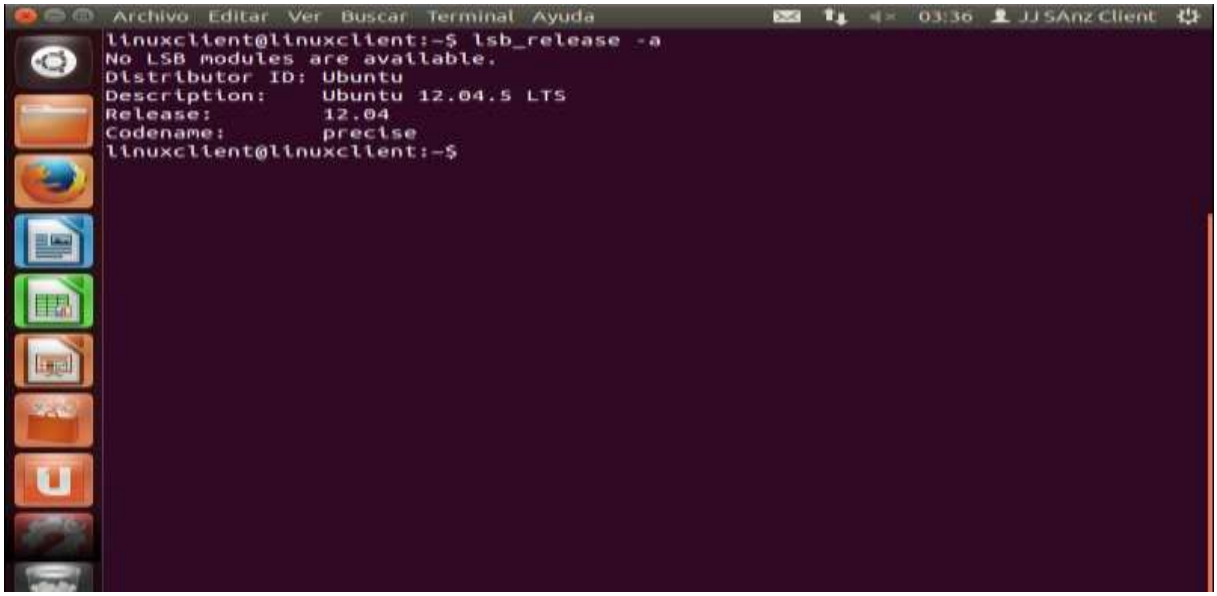
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

```
linuxserver@UbuntuServer: ~
Archivo  Editar  Pestañas  Ayuda
  GNU nano 2.5.3            Archivo: /etc/ssh/sshd_config                Modificado

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes
AllowUsers racy
Nombre del archivo a escribir: /etc/ssh/sshd_config
^G Ver ayuda      M-D Format DOS    M-A Añadir        M-B Respald fich
^C Cancelar       M-M Format Mac    M-P Anteponer     ^T A Ficheros
linuxserver@U...                                                  02:11
```

```
linuxserver@UbuntuServer: ~
Archivo  Editar  Pestañas  Ayuda
Found kernel: /memtest86+.bin
Replacing config file /run/grub/menu.lst with new version
Updating /boot/grub/menu.lst ... done

Configurando p11-kit (0.23.2-5~ubuntu16.04.1) ...
Procesando disparadores para initramfs-tools (0.122ubuntu8.1) ...
update-initramfs: Generating /boot/initrd.img-4.4.0-38-generic
W: mdadm: /etc/mdadm/mdadm.conf defines no arrays.
Procesando disparadores para libc-bin (2.23-0ubuntu3) ...
linuxserver@UbuntuServer:~$ clear
[3;J
linuxserver@UbuntuServer:~$ sudo /etc/ssh/sshd_config
[sudo] password for linuxserver:
sudo: /etc/ssh/sshd_config: orden no encontrada
linuxserver@UbuntuServer:~$ sudo nano /etc/ssh/sshd_config
linuxserver@UbuntuServer:~$ sudo /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
linuxserver@UbuntuServer:~$
```

Ahora configuraremos algunos comandos para el Cliente-Linux, sin tantas configuraciones, a continuación:

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



Ahora toca el Cliente, hacer algunos comandos, para actualizar e instalar el cliente ssh(secure Shell):

Sudo ap-get update; sudo apt-get upgrade

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

```
Obj http://security.ubuntu.com precise-security/main Translation-en
Obj http://pe.archive.ubuntu.com precise-backports/main Translation-en
Obj http://security.ubuntu.com precise-security/multiverse Translation-en
Obj http://pe.archive.ubuntu.com precise-backports/multiverse Translation-en
Obj http://pe.archive.ubuntu.com precise-backports/restricted Translation-en
Obj http://security.ubuntu.com precise-security/restricted Translation-en
Obj http://pe.archive.ubuntu.com precise-backports/universe Translation-en
Obj http://security.ubuntu.com precise-security/universe Translation-en
Descargados 1.120 kB en 8min. 41seg. (2.148 B/s)
Leyendo lista de paquetes... Hecho
linuxclient@linuxclient:~$ sudo apt-get upgrade
[sudo] password for linuxclient:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los siguientes paquetes se han retenido:
  linux-headers-generic-lts-trusty linux-image-generic-lts-trusty
Se actualizarán los siguientes paquetes:
  bind9-host dnsutils firefox firefox-locale-en firefox-locale-es
  gir1.2-gdkpixbuf-2.0 isc-dhcp-client isc-dhcp-common libbind9-80 libdns81
  libgdk-pixbuf2.0-0 libgdk-pixbuf2.0-common libisc83 libisccc80 libisccfg82
  liblwres80 libssl1.0.0 linux-generic-lts-trusty linux-libc-dev openssl
  python-imaging thunderbird thunderbird-gnome-support thunderbird-locale-en
  thunderbird-locale-en-us thunderbird-locale-es thunderbird-locale-es-es
27 actualizados, 0 se instalarán, 0 para eliminar y 2 no actualizados.
Necesito descargar 105 MB de archivos.
Se liberarán 183 kB después de esta operación.
¿Desea continuar [S/n]? s
Des:1 http://pe.archive.ubuntu.com/ubuntu/ precise-updates/main libssl1.0.0 i386
1.0.1-4ubuntu5.38 [1.012 kB]
1% [1 libssl1.0.0 754 kB/1.012 kB 75%]                    77,9 kB/s 22min. 15seg.
```

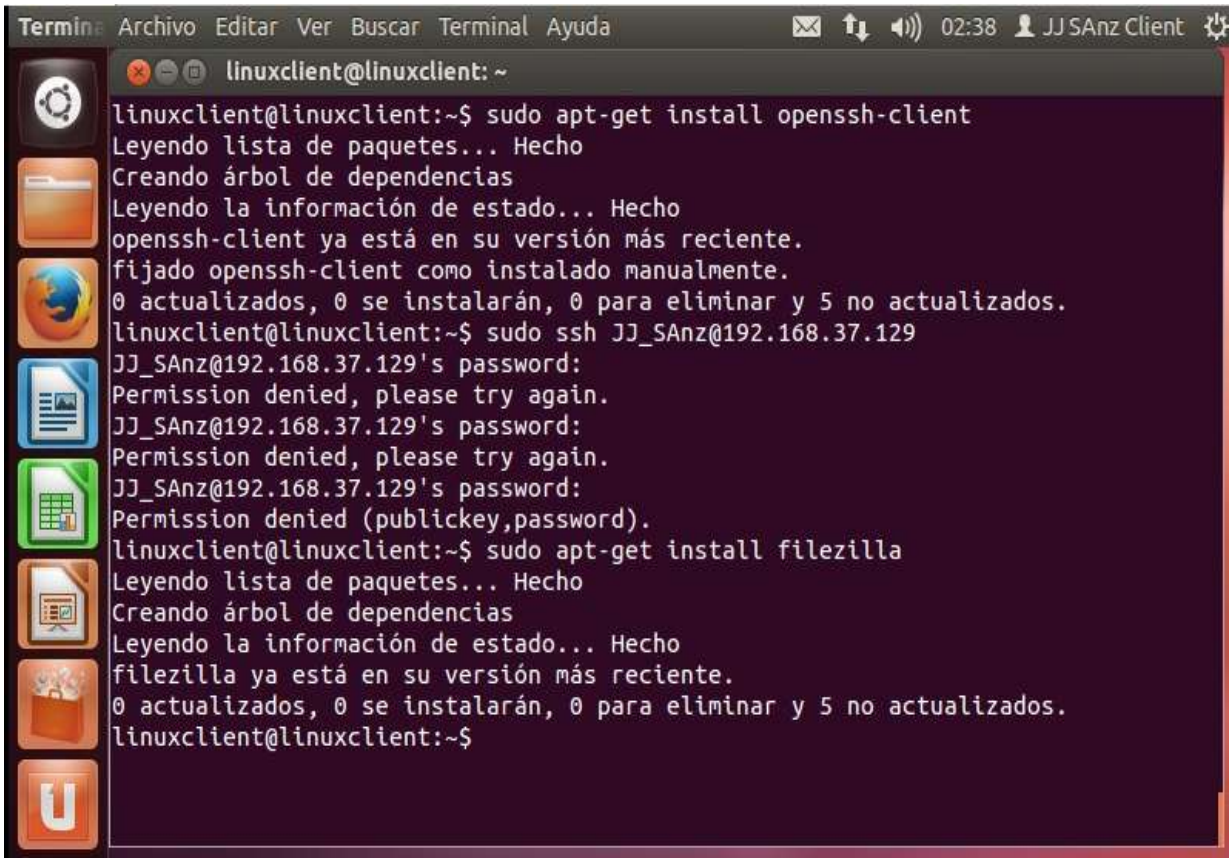
Luego instalamos el cliente: Sudo apt-get install openssh-client

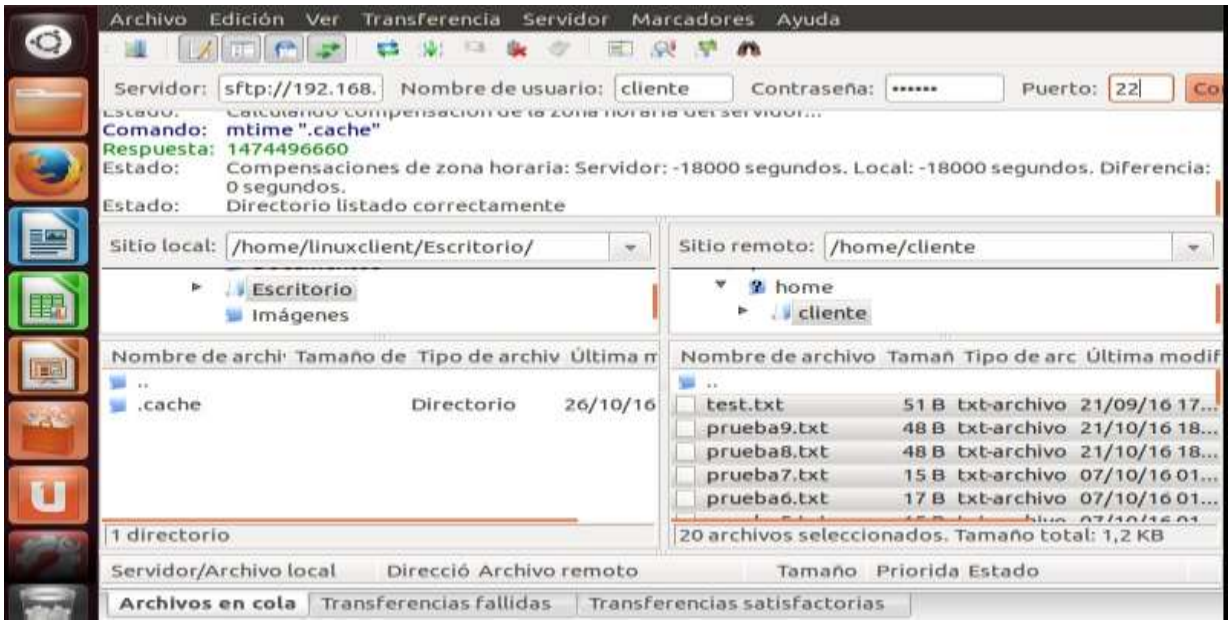
Para conectarnos instalamos Filezilla: Sudo filezilla

Y nos conectamos al servidor a través del siguiente comando, antes verificando que haya conexión: ping 192.168.37.128, y en el filezilla, ponemos la ip del servidor: 192.168.37.128, el nombre usuario del servidor: cliente, y la clave y se conecta a través del puerto 22.

```
Terminal                                   02:26  JJ SAnz Client
linuxclient@linuxclient: ~
linuxclient@linuxclient:~$ ping 192.168.37.129
PING 192.168.37.129 (192.168.37.129) 56(84) bytes of data.
64 bytes from 192.168.37.129: icmp_req=1 ttl=64 time=1.38 ms
64 bytes from 192.168.37.129: icmp_req=2 ttl=64 time=2.67 ms
64 bytes from 192.168.37.129: icmp_req=3 ttl=64 time=2.10 ms
64 bytes from 192.168.37.129: icmp_req=4 ttl=64 time=2.72 ms
64 bytes from 192.168.37.129: icmp_req=5 ttl=64 time=2.68 ms
```

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis





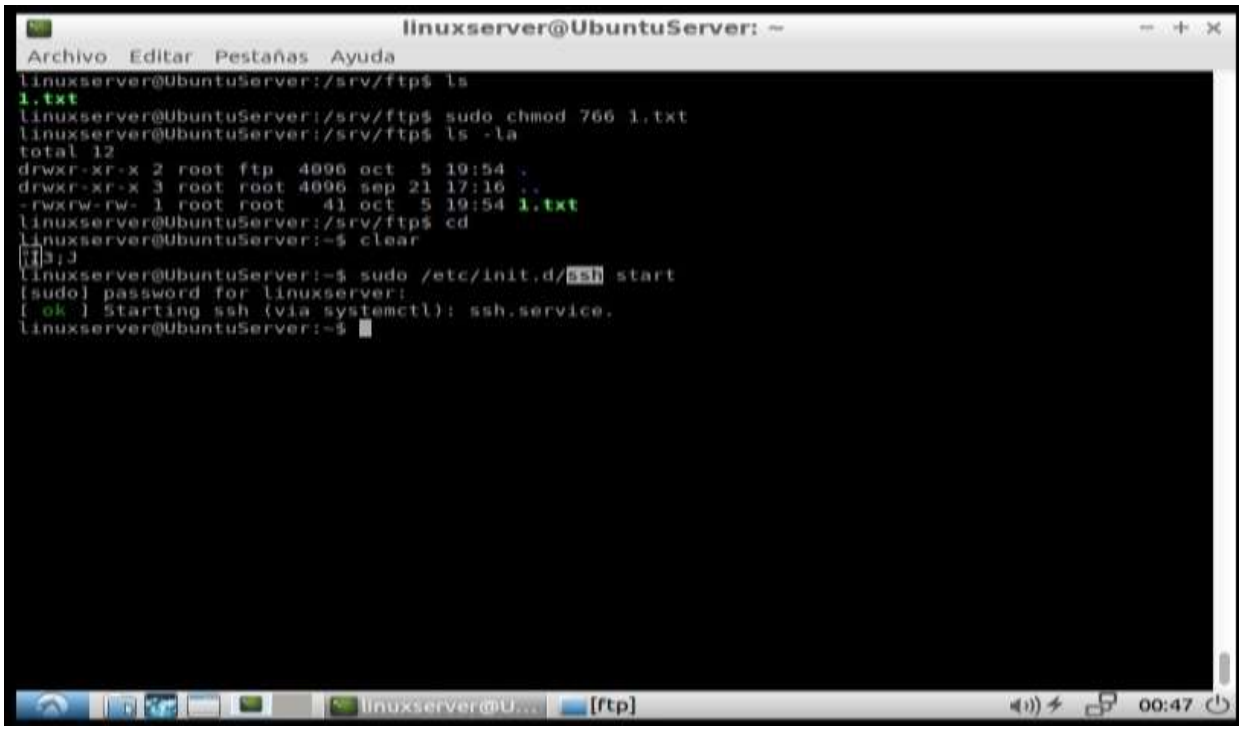
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En este apartado mostraremos los distintos escenarios en el que las técnicas de encriptación favorecen a mejorar la transferencia segura de archivos en un entorno para que este sea fiable, manteniendo distintos niveles de seguridad informática: confidencialidad e integridad de los datos, para que estos principios de seguridad se cumplan se necesitan establecer dichas técnicas de encriptación en una red informática.

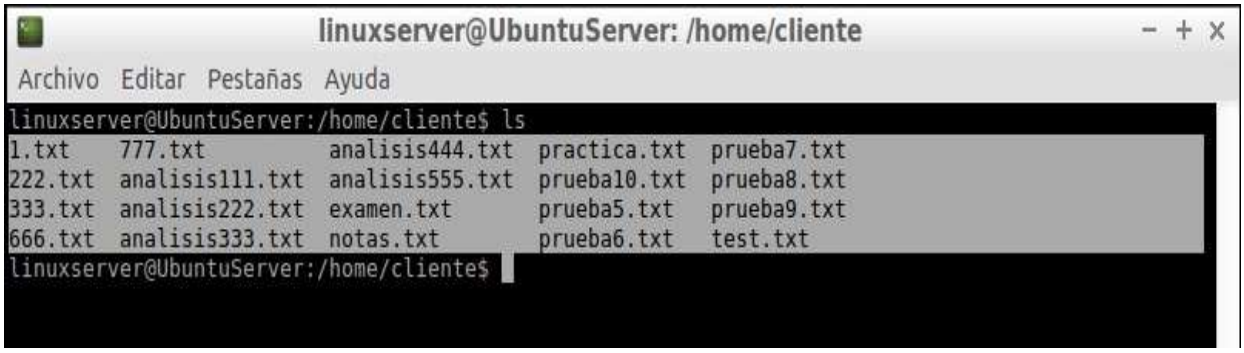
En este apartado no mostraremos los distintos paquetes que se debieron descargar para cada escenario y las configuraciones pertinentes que se necesitaron, ya que se podría confundir un poco para los que no conozcan o tengan el conocimiento técnico para trabajar en estos escenarios de entorno Linux, ya que las configuraciones son algo extensas y se ha tomado su tiempo para levantar cada escenario específico.

Para el 1er escenario, se necesita levantar el servidor SFTP (Secure Shell File Transfer Protocol), que significa que será una transferencia segura, a continuación demostraremos que principios de seguridad se obtendrá, en cuanto a la transferencia segura de archivos en una red informática para este caso.



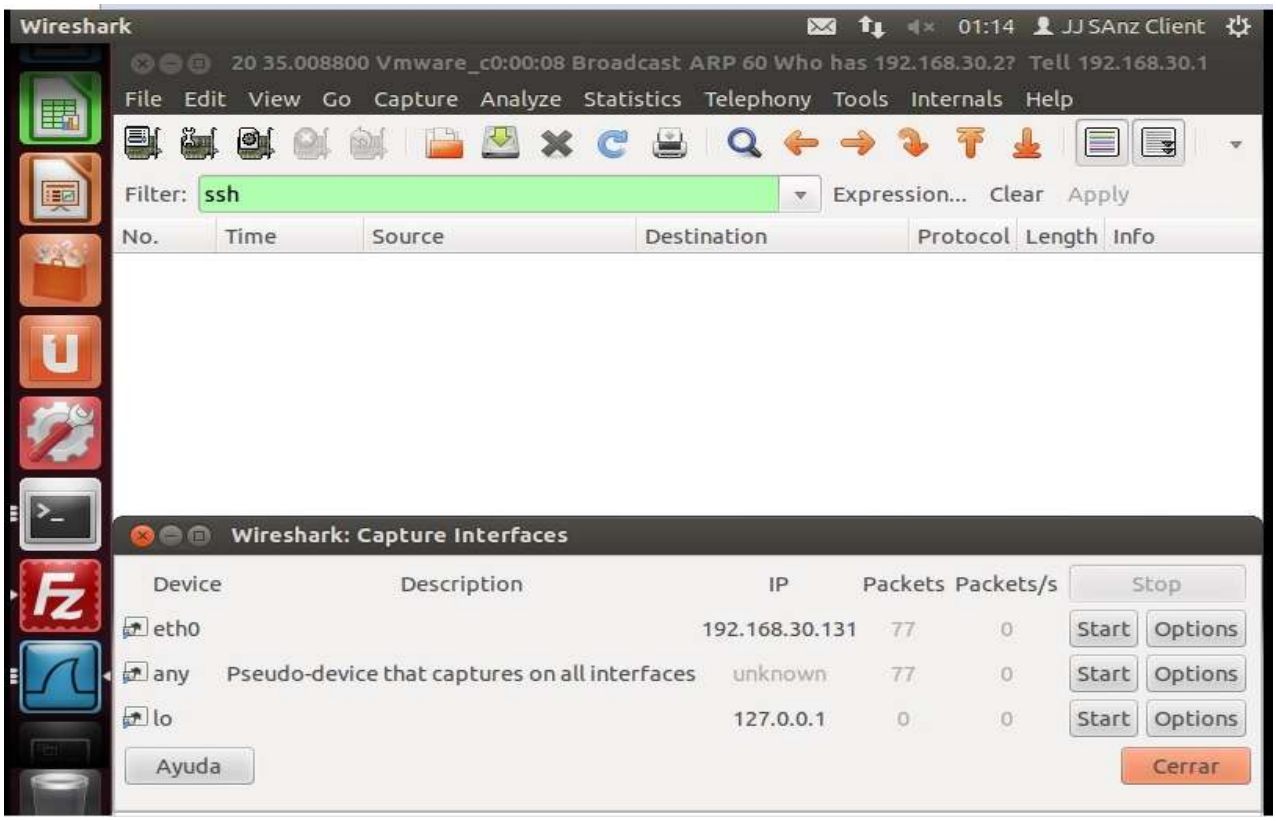
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Mostraremos los archivos que se van a transferir, así como el directorio (cliente) en el que se encuentran alojados en el servidor linuxserver.



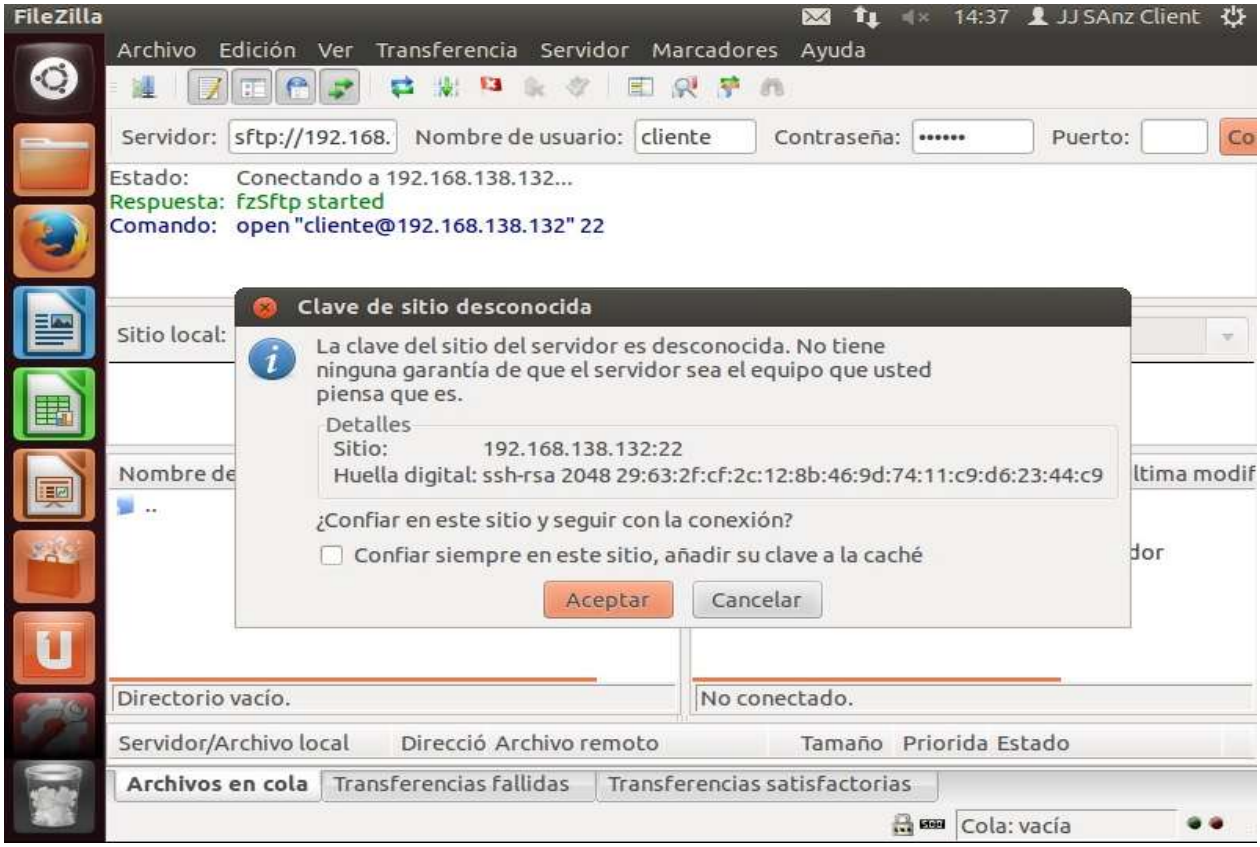
Ahora desde el terminal abriremos el Wireshark: sudo Wireshark

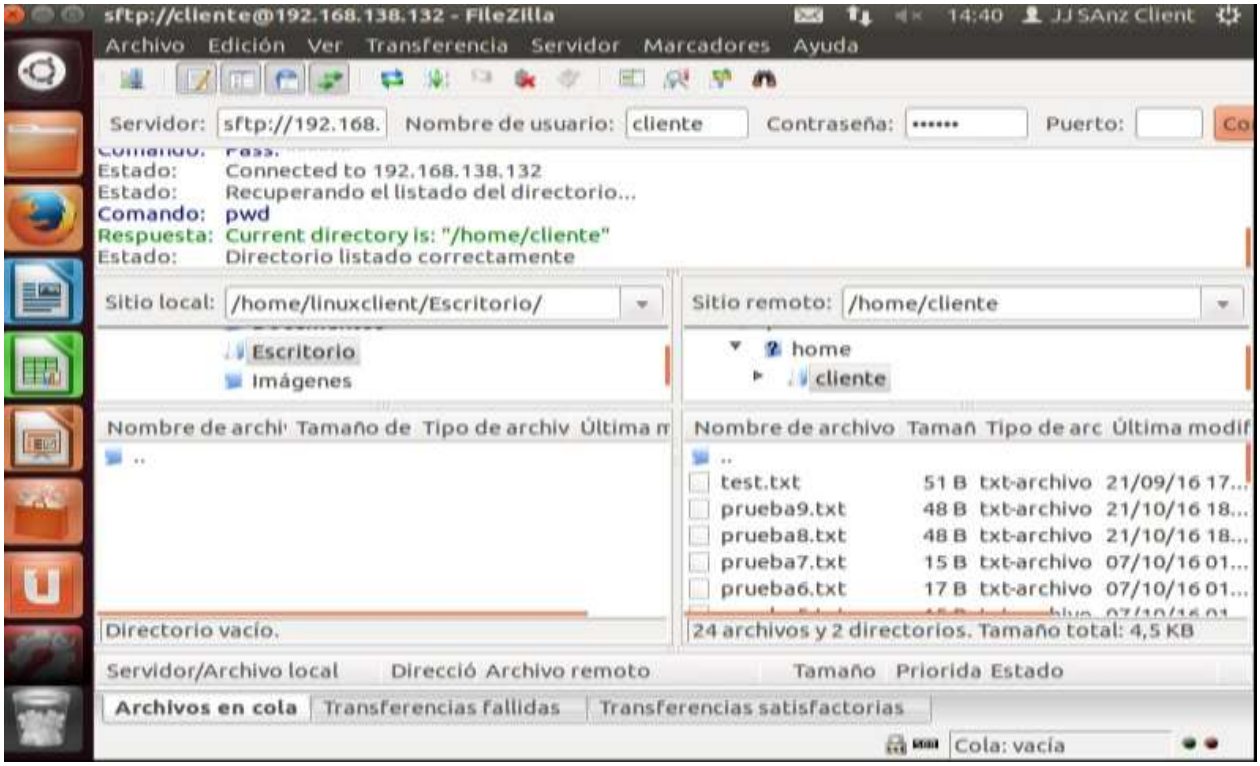
A continuación, capturaremos los paquetes antes de ser transferidos.



Luego desde la terminal tenemos que abrir una interfaz denominada Filezilla, previamente instalada: sudo filezilla, que nos permitirá conectarnos al servidor SFTP, para iniciar la transferencia segura de archivos en un entorno para que sea fiable.

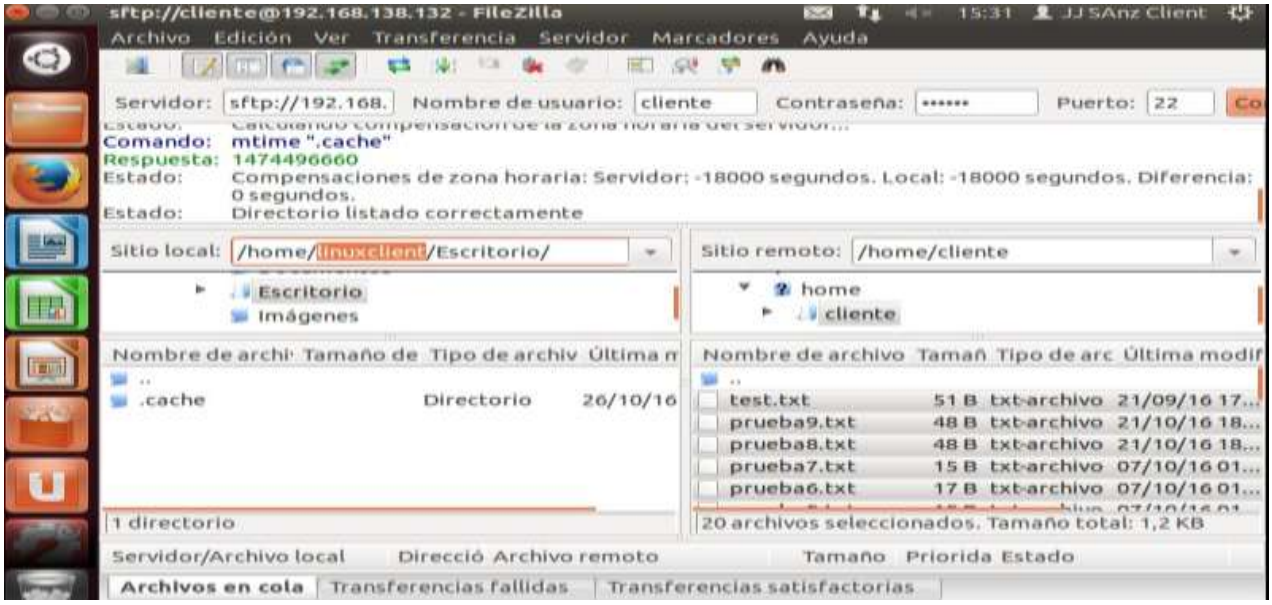
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

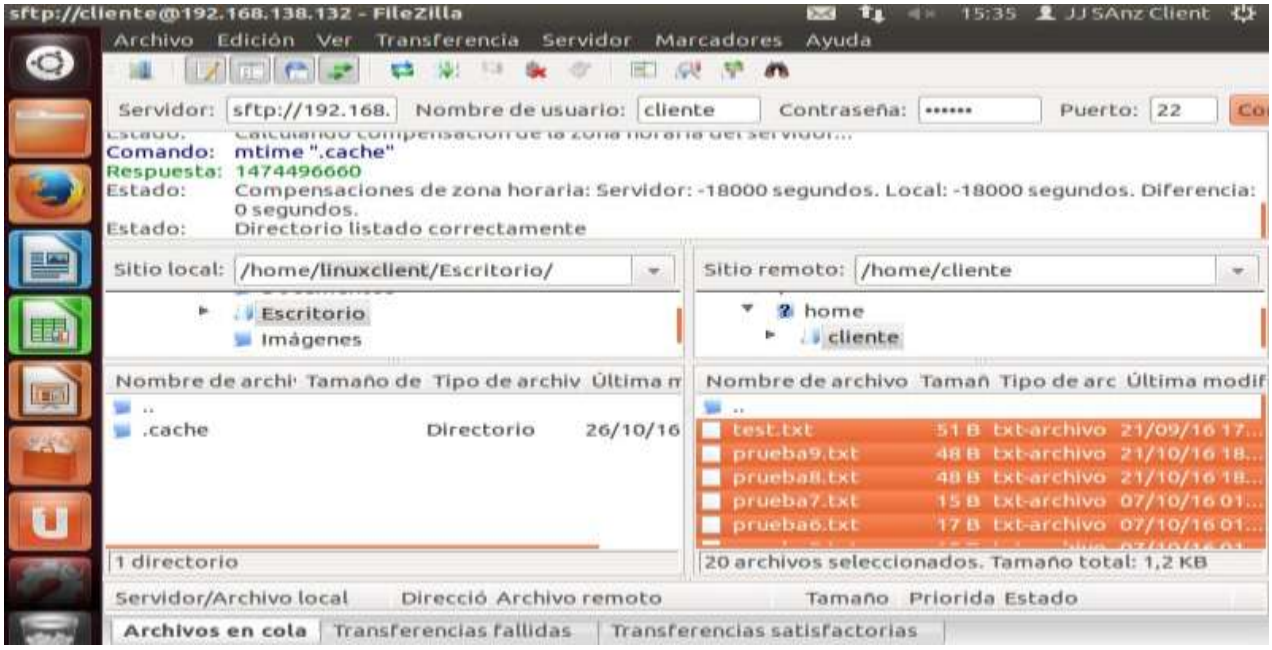




Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

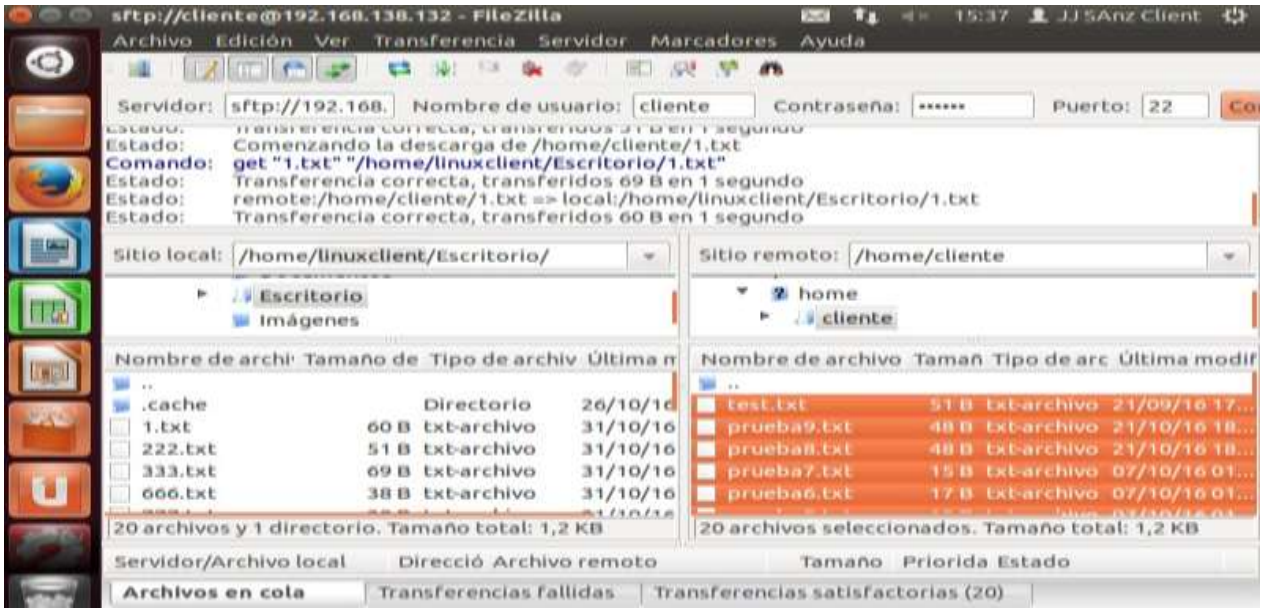
Nos conectamos con el ip del servidor: que es 192.168.138.132, el usuario del servidor: cliente, una contraseña: adminV, y en el puerto 22.



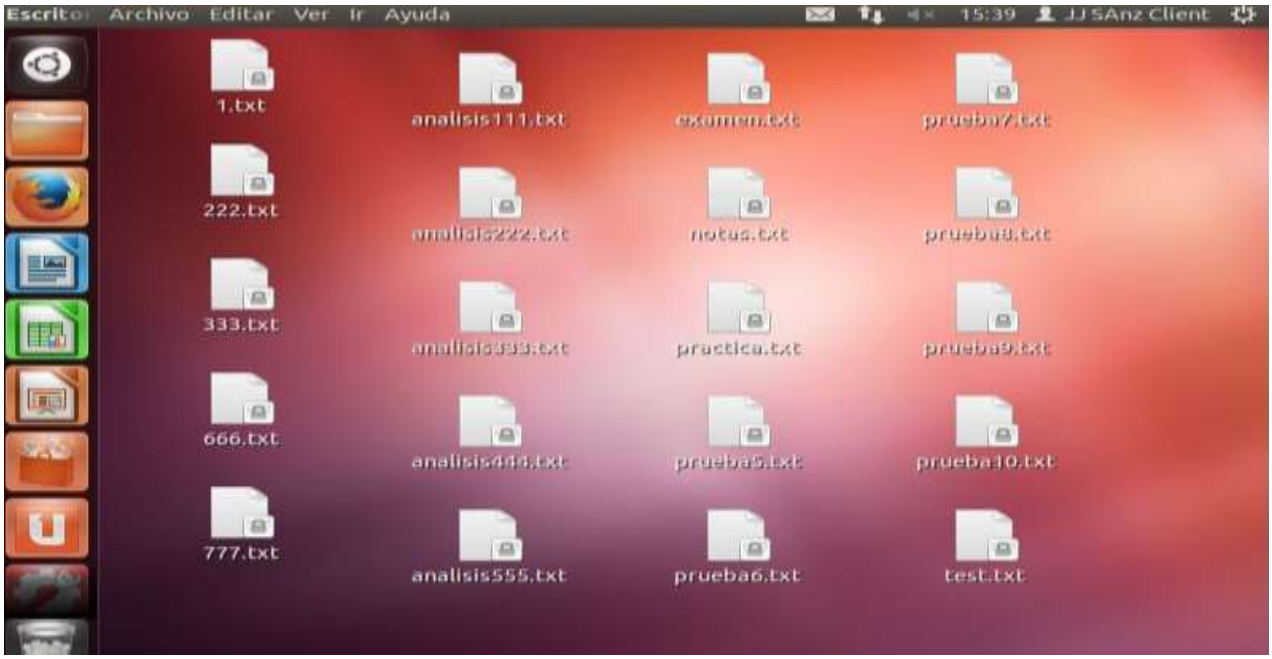


Ahora seleccionados los archivos vamos a transferir del servidor al cliente.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

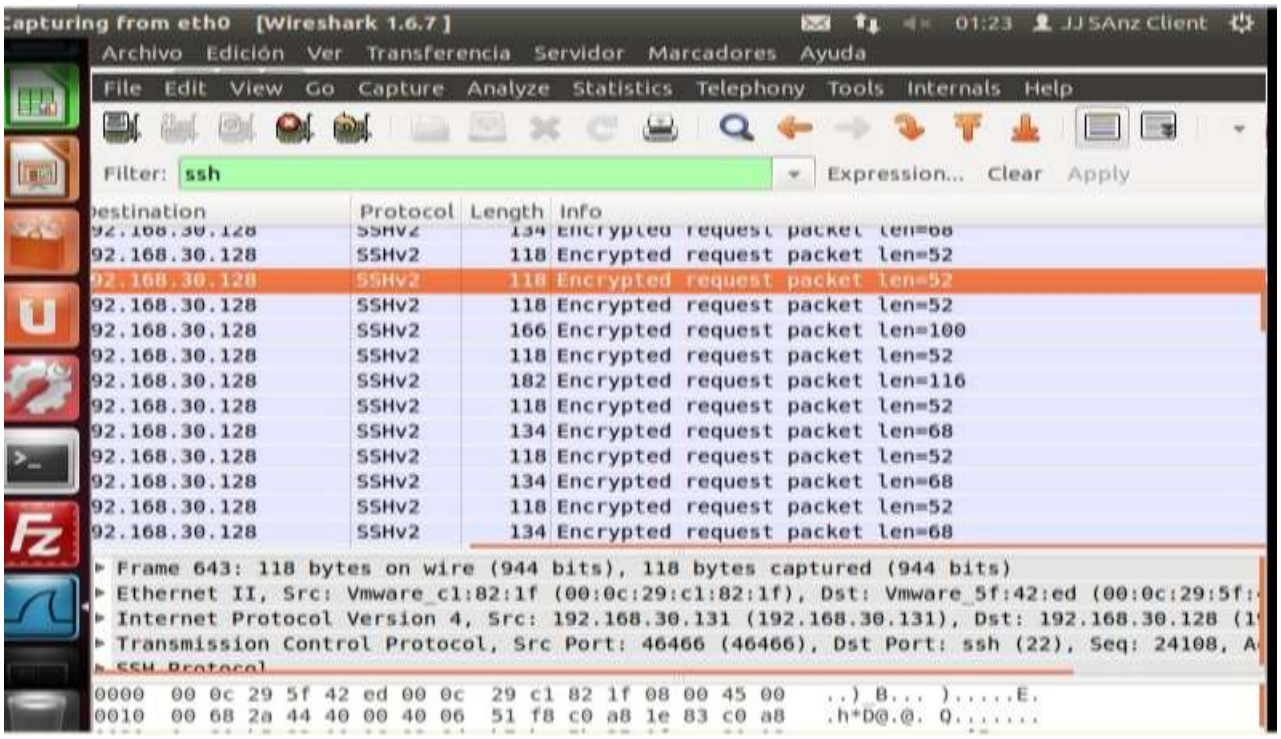


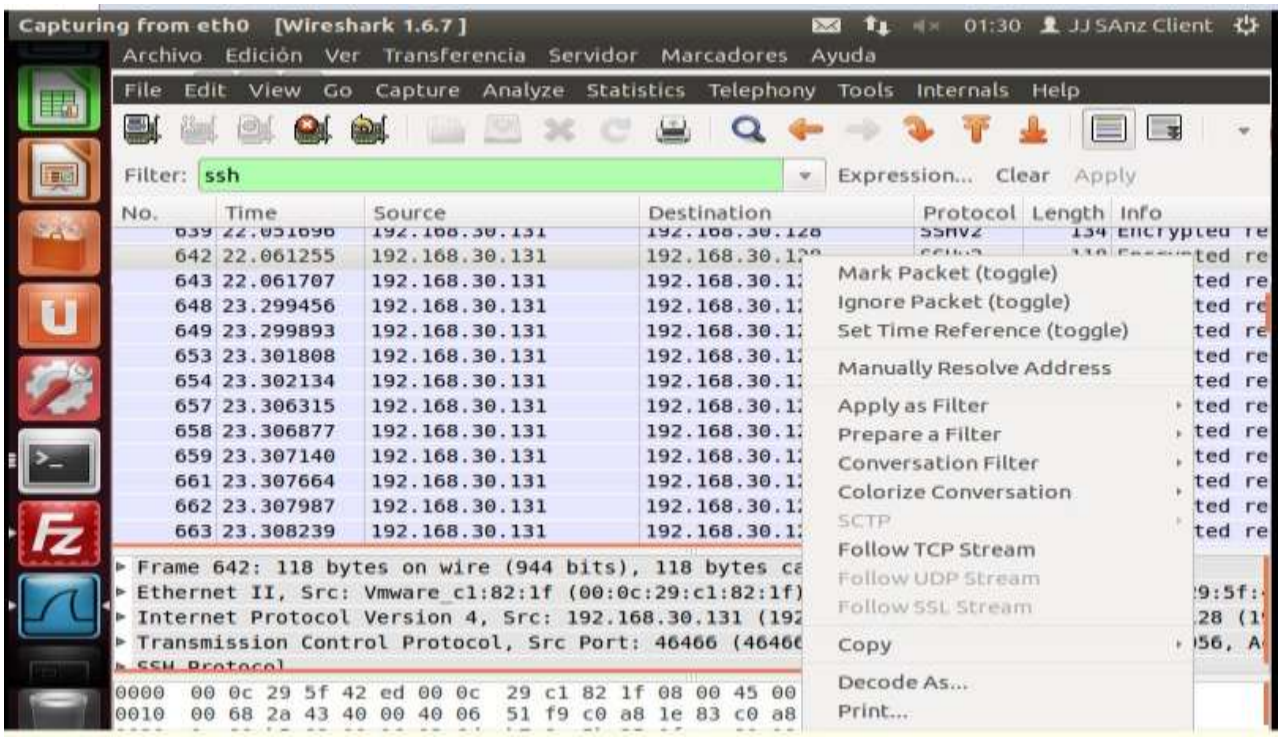
Verificamos en el escritorio del Cliente Ubuntu los archivos transferidos.



Después en el wireshark, revisamos el análisis de paquetes que se obtuvieron.

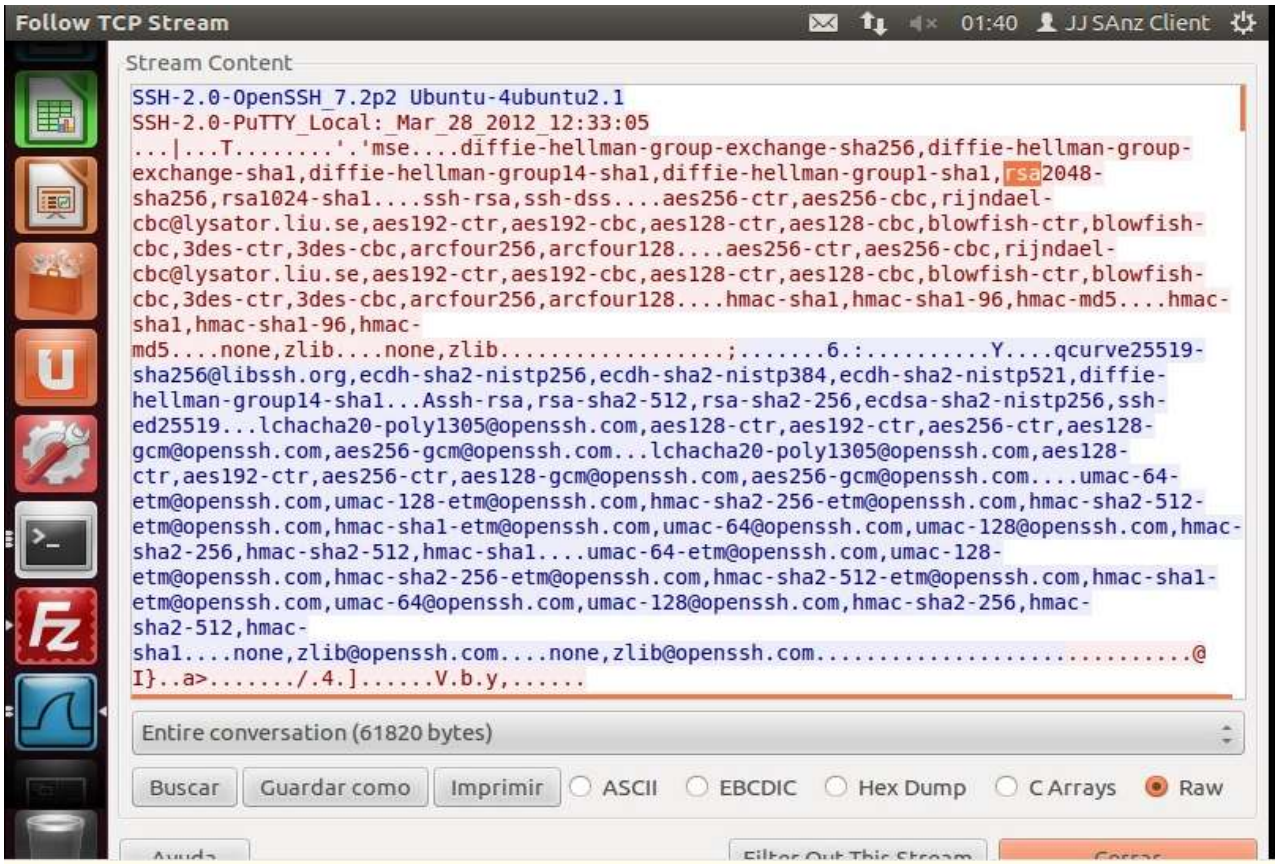
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



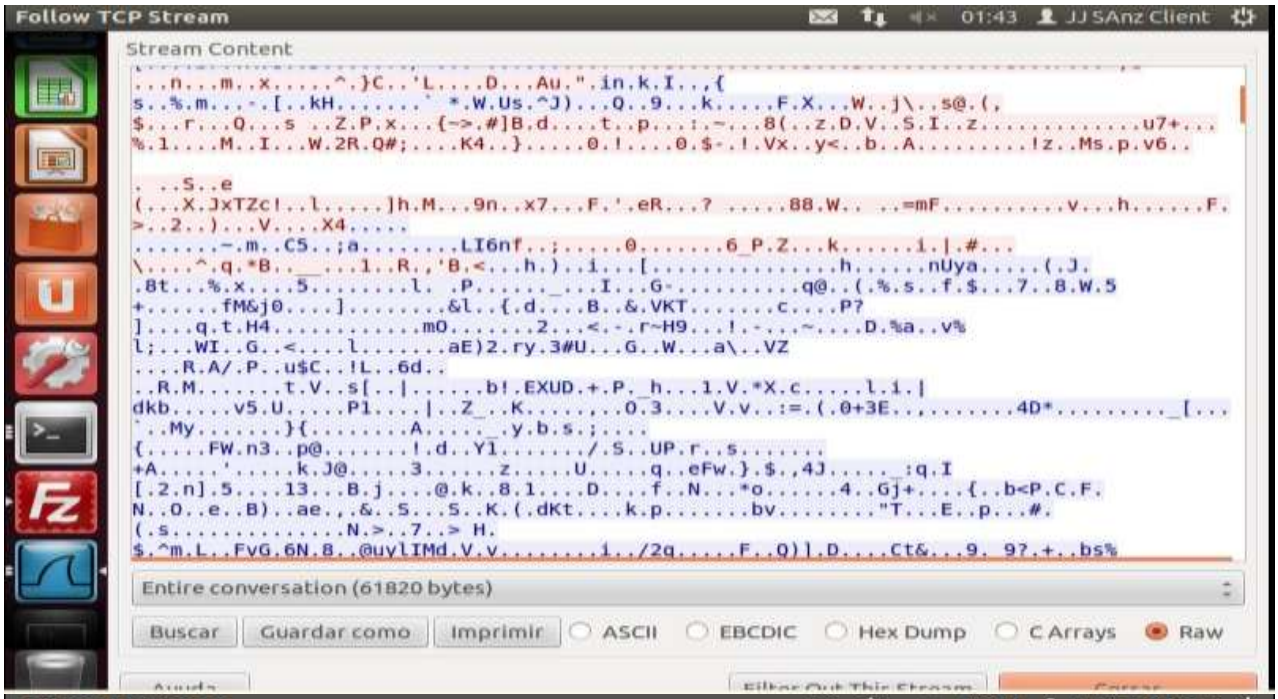


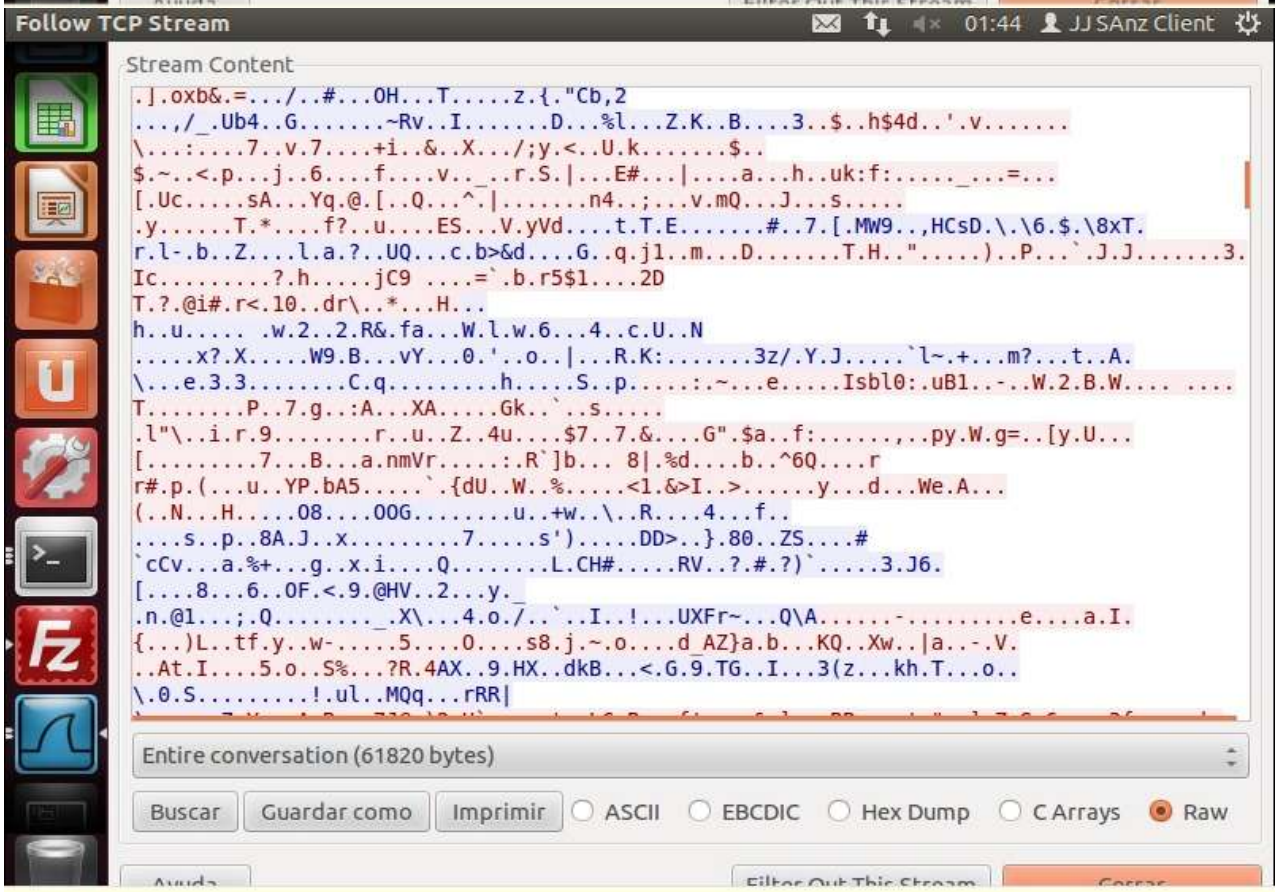
Ahora, vamos a mostrar los datos que tienen los paquetes después de haber sido transferidos en un entorno SFTP con encriptación RSA de 2048 bits de clave y cifrado AES de 256 bits.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

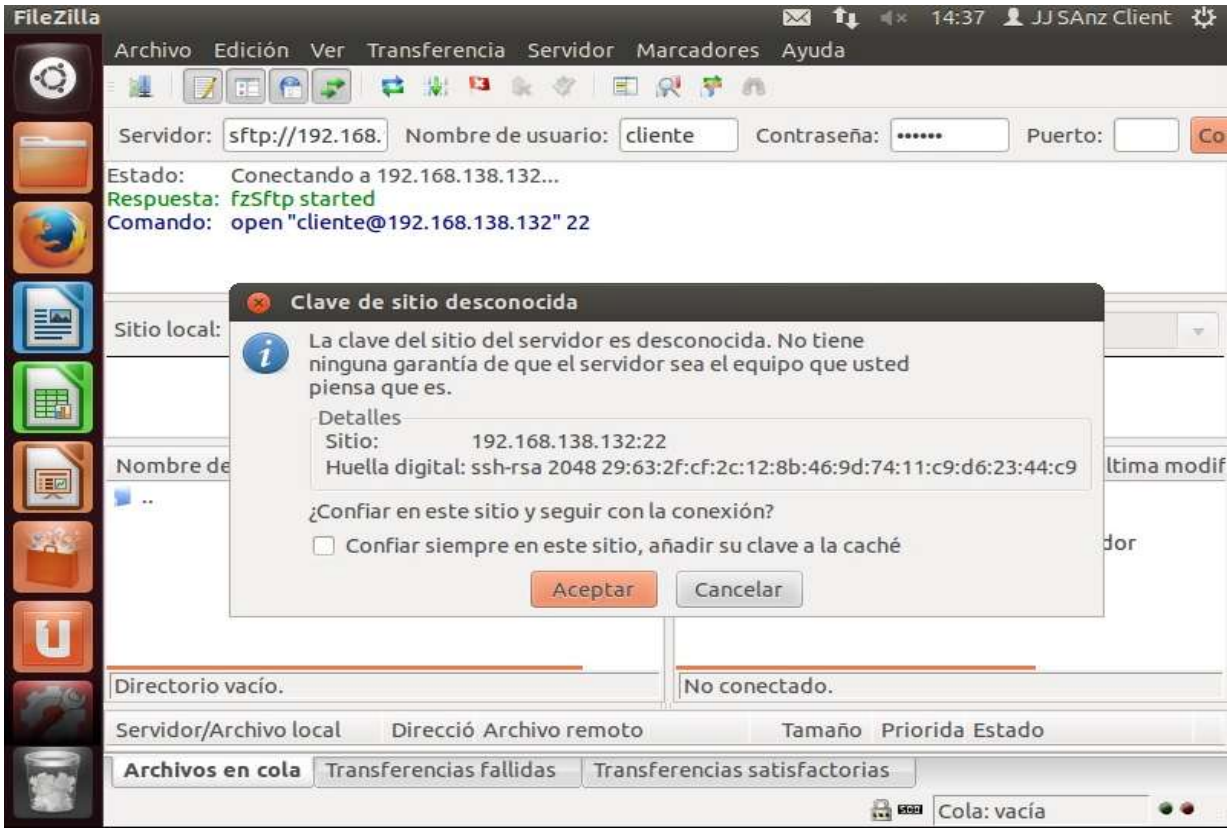




Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

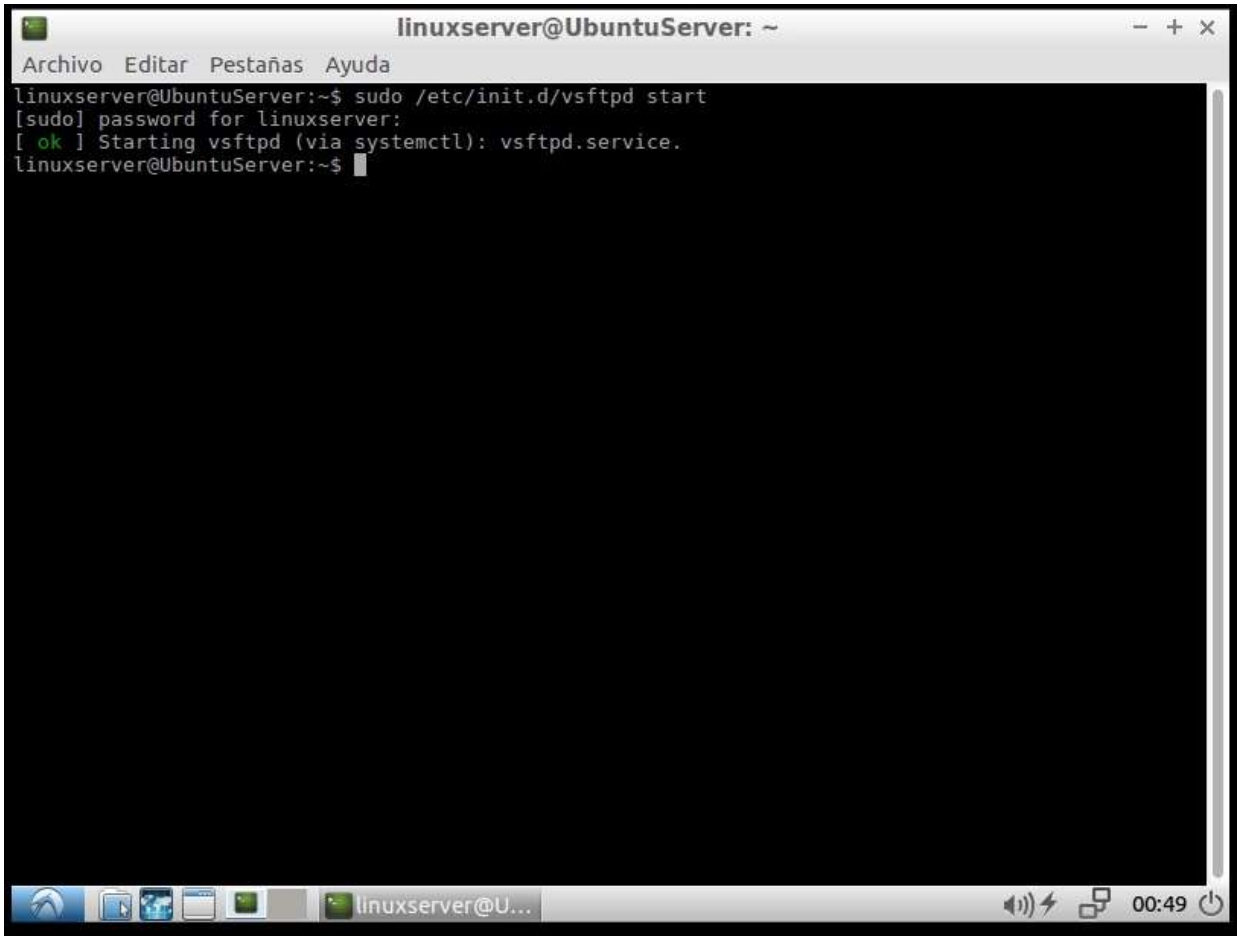
Luego, de haber demostrado para este 1 escenario las pruebas dieron como resultados 2 niveles de seguridad informática: integridad e confidencialidad de los datos; a través de esta técnica de encriptación se cumplen 2 principios: los datos no podrán ser vistos por terceros, permitiéndose la confidencialidad de los mismos, de la misma forma estos datos no podrán ser manipulados por terceros abarcando el principio de integridad de los mismos.



Por esta razón se considera el escenario más eficiente a tomar en cuenta, y que se ha demostrado que se cumplen los principios de confidencialidad e integridad de los datos, ya que es el principal objetivo de esta investigación, pero consecuentemente, se demostrara otros escenarios donde también verificaremos los niveles de seguridad de la información que se cumplen, y luego habrá un escenario que no implica ninguna técnica, siendo más vulnerable en aspectos de seguridad cuando se transmiten datos en una red informática.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Para el Escenario 2, levantaremos un servidor FTP (File Transfer Protocol), como se tiene por entendido, este servidor transmite la información en texto plano, lo que provoca una o más debilidades en nuestra red, dejando pasar todo el tráfico a vista y paciencia de crackers o terceras personas que pueden ver y capturar dichos archivos de nuestra red informática.



Para este escenario hemos asignado un usuario específico al servidor, llamado cliente que tendrá permisos especiales para subir y descargar archivos solo dentro de su directorio. En el servidor, visualizamos el directorio asignado a este usuario y los archivos alojados en el servidor dentro de su propia carpeta.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

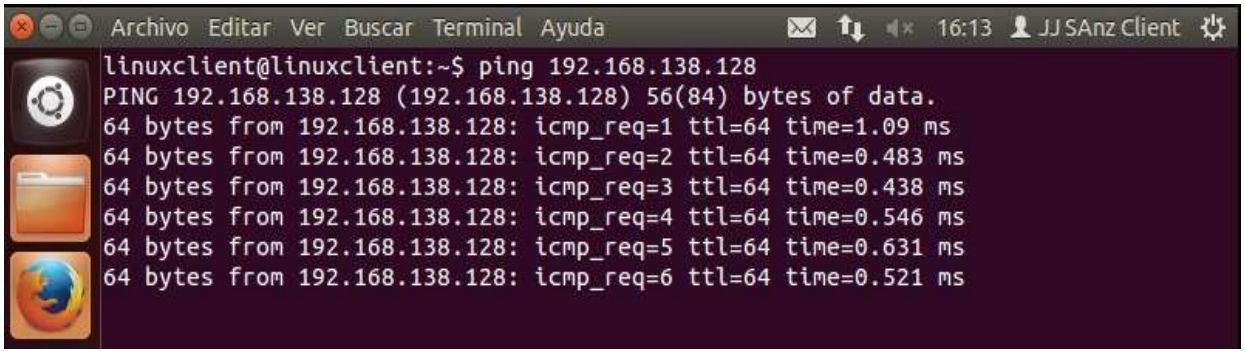
```
linuxserver@UbuntuServer: /home/cliente
Archivo  Editar  Pestañas  Ayuda
linuxserver@UbuntuServer:/home/cliente$ ls
1.txt    777.txt          analisis444.txt  practica.txt  prueba7.txt
222.txt  analisis111.txt  analisis555.txt  prueba10.txt  prueba8.txt
333.txt  analisis222.txt  examen.txt       prueba5.txt   prueba9.txt
666.txt  analisis333.txt  notas.txt        prueba6.txt   test.txt
linuxserver@UbuntuServer:/home/cliente$
```

Ahora, iremos a la máquina cliente de Linux-Ubuntu, que viene siendo cualquier cliente en la red intentando hacer una conexión con el servidor FTP, luego, verificamos la ruta donde deseamos transferir o descargar dichos archivos del servidor, y debemos darnos cuenta que no existe ningún archivo en esa ruta donde se alojarán los nuevos archivos.

```
Termina  Archivo  Editar  Ver  Buscar  Terminal  Ayuda   00:59  JJ SAnz Client
linuxclient@linuxclient: ~
linuxclient@linuxclient: ~/Escritorio
linuxclient@linuxclient:~$ pwd
/home/linuxclient
linuxclient@linuxclient:~$ ls
Descargas   Escritorio  Música      pruebasftp  Vídeos
Documentos  Imágenes    Plantillas  Público
linuxclient@linuxclient:~$ cd Escritorio/
linuxclient@linuxclient:~/Escritorio$ ls -l
total 0
linuxclient@linuxclient:~/Escritorio$
```

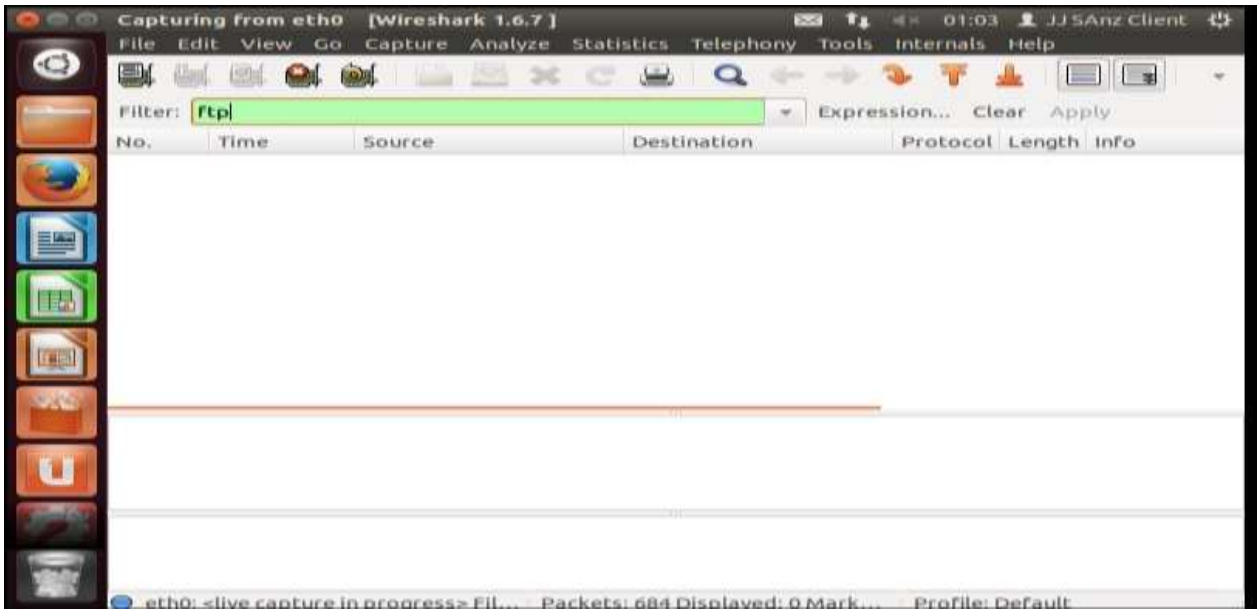
Antes de transferir los archivos verificamos nuestra ip en la red, luego verificamos la conexión con el servidor con el ip 192.168.138.128.

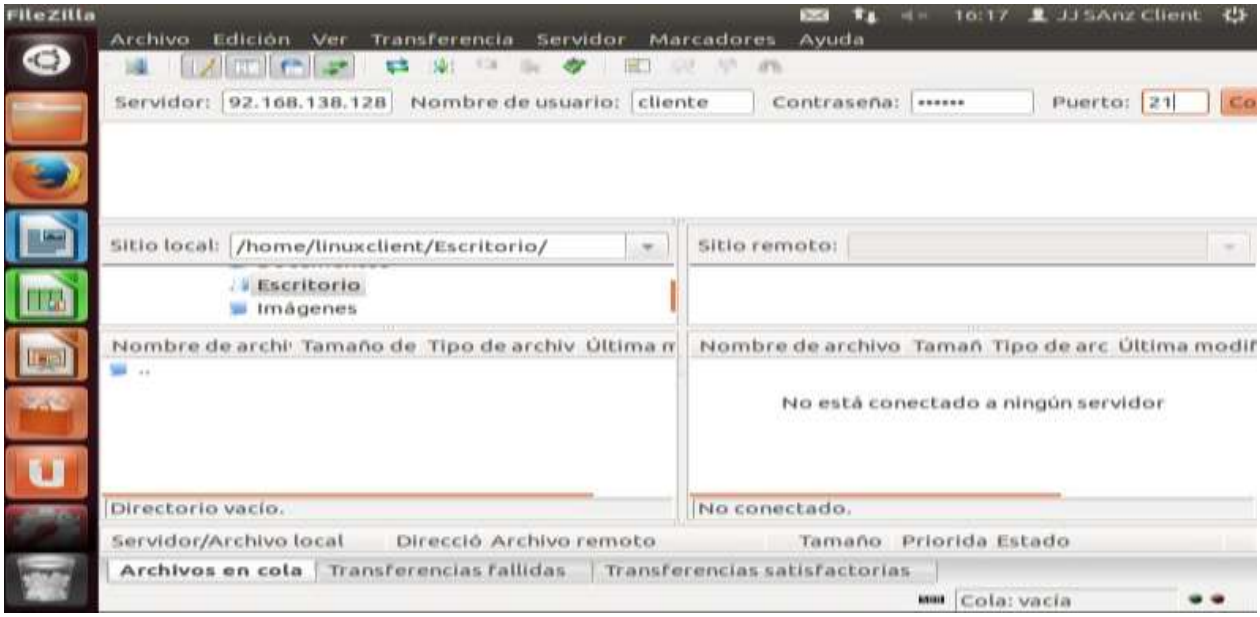
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



Antes de proceder a transferir, iniciaremos el analizador de tráfico en la red, llamado Wireshark, y capturamos todo lo que pasa a través de la tarjeta de red del cliente. Posteriormente, iniciaremos el filezilla para conectarnos a nuestro servidor en Linux-Ubuntu, con el IP: 192.168.138.128; usuario: cliente; contraseña: adminV; puerto: 21.

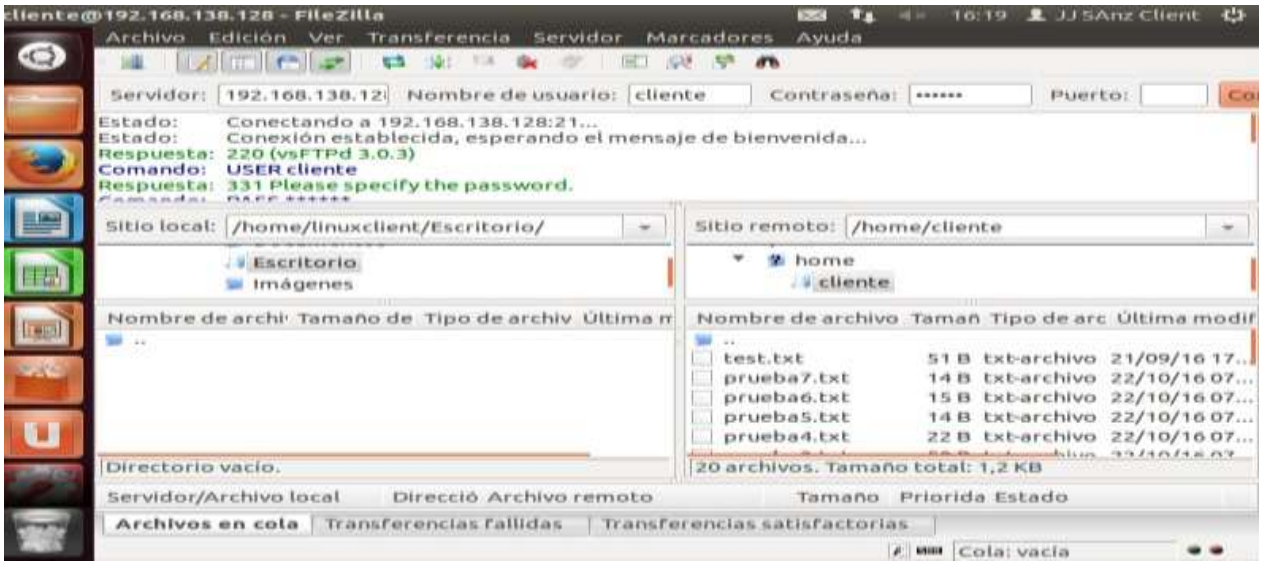
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



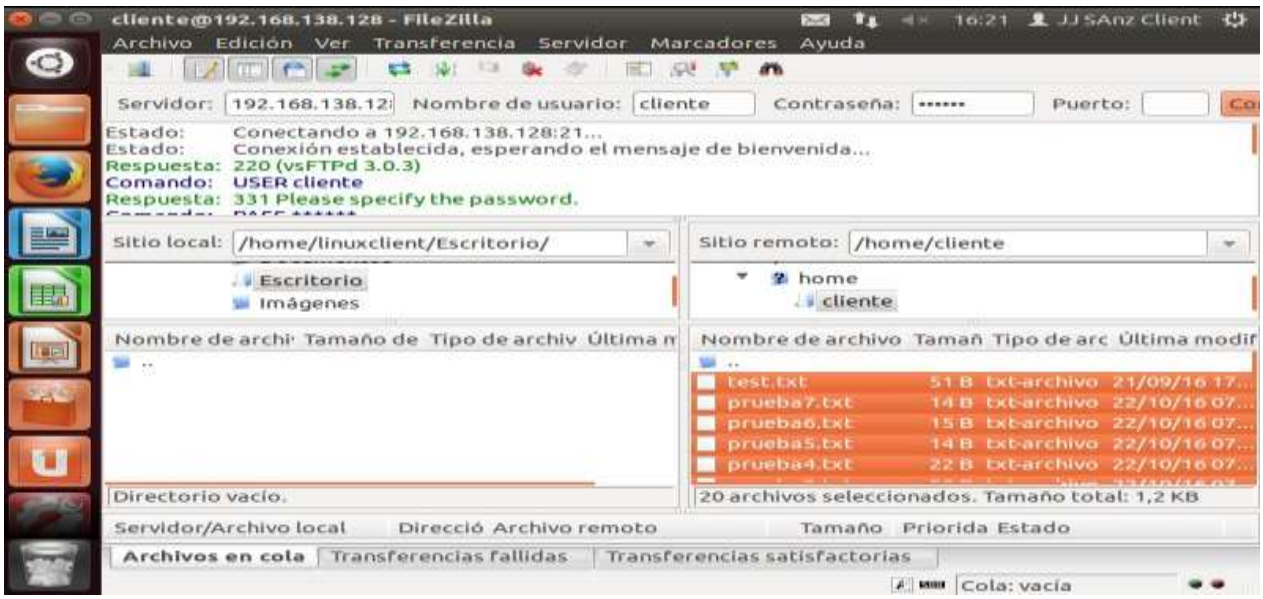


Después de conectarnos con los datos correctos, en la parte izquierda vemos el Directorio del Cliente, y a la derecha el directorio del Servidor, que en este caso se le asignó un usuario específico con permisos especiales denominado Cliente, para que tenga control total, pero solo sobre su directorio que en este escenario se llama cliente.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

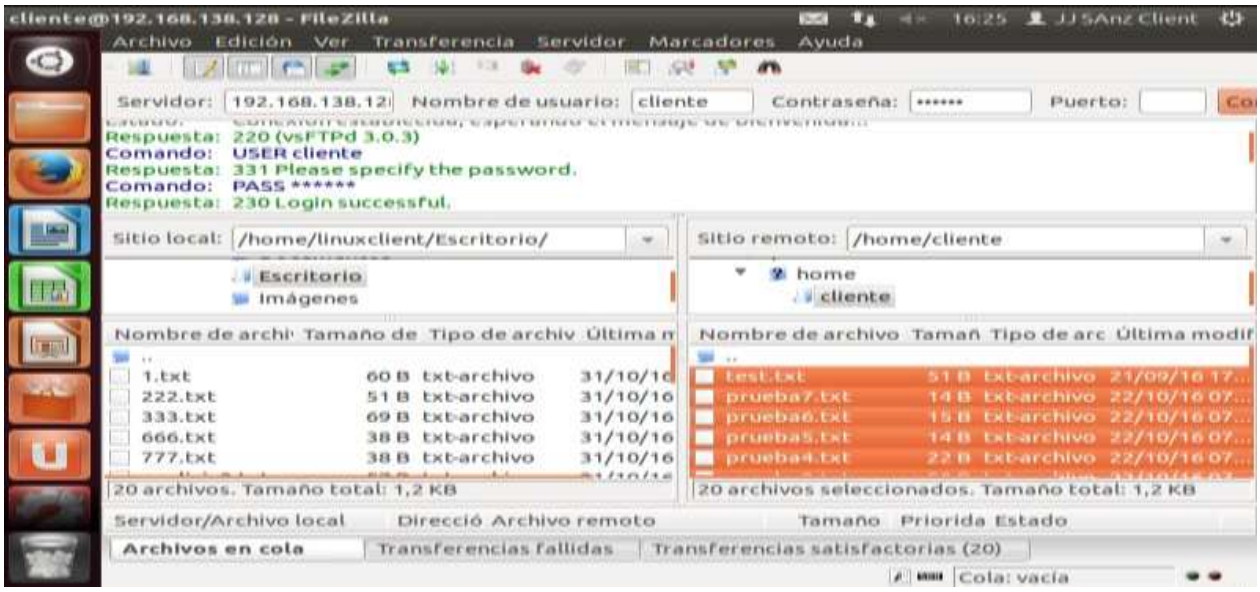


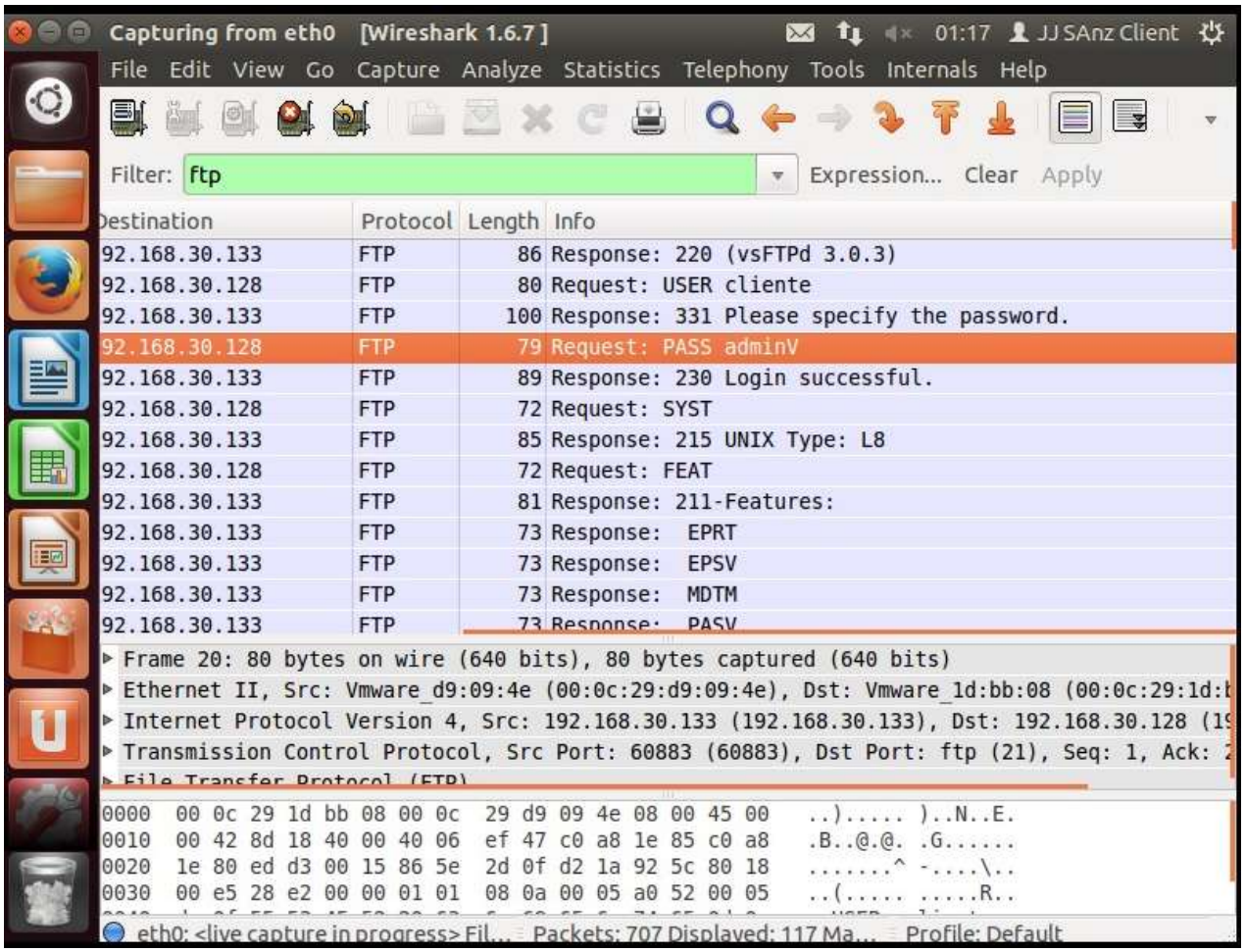
Seleccionamos los archivos a transferir desde el servidor al cliente, que en este caso son 20 archivos y lo transferiremos al escritorio del host Cliente, que como habíamos verificado está vacío, como nos muestra la *Figura* anterior.



Después de transferir, nos muestra abajo un mensaje transferencias satisfactorias 20. Veremos, luego, el resultado del análisis que ha tenido el Wireshark, en la obtención de todos esos datos que han viajado en la red en texto plano, para demostrar, que se ha vulnerado todos los principios de seguridad informática que debe existir en una red informática, ya que sin ellos podríamos decir que no estamos ante nada seguro.

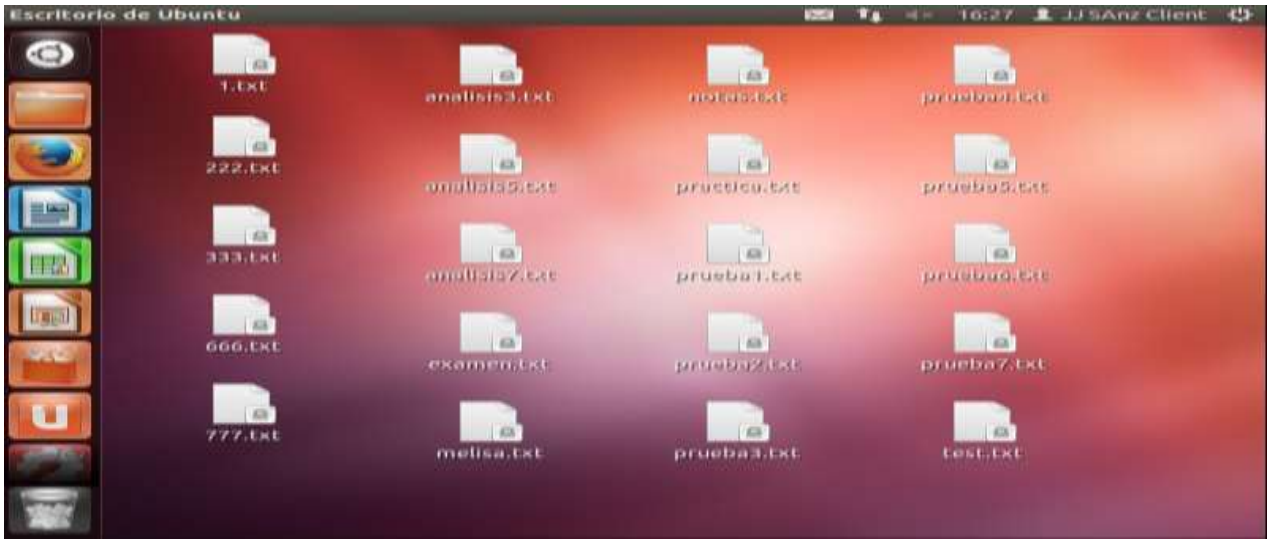
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



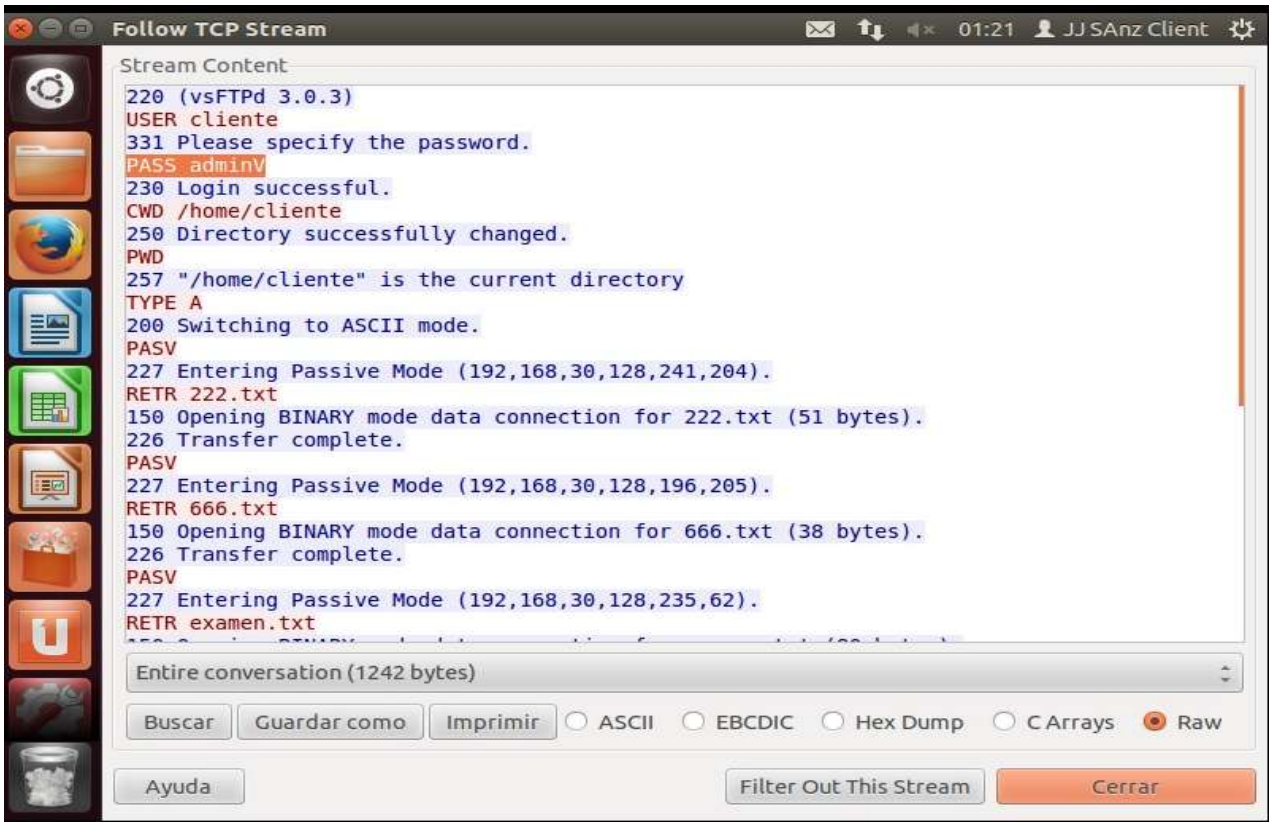


Ahora, por nuestra cuenta nos toca verificar que los 20 archivos hayan llegado al directorio seleccionado en el host cliente de la red, que no era más que el Escritorio.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

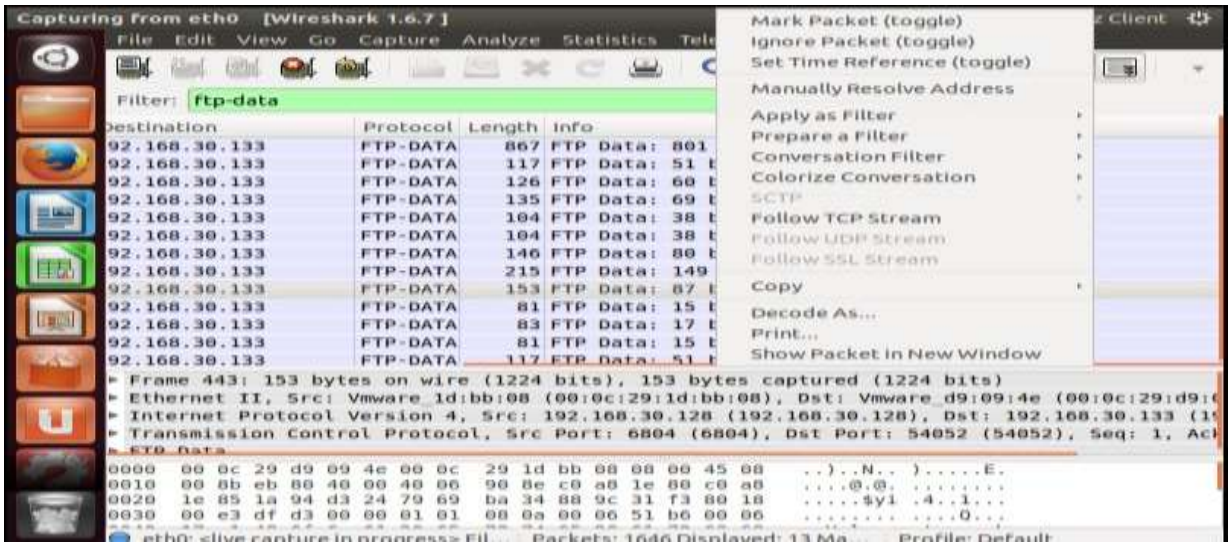


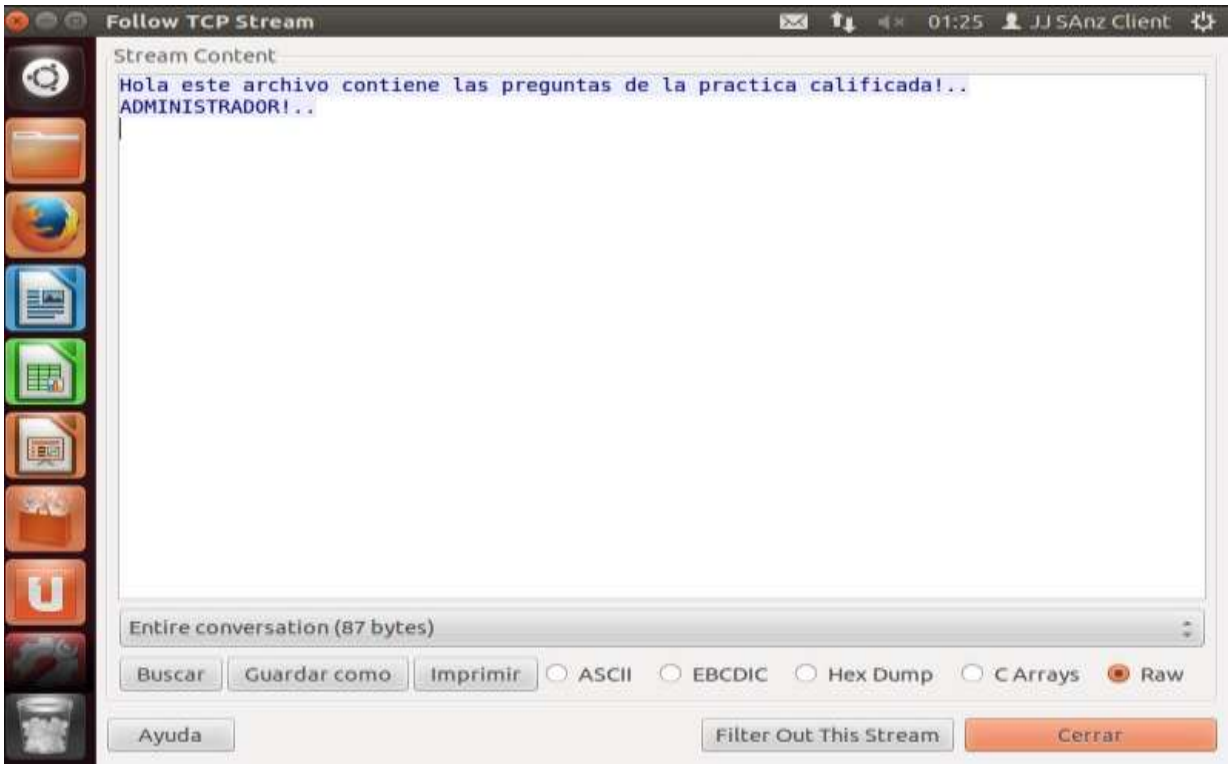
Después, en el Wireshark, observamos que nos deja pasar el login y nuestra



contraseña en texto plano, además de los nombres de los archivos; luego nos toca mostrar el contenido de la cadena de los archivos transmitidos. Para ello, nos centraremos en solo 2 archivos transmitidos (notas.txt y practica.txt) de los 20, para ahorrarnos tiempo, de lo que llevaría mostrar el contenido de los 20 archivos.

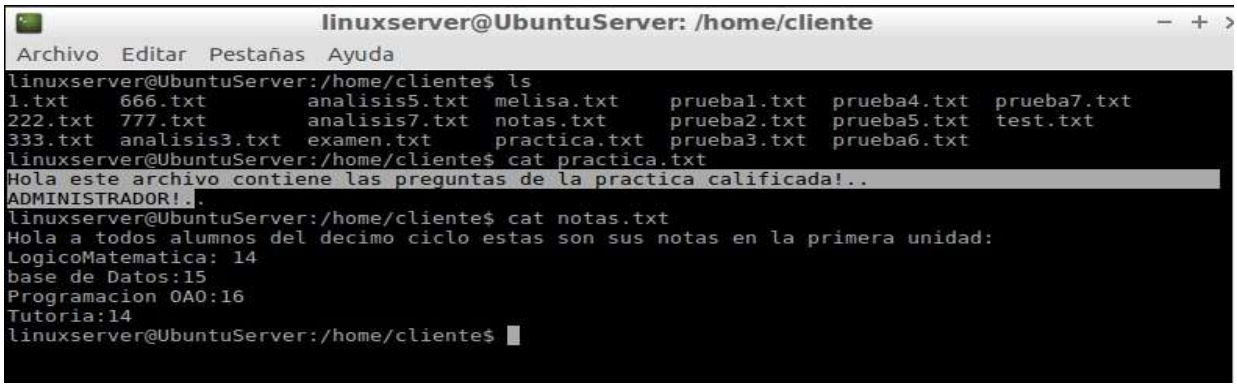
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

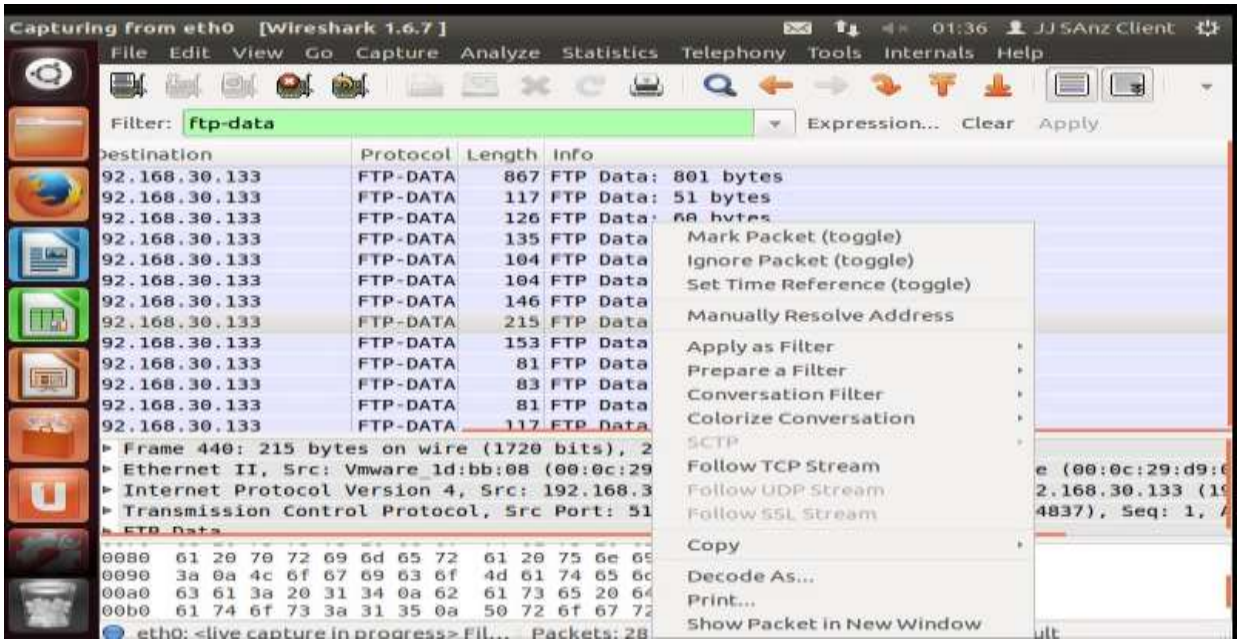




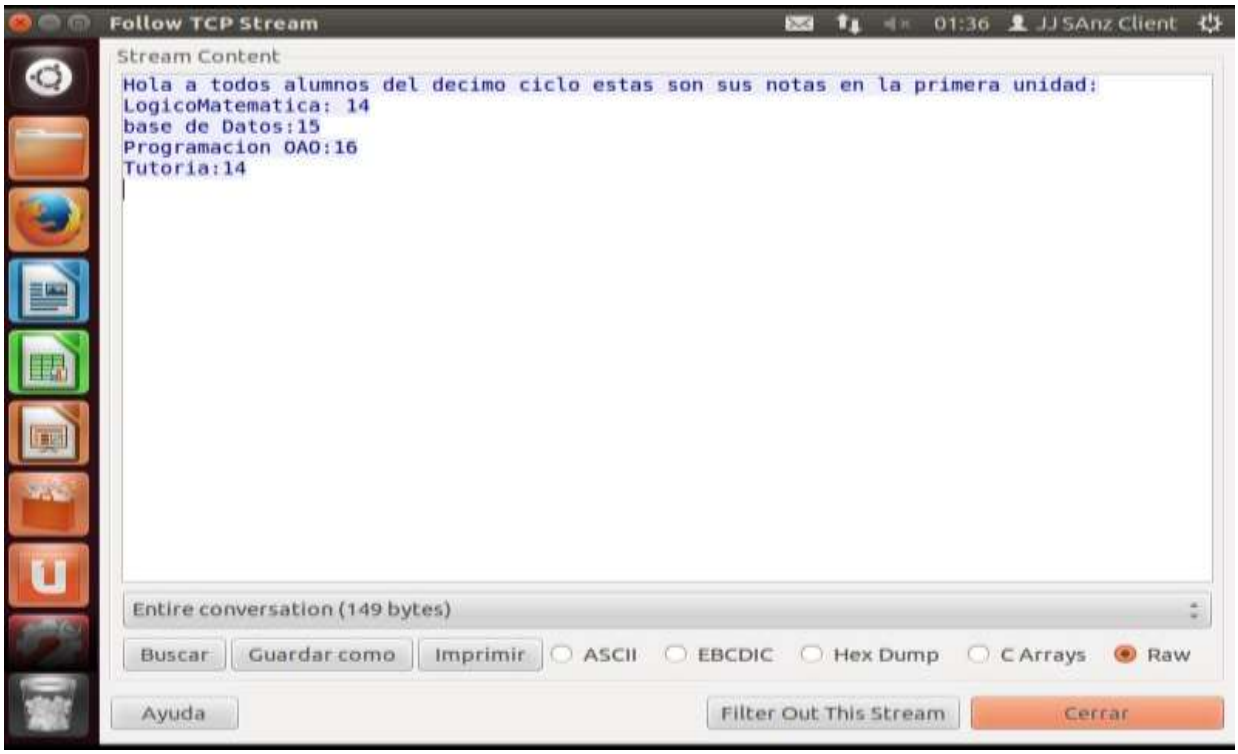
Ahora, desde el servidor de Linux-Ubuntu, verificaremos el contenido de los archivos (practica.txt y notas.txt), de tal forma de verificar, que los datos que nos muestra el Wireshark son correctos.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis





Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



Por tanto, ha quedado demostrado, que para este escenario donde no existe la implementación de ninguna técnica de Encriptación en la red informática, se está expuesto a que nuestra información sea divulgada o escuchada por cualquier persona que se infiltre en la red, siendo un escenario que no ofrece garantías en lo que respecta la seguridad en la transferencia de archivos en un entorno de red, lo que generaría la infiltración de un virus informático, posteriormente caídas de servicio, suplantación de identidades, etc.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

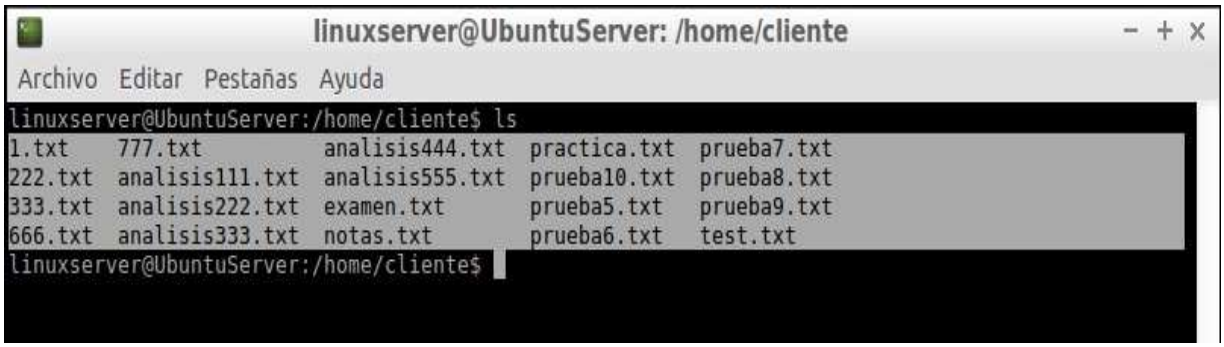
Por último, hemos analizado otro escenario, donde la implementación de la seguridad permite mitigar posibles ataques a la red informática como ya se había comentado.

En este 3er escenario, hemos trabajado con un servidor FTPS (File Transfer Protocol Secure), que trabaja con seguridad basada en SSL/TLS. Para ello, hemos instalado un certificado SSL/TLS, sobre el servidor FTP, donde no existe ninguna seguridad de por medio, como se ha demostrado en el escenario anterior.

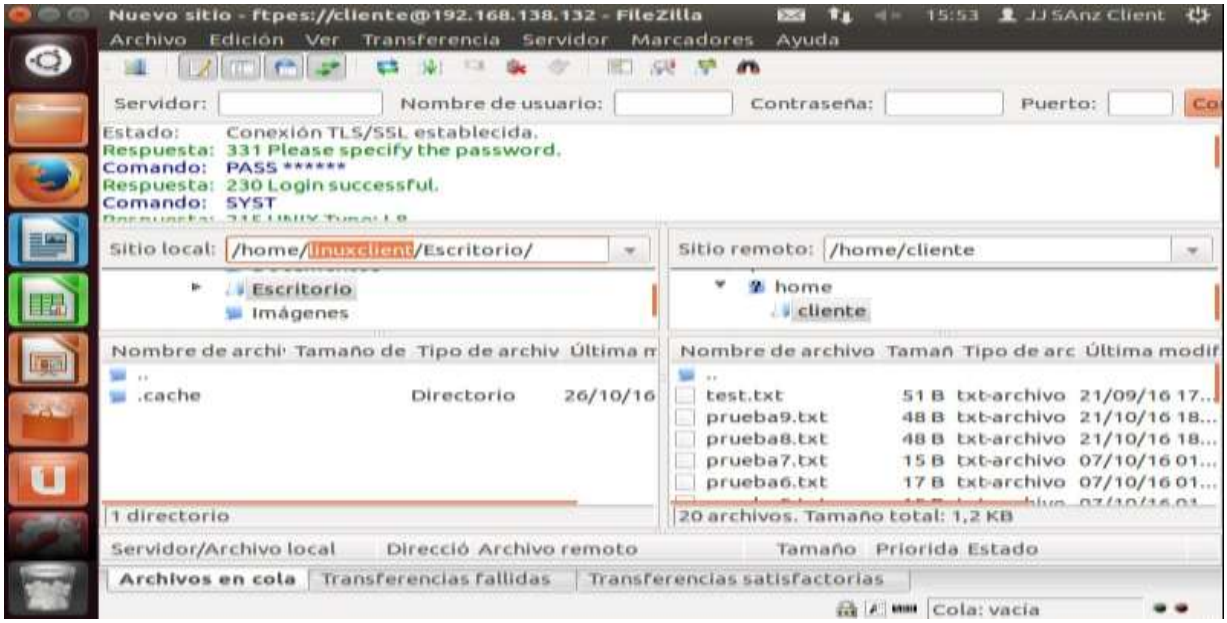
```
linuxserver@UbuntuServer: ~
Archivo  Editar  Pestañas  Ayuda
gai.conf                lvm             rc5.d                   X11
gconf                   lxdm            rc6.d                   xdg
ghostscript             machine-id      rc.local                xinetd.conf
gnome                   magic           rcS.d                   xinetd.d
gnome-app-install       magic.mime      resolvconf              xml
gnome-system-tools      mailcap         resolv.conf             zsh_command_not_found
groff                   mailcap.order   rmt
linuxserver@UbuntuServer:/etc$ sudo nano vsftpd.conf
[sudo] password for linuxserver:
linuxserver@UbuntuServer:/etc$ sudo /etc/init.d/vsftpd restart
[ ok ] Restarting vsftpd (via systemctl): vsftpd.service.
linuxserver@UbuntuServer:/etc$ cd
linuxserver@UbuntuServer:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout /etc
/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
[sudo] password for linuxserver:
Generating a 1024 bit RSA private key
.....................................++++++
.......................++++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PE
State or Province Name (full name) [Some-State]:Lambayeque-Chiclayo
Locality Name (eg, city) []:Chiclayo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:JJ SAnz Company
Organizational Unit Name (eg, section) []:Student
Common Name (e.g. server FQDN or YOUR name) []:SanchezVallejosJ
Email Address []:vallejosjm@crece.uss.edu.pe
linuxserver@UbuntuServer:~$
linuxserver@U...                                        02:51
```

Ahora enviaremos los mismos archivos del escenario anterior (20 archivos), desde el servidor.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

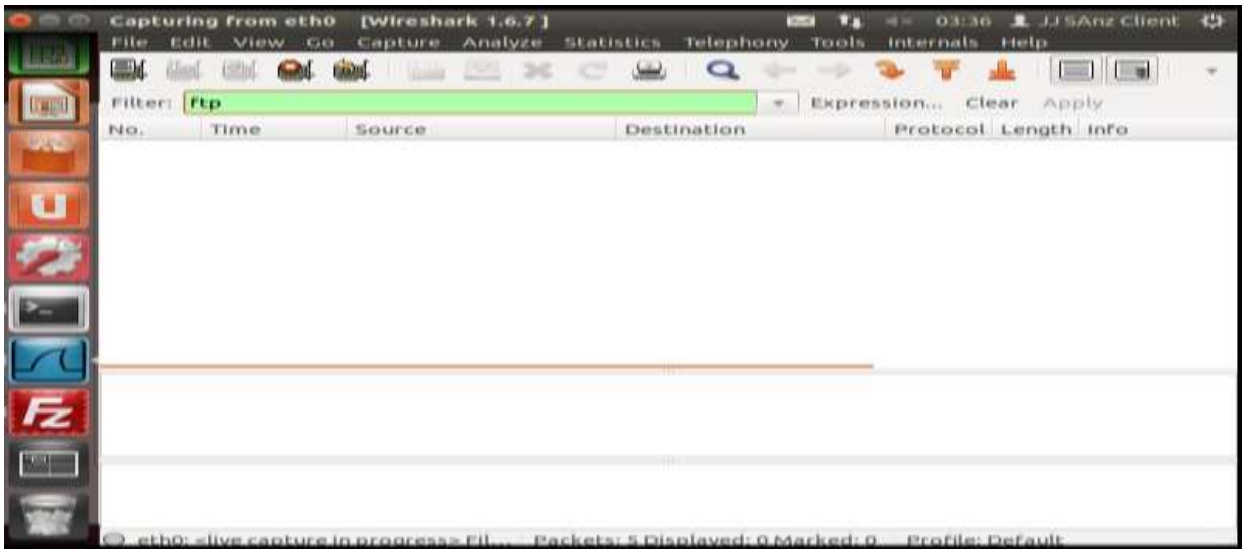


Ahora nos conectaremos desde la maquina cliente al servidor: 192.168.138.132; usuario: cliente; clave:adminV; puerto:21.



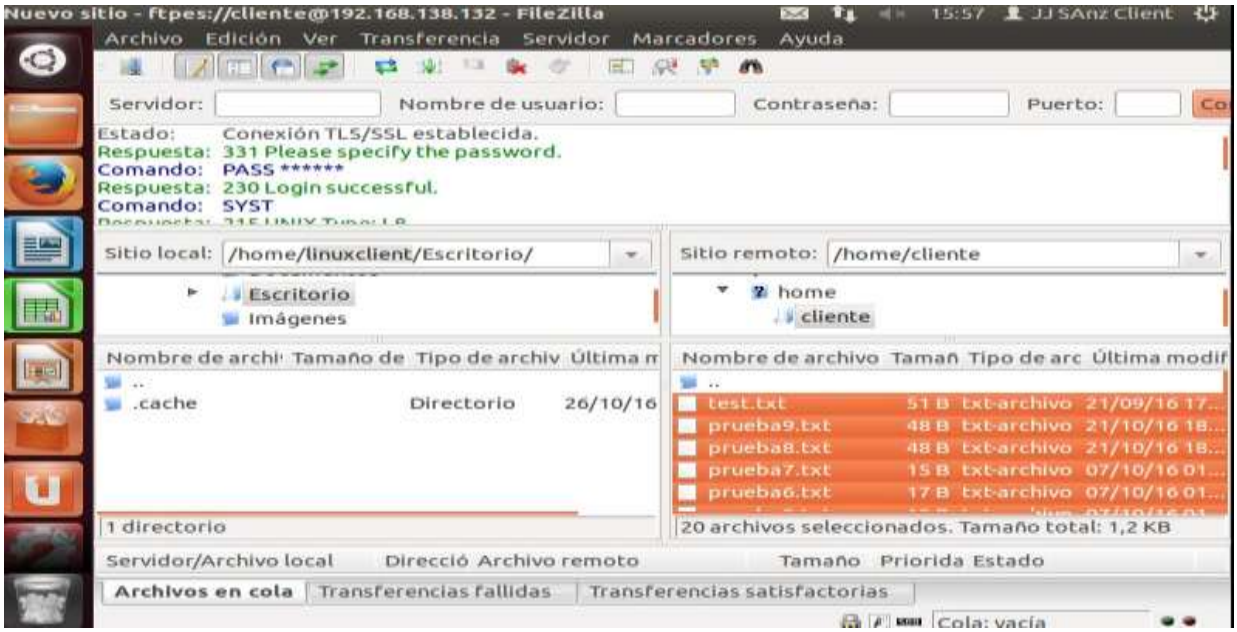
Cargamos el wireshark, y verificamos que el escritorio del cliente esté sin ningún archivo listo para la transferencia segura.

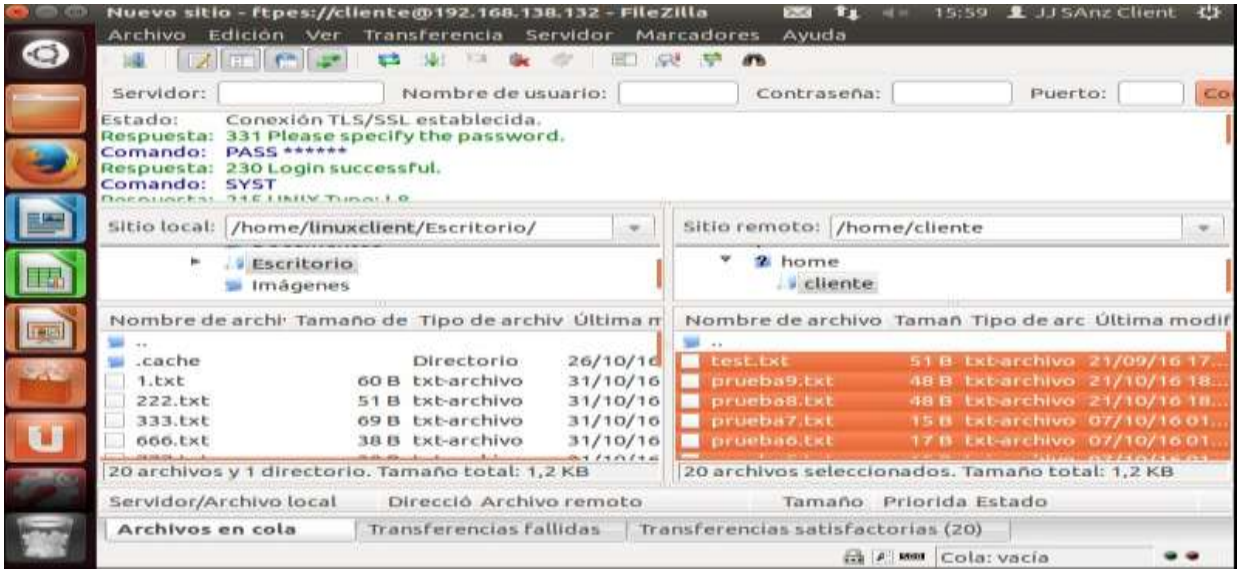
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis



Ahora, seleccionaremos los archivos a transferir desde el servidor, en la parte derecha donde está su directorio, desde la interfaz de Filezilla, luego procederemos a transferir los archivos.

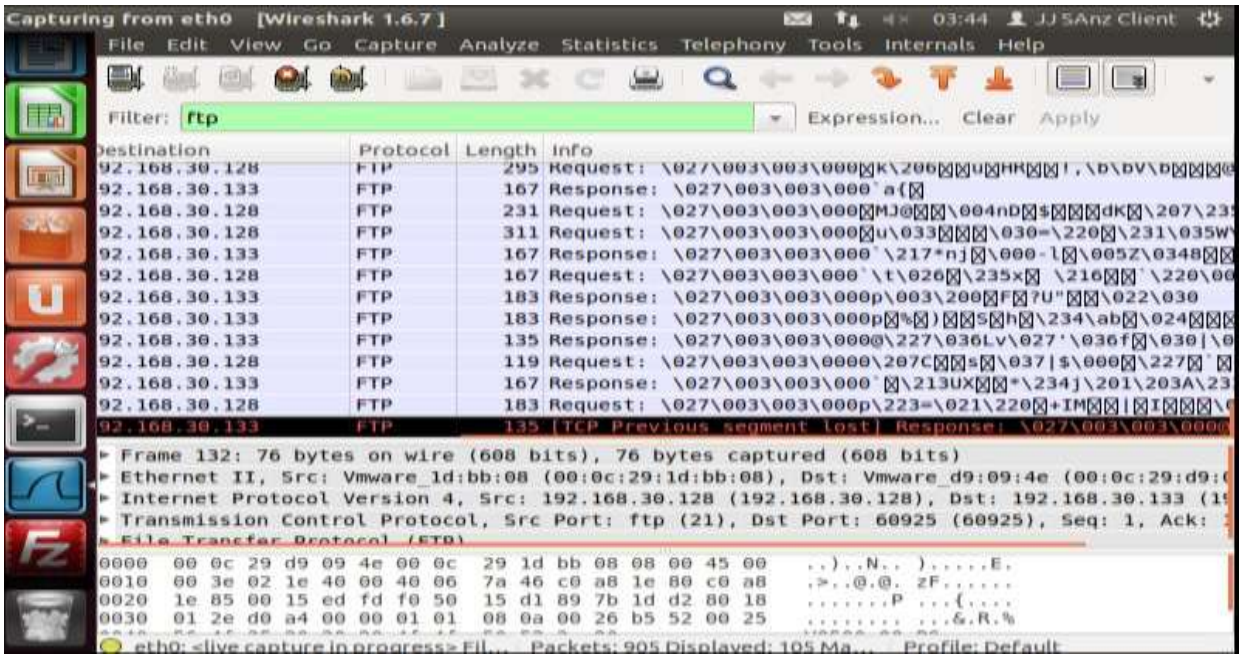
Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

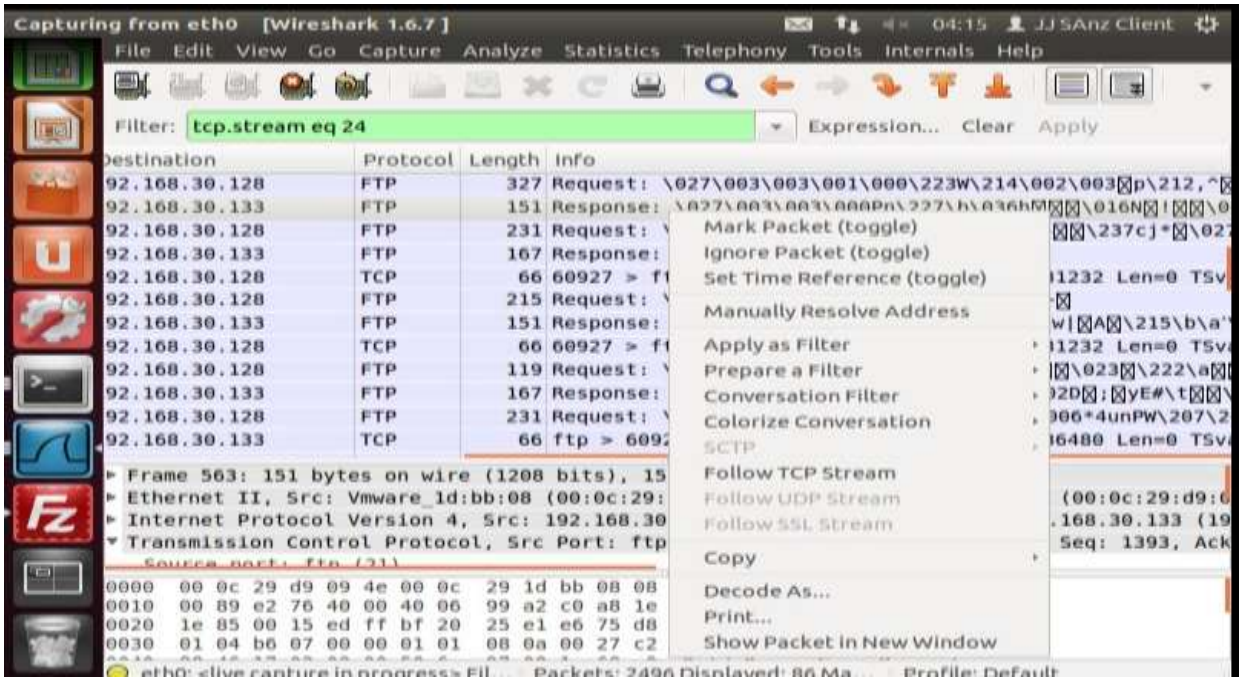




Ahora desde el Wireshark, procederemos a hacer el análisis de los paquetes transferidos en la red informática.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

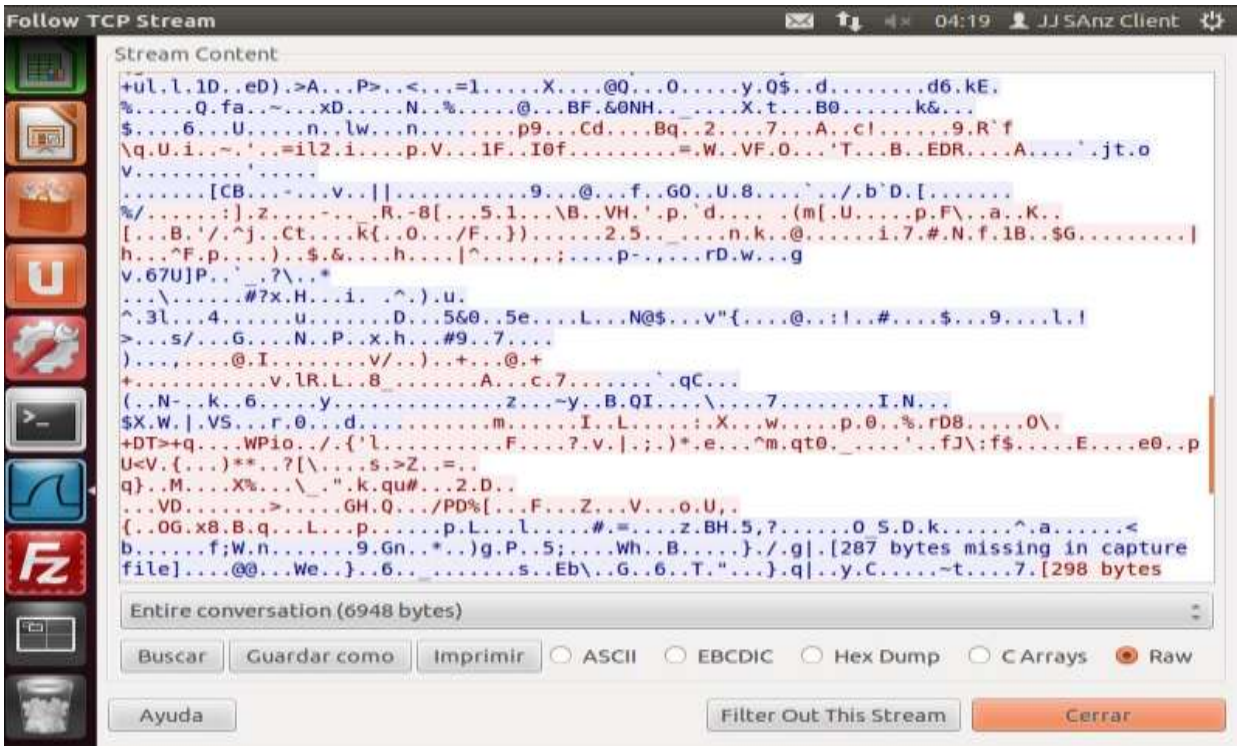




Ahora, analizaremos el resultado del análisis mostrado por el wireshark, donde nos muestra, que efectivamente las técnicas de encriptación RSA y AES de 1024 bits, que se generó con el certificado SSL/TLS, es invulnerables si se implementan en una red informática.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

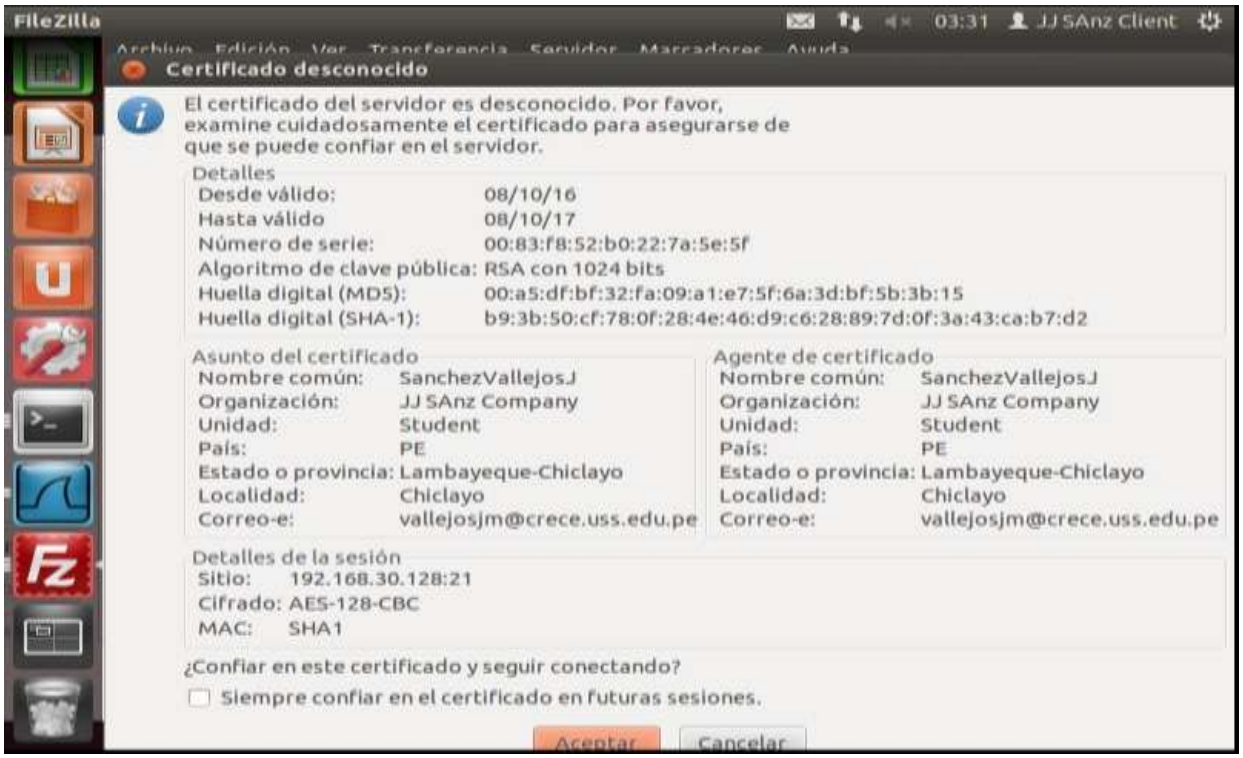
Follow TCP Stream
03:49
JJ SAnz Client
Stream Content
220 (vsFTPd 3.0.3)
AUTH TLS
234 Proceed with negotiation.



EL resultado del análisis, han dado como resultado un escenario, donde no se le puede de ninguna forma vulnerar a la red, para conocer su tráfico, siendo un escenario eficiente, además cumple ciertos principios de seguridad: confidencialidad, integridad de la información transmitida ,en cambio no tan avanzado como el primer escenario, ya que esta última técnica genera claves de encriptación de 1024 bits, a comparación del 1er escenario donde las claves de encriptación son de 2048 bits, viene siendo el doble de seguridad, además en cuestiones de transferencia de archivos de mayores dimensiones, será más rápida la transferencia de los datos en una red informática, donde los recursos a administrar son mayores a comparación que en una red informática de menores

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

recursos.



Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

a) Se analizó 2 protocolos con respecto a la seguridad en la transferencia segura de archivos SSHv2, y TLS, siendo los más seguros; también se analizó 2 algoritmos de encriptación como RSA de encriptación asimétrica y AES de encriptación simétrica, estos por ser los que mejor están constituidos en su criptosistema o por su tecnología, seguridad, velocidad, fácil comprensión de su funcionamiento, etc.

b) Se implementó la topología contextual Física y Lógica de la red con respecto a la transferencia segura de archivos, donde cada red es segmentada con Vlans, basado en el modelo estrella extendida que es el más utilizado por su facilidad de implementación y administración.

c) Se ha levantado un prototipo del diseño realizado con respecto a la transferencia segura de archivos en un entorno para que sea fiable, este prototipo de red, ha sido ejecutado sobre la plataforma Linux Ubuntu, donde se instaló un servidor y un cliente Linux-Ubuntu de las versiones 16.04.1 LTS Xenial Xerus y 12.045 LTS precise pangolín, realizando una conexión cliente-servidor, simulado en máquinas virtuales utilizando la herramienta VMware Workstation 8.

d)) Finalmente las pruebas de transferencias seguras en un entorno para que sea fiable las hemos realizado con el Sniffer Wireshark, desde la plataforma Ubuntu-Linux, se analizó un escenario donde no se implementó ninguna técnica de encriptación, es decir, un escenario donde la transferencia se realizó en texto plano, lo que ocasionó que se logré vulnerar los datos transmitidos, a su vez se vulneró los principios de seguridad: confidencialidad, integridad, y autenticación; luego se ha implementado 2 escenarios eficientes que se probaron en el sniffer Wireshark, para asegurar que nuestra red mitigue ciertas amenazas. Finalmente, las pruebas realizadas con el sniffer wireshark dieron como resultado el escenario más eficiente en cuestiones de seguridad de los datos transmitidos, cumpliendo ciertos niveles de seguridad: confidencialidad e integridad de los datos transmitidos, y autenticación, así como también el mejor tiempo de procesamiento para la técnica RSA de 2048 bits de clave con cifrado AES de 256 bits, permitiendo que los datos sean encriptados y transferidos en el menor tiempo posible, siendo 45 segundos, además permitiendo una mayor tecnología de encriptación con clave de 2048 bits, comparado con la técnica RSA de 1024 bits de clave, con cifrado AES de 128 bits, este último con 320 segundos de

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

tiempo de procesamiento; en cuanto el margen de error en la transmisión de la Técnica 1(escenario más eficiente) ha dado 28.4%, esto por ser la técnica más veloz al transferir grandes cantidades de información, generando una mínima pérdida de paquetes, comparado con la Técnica 2 con una margen de error en la transmisión de 27%.

6.2. Recomendaciones

La implementación de encriptación con la técnica RSA de 2048 bits de clave con cifrado AES de 256 bits, dará como resultado, si se implementa en las organizaciones, que los datos no sean expuestos en la red y sean capturados por algún cyber-criminal como lo es un cracker, ya que la información que se transmita puede ser de carácter confidencial, y pueda ser manipulada; por este motivo debe ser trasmitida debidamente cifrada o encriptada con el protocolo SSH v2 que trabaja con esta técnica. Finalmente se mitigará el impacto que generé un ataque informático a una red local, que se implemente esta técnica de encriptación con respecto a la transferencia de archivos en una red para que sea fiable, además del riesgo que generaría a una empresa u organización el robo o pérdida de dicha información, la suplantación de identidades, la interrupción del servicio también se reducirá. Finalmente, el valor del servicio que una empresa o negocio requiere será optimizado en el tiempo de trabajo continuo con las técnicas de encriptación donde incrementará la seguridad en un entorno de red para que sea fiable. Consecuentemente, el escenario con el protocolo TLS que trabaja con el algoritmo de encriptación RSA de 1024 bits de clave y cifrado AES de 128 bits, también es escenario recomendado para ser implementado en una red local que necesite mejorar la seguridad con respecto a la transferencia de los archivos en un entorno para que sea fiable, está técnica es eficiente en cuestiones de seguridad, ya que provee niveles o principios de seguridad tales como la confidencialidad, integridad y autenticación, al igual que el protocolo SSH v2 del escenario más eficiente, la diferencia es la tecnología de encriptación y la velocidad de transferencia que proporciona el protocolo SSH v2, con respecto al protocolo TLS/SSL, pero en escenarios donde se necesite implementar una red local con seguridad respecto a la transferencia de archivos, se recomienda también el protocolo TLS/SSL, la diferencia existe en una red donde los recursos a administrar son mayores y el tiempo de transmisión viene siendo un factor primordial, los resultados nos muestran que este protocolo es menos avanzado que el protocolo SSH v2, en cuestiones de tiempo de procesamiento y longitud de clave o por su tecnología.

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Referencias

Agulló, D., Guerra, M. C., Silva, F., & Vivanco, R. (2012). *Seguridad e integridad de la transferencia de datos*. *Conicyt*, 1-13.

Bareño , R., Navarro, W., Cárdenas, S., Sarmiento, H., Duarte, N. & Vargas, G., (2015). *Analisis de la seguridad en la implementación de Servicios Corporativos sobre el protocolo IPV6*. Revista de Tecnología. Volumen (14), 127-138. .Recuperado de: https://dialnet.unirioja.es/descarga/articulo/6041589.pdf

Benton, K., & Bross, T. (2013). *Timing Analysis of SSL/TLS Man in the Middle Attacks. Arxiv*, 1-9.

Blanco Galicia, R (2010). *Analisis de Algoritmos Criptográficos y su aplicación al cifrado de arhivos*. Mexico D.F.: Instituto politecnico nacional. Recuperado de: http://itzamna.bnct.ipn.mx:8080/bitstream/handle/123456789/6239/IF2.45.pdf?sequence=1&isAllowed=y

Díaz López, P (2012). *Algoritmo de Encripción Híbrido: Cifrado Simétrico AES (Advanced Encryption Standar) en Combinación con curva Elíptica*. (Tesis de Maestría). Mexico D.F.: Instituto politecnico nacional. Recuperado de: http://tesis.ipn.mx/handle/123456789/17679?show=full

Escrivá Gascó, G.,Romero Serrano, R., & Ramada, D. (2013). *Seguridad Informática*. Macmillan Iberia. (1 Edición). Madrid

EstudioNeobox, (2011). Glosario de Seguridad Informática. Recuperado de: https://carrmen.jimdo.com/glosario-de-terminos/

Forné, J., Melús, J. L., & Soriano, M. (2011). *Criptografia y seguridad en comunicaciones. Fecyt*, 15-25.

Franchi, M. (2012). *Algoritmos de Encriptación de Clave Asimétrica.* Argentina.: Universidad Nacional de la Plata. Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/26137/Documento_completo.pdf?sequence=1

Gallegos García, G. (2011). *Diseño de protocolos criptográficos para votación electrónica.* (Tesis Doctoral). Mexico D.F.: Instituto politecnico nacional. Recuperado de: http://itzamna.bnct.ipn.mx:8080/bitstream/handle/123456789/10008/215.pdf?sequence=1&isAllowed=y

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

García, G. (2009). Términos de *Seguridad Informática*. Instituto Santa Maria. Recuperado de:

https://www.taringa.net/posts/apuntes-y-monografias/3324455/Terminos-de-seguridad-informatica.html

González Manzano, L., & Fuentes García-Romero de Tejada, J. (2014). *Sistemas seguros de acceso y transmisión de datos*. IC Editorial. (1 Edición). Málaga. Consultado en:

http://ebookcentral.proquest.com/lib/bibsipansp/reader.action?docID=4184164

Hernández, L. E., Carreto, C., & Menchaca, R. (2012). *Modelo de seguridad para redes aplicado a dispositivos moviles*. *Risce*, 17-25.

Jara, H., & Pacheco F. *Ethical Hacking 2.0*. (2011) *Implementación de un Sistema para a Gestión de la Seguridad*. Fox Andina Editorial. Recuperado de: https://www.slideshare.net/WaldirNuezFrancia1/ethical-hacking-20-52184537?qid=bc40e482-ecdc-4dd9-a200-2dbda96661d3&v=&b=&from_search=1

Kaschel, H., & Alvarado,J. (Noviembre de 2014). *Criptografía de Curva Elíptica Aplicada a Seguridad para Redes WBAN bajo la Norma IEEE 802.15.6*. XV Congreso Internacional de Telecomunicaciones SENACITEL. Valdivia, Chile. Recuperado de: https://www.researchgate.net/publication/284174516_Criptografia_de_curva_elipticca_aplicada_a_seguridad_para_redes_WBAN_bajo_la_Norma_IEEE_802156

Lin Rivest, R., Shamir, A., & Adleman, L. (2013). A Method for obtaining digital signatures and Public-Key Cryptosystems. ACM, 14-67.

Marc Jean, R. (2004). Seguridad en la Informática de empresa. Riesgos, amenazas, prevención y soluciones. Barcelona: Ediciones ENI. recuperado de: https://books.google.com.pe/books?hl=es&lr=&id=K8XdRni4t94C&oi=fnd&pg=PA9&dq=seguridad+en+la+transferencia+de+archivos&ots=Ph6EnBWQiv&sig=YJrMtdSWwPrP94mW3fRY19O3PFY&redir_esc=y#v=onepage&q=seguridad%20en%20la%20transferencia%20de%20archivos&f=false

Medina Vargas, Y. & Miranda Mnedez, H. (2015). Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES. Revista Mundo Fesc. Volumen (9), 14-21. Recuperado de: https://doaj.org/article/88e5a0984a0440edb2e1477cbfacd569

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Mejia, R. (2014). Implementación de Protocolo SSL, TLS, SSH. San Salvador: Universidad Francisco Gavidia. Recuperado de: https://es.slideshare.net/abnerparada/protocolo-ssl-tls-y-ssh

Molina Morán, M., Mendoza Delgado, A., Melgar Flores, R. & López García, L. (2016). Aplicación de Algoritmos de Llave Pública para certificar la sobrevivencia de Pensionados en el extranjero del el Salvador. Revista de la Alta Tecnología y la Sociedad. Volumen (8), 1-9.

Montero Miguel, R. (2000). Administración de servicios de transferencia de archivos y contenidos multimedia. Ra-Ma Editorial. http://site.ebrary.com/lib/bibsipansp/reader.action?docID=11046103&ppg=14#

Padron Godínez, A., Prieto Meléndez, R., Herrera Becerra, A., & Calva Olmos, G. (2014). *Implementación de protocolos de comunicación seguros*. *SOMI*, 89-126.

Paguay Cuvi, M. (2015). Análisis De Algoritmos Matemáticos De Criptografía Pública Para Mejorar El Aprendizaje De La Materia De Criptografía En La Carrera De Ingeniería En Sistemas De La ESPOCH. Ecuador. Escuela Superior Politécnica De Chimborazo. Recuperado de: http://dspace.espoch.edu.ec/bitstream/123456789/4431/1/20T00643.pdf

Pousa, A. (2011). *Análisis de rendimiento de un algoritmo de criptografía. Instituto de Investigacion en Informatica LIDI*, 10.

Shazia Riaz, Shafia, Asma Sajid, & Madiha Kanwal. (2014). *Performance analysis of SSL/TLS* IJISET. *IJISET*, 2348-7968.

Stallings, W. (2008). *Fundamentos de seguridad en redes.* Madrid: Pearson.

System, C. (2014). *CCNA 5.02. EE.UU*: Pearson Education.

Tori C. (2008). *Hacking Etico.* Copyright. Argentina.

Trelles Araujo, P. (11 de Febrero de 2010). Seguridad Informática. Academia Latinoamericana de Seguridad Informatica - Microsoft TechNet. Recuperado de: https://www.slideshare.net/Tcherino/seguridad-informatica-3143924?qid=ad8a7ea0-8164-4e11-ab84-75887efd0ef0&v=&b=&from_search=3

Velasco Sánchez, P. (2015). *Analisis De Los Mecanismos De Encriptacion Para La Seguridad De La Informacion En Redes De Comunicaciones.* (Tesis de Maestría). Ecuador. Pontificia Universidad Católica del Ecuador. Recuperado de:

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

http://repositorio.puce.edu.ec/bitstream/handle/22000/11130/C.E.%20-%20U.T.Paola%20Velasco.pdf?sequence=1&isAllowed=y

Vera Parra, N.,López,D., & Manta Caro,H. (2014). Modelo test-bed de Simulación y Evaluación de criptografía de curva elíptica en redes IPv6 de próxima generación. Revista Tecnura. Volumen (18), 27-37. Recuperado de: https://doaj.org/article/1074e6d94bba4f01be56af5d37df0a54

Villegas Gómez, R. (2009). *Comparativa de seguridad de algoritmos de cifrado asimetrico.* Mexico D.F.: Instituto politécnico Nacional. Recuperado de: http://itzamna.bnct.ipn.mx:8080/bitstream/handle/123456789/8613/137.pdf?sequence=1&isAllowed=y

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

Anexos N° 1

Pruebas de la Técnica 1

Figura N° 1. Prueba Técnica 1

Figura N° 2. Prueba Técnica 1

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

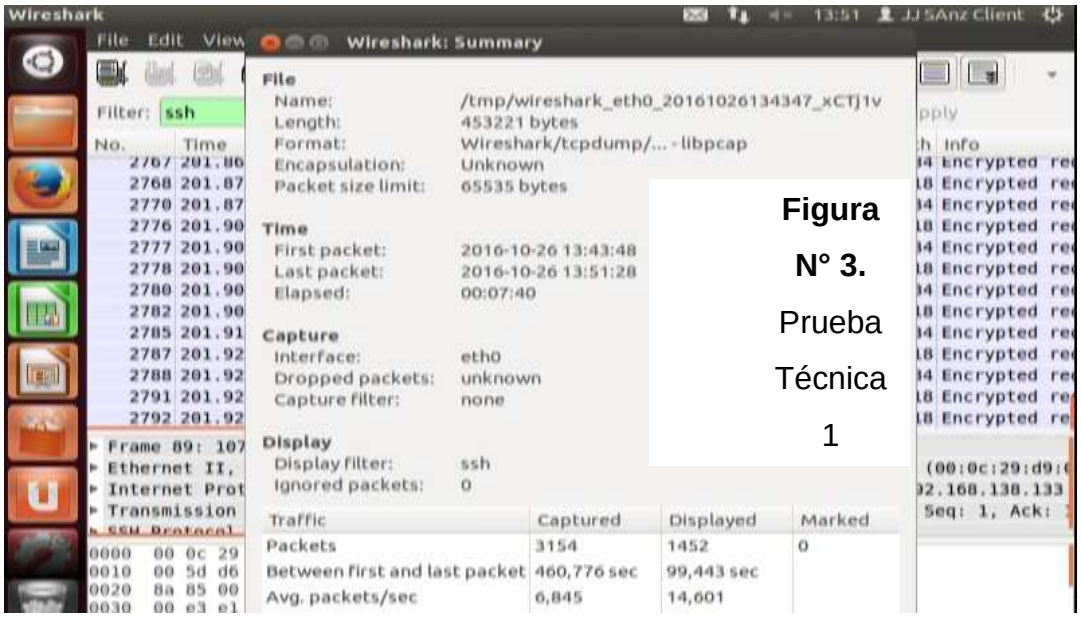


Figura N° 3. Prueba Técnica 1

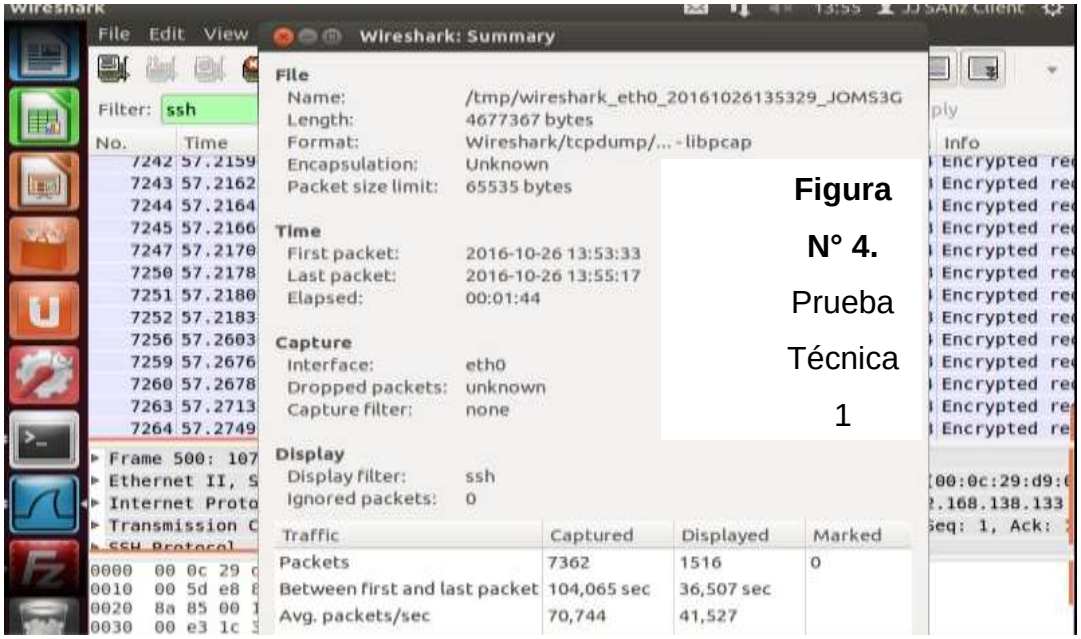


Figura N° 4. Prueba Técnica 1

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

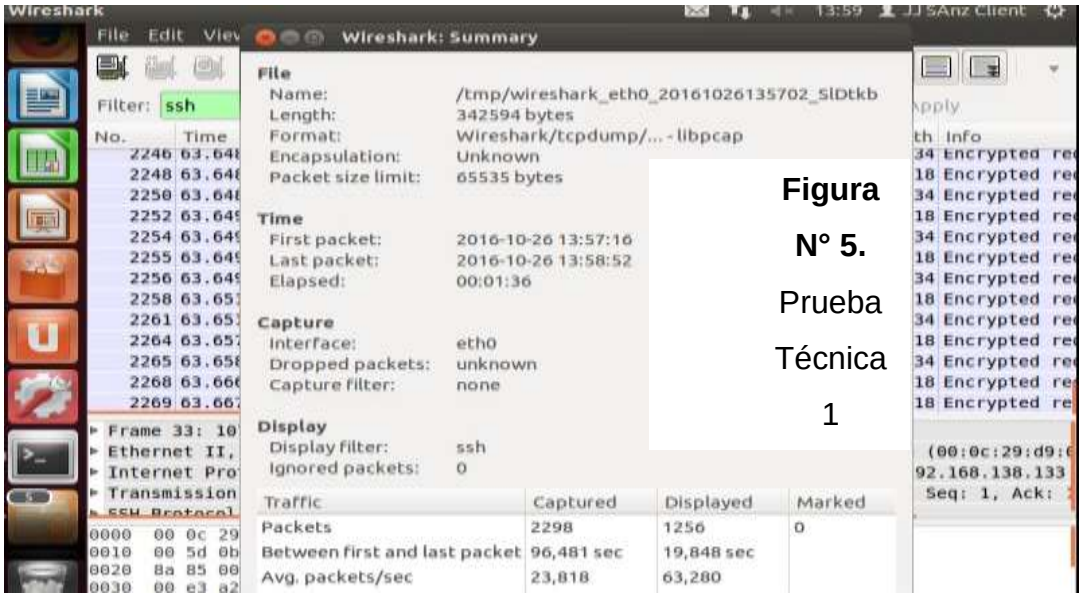


Figura N° 5. Prueba Técnica 1

Pruebas de la Técnica 2

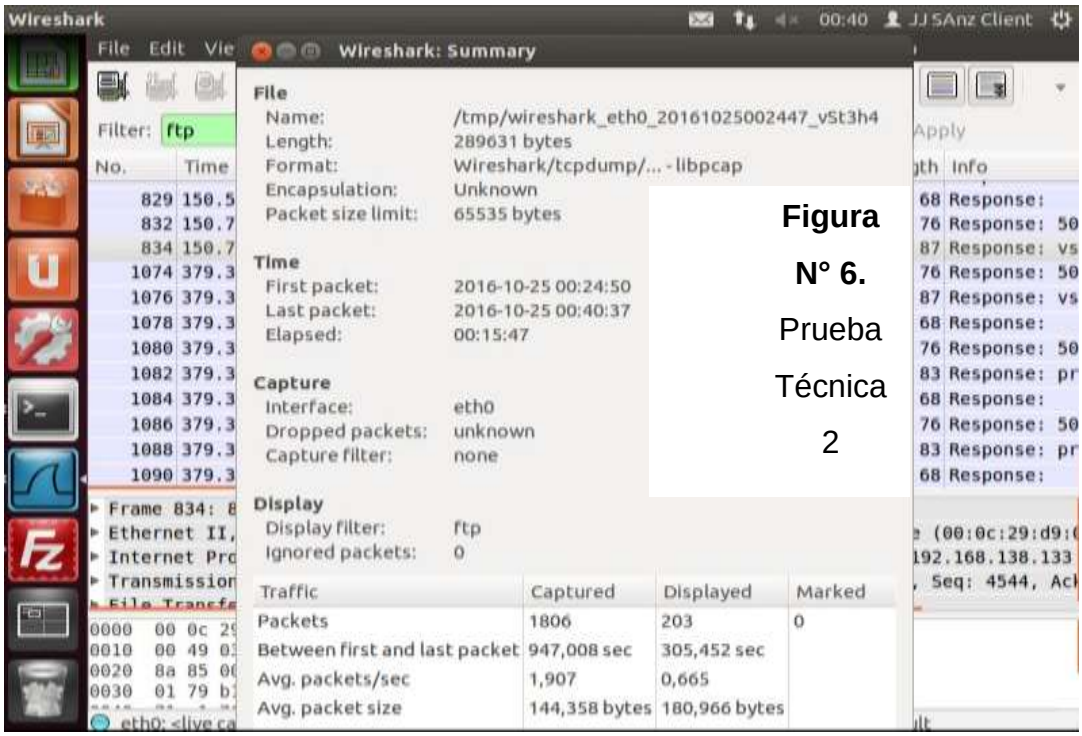


Figura N° 6. Prueba Técnica 2

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

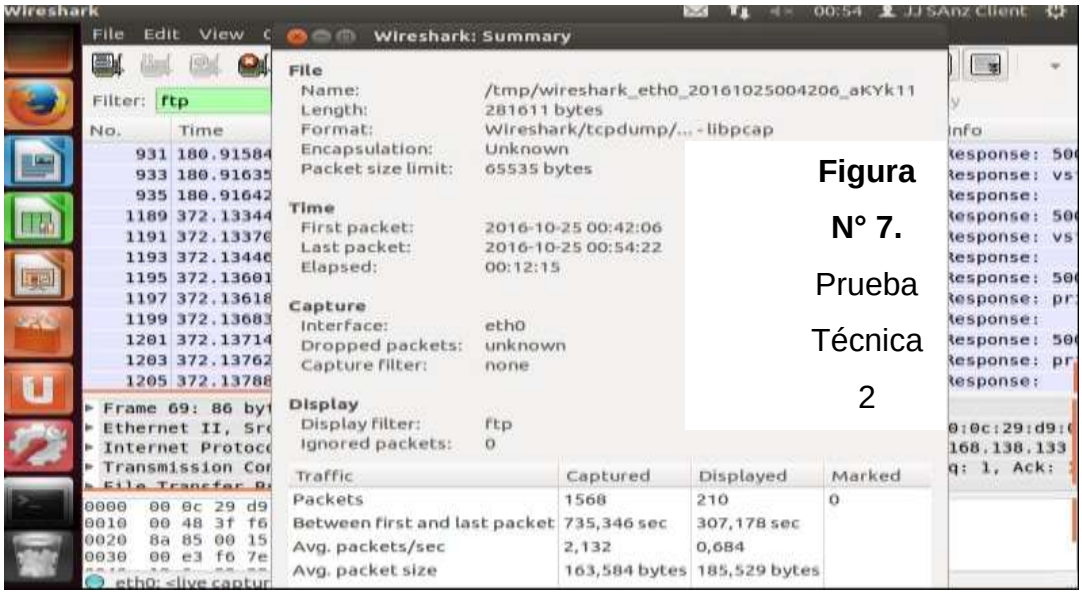


Figura N° 7. Prueba Técnica 2

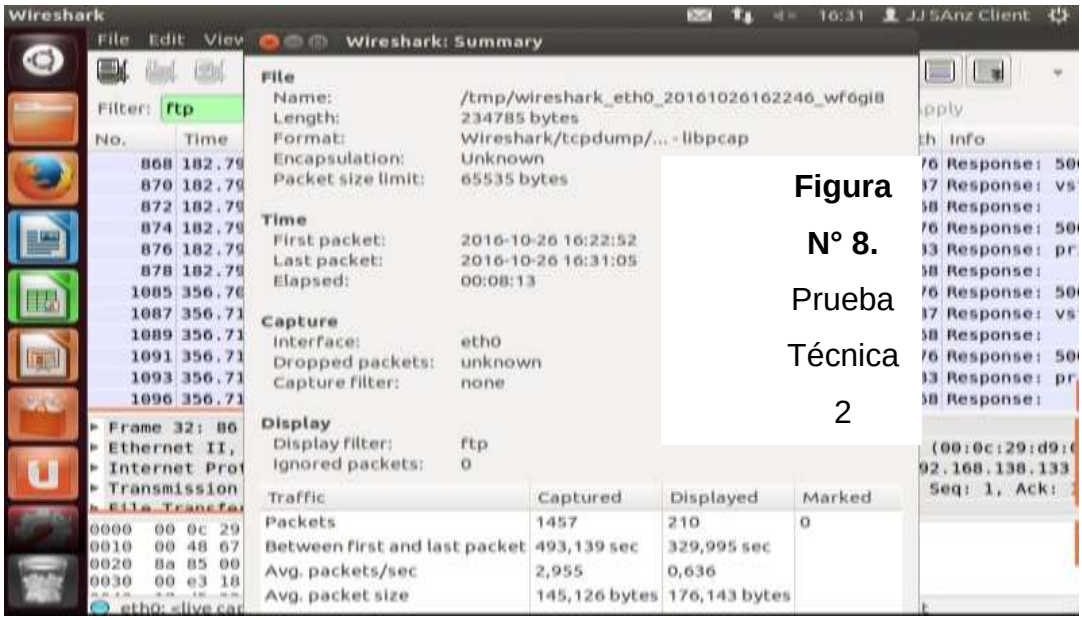


Figura N° 8. Prueba Técnica 2

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis

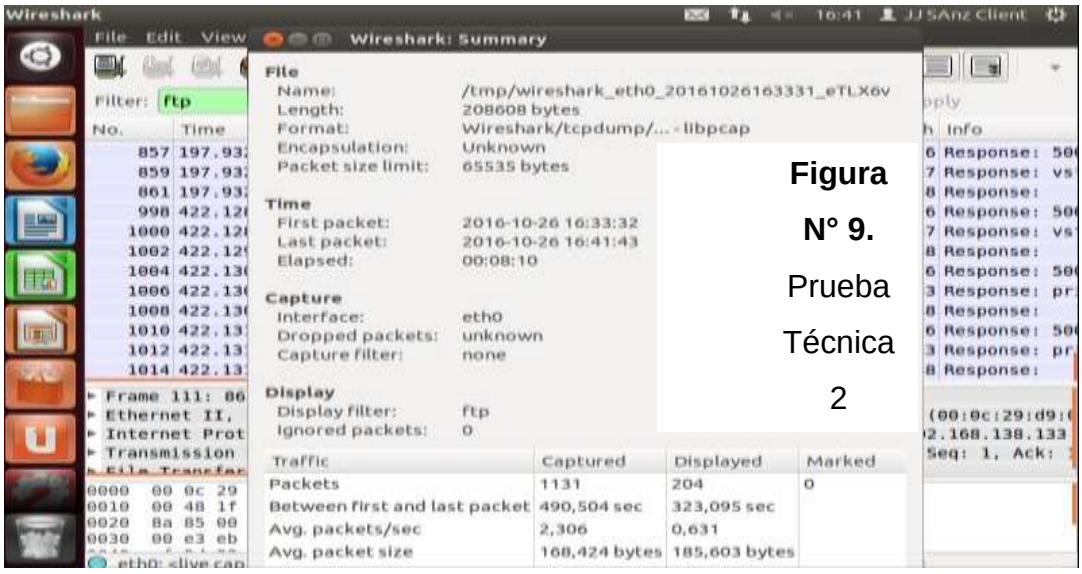


Figura N° 9. Prueba Técnica 2

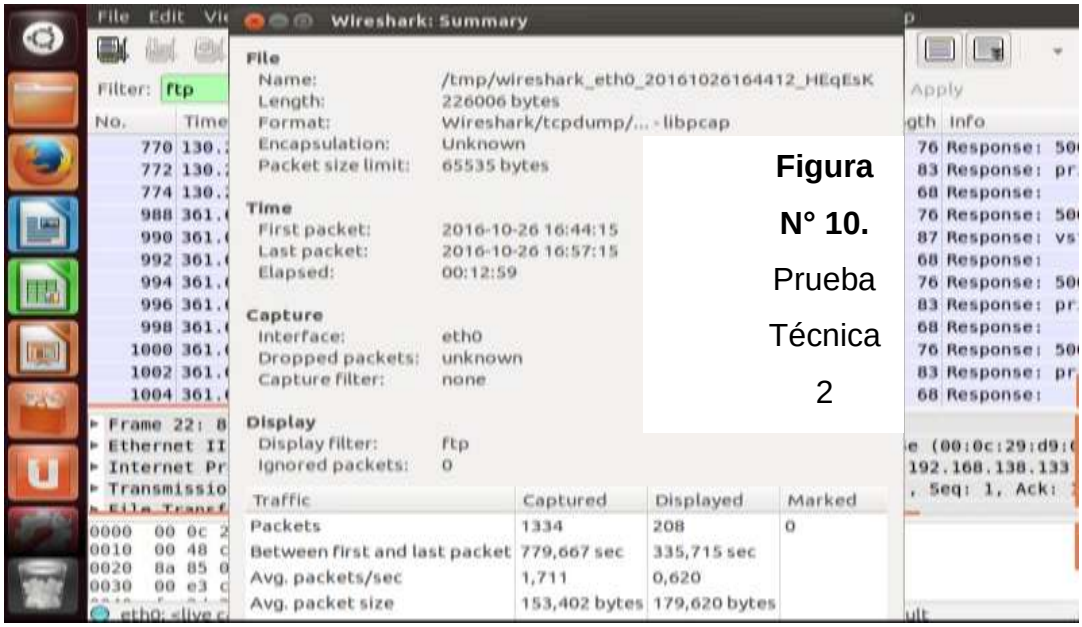


Figura N° 10. Prueba Técnica 2

Tesis publicada con autorización del autor
Algunos Derechos Reservados. No olvide citar esta tesis