ATAQUE APLICADO A MÁQUINAS VIRTUALES WINDOWS SERVER 2008 Y LINUX CENTOS EN ENTORNO CONTROLADO PARA DESARROLLO DE BUENAS PRÁCTICAS DE SEGURIDAD

JULIAN PATIÑO CASTRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

CEAD JOSÉ ACEVEDO Y GÓMEZ.

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTÁ

2018

ATAQUE APLICADO A MÁQUINAS VIRTUALES WINDOWS SERVER 2008 Y LINUX CENTOS EN ENTORNO CONTROLADO PARA DESARROLLO DE BUENAS PRÁCTICAS DE SEGURIDAD

JULIAN PATIÑO CASTRO

Proyecto para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMATICA

Director Temático

ING YOLIMA MERCADO

Director Metodológico

ING YOLIMA MERCADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

CEAD JOSÉ ACEVEDO Y GÓMEZ.

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTÁ

2018

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 02 de septiembre de 2017

DEDICATORIA

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre Mariela.

Por haberme dado la vida en primera instancia por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido convertirme en profesional, pero más que nada, por su amor.

A mi Familia

Por sus consejos y apoyo de manera directa o indirecta en algún punto de mi vida profesional que me ha ayudado a crecer como persona

AGRADECIMIENTOS

Quiero agradecer a todos mis Tutores, compañeros de especialización, compañeros de trabajo ya que de ellos he aprendido de muchas formas a valorar los estudios y a superarme cada día, también agradezco a mi madre porque siempre ha estado en los días más difíciles de mi vida como estudiante. Y agradezco a Dios por darme la oportunidad de escribir una historia en este mundo y mostrarme el camino a lograr mis metas planteadas las cuales darán fruto en el futuro y por ende me debo esforzar cada día para ser mejor como profesional y ser humano en general

CONTENIDO

pág.

LISTA DE FIGURAS

INTRODUCCION

Debido a la gran cantidad de vulnerabilidades a los cuales está expuesta la infraestructura informática hoy en día, junto con la integración y avance del internet de las cosas facilitando la vida de los usuarios en tareas comunes y rutinarias, no se ha logrado evaluar de manera adecuada el tema de seguridad en cuanto esto implica y cada vez más se abren brechas difíciles de tapar o solucionar ya que se integra a la labor diaria un sin número de elementos informáticos que funcionan sobre el protocolo ip y que son vulnerables a ser atacados, en este proyecto se realizara un proceso de escaneo e identificación de las principales vulnerabilidades en cuanto a servicios de infraestructura informática como FTP y HTTP, que en muchas ocasiones en la mediana empresa se enfoca al servicio pero se deja de lado la seguridad lo cual en la mayoría de los casos termina en un proceso de trabajo reactivo por parte de los profesionales de seguridad para solucionar incidentes que se hubieran podido prevenir si se hubiera trabajado de manera proactiva sobre los posibles eventos a ocurrir y de manera anticipada evitar la consecución de los mismos, para lo cual se hace necesario realizar un analizar a profundidad las graves falencias de seguridad de estos protocolos y pensar en realizar un fortalecimiento de la infraestructura teniendo en cuenta temas importantes como la evangelización de los usuarios de los sistemas en cuanto a buenas prácticas de la industria con el fin de evitar caer en técnicas de ingeniería social muy utilizadas hoy en día por los delincuentes informáticos.

1 PROBLEMA DE INVESTIGACION

¿Porque es importante la Seguridad?

La seguridad hoy en día es un tema que se traslada incluso a lo intangible con el aumento de los servicios que se ofrecen de tipo tecnológico la integración y el auge del internet de las cosas, la computación en la nube, el comercio electrónico todo esto generalizado en el proceso de globalización han trasladado el mundo entero a los sistemas de información, hoy en día casi todo está digitalizado y depende de las redes y la informática todo esto en pro de ser cada vez más eficientes y eficaces en la ejecución de tareas procesos de investigación elaboración de productos y prestación de servicios, las compañías se enfocan tanto en competir y en prestar un mejor servicio que dejan de lado aspectos fundamentales como la seguridad del entorno en el cual navega su propio negocio, realizando una analogía es como quien se preocupa por pintar arreglar modernizar su casa haciéndola espectacular pero olvida ponerle chapas a las puertas y rejas a las ventanas, la internet es un mundo que puede representar grandes oportunidades pero de igual forma grandes amenazas que deben ser afrontadas, el aumento de malware y personas que se dedican a delitos informáticos va en crecimiento ya que no en todos los sectores se le ha dado la importancia a la seguridad como lo merece, muchas personas pensaran en que este tipo de problemas los sufren únicamente las empresas que están comenzando que no cuentan con un capital o el conocimiento para aplicar normas a su infraestructura, pero esto está muy alejado de la realidad, ya que de este problema han sido víctimas incluso las grandes multinacionales como Coca cola con un caso muy citado en el 2009 en el cual hackers de origen chino suplantaron la cuenta de correo del CEO de la compañía y enviaron un comunicado al vicepresidente regional en china el cual era su objetivo, en el mail indicaban seguir un enlace para revisión de una información estratégica del negocio, pero por el contrario descargo malware de tipo keyloger con el cual lograron monitorear y extraer credenciales de varios sistemas del grande de las bebidas en su regional de

Asia comprometiendo la operación en dicho continente, y con el cual lograron volcar varios negocios que tenía el gigante estadounidense en el continente asiático.

1.1 Antecedentes Del Problema

El tema de Seguridad Informática cuenta con gran cantidad de información referente al tratamiento de esta problemática generalizada que crece día a día y que comenzó como un hobby por ganar privilegios por parte de personas con conocimientos informáticos avanzados debido a su curiosidad, pero con el paso del tiempo se involucraron diferentes fines de tipo lucrativo, político, económico, social que han llevado a observar este problema de manera determinante a nivel global ya que para ser víctima de un ataque ya no es necesario ser empresas que muevan grandes cantidades de dinero, sino que cualquier equipo conectado a internet puede ser vulnerable y propagar un ataque de manera distribuido, por esta razón una de las principales ramas de profundización de la ingeniería de sistemas es la seguridad Informática como eje principal del medio de gestión para mitigar este problema y evitar que los medios de información colapsen y sean afectadas las distintas economías mundiales, teniendo en cuenta que prácticamente toda la información hoy en día se mueve a través de internet.

Como se observa es un problema que afecta de manera global a todas las empresas que estén conectadas a la red, que hoy en día son casi la totalidad, de igual forma sus efectos devastadores pueden ir desde la fuga parcial de información hasta el cierre total de una compañía por lo cual se han creado distintas ramas de estudio de la Ingeniería de sistemas que profundizan especialmente en los efectos ocasionados a pequeña y gran escala por este tipo de problemática, dentro de las ramas de profundización se pueden encontrar, la seguridad informática a nivel de infraestructura, la seguridad de la información teniendo en cuenta a la información como activo más importante para la compañía, y la ciberseguridad que es un

concepto global de seguridad tanto Informatica como de la información que se mueven ya no solo a nivel de cada empresa si no que circule a través de internet, intensificando las formas de ataque y defensa que deben ser implementadas cuando no se tiene certeza absoluta de que recorrido tiene una fuente de información para llegar a su destino moviéndose a través de la red.

1.2 Planteamiento Del Problema

La seguridad hoy en día es un tema que se traslada incluso a lo intangible con el aumento de los servicios que se ofrecen de tipo tecnológico la integración y el auge del internet de las cosas, la computación en la nube, el comercio electrónico todo esto generalizado en el proceso de globalización han trasladado el mundo entero a los sistemas de información, hoy en día casi todo está digitalizado y depende de las redes y la informática todo esto en pro de ser cada vez más eficientes y eficaces en la ejecución de tareas procesos de investigación elaboración de productos y prestación de servicios, el enfoque tanto en competir y en prestar un mejor servicio que deja de lado aspectos fundamentales como la seguridad del entorno en el cual navega el negocio, la internet es un mundo que puede representar grandes oportunidades pero de igual forma grandes amenazas que se deben afrontar, el aumento de malware y personas que se dedican a delitos informáticos va en crecimiento ya que no en todos los sectores se le ha dado la importancia a la seguridad como lo merece, por tal razón se ha planteado revisar las falencias expuestas de protocolos como FTP y HTTP y las razones por las cuales se deben implementar protocolos seguros en el cual se evalúa desde un laboratorio controlado identificar una serie de vulnerabilidades básicas presentes en un entorno de red de forma común como son enumeración de puertos e identificación de servicios que funcionan bajo protocolos no seguros como lo son ftp y http, realizando una descripción de los errores más comunes que se cometen, como identificarlos y corregirlos con el fin de implementar buenas prácticas de seguridad que le permitan

a la empresa realizar un fortalecimiento de sistemas basados en las recomendaciones propuestas por el profesional de seguridad.

1.3 Formulacion Del Problema

La no implementación de medidas de seguridad en distintas capas es un factor común en las empresas pequeñas tipo pyme que debido a factores de múltiples tipos en particular temas de presupuesto ven la seguridad como un tema secundario en la empresa y deciden asumir el riesgo como parte normal del negocio sin tener en cuenta el impacto que genera una indisponibilidad de servicio prolongada. dada la necesidad de muchas empresas y en diferentes entornos de desplegar distintos tipos de aplicaciones que hacen parte de su Core de negocio debido a la masificación de servicios, comercio electrónico y en fin todos los temas relacionados con la globalización se enfocan en la funcionalidad y aplicabilidad de las mismas pero muchas veces dejan de lado todo los temas relacionados con seguridad lo cual es un gran fallo de cara a la estabilidad total de la empresa, ya que cuando sus aplicaciones se publican y son accedidas desde internet de igual forma son expuestos sus fallos a nivel de infraestructura en todas las capas que están detrás del web Service que está expuesto, dichos problemas la mayoría de los casos se evidencian después de un ataque que genera algún tipo de indisponibilidad en el servicio y solo en este momento se empieza a trabajar de manera correctiva sobre dicha falencia, lo cual va en contra de las buenas prácticas de la industria, en muchas ocasiones de igual forma se presentan ataques de ingeniería social en el cual personal no capacitado brinda acceso a personal no autorizado o entrega mucha más información de la que debería precisamente por no conocer de los riesgos a los que están expuestos, lo cual ha generado un gran problema que se presenta de manera recurrente en la mediana y pequeña empresa que no implementan normas y buenas prácticas de la industria que permitan gestionar de mejor manera el uso de sus activos informáticos, por estas razones en la pequeña

y mediana empresa se evidencia que la seguridad no es prioridad en el desarrollo normal del negocio, no se delega presupuesto a personal que se dedique a garantizar la integridad, disponibilidad y confidencialidad de la información, se acostumbra a trabajar de manera reactiva solo en el momento que el problema ocurre, la escusa principal de las empresas es la falta de presupuesto pero cuando el problema ocurre terminan invirtiendo mucho más para solucionarlo.

2 OBJETIVOS

2.1 Objetivo General

Identificar los principales fallos de seguridad de sistemas operativos Windows y Linux en referencia a servicios FTP y HTTP con el fin de generar sugerencias en cuanto a corrección de fallas encontradas con base en las mejores prácticas de la industria.

2.2 Objetivos Específicos

- Identificar las principales vulnerabilidades a las cuales está expuesto un sistema informático al usar protocolos no cifrados mediante un proceso de escaneo y numeración.
- corregir fallas encontradas en el proceso de escaneo mediante indicaciones de implementación de protocolos que ofrezcan cifrado
- documentar los puntos de mejora sugeridos en este proyecto para implementación futura, de igual forma para procesos de auditoría.

3 JUSTIFICACIÓN

Este trabajo se realiza basado en la identificación de un problema generalizado al cual está expuesto cualquier infraestructura tecnológica “NO IMPLEMENTAR SEGURIDAD “como se ha evidenciado puede generar incluso el cierre total de una empresa ante la falta de implementación de medidas de seguridad, teniendo en cuenta que debido al proceso de globalización es un problema que afecta a cualquier empresa conectada a la red sin importar su Core de negocio. Basado en cantidad de incidentes reportados en medios digitales y escritos se toma la decisión de presentar el desarrollo de un proyecto enfocado al fortalecimiento general de la seguridad que puede ser aplicado en cualquier entorno en el cual se use infraestructura tecnológica, por medio de un ejercicio práctico en el cual se plantea dar solución a una problemática generalizada en empresas pequeñas y medianas que no implementan buenas prácticas de seguridad en el despliegue de sus servicios en internet ya que aplican su enfoque mayormente en la funcionalidad dejando de lado la seguridad lo cual se evidencia es una de las grandes causas de fallos de seguridad en nuestra problemática actual, por lo cual este trabajo servirá como guía de implementación de buenas prácticas de fortalecimiento y seguridad de sistemas y de igual forma como manual de capacitación de usuarios en cuanto a formas de ataque usadas para vulnerarlos con técnicas de ingeniería social, teniendo en cuenta esta problemática y plenamente identificada la causa se pretende enumerar las principales falencias en las cuales se incurre de manera generalizada, atacar el problema y con base en dichas pruebas, implementar buenas prácticas y documentarlas, esto permite generar conciencia a nivel empresarial y determinar que no se necesitan grandes presupuestos para implementar este tipo de soluciones, existe gran cantidad de soluciones de software libre para llevar a cabo este proyecto, lo cual implica esfuerzo en cuanto a conocimiento y estudio pero no grandes inversiones de dinero que finalmente se ve reflejado en un proceso de crecimiento personal y profesional para quien lo implementa y es una forma de contribuir a la sociedad devolviendo un poco de todo

lo que se ha aprendido ante personas altruistas que aportan su conocimiento para el mejoramiento de un problema o la satisfacción de una necesidad.

Se han implementado grandes soluciones que ayudan a mitigar este tipo de inconvenientes por lo cual el desarrollo de este proyecto se forma como una base estructural de implementación de buenas prácticas que cualquier empresa con bajo presupuesto debería implementar como medidas básicas de seguridad lo cual garantiza minimizar el impacto negativo que una indisponibilidad de servicio o fuga de información crearía en la confiabilidad de su negocio por lo cual este trabajo expondrá en detalle falencias y correcciones a implementar en un proceso de fortalecimiento de sistemas.

Para conocer a profundidad las falencias de estos protocolos que no implementan cifrado se realiza un proceso de evaluación inicial de los sistemas informáticos para identificar los riesgos y posibles amenazas que pueden explotar una vulnerabilidad ocasionando con esto indisponibilidad de los servicios, contando con esta información se realizara un pentesting controlado el cual permitirá determinar hasta qué punto puede alcanzar un atacante al ingresar a un sistema valiéndose de la explotación de una o varias vulnerabilidades encontradas en tareas de escaneo, enumeración, escalacion de privilegios y acceso a la data, todo esto con el fin de enumerar las falencias encontradas y realizar sugerencias de como parchar el sistema y corregir de esta forma los problemas encontrados, esto no garantizara una seguridad absoluta ya que no existe, pero minimizara el riesgo en cuanto a medidas estándar, de igual forma se generara una evangelización básica en cuanto a tips para no caer en ataques de ingeniería social, ya que hoy en día no es suficiente salvaguardar los activos informáticos de tipo físico y lógico cuando los atacantes se enfocan en acceder usando de por medio al eslabón más débil de la cadena **“los usuarios de los sistemas “.**Finalmente con los hallazgos encontrados, se propondrán las soluciones planteadas a estos hallazgos desde la perspectiva del profesional de la seguridad y apoyado en la documentación referenciada en buenas prácticas de la industria para que la persona o empresa que

revise el documento pueda entender de manera generalizada el contexto del problema y pueda generar un plan de diseño e implementación de acuerdo a su infraestructura, se describirá de manera muy gráfica todo el entorno de pruebas realizadas usando máquinas virtuales en un ambiente controlado por el profesional de la seguridad.

La no implementación de este tipo de proyectos a nivel global generara repercusiones nefastas en los sistemas informáticos que cada vez serán vulnerables a una mayor cantidad de ataques que comprometerán cada vez en mayor nivel una infraestructura tecnológica, y la falta de personal capacitado para hacer frente a este tipo de incidencias ocasionara el fin de muchas empresas que tienen expuesto su Core de negocio en la internet.

4 MARCO DE REFERENCIA

El tema de Seguridad Informática cuenta con gran cantidad de información referente al tratamiento de esta problemática generalizada que crece día a día y que comenzó como un hobby por ganar privilegios de personas con conocimientos informáticos avanzados debido a su curiosidad, pero con el paso del tiempo se involucraron diferentes fines de tipo lucrativo, político, económico, social que han llevado a observar este problema de manera determinante a nivel global ya que para ser víctima de un ataque ya no es necesario ser empresas que muevan grandes cantidades de dinero, sino que cualquier equipo conectado a internet puede ser vulnerable y propagar un ataque de manera distribuida, por esta razón una de las principales ramas de profundización de la ingeniería de sistemas es la seguridad Informatica como eje principal del medio de gestión para mitigar este problema y evitar que los medios de información colapsen y sean afectadas las distintas economías mundiales, teniendo en cuenta que prácticamente toda la información hoy en día se mueve a través de internet.

4.1 MARCO TEORICO

Basado en un artículo científico publicado por el Instituto de ciberseguridad de España [1] que comprende una serie de ataques a protocolos no seguros mediante un analizador de protocolos como Wireshark se determinan los pasos necesarios para implementar ataques usando este analizador de protocolos y capturar información que circule en la red que no implemente cifrado en los protocolos de transmisión, se debe identificar en primera instancia el alcance que debe tener el objetivo esto se realiza mediante un análisis de vulnerabilidades a las cuales puede estar expuesta la infraestructura y de que forma un atacante podría explotarlas para generar una indisponibilidad en un servicio o un robo de información, las cuales son las principales causas por las cuales se genera un ataque, teniendo claro esto y basado en investigaciones realizadas por reconocidas firmas de seguridad

informática en sus artículos y publicaciones como beyondsecurity.com es necesario realizar un estudio a profundidad de todo el proceso de comunicación existente en el modelo OSI o el stack de protocolos de TCP/IP ya que de su entendimiento se pueden segregar e identificar de manera más amplia los distintos ataques en cada una de las capas desde la física hasta la capa de aplicación y permite identificar de forma clara en qué fase es más vulnerable la infraestructura, según estudios publicados por reconocidas revistas informáticas con reconocimiento científico como [2] http://recibe.cucei.udg.mx es claro además tener en cuenta que los usuarios de los sistemas entran a ser parte de esta cadena por lo cual también son vulnerables a ser hackeados, y según estadísticas ante el nacimiento de una técnica que se dedida a vulnerar directamente a los usuarios conocida como ingeniería social se han logrado perpetrar grandes ataques sin necesidad de vulnerar la infraestructura mediante ataques de fuerza bruta, por esta razón muchos temas deben ser tenidos en cuenta para atacar esta problemática como se analiza de manera científica en artículos desarrollados por la universidad tecnológica de Pereira [3] http://repositorio.utp.edu.co y por esta razón para atacar un problema grande en muchas ocasiones es más eficiente segmentarlo en problemas más pequeños que se puedan medir , evaluar su impacto probabilidad de ocurrencia y de esta forma determinar el modelo de acción a seguir para prevenirlo o mitigarlo en caso de ocurrir.

4.2 MARCO CONCEPTUAL

Para la realización de un análisis de vulnerabilidades, en primera instancia se debe entender que es una vulnerabilidad.

[4] Vulnerabilidad: Una vulnerabilidad es un defecto o debilidad que se puede llegar a presentar en el diseño, implementación, operación o administración de un sistema que podría ser explotado en determinada situación para comprometer los objetivos de seguridad del sistema.

Conforme a ésta definición, se evidencia que una vulnerabilidad se puede encontrar en múltiples escenarios del ciclo de vida de una aplicación, esto se puede llegar a convertir en un riesgo que tiene una probabilidad realmente alta de Materializarse al no tomar las medidas necesarias para mitigarlo en el momento adecuado.

Ya teniendo claro el concepto de vulnerabilidad, luego de que se han hecho evidentes en un sistema informático, lo siguiente que se debe analizar serán las amenazas.

[5] Amenaza: Una amenaza es cualquier cosa, situación, elemento o individuo, un atacante externo, un usuario interno, una inestabilidad del sistema, entre algunas que cabe mencionar que pueden generar daño en el normal funcionamiento de una infraestructura o aplicación dentro de los más críticos podríamos resaltar recursos de valor, tales como los datos en una base de datos o en el sistema de archivos) mediante la explotación de una vulnerabilidad.

Con esto se entiende que las amenazas serán las encargadas de explotar las vulnerabilidades que tiene el sistema informático y directamente esto se convierte en el elemento u factor que ejecuta la acción que ocasiona el daño sobre el sistema.

Para poder identificar las vulnerabilidades, se deben ejecutar una serie de pruebas que permitan descubrirlas. Por lo cual lo siguiente a identificar es que es una prueba?

[6] Prueba: Una prueba es la ejecución de una acción para demostrar que una aplicación cumple con los requisitos de seguridad establecidos dentro de sus parámetros de funcionamiento normal.

Las pruebas que se ejecuten serán las encargadas de la demostración de la existencia o no de una vulnerabilidad en un sistema informático. Por tal razón la importancia en la elección de los tipos de pruebas que deben ser ejecutadas y que cantidad de las mismas se van a realizar, ya que esto generara influencia directa en el resultado final y en consecuencia permitirá evitar que las amenazas exploten algún tipo de vulnerabilidad.

En la actualidad existe una distribución de Linux llamada Kali que centraliza una cantidad importante de herramientas enfocadas al pentesting y la seguridad informática segmentadas en grupos lo que facilita su entendimiento y aplicación. Ahora se determinara en qué consiste una prueba de pentesting.

[7] Pentesting: Una prueba de pentesting es un método de evaluación de la seguridad de un sistema informático o red, en el cual se valida y se verifica de manera metódica la eficacia de los controles de seguridad de la aplicación. Una prueba de pentesting de aplicaciones web se centra sólo en la evaluación de la seguridad de una aplicación web. Dicho proceso consiste en realizar un análisis activo de la aplicación de las vulnerabilidades, fallas técnicas, o de diseño. Por norma de buenas prácticas dichos hallazgos o evidencias se presentaran al área encargada del elemento o servicio, junto con una evaluación del impacto, una propuesta de mitigación o una solución técnica.

Se pueden clasificar las pruebas de penetración como de caja blanca o de caja negra. Las pruebas de caja blanca se realizan con el consentimiento y apoyo de la empresa involucrada a la cual se suministra acceso directo a la red y en ocasiones ciertas credenciales para evaluar a fondo la estabilidad de los componentes que hacen parte correlacionada del negocio, en contra parte las pruebas de caja negra no se cuenta con acceso concedido por la empresa por lo cual se deben generar toda una serie de análisis sobre levantamiento de información para poder escanear

detectar fallos explotarlos y de esta manera ir ganando acceso para escalar privilegios dentro del sistema a evaluar.

Finalmente se determinara que es hardering.

[8] Hardering: El hardering o fortalecimiento puede entenderse como una “técnica basada en un conjunto de actividades llevadas a cabo por el administrador de un Sistema operativo para reforzar al máximo posible la seguridad de éste por tal razón se hace preciso identificar las ventajas de un sistema operativo y que el mismo sea Capaz de soportar y administrar de manera adecuada los recursos de memoria y procesos por medio del hardering mejorando la seguridad del mismo.

5 DISENO METODOLÓGICO

5.1 TIPO DE INVESTIGACION

El presente proyecto implementara una metodología de investigación aplicada de tipo tecnológico basado en un caso práctico de implementación de un laboratorio de máquinas virtuales en un entorno controlado en el cual el profesional de seguridad implementara una serie de medidas para evaluar el sistema actual del entorno con el cual se desarrolló la práctica de laboratorio consistente en instalar y publicar servicios de uso común en cualquier empresa pero que no cuentan con las medidas sugeridas de seguridad según marcos de trabajo o frameworks de buenas prácticas como iso 27000, ITIL entre otras, por tal razón el profesional de seguridad basado en su experiencia en sistemas realizara una serie de prácticas documentadas basado en documentación guía pero no usando un modelo especifico o trabajo como marco de referencia, con el fin de generar nuevo conocimiento o comprobar hipótesis acerca de la inestabilidad que puede llegar a presentar un sistema informático en cuanto al nivel de riesgo que puede terminar en una indisponibilidad de servicio debido a la no implementación de seguridad en el despliegue de servicios tecnológicos.

5.2 Método De Investigación

Para el desarrollo de este proyecto se usara el método Analítico Sintético que de acuerdo a concepto se podría definir como estudiar un fenómeno descomponiéndolo en sus partes para examinarlas por separado y de nuevo integrarlas para lograr un concepto general, por tal razón hablar de seguridad en términos generales implica descomponer el concepto en fracciones más específicas identificar sus variables y establecer una correlación entre las mismas para volverlas a integrar y de esta manera explicarlo como un todo de manera más general, por tal razón Se usara un ambiente de máquinas virtuales en las cuales no se implementaran las medidas de seguridad estándar que la mayoría de los casos emplean las grandes corporaciones y se correrán una serie de procedimientos y el uso de algunas utilidades de pentesting basados en software libre para degradar la seguridad de las máquinas virtuales y comprometerlas esto con el fin de ganar acceso a las mismas para acceder a sus servicios FTP y HTTP y evidenciar falencias que deben ser corregidas, se recrearan casos ficticios de ingeniería social los cuales también son métodos bastante usados por los atacantes para segmentar el alcance de sus objetivos e identificar quien o quienes podrían colaborar directa o indirectamente en sus procesos de acceso a un sistema y finalmente se sugerirán correcciones de las vulnerabilidades encontradas para su despliegue acompañado de una serie de buenas prácticas en cuanto a capacitaciones de usuarios para evitar ser víctimas de ataques de ingeniería social, de esta forma identificar la ausencia de seguridad y sus consecuencias permitirá identificar de manera más fácil a que hace referencia el concepto de seguridad en sistemas informáticos.

5.3 Fuentes Y Técnicas De Recolección De Información

Las técnicas de recolección de información para este caso son las siguientes:

Observación, recopilación documental son la base de este proyecto Ya que por medio de la observación se identifica el problema base y la necesidad a satisfacer que en este caso es la implementación de medidas de seguridad y el fortalecimiento de los sistemas, por medio de la recopilación documental se identifican temáticas que el profesional de seguridad usara como modelo base para realizar sus pruebas e identificar sus propias hipótesis basadas en los resultados obtenidos, lo cual será documentado en el desarrollo del proyecto para entregar como producto final una serie de hallazgos y recomendaciones a implementar basados en los resultados obtenidos.

5.4 Delimitación Y Alcance

Se realiza un proceso de evaluación inicial de los sistemas informáticos para identificar los riesgos y posibles amenazas que pueden explotar una vulnerabilidad ocasionando con esto indisponibilidad de los servicios, contando con esta información se programara un plan de pentesting controlado el cual atacara dos servicios básicos expuestos con antelación bajo protocolos no seguros como FTP y HTTP para determinar hasta qué punto puede alcanzar un atacante ingresar a un sistema valiéndose de la explotación de una o varias vulnerabilidades encontradas en tareas de escaneo, enumeración, escalacion de Privilegios y acceso a la data, todo esto con el fin de enumerar las falencias encontradas y dar sugerencia de las distintas formas de corregir el problema, esto no garantizara una seguridad absoluta ya que no existe, pero minimizara el riesgo en cuanto a medidas estándar, de igual forma se generara una evangelización básica en cuanto a tips para no caer en ataques de ingeniería social, ya que hoy en día no es suficiente salvaguardar nuestros activos informáticos de tipo físico y lógico cuando los atacantes se enfocan

en acceder usando de por medio al eslabón más débil de la cadena **“los usuarios de los sistemas “.**Finalmente basado en los hallazgos encontrados, se plantearan las soluciones a estos hallazgos desde la perspectiva del profesional de la seguridad y apoyado en la documentación referenciada en buenas prácticas de la industria para que la persona o empresa que revise el documento pueda entender de manera generalizada el contexto del problema y pueda plantear un plan de diseño e implementación de acuerdo a su infraestructura, se describirá de manera muy gráfica todo el entorno de pruebas realizadas usando máquinas virtuales en un ambiente controlado por el profesional de la seguridad.

Este proyecto en su fase de planeación, ejecución y entrega de resultados se ha estructurado según cronograma para realizar entrega en un plazo de 16 semanas tiempo durante el cual dura el semestre planteado para el desarrollo de la asignatura proyecto de grado II, con el fin de determinar las fases tiempos establecidos, avances, entregables, retroalimentación por parte del director de curso, seguimiento y finalmente entrega del proyecto para evaluación final, durante el tiempo estipulado para las tres fases de desarrollo de este proyecto se contemplan variaciones en los tiempos de ejecución de cada una de las fases de acuerdo a las recomendaciones dadas por el director de curso, esto con el fin de poder establecer la ejecución de los objetivos siguiendo la normatividad estipulada por la universidad con el fin de realizar la entrega de un proyecto que cumpla con las metas planteadas y en las cuales plasme el conocimiento adquirido por el profesional de seguridad a lo largo del desarrollo de su carrera de posgrado.

El proyecto se segmenta en tres fases la etapa de planeación en la cual se diseña el plan de pruebas y cronograma a ejecutar, la fase de ejecución que contemplara la instalación de las máquinas virtuales despliegue de servicios ftp y http en sistemas operativos Windows server y Linux las cuales denominaremos víctimas y una tercera instancia Kali Linux denominada atacante que llevara a cabo un proceso de escaneo identificación de servicios y vulneración de los mismos, acompañado de la sugerencia de implementación de buenas prácticas de seguridad para

garantizar la mitigación del riesgo expuesto teniendo en cuenta de que el riesgo es una variable que siempre existirá y nunca se podrá reducir a un 0% por lo cual la idea es sugerir un plan de mejora continua que contemple auditorias para reducir el riesgo de los mismos, y finalmente la fase de entrega de resultados en los cuales se expondrá al director del curso los hallazgos y sugerencias de corrección e implementación de buenas prácticas por el profesional de seguridad para que sean evaluados por parte de la universidad.

6 PRODUCTO RESULTADO A ENTREGAR

Por medio del presente proyecto se entregara un documento para la implementación de buenas prácticas de seguridad el cual resaltara las principales falencias a las cuales se ve expuesto un servicio o recurso en un entorno de red y de igual forma como atacar este problema y prevenirlo de manera proactiva para que la probabilidad de que ocurra un incidente referenciado a esto se minimice en probabilidad, de igual forma una serie de recomendaciones a forma de capacitación a usuarios finales en cuanto a prevenir ataques de ingeniería social que permitan acceder a sistemas de información sin vulnerar la tecnología, dicho documento a entregar sirve de marco de referencia e implementación en infraestructuras tecnológicas que cuente con sistemas operativos Windows y Linux de similares características a las utilizadas en el ambiente virtualizado.

7. RECURSOS NECESARIOS PARA EL DESARROLLO

Para este tipo de actividad se tiene estimado el uso de un equipo base con características de procesador Core i5, 16 gb de memoria RAM necesarias para poder desplegar 3 máquinas virtuales una atacante y dos víctimas y lograr que las pruebas se ejecuten sin problemas de rendimiento de la maquina base, una conexión a internet de banda ancha con pago mensual, y una dedicación al proyecto en cuanto a recolección de información, determinación del alcance, diseño, implementación de máquinas virtuales ejecución de pruebas, entrega de resultados y proceso de evaluación en un tiempo dedicado de 19 horas distribuidas en los tres meses de la duración del proyecto a lo cual se emplearan recursos personales para la ejecución del proyecto pero que se estima un costo aproximado en cuanto a los activos utilizados en la actividad que se aproximan al monto identificado en la siguiente tabla :

ELEMENTO	COSTO
Equipo host para virtualización	2.500.000
Conexión internet banda ancha 3 meses	240.000
Horas dedicadas profesional de seguridad	950.000
TOTAL	3.690.000

Figura 1 Cronograma De Actividades

8. CRONOGRAMA DE ACTIVIDADES																
ACTIVIDAD	**Semana 1 Agosto**	**Semana 2 Agosto**	**Semana 3 Septiembre**	**Semana 4 Septiembre**	**Semana 5 Septiembre**	**Semana 6 Septiembre**	**Semana 7 Octubre**	**Semana 8 Octubre**	**Semana 9 Octubre**	**Semana 10 Octubre**	**Semana 11 Noviembre**	**Semana 12 Noviembre**	**Semana 13 Noviembre**	**Semana 14 Noviembre**	**Semana 15 Diciembre**	**Semana 16 Diciembre**
Análisis de la problemática	x	x														
documentación			x	x												
Determinación del alcance					x	x										
Despliegue de las máquinas virtuales							x	x								
Pruebas de penetración									x	x						
Evaluación de resultados											x	x				
sugerencia de medidas correctivas													x	x		
Entrega de informe final															x	x

9. PLANEACIONDEL PROYECTO

9.1 Análisis De La Problemática

La causa raíz del problema se deriva en que algunas empresas no dan importancia relevante al tema de seguridad en el entono de su negocio por lo cual se realizara un proceso de hardering o fortalecimiento de sistemas operativos virtualizados Windows y Linux en los cuales se utilizaran máquinas virtuales desplegadas sobre el software de virtualización Virtual box de Oracle para instalar una versión de evaluación de 180 días de Windows 2008 server R2 en el cual se publicara un servicio ftp usado en las empresas como servidor de archivos de manera interna, de igual forma se instalara una segunda instancia de Linux Centos 7 y se publicara un servicio web interno por http por el puerto 80, se instalara una tercera máquina virtual atacante, con la distribución Kali 2017.1 usada para pentesting, la cual cuenta con un número suficiente de herramientas para realizar el proceso de escaneo identificación y ataque de los servicios expuestos en la práctica esto con el fin de mostrar graves errores de seguridad que se presentan en una infraestructura empresarial común enfocado a los protocolos FTP y HTTP, trasladado a un ambiente controlado de máquinas virtuales para mostrar de manera práctica las medidas tomadas por el profesional de seguridad en este caso, el estudiante de Especialización de la UNAD para identificar los escenarios en los cuales un ataque puede ser llevado a cabo desde sus fases de reconocimiento del objetivo, hasta la implementación del ataque para distintos fines.

9.2 Documentación

Como se ha identificado en el punto número 7 en los recursos necesarios para la implementación del laboratorio se cuenta con un equipo físico propiedad del profesional de seguridad informática, que cuenta con las siguientes características:

Procesador CoreI5 de 4 núcleos

16 gb de memoria RAM

Disco duro de 1 terabyte

Tarjeta aceleradora de video de 2gb

Sistema operativo básico instalado Windows 7 profesional edition

Software de virtualización Virtualbox

Imágenes Iso para despliegue de máquinas virtuales:

Windows server 2008 R2

Linux Centos 7

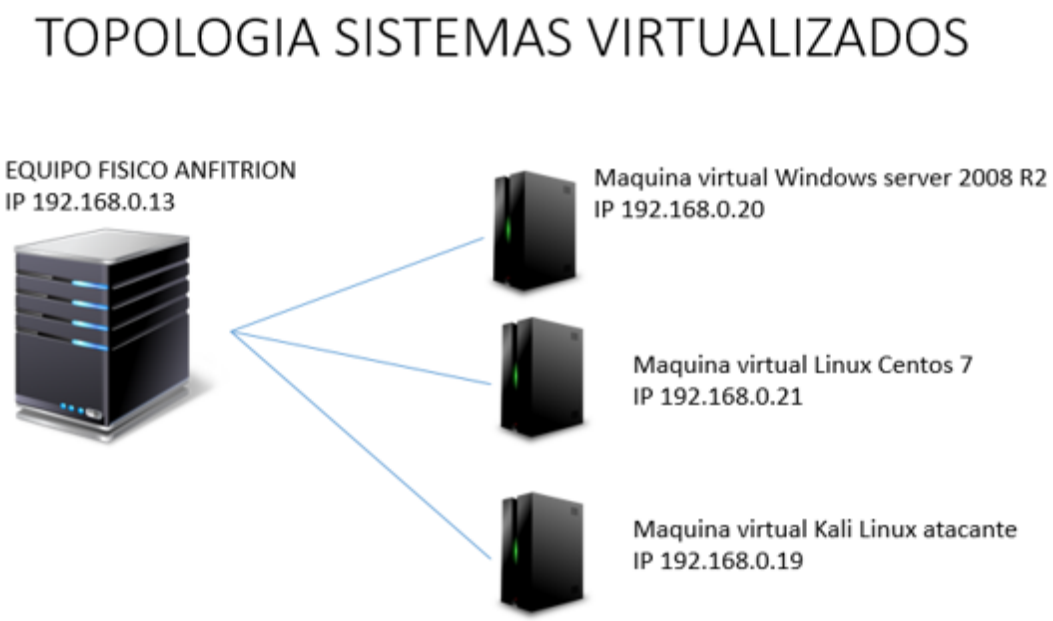
Kali Linux

Con estos recursos relacionados se procederá al despliegue de los objetivos planteados en este proyecto los cuales basan en la experiencia y estudios adquiridos a lo largo de su carrera por parte del profesional en seguridad el cual se encargara de determinar el alcance diseñar el plan de pruebas, ejecutar el ataque, y posteriormente analizar los resultados para sugerir implementación de correcciones a dichos sistemas, con el fin de implementar dichas medidas identificadas como un plan de mejora continua en pro de la seguridad de la infraestructura física y aplicaciones usadas para este laboratorio.

10. DESPLIEGUE DE MAQUINAS VIRTUALES

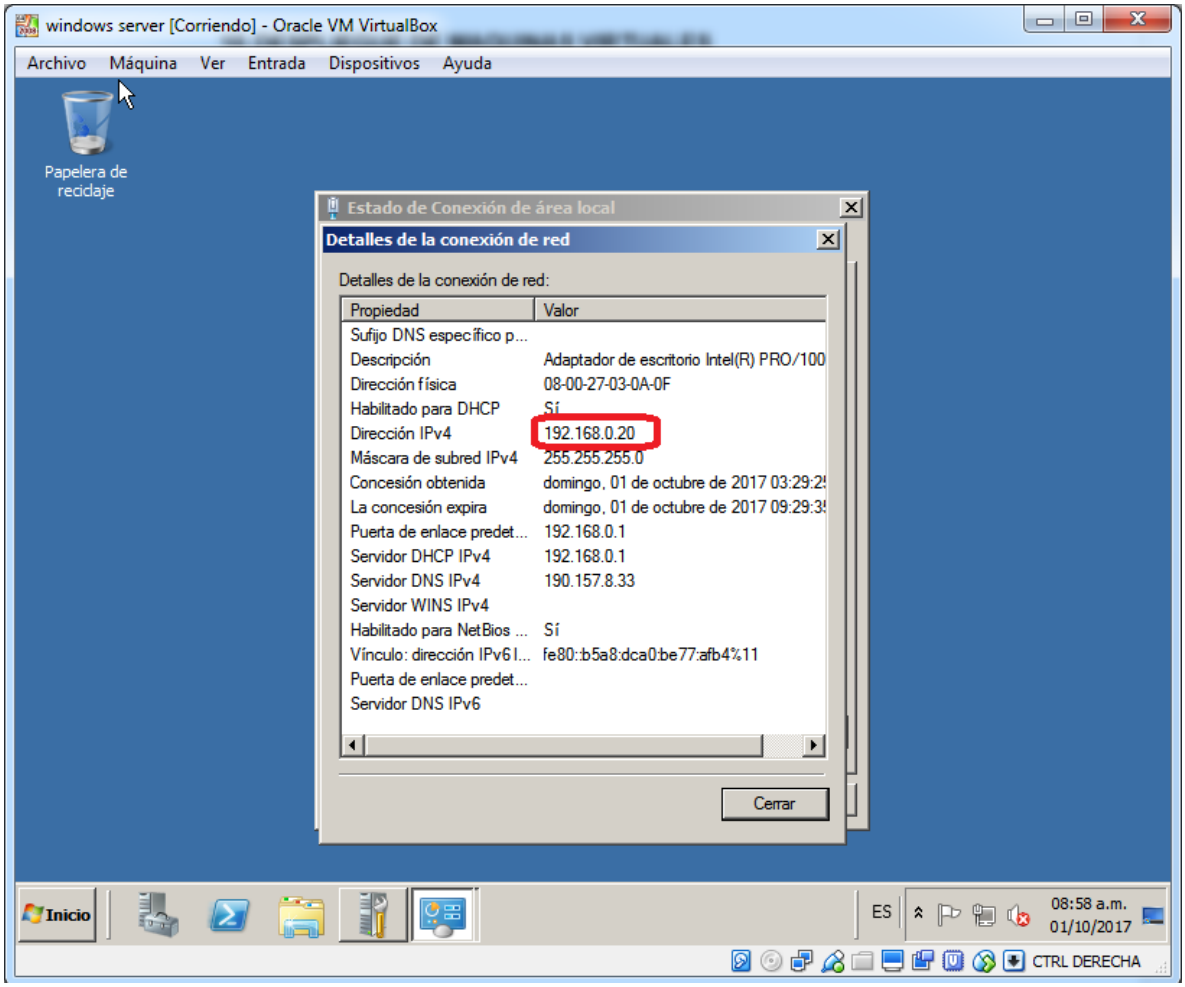
Para este proyecto se usaran los siguientes sistemas operativos virtualizados de acuerdo al siguiente mapa topológico.

Figura 2 Topología sistemas virtualizados



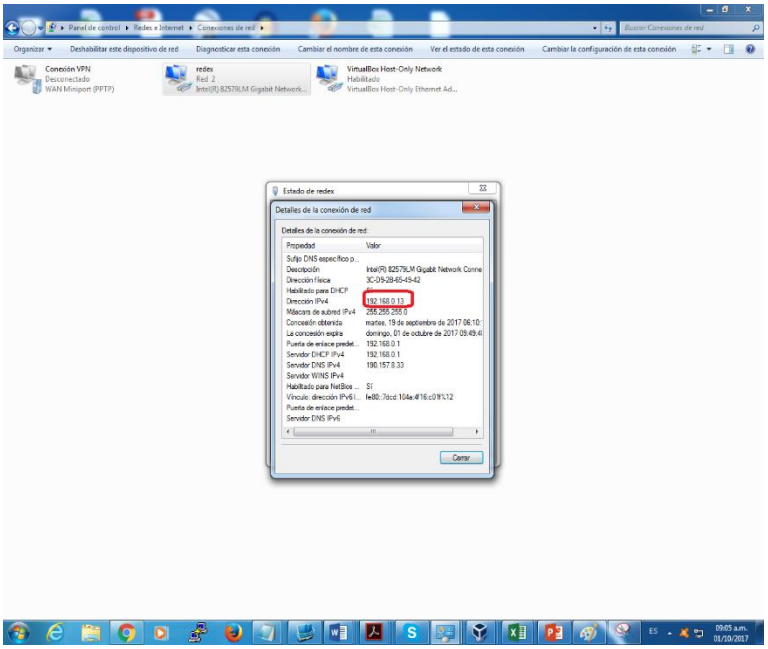
En la primera fase se realizara la instalación de un servicio ftp para servidor de archivos en la maquina Virtualizada Windows server el cual se configurara de la siguiente manera:

Figura 3 verificacion de Ip servidor Windows



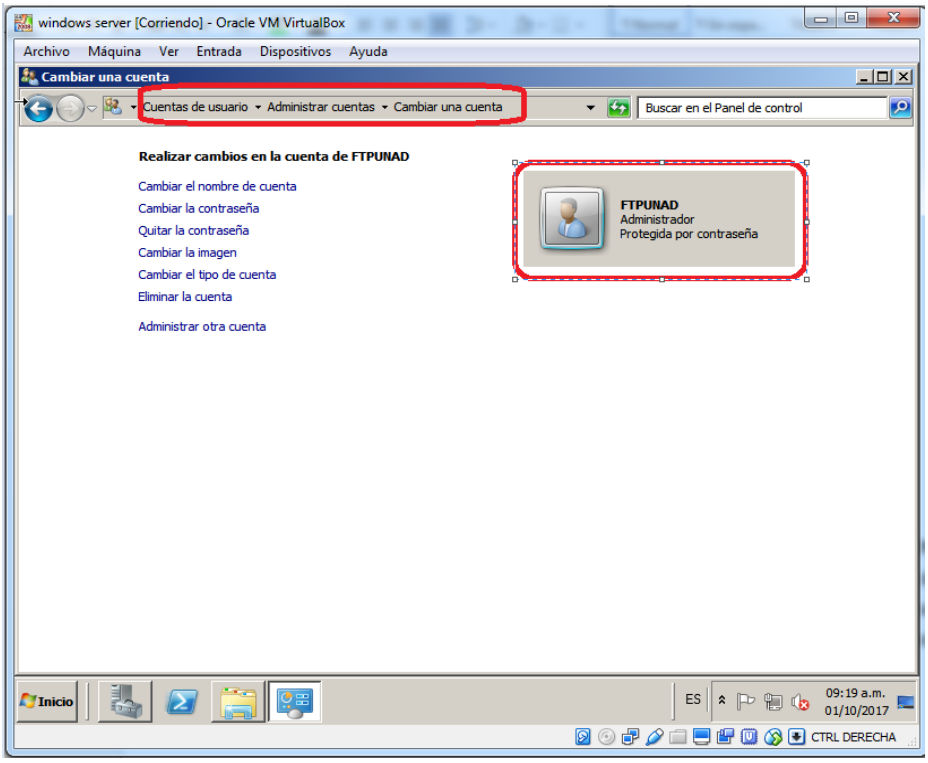
Se realiza el despliegue de la primera máquina virtual con sistema operativo de evaluación de 180 días de Windows server 2008 R2 en Virtualbox se le asigna el adaptador puente modo bridge para que tome un rango de direccionamiento ip del mismo segmento que el host anfitrión el cual es un Windows 7 profesional el cual va a contener virtualizadas las 3 máquinas que se utilizaran en este proyecto y servirá de cliente para probar los servicios básicos desplegados.

Figura 4 verificación configuración tarjeta de red



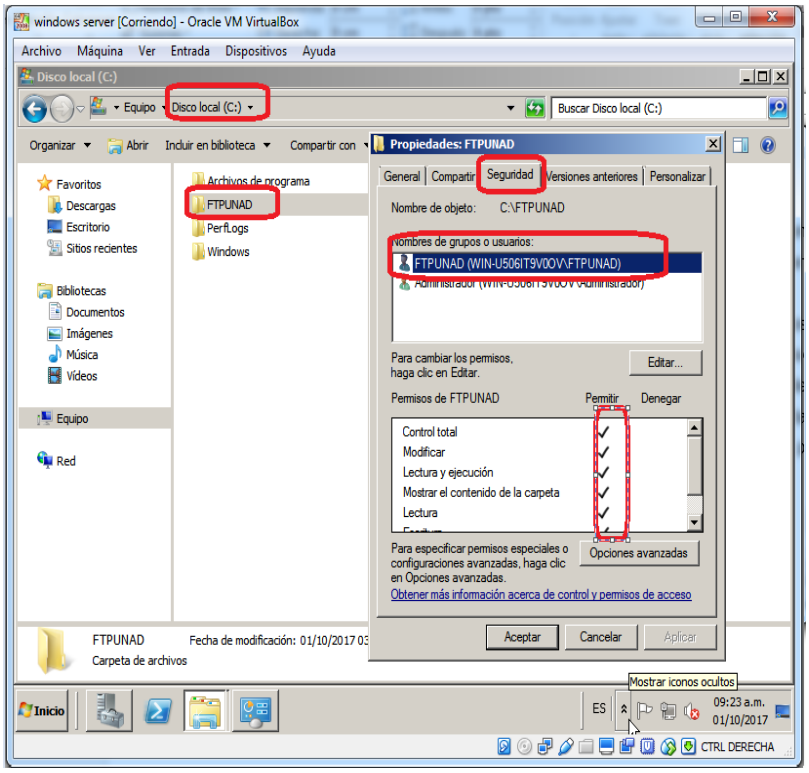
10.1 Instalación De Servicio Ftp Windows Server 2008 R2

Figura 5 configuración FTP



Para poder desplegar un servicio de ftp usando EL SERVIDOR DE APLICACIONES Internet Información Server de Microsoft conocido como IIS previamente se debe crear en el sistema operativo el repositorio contenedor de los archivos a los cuales brindara el servicio nuestro servidor FTP y se deben crear los usuarios que podrán conectarse a usar el servicio de la siguiente forma:

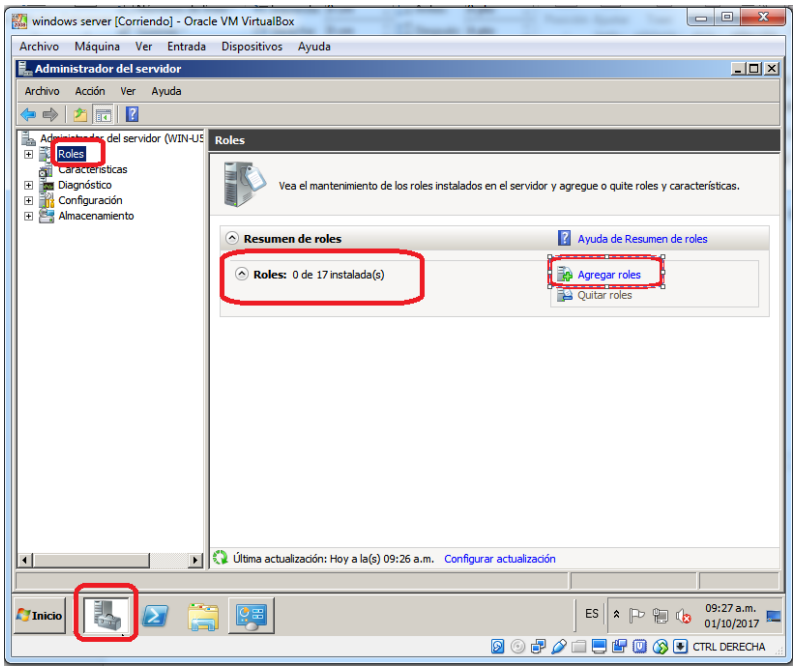
Figura 6 seguridad servicio FTP



En el panel de control de Windows server en administración de cuentas de usuarios se ha creado un nuevo usuario del sistema que podrá conectarse a este servidor para hacer el uso del servicio ftp

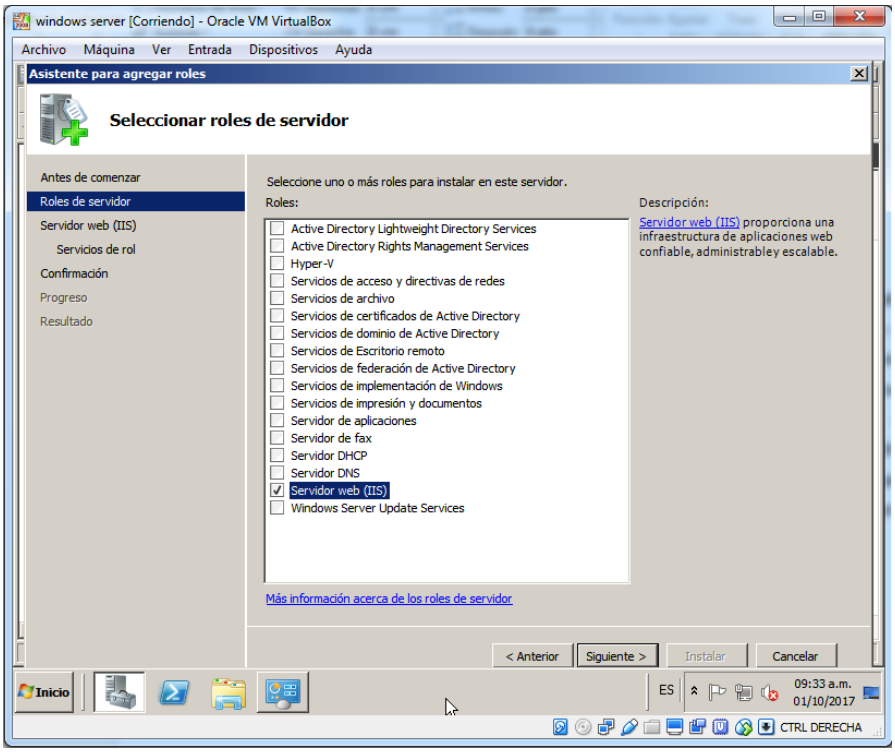
de igual forma en la raíz del disco c se ha creado una carpeta contenedora llamada FTPUNAD, a la cual al darle click derecho propiedades en la pestaña de seguridad se le ha dado acceso y control total al usuario ftpunad que se creó anteriormente.

Figura 7 asignación de rol



Ahora en la parte inferior lateral izquierda existe un icono que permite administrar el servidor, como se observa el servidor actualmente no cuenta con ningún rol, por lo cual no ofrece ningún servicio, por lo cual en la pestaña roles se le dará la opción de agregar roles.

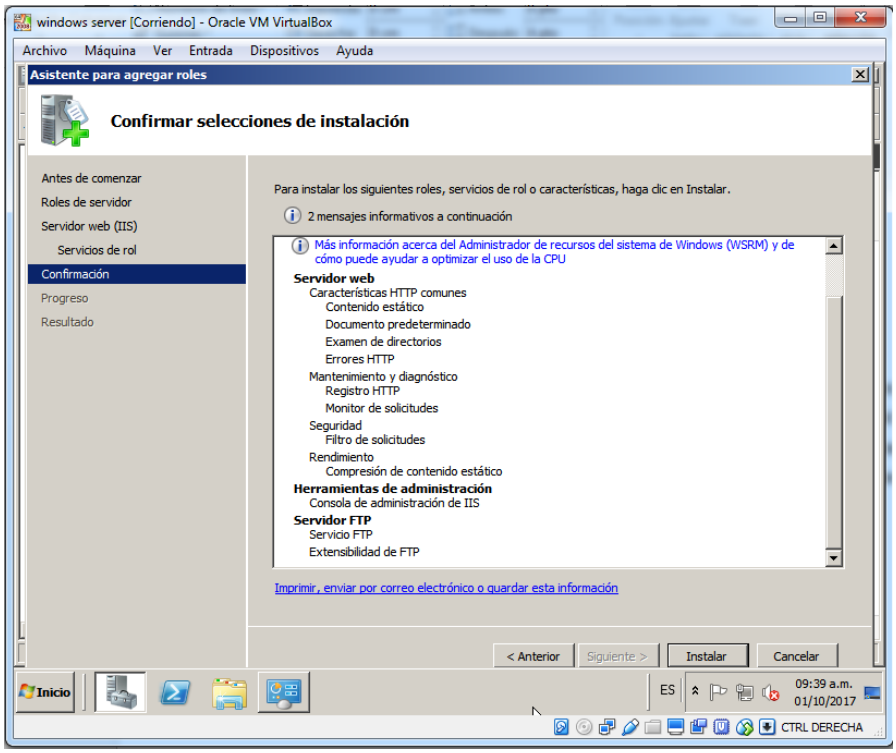
Figura 8 rol IIS



Se le asignara el rol de servidor web y se le dará en siguiente

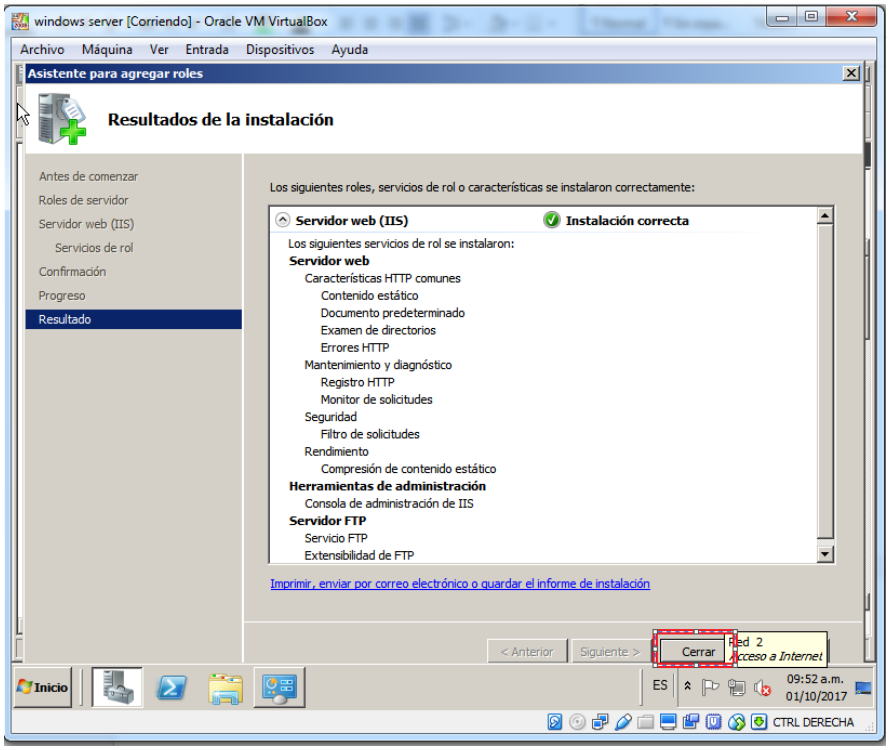
En la parte inferior se seleccionaran las opciones de servidor ftp para que dichas características sean integradas al servidor web de internet información server

Figura 9 Instalar Roles



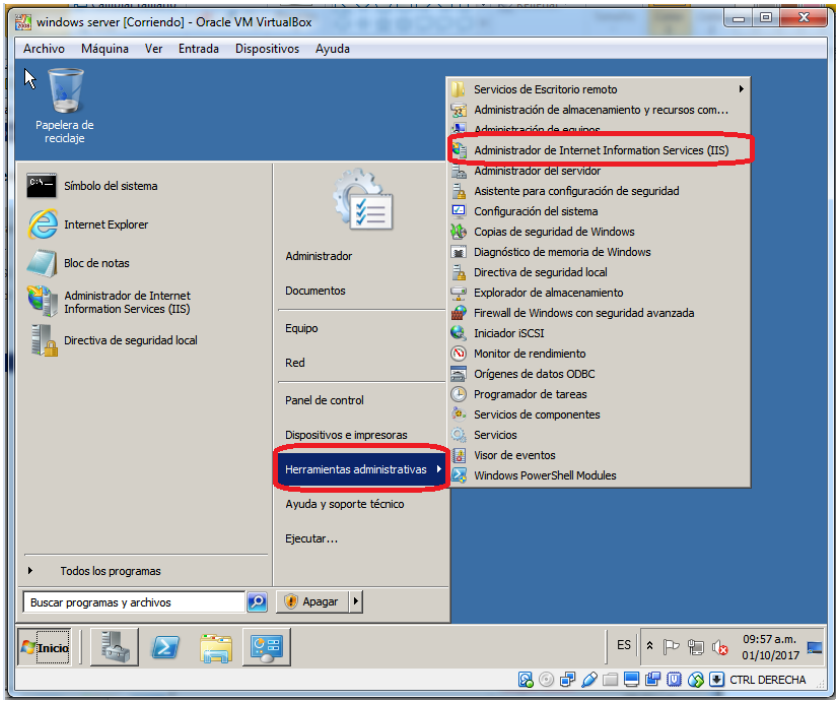
Y se le dará instalar para que dichos roles sean agregados al servidor

Figura 10 verificación



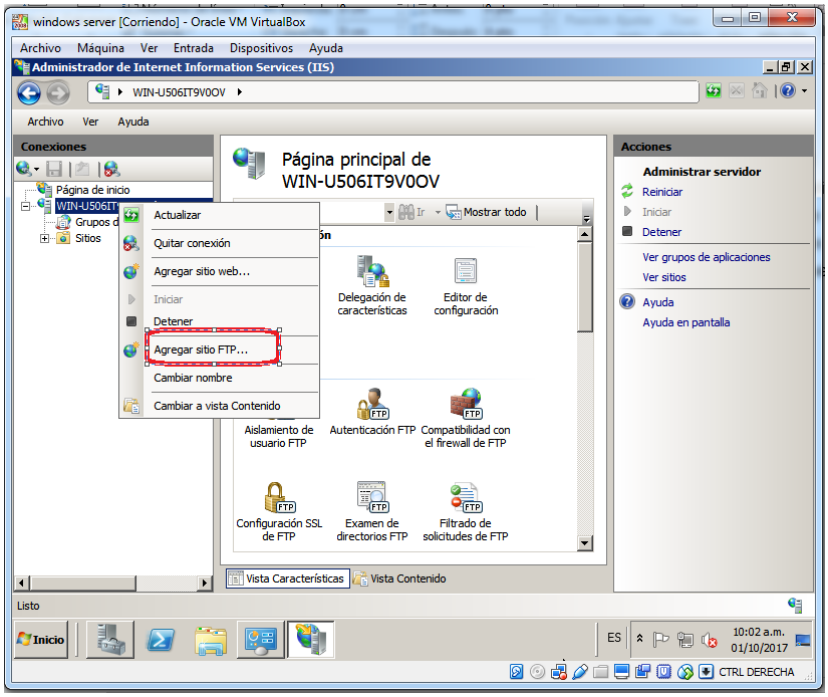
Verificamos que los servicios se han instalado de manera correcta y le damos cerrar.

Figura 11 Servidor IIS



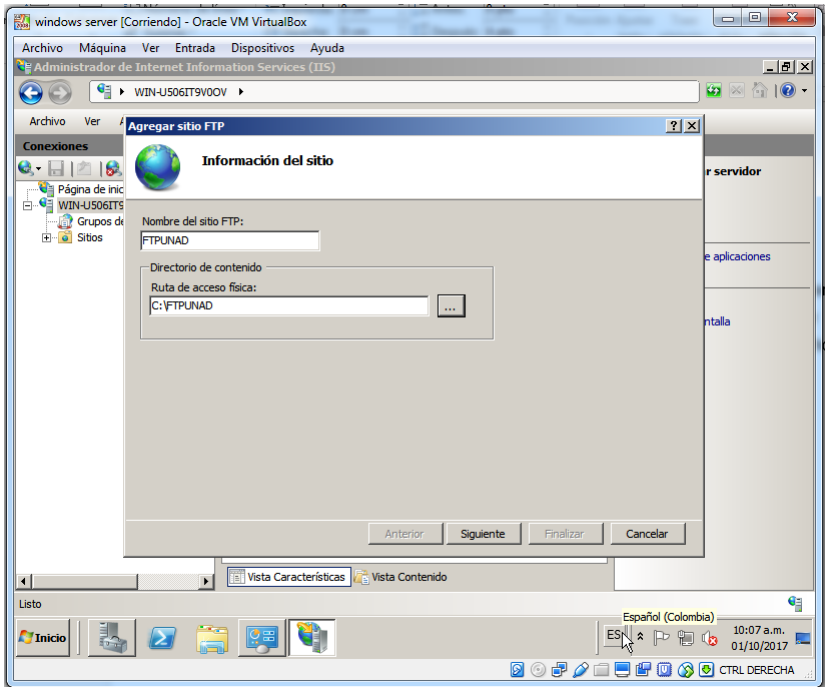
Ahora en el panel de herramientas administrativas verificamos que existe un menú de administración de internet información server.

Figura 12 agregar sitio FTP



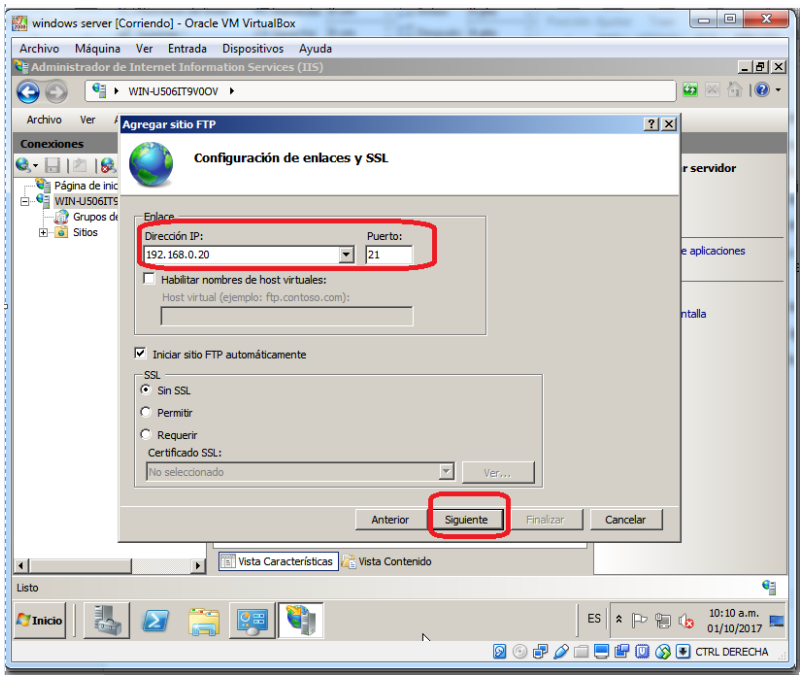
Al ingresar a internet information server le damos click derecho y agregar sitio FTP

Figura 13 Nombrar Sitio



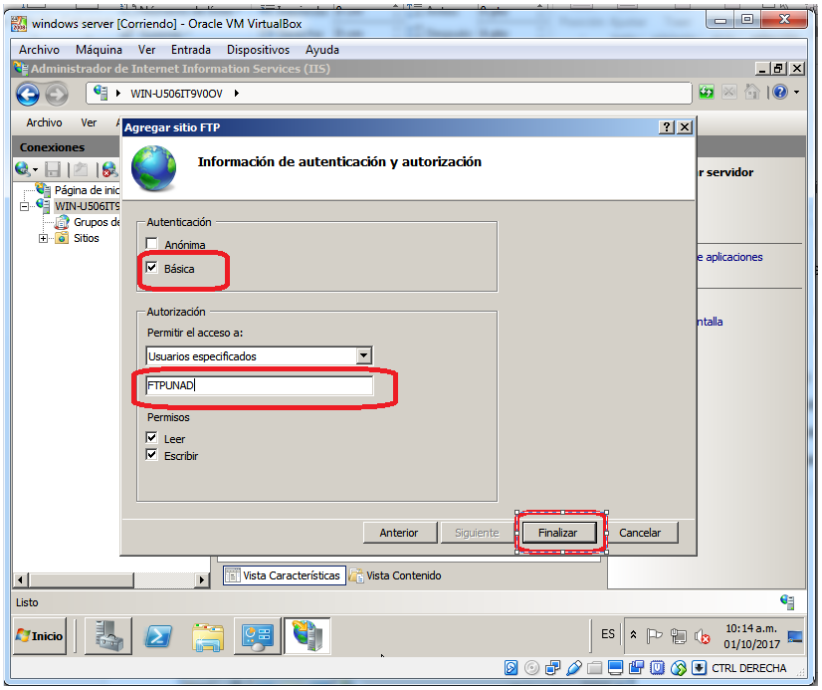
Le colocamos el nombre a nuestro servicio FTPUNAD y se le indica la ruta donde creamos la carpeta ftpunad en la raíz del disco C a la cual tiene permisos de control el usuario ftpunad creado de igual forma anteriormente.

Figura 14 Asignación de Puerto



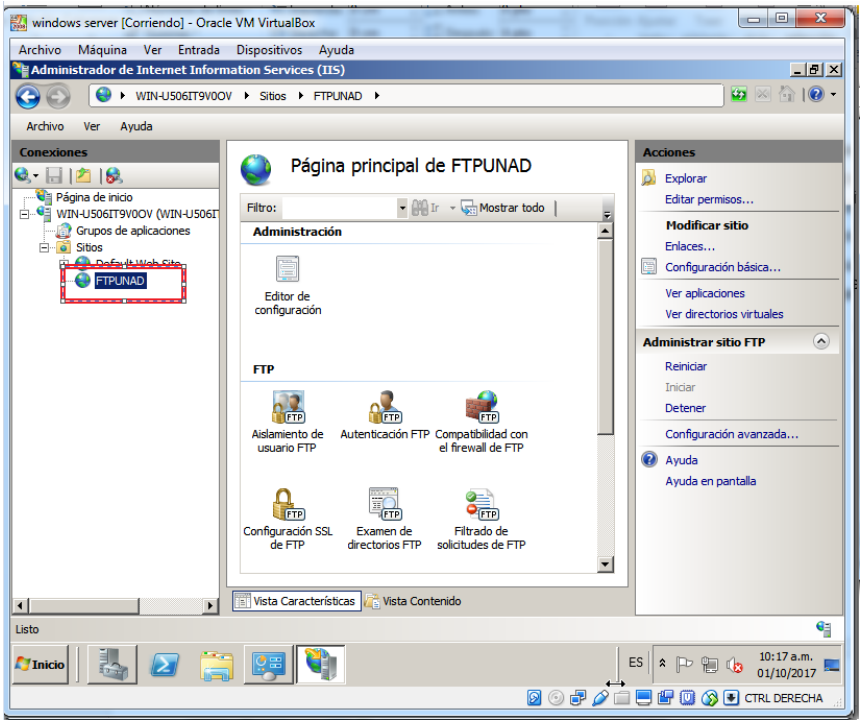
Le agregamos la ip de nuestra máquina virtual como y se le asigna el puerto 21 para escuchar las peticiones del servicio, y le damos siguiente.

Figura 15 Autenticación



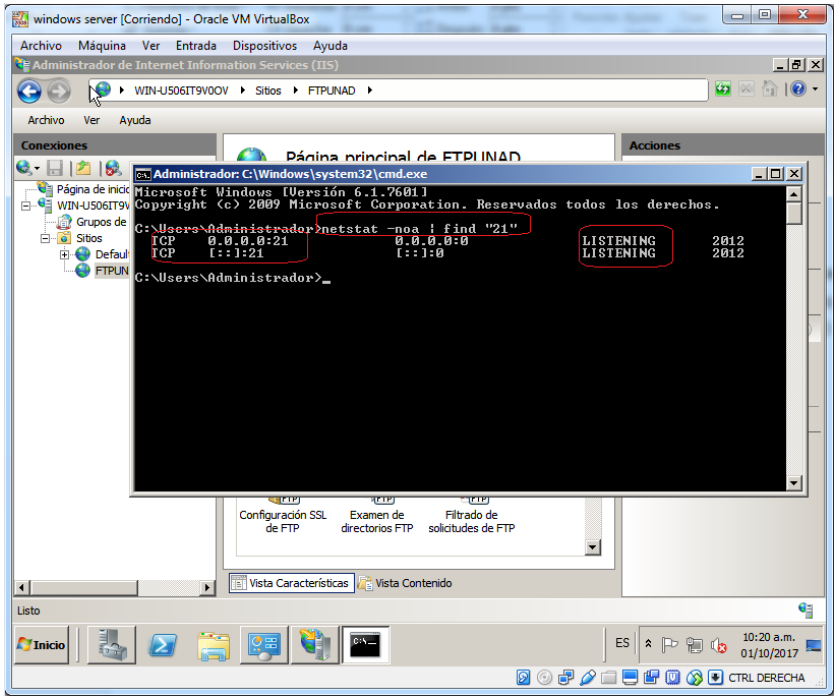
En la forma de autenticación le damos básica y le indicamos que a nuestro repositorio únicamente se podrá conectar el usuario FTPUNAD, y le damos finalizar.

Figura 16 Publicación



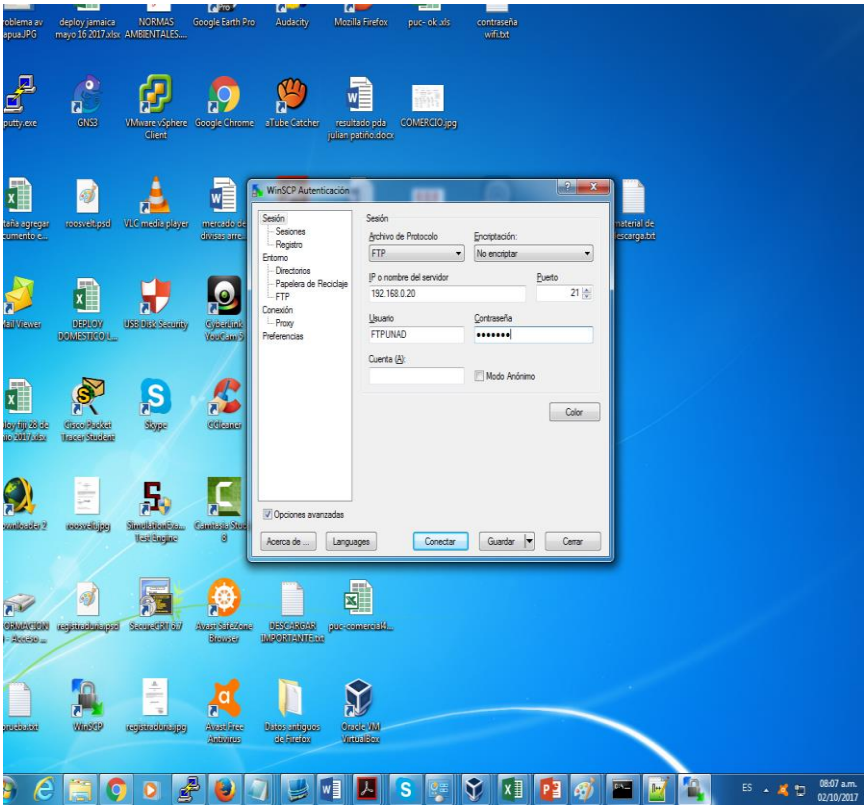
Como se verifica ya existe un nuevo servicio publicado denominado FTPUNAD

Figura 17 Verificación Línea de comando



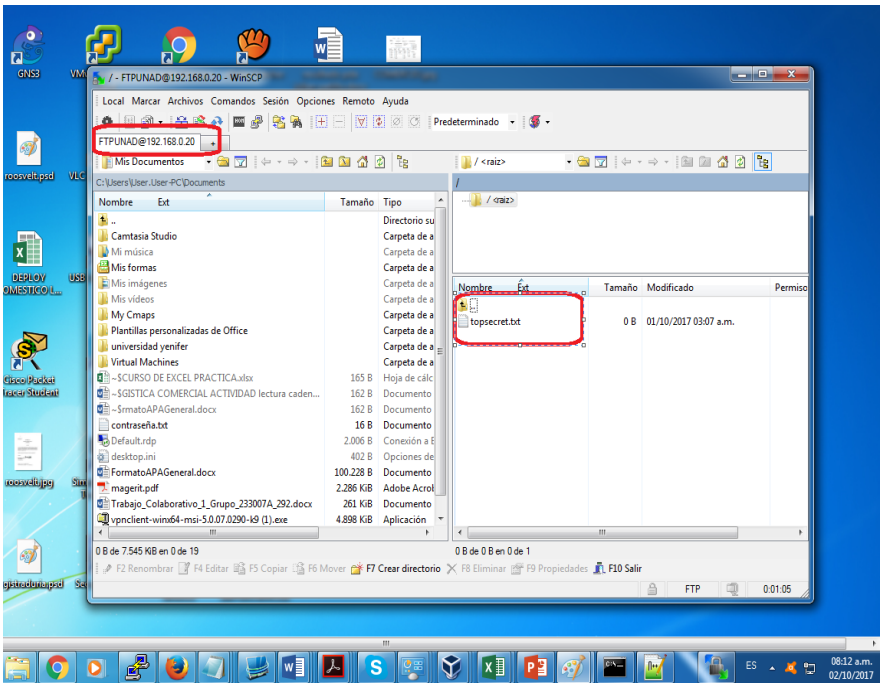
Verificamos de manera local desde la línea de comando con netstat –noa | find “21” de que verifica que el estado del puerto 21 y como se observa en la imagen el puerto está escuchando de manera adecuada.

Figura 18 Probar servicio cliente FTP



Ahora se procede a probar el servicio desde la maquina cliente en este caso es el host real donde se encuentran instaladas las máquinas virtuales, ingresando el usuario y credenciales creadas para tal fin.

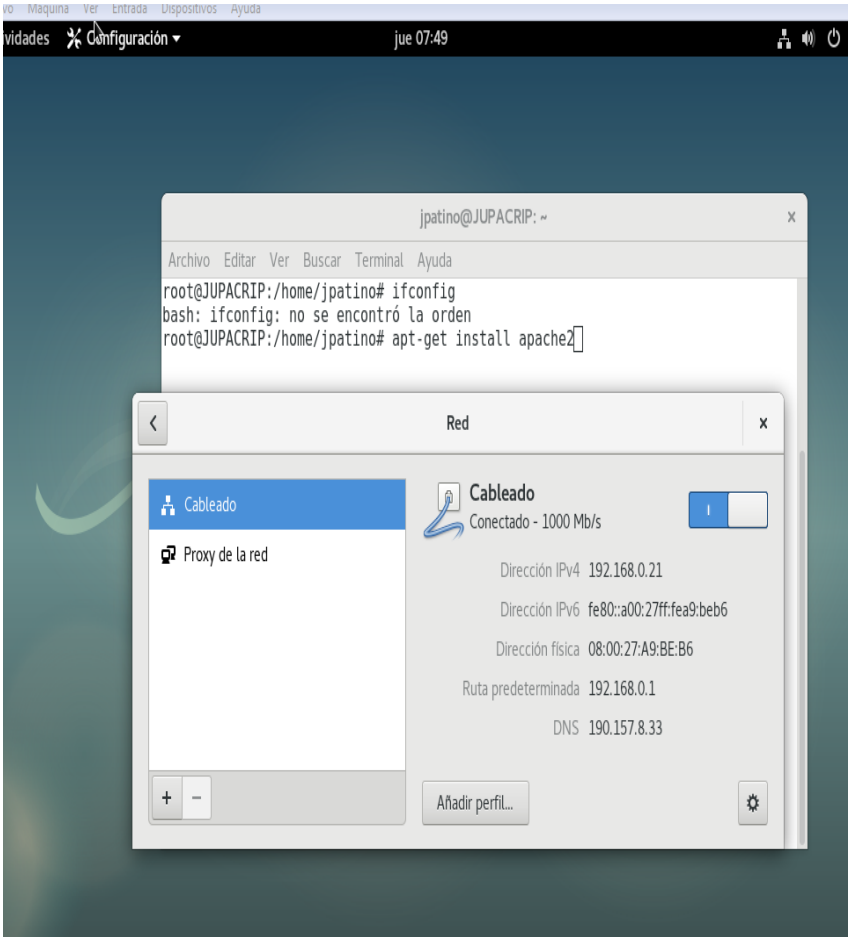
Figura 19 Acceso al archivo



Y se observa que se ha accedido de manera correcta al servicio de servidor de archivos en Windows server usando conexión ftp desde el cliente usando winscp.

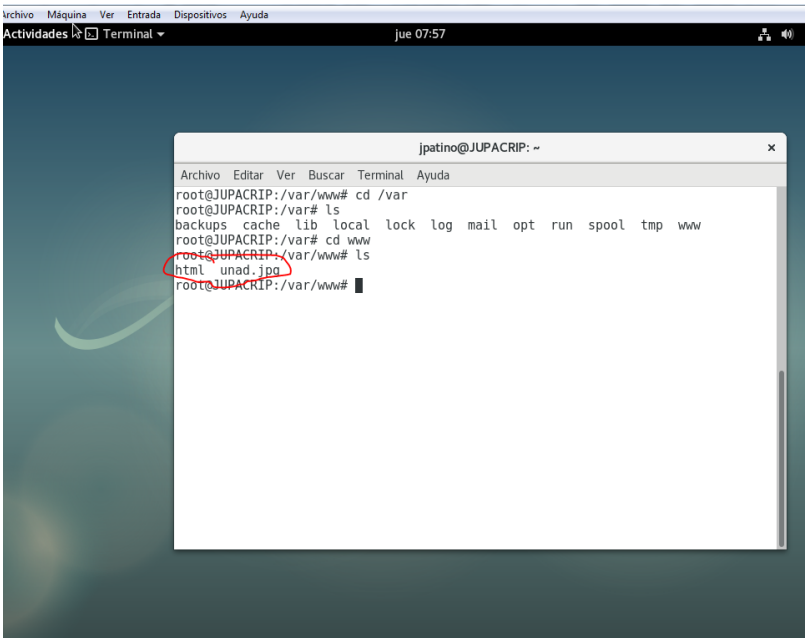
10.2 Segunda Parte Instalación De Servicio Web En Linux Debían

Figura 20 tarjeta de red servicio http



En el despliegue del segundo servicio se procederá a instalar un servidor web apache en el equipo debían cuya ip se relaciona en el mapa de la topología de la sección anterior con dirección ip 192.168.0.21, dicho servicio es de uso interno de la compañía en el cual pedirá ingreso de credenciales de usuario y el puerto de escucha del servicio es el puerto 80 que es por defecto del servicio http

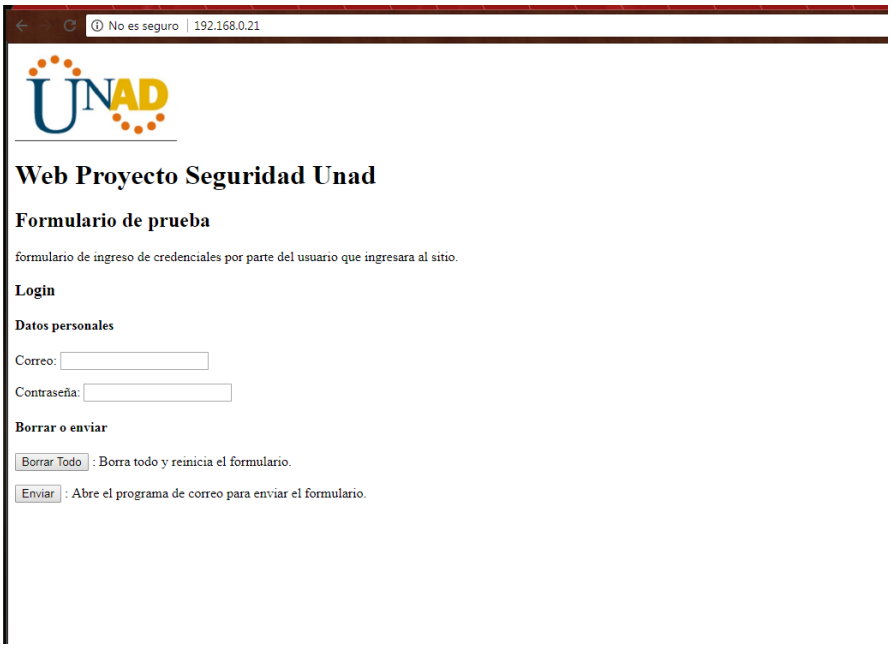
Figura 21 creación sitio http



Se crea una página de inicio en HTML y una imagen de la universidad para realizar la simulación de la página de inicio de un sitio web para que los usuarios ingresen su información de acceso al sistema

Se prueba que el sitio web suba

Figura 22 Verificación Sitio web



El cual muestra un formulario de ingreso de información con el cual se realizara la simulación de un servicio de uso empresarial

11. PRUEBAS DE PENETRACION

11.1 Escaneo General

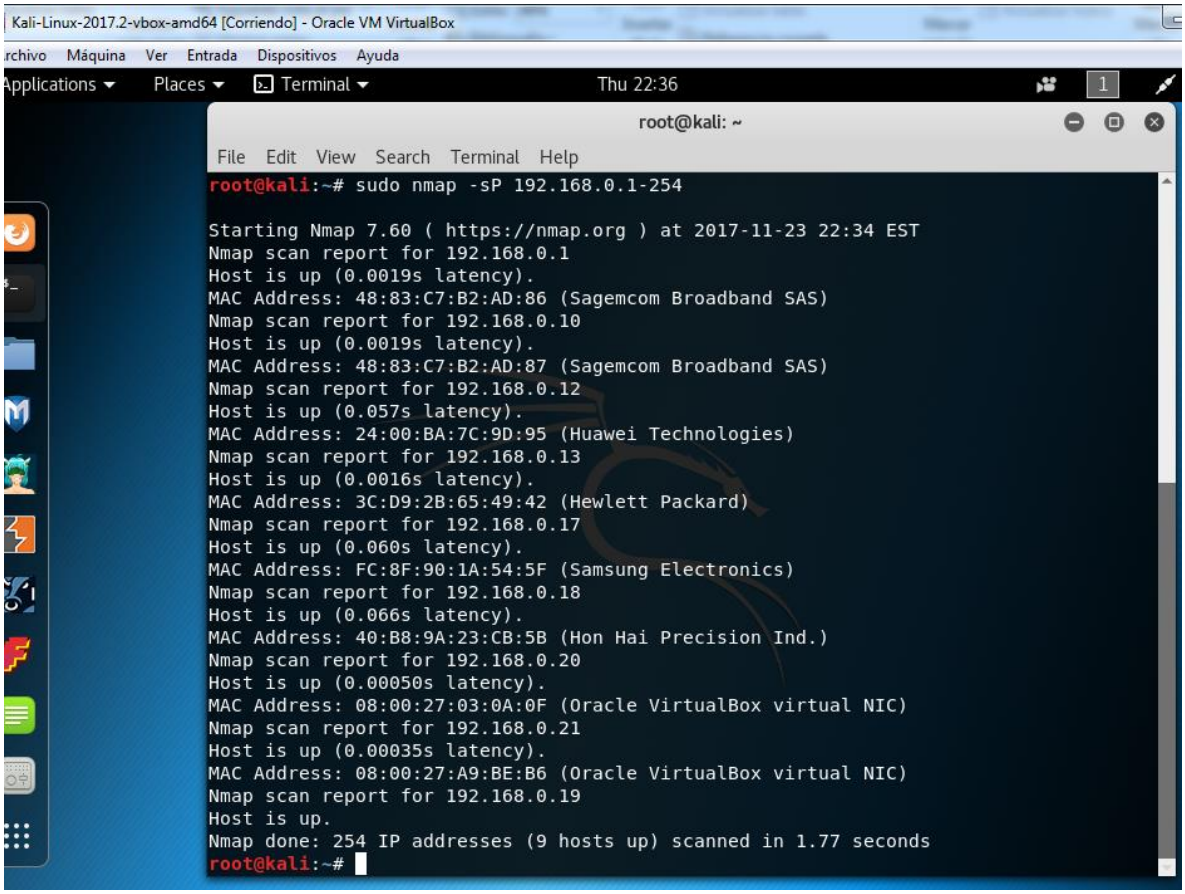
Tratando de realizar el ejercicio lo más cercano a la realidad posible se interpreta de que esta red no cuenta con seguridad en las interfaces de los switches que llegan a cada uno de los puntos de red de la compañía por lo cual la maquina Kali atacante se pudo conectar a uno de los puntos de red en un Jack de cualquier piso o ubicación de la compañía y se le asigno dirección ip dentro del rango de trabajo de los demás host que se encuentran en el interior.

El equipo atacante perteneciente desea conocer que equipos están disponibles para poder planear su ataque por lo cual procederá a escanear el segmento de red en donde nos encontramos para determinar que equipos están activos mediante el siguiente comando:

Sudo nmap -sP 192.168.0.1-254

Se tratara de encontrar todos los equipos activos que se encuentren en este segmento y adicional a esto me traerá la Mac asociada a cada host lo cual es muy importante para realizar el proceso de explotación posteriormente.

Figura 23 escaneo nmap



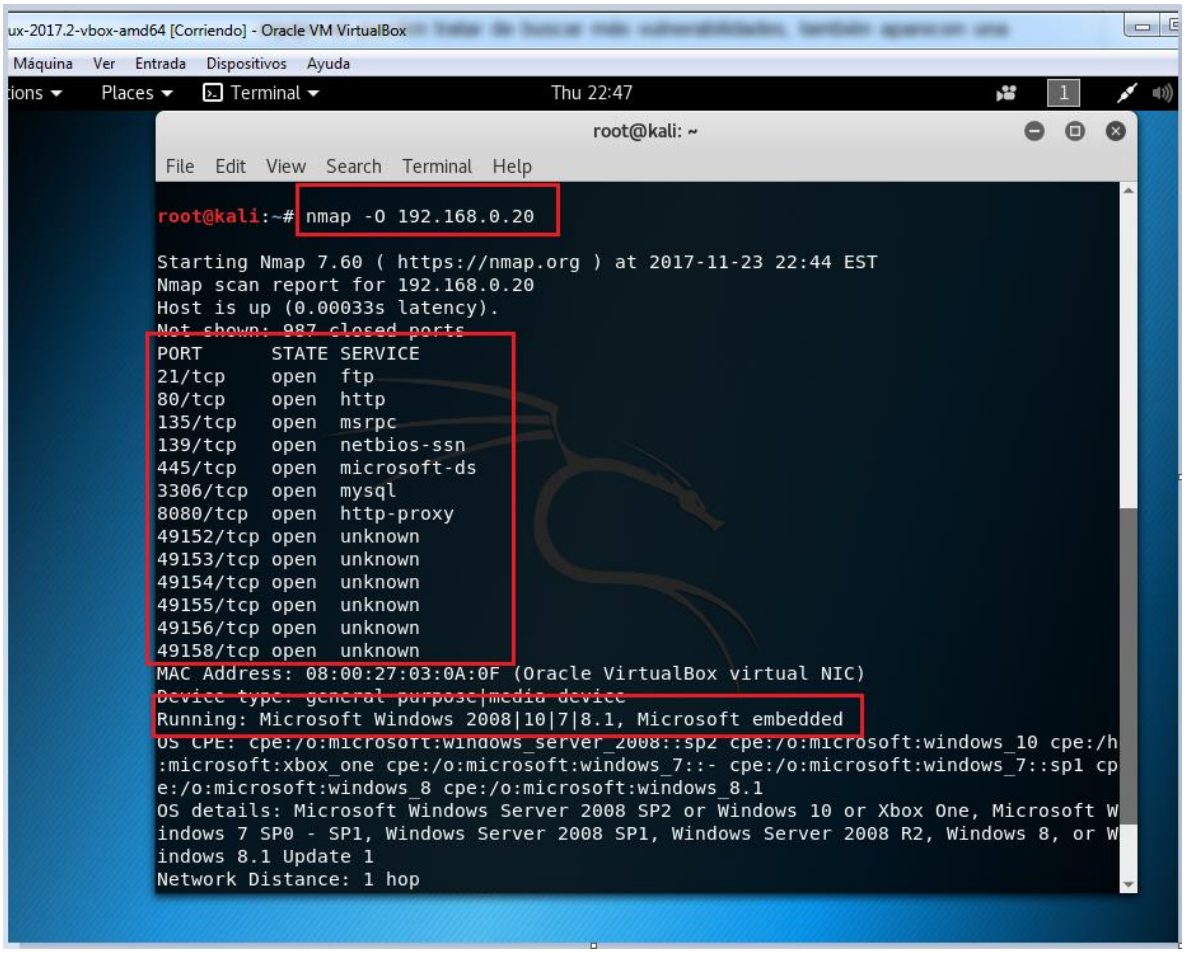
Como se observa en la gráfica detecto 9 dispositivos que están usando direccionamiento ip del rango desde 192.168.0.1 hasta 192.168.0.254, identifico que la ip 192.168.0.1 es un router marca sagemcon con lo cual por el modelo del equipo se pueden tratar de buscar más vulnerabilidades, también aparecen una impresora y teléfonos celulares que estaban usando el dhcp inalámbrico en el momento del escaneo, pero de esta forma el atacante puede identificar qué tipos de equipos están disponibles y empezara a segmentar sus ataques dependiendo sus necesidades.

Según el planteamiento del ejercicio las dos máquinas que le interesan al atacante son la 192.168.0.20 y 192.168.0.21

El atacante deberá conocer qué tipo de sistemas operativos manejan dichas maquinas por lo cual continuando con Nmap ahora debemos determinar que versión de sistema operativo tienen:

nmap -O 192.168.0.20

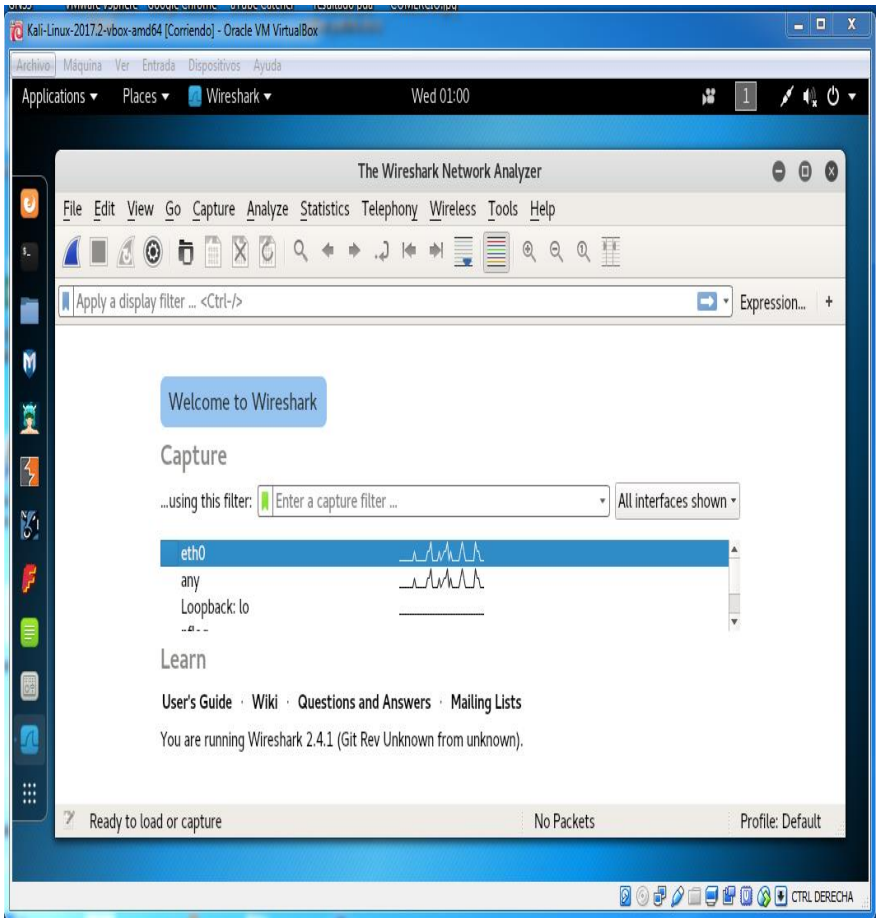
Figura 24 identificación de puertos y servicios



Con este comando se ha recolectado información bastante importante se observa que el sistema operativo de la maquina atacada es Windows server 2008, que tiene varios puertos abiertos dentro de los que se encuentra ftp y http como los más representativos ya que son blancos fáciles de atacar con el fin de ganar más acceso a la maquina víctima.

11.2 Ataque servicio FTP Windows Server 2008

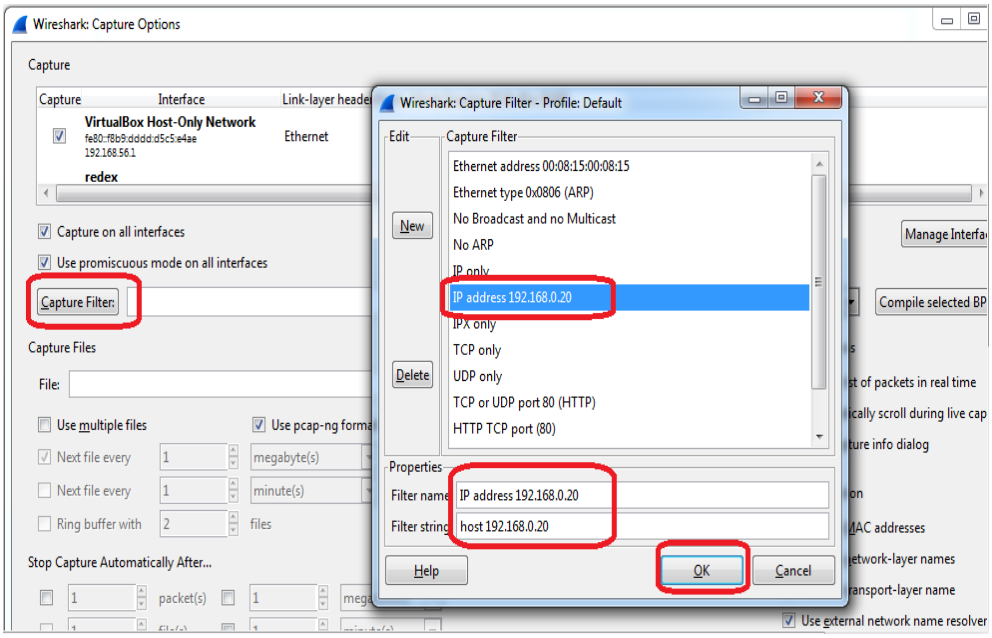
Figura 25 Wireshark maquina Kali



Después de haber publicado el servicio en el servidor ftp en Windows server se procederá a realizar un escaneo del tráfico desde una maquina atacante Kali Linux para demostrar la inseguridad al implementar un protocolo sin cifrado como lo es FTP y poner en evidencia algunas falencias del envio en texto plano como lo hace este protocolo, poniendo en riesgo y comprometiendo la seguridad de nuestro servidor de archivos para mostrar de manera gráfica lo sencillo que le resulta al atacante vulnerar este tipo de servicio.

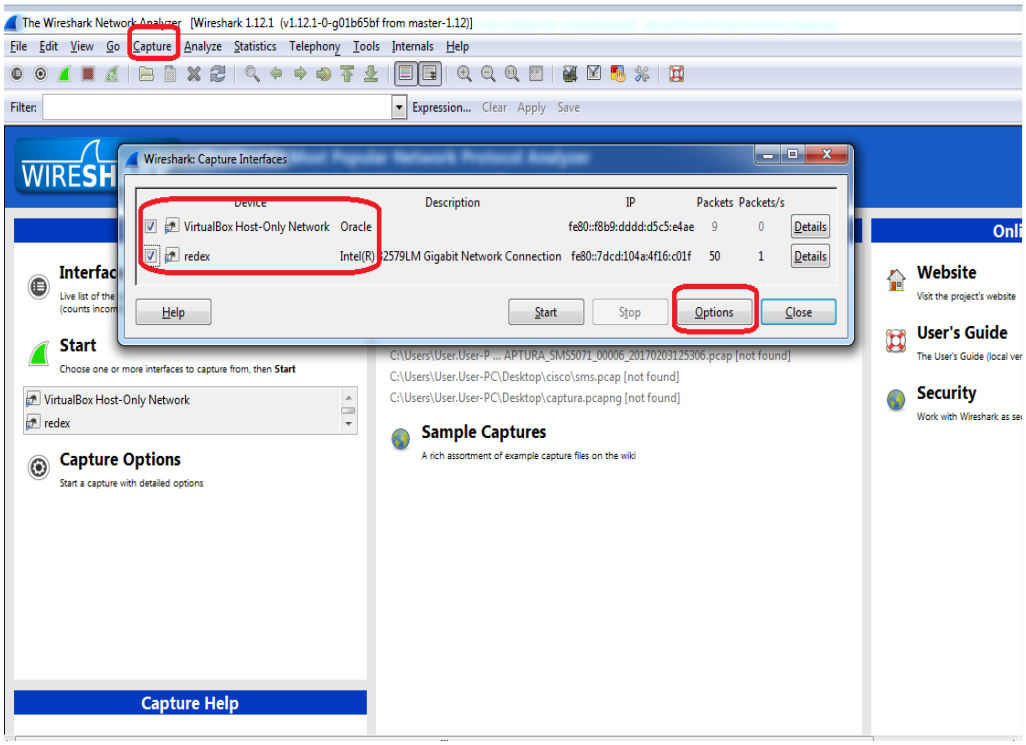
En nuestra maquina Kali Linux atacante conectada al mismo segmento de red de nuestra victima usaremos el analizador de protocolos Wireshark para descifrar los datos de autenticación del cliente que trate de conectarse al servidor ftp que sabemos es la maquina con ip 192.168.0.20

Figura 26 configuración de la captura



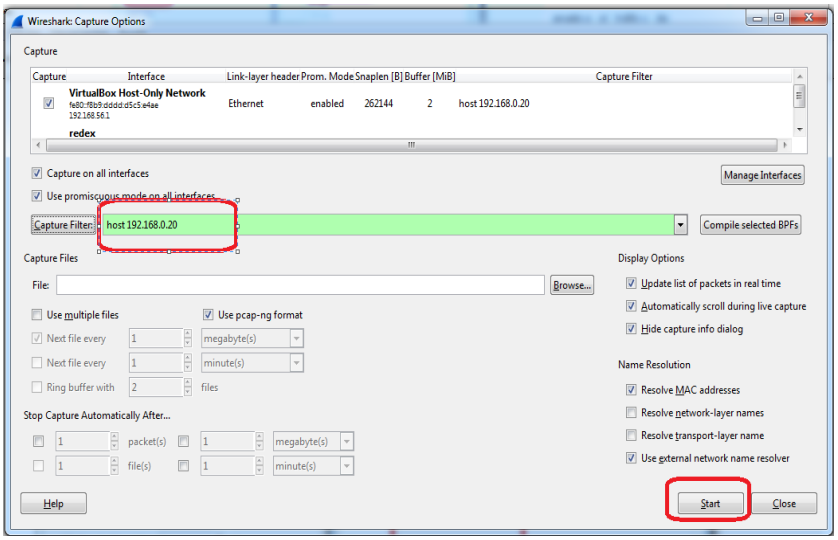
Lo primero es seleccionar la opción capture, luego la opción interfaces y seleccionaremos las dos interfaces disponibles y luego options

Figura 27 seleccionar interface en modo promiscuo



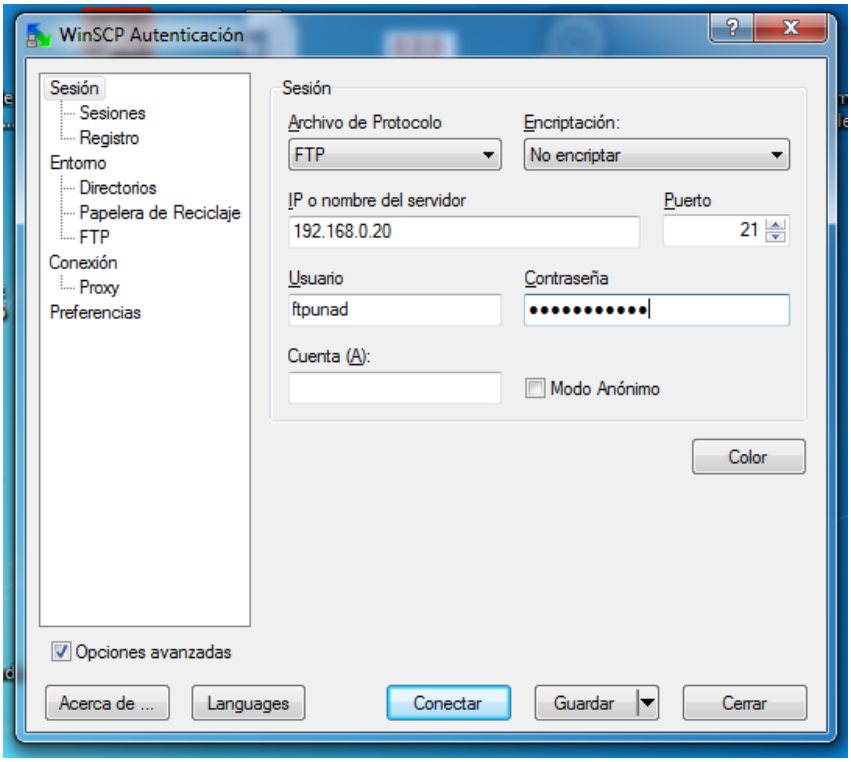
Luego dentro de options tomamos la opción capture Filter y dentro de los filtros que solo analice el tráfico de la ip 192.168.0.20 que es nuestro server ftp y damos ok

Figura 28 aplicar filtro



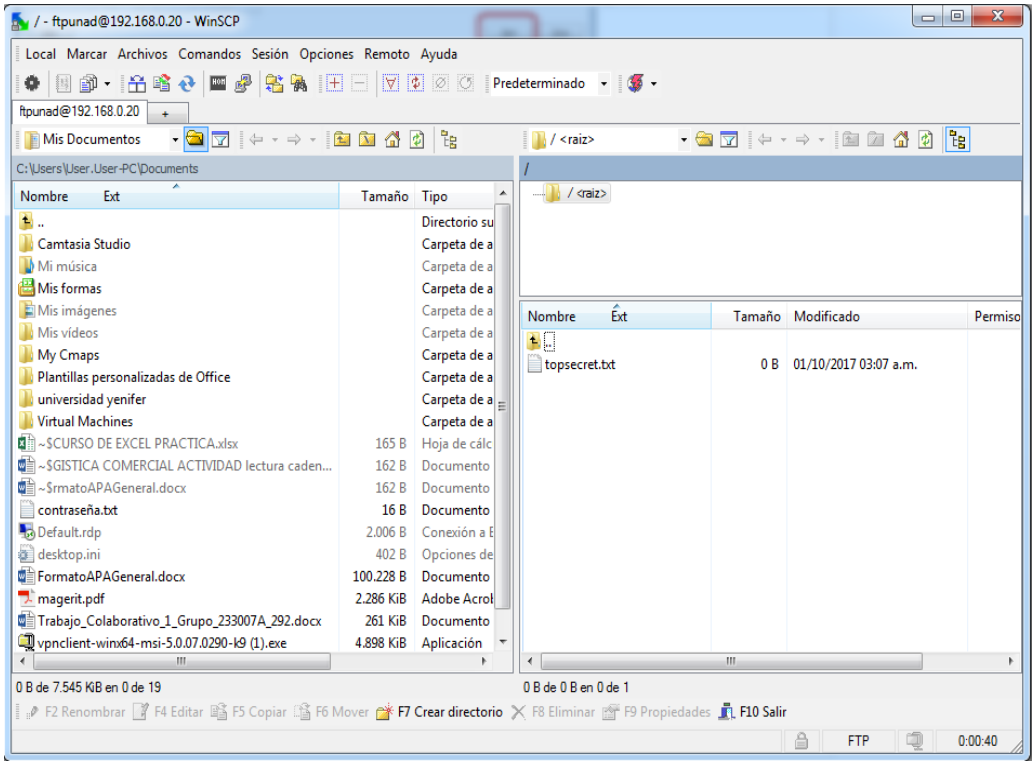
Nos regresa a la ventana anterior validamos el filtro aplicado al host 192.168.0.20 y le damos start.

Figura 29 Conexión FTP Snifer



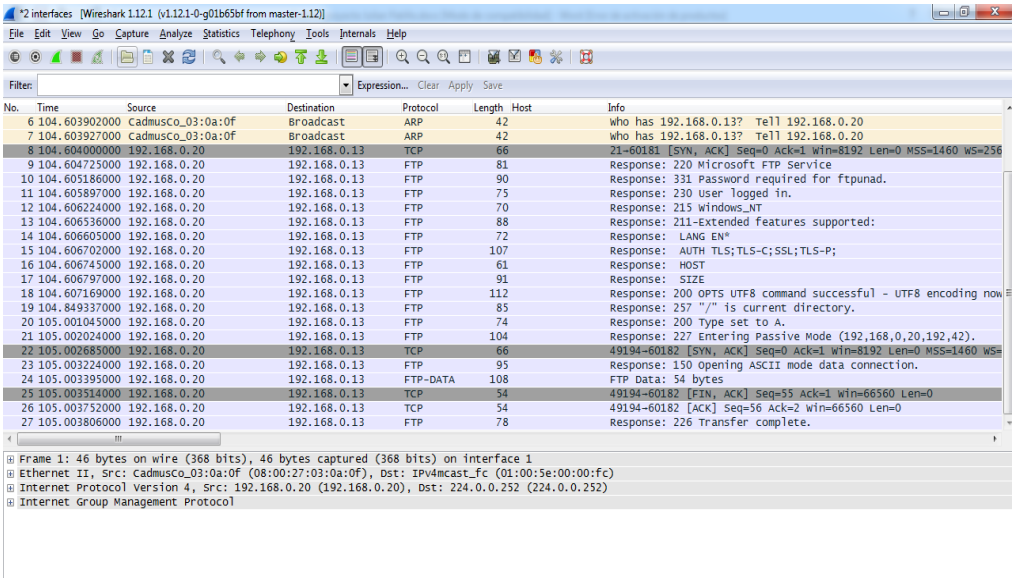
Desde nuestra maquina cliente probamos conexión usando el cliente winscp ingresamos la ip del servidor 192.168.0.20, el usuario ftpunad y el password y le damos conectar.

Figura 30 Conexión del servicio



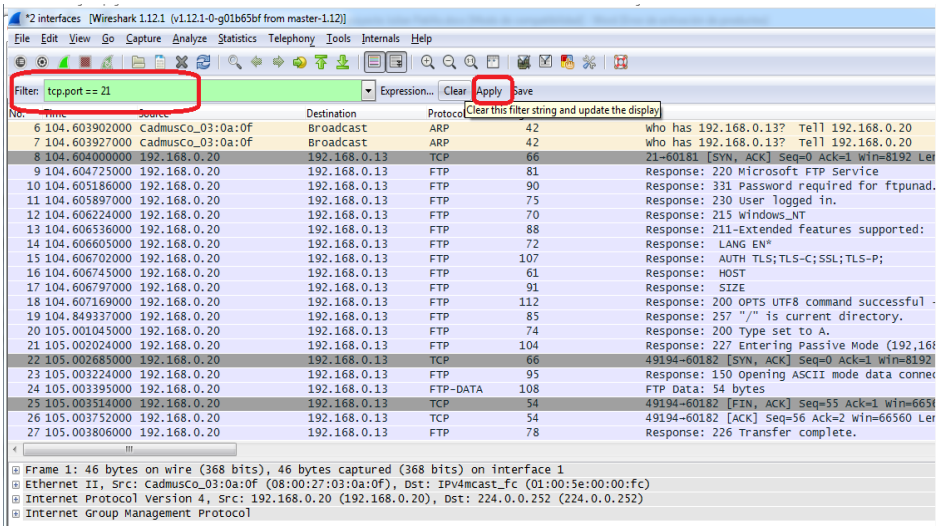
Validamos de que se ha realizado la conexión y el contenido es un documento txt llamado top secret.

Figura 31 Validación de trafico



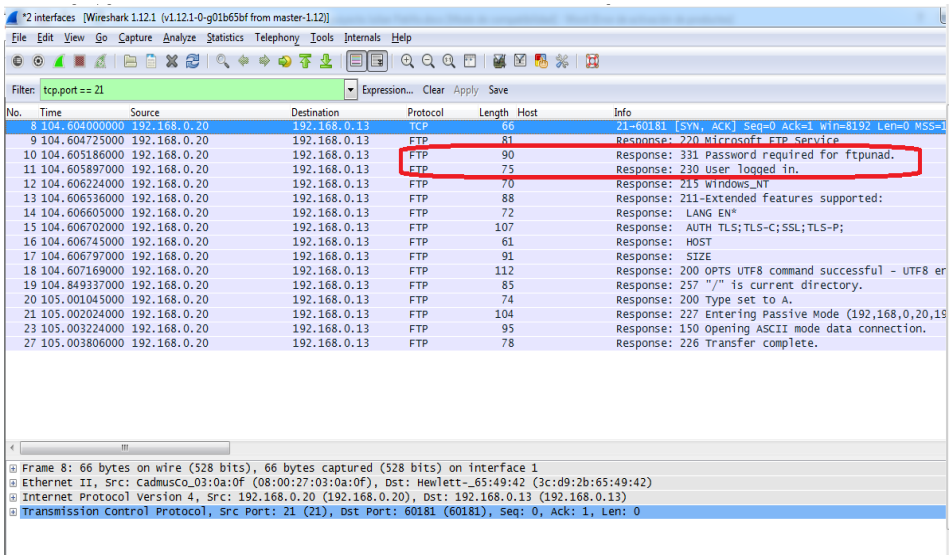
Ahora abrimos Wireshark y validamos que capturo tráfico de esa ip 192.168.0.20 pero es bastante información que no nos dice nada a simple vista.

Figura 32 Filtro Puerto 21



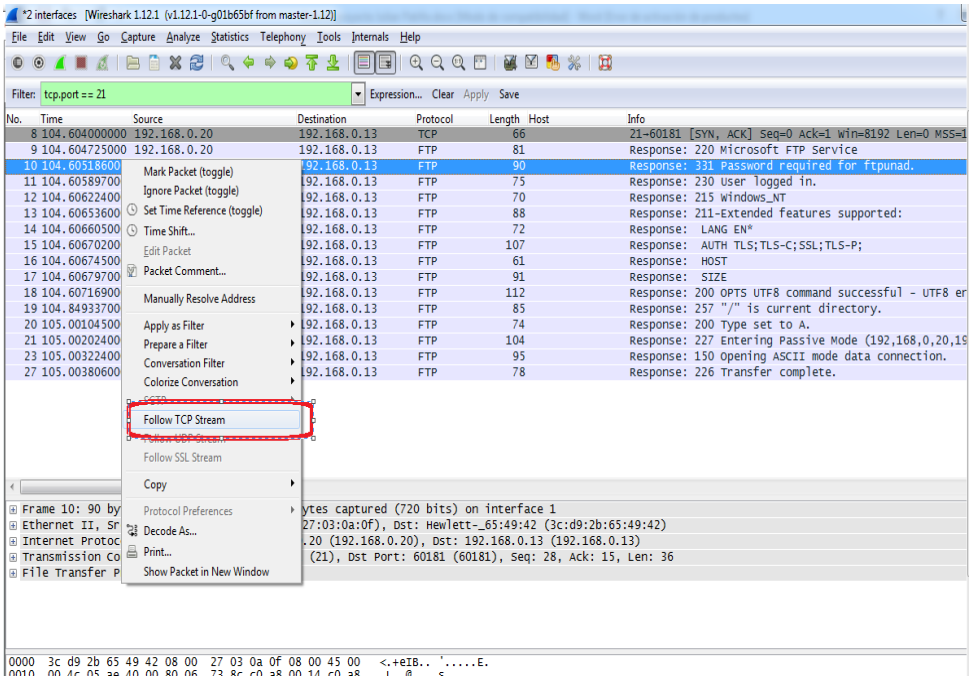
Por lo cual a ese tráfico ya capturado le aplicaremos un nuevo filtro al puerto 21 que es el puerto del servicio ftp y le damos apply.

Figura 33 trafico Ftp



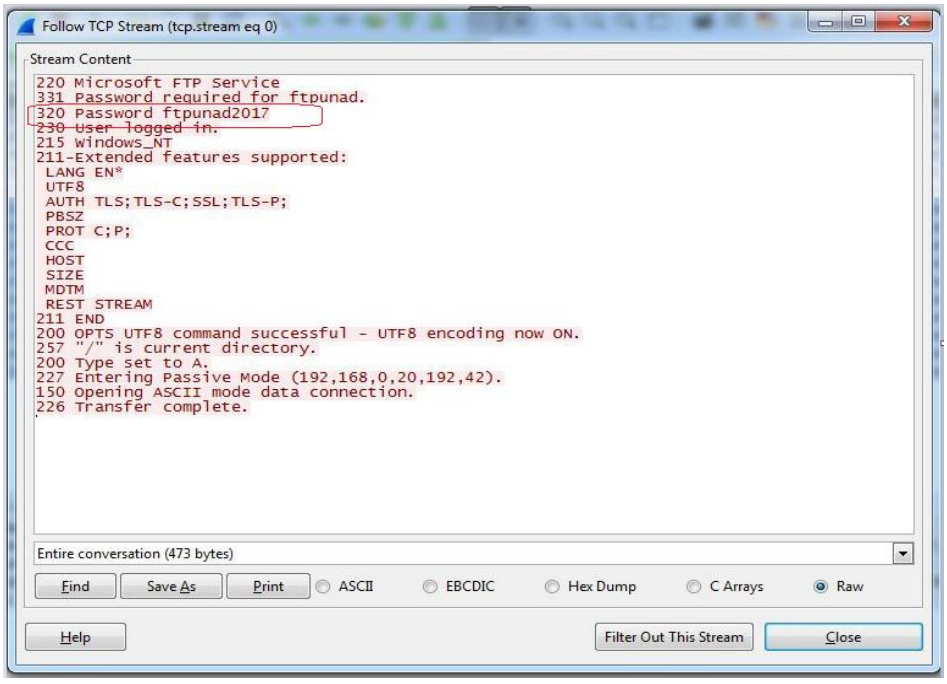
Como se observa ya solamente esta filtrado el trafico ftp y hay dos líneas en particular donde se identifica que el usuario es ftpunad y que se envio un password

Figura 34 Follow TCP Stream



a esa línea en particular le daremos click derecho y tomaremos la opción follow tcp stream

Figura 35 captura de credenciales

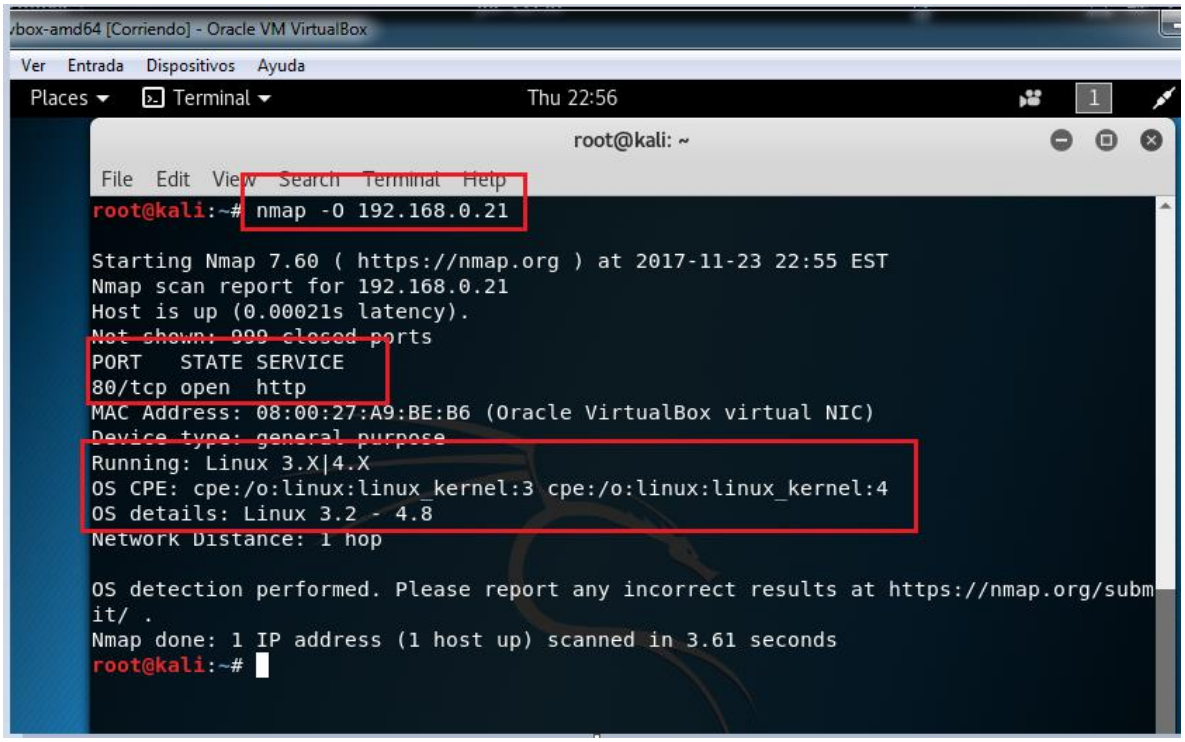


Y verificamos que se ha capturado la contraseña que estaba en texto plano y es ftpunad2017 por lo cual la información contenida en ese servidor ya se encuentra comprometida por usar ftp que no brinda seguridad.

11.3 Ataque servicio Web Servidor Linux Debían

Teniendo las credenciales de conexión del servicio ftp en el Windows server se procederá a realizar el escaneo de la maquina Linux debían que tiene ip 192.168.0.21 de la misma manera que se realizó con la maquina Windows.

Figura 36 escaneo servidor web



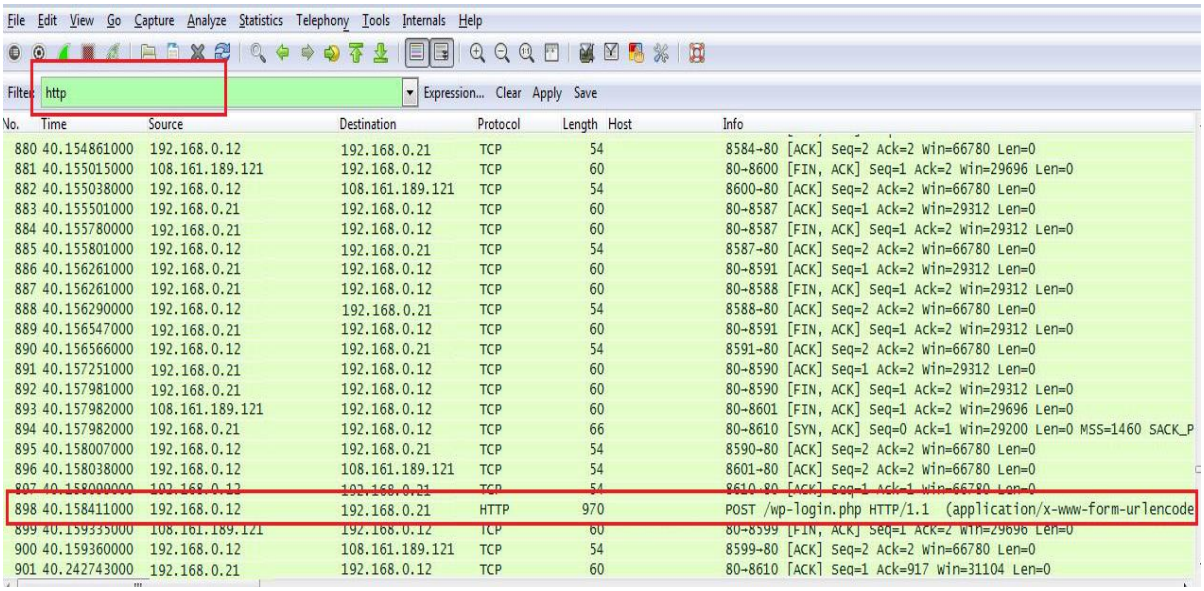
En el escaneo realizado nos muestra que la maquina tiene un sistema operativo Linux pero no muestra que tipo de distribución es por lo cual se complica un poco más el trabajo del hacker en cuanto a descubrir las versiones exactas, esto es un plus de Linux sobre Windows ya que al escanear el Windows mostro la versión especifica del sistema operativo de la maquina víctima.

Pero si se observa que hay un servicio publicado por http puerto 80 el cual se tratara de vulnerar de igual forma.

Figura 37 Test servicio Web

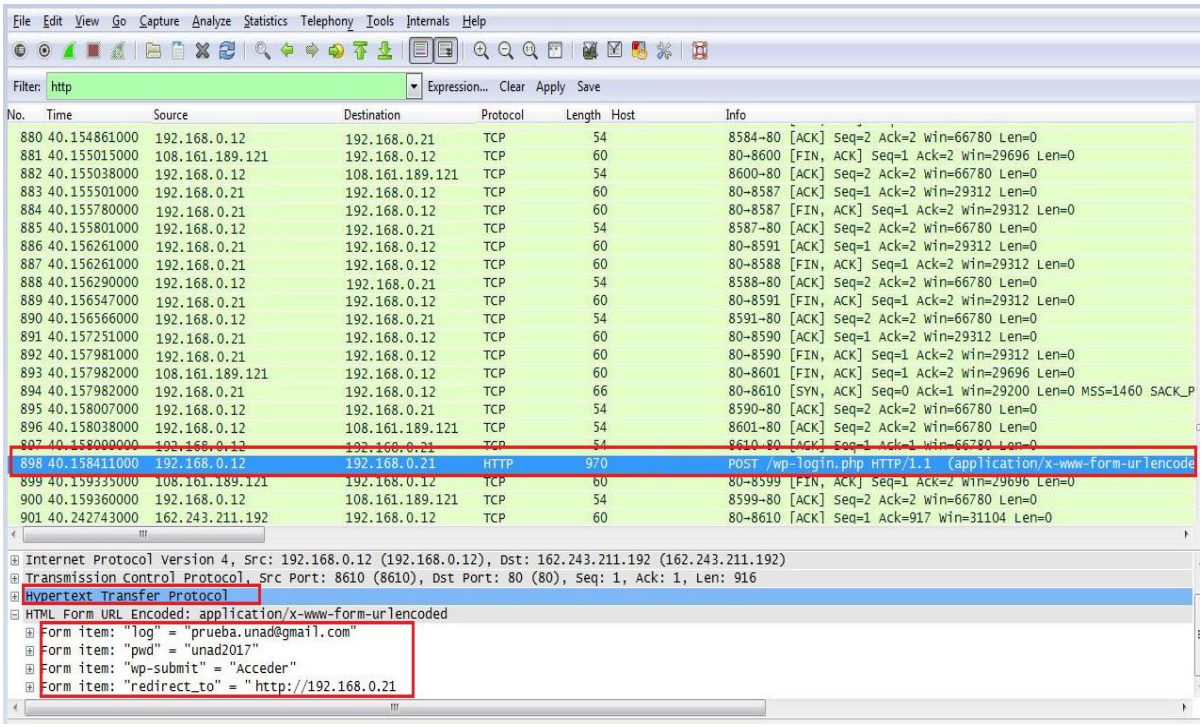
Se abre un navegador en una maquina cliente para probar el uso del servicio publicado haciendo el uso del protocolo http mediante este formulario para realizar un inicio de sesión en la plataforma.

Figura 38 Conexiones servidor web



Se procede a realizar un escaneo de las conexiones utilizando Wireshark y se observa que desde una maquina cliente con ip 192.168.0.12 se procede a realizar el envio de datos hacia la ip 192.168.0.21 mediante http utilizando el método post como se observa en la imagen superior.

Figura 39 Captura de credenciales



Al revisar el contenido del paquete capturado por Wireshark se observa que el método post mediante el uso del protocolo http usando el puerto 80 envía todo el contenido en texto plano, o sea sin realizar un proceso de cifrado de la data enviada y de esta forma se observa que el atacante ha podido capturar de una manera muy sencilla credenciales de inicio de sesión a un sistema informático y de esta forma comprometer la información del sitio dependiendo los privilegios con los que cuente la sesión capturada.

11.4 Ataque de Ingeniería Social

la Ingeniería social hoy en día corresponde a técnicas en las cuales no implican acceder a los sistemas de información tratando de vulnerarlos por ataque de fuerza bruta o tratando de escalar privilegios realizando procesos de scanning o enumeración de vulnerabilidades, los atacantes se han dado cuenta que en muchas ocasiones la forma más efectiva de obtener información confidencial es atacar el

eslabón más débil de la cadena, que viene siendo el usuario final, por dicha razón el atacante que conoce de técnicas de persuasión directa e indirecta para poder engañar a su víctima y ganar su confianza, por lo cual se procederá a describir un ataque común de ingeniería social al cual se vería expuesta una empresa de mediano o pequeño nivel:

basado en la experiencia en el campo laboral se ha concluido que los pequeños y medianos negocios no cuentan con protocolos de seguridad en el acceso de visitantes por lo cual en primera instancia usando técnicas de footprinting o reconocimiento se puede navegar en la red buscando información relevante acerca del objetivo, buscar datos de una persona importante de la compañía para que en mi primer acercamiento con una posible victima pueda saber con qué temas abordarla y tratar de confundirla, como se explicaba algunas empresas no cumplen con protocolos de seguridad en acceso a visitantes por lo cual la secretaria está en la entrada en una recepción a la que posiblemente lleguen muchas personas a entregar correspondencia u encomiendas de diferente tipo para otras áreas de la compañía un error muy común es que el equipo de dicha secretaria posiblemente está conectado a toda la red que muy probablemente no está segmentado por Vlans y los sistemas contra intrusos no son muy robustos, a lo el atacante se podría hacer pasar como un mensajero que viene a entregar una encomienda o como un cliente que viene a reunirse con una persona que con antelación se sabe que no está presente en ese momento y ganándose la confianza de la secretaria se le pide que le permita un momento su equipo para descargar el documento que lo acredita como visitante autorizado o que si lo puede imprimir de la usb que el atacante trae previa manipulación de los iconos puede ser un pdf pero en realidad es un .exe para que ella cuando lo ejecute ingrese el código arbitrario que el atacante necesita posiblemente instalando un troyano que contenga un keyloger y se cierre después de haberlo ejecutado sin ejecutar ninguna acción adicional y proceder a decirle a la víctima perdón pero posiblemente ese no es el documento y solicitara regresar después con la copia ya impresa, en algunos casos como se comentaba en

empresas pequeñas dicha secretaria no le dará importancia al hecho y si lo informa dirá que vino una persona a preguntar por tal otra y que no estaba pero que regresara después cuando esté presente y trayendo el documento de autorización, lo que no saben es que el equipo de la recepción tiene instalado un keyloger y muy probablemente uno de sus puertos se encuentra abierto y a la escucha de peticiones que le permitan al malware instalado generar comunicación remota con su administrador y comenzar a enviar los datos capturados por teclado y empezar a conocer de qué manera poder empezar a ganar más acceso dentro de la red en busca de poder acceder a las bases de datos o que dentro de los datos capturados se tengan números de cuenta tarjetas o contraseñas que le permitan al atacante obtener lo que busca con el mínimo de riesgo de ser descubierto.

12. SUGERENCIA DE FORTALECIMIENTO DEL SISTEMA BASADO EN LAS VULNERABILIDADES ENCONTRADAS

En primera instancia se encontraron vulnerabilidades en el servicio de FTP para compartir archivos en un servidor Windows 2008 server, lo cual deja como conclusión que en los servicios hoy en día no se recomienda usar FTP en un entorno de red LAN y mucho menos en servicios que sean expuestos a internet, por tal razón para solucionar este inconveniente existen dos vertientes a tomar en cuenta de las cuales se expondrán sus principales fortalezas y características para lograr tomar la decisión de la mejor alternativa a implementar.

12.1 FTPS

FTPS es una de las variantes del protocolo FTP utilizadas para la transmisión de datos de forma segura y cifrada por la red. En este protocolo, cada camino implica el uso de una capa SSL / TLS por debajo del protocolo FTP estándar para cifrar la información de control del servidor y/o los canales de datos.

12.1.1 Ventajas de FTPS

Muy conocido y ampliamente utilizado.

El método de comunicación entre cliente y servidor puede ser leído por el usuario.

Permite transferencia de archivos servidor-servidor sin necesidad de un cliente.

SSL y TLS ofrecen algoritmos de autenticación seguros.

FTP a través de SSL y TLS es muy utilizado en muchos ámbitos de Internet.

12.1.2 Inconvenientes de FTPS

Algunos problemas con el listado de directorios.

Requiere un canal secundario de comunicación, lo que puede generar algunos problemas con cortafuegos.

No tiene un estándar de codificación de caracteres.

No todas las conexiones SSL son compatibles con FTP y TLS.

12.2 SFTP

SFTP es otra variante del protocolo FTP para la transmisión de datos segura. Se utiliza habitualmente con el protocolo SSH para proporcionar dicha transferencia segura de archivos, aunque también puede utilizarse con otros protocolos de transferencia de datos seguros.

12.2.1 Ventajas de SFTP

Dispone de estándares que definen perfectamente la mayoría de las operaciones.

Utiliza únicamente una conexión, sin necesidad de establecer conexiones adicionales.

Conexión siempre asegurada.

Directorios legibles por la máquina.

Incluye operaciones de autorización, atributos, permisos, bloqueo de archivos y más funciones adicionales.

12.2.2 Inconvenientes de SFTP

La comunicación se realiza en binario. Es muy complicada de comprender para un usuario.

Las claves SSH son complicadas de configurar, validar y gestionar.

Puede generar algunos problemas entre aplicaciones al no tener un estándar definido.

No permite copia de servidor a servidor.

No permite el borrado recursivo de directorios.

Algunos sistemas no son compatibles con SSH / SFTP

Para finalizar, recordar que tanto FTPS como SFTP nos garantizan una seguridad adicional para la transmisión de datos, pero a cambio nos van a consumir bastantes recursos adicionales de nuestro sistema y se va a reducir notablemente la velocidad de transferencia ya que depende tanto del emisor como del receptor el hecho de cifrar y descifrar tanto las comunicaciones como los datos recibidos.

12.3 Conclusiones de solución FTP

Según las características observadas de las dos posibles soluciones y en cuanto a la experiencia desarrollada por el profesional de seguridad se recomienda la implementación de SFTP como la opción más adecuada en cuanto a seguridad, flexibilidad, robustez y confianza que ofrece la transmisión de datos usando SSH como protocolo base.

12.4 Implementación De Https

Concretamente relacionado con el protocolo HTTPS, este es el protocolo utilizado para la transferencia segura de datos de Hipertexto. Por su siglas en ingles HTTPS es “Hyper Text Transfer Protocol” la letra ‘S’ añadida al final, viene hacer referencia con “Secure Sockets Layer” (SSL), en pocas palabras el protocolo de seguridad que utiliza el navegador para transmitir información de forma segura.

Anteriormente este protocolo de seguridad sólo se aplicaba en sitios web de comercio electrónico y banca, debido a que por su naturaleza requieran mayor seguridad para evitar la fuga de información (tarjetas de crédito).

12.4.1 Ventajas del HTTPS

Por supuesto la primera ventaja de este nuevo protocolo es la seguridad para el usuario, especialmente en una sociedad donde las compras online, transferencias de dinero y operaciones bancaria son cada vez más comunes. Ofrecer HTTPS garantiza 100% autenticación del usuario, se evitan futuras suplantaciones, spammers y fuga de archivos confidenciales.

12.4.2 Desventajas del https

Al realizar una migración de protocolos, es muy posible que si esta se implementa de forma errónea los resultados orgánicos bajarán notablemente en las SERPs, es decir, perder posicionamiento en Google.

El certificado SSL requiere un manejo de la información en dos sentidos, primero encriptación y luego des encriptación, este tipo de labores aumentará la carga de la web y por consiguiente el rendimiento del sitio.

Se debe renovar el certificado HTTPS periódicamente lo cual implica una inversión más de dinero. También implica un poco de trabajo pues se debe realizar mantenimiento periódico de Open SSL y las bibliotecas TLS.

Implementar un correcto re direccionamiento 301 de http a htpps, es decir, se debe crear una regla en .htaccess que permita redirigir de forma correcta todas las URLs ya que de lo contrario arrojará error 404 y por lo consiguiente un sinfín de errores de servidor aparecerá en elWeb master Tools.

12.4.3 Puntos vitales para establecer el https correctamente

Antes de comprar el protocolo https se debe verificar que cuenta con certificados de 2048 bits, este es el recomendado por Google. Se debe Contratar el servicio solo con compañías fiables y reconocidas en el sector.

Definir previamente el tipo de certificado que se necesita, por regla general se utiliza el protocolo single para dominios del tipo www.dominio.com, también multi-domain para dominios como el anterior, cdn.dominio.com o en su defecto www.dominio.es)

Por último se encuentra el certificado wildcard certificate utilizado para los sitios que poseen demasiadas Url dinámicas como pueden ser a1.dominio.com, b2.dominio.com, c3.dominio.com, etc.

Recordar utilizar un servidor web que soporte HSTS (HTTP estricto) y además que este se encuentre activado, lo anterior lo se puede consultar directamente con el proveedor del Hosting o realizando un PING en php.

Es importante la fecha de caducidad del protocolo, una fecha vencida genera un error de seguridad que mostrará la URL como una posible suplantación del sitio web.

12.5 recomendaciones prevenir ataques de Ingeniería Social

las recomendaciones a realizar con este tipo de ataques así como con la mayoría del malware, es primero capacitar al personal de la compañía, exponerles los riesgos a los cuales están expuestos, se debe tener en cuenta que en muchas ocasiones el atacante puede ser alguien de la misma compañía por lo cual le sería más fácil este tipo de técnicas, controlar el acceso de medios extraíbles en estaciones de trabajo que puedan ser acezadas por personal no autorizado y tener especial énfasis en aquellas estaciones que son manejadas por personal no técnico, cumplir con los protocolos de acceso establecidos dentro de la seguridad física como uso de cámaras medios biométricos si es posible, validación de identidad de visitantes entre otros, y siempre teniendo la precaución de no entregar información que pueda empezar a comprometer la seguridad de la empresa.

13. CONSOLIDACIÓN GENERAL DE SUGERENCIAS

Para evitar este tipo de ataques se debe implementar seguridad en las primeras capas del modelo tcp/ip

1. a nivel físico no deben haber puntos de red accesibles para que cualquiera conecte un equipo
2. a nivel de capa 2 se deben configurar políticas de seguridad en los switches para que identifique los equipos por mac y si algún equipo nuevo se conecta y no está dentro de sus tablas de mac no le permita tener acceso a dirección ip
3. se deben aplicar acl en los switches y en los routers para que nadie ponga sus tarjetas de red en modo promiscuo y así escanee otro tipo de trafico diferente al que viene hacia cada uno
4. no se deben tener servicios como telnet, ftp, http ya que no cuentan con ningún tipo de seguridad y todo lo que se envía va en texto plano y en este caso en particular se pudieron capturar credenciales de acceso a un servidor con lo cual se puede empezar a explotar más vulnerabilidades en ese servidor que terminen comprometiendo toda la red.

5. Implementar buenas prácticas en cuento a evangelización de los usuarios para que eviten ser víctimas de ataques de ingeniería social y también comprometan información confidencial hacia un atacante.

6. Por encima de la interfaz, podríamos restringir direcciones de origen fuera de su rango válido, esto evitará que alguien en nuestra red envíe tráfico spoofeado a Internet.

7. Es importante que no se permita la salida de ningún paquete que tenga como dirección IP de origen una que no pertenezca a su subred.

8. El cifrado y la Autenticación: la Realización del cifrado y la autenticación también reducirán amenazas de spoofing. Estas dos características están incluidos en Ipv6, que eliminará las actuales amenazas de spoofing.

14. BIBLIOGRAFIA

[1] Autor, A. A Instituto de Ciberseguridad de España “análisis de tráfico con Wireshark “ https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

[2] Autor, A. A. Ana Laura Hernández Saucedo “Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web

http://recibe.cucei.udg.mx/revista/es/vol4-no1/computacion05.html

[3] Autor, A. A. Cesar Augusto Mejía Londoño universidad tecnológica de Pereira vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo osi en las redes de datos de las organizaciones http://recursosbiblioteca.utp.edu.co/tesisd/textoyanexos/0058R173.pdf

[4] Autor, A. A Net Cloud Ingeniering Amenaza vs. Vulnerabilidad https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/

[5] Autor, A. A Departamento de seguridad Informatica Amenazas a la Seguridad de la Información

http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[6] Autor, A. A Eugenio Picón Prueba Pericial Informatica https://peritoinformatico.es/prueba-pericial-informatica/

[7] Autor, A. A Ciberseguridad.net Pentesting https://cyberseguridad.net/index.php/pentesting

[8] Autor, A. A Smartekh Qué Es Hardening http://blog.smartekh.com/que-es-hardening

Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web

http://recibe.cucei.udg.mx/revista/es/vol4-no1/computacion05.html Autor, A. A. Ana Laura Hernández Saucedo Citado 1, ***Febrero 2015***

Auditando con Nmap y sus scripts para escanear vulnerabilidades
https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear vulnerabilidades/Autor, A. A. Ignacio Pérez Citado 12 Feb 2015

Sitios para practicar y aprender hacking
http://www.blog.andaluciaesdigital.es/sitios-para-practicar-y-aprender-hacking/
Autor, A. A. blog de Andalucía Citado Feb 2016

las mejores distros utilizadas por hackers
http://adictec.com/las-mejores-distros-utilizadas-por-hackers/
Autor, A. A. adictec Citado jun 2015

Ataques informáticos Debilidades de seguridad comúnmente explotadas
https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf
Autor, A. A. Jorge Mieres Citado enero 2009

Diferencias entre SFTP y FTPS
https://www.adslzone.net/redes/windows/lan/diferencias-entre-ftps-y-sftp/
Autor, A. A.adsl zone marzo 15 de 2016