UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

EVALUACIÓN DE TÉCNICAS DE ETHICAL HACKING PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD INFORMATICA EN UNA EMPRESA PRESTADORA DE SERVICIOS

PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor
Bach. Durand More, Andrés David
ORCID: 0000-0002-4076-0982

Asesor
Dr. Mario Ramos Moscol
ORCID: 0000-0003-3812-7384

Línea de Investigación

Infraestructura, Tecnología Y Medio Ambiente

Pimentel, Perú 2019

“EVALUACIÓN DE TÉCNICAS DE ETHICAL HACKING PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD DE INFORMATICA EN UNA EMPRESA PRESTADORA DE SERVICIOS”

Aprobación del informe de Investigación

Bach. Durand More, Andrés David
Autor

Dr. Mario Ramos Moscol
Asesor

Mg. Bravo Ruiz Jaime Arturo
Presidente de Jurado

Ing. Díaz Vidarte Miguel Orlando
Secretario(a) de Jurado

Ing. Atalaya Urrutia Carlos William
Vocal de Jurado

DEDICATORIA

Dedicado a mis queridos padres, ya que con su apoyo me han cuidado por mi bienestar y educación, poniendo su confidencia en cualquier desafío que se presentó en la vida y que no dudaron en mi inteligencia y capacidad, motivándome siempre para alcanzar mis anhelos.

El autor

AGRADECIMIENTO

En primer lugar, agradecer por los resultados obtenidos en este proyecto, y están dedicados a las personas que formaron parte de su culminación.

Mi agradecimiento más sincero a mis queridos padres por ayudarme, orientarme y apoyarme en la culminación de este sueño muy importante.

Quiero agradecer a mi asesor de tesis, el Dr. Mario Ramos por su orientación académicamente cada vez que era necesario sin el cual no hubiese podido salir adelante.

Finalmente, un agradecimiento a esta prestigiosa universidad, por abrir sus puertas a los jóvenes como yo, preparándome para un mejor futuro competente y formándome una persona de bien.

El autor

RESUMEN

La presente investigación realizada ha tenido como objetivo evaluar técnicas de Ethical Hacking ejecutando pruebas de penetración sobre la seguridad informática de una red de datos que permitan el diagnóstico de vulnerabilidades en una empresa prestadora de servicios.

La presente investigación, es de tipo cuantitativo y de diseño cuasi experimental, dado que se tomarán resúmenes de herramientas de hacking ético en determinados momentos sobre la red de la empresa prestadora de servicios. La muestra para la investigación fueron los dispositivos conectados en la red de la empresa prestadora, se trabajó directamente con un equipo autorizado con acceso directo a toda la red, con el fin de optimizar resultados que, al ser procesados, se concluyó que existen vulnerabilidades en la red actual de trabajo.

Concluyendo que en la presente investigación existen políticas y normas de mitigación de vulnerabilidades, tanto físicas como lógicas que se deben implementar con el fin de disminuir fallas en la red y acceso a intrusos para el perjuicio de la documentación existente en la empresa.

Palabras clave: detección de vulnerabilidades, amenazas, seguridad informática, Hacking ético.

ABSTRACT

The investigation was aimed at evaluating Ethical Hacking techniques by executing penetration tests to the security of a data network that allows the diagnosis of vulnerabilities in a service provider.

This research will be quantitative and of a quasi-experimental design, since summaries of ethical hacking tools will be taken at certain times on the network of the service provider. The sample for the investigation was the devices connected to the local network of the company, we worked directly with an authorized workstation with direct access to the entire network, in order to optimize results that when processed, it was concluded that there are vulnerabilities in the Current network of work.

Concluding that in the present investigation there are policies and norms of mitigation of vulnerabilities, both physical and logical that must be implemented in order to reduce network failures and access to intruders for the damage of the existing documentation in the company.

Keywords: vulnerability detection, threats, computer security, ethical hacking.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

I. INTRODUCCION

1.1. Realidad problemática

Internacional

Muchas de las empresas a nivel mundial públicas y privadas, entre ellas se encuentran las empresas prestadoras de servicios, tienen lugares físicos que trasfieren la información en volúmenes mínimos y máximos, sin embargo el alto crecimiento del desarrollo tecnológico, tiene un impacto o evolución en las empresas, gobierno y entidades, tal es así que existe un incremento en número de ataques en los últimos años por parte de hackers que afectan a los usuarios de Internet y, por consiguiente, la pérdida de información muy valiosa.

Pues inicialmente los ataques o penetraciones que había fueron mínimos, pues se conseguía la ralentización del equipo; posteriormente empezaron a malograr sistemas totalmente completos, luego se borraba los archivos o extraía información muy confidencial sobre dichas empresas. Ante ello a efectos de proteger los sistemas, el administrador debe cumplir un papel importante ya que restringen al máximo los accesos a los equipos informáticos, es así consecuentemente los crackers dieron inicio a los ataques mucho más destructivos y estructurados.

Según (Peiris & Armstrong, 2014), menciona son más importantes de una empresa. Pues muchos de los activos se manipulan ahora por sistemas computarizados, hasta bases de datos. El mal uso de los sistemas, que se emplean no están debidamente capacitados, ya que son el lugar débil en toda empresa, otro punto importante favorable para la competencia", añade. "es importante tratar de advertir; buscar vulnerabilidades a fin de tomar las medidas correspondientes y de esta manera prevenir un incidente". Por otro lado, dice que "es necesario tener un compromiso a efectos de proteger la información a cualquier nivel ya sea empresarial o social, razón por la cual, las empresas pequeñas, medianas y grandes usan toda clase de dispositivos electrónicos, sin embargo se debe hacer un análisis de vulnerabilidades, luego de un semestre o de manera anual", es conveniente se realicen las pruebas de penetración con la finalidad de avalar una mejor seguridad para a la empresa, Igualmente, hay muchos casos de espionaje industrial, lo cual se dan a través de las técnicas de Ethical Hacking, lo cual se busca sacar provecho de esa información

Para equilibrar esto ha surgido el Ethical Hacking, que sirve para detectar las debilidades. Esto permite que a las empresas puedan prepararse ante posibles riesgos que por lo general los sistemas se encuentran expuestos y deben ser conscientes del valor de cuidar el mínimo detalle. Así mismo las debilidades pequeñas permite a los atacantes organizar ataques con la finalidad de penetrar y efectuar todo tipo intervención. Entonces de esta manera se obtiene información es muy útil de las organizaciones, y es muy útil para la toma de acciones preventivas contra posibles intrusiones maliciosas. Bajo ese escenario, los hackers éticos realizar escenarios de prueba y realizar ataques (pen-testing), en efecto, la seguridad informática garantiza y determina que el uso de esta herramienta es de mucha utilidad y ayuda a prevenir y proteger la información, sin embargo las empresas deben ser conscientes de la gran importancia de la seguridad y cuán importante también es en los sistemas financieros en la actualidad, ya que es un punto más vulnerados en las empresas.

Realmente muchas empresas se sienten preocupadas ya que quieren por evitar los casos de fraude. Muchos de los casos de phishing, se dan generalmente por infecciones de malware, pero son menos preocupantes para las empresas, a diferencia de los ataques de denegación de servicios.

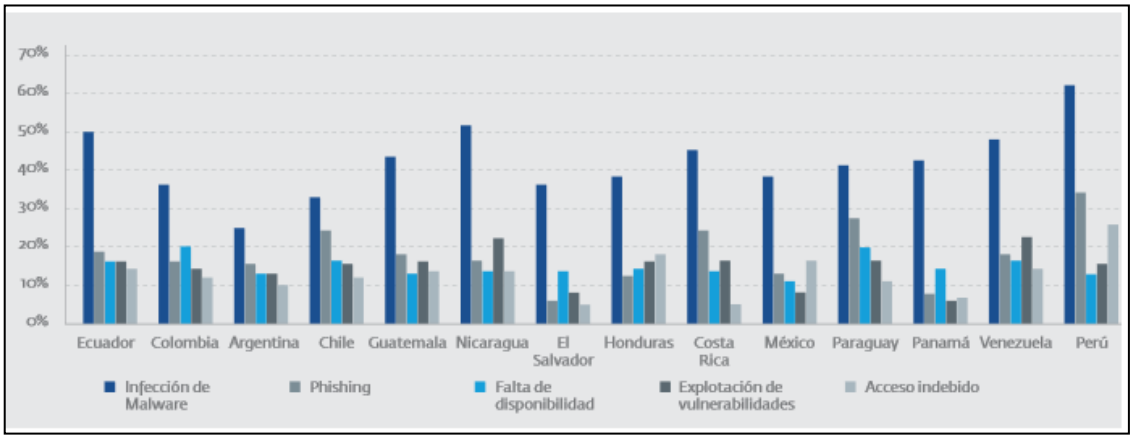


Figura 1: Nivel de Vulnerabilidad a nivel de Latinoamérica
Fuente: (Symantec Security Response, 2013)

Nacional

Por su parte (Cruz Saavedra, 2014). En Trujillo, en su artículo indica que los incidentes más significativos fueron la infección de Malware, phishing, accesos indebidos, explotación de vulnerabilidades y falta de disponibilidad en ese orden respectivamente. Sin

duda nuestro país no es ajeno a estos ciber-ataques, las empresas conocen de los riesgos que los ciber-ataques representan para sus operaciones, productividad y prestigio para sus negocios. Es por ello que, ahora la ciberseguridad es fundamental para la protección de los equipos o sistemas de información.

Dicha visión arbitraria en la gestión de la seguridad informática hace que éste crucial activo y sea desatendido. En el Perú, esta falta del mismo puede verse manifestado en los niveles bajos de la seguridad que presenta nuestro país frente a otros de Latinoamérica y Caribe. Según el estudio de The Business Software Alliance, el 65% de software utilizado en el Perú es ilegal, por lo que en términos más prácticos podríamos decir también que, uno de cada cuatro software es pirata e infectado por virus, arriesgando la información al hurto o pérdida. Esto significa que, a pesar de que las empresas están implantando políticas de seguridad informática, se tiene que lidiar con este desbalance y trabajar mucho más para mejorar los estándares.

En el Perú, las empresas mucho comprometen la continuidad de sus operaciones ya que es un problema que afecta al mínimo y estas dependen de sus redes informáticas. Si bien las insuficientes medidas de seguridad en las redes específicamente en los servicios de red de datos, se ha generado un problema que va en crecimiento. Hoy en día los atacantes consideran que las organizaciones ya tienen un mejor orden y están más organizados, y diariamente van ganando habilidades con la finalidad que permitan tener mayores beneficios.

Local

Las empresas prestadoras de servicios poseen información valiosa para el desempeño de sus funciones, los cuales no han sido sometidos al tipo de técnica de “Ethical Hacking” para diagnostica o detectar vulnerabilidades, a medida de que se realiza el análisis se van presentando niveles de vulnerabilidad, uno de ellos por ejemplo un nivel alto de vulnerabilidad, está expuesto en un riesgo la información que puede ser alterada o robada en su totalidad, finalmente todo ello tiene un impacto positivo o negativo especialmente en el control de la información la misma que esta es el centro de cualquier empresa o institución,

estas vulnerabilidades detectadas, son utilizadas por el personal externo o de la misma organización.

Es por ello que se ha visto la necesidad de realizar una evaluación de las técnicas de hacking ético para evaluar, diagnosticar vulnerabilidades en la seguridad informática, con el único objetivo de evaluar las técnicas, identificarlas, clasificarlas y mitigarlas sobre una red de datos y de esta manera poner de una red de datos más eficiente y que garantice y sea segura ante los diferentes ataques de intrusos o terceros.

1.2. Antecedentes de Estudio

Internacional

Según (Oñate & Martinez, 2017)**,** nos informa que en el presente proyecto de investigación tuvo como objetivo investigar la seguridad de la información de todos los elementos implicados en el proceso, provisión o envío de la información en el Gobierno Provincial de Imbabura. Se hizo uso de la norma ISO/IEC 27001:2005 la misma que sirvió como una guía en el desarrollo de todas actividades detalladas en la presente investigación con la finalidad de realizar la implementación un sistema de gestión de seguridad de la información.

La citada norma estableció tres requisitos fundamentales que permitan realizar un buen análisis del diseño del sistema de gestión de seguridad de la información, como primer requisito fue realizar un inventario de todos los activos de información del Gobierno Provincial de Imbabura, tomándose mucho énfasis a la data center que funcionaba el centro de operaciones y procesamiento de la información del Gobierno Provincial. Así mismo se realizó la técnica de Hacking Ético, la misma que consistió en una perspectiva black-box (caja negra), realizando detecciones de vulnerabilidades, por otro lado, en el Gobierno existe mucho desconocimiento sobre los sistemas a evaluar y gradualmente en varios procesos para descubrir las características del equipo y las principales vulnerabilidades encontradas. De tal forma se intenta hacer un ataque de hacking Ético, el mismo que desde cualquier lugar del mundo, se puede hacer con intenciones maliciosas. Otro objetivo fue ya una vez que se han identificado los problemas se procedió a elegir los mejores controles para la norma ISO/IEC

27001:2005, en la presente investigación también le permitió realizar un tratamiento del riesgo a todos los activos de la información del Gobierno Provincial de Imbabura, como también se implementó otro tipo de controles que permitan garantizar a través de políticas de seguridad la custodia de la información del gobierno.

Según (Hurtado & Mendaño, 2016), en dicha investigación uno de sus objetivos es medir de manera estratégica las defensas de los sistemas informativos de dicha institución, a la vez se realizaron una serie de recomendaciones con el fin de mitigar las fallas encontradas, y por lo general ayudan a la creación de un plan de mitigación; además es muy importante recordar ya que les permite descubrir errores y es una gran ventaja evaluar o intenten vulnerar los sistemas informáticos. Pero hay que tener en cuenta que estas personas muchas de ellas se dedican a evaluar todo tipo de vulnerabilidades con el propósito de ser un Hacker Ético, lo cual le permite poner en evidencia las correcciones y mejorar de una u otra manera la seguridad de cualquier persona natural u organización, todo ello mediante una evaluación rigurosa de la seguridad perimetral, de los resultados obtenidos de la presente investigación se detectaron fallas en ciertos sistemas, lo cual le permitió al investigador recopilar de la información de manera eficiente, así mismo se identificaron los servicios, protocolos, accesos mediante autenticación por defecto, etc. Tener una adecuada administración de redes de datos nos permite realizar todo tipo de actividades de manera periódica, de esta manera no se evidencia el tráfico de red.

Según (Acosta, 2013), tuvo como objetivo: mencionar que las personas responsables de la SNGR, tienen mayor riego y con más probabilidad de amenazas, sin embargo estas pueden ser reducidas o controladas actuando con la implementación de medidas preventivas que cada organización necesita. Concluyó que, los puertos abiertos y servicios se encontraron activos de manera innecesaria y no son útiles por los servidores DNS0, DNS1 y por el Firewall, del análisis se pudo identificar que un servidor forma parte del Firewall, representando un alto nivel crítico, y que carece de políticas y procedimientos de seguridad, por otro lado, se observa tecnológicamente su infraestructura también carece de medidas preventivas para la identificación de malware o intrusos para los Host y RED, NI CUENTA CON UN Sistema Anti-Virus para el Firewall, con este riesgo la red y la infraestructura se encuentra en riego y está expuesta a posibles intrusiones de programas maliciosos; exponiendo a introducir en todo tipo de virus o al robo de información en las diferentes áreas.

Nacional

Según (Aguilar & De la Cruz, 2015), comunica en ese tiempo ha logrado ampliar su mercado, posicionarse y competir con otras entidades financieras en dicha provincia. Su principal característica son sus intereses bajos, su atención de primera y personalizada, de tal manera que tiene enlace a nivel nacional. Dicha entidad utiliza los sistemas y aplicaciones web, lo cual manejan información en grandes cantidades, la misma que tiene carácter riesgoso y confidencial, pues esta información de acuerdo al investigador es transmitida mediante una red informática con la mayor posibilidad en seguridad, de esta manera reducir al más mínimo riesgo informático. Pues dicha implementación tuvo como objetivo principal en la investigación mejorar la seguridad en la transferencia de datos.

Según (Fernández & Pacheco, 2014), En esta investigación se pudo hacer análisis y plan demostró que si es factible minimizar los riesgos, amenazas y vulnerabilidades a un 73% de todos los activos de información. donde se logró utilizar un 25% de controles de la citada norma con la finalidad de elaborar el Plan de Sistema de Gestión de Seguridad de la Información para la Comandancia de Operaciones Guardacostas. Se efectuó el análisis al 100% de Riesgos de información focalizados en el momento de realizar el análisis Situacional, la presente investigación se realizó en distintas áreas SIMTRAC, COSPAS y SARSAT de la Comandancia, tal es así que se pudo medir el impacto a los riesgos en dichas áreas, encontrándose que el 48% de activos de la información son vulnerables de acuerdo a la evaluación selectiva efectuada.

Según (Bermeo, 2017), nos comenta que tuvo como objetivo: efectuar una Implementación de Hacking Ético; como medio de ayuda en la detección y evaluación de vulnerabilidades de red de datos; se ha realizado el análisis, utilizando herramientas tecnológicas para la seguridad, de la actual red de datos– Tumbes; por lo que se ha evaluado los problemas de vulnerabilidad a los que se encuentra expuesta la red y; es importante mencionar que el investigador formulo la propuesta tecnológica de seguridad, la misma que logrará estableciendo políticas de comunicación.

Según (Gonzales, 2016)**,** tuvo como objetivo: usar herramientas de Hacking, permitiéndole diagnosticar vulnerabilidades en una red de datos de la universidad de Huánuco, teniendo como escenario su Sede principal, pudo concluir que, la metodología aplicada y utilizada para evaluar vulnerabilidades, es versátil, de mucha utilidad y muy confiable, pues se conserva un marco organizado y claramente definido, mostrando resultados favorables en el periodo y dentro de su proceso de detección, asimismo para llevar adelante las pruebas de penetración el personal cuenta con una experiencia suficiente que asegurara un proceso transparente y teniendo resultados garantizados al termino de la evaluación de vulnerabilidades. En ese sentido en el proceso de la fase de explotación, cuyo proceso es importante a fin de determinar que tanto se encuentra expuesto la web, los datos, y la red pública de manera general, en efecto pues nos permite ver una perspectiva externa a la universidad, por ejemplo de la información encontrada podemos observar que un falso positivo no indica que dicha vulnerabilidad no exista, a la vez se pudo comprobar que la herramienta utilizada no lo comprobó, asimismo, en un test de penetración, es necesario tener muy en cuenta que no se puede brindar una solución ni convertir la red o web, no vulnerable, pues el día a día la información se vuelve muy vulnerable, considerando los diferentes intentos de mantenerlo protegido y del buen uso de los beneficiarios y los grandes avances de la tecnología de los últimos tiempos.

Local

Según (Niño, 2018), La presente investigación utiliza el modelo PDCA y la metodología Magerit VS 3, se explica el caso de estudio a ODEI Lambayeque, es por ello que es necesario establecer normas y procedimientos con el fin de preservar los activos más fundamentales para el éxito de la institución, que tanto carece la institución, dicho sistema propone mantener la confidencialidad, integridad y disponibilidad de los activos de información, es por ello que para el desarrollo del sistema se eligió la citada norma sirviendo de guía para desarrollar el caso de estudio.

En las conclusiones se pudo verificar que se aplicó la metodología MAGERIT, lo que permitió conocer las amenazas a las cuales se encuentra expuestas los activos de

información en ODEI Lambayeque, esto después de un análisis de riesgos de orden cuantitativo en el cual se concluyó que el nivel de madurez en cuanto a seguridad de la información en la institución era muy bajo. Asimismo, se pudo corroborar que, la norma NTP ISO/IEC 27001:2014 es una solución al problema ante la ausencia gestión de seguridad de la información en ODEI Lambayeque, ya que es una metodología basada en el estándar internacional ISO/IEC 27001:2013; permitiendo implementar un sistema de gestión en la institución con el objetivo de establecer y mantener un ambiente razonablemente seguro para poder fortalecer las salvaguardas en cuanto a confidencialidad, integridad y disponibilidad de los activos de información, así como fortalecer el monitoreo en los procesos CORE de la institución.

Según (Fernández C. , 2017), La presente investigación tuvo como objetivo efectuar pruebas de rendimiento y seguridad, primeramente ha procedido al análisis de transferencia de registros, bajo el patrón Cliente/Servidor VPN, teniéndose previsto las diferentes longitudes de archivos. Como parte de las conclusiones finales de esta investigación se evidenció que la ejecución de RPV, es conveniente desde varios factores ya sea de seguridad, de confiabilidad y económico, etc., trayendo consigo usuarios asociados a la conexión remota y distantes, en efecto se debe considerar la sobrecarga por utilizar la VPN pues no influye significativamente en la red de datos.

Según (Maco, 2008)**,** En la presente investigación el investigador sostiene que del análisis efectuado a la Caja Sipán de la ciudad de Chiclayo en relación a la seguridad de su información que custodia, se pudo encontrar que dicha Caja no cuenta con equipos que se dediquen a realizar análisis y hacer seguimiento, tal es así que dicha Entidad debe contar con un plan para un seguimiento y control. Por otro lado, existen otros problemas encontrados en la Caja Sipán, como es la disconformidad en relación a los equipos y su calidad que respalde la seguridad de la información. Así también la Caja Sipán tiene un plan de seguridad, pero no está implementado con las respectivas políticas de seguridad y es mas no era de conocimiento del personal. Ahora bien, las faltas o problemática conllevan a la organización a pérdidas cuantificables en grandes dimensiones. Sin embargo, estas políticas no son de conocimiento de los colaboradores. Sobre este escenario se concluye que el problema principal de la organización es la falta de plan de seguridad, supeditado a las

normas de calidad que avalen la seguridad, integridad, confiabilidad de la información en dicha empresa".

1.3. Teorías relacionadas al tema

Según (López, 2015). Seguridad informática hace referencia a una práctica de defensa a las computadoras y servidores, los sistemas informáticos, los dispositivos móviles, y electrónicos, la seguridad permite identificar y eliminar vulnerabilidades en las redes, siendo esto la habilidad ante cualquier ataque malicioso.

La Seguridad informática es un campo muy amplio, y va ligado estrechamente al concepto de seguridad. Su propia definición de informática menciona que el principal activo es la información, y como tal tiene poder. Por lo tanto, se puede concluir que todas las técnicas, métodos, procesos, almacenamientos, transmiten y realizan procesamiento de la información y de esta manera implementar de forma segura y también protegiendo la información de cualquier organización. Pues la seguridad juega un papel importante el día a día ya que se convierte en algo indispensable y primordial, es por ello que en la actualidad las compañías con redes, deben contar con políticas de seguridad y que permita tener direccionamiento a una buena coordinación y conveniencia.

Por otro lado, tiene como objetivo implantar reglas para ayudar a reducir riesgos a su infraestructura, como también a la información en general.

Red informática

Cuando hablamos de una red informática, hacemos mención a los dispositivos interconectados, en la cual intercambian recursos compartidos y de información. Esencialmente, se basa a una red informática la comunicación que circula dentro de la misma, siendo un proceso con roles definidos, estos ayudan a conectar, emitir y recibir información en distintos instantes de tiempo.

Según (Dias, 2014), Para crear una red, es importante un hardware para realizar un enlace entre los dispositivos, por ejemplo las tarjetas, cables y otros, y al software, es quien

efectúa las regulaciones de comunicación entre los mismos, vale decir, protocolos y servicios entre otros (PAN, LAN, WLAN, CAN, MAN, WAN, VLAN).

1.3.1. El Modelo OSI

El modelo OSI utiliza capaz estructuradas y estas se dividen en siete a efectos de realizar las actividades en la red de datos. Sin embargo, para cada capa une varios protocolos. El modelo OSI maneja principalmente el diseño y la ingeniería para las soluciones de red. Por otro lado, para las organizaciones estas capas son representadas en las operaciones a nivel de tipo de transferencia de datos, mediante una red.

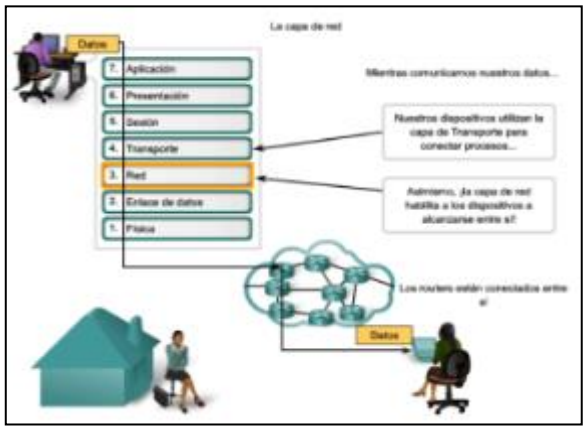


Figura 2 El Modelo OSI
FUENTE: Universidad de México

El Modelo OSI de red separa los métodos y protocolos necesarios para una conexión de red en siete capas, las mismas que detallamos a continuación:

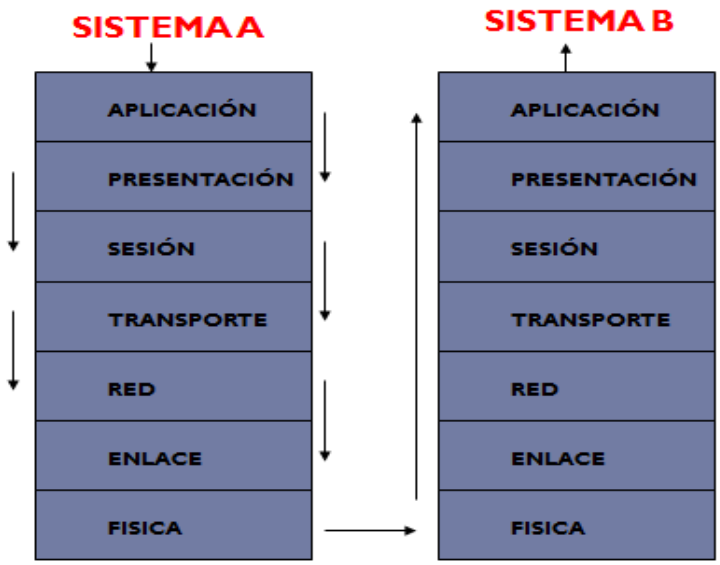


Figura 3 El Modelo OSI por capas
FUENTE: Elaboración Propia

- **Capa Física o Capa 1**

Esta capa es la más sencilla y se encarga de la topología, su función primordial es tener definición de los componentes analógicos que hay en la red y garantizar la conexión, como se mencionó anteriormente la capa física es el elemento más básico ya que en esta solo convergen solo elementos físicos y no elementos lógicos lo cual requieren de interpretación para comprenderlos por completo.

A pesar que la capa física es la más simple es de suma importancia debido a que es la base de todo el modelo OSI, pues sin esta capa las demás no pueden funcionar.

1.3.2. Protocolos TCP/IP

En el año 70 fue desarrollada para ser utilizada en la red ARPANET, ya que fue la WAN implantada en los EEUU, en la actualidad TCP/IP es usada por cualquier dispositivo que quiera conectarse a internet.

Es formada por 04 capas o niveles, capa de acceso a la red, internet, transporte, aplicación, por ello las dos capas superiores solo se usan en el host origen y destino, las dos inferiores son las que permiten el tráfico de red.

Los protocolos constan de cuatro capas, que se detallan a continuación.

- **Capa de Acceso a la red**

El Modelo OSI, tiene la equivalencia de la capa de enlace de datos y la capa física, la capa de acceso a la red, es un nivel que no se define en el modelo, pues se menciona que se utiliza un enlace entre equipos, pues no se define ningún protocolo ya que se puede utilizar cualquiera como por ejemplo Ethernet, wifi, PPP, etc.

- **Capa de internet**

Esta capa es importante ya que de alguna manera esta arquitectura que define un funcionamiento basado en paquetes de manera que nos va a permitir un intercambio entre cualquier dispositivo conectado a internet ya que gracias a esta capa un paquete pueda llegar de un origen a un destino. Por lo cual su funcionalidad se basa en el canje de paquetes a través de una red, asimismo esta capa correspondería a la capa de red del modelo OSI, y usa un protocolo IP.

- **Capa de transporte**

Esta capa tiene como objetivo una transmisión de datos de forma óptima y libre de errores entre dos aplicaciones, por lo cual el nivel de transporte se va a encargar de segmentar en paquetes y enviarlos en un orden adecuado a su destino y asegurar que todos los correctos, así mismo correspondería a la capa de transporte del modelo OSI, y se pueden utilizar 02 protocolos, el protocolo TCP, que es totalmente fiable y el protocolo UDP que es muy rápido.

- **Capa de aplicación**

Esta capa tiene como objetivo dar servicios específicos a los usuarios a través de correo electrónico, mensajería, etc. Esta capa correspondería a la capa de aplicación, de presentación y de sesión del modelo OSI, y los protocolos como HTTP, SMTP, DNS, etc.

1.3.3. Los Puertos de red

Los puertos de red son aquellos que cuya función es comunicarse con un programa a través de una red, de acuerdo al modelo OSI corresponde a la capa de trasporte o capa 4, existen 03 tipos de puertos, los puertos conocidos, los puertos registrados y los puertos dinámicos o privados.

1.3.4. La Seguridad de la Información

Según (Niño, 2018), Define como un vinculado de acciones preventivas y reactivas, permite a las organizaciones o empresas resguardar y mantener protegidos sus sistemas informáticos, buscando la confidencialidad, la integridad y disponibilidad de la seguridad información a efectos de evitar cualquier intrusión, amenazas y vulnerabilidades o ataque malicioso.

La seguridad de la información y la tecnología se ha puesto a disposición del ser humano, de tal manera que sea más rápida y fácil y que trasmitimos mediante los medios informáticos, siendo cada día más necesario para nuestra existencia.

1.3.5. La Importancia de Seguridad de Información

Este tema muy importante ya que no está a conocimiento de muchos, para mucha gente u organización es normal pertenecer en redes sociales y publicar ciertas historias de su vida cotidiana, ya que mientras más conocidos sean y más amistades encuentren en las redes sociales más importantes se creen y es esta una "vulnerabilidad" lo que se está explotando ya que se está exponiendo a un riesgo.

Es importante la seguridad de la información debido al siguiente detalle:

- Proteger toda la información relacionada con las organizaciones, clientes, y personas de acceso no autorizados.
- Proteger la información de problemas legales a causa de fuga de datos importantes o confidenciales.

Por otro lado, según (Gómez & Andrés, 2012). Es importante la seguridad de la información ya que comprende varios aspectos como es la disponibilidad, la integridad, confidencialidad, identificar los problemas, hacer un análisis y recuperación ante cualquier riesgo.

1.3.6. Elementos de la Seguridad de la Información

Se caracteriza por sus tres elementos o pilares fundamentales, los cuales son confidencialidad, la disponibilidad e integridad. A continuación, hablaremos de forma resumida en tres pilares:

La Confidencialidad.

Este pilar asegura la información sea asequible solo para aquellos que estarán autorizados, pues la confidencialidad hace referencia a la necesidad de mantener u ocultar un secreto sobre una determinada información o recursos.

Se trata básicamente de la propiedad por la que esa información solo es accesible con la debida y comprobada autorización correspondiente.

La Integridad.

Este pilar asegura la precisión, completitud y validez la información para los procesos de negocio, asimismo asegura que no se realicen modificaciones de datos en un sistema por personal si no cuenta con la autorización correspondiente.

La Disponibilidad.

Este pilar asegura a los usuarios permitidos cuenten con accesos a los datos, recursos que sean necesario. Pues tiene como objetivo que todo usuario pueda acceder a la información cuando lo necesitemos, a través de los canales adecuados y siguiendo los procesos correctamente definidos y de esta manera evitar interrupciones no autorizadas, es decir la disponibilidad asegura el funcionamiento de los sistemas cuando sea requerido.

A continuación, el triángulo de la seguridad.

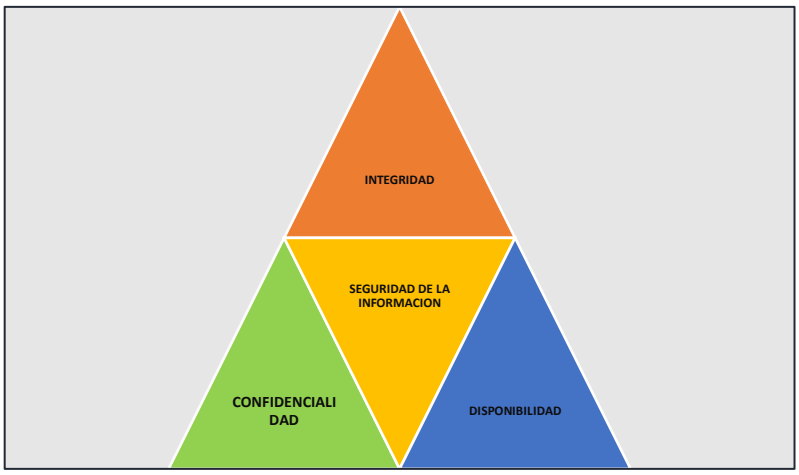


Figura 4: Triangulo de la Seguridad
Fuente: Elaboración propia

1.3.7. La Gestión de riesgos de la información

Según (ISACA, 2018), define como un proceso de la cual identifica las vulnerabilidades y amenazas a través de los recursos, con la finalidad de reducir o evitar un riesgo a cierto nivel en una organización.

La gestión de gestión de riesgos tiene como objetivo como se ha mencionado es en reducir los distintos riesgos en cualquier ámbito de la organización. Cabe indicar que podemos hacer referencia a un sin número de amenazas por causas ambientales o tecnológicas que afectas a las organizaciones y sus políticas de privacidad.

1.3.8. Factores de Riesgos en la seguridad informática

Existen 03 factores de riesgo definidos y que son considerados fundamentales.

- **Factor ambiental:** hace referencia a las lluvias, terremotos, inundaciones, rayos, calor humedad y otro factor externo.
- **Factor Tecnológico:** se refiere a daños de software y/o hardware, que se evidencian a través de ataque por virus informáticos, entre otros, etc.
- **Factor Humano:** hace referencia a los fraudes, modificaciones, sabotaje, crackers, vandalismo, hackers, falsificación de información, contraseñas robadas, intrusión no autorizada, entre otros, etc.

1.3.9. Los Riesgo en la seguridad Informática

En el ámbito de la ciberseguridad podemos definir un riesgo como una posibilidad de que ocurra amenazas de seguridad, utilizando una vulnerabilidad, generando un impacto con pérdidas o daños.

1.3.10. Las Amenazas en la seguridad Informática

La amenaza, es una acción que tiene un potencial efecto negativo sobre un activo, es decir en el campo de la informática, es cualquier cosa que comprometa o afecte a un sistema.

Figura 5: Amenazas en la Seguridad Informática
FUENTE Huerta, 2000

Hay que tener en cuenta que una amenaza por sí misma no provoca un daño, si bien puede afectar a la disponibilidad, integridad y confidencialidad. Pues para que exista un daño es necesario que exista una debilidad o fallo en el sistema, que permita que dicho daño se materialice.

1.3.11. La vulnerabilidad en la seguridad informática

Una vulnerabilidad, son las debilidades, fallos o agujeros en cualquier sistema operativo que ser de diferente naturaleza, como por ejemplo pueden ser de diseño, arquitectura, configuración, estándares o de procedimientos, vale decir que cuando se dice que un sistema informático es vulnerable, significa que tiene un agujero que puede ser utilizado para colarse dentro del sistema.

1.3.12. Tipos de vulnerabilidades en informática

Según (TECNOLOGIA & INFORMATICA, 2019). El tema de las vulnerabilidades es motivo de muchos problemas frecuentes a la seguridad de la información ya que abiertamente es aprovechado por los usuarios e inclusive por los ciber delincuentes y hackers, por lo cual se resume que las vulnerabilidades se clasifican en 04 tipos:

- **Crítica**

Se precisa que este tipo de vulnerabilidad informática, nos permite la trasmisión de posibles amenazas, debido a que no es necesaria la intervención del usuario u organización.

- **Importante**

Se precisa que este tipo de vulnerabilidad informática, tiene la capacidad de poner a un riesgo la confidencialidad, la disponibilidad e integridad de datos de una organización.

- **Moderada**

En este caso es una vulnerabilidad de tipo sencilla ya que permite disminuir el riesgo a través de configuraciones, auditorías a los sistemas de seguridad de cualquier organización.

- **Baja**

La vulnerabilidad de tipo baja, definitivamente su impacto es mínimo, ya que es difícil de ser aprovechado por algún atacante, pues realmente no tiene mucha afectación a los usuarios u organizaciones.

Es por ello que, de acuerdo a estas clasificaciones antes mencionadas sobre los tipos de vulnerabilidades, se puede concluir que cada tipo enumera el grado de peligro, actualmente existen vulnerabilidades destacadas o conocidas, tales como: desborde de buffers, condición de carrera o race condition, error de formato, XSS o "Phishing", de inyección SQL, denegación de servicio DDos, y Windows Spoofing o ventanas engañosas.

1.3.13. Los Ataques Informáticos

En el mundo de la informática existe una categoría llamada malware la cual quiere decir, software mal intencionado, lo cual podemos encontrar una serie de virus que dan lugar a la aparición de debilidades en sistemas y métodos de encubrimiento de cualquier intruso, convirtiéndolo en una práctica que aumenta aceleradamente.

Figura 6: Ataques informáticos
Fuente: Recuperado de https://www.optical.pe/tipos-de-ataques-informaticos-y-previsiones-para-el-2019/

1.3.14. Los Ataques por capas según Modelo OSI

A continuación, se muestra una infografía sobre tipos de ciber ataques en las diferentes capas del modelo OSI. Como se observa consta de 07: la misma que se deriva de una amenaza. A continuación

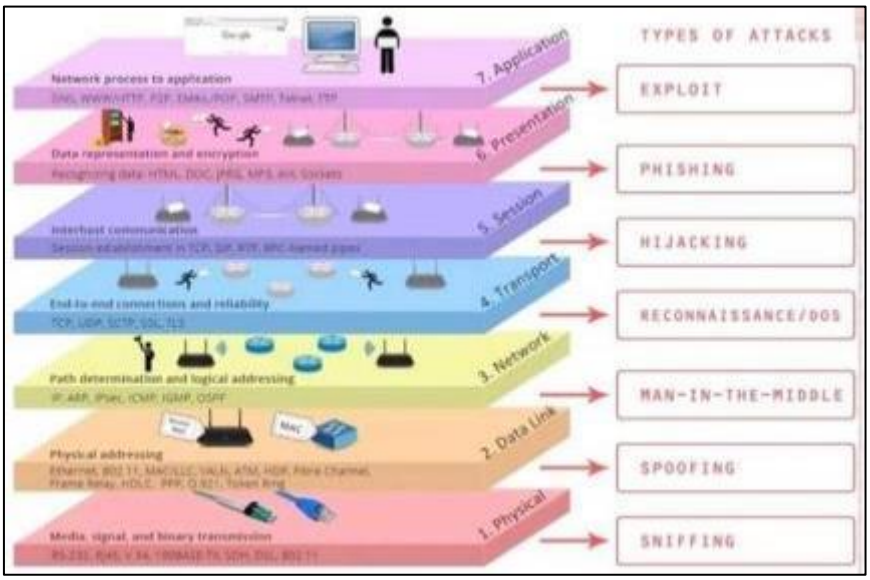


Figura 7: Tipos de Ataques por Capas
FUENTE: www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security

Los ataques también se pueden clasificar en base a capas. Cada capa se somete a diferentes tipos de ataques.

1.3.15. Ataque de Escaneo de Puertos

Se utiliza para la detección de servicios comunes y vulnerabilidades en los puertos abiertos, esta técnica de ataque se encarga básicamente de hacer la evaluación de vulnerabilidades a través de una máquina.

1.3.16. Ataque de Denegación de Servicio (DDoS)

Esta técnica de ataque se efectúa, principalmente a este propósito de realizar una denegación los servicios a todos los usuarios y considerando a otros más a quienes están dirigidos. En ese sentido un ataque DDoS, incluyen colapsos al sistema hasta cierto punto de quedar inutilizable, cabe mencionar que este tipo de ataque, tiene su forma muy sencilla

como dañar o eliminar información, los ataques implican una serie de actos de piratería y son considerados los más temidos.

1.3.17. Ataque de Fuerza Bruta

Esta técnica cuya proveniencia es de la criptografía, tiene una manera muy particular ya que resuelve problemas a través de algoritmos de programación, su objetivo es romper códigos cifrados y por descifrar.

Hoy en día, los ataques de fuerza bruta son utilizados para hackear redes sociales, emails, auditar redes inalámbricas y otras de carácter social.

1.3.18. Ataque de hombre en el medio

Esta técnica de prueba pasiva realiza interceptaciones de comunicación a una computadora a un teléfono y a una red wifi, permitiendo acceder y ver lo que se hace en ello, es preciso mencionar que al no encontrar cifrada una red wifi y dentro del rango de conexión hay un atacante cerca, este mismo puede realizar una inserción de tipo man in the middle.

1.3.19. Seguridad informática

Según (López, 2015), indica que seguridad informática es la disciplina que guarda relación con diversas técnicas, dispositivos y también diversas aplicaciones que permiten velar por la integridad y su privacidad de toda información de los sistema y usuarios de cualquier organización.

Por otro lado, es un proceso que asegura que todo recurso del sistema sea utilizado de tal manera que se tenga acceso para ella y de ser posible que todo individuo se encuentre debidamente acreditado y con ciertos límites de verificación o autorización en cada organización. También es definida, como una preservación de los elementos importantes de la seguridad de los sistemas, es decir su confidencialidad, la disponibilidad y la integridad.

Hoy en día hablar de seguridad informática estable establece un buen número de normas que permiten reducir los riesgos o infraestructura informática. Definitivamente

dichas normas incluyen ciertas autorizaciones, planes de emergencia, restricciones, perfiles de usuarios, por lo cual se debe tener todo lo necesario que nos permita evaluar el nivel de seguridad y reducir su impacto principalmente en los trabajadores y sus desempeños en las organizaciones.

1.3.20. Objetivo de la Seguridad Informática

Su principal objetivo es resguardar los recursos de las personas o empresas que son muy valiosos en hardware o software. Asimismo, se adoptan acciones de prevención a efectos que las organizaciones, personas o empresas tengas las facilidades para el cumplimiento de los objetivos trazados, de esta manera se podrá controlar y a la ve proteger los sistemas, recursos, económicos, legales y bienes tangibles e intangibles.

Es por ello que otro de los objetivos de la seguridad es contrarrestarlos ataques de malware, virus, y las vulnerabilidades que sufren hoy en día las empresas.

1.3.21. Principales Técnicas para evaluar vulnerabilidades

Según (Hernández & Mejía, 2015), los ataques se han ido en aumento a las diferentes redes de datos de las organizaciones, para lo cual se detallan las diferentes técnicas para el diagnóstico de vulnerabilidades, con el fin de evitar los ataques informáticos, estas técnicas tiene enfoques diferentes, tales como:

- Black Box
- White Box
- Análisis estático y dinámico del código
- Prueba de penetración
- Pruebas pasivas
- Pruebas activas
- Fuzz testing (prueba de caja negra)

A continuación, un breve análisis a cada técnica mencionada:

TECNICAS	DESCRIPCION
Black Box	Permite Detectar Vulnerabilidades en aplicaciones web, basándose en un enfoque real, el del atacante.
White Box	En ésta técnica, se tiene acceso al código fuente, a las credenciales válidas, a la configuración y datos técnicos del servidor.
Análisis Estático de Código	Se analiza el código fuente directamente, para poder determinar vacíos de seguridad.
Análisis Dinámico de Código	Al hacer el análisis, se comunica con la aplicación mediante front-end, para identificar debilidades de arquitectura de la aplicación.
Pruebas de Penetración	Simula ataques de delincuentes informáticos. Se analiza el sistema en busca de vulnerabilidades las cuales pueden ser de configuración, falla de hardware o software, errores operativos en proceso o contramedidas técnicas.
Pruebas Pasivas	Analiza el tráfico de telecomunicaciones. Su característica es detectar fallas mediante un examen de livetrafficor log files o paquetes capturados.
Pruebas Activas	Se usa en subprocesos para comprobar si las advertencias reportadas en un análisis del programa son errores reales.
Fuzz testing o pruebas de caja negra	En una prueba al sistema usa datos aleatorios o alterados para detectar fallas en el comportamiento del sistema.

Tabla 1: Técnicas Ethical Hacking para detectar Vulnerabilidades Informáticas
AUTOR: Oswaldo Tamayo, 2016

1.3.22. Definición de Ethical Hacking

El Ethical Hacking en su definición de manera individual hace referencia a un Hacker Ético, este individuo como bien lo dice es un profesional ético con habilidades como hacer evaluaciones a un sistema de forma general, poniendo en práctica todas las secuencias y pasos a seguir, de tal forma que se aplique un criterio trasversal. También se define como el servicio de auditoria de tecnologías de la información ofrecida principalmente por empresas especializadas en la materia.

En la actualidad muchas organizaciones a nivel mundial son víctimas de ataques de hackers o llamados piratas informáticos, pues estos tienen la capacidad de robar información muy valiosa, comprometiendo sistemas, y hasta el borrar o dañar archivos e información significativa en minutos o segundos.

Según (Astudillo, 2017), Es muy importante tomar acciones que permitan a las empresas u organizaciones proteger la información de toda formas posibles, pues el objetivo principal de Ethical Hacking de acuerdo a lo investigado, es brindar protección de los sistemas de las organizaciones y de esta manera evitar ataques maliciosos.

Por otro lado según (Astudillo, 2017). El principal objetivo del Ethical Hacking es de analizar y detectar las debilidades en los sistemas, efectuando pruebas de intrusión, los mismos que ayudan a evaluar una seguridad ya sea física y lógica a nivel de todo sistema de información, así como las redes informáticas, servidores, bases de datos y aplicaciones web, etc.

Las personas que administran las redes o se han dedicado a la seguridad con el fin de poner un alto o restringir los accesos, sin embargo, a medida que el avance tecnológico avanza los ataques, intrusiones, daños a los sistemas, robos y fraudes de información han generado grandes pérdidas económicas, lo cual es importante se realiza de manera periódica en las empresas una evaluación de técnicas de Ethical Hacking con la finalidad de minimizar los riegos y las vulnerabilidades en los sistemas.

1.3.23. Tipos de Hacker

a. Hacker de sombrero negro

Es un Hacker dedicado a la explotación y obtención de debilidades en muchos sistemas de información, redes informáticas, sistemas operativos, base de datos, etc., con la finalidad de su propio beneficio, tal es así que desarrollan virus o programas informáticos maliciosos para que logren sus propios objetivos.

b. Hacker de sombrero gris

Este tipo de Hacker trabaja en varias ocasiones a la ofensiva y otras de una manera defensiva, todo su actuar en el marco de los límites y muchas veces en contra de la legalidad.

c. Hacker de sombrero blanco

Este tipo de Hacker trabaja en empresas de seguridad informática, los mismos que por ética, se centran en proteger, analizar, detectar y corregir vulnerabilidades, de tal forma que puedan implementar medidas de seguridad.

d. Hacker Ético

Se define como un experto en sistemas de informática, por ejemplo, en programación de computadoras, redes de cualquier tipo, también es un experto de internet y su navegación. El Hacker realiza investigación, opiniones, y finalmente comparte todo tipo de información, la cual el profesional ético busca un mejoramiento en su vida personal o simplemente por diversión.

1.3.24. Tipos de Ethical Hacking

Según (Hurtado & Mendaño, 2016). A continuación, se van a detallar principalmente los tipos de pruebas de penetración en Ethical Hacking.

A. **Pruebas de penetración con objeto:** en esta prueba se examina las debilidades específicamente en partes en los sistemas informáticos.
B. **Pruebas de penetración sin objeto:** en esta prueba se examinan todos los elementos del sistema informático.
C. **Pruebas de penetración ciega:** en esta prueba la información es utilizada públicamente y está disponible a toda la empresa u organización.
D. **Pruebas de penetración informadas:** en esta prueba la información es utilizada por la organización misma, y en esta prueba se tiene acceso privilegiado.
E. **Pruebas de penetración externas:** esta prueba es hecha fuera de los ambientes de una organización o empresa, debido a que se puede evaluar políticas y mecanismos externos.
F. **Pruebas de penetración internas:** esta prueba es hecha dentro de las infraestructuras de la empresa u organización, con la finalidad de evaluar mecanismos y políticas internas.

1.3.25. Modalidades de Ethical Hacking

De acuerdo a la descripción de pruebas y su tipología se puede ubicar en dos modalidades:

Red Teaming: se trata de una prueba encubierta, vale decir sólo ciertas personas saben de ella, bajo esta modalidad se hace uso de la técnica de ingeniería social.

Blue Teaming: en esta prueba el personal de informática conoce y estos mismos toman conocimiento de posibles fallos dentro de la organización.

1.3.26. Fases del Ethical Hacking

- Recolección de la información
- Descripción de la red
- Explotación o escaneo
- Obtener acceso
- Mantener acceso
- Elaboración de informes

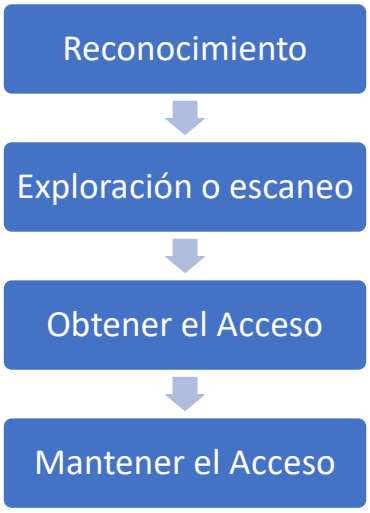


Figura 8: Fases del Ethical Hacking
Fuente: Elaboración propia

1.3.26.1. Reconocimiento

Se busca en esta fase recolectar toda la información posible, esencial y necesaria, haciendo utilización de diferentes herramientas y técnicas de hacking. Así mismo hay dos formas de reconocimiento pasivo y reconocimiento activo.

- Reconocimiento Pasivo: El atacante recolecta la información necesaria no interactuando con su objetivo, es más se puede averiguar por diferentes medios dominios y de los DNS, etc.
- Reconocimiento Activo: El atacante recolecta información necesaria con interacción con su objetivo, utiliza una técnica como ingeniería social.

1.3.26.2. Exploración o Escaneo

Aquí es esta fase se ejecuta el escaneo de una red, a su vez lanzar un ataque para identificar vulnerabilidades, además se pueden realizar mapeo de red, escaneo de puertos y servicios, todo ello a través de herramientas de hacking ético.

Por otro lado, en esta fase el atacante efectúa una serie de análisis para obtener información de los sistemas operativos y también de la red de datos, como los puertos abiertos, los hosts y otros.

1.3.26.3. Obtener Acceso

En esta fase se puede escalar privilegios a fin de obtener el control absoluto del sistema, ya que cualquier sistema o dispositivo que esté conectado a la red se encontrará comprometido. Así mismo la explotación se realiza a internet y servicios LAN, etc. Los ataques a cualquier sistema pueden ser por, aplicaciones, servidores web, etc.

1.3.26.4. Mantener el Acceso

En esta fase el mantener el acceso se busca a través de los ataques o intrusiones ataques, ya que puede realizarse haciendo uso de puertas traseras, Spyware o troyanos, el profesional hacker tiene ventaja ya que puede mantener el acceso a fin de lanzarse con nuevos ataques, lo cual afectan o instalan, modifican los archivos de información.

1.3.26.5. Limpieza de Huellas

En esta fase el hacker procede a realizar con la destrucción de toda la evidencia de las actividades que efectuó, pues esto le permitirá eliminar toda la evidencia del sistema y de esta manera evitar alguna acción legal.

1.3.27. Beneficios del Ethical Hacking

A continuación, se detallan los beneficios que se pueden obtener al momento de realizar un Ethical hacking, por lo cual se describen de manera general son los más importantes:

a. Se muestra una visión acerca de las vulnerabilidades encontradas a fin de prevenir.
b. Se pueden demostrar configuraciones inadecuadas, considerando algunas aplicaciones instaladas (firewall, sistemas de cómputo, servidores, switches, routers, etc.).
c. Realiza un reconocimiento al sistema que necesita efectuar actualizaciones.
d. Disminución en el tiempo de respuesta y evalúa y realiza esfuerzos necesarios para afrontar situaciones de riesgo.
e. Realiza un informe preciso acerca de todas las debilidades encontradas, permitiendo aplicar acciones correctivas en los plazos previstos.

Cabe mencionar que es un procedimiento que tiene muchas ventajas para las empresas, ya que permiten adelantarse ante cualquier ataque. Es por ello que con un buen servicio de Ethical Hacking, se detecta el uso inadecuado de la información de las organizaciones.

1.3.28. Metodologías del Ethical Hacking

En cada prueba de pentesting, es importante la metodología ya que permite definir el cómo se realizará. A continuación, detallamos 03 metodologías consideradas las principales, para los cuales se hablará de metodologías como OSSTMM, ISAAF y OWAS, por lo cual se realizará un breve comparativo de dichas metodologías:

1.3.28.1. Metodología OSSTMM

Es una metodología profesionalmente con estándares completos y son más comúnmente utilizados a las Auditorías de Seguridad de información a efectos de revisar los niveles de seguridad y desde cualquier punto de Internet. A todo ello incluye una metodología de trabajo a través de fases, la cual se lleva a cabo una ejecución de auditoría.

Según (Hurtado & Mendaño, 2016), Tiene como propósito principal un manual que permite la caracterización estrecha, realizando un análisis mediante la correlación de los resultados, de tal manera que sea la forma más consistente y confiable. Dicha metodología se enfatiza por su manual, se adapta a cualquier forma de auditar, lo cual consta de Ethical Hacking, pruebas de penetración, análisis de principales vulnerabilidades red-teaming8, blue-teaming, análisis de seguridad, entre otras.

1.3.28.2. Metodología ISSAF

Es el framework muy interesantes en ámbito de metodología de testeo. Se puede realizar algún análisis de manera detallada con todos aspectos posibles que afectan al testeo de seguridad. ISSAF, a través de su información la misma que se encuentra muy organizada, mediante los llamados "Criterios de Evaluación", cada criterio ha sido revisado por expertos.

ISSAF es utilizada principalmente para evaluar los requerimientos de las organizaciones y son utilizados como referencias, estas referencias sirven para realizar otras implementaciones.

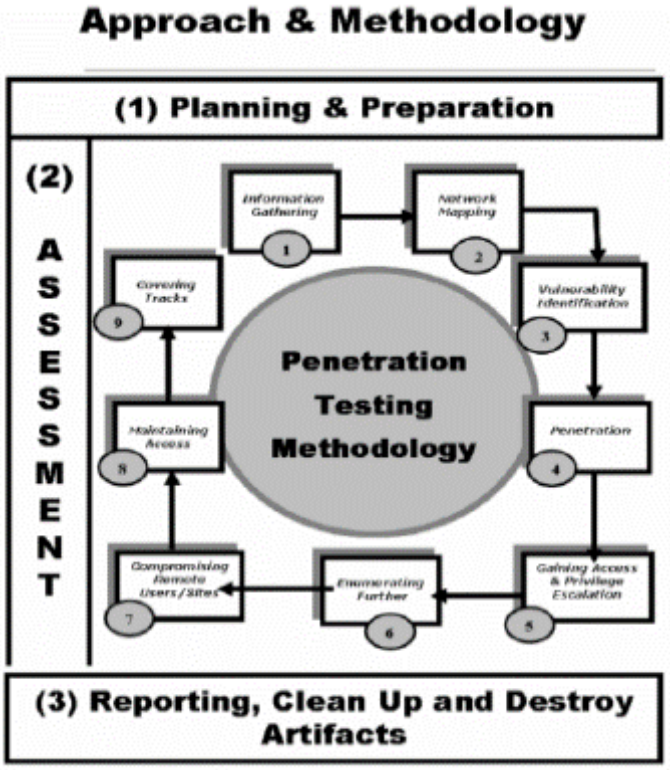


Figura 9: Fases de Evaluación de Metodología ISSAF
Fuente: dataceta.unad.edu.co

Esta metodología tiene como objetivo aportar con un procedimiento, con la finalidad de realizar la comprobación de sistemas de información y que se evidencien las situaciones reales, pues se han catalogado grandes aspectos sobre la administración de proyectos de Testeo, utilizando una forma sistemática en dichas labores, así como también en la ejecución.

1.3.28.3. Metodología OWASP

La metodología OWASP añade, elementos importantes correspondidos con el llamado "ciclo de vida del desarrollo de software" con la finalidad de ver el "perímetro" del testeo a perpetrar, se inició antes que las aplicaciones web produzcan adecuadamente.

OWASP diseña su parte uno, bajo elementos o claves que permitirán introducir un framework, pues de manera específica su diseño es evaluado a fin de garantizar la seguridad, cuenta con un programa de testeo para aplicaciones web, en donde se debe incluir elementos de características de testeo, como por ejemplo procesos, tecnología y personas.

1.3.29. Comparación de las Metodologías

Según (Hurtado & Mendaño, 2016), se ha realizado un comparativo de 03 metodologías ISSAF, OWASP, OSSTMM", de acuerdo a la siguiente tabla:

CARACTERÍSTICAS	METODOLOGÍAS		
	ISSAF	OWASP	OSSTMM
Se establecen los requisitos precedentes para la evaluación.	SI	NO	NO
Se definen un proceso detallado.	SI	NO	NO
Se recomienda herramientas y metodología.	SI	SI	NO
Se presentan evaluaciones de análisis en el proceso de riesgos.	SI	NO	NO
Clasifica y Enumera las vulnerabilidades detectadas.	SI	NO	NO
Crea reportes e informes.	SI	SI	NO
Presentan contramedidas y recomendaciones.	SI	NO	NO
Se tiene previsto los documentos y referencias a los enlaces externos.	SI	SI	NO

Tabla 2: Comparativo de Metodologías para Ethical Hacking
Fuente: Hurtado & Mendaño, 2016. Recuperado de: https://bibdigital.epn.edu.ec/handle/15000/16836

1.3.30. Herramientas de Hacking Ético.

A efectos de evaluar las técnicas de hacking ético es necesario otros aspectos importantes como son las herramientas que ayudan a prever a formar parte de alguna etapa de prueba de pentesting. Por lo cual pasamos a detallar las más utilizadas.

- **Herramienta Netcraft**

Esta herramienta monitorea y posibilita la identificación del tipo de servidor y sistema operativo, u otras actividades, etc., su uso se da por los navegadores y se recopila en tipo pasivo a la información.

- **Herramienta Metasploit Framework**

Esta herramienta para ejecutar y desarrollar exploits, sobre una maquina remota, se usa para explotar vulnerabilidades, simular ataques, y permite atacar diferentes plataformas y está desarrollado en Ruby.

- **Herramienta TCH Hydra**

Es una herramienta que se utiliza para probar la seguridad de las contraseñas de los sistemas o redes. Puede usarse para escanear web, crafters de paquetes, Gmail, redes inalámbricas, crafters de paquetes, etc.

- **Herramienta Ettercap**

Es una herramienta multiplataforma que es utilizado para auditorias de redes ya que no soporta direcciones pasivas y activas de distintos servicios o protocolos, puede interceptar y mejorar un ataque "hombre en el medio".

- **Herramienta Wireshark**

Dicha herramienta es multiplataforma y se utiliza para realizar análisis de paquetes o servicios a una red, es muy versátil, monitorea, soluciona y previene posibles problemas futuros.

- **Herramienta Openvas**

Es una herramienta que brinda una completa solución, es poderosa en escaneo, análisis de vulnerabilidades y es libre y gratuito, también es multiplataforma.

- **Herramienta Maltego**

Es una herramienta es utilizada para la recopilación de información de la organización y arranca desde Kali lunix.

- **Herramienta whatweb**

Es una herramienta es utilizada para las tecnologías a través de la web, su uso es disponible en varias plataformas y se ejecuta a través de una consola de comandos.

- **Herramienta Sqlmap**

Esta herramienta es de código abierto y sirve para automatizar y mejorar los procesos en la explotación, detección de las vulnerabilidades de inyección SQL.

- **Herramienta Nmap**

Según (Bermeo, 2017) Es una herramienta potente es utilizada para la detección y escaneo de redes y para las auditorías de seguridad, permite equilibrar los servicios que se están ejecutando en el dispositivo, como también escaneo de puertos, scripts, redes y vulnerabilidades.

- **Herramienta Nessus**

Según (Hurtado & Mendaño, 2016) Es una herramienta para escanear vulnerabilidades, realiza el escaneo en cualquier sistema operativo, puede escanear varias máquinas en forma simultánea, así mismo se integra, por sus coincidencias con las herramientas NMAP y METAEXPLOIT.

- **Herramienta Fierce**

Es una herramienta y se utiliza para el reconocimiento, escaneos de direcciones IP y dominios.

1.4. Formulación del problema

¿Cómo la evaluación de las técnicas de Ethical Hacking influyen en el diagnóstico de vulnerabilidades de la seguridad informática en las empresas prestadoras de servicios?

1.5. Justificación e importancia del estudio

Según (Hernández & Baptista, 2014), testifican sobre la justificación en una investigación especifica cuáles son los motivos para los cuales se efectúa un estudio, se define sus principales beneficiarios, el propósito y lo que se debe conseguir en el desarrollo del mismo.

La presente investigación es pertinente ante una realidad problemática expuesta y basa en un diseño de una infraestructura de red física y lógica que permite simular una organización con recursos tecnológicos interconectados y sobre ello realizar prácticas de las técnicas de hacking ético, con esto se busca que cualquier persona interesado pueda evaluar y aplicar las técnicas de hacking para generar habilidades en el tema seguridad informática.

Hoy en día las empresas prestadoras tienen una infraestructura tecnológica, expuestas a las debilidades y amenazas, lo cual los hackers sacan el máximo provecho para acceder, sustraer o robar información relevante de una organización a través de una serie de procedimientos metodológicos y prácticos. El presente trabajo, permitirá tener una idea precisa en relación al impacto de una posible intrusión y a través de la evaluación de las técnicas del Ethical Hacking se podrá proporcionar o evidenciar soluciones de cómo evitarlas y mitigarlas en cada caso que se pueda presentar dentro de una organización.

En respuesta a lo anterior se evaluará las técnicas de Ethical Hacking para el diagnóstico de vulnerabilidades enfocado especialmente en los procesos del área de tecnología de una empresa prestadora de servicios. Por este motivo urge la necesidad de conocer, analizar y detectar vulnerabilidades a la seguridad informática de una red de datos, mediante la evaluación de técnicas de Ethical Hacking es una tecnología de los últimos tiempos y actualmente es utilizada en todo el mundo por profesionales dedicados al Ethical Hacking, la existencia de cada año se incrementa las vulnerabilidades y son detectadas en su mayoría a empresas y organizaciones ha permitido realizar la presente investigación con la

finalidad de evaluar y determinar el grado de niveles de vulnerabilidad, puertos abiertos, y archivos enviados por cualquier sistema de la red de datos, y de esta manera conocer que tan vulnerables son los sistemas empresariales.

El presente informe se justifica desde la perspectiva de tres puntos importantes. Justificación práctica, de acuerdo al problema se evalúa una estrategia de acciones para su aplicación, el mismo que contribuirá a resolverlo.

Justificación teórica, de acuerdo a los antecedentes previos a la investigación, generará discusión y reflexión a la vez, debido que las investigaciones de nivel internacional, nacional y local, hacen referencia a la presente investigación sobre como evaluar técnicas de Ethical Hacking en cada área o escenario investigado y con un conocimiento fehaciente de ingeniería. Finalmente, desde la justificación metodológica, el presente trabajo mostrará y aportará a un nuevo modelo para las empresas de los diferentes sectores empresariales.

1.6. Hipótesis

$H_0 =$ La evaluación de Técnicas de Ethical Hacking influirán en el diagnóstico la seguridad informática, estableciendo niveles de riesgo, reconocimiento y confidencialidad en una empresa prestadora de servicios.

1.7. Objetivos

1.7.1. Objetivo general

Evaluar técnicas de Ethical hacking sobre la seguridad informática de una red de datos que permitan el diagnóstico de vulnerabilidades en una empresa prestadora de servicios.

1.7.2. Objetivos específicos

a. Definir técnicas de Ethical Hacking para el diagnóstico de vulnerabilidades en una empresa prestadora de servicios.
b. Conocer la situación actual de la seguridad informática, implementando técnicas sobre una red de datos, dentro de una empresa prestadora de servicios.
c. Identificar las debilidades usando las técnicas de Ethical Hacking sobre la seguridad informática en una empresa prestadora de servicios.
d. Clasificar las vulnerabilidades detectadas sobre la Seguridad informática en una empresa prestadora de servicios.
e. Proponer lineamientos de seguridad para garantizar la confidencialidad, integridad y disponibilidad en una red de datos de una empresa prestadora de servicios, postulando medidas de mitigación de las vulnerabilidades ya clasificadas.

II. MATERIAL Y METODO

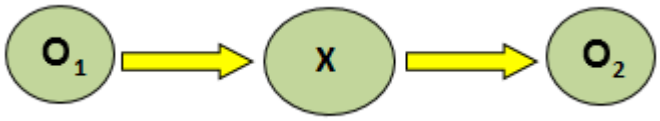
2.1.Tipo y diseño de la investigación

Tipo de investigación

Por su naturaleza, el estudio planteado es del tipo cuantitativo. Por un lado, el estudio analiza y evalúa los datos de las variables de estudio y las características de la realidad. Por el otro lado, se elaborará la "Evaluación de técnicas de Ethical Hacking para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa prestadora de servicios"

Diseño de la investigación

En esta investigación cuasi-experimental existe solo un grupo por lo que no se puede realizar la comparación de grupos. El diseño presenta la siguiente estructura:



DONDE:

O_1 = Nivel de seguridad de la información de la empresa prestadora de servicios, antes de evaluar técnicas.

X = Evaluación de técnicas de Ethical hacking.

O_2 = Nivel de seguridad de la información de la empresa prestadora de servicios, después de evaluar técnicas.

2.2.Población y muestra

Población

Consideramos como población para el presente trabajo las técnicas que se obtuvieron en la revisión sistemática de los papers, se han investigado 07 técnicas las más usadas en la actualidad para detectar las vulnerabilidades se detallan a continuación:

1. **Black-box**: según (Sreenivasa & Kuman, 2012). Se trata de una técnica establecida que permite descubrir vulnerabilidades en las distintas aplicaciones web, realiza pruebas a la aplicación desde la vista del atacante.
2. **White-box:** según (Sreenivasa & Kuman, 2012)**,** se trata de una técnica con accesos a la información de la organización
3. **Análisis estático de código o auditoria de código fuente**: según (Sreenivasa & Kuman, 2012), esta técnica se encarga de realizar un análisis directamente al código fuente a fin de determinar bugs o huecos en la seguridad.
4. **Pruebas de penetración:** según (López De Jiménez, 2017), es una técnica que consiste en ejecutar y hacer una evaluación activa, tiene como propósito detectar debilidades altamente potenciales. También se realiza ataques de manera local y remota, buscando explotar vulnerabilidades, pero sin dañar la infraestructura y sistemas web de la información.
5. **Pruebas pasivas:** según (Mammar, Cavalli , & Jimenez, 2011), estas pruebas realizan un análisis de tráfico y detección fallas, examinando los paquetes capturados, estas pruebas por lo general son efectuadas a través del internet.
6. **Pruebas activas**: según (Zhang, Shao, & Zheng, 2008), realiza un análisis para verificar si los errores son evidentes.
7. **Fuzz testing (man in the middle)** (pruebas de caja negra): según (Zhang, Shao, & Zheng, 2008), se detectan datos aleatorios dañados, lo cual viola los elementos de seguridad.

Muestra

El presente trabajo de investigación se trabajará con 03 técnicas de Ethical Hacking que vamos a poner en práctica para el presente proyecto.

2.3.Variables, Operacionalización

2.3.1. Variable

Variable Independiente: Técnicas de Ethical Hacking

Variable Dependiente: Nivel de Seguridad de la Información

2.3.2. Operacionalización

Variable Independiente	Dimensiones	Indicador	Unidad de Medida	Técnicas e instrumentos de recolección de datos
Técnicas de Ethical Hacking	Métrica base	Métricas para clasificación de Técnicas de Ethical Hacking	Ordinal	Tabla de Métricas de Técnicas de Ethical Hacking

Tabla 3: Operacionalización Variable Independiente

Variable Dependiente	Dimensiones	Indicador	Unidad de Medida	Técnicas e instrumentos de recolección de datos
Nivel de seguridad de la información de la empresa prestadora de servicios	Nivel de riesgo	$NRV = \frac{N_v}{NTV} X100\%$ NRV= Nivel de riesgo de vulnerabilidad Nv= Número total de vulnerabilidades por nivel de riesgo NTV= Número total de vulnerabilidades detectadas	Nivel Porcentual	Hoja de reportes del sistema.
	Reconocimiento de Puertos	Número total de puertos abiertos, expuesto a cyber ataques	Ordinal	Hoja de reportes del sistema.
	Confidencialidad	$C = \frac{AE - AR_D}{AE}$ x 100% AE= Total de archivos evaluados AR_d= Total de archivos recibidos dañados.	Nivel Porcentual	Observación. Hoja de reportes del sistema.

Tabla 4: Operacionalización Variable dependiente

2.4.Técnicas e instrumentos de recolección de datos, validez y confiabilidad

2.4.1. Técnicas e Instrumentos

Técnica:

Como técnica de recolección se usará las fases del Ethical Hacking para evaluar las técnicas y diagnosticar o detectar las vulnerabilidades a la seguridad informática, aplicando la metodología ISSAF las cuales son las siguientes:

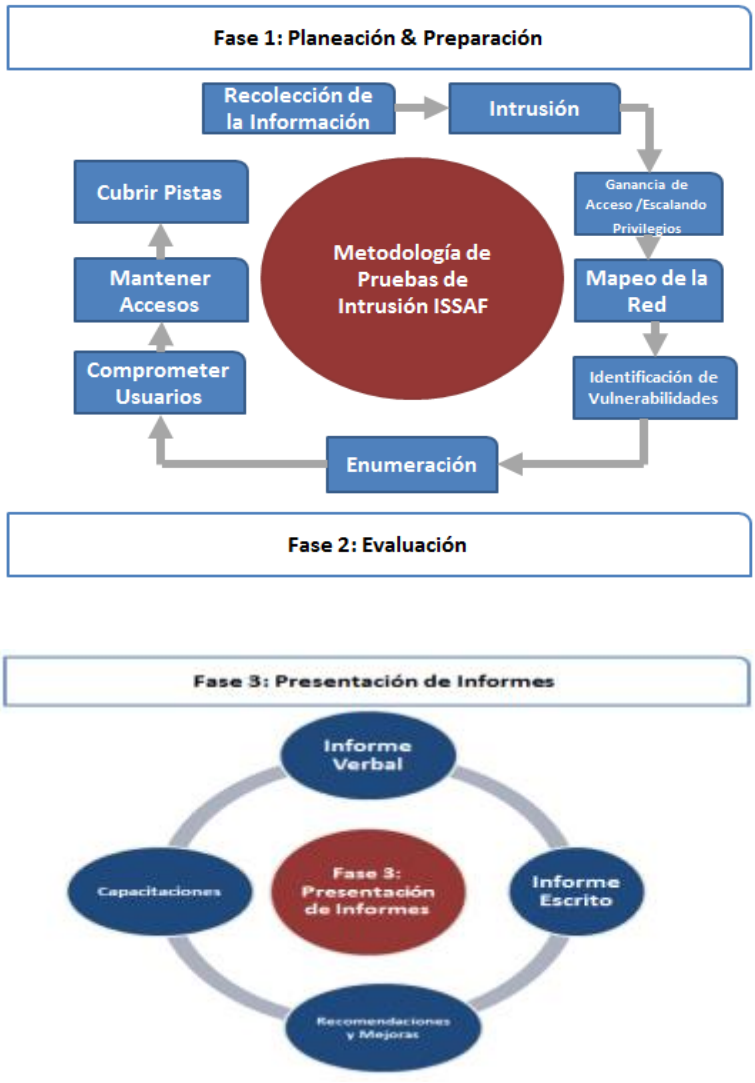


Figura 10: Fases de utilizadas de la Metodología ISSAF
Fuente: Elaboración Propia

La metodología ISSAF se va a utilizar cumpliendo una serie de procedimientos ya sea en el desarrollo, dirección y administrar sus sistemas y que estos encuentren seguros empleando rigor en cada proceso.

Fase I: Planeación y preparación. – aquí se hará el proceso que inicialmente intercambiar la información, luego vamos a realizar una planificación, desarrollo, preparación y hacer pruebas. Se precisa que, para efectuar una prueba, la metodología es similar a las existentes, ya que el auditor se exige como también el cliente o usuario, es conlleva a realizar un acuerdo mutuo con la formalidad respectiva, ya a través de un contrato que asegure el bienestar administrativo y legalmente.

1. **Recolección de la información:** es un método técnico y a la vez no técnico ya que se utiliza para buscar mucha información de datos, es considerada como una etapa de control auditable, permitiendo velar por la seguridad de información, de esta manera proseguir con las demás fases de esta metodología.
2. **Intrusión:** aquí se obtiene acceso no autorizado o ataque wifi a fin de llegar al mayor de acceso y evitando todas las medidas de seguridad, en efecto es importante buscar codificación que esté disponible o sea público o propio para realizar o probar a través de pruebas con las herramientas, considerando un entorno privado o aislado desaprobando o confirmando las vulnerabilidades y realizando la respectiva documentación de las soluciones respetivas.
3. **Ganando acceso y escalando privilegios:** se puede acceder a los dispositivos en la red, a su vez se confirma y documenta todas las intrusiones a la difusión de los ataques automatizados, permitiendo entrar en un alcance mayor sobre el impacto para las organizaciones que tiene a su custodio y administran un sistema determinado.
4. **Mapeo de la red:** es todo aquello que tiene que ver con una red de dato y la información del mismo, es adquirida del elemento de recopilación y se difunde produciendo diferentes tipologías, de tal manera se puede recurrir a las herramientas especializadas y aplicaciones que se utilizan para cooperar al descubrimiento de información de manera técnica y precisa la misma que

se recopila de los hosts y todas las redes involucradas en la prueba de penetración, por ejemplo:

- Hosts disponibles
  Detección de los usuarios en la red a través de 03 herramientas:
  IP SCAN: CABLEADO
  Net Analyzer: WIFI
- Escaneo de puertos y de protocolos:
  NMAP por cada PC
- Mapeo de la red
  NESSUS para la red
- Identificación de servicios críticos
  NESSUS y ETTERCAP
- Identificación de rutas y de sistemas operativos
  NESSUS
- Identificación de archivos dañados
  ETTERCAP, ataque man in the middle

Fase II: Evaluación. - se caracteriza esta fase por efectuar la prueba de penetración, donde se considera como "el enfoque por capas", pues cada una de las denominadas capas expresa o los mismos que representan niveles de acceso.

5. **Identificación de vulnerabilidad**: es aquí donde se escogen los elementos de manera específica a fin de que sean comprobados, y también posteriormente como se probaran.
   En efecto esta metodología, se desarrolla y el auditor tiene que utilizar actividades como las de, detectar los elementos o servicios vulnerables, proyectar el impacto, nivelar las rutas de ataque, se realiza una validación de los falsos positivos y también de los falsos negativos, todo esto con el fin identificar, detectar y clasificar las vulnerabilidades de un sistema y su operación del mismo.

6. **Enumeración:** aquí se hace la obtención del encriptamiento para obtener contraseñas usando la técnica sniffing o Keylogger, explorar las sesiones, contrarrestar ataques y hacer un mapeo de las redes.
7. **Comprometiendo usuarios/o sitios remotos:** se comprueba que un escritorio remoto es vulnerable, además aquí se expone a toda una red o sistema, por tal motivo, los elementos de autenticación son claves para la comunicación de los usuarios y redes empresariales, de tal manera que el dato obtenido no se modifique mientras viaje a través de la red, cabe indicar que estas acciones no garantizar de sean comprometidos.
8. **Mantener el acceso:** podemos considerar que se utiliza para tener privilegios en los sistemas, accediendo y manteniendo acceso a la integridad. Es decir, es el túnel de acceso y es de utilidad de forma muy frecuente. Es por ello que vamos a probar la consistencia de la red.
9. **Cubrir pistas:** aquí se detalla lo realizado y se generan registros por un auditor, en esta prueba podemos, ocultar archivos y borrar registros, con el fin de no dejar pistas de la intrusión.

Fase III: Presentación de informes.- este es el último paso ya que de manera general se realiza un informe general de todo lo encontrado en los sistemas durante la intrusión, estos reportes son alcanzados a la organización o dueño del sistema, pues debe conocer del problema; ya que se detalla en un informe final una vez que se haya finalizado sobre los elementos de prueba presentados inicialmente, asimismo se define las recomendaciones generales para la mejora de acuerdo a los resultados obtenidos.

Instrumento

Los instrumentos o técnicas para el procedimiento de recolección, fueron la Hoja de reportes del sistema y observación; las mismas que han sido utilizadas de la siguiente manera:

Hojas de reporte del sistema: se generarán a través de las diferentes técnicas o herramientas utilizadas, las mismas que especializadas.

Observación: en función de los datos que se pretenden obtener, se utilizó la técnica de observación, la misma que consiste en registrar sistemáticamente, y confiable de comportamiento.

2.4.2. Validez y confiabilidad

En este caso la validez fue determinada por medio de las técnicas de recolección, utilizando 03 técnicas de Ethical Hacking, de acuerdo a la operacionalización y sean aptas para su evaluación.

La confiabilidad se determinó por medio del análisis de vulnerabilidades, aplicando las herramientas de Ethical Hacking, a través de NESSUS, NMAP y ETTERCAR.

2.5.Procedimiento de análisis de datos

Obtenido los resultados, producto de la aplicación del instrumento se procederá a su ordenación para analizarlo mediante la estadística descriptiva. Estos datos serán, evaluados, clasificados, comparados, tabulados y para mejor entendimiento graficados, con la finalidad de evaluar y representar objetivamente la realidad encontrada en la red de datos.

Realizada la tabulación se realizará el análisis e interpretación de resultados obtenidos. A fin que los resultados obtenidos permitan y sirvan y sean fáciles de analizar e interpretar utilizaremos el gráfico de barras de ser necesario ya que es la forma más accesible de presentar los datos.

Fórmula de la Media

$$\overline{X} = \frac{X_1 + X_2 + X_3 + \cdots + X_n}{N}$$

2.6.Criterios éticos

Según (Morales, 2015), menciona que para el desarrollo de una investigación se proponiendo 3 principios éticos:

Principio del valor fundamental de la vida humana:

Según (Morales, 2015), Implica el mutuo respeto y dignidad.

Principio de Libertad y responsabilidad:

Según (Morales, 2015), menciona la libertad y su participación con el debido consentimiento.

Principio de Totalidad:

Según (Morales, 2015), la persona copera de manera personal.

2.7.Criterios de rigor científico

Confiabilidad: Según (Morales, 2015), se realizarán hojas de reporte y hojas de cálculo en formato Excel.

Validación: Según (Morales, 2015), se hará a través de reportes de las herramientas especializadas.

.

III. RESULTADOS

3.1.Resultado en Tablas y Figuras

3.1.1. FASE I: Planeación y Preparación

3.1.2. Recolección de la Información

Los resultados han sido divididos con la evaluación de 03 técnicas y se ha utilizado como recolección de la información las herramientas especializadas como es NESSUS SCAN, NMAP y ETTERCAP para buscar el número total de dispositivos conectados a la red. A continuación, vamos a explicar el porqué del uso de estas herramientas especializadas.

Uso de Herramienta Especializada NESSUS:

En primer lugar, presentamos aquellos resultados relacionados a la técnica de prueba de penetración en la cual hemos hecho uso la herramienta NESSUS ya que sirve para la detección de vulnerabilidades, sobre sale porque realiza análisis a las vulnerabilidades de alta severidad.

Justificación: Según (David A. Franco, 2013), uso 03 herramientas de hacking para los laboratorios de prueba de penetración (NESSUS, NEXPOSE y UDECESCANER), en este caso precisamos que se realizó un mapeo entre el nivel de seguridad que arrojo por cada herramienta y con una escala definida a efectos de realizar una comparación entre las herramientas.

Tabla 1. Mapeo entre las escalas de severidad utilizadas por las herramientas de evaluación y la escala definida por los autores.

UdeCEscaner	Nexpose	Nessus	Nueva escala
Alto	Critico	Critico, Alto	Alto
Medio	Severo	Medio	Medio
Bajo	Moderado	Bajo, Info	Bajo

Figura 11: Escala de Severidad por las Herramientas de Evaluación de Vulnerabilidades
***Fuente:* (David A. Franco, 2013)**

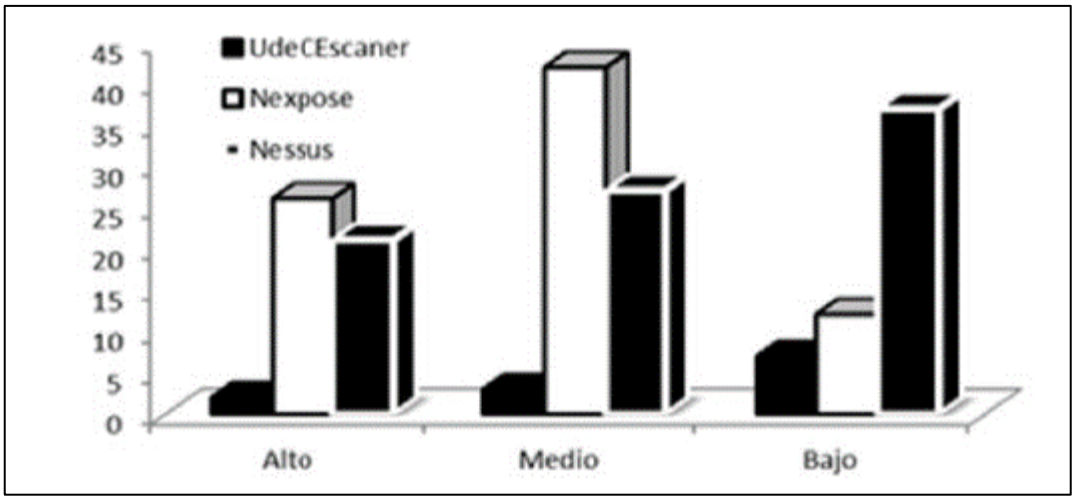


Figura 12: Resultados para un laboratorio de pruebas de penetración
***Fuente:* (David A. Franco, 2013)**

apreciamos la figura 12, justificó que la herramienta que detectó más vulnerabilidades fue NESSUS, seguidamente NEXPOSE y UDECESCANER. Pues la herramienta UDECESCANER presentó un mínimo número de vulnerabilidades a diferencia de lo encontrado por las demás herramientas. NESSUS detecto vulnerabilidades de severidad alta también se informó que mayormente en los servicios OpenSSH y Apache, pues presentan fallas a nivel de desbordamiento de memoria y ejecución de código remota.

A continuación, se detalla un comparativo entre las características de las herramientas de detección de vulnerabilidades.

Herramienta/Parámetro	UdeCEscaner	Nexpose	Nessus
Facilidad de uso	Alta	Alta	Alta
Requerimientos del sistema	Bajo	Alto	Medio
Facilidad de instalación	Simple	Compleja	Media
Interfaz amigable	Alto	Alto	Alto
Complejidad	Baja	Alto	Alto
Nº de vulnerabilidades detectadas	80	195	305
Legibilidad del reporte final	Alta	Alta	Alta
Contenido del reporte	Medio	Alta	Medio
Velocidad de detección	Alta	Baja	Medio

Figura 13: Comparación entre las características de las herramientas de detección de vulnerabilidades.
Fuente: (David A. Franco, 2013)

Según (Hurtado & Mendaño, 2016). Usó la herramienta NESSUS para brindar un reporte general a nivel de red o segmento, obteniendo las vulnerabilidades en todas las capas del modelo OSI.

Proceso de Instalación:

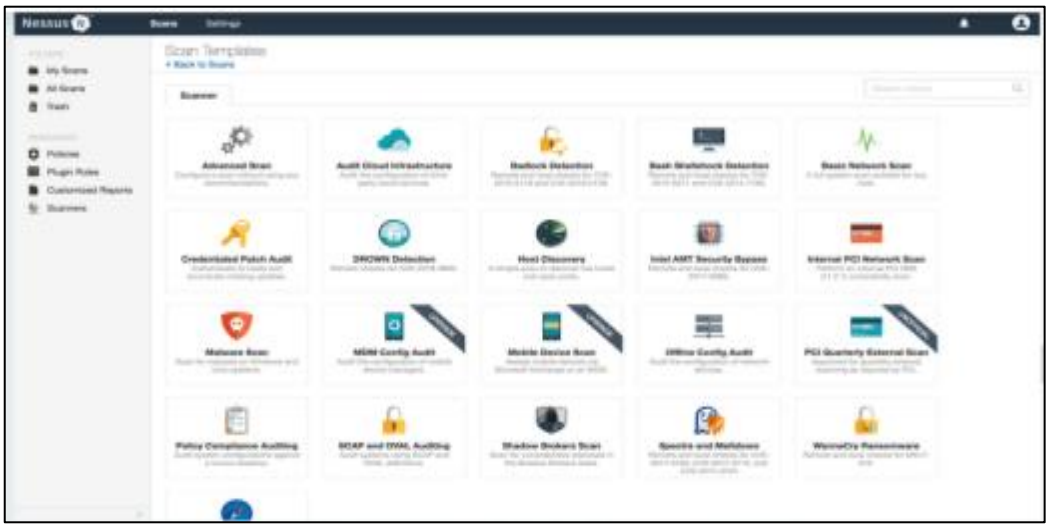


Figura 14: Instalación de Herramienta para Prueba de Penetración
Fuente: https://es-la.tenable.com/products/nessus?tns_redirect=true

Figura 15: Uso de Herramienta Especializada NESSUS para escaneo de vulnerabilidades
FUENTE: www.nessus.com

Como se ha justificado en la presente investigación se hará uso de la herramienta NESSUS porque brinda soluciones y es la más usada para la detección de vulnerabilidad, configuración y compatibilidad a diferencia de otras herramientas, es por este motivo que se está haciendo uso de esta herramienta para esta evaluación de las vulnerabilidades en la red de datos de la empresa prestadora.

Uso de Herramienta Especializada NMAP:

En segundo lugar, presentamos aquellos resultados relacionados a la técnica de prueba pasiva, en la cual hemos hecho uso la herramienta NMAP ya que sirve para el escaneo de redes, utiliza paquetes IP sin procesar para verificar los servicios que se ejecutan en los dispositivos remotos, también podemos identificar quipos activos, y sistemas en operación, existencia de filtros o firewalls, entre otros.

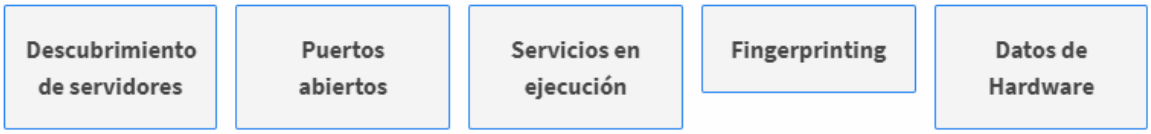
Justificación: Según (Narvaez Portillo , 2015) justifica el uso de herramientas AIRCRACK.NG, BURPSUITE, HYDRA, METASPLOIT, NMAP, WIRESHARK, en la cual resume y considera la descripción de su funcionamiento, características, objetivo de pruebas y resultados obtenidos, pues en dicho resumen considera la herramienta NMAP que usaremos en la presente investigación.

Herramienta	Objetivo	Resultados
Aircrack-ng	Probar el conjunto de herramientas Aircrack-ng, mediante su empleo en la tarea de descifrar la clave de la red inalámbrica WLAN-UPS-ESTUDIANTES	Se detectan las características de la red WLAN-UPS-ESTUDIANTES como: Dirección MAC, canal por el cual transmite la red, tipo de encriptación y tipo de cifrado, así como la actividad de autenticación y des autenticación ente cliente Punto de Acceso y finalmente en el proceso de combinaciones para descifrado de claves con 5799644 registros, sin que la clave sea encontrada se concluye que la misma es fuerte y cumple con los estándares requeridos.
Burpsuite	Interceptar una búsqueda dirigida a la página web de la Universidad	Se observa la intercepción de la petición de ingreso a la página principal de la Universidad, así como una captura de la portada de la página.
Hydra	Verificar la contraseña de inicio de sesión de una máquina del Laboratorio 6 del Cecasis	Se obtienen tres opciones válidas de contraseñas
Metasploit	Realizar una exploración al sistema operativo Windows 7	Se encuentra vulnerabilidad que presenta la posibilidad de ejecución de código remoto
Nmap	Escaneo de puertos y sistema operativo a dirección de host conectado a la red de la Universidad	Se encuentran abiertos los puertos 135, 139, 443, 445, 1040, 3306, 8036, de los cuales 135, 139 y 445 tienen exploits conocidos para vulnerar. En cuanto al sistema operativo encuentra que se trata de Windows 7 para puerto 135 y Apache httpd 2.4.3, para puertos 443 y 8083.
Wireshark	Observar el intercambio de paquetes durante un saludo en tres vías ejecutado entre dos máquinas	Se observa el intercambio de paquetes SYN , ACK entre dos direcciones

Figura 16: ***Resumen de pruebas desarrolladas por herramientas***
Fuente: **(Narvaez Portillo , 2015)**

Existen herramientas muy usadas en los últimos tiempos en la seguridad informática, sin embargo, NMAP resalta porque es muy utilizada para hacking ético. Por ejemplo, los administradores de los sistemas lo utilizan para identificar posibles aplicaciones no autorizadas ejecutándose en una red o servidor, los intrusos pueden aprovechar y usar para descubrir potenciales objetivos de ataque.

NMAP tiene una caracterización ya que proporciona los servicios que se mencionar:



Justificaciones Científicas:

Según (R. Sri & M. Mohan, 2020) justifica que, en los resultados de la comparación de diferentes herramientas SPARTA, NMAP, NETCRAFT, ZENMAP, VIRUS TOTAL, IP TRACKING, todas involucradas es la identificación de los ataques, y concluye que los ciberataques pueden ser posibles.

Tools	Attacks
Sparta	Examined IP ranges, a dictionary attack is possible
Network Mapper (Nmap)	Found the source of other hosts or new attacks
Netcraft	Detect the Phishing attacks
Zenmap	Discovered the open ports exposing their networks to cyber-attacks.
Virus total	Different malware can be inserted using these vulnerabilities.
IP tracking	DDoS attack

Figura 17*: *Resultados de comparación de diferentes herramientas
Fuente: (R. Sri & M. Mohan, 2020)

Según (Waheed Ali, Ghanem, & Baharí, 2013) justifica y realiza la comparación de los resultados, mediante una pruebas exhaustivas contra la precisión de la base de 03 herramientas NMAP, AMAP, ETTERCAP, el comparativo consistió en analizar una base de datos y buscar coincidencia con un algoritmo y de forma sencilla a través de fases.

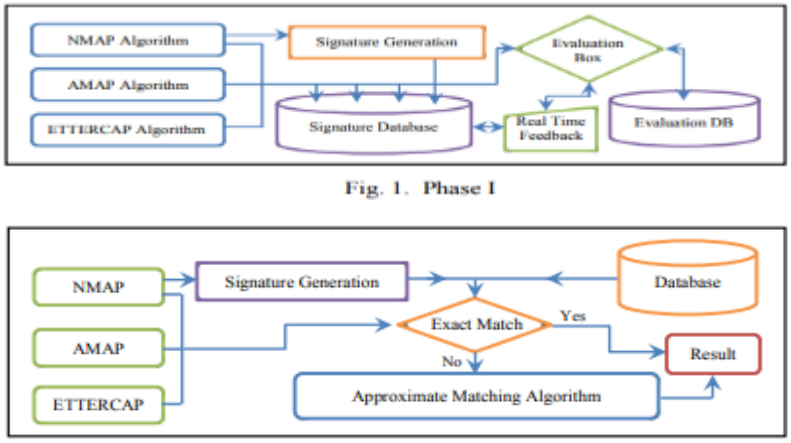


Figura 18*: *Creación de la base de datos y evaluación del sistema
***Fuente:* (Waheed Ali, Ghanem, & Baharí, 2013)**

Según (Bermeo, 2017) NMAP Es una herramienta potente es utilizada para la detección y escaneo de redes y para las auditorías de seguridad, permite equilibrar los servicios que se están ejecutando en el dispositivo, como también escaneo de puertos, scripts, redes y vulnerabilidades.

Proceso de Instalación y pruebas:

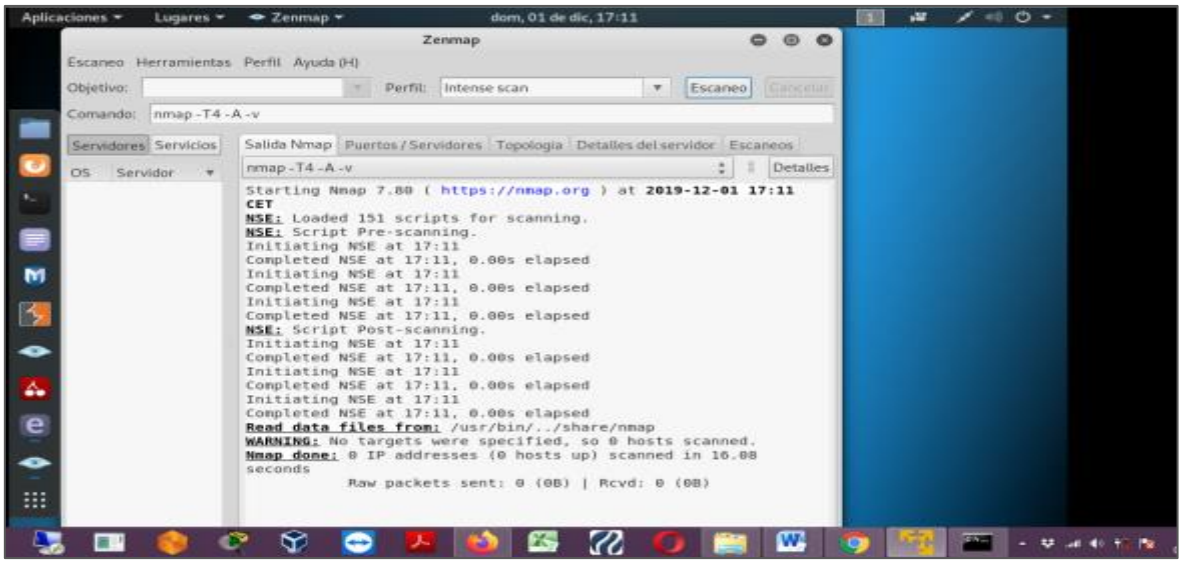


Figura 19: Instalación Herramienta para Prueba Pasiva
FUENTE: Elaboración Propia

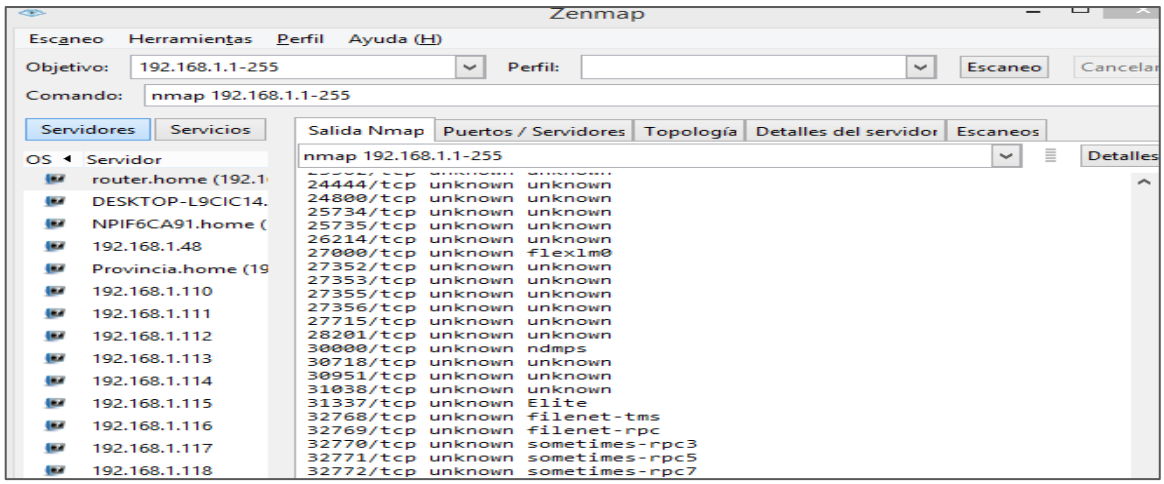


Figura 20: Uso de Herramienta NMAP para escaneo de puertos abiertos
FUENTE: Reporte Sistema

https://nmap.org/

Como se ha justificado en la presente investigación se hará uso de la herramienta NMAP porque sirve para el escaneo y permite evaluar los servicios se están ejecutando remotamente, identificación de equipos activos, sistemas operativos, filtros o firewalls, y otros. es por este motivo se hará uso de esta herramienta para esta evaluación de las vulnerabilidades en la red de datos de la empresa prestadora.

Uso de Herramienta Especializada ETTERCAP

En tercer lugar, presentamos aquellos resultados relacionados a la técnica de prueba Fuzztesting, en la cual hemos hecho uso la herramienta ETTERCAP ya que sirve para ataques de intermediarios, pues cuenta con rastreo de conexiones activas, así como también filtración de contenido y muchos otros contenidos muy interesantes. También permite la disección de forma activa y pasiva en protocolos y en muchas características para analizar redes y hosts.

Justificación: Según (Coteron Tene, 2012) justifica el uso de herramientas de Hacking ético CAIN & ABEL, ETTERCAP, WIRESHARK, TPCDUMP y CAPSA en la cual realizó una escala de valoración de criterio y se define la escala numérica porque se evaluaron las alternativas en base a las características de las herramientas utilizadas en esta investigación que justifica el uso.

CRITERIOS (b, d, g, i)	
ESCALA	INTERPRETACION
1	Malo
2	Regular
3	Buena
4	Muy Buena
5	Excelente

CRITERIOS (a, c, e, f, h)	
ESCALA	INTERPRETACION
1	No
5	Si

	CRITERIOS	PESO	CAIN & ABEL	ETTERCAP	WIRESHARK	TCPDUMP	CAPSA
a)	Software libre Open Sourse	13	5 / 65	5 / 65	5 / 65	5 / 65	1 / 13
b)	Interfaz Gráfica de uso	11	5 / 55	4 / 44	3 / 33	1 / 11	5 / 44
c)	Monitorea distintos S. O.	10	1 / 10	5 / 50	5 / 50	1 / 10	1 / 10
d)	Eficiencia en la captura de tráfico	14	4 / 48	5 / 70	5 / 70	5 / 70	4 / 48
e)	Envenenamiento ARP	11	5 / 55	5 / 55	1 / 11	1 / 11	1 / 11
f)	Ataque DoS	12	1 / 12	5 / 60	1 / 12	1 / 12	1 / 12
g)	Filtrado de Paquetes	6	1 / 6	4 / 24	5 / 30	4 / 24	4 / 24
h)	modificabilidad de Paquetes	11	1 / 11	5 / 55	1 / 11	1 / 11	1 / 11
i)	Escaneo de HOST	13	5 / 65	5 / 65	3 / 39	3 / 39	5 / 65
	TOTAL	100	327 SEGUNDA	488 PRIMERA	321 TERCERA	253 CUARTA	238 QUINTA

SELECCIÓN DE HERRAMIENTA

Figura 21: Escala y selección de herramientas para realizar la detección de vulnerabilidades
Fuente: (Coteron Tene, 2012)

En esta investigación los valores se han obtenido como se observan en la figura 21 las 03 herramientas (ETTERCAP, CAÍN & ABEL Y WIRESHARK) son importantes y muy necesarias para efectuar la detección de las vulnerabilidades de los hosts seleccionados. Por eso el presente trabajo se hará uso de la herramienta ETTERCAP.

Justificación Científica: Según (Sudhakar, R, & K, 2017), justifica y realiza el uso de herramientas ETTERCAP, ARPWATH, WIRESHARK, ARPSPOOF, URLSNARF, NMAP-F, TPCDUMP, a fin de realizar un análisis comparativo de estas herramientas para la detección de envenenamiento por ARP.

Tools and Commands	Functions or Purposes
Ettercap	Scanning the network, ARP spoofing and Sniffing
ARPWATCH	Monitor Ethernet Activity (Detection) and Informing via mail
Wireshark	Sniffing (Packet capturing)
Arpspoof -i eth0	ARP spoofing
Urlsnarf -i eth0	Snarfing the url
Namp -F or Nmap	Port scan
TCP dump	Sniffing

Figura 22: Herramientas y Comandos y sus Funciones para detección de envenenamiento
Fuente: (Sudhakar, R, & K, 2017)

Parameters	Cryptography Scheme[8]	Centralized detection and validation server [7]	Passive detections (Wireshark)	Ettercap tool
Affinity of IP Exhaustion problems	yes	yes	no	no
Comply with single point of failure	no	no	yes	yes
IP Aliasing	yes	yes	no	no
Backward compatibility	no	yes	yes	yes

Figura 23: Parámetros por Herramientas para detección de envenenamiento
Fuente: (Sudhakar, R, & K, 2017)

Como se mencionó anteriormente, existen formas de realizar ataques fundamentados en vulnerabilidad e ineficacia de la red de datos como escuchas sin cifrado sólido beneficios que dependen en criptografía, pues otras personas pueden leer su información en la medida que navega por el sistema. Pues aquí, se están comparando las herramientas de hacking ético, que se utilizará en esta presente investigación. Como se ha justificado se hará uso de la herramienta ETTERCAP porque es una herramienta para la detección de envenenamiento.

ETTERCAP, es una herramienta multiplataforma que es utilizado para auditorias de redes ya no soporta direcciones pasivas y activas de distintos servicios o protocolos, puede interceptar y mejorar un ataque "hombre en el medio".

Proceso de Instalación:

Figura 24: Instalación Herramienta para Prueba Fuzz Testing

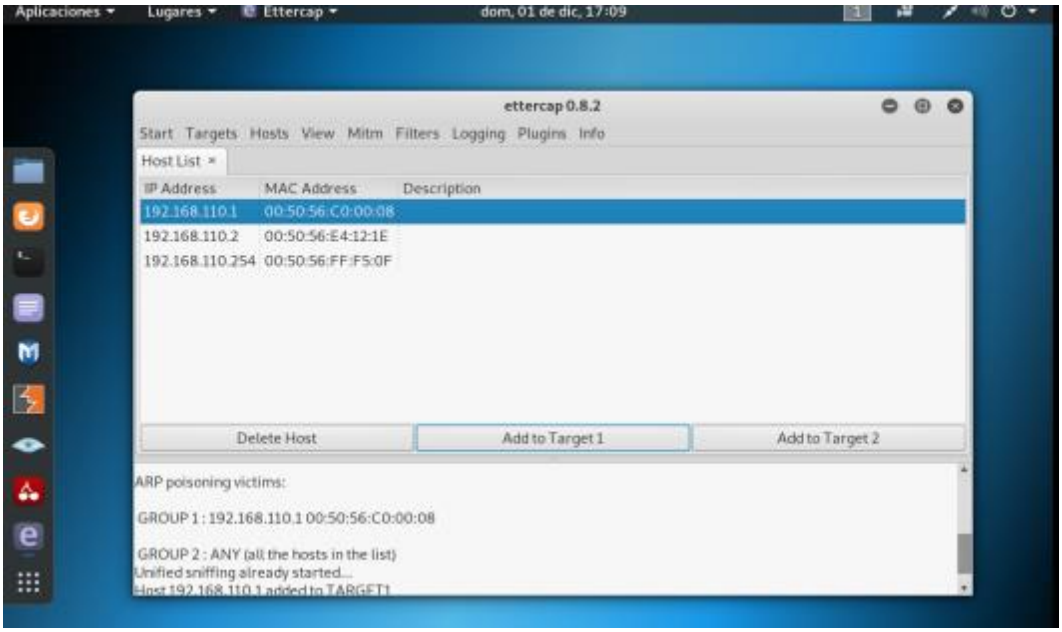


Figura 25: Uso de Herramienta Ettercap para Ataque de Hombre en medio
FUENTE: Reporte Sistema

3.1.3. Intrusión

El equipo del auditor que se ha utilizado para evaluar las técnicas de Ethical Hacking es una laptop de la red local con las siguientes características de red:

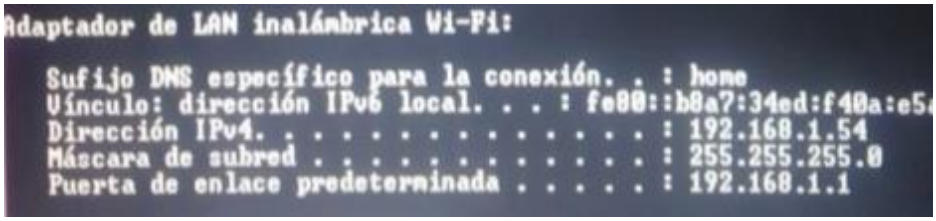


Figura 26: Equipo utilizado para la evaluación de técnicas

3.1.4. Ganando Acceso y Escalando Privilegios

Un resumen general acerca de los niveles de vulnerabilidades documentados en los reportes NESSUS, NMAP, permitiendo dar un mayor enfoque al objetivo de esta investigación.

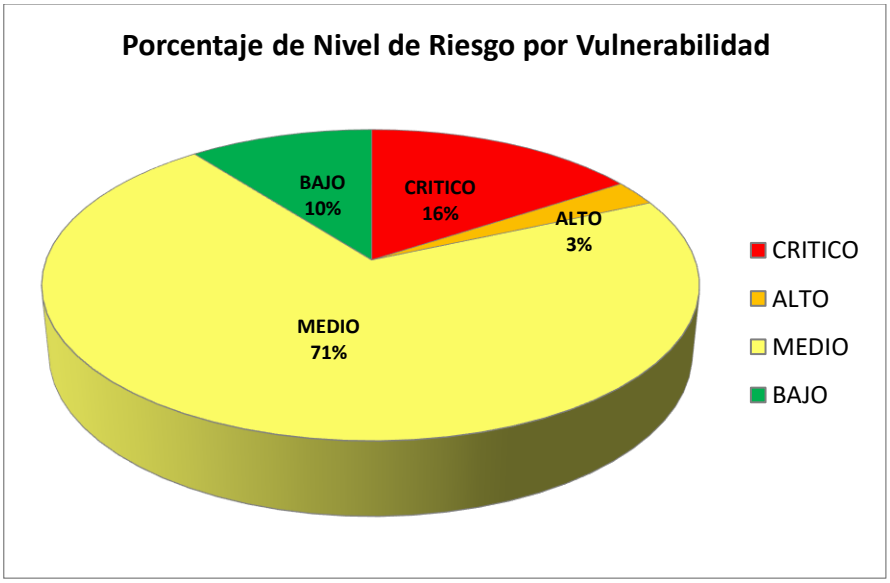


Figura 27: Reporte por nivel de riesgo por vulnerabilidad

En la figura 27, se observa que se detectaron a través del reporte todos los niveles de riesgos por vulnerabilidad, en la cual se indica que el 71% de las vulnerabilidades es de los siguientes niveles MEDIO, el 16% CRÍTICO, el 10% BAJO y 3% de ALTO.

3.1.5. Mapeo de la Red

Para evaluar las técnicas de Ethical Hacking, se ha tenido como escenario la topología actual de la empresa prestadora y se ha mapeado la red de datos con las herramientas anteriormente mencionadas, determinando la siguiente topología en el proyecto de investigación:

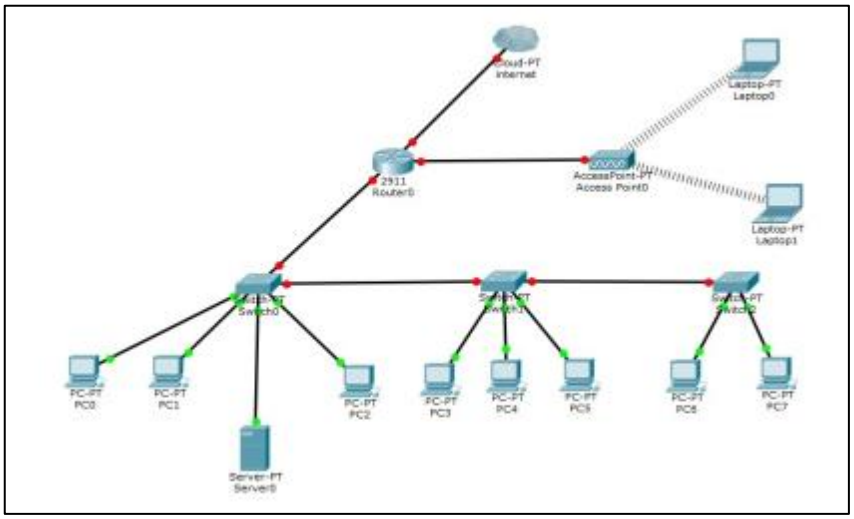


Figura 28: Topología actual de red de datos

Como se aprecia en la figura 28, se denota un crecimiento desordenado y en cascada lo que produce sobrecarga en el switch principal afectando en velocidad y capacidad a los equipos o dispositivos conectados.

Se detectan 14 dispositivos conectados y se observa que el cableado CAT 5E y 6 está deteriorado.

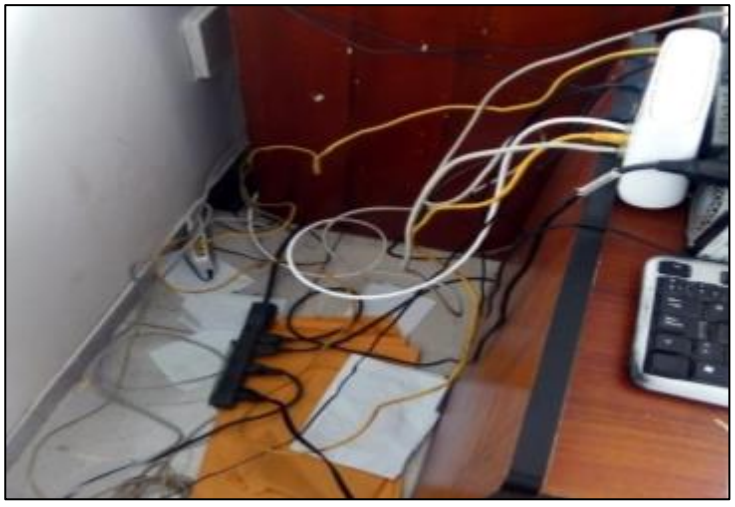


Figura 29: Cableado Actual de la Red de datos

3.1.6. FASE II: Identificación de Vulnerabilidades

En esta fase para la evaluación de las 03 técnicas hemos realizado la identificación de las vulnerabilidades utilizando las principales herramientas como es NESSUS, NMAP y ETTERCAP.

3.1.7. Técnica de Prueba de Penetración

El proceso consistió en realizar un análisis activo del sistema a través del escaneo a fin de buscar posibles debilidades en la red de la empresa prestadora.

Escaneo de Vulnerabilidades detectadas con Nessus.

Para la técnica de Prueba de penetración se ha realizado el escaneo de vulnerabilidades detectadas por hosts en la empresa prestadora de servicios, a través de la herramienta NESSUS SCAN. A continuación, el detalle:

192.168.1.1			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
SSL CERTIFICATE	935	ABIERTO	**MEDIO**
SSL AUTO CERTIFICATE		ABIERTO	**MEDIO**
IP Forwarding		ABIERTO	**MEDIO**
DHCP	6160	ABIERTO	BAJO
192.168.1.46			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
			INFO
192.168.1.54			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
MS		ABIERTO	**CRITICO**
MS		ABIERTO	**MEDIO**
SMB	233	ABIERTO	**MEDIO**
192.168.1.110			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
			INFO
192.168.1.111			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
SSL	935	ABIERTO	**MEDIO**
SSL CERTIFICATE		ABIERTO	**MEDIO**
SSL CIPHER		ABIERTO	**MEDIO**
SMB	233	ABIERTO	**MEDIO**
192.168.1.112			

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
SMB	233	ABIERTO	**MEDIO**
192.168.1.113			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
SMB	233	ABIERTO	**MEDIO**
192.168.1.115			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
SMB	233	ABIERTO	**MEDIO**
192.168.1.116			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
MS		ABIERTO	**CRITICO**
Microsoft RDP RCE		ABIERTO	**CRITICO**
Escritorio Remoto		ABIERTO	**CRITICO**
MS		ABIERTO	**ALTO**
SSL CERTIFICATE	935	ABIERTO	**MEDIO**
SSL AUTO CERTIFICATE		ABIERTO	**MEDIO**
Microsoft Security		ABIERTO	**MEDIO**
Escritorio Remoto		ABIERTO	**MEDIO**
SMB		ABIERTO	**MEDIO**
SSL sin hash		ABIERTO	**MEDIO**
SSL CIPHER	233	ABIERTO	**MEDIO**
Terminal Network		ABIERTO	**MEDIO**
Terminal Encryption		ABIERTO	**MEDIO**
SSL	935	ABIERTO	**BAJO**
Terminal Services		ABIERTO	**BAJO**
192.168.1.117			
PROTOCOLO	**PUERTO**	**ESTADO**	**NIVEL VULNERABILIDAD**
MS		ABIERTO	**CRITICO**
Escritorio Remoto		ABIERTO	**CRITICO**
SSL CERTIFICATE	935	ABIERTO	**MEDIO**
SSL AUTO CERTIFICATE		ABIERTO	**MEDIO**
Microsoft Security		ABIERTO	**MEDIO**
SMB		ABIERTO	**MEDIO**
SSL sin hash		ABIERTO	**MEDIO**
SSL CIPHER	233	ABIERTO	**MEDIO**
SSL	935	ABIERTO	**BAJO**

Tabla 5: Niveles de Vulnerabilidad Detectadas en la prueba de penetración
FUENTE: Elaboración Propia

Con la herramienta especializada de Nessus ha permitido documentar los resultados, a través de un informe detallado por cada host producto de la evaluación de la técnica de prueba de penetración.

El siguiente resultado de las vulnerabilidades encontradas por nivel de riesgo en la Empresa Prestadora.

HOTS	RESULTADO OBTENIDOS DEL ESCANEO				
	CRITICO	ALTO	MEDIO	BAJO	INFO
192.168.1.1	0	0	3	1	23
192.168.1.46	0	0	0	0	4
192.168.1.53	1	0	2	0	22
192.168.1.110	0	0	0	0	5
192.168.1.111	0	0	4	0	23
192.168.1.112	0	0	1	0	27
192.168.1.113	0	0	1	0	13
192.168.1.115	0	0	1	0	12
192.168.1.116	3	1	9	2	40
192.168.1.117	2	0	6	1	36
	6	1	27	4	205

Tabla 6: Resultados del escaneo de Vulnerabilidades en la prueba de Penetración
FUENTE: Elaboración Propia

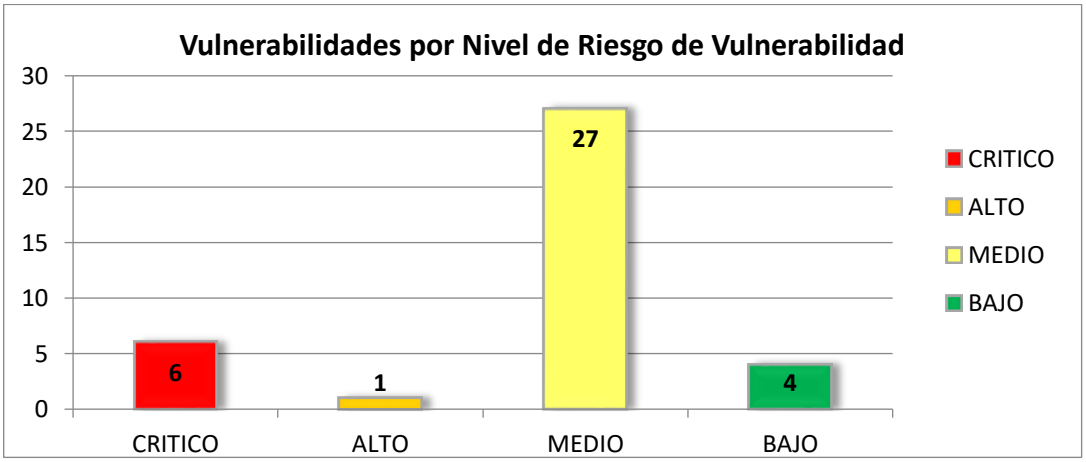


Tabla 7: Evaluación del riesgo por nivel de vulnerabilidad en la prueba de penetración:
FUENTE: Elaboración Propia

En la tabla 6 se muestra los tipos de niveles vulnerabilidades encontradas de acuerdo al porcentaje de cumplimiento en la empresa que se define en: ALTO cumplimiento del 3%, MEDIO cumplimiento del 71% y BAJO cumplimiento del 10% para este caso se consideran vulnerabilidades de nivel CRÍTICO cumplimiento del 16% consideradas vulnerabilidades potenciales.

3.1.8. Técnica de Prueba Pasiva

El proceso consistió en realizar un análisis del tráfico de telecomunicaciones. Detectando vulnerabilidades mediante puertos abiertos.

Escaneo de Vulnerabilidades detectadas con NMAP.

En detalle mostramos las direcciones IPs escaneadas en la red de la empresa.

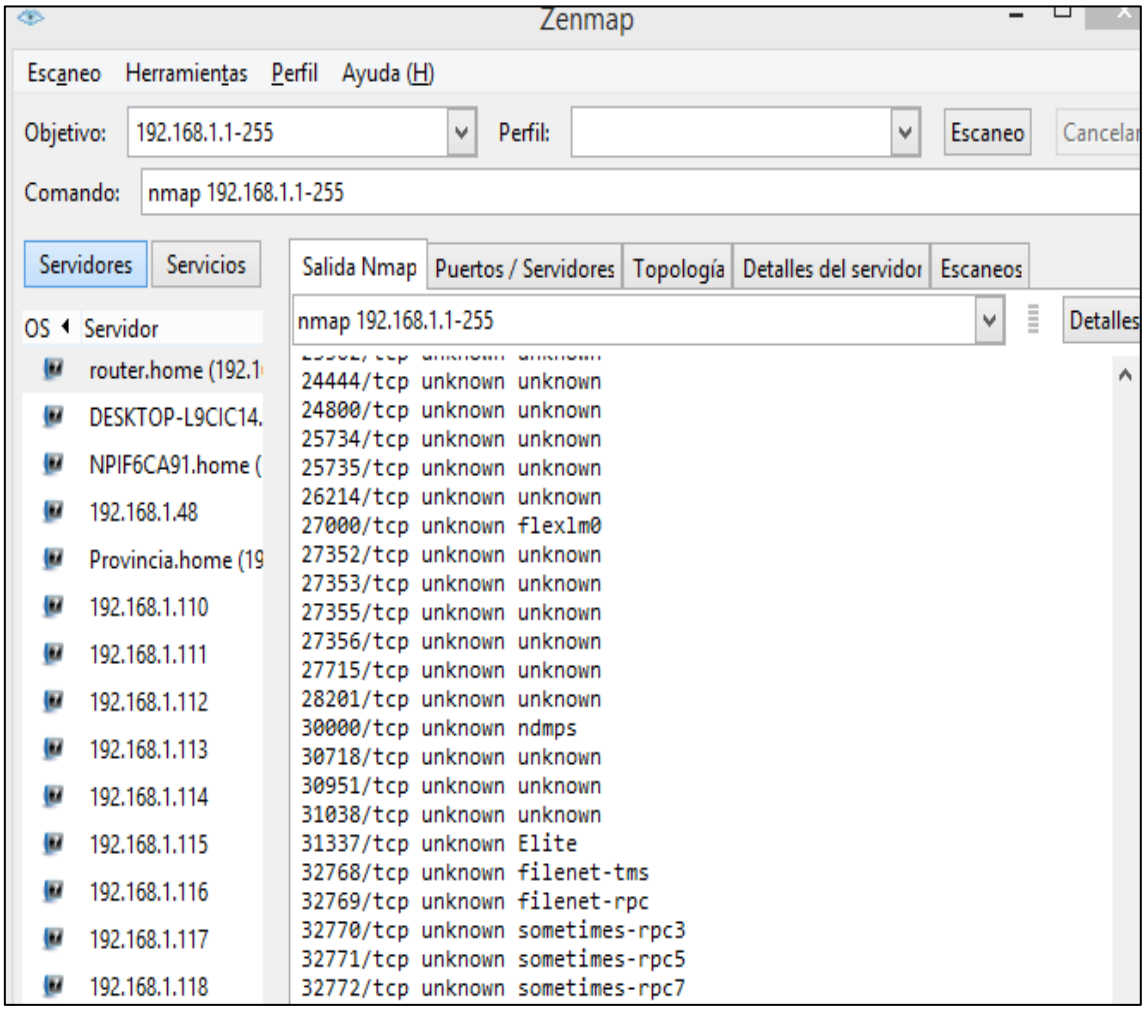


Tabla 8: Escaneo de Vulnerabilidades por direcciones IP en la Prueba Pasiva.
FUENTE: Reporte Nmap

A continuación se ha realizado el escaneo de vulnerabilidades detectadas por direcciones IP, a través de la herramienta especializada NMAP, (Durand , 2019).

192.168.1.1				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
80	TCP	OPEN	HTTP	NMAP
443	TCP	OPEN	HTTPS	NMAP
192.168.1.46				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
80	TCP	OPEN	HTTP	NMAP
443	TCP	OPEN	HTTPS	NMAP
515	TCP	OPEN	PRINTER	NMAP
631	TCP	OPEN	IPP	NMAP
3910	TCP	OPEN	PRNREQUEST	NMAP
3911	TCP	OPEN	PRNSTATUS	NMAP
192.168.1.110				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
192.168.1.111				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5040	TCP	OPEN	UNKNOWN	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
192.168.1.112				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
2869	TCP	OPEN	ICSLAP	NMAP
2968	TCP	OPEN	ENPP	NMAP
192.168.1.113				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
2968	TCP	OPEN	ENPP	NMAP
5040	TCP	OPEN	UNKNOWN	NMAP
5357	TCP	OPEN	WSDAPI	NMAP

192.168.1.114				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
2968	TCP	OPEN	ENPP	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
192.168.1.116				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
2869	TCP	OPEN	ICSLAP	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
5432	TCP	OPEN	POSTGRESQL	NMAP
192.168.1.117				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
2869	TCP	OPEN	ICSLAP	NMAP
2968	TCP	OPEN	ENPP	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
192.168.1.118				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
2869	TCP	OPEN	ICSLAP	NMAP
2968	TCP	OPEN	ENPP	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5357	TCP	OPEN	WSDAPI	NMAP

Tabla 9: Escaneo de vulnerabilidades de puertos por protocolo en Prueba Pasiva
FUENTE: **(Durand , 2019)**

Tabulada la información obtenemos el siguiente resultado de las vulnerabilidades encontradas por protocolo en la Empresa Prestadora.

	PROTOCOLOS															
IPs	HTTP	HTTPS	PRINTER	IPP	PRNREQUEST	PRNSTATUS	MSRPC	NETBIOS-SSN	MICROSOFT-DS	MS-WBT-SERVER	UNKNOWN	WSDAPI	RTSP	ICSLAP	ENPP	POSTGRESQL
192.168.1.1	1	1														
192.168.1.46			1	1	1	1										
192.168.1.110																
192.168.1.111							1	1	1	1	1	1				
192.168.1.112							1	1	1				1	1	1	
192.168.1.113							1	1	1		1	1			1	
192.168.1.114							1	1	1			1			1	
192.168.1.116							1	1	1	1		1	1	1		1
192.168.1.117							1	1	1	1		1	1	1	1	
192.168.1.118							1	1	1	1		1	1	1	1	
Total	1	1	1	1	1	1	7	7	7	4	2	6	4	4	5	1

Tabla 10: Resultado del escaneo de puertos abiertos en la Prueba Pasiva.
FUENTE: Reporte NMAP

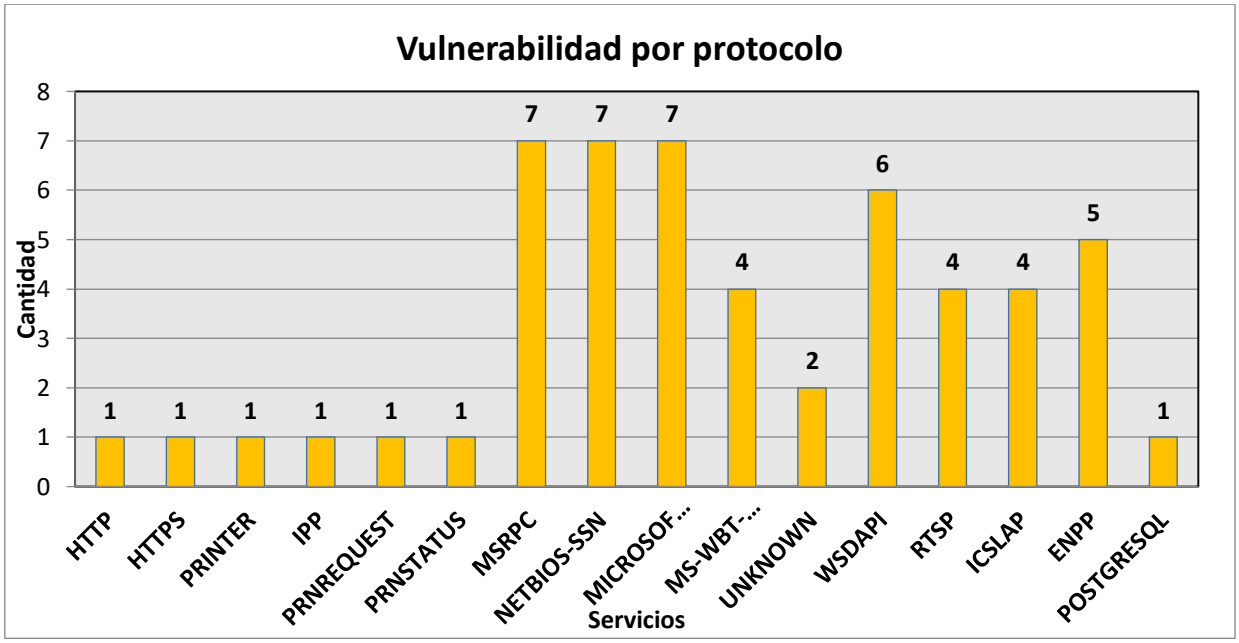


Figura 30: Resumen de vulnerabilidad detectadas por protocolo en la Prueba Pasiva.
FUENTE: elaboración propia

Como se observa en la figura 21, se detectaron vulnerabilidades por protocolos abiertos de más frecuencia en la red de datos, los mismos que se han clasificado de manera ordinal.

3.1.9. Técnica de Prueba Fuzz testing o Caja Negra.

El proceso consistió en realizar un análisis de datos aleatorios o archivos a evaluar, esto con la finalidad de evaluar y detectar los comportamientos que originen la violación del elemento de confidencialidad mediante los dispositivos conectados a la red.

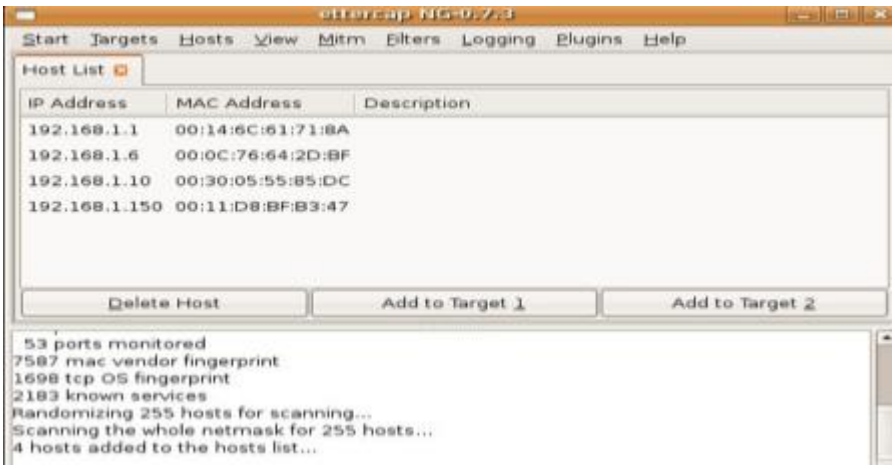


Figura 31: Ataque tipo Man in the Middle en la Prueba de Fuzztesting

Ataque tipo Man in the Middle detectados con ETTERCAP

La prueba MiTM se desarrolló utilizando un total de 100 archivos enviados a cada dispositivo en la red.

IP	ARCH RECIBIDOS	ARCH ENVIADOS	%ARCH CORRUPTOS
192.168.1.1	97	100	3
192.168.1.46	80	100	20
192.168.1.54	81	100	19
192.168.1.110	90	100	10
192.168.1.111	94	100	6
192.168.1.112	86	100	14
192.168.1.113	94	100	6
192.1681.115	86	100	14
192.168.1.116	96	100	4
192.168.1.117	88	100	12

Tabla 11: Resultado del Análisis de archivos a cada dispositivo en la Prueba Fuzz testing
FUENTE: Elaboración propia

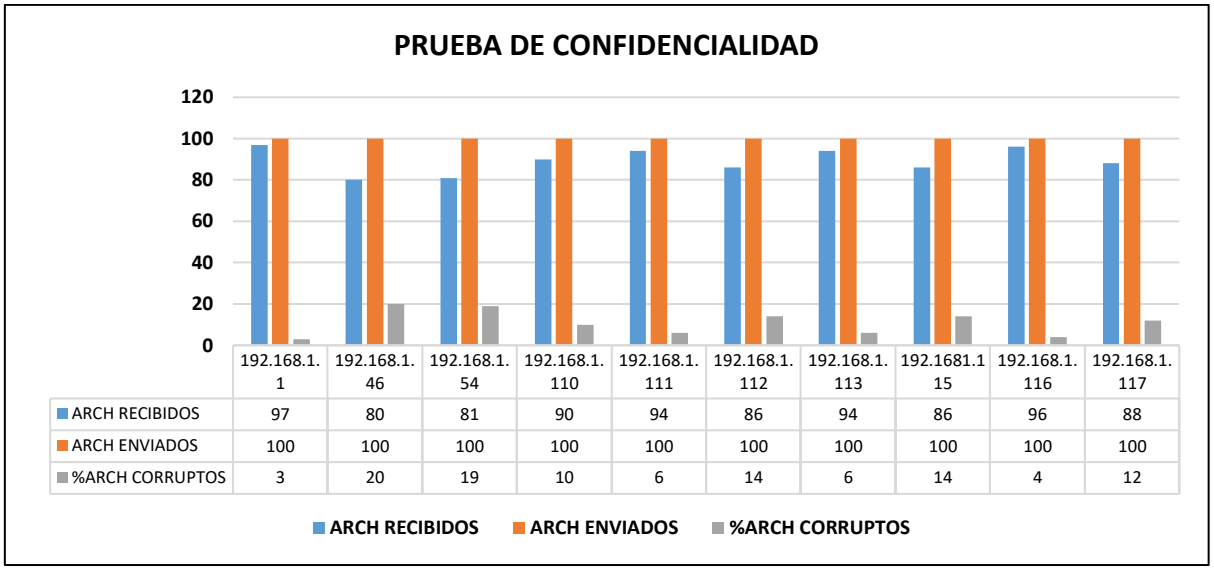


Figura 32: Resumen de vulnerabilidad detectada por archivos en la prueba de Fuzztesting

.

Se aprecia un porcentaje PROMEDIO sobre la red de datos, de los ARCHIVOS CORRUPTOS O DAÑADOS, que representa el 10.8% del total de archivos analizados.

3.1.10. FASE III: Mitigación de las Vulnerabilidades

Como escenario utilizado para la evaluación de las técnicas de Ethical Hacking para desarrollar las pruebas de instrucción, donde se encontraron vulnerabilidades las mismas que ya se encuentran clasificadas, y se va a proceder a mitigar las vulnerabilidades más críticas de la siguiente manera:

Técnica de Penetración: Vulnerabilidades clasificadas por Niveles

Vulnerabilidad Nivel Crítico:

Problema:

1. MS: Microsoft Security Login. Es decir, Certificado de autenticidad en licencia del Sistema Operativo detectado (LICENCIA NO ORIGINAL)
2. Escritorio Remoto activado. Algún intruso puede acceder de manera LOCAL y robar información vital para la empresa.

Medida de Mitigación:

1. Actualización y cambio de SISTEMA OPERATIVO a WINDOWS 10 1903, dado que Microsoft dejó de brindar soporte a Windows 7 y se encuentra vulnerable a cyber-ataques.
2. Desactivar Escritorio Remoto por cada host dentro de la red de trabajo.

Vulnerabilidades Nivel Alto:

Problema:

1. MS: Microsoft Security Login. Es decir, Certificado de autenticidad en licencia del Sistema Operativo detectado (LICENCIA NO ORIGINAL)

Medida de Mitigación:

1. Actualización y cambio de SISTEMA OPERATIVO a WINDOWS 10 1903, dado que Microsoft dejó de brindar soporte a Windows 7 y se encuentra vulnerable a cyber-ataques.

Vulnerabilidades Nivel Medio:

Problema:

1. SMB: Samba Server. Es decir, servicio de compartimiento y acceso libre de archivos sea en red o remota activado.
2. SSL CIPHER: Cifrado Secure Socket Layer. Es decir, capa de seguridad para cifrado de datos, dentro de un paquete.

Medida de Mitigación:

1. Si se comparte archivos, que sea exclusivamente usando el protocolo FTP en red, de tal manera que no tenemos puertos innecesariamente abiertos cumpliendo funciones de entrada a múltiples accesos no identificados.
2. Activar Antivirus y establecer cifrado de datos en los archivos con CLAVES HASH por archivo compartido.

Técnica de Prueba Pasiva: Vulnerabilidades clasificadas por puertos o protocolos abiertos

Problema:

1. Puertos Abiertos Encontrados:
2. Msrpc: Escritorio Remoto Windows
3. Netbios-Ssn, Microsoft-Ds, Ms Wbt-Server: Compartir Archivos En Red
4. Wsdapi: Tabla Arp De Direccionamiento Ip
5. Enpp: Impresión De Documentos En Red

Medida de Mitigación:

1. Desactivación de Escritorio Remoto
2. Activar compartido de archivos FTP
3. Desactivar la respuesta de broadcast de red
4. Compartir solo las impresoras necesarias

Técnica de Prueba Fuzztesting o Caja Negra: Vulnerabilidades clasificadas por ataque de archivos

Problema:

1. El porcentaje PROMEDIO de los archivos corruptos sobre la red de datos, representa al 10.8% del total de archivos enviados.

Medida de Mitigación:

1. Creación de correos corporativos y envío de archivos a través de los mismos.

En esta técnica se trabajó con la herramienta especializada Ettercap, efectuando un ataque a las conexiones de la red, envenenamiento de archivos.

3.2. Discusión de Resultados

De acuerdo a los indicadores se discuten los resultados.

Realizada la evaluación de las técnicas los tipos de niveles vulnerabilidades encontradas, puertos abiertos, y confidencialidad de acuerdo al porcentaje de cumplimiento en la empresa que se define del acuerdo a lo siguiente:
La técnica de penetración: ALTO cumplimiento del 3%, MEDIO cumplimiento del 71% y BAJO cumplimiento del 10% para este caso se consideran vulnerabilidades de nivel CRÍTICO cumplimiento del 16% consideradas vulnerabilidades potenciales.

En la técnica de prueba pasiva, se detectaron vulnerabilidades por protocolos abiertos, cabe resaltar que la función de cada protocolo debe ser cumplida siempre y cuando se esté utilizando y el estado se convierta de LISTENER a ESTABLISHED, es decir el puerto está escuchando en la red, los mismos que han clasificado de manera ordinal.

En la técnica de caja negra o Fuzztesting, según (Hurtado & Mendaño, 2016) menciona y detalla los elementos para realizar un ataque, en nuestro caso discutimos lo mencionado por los investigadores, ya que se ha podido realizar un ataques tipo Man- in- the- Middle, teniendo una de sus importantes características es el espionaje de conexiones y se hizo también el envenenamiento de archivos, pues consistió en escuchar todo el tráfico que genera el objetivo o víctima, teniendo como puerta de enlace una máquina o varias como escenario.

Los resultados obtenidos hacen referencia al nivel de riego encontrado, reconocimiento de puertos, y la confidencialidad ya que las técnicas de Ethical Hacking nos han permitido evaluar y diagnosticar que tan vulnerables es ingresar en una red de datos.

3.2.1. Resumen de la Metodología de evaluación de Técnicas de Ethical Hacking.

Se aplicó la metodología ISAAF, con el fin de evaluar y comparar las 03 técnicas de Ethical Hacking, lo cual es nuestro principal objetivo de ésta investigación.

METODOLOGIA DE EVALUACIÓN DE LAS TECNICAS	PRUEBA DE PENETRACIÓN	PRUEBA PASIVA	FUZZ TESTING
FASE I:			
1.- Recolección de la información	Herramienta Nessus	Herramienta Nmap	Herramienta Etthercap
2.- Intrusión	Red Local	Red Local	Red Local
3.- Ganando acceso y escalando privilegios	Privilegio de administrador de red LAN	Privilegio de administrador de red LAN	Privilegio de administrador de red LAN
4.- Mapeo de la red	Escanner IP y topología de red	Escanner IP y topología de red	Escanner IP y topología de red
FASE II:			
5.- Identificación de vulnerabilidades	1.- Licencias no originales	1.- MSRPC: Escritorio Remoto de Windows	1.-El porcentaje PROMEDIO de los archivos corruptos sobre la red de datos, representa al 10.8% del total de archivos enviados.
	2.- Escritorio Remoto activo	2.- NETBIOS-SSN, MICROSOFT-DS, WBT-SERVER: Archivos Compartidos	
	3.- Actualizaciones de Seguridad SO		
	4.- SMB Archivos Compartidos	3.- WSDAPI: Tabla ARP de direccionamiento IP	
	5.- SSL CIPHER: Cifrado de datos	4.- ENPP: Impresión de documentos en red	
FASE III:			
6.- Mitigación de Vulnerabilidades	1.- Compra de licencias W10 OLP	1.- Desactivación de Escritorio Remoto	1.- Creación de correos corporativos y envío de archivos a través de los mismos
	2.- Desactivación de Escritorio Remoto	2.- Activar compartido de archivos FTP	
	3.- Cambio o actualizacion al SO W10	3.- Desactivar la respuesta de broadcast de red	
	4.- Activar compartido de archivos FTP	4.- Compartir solo las impresoras necesarias	
	5.- Establecer claves hash por trasferencia de archivos		

Tabla 12: Resultado Evaluación de 03 técnicas de Ethical Hacking
FUENTE: Elaboración Propia

Según (Patil, Jangra, Bhale, Raina, & Kulkarmi, 2017), en su investigación sobre Ethical Hacking, el cual abordo el problema de la necesidad de seguridad cibernética, desarrollando un análisis del proceso de Ethical Hacking, el mismo que constó de 05 fases FASE 1: Reconocimiento. FASE 2: Escaneo. FASE 3: Obteniendo acceso. FASE 4: Manteniendo el acceso. FASE 5: Cubriendo huellas. Adicionalmente, se describieron las herramientas utilizadas para cada una de estas fases.

Es por ello que nuestra investigación, la comparamos con este estudio serio ya que hemos podido utilizar una metodología para evaluar técnicas y poder diagnosticar vulnerabilidades en una empresa prestadora, la cual ha sido nuestro escenario principal, de esta manera hemos podido también conocer la condición de la red y si está protegido ante cualquier ataque de intrusos.

3.2.2. Métricas para la evaluación de las Técnicas de Ethical Hacking

Se tomarán como normas para futuras políticas de seguridad las siguientes métricas para poder mejorar la seguridad de una red de datos en cualquier organización.

Para realizar esta evaluación hemos propuesto las métricas base, según el modelo CVSS.

METRICAS PARA LA EVALUACIÓN DE LAS TECNICAS	PRUEBA DE PENETRACIÓN	PRUEBA PASIVA	FUZZ TESTING
Vector de Acceso	Red Local	Red Local	Remoto
Complejidad de Acceso	Bajo	Bajo	Alto
Autenticacion	Simple	Simple	Simple
Impacto en el nivel de riesgo	Alto	Medio	Alto
Impacto en el reconocimiento de puertos	Alto	Alto	Bajo
Impacto en la confidencialidad	Bajo	Bajo	Alto
Facilidad de correccion	Correccion compleja	Correccion compleja	Correccion compleja
fiabilidad del informe de vulnerabilidad	Identificada y corregida	Identificada y corregida	Identificada y corregida

Tabla 13: Métricas para la Evaluación de Técnicas de Ethical Hacking.
FUENTE: Elaboración Propia

3.3. Aporte científico

3.3.1. Descripción de la empresa

INDUSTRIAS TRIVECA S.A.C, es una empresa realiza varios proyectos con las EPS a nivel nacional, actualmente tiene contratos en la Zona Norte donde aparte de la venta de medidores de agua potable también realiza servicios comerciales e informáticos y proyectos de telemetría y automatización.

La gestión de estos proyectos de la Gerencia de tecnologías de la información, dichos proyectos los viene trabajando actualmente en un sistema de escritorio hecho en lenguaje .Net y con la base de datos SQL Server 2008, la cual, tiene que pagar por licencia de software y actualmente tiene errores como falta de integridad de datos, diseño deficiente generando demoras en los procesos.

3.3.2. Métricas para el diagnóstico de vulnerabilidades

En la tabla 13 se definen nuevas métricas para iniciar el diagnostico de vulnerabilidades de hacking ético en la red de datos de la empresa prestadora de servicios. Se explica de la siguiente manera:

- **AV: VECTOR DE ACOSO**: se define como el objetivo a diagnosticar o explotar la vulnerabilidad, desde cualquier red.
- **AC: COMPLEJIDAD DE ACCESO:** dificultades que se presentan al momento de realizar el diagnóstico de la vulnerabilidad, es decir baja.
- **AU: AUTENTICACIÓN:** es decir, el usuario o cualquier tipo de privilegio de acceso al objetivo a diagnosticar.

- **IMPACTO EN EL NIVEL DE RIESGO:** nivel de vulnerabilidades detectadas (Alto = Crítico, Medio=Alto, Bajo= Normal).
- **RP: IMPACTO EN EL RECONOCIMIENTO DE PUERTOS:** nivel de riesgo en puertos abiertos innecesarios.
- **C: IMPACTO EN LA CONFIDENCIALIDAD:** Transmisión de datos en un entorno seguro. En este caso el impacto es total.
- **FC: FACILIDAD DE CORRECIÓN:** Nivel de complejidad para aplicar una solución al problema encontrado.
- **IV: FIABILIDAD DEL INFORME DE VULNERABILIDAD:** Aplicación de soluciones en un entorno real, en tiempo real y para futuros ataques en la empresa.

Estas métricas nos permiten establecer niveles y discriminar tipos de ataques en tiempo real, con el fin de obtener soluciones de acuerdo al nivel de complejidad de la vulnerabilidad encontrada.

Visión

La empresa prestadora de servicios INDUSTRIAS TRIVECA SAC, para el año 2020 será reconocida como la empresa con mayor eficacia en resolución de problemas y de calidad en el servicio de agua potable en la REGION PIURA.

Objetivos Institucionales:

- Ofrecer un servicio eficaz a los clientes
- Controlar en tiempo real las fallas detectadas por los usuarios que afectan al servicio de agua potable.
- Contar con el factor humano eficiente en la detección y mitigación de ataques en tiempo real a la Institución.
- Obtener buenas referencias de los usuarios por el servicio brindado.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1.Conclusiones

a) En la presente investigación, hemos definido y evaluado 03 técnicas de Ethical Hacking, para el diagnóstico de vulnerabilidades en una red de datos de la empresa prestadora, las técnicas definidas fueron pruebas de penetración, pruebas pasivas, y pruebas de caja negra o fuzztesting.
b) La situación actual de la seguridad informática de la empresa prestadora es deficiente, dado que presenta muchas falencias en su estructura física y lógica, estando expuesto a futuros ataques.
c) Se identificó que las principales debilidades, al momento de la evaluación de las técnicas, son permanecer en una red LAN local, y mantener el acceso con altos privilegios, lo cual son muy vulnerables a posibles ataques externos.
d) Se encontraron vulnerabilidades con niveles críticos, lo cual permite ataques sin posibilidad alguna de poder repelerlos.
e) Se propusieron lineamientos de seguridad, para garantizar la confidencialidad y reducir el nivel de riesgos, de igual manera, reducir el número total de puertos abiertos, ya que esto se convierte a múltiples puertas de acceso para atacantes externos, y finalmente plantear medidas de mitigación a las vulnerabilidades clasificadas.

4.2.Recomendaciones

a) Se recomienda implementar las técnicas de Ethical Hacking, evaluadas en la presente investigación, estas técnicas van a permitir aplicar, examinar y minimizar los riesgos de vulnerabilidades ya detectadas en una red de datos de la empresa prestadora.
b) Se recomienda rediseñar la estructura física de la empresa prestadora, y de esta manera se puede reducir tiempos en la transferencia de la información de manera unidireccional decir aplicando topología estrella, con el fin de obtener agilidad en cuanto a trasmisión de datos y por ende evitar ataques externos.
c) Se recomienda a la empresa prestadora gestionar adecuadamente los accesos o privilegios de usuarios, controlando la seguridad en la conexión de la red pública o privada, revisando eventos y actividades criticas llevadas a cabo por los usuarios.
d) Es importante que las actualizaciones de firmware en el hardware de red, de esta forma se pueda detectar nuevas debilidades críticas o corregir de manera inmediata, además de actualizar licencias, firewalls, versiones, etc., de cada uno de los servicios.
e) Se recomienda la adquisición de un software para realizar continuamente análisis de vulnerabilidades, proponiendo lineamientos de seguridad y confidencialidad con el propósito de simular ataques examinados y plantear mecanismos de mitigación, en caso producirse por un atacante externo.

REFERENCIAS

27001 ACADEMY. (2018). Disponible en http://advisera.com/27001academy/es/.

27001:2014, NORMA TÉCNICA PERUANA NTP-ISO/IEC. (2014). PECERT Sistema de Coordinación de la Administración Pública. Coordinación de Emergencias en Redes Teleinformáticas. Disponible en http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf.

Acosta, O. (2013). Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaria nacional de gestión de riesgos utilizando metodologías de ethical hacking. Escuela Politécnica Nacional - EPN, Quito, Ecuador. Recuperado de: https://bibdigital.epn.edu.ec/handle/15000/6059

Aguilar, S. & De la Cruz, V. (2015). Implementación de una solución de Hacking Ético para mejorar la seguridad en la infraestructura informática de la Caja Municipal de Sullana – Agencia Chimbote. (Bachelor's thesis). Recuperado de: http://repositorio.uns.edu.pe/handle/UNS/1964

Astudillo, K. (2017). Hacking ético 101. Babelcube Inc.

Banda, R.; Phiri, J.; Nyirenda, M. & Kabemba, M. (2019). Technological Paradox of Hackers Begetting Hackers: A Case of Ethical and Unethical Hackers and their Subtle Tools. The University of Zambia, UNZA. Lusaka, Zambia. Recuperado de: https://www.researchgate.net/publication/331952715

Cornejo, G. & Manchola, S. (2016). Investigación sobre el Hacker y sus posibles comienzos en la comunidad estudiantil. Caso Universidad Piloto de Colombia. 8th Euro American Conference on Telematics and Information Systems. Recuperado de: http://repository.unipiloto.edu.co/handle/20.500.12277/1132

Días, C. (2014). Hacking ético y seguridad en red. Trabajo Final de Carrera. Universitat Oberta de Catalunya UOC, Barcelona, España. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/34501/7/cdiasTFC0614memoria.pdf

ETIC Solutions. (2017). Análisis de Vulnerabilidad. Recuperado de https://etic-solutions.net/etic/servicios/analisis-de-vulnerabilidades.

Fernández, C. (2017). Análisis Comparativo de Técnicas de Cifrado utilizadas en la confidencialidad de la información en una Red Privada Virtual. Tesis de Grado. Universidad Nacional Pedro Ruiz Gallo, Chiclayo. Recuperado de: http://repositorio.unprg.edu.pe/handle/UNPRG/3139

Fernández, D. & Pacheco, O. (2014). Mejora de seguridad de información en la Comandancia de Operaciones Guardacostas basada en la Norma Técnica Peruana NTP-ISO/IEC 27001:2008. Universidad de San Martín de Porres, Lima, Perú. Ingeniería de Computación y Sistemas. Recuperado de: http://www.repositorioacademico.usmp.edu.pe/handle/usmp/1470

Franco, G. (2019). Análisis de vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería En Networking y Telecomunicaciones). Recuperado de: http://repositorio.ug.edu.ec/handle/redug/39259

Giannone, A., Amatriain, H., Rodríguez, D., & Merlino, H. (2018). Método de inclusión de Hacking ético en el proceso de testing de software. In XXIV Congreso Argentino de Ciencias de la Computación (La Plata, 2018). Recuperado de: http://sedici.unlp.edu.ar/handle/10915/73243

Gómez, J. (2015). Introducción al Hacking Ético de sistema y redes. School of Hacking. UGR Cyber Security Group. Recuperado de: https://ucys.ugr.es/download/taller1/Taller1_Intro_hacking.pdf

Gómez, L. & Andrés, Á. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. 2ª edición Asociación Española de Normalización y Certificación, AENOR.

Hernández, M.; Baquero, L. & Gil, C. (2018). Ethical Hacking on Mobile Devices: Considerations and practical uses. Fundación Universitaria Los Libertadores, Bogotá D.C., Colombia. Recuperado de: https://www.researchgate.net/publication/331718779

Himanen, P & Castells, M. (2002). La ética del hacker y el espíritu de la era de la información. España: Editorial Desino.

Hurtado, M. & Mendaño, L. (2016). Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado (Bachelor's thesis, Quito, 2016.). Recuperado de: https://bibdigital.epn.edu.ec/handle/15000/16836

Kumar, S. & Agarwal, D. (2018). Hacking Attacks, Methods, Techniques And Their Protection Measures. Sangam University, Bhilwara, India. Recuperado de: https://www.researchgate.net/publication/324860675

López, R. (2015). Propuesta de implementación de una metodología de auditoría de seguridad informática. Universidad Autónoma de Madrid. Recuperado de: https://repositorio.uam.es/handle/10486/668900

Maco, A. (2008). Formulación de un Plan de Seguridad de Información Aplicando las Normas ISO 27001 y 27002: De la Universidad Católica Santo Toribio de Mogrovejo.

Mammar, A., Cavalli, A., & Jimenez, W. (2011). Using testing techniques for vulnerability detection in C programs. Testing Software and Systems, 80–96. Recuperado de http://link.springer.com/chapter/10.1007/978-3-642-24580-0_7

Niño, N. (2018). Modelo de un Sistema de Gestión de Seguridad de la Información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática – INEI Filial Lambayeque. Tesis de Post Grado. Universidad Nacional Pedro Ruiz Gallo, Chiclayo. Recuperado de: http://repositorio.unprg.edu.pe/handle/UNPRG/1938

Oñate, O. & Martínez, C. (2017). Mejoras en la Seguridad de la Red Inalámbrica de la Universidad Nacional de Chimborazo, aplicando Hacking Ético. Universidad Nacional de Chimborazo, Riobamba, Ecuador. Recuperado de: http://dspace.unach.edu.ec/handle/51000/4170.

Ortiz, B. (2015). Hacking ético para detectar fallas en la seguridad informática de la intranet del Gobierno Provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGS), basado en la norma ISO/IEC 27001: 2005 (Bachelor's thesis). Recuperado de: http://repositorio.utn.edu.ec/handle/123456789/4332.

Patil, S.; Jangra, A.; Bhale, M.; Raina, A. & Kulkarni, P. (2017). Pimpri Chinchwad College of Engineering (PCCOE). Recuperado de: https://ieeexplore.ieee.org/document/8391982

Rocha, D.; Kreutz, D. & Turchetti, R. (2017). A free and extensible tool to detect vulnerabilities in Web systems. Iberian Conference on Information Systems and Technologies, CISTI. Madrid, España. Recuperado de: https://ieeexplore.ieee.org/document/6263139.

Gonzales, B. (2016). Uso de herramientas de Ethical hacking con kali Linux para el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la sede central de la Universidad de Huánuco. Recuperado de http://repositorio.udh.edu.pe/bitstream/handle/123456789/675/GONZALES%20COTERA%20BERNIER.pdf?sequence=1&isAllowed=y

Sreenivasa, R., & Kuman, N. (2012). International Journal of Enterprise Computing and Business Systems ISSN (Online): 2230-8849 Web Application Vulnerability Detection Using Dynamic Analysis. International Journal of Enterprise Computing and Business Systems ISSN (Online): 2230-8849, 2(1).

Ushmani, A. (2018). Ethical Hacking. Western Governor University. Salt Lake City, Utah. Recuperado de: https://www.researchgate.net/publication/331481853

Vallejo, M. R. L. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. Revista Publicando, 4(10 (1)), 31-51. Recuperado de: https://revistapublicando.org/revista/index.php/crv/article/view/407

Morales, F. (2015). Modelo De Inventario Abc Para Mejorar El Proceso Logístico De La Compañía Invita Sede Lima-2014. Recuperado de http://repositorio.uss.edu.pe/bitstream/handle/uss/3028/TESIS%202.pdf?cv=1&sequence=1

Wolf, G., & Soria Guzmán, I. (2016). Ética Hacker, seguridad y vigilancia. Recuperado de: http://ru.iiec.unam.mx/

Zhang, X.; Shao, L. & Zheng, J. (2008). A Novel Method of Software Vulnerability Detection based on Fuzzing Technique. Recuperado de: https://ieeexplore.ieee.org/abstract/document/4770021

Rina Elizabeth López De Jiménez (2017), Pentesting para las organizaciones por que la aplicación web sea más rápida o que desarrollen un mejor software. https://ieeexplore.ieee.org/abstract/document/7942364.

Yien Wang, Jianhua Yang (2017), Ataque ético y defensa de la red: elija su mejor herramienta de exploración de vulnerabilidades de red https://ieeexplore.ieee.org/document/7929663.

W. Hasala Peiris, Helen Armstrong (2014), Un enfoque de Análisis de Vulnerabilidades de acceso Sistema de Información de organizaciones. https://ieeexplore.ieee.org/document/6609194.

ISACA (2018). Cybersecurity Fundamentals Online Course. Retrieved from https://www.isaca.org/Education/on-demand-learning/pages/cybersecurity-fundamentals-online-course.aspx

Tecnología & Informática (2019). Vulnerabilidades informáticas: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

Hernández, Fernández, y Baptista. (2014). Metodología de la investigación. México: Mc Graw Hill Ediciones.

Bermeo O. (2017). Implementación de hacking ético para la detección y evaluación de vulnerabilidades de red en la empresa complex del Perú S.A.C.-Tumbes; 2017". Recuperado de http://repositorio.uladech.edu.pe/handle/123456789/10386.

Hernández, L. & Mejía, J. (2015). Guía de Ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. Recuperado de https://www.redalyc.org/articulo.oa?id=512251501005.

Durand D. (2019). Reporte de red de datos con herramientas de Hacking Ético, escaneo de puertos con Nmap.

Cruz S. (2014). Aplicación de auditoría penetration testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa Data Business SAC, Trujillo. http://repositorio.upn.edu.pe/handle/11537/10239?show=full

David A. Franco, Jorge L. Perea y Luis C. Tovar (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios.

https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

María Elizabeth Narváez Portillo (2015). Análisis de La Distribución Kali Linux, su Aplicación en la Configuración de un Sistema Detector de Intrusiones y La Validación del Sistema en la Red de Datos de la Sede Sur en Quito de la Universidad Politécnica Salesiana.

https://dspace.ups.edu.ec/bitstream/123456789/10179/1/UPS%20-%20ST001825.pdf

R. Sri Devi; M. Mohan Kumar (2020) Prueba de la debilidad de la seguridad de las aplicaciones web mediante Ethical Hacking https://ieeexplore.ieee.org/document/9143018

Waheed Ali H. M. Ghanem; Baharí Belaton (2013). Improving accuracy of applications fingerprinting on local networks using NMAP-AMAP-ETTERCAP as a hybrid framework. https://ieeexplore.ieee.org/document/6719998

María Fernanda Coteron Tene (2012). Técnica sniffer para detectar vulnerabilidades en el servidor web, mail y ftp del Hospital Regional docente Ambato.

https://repositorio.uta.edu.ec/bitstream/123456789/2895/1/Tesis_t759si.pdf

Sudhakar; R. K. Aggarwal (2017). A Survey on Comparative Analysis of Tools for the detection of ARP Poisoning Recuperado de https://ieeexplore.ieee.org/document/8343546

ANEXOS

ANEXOS

Anexo 01: Matriz de Consistencia Lógica

Tipo de investigación	Problema	Variables	Indicadores	Población	Muestra	Método de recolección de Datos	Técnicas de procesamiento de datos
De acuerdo a su naturaleza, el estudio planteado es del tipo cuantitativo.	¿Cómo la evaluación de las técnicas de Ethical Hacking influyen en el diagnóstico de vulnerabilidades de la seguridad informática en las empresas prestadoras de servicios?	1. VARIABLE INDEPENDIENTE Técnicas de Hacking Ético. 2. VARIABLE DEPENDIENTE Seguridad de la Información.	VARIABLE INDEPENDIENTE Métricas para clasificación de Técnicas de Hacking Ético VARIABLE DEPENDIENTE $NRV = \frac{N_v}{NTV} X100\%$ NRV= Nivel de riesgo de vulnerabilidad Nv= Número total de vulnerabilidades por nivel de riesgo NTV= Número total de vulnerabilidades detectadas $C = \frac{AE - AR_D}{AE} \text{ x } 100$ AE= Total de archivos evaluados ⟦AR⟧_d= Total de archivos recibidos dañados.	Las técnicas de Ethical Hacking. 1. Black-box, 2. White-box, 3. Análisis estático de código, 4. Pruebas de penetración, 5. Pruebas pasivas, 6. Pruebas activas, 7. Fuzz testing.	03 técnicas de Ethical Hacking: 1. Prueba de penetración 2. Pruebas Pasivas 3. Fuzz Testing	Como instrumentos de medición de datos se consideran: 1. Test de pruebas. 2. Análisis de tráfico de red 3. Observación de cableado estructurado	se utilizó las fases de la metodología ISSAF 1. Fase 1: Planeación y Preparación. 2. Fase 2. Evaluación. 3. Fase 3. Presentación de Informes. Se estimarán, mediante cuadros estadísticos, los valores cuantitativos, confidencialidad y porcentajes de los resultados.

Diseño de investigación	Hipótesis	Objetivo General	Objetivos específicos	Método propuesto y desarrollado	Resultados preliminares
Por su naturaleza, el estudio corresponde al tipo de diseño cuasi experimental.	H_0= La evaluación de Técnicas de Ethical Hacking influirán en el diagnóstico la seguridad informática, estableciendo niveles de riesgo, reconocimiento y confidencialidad en una empresa prestadora de servicios.	Evaluar técnicas de Ethical hacking sobre la seguridad informática de una red de datos que permitan el diagnóstico de vulnerabilidades en una empresa prestadora de servicios.	a. Definir técnicas de Ethical Hacking para el diagnóstico de vulnerabilidades en una empresa prestadora de servicios. b. conocer la situación actual de la seguridad informática, implementando técnicas sobre una red de datos, dentro de una empresa prestadora de servicios. c. Identificar las debilidades usando las técnicas de Ethical Hacking sobre la seguridad informática en una empresa prestadora de servicios. d. Clasificar las vulnerabilidades detectadas sobre la Seguridad informática en empresa prestadora de servicios. e.Proponer lineamientos de seguridad para garantizar la confidencialidad, integridad y disponibilidad en una red de datos de una empresa prestadora de servicios, postulando medidas de mitigación de las vulnerabilidades ya clasificadas.	"Se propone la implementación del Método Propuesto en base a 6 actividades: 1.Se definirán técnicas de Ethical Hacking para el diagnóstico de vulnerabilidades en una empresa prestadora de servicios. 2. se conocerá la situación actual de la seguridad informática sobre una red de datos usando 03 técnicas de hacking ético 3. se van a identificar las debilidades de las técnicas de hacking ético sobre la seguridad informática 4. Clasificar las vulnerabilidades detectadas sobre la Seguridad informática 5. Mitigar las vulnerabilidades ya clasificadas, estableciendo lineamientos de seguridad para garantizar la confidencialidad, disponibilidad e integridad en una red de datos 6. Evaluar de las técnicas aplicadas de Hacking Ético sobre la seguridad informática. Este método propuesto nos brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de la seguridad informática. En cuanto a las pruebas propuestas, se propone desarrollar la Metodología ISSAF"	1. Se espera evaluar técnicas de Ethical Hacking que detecte vulnerabilidades a la seguridad informática en una empresa prestadora de servicios. 2. Se espera poder documentar una serie de pasos que permitan garantizar la seguridad, confidencialidad e integración de la información que se encuentra en la infraestructura de la red interna de una empresa prestadora de servicios. 3. Se espera mitigar las vulnerabilidades de una red de datos a través de las técnicas y herramientas de Hacking Ético.

Anexo 1: Matriz de Consistencia Lógica

Anexo 2

INFORMES DE PRUEBAS

REPORTES NESSUS

REPORTES NMAP

REPORTES ETTHERCAP

My Basic Network Scan

Report generated by Nessus™ Tue, 08 Oct 2019 09:59:01 GMT-0500

For Trial Use Only

TABLE OF CONTENTS

Hosts Executive Summary

For Trial Use Only

Hosts Executive Summary

For Trial Use Only

192.168.1.1

Vulnerabilities Total: 27

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	50686	IP Forwarding Enabled
LOW	3.3	10663	DHCP Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	11936	OS Identification
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported

For Trial Use Only

INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	22964	Service Detection
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

192.168.1.46

Vulnerabilities Total: 4

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	11933	Do not scan printers
INFO	N/A	14274	Nessus SNMP Scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

For Trial Use Only

192.168.1.53

Vulnerabilities Total: 25

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	11414	IMAP Service Banner Retrieval
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection

For Trial Use Only

INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	18528	SMTP Server Connection Check
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.1.110

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	5

Vulnerabilities Total: 5

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	19506	Nessus Scan Information

For Trial Use Only

192.168.1.111

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	23

Vulnerabilities — Total: 27

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported

For Trial Use Only

INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

192.168.1.112

Vulnerabilities Total: 28

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

For Trial Use Only

INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.1.113

Vulnerabilities Total: 14

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

For Trial Use Only

192.168.1.115

Vulnerabilities Total: 13

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

For Trial Use Only

192.168.1.116

Vulnerabilities Total: 55

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure

For Trial Use Only

INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	26024	PostgreSQL Server Detection
INFO	N/A	66173	RDP Screenshot
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information

INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled
INFO	N/A	66717	mDNS Detection (Local Network)

192.168.1.117

2	0	6	1	36
CRITICAL	HIGH	MEDIUM	LOW	INFO

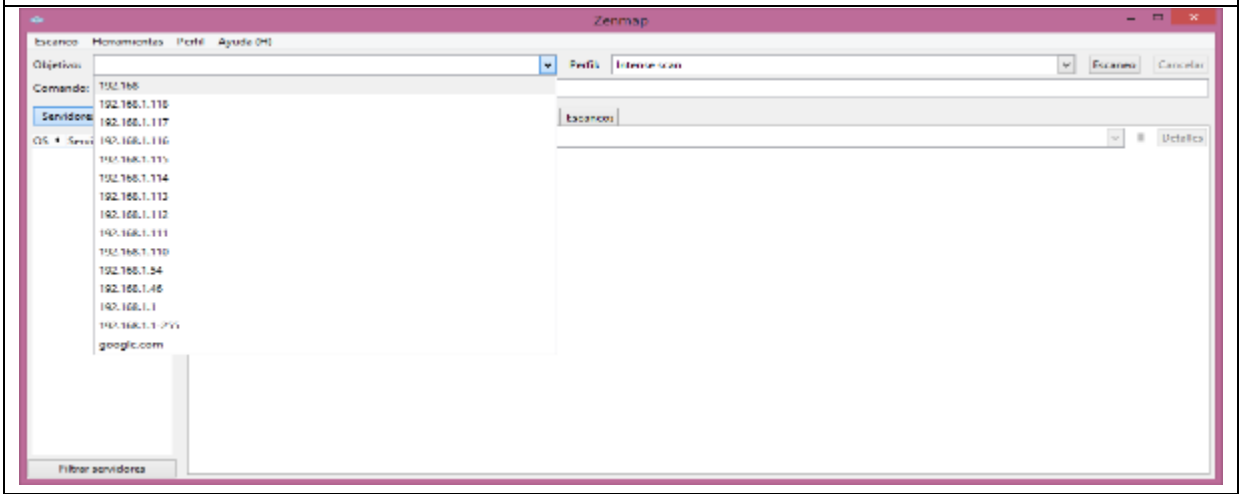
Vulnerabilities Total: 45

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address

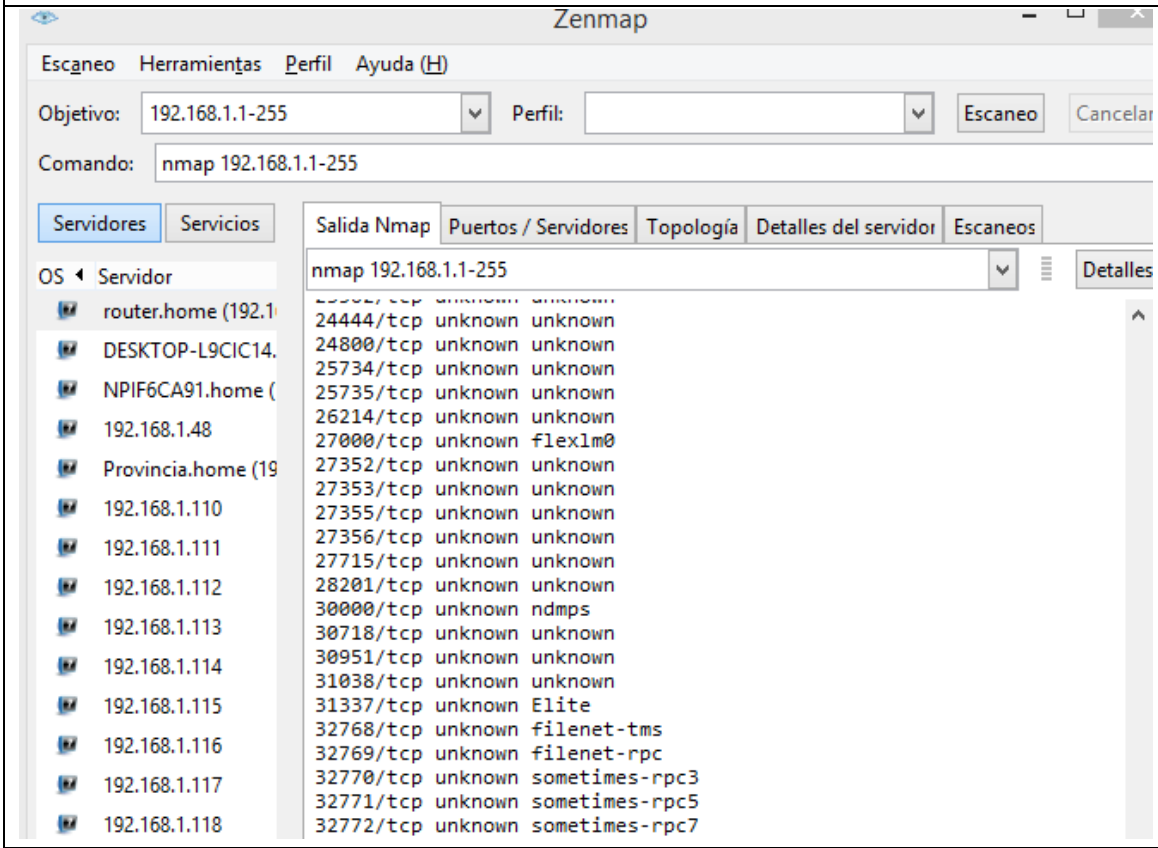
For Trial use only

INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information

INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

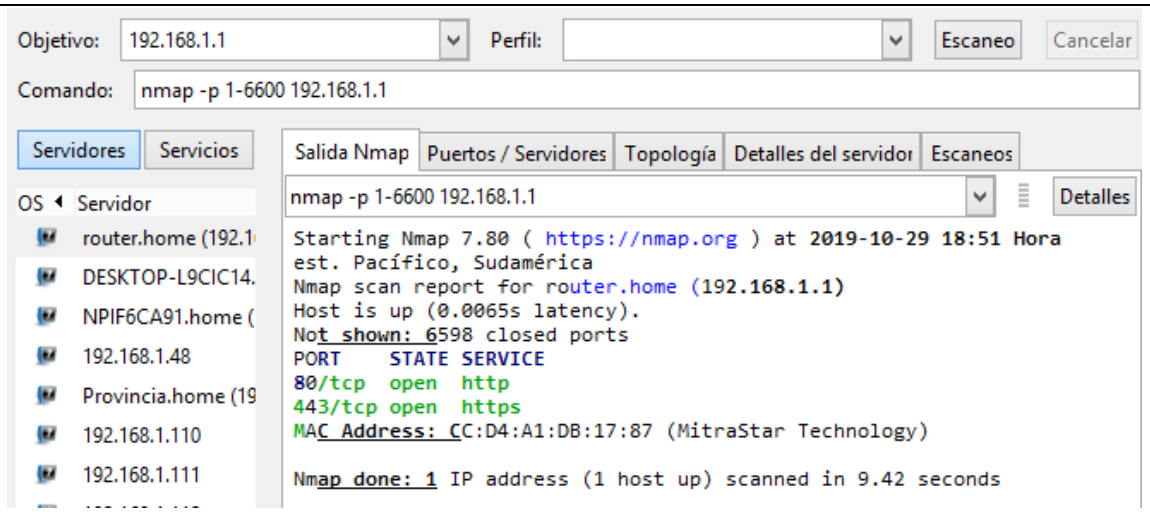


ESCANEO DE IPs EN LA RED DE DATOS

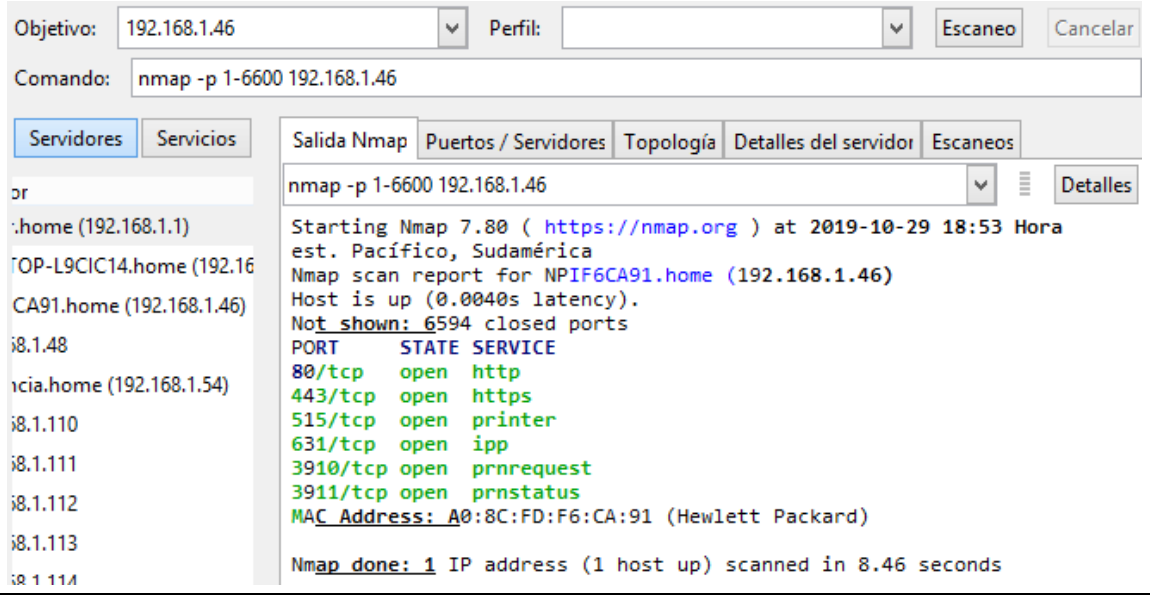


ESCANEO DE PUERTOS POR PC

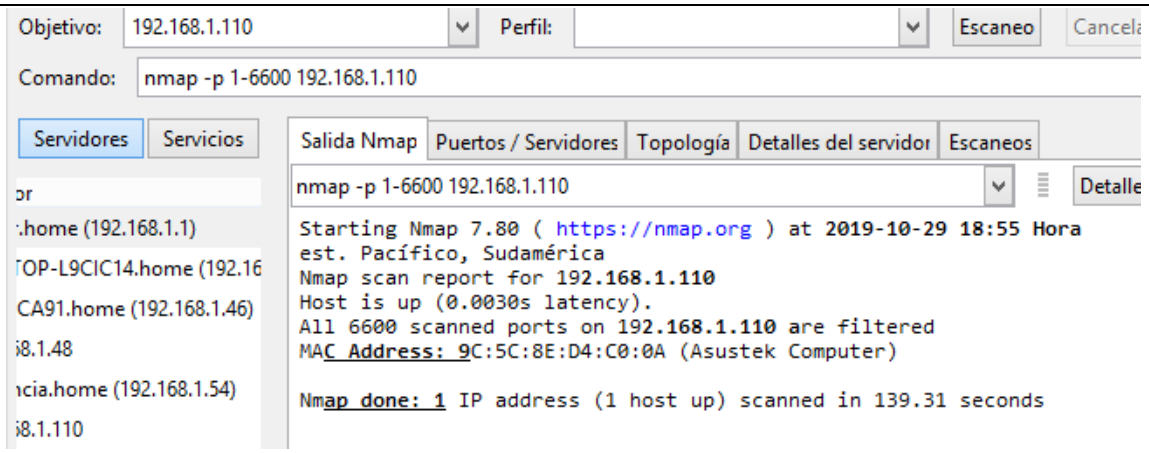
192.168.1.1



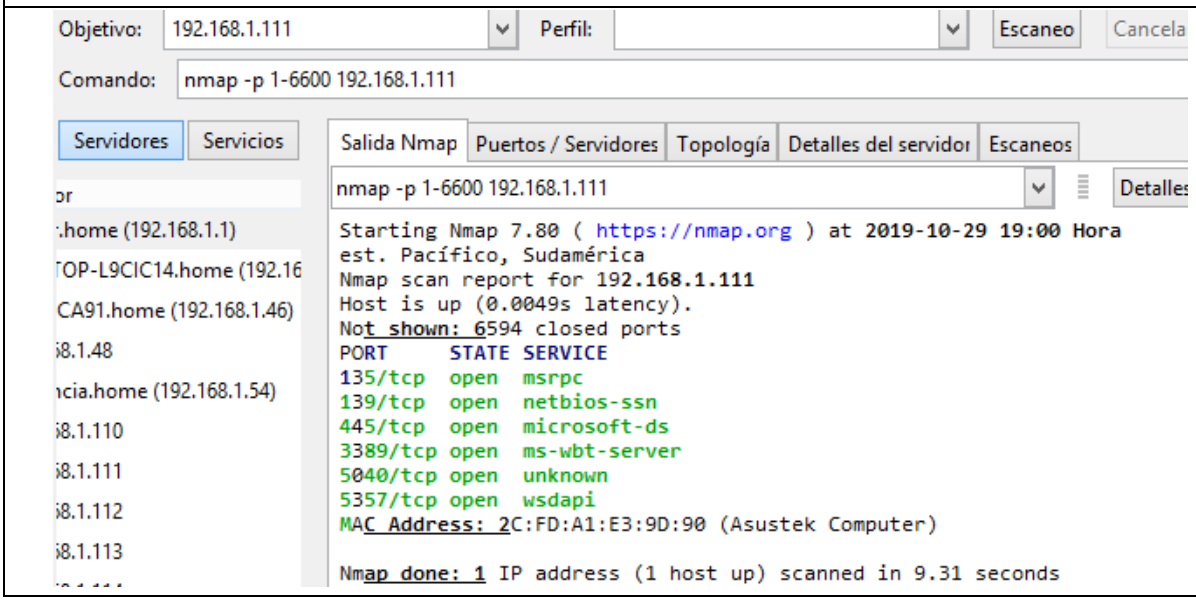
192.168.1.46



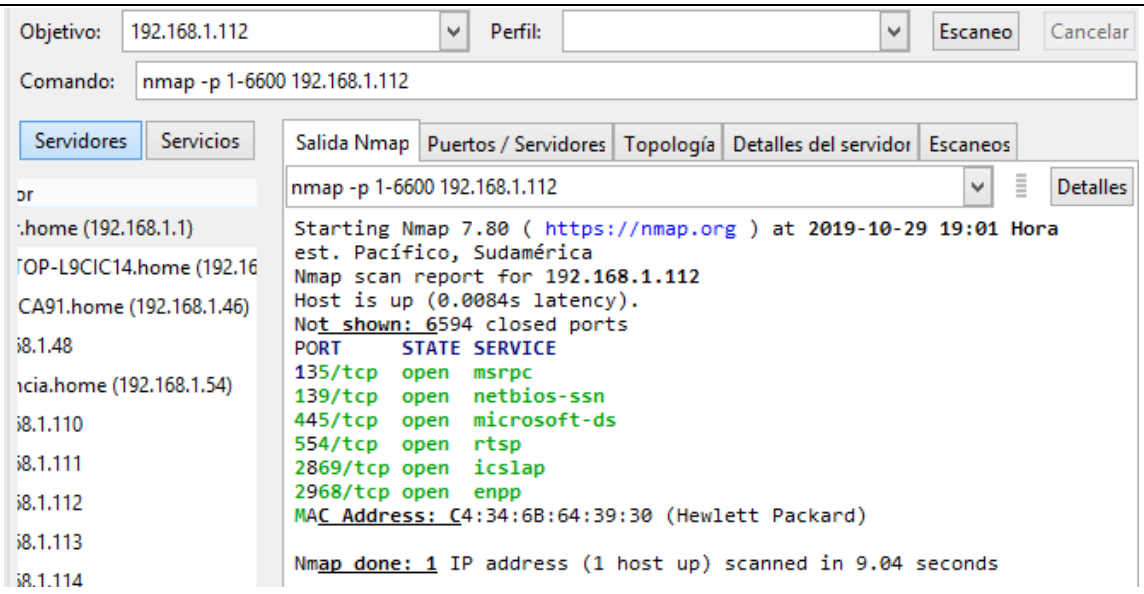
192.168.1.110



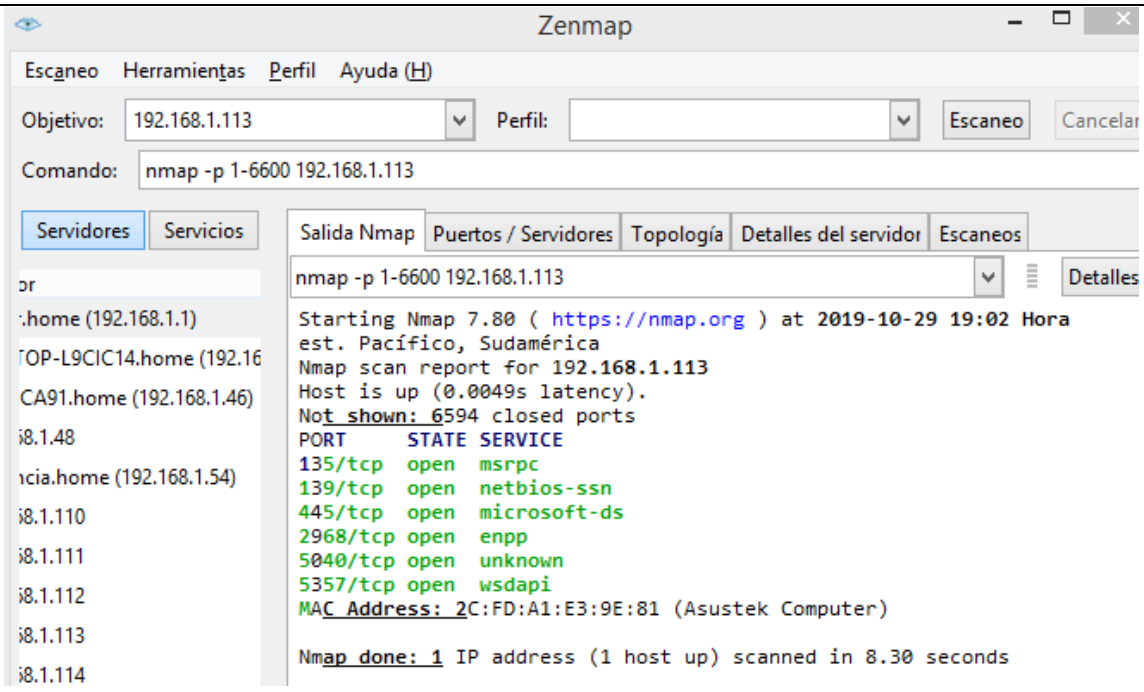
192.168.1.111



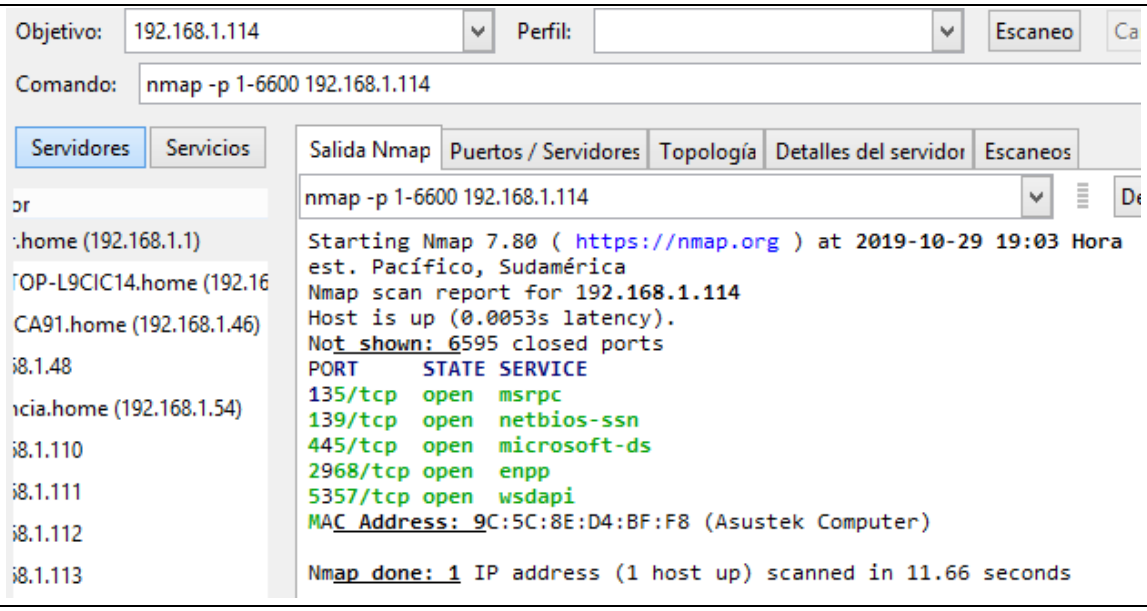
192.168.1.112



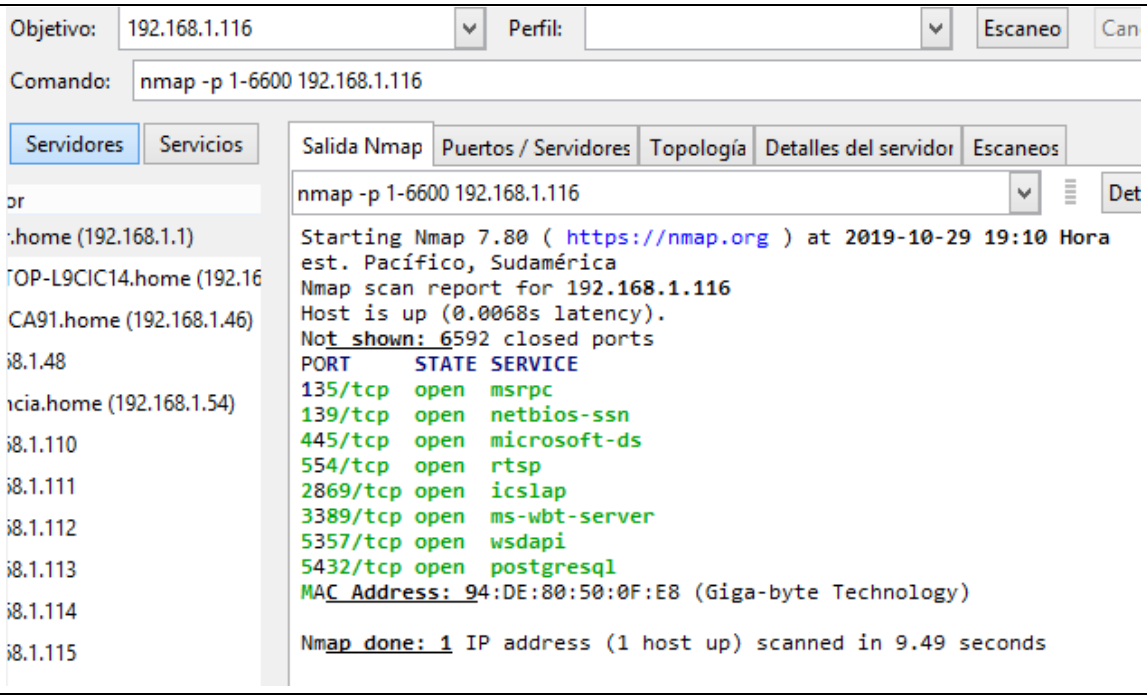
192.168.1.113



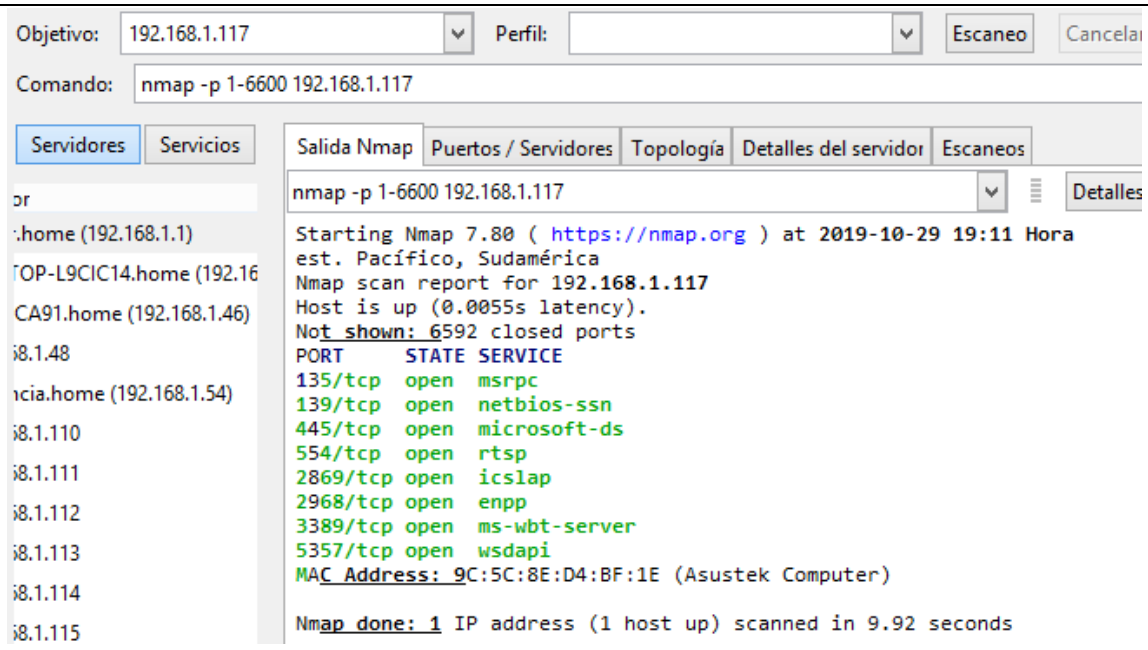
192.168.1.114



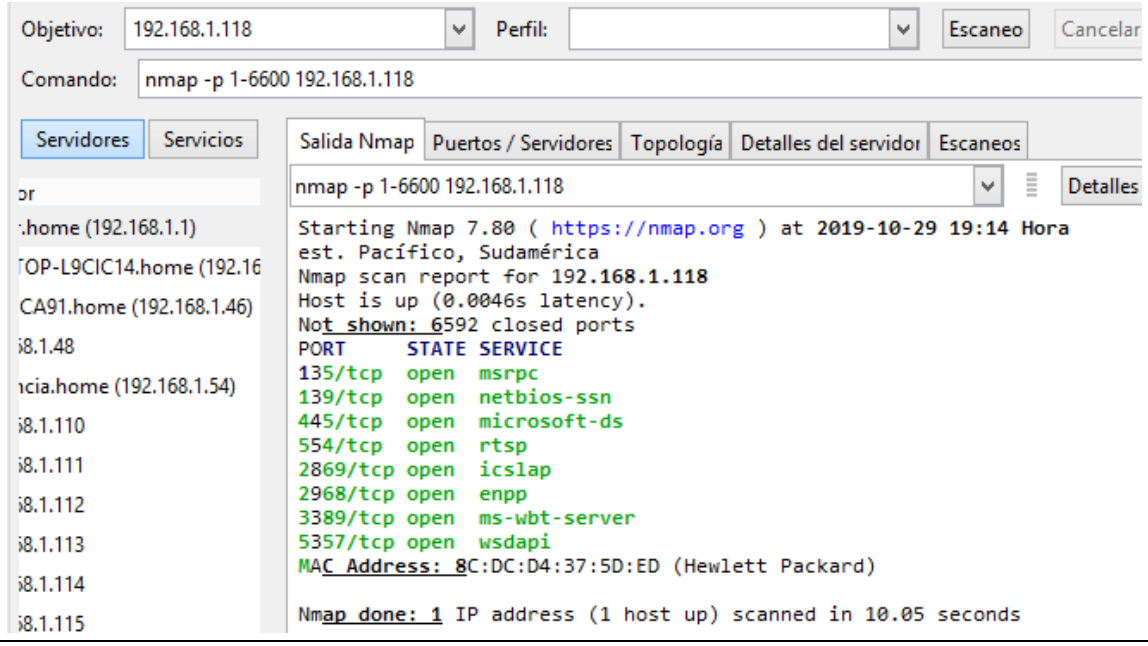
192.168.1.116

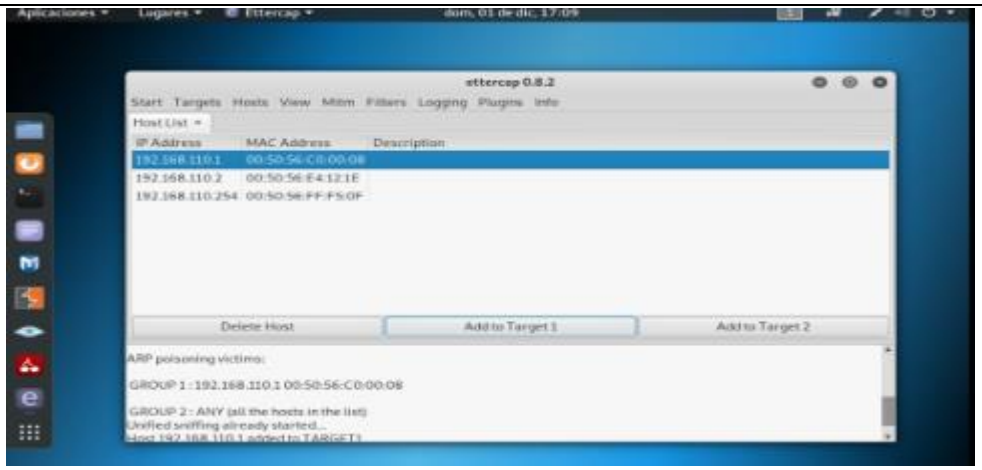


192.168.1.117

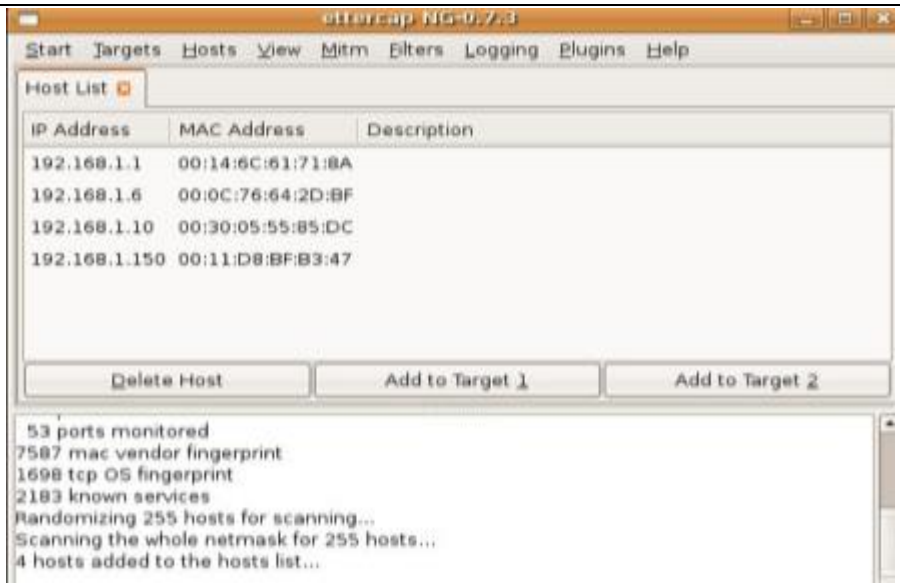


192.168.1.118



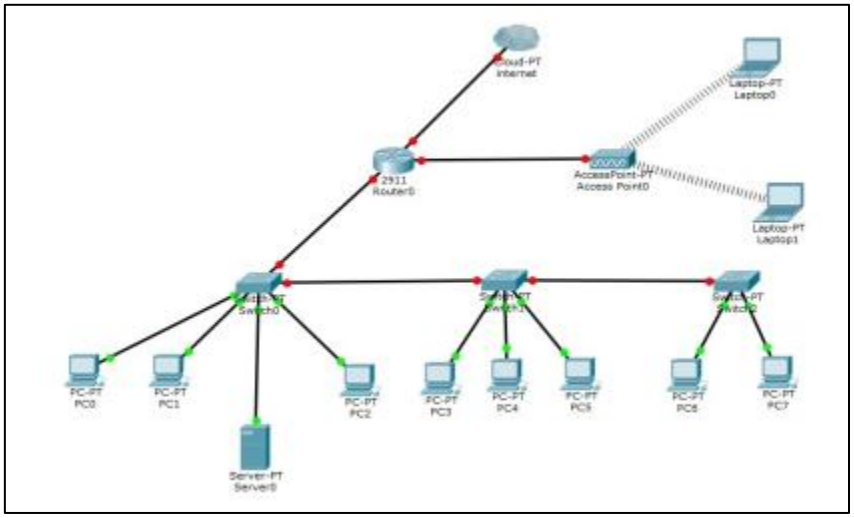


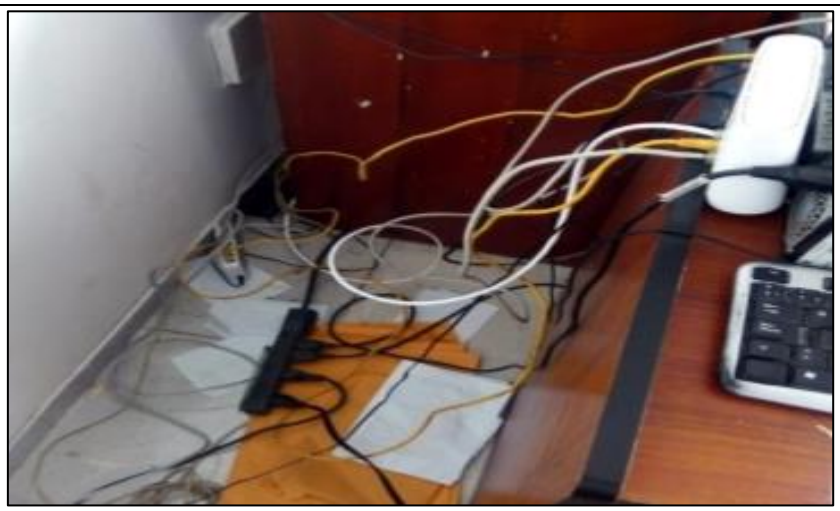
MAN IN THE MIDDLE



Anexo 03

OBSERVACION

TOPOLOGIA DE LA RED DE DATOS DE LA EMPRESA PRESTADORA


CABLEADO ACTUAL DE LA RED DE DATOS DE LA EMPRESA PRESTADORA


INSTALACIONES DE CENTRO DE OPERACIONES DE LA EMPRESA PRESTADORA

REALIZANDO ANALISIS DE VULNERABILIDADES