UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniero en Sistemas y Computación

TRABAJO DE TITULACIÓN

"Análisis del mecanismo de detección y defensa híbrido frente a los ataques IP Spoofing hacia un servidor NTP en la red de datos institucional de la Universidad Nacional de Chimborazo"

Autor: Juan Javier Toaquiza Morocho

Tutora: Ing. Lorena Paulina Molina Valdiviezo., Ph. D

Riobamba – Ecuador

Año 2019

Los miembros del Tribunal de Graduación del proyecto de investigación de título: **"Análisis del mecanismo de detección y defensa híbrido frente a los ataques IP Spoofing hacia un servidor NTP en la red de datos institucional de la Universidad Nacional de Chimborazo"**, presentado por el Sr. Juan Javier Toaquiza Morocho y dirigida por: Ing Lorena Molina Valdiviezo.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Lorena Molina
Director del Proyecto

Firma

Ing. Gonzalo Allauca
Miembro del Tribunal

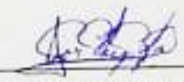
Firma

Ing. Diego Reina
Miembro del Tribunal

Firma

DERECHOS DE AUTORÍA

La responsabilidad del contenido de este proyecto de Graduación corresponde exclusivamente a: el Sr. Juan Javier Toaquiza Morocho bajo la dirección de la Ing. Lorena Paulina Molina Valdiviezo y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.



Juan Javier Toaquiza Morocho

060516382-3

DEDICATORIA

Dedico este proyecto de investigación a Dios todo por su gran amor y misericordia, por darme la fuerza necesaria para seguir adelante y llegar a este punto de mi vida profesional. Dedico también a mi madre que desde el cielo nunca me dejó solo y siempre estuvo conmigo, a mi padre que con su arduo trabajo confió en mí y me apoyo siempre. A mis hermanos por ser el complemento fundamental en casa, por su apoyo incondicional, y por su paciencia. A mi familia por estar en los momentos difíciles apoyándome y dándome palabras de ánimo. A mis amigos y compañeros que siempre han estado pendientes no solamente de mí sino de mi familia, apoyando con un granito de arena para poder llegar hasta esta etapa de mi vida.

Juan Javier Toaquiza Morocho

AGRADECIMIENTO

En el presente trabajo de investigación quiero agradecer a primeramente a Dios por permitirme llegar a esta etapa de mi vida, a mi padre y a mis hermanos que siempre me apoyaron.

Mi más sincero agradecimiento a la Universidad Nacional de Chimborazo, institución que se convirtió en mi segundo hogar abriéndome sus puertas para poder culminar con una etapa más en mi vida, preparándome como persona de bien y como profesional apto para poder servir con la sociedad con conocimientos sólidos y soluciones reales para el progreso del país.

Agradezco a la Ing. Lorena Molina que gracias a sus palabras y gran conocimiento culminamos con éxito la investigación.

Agradezco a Mónica Chacha, Alexis Mata, Alex Manobanda extraordinarias personas y amigos durante los años transcurridos de m vida universitaria

Juan Javier Toaquiza Morocho

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

En la actualidad, la seguridad de los sistemas informáticos ha aumentado juntamente con la evolución y avance de la tecnología, siendo la protección de datos e información un factor muy relevante para el desarrollo de una empresa. Si mencionamos seguridad la idea es tener nuestra información protegida y sin que haya ningún tipo de delito informático, sin embargo, los análisis y evaluaciones de anterior ataques IP Spoofing obligan a las empresas o centros educativos a implementar mecanismos de defensa y detección, con la finalidad de mitigar estos ataques. La Universidad Nacional de Chimborazo siendo una entidad educativa, cuenta con una gran cantidad de usuarios conectados a la red de datos, generando una gran demanda de concurrencia, por ende, la seguridad es lo más primordial sin importar el día o la hora, el departamento de Tecnologías de la Información (TI) tiene como fin brindar una seguridad óptima para un mejor servicio, esto permite mitigar los ataques IP Spoofing hacia un servidor NTP mediante la implementación del mecanismo de detección y defensa híbrido.

Por lo tanto, la presente investigación tuvo como objetivo el análisis del mecanismo de detección y defensa hibrido frente ataques IP Spoofing hacia un servidor NTP en la red de datos institucional de la Universidad Nacional de Chimborazo (UNACH).

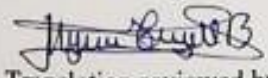
Se realizó mediciones de los ataques IP Spoofing, del tiempo de respuesta del servidor NTP y del nivel de vulnerabilidad del servidor durante dos semanas en el departamento de TI de la Unach para comprobar la mejora de seguridad en el mencionado servidor obteniendo un nivel de seguridad de un 80% aplicando los mecanismos (filtro anti-spoofing, Iptables firewall).

Palabras Clave: Ataques Informáticos, Cibersecurity IP Spoofing, Servidor NTP

Abstract

Nowadays, the security of computer systems has increased along with the evolution and advancement of technology; it is the protection of data and information a very relevant factor for the development of a company. If we mention security, the idea is to have our data protected. Without any cybercrime, however, the analyses and evaluations of previous IP Spoofing attacks force companies or educational centers to implement defense and detection mechanisms, with the purpose to mitigate these attacks. The National University of Chimborazo (UNACH) is an educational institution that has a large number of users connected to the data network, generating a high demand for concurrency. Therefore, security is the most important, regardless of the day or time. The department Information Technology (IT) aims to provide optimal security for a better service. This allows mitigating IP Spoofing attacks to an NTP server by implementing the hybrid detection and defense mechanism. This present investigation aimed to analyze the hybrid detection and defense mechanism against IP Spoofing attacks towards an NTP server in the institutional data network of the National University of Chimborazo. Measurements of the IP Spoofing attacks, the response time of the NTP server and the vulnerability level of the server were made during two weeks in the UNACH. department to verify the security improvement on the mentioned server obtaining a security level of 80% applying the mechanisms (anti-spoofing filter, Iptables firewall).

Keywords: Computer Attacks, Cybersecurity IP Spoofing, NTP Server



Translation reviewed by: Trujillo, Myriam

Linguistic Competences Professor

INTRODUCCIÓN

Para cualquier empresa o centro educativo la seguridad de los datos es importante y en la actualidad estar al tanto frente a los diferentes tipos de ataques es disminuir el riesgo de ciertas amenazas o vulnerabilidades , en el caso de un servidor NTP siempre a existido el riesgo de sufrir diferentes tipos de ataques por ejemplo los ataques UDP, dichos ataques se enfocan en alterar o cambiar la configuración de un reloj, de esta forma se genera una denegación de servicios. (Silvia M. Quiroz-Zambrano, 2017)

La suplantación de IP es un ataque informático que afecta a la capa 2 del modelo OSI, el objetivo de suplantar una IP es cambiar la direccion de origen y enviar una gran cantidad de paquetes hacia un usuario, de esta manera el remitente cree que el envio de paquetes lo realizo un usuario dentro de su propia subred.

El servidor Network Time Protocol (NTP) es un protocolo diseñado con el objetivo de sincronizar el tiempo entre sistemas informáticos los cuales están interconectados a través de una red LAN en el caso práctico en la red de datos institucional de la Universidad Nacional de Chimborazo(UNACH), considerando el tiempo como un bloque de construcción fundamental para equipos de red, y sistemas informáticos es indispensable salvaguardar todos los equipos mencionados o que forman parte de un entorno de red LAN, por ende, la seguridad es indispensable y en casos obligatoria y más al tratarse de una red de un Centro Educativo.

Los mecanismos de detección y defensa híbridos consisten en la implementación de equipos de red como Firewall, listas de acceso o filtros de entrada y salida en todo el contorno e infraestructura de la red LAN, al contar con el apoyo del departamento de Tecnologías de la Información se va implementó el servidor NTP y se aplicó del mecanismo de detección y defensa hibrido en la red de datos de la UNACH, la seguridad informática en una red educativa es primordial.

CAPITULO I

Planteamiento del Problema

Problema y Justificación

La seguridad informática es un tema de relevancia, debido a que la idea principal es mantener los datos protegidos por lo que se ha convertido en una prioridad, sin embargo, la gran cantidad de ataques existentes hacia redes informáticas, han generado la idea de crear mecanismos de detección y defensa contra dichos ataques y uno de ellos es el ataque IP Spoofing (Suplantación IP) su objetivo es ocultar la identidad del remitente o hacerse pasar por otro sistema informático, esta técnica puede emplearse para muchas otros ámbitos por ejemplo enmascararse como otro dispositivo para que las respuestas se envíen a ese dispositivo específico o para un ataque de Denegación de Servicios (DOS), este ataque crea paquetes IP con una dirección IP de origen.

Los ataques de suplantación IP o IP Spoofing siempre han sido un problema para las empresas o cualquier institución ya sea pública o privada, teniendo en cuenta el objetivo de proteger los datos existen técnicas de prevenir este mencionado ataque, optando por prevenir este ataque o protegerse del mismo, cabe resaltar que estas técnicas no bloquean o eliminan el ataque, sin embargo, ayudan a mitigar el ataque y en base a esto hay menor riesgo de sufrir ataques IP Spoofing.

Las redes LAN proporcionan servicios a dispositivos interconectadas dentro de su rango sin darle prioridad a que exista una distancia corta o una distancia demasiado larga ya que sus equipos brindan una gran señal y por ende un mejor servicio, en el caso práctico la red institucional de la Unach consta con un servicio de red LAN, con un data center en el departamento de Tecnologías de la Información, en donde se va a implementar un servidor NTP para el análisis de un mecanismo de detección y defensa hibrido.

Al implementar equipos en toda la infraestructura de la red, se aumenta el grado de seguridad de todos los servicios brindados por la Universidad Nacional de Chimborazo, además en la actualidad es recomendable tener equipos actualizados, la seguridad informática en una red educativa es primordial.

La Unach siendo una institución que cuenta con una gran cantidad de usuarios conectados a la red de datos, genera una gran demanda de concurrencia en la red por ende la seguridad es lo más primordial sin importar el día o la hora, al contar con el apoyo del departamento de Tecnologías de la Información se va a implementar un servidor NTP para toda la red de datos, con el fin de brindar una seguridad idónea para un mejor servicio, lo cual permitirá disminuir los ataques IP Spoofing hacia mencionado servidor mediante el análisis de un mecanismo de detección y defensa hibrido, el mismo que consiste en la implementación de equipos de red como Firewall en todo el contorno e infraestructura de la red LAN.

En la actualidad la seguridad de servidores en un departamento de tecnologías de la información es importante, en base a estudios los ataques al servidor NTP son frecuentes, entre los cuales están los ataques ON-PATH y OFF-PATH los cuales se detallan en el marco teórico de esta investigación, estos ataques ocasionan un alto grado de vulnerabilidad del mencionado servidor, sin importar la institución o empresa, simplemente causan efectos negativos como la alteración en la configuración de relojes, o fallos al momento de iniciar determinadas aplicaciones.

Objetivos

Objetivo General

- Analizar el mecanismo de detección y defensa hibrido frente a los ataques IP Spoofing hacia un servidor NTP en la red de datos institucional de la Universidad Nacional de Chimborazo.

Objetivos Específicos

- Estudiar el mecanismo de detección y defensa hibrido frente ataques IP Spoofing. en los entornos de redes LAN.
- Implementar un servidor NTP en el departamento de Tecnologías de la información de la UNACH.
- Aplicar el mecanismo de defensa hibrido, hacia el servidor NTP de la red de datos de la UNACH, a través de la generación de ataques IP Spoofing.

CAPITULO II

2. Marco Teórico

2.1. Seguridad de Redes

El objetivo primordial de la seguridad de redes es mantener los datos o la información protegido, centrándose en tres fundamentos como son: la confidencialidad, disponibilidad e integridad de cualquier tipo de información, sin embargo desde que fue creada la primera computadora hasta la actualidad existen varios problemas involucrados con la seguridad informática, por ejemplo, los costos de implementar seguridad, o que la seguridad no se considera esencial al momento de diseñar un proyecto sino después de este estar implementado, otro de los problemas más frecuente es la gente mas no la tecnología, ya que personas no autorizadas pueden causar daño a la seguridad de la información (Gregory B. White, 2017).

La información almacenada en un sistema informático son activos valiosos no solo para las personas sino para cualquier institución pública o privada, por ende, es necesario brindar una protección adecuada a estos activos frente a diferentes vulnerabilidades existentes en los sistemas de seguridad (Solarte, 2015).

2.2. Ataques Informáticos

Hoy en día es considerado una complejidad proteger los datos y la tecnología de la información y comunicación (TICs) lo que ha llevado a un mayor incremento en el riesgo de sufrir daños a los sistemas informáticos, de esta manera aumento el número de ataques informáticos aprovechando los fallos de seguridad existentes (Hernández Saucedo, 2015).

Desde que surgió la primera computadora han existido los ataques informáticos, los mismos que con el transcurrir de los años se han vuelto más difíciles de detectar, es decir

cualquier persona sin ser un experto en hacking puede causar daños a la información de cualquier sistema, un ataque es considerado como un evento que ataca contra la seguridad de la información de una organización analizando que esta tenga fallas en el hardware o software (Diana Suárez, 2017).

2.2.1. Tipos de Ataques Informáticos

Hoy en día los ataques informáticos van dirigidos a las empresas con el objetivo de que la mencionada sufra una cuantiosa pérdida económica, estos ataques pueden ser dirigidos al sistema operativo o a cualquier aplicación generando un error en su configuración, existen 2 tipos de ataques estos son:

- **Ataques pasivos:** no alteran ni modifican la información, se enfocan en monitorear y observar la información.
- **Ataques activos:** modifican la información y causan serios daños a las víctimas, alterando sus datos.

Entre los incidentes de seguridad más comunes están, ciber espionaje, infección por malware, denegación de servicio (DoS), worms, keyloggers entre otros, mencionaremos el ataque IP Spoofing el cual está centrado la investigación, sin embargo, se van a explicar brevemente otros tipos de ataques: (Juan Zhao, 2019)

Denegación de servicios (DoS): El objetivo de este ataque es afectar la disponibilidad de los servicios que ofrezca la red afectada, este ataque puede originarse por el uso de un dispositivo de radiofrecuencia generando interferencias y de esta forma limitando al usuario de interactuar con el servicio (Ballesteros, 2016).

Phishing: Considerado un delito cibernético de gran problema para la seguridad, el atacante tiene como fin causar daño a la autenticación de usuario mediante la

manipulación de sus datos, generando un correo electrónico falso. Existen diferentes tipos de ataques Phishing, por ejemplo, Spoofing email, Fake Social Network Accounts, y Trojan Horse (Gupta, 2016).

Spyware: Un ataque cuyo objetivo es infiltrarse y obtener datos de la víctima sin que este se dé cuenta, una vez infiltrado es capaz de espiar cualquier tipo de aplicación que se encuentre instalada en el dispositivo accedido remotamente (Chatterjee, 2018).

ARP Spoofing: Envía mensajes ARP falsos, para vincular la dirección MAC con la dirección IP, intenta suplantar la dirección de la puerta de enlace, de esta forma logra generar tráfico en la red.

MAC Flooding: Envía direcciones MAC hacia el switch, su finalidad es copar la tabla CAM, por ende, esta va a colapsar evitando almacenar más registros.

DHCP SPoofing: Genera un servidor falso el mismo que proporciona direcciones IP a diferentes usuarios, mediante dichas direcciones logra espiar el tráfico, sin embargo, para que este ataque funcione el servidor verdadero debe saturar todas las direcciones con las que cuente, para que trabaje el servidor falso (Pedro Alcívar Marcillo, 2016).

Otros ataques informáticos (Herrera Zurita, 2016):

Tabla 1: *Ataques Informáticos*

Ataque	Descripción
Gusanos y Troyanos	Brindan acceso remoto a un atacante.
Adware	Anuncios existentes en la red.
Host	No existe encabezado de host en la petición HTTP 1.1.
URL referencia	Incorpora una URL falsa
Ransomware	Causa daño al funcionamiento de los equipos.

2.3. Ataque IP Spoofing

El ataque IP Spoofing se encarga de falsificar la dirección IP obtenida anteriormente por un escaneo a la red o realizando un ataque MITM. (Figueredo, 2016). La suplantación de IP se usa casi siempre en lo que actualmente es uno de los ataques más difíciles de defender: los ataques de denegación de servicio o DoS (Rashid, 2013).

Un ataque IP Spoofing involucra la inundación de varios paquetes IP por personas sin autorización, los diferentes equipos no evalúan la dirección IP de origen solo se centra en la dirección IP destino, el objetivo de estas personas no autorizadas es que el usuario no reciba los datos o paquetes esperados, además de minimizar el ancho de banda de la red (S Rajashree, 2018).

IP Spoofing ha sido reconocido como uno de los mayores problemas que existen en el mundo de la seguridad de redes, por usar direcciones que han sido asignadas a otros o en tal caso direcciones no asignadas aún. Los atacantes que utilizan IP Spoofing pueden ocultar su ubicación, una serie de ataques basados en suplantación IP incluyen SYN flooding, amplificación de DNS (Yao, 2014).

2.3.1. Técnicas para prevenir IP Spoofing

El ataque IP Spoofing se utiliza en el ataque DoS para enviar información a las víctimas de distintas ubicaciones o direcciones, con el objetivo de inundar la red generando tráfico, debido a esto es complicado detener el ataque rastreando la dirección IP verdadera, sin embargo, existen técnicas para prevenir el ataque IP Spoofing, conocidas por su frecuente manejo para mitigar el ataque, las cuales se describen.

Filtrado de ingreso: Una técnica simple, a la vez de eficaz para prevenir el ataque IP Spoofing, consiste en almacenar una lista de direcciones en una lista de control de acceso (ACL), de esta forma el operador debe borrar el paquete ingresado si es invalido.

Filtrado de salida: Evalúa el paquete saliente, analizando la dirección IP de origen, si dicha dirección no consta en la lista se eliminará el paquete.

Reenvió de ruta inversa de unidifusión: Filtra el paquete en una tabla y si es diferente a las direcciones existentes se cae, si las rutas son simétricas esta técnica funcionara, sin embargo, puede haber errores y por ende validar paquetes falsificados (Patel, 2015).

Tabla 2: *Prevención IP Spoofing*

Técnicas	D**escripción**
Reconocimiento de Suplantación de Dirección IP	Hoy en día hay un alto grado de estar expuestos a sufrir ataques de Suplantación IP, al navegar por internet no nos cercioramos si estamos en una página segura, lo ideal es mantener un modo seguro de navegación y sobre todo estar alterar a sufrir cualquier daño que puede tener consecuencias.
Protección ante suplantaciones de Dirección IP	Es cierto que no se puede eliminar la suplantación IP y más al tratarse de usuarios con poco conocimiento de ciberataques, lo recomendable es tener en cuenta una manera de precaución o de estar alerta para no correr el riesgo, se recomienda tener cuidado al navegar por internet o responder correos electrónicos.
Prevenir la Suplantación de Dirección IP	Anteriormente se describía ciertas maneras de prevenir los ataques de suplantación como son: no responder a correos electrónicos, navegar por internet con discreción etc., además de aquellos se recomienda no responder mensajes en donde soliciten detalles de su cuenta o información personal, en los sitios web o

	servicios que se frecuenten estar atentos a cualquier cambio repentino o a mensajes de inicio se sesión repentinos, a los que los usuarios no estén familiarizados.

2.4. Servidor Network Time Protocol (NTP)

Uno de los servidores más conocidos desde la antigüedad, creado con la finalidad de sincronizar el tiempo entre los sistemas existentes en una determinada red (Aanchal Malhotra, 2016).

El protocolo de tiempo de red se centra en sincronizar los relojes de las computadoras en redes de latencia variable con conmutación de paquetes, está integrado en numerosos sistemas operativos y dispositivos de internet, el servidor NTP recibe millones de solicitudes de tiempo por día, cuando NTP falla en el sistema, varias aplicaciones en el sistema pueden fallar, todas al mismo tiempo. El NTP se puede utilizar para limpiar cachés. (Lombardi, 2015). La seguridad en NTP en la actualidad ha mejorado, sus primeras versiones no contaban con una técnica de autenticación estandarizado, sin embargo, a partir del lanzamiento de NTPv3 se agregó una autenticación utilizando una contraseña simétrica precompartida. Posteriormente la versión NTPv4 incorporo un mecanismo de autenticación de contraseña publica cuyo nombre fue AutoKey, con el pasar del tiempo se introdujo la propuesta del protocolo de seguridad de tiempo de red (NTS). En Linux y Mac OS X, el cliente crea un NTP o sondea un servidor cada cierto tiempo, en Windows los clientes sincronizan el reloj en 9 horas o en 15 horas, la ventaja de utilizar Windows es reducir el riesgo de ser atacado mediante un cambio en la configuración del reloj (Dowling, 2016).

2.4.1. Ataques a NTP

La seguridad en el servidor NTP es importante, si esté falla varias aplicaciones pueden tener dificultades en su funcionamiento al mismo tiempo, por ende, mantener a salvo los sistemas que este servidor controla es indispensable, se detallan ataques frecuentes que hacen vulnerable al protocolo de tiempo de red.

Ataque on-path: el ataque cambia la hora del servidor ya sea alterando en minutos la configuración o inclusive en años el tiempo configurado, debido a que este ataque monitorea cuando un cliente accede a cualquier servicio de la red o inicializa ntpd (Aanchal Malhotra, 2016).

Ataque off-path: genera una conexión anónima entre el cliente y el servidor, mediante una superposición de la dirección IPv4, ocasionando una fragmentación discreta entre los servidores (Aanchal Malhotra, 2016).

Ataque DoS: generan una sobrecarga al servidor mediante él envió de una gran cantidad de paquetes, sin embargo, estos ataques son mitigados por el mismo servidor NTP, más no por otro tipo de servidores (Mizrahi, 2016).

2.5. Mecanismo de Detección y Defensa Híbrido en Seguridad de Redes

Se considera un mecanismo de defensa y detección aquellos que tienen la obligación de brindar protección a los bienes y servicios informáticos de una empresa o de una entidad educativa, tienen como objetivo actuar cuando el ataque es producido y antes de que este pueda causar daños a algún sistema o servidor.

2.5.1. Mecanismo de defensa frente a Suplantación IP

Un mecanismo de defensa para la suplantación IP es mediante el conteo de saltos y salto de filtrado agregando una lista de control de acceso en el router para de esta manera permitir o denegar el permiso de direcciones IP en el rango a la que este configurada nuestra red. (S Rajashree, 2018)

2.5.2. Mecanismo de Detección usando Iptables

Mediante el uso de Iptables firewall se configuran reglas para el control de direcciones IP mediante la creación de un script y ejecutando para verificar las direcciones IP que acceden a un servidor o una máquina.

2.6. Herramientas Utilizadas

2.6.1. CentOS

La distribución de Linux CentOS es completamente gratuita derivada de las fuentes Red Hat Enterprise Linux (RHEL), esta distribución es estable, manejable e ideal para administrar sistemas y servicios. Al ser un sistema de código abierto brinda seguridad y es compatible con diferentes aplicaciones (Herney Perafana, 2018).

2.6.2. Kali Linux

Sistema operativo basado en Debian diseñado para testeo de vulnerabilidades y permite auditar sistemas o redes en su totalidad, además permite generar ataques informáticos e incorpora aplicaciones para rastrear los orígenes de estos ataques entre los cuales destaca Spoofing y Sniffing o incorpora aplicaciones para monitoreo de tráfico de red (Gabriela Vargas, 2019).

2.6.3. Hping3

Herramienta de código abierto diseñada para medir las vulnerabilidades de una red y para explorar vulnerabilidades del protocolo TPC/IP. Hping 3 permite generar o simular

ataques informáticos generando paquetes por ello es considerado una herramienta de alto rango para hacer ataques de inundación TCP SYN (Cesar Alejandro Vargas, 2016).

2.6.4. Ettercap

Herramienta diseñada para generar diferentes tipos de ataques, orientada a la suplantación pudiendo generar desde un ataque ARP Spoofing a un ataque Man in the Middle analizando los diferentes tipos de hosts conectados a una subred. Ettercap es compatible con diferentes plugins para mejorar su funcionamiento (Cruz, 2018).

2.6.5. Wireshark

Herramienta diseñada para realizar el escaneo de cualquier tipo de red ya sea Ethernet o Wifi, cuenta con una interfaz amigable y de simple uso e incorpora opciones de captura y filtrado. Wireshark no solo es considerado un Snnifer adicionalmente por sus novedosas características se puede denominar un Sistema de Detección de Intrusos (IDS), además destaca su velocidad para detectar ataques en la red (Vivens Ndatinya, 2015) (Piyush Goyal, 2017).

CAPITULO III

3. Metodología

La investigación está basada en el método cuantitativo porque buscó la medición de variables establecidas como es el ataque IP Spoofing y el mecanismo de detección y defensa híbrido.

Basado en un estudio longitudinal la investigación obtuvo datos realizando varias pruebas durante un determinado período de tiempo, con la finalidad de examinar las variaciones de estos datos en los ataques IP Spoofing generados en la red de datos de la Universidad Nacional de Chimborazo.

Además, se analizó los datos mediante la comparación de dos escenarios de ataques, el primero sin contar con el mecanismo de detección y el segundo ya incorporado el mecanismo de detección y defensa.

El primer escenario se verificó sobre el entorno real de la red LAN de la Unach, generando ataques IP Spoofing hacia el servidor NTP en determinados períodos de tiempo, para analizar el grado de seguridad con el que cuenta la misma. Posteriormente, el segundo escenario se verificó en el mismo entorno real de la red, generando ataques IP Spoofing hacia el servidor NTP, y se incorporó el mecanismo de detección y defensa híbrido, obteniendo los resultados en los mismos períodos de tiempo. Finalmente, se realizó el análisis comparativo e interpretación de los datos obtenidos de los dos escenarios respecto al números de ataques IP Spoofing hacia el servidor NTP de la Unach.

3.1. Hipótesis

Ho: La aplicación del mecanismo de detección y defensa frente a ataques de IP Spoofing no permite mejorar la seguridad del servidor NTP de la red de datos institucional de la Universidad Nacional de Chimborazo.

Ha: La aplicación del mecanismo de detección y defensa frente a ataques de IP Spoofing permite mejorar la seguridad del servidor NTP de la red de datos institucional de la Universidad Nacional de Chimborazo.

3.2 Identificación de variables

3.2.1 Variable Independiente.

Ataques IP Spoofing

3.2.2 Variable Dependiente.

Mecanismo de detección y defensa hibrido

3.3 Tipo de Estudio

3.3.1 Según el objeto de estudio

Investigación Aplicada: Da solución al problema, mediante la aplicación del mecanismo de detección y defensa híbrido frente a ataques IP Spoofing.

3.3.2 Según la fuente de investigación

Investigación Bibliográfica: Recolección de la información, utilizando técnicas y estrategias para acceder a documentos como: tesis, journals, libros para la investigación.

3.3.3 Según el nivel de conocimientos:

Investigación Descriptiva: Se realiza un análisis sobre las vulnerabilidades y riegos que conllevan los ataques IP Spoofing y afectan la optimización de la red, mediante la

medición y evaluación de diferentes parámetros, datos, componentes del fenómeno a investigar.

3.3.4 Según las variables

Investigación Experimental: Análisis de la red de datos de la Unach, con el objetivo de comprobar la hipótesis de investigación, se estudia 2 escenarios reales, el primer escenario atacando la red sin aplicar el mecanismo de detección y defesa híbrido y el segundo aplicado este mecanismo.

3.4 Población y Muestra

Se trata de una población infinita debido a que se obtuvo datos de diferentes mediciones de ataques IP Spoofing.

La muestra que se tomó fue en base a 3 horarios de ataques en un período de tiempo de 5 días.

3.5 Unidad de Análisis

Los ataques se llevaron a cabo durante 10 días y cada día durante 3 periodos de tiempo (8 am, 12 pm, 17 pm). Los datos obtenidos durante los ataques fueron registrados y analizados en un software estadístico.

3.6 Operacionalización de variables

Tabla 3. *Operacionalización de las variables*

Variable	**Tipo**	**Definición Conceptual**	**Dimensión**	**Indicadores**
Ataques IP Spoofing	Independiente	Ataque encargado de falsificar la dirección IP, impide recibir paquetes y minimiza el ancho de banda de la red	Ataques activos Experimentación	- Número de ataques IP Spoofing detectados - Tiempo de Respuesta del Servidor - Nivel de Vulnerabilidad del Servidor
Mecanismo de detección y defensa híbrido	Dependiente	Brindan protección a los bienes y servicios informáticos, actúan cuando el ataque es producido y antes de que este pueda causar daños a algún servidor.	Ataques activos Experimentación	- Número de ataques IP Spoofing detectados - Tiempo de Respuesta del Servidor - Nivel de Vulnerabilidad del Servidor

3.7 Procedimientos

Para el análisis y la aplicación del mecanismo de detección y defensa hibrido frente a los ataques IP Spoofing, Se realizo el estudio de mecanismo de seguridad, técnicas o herramientas las cuales logran mitigar el ataque. Para ello se plantea el siguiente orden cronológico de acciones:

Primer Paso:

Estudio de los ataques IP Spoofing y de los mecanismos existentes de detección y defensa en Servidores de Protocolo de tiempo de red.

Segundo Paso:

Implementación de un servidor Network Time Protocol (NTP) en el departamento de Tecnologías de la información de la UNACH.

Tercer Paso:

Generación de ataques IP Spoofing y análisis del comportamiento de estos en la red de datos institucional de la UNACH.

Cuarto Paso:

Aplicación del mecanismo de detección y defensa hibrido ante el ataque IP Spoofing, en la red de la UNACH sobre el entorno red real.

Quinto Paso:

Análisis de los resultados obtenidos sobre el entorno real de la red, determinando en consecuencia el desempeño que posee el mecanismo de detección y defensa hibrido frente al ataque IP Spoofing en la Red de la Unach.

3.7.1 Técnica de Investigación

Técnica de Observación. Permite analizar el comportamiento de los ataques IP Spoofing para obtener información, acerca de los daños que este ocasiona a un servidor NTP, para implementar el mecanismo de detección y de esta forma mitigar el ataque.

3.8 Procesamiento y Análisis

Revisión literaria sobre el tema de investigación

Se investigó fuentes bibliográficas en diferentes repositorios para adquirir conocimiento y tener una idea clara del tema investigado, además analizar libros, artículos y documentos de trabajos realizados anteriormente.

Estudio de los ataques IP Spoofing y el mecanismo de detección y defensa híbrido.

Se estudió los ataques analizando los antecedentes de daños generados por el ataque IP Spoofing hacia diferentes servidores, mediante este estudio se consideró el mejor mecanismo a implementar.

Implementación del servidor NTP en la red de datos institucional de la Universidad Nacional de Chimborazo

Para realizar la investigación se implementó el servidor de tiempo de red (NTP) en el departamento de tecnologías de la información de la Universidad Nacional de Chimborazo en el sistema operativo CentOS 7.

Generación de ataques IP Spoofing

Posteriormente de haber implementado el servidor NTP en la red de datos de la UNACH se realizó ataques IP Spoofing, con la finalidad de medir el grado de seguridad del servidor y los daños que ocasionan los ataques generados al servidor o incluso a diferentes servidores ubicados en el departamento de TICs de la Unach. Para ello, se utilizó el

sistema operativo Kali Linux y se utilizó la herramienta Hping3 para modificar la dirección IP.

Aplicación del mecanismo de detección y defensa híbrido

Una vez evaluado los daños ocasionados por los ataques IP Spoofing se realizó la aplicación e implementación de un mecanismo óptimo con la finalidad de mitigar el número de ataques hacia el servidor NTP y reducir el número de daños que estos ataques hayan generado, al ser un mecanismo de detección y defensa se logró de esta manera aumentar el grado de seguridad en el servidor.

CAPITULO IV

4. Resultados y Discusión

4.1. Implementación y configuración del Servidor NTP en la red de la Unach.

En el Departamento de Administración de Redes de la Universidad Nacional de Chimborazo se instaló y configuró un servidor Network Time Protocol (NTP) en el sistema operativo CentOS 7.

Para ello, el departamento de Administración de Redes facilitó la apertura para la ejecución de la investigación, y la máquina con el sistema operativo mencionado con las siguientes características:

- Memoria RAM 4GB
- Disco Duro 40GB

A continuación, se describe los pasos para instalar y configurar dicho servidor:

Paso 1: Descargar los paquetes necesarios para el Servidor NTP.

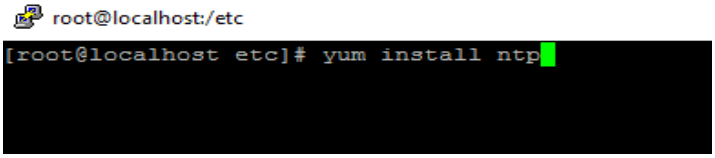


Ilustración 1: Instalación Servidor NTP

Paso 2: Configuración Dirección IP asignada al servidor NTP en el archivo ntp.conf con su respectiva mascara de red.

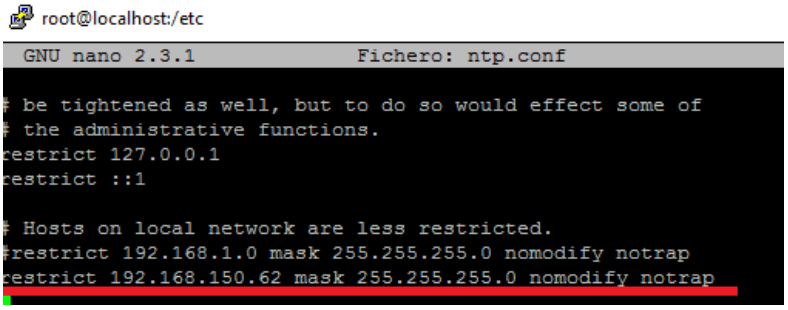


Ilustración 2: Dirección IP Servidor NTP

Paso 3: Se inicia el Servidor NTP:

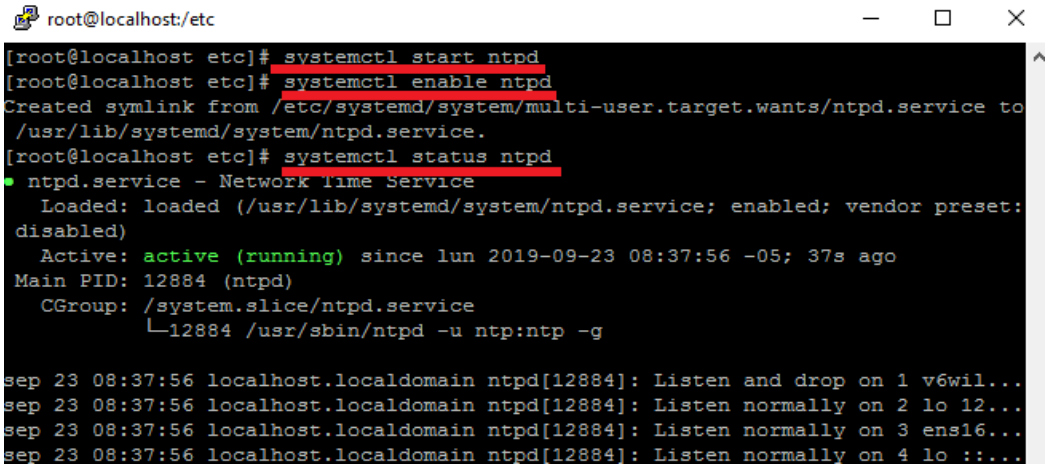


Ilustración 3: Arranque Servidor NTP

Paso 4: Configuración Cliente Windows 10 sincronizado al servidor NTP previamente instalado.

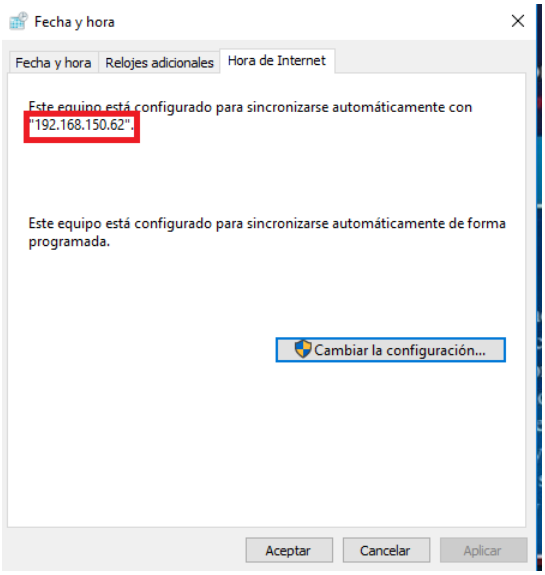


Ilustración 4: Cliente Windows

4.2. Generación de Ataques IP Spoofing

4.2.1. Ataques IP Spoofing con Hping3

En el Sistema operativo Kali Linux y con la herramienta Hping3 se realizó los ataques IP Spoofing dirigidos hacia el servidor NTP de la Unach en base a la dirección IP asignada en la configuración de dicho servidor.

A continuación, se describe los pasos para generar ataques IP Spoofing con la herramienta Hping3.

Paso 1: Verificar la dirección IP de la máquina atacante la cual será modificada en el paso 2 por medio de la herramienta Hping3.

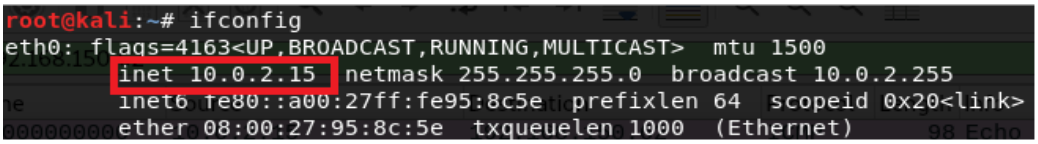


Ilustración 5: Dirección IP Kali Linux

Paso 2: Por medio del uso de la herramienta Hping3 se realizó el cambio de direccion IP por una direccion IP falsa, y se envió paquetes hacia el Servidor NTP por medio de su dirección IP conocida. En la Ilustración 6 se visualiza la dirección IP del Servidor NTP (amarillo) y la direccion IP de origen falsa (rojo).

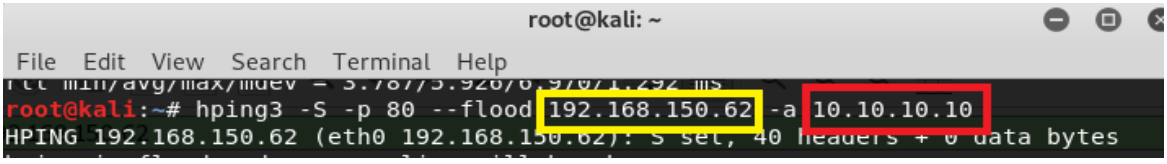


Ilustración 6: Estructura Ataque IP Spoofing

Paso 3: Por medio de la herramienta Wireshark se comprobó el ataque IP Spoofing hacia el servidor NTP. En la Ilustración 7 se visualiza el envió de paquetes con la dirección IP de origen verdadera (amarillo) y el envió de paquetes con la dirección IP falsa (rojo), ambas dirigidas hacia la dirección IP del servidor NTP (negro).

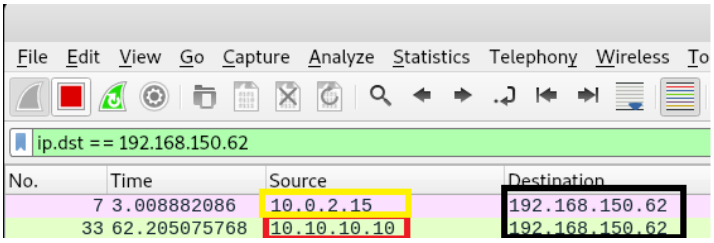


Ilustración 7: Ataque de Suplantación IP con Hping3

4.2.2. Ataques IP Spoofing con Ettercap

En el Sistema operativo Kali Linux y con la herramienta Ettercap se realizó los ataques IP Spoofing Man in the Middle (hombre en el medio) dirigidos hacia una máquina Windows (Cliente) sincronizada al servidor NTP de la Unach con el objetivo de robar su direccion IP.

A continuación, se describe los pasos para generar ataques IP Spoofing con Ettercap.

Paso 1: Mediante la herramienta Ettercap verificamos la interfaz en la que estamos conectados hacia Internet.

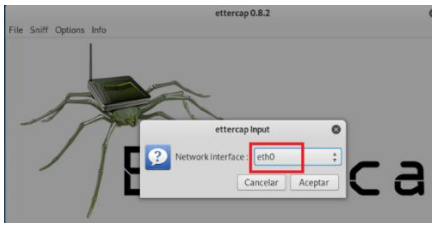


Ilustración 8: Herramienta Ettercap

Paso 2: Se realiza un escaneo de todos los hosts conectados dentro de nuestra subred en donde debe aparecer la IP de nuestra máquina víctima.

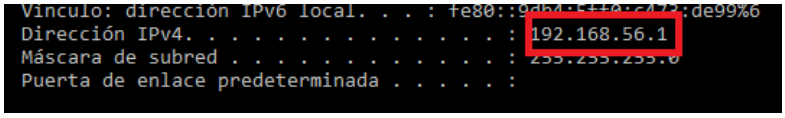


Ilustración 9: Direccion IP Cliente Windows

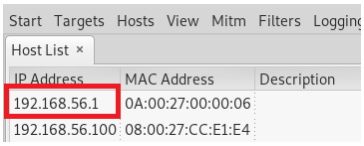


Ilustración 10: Escaneo hosts conectados

Paso 3: Elegimos la direccion IP victima como Target 1 y la direccion por la cual nos vamos a hacer pasar como Target 2 y mediante la herramienta Wireshark se comprobó el ataque IP Spoofing Man In The Middle generado hacia el Cliente Windows sincronizado con nuestro servidor NTP.

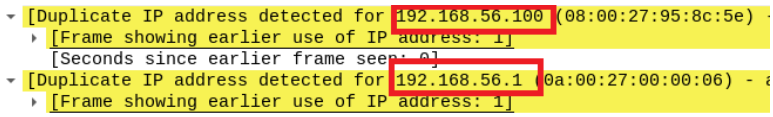


Ilustración 11: Ataque de Suplantación IP con Ettercap

4.3. Resultados Escenario 1 Sin Mecanismo de Detección y Defensa Híbrido

4.3.1. Resultados de Ataques IP Spoofing Escenario 1 con Hping3

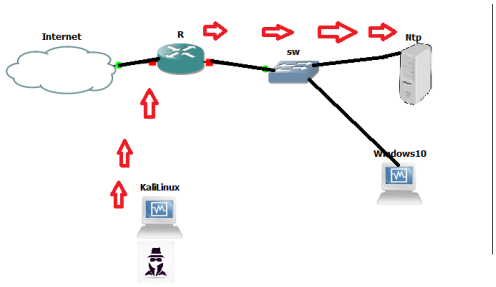


Ilustración 12: Escenario 1 ataque Hping3

Se atacó el servidor NTP de la red de la Unach con ataques IP Spoofing en los siguientes períodos de tiempo:

Tabla 4. *Periodos de Ataques IP Spoofing Hping3*

Número de ataques	Hora de Ataques	Días de Ataques

1500	8:00 am	Lunes
	12:00 pm	Martes
	17:00 pm	Miércoles
		Jueves
		Viernes

Con la distribución de Ubuntu Kali Linux se realizó ataques hacia el servidor NTP de la Unach en los periodos de tiempo mencionados en la **Tabla 4**, obteniendo como resultados el número de ataques IP Spoofing detectados y no detectados, además del tiempo de respuesta del servidor NTP y el nivel de vulnerabilidad de dicho servidor con la utilización de la herramienta Wireshark y el software SPSs para obtener promedios de los indicadores mencionados.

Tabla 5. *Ataques IP Spoofing Hping3*

	Ataques IP Spoofing Detectados	**Ataques IP Spoofing no Detectados**
Día 1	93	207
Día 2	100	200
Día 3	107	193
Día 4	108	192
Día 5	109	191
Total, de Ataques	517	983
Promedio	103,4	196,6

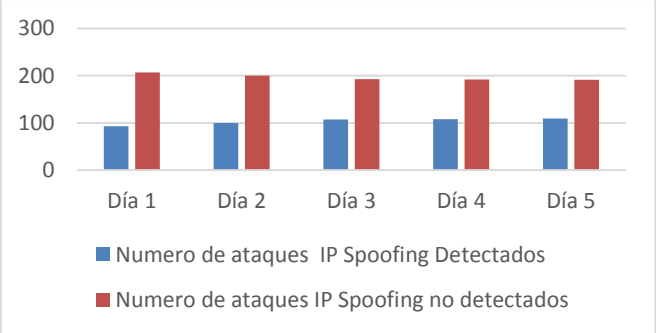


Ilustración 13: Resultados Ataques IP Spoofing Escenario 1 Hping3

En la **Ilustración 13** se muestra el número de ataques IP Spoofing detectados y no detectados durante los periodos de tiempo mencionado en la Tabla 4, en base a los resultados tenemos un total de 517 ataques de 1500 generados obteniendo un 34,47% del total de ataques IP Spoofing, lo que implica un alto índice de inseguridad en el servidor NTP implementado en la Unach.

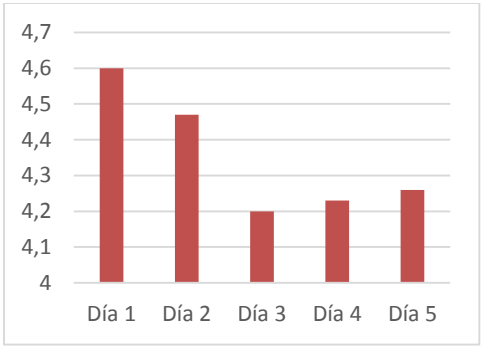


Ilustración 14: Tiempo de Respuesta del Servidor Escenario 1

En la **Ilustración 14** se muestra el tiempo de respuesta del servidor NTP durante la generación de los 1500 ataques IP Spoofing hacia este, obteniendo un promedio de tiempo de respuesta del servidor de 4,352 segundos, lo que detalla una lentitud de tiempo de respuesta al tratarse de un servidor de un Centro Educativo.

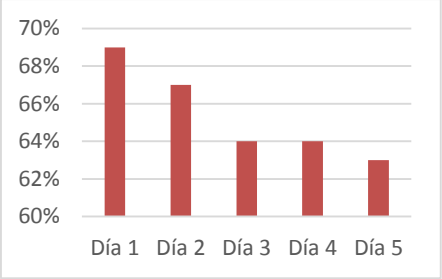


Ilustración 15: Nivel de Vulnerabilidad del Servidor Escenario 1

En la **Ilustración 15** se muestra el nivel de vulnerabilidad del servidor NTP por día luego de haber generado los ataques IP Spoofing, obteniendo un promedio de 65% de vulnerabilidad en el servidor lo cual representa un alto porcentaje.

4.3.2. Resultados de Ataques IP Spoofing Escenario 1 con Ettercap

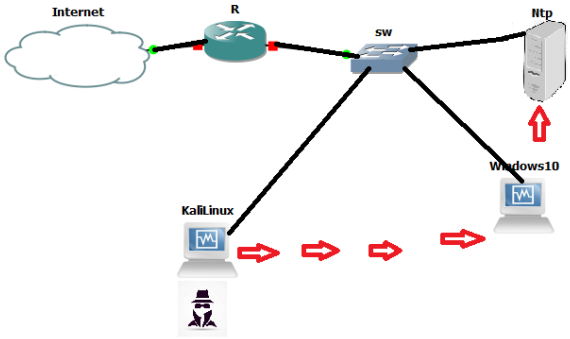


Ilustración 16: Escenario 1 ataque Ettercap

Se atacó un cliente Windows sincronizado al servidor NTP de la red de la Unach con ataques IP Spoofing en los siguientes periodos de tiempo:

Tabla 6. *Periodos de Ataques IP Spoofing Ettercap*

Número de ataques	Hora de Ataques	Días de Ataques
750	9:00 am	5
	13:00 pm	
	16:00 pm	

Con la distribución de Ubuntu Kali Linux se realizó ataques hacia un cliente Windows 10 sincronizado con el servidor NTP de la Unach en los periodos de tiempo mencionados en la **Tabla 6**, obteniendo como resultados el número de ataques IP Spoofing detectados y no detectados con la utilización de la herramienta Wireshark del indicador mencionado.

Tabla 7. *Ataques IP Spoofing Ettercap*

	Ataques IP Detectados	Ataques IP no Detectados
Día 1	116	34
Día 2	118	32
Día 3	124	26
Día 4	125	25
Día 5	124	26
Total, de Ataques	607	143
Promedio	121,4	28,6

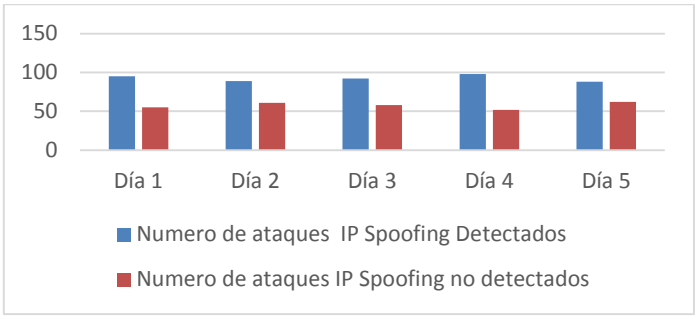


Ilustración 17: Resultados Ataques IP Spoofing Escenario 1 Ettercap

En la **Ilustración 17** se muestra el número de ataques IP Spoofing detectados y no detectados durante los periodos de tiempo mencionado en la Tabla 5, en base a los resultados tenemos un total de 462 ataques de 750 generados obteniendo un 61,6% del total de ataques IP Spoofing, lo que implica un índice de inseguridad leve en el servidor NTP implementado en la Unach a comparación del número de ataques detectados con Hping 3.

4.4. Resultados Escenario 2 Aplicación Mecanismo de Detección y Defensa Híbrido

4.4.1. Mecanismo Aplicado

4.4.1.1. Configuración Filtro Anti-Spoofing

Aplicar una ACL como un filtrado anti-spoofing con el objetivo de evitar que ingresen a la red LAN paquetes de direcciones IP cuyo origen sean falsas o suplantadas, es decir de cualquier red con una dirección IP diferente a la asignada a la Red de la Unach por su Proveedor de Servicio de Internet (ISP), de esta manera se mitiga el ataque IP Spoofing del exterior.

A continuación, se describe los pasos para configurar dicho filtro anti-spoofing:

Paso 1: Crear de una lista de control de acceso permitiendo que solo direcciones IP dentro del rango asignado puedan enviar paquetes.

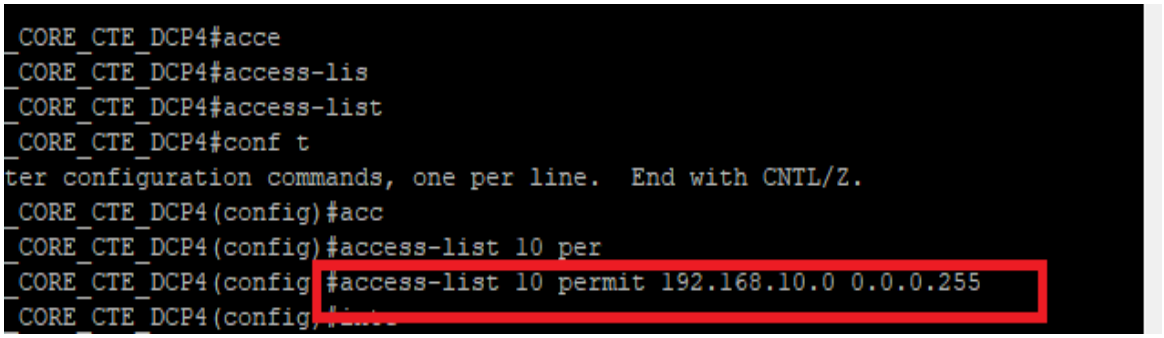


Ilustración 18: Creación ACL filtro Anti-Spoofing

Paso 2: Ingresar a la interfaz para poder habilitar nuestra ACL

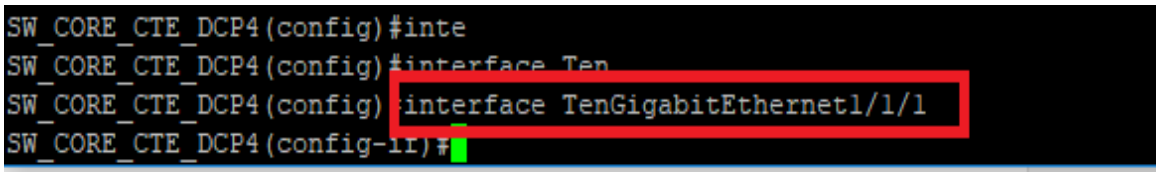


Ilustración 19: Acceso a la interfaz filtro Anti-Spoofing

Paso 3: Habilitar la ACLs creada

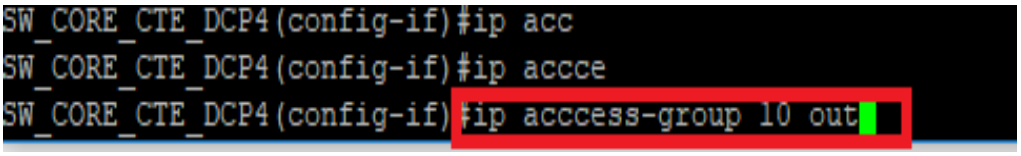


Ilustración 20: ACL habilitada filtro Anti-Spoofing

4.4.1.2. Configuración Iptables Servidor NTP

Aplicar un sistema de firewall el cual está vinculado con el kernel de CentOS 7 para mitigar ataques internos de suplantación IP, configurando un script con reglas de direcciones IP que se pueden sincronizar y enviar paquetes hacia el servidor NTP de la Unach.

A continuación, se describe el script configurado con Iptables:

En un script creado con el nombre defensa_ip configuramos los rangos de direcciones IP y las direcciones que no deseamos que tengan acceso al servidor NTP, además se debe añadir la interfaz por la cual el servidor tiene acceso a internet.

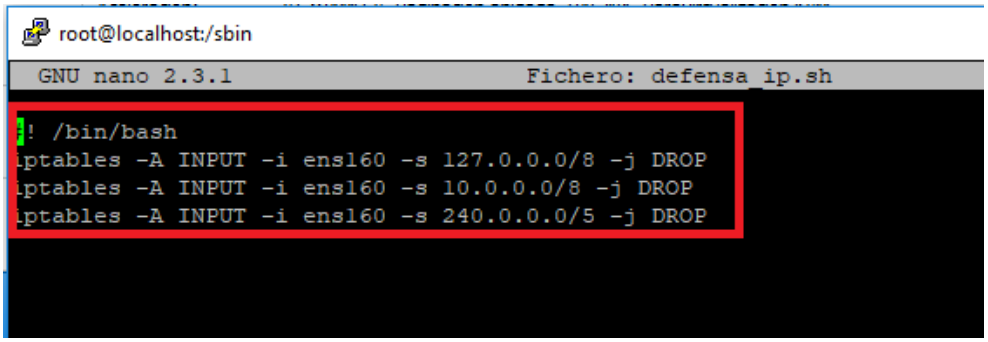


Ilustración 21: Configuración Iptables

Una vez realizada todas las configuraciones ejecutamos el script.

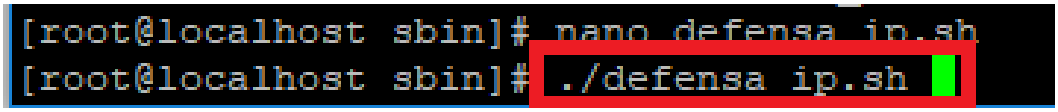


Ilustración 22: Configuración Iptables

4.4.2. Resultados Ataques IP Spoofing Aplicado el Mecanismo

4.4.2.1. Ataques IP Spoofing con Hping3

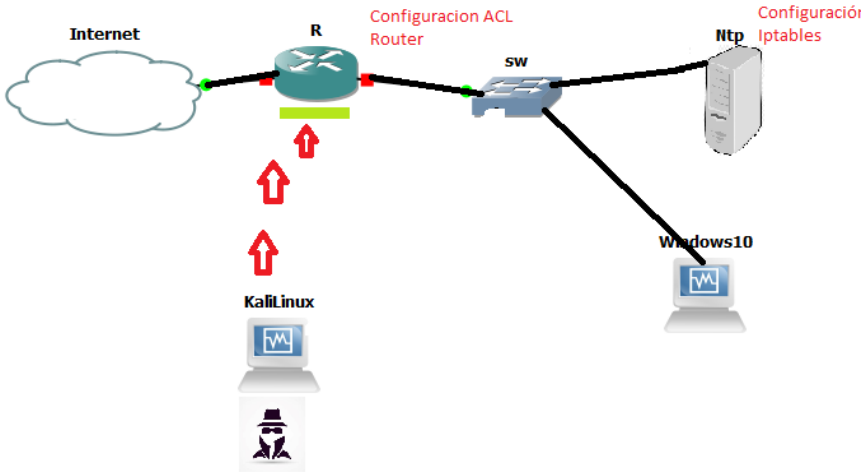


Ilustración 23: Escenario 2 ataque Hping3 con Mecanismo

En los mismos periodos de tiempo de la **Tabla 4,** se realizó ataques IP Spoofing hacia el servidor NTP, con la utilización de la herramienta Wireshark se analizó los resultados de los indicadores expuestos en los anteriores ataques, de esta manera verificar la eficiencia de los mecanismos aplicados en la red de datos institucional de la Unach.

Tabla 8. *Ataques IP Spoofing Hping3 Aplicado el Mecanismo*

	Ataques IP Spoofing Detectados	**Ataques IP Spoofing no Detectados**
Día 1	226	74
Día 2	240	60
Día 3	235	65
Día 4	241	59
Día 5	249	51
Total, de Ataques	1191	309
Promedio	238,2	61,8

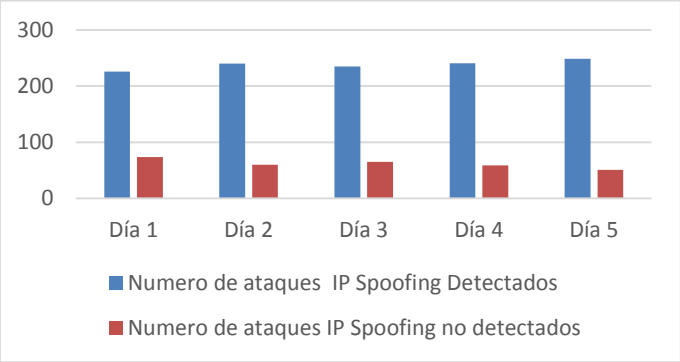


Ilustración 24: IP Spoofing Hping3 aplicado el Mecanismo

En la **Ilustración 24** se muestra el número de ataques IP Spoofing detectados y no detectados durante los periodos de tiempo mencionados en la Tabla 4, en base a los resultados tenemos un total de 1191 ataques de 1500 generados obteniendo un 79,4% del total de ataques IP Spoofing, lo que implica una mejora en la seguridad en el servidor NTP implementado en la Unach y una eficiencia de los mecanismos aplicados.

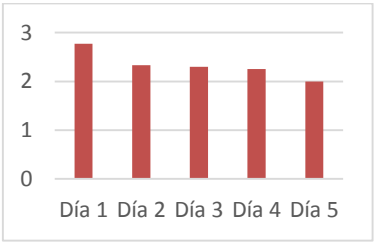


Ilustración 25: Tiempo de Respuesta Aplicado el Mecanismo

En la **Ilustración 25** se muestra el tiempo de respuesta del servidor NTP durante la generación de los 1500 ataques IP Spoofing hacia este, obteniendo un promedio de tiempo de respuesta del servidor de 2,33 segundos, lo que detalla una mejora en el tiempo de respuesta del servidor.

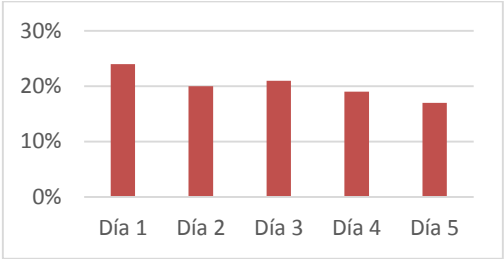


Ilustración 26: Tiempo de Respuesta Aplicado el Mecanismo

En la **Ilustración 26** se muestra el nivel de vulnerabilidad del servidor NTP por día luego de haber generado los ataques IP Spoofing, obteniendo un promedio de 20% de vulnerabilidad en el servidor lo cual representa una notable mejoría.

4.4.2.2. Ataques IP Spoofing con Ettercap

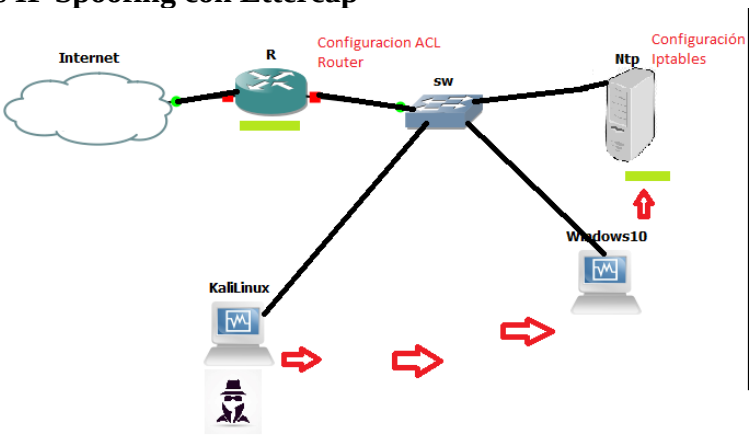


Ilustración 27: Escenario 2 ataque Ettercap con Mecanismo

Se realizó ataques hacia un cliente Windows 10 sincronizado con el servidor NTP de la Unach en los periodos de tiempo mencionados en la **Tabla 6**, obteniendo como resultados el número de ataques IP Spoofing detectados y no detectados con la utilización de la herramienta Wireshark del indicador mencionado después de haber aplicado los mecanismos.

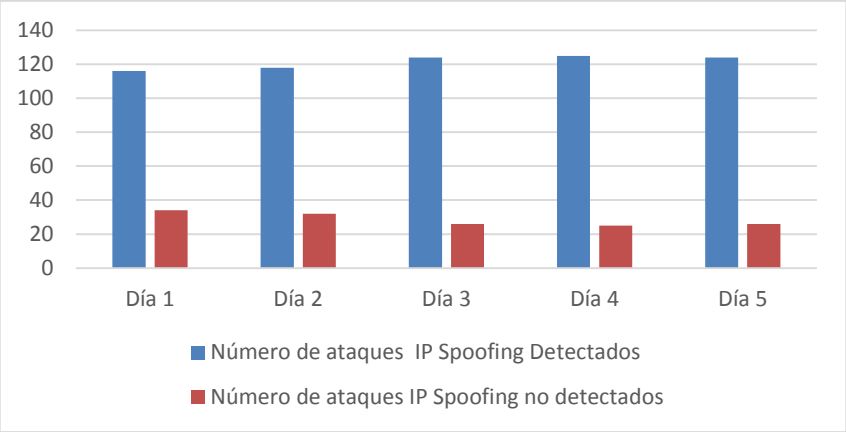


Ilustración 28: IP Spoofing con Ettercap Aplicado el Mecanismo

En la **Ilustración 28** se muestra el número de ataques IP Spoofing detectados y no detectados durante los periodos de tiempo mencionado en la **Tabla 6**, en base a los resultados tenemos un total de 607 ataques de 750 generados obteniendo un 80,93% del total de ataques IP Spoofing, lo que implica una mejora de seguridad en el servidor NTP y una eficiencia en los mecanismos aplicados.

4.5. Comprobación de Hipótesis

Para realizar la prueba de la hipótesis se utilizó los datos tomados durante los periodos de tiempo mencionados en la **Tabla 4** y **Tabla 6** mediante esta prueba se verifica si la hipótesis nula **Ho** es rechazada. Se aplicó la distribución T student.

4.5.1. Planteamiento de Hipótesis

Ho: La aplicación del mecanismo de detección y defensa frente a ataques de IP Spoofing no permite mejorar la seguridad del servidor NTP de la red de datos institucional de la Universidad Nacional de Chimborazo.

Ha: La aplicación del mecanismo de detección y defensa frente a ataques de IP Spoofing permite mejorar la seguridad del servidor NTP de la red de datos institucional de la Universidad Nacional de Chimborazo.

4.5.2. Comprobación por Indicador

4.5.2.1. Indicador: Cantidad de Ataques IP Spoofing Hping3 Detectados

Se analizó los datos obtenidos de los ataques IP Spoofing detectados sin el mecanismo de detección y defensa híbrido y con la aplicación del mecanismo (Filtro Anti-Spoofing, Iptables Firewall, Wireshark) y con el uso del software SPSs se obtuvo los siguientes datos.

Tabla 9. *Total, de Ataques IP Spoofing Hping3*

Total, de Ataques	**Ataques por Día**	**Total, de Días**	**Ataques por hora**	**Total, de Horas**
3000	300	10	100	3

En la **Tabla 9** se muestra el número total de ataques generados durante un periodo de tiempo de 10 días, 5 días de ataques sin la aplicación del mecanismo de detección y defensa hibrido y 5 días con la aplicación de este, para obtener el número de ataques detectados, obteniendo los resultados que se detallan:

Tabla 10. *Muestras Emparejadas Ataques con Hping3 Detectados*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Sin Mecanismo	34,47	15	6,116	1,579
	Con Mecanismo	79,40	15	3,979	1,027

En la **Tabla 10** se observa las medias del número de ataques al Servidor NTP, teniendo un promedio de 34,47 en número de Ataques IP Spoofing sin el mecanismo, y 79,40 ataques IP Spoofing al Servidor con el mecanismo, se verifica que en su promedio hay una diferencia entre las medias de los Ataques IP Spoofing con y sin mecanismo. El número de muestras es de 15 en ambos casos y su desviación estándar es mayor en el

escenario 1 que en el escenario 2, puesto que en la primera su desviación es de 6,1 y en la segunda de 3,9.

Tabla 11. *Diferencias Emparejadas Ataques Hping3 Detectados*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	Gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Sin Mecanismo – Con Mecanismo	-44,933	7,285	1,881	-48,967	-40,899	-23,889	14	,000

En la **Tabla 11** se observa el Sig(bilateral) que es de un valor de 0,000; esto quiere decir que este valor se encuentra en una zona de rechazo de la hipótesis nula **Ho** y por consiguiente se valida la hipótesis de investigación alternativa **Ha**, esto significa que existe mejoría en la seguridad del Servidor ya que así lo indica el Sig(bilateral) ratificado por las medias de la **Tabla 10**.

4.5.2.2. Indicador: Tiempo de Respuesta del Servidor

Se analizó los datos obtenidos del tiempo de respuesta del servidor NTP sin el mecanismo de detección y defensa híbrido y con la aplicación del mecanismo, y con el uso de un software estadístico se obtuvo los siguientes datos.

Tabla 12. *Muestras Emparejadas Tiempo de Respuesta*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Sin Mecanismo	4,3533	15	,42906	,11078
	Con Mecanismo	2,3300	15	,28523	,07365

En la **Tabla 12** se observa las medias del Tiempo de Respuesta del Servidor NTP, teniendo un promedio de 4,3 segundos sin el mecanismo, y 2,33 segundos con el mecanismo, se verifica que en su promedio hay una diferencia entre las medias del

Tiempo de Respuesta del Servidor con y sin mecanismo. El número de muestras es de 15 en ambos casos y su desviación estándar es mayor en el escenario 1 que en el escenario 2, puesto que en la primera su desviación es de 0,42906 y en la segunda de 0,28523.

Tabla 13. *Diferencias Emparejadas Tiempo de Respuesta*

Prueba de muestras emparejadas

		Diferencias emparejadas					T	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Sin Mecanismo – Con Mecanismo	2,02333	,48656	,12563	1,75389	2,29278	16,106	14	,000

En la **Tabla 13** se observa el Sig(bilateral) que es de un valor de 0,000; esto quiere decir que este valor cae en zona de rechazo de la hipótesis nula **Ho** y por consiguiente se valida la hipótesis de investigación alternativa **Ha**, esto significa que existe mejoría en el tiempo de Respuesta del Servidor NTP ya que así lo indica el Sig(bilateral) ratificado por las medias de la **Tabla 12**.

4.5.2.3. Indicador: Nivel de Vulnerabilidad del Servidor NTP

Se analizó los datos obtenidos del nivel de vulnerabilidad del servidor NTP sin el mecanismo de detección y defensa híbrido y con la aplicación del mecanismo, y con el de un software estadístico se obtuvo los siguientes datos.

Tabla 14. *Muestras Emparejadas Nivel de Vulnerabilidad*

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Sin Mecanismo	65,533	15	6,11633	1,57923
	Con Mecanismo	20,600	15	3,97851	1,02725

En la **Tabla 14** se observa las medias del Nivel de Vulnerabilidad del Servidor NTP, teniendo un promedio de 65% sin el mecanismo, y 20% con el mecanismo, se verifica que en su promedio hay una diferencia entre las medias del Nivel de Vulnerabilidad del Servidor con y sin mecanismo. El número de muestras es de 15 en ambos casos y su desviación estándar es mayor en el escenario 1 que en el escenario 2, puesto que en la primera su desviación es de 6,11633 y en la segunda de 3,97851.

Tabla 15. *Diferencias Emparejadas Nivel de Vulnerabilidad*

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Sin Mecanismo - Con Mecanismo	44,9333	7,28469	1,88090	40,89921	48,96746	23,889	14	,000

En la **Tabla 15** se observa el Sig(bilateral) que es de un valor de 0,000; esto quiere decir que este valor cae en zona de rechazo de la hipótesis nula **Ho** y por consiguiente se valida la hipótesis de investigación alternativa **Ha**, esto significa que existe mejoría en el tiempo de Nivel de Vulnerabilidad del Servidor NTP ya que así lo indica el Sig(bilateral) ratificado por las medias de la **Tabla 14**.

4.5.2.4. Indicador: Cantidad de Ataques IP Spoofing Ettercap Detectados

Se analizó los datos obtenidos de los ataques IP Spoofing detectados sin el mecanismo de detección y defensa híbrido y con la aplicación del mecanismo y con el uso de un software estadístico se obtuvo los siguientes datos.

Tabla 16. *Total, de Ataques IP Spoofing Ettercap*

Total, de Ataques	Ataques por Día	Total de Días	Ataques por hora	Total, de Horas

1500	150	10	50	3

Tabla 17. *Muestras Emparejadas Ataques Ettercap Detectados*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Sin Mecanismo	30,800	15	2,73078	,70508
	Con Mecanismo	40,466	15	1,68466	,43498

En la **Tabla 17** se observa las medias del número de ataques al Servidor NTP, teniendo un promedio de 30,80 en número de Ataques IP Spoofing sin el mecanismo, y 40,46 ataques IP Spoofing al Servidor con el mecanismo, se verifica que en su promedio hay una diferencia entre las medias de los Ataques IP Spoofing con y sin mecanismo. El número de muestras es de 15 en ambos casos y su desviación estándar es mayor en el escenario 1 que en el escenario 2, puesto que en la primera su desviación es de 2,7 y en la segunda de 1,6.

Tabla 18. *Diferencias Emparejadas Ataques Ettercap Detectados*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Sin Mecanismo - Con Mecanismo	-9,6666	3,22195	,83190	-11,45092	-7,88241	-11,620	14	,000

En la **Tabla 18** se observa el Sig(bilateral) que es de un valor de 0,000; esto quiere decir que este valor cae en zona de rechazo de la hipótesis nula **Ho** y por consiguiente se valida la hipótesis de investigación alternativa **Ha**, esto significa que existe mejoría en la seguridad del Servidor ya que así lo indica el Sig(bilateral) ratificado por las medias de la **Tabla 17**.

Conclusiones

- La implementación de un servidor Network Time Protocol (NTP) en la red de datos institucional de la Universidad Nacional de Chimborazo permitió proporcionar un nuevo servidor para sincronizar diferentes equipos de la infraestructura de red de la Unach.
- Al tener el apoyo del Departamento de Tecnologías de la Información de la Unach se pudo realizar y trabajar directamente con el proyecto de investigación en el entorno real de la red, usando el sistema operativo CentOS para la implementación del servidor y configuración de las Iptables, y teniendo el acceso al router para la configuración del filtro anti-spoofing.
- El estudio del mecanismo de detección y defensa hibrido permitió elegir el mejor para la aplicación en el entorno real de la red, de esta manera se cumplió el objetivo de mitigar los ataques IP Spoofing y disminuir el nivel de vulnerabilidad del servidor NTP en un 60% a comparación de los resultados sin mecanismo, en base a los datos y cálculos obtenidos en un software estadístico se rechazó la hipótesis nula, por ello, la hipótesis alternativa se cumplió ya que hubo una mejoría en la seguridad con la aplicación del mecanismo de detección y defensa híbrido.
- La aplicación del mecanismo en el entorno real de la red de la Unach permitió generar experiencia al trabajar con el departamento de Administración de Redes, además, mediante la comprobación de la hipótesis se puede analizar y aplicar el mecanismo en otros centros educativos o empresas.

Recomendaciones

- Analizar y estudiar el mecanismo aplicado en la infraestructura de la red para futuros trabajos de investigación, no solo en un servidor NTP sino en otros servidores, o a su vez tener una guía de seguridad para aplicarlo en otras empresas.
- Utilizar Kali Linux para realizar pruebas de seguridad informática y generar ataques pues al tratarse de una distribución destinada a auditoria informática es necesario tener conocimiento de su manejo y del uso de herramientas que vienen incorporadas en este sistema
- Al trabajar en un entorno real de red hay que tener cuidado y trabajar bajo la supervisión de una persona con experiencia, debido a que se pueden ocasionar errores o por algún descuido generar problemas a los usuarios finales.
- Estudiar ataques informáticos y los daños que estos pueden ocasionar, desde un ataque de denegación de servicios DoS o un ataque Man in the Middle y buscar soluciones frente a estos ataques, si bien ningún tipo de seguridad brinda un 100% de eficiencia mediante los mecanismos podemos mitigar estos ataques.

5. Bibliografía

Aanchal Malhotra, I. E. (2016). *Attacking the Network Time Protocol*. Obtenido de https://pdfs.semanticscholar.org/342e/3f74a564608643d99982e53c665f19117c14.pdf

Alonso, A. B. (2011). *Dispositivos Moviles.* OVIEDO EPSIG.

Apache, C. (2018). *Apache Cordova*. Recuperado el 15 de 9 de 2018, de Apache Cordova: https://cordova.apache.org/docs/en/latest/guide/overview/index.html

Azure, M. (2016). *Microsoft Azure*. Recuperado el 2018, de https://azure.microsoft.com/es-es/overview/what-is-azure/

Ballesteros, J. &. (2016). *Seguridad en Redes Inalámbricas de Acceso Local Bajo.*

Cesar Alejandro Vargas, C. C.-R. (2016). *Software Defined Networking for Electrical*. 1-6.

Chatterjee, R. D. (2018). *The spyware used in intimate partner violence*. Obtenido de https://ieeexplore.ieee.org/abstract/document/8418618

Cruz, J. C. (2018). *ANÁLISIS DE ATAQUES DE RED DEL TIPO DHCP SPOOFING, TCP SYN FLOOD Y PAQUETES MALFORMADOS.* 1-17.

Diana Suárez, A. Á. (2017). *Una forma de interpretar la seguridad informática. Journal of Engineering and Technology*. Obtenido de http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015/1072

Dowling, B. (2016). *Authenticated Network Time Synchronization*. *Security Symposium*. Obtenido de https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/dowling

Figueredo, D. D. (2016). *TÉCNICAS DE SUPLANTACIÓN EN REDES AD HOC*. 1-12. Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/15337/DiazFigueredoDanielEnrique2016.pdf?sequence=3&isAllowed=y

Framework, I. (2018). *Framework Ionic*. Recuperado el 13 de 10 de 2018, de Framework Ionic: https://ionicframework.com/docs/intro/concepts/

Gabriela Vargas, T. G. (2019). *Obtención de claves en redes WLAN/WPS usando Wifislax y Denegación de Servicios con Kali Linux*. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 1-15.

Gregory B. White, E. A. (2017). *Computer System and Network Security. CRC press*. Obtenido de https://www.taylorfrancis.com/books/9781351458726

Gupta, S. S. (2016). *A literature survey on social engineering attacks: Phishing attack.*

Hernández Saucedo, A. L. (2015). *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web*. *Revista electrónica de Computación, Informática Biomédica y Electrónica*.

Herney Perafana, N. G. (2018). *Design of a high availability cluster for a university virtual educational*. *Revista Ingeniería UC*, 1-9.

Herrera Zurita, A. (2016). *Aprendizaje automático para la detección de ataques informáticos.*

Juan Zhao, S. S. (2019). *Transfer learning for detecting unknown*. *EURASIP Journal on Information Security*. Obtenido de https://link.springer.com/content/pdf/10.1186%2Fs13635-019-0084-4.pdf

Lisandro, G. N. (2015). *Un análisis comparativo de rendimiento en aplicaciones móviles* . Junin.

Lombardi, A. N. (2015). *Practical Limitations of NTP Time Transfer* .

Luis Corral, A. S. (2012). *Mobile multiplatform.* Canada: Ontario.

Marcia Cordero, M. V. (2016). *Detección y mitigación de ataques ARP Spoof. GEEKS DECC-REPORTS*, 1-7.

Marques. (2009). *Bases de Datos. Universitat Jaume I. Servei de Comunicació i.*

Marset, R. N. (2007). *Modelado,Diseño e Implementación de Servicios Web 2006-07.* ELP-DSIC-UPV .

MARULANDA, I. C. (2014). *DISEÑO E IMPLEMENTACION DE UN APLICATIVO MÓVIL PARA LA.* Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/5135/62138456C157.pdf?sequence=1

Microsfot. (2017). *Visual Studio. Recuperado el 2018*, de https://docs.microsoft.com/es-es/dotnet/csharp/getting-started/introduction-to-the-csharp-language-and-the-net-framework

Microsoft. (2017). *C#.* Recuperado el 2018, de https://docs.microsoft.com/es-es/dotnet/csharp/getting-started/introduction-to-the-csharp-language-and-the-net-framework

Mizrahi, T. (2016). *Network Time Protocol Version 4(NTPv4).*

Patel, S. &. (2015). Various anti IP spoofing techniques. Obtenido de https://pdfs.semanticscholar.org/511c/064e613807666b4d255e71c3b012b57ac058.pdf

Pedro Alcívar Marcillo, A. C. (2016). *CASO DE ESTUDIO: PROTEGIENDO LA RED CON MIKROTIK DE LOS ATAQUES INTERNOS ARP SPOOFING, MAC FLOODING Y DHCP SPOOFING.* Obtenido de http://sigloxxi.espam.edu.ec/Ponencias/VII/ponencias/54.pdf

Pelachano. (2009). *Servicios_web_Estandares_extensiones_y_perspectivas*. Recuperado el 2018, de https://www.researchgate.net/profile/Vicente_Pelechano/publication/228634068_Serv

Piyush Goyal, A. G. (2017). *Comparative Study of two Most Popular Packet Sniffing Tools- Tcpdump and . International Conference on Computational Intelligence and Communication Networks* , 1-16.

Rashid, S. &. (2013). *Proposed Methods of IP Spoofing Detection & Prevention. International Journal of Science and Research*. Obtenido de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.683.7937&rep=rep1&type=pdf

Roger S. Pressman, P. (2010). *Ingeniería del software Un enfoque práctico.* México: McGraw-Hill.

S Rajashree, S. K. (2018). *Security with IP Address Assignment and Spoofing for Smart IOT Devices*. *International Conference on Advances in Computing, Communications and Informatics*, 1-5. Obtenido de https://ieeexplore.ieee.org/abstract/document/8554660/

Silvia M. Quiroz-Zambrano, D. G.-V. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Solarte, F. N. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. *Revista Tecnológica-ESPOL*.

Vivens Ndatinya, Z. X. (2015). *Network forensics analysis using Wireshark* . 1-16.

Yao, G. B. (2014). Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. Obtenido de https://ieeexplore.ieee.org/abstract/document/6987335/

Anexos

Anexo No. 1. Metodología Research

Tabla 19. *Metodología Research*

CONSULTA	GOOGLE SCHOLAR	ACM DIGITAL LIBRARY	IEEE	SCIENCE DIRECT	TOTAL
"ip spoofing attacks"	46	1	2	23	72
"servidores NTP" seguridad	34	54	0	6	94
"detección de ataques “seguridad de redes	41	20	5	12	78

Anexo No. 2. Ataques Generados con Hping3 por Día

Tabla 20. *Ataques con Hping3 Día 1*

DÍA 1		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	25	75
12:00 p. m.	30	70
17:00 pm	38	62
TOTAL	**93**	**207**
PROMEDIO	**31**	**69**

Tabla 21. *Ataques con Hping3 Día 2*

DÍA 2		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	27	73
12:00 p. m.	33	67
17:00 pm	40	60
TOTAL	**100**	**200**
PROMEDIO	**33,33333**	**66,66667**

Tabla 22. *Ataques con Hping3 Día 3*

DÍA 3		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	25	75
12:00 p. m.	42	58
17:00 pm	40	60
TOTAL	**107**	**193**
PROMEDIO	**35,66667**	**64,33333**

Tabla 23. *Ataques con Hping3 Día 4*

DÍA 4		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	30	70
12:00 p. m.	35	65
17:00 pm	43	57
TOTAL	**108**	**192**
PROMEDIO	**36**	**64**

Tabla 24*. Ataques con Hping3 Día 5*

DÍA 5		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	34	66
12:00 p. m.	34	66
17:00 pm	41	59
TOTAL	**109**	**191**
PROMEDIO	**36,33333**	**63,66667**

Tabla 25. *Ataques con Hping3 Día 6*

DÍA 6		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	71	29
12:00 p. m.	74	26
17:00 pm	81	19
TOTAL	**226**	**74**
PROMEDIO	**75,33333**	**24,66667**

Tabla 26. *Ataques con Hping3 Día 7*

DÍA 7		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	80	20
12:00 p. m.	81	19
17:00 pm	79	21
TOTAL	**240**	**60**
PROMEDIO	**80**	**20**

Tabla 27. *Ataques con Hping3 Día 8*

DÍA 8		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	84	16
12:00 p. m.	76	24
17:00 pm	75	25
TOTAL	**235**	**65**
PROMEDIO	**78,33333**	**21,66667**

Tabla 28. *Ataques con Hping3 Día 9*

DÍA 9		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	80	20
12:00 p. m.	82	18
17:00 pm	79	21
TOTAL	**241**	**59**
PROMEDIO	**80,33333**	**19,66667**

Tabla 29. *Ataques con Hping3 Día 10*

DÍA 10		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
8:00 a. m.	83	17
12:00 p. m.	86	14
17:00 pm	80	20
TOTAL	**249**	**51**
PROMEDIO	**83**	**17**

Anexo No. 3. Ataques Generados con Ettercap por Día

Tabla 30. *Ataques con Ettercap Día 1*

DÍA 1		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	33	17
13:00 p. m.	31	19
16:00 pm	31	19
TOTAL	**95**	**55**
PROMEDIO	**31,66667**	**18,33333**

Tabla 31. *Ataques con Ettercap Día 2*

DÍA 2		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	28	22
13:00 p. m.	31	19
16:00 pm	30	20
TOTAL	**89**	**61**
PROMEDIO	**29,66667**	**20,33333**

Tabla 32. *Ataques con Ettercap Día 3*

DÍA 3		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	33	17
13:00 p. m.	29	21
16:00 pm	30	20
TOTAL	**92**	**58**
PROMEDIO	**30,66667**	**19,33333**

Tabla 33. *Ataques con Ettercap Día 4*

DÍA 4		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	35	15
13:00 p. m.	29	21
16:00 pm	34	16
TOTAL	**98**	**52**
PROMEDIO	**32,66667**	**17,33333**

Tabla 34. *Ataques con Ettercap Día 5*

DÍA 5		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	33	17
13:00 p. m.	24	26
16:00 pm	31	19
TOTAL	**88**	**62**
PROMEDIO	**29,33333**	**20,66667**

Tabla 35. *Ataques con Ettercap Día 6*

DÍA 6		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	40	10
13:00 p. m.	38	12
16:00 pm	38	12
TOTAL	**116**	**34**
PROMEDIO	**38,66667**	**11,33333**

Tabla 36. *Ataques con Ettercap Día 7*

DÍA 7		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	37	13
13:00 p. m.	40	10
16:00 pm	41	9
TOTAL	**118**	**32**
PROMEDIO	**39,33333**	**10,66667**

Tabla 37. *Ataques con Ettercap Día 8*

DÍA 8		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	41	9
13:00 p. m.	42	8
16:00 pm	41	9
TOTAL	**124**	**26**
PROMEDIO	**41,33333**	**8,66667**

Tabla 38. *Ataques con Ettercap Día 9*

DÍA 9		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	42	8
13:00 p. m.	41	9
16:00 pm	42	8
TOTAL	**125**	**25**
PROMEDIO	**41,66667**	**8,33333**

Tabla 39. *Ataques con Ettercap Día 10*

DÍA 10		
Hora de ataque	**Ataques IP Spoofing Detectados**	**Ataques IP Spoofing no detectados**
9:00 a. m.	41	9
13:00 p. m.	43	7
16:00 pm	40	10
TOTAL	**124**	**26**
PROMEDIO	**41,33333**	**8,66667**

Anexo No. 4. Apertura Departamento TI Unach

Anexo No. 5. Oficio Departamento de Administración de Redes