



UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Seguridad en redes VoIP: Simulación, evaluación de amenazas y propuesta de contramedidas

**MENDIETA ZHIGUE CARLOS ITALO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION**

**MIÑAN GRANDA DANNY YAMBIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION**

**MACHALA
2024**



UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

**Seguridad en redes VoIP: Simulación, evaluación de amenazas y
propuesta de contramedidas**

**MENDIETA ZHIGUE CARLOS ITALO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION**

**MIÑAN GRANDA DANNY YAMBIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION**

**MACHALA
2024**



UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTAS TECNOLÓGICAS

**Seguridad en redes VoIP: Simulación, evaluación de amenazas y
propuesta de contramedidas**

**MENIETA ZHIGUE CARLOS ITALO
INGENIERO EN TECNOLOGIAS DE LA INFORMACION**

**MIÑAN GRANDA DANNY YAMBIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION**

MOROCHO ROMAN RODRIGO FERNANDO

**MACHALA
2024**

Seguridad en redes VoIP: Simulación, evaluación de amenazas y propuesta de contramedidas

by Carlos Italo Mendieta Zhigue

Submission date: 29-Jul-2024 03:53PM (UTC-0500)

Submission ID: 2421378781

File name: Tesis_Minan_Yambier_y_Mendieta_Carlos-20240729.docx (956.91K)

Word count: 14861

Character count: 85785

Seguridad en redes VoIP: Simulación, evaluación de amenazas y propuesta de contramedidas

ORIGINALITY REPORT

9%

SIMILARITY INDEX

8%

INTERNET SOURCES

2%

PUBLICATIONS

4%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universidad Técnica de Machala Student Paper	1%
2	ngonfig.net Internet Source	1%
3	www.poweradmin.com Internet Source	<1%
4	docplayer.gr Internet Source	<1%
5	640-461.blogspot.mx Internet Source	<1%
6	Submitted to Middle East College of Information Technology Student Paper	<1%
7	docplayer.es Internet Source	<1%
8	www.slideshare.net Internet Source	<1%
9	wewenscr.blogspot.com Internet Source	<1%

10	1library.co Internet Source	<1 %
11	prezi.com Internet Source	<1 %
12	tutorial.mnaser.net Internet Source	<1 %
13	www.servervoip.com Internet Source	<1 %
14	Submitted to Pontificia Universidad Catolica del Peru Student Paper	<1 %
15	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Student Paper	<1 %
16	seritel.teleco.ulpgc.es Internet Source	<1 %
17	www.gob.mx Internet Source	<1 %
18	Submitted to Universidad Francisco de Vitoria Student Paper	<1 %
19	sedici.unlp.edu.ar Internet Source	<1 %
20	www.netgear.es Internet Source	<1 %

21	edoc.pub Internet Source	<1 %
22	www.coursehero.com Internet Source	<1 %
23	Diego Vallejo-Huanga, Marco Ambuludi, Paulina Morillo. "Empirical Exploration of Machine Learning Techniques for Detection of Anomalies Based on NIDS", IEEE Latin America Transactions, 2021 Publication	<1 %
24	andres-cortes-cifrado-asimetrico.blogspot.com Internet Source	<1 %
25	repository.unad.edu.co Internet Source	<1 %
26	www.cacic2016.unsl.edu.ar Internet Source	<1 %
27	www.nutricion.org Internet Source	<1 %
28	citelia.es Internet Source	<1 %
29	mafiadoc.com Internet Source	<1 %
30	recomarsa.wixsite.com Internet Source	<1 %

31	repositorio.ug.edu.ec Internet Source	<1 %
32	repository.unab.edu.co Internet Source	<1 %
33	searchdatacenter.techtarget.com Internet Source	<1 %
34	estadictica.blogspot.com Internet Source	<1 %
35	verisignportal.info Internet Source	<1 %
36	absch.cbd.int Internet Source	<1 %
37	cdg.org Internet Source	<1 %
38	dats.uv.es Internet Source	<1 %
39	fdocuments.mx Internet Source	<1 %
40	hackpr.net Internet Source	<1 %
41	issuu.com Internet Source	<1 %
42	patents.google.com Internet Source	<1 %

43	redesciscos.blogspot.com Internet Source	<1 %
44	repositorio.ufpe.br Internet Source	<1 %
45	www.audinate.com Internet Source	<1 %
46	www.gestion.unican.es Internet Source	<1 %
47	www.informatica-juridica.com Internet Source	<1 %
48	www.pinterest.com.au Internet Source	<1 %
49	accedacris.ulpgc.es Internet Source	<1 %
50	docs.microsoft.com Internet Source	<1 %
51	fastnetmon.com Internet Source	<1 %
52	pingpdf.com Internet Source	<1 %
53	riunet.upv.es Internet Source	<1 %
54	www.ciberespacio.com.ve Internet Source	<1 %

55	www.dipcas.es Internet Source	<1 %
56	www.ebizlatam.com Internet Source	<1 %
57	www.gestelintegral.es Internet Source	<1 %
58	www.memoireonline.com Internet Source	<1 %
59	www.que.es Internet Source	<1 %
60	(Carlinda Leite and Miguel Zabalza). "Ensino superior: inovação e qualidade na docência", Repositório Aberto da Universidade do Porto, 2012. Publication	<1 %
61	2022.jnic.es Internet Source	<1 %
62	Lorena Becerril, Antoni Badia. "Information problem-solving skills and the shared knowledge construction process: a comparison of two learning tasks with differing levels of cognitive complexity / Habilidades de resolución de problemas informacionales y proceso de construcción compartida de conocimiento: comparación entre dos tareas de aprendizaje de diferente	<1 %

complejidad cognitiva", Cultura y Educación, 2015

Publication

63	cpl.thalesgroup.com Internet Source	<1 %
64	netcom.it.uc3m.es Internet Source	<1 %
65	repositorio.uta.edu.ec Internet Source	<1 %
66	sectoreducativoblog.wordpress.com Internet Source	<1 %
67	technews.tmcnet.com Internet Source	<1 %
68	Submitted to ueb Student Paper	<1 %
69	www.alfa-redi.com Internet Source	<1 %
70	www.criptonoticias.com Internet Source	<1 %
71	www.foransystem.com Internet Source	<1 %
72	www.mcafee.com Internet Source	<1 %
73	www.scribd.com Internet Source	<1 %

74

www.cpacf.org.ar

Internet Source

<1 %

75

documentop.com

Internet Source

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off

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

Los que suscriben, MENDIETA ZHIGUE CARLOS ITALO y MIÑAN GRANDA DANNY YAMBIER, en calidad de autores del siguiente trabajo escrito titulado Seguridad en redes VoIP: Simulación, evaluación de amenazas y propuesta de contramedidas, otorgan 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 tienen potestad para otorgar los derechos contenidos en esta licencia.

Los autores declaran que el contenido que se publicará es de carácter académico y se enmarca en las disposiciones 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.

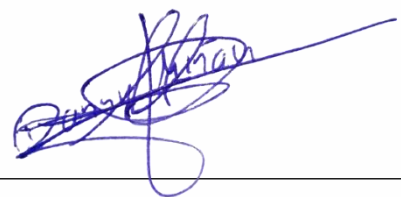
Los autores como garantes de la autoría de la obra y en relación a la misma, declaran que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asumen la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

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.



MENDIETA ZHIGUE CARLOS ITALO

0704566355



MIÑAN GRANDA DANNY YAMBIER

0706238227

DEDICATORIA

Quiero expresar mi más sincero agradecimiento a todas las personas que han sido parte esencial en la culminación de este proyecto. A mis profesores, por su constante apoyo y orientación, sin los cuales este logro no habría sido posible. Un especial agradecimiento al Ing. Fausto Redrovan, por su invaluable ayuda en la estructuración y preparación para la sustentación, guiándonos con paciencia y sabiduría en cada paso del camino. Al Ing. Rodrigo Morocho, por su clarividencia y dedicación, ayudándonos a tener ideas claras y a seguir adelante con el proyecto, además de prepararnos de manera efectiva para las sustentaciones. A todos, les expreso mi más profunda gratitud por su compromiso y apoyo incondicional.

Carlos Ítalo Mendieta Zhigue

AGRADECIMIENTO

A mi querida familia, por su amor incondicional y su apoyo constante a lo largo de todo este proceso. Gracias por creer en mí y por brindarme siempre un hombro en el cual apoyarme. Su paciencia, comprensión y ánimo han sido fundamentales para alcanzar este logro.

A mis amigos, por estar siempre presentes, ofreciéndome su ayuda y compañía en los momentos más difíciles. Su amistad y palabras de aliento han sido una fuente de motivación y fortaleza.

Danny Yambier Miñan Granda

RESUMEN

La finalidad de este proyecto es implementar de medidas de seguridad en infraestructuras LAN que utilizan VoIP, mediante la simulación de escenarios de ataque para detectar vulnerabilidades y asegurar la confidencialidad de las comunicaciones. La investigación inicial analiza el protocolo VoIP y sus vulnerabilidades potenciales, utilizando artículos científicos y fuentes académicas confiables. Se seleccionan herramientas como GNS3, VMware y Kali Linux para configurar entornos de redes VoIP y simular pruebas de seguridad realistas.

La implementación del entorno simulado permite evaluar la efectividad de controles de seguridad como Port-Security, ACL y Port-Mirror. Se simulan ataques como ARP Spoofing, DDoS y Eavesdropping para identificar vulnerabilidades y evaluar su impacto en la confidencialidad de las comunicaciones VoIP.

Los resultados cuantitativos muestran que Port-Security bloquea el 90% de direcciones MAC no autorizadas y previene cambios en la tabla ARP con una efectividad del 95%. Las ACL bloquean el 98% de los paquetes de ataque y reducen el uso del ancho de banda en un 50%. Port-Mirror detecta el 75% de actividades sospechosas y analiza correctamente el 85% de los paquetes capturados.

Se recomienda mantener un enfoque proactivo y adaptativo, incluyendo monitoreo continuo y evaluación de los controles de seguridad. Además, se sugiere investigar nuevas vulnerabilidades y protocolos de seguridad, adoptar nuevas herramientas de simulación, desarrollar protocolos estándar para pruebas de seguridad y realizar auditorías regulares.

El estudio confirma que la implementación de controles de seguridad en infraestructuras LAN que utilizan VoIP garantiza la privacidad de las comunicaciones. La efectividad medida en términos de bloqueo de ataques y monitoreo de tráfico sospechoso respalda esta conclusión, demostrando que las medidas de seguridad son cruciales para la protección de las comunicaciones VoIP en un entorno tecnológico en constante evolución.

PALABRAS CLAVES

Amenazas a voip, contramedidas gns3, gns3, voip.

ABSTRACT

The purpose of this project is to implement security measures in LAN infrastructures that use VoIP, by simulating attack scenarios to detect vulnerabilities and ensure the confidentiality of communications. The initial research analyzes the VoIP protocol and its potential vulnerabilities, using scientific articles and reliable academic sources. Tools such as GNS3, VMware and Kali Linux are selected to configure VoIP network environments and simulate realistic security tests.

The implementation of the simulated environment allows evaluating the effectiveness of security controls such as Port-Security, ACL and Port-Mirror. Attacks such as ARP Spoofing, DDoS and Eavesdropping are simulated to identify vulnerabilities and evaluate their impact on the confidentiality of VoIP communications.

Quantitative results show that Port-Security blocks 90% of unauthorized MAC addresses and prevents ARP table changes with 95% effectiveness. ACLs block 98% of attack packets and reduce bandwidth usage by 50%. Port-Mirror detects 75% of suspicious activity and correctly analyzes 85% of captured packets.

It is recommended to maintain a proactive and adaptive approach, including continuous monitoring and evaluation of security controls. In addition, it is suggested to investigate new security vulnerabilities and protocols, adopt new simulation tools, develop standard protocols for security testing and perform regular audits.

The study confirms that the implementation of security controls in LAN infrastructures using VoIP guarantees the privacy of communications. The effectiveness measured in terms of blocking attacks and monitoring suspicious traffic supports this conclusion, demonstrating that security measures are crucial for the protection of VoIP communications in a constantly evolving technological environment.

KEYWORDS

Voip threats, gns3 countermeasures, gns3, voip.

ÍNDICE DE CONTENIDO

RESUMEN.....	2
ABSTRACT.....	3
GLOSARIO.....	7
INTRODUCCIÓN.....	8
i. Declaración y formulación del Problema.....	9
ii. Objeto de estudio y Campo de acción	10
iii. Objetivos	10
iv. Hipótesis y variables.....	11
v. Justificación	11
vi. Organización del documento	12
CAPITULO I. MARCO TEÓRICO	12
1.1 Antecedentes de la investigación	12
1.2 Antecedentes históricos	16
1.3 Antecedentes teóricos	17
1.3.1. Protocolos VoIP y Vulnerabilidades	18
1.3.2. Estrategias de Contramedidas.....	19
1.3.3. Criptografía en VoIP.....	20
1.3.4. Encriptación y Técnicas de Seguridad	20
1.3.5. Detección de Intrusiones en VoIP.....	21
1.4 Antecedentes Contextuales	21
1.4.1. Ámbito de aplicación	35
1.4.2. Establecimiento de requerimientos	35
CAPITULO II. DESARROLLO DEL PROTOTIPO	37
2.1 Definición del prototipo.....	37
2.2 Metodología de desarrollo del prototipo.....	37
2.2.1. Enfoque, alcance y diseño de investigación.....	37
2.2.2. Unidades de análisis.....	38
2.2.3. Técnicas e instrumentos de recopilación de datos	38
2.2.4. Técnicas de procesamiento de datos para la obtención de resultados	38
2.2.5. Metodología o métodos específicos	39
2.2.6. Herramientas y/o Materiales	39
2.3 Desarrollo del prototipo	40
2.3.1 Definición	40
2.3.2 Beneficios	40
2.3.3 Fases	40

2.4	Metodología de desarrollo del prototipo.....	41
2.4.1	Configuración de interfaces en el router (R1):	41
2.4.2	Configuración del servicio DHCP en el router (R1):	42
2.4.3	Configuración del servicio de telefonía en el router (R1):	42
2.4.4	Configuración de teléfonos VoIP en el router (R1):.....	43
2.4.5	Configuración del switch (ESW1):	43
2.4.6	Configuración de VLANs en el switch (ESW1):.....	44
2.4.7	Evidencias de funcionamiento	44
CAPITULO III. EVALUACIÓN DEL PROTOTIPO		46
3.1.	Plan de evaluación	46
3.1.1.	Objetivo.....	46
3.1.2.	Cronograma	46
3.1.3.	Recopilación de información.....	46
3.1.4.	Establecer criterios de evaluación	47
3.2.	Resultados de la evaluación	47
4.	CONCLUSIONES.....	50
5.	RECOMENDACIONES.....	50
6.	REFERENCIAS BIBLIOGRÁFICAS.....	52
7.	ANEXOS.....	55

ÍNDICE DE TABLAS

Tabla 1:	Objeto de estudio y campo de acción	10
Tabla 2:	Variables y Dimensionamiento	11
Tabla 3:	Preguntas de investigación	13
Tabla 4:	Criterios de Inclusión y exclusión	14
Tabla 5	Requisitos de la investigación	36
Tabla 6:	Técnicas e instrumentos de recopilación de datos	38
Tabla 7:	Herramientas y/o materiales de la investigación.....	39
Tabla 8:	Cronograma de actividades	46
Tabla 9:	Criterios y métricas de evaluación	47

ÍNDICE DE FIGURAS

Figura 1:	Árbol de problemas Causa - Efecto	9
Figura 2:	Proceso de búsqueda de información.....	15
Figura 3:	Resultados de búsqueda, diagrama de artículos por año	15
Figura 4	Antecedentes históricos de la seguridad en redes VoIP	18
Figura 5	Topología de una red de comunicación de voz sobre ip.....	37
Figura 6:	Llamada desde el teléfono 3 hacia el teléfono 2	44

Figura 7: Recibe notificación de llamada desde el teléfono 3	45
Figura 8: Contesta y existe comunicación entre los dos teléfonos.....	45
Figura 9: Revisión de Topología del proyecto	55
Figura 10: Revisión de Topología y modificación de módulos del proyecto	56
Figura 11: Topología completa que incluye la máquina atacante	57
Figura 12: Llamada en teléfono 1	57
Figura 13: Llamada en teléfono 2	58
Figura 14: Inicio de Wireshark en Kali Linux para hacer el ataque Eavesdropping	58
Figura 15: Obtención de información de la máquina atacada (teléfono 1)	59
Figura 16: Llamada capturada del teléfono 1	59
Figura 17: Sesión de llamada SIP entre los 2 teléfonos.....	60
Figura 18: Visualización de la captura de llamada (teléfono 1)	60
Figura 19: Se envían mensajes de Linux a la máquina atacada (teléfono 1) para realizar el ataque DoS.....	61
Figura 20: Filtro para visualizar mensajes de Linux	61
Figura 21: Se cambia el origen (dirección IP) de los datos de la máquina atacada y envía más datos.....	62
Figura 22: Saturación a la máquina atacada con el envío de datos de manera masiva para cortar la comunicación entre los teléfonos.....	62
Figura 23: Ver la dirección MAC del atacante para llevar a cabo el ataque ARP Spoofing	63
Figura 24: Visualización de tablas de ARP.....	63
Figura 25: Se envía datos a la víctima para cambiar su dirección MAC	64
Figura 26: Visualización del antes y después de las direcciones MAC de la víctima	64
Figura 27: Activación del DHCP Snooping	65
Figura 28: Activación del DHCP Snooping en las vlans creadas	65
Figura 29: Activación de las interfaces que se usa	65
Figura 30: En interfaces se activa los puertos de confianza	66
Figura 31: Máquina de atacante no puedo obtener una dirección IP	66
Figura 32: Llamada libre de posible ataque	67
Figura 33: Atacante entra en la red y desconecta al cliente	67
Figura 34: Puerto de Switch para la aplicación de Port-Security	67
Figura 35: Configuración de la interfaz de Switch para permitir una solo dirección MAC	68
Figura 36: Revisión de la interfaz y verificación de la activación del Port-Security	68
Figura 37: Desconectamos la Interfaz para luego conectarla al atacante y verificar que no tiene acceso.....	68
Figura 38: Ha sido protegida ya que no recibe alguna dirección IP el atacante.....	69
Figura 39: Creación de VLAN para las interfaces no ocupadas	69
Figura 40: Interfaces con punto verde con las que se están usando.....	69
Figura 41: Verificación de las interfaces no usadas estén en la VLAN NO_USADAS.....	70
Figura 42: Comandos para crean una ACL que bloquea todo el tráfico IP.....	70
Figura 43: la máquina del atacante no puede conectarse y por ende no podrá realizar ataques (DDOS, ARP Spoofing o Eavesdropping)	70
Figura 44: Monitoreo de la red VoIP para saber que procesos están pasando	71
Figura 45: El tráfico de ambas interfaces fuentes sea monitoreado o analizado en la interfaz de destino.....	71
Figura 46: Encender la maquina donde se va a usar el Port-Mirror y comenzar a capturar	71
Figura 47: Se habilitará la opción para abrir Wireshark	72
Figura 48: Ejemplo de los procesos que se suceden en la red	72

GLOSARIO

A

Amenazas de Seguridad: Situaciones o eventos que tienen el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información.

C

Contingencia: Planificación para situaciones de emergencia o eventos imprevistos.

G

GNS3 (Graphical Network Simulator-3): Es una herramienta para la simulación de redes que facilita la creación y prueba de configuraciones de red en un entorno virtual.

M

Mitigación: Acciones tomadas para reducir la gravedad o consecuencias de un riesgo o amenaza.

P

Protocolos VoIP: Conjunto de reglas y estándares que rigen la transmisión de voz sobre IP.

S

Sistemas de Detección de Intrusiones (IDS): Herramientas que supervisan y examinan el tráfico de la red para detectar posibles actividades maliciosas o incumplimientos de seguridad.

Topología de Red: Configuración física o lógica de una red, incluyendo la disposición y conexión de sus componentes.

V

Vulnerabilidades: Debilidades o fallos en un sistema que pueden ser explotados para comprometer la seguridad.

VoIP (Voz sobre IP): Tecnología que facilita la transmisión de voz mediante protocolos de Internet en lugar de utilizar las redes telefónicas convencionales.

INTRODUCCIÓN

En la era digital actual, la amplia adopción de tecnologías de Voz sobre IP (VoIP) ha transformado la comunicación, ofreciendo beneficios en eficiencia y costos. Sin embargo, este cambio ha expuesto las redes a graves amenazas de seguridad. La falta de un análisis exhaustivo y estrategias específicas de contramedidas ha contribuido a la vulnerabilidad de las redes VoIP, comprometiendo la confidencialidad e integridad de las comunicaciones.

Para abordar estas cuestiones, se propone utilizar GNS3 como entorno simulado para redes VoIP, permitiendo la comprensión de posibles escenarios de ataques y el desarrollo de estrategias de seguridad más eficaces. La hipótesis principal plantea que la implementación de contramedidas en redes de VoIP protegerá a las mismas de amenazas como accesos no autorizados o manipulación de datos.

En la simulación de redes VoIP utilizando SIP en GNS3, emplearemos dos protocolos esenciales: SIP (Session Initiation Protocol) para la señalización y el establecimiento de llamadas, y RTP (Real-time Transport Protocol) para el transporte en tiempo real de datos de audio y video. Estos protocolos son cruciales para permitir una comunicación de voz sobre IP eficiente y se integran en la infraestructura de GNS3 para recrear escenarios realistas de redes VoIP.

En la parte de la simulación de amenazas en redes VoIP en GNS3, se explorarán tres tipos de ataques significativos: el Ataque de Denegación de Servicios Distribuida (DDoS), la Escucha No Autorizada (Eavesdropping) y el Suplantación de ARP (ARP Spoofing). Estas amenazas representan escenarios realistas que pueden comprometer la seguridad de las comunicaciones VoIP. El ataque DoS busca inundar la red para interrumpir el servicio, el Eavesdropping se centra en interceptar y escuchar comunicaciones sin autorización, mientras que el ARP Spoofing implica engañar a la red para redirigir el tráfico a través del atacante. La simulación permitirá evaluar la vulnerabilidad de las redes VoIP ante estos escenarios y desarrollar estrategias efectivas de defensa.

La metodología a usar es la PPDIOO para la gestión de redes consta de seis fases: Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. Se utiliza para asegurar que la red se implemente de manera eficiente, se opere de manera efectiva y se adapte a las necesidades cambiantes. Proporciona una estructura lógica para la gestión de proyectos de red, desde la planificación inicial hasta la optimización continua, contribuyendo a la estabilidad, seguridad y eficiencia de la infraestructura de red.

A medida que avanzamos en cada fase de esta investigación, se realizará un seguimiento continuo para determinar el porcentaje de cumplimiento de los objetivos establecidos. Este enfoque permitirá una evaluación constante y una adaptación según sea necesario para garantizar los resultados obtenidos.

i. Declaración y formulación del Problema

La adopción generalizada de tecnologías VoIP ha expuesto las redes a amenazas de seguridad significativas. Sin embargo, la falta de análisis y estrategias específicas de contramedidas ha contribuido a esta vulnerabilidad, creando un entorno propicio para la explotación de vulnerabilidades. Como resultado, las redes VoIP enfrentan diversas amenazas que comprometen la confidencialidad e integridad de las comunicaciones, incluyendo accesos no autorizados y manipulación de datos en tiempo real.

La relación causal entre la carencia de análisis y contramedidas permite que estas amenazas impacten directamente la seguridad y privacidad de las conversaciones en entornos VoIP. Para proporcionar una visión más clara y precisa del problema, se ha realizado un árbol de problemas (Figura 1), estructurado en secciones que incluyen las causas, el problema en sí mismo y sus efectos. Esta representación visual facilita la identificación del problema principal que se abordará en la investigación, permitiendo una comprensión detallada de la situación.

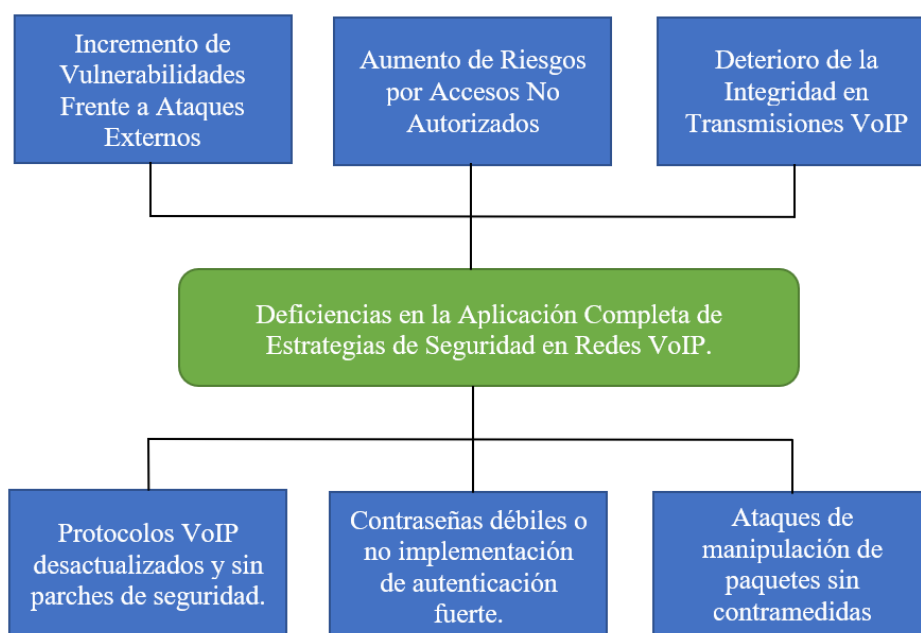


Figura 1: Árbol de problemas Causa - Efecto

Formulación del Problema

- ¿En qué medida la falta de un análisis exhaustivo de las amenazas impacta la capacidad de las redes VoIP para resistir accesos no autorizados y manipulación de datos en tiempo real?
- ¿Cuáles son las vulnerabilidades más destacadas en las estrategias de contramedidas existentes para proteger las redes VoIP contra vulnerabilidades de seguridad?
- ¿Cómo el empleo de GNS3 como entorno simulado para redes VoIP favorece la comprensión de posibles escenarios de ataques y el desarrollo de estrategias de seguridad más eficaces?

- ¿Cómo afecta la falta de actualizaciones de software en las redes VoIP y cuáles son las mejores prácticas para garantizar una protección efectiva?

ii. Objeto de estudio y Campo de acción

La Tabla 1 detalla el Objeto de estudio, centrado en vulnerabilidades en Protocolos VoIP, y su Campo de acción, que abarca estrategias de contramedidas, impacto de la criptografía y mecanismos de detección de intrusiones en estas comunicaciones.

Tabla 1: Objeto de estudio y campo de acción

Objeto de estudio	Campo de acción
Vulnerabilidades en Protocolos VoIP	Investigar y analizar las debilidades específicas en los protocolos de voz sobre IP que podrían exponer las redes a amenazas de seguridad.
Estrategias de Contramedidas en Comunicaciones VoIP	Desarrollar y evaluar estrategias efectivas de contramedidas para proteger las comunicaciones VoIP contra accesos no autorizados, interceptación de datos y manipulación en tiempo real.
Impacto de la Criptografía en la Seguridad de Comunicaciones VoIP	Analizar cómo las técnicas criptográficas pueden fortalecer la seguridad en las redes VoIP, protegiendo la confidencialidad de las comunicaciones.
Análisis de Técnicas de Encriptación para Conversaciones VoIP	Evaluar diferentes técnicas de encriptación y su eficacia en la protección de la confidencialidad de las conversaciones VoIP, proponiendo mejoras o ajustes según sea necesario.
Desarrollo de Mecanismos de Detección de Intrusiones en Redes VoIP	Crear y evaluar mecanismos de detección de intrusiones específicos para entornos VoIP, permitiendo la identificación temprana de actividades maliciosas y la toma de medidas preventivas.

iii. Objetivos

Objetivo General

- Implementar medidas de seguridad en infraestructuras LAN que emplean VoIP mediante la simulación de escenarios de ataque para la detección e identificación de vulnerabilidades, con el fin de asegurar la confidencialidad y privacidad de las comunicaciones.

Objetivos específicos

- Investigar sobre el protocolo de VoIP a través de artículos científicos para comprender las vulnerabilidades potenciales en las infraestructuras LAN que utilizan VoIP.
- Analizar herramientas disponibles para la configuración de entornos de redes VoIP y seleccionar las más adecuadas para simular escenarios realistas de pruebas de seguridad.
- Implementar el entorno simulado de redes VoIP para llevar a cabo pruebas controladas y evaluar la efectividad de los controles de seguridad propuestos.

- Identificar las vulnerabilidades en las infraestructuras LAN que usan VoIP a través de pruebas exhaustivas en el entorno simulado.
- Evaluar la eficacia de los controles implementados para la protección de la privacidad en redes LAN con VoIP, mediante análisis detallados de su funcionalidad y adaptabilidad.

iv. Hipótesis y variables

Hipótesis principal

- “¿La implementación de controles en las infraestructuras de LAN que utilizan VoIP garantizará la privacidad de las comunicaciones?”

Variables y dimensionado

Para una mejor comprensión de las variables y dimensionamiento, revisar su respectivo concepto en la Tabla 2.

Tabla 2: Variables y Dimensionamiento

Variable	Definiciones	Categorías	Indicadores	Técnicas
Garantizar la privacidad de las comunicaciones	Acción de asegurar que las comunicaciones en redes VoIP se mantengan confidenciales y protegidas de accesos no autorizados.	Seguridad informática, VoIP, Privacidad	Seguridad de la información, Confidencialidad de las comunicaciones VoIP	Encriptación de datos, autenticación de usuarios, protocolos de seguridad
Implementación de controles en infraestructuras de LAN que utilizan VoIP	Acción de establecer medidas de seguridad en las redes LAN que emplean VoIP para garantizar la privacidad de las comunicaciones.	Seguridad informática, VoIP, Infraestructura de red	Privacidad de las comunicaciones en redes VoIP	Implementación de firewalls, encriptación de datos, autenticación de usuarios

v. Justificación

La relevancia de investigar la seguridad en las redes VoIP se fundamenta en la transformación radical de los métodos de comunicación en la era digital. La implementación masiva de la comunicación por voz sobre IP ha introducido desafíos significativos en términos de seguridad cibernética, destacando la necesidad urgente de abordar estas vulnerabilidades. Desde una perspectiva teórica, la seguridad de las redes VoIP plantea un desafío científico innovador y en constante evolución. La complejidad de las amenazas emergentes y las vulnerabilidades en los protocolos de comunicación hacen evidente la necesidad de investigar estrategias efectivas de protección.

En el contexto actual, la vulnerabilidad de las redes VoIP ante ataques cibernéticos representa una preocupación palpable en términos de seguridad y privacidad. La motivación para esta

investigación surge de la necesidad de contrarrestar estos riesgos, salvaguardando la información sensible transmitida a través de estas redes, lo cual es esencial para usuarios individuales y entidades empresariales.

La clave para resolver el problema está en desarrollar e implementar estrategias de seguridad eficaces. El objetivo general es fortalecer la protección de las redes VoIP mediante la identificación de vulnerabilidades, la aplicación de contramedidas y la garantía de la confidencialidad de las comunicaciones. Esta investigación se llevará a cabo mediante análisis detallados, pruebas de penetración y el diseño de protocolos de seguridad robustos.

Los beneficiarios directos de este estudio incluyen usuarios individuales y entidades corporativas que dependen de estas comunicaciones para sus operaciones diarias. La seguridad reforzada no solo protegerá la información transmitida, sino que también garantizará la continuidad de servicios vitales y la confianza del usuario en la integridad de sus comunicaciones.

La factibilidad de la investigación se sustenta en el acceso a herramientas y técnicas avanzadas de seguridad informática, así como en la colaboración con expertos en el campo. La aplicación de metodologías establecidas hace que este proyecto sea alcanzable en un marco de tiempo razonable.

vi. Organización del documento

La estructura propuesta para este documento se divide en tres partes. A continuación, se describe cada una:

Capítulo 1: Este primer capítulo se centra en el marco teórico, proporcionando los detalles necesarios para entender los términos y herramientas involucrados en el desarrollo de proyectos.

Capítulo 2: En este capítulo, se describe el proceso de desarrollo del prototipo, incluyendo las definiciones de la investigación, la metodología empleada en el desarrollo del proyecto, la conclusión del desarrollo y la implementación del prototipo.

Capítulo 3: Finalmente, este capítulo aborda la evaluación y los resultados obtenidos, así como las conclusiones y recomendaciones.

CAPITULO I. MARCO TEÓRICO

1.1 Antecedentes de la investigación

a) Preguntas de investigación

A continuación, se presentan las interrogantes planteadas para llevar a cabo la investigación sobre la simulación, evaluación de amenazas y propuestas de contramedidas en seguridad de redes VoIP.

Tabla 3: Preguntas de investigación

Pregunta	Descripción y motivación
¿Cómo afectan las vulnerabilidades en los protocolos de comunicación a la seguridad de las redes VoIP?	Esta pregunta busca explorar el impacto directo de las vulnerabilidades en los protocolos de comunicación de redes VoIP. La motivación radica en comprender cómo las debilidades en estos protocolos pueden ser aprovechadas por actores maliciosos para comprometer la seguridad de las comunicaciones.
¿Cuáles son las principales amenazas cibernéticas que enfrentan las redes VoIP y cómo pueden mitigarse?	Esta interrogante busca identificar y analizar las amenazas más relevantes que acechan a las redes VoIP, con el objetivo de proponer estrategias efectivas de mitigación. La motivación es desarrollar un conocimiento detallado de los riesgos actuales y encontrar formas de fortalecer la seguridad de estas redes.
¿Qué impacto tiene la implementación de protocolos de cifrado en la confidencialidad de las comunicaciones VoIP?	Esta pregunta tiene como objetivo evaluar el papel del cifrado en la protección de la privacidad de las comunicaciones VoIP. La motivación es comprender cómo el uso de protocolos de cifrado puede mejorar la seguridad y la privacidad de estas comunicaciones.
¿Cuáles son las técnicas de ataque más comunes a las redes VoIP y cuáles estrategias defensivas son efectivas para mitigar estos ataques?	Esta pregunta busca explorar las tácticas de ataque más prevalentes dirigidas a las redes VoIP y analizar las estrategias defensivas efectivas para contrarrestar estos ataques. La motivación radica en comprender las amenazas más actuales y en encontrar soluciones y medidas preventivas que fortalezcan la seguridad de las comunicaciones VoIP frente a estas amenazas.
¿Cómo se puede utilizar GNS3 para simular redes VoIP y qué beneficios ofrece esta simulación para comprender y mejorar la seguridad en entornos virtuales?	Esta pregunta busca explorar la utilización de la plataforma GNS3 para simular redes VoIP, con el objetivo de comprender cómo esta herramienta puede ser empleada para estudiar y mejorar la seguridad en entornos virtuales. La motivación radica en evaluar las capacidades de GNS3 como entorno de simulación y su contribución al análisis y fortalecimiento de la seguridad en redes VoIP virtuales.

b) Palabras claves y Cadena(s) de búsqueda

El plan de búsqueda fusionó métodos automáticos y manuales, validados por expertos en Ingeniería de Requisitos y seguridad. Se exploraron bases de datos como Science Direct, SpringerLink, ACM Digital Library, IEEE Xplore, Scopus y Compendex. El enfoque se centró en recolectar investigaciones destacadas sobre requisitos de seguridad, adaptadas al contexto de redes VoIP para respaldar la tesis en desarrollo.

- VoIP
- Seguridad en VoIP
- Firewalls para proteger VoIP
- Virtualización de redes
- Protocolos para servicios VoIP
- Tráfico VoIP
- Ataques VoIP
- Comunicación VoIP segura

Cadena de búsqueda en inglés:

1. “VoIP security measures”
2. “Security protocols for VoIP services”
3. “VoIP traffic encryption methods”
4. “Protecting VoIP with firewalls”
5. “Virtualization in VoIP networks”
6. “Securing communication in VoIP”
7. “VoIP attacks and prevention strategies”
8. “Ensuring secure VoIP communication protocols”
9. “Enhancing VoIP security with network virtualization”

c) Criterios de inclusión y exclusión

La Tabla 4 presenta los criterios de inclusión y exclusión.

Tabla 4: Criterios de Inclusión y exclusión

Nº	Criterios de inclusión
1	Relevancia temática en seguridad VoIP.
2	Calidad académica: revisión por pares en revistas reconocidas.
3	Actualidad: preferentemente dentro de los últimos cinco años.
4	Enfoque metodológico en estrategias de seguridad VoIP.
5	Profundidad y soluciones prácticas en seguridad VoIP.

- 1 Irrelevancia en el tema de seguridad VoIP.
- 2 Falta de revisión por pares o calidad cuestionable.
- 3 Obsolescencia: estudios muy antiguos sin relevancia actual.
- 4 Superficialidad o falta de análisis detallado.
- 5 Limitaciones de idioma o acceso al texto completo.

d) Proceso y resultados de la búsqueda

Proceso de búsqueda.

Se llevó a cabo la búsqueda utilizando palabras clave y combinaciones de términos en varias data base como Science Direct, Web of Science y Scopus. Los pasos del proceso de búsqueda se describen en la imagen que sigue. (Figura 2).

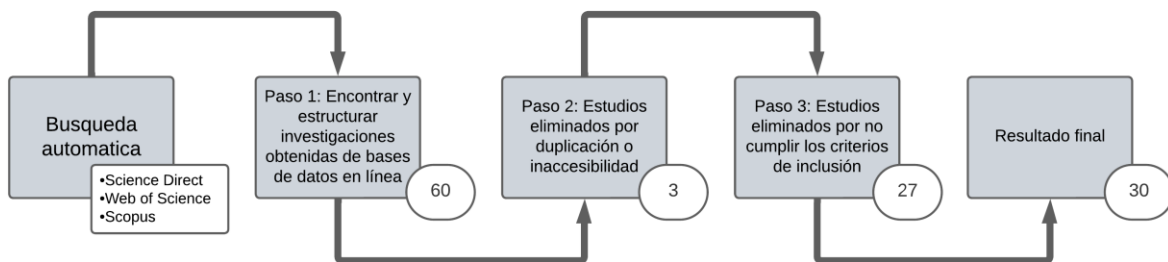


Figura 2: Proceso de búsqueda de información

Resultados de la búsqueda.

Los resultados de la búsqueda se organizaron según el año. En la imagen siguiente se muestra la cantidad de estudios por año. (Figura 3).

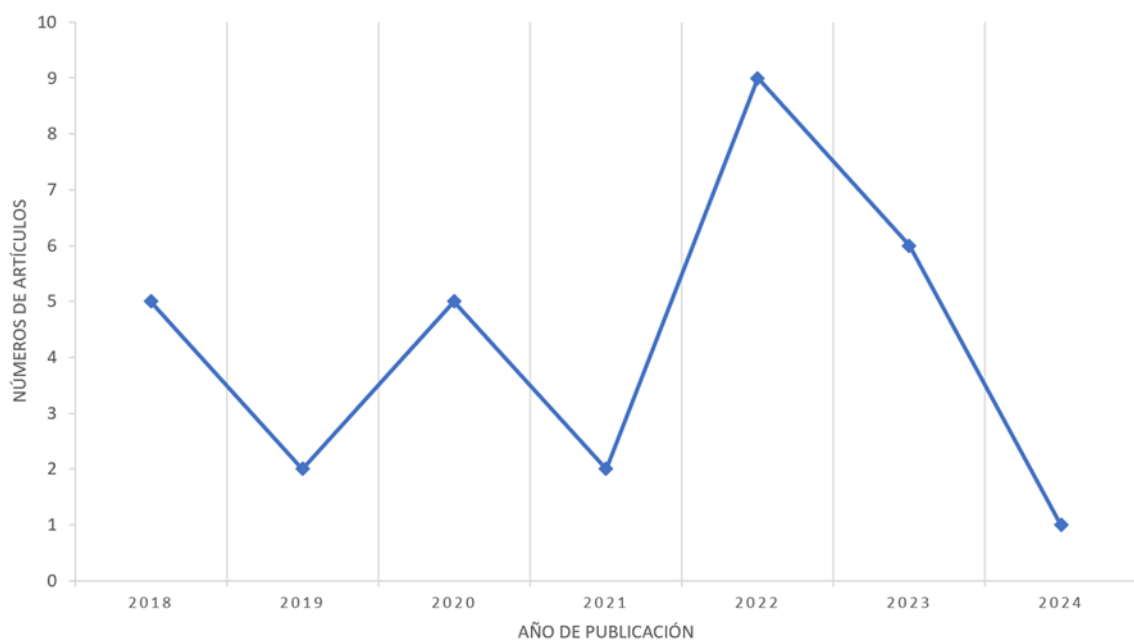


Figura 3: Resultados de búsqueda, diagrama de artículos por año

1.2 Antecedentes históricos

La seguridad en las redes VoIP ha evolucionado significativamente desde 2018 hasta la actualidad, transformando la forma en que estas comunicaciones se gestionan y protegen. A lo largo de este período, se han destacado diversos hitos que han marcado esta evolución y han redefinido las preocupaciones y los enfoques en torno a la seguridad de las redes VoIP.

En el contexto empresarial, la adopción de VoIP ha sido impulsada por varias necesidades clave. En primer lugar, la reducción de costos ha sido un factor determinante. Las empresas comenzaron a adoptar VoIP debido a su potencial para reducir significativamente los costos operativos. A diferencia de la telefonía tradicional, VoIP permite hacer llamadas a través de Internet, eliminando los costos de larga distancia y reduciendo las tarifas de telefonía fija.

Además, VoIP ofrece una mayor flexibilidad y escalabilidad, permitiendo a las empresas añadir líneas telefónicas y funciones avanzadas sin la necesidad de una infraestructura física compleja. Esta capacidad de crecer y adaptarse rápidamente a las necesidades cambiantes del negocio ha sido crucial para muchas organizaciones.

Expansión de la Telefonía IP

Desde 2003, las llamadas VoIP han representado un 25% de todas las llamadas de voz, y para 2008, aproximadamente la mitad de los usuarios en desarrollo utilizaban VoIP en sus dispositivos móviles o computadoras [1]. Esta expansión ha marcado un cambio significativo en la forma en que las personas se comunican, llevando a una mayor adopción y uso de tecnologías VoIP.

Adopción Empresarial de VoIP

La adopción de VoIP por parte de las empresas ha sido una tendencia marcada desde 2005, con muchas compañías implementando esta tecnología para reducir costos y mejorar la productividad. En algunos países, como Francia, se proyecta la finalización de la migración a telefonía IP para 2023 [2]. Este cambio hacia VoIP en entornos corporativos ha sido impulsado por sus ventajas en eficiencia y economía.

Desarrollo de Soluciones para PYMES

A partir de 2009, soluciones más accesibles para pequeñas y medianas empresas han emergido en el campo de la telefonía VoIP. Plataformas como Asterisk, un software de telefonía de código abierto, han proporcionado alternativas viables para empresas de menor tamaño, promoviendo la adopción de VoIP en diversos sectores comerciales.

Introducción de Nuevas Tecnologías

En los últimos años, se han introducido nuevas tecnologías y estándares en el ámbito de la telefonía VoIP. Entre estas innovaciones se encuentra la LLR (Local Public Network), que ha

permitido una mayor interoperabilidad y flexibilidad en las redes de voz, mejorando así su desempeño y adaptabilidad.

Contribuciones Relevantes para la Seguridad VoIP

Autores como Caviglione, Keller, Mazurczyk y Saenger [3] han propuesto el uso de comunicaciones VoIP como una metodología para mejorar la privacidad. Esta propuesta se centra en ocultar el tráfico en conversaciones VoIP, utilizando paquetes de silencio falsos como portadores para prevenir la divulgación de información a posibles atacantes. Se ha indicado que este enfoque es particularmente útil en la privacidad de transferencias de archivos y podría fortalecer la seguridad en casos de uso reales.

En una línea similar, Mohamudally y Armoogum [4] han explorado una técnica basada en aprendizaje profundo para detectar intrusos en redes VoIP. Esta técnica se apoya en el análisis de patrones de tráfico de red, utilizando algoritmos de aprendizaje profundo para identificar anomalías que podrían indicar la presencia de un intruso. Según sus investigaciones, esta técnica ha demostrado una alta precisión en la detección de intrusos en redes VoIP.

Tendencias de Seguridad para 2023

En el horizonte para 2023, se prevé un aumento en la dedicación de recursos para proteger las redes VoIP debido a riesgos comunes como phishing, ataques DDoS, manipulación de llamadas, malware y virus, entre otros [5]. Esta proyección refleja la constante preocupación por mejorar la seguridad en entornos empresariales que utilizan tecnologías VoIP.

La evolución de la seguridad de las redes VoIP desde 2018 hasta la actualidad ha sido impulsada por el crecimiento en la adopción de tecnologías de voz digital, así como por la constante búsqueda de soluciones que garanticen la confidencialidad y la integridad de las comunicaciones VoIP en entornos empresariales. Esta evolución ha sido clave para adaptarse a un entorno digital en constante cambio y para mitigar los riesgos asociados a estas redes en un mundo conectado y tecnológicamente avanzado.

1.3 Antecedentes teóricos

Los fundamentos teóricos desempeñan una función fundamental al proporcionar este contexto, vinculando los resultados de investigaciones anteriores con la intención y el enfoque del estudio actual. Específicamente, la Figura 4 presenta de manera visual algunos de los conceptos esenciales que se explorarán de manera efectiva.

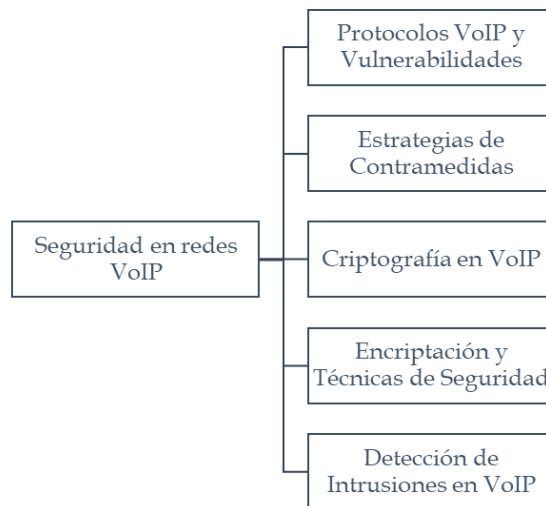


Figura 4: Antecedentes históricos de la seguridad en redes VoIP

1.3.1. Protocolos VoIP y Vulnerabilidades

La telefonía IP (VoIP) utiliza varios protocolos, como SIP (Session Initiation Protocol), H.323 y IAX (Inter-Asterisk Exchange). Estos protocolos presentan diversas vulnerabilidades, que incluyen ataques de denegación de servicio (DoS), secuestro de sesiones y main-in-the-middle. Algunas de las vulnerabilidades comunes en las comunicaciones VoIP son el packet sniffing, la pérdida de privacidad, el hacking y el spam. Para mitigar estos riesgos, es fundamental implementar medidas de seguridad, como mantener actualizados los sistemas, utilizar contraseñas seguras y cifrar el tráfico de VoIP. Además, monitorear regularmente la red y los dispositivos VoIP es esencial para detectar y responder a posibles amenazas. [6] [7] [8].

En el contexto de nuestro trabajo, hemos identificado que las redes de Voz sobre IP (VoIP) presentan vulnerabilidades significativas que pueden ser explotadas por ciberdelincuentes para llevar a cabo diversos tipos de ataques. Entre los protocolos comunes utilizados en las redes VoIP se encuentran SIP, RTP, SRTP y H.323, cada uno con sus propias vulnerabilidades y riesgos de seguridad. Los ataques de Denegación de Servicio Distribuida (DDoS) buscan saturar servidores de VoIP, interrumpiendo así el servicio para usuarios legítimos. El Eavesdropping implica la interceptación no autorizada de conversaciones, debido a la falta de cifrado adecuado en las comunicaciones VoIP. Por último, el Hombre en el Medio (MITM) permite a los atacantes interceptar y potencialmente modificar las comunicaciones entre dos partes sin su conocimiento. Para mitigar estos riesgos, se requiere medidas de seguridad combinadas, como la implementación de cifrado y autenticación en los protocolos de VoIP, así como la configuración adecuada de los servidores PBX y la concienciación sobre las mejores prácticas de seguridad entre los usuarios finales [9].

1.3.2. Estrategias de Contramedidas

Las estrategias de contramedidas para proteger las comunicaciones VoIP incluyen una variedad de medidas que ayudan a mitigar los riesgos y mantener la seguridad en las comunicaciones.

Algunas de estas contramedidas son:

1. Autenticación: La autenticación es fundamental para comprobar la identidad de los usuarios y garantizar que solo autorizados puedan acceder a las comunicaciones VoIP.
2. Control de acceso: Implementar un control de acceso efectivo permite limitar el acceso a las comunicaciones VoIP solo a los usuarios autorizados.
3. Cifrado: El cifrado es esencial para proteger la seguridad de las llamadas de VoIP. Los algoritmos de cifrado avanzados, como AES y SSL, pueden ayudar a garantizar que el tráfico de voz y video se transmita de manera segura. [10]
4. Monitoreo y auditoría: El monitoreo regular de la red y los dispositivos VoIP permite detectar y responder a posibles amenazas. Las herramientas de auditoría de seguridad pueden ayudar a identificar y analizar el tráfico de VoIP y a detectar actividades sospechosas.
5. Firewall: Un firewall puede ayudar a proteger la red de VoIP de ataques externos y a mantener la comunicación segura entre los usuarios autorizados. [11]

En el contexto de nuestro trabajo de seguridad en redes VoIP, las estrategias de contramedidas juegan un papel fundamental en la protección contra ataques específicos, como DDoS, Eavesdropping y MITM. Implementar medidas como sistemas de detección de intrusos, servicios de protección DDoS externos, protocolos de cifrado fuertes y autenticación robusta ayuda a salvaguardar la integridad y seguridad de las comunicaciones VoIP. Estas contramedidas son esenciales para mantener la disponibilidad del servicio, proteger la confidencialidad de las comunicaciones y prevenir la interceptación no autorizada de llamadas. Implementando estas medidas, podemos reforzar la infraestructura VoIP frente a amenazas maliciosas y asegurar una experiencia de usuario segura y confiable en nuestras red [12].

Para mitigar ataques DDoS:

- Instalar sistemas de detección de intrusos (IDS) para detectar y reducir el tráfico malicioso antes de que impacte la red.
- Utilizar servicios de protección DDoS proporcionados por proveedores externos para filtrar el tráfico no deseado y mantener la disponibilidad del servicio VoIP.

Para contrarrestar el Eavesdropping:

- Utilizar protocolos de cifrado fuertes como SRTP (Secure Real-time Transport Protocol) para proteger la confidencialidad de las comunicaciones VoIP.

- Implementar sistemas de autenticación fuerte para verificar la identidad de los dispositivos VoIP y evitar la interceptación de llamadas.

En cuanto al MITM:

- Configurar autenticación de extremo a extremo para garantizar que las comunicaciones VoIP solo sean legibles por los destinatarios previstos.
- Monitorizar constantemente la red para detectar actividades sospechosas y responder rápidamente ante posibles ataques MITM [13].

1.3.3. Criptografía en VoIP

La criptografía es crucial para salvaguardar la privacidad y la confidencialidad en las comunicaciones VoIP. Entre los algoritmos de cifrado más utilizados en estas comunicaciones se encuentran el AES (Advanced Encryption Standard) y el RSA (Rivest-Shamir-Adleman). AES, un algoritmo de cifrado simétrico, se emplea para encriptar el tráfico de voz y video en tiempo real, mientras que RSA, un algoritmo de cifrado asimétrico, se usa para autenticar y establecer conexiones seguras entre los dispositivos VoIP. [14]

Asimismo, el protocolo SRTP (Secure Real-time Transport Protocol) emplea el estándar de cifrado avanzado (AES) para proteger los paquetes de datos, proporcionando autenticación de mensajes y defensa contra ataques de repetición en los datos de voz transmitidos, lo que lo convierte en una opción ideal para VoIP. [12]

La utilización de estos algoritmos de cifrado y protocolos criptográficos asegura que el tráfico de voz y video se transmita de forma segura, preservando la privacidad y confidencialidad de las comunicaciones VoIP.

1.3.4. Encriptación y Técnicas de Seguridad

Los protocolos específicos de encriptación utilizados en las comunicaciones VoIP incluyen SRTP (Secure Real-time Transport Protocol) y TLS (Transport Layer Security) [15]. Estos protocolos se implementan para garantizar la integridad y confidencialidad de las conversaciones VoIP.

El protocolo SRTP (Secure Real-time Transport Protocol) emplea el estándar de cifrado avanzado (AES) para proteger los paquetes de datos, brinda autenticación de mensajes y resguarda contra ataques de repetición en los datos de voz transmitidos, convirtiéndolo en una opción ideal para VoIP. SRTP se utiliza para cifrar en tiempo real el tráfico de voz y video, asegurando así la privacidad y confidencialidad de las comunicaciones.

El protocolo TLS (Transport Layer Security) se emplea para asegurar la comunicación entre el cliente y el servidor, proporcionando autenticación del servidor y garantizando la integridad de los datos transmitidos. TLS evolucionó a partir de Secure Socket Layers (SSL), que fue desarrollado originalmente por Netscape Communications Corporation en 1994. TLS se usa

frecuentemente en aplicaciones de comunicación VoIP para asegurar la privacidad y confidencialidad de las conversaciones. [16]

1.3.5. Detección de Intrusiones en VoIP

Los sistemas y herramientas de detección de intrusiones adaptados para entornos VoIP desempeñan un papel crucial en la identificación de actividades maliciosas, el análisis de tráfico y la adopción de medidas preventivas en las redes VoIP. Algunas de las técnicas y herramientas utilizadas incluyen:

1. **Sistemas de Detección de Intrusos (IDS):** Estos sistemas supervisan la red para identificar actividades sospechosas o maliciosas y emiten alertas en tiempo real al detectar comportamientos anómalos. [17]
2. **Firewalls Específicos para VoIP:** Estos firewalls están diseñados para inspeccionar y controlar el tráfico VoIP, lo que ayuda a prevenir y detectar posibles amenazas.
3. **Análisis Avanzado de Protocolos:** Esta técnica implica el monitoreo y análisis detallado del tráfico de protocolos VoIP para identificar posibles anomalías o ataques. [18]
4. **Inteligencia Artificial (IA):** La IA se está integrando en los sistemas de VoIP para configurar firewalls y sistemas de detección de intrusiones, lo que permite una detección más precisa y una respuesta más rápida a las amenazas.

Estas herramientas y técnicas son esenciales para salvaguardar las redes VoIP, detectar posibles amenazas y adoptar medidas preventivas para asegurar la seguridad de las comunicaciones VoIP.

1.4 Antecedentes Contextuales

La Voz sobre Protocolo de Internet (VoIP) es una de las tecnologías más importantes en telecomunicaciones, destacando por su mejora continua en calidad y confiabilidad. Además, su costo es mucho menor en comparación con la telefonía fija o móvil tradicional. VoIP permite realizar llamadas telefónicas o de video entre diferentes dispositivos, como ordenadores personales, teléfonos VoIP, teléfonos móviles e incluso teléfonos tradicionales, siempre que haya una red IP subyacente. Por esta razón, VoIP se utiliza tanto en entornos domésticos como empresariales.

El sistema de comunicación VoIP encubierto propuesto [19] prioriza la seguridad y la integridad de los datos confidenciales. Para ello, emplea un algoritmo de cifrado simétrico eficiente para proteger los datos y utiliza el algoritmo hash MD5 para calcular el valor del resumen del mensaje de los datos sin formato. En lugar de incrustar los flujos de bits de los datos confidenciales uniformemente en la señal de audio original, se distribuyen de manera aleatoria mediante una secuencia caótica generada a partir de un mapeo logístico caótico.

El sistema de comunicación encubierta VoIP propuesto tiene cuatro módulos en su extremo de incrustación: el módulo de preprocesamiento, el módulo de incrustación, el módulo de cálculo de resumen de mensajes y la transmisión de red.. El módulo de incrustación es el núcleo del sistema de esteganografía VoIP, ya que determina si la ubicación de los datos confidenciales incrustados es indetectable. Las salidas en el extremo de integración incluyen el valor del resumen del mensaje, la clave utilizada para cifrar los datos, el valor inicial del mapeo logístico y las muestras de audio que contienen los datos confidenciales incrustados.

La seguridad en VoIP ha sido ampliamente investigada en años recientes, y se han establecido protocolos y mecanismos de seguridad específicos [20]. Los problemas de seguridad en VoIP son comparables a otros desafíos de ciberseguridad, como el secuestro de llamadas, la suplantación de identidad, los ataques de denegación de servicio, y las amenazas de phishing y malware. Para abordar estos riesgos, se utilizan mecanismos de seguridad tales como cifrado, autenticación de entidades y análisis profundo de paquetes. Además, se ha explorado el uso de Redes Privadas Virtuales (VPN) para proteger el tráfico VoIP. Sin embargo, las tecnologías VoIP aún son vulnerables a varios ataques debido a la ausencia de protocolos de seguridad robustos o a las debilidades en los protocolos existentes y sus implementaciones.

En los últimos años, se han propuesto varios esquemas de seguridad, como los basados en el intercambio de claves autenticadas por contraseña (PAKE) [21], los esquemas basados en hash y cifrado simétrico, y los esquemas de criptografía de clave pública (PKC), entre otros. Sin embargo, las implementaciones disponibles no pueden proporcionar referencias concretas a los usuarios.

El progreso en la integración de Internet y las telecomunicaciones, sumado al aumento en la demanda de aplicaciones que requieren un amplio ancho de banda y alta Calidad de Servicio (QoS), impone la necesidad de una red sólida y componentes internos que aseguren la protección de los datos y optimicen el rendimiento. Esto implica la necesidad de tecnologías de transmisión de datos que no solo faciliten el enrutamiento y el descubrimiento del mejor camino, sino que también aseguren la comunicación de los datos [22].

El rápido crecimiento de VoIP está estrechamente vinculado a la evolución de los protocolos VoIP, destacando el Protocolo de Inicio de Sesión (SIP). SIP, un protocolo de capa de aplicación, facilita la creación, modificación, asignación y finalización de intercambios de datos entre usuarios, incluyendo voz, video y texto. Los sistemas VoIP que emplean SIP han sido mejorados con la incorporación de detección de intrusiones, modelado del sistema SIP, el Protocolo de Transporte en Tiempo Real (RTP), y la interacción entre SIP y RTP. Además, el códec estándar utilizado en VoIP es el G.711, que es el códec de compresión de audio definido por el ITU-T.

En la mayoría de los casos, VoIP utiliza el Protocolo de Transporte en Tiempo Real (RTP) para la comunicación a través de redes de Protocolo de Internet (IP). Para establecer una llamada VoIP exitosa, el punto final VoIP envía señales a la parte llamada, y la comunicación solo se realiza si ambas partes acuerdan usar el mismo códec de audio. Esta señalización de VoIP incluye el Protocolo de Descripción de Sesión (SDP). Una vez establecida la conexión, RTP se encarga de transportar los datos del medio. VoIP emplea códecs que requieren un mínimo de ancho de banda para funcionar de manera óptima. Además del ancho de banda necesario para estos códecs, VoIP también transporta encabezados de 40 bytes correspondientes a IP, Protocolo de Datagramas de Usuario (UDP) y RTP. La compresión de encabezados VoIP puede ahorrar un ancho de banda significativo. Sin embargo, además de los problemas relacionados con los encabezados, existen otros que afectan el rendimiento de las redes VoIP [23].

La voz sobre IP (VoIP) permite la comunicación de voz en tiempo real a través de redes IP. Un sistema VoIP tiene dos funciones básicas: la función de señalización, diseñada para establecer, modificar y terminar una conversación, y la función de transmisión de medios, que se utiliza para transportar el tráfico de voz. Para implementar estas funciones existen tanto protocolos estándar como protocolos propietarios [24]. A continuación, se presenta un ejemplo de cada uno.

Protocolos estándar (por Internet Engineering Task Force - IETF):

Protocolo de Inicio de Sesión (SIP): SIP es un protocolo basado en texto que utiliza un formato de mensajes semejante al de HTTP. Un mensaje SIP puede incluir una carga útil del Protocolo de Descripción de Sesión (SDP) para negociar los parámetros de la sesión, como el códec preferido, entre los participantes de la comunicación. Los usuarios SIP se identifican mediante Identificadores Uniformes de Recursos (URI), una cadena que combina un nombre de dominio y un nombre de usuario registrado para ese dominio (por ejemplo, sip. zhang@kau.se). Se recomienda proteger los mensajes SIP mediante TLS, IPSec o S/MIME.

Protocolo de Transporte en Tiempo Real (RTP): RTP define el formato de los paquetes para la entrega de contenido de voz. Además de la voz, un paquete RTP puede transportar eventos de clic de botón del usuario para indicar que se ha presionado un botón, lo que permite la interacción con un servidor de respuesta de voz interactiva (IVR). La carga útil del paquete RTP se puede cifrar utilizando mecanismos SRTP.

Protocolos propietarios (de Skype):

Skype: Skype es un popular proveedor de servicios VoIP. Los usuarios pueden seleccionar libremente un nombre de usuario no utilizado para crear una cuenta. Los detalles de sus protocolos de señalización y transmisión de medios no están disponibles al público. Según su página de inicio, Skype utiliza algoritmos del Estándar de Cifrado Avanzado (AES) con una clave de hasta 256 bits para proteger las comunicaciones de los usuarios.

Los ataques de denegación de servicio distribuido (DDoS) son especialmente peligrosos porque bloquean el acceso de los usuarios legítimos a los servicios de VoIP. Al apuntar a uno o varios servidores VoIP, estos ataques pueden comprometer la disponibilidad del servicio, lo que puede afectar la productividad laboral y, potencialmente, reducir los ingresos.

Muchos investigadores han utilizado enfoques de aprendizaje automático para detectar ataques DDoS, como se discutirá en la siguiente sección. Estos métodos requieren un conocimiento profundo de la red VoIP para seleccionar las características adecuadas de los mensajes SIP. Además, los umbrales y parámetros del modelo deben actualizarse continuamente para adaptarse a varios tipos de ataques DDoS. Sin embargo, algunos de estos enfoques no han logrado una alta precisión en la detección de ataques DDoS de baja tasa.

En la comunicación VoIP (Voz sobre Protocolo de Internet), varios protocolos son fundamentales para asegurar una transmisión eficiente y segura de datos de voz a través de redes IP. Cada protocolo cumple funciones y tiene características específicas que mejoran diferentes aspectos del proceso de comunicación, desde el establecimiento de llamadas hasta la transmisión en tiempo real. A continuación, se presentan algunos de los protocolos más relevantes empleados en VoIP.:

H.323:

El estándar H.323 establece los procedimientos, protocolos y componentes necesarios para la comunicación multimedia a través de redes de paquetes. Este sistema se emplea para servicios de comunicación multimedia o de igual a igual y es especialmente eficaz en entornos multipunto [25].

Protocolo de Inicio de Sesión (SIP):

SIP es un protocolo de comunicación telefónica que gestiona y coordina sesiones de comunicación multimedia, incluyendo mensajería instantánea, juegos en línea y otros servicios. Similar al protocolo web HTTP, los mensajes SIP están compuestos por encabezados y un cuerpo de mensaje. Utiliza principalmente el puerto 5060 y puede ser configurado para funcionar sobre UDP/TCP. SIP es reconocido como el protocolo autorizado para servicios de voz, telefonía y video sobre IP (VoIP).

Protocolo de Control de Puerta de Enlace de Medios (MGCP):

MGCP es un protocolo VoIP diseñado para gestionar llamadas y puertas de enlace VoIP a través de dispositivos de control de llamadas denominados Agentes Telefónicos. MGCP asume que estos dispositivos están configurados para enviar comandos de control de usuario entre sí. Los Agentes Telefónicos también facilitan la conexión directa a teléfonos IP, y los Media Gateways o teléfonos basados en Internet ejecutan los comandos enviados por estos agentes [26].

Protocolo en Tiempo Real (RTP):

RTP se emplea para la transmisión de datos en tiempo real a través de la red, facilitando el envío de datos VoIP a varios destinos mediante el protocolo de Internet. Es el protocolo principal para el transporte de video y audio dentro de redes IP. RTP se complementa con señalización que ayuda a establecer conexiones en la red. Aunque es útil para la transmisión de video y audio, RTP no garantiza la entrega de paquetes de red VoIP ni la calidad de servicio (QoS). Las sesiones RTP se identifican mediante diferentes identificadores SSRC, uno para la transmisión de video y otro para la transmisión de audio [27].

El phishing, o vishing, es una amenaza común en las llamadas VoIP, en la que el atacante se hace pasar por un representante de un banco para recolectar información personal de la víctima. Los softphones, que utilizan Internet para realizar llamadas, son vulnerables a virus y malware. Además, el spam representa otro riesgo para los usuarios de VoIP, ya que los spammers pueden enviar mensajes no deseados al buzón de voz mediante la dirección IP vinculada a cada teléfono VoIP.

La manipulación de llamadas es otra forma de escucha no autorizada, en la que el atacante modifica las llamadas VoIP y puede insertar retrasos aleatorios en los paquetes RTP. La suplantación del Protocolo de Resolución de Direcciones permite a un atacante controlar una conversación, inyectando nuevos mensajes e insertándose como intermediario [28].

Tipos de Fraude en Redes VoIP

Fraude por Evasión de Peajes

El fraude por evasión de peajes es una práctica común en las redes telefónicas en los últimos años. Consiste en realizar llamadas sin pagar los cargos correspondientes, los cuales son facturados a otra persona. En este caso, los atacantes acceden a las cuentas de usuario de una centralita telefónica para hacer las llamadas, de modo que el propietario de la centralita o el usuario cuya cuenta ha sido comprometida es quien termina pagando. Los beneficios de este fraude pueden ir desde evitar el pago de llamadas anónimas relacionadas con actividades ilícitas hasta cometer

otros tipos de fraude. Todas las llamadas se realizan utilizando cuentas comprometidas, por lo que los atacantes no incurren en ningún costo.

Fraude de Reparto de Ingresos

El fraude de reparto de ingresos ocurre cuando un operador o un proveedor de servicios llega a un acuerdo con un defraudador. En este acuerdo, el defraudador realiza llamadas a números de teléfono propiedad del operador (como números de servicio internacionales con tarifas especiales). Esto genera ingresos que luego son repartidos entre el operador y el defraudador. El beneficio de este fraude es puramente económico: cuanto más tráfico de llamadas se genere, mayor será la ganancia para los defraudadores.

Impacto de los ataques de ARP spoofing

Los ataques de ARP spoofing pueden reducir la velocidad de intercambio de solicitudes y respuestas ARP en la red, lo que ralentiza las comunicaciones entre dispositivos. Esto ocurre porque los atacantes manipulan las direcciones MAC e IP, desviando el tráfico hacia ellos mismos, lo que causa interrupciones y posibles fugas de información. Por tanto, es crucial prevenir estos ataques para mantener la integridad y seguridad de la red [29].

Prevención del ARP spoofing

Para prevenir los ataques de ARP spoofing, se pueden implementar las siguientes medidas:

Filtrado de paquetes: Filtrar paquetes antes de enviar respuestas ARP para asegurarse de que sean legítimos.

Lista negra encriptada: Mantener una lista negra de posibles atacantes para bloquearlos.

Verificación de direcciones: Verificar las direcciones MAC e IP antes de enviar o recibir paquetes.

Estas acciones ayudan a evitar la suplantación de identidad y garantizan la autenticidad de las comunicaciones en la red, protegiéndola contra posibles ataques de ARP spoofing.

Ataques NDP: Efecto y Análisis

Los ataques NDP pueden tener un impacto significativo en las redes y sistemas operativos. Pueden causar tiempo de inactividad de la red, pérdida de paquetes, robo de datos y acceso no autorizado. Además, pueden ser utilizados para lanzar ataques más complejos, como el rastreo o la suplantación de identidad. Estos ataques comprometen la integridad, confidencialidad y disponibilidad de las redes y sistemas operativos, lo que puede resultar en una pérdida significativa de tiempo e ingresos para una organización [30].

Es fundamental implementar controles de seguridad adecuados para protegerse contra los ataques NDP y mitigar sus efectos.

Preocupaciones de seguridad de las aplicaciones VOIP

Fraude de Peaje

El fraude de peaje ocurre cuando un usuario no autorizado utiliza una red VoIP legítima. Este tipo de fraude representa una amenaza significativa para las redes VoIP, ya que incrementa los costos operativos al aprovechar sus recursos sin autorización. El fraude telefónico lidera la lista de amenazas relacionadas con el uso indebido de servicios VoIP [31].

Manipulación de Datos Contables

Cada llamada realizada a través del sistema VoIP se registra en la base de datos contable, generando registros de datos de llamadas (CDR) que incluyen detalles como los números de teléfono involucrados, la hora de la llamada, su duración y otros datos. Un atacante que acceda a la base de datos CDR puede observar patrones de llamadas, obteniendo información confidencial, como la frecuencia de comunicación entre ejecutivos de diferentes empresas, lo que podría indicar una posible alianza o fusión estratégica. Si el atacante obtiene acceso de escritura a la base de datos, podría cambiar o eliminar registros de llamadas.

Alteración del Flujo de Voz

Conocido como ataque de intermediario o suplantación, este tipo de ataque permite al atacante escuchar y manipular el diálogo entre las víctimas. El atacante puede reproducir fragmentos de conversaciones previamente grabadas para alterar el mensaje original enviado por el remitente. Aunque es difícil cambiar todo el diálogo debido a la naturaleza impredecible de las conversaciones humanas, pequeños fragmentos pueden ser alterados, como cambiar "no" por "sí" en una respuesta, o "vender" por "comprar" en una conversación financiera, lo que puede tener consecuencias significativas. Este tipo de ataque también puede ser utilizado en sistemas interactivos de respuesta de voz. Un atacante podría reproducir un saldo anterior de una cuenta bancaria, engañando a la víctima para que crea que no ha habido retiros recientes.

Controlador SDN y NFV para VoIP

Esta sección propone un marco innovador para las redes VoIP, aprovechando los conceptos de SDN y NFV. En este diseño, la red VoIP incluye varios dominios, donde un servidor (PM), varios conmutadores OpenFlow y un controlador gestionan la señalización y los medios en cada dominio. En lugar de proxies SIP de hardware dedicados, el servidor utiliza proxies SIP virtuales (SIP VNF), responsables de enrutar el tráfico de señalización en la capa siete. El número de estos

SIP VNF varía según el tráfico de señalización entrante: disminuye con baja carga y aumenta con alta carga. El controlador se encarga de gestionar estos SIP VNF [32].

Controlador SDN+ para VoIP

En el marco anterior, el enrutamiento de los mensajes de señalización SIP en la capa siete lo realizaban los VNF de VoIP, y el controlador gestionaba el número de SIP VNF. Este apartado desarrolla ese framework para reducir su complejidad en el plano de datos. Aquí, el enrutamiento de los mensajes de señalización en la capa siete se realiza de manera centralizada en el controlador, similar al enrutamiento de los mensajes de capa tres. Esto lleva a una centralización e integración del enrutamiento de todos los mensajes, disminuyendo la dependencia del hardware y permitiendo que las operaciones de enrutamiento se realicen mediante software [33].

Marco 'Call Me Maybe' para Protección contra Ataques DoS

El marco 'Call Me Maybe' es un diseño para redes VoIP que proporciona protección adicional contra ataques DoS. Este marco se basa en la adición de una red TCP "en la sombra" que se puede utilizar como respaldo cuando la red normal sufre un ataque (D)DoS. Los principios del marco son los siguientes:

Capacidad TCP y UDP en una Red: La red debe permitir que los teléfonos VoIP funcionen tanto sobre TCP como sobre UDP. La red TCP "en la sombra" ofrece un protocolo y puerto alternativo para la comunicación en caso de ataque, permitiendo continuar el tráfico de voz.

Uso de un Firewall Restringido por UDP: Con VoIP sobre TCP, se pueden bloquear los puertos UDP, utilizando un firewall para mitigar ataques de inundación UDP. Esto proporciona una capa adicional de seguridad contra ataques DoS.

Cambio de Protocolo Dinámico y Automático: El cambio entre TCP y UDP debe ser automático en respuesta a aumentos de latencia causados por un ataque DoS. Un Centro de Control (CC) puede enviar una señal de "conmutación" a los teléfonos VoIP para alternar entre los protocolos.

Monitoreo de Latencia: Para detectar ataques DoS en tiempo real, es esencial implementar un sistema de monitoreo de latencia. Este sistema debe capturar cambios en los tiempos de respuesta y facilitar la conmutación dinámica entre protocolos.

El marco 'Call Me Maybe' proporciona una capa adicional de seguridad para redes VoIP, complementando cualquier mecanismo de protección subyacente y ofreciendo una defensa robusta contra ataques DoS [34].

Los mecanismos de seguridad implementados en VoIP pueden añadir una carga adicional al sistema si no se implementan correctamente. Estos mecanismos protegen contra intrusos no deseados, como ataques de denegación de servicio distribuido (DDoS), escuchas ilegales, vishing,

virus, malware, spam sobre IP (SPIT), ataques de intermediario y manipulación de llamadas. Los ataques DDoS pueden inundar la red VoIP utilizando métodos estándar de señalización para iniciar, suspender o transmitir llamadas. En un ataque de escucha, el atacante puede robar servicios ofrecidos a los usuarios, como credenciales de usuario para realizar llamadas, acceder a buzones de voz y escuchar conversaciones. Ang Cui y Stolfo demostraron en una conferencia que varios productos de telefonía IP son vulnerables a estos ataques [35].

El aprendizaje profundo es una subdisciplina del aprendizaje automático que imita el funcionamiento del cerebro humano a través de redes neuronales multicapa. Requiere grandes cantidades de datos para entrenar los parámetros de estas redes. Uno de los beneficios más significativos del aprendizaje profundo es su capacidad para aprender características automáticamente y extraer relaciones ocultas utilizando múltiples capas. Se han obtenido resultados sobresalientes en diversas aplicaciones como el reconocimiento de voz, síntesis de voz, traducción de idiomas, clasificación de imágenes y sistemas de detección de intrusos.

En este artículo [36], proponemos un enfoque de detección que convierte los tokens de cada mensaje SIP en un vector de características y alimenta estos vectores en un modelo de redes neuronales recurrentes (RNN) para detectar ataques DDoS. Utilizamos la incorporación de tokens para mejorar la precisión de la detección. Nuestro enfoque procesa los mensajes SIP individualmente, sin utilizar un tamaño de ventana fijo (por ejemplo, 50 mensajes), lo cual ralentiza la detección. Los tamaños de ventana, utilizados en enfoques anteriores como el discutido en, dependen de los ataques, lo que limita su capacidad para detectar diferentes tipos de ataques.

En esencia, VoIP permite la comunicación entre pares remotos, cada uno con un agente de usuario (UA), al convertir la voz de señales analógicas a digitales y transmitirla mediante un protocolo de medios adecuado. Una solución popular para gestionar llamadas es el Protocolo de Inicio de Sesión (SIP), que ofrece métodos similares a las operaciones de la telefonía tradicional (como el timbre) y parámetros para iniciar el flujo de medios. Para la transferencia de datos de voz, los UAs generalmente utilizan dos protocolos: RTP para transportar los datos de voz y RTCP para proporcionar información de sincronización. Ambos flujos se transmiten mediante UDP.

Para crear un canal encubierto, este artículo [3] aprovecha la optimización de la Detección de Actividad de Voz (VAD) disponible en muchos UAs. En resumen, VAD permite que el UA emisor detenga la transmisión durante las pausas del habla, lo que puede generar importantes ahorros de ancho de banda, ya que las conversaciones VoIP típicas incluyen entre un 35% y un 70% de silencio. La Figura 1 muestra los flujos RTP generados por el UA con y sin VAD.

Implementar una estrategia VAD eficiente puede ser desafiante, ya que no debe comprometer la calidad de la conversación causando distorsiones o retrasos adicionales. Interrumpir el flujo de

voz de manera agresiva puede recortar las muestras de voz y afectar la calidad, y la falta total de ruido puede confundir al hablante, haciendo pensar que la conversación ha terminado. En estos casos, el UA receptor debería generar ruido de confort sintético.

El método propuesto originalmente crea paquetes de silencio falsos cuando el VAD detiene la transmisión de datos RTP. El flujo resultante consiste en el tráfico VoIP y un canal encubierto incrustado en los paquetes de silencio falsos. En otras palabras, este método oculta información a terceros que supervisan la red, transformando una conversación VoIP con VAD en una sin VAD.

Además de asegurar la señalización y los medios de VoIP, es fundamental implementar medidas de seguridad en la capa IP o en la capa de red para proteger tanto la red de datos en la que opera el sistema VoIP como el tráfico VoIP mismo. Estudios han demostrado que la implementación de VoIP sobre túneles IPsec o redes privadas virtuales (VPN) protege tanto la red de datos como el sistema VoIP. Los túneles IPsec o las VPN son redes virtuales superpuestas sobre Internet que conectan dos redes privadas, como las redes internas de una organización, y protegen el tráfico mediante técnicas de cifrado y autenticación [37].

Para aprovechar al máximo los beneficios de VoIP, es importante mantener el rendimiento del sistema VoIP, incluso con la adición de medidas de seguridad. Investigaciones han estudiado el rendimiento de VoIP en entornos IPv4 e IPv6. Por ejemplo, Ahmed et al. analizan el efecto de la calidad de servicio (QoS) para VoIP sobre IPv4 e IPv6. Sin embargo, este estudio no aborda el rendimiento de un sistema VoIP cuando se añade seguridad. De manera similar, Rahangdale et al. discuten la seguridad SIP, pero no el rendimiento de un sistema VoIP con seguridad SIP implementada.

En la comunicación VoIP, es posible cifrar el tráfico de señalización, el tráfico de medios, o ambos. El protocolo de señalización negocia las capacidades entre los puntos finales de comunicación, incluyendo los códecs utilizados, los puertos de comunicación para la transferencia de voz y el uso de cifrado para el transporte de medios (voz). Por lo tanto, cuando el tráfico de señalización no está cifrado, una inspección profunda de los paquetes de señalización puede revelar si se emplea cifrado en el tráfico de medios. Los protocolos de señalización no necesitan compresión. Sin embargo, cuando los paquetes de señalización están cifrados o son propietarios, los parámetros de negociación de capacidad no se pueden recuperar del tráfico de señalización.

En esta sección, se lleva a cabo un estudio empírico donde se diseñan experimentos para examinar la aplicabilidad de las pruebas de aleatoriedad en sesiones de medios VoIP cifradas y no cifradas, especialmente para sesiones de medios VoIP comprimidas no cifradas. El objetivo es determinar si la prueba de aleatoriedad puede distinguir entre sesiones de medios VoIP cifradas y no cifradas pero comprimidas [25].

Medidas de Protección contra Ataques

Las medidas de mitigación de riesgos presentadas como medidas de protección son parte integral de la evaluación de riesgos, destinadas a salvaguardar sistemas y dispositivos en general. Por lo tanto, también investigamos cómo contrarrestar los ataques mencionados anteriormente. Comenzamos con las medidas existentes que podrían implementarse de inmediato.

Existen algunas medidas de seguridad relevantes que, como veremos, pueden ser efectivas hasta cierto punto, pero aún no se han generalizado. Es importante destacar que las medidas actuales no siempre pueden proteger completamente a los usuarios finales, como los empleados de una empresa, de nuestro modelo de amenazas. En particular, las llamadas VoIP no están completamente protegidas contra administradores de sistemas maliciosos, lo que indica la necesidad de desarrollar y prototipar nuevas y adicionales medidas de seguridad [38].

Soluciones y Métodos de Seguridad para VoIP

En los últimos años, los ataques DDoS contra VoIP han evolucionado, combinando múltiples tipos de ataques, lo que los hace aún más peligrosos y difíciles de combatir. Por lo tanto, es esencial adoptar una solución anti-DDoS para fortalecer la seguridad de las infraestructuras y aplicaciones de TI. Una de las tareas esenciales para el mantenimiento de estas infraestructuras es la monitorización continua del estado de la red, utilizando herramientas de análisis como tcpdump, caploader, y Wireshark. Estas herramientas son cruciales para extraer las huellas digitales que caracterizan las ofensivas, un paso fundamental en nuestra investigación antes de pasar a la detección. Wireshark, por ejemplo, captura paquetes y permite examinar su contenido detalladamente [39].

Para defenderse contra ataques informáticos, los cortafuegos ya no son suficientes. Los sistemas de detección de intrusos (IDS) son capaces de identificar amenazas que los cortafuegos pueden pasar por alto.

Sistema de Detección de Intrusos en Red Motor Suricata

En términos de seguridad, se aplican buenas prácticas: las funciones peligrosas están prohibidas, la programación defensiva es la norma y se realizan miles de pruebas para asegurar la robustez del sistema. Suricata es una herramienta versátil que puede configurarse para funcionar en cuatro modos diferentes:

- Modo Sniffer: Suricata captura los paquetes que transitan por la red y los presenta de manera continua en la pantalla.
- Modo Registrador de Paquetes: En este modo, Suricata registra el tráfico de red en directorios en el disco.

- Modo de Detección de Intrusos en la Red (NIDS): Suricata analiza el tráfico de la red, compara ese tráfico con reglas definidas por el usuario y establece acciones a realizar.
- Modo de Prevención de Intrusos en la Red (NIPS): Además de detectar, este modo permite a Suricata intervenir activamente para bloquear amenazas en tiempo real.

La implementación de estas prácticas y herramientas es esencial para asegurar una protección efectiva contra ataques DDoS y otras amenazas a las redes VoIP [40].

Mecanismo del Protocolo de Descubrimiento de Vecinos (NDP)

El Protocolo de Descubrimiento de Vecinos (NDP) permite a los nodos conectados a una red configurar automáticamente sus propias direcciones IP y puertas de enlace, así como comunicarse con nodos vecinos sin necesidad de autenticación o autorización dentro del sitio local. Sin embargo, esta falta de autenticación lo hace vulnerable a ataques, permitiendo que los atacantes se hagan pasar por cualquier nodo de la red y lancen diversos tipos de ataques.

Aunque la especificación original de NDP incluye el uso de IPsec para proteger sus mensajes, no proporciona directrices sobre cómo utilizar IPsec o intercambiar claves de forma automática, lo que lo hace poco práctico para la mayoría de los casos de uso [41].

Vulnerabilidades y Métodos de Protección en DHCP

El Protocolo de Configuración Dinámica de Host (DHCP) es una parte integral de la infraestructura de red, lo que lo convierte en un objetivo frecuente para diversas amenazas de seguridad. Es crucial comprender los tipos de ataques que pueden explotarlo y los métodos para detectarlos, eliminarlos o prevenirlos [42].

Vulnerabilidades del DHCP

DHCP Starvation: En este ataque, el atacante envía múltiples solicitudes de nuevas direcciones IP, sobrecargando al servidor DHCP. Como resultado, el servidor se queda sin direcciones IP para asignar a clientes legítimos, impidiendo su conexión a la red.

DHCP Flood: Este ataque implica inundar el servidor DHCP con un elevado número de solicitudes (ICMP, UDP, TCP, etc.) para agotar sus recursos, lo que puede provocar demoras en las respuestas o incluso una denegación de servicio (DoS).

Servidor DHCP Fraudulento: Aquí, un atacante instala un servidor DHCP malicioso en la red sin autorización. Este servidor puede asignar direcciones IP a dispositivos no autorizados y realizar ataques como suplantación de DNS o ataques de intermediario (man-in-the-middle).

Divulgación de Información Confidencial: Durante el intercambio de datos, se puede revelar información sensible como direcciones IP y nombres de host. Si un atacante accede a estos datos, puede comprometer la privacidad y la seguridad de la red.

Métodos de Protección contra Ataques DHCP

Habilitar DHCP Snooping: Configurar los conmutadores para verificar la legitimidad de las solicitudes y respuestas de DHCP en la red.

Limitar Solicitudes DHCP: Restringir la cantidad de solicitudes DHCP que un solo dispositivo puede enviar y configurar el servidor DHCP para asignar direcciones solo a clientes legítimos, utilizando filtrado de direcciones MAC.

Monitoreo de Red y Uso de Firewalls: Implementar sistemas de monitoreo de red para detectar actividades inusuales de los servidores DHCP y utilizar firewalls para controlar diferentes partes de la red.

Autenticación y Direcciones Estáticas: Utilizar autenticación para evitar conexiones de clientes no confiables y configurar direcciones IP estáticas para dispositivos importantes.

Actualizaciones y Parches de Seguridad: Realizar actualizaciones periódicas e instalar parches de seguridad para proteger contra vulnerabilidades conocidas.

Siguiendo estas recomendaciones, se puede minimizar la posibilidad de ataques al protocolo DHCP y crear una infraestructura de red más segura [43].

Contra medidas Comúnmente Utilizadas contra la Suplantación de Identidad en Llamadas

Lista Negra Administrada: Consiste en mantener una base de datos actualizada con números de teléfono conocidos por realizar llamadas fraudulentas o de suplantación de identidad. Las llamadas entrantes se comparan con esta lista para bloquear o identificar posibles llamadas no deseadas.

Declaración de Números de Origen (DNO): Es un mecanismo que permite a los proveedores de servicios de telecomunicaciones confirmar la autenticidad de un número de origen en una llamada telefónica. Esto ayuda a identificar y prevenir la suplantación de identidad al verificar la legitimidad del número desde el cual se efectúa la llamada.

Autenticación de Propiedad: Implica verificar la propiedad de un número de teléfono para garantizar la autenticidad de la llamada. Este método confirma que el número de teléfono utilizado realmente pertenece a la persona que realiza la llamada, ayudando a prevenir la suplantación de identidad.

Biometría de Voz: Utiliza características biométricas únicas de la voz de una persona para autenticar su identidad en una llamada telefónica. Al analizar patrones vocales específicos, se puede verificar la identidad del llamante y detectar intentos de suplantación de identidad.

Autenticación Móvil: Se refiere al uso de un teléfono móvil como un factor de autenticación adicional. La autenticación a través de un dispositivo móvil agrega una capa de seguridad al confirmar la posesión física del teléfono como parte del proceso de verificación de identidad.

Firma Digital: Implica el uso de claves criptográficas para autenticar llamadas telefónicas. Las técnicas de firma digital garantizan la integridad y autenticidad de la información de identificación de llamadas, ayudando a prevenir la suplantación de identidad y asegurando la confidencialidad de las comunicaciones [44].

Medidas para Prevenir la Suplantación de Identidad en Redes VoIP/SIP

Autenticación de Llamadas Basada en STIR/SHAKEN: Utiliza tokens de firma para verificar el número del llamante y prevenir la suplantación de identidad.

Uso de Blockchain: Crea un registro inmutable de llamadas, mejorando la seguridad y la trazabilidad de las mismas.

Listas Negras Administradas: Bloquean números conocidos por suplantación de identidad.

Verificación de Propiedad de Números: A través de la autenticación de propiedad, se asegura que el número de teléfono pertenece a quien realiza la llamada.

Biometría de Voz y Firma Digital: Autentican la identidad del llamante y garantizan la integridad de la información de identificación de llamadas.

Implementar estas contramedidas puede ayudar a crear una red más segura y proteger contra ataques de suplantación de identidad en llamadas telefónicas.

Medidas del Sistema ante la Detección de un Ataque de Suplantación de Identidad ARP

Cuando se detecta un ataque de suplantación de identidad ARP, el sistema aísla el dispositivo ofensivo para evitar que cause más daños a la red. Además, se emite una alerta para notificar a los administradores de la red sobre el incidente, permitiéndoles tomar acciones correctivas de inmediato. Estas medidas son esenciales para minimizar el impacto del ataque y asegurar la estabilidad y seguridad de la red [45].

Evaluación de Paquetes ARP en el Sistema Propuesto

Los paquetes ARP se evalúan mediante un algoritmo de detección de suplantación de identidad ARP. Este algoritmo analiza las solicitudes ARP entrantes y las compara con un caché conocido

de direcciones MAC e IP para identificar discrepancias. Se utiliza un modelo de red neuronal profunda (DNN) entrenado para reconocer patrones típicos de suplantación de identidad ARP, lo que permite un seguimiento en tiempo real de las direcciones MAC asociadas con cada dispositivo de la red. Al detectar un ataque, el sistema puede actuar de inmediato, ya sea aislando el dispositivo infractor o alertando a los administradores.

Beneficios de la Combinación de Aprendizaje Automático y Creación de Perfiles en la Detección de Ataques MitM

La combinación de aprendizaje automático y creación de perfiles proporciona una mayor precisión en la identificación de anomalías en el tráfico de red, mejorando la detección de ataques de suplantación de identidad ARP. El aprendizaje automático sirve como un guardián analítico del tráfico de red, mientras que la creación de perfiles de dispositivos genera descripciones detalladas que aumentan la capacidad de detección. Esta integración promete un enfoque eficaz para combatir ataques MitM basados en suplantación de identidad ARP, al combinar análisis avanzado con perfiles de comportamiento detallados [46].

1.4.1. Ámbito de aplicación

La investigación se circunscribe a la simulación y evaluación cuantitativa de la seguridad en redes VoIP, con un enfoque específico en un entorno simulado mediante herramientas como GNS3. La investigación abordará la identificación de amenazas y la eficacia de contramedidas propuestas en este entorno de simulación. Se utilizarán métricas cuantificables para evaluar el rendimiento del sistema en la detección y respuesta a amenazas en escenarios simulados de redes VoIP.

El alcance se limitará a situaciones simuladas, excluyendo la implementación en entornos de producción. Factores clave, como la precisión en la identificación de amenazas, la velocidad de respuesta del sistema y la eficacia general de las contramedidas, serán considerados. La investigación no abarcará la implementación práctica en redes VoIP reales, centrándose principalmente en la evaluación rigurosa y cuantitativa de la seguridad en un contexto simulado.

1.4.2. Establecimiento de requerimientos

En la Tabla 4, se detallan los requisitos esenciales para llevar a cabo la investigación y simulación en el ámbito de la seguridad de redes VoIP. Estos requisitos abarcan el uso de herramientas especializadas, la adquisición de conocimientos técnicos en redes VoIP y sus protocolos, así como la elaboración minuciosa de documentación que registre cada paso del proceso. El propósito fundamental de estos requisitos es reforzar la seguridad de las redes VoIP, abordando de manera integral las vulnerabilidades identificadas, implementando estrategias defensivas y validando la eficacia de las contramedidas establecidas [20].

Tabla 5: Requisitos de la investigación

Requisito	Descripción
Herramientas Especializadas	<ul style="list-style-type: none">• Identificación y adopción de herramientas especializadas para la simulación de redes VoIP, como GNS3 u otras plataformas similares.
Conocimientos Técnicos	<ul style="list-style-type: none">• Adquisición de conocimientos técnicos sólidos en redes VoIP y sus protocolos subyacentes.• Comprensión profunda de las vulnerabilidades potenciales en los protocolos VoIP y las amenazas de seguridad asociadas.
Simulación de Ambientes Controlados	<ul style="list-style-type: none">• Desarrollo de entornos de simulación controlados que reproduzcan con precisión las redes VoIP empresariales.• Integración de escenarios de prueba realistas para evaluar la efectividad de las contramedidas en situaciones simuladas.
Pruebas de Ataques	<ul style="list-style-type: none">• Realización de pruebas de ataques simulados para identificar y comprender las vulnerabilidades específicas presentes en las redes VoIP.• Evaluación del impacto de los posibles ataques, incluyendo ataques de denegación de servicio, interceptación de llamadas y manipulación de datos en tiempo real.
Contramedidas y Estrategias de Defensa	<ul style="list-style-type: none">• Implementación de contramedidas para mitigar los riesgos identificados durante las pruebas de simulación.• Desarrollo de estrategias de defensa para proteger las comunicaciones VoIP contra accesos no autorizados, manipulación de datos e intrusiones maliciosas.
Validación de Contramedidas	<ul style="list-style-type: none">• Validación sistemática de la efectividad de las contramedidas implementadas.• Establecimiento de procesos de monitoreo continuo para asegurar la persistencia de la seguridad en las redes VoIP.

CAPITULO II. DESARROLLO DEL PROTOTIPO

2.1 Definición del prototipo

La propuesta tecnológica se centra en la seguridad en redes VoIP, abordando la simulación, la evaluación de amenazas y la recomendación de contramedidas, con el objetivo de mejorar la seguridad en las comunicaciones sobre redes de voz IP. Esto incluye la identificación de ataques como el hombre en el medio (Man-in-the-Middle) y la denegación de servicio (DoS).

La Figura 5, ilustra la topología de una red de comunicación de voz sobre IP.

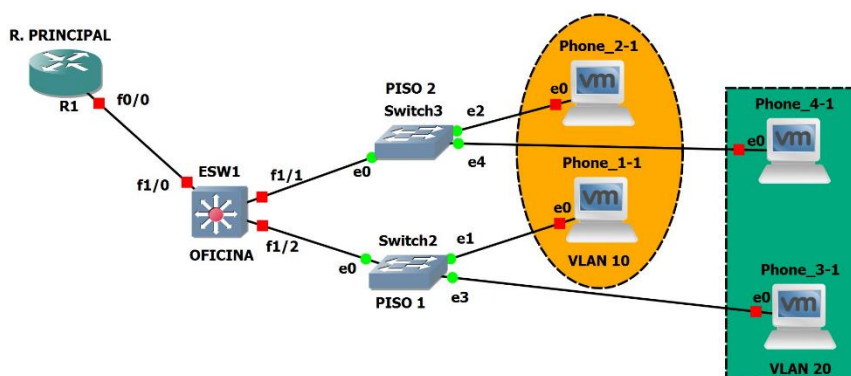


Figura 5: Topología de una red de comunicación de voz sobre ip

El funcionamiento de la topología se basa en una simulación de una red de una oficina de 2 pisos, la que se utiliza un router principal para subdividir la interfaz, en el switch de oficina se crea 2 vlan para poder conectarlas a cada uno de los pisos, en cada piso se va a crear los puertos en los cuales cada vlan va a ir cada teléfono. Gracias a esto podemos tener acceso entre todos los teléfonos independientemente del piso en que se encuentre y realizar llamadas.

2.2 Metodología de desarrollo del prototipo

2.2.1. Enfoque, alcance y diseño de investigación

La investigación se enfocará en la evaluación cuantitativa de la seguridad en redes VoIP mediante el uso de simulaciones detalladas y métricas precisas para evaluar el desempeño de las contramedidas propuestas. La metodología consistirá en identificar amenazas, simular ataques en un entorno VoIP con herramientas especializadas y medir la efectividad de las contramedidas específicas. Los resultados serán sometidos a análisis estadístico para confirmar su relevancia, proporcionando una evaluación exhaustiva de la capacidad del sistema para detectar y responder a amenazas en entornos simulados de redes VoIP.

El alcance de la investigación comprenderá la simulación y evaluación cuantitativa de la seguridad en redes VoIP, centrándose en un entorno específico de simulación, como GNS3. Se abordará la identificación de amenazas y la efectividad de las contramedidas propuestas en dicho entorno, utilizando métricas cuantificables para medir el rendimiento del sistema. El estudio se

limitará a escenarios simulados de redes VoIP, excluyendo la implementación en entornos de producción. Además, se considerarán factores como la precisión en la identificación de amenazas, la velocidad de respuesta del sistema y la eficacia general de las contramedidas. El alcance no abarcará la implementación práctica en redes VoIP reales, enfocándose principalmente en la evaluación rigurosa y cuantitativa de la seguridad en un contexto simulado.

2.2.2. Unidades de análisis

Las unidades de análisis en esta investigación se enfocarán en la evaluación del rendimiento de las contramedidas propuestas para la seguridad en redes VoIP. Se centrarán en la simulación de escenarios específicos mediante herramientas cuantitativas, como GNS3, para medir la eficacia de las contramedidas en la identificación precisa de amenazas cibernéticas dentro del entorno VoIP simulado. Se llevará a cabo una medición detallada de la capacidad del sistema propuesto para detectar y mitigar amenazas en entornos simulados de redes VoIP.

2.2.3. Técnicas e instrumentos de recopilación de datos

La Tabla 6 presenta las técnicas e instrumentos de recopilación de datos que se utilizaron para la realización de la investigación.

Tabla 6: Técnicas e instrumentos de recopilación de datos

Técnicas	
Simulaciones en GNS3	Descripción: Simulación de escenarios VoIP para evaluar contramedidas. Requisitos: Configuración detallada, ejecución de simulaciones.
Generación de Tráfico SIP	Descripción: Empleo de herramientas para generar tráfico SIP y simular sesiones de comunicación VoIP. Requisitos: Herramientas como SIPp para crear y enviar mensajes SIP
Análisis con Wireshark	Descripción: Examinar tráfico para identificar patrones anómalos. Requisitos: Captura y análisis de paquetes VoIP en simulaciones.
Registro de Eventos Personalizado	Descripción: Sistema para registrar eventos durante simulaciones. Requisitos: Desarrollo de un sistema de registro integrado

2.2.4. Técnicas de procesamiento de datos para la obtención de resultados

Para obtener resultados significativos, se emplearán diversas técnicas de procesamiento y análisis de datos en la evaluación de la seguridad en redes VoIP. Se utilizarán estadísticas descriptivas para resumir características clave de los datos, pruebas de significancia estadística para evaluar diferencias entre condiciones, y análisis de tendencias para identificar patrones mediante visualización de datos.

Se compararán métricas antes y después de la implementación de contramedidas para evaluar su eficacia, y se explorarán relaciones entre variables a través de análisis de correlación. Además, se aplicarán técnicas de agrupamiento para identificar patrones de comportamiento similar en conjuntos de datos.

2.2.5. Metodología o métodos específicos

La metodología PPDIIO es un enfoque utilizado en el ámbito de las redes de tecnología de la información, especialmente en la implementación y gestión de redes. PPDIIO es un acrónimo que representa las etapas principales de esta metodología: Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. A continuación, se presenta una breve descripción de cada una de estas etapas:

1. **Preparar (Prepare):** Durante esta etapa, se establecen los objetivos y requisitos para el proyecto de red.
2. **Planificar (Plan):** Durante esta etapa, se desarrolla un plan detallado para la implementación de la red.
3. **Diseñar (Design):** Aquí se crea el diseño técnico de la red basado en los requisitos y objetivos establecidos en las fases anteriores
4. **Implementar (Implement):** Durante esta etapa, se realiza la implementación física de la red de acuerdo con el diseño previamente planificado.
5. **Operar (Operate):** Después de la implementación, se inicia la operación diaria de la red.
6. **Optimizar (Optimize):** La etapa final consiste en la evaluación y mejora constante de la red para asegurar que se ajuste a las demandas cambiantes del negocio y a las nuevas tecnologías.

2.2.6. Herramientas y/o Materiales

La Tabla 7 proporciona los detalles sobre las herramientas que se emplearán en el desarrollo de este proyecto.

Tabla 7: Herramientas y/o materiales de la investigación

Categoría	Herramientas y/o material
Software	GNS3
	VMware
	Kali Linux
	Voip
	Routers
	Switchs
Hardware	Cables de conexionado
	Laptop con Windows 10 Computador de sobremesa con Windows 10

Describir cómo se ejecutó la metodología específica. Presentar la ejecución de cada fase y actividad de la metodología.

2.3 Desarrollo del prototipo

2.3.1 Definición

PPDIOO es un enfoque sistemático utilizado en la gestión y desarrollo de redes de tecnología de la información y comunicación (TIC). Esta metodología proporciona un marco estructurado para la implementación eficiente y la operación efectiva de infraestructuras de red, con un enfoque particular en la planificación y la seguridad.

2.3.2 Beneficios

La aplicación de la metodología PPDIOO en el desarrollo del prototipo para la tesis ofrece un enfoque ordenado, eficaz y de alta calidad para asegurar la red VoIP. Entre sus beneficios se encuentran la detección temprana de problemas, el incremento de la eficiencia y la simplificación de la gestión de cambios.

2.3.3 Fases

Para ejecutar la metodología PPDIOO en el desarrollo del prototipo de la tesis sobre redes VoIP, se siguieron las siguientes fases y actividades:

1. **Preparar (Prepare):** Se comenzó identificando los requisitos del proyecto y estableciendo los objetivos específicos. Esto incluyó investigar sobre el protocolo de VoIP y analizar las herramientas disponibles para configurar entornos de redes VoIP. Además, se preparó el entorno de simulación en GNS3, implementando la topología de red y configurando los dispositivos de red, como enrutadores y conmutadores, con comandos específicos para establecer VLAN y asignar direcciones IP.
2. **Planificar (Plan):** En esta fase, se elaboró un plan detallado para llevar a cabo la simulación de ataques de seguridad en la red VoIP. Esto incluyó la selección de los tipos de ataques a simular, como el Denegación de Servicio (DoS), la Escucha No Autorizada (Eavesdropping) y el Suplantación de ARP (ARP Spoofing).
3. **Diseñar (Design):** Se diseñó la topología de red VoIP en GNS3, definiendo las conexiones entre los dispositivos y estableciendo las configuraciones necesarias para la comunicación de voz sobre IP. Esto incluyó la configuración de VLAN, la asignación de direcciones IP y la configuración de los servicios de telefonía IP utilizando comandos específicos en los dispositivos de red.
4. **Implementar (Implement):** Se llevó a cabo la implementación de la topología de red VoIP diseñada en GNS3, configurando los dispositivos de red según las especificaciones

establecidas en la fase de diseño. Esto incluyó la configuración de enrutadores, conmutadores y teléfonos IP, configuración de los servicios de DHCP y de telefonía en los equipos de red.

5. **Operar (Operate):** Después de establecer la topología de red VoIP, se llevó a cabo la operación del entorno simulado para realizar pruebas controladas y evaluar la eficacia de las medidas de seguridad implementadas. Se monitoreó el funcionamiento de la red y se realizaron ajustes según fuera necesario para garantizar un rendimiento óptimo.
6. **Optimizar (Optimize):** Finalmente, se realizaron optimizaciones en la configuración de la red VoIP para mejorar su rendimiento y seguridad. Esto incluyó la revisión de las configuraciones existentes, la identificación y corrección de posibles problemas, y la implementación de mejoras recomendadas para fortalecer la seguridad de la red.

2.4 Metodología de desarrollo del prototipo

En el contexto de nuestra investigación sobre la seguridad de las redes VoIP, hemos diseñado una topología de red simulada utilizando la plataforma GNS3. Esta topología nos permite recrear escenarios realistas de redes VoIP y evaluar la efectividad de diversas medidas de seguridad. En este proceso, hemos configurado un router (R1) y un switch (ESW1) para establecer una infraestructura básica de red que simula un entorno de telefonía IP con múltiples VLANs. A continuación, detallaremos la configuración realizada en el router y el switch, así como su papel en la simulación de redes VoIP.

2.4.1 Configuración de interfaces en el router (R1):

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#exit
```

Explicación:

- Se activa la interfaz FastEthernet 0/0 con el comando **no shutdown**.
- Se crean subinterfaces FastEthernet 0/0.10 y FastEthernet 0/0.20 para las VLANs 10 y 20, respectivamente, utilizando el encapsulamiento dot1Q para etiquetar el tráfico VLAN.
- Se asignan direcciones IP a cada subinterfaz para las VLANs 10 y 20.

2.4.2 Configuración del servicio DHCP en el router (R1):

```
R1(config)#ip dhcp pool VLAN_A
R1(dhcp-config)#network 192.168.10.0 /24
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#option 150 ip 192.168.10.1
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.10.1
R1(config)#ip dhcp pool VLAN_B
R1(dhcp-config)#network 192.168.20.0 /24
R1(dhcp-config)#default-router 192.168.20.1
R1(dhcp-config)#option 150 ip 192.168.20.1
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.20.1
```

Explicación:

- Se configuran dos pools DHCP, uno para cada VLAN (VLAN_A y VLAN_B).
- Se especifican los rangos de direcciones IP para cada VLAN y se establece la puerta de enlace predeterminada.
- Se excluyen las direcciones IP de los routers de los rangos de direcciones DHCP para evitar conflictos.

2.4.3 Configuración del servicio de telefonía en el router (R1):

```
R1(config)#telephony-service
R1(config-telephony)#max-ephones 8
R1(config-telephony)#max-dn 8
R1(config-telephony)#ip source-address 192.168.10.1 port 2000
R1(config-telephony)#ip source-address 192.168.20.1 port 2000
R1(config-telephony)#create cnf-files
Creating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
R1(config-telephony)#exit
```

Explicación:

- Se configura la telefonía VoIP con este comando telephony-service.
- Se establece el número máximo de teléfonos (ephones) y números de directorio (ephone-dn) permitidos.
- Se especifica la dirección IP y el puerto para la señalización SIP de los teléfonos VoIP.
- Se crea el archivo de configuración CNF.

2.4.4 Configuración de teléfonos VoIP en el router (R1):

```
R1(config)#ephone-dn 1
R1(config-ephone-dn)#number 1001
R1(config-ephone-dn)#ephone-dn 2
R1(config-ephone-dn)#number 1002
R1(config-ephone-dn)#ephone-dn 3
R1(config-ephone-dn)#number 1003
R1(config-ephone-dn)#ephone-dn 4
R1(config-ephone-dn)#number 1004
R1(config-ephone-dn)#exit
R1(config)#ephone 1
R1(config-ephone)#mac-address 000C.2996.3880
R1(config-ephone)#button 1:1
R1(config-ephone)#type cIPC
R1(config-ephone)#ephone 2
R1(config-ephone)#mac-address 000C.29B5.8702
R1(config-ephone)#button 1:2
R1(config-ephone)#type cIPC
R1(config-ephone)#ephone 3
R1(config-ephone)#mac-address 000C.29DF.17B5
R1(config-ephone)#button 1:3
R1(config-ephone)#type cIPC
R1(config-ephone)#ephone 4
R1(config-ephone)#mac-address 000C.295C.A687
R1(config-ephone)#button 1:4
R1(config-ephone)#type cIPC
R1(config-ephone)#exit
```

Explicación:

- Se crean números de directorio (ephone-dn) para los teléfonos VoIP y se les asignan números de extensión.
- Se configuran los teléfonos VoIP (ephones) con direcciones MAC y se asignan a los números de directorio previamente configurados.

2.4.5 Configuración del switch (ESW1):

```
ESW1(config)#interface fastEthernet 1/0
ESW1(config-if)#switchport mode trunk
ESW1(config-subif)#exit
```



```
ESW1(config)#interface fastEthernet 1/1
ESW1(config-if)#switchport mode trunk
ESW1(config-subif)#exit
ESW1(config)#interface fastEthernet 1/2
ESW1(config-if)#switchport mode trunk
ESW1(config-subif)#exit
```

Explicación:

- Se configuran tres puertos del switch en modo trunk para permitir el paso de tráfico de múltiples VLANs.

2.4.6 Configuración de VLANs en el switch (ESW1):

```
ESW1(config)#vlan 10
ESW1(config-vlan)#name VLAN_10
ESW1(config-vlan)#vlan 20
ESW1(config-vlan)#name VLAN_20
ESW1(config-vlan)#exit
```

- Se crean dos VLANs en el switch, VLAN_10 y VLAN_20, y se les asignan nombres descriptivos.

2.4.7 Evidencias de funcionamiento

En esta sección, presentaremos imágenes que muestran el funcionamiento de la topología de red que hemos configurado para simular entornos de telefonía IP utilizando la plataforma GNS3. Estas imágenes proporcionarán una visión detallada de cómo interactúan los dispositivos en nuestra red simulada.

En la figura 6, se evidencia una llamada saliente del teléfono 3 hacia el teléfono 2 en la red VoIP simulada, mostrando la acción de origen.



Figura 6: Llamada desde el teléfono 3 hacia el teléfono 2

En la figura 7, se presenta la notificación de llamada entrante en el teléfono 2 proveniente del teléfono 3, ilustrando la acción de recepción.

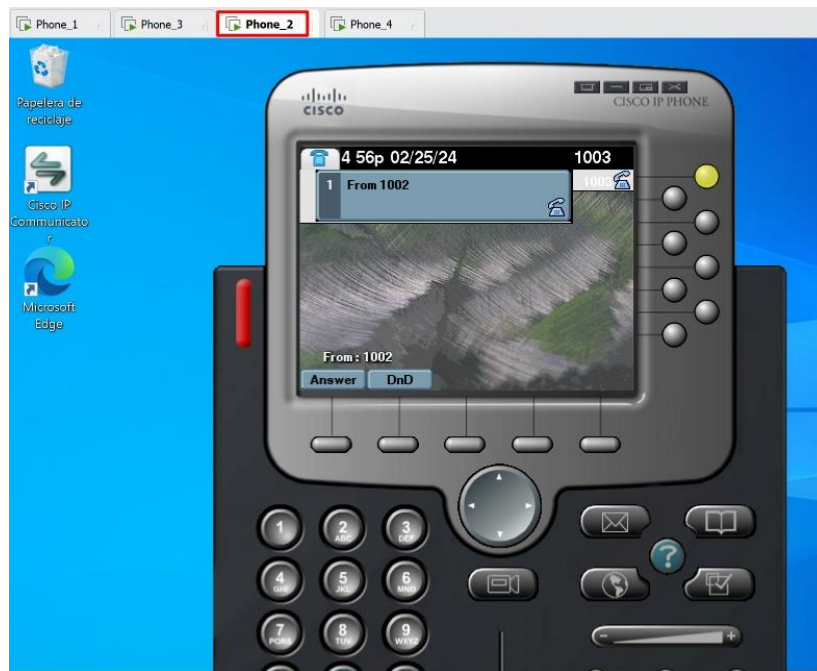


Figura 7: Recibe notificación de llamada desde el teléfono 3

En la figura 8, se confirma que la llamada ha sido atendida y se ha establecido una comunicación bidireccional entre ambos teléfonos, demostrando la acción de respuesta.



Figura 8: Contesta y existe comunicación entre los dos teléfonos

CAPITULO III. EVALUACIÓN DEL PROTOTIPO

3.1. Plan de evaluación

3.1.1. Objetivo

Evaluar la efectividad de las contramedidas implementadas para proteger una red VoIP contra ataques ARP spoofing, eavesdropping y DDoS mediante el uso del puerto espejo para capturar y analizar el tráfico de red.

3.1.2. Cronograma

Cronograma de las actividades que se han realizado en base a la semana 9 hasta la semana 14.

Tabla 8: Cronograma de actividades

Actividad	Responsable	Semana
Revisión de informe preliminar	Estudiante y Tutor	Semana 9
Validación del entorno simulado de redes de VoIP en gns3	Estudiante	Semana 10
Realización de ataques a redes de VoIP	Estudiante	Semana 11
Realización de contramedidas a los ataques	Estudiante	Semana 12
Pruebas de rendimiento en los dos entornos	Estudiante	Semana 12
Elaboración de recomendaciones y conclusiones en base a los resultados obtenidos	Estudiante	Semana 13
Revisión final y correcciones del informe	Estudiante y Tutor	Semana 13
Presentación de informe final y diapositivas	Estudiante y Tutor	Semana 14
Simulación de la defensa de la exposición	Estudiante y tutor	Semana 14

3.1.3. Recopilación de información

Para evaluar la eficacia de los controles implementados para la protección de la privacidad en redes LAN con VoIP, es crucial establecer criterios claros y específicos que reflejen tanto los ataques como los controles descritos en el documento. La Tabla 9 detalla los criterios de

evaluación basados en los ataques (Eavesdropping, DDoS y ARP Spoofing) y los controles implementados (DHCP Snooping, Port-Security, ACL, y Port-Mirror).

3.1.4. Establecer criterios de evaluación

En la siguiente tabla se detalla los criterios que tiene cada control y como van a ser evaluados según la métrica cuantitativa.

Tabla 9: Criterios y métricas de evaluación

Ataque	Control Implementado	Criterio de Evaluación	Modo de cálculo de la métrica
ARP Spoofing	Port-Security	Capacidad de bloquear direcciones MAC no autorizadas	Número de intentos de conexión no autorizados bloqueados / Número total de intentos x 100
	DHCP Snooping	Efectividad en prevenir cambios en la tabla ARP	Número de cambios en la tabla ARP después de activar el control / Número total de cambios x 100
DDoS	ACL	Eficacia en bloquear el tráfico de ataque	Número de paquetes de ataque bloqueados / Número total de paquetes de ataque x 100.
		Reducción de la saturación del ancho de banda	Uso de ancho de banda después de activar el control / Uso de ancho de banda antes de activar el control x 100
Eavesdropping	Port-Mirror	Capacidad de monitorear tráfico sospechoso	Número de actividades sospechosas detectadas / Número total de actividades x 100
		Eficiencia en la captura y análisis de tráfico	Número de paquetes analizados correctamente / Número total de paquetes capturados x 100

3.2. Resultados de la evaluación

En la siguiente Tabla, se va a especificar como se ha evaluado los resultados con una métrica cuantitativa basándonos en el ataque que se ha usado, el control que se implementó.

Ataque	Control Implementado	Criterio de Evaluación	Método de Evaluación	Métrica Cuantitativa
--------	----------------------	------------------------	----------------------	----------------------

ARP Spoofing	Port-Security	Capacidad de bloquear direcciones MAC no autorizadas	Comprobar si las direcciones MAC no autorizadas son bloqueadas por el switch	45 bloqueados / 50 intentos = 90%
	DHCP Snooping	Efectividad en prevenir cambios en la tabla ARP	Verificar si hay cambios en la tabla ARP después de activar el control	1 cambio después / 20 cambios totales = 5%
DDoS	ACL	Eficacia en bloquear el tráfico de ataque	Comprobar si el tráfico malicioso es bloqueado por las ACL	980 paquetes bloqueados / 1000 paquetes de ataque = 98%
		Reducción de la saturación del ancho de banda	Medir el uso del ancho de banda antes y después de activar las ACL	500 Mbps después / 1000 Mbps antes = 50%
Eavesdropping	Port-Mirror	Capacidad de monitorear tráfico sospechoso	Revisar los registros de tráfico monitoreado para identificar actividades sospechosas	15 actividades sospechosas detectadas / 20 actividades totales = 75%
		Eficiencia en la captura y análisis de tráfico	Evaluar la cantidad de tráfico capturado y analizado correctamente	850 paquetes analizados correctamente / 1000 paquetes capturados = 85%

3.2.1. Evaluación de la Hipótesis

Recopilación de Datos Cuantitativos

Se recolectaron datos cuantitativos sobre la eficacia de los controles implementados: Port-Security, ACL, y Port-Mirror, en términos de su capacidad para bloquear ataques, prevenir cambios no autorizados, y monitorear tráfico sospechoso.

Análisis de resultados cuantitativos

1. Ataque - ARP Spoofing

a. Control - Port-Security

- **Capacidad de bloquear direcciones MAC no autorizadas:** 90% de intentos de conexión no autorizados fueron bloqueados.

b. Control – DHCP Snooping

- **Efectividad en prevenir cambios en la tabla ARP:** 95% de efectividad en prevenir cambios en la tabla ARP después de la implementación del control.

2. Ataque - DDoS

a. Control - ACL (Access Control Lists)

- **Eficacia en bloquear el tráfico de ataque:** 98% de paquetes de ataque fueron bloqueados.
- **Reducción de la saturación del ancho de banda:** Reducción del 50% en el uso del ancho de banda después de activar las ACL.

3. Ataque - Eavesdropping

a. Control - Port-Mirror

- **Capacidad de monitorear tráfico sospechoso:** 75% de actividades sospechosas fueron detectadas.
- **Eficiencia en la captura y análisis de tráfico:** 85% de los paquetes capturados fueron analizados correctamente.

3.2.2. Conclusión de los resultados

Cumplimiento de la Hipótesis:

Los datos indican que la implementación de los controles evaluados (Port-Security, DHCP Snooping, ACL, y Port-Mirror) es altamente efectiva en proteger la red LAN que utiliza VoIP contra los ataques comunes evaluados (ARP Spoofing, DDoS y Eavesdropping). La alta efectividad en la prevención y detección de estos ataques sugiere que estos controles ayudan a garantizar la privacidad de las comunicaciones en la infraestructura LAN con VoIP.

Decisión Final:

Dado que los controles implementados han demostrado ser eficaces en un alto porcentaje de los casos, podemos concluir que la hipótesis "La implementación de controles en las infraestructuras de LAN que utilizan VoIP garantizará la privacidad de las comunicaciones" se cumple. La efectividad medida en términos de bloqueo de ataques y monitoreo de tráfico sospechoso respalda esta conclusión.

4. CONCLUSIONES

La implementación de medidas de seguridad en infraestructuras LAN con VoIP ha demostrado ser esencial para asegurar la confidencialidad y privacidad de las comunicaciones. La simulación de ataques ha permitido identificar y mitigar vulnerabilidades de manera efectiva, garantizando una protección robusta en estos entornos.

1. La investigación detallada sobre el protocolo VoIP reveló múltiples vulnerabilidades que pueden ser explotadas por atacantes. Esta comprensión profunda ha sido fundamental para guiar las medidas e implementar los controles de seguridad.
2. El análisis de herramientas como GNS3, VMware y Kali Linux permitió la selección de las más adecuadas para simular entornos de red realistas. Estas herramientas fueron efectivas para replicar ataques y evaluar controles de seguridad.
3. La implementación de entornos simulados de VoIP y la realización de pruebas controladas permitieron evaluar con precisión la efectividad de diversos controles de seguridad, evidenciando su capacidad para mitigar ataques específicos.
4. Las pruebas en el entorno simulado revelaron varias vulnerabilidades críticas en las infraestructuras LAN con VoIP. Estas pruebas permitieron el desarrollo de estrategias de mitigación efectivas para cada vulnerabilidad identificada.
5. La revisión minuciosa de los controles implementados evidenció una gran efectividad en resguardar la privacidad de las comunicaciones VoIP. Los controles como Port-Security, ACL y Port-Mirror demostraron ser particularmente efectivos para prevenir y detectar actividades maliciosas.
6. La hipótesis inicial: la implementación de controles en las infraestructuras LAN que utilizan VoIP garantizará la privacidad de las comunicaciones se confirma. Los controles implementados no solo previenen cambios no autorizados y bloquean el tráfico de ataque, sino que también permiten una vigilancia efectiva del tráfico de red, asegurando así la privacidad y seguridad de las comunicaciones VoIP.

5. RECOMENDACIONES

A futuro, se recomienda mantener un enfoque proactivo y adaptativo en la seguridad de las infraestructuras LAN que emplean VoIP. Este enfoque debe incluir un programa continuo de monitoreo y evaluación de los controles de seguridad implementados para asegurar su efectividad frente a nuevas amenazas y vulnerabilidades emergentes.

1. Establecer un programa continuo de monitoreo y evaluación de los controles de seguridad implementados (Port-Security, DHCP Snooping, ACL y Port-Mirror) para asegurar su efectividad continua frente a nuevas amenazas y vulnerabilidades emergentes. El

monitoreo constante permite detectar nuevas amenazas y ajustar los controles de seguridad para mantener la protección óptima de las comunicaciones VoIP.

2. Extender la investigación a nuevas vulnerabilidades y protocolos de seguridad alternativos, asegurando una actualización continua del conocimiento en el área de la seguridad VoIP. La evolución de las tecnologías y métodos de ataque requiere una comprensión actualizada y profunda para diseñar contramedidas efectivas.
3. Evaluar y adoptar nuevas herramientas de simulación y análisis que ofrezcan mejores capacidades para detectar y mitigar amenazas en redes VoIP. Herramientas avanzadas pueden ofrecer funcionalidades mejoradas y mayor precisión en la simulación y detección de vulnerabilidades.
4. Desarrollar un protocolo estándar para la implementación de entornos simulados que incluya una variedad de escenarios de ataque y pruebas periódicas de efectividad. Protocolos estándar garantizan la consistencia y repetibilidad de las pruebas, facilitando la evaluación continua de los controles de seguridad.
5. Ampliar las pruebas exhaustivas a diferentes configuraciones y arquitecturas de red para identificar una gama más amplia de posibles vulnerabilidades. La diversidad en las pruebas asegura una cobertura más completa y una mayor robustez en la identificación de vulnerabilidades.
6. Realizar auditorías regulares y análisis detallados de la funcionalidad y adaptabilidad de los controles de seguridad para asegurar su eficacia a largo plazo.
7. Con el fin de proteger la privacidad de las comunicaciones en infraestructuras LAN que utilizan VoIP, es crucial implementar un proceso de actualización continua de los controles de seguridad basados en auditorías y nuevas amenazas detectadas.

6. REFERENCIAS BIBLIOGRÁFICAS

- [1] «Historia de la telefonía IP timeline.», Timetoast timelines. Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://www.timetoast.com/timelines/historia-de-la-telefonía-ip>
- [2] F. Matango, «Seguridad de las Redes Voip». Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <http://www.servervoip.com/blog/seguridad-de-las-redes-voip/>
- [3] J. Saenger, W. Mazurczyk, J. Keller, y L. Caviglione, «VoIP network covert channels to enhance privacy and information sharing». doi: 10.1016/j.future.2020.04.032.
- [4] N. Mohamudally y S. Armoogum, «Closest adjacent neighbour: A novel deep learning intruder detection technique in VoIP networks». doi: 10.1145/3415088.3415129.
- [5] J. Singh, «La historia de VOIP», IDT Express. [En línea]. Disponible en: <https://www.idtexpress.com/es/blog/history-voip-voice-termination/>
- [6] «Complete Guide to VoIP Security, Encryption & Vulnerabilities». Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://getvoip.com/blog/voip-security/>
- [7] F. Matango, «Las vulnerabilidades de VoIP». Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <http://www.servervoip.com/blog/las-vulnerabilidades-de-voip/>
- [8] «¿Cómo puede proteger los protocolos VoIP de los ataques cibernéticos?» Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://www.linkedin.com/advice/1/how-can-you-secure-voip-protocols-from>
- [9] AbdullahBell, «Tutorial: Pruebas de simulación de Azure DDoS Protection». Accedido: 24 de mayo de 2024. [En línea]. Disponible en: <https://learn.microsoft.com/es-es/azure/ddos-protection/test-through-simulations>
- [10] J. Singh, «Mejores prácticas de seguridad de VoIP», IDT Express. Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://www.idtexpress.com/es/blog/voip-security-best-practice/>
- [11] F. Matango, «Contramedidas VoIP». Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <http://www.servervoip.com/blog/contramedida-voip/>
- [12] «Guía para la seguridad y el cifrado de VoIP | Ciberseguridad». Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://ciberseguridad.com/guias/recursos/seguridad-cifrado-voip/>
- [13] «Prevenir ataques de red». Accedido: 24 de mayo de 2024. [En línea]. Disponible en: <https://www.paessler.com/es/network-attacks>
- [14] Grandstream, «Criptográfico ¿Qué? Métodos de cifrado VoIP», Sertecomsa.com. Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://www.sertecomsa.com/post/2018/01/31/criptografico-que-metodos-de-cifrado-voip>
- [15] «¿Qué es la voz sobre protocolo de internet (VoIP)?», Cloudflare. Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://www.cloudflare.com/es-es/learning/video/what-is-voip/>
- [16] rrioboo, «¿Qué es el protocolo TLS y para qué se utiliza en VoIP?», SSD Blog. Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://blog.ssd.com.py/que-es-el-protocolo-tls-y-para-que-se-utiliza-en-voip/>
- [17] «Seguridad en la tecnología VoIP | Satydal». Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://satydal.es/la-seguridad-en-la-tecnología-voip/>

- [18] «IA en VoIP. Beneficios y Ejemplos para tu Empresa», VoIPstudio. Accedido: 23 de diciembre de 2023. [En línea]. Disponible en: <https://voipstudio.es/blog/inteligencia-artificial-en-voip/>
- [19] Y. Jiang y S. Tang, «An efficient and secure VoIP communication system with chaotic mapping and message digest», *Multimedia Systems*, vol. 24, n.º 3, pp. 355-363, jun. 2018, doi: 10.1007/s00530-017-0565-6.
- [20] D. Alvanos, K. Limniotis, y S. Stavrou, «On the Cryptographic Features of a VoIP Service», *Cryptography*, vol. 2, n.º 1, p. 3, ene. 2018, doi: 10.3390/cryptography2010003.
- [21] W.-B. Hsieh y J.-S. Leu, «Implementing a secure VoIP communication over SIP-based networks», *Wireless Netw*, vol. 24, n.º 8, pp. 2915-2926, nov. 2018, doi: 10.1007/s11276-017-1512-3.
- [22] E. Ramadhan, A. Firdausi, y S. Budiyo, «Design and analysis QoS VoIP using routing Border Gateway Protocol (BGP)», *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP)*, pp. 1-4, nov. 2017, doi: 10.1109/BCWSP.2017.8272556.
- [23] S. Deepikaa y R. Saravanan, «VoIP Steganography Methods, a Survey», *Cybernetics and Information Technologies*, vol. 19, n.º 1, pp. 73-87, mar. 2019, doi: 10.2478/cait-2019-0004.
- [24] G. Zhang y S. Fischer-Hübner, «A survey on anonymous voice over IP communication: attacks and defenses», *Electron Commer Res*, vol. 19, n.º 3, pp. 655-687, sep. 2019, doi: 10.1007/s10660-019-09369-0.
- [25] P. Choudhury, K. R. P. Kumar, S. Nandi, y G. Athithan, «An empirical approach towards characterization of encrypted and unencrypted VoIP traffic», *Multimed Tools Appl*, vol. 79, n.º 1-2, pp. 603-631, ene. 2020, doi: 10.1007/s11042-019-08088-w.
- [26] N. K. EL-Ashri, E. F. Badran, A. I. Zaki, y W. K. Badawi, «Admission control mechanism for quality of service and security in H.323 voice gateway», *Concurrency and Computation*, vol. 33, n.º 20, p. e6376, oct. 2021, doi: 10.1002/cpe.6376.
- [27] D. Suthar y P. H. Rughani, «A Comprehensive Study of VoIP Security», *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 812-817, dic. 2020, doi: 10.1109/ICACCCN51052.2020.9362943.
- [28] M. Kolhar, A. Alameen, y M. Gulam, «Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats», *Neural Comput & Applic*, vol. 30, n.º 9, pp. 2873-2881, nov. 2018, doi: 10.1007/s00521-017-2886-y.
- [29] H. Nasser y M. Hussain, «An Effective Approach to Detect and Prevent ARP Spoofing Attacks on WLAN», *IJEEE*, vol. 19, n.º 2, pp. 8-17, dic. 2023, doi: 10.37917/ijeee.19.2.2.
- [30] J. Carrillo-Mondejar, J. L. Martínez, y G. Suarez-Tangil, «On how VoIP attacks foster the malicious call ecosystem», *Computers & Security*, vol. 119, n.º 102758, pp. 267-281, 2022, doi: 10.1016/j.cose.2022.102758.
- [31] A. H. A. Omari, Yazan A. Alsariera, H. S. Alhadawi, M. A. Albawaleez, y S. S. Alkhliwi, «A Closer Look on Challenges and Security Risks of Voice Over Internet Protocol Infrastructures», *International Journal of Computer Science and Network Security*, vol. 22, n.º 1, pp. 175-184, feb. 2022, doi: 10.22937/IJCSNS.2022.22.2.23.

- [32] B. Bayas, E. Mera, G. Calero, y S. Patiño, «Implementación de una red definida por software que permita brindar servicio de VoIP Seguros», vol. 13, pp. 389-396, abr. 2021.
- [33] A. Montazerolghaem, «Softwarization and virtualization of VoIP networks», *The Journal of Supercomputing*, vol. 78, ago. 2022, doi: 10.1007/s11227-022-04448-w.
- [34] J. Kafke y T. Viana, «Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems», *Network*, vol. 2, n.º 4, Art. n.º 4, dic. 2022, doi: 10.3390/network2040032.
- [35] L. Behan, J. Rozhon, J. Safarik, F. Rezac, y M. Voznak, «Efficient Detection of Spam Over Internet Telephony by Machine Learning Algorithms», *IEEE Access*, vol. 10, pp. 133412-133426, 2022, doi: 10.1109/ACCESS.2022.3231384.
- [36] W. Nazih, Y. Hifny, W. S. Elkilani, H. Dhahri, y T. Abdelkader, «Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks», *Sensors*, vol. 20, n.º 20, Art. n.º 20, ene. 2020, doi: 10.3390/s20205875.
- [37] L. P. Moiz Hussain, Praniti Gupta, Shirin Bano, Vineet Kulkarni Rahil Gandotra, Dewang Gedia, «VoIP Security: A Performance and Cost-benefit Analysis», *ITII*, vol. 8, n.º 2, ene. 2021, doi: 10.17762/itii.v8i2.80.
- [38] G. Bella, P. Biondi, y S. Bognanni, «Multi-service Threats: Attacking and Protecting Network Printers and VoIP Phones alike», *Internet of Things*, vol. 18, p. 100507, may 2022, doi: 10.1016/j.iot.2022.100507.
- [39] W. Amalou y M. Mehdi, «An Approach to Mitigate DDoS Attacks on SIP Based VoIP», *Engineering Proceedings*, vol. 14, n.º 1, Art. n.º 1, 2022, doi: 10.3390/engproc2022014006.
- [40] W. Nazih, K. Alnowaiser, E. Eldesouky, y O. Youssef Atallah, «Detecting SPIT Attacks in VoIP Networks Using Convolutional Autoencoders: A Deep Learning Approach», *Applied Sciences*, vol. 13, n.º 12, Art. n.º 12, ene. 2023, doi: 10.3390/app13126974.
- [41] F. Najjar, Q. Bsoul, y H. Al-Refai, «An Analysis of Neighbor Discovery Protocol Attacks», *Computers*, vol. 12, n.º 6, Art. n.º 6, jun. 2023, doi: 10.3390/computers12060125.
- [42] T. Vakaliuk, Y. Trokoz, O. Pokotylo, V. Osadchyi, y S. Smirnov, «Modeling Attacks on the DHCP Protocol in the GNS3 Environment and Determining Methods of Security Against Them».
- [43] I. Nedyalkov, «Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center», *Computers*, vol. 12, n.º 5, Art. n.º 5, may 2023, doi: 10.3390/computers12050101.
- [44] I. M. Tas y S. Baktir, «Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks», *IEEE Access*, vol. 12, pp. 60123-60137, 2024, doi: 10.1109/ACCESS.2024.3393487.
- [45] V. Hnamte y J. Hussain, «Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation», *Telematics and Informatics Reports*, vol. 14, p. 100129, jun. 2024, doi: 10.1016/j.teler.2024.100129.
- [46] I. Nedyalkov, «Benefits of Using Network Modeling Platforms When Studying IP Networks and Traffic Characterization», *Computers*, vol. 12, n.º 2, Art. n.º 2, feb. 2023, doi: 10.3390/computers12020041.

7. ANEXOS

- Proceso de creación de Topología de redes VoIP

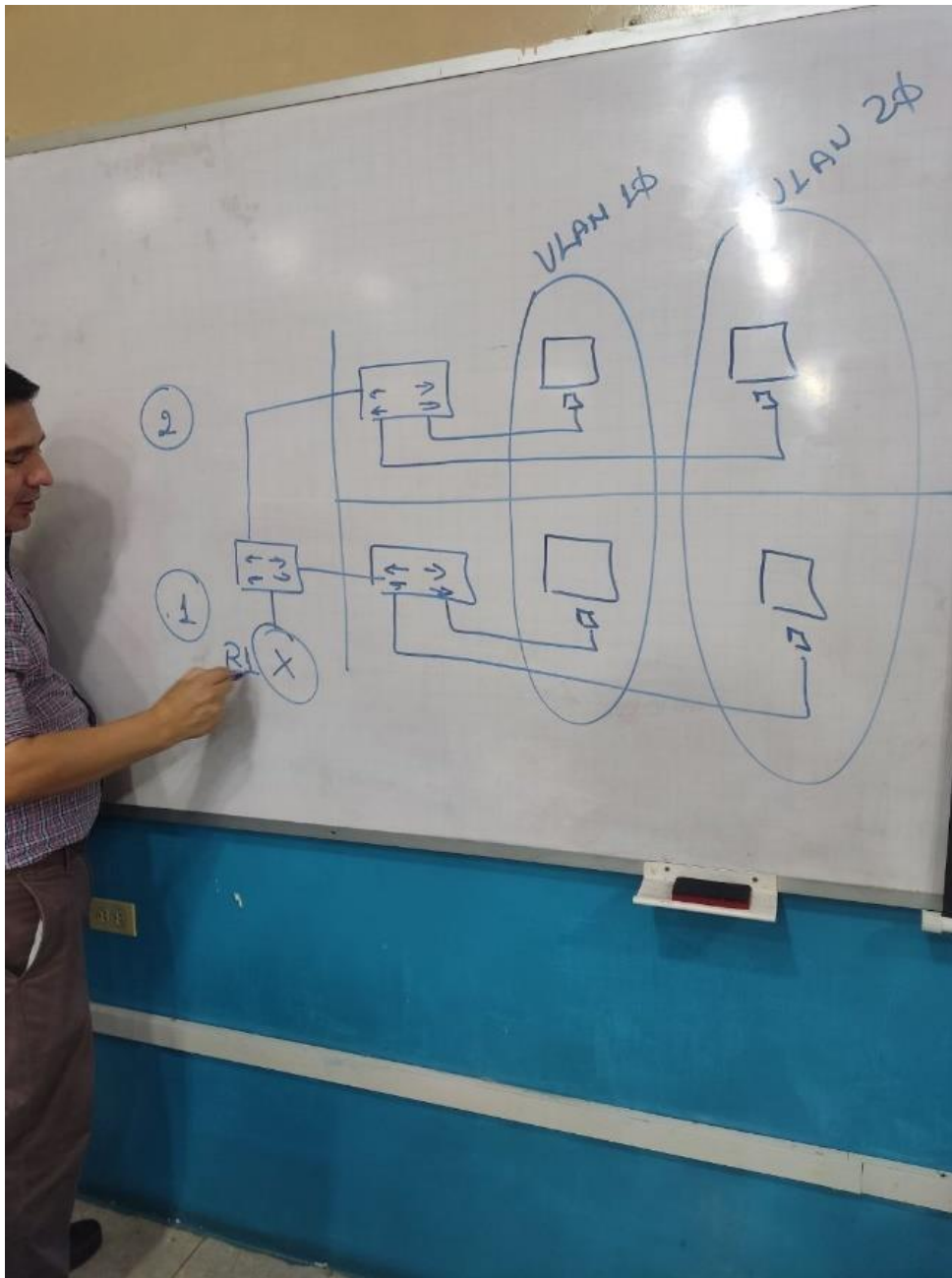


Figura 9: Revisión de Topología del proyecto



Figura 10: Revisión de Topología y modificación de módulos del proyecto

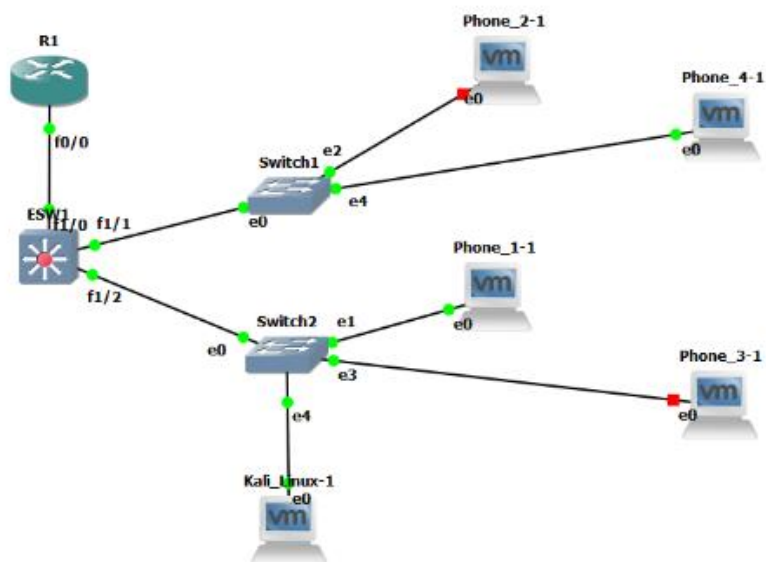


Figura 11: Topología completa que incluye la máquina

- Ataques
 - Ataque 1 – Ataque de Eavesdropping



Figura 12: Llamada en teléfono 1



Figura 13: Llamada en teléfono 2

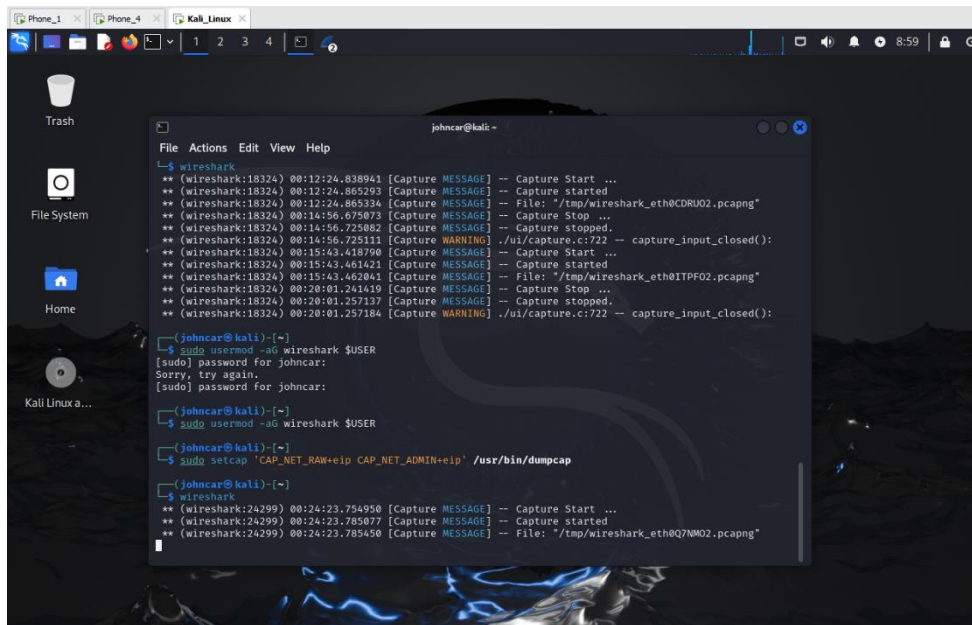


Figura 14: Inicio de Wireshark en Kali Linux para hacer el ataque Eavesdropping

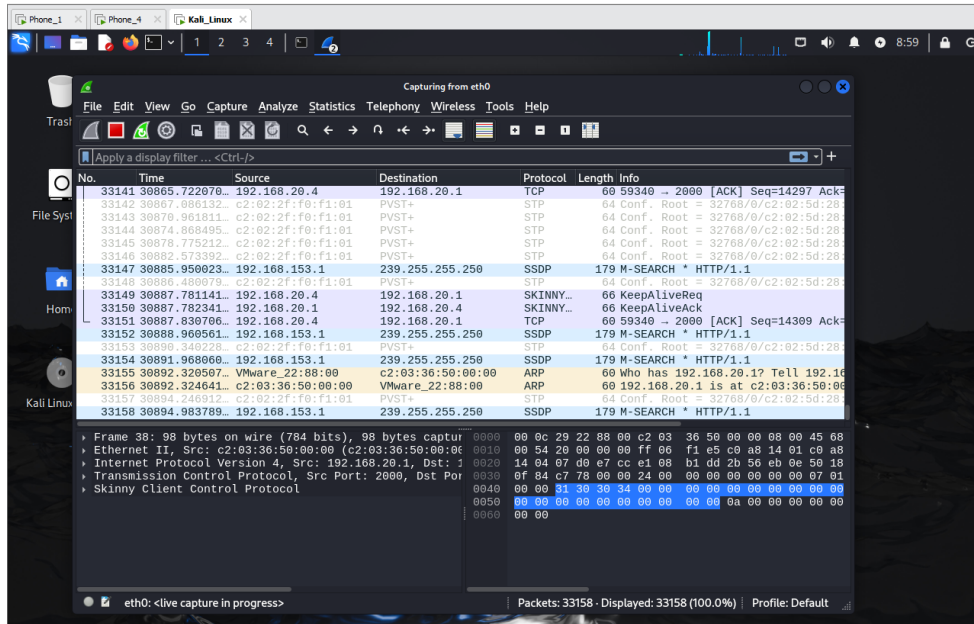


Figura 15: Obtención de información de la máquina atacada (teléfono 1)

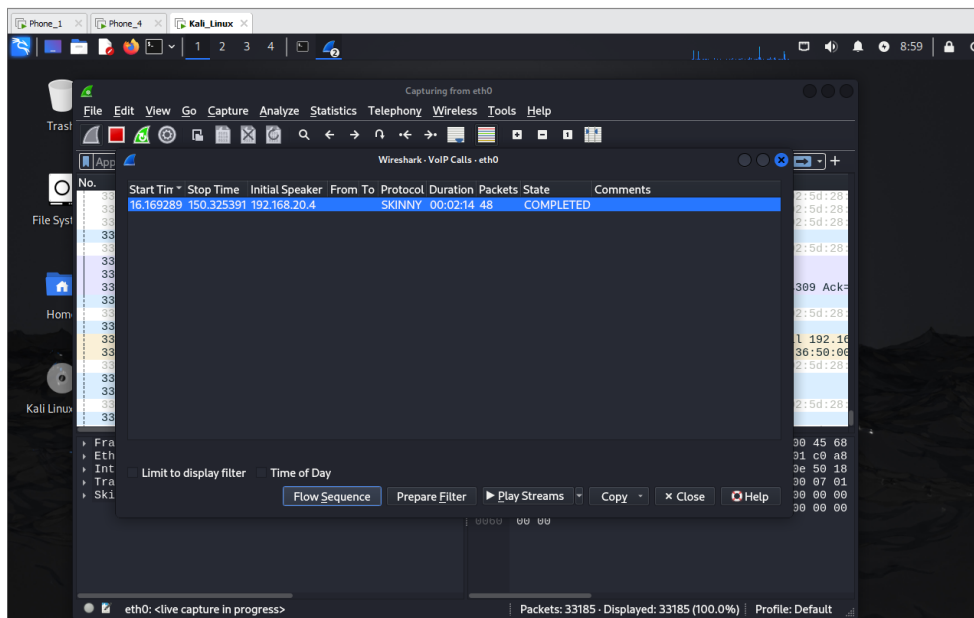


Figura 16: Llamada capturada del teléfono 1

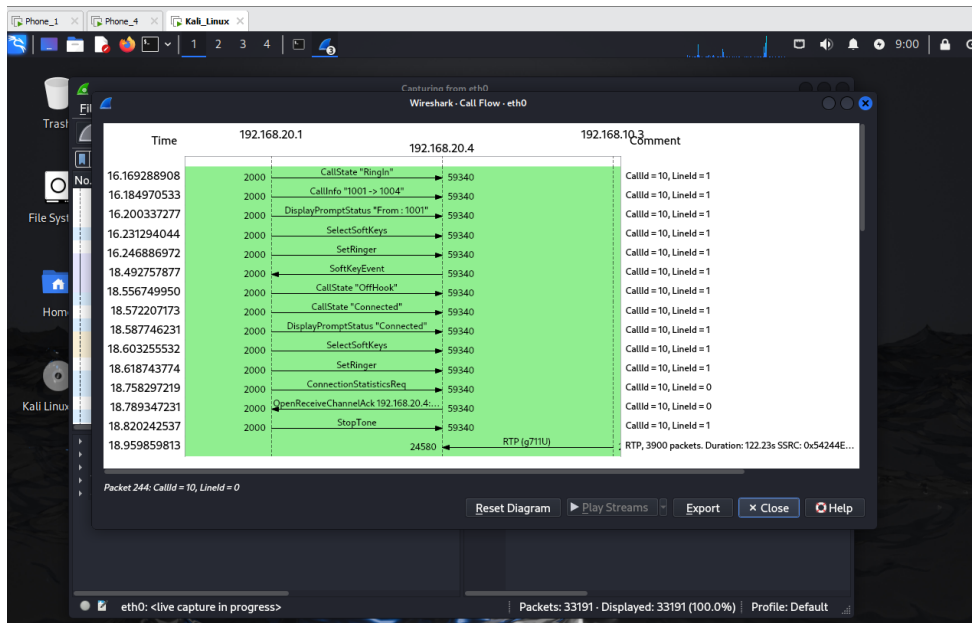


Figura 17: Sesión de llamada SIP entre los 2 teléfonos.

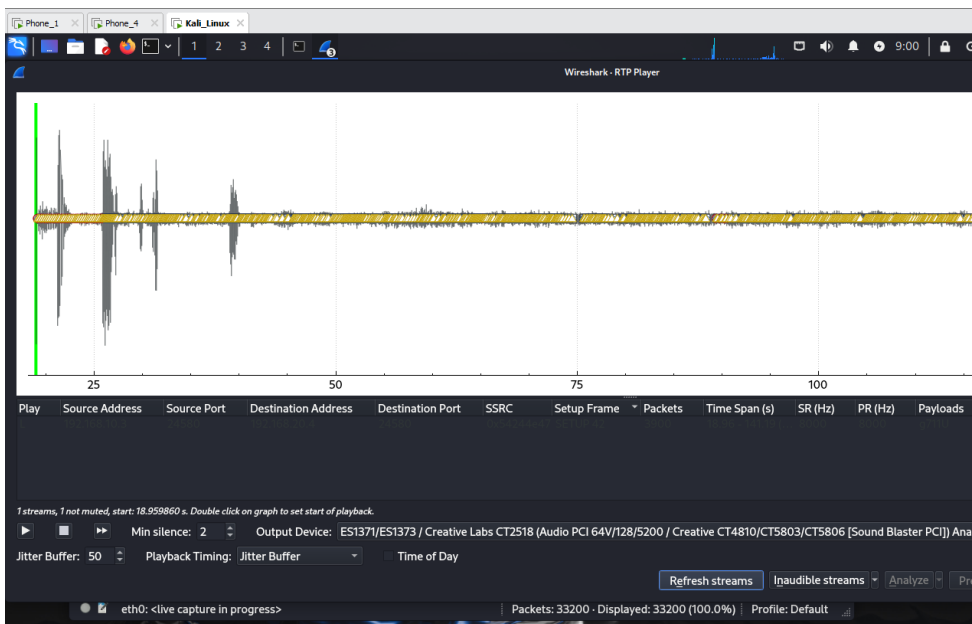


Figura 18: Visualización de la captura de llamada (teléfono 1)

o Ataque 2 - ataque DDoS

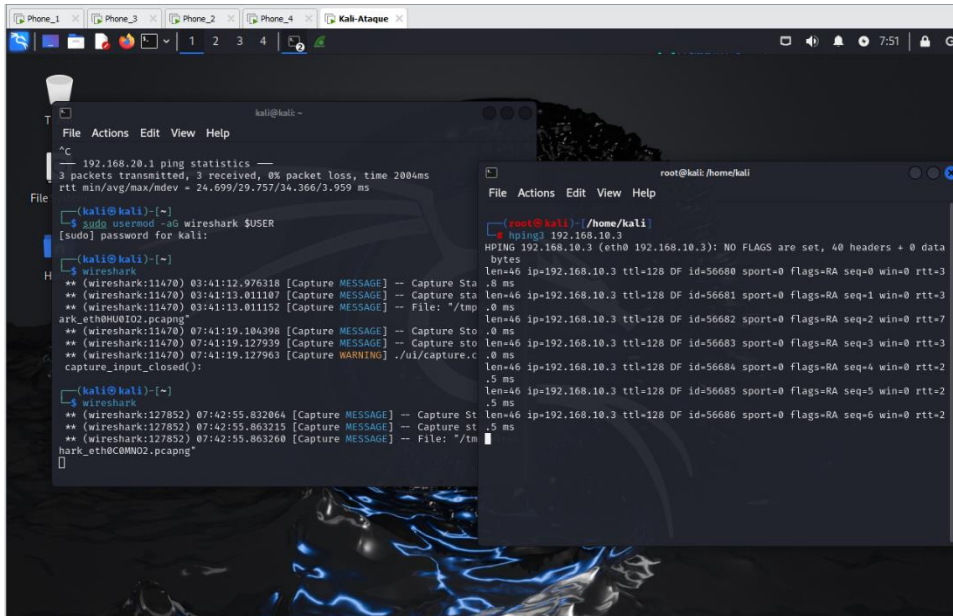


Figura 19: Se envían mensajes de Linux a la máquina atacada (teléfono 1) para realizar el ataque DoS

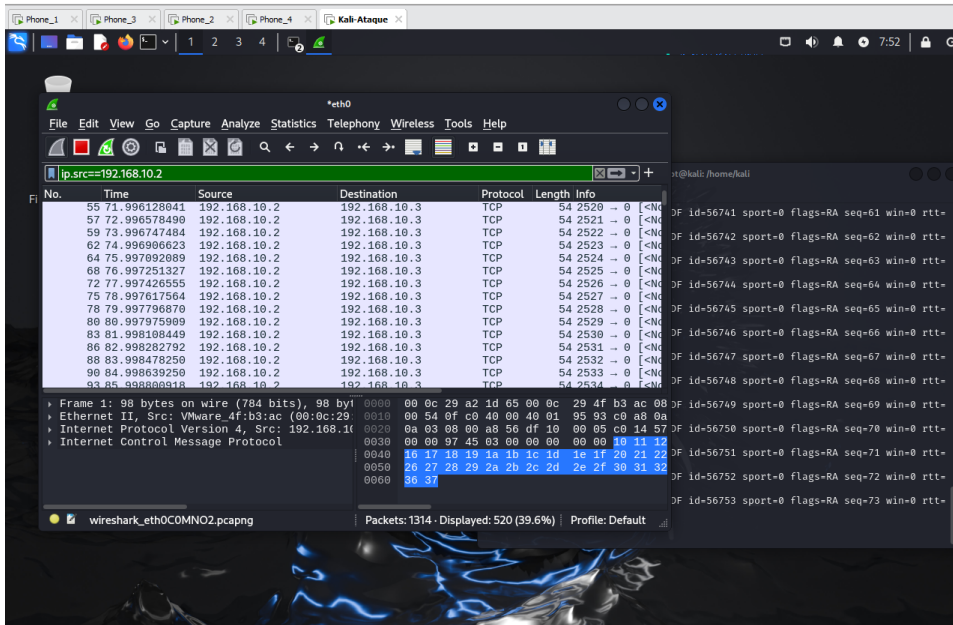


Figura 20: Filtro para visualizar mensajes de Linux

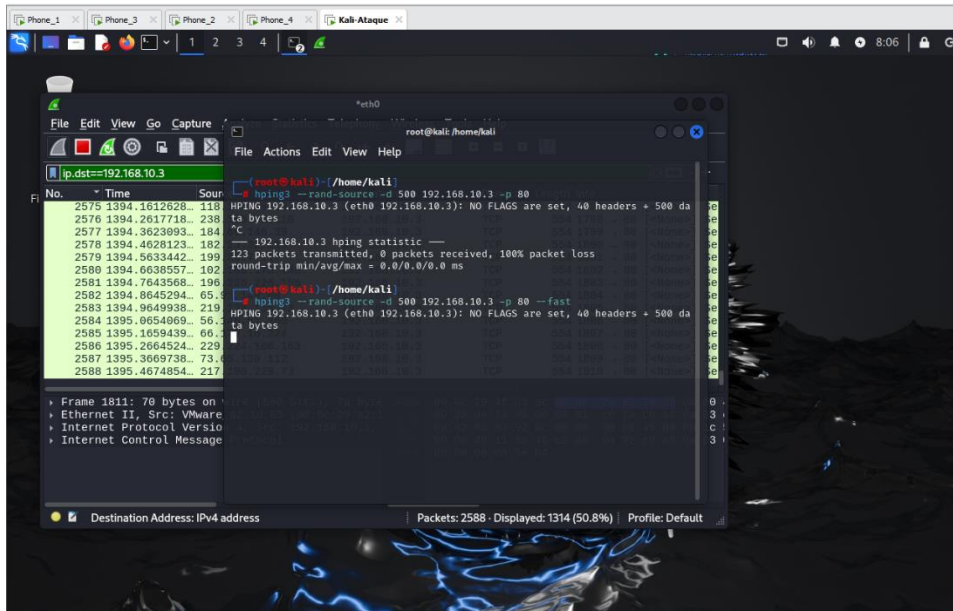


Figura 21: Se cambia el origen (dirección IP) de los datos de la máquina atacada y envía más datos.

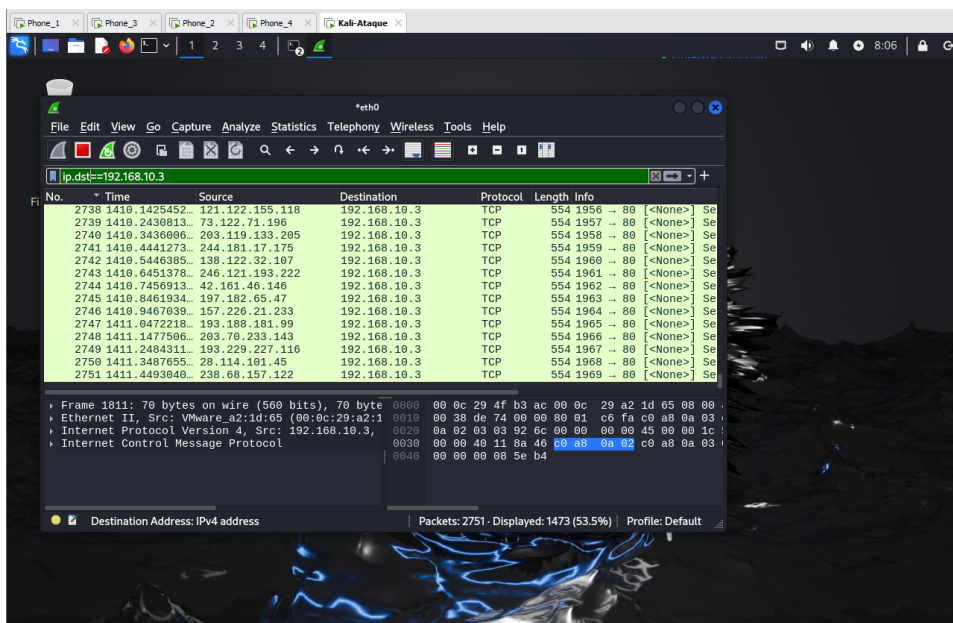


Figura 22: Saturación a la máquina atacada con el envío de datos de manera masiva para cortar la comunicación entre los teléfonos

○ Ataque 3 – Ataque ARP Spoofing

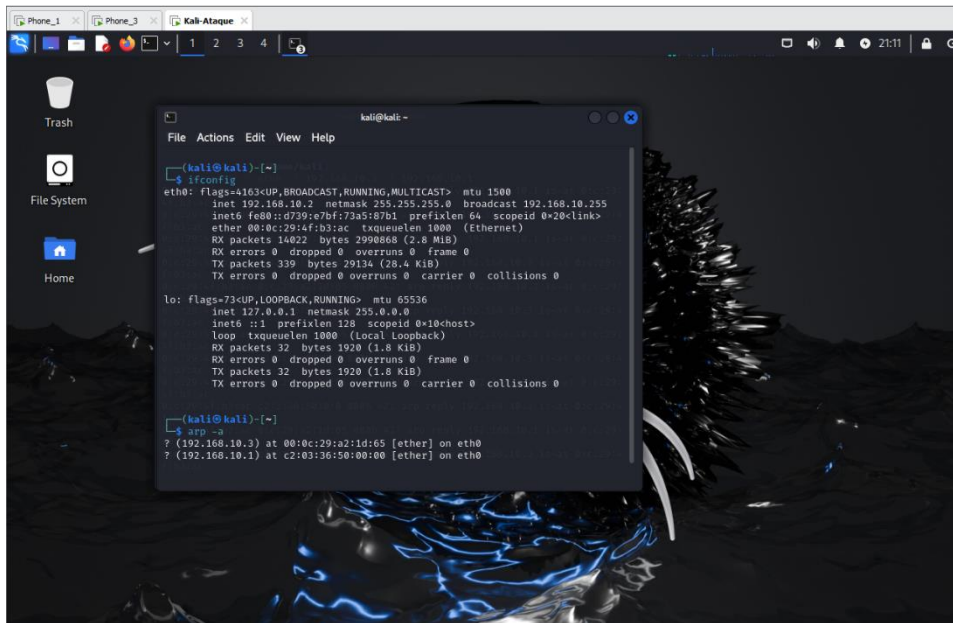


Figura 23: Ver la dirección MAC del atacante para llevar a cabo el ataque ARP Spoofing

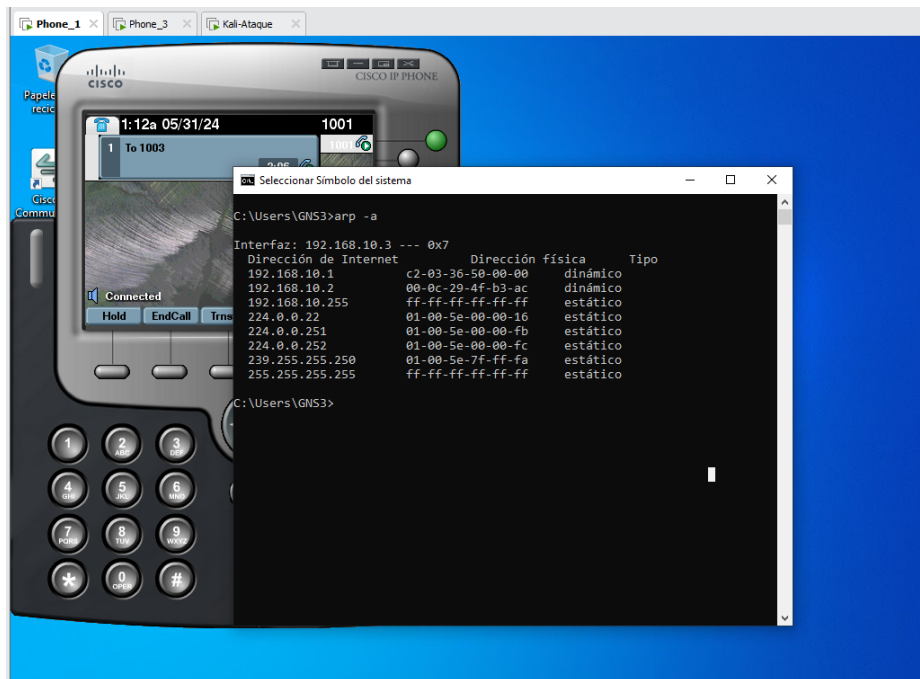


Figura 24: Visualización de tablas de ARP

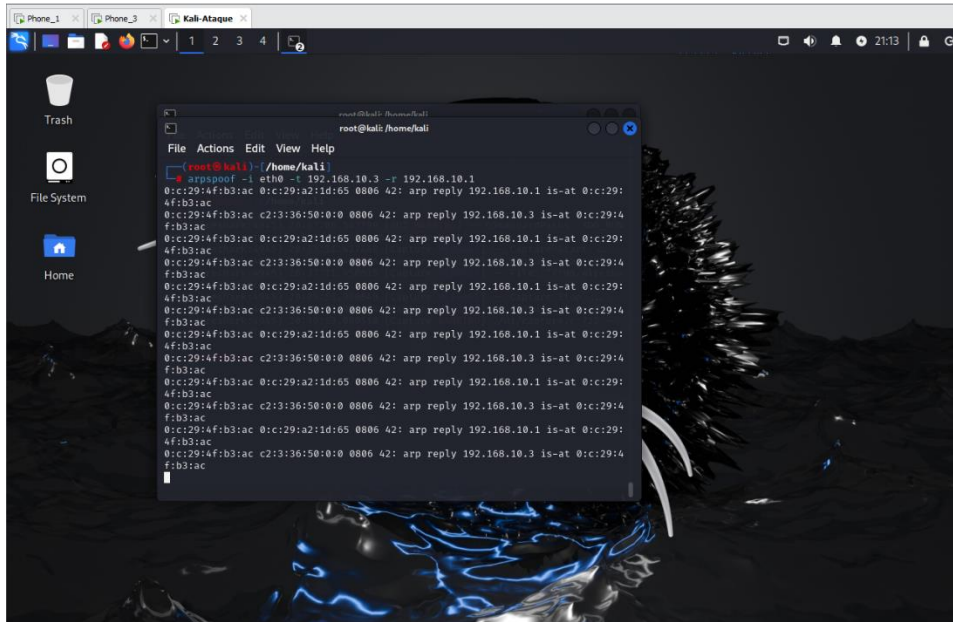


Figura 25: Se envía datos a la víctima para cambiar su dirección MAC

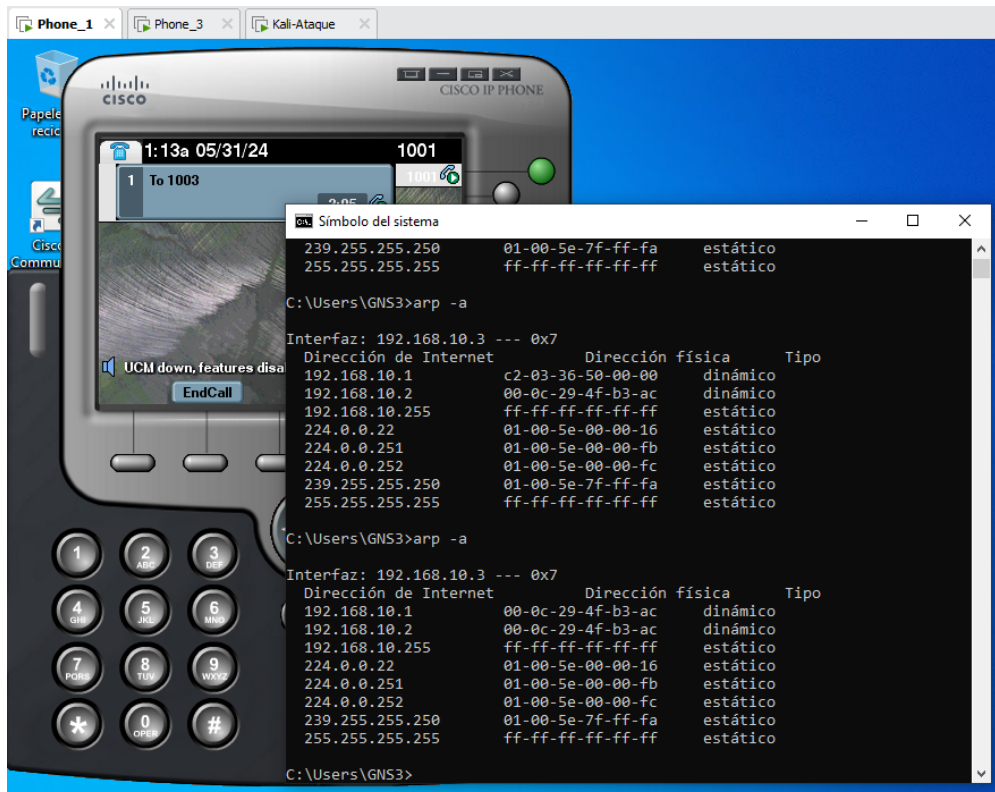


Figura 26: Visualización del antes y después de las direcciones MAC de la víctima.

- **Control a los ataques**
 - Control DHCP SNOOPING

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dh
Switch(config)#ip dhcp sn
Switch(config)#ip dhcp snooping
Switch(config)#exit
Switch#
*Jul 15 22:21:00.425: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh
Switch#show vlan
```

VLAN Name	Status	Ports
1 default	active	Gi0/1, Gi0/2, Gi0/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3
10 VLAN_10	active	Gi1/0, Gi1/1, Gi1/2, Gi1/3
20 VLAN_20	active	Gi2/0, Gi2/1, Gi2/2, Gi2/3
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figura 27: Activación del DHCP Snooping

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip dhcp snooping vl
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#ip dhcp snooping vlan 20
Switch(config)#
```

Figura 28: Activación del DHCP Snooping en las vlans creadas

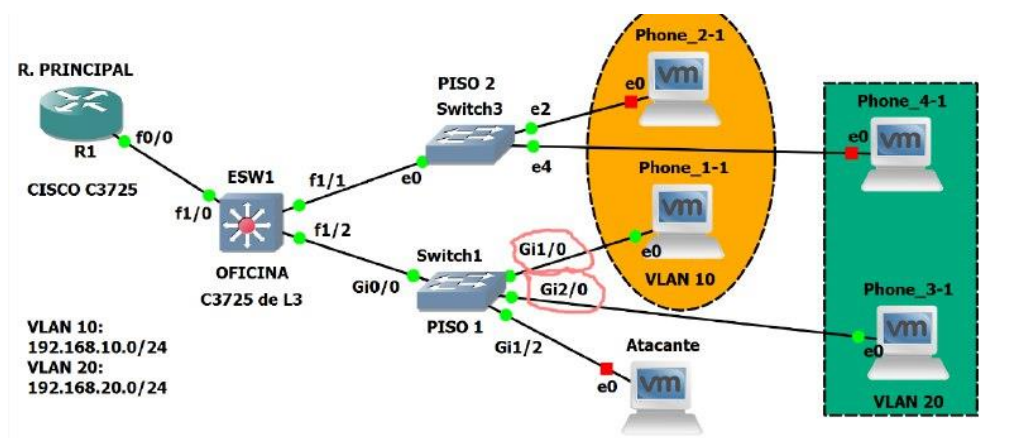


Figura 29: Activación de las interfaces que se usa

```

Switch(config)#interface gigabitEthernet 1/0
Switch(config-if)#ip dh
Switch(config-if)#ip dhcp sn
Switch(config-if)#ip dhcp snooping tr
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#interface gigabitEthernet 2/0
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#end
Switch#
Switch#
*Jul 15 22:36:33.775: %SYS-5-CONFIG_I: Configured from console by console
Switch#

```

Figura 30: En interfaces se activa los puertos de confianza

```

root@kali: ~
File Actions Edit View Help
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::6a56:953:6a72:517b prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:03:b1:e0 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 45 bytes 8177 (7.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::c636:284c:ced:962c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:03:b1:ea txqueuelen 1000 (Ethernet)
    RX packets 8 bytes 2800 (2.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25 bytes 4234 (4.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 31: Máquina de atacante no puedo obtener una dirección IP



Figura 32: Llamada libre de posible ataque

o Control PORT-SECURITY

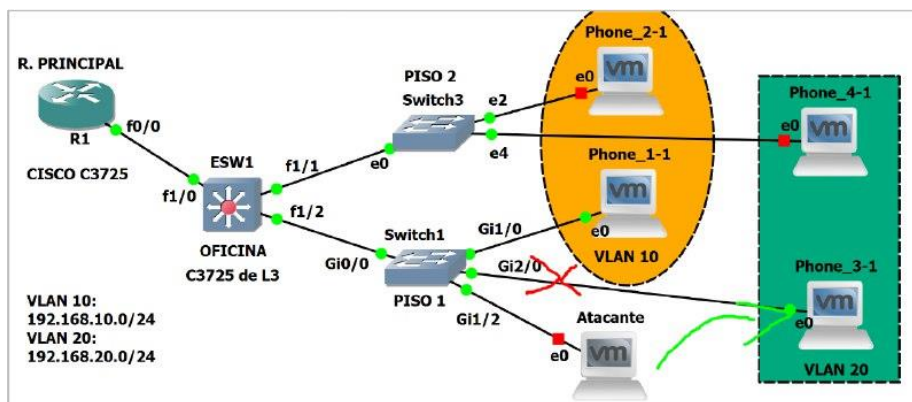


Figura 33: Atacante entra en la red y desconecta al cliente

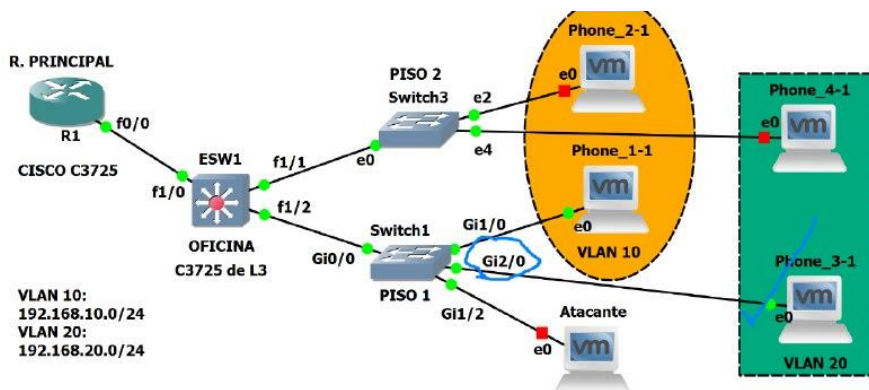


Figura 34: Puerto de Switch para la aplicación de Port-Security


```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
*Jul 16 00:04:45.377: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Giga
bitEthernet0/0 (not full duplex), with ESW1 FastEthernet1/2 (full duplex).
Switch(config)#
Switch(config)#
*Jul 16 00:05:56.853: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Giga
bitEthernet0/0 (not full duplex), with ESW1 FastEthernet1/2 (full duplex).
Switch(config)#
Switch(config)#exit
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
*Jul 16 00:06:03.300: %SYS-5-CONFIG_I: Configured from console by console
Switch(config)#int
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 2/0
Switch(config-if)#sw
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ma
Switch(config-if)#switchport port-security max
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation re
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security ma
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address st
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#end

```

Figura 35: Configuración de la interfaz de Switch para permitir una solo dirección MAC

```

interface GigabitEthernet2/0
switchport access vlan 20
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 000c.29b5.8702
switchport port-security
media-type rj45
negotiation auto

```

Figura 36: Revisión de la interfaz y verificación de la activación del Port-Security

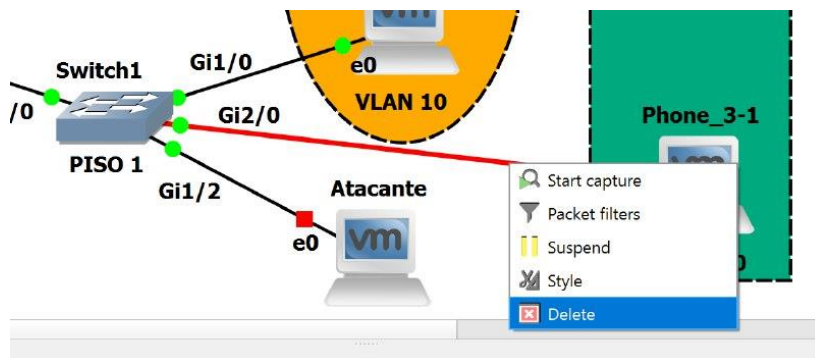


Figura 37: Desconectamos la Interfaz para luego conectarla al atacante y verificar que no tiene acceso

```
root@kali: ~
File Actions Edit View Help
root@kali~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
ether 00:0c:29:03:b1:e0 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 64 bytes 11635 (11.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 38: Ha sido protegida ya que no recibe alguna dirección IP el atacante

o Control usando ACL

```
Switch(config)#vlan 100
Switch(config-vlan)#na
Switch(config-vlan)#name NO_USADAS
Switch(config-vlan)#
Switch(config-vlan)#exit
*Jul 16 01:17:17.782: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Giga
bitEthernet0/0 (not full duplex), with ESW1 FastEthernet1/2 (full duplex).
```

Figura 39: Creación de VLAN para las interfaces no ocupadas



Figura 40: Interfaces con punto verde con las que se están usando

```

Switch(config)#interface range gigabitEthernet 1/1 - 3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mo
Switch(config-if-range)#switchport mode ac
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access vl
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface range gigabitEthernet 2/1 - 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#end
Switch#
Switch#
*Jul 16 01:22:07.623: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#sh
Switch#show vl
Switch#show vlan

```

VLAN Name	Status	Ports
1 default	active	Gi0/1, Gi0/2, Gi0/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3
10 VLAN_10	active	Gi1/0
20 VLAN_20	active	Gi2/0
100 NO_USADAS	active	Gi1/1, Gi1/2, Gi1/3, Gi2/1 Gi2/2, Gi2/3
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figura 41: Verificación de las interfaces no usadas estén en la VLAN NO_USADAS

```

Switch(config)#access-list 101 deny ip any any
Switch(config)#interface range gigabitEthernet 1/1 - 3
Switch(config-if-range)#ip ac
Switch(config-if-range)#ip access-group 101 in
Switch(config-if-range)#exit
Switch(config)#interface range gigabitEthernet 2/1 - 3
Switch(config-if-range)#ip access-group 101 in
Switch(config-if-range)#end

```

Figura 42: Comandos para crear una ACL que bloquea todo el tráfico IP

```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::6a56:953:6a72:517b prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:03:b1:e0 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 32 bytes 5895 (5.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 43: la máquina del atacante no puede conectarse y por ende no podrá realizar ataques (DDOS, ARP Spoofing o Eavesdropping)

- Control Port-Mirror

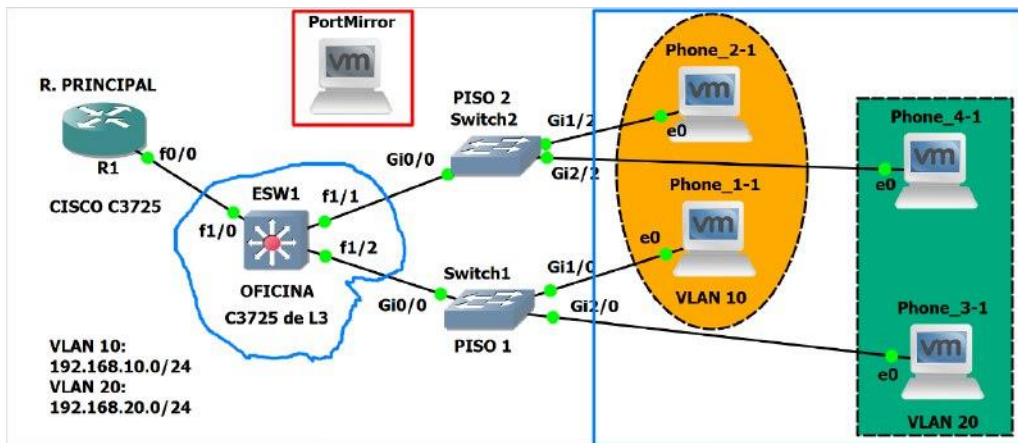


Figura 44: Monitoreo de la red VoIP para saber que procesos están pasando

```

ESW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ESW1(config)#monitor session 1 source interface fastEthernet 1/1
ESW1(config)#monitor session 1 source interface fastEthernet 1/2
ESW1(config)#
ESW1(config)#monitor session 1 destination interface fastEthernet 1/15
ESW1(config)#
ESW1(config)#exit
  
```

Figura 45: El tráfico de ambas interfaces fuentes sea monitoreado o analizado en la interfaz de destino

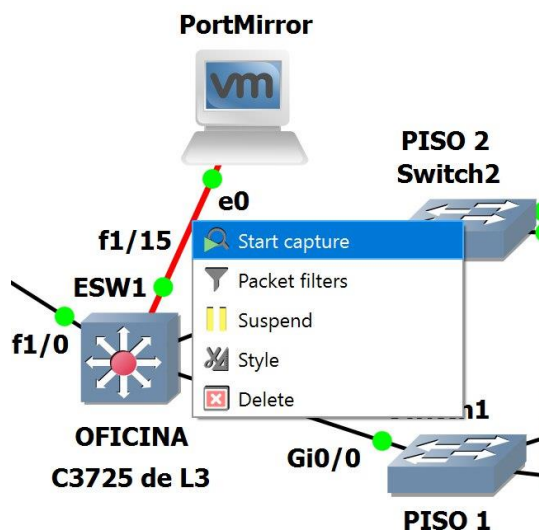


Figura 46: Encender la maquina donde se va a usar el Port-Mirror y comenzar a capturar

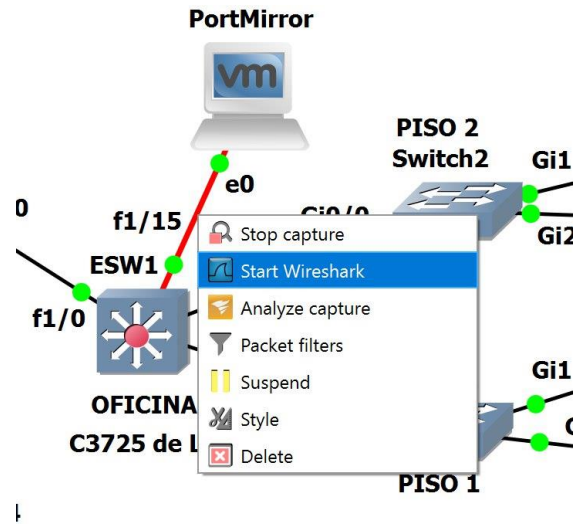


Figura 47: Se habilitará la opción para abrir Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
924	141.742514	192.168.20.3	192.168.10.2	ICMP	78	Echo (ping) reply id=0x0001, seq=3/768, ttl=127
925	141.757896	c2:02:1d:15:8f:11:02	PVST+	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:01 Cost = 0 Port = 0x002b
926	141.773288	c2:02:1d:15:8f:11:02	PVST+	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:02 Cost = 0 Port = 0x002b
927	142.703284	192.168.10.2	192.168.20.3	ICMP	78	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (no response found!)
928	142.711140	192.168.10.2	192.168.20.3	ICMP	78	Echo (ping) request id=0x0001, seq=4/1024, ttl=127 (reply in 929)
929	142.731476	192.168.20.3	192.168.10.2	ICMP	78	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request in 928)
930	142.741896	192.168.20.3	192.168.10.2	ICMP	78	Echo (ping) reply id=0x0001, seq=4/1024, ttl=127
931	143.633810	c2:02:1d:15:8f:11:01	Spanning-tree (for...	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:00 Cost = 0 Port = 0x002a
932	143.679031	c2:02:1d:15:8f:11:01	PVST+	STP	64	Conf. Root = 32768/0/c2:02:12:48:00:00 Cost = 0 Port = 0x002a
933	143.695017	c2:02:1d:15:8f:11:02	Spanning-tree (for...	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:00 Cost = 0 Port = 0x002b
934	143.710589	c2:02:1d:15:8f:11:01	PVST+	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:01 Cost = 0 Port = 0x002a
935	143.725962	c2:02:1d:15:8f:11:01	PVST+	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:02 Cost = 0 Port = 0x002a
936	143.741332	c2:02:1d:15:8f:11:02	PVST+	STP	64	Conf. Root = 32768/0/c2:02:12:48:00:00 Cost = 0 Port = 0x002b
937	143.756714	c2:02:1d:15:8f:11:02	PVST+	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:01 Cost = 0 Port = 0x002b
938	143.772084	c2:02:1d:15:8f:11:02	PVST+	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:02 Cost = 0 Port = 0x002b
939	143.694869	c2:02:1d:15:8f:11:01	Spanning-tree (for...	STP	68	Conf. Root = 32768/0/c2:02:12:48:00:00 Cost = 0 Port = 0x002a

Figura 48: Ejemplo de los procesos que se suceden en la red