UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“Nftables como firewall a nivel del kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021”

Tesis presentada por **:** Bach. Axell Alberto Ñacari Valverde

Para optar el título profesional de : Ingeniero de Sistemas.

Tipo de Investigación **:** Aplicada

Área de Investigación : Tecnología de información & Comunicaciones

Asesor **:** Mg. Ing. Hubner Janampa Patilla

Ayacucho - Perú

2021

DEDICATORIA

A mi familia, por su apoyo incondicional a lo largo de mi vida, sin importar las circunstancias.

A Celia y Allison, quienes a pesar de la distancia, nunca dejan de ser mi mayor fuente de inspiración

AGRADECIMIENTO

A la Universidad Nacional de San Cristóbal de Huamanga, por ser mi Alma Máter y centro de enseñanza lejos de mi tierra natal.

A los docentes de la Escuela Profesional de Ingeniería de Sistemas, quienes con esmero, dedicación y paciencia supieron brindarme el conocimiento y formación suficientes para poder convertirme en profesional.

A mi asesor, el Mg. Ing. Hubner Jananpa Patilla, por su tiempo, consejo y valiosa guía durante la elaboración del presente proyecto.

Contenido

CAPÍTULO III

Metodología de la investigación

CAPÍTULO IV

Implementación del cortafuego (firewall) con Nftables en la entidad

CAPÍTULO V

Conclusiones y recomendaciones

Resumen

En la actualidad, en el Perú, y con la pandemia a nivel mundial, los ataques informáticos se vienen incrementado, pues con el avance diario de la tecnología también surgen nuevas modalidades de ataques y amenazas, las cuales se centran especialmente en empresas e instituciones, generando perjuicio no solamente económico, sino a nivel de imagen y vulneración de información. Como consecuencia inmediata a ello se han determinado por establecer diversas medios que contribuyan a la seguridad informática, especialmente orientada hacia la protección de datos, entre los cuales resaltan los Sistemas de Detección de Intrusiones (IDS) siendo actualmente el medio más efectivo a la hora de ofrecer protección a nivel de paquetes de red, pues monitorean el tráfico de red entrante y saliente e identifican el uso no autorizado del mal manejo de las redes informáticas en las cuales son empleados. Estos, al ser muy sofisticados, detectan ataques que no podrían, valga la redundancia, ser detectados por firewall básicos, antivirus u otras soluciones habituales en lo que a la seguridad informática respecta. No obstante, a pesar de su capacidad efectiva, son muy pocas las entidades y/o empresas que hacen uso de sus beneficios, toda vez que la falta de conocimiento, el factor económico, entre otros, se presentan como las dificultades principales.

El objetivo de la investigación fue implementar los nftables a nivel de cortafuegos bajo el kernel de Linux con el fin de filtrar de paquetes en entornos libres, que pueda ser aplicado a empresas e instituciones del Perú mediante técnicas y reglas de seguridad informática. Con el fin de lograr los objetivos de la presente investigación, se tuvo a bien optar por virtualizar el entorno donde se emplearon las herramientas necesarias para llevar a cabo las pruebas correspondientes a la investigación y la implementación, para así, posteriormente, poder comprobar el funcionamiento de Nftables a nivel de cortafuegos.

Se implementará un nftables a nivel de cortafuegos, basado en palabras clave de protocolo, perfilado de reglas y mediante algoritmos de comparación de patrones. Se utilizará el Sistema Operativo Linux y algunas herramientas de seguridad informática.

Palabra clave: nftables a nivel de cortafuego, filtrado de paquetes, Seguridad Empresarial, Ataques informáticos.

Introducción

El software libre, entre otras cosas, persigue que se proporcione a la comunidad usuaria una base común que sirva de sustento para el desarrollo de nuevas herramientas con las que poder llevar a cabo trabajos de diversa índole con total seguridad, tanto dentro de las empresas particulares, como las estatales.

Siendo así, para este caso específico, la distribución Linux se constituye como una salida viable a la situación de inseguridad actual, además de representar un medio alternativo al alcance de las personas para futuros proyectos en diversas ramas de la ingeniería de sistemas como seguridad informática, redes, telecomunicaciones, entre otros; debido a que ofrece diversas soluciones de seguridad de manera gratuita. Por su parte, una de las soluciones de seguridad más actuales, Nftables, ofrece las herramientas adecuadas para administrar la seguridad de información, convirtiéndose en una herramienta fundamental para que los responsables de la gestión de seguridad de las diferentes entidades puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.

El presente trabajo surge de la necesidad de obtener una herramienta al alcance de las personas, a nivel académico y laboral, que permita la realización de tareas, sin necesidad de contar con medios económicos elevados o trabajos de una configuración demasiado avanzada o compleja que generen dificultad al momento de utilizarse.

Los objetivos específicos son a) Aplicar los Nftables a nivel de IPv4 en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021. b) Aplicar los Nftables a nivel de ARP en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021. c) Aplicar los Nftables a nivel de Ethernet en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021.

CAPÍTULO I

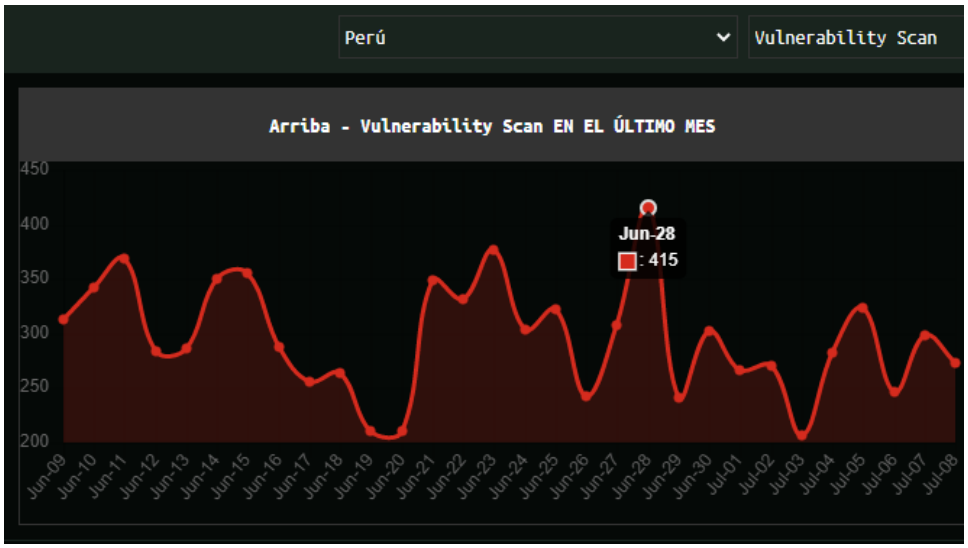
Planteamiento del problema

1.1 Diagnóstico y enunciado del problema

"De las empresas peruanas que participaron en la encuesta, el 61% aseguró contar con políticas relacionadas al tema de seguridad; no obstante, apenas el 29% señaló contar con un plan de respuesta y continuidad del negocio, y tan solo un 23% advirtió que clasifica su información. Del mismo modo, causa sorpresa que incluso las medidas de control más básicas, aquellas que son de esperarse ver en todas las empresas, como el uso de una solución antivirus, un respaldo de información o el empleo de algún Firewall, no han sido implementadas completamente por dichas empresas, llegando a mostrar un porcentaje de 78%, 62% y 62%, respectivamente" (Reporte de seguridad ESET Latinoamérica, 2021).

Figura 1

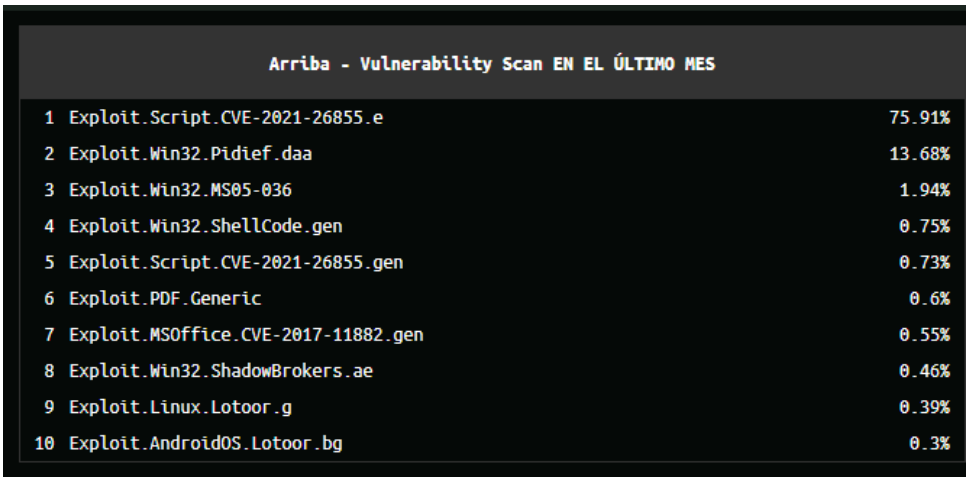
Estadística de los ciberataques informáticos a redes en Perú en el 2021



Nota. El gráfico cuantifica los ataques de red registrados en el Perú entre el 09 de junio del 2021 al 8 de julio del 2021. De donde se aprecia que se registró mayor incidencia el 28 de junio del 2021, llegando a mostrarse 415 de ataques en solo ese día. Tomado de (https://cybermap.kaspersky.com/, 2021).

Figura 2

Estadística de los tipos de ataques con mayor frecuencia a redes en Perú en el 2021



Arriba - Vulnerability Scan EN EL ÚLTIMO MES

1	Exploit.Script.CVE-2021-26855.e	75.91%
2	Exploit.Win32.Pidief.daa	13.68%
3	Exploit.Win32.MS05-036	1.94%
4	Exploit.Win32.ShellCode.gen	0.75%
5	Exploit.Script.CVE-2021-26855.gen	0.73%
6	Exploit.PDF.Generic	0.6%
7	Exploit.MSOffice.CVE-2017-11882.gen	0.55%
8	Exploit.Win32.ShadowBrokers.ae	0.46%
9	Exploit.Linux.Lotoor.g	0.39%
10	Exploit.AndroidOS.Lotoor.bg	0.3%

Nota. La figura representa los ataques con mayor frecuencia durante el período de 9 junio a 8 julio del 2021 las cuales son de tipo Exploit.sccrpt.CVE-2021-26855.e con un 75.91%. Tomado de (https://cybermap.kaspersky.com/, 2021).

“Las amenazas tanto cibernéticas como de privacidad vienen aumentando y extendiéndose. Según la Encuesta Global de Seguridad de la Información 2019-2020 de EY, 59% de las organizaciones han enfrentado algún incidente considerable o grave en el último año. Sin duda que este año ha planteado enormes desafíos y expuso, más que antes, las deficiencias existentes en todos los ámbitos de la sociedad a nivel mundial. Aun así, también resaltó el papel fundamental de la tecnología en nuestro modo de hacer frente como sociedad a esta crisis. Uno de los principales retos tanto para las industrias como para las organizaciones ha sido reforzar el nivel de seguridad de la información y la protección de todos sus sistemas informáticos ante al incremento considerable de los ciberataques en esta pandemia; mas aún, en un contexto que las obligó a seguir la adopción de nuevas formas de trabajo y poner interés en acelerar su transformación digital” (Diario Gestión, 2020).

“Durante el período comprendido entre octubre 2013 y diciembre de 2020, se registraron 12169 delitos relacionados a la Ley de Delitos Informáticos. El 78% de dichos delitos están vinculados al fraude informático, secundado por la suplantación de identidad con un 13%; y los delitos contra los datos y los sistemas informáticos alcanzaron un 6%. Por su parte, el delito con mayor incidencia, con relación al fraude informático, pertenece a las operaciones y transferencias por medios electrónicos y/o de fondos sin autorización, con un 86%. Asimismo, se puede apreciar que el registro total de los delitos cometidos ha tenido un crecimiento constante año a año,

donde los reportes del 2020 conforman el 134% de crecimiento, comparado a los registros del 2017". (División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú DIVINDAT, s.f.).

Figura 3

Estadística de los tipos de delitos con mayor frecuencia en el Perú, entre los años 2013 al 2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	**14**	**3**	**6**	**4**	**5**	**1**	**2**	**19**	**54**	**0.4%**
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6%**
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4%**
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2%**
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						**3**	**2**	**8**	**13**	**0.1%**
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

Adaptado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.

Nota. El gráfico indica los delitos registrados en el Perú entre los años del 2013 al 2020. De donde podemos indicar que se registró mayor delito en fraude informático con un total de 78.2%. Fuente: DIVINDAT – Perú.

Figura 4

Estadística de delitos subgenérico del año 2013 al año 2020 en el Perú

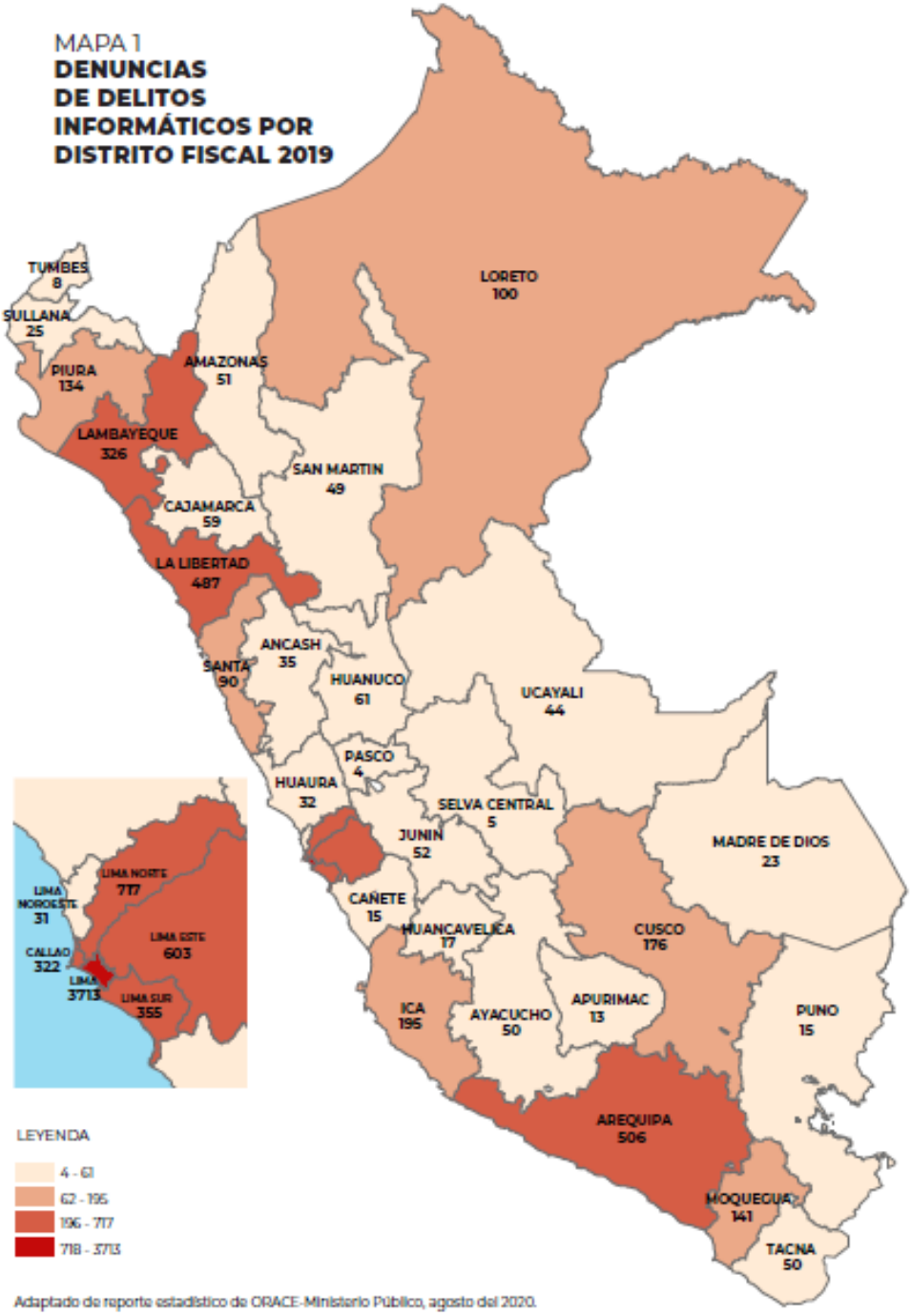
DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
LIMA	67	325	550	708	1485	2366	3713	1116	10 340	47.68%
LIMA NORTE	3	24	24	99	174	357	717	220	1618	7.46%
AREQUIPA	1	18	47	155	255	291	506	115	1388	6.40%
LIMA ESTE	3	17	26	53	147	251	603	183	1283	5.92%
LA LIBERTAD	3	20	35	36	94	213	487	232	1120	5.16%
LAMBAYEQUE	1	11	31	82	119	182	326	124	876	4.04%
CALLAO	3	15	16	52	57	130	322	101	696	3.21%
LIMA SUR	1	4	9	27	52	120	355	119	687	3.17%
CUSCO	4	33	42	41	79	81	176	81	537	2.48%
ICA		3	10	22	24	91	195	57	402	1.85%
PIURA	3	10	33	15	34	68	134	40	337	1.55%
LORETO	1	7	15	24	48	93	100	32	320	1.48%
MOQUEGUA	1	2	1	5	19	46	141	47	262	1.21%
SANTA		3	3	6	36	20	90	27	185	0.85%
HUANUCO		3	2	3	30	25	61	36	160	0.74%
JUNIN		5	7	5	16	44	52	27	156	0.72%
UCAYALI		4	6	9	18	43	44	15	139	0.64%
SAN MARTIN		3	4	6	32	31	49	13	138	0.64%
AMAZONAS	2	1	2	6	30	18	51	20	130	0.60%
CAJAMARCA	1	3	2	4	5	21	59	31	126	0.58%
AYACUCHO	2	3	2	9	9	24	50	15	114	0.53%
TACNA		6		5	4	20	50	15	100	0.46%
SULLANA		3	12	9	12	15	25	15	91	0.42%
HUAURA		4	6	8	11	20	32	10	91	0.42%
ANCASH		2	4	5	12	20	35	8	86	0.40%
LIMA NOROESTE			2	6	3	15	31	15	72	0.33%
PUNO	1		3	3	12	8	15	6	48	0.22%
APURIMAC		3	1	1	2	18	13	4	42	0.19%
MADRE DE DIOS		2	3		3	1	23		32	0.15%
TUMBES		4	3	2	5	6	8	1	29	0.13%
HUANCAVELICA	1	1	2	3		4	17	1	29	0.13%
CAÑETE		1	1	1	1	1	15	3	23	0.11%
SELVA CENTRAL			3		1	1	5	8	18	0.08%
PASCO	1				2	4	4	1	12	0.06%
TOTAL	**99**	**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21 687**	**100.00%**

Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de

Nota. El gráfico indica la cantidad de delito subgenérico en los departamentos del Perú entre los años 2013 al 2020. De donde podemos indicar que se registró mayor incidencia en el departamento de Lima, llegando a registrar 10340 de delitos. Fuente: DIVINDAT – Perú.

Figura 5

Estadística de denuncias de delitos informáticos por distrito fiscal año 2019



Nota. El gráfico indica la cantidad de denuncias de delitos informáticos por distrito fiscal año 2019. De donde podemos indicar que se registró en el distrito de Lima mayor cantidad de denuncias, llegando a registrar 3713 de denuncias en el año 2019. Fuente: DIVINDAT – Perú.

Figura 6

Estadística de denuncias de delitos informáticos por distrito fiscal julio 2020

Nota. El gráfico indica la cantidad de denuncias de delitos informáticos por distrito fiscal, julio 2020. De donde podemos indicar que se registró mayor incidencia en Lima, llegando a registrar 1116 de denuncias. Fuente: DIVINDAT – Perú.

Figura 7

Estadística de delitos informáticos según tipo subgenérico, año 2013-2020

DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Sin especificar			57	643	1513	2431	4415	1325	10384	48%
Contra el patrimonio	99	535	812	614	931	1657	3228	1138	9014	42%
Contra la fe pública		2	7	45	123	160	335	116	788	4%
Contra datos y sistemas informáticos		2	16	41	118	159	281	79	696	3%
Contra la indemnidad y libertad sexuales			4	35	68	137	115	25	384	2%
Contra la intimidad y el secreto de las comunicaciones			6	25	49	72	68	40	260	1%
Disposiciones comunes		1	5	7	39	32	62	15	161	0.7%
TOTAL	**99**	**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21687**	**100.0%**

Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

Nota. El gráfico indica los delitos informáticos según tipo subgenérico en el Perú entre los años 2013 a 2020. De donde podemos indicar que se registró mayor cantidad de delitos en el año 2020 llegando a registrar 21687. Fuente: DIVINDAT – Perú.

Figura 8

Estadística de Fiscalías asignadas con el mayor número de registros de delitos informáticos.

Distrito Fiscal	FISCALIA ASIGNADA	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL
LIMA	01° FPP DE SAN ISIDRO				1	72	136	218	54	481
LIMA	02° FPP DE MIRAFLORES			1	8	106	136	161	57	469
LIMA	02° FPP DE SAN ISIDRO				1	61	135	212	55	464
LIMA	01° FPP DE MIRAFLORES				8	98	132	162	43	443
AREQUIPA	01° FPP CORPORATIVA DE AREQUIPA		6	19	49	84	92	149	33	432
AREQUIPA	03° FPP CORPORATIVA DE AREQUIPA	1	2	3	36	76	98	158	42	416
AREQUIPA	02° FPP CORPORATIVA DE AREQUIPA		3	17	60	85	72	117	29	383
LAMBAYEQUE	03° FPP CORPORATIVA DE CHICLAYO		4	11	41	65	77	120	54	372
LA LIBERTAD	01° FPP CORPORATIVA DE TRUJILLO	1	9	12	15	31	75	182	27	352
LA LIBERTAD	03° FPP CORPORATIVA DE TRUJILLO	1	1	12	4	16	41	140	133	348
LA LIBERTAD	02° FPP CORPORATIVA DE TRUJILLO	1	5	9	6	32	86	139	55	333
TOTAL		**4**	**30**	**84**	**229**	**726**	**1080**	**1758**	**582**	**4493**

Nota. El gráfico indica las fiscalías asignadas con el mayor número de registros de delitos informáticos en el Perú, año 2013 al 2020. De donde podemos indicar que se registró mayor registro en el año 2010, llegando a registrar 1758 de ataques en ese año. Fuente: DIVINDAT – Perú.

Figura 9

Estadística de denuncias por delitos informáticos según estado procesal

ESTADO	CANTIDAD	%
Archivadas	12608	58%
En proceso	8842	41%
Sobreseimiento	125	1%
Sentencia	108	0%
Terminación anticipada	4	0%
TOTAL	**21 687**	

Nota. El gráfico indica la cantidad de denuncias interpuestas por delitos informáticos según estado procesal en el Perú, año 2013 al 2020. De donde podemos indicar que la mayor cantidad son archivadas, llegando a un porcentaje del 58%. Fuente: DIVINDAT – Perú.

1.2 Definición del problema de investigación

Problema general

¿Cómo los Nftables se utilizan a nivel de cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021?

Problemas específicos

a. ¿Cómo los Nftables a nivel IPv4 se utilizan en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021?

b. ¿Cómo los Nftables a nivel de ARP se utilizan en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021?

c. ¿Cómo los Nftables a nivel de Ethernet se utilizan en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021?

1.3 Objetivo general

Implementar los Nftables a nivel de cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021.

1.4 Objetivos específicos

a. Aplicar los Nftables a nivel de IPv4 en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021.

b. Aplicar los Nftables a nivel de ARP en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021.

c. Aplicar los Nftables a nivel de Ethernet en cortafuegos bajo el kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021.

1.5 Justificación

La función inherente a la seguridad informática es limitar el acceso no autorizado a una computadora o sistema. Bajo un esquema de seguridad sin fallos, la información nunca se comprometería porque los usuarios no autorizados nunca obtendrían acceso. Sin embargo, a pesar que a la fecha no existe tal sistema de seguridad perfecto, hay mecanismos disponibles para dar el mayor alcance de seguridad posible.

Aun así, las barreras de capacitación, divulgación, economía, entre otras, impiden que los equipos en general, ya sean de hogares, empresas y/o instituciones, posean medios de protección adecuados. En ese sentido, el presente trabajo se justifica en brindar, además de un aporte académico a la sociedad, una salida viable a la situación de inseguridad informática que se vive hoy en día, la cual evoluciona a pasos agigantados generando perjuicio no solo económico, sino de diversas índoles.

1.6 Delimitación

La investigación se realizó sobre nftables como cortafuegos a nivel de kernel de Linux para filtrado de paquetes, abarcando la interfaz de red, métodos de captura, motor de reglas y filtrado de eventos.

CAPÍTULO II

Revisión de la literatura

2.1 Antecedentes de la investigación

Según Pacheco y Martínez (2009), en su tesis denominada “Diseño e implementación de un servidor firewall en linux”, de la Universidad Tecnológica de Bolívar Cartagena de Indias, concluye que; “dentro del proceso de implementación podemos observar la relevancia que representa iptables como un medio para proteger y garantizar la seguridad del acceso a redes en el flujo de información entre las mismas; del mismo modo se pudo constatar la existencia de reglas utilizadas por algunas empresas para el tema de seguridad, las cuales no llegan a ser eficientes según el nivel de protección requerido según sus políticas. Los cortafuegos (firewall) son muy útiles, siempre y cuando se definan adecuadamente todas las políticas para permisos de acceso y puedan cumplirse eficazmente; los firewall por sí solos no representar la solución definitiva a la implementación de seguridad en una red, debido a que la seguridad no solamente es un concepto estático, sino, por el contrario, son un concepto dinámico debido a los continuos ataques que puede sufrir una red, motivo por el cual se requiere experticia por parte del administrador de la red, donde es necesaria una vigilancia de manera continua, apoyada en el empleo de soluciones que nos faciliten esta labor, para de este modo poder garantizar el buen funcionamiento del firewall”.

Según Cohn (2008), en su tesis denominada “Análisis, diseño e implementación de una aplicación para la administración de las herramientas de seguridad en una red local” de la universidad Pontificia Universidad Católica del Perú, concluye que; “Mientras más sencilla e intuitiva sea una aplicación para los usuarios finales, disminuyen los riesgos de configurarla inadecuadamente; del mismo todo, el tiempo empleado en realizar dichas configuraciones es menor, lo cual nos permite asignar al personal la realización de tareas críticas. Sin embargo, a pesar de las herramientas que nos permiten configurar y asegurar las redes y sistemas; siempre estará presente un nivel de riesgo y exposición a ataques, mientras que los usuarios no tomen consciencia en relación a los riesgos a los que se hallan expuestos”.

2.2 Marco teórico.

Nftables

Según Netfilter (2021) “nftables reemplaza las populares {ip, ip6, arp, eb} tables. Este software proporciona un nuevo marco de clasificación de paquetes en el kernel que se basa en una máquina virtual (VM) específica de la red y una nueva herramienta de línea de comandos del espacio de usuario. Nftables reutiliza los subsistemas Netfilter existentes, como la infraestructura de enlace existente, el sistema de seguimiento de conexiones, NAT, el subsistema de registro y cola del espacio de usuario. Este software también proporciona libnftables, la biblioteca de espacio de usuario de alto nivel que incluye soporte para JSON”.

“nftables es un subsistema del kernel de Linux que proporciona filtrado y clasificación de paquetes, datagramas, tramas de red. Ha estado disponible desde el lanzamiento del kernel de Linux 3.13 el 19 de enero de 2014” (KernelNewbies, 2021).

IPv4

En su definición de IPv4, Rosen (2014), menciona que:

> “El protocolo IPv4 es uno de los protocolos centrales de la Internet basada en estándares de hoy y que enruta la mayor parte del tráfico en Internet. El protocolo IPv4 proporciona una conectividad de extremo a extremo entre dos hosts cualesquiera. Otra función importante de la capa IP es reenviar paquetes (también llamado enrutamiento) y administrar tablas que almacenan información de enrutamiento”.

Asimismo, asegura que el IPv4 comprende lo siguiente:

A. Encabezado IPv4

“El encabezado IPv4 consta de información que define como un paquete debe ser manejado por la pila de la red del kernel: el protocolo que se usa, la dirección de origen y destino, la suma de verificación, la

identificación (id) del paquete que se necesita para la fragmentación. Esta información se almacena en 13 miembros del encabezado de IPv4 (el decimocuarto miembro, Opciones de IP, que es una extensión del encabezado IPv4, es opcional)". Rosen (2014)

B. Inicialización de IPv4

Rosen (2014), menciona que "los paquetes IPv4 son paquetes con el tipo de Ethernet 0x0800 (el tipo de Ethernet se almacena en los dos primeros bytes del encabezado de Ethernet de 14 bytes). Cada protocolo debe definir un controlador de protocolo y cada protocolo debe inicializarse para que la pila de red pueda manejar paquetes que pertenecen a este protocolo. Para que comprenda qué causa que los paquetes IPv4 recibidos sean manejados por métodos IPv4".

C. Recibir Paquetes IPv4

Según Rosen (2014), "el principal método de recepción de IPv4 es el método ip_rcv (), que es el controlador de todos los paquetes IPv4 (incluidas las multidifusiones y las difusiones). De hecho, este método consiste principalmente en controles de cordura. El trabajo real se realiza en el método ip_rcv_finish () que invoca".

D. Recepción de Paquetes de Multidifusión IPv4

Según Rosen (2014), menciona que "el método ip_rcv() también es un controlador para paquetes de multidifusión. Como se mencionó anteriormente, después de algunas comprobaciones de cordura, invoca el método ip_rcv_finish(), que realiza una búsqueda en el subsistema de enrutamiento llamando a ip_route_ input_noref()".

Protocolo de Resolución de Direcciones (Arp)

Según Latifi (2016, pp. 407-408), menciona que:

"ARP se utiliza para asignar direcciones de protocolo de Internet a direcciones de máquinas físicas. La tabla de caché ARP se utiliza para mantener la

relación entre la dirección mac y su dirección IP correspondiente. Proporciona las reglas de los protocolos para realizar esta correlación y proporciona conversiones de direcciones en ambas direcciones. Una máquina host está recibiendo un paquete entrante con la dirección de destino en una red de área local llega a la puerta de enlace, solicita al programa ARP que encuentre el host físico o la dirección MAC para la dirección IP entrante. El programa ARP busca en la tabla de caché y, si encuentra la dirección, enruta el paquete a la dirección de destino requerida. Si no hay una entrada en la tabla de caché, ARP enviará el paquete a todos los clientes y si algún destino descubre que pertenece a ese cliente, enruta ese paquete a ese destino. Este protocolo actualiza la tabla de caché ARP para referencia futura y luego envía el paquete a la dirección MAC. Podemos encontrar la dirección ARP del hardware disponible con el siguiente comando".

"La tabla de caché ARP se almacena en la tabla de enrutamiento del sistema que crea dinámicamente las rutas del host. Las entradas ARP se pueden agregar, eliminar o cambiar con la utilidad ARP. Las entradas agregadas manualmente son permanentes o temporales y se publican, en cuyo caso el sistema responderá a las solicitudes de ARP a los hosts. Un host que responde a una solicitud de mapeo ARP para la dirección del host local. Si el host local responde a las solicitudes de direcciones que no sean él mismo con su propia dirección, se denomina APR de proxy. La ruta a una red Ethernet conectada directamente se prescribe como clonación".

"Los tiempos de espera normales para estas rutas serán 20 minutos después de la validación y las entradas no se validan cuando no se utilizan".

Ethernet

Según Carthern (2015), menciona que "Ethernet es una arquitectura de red de área local desarrollada por Xerox Corporation. La especificación de Ethernet es la base del estándar IEEE 802.3, que especifica capas físicas y

de enlace de datos. Ethernet es el estándar de red más utilizado en el mundo. Normalmente, Ethernet se utiliza para admitir implementaciones de redes locales, pero las distancias admitidas por Ethernet han aumentado en kilómetros".

"Independientemente de si estamos hablando de una red o de cientos de redes conectados entre sí, el tipo más popular de red conmutada por paquetes es el Ethernet. Desarrollado hace 30 años por Xerox PARC y luego estandarizado por Xerox, Intel y Digital Equipment Corporation, Ethernets originalmente consistía de un solo cable que conecta los nodos en una red. A medida que Internet explotó, la computación cliente-servidor se convirtió en la norma, y cada vez más computadoras unidas entre sí, una tecnología más simple y barata conocida como par trenzado ganó aceptación". (Davis et al., 2004)

Protocolo de internet

Para Davis et al. (2004) existe un protocolo "que permite el intercambio de paquetes entre redes como si las redes conectadas fueran una única red homogénea. Este protocolo es conocido como el Protocolo de Internet, o IP, y fue definido por RFC 791 en septiembre de 1981"

Protocolo de Datagrama de Usuario (UDP)

Según Davis et al. (2004) "en la capa de Internet de nuestra pila de protocolos TCP / IP, la única información disponible es la dirección del nodo remoto. No hay otra información disponible para el protocolo, y no se necesita ninguno. Sin embargo, sin información adicional como número de puerto, su nodo receptor está limitado a realizar una sola red comunicación en cualquier momento. Dado que los sistemas operativos modernos permiten múltiples aplicaciones para que se ejecuten simultáneamente, debe poder abordar múltiples aplicaciones en el nodo receptor simultáneamente, en lugar de solo una".

Protocolo de Control de Transmisión (TCP)

Davis et al. (2004) afirman que:

"TCP, por otro lado, proporciona un mecanismo conocido como entrega de flujo confiable que garantiza la entrega de un flujo de información desde un nodo de red a otro sin duplicación o pérdida de datos. TCP tiene una serie de características que describen la interfaz entre él y los programas de aplicación que lo utilizan":

A. Circuito virtual

"Usar TCP es muy parecido a hacer una llamada telefónica. El remitente solicita una conexión con el receptor. Ambos extremos negocian los parámetros de la conexión y acordar varios detalles que definen la conexión. Una vez que se finaliza la conexión, las aplicaciones pueden continuar. En lo que respecta a las aplicaciones, una conexión dedicada y confiable existe entre el emisor y el receptor, pero esto es una ilusión".

B. Transferencia en Búfer

"La capa TCP, independientemente de la aplicación, determina la forma óptima de empaquetar los datos que se envían, utilizando cualquier tamaño de los paquetes que sean apropiados. Para aumentar la eficiencia y disminuir el tráfico de red, TCP normalmente espera, si es posible, hasta que tiene una cantidad relativamente grande de datos para enviar antes de enviar el paquete, incluso si la aplicación está generando datos l byte a la vez. La capa TCP receptora entrega datos al recibir la aplicación exactamente de la forma en que se envió, por lo que puede existir un búfer en cada extremo, independientemente de la aplicación".

C. Orientación de la Secuencia

"El nodo receptor envía datos al receptor aplicación exactamente en la misma secuencia en que se envió".

D. Dúplex Completo

"Las conexiones proporcionadas por TCP sobre IP son dúplex completo, que significa que los datos se pueden transmitir en ambas direcciones simultáneamente a través de dos flujos de paquetes independientes. Las secuencias se pueden utilizar para transferir datos o para enviar información de control o comandos al remitente, y cualquiera de las dos corrientes puede terminarse sin dañar a la otra".

E. Flujo no Estructurado

"TCP no garantiza que la estructura de los datos sea íntegra, aunque la entrega está garantizada. Depende de las aplicaciones determinar el contenido de la transmisión y ensamblar o desmontar el flujo de datos en cada extremo de la conexión. Las aplicaciones hacen esto almacenando en búfer los paquetes entrantes cuando es necesario y ensamblándolos en un orden que las aplicaciones reconozcan".

Trama Ethernet

"En una red Ethernet, todos los dispositivos mantienen un flujo de intercambio de paquetes de datos entre sí, a los cuales se le denomina paquetes Ethernet. Incluyen la trama Ethernet, también conocida como trama de datos, la cual se divide en varios conjuntos de datos. Estos registros se basan en código binario que brinda importante información, la cual consta de direcciones, información de control, datos de uso y sumas de comprobación". (IONOS, 2021)

"Según sea el estándar Ethernet, las tramas tendrán una estructura diferente y podrían contener más o menos campos de datos, según dependan del protocolo de red". (IONOS, 2021)

Tipos y Estructura de una Trama Ethernet

"En el modelo OSI, en la capa de enlace es en la que se encuentra la trama responsable de transmitir y separar el flujo de datos de bits en bloques o

tramas. Ethernet I, que fue la primera versión de Ethernet, aún estaba basada en campos de datos de 16 bits sin bytes definidos. Actualmente, dichas tramas, que son más modernas, se emplearon inicialmente vez en la denominada estructura Ethernet II, poco antes de que IEEE logre desarrollar Ethernet en el año 1983 en el protocolo estándar IEEE 802.3" (IONOS, 2021)

A. Ethernet II

"Ethernet II emplea la estructura de la trama clásica con un campo de tipo (Type) que abarca diversos protocolos en la capa de red. En el modelo OSI, la capa de red es importante para realizar la conexión y entregar direcciones de red". (IONOS, 2021)

B. Ethernet 802.3raw

"En discordancia al modelo de Ethernet II, esta trama define un final preciso en la secuencia de bits para SFD. De esta manera el receptor logra identificar el paquete de datos como estándar 802.3. Estas tramas carecen de un identificador de protocolo, ya que Novell solo las emplea para IPX. Asimismo, los datos a transmitirse son siempre antecedidos de 2 bytes, los cuales están formados permanentemente por 1. Este es el único método para poder diferenciar un marco raw de otros marcos del grupo familiar 802.3". (IONOS, 2021)

C. Ethernet IEEE 802.3

"Esta es la estructura de trama LAN más conocida y totalmente empleada actualmente. No obstante, algunas redes y protocolos necesitan más espacio para cierta información determinada. Debido a ello, existen diferentes tramas basadas en Ethernet IEEE 802.3, las cuales brindan bloques de datos extras para información específica". (IONOS, 2021)

D. Ethernet IEEE 802.3 SNAP

"El campo denominado SNAP tiene utilidad para poder definir más allá de 256 protocolos. Para lograrlo, se otorgan a libertad 2 bytes para colocar el número de protocolo. Asimismo, el productor o creador puede agregar un identificador no repetitivo de 3 bytes. A diferencia de protocolos que lo anteceden, SNAP también nos ofrece la compatibilidad inversa con Ethernet II, DSAP, SSAP y Control son fijos". (IONOS, 2021)

E. VLAN 802.1q - Ethernet II etiquetada y IEEE 802.3 etiquetada

"Los marcos con etiquetas poseen una en especial, llamada VLAN, la cual se utiliza para poder ser incluidos en una red de área local virtual (VLAN), la misma que divide la estructura de una red a nivel físico y lógico. Esto puede traducirse en lo siguiente: con el uso de las VLAN, todas las subredes son capaz de implementarse sin el requisito de agregar ningún tipo de hardware. De esta manera, una subred es virtualizada y no se crea en el mundo físico. El reconocimiento de tramas Ethernet dentro de una VLAN necesita el campo Tag". (IONOS, 2021)

Filtrado de Paquetes

"Filtrar paquetes es la técnica más empleada para implementar un firewall; debido a ello no todos los paquetes de datos que enviados entre los equipos representan una amenaza, sin embargo, no es necesario que todos ellos lleguen al sistema de destino" (Seoani, 2014)

Asimismo, Seoani asegura que el filtrado de paquetes presenta lo siguiente:

A. Parámetros Utilizados para Filtrar Paquetes

Seoani (2014), menciona que "los paquetes IP brindan, en la cabecera, toda la información que puede emplearse para identificar los paquetes que pasarán y los que serán eliminados, un enrutador, por ejemplo, para que pueda realizar el filtrado de paquetes se configurará de cualquiera de los tres modos posibles siguientes para administrar los paquetes que entran y salen por medio de las interfaces que posee:

- Restringir todas las conexiones externas, exceptuando aquellas conexiones de tipo SMTP para dejar que el equipo reciba e-mails.
- Negar las conexiones a sistemas catalogados como no seguros.
- Aceptar conexiones de e-mail, FTP, entre otras, pero restringir otros servicios como el TFTP u otros que sean considerados peligrosos.

A fin de ejecutar alguna de las acciones mencionadas se requiere configurar un conjunto de reglas, las cuales se irán consultando, de manera ordenada, para poder establecer qué paquetes pasan o no".

B. Reglas de Filtrado

"Las reglas empleadas para filtrado nos otorgan la posibilidad de establecer políticas de seguridad en nuestro sistema, dejando de lado los accesos sin autorización sin crear inconvenientes a los accesos que sí necesitamos permitir. Estas instrucciones suelen expresarse como un conjunto de condiciones y acciones que han de consultarse cuando se dé con la regla que nos posibilite la toma correcta de una decisión, ello hace particularmente importante que las instrucciones sean establecidas en un orden prioritario en cuanto a la actuación y que puedan ser revisadas cada cierto tiempo por los administradores". (Seoani, 2014)

El mismo autor menciona que "las reglas pueden ser agrupadas en tres tipos:

- Autoprotección del firewall: se restringen todos los datagramas dirigidos de manera directa hacia el firewall.
- Reglas de salida, estas pueden ser de carácter permisivo o restrictivo. Si son de carácter permisivo, se restringen todas las excepciones y las demás se permiten; si son de tipo restrictivo, se restringe todo, menos las excepciones aceptadas.
- Reglas de entrada: se prohíbe todo, menos todas las excepciones que hayan sido autorizadas de manera específica".

Open Source

Huebner y Zanero (2010) lo definen “como cualquier software que se distribuye junto con el código fuente, o donde cualquier usuario puede obtener el código fuente por un costo de reproducción no superior al razonable. El código fuente obtenido debe estar en la forma en que un programador modificaría el programa y debe estar completo y compilado correctamente para el ejecutable”.

“Entre otras tareas fundamentales, el procesamiento de texto y la creación de documentos son una parte importante del código abierto. La mayoría de las herramientas open source vienen con documentación escrita usando SGML o TeXinfo (ambos descritos en este capítulo). Herramientas completas como OpenOffice, dedica una parte importante al procesamiento de textos”. (Koranne, 2010)

“El código abierto es una forma de licenciar software. Significa que el software se puede distribuir libremente y contiene el código fuente. Esto significa que los usuarios pueden hacer copias, dárselas a amigos e incluso obtener una copia del código fuente. La idea detrás del código abierto es animar a los usuarios a examinar el código fuente de un producto y, si es posible, mejorarlo. La creencia es que, a través de la revisión y las mejoras realizadas por tantas personas, un producto alcanzará un mayor nivel de calidad más rápido que los comerciales” (Easttom, 2014).

Seguridad Empresarial

“La Seguridad Empresarial es un concepto ampliamente conocido, y aunque hasta la fecha de adolezca de una definición exacta, entre otros motivos por la variabilidad del modelo, la podemos entender como un conjunto de políticas, procedimientos y recursos humanos, organizativos y técnicos que son destinados a la protección de las personas, así como a los activos

tangibles e intangibles y a la reputación misma de cualquier organización". (Muñoz, 2016)

Seguridad de Redes Informáticas

A. Seguridad

Migga (2020), afirma que:

"La seguridad es un proceso continuo de protección de un objeto contra personas no autorizadas. Es como un estado de estar o sentirse protegido de cualquier daño. Ese objeto en ese estado puede ser una persona, una organización (como un negocio), o propiedad como un computadora (sistema o un archivo). La seguridad proviene de seguro, lo que significa, de acuerdo con el Diccionario Webster, un estado de estar libre de preocupaciones, ansiedad, o miedo".

También Migga (2020) menciona que, "este estado de seguridad se puede garantizar si los siguientes cuatro mecanismos de protección están en su lugar: disuasión, prevención, detección y respuesta.

- La disuasión, generalmente, es la primera línea de defensa contra los intrusos que pueden intentar acceder. Funciona creando una atmósfera destinada a asustar a los intrusos. A veces, esto puede implicar advertencias de graves consecuencias si la seguridad es violada.
- La prevención, básicamente, es el proceso de intentar evitar que los intrusos accedan a los recursos del sistema. Las barreras incluyen cortafuegos, zonas desmilitarizadas, DMZ, y el uso de elementos de acceso como claves, tarjetas de acceso, datos biométricos y otros para permitir que solo los usuarios autorizados utilicen y accedan a una instalación.
- La detección tiene lugar cuando el intruso ha conseguido o está a punto de conseguir acceso al sistema. Las señales del proceso de

detección incluyen alertas a la existencia de un intruso. A veces, estas alertas pueden ser en tiempo real o almacenarse para análisis adicional por parte del personal de seguridad.

- La respuesta es un mecanismo de secuelas que intenta responder a la falla del primeros tres mecanismos".

B. Seguridad Informática

Según Migga (2020), menciona que "es un estudio de la rama de informática, centrado en la creación de un entorno que ofrezca cierto nivel de seguridad para el uso de las computadoras. Se centra en el comportamiento de los usuarios y los protocolos necesarios para crear un entorno seguro para cualquiera que utilice computadoras. Este campo, por lo tanto, involucra cuatro áreas de interés: el estudio de la ética informática, el desarrollo de protocolos tanto de software como de hardware, y el desarrollo de mejores prácticas. Es un campo de estudio complejo que involucra diseños matemáticos detallados de protocolos criptográficos".

C. Objetivos Fundamentales de la Seguridad Informática

Según Van Oorschot (2020, pag. 21-23), "La seguridad informática es la práctica combinada de arte, ciencia e ingeniería de proteger activos relacionados con la computadora de acciones no autorizadas y sus consecuencias, ya sea previniendo tales acciones o detectando y luego recuperándose de ellas. La seguridad informática tiene como objetivo proteger los datos, el hardware y el software de las computadoras, además de las comunicaciones relacionadas a redes, dispositivos y elementos del mundo físico que controlan, desde mal uso intencional por partes no autorizadas, es decir, acceso o control por parte de entidades distintas a los propietarios legítimos o sus agentes autorizados. Mecanismos que protegen las computadoras contra involuntarios daños o errores, o que entran en las categorías de fiabilidad y redundancia".

“El objetivo general de la seguridad informática es respaldar los servicios informáticos proporcionando propiedades de seguridad que ayudan a cumplir las expectativas.

Principales propiedades de interés.

1) confidencialidad: la propiedad de la información no pública que permanece accesible solo para partes autorizadas, ya sean almacenadas (en reposo) o en tránsito (en movimiento). Esto es compatible por control de acceso (abajo), incluidos los mecanismos aplicados por un sistema operativo. A los medios técnicos comunes, el cifrado de datos, implican algoritmos criptográficos con clave; el acceso a una clave secreta permite la recuperación de información significativa a partir de datos cifrados.

La confidencialidad también se puede proporcionar por medios procedimentales, por ejemplo, al permitir medios de almacenamiento a los que solo puedan acceder físicamente las personas autorizadas.

2) integridad: propiedad de los datos, software o hardware que permanece inalterada, excepto por partes autorizadas. Si bien los códigos de detección y corrección de errores abordan algunos errores (incluso en hardware), controles de acceso y sumas de comprobación criptográficas es utilizado para combatir violaciones de integridad maliciosas. La integridad de las personas (para resistir el soborno, chantaje, coacción) es un uso diferente de esta palabra, pero está relacionado e importante.

3) autorización (acceso autorizado): propiedad de que los recursos informáticos sean accesibles solo por entidades autorizadas, por ejemplo, las aprobadas por el propietario del recurso o el dominio administrador. El acceso autorizado se logra a través de mecanismos de control de acceso, que restringen el acceso a dispositivos físicos, servicios de software e información.

4) disponibilidad: propiedad de la información, los servicios y los recursos informáticos restantes accesible para uso autorizado. Aparte de hardware y

software confiables, esto requiere protección contra la eliminación intencional y la interrupción, incluidos los ataques de denegación de servicio con el objetivo de abrumar los recursos".

"Al hablar de seguridad, los agentes que representan a los usuarios, las entidades comunicantes o el sistema los procesos se denominan principales". "Un principal tiene privilegios asociados que especifican los recursos autorizados a acceder. Por tanto, la identidad de un director es importante, pero se afirma las identidades deben ser verificadas. Esto conduce a los siguientes dos objetivos adicionales.

5) autenticación: garantía de que un principal, datos o software son genuinos en relación con las expectativas que surgen de las apariencias o el contexto. La autenticación de la entidad proporciona garantías que la identidad de un principal involucrado en una transacción es como se afirma; este apoyo"

D. Seguridad de la Red

Según Migga (2020), señala que "la seguridad de las redes informáticas es un estudio más amplio de la seguridad informática. Sigue siendo una rama de la informática, pero mucho más amplio que la de la seguridad informática".

"Se trata de crear un entorno en el que haya una red informática, incluidos todos sus recursos, que son muchos; todos los datos que contiene tanto en almacenamiento como en tránsito; y todos sus usuarios están seguros". "Debido a que es más amplio que la seguridad informática, este es un método más complejo del campo de estudio que la seguridad informática que involucra diseños matemáticos más detallados de protocolos y mejores prácticas criptográficas, de comunicación, transporte e intercambio".

E. Seguridad de la Información

Según Migga (2020), afirma que "la seguridad de la información es un campo de estudio aún mayor, incluida la seguridad informática y de redes informáticas. Este estudio se encuentra en una variedad de disciplinas,

incluidas ciencias de la computación, negocios administración, estudios de información e ingeniería. Involucra la creación de un estado en el que la información y los datos estén seguros. En este modelo, la información o los datos están en movimiento a través de los canales de comunicación o almacenados en bases de datos en un servidor. Esto, por tanto, implica el estudio no solo de diseños matemáticos más detallados de criptografía, comunicación, transporte, e intercambiar protocolos y mejores prácticas, pero también el estado de los datos y la información en movimiento".

Ciberataques

Para Prasad y Rohokale (2020):

"El ciberataque es un intento ilegítimo de obtener información o dinero beneficios. Aproximadamente, los ciberataques se clasifican como ataques basados en la web y ataques basados. Algunas personas consideran tres tipos de ciberataques como ataques naturales, meteduras de pata o errores humanos, y amenazas intencionales de personas internas o externas, piratas informáticos y ciberdelincuentes. Esta sección cubre varios ciberataques como puertas traseras, Ataque DoS, escuchas clandestinas, suplantación de identidad, manipulación, ataque de repudio, ataque de ingeniería, malware, adware, etc".

Tipos de ciberataques

A. Backdoors

"Evitar la entrada convencional a un sistema informático y creando una nueva entrada oculta para evadir las políticas de seguridad se denomina ataque de puerta trasera. En este ataque, el atacante instala software de registro de claves o cualquier otro software y a través del cual los atacantes obtienen acceso al sistema de víctimas. Es un ataque muy grave porque vía este se modifica archivos, información o instala software no deseado. Los famosos ataques de puerta trasera incluyen la exposición de interfaces de

administración y gestión, adición de características o funciones redundantes, creación de parámetros ocultos, usuarios redundantes, autorización para acceso de terceros, autenticación y autorización entre los componentes de la aplicación, explotar a los usuarios antiguos en el sistema para permitir fraude de identidad, endurecimiento defectuoso, exposición de datos de configuración y falta de aislamiento entre diferentes entornos". Simsolo (2016)

B. Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS)

"Los ataques DoS se aplican contra una disponibilidad. En este ataque, el atacante ataca al sistema para que el usuario real no pueda acceder a los datos o recursos durante este ataque. Eso niega al usuario real el uso de recursos y reduce los servicios del sistema durante el ataque. Generalmente en un ataque DoS, una sola máquina informática utiliza la conexión de internet para atacar el servidor de destino sobrecargando sus recursos como ancho de banda, búfer de conexión TCP, búfer de aplicación / servicio, ciclos de CPU, etc. Por su parte, la comunicación móvil también está sufriendo mucho debido a los ataques DoS. La mayoría de nodos móviles como teléfonos móviles; las laptops comparten los medios físicos que utilizan".

"El ataque DoS puede interrumpir la conexión móvil o la conexión a Internet inundando sus recursos. Allí hay varios tipos de ataques DoS, como ataque de inundación directo, control remoto ataque de red, ataque de inundación reflectante, virus, gusano, ataque de lágrima, protocolo ataque de violación, ataque de fragmentación, etc". (Prasad y Rohokale, 2020)

"Negación distribuida de ataque de servicio (DDoS) utiliza muchos dispositivos informáticos y una cantidad de conexiones a Internet para atacar una gran cantidad de servidores inundando sus recursos y cerrando abajo de ellos. Con el crecimiento de los servicios de IoT, la amenaza DDoS también

está aumentando. DDoS puede funcionar como una subparte de BOTNET al comprometer miles de servidores en un momento". (Neuman, 2000)

C. Escucha Pasiva

"En este ataque, el atacante escucha la conversación del sistema o la red sin su conocimiento y usa esa conversación para otro atacante o enemigo de ese organización. Es un tipo de ataque pasivo en el que el fisgón solo observa y roba la información que las computadoras, teléfonos inteligentes u otras entidades de la red son transmitiendo. Posteriormente, ayuda en ataques activos proporcionando toda la información necesaria sobre la red. Hay varios programas como Carnivore y Narus que proporcionan información que se puede utilizar para escuchar a escondidas. Las redes Wi-Fi públicas son los objetivos muy fáciles para los ataques de espionaje porque cualquiera puede unirse a la red contraseña fácilmente disponible. Escuchar a escondidas es una seria amenaza para el sensor inalámbrico redes e Internet de las cosas". (Prasad y Rohokale, 2020)

D. Suplantación

Liska (2003) afirma que "la suplantación de identidad es un ataque en el que el atacante o el programa actúan como si fueran un usuario legítimo de ese sistema o red. Ocultando la originalidad de la red y haciéndose pasar por el administrador del sistema o la víctima. Tales amenazas son frecuentemente iniciadas a través de correos electrónicos en los que se falsifica la dirección IP del remitente. Al robar y usar la identidad de otra persona, el atacante monitorea el tráfico de la red y registra la información para obtener información sobre nombres de usuario y contraseñas de los usuarios de la red. Tres tipos de ataques de suplantación son posibles, incluida la suplantación de ARP, la suplantación de IP y suplantación de DNS. La suplantación de IP se utiliza en ataques DoS y ataques man in the middle. El usuario nunca llega a saber

sobre el ataque de suplantación de identidad porque todos los paquetes son recibidos por el destinatario previsto".

E. Manipulación

"La manipulación es un ataque basado en web en el que el atacante cambia algunos parámetros en el URL del sitio web o ruta sin el conocimiento del usuario. La URL parece legítima para el usuario. Los piratas informáticos realizan manipulaciones para obtener acceso ilegal al sistema o información. Cuando se está recibiendo alguna información intercambiada entre el cliente y el servidor, que es manipulado por el pirata informático, la privacidad también se ve afectada al cambiar los detalles del usuario". (Prasad y Rohokale, 2020)

F. Adware

"El adware es un tipo de software que admite anuncios integrados en la propia aplicación mientras se ejecuta el programa. Es similar al malware, ya que utiliza anuncios para infligir virus mortales a las computadoras. Las ventanas emergentes aparecen continuamente en la pantalla donde el usuario está trabajando. Generalmente, el adware malicioso ingresa al sistema con programas y utilidades de software gratuitos descargado de Internet". (Prasad y Rohokale, 2020)

G. Ransomware

Smith (2017) asegura que "es un tipo de amenaza en la que los atacantes restringen el acceso de los usuarios al sistema y luego piden una cantidad para eliminar la restricción. Este rescate se paga en línea con diversos métodos de pago, después de los cuales el usuario puede acceder a ese servicio. Sistemas bloqueados con ransomware simplemente no se pueden desbloquear más que con la ayuda de un experto en seguridad. El ataque avanzado de ransomware cifra algunos archivos importantes en el sistema de la víctima y exige algún pago para descifrar y liberar los archivos. El 13 de

mayo de 2017, el ataque masivo de ransomware global WannaCry conmovió al mundo. Golpeó la salud centros de atención, industrias y oficinas gubernamentales de todo el mundo al tomar el control de los sistemas informáticos afectados hasta que las víctimas pagaran un rescate. El ransomware detuvo la propagación con el interruptor de apagado oculto dentro del código".

H. Spyware

"El software espía es un software que funciona como un agente secreto. El principal objetivo de los espías es recopilar la información con el uso de internet y sin el conocimiento del usuario. El software espía se puede encontrar en software gratuito que está disponible gratuitamente en Internet para todo el mundo. Cuando la víctima instala software gratuito, el software espía también se instala en el backend a través del cual el atacante obtiene la información del sistema de la víctima". (Prasad y Rohokale, 2020)

I. Scareware

"Scareware es un tipo de amenaza en la que los mensajes sugieren la descarga del software emergente en sistemas originales. El principal objetivo del Scareware es generar preocupación entre los usuarios o la víctima y provocarles que descarguen software irrelevante. Los cuadros de diálogo emergente parecen un cuadro de diálogo del sistema, pero no son lo mismo". (Prasad y Rohokale, 2020)

J. Phishing

"El phishing es una amenaza cibernética. El objetivo principal del phishing es obtener información confidencial como nombre de usuario, contraseña, detalles de la cuenta bancaria, etc. El atacante hace una copia idéntica de una página web original y luego se la envía a la víctima, la cual no puede identificar las diferencias porque tanto la página web falsa como la página web original, tienen el mismo aspecto". (Prasad y Rohokale, 2020)

K. Ataques de Contraseña

“El ataque de contraseña se realiza cuando un atacante desea conocer la contraseña de la víctima. Un atacante puede adivinar la contraseña o crear un programa que pueda adivinar la contraseña y lo prueba en el sistema mediante el método de fuerza bruta, o utiliza una base de datos que contiene una contraseña común y la prueba en el sistema o en los datos de inicio de sesión de cualquier sitio web”. (Prasad y Rohokale, 2020)

L. Ataques de Huella

Graves (2010) señala que “también es conocido como Footprinting, y es un proceso de elaboración de un mapa de la red o el sistema de una organización, en la cual se implanta la huella para recopilar información. Al principio, un atacante tiene que elegir un sistema de destino, aplicación o ubicación física. Una vez que el atacante conoce un sistema objetivo, él o ella pueden obtener información más específica del objetivo”.

“El objetivo principal del Footprinting es encontrar detalles como la arquitectura de la red, tipos de aplicación y servidor(es) donde se encuentran los datos o la información importante almacenada. Cuando un atacante ataca al objetivo, puede saber sobre el funcionamiento del sistema, su versión y tipo de aplicaciones, lo que facilita su ataque el objetivo”.

M. Escucha Telefónica

“Las escuchas telefónicas se realizan colocando un dispositivo de monitoreo a través de un mecanismo incorporado en una de las tecnologías de la comunicación utilizadas por la organización objetivo. Oficialmente, solo el personal autorizado puede acceder a conversaciones en vivo para monitorearlas o incluso grabarlas”.

“Los Packet Sniffers, son programas utilizados para capturar datos transmitidos en una red, son herramientas de escucha telefónica de uso

común. Varias otras herramientas, como los troyanos de escucha telefónica, se utilizan para diferentes aplicaciones". (Prasad y Rohokale, 2020)

N. Ingeniería Social

"La ingeniería social es un tipo de ataque no técnico que explota la mentalidad humana. Es un procedimiento para engañar a la persona y obtener la información del usuario que es útil para los atacantes. La ingeniería social se basa en la naturaleza humana para ganar la confianza de los demás". Graves (2010)

O. Rastreo de Paquetes

"El rastreo de paquetes se conoce como monitoreo de red o análisis de red. También puede ser utilizado por un administrador de red para monitorear y solucionar problemas de tráfico de red. El administrador de la red puede identificar los errores utilizando datos capturados que pueden ayudar a mantener una mejor transmisión o comunicación de la red". (Bradley, 2013)

"En el rastreo de paquetes, en palabras simples, se capturan todos los paquetes de datos en una red determinada. Una vez el paquete sin procesar es capturado, es analizado por el atacante. A través de los paquetes capturados, uno puede conocer la contraseña o los tokens de autenticación si se pasan en texto sin cifrar. Los piratas informáticos también pueden capturar paquetes para su uso posterior". (Prasad y Rohokale, 2020)

P. Vulnerabilidades de Contraseña

"Las contraseñas son la información clave que se necesita para acceder a un sistema. Los usuarios seleccionan contraseñas fáciles de adivinar, como número de teléfono móvil, fecha de nacimiento, nombre de mascota, etc. Debido a este factor humano, la mayoría de las veces, la adivinación de la contraseña tiene éxito si se identifica o se adivina fácilmente cierta información sobre el objetivo. Información que un hacker puede utilizar para

la recopilación o Footprinting y así adivinar la contraseña de un usuario". Graves (2010)

Q. Virus y Gusanos

"Se utilizan para infectar o modificar el contenido del sistema para que los espías puedan acceder de manera más fácil al sistema informático. Estos virus y gusanos actúan como portadores de troyanos y puertas traseras. Son los responsables de propagar la infección a gran escala. Por su parte, los gusanos tienen capacidad de autorreplicación y pueden propagarse rápidamente desde el sistema". (Prasad y Rohokale, 2020)

R. Bombas Lógicas

"Las bombas lógicas también se denominan código de escoria, son código de programación añadido al software de una aplicación o sistema operativo que permanece inactivo hasta que un evento ocurre, activando el código en acción. El software malintencionado también es desencadenado por la respuesta a cierto evento, cuando se alcanza una fecha u hora determinada. Las bombas lógicas esperan hasta que inicie sesión en el sitio web de la banca o redes sociales. Esto activa el registrador de teclas y envía a la víctima credenciales para el atacante remoto". (Prasad y Rohokale, 2020)

S. BOT y BOTNET

Según el Data Security Council of India (2011), "el bot no es más que un robot o una máquina con códigos de software autónomos integrados que le hacen comportarse de forma inteligente. Los BOT son utilizados por los espías para publicar automáticamente mensajes de spam en las páginas web abiertas por los usuarios".

"BOTNET es un grupo de sistemas de máquinas robot infectadas. Los BOTNET son principalmente utilizados para introducir ataques DDoS, para producir spam en grandes cantidades, para crear estafas de marketing en Internet, para robar números de serie de aplicaciones, ID de inicio de sesión,

y robar información confidencial, como números de tarjetas de crédito, etc". "Con el BOTNET, en una fracción de tiempo, una gran red de máquinas informáticas puede ser infectada o paralizada".

T. Troyanos

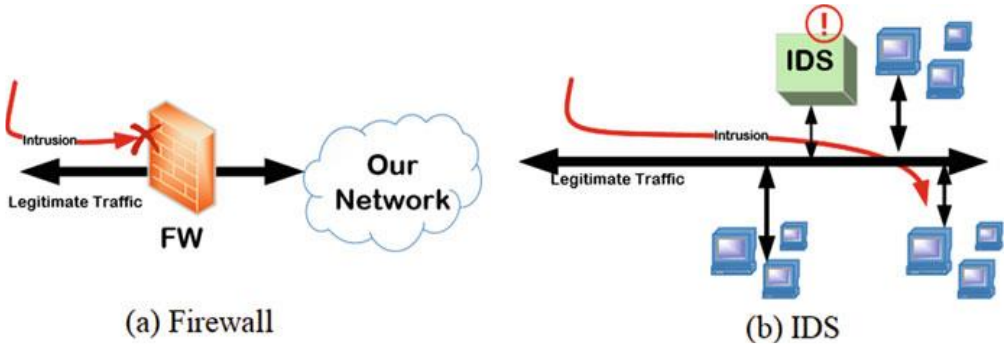
Dimitroya (2015) afirma que, "es un programa malicioso que enmascara una aplicación y toma control de la computadora o sistema de la víctima. A diferencia del verdadero virus, el caballo de Troya no se replica manteniendo a la víctima inconsciente del ataque. Este tipo de códigos maliciosos están ocultos dentro de algún archivo adjunto de correo normal o en algunos programas como juegos. Los ataques de caballo de Troya son los siguientes: Puerta trasera o remota, troyanos de acceso (RAT), kits de explotación, rootkits, troyanos de ransomware, banca troyanos, Troyanos DDoS y DoS, troyanos de descarga, etc".

Sistema de Detección de Intrusos (IDS)

Según Kwangjo et al. (2018), "un IDS se convierte en una medida de seguridad estándar en las redes informáticas. A diferencia de Firewall, los IDS generalmente se encuentran dentro de la red para monitorear todos los tráficos. Se puede considerar el uso de firewall e IDS para proteger la red de manera eficiente. IDS es un proceso autónomo definido de detección de intrusos que consiste en encontrar eventos de violación de políticas de seguridad o prácticas de seguridad estándar en redes informáticas. Además de identificar los incidentes de seguridad, los IDS también tienen otras funciones: documentar las amenazas existentes y disuadir a los adversarios. IDS requieren propiedades particulares que actúan como una contramedida pasiva, monitoreando solo en su totalidad o en parte de las redes, y tiene como objetivo una alta tasa de detección de ataques y una baja tasa de falsos tasa de alarma".

Figura 10

Gráfico descriptivo del uso conjunto de un IDS y un Firewall



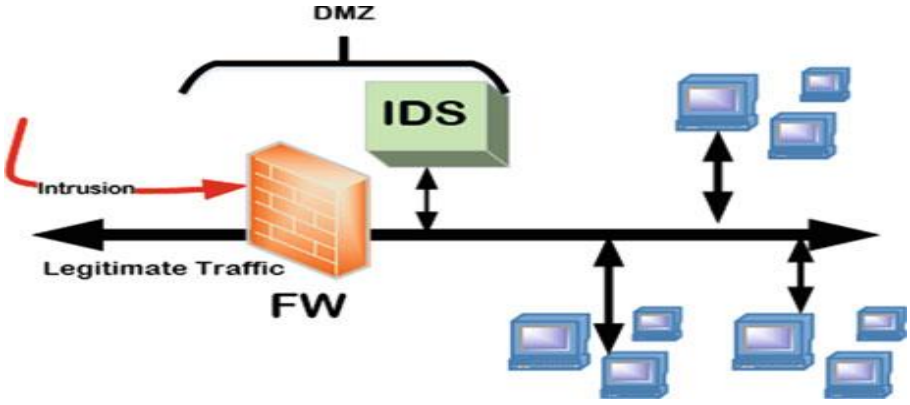
Nota. El gráfico nos muestra el uso de un IDS dentro de una red, y un Firewall actuando como filtro antes de "ingresar" a ella. Recuperado de: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

Clasificación IDS

Según Kwangjo et al. (2018), "podemos dividir los IDS según la ubicación y la metodología implementada en un la red. Por el posicionamiento del módulo IDS en la red, podríamos distinguir IDS en tres clases: IDS basados en red, basados en host e híbridos. El primer IDS, IDS basado en red, coloca el módulo IDS dentro de la red donde se puede monitorear todo. Este IDS comprueba si hay actividades maliciosas al inspeccionar todos los paquetes que se mueven a través de la red".

Figura 11

Gráfico descriptivo de un IDS basado en red

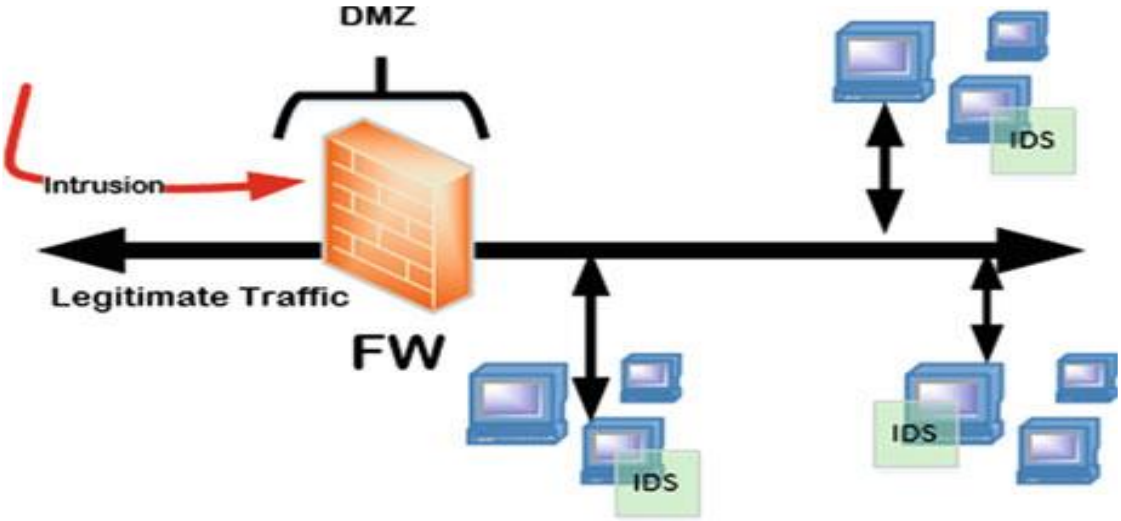


Nota. El gráfico nos muestra el uso de un IDS basado en red, el cual actúa inmediatamente después de pasar el filtro de firewall. Recuperado de: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

“Por otro lado, está el IDS basado en host que coloca el módulo IDS en cada cliente de la red. Los módulos examinan todos los tráficos entrantes y salientes del cliente correspondiente y conducen a un seguimiento detallado del cliente en particular. Hay dos tipos de IDS que tienen inconvenientes: el IDS basado en red puede sobrecargar la carga de trabajo y luego perder algunos actividades maliciosas, mientras que el IDS basado en host no monitorea toda el tráfico de red, teniendo menos carga de trabajo que el IDS basado en red”.

Figura 12

Gráfico descriptivo de un IDS basado en host

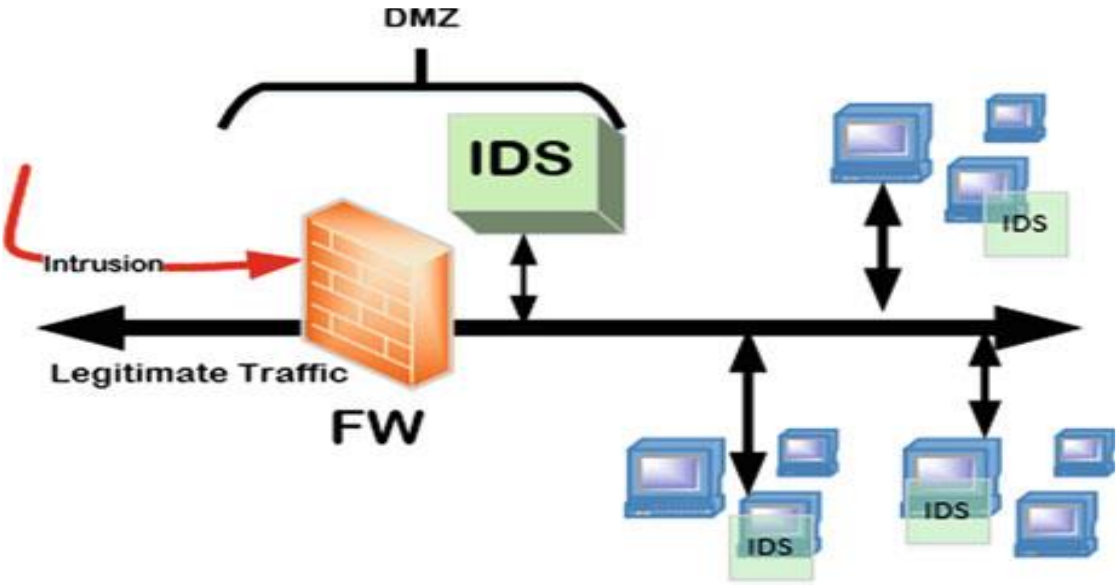


Nota. El gráfico nos muestra el uso de un IDS basado en host, el cual actúa de manera individual en cada cliente de una red. Recuperado de: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

“Por lo tanto, el IDS híbrido, coloca los módulos IDS en la red, así como los clientes para monitorear tanto clientes específicos como actividades de red al mismo tiempo”.

Figura 13

Gráfico descriptivo de un IDS de tipo híbrido



Nota. El gráfico nos muestra el uso de un IDS híbrido, combinando IDS de red e IDS basado en host. Recuperado de: https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

Según el método de detección, los IDS se pueden dividir en tres tipos diferentes:

"IDS basados en especificaciones, anomalías y mal uso. Un IDS basado en mal uso, conocido como IDS basado en firmas, busca cualquier actividad maliciosa al hacer coincidir las firmas conocidas o patrones de ataques con los tráficos monitoreados. Este IDS se adapta para detección de ataques conocidos; sin embargo, los ataques nuevos o desconocidos (también denominados como exploit día cero) son difíciles de detectar".

"Un IDS basado en anomalías detecta un ataque por perfilar el comportamiento normal y luego activa una alarma si hay alguna desviación de eso. La fuerza de este IDS es su capacidad para la detección de ataques desconocidos. Los IDS basados en mal uso generalmente logran un mayor rendimiento de detección de ataques conocidos que los IDS basado en anomalías".

"Un IDS basado en especificaciones define manualmente un conjunto de reglas y restricciones para expresar las operaciones normales. Cualquier desviación de las reglas y restricciones durante la ejecución se marca como maliciosa".

Modelo TCP/IP

Según Howser (2015), menciona que "el modelo TCP/IP es el protocolo de red más utilizado. Dado que ahora tiene un conocimiento firme del modelo OSI, mostraremos la correlación entre los modelos TCP/IP y OSI. Como se discutió, el modelo OSI tiene siete capas, y el protocolo TCP / IP tiene cuatro capas".

Según Migga (2020), "el modelo TCP/IP no coincide de manera exacta con el modelo OSI. Por ejemplo, tiene de dos a tres niveles menos que las siete capas del modelo OSI. Fue desarrollado para el Departamento de Defensa de EE. UU. a través de la Agencia de Proyectos de Investigación Avanzada (DARPA); sin embargo, a lo largo de los años, ha experimentado un crecimiento fenomenal en popularidad y ahora es el estándar de facto para Internet y muchas intranets. Consta de dos protocolos principales: el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP), de ahí la designación TCP/IP".

Modelo OSI

Según Carthern (2015), "el modelo OSI es un modelo conceptual, también conocido como modelo de siete capas, que fue establecido por la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones-Sector de Normalización de las Telecomunicaciones (UIT-T) para desarrollar elementos comunes en función de interfaz entre protocolos de comunicación".

“Es importante tener en cuenta que el modelo OSI no es una regla establecida, sino simplemente una guía de referencia para que los proveedores sigan y para que sus productos puedan interactuar entre sí”.

Según Howser (2020), “el modelo teórico más útil es el modelo OSI de siete capas introducido por el ISO en 1984. Este modelo es muy útil cuando se habla de problemas con los distintos servicios proporcionados por dispositivos en Internet, pero con una o dos excepciones, el modelo OSI completo rara vez se ha implementado. Mientras se desarrollaba el modelo, las instalaciones del sistema operativo UNIX estaban desarrollando un conjunto de protocolos para transferencia de archivos (FTP), acceso remoto mediante un terminal tonto (Telnet) y correo electrónico (SMTP). Este conjunto de servicios estaba destinado a ser útil en muchas redes usando TCP/IP. Como suele ocurrir en la industria informática, la costumbre superó la propuesta y TCP/IP se convirtió en el estándar de facto en Internet”.

El mismo autor señala que “el modelo OSI divide o agrupa las funciones de comunicación en siete capas lógicas: física, de datos enlace, red, transporte, sesión, presentación y aplicación. Cada capa soporta la capa superior, y es servido por el nivel debajo de él. Es importante tener en cuenta que el procesamiento es autónomo y transparente, a las otras capas. Las capas de aplicación, presentación y sesión definen cómo las aplicaciones dentro de las unidades se comunican entre sí y con los usuarios. Los ejemplos tradicionales de unidades terminales en una red son PC, servidores, impresoras y escáneres. Sin embargo, con la evolución de la Web de las cosas, incluso sus dispositivos y las bombillas pueden ser unidades finales”.

Puertos y Firewall

Puertos

Según Gutiérrez (2019), menciona que “los puertos son la entrada y salida de paquetes, es en estos que se corren lo que se llaman servicios, que son

aplicaciones que están haciendo uso de puerto para comunicar algo a otro sistema. Los puertos son extremadamente relevantes en el área del hacking, ya que pueden ser utilizados para obtener mucha información de un sistema, y prácticamente todos los ataques informáticos utilizan un puerto para realizar el ataque, o para comunicar información al haberse comprometido un sistema".

Firewall

"También conocidos en español como cortafuegos, o muro de fuego, representan uno de los principales mecanismos utilizados para preservar la seguridad de alto nivel. En el ámbito de la seguridad informática, se entenderá como fuego a cualquier amenaza que pudiera provenir de afuera de nuestro sistema o trate de salir del mismo. Es un sistema que revisa y previene los intentos de conexiones indeseados por parte de los equipos, desde y hacia la red. Sintetizando, vale esclarecer que un firewall puede ser tanto un recurso a nivel de hardware como de software; en otra palabras, se puede tener una máquina diseñada especialmente para esta función o emplear una aplicación que ha de ser instalada en uno de los equipos pertenecientes a nuestra red". (Seoani, 2014)

"Los muros de fuego pueden ser una herramienta eficaz para la protección de un sistema o red local, con respecto a las amenazas de seguridad que provengan de la red misma, a la vez que al mismo tiempo brindan acceso al exterior mediante redes de área ancha e Internet" (Stallings, 2004, pp. 376).

Según Migga (2020, pp. 251-252), "un cortafuegos es un recurso de hardware, una herramienta de software, o incluso la unión de ambos, que escanea y luego filtra los paquetes del tráfico que quiera salir o entrar de la red local a protegerse. Es un medio que divide una red con protección o parte de una red, y ahora cada vez más un dispositivo de usuario, de una red

desprotegida: la red defectuosa, como Internet. En muchos algunos casos, la red defectuosa puede incluso formar parte de la red de la empresa. Por definición, un firewall es una herramienta que proporciona un filtro de paquetes entrantes y salientes".

Tipos de Firewall

Según Migga (2020, pp. 254), "los cortafuegos se utilizan mucho para ofrecer servicios de seguridad de red. Esto ha resultado en un amplio repertorio de cortafuegos. Para comprender los diferentes tipos de firewalls, solo necesitamos mirar el tipo de servicios de seguridad que ofrecen en diferentes capas de la pila TCP/IP. Los muchos tipos de cortafuegos se clasifican según la capa de red: El primer tipo es el enrutador de inspección o filtrado de paquetes. El segundo tipo es la inspección de la aplicación o el servidor proxy".

A. Cortafuegos de Filtrado de Paquetes

Según Migga (2020, pp. 255-256), "el primer tipo de cortafuegos, son enrutadores que inspeccionan el contenido de las direcciones y puertos de origen o destino de TCP, UDP, UDP entrantes o salientes y paquetes ICMP que se envían entre redes; aceptan o rechazan el paquete según las políticas de paquetes específicas establecidas en la política de seguridad de la organización. Recordar que un enrutador es una máquina que reenvía paquetes entre dos o más redes. El enrutador de inspección de paquetes, por lo tanto, trabajando a nivel de red, está programado para comparar cada paquete con una lista de reglas establecidas de la política de seguridad de la organización, antes de decidir si se debe reenviar o no. Se permite que los datos salgan del sistema sólo si las reglas de los cortafuegos lo permiten".

B. Servidor Proxy de Aplicación: Basado en Filtrado Sobre Servicios Conocidos

Según Migga (2020, pp. 259-261), “un servidor proxy, a veces es solo un firewall de aplicaciones, es un servidor de máquina que se encuentra entre una aplicación cliente y el servidor que ofrece los servicios de la aplicación cliente puede querer. Se comporta como servidor para el cliente y como cliente para el servidor, por lo tanto, un proxy, que proporciona un nivel más alto de filtrado que el servidor de filtro de paquetes al examinar los flujos de datos de paquetes de aplicaciones individuales. Como cada flujo de datos entrante se examina, un proxy de aplicación apropiado, un programa, similar al sistema normal daemons, es generado por el servidor para esa aplicación en particular. El proxy inspecciona el flujo de datos y toma la decisión de reenviar, descartar o referir para una inspección más detallada. Cada uno de estos servidores especiales se denomina servidor proxy”.

“Un firewall proxy funciona interceptando primero una solicitud de un host en la red y luego pasarlo a su destino, generalmente Internet. Sin embargo, antes de pasarlo, el proxy reemplaza la dirección de origen IP en el paquete con su propia dirección IP y luego la transmite. Al recibir un paquete de una red externa, el proxy inspecciona el paquete, reemplaza su propia dirección IP de destino en el paquete con el del host interno y lo pasa al host interno. El interno host no sospecha que el paquete sea de un proxy”.

Protocolo

Según Zhao (2020), “protocolo es importante para conectar los productos. La comunicación IoT, los protocolos se pueden clasificar en algunos tipos, que son los siguientes: Primero, la red de sensores incluye WirelessHART, IEC 62591 (WirelessHART), ISA 100.11a, y Zigbee. En segundo lugar, la comunicación M2M incluye CoAP, OPC-UA, DDS y Modbus. En tercer lugar, la mensajería incluye MQTT, AMQP y XMPP. Cuarto, el de baja potencia, la

red de área amplia (LPWAN) incluye NB-IoT, Sigfox, LoRa y LoRaWAN. En quinto lugar, la red de área local inalámbrica (WLAN) incluye IEEE 802.11. En sexto lugar, la red de área personal inalámbrica (WPAN) incluye IEEE 802.15.4".

Los protocolos anteriores se describen a continuación.

A. Red de Área Local Inalámbrica (WLAN)

Según Zhao (2020), "es un sistema de transmisión de datos que Utiliza tecnología de radiofrecuencia (RF) para sustituir la red local existente de alambres de cobre trenzados (es decir, coaxiales) por ondas electromagnéticas para hacer la LAN con Wirelessness. Con una arquitectura de acceso simple, la red permite a los usuarios lograr el reino ideal de información y conveniencia".

B. Red de Área Personal Inalámbrica (WPAN)

Según Zhao (2020), "la tecnología de comunicación de la red de área personal inalámbrica (WPAN), utiliza conexión de comunicación inalámbrica. Recomendado por IEEE, existen tres tecnologías, que son 802.15 sobre la base de la tecnología Bluetooth, de alta frecuencia 802.15.3 (es decir, UWB) y 802.15.4 de baja frecuencia (es decir, Zigbee). WPAN está diseñado para realizar actividades dentro de un rango pequeño, comunicación inalámbrica emergente de negocios, tecnología de red con tipos enriquecidos, grupos específicos e inalámbricos y conexiones integradas".

C. Protocolo Extensible de Mensajería y Comunicación de Presencia (XMPP)

Según Zhao (2020), "el protocolo XMPP tiene una aplicación flexible para el desarrollo y escalable. Desarrollar aplicaciones o agregue nuevas funcionalidades fácilmente a los sistemas existentes del cliente, El protocolo XMPP en el lado del servidor permite que el servidor se comunique con otro.

XMPP define los roles de cliente, servidor y puerta de enlace. El servidor tiene las siguientes funcionalidades, como registrar la información del cliente, conectar la gestión, e información de enrutamiento. Para conectar sistemas heterogéneos de mensajería instantánea, se utiliza la puerta de enlace".

Linux

Para Membrey (2013):

"Linux es solo un kernel de sistema operativo, lo que significa que es capaz de administrar los bits y piezas de bajo nivel, tales como la manipulación de controladores de los diferentes dispositivos y sencillo acceso a las redes y los dispositivos de almacenamiento. En realidad, aquello que hace que Linux resulte muy útil, es todo el software que lo envuelve, pues este software es de código abierto y cualquiera puede armarlo de la forma que quiera".

Según Thomas y Channelle (2009), "Linux es un sistema operativo, lo que quiere decir que se parece un poco a Windows. Es el software central que ejecuta su computadora y le permite hacer cosas en ella. Como se mencionó anteriormente, según la definición más estricta del término, un sistema operativo es el software fundamental que es necesario para que su PC funcione".

Ventajas y desventajas de Linux

Según Villanueva (2021) las ventajas son las siguientes:

A. Es gratuito

"Es una de las ventajas más grandes que ofrece, debido a que evita que incurramos en costos excesivos de licencias que no siempre se utilizan completamente".

B. Es de código libre

“Además de la gratuidad, nos ofrece la ventaja de ser de código abierto, lo que significa que puede ser modificado según nuestras necesidades. Esto hace que pertenezca al ecosistema de software libre”.

C. Posee mucho software libre

“No solo el sistema operativo es gratuito y de código libre, sino que también mucho de los programas con los que viene, así como otros disponibles en el entorno Linux, son igual de gratuitos y open source”.

D. Tiene mayor estabilidad

“Es uno de sus puntos más fuerte por tener un rendimiento más estable. Debido a ello, Linux es uno de los sistemas operativos más elegidos por diversas empresas alrededor del mundo. Esta estabilidad le permite ser ideal a nivel de servidores en la nube debido a la confiabilidad que”.

E. No requiere muchos recursos

“En general, las distribuciones de Linux no requieren de muchos recursos hardware, por lo cual pueden ser instaladas en diversos equipos sin caer en costes adicionales por equipamiento”.

F. Posee buen entorno gráfico

“Así como existe variedad de software disponible para entorno Linux, también se dispone de múltiples soluciones desarrolladas por programadores expertos en el ámbito del entorno gráfico. En ese sentido, se puede afirmar que Linux también goza de muy buenos entornos gráficos en sus distribuciones”.

G. Distribuciones variadas

“Dada la variada cantidad de distribuciones de Linux, se tiene prácticamente una distribución para necesidad que se pueda tener según el usuario final. Lo cual lo convierte en una de sus principales ventajas”.

H. Es más seguro

“Linux se consolida como el sistema operativo más seguro debido a que, al estar en constante evolución, y al ser desarrollado por toda una comunidad, los ataques y vulnerabilidades se corrigen de un modo más rápido”.

I. No se requieren grandes conocimientos informáticos

“Al ser sustentado por una comunidad ampliamente especializada y participativa, siempre se contemplan todos los aspectos principales, entre ellos el de la facilidad de uso, lo cual lo convierte en una herramienta fácil de usar, sin la necesidad de conocimientos avanzados”.

Por otra parte, Villanueva (2021) también nos explica cuáles son las principales desventajas:

A. Incompatibilidad con Windows y otros sistemas

“Al poseer un kernel propio, muchas veces se generan problemas de compatibilidad con otros sistemas, lo cuales al ser más comerciales, de un modo u otro imponen sus productos en el mercado. Sin embargo, existen soluciones que, aunque no completas, presentan una salida ante tal situación”.

B. Carencia de soporte

“Al no ser tan comercial ni difundido en muchas regiones, muchos problemas que se presentan no siempre cuentan con soluciones fáciles de encontrar, quedando en la mayoría de los casos, la solución, a manos del usuario”.

C. Incompatibilidad con el hardware

“Es una falencia poco común, pero puede presentarse el caso en que algún dispositivo o componente externo no sea compatible con Linux, y por lo tanto quede sin operatividad”.

D. Incompatibilidad entre particiones

“Debido a la incompatibilidad existente entre sistemas, por tener cada uno un kernel propio, las particiones entre otros sistemas y Linux no son compatibles, en otras palabras, no se reconocen las particiones entre sistemas. Esto se convierte en una dificultad si se tienen instalados diferentes sistemas”.

E. Algunas veces se requiere de Unix

“Generalmente Linux es autosuficiente; sin embargo, a veces tendremos que utilizar a Unix para ciertas situaciones”.

F. Proveedores de internet que no dan soporte Linux

“Esta es una desventaja que no incluye a Linux de manera directa; sin embargo, se toma en consideración debido a que muchos proveedores de servicio de internet, conocidos como ISP, en ocasiones no dan soporte a problemas que no estén relacionados, por ejemplo, con Windows”.

G. Escaso software comercial

“Así como Linux posee una variedad de software libre y gratuito, por otra parte carece de software comercial, lo que algunas veces evita que se puedan ubicar soluciones comerciales según requerimientos del usuario”.

H. Algunas limitaciones para videojuegos

“Para alguien inmerso en el mundo de los videojuegos, es posible que sus necesidades no acaben completamente satisfechas en un entorno Linux, y esto es debido al hecho de que tratamos con un sistema operativo orientado a ser liviano, que evita consumir demasiados recursos, todo lo opuesto a lo que acontece con los videojuegos más poderosos, los cuales necesitan máquinas de última generación”.

Ubuntu

Pérez (s.f.) afirma que:

"El sistema operativo Ubuntu se encuentra en el ámbito del software libre, este sistema se basa en GNU/Linux, siendo un sistema relativamente nuevo, pues se creó a inicios del año 2004, versión denominada Warty Warthong. Esta versión de Linux se basó en otra de ellas llamada Debian".

Por su parte, Stallman (2004) indica que:

"El primer sistema operativo en asumir el compromiso de realizar lanzamientos programados con una cadencia predictible, de seis meses, fue Ubuntu, y lo hizo desde octubre de 2004. Ya en el año 2006, se decidió que cada cuarta entrega, realizada luego de dos años, reciba soporte en el largo plazo para todas las implementaciones que se suscitaran de manera masiva. Así surgió la denominación LTS para todas las emisiones estables y mantenidas".

Máquina virtual

Ramírez (2020) señala, con respecto a las máquinas virtuales, que:

"Una vez aclarado que máquina virtual no es en realidad una máquina física llena de engranajes, para nada, que contenga un casco de realidad virtual, sino líneas de código, software, se puede entrar detalle sobre qué son en realidad".

"En primer lugar se debe saber que existen dos tipos de máquinas virtuales cuya diferencia es la funcionalidad que poseen: las máquinas de sistema y las otras que son de proceso. En ese sentido, la mayoría de veces cuando se habla de máquina virtual, se hace alusión a una máquina de sistema".

Máquinas virtuales de sistema

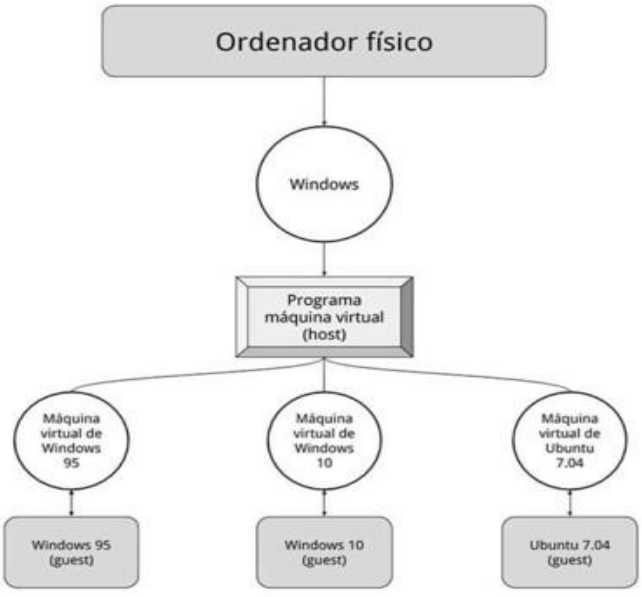
"En este tipo definimos a aquella que simula a una computadora completa. En otras palabras, es un programa que se puede hacer pasar por un dispositivo real, de tal manera que se puede ejecutar otro sistema operativo en su interior. Asimismo, cuenta con sus propios recursos, tal cual fuera una

máquina física, por lo que posee almacenamiento, velocidad de procesamiento, tarjeta gráfica y demás componentes de hardware, aunque todos ellos son virtualizados".

"Que sean virtuales los componentes, no necesariamente significa que no existan. Por poner ejemplo, una máquina virtual puede contener algunos recursos reservados de 4 GB de RAM y 50 GB de almacenamiento, que efectivamente tienen que conseguirse de algún lugar: en este caso, de la computadora física donde se ha instalado la máquina virtual. También se le conoce como host, hipervisor o simplemente anfitrión. Existen otros dispositivos que realmente podrían no existir físicamente, como por ejemplo un CD que en verdad es el contenido de alguna imagen de tipo ISO en lugar de un lector real".

Figura 14

Gráfico descriptivo de un ordenador virtual de sistema



Nota. El gráfico describe la estructura virtual de trabajo de un ordenador (computador) físico. Recuperado de: https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

“Para poder funcionar, la máquina virtual realiza un mapeo de los dispositivos virtuales que puede ofrecer al usuario con base en todos los dispositivos existentes en la máquina física. Por ejemplo, la máquina puede venir simulando una tarjeta de sonido, aunque realmente está conectada con la tarjeta de sonido existente en la placa base de la PC original”.

“El trabajo de virtualización se puede realizar mediante software o con ayuda de algún hardware. En tal caso se logra conseguir un mayor desempeño. En vista a ello, a partir del año 2005 es casi común que las computadoras cuenten con procesadores capaces de realizar dicha función”.

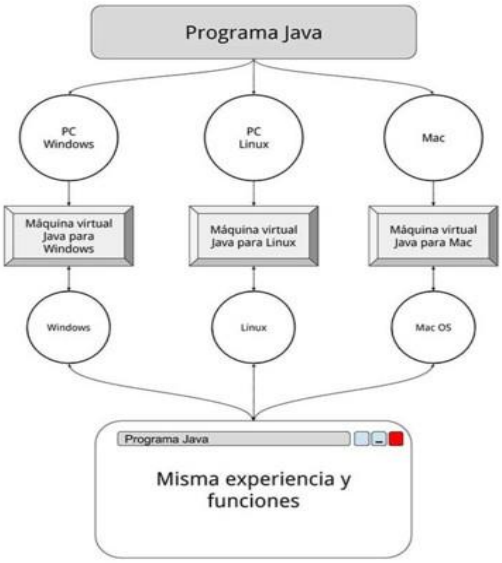
Máquinas virtuales de proceso

“Para este tipo de máquinas, las de proceso, se aprecia menor complejidad con respecto a las de sistema; ya que en lugar de simular un equipo en su totalidad, se encarga de ejecutar todo un proceso en específico, como un programa, en su entorno de ejecución”.

“Esta característica resulta de mucha ayuda al momento de implementar aplicaciones para distintas plataformas, pues en lugar de vernos obligados a programar de manera específica para cada sistema, el ecosistema de trabajo, la máquina virtual, es el encargado de interactuar con el sistema operativo”.

Figura 15

Gráfico descriptivo de un ordenador virtual de proceso



Nota. El gráfico describe la estructura virtual de trabajo de un ordenador de proceso (simula la máquina virtual de Java). Recuperado de: https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

"Las máquinas virtuales de este tipo, nos brindar la oportunidad de urilizar aplicaciones que se comportan de igual manera en plataformas muy diferentes como Linux, Windows o MacOS; sin embargo, a nivel de usuario, no se percibirán de manera muy detallada los cambios; debido a ello, salvo excepciones de uso, al hablar de máquinas virtuales nos referimos a las máquinas virtuales de sistema".

Usos de las máquinas virtuales

A. Posibilidad de experimentar con diversos sistemas operativos.

"Esta opción nos da la facilidad de evitar una instalación tediosa de cualquier sistema operativo, haciendo este proceso más fácil y rápido de lo que se haría normalmente en una máquina convencional. De este modo, cuando haya alguna nueva versión de algún sistema operativo cualquiera, es más fácil y seguro hacer las pruebas mediante el uso de una máquina virtual, evitando

exponer nuestros recursos a nivel de software y hardware. Si en el proceso surge algún error, nos basta con eliminar la máquina virtual y no se requiere mayor inversión de tiempo o correr riesgos a nivel de nuestros datos”

B. Hacer correr programas antiguos.

“Supongamos que, como sucede muchas veces, dependemos de un software desfasado, que por diversos motivos no podemos reemplazar y se torna una dificultad con la que lidiar de manera constante. En tal situación, cuando no se pueda hacer dicho reemplazo o la actualización del software, no hay más opción que seguir usando dicho sistema con el sistema operativo con el que sea compatible además del software que requiera, también desfasado. Ante esto, una salida viable sería el uso de una máquina virtual, en la cual podemos instalar el sistema compatible, sin la necesidad de algún equipo adicional más que el host de la máquina”.

C. Permite utilizar aplicaciones de otros sistemas.

“Es posible que en algún momento se requiera una máquina virtual para hacer correr aplicaciones que fueron desarrolladas para otros sistemas diferentes al que se emplea. Como cuando se utiliza Linux para usar una aplicación desde MacOS, o viceversa”.

D. Para testear un aplicativo en múltiples sistemas.

“Como desarrollador de alguna aplicación vas a necesitar que esta actúe de manera correcta en la mayor cantidad de configuraciones que sean posibles, esto también incluye múltiples versiones de los sistemas operativos. Ante esto, una alternativa es tener varias máquinas virtuales con diversos sistemas, o un sistema operativo con múltiples en cada máquina”.

E. Como medio adicional de seguridad.

"Al tener una máquina virtual aislada del resto, esta te proporciona un nivel adicional de seguridad en cuanto a la ejecución de tareas precisas, pues son aquellas en las que se tiene que estar seguro de que algún aplicativo no tendrá opción de acceder al resto de los datos. Debido a esto es que se suelen emplear para realizar tareas muy peligrosas como la instalación de virus y otros software con motivo de estudio".

F. Para sacar provecho su gran dinamicidad.

"Dada su naturaleza no física las máquinas virtuales resultan muy útiles en múltiples ocasiones en donde se necesita una gran dinamicidad y versatilidad a nivel de sistema operativo. Se pueden guardar respaldos, como copias de seguridad o backups, extenderlas, o cambiarlas a un hardware completamente distinto y seguirán en funcionamiento sin presentar problemas. Debido a esto son de gran importancia, por ejemplo, en empresas que cuenten con servidores de tipo web que albergan una gran de máquinas, cada una con todas las páginas web de sus clientes".

VMWare

"Es entorno de virtualización a través de software para las arquitecturas de 32 bits, en ella se simula una computadora física con algunas especificaciones de hardware determinadas y brinda un ecosistema de ejecución muy parecido a todos los efectos de una máquina real, a excepción del acceso físico a su hardware". EcuRed (s.f.)

Para Castillo (2018):

"Sin duda alguna, VMware es la plataforma de virtualización número uno en el mercado actual. Esta compañía se ha perfeccionado a la vez que ha ido ampliando a través de los años su conjunto de herramientas de virtualización, lo que la ubica sin lugar a dudas como unos de los líderes en este mercado.

VMWare posee aplicaciones orientadas a toda clase de funciones: servidores, programas, virtualización de recursos de hardware, aplicaciones empresariales, domésticas y demás relacionadas. La gran mayoría de sus herramientas cuentan con una licencia de pago, aunque, como en otros casos, nos dejará usarlas por medio de una versión de prueba gratis durante un tiempo determinado".

Características VMWare

Velasco (2017) indica que:

"Las características más resaltantes, ofrecidas por VMware Worskstation, son las siguientes:

A. Posee diversas herramientas y múltiples funciones para entornos a nivel de empresas.

B. Posibilita trabajar con archivos compartidos de manera fácil entre el sistema virtualizado y el host.

C. Tiene compatibilidad con los lectores de Smart Cards.

D. Es compatible USB versión 3.0.

E. Permite la realización de copias de seguridad para casos de respaldo de estado de máquinas virtuales.

F. Posee una herramienta específica para compartir MV.

G. Tiene capacidad de integración con ESXi/vSphere y vCloud Air.

H. Posee gráficos 3D de compatibilidad con OpenGL y DirectX 10".

"Además de lo mencionado, la mayoría de sus funciones no necesitan agregar configuración alguna como sí sucede en el caso de otras herramientas, como, por ejemplo, realizar la configuración de una y una impresora. Otra característica muy interesante son los Linked Clones, que representan una función que posibilita la creación de una máquina virtual sin ser copiada completamente, ahorrando una gran cantidad de espacio".

Población

Para Chávez (2007):

"La población es el universo de estudio de la investigación, sobre el cual se pretende generalizar los resultados, constituida por características o estratos que le permiten distinguir los sujetos, unos de otros".

Según Tamayo y Tamayo (1997), "la población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación".

Lepkowski (Como se citó en Hernández Sampieri, Fernández y Baptista, 2014) menciona que una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones.

Muestra

"No siempre, pero en la mayoría de las situaciones sí realizamos el estudio en una muestra. Sólo cuando queremos efectuar un censo debemos incluir todos los casos (personas, animales, plantas, objetos) del universo o la población" (Hernández Sampieri et al., 2014).

CAPÍTULO III

Metodología de la investigación

3.1 Tipo y nivel de investigación

A. Tipo de investigación

De acuerdo a Hernández, Fernández y Baptista (2014), “la Investigación aplicada se distingue por tener propósitos prácticos inmediatos definidos, es decir, se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad. Para realizar investigaciones aplicadas es muy importante contar con el aporte de las teorías científicas, que son producidas por la investigación básica y sustantiva". Por esta consideración el tipo de investigación es aplicada.

B. Nivel de investigación

De acuerdo al autor Hernández Sampieri et. al (2014), "los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis. Una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de dicho objeto; y agrega La investigación descriptiva es uno de los tipos o procedimientos investigativos más populares y utilizados por los principiantes en la actividad investigativa. Los trabajos de grado, en los pregrados y en muchas maestrías, son estudios de carácter eminentemente descriptivo. En tales estudios se muestran, narran, reseñan o identifican hechos, situaciones, rasgos característicos de un objeto de estudio, o se diseñan productos, modelos, prototipos, guías, etcétera”.

De acuerdo con Carrasco (2019), señala que, “la investigación descriptiva se soporta principalmente en técnicas como la encuesta, la entrevista, la observación y revisión documental. Este tipo de investigación estudia, analiza, describe y especifica situaciones y propiedades de personas, grupos, comunidades o cualquier otro fenómeno u objeto que sea sometido al análisis. Por esta consideración el nivel de investigación es descriptivo”.

3.2 Diseño de investigación

De acuerdo con el autor Hernández Sampieri et. al. (2014), se puede definir la investigación no experimental, “como aquella investigación que se realiza sin manipular deliberadamente las variables, se trata de estudios donde no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para posteriormente analizarlos” (p. 191).

“El diseño de investigación transversal descriptivo, se empela para analizar y conocer las características, cualidades internas y externas, propiedades y rasgos esenciales de los hechos y fenómenos de un hecho realizado a momento determinado del tiempo. De acuerdo a Hernández et. al. (2014), una investigación de diseño transversal es cuando se recolectan datos en un solo momento o en un tiempo único y su propósito es describir variables y analizar los hechos tal como se dan. Los instrumentos de recolección de datos, son usados durante el proceso de forma única”. (Carrasco, 2019)

“En esta investigación se tienen que conocer e interpretar diversos procesos y características, así como estudiar rasgos y poder entender distintas funcionalidades para encontrar los datos necesarios para la construcción modelo operativo; debido a ello, el diseño de la presente investigación es no experimental de tipo transversal descriptivo”.

3.3 Hipótesis de la investigación

“No en todas las investigaciones cuantitativas se planean hipótesis. El hecho de formulemos o no hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas que formulan hipótesis son aquellas cuyo planteamiento define que su alcance será correlacional o explicativo, o en las que tienen un alcance descriptivo, pero que intentan pronosticar una cifra o un hecho” (Hernández, Baptista y Collado, 2014, p. 104). “Las investigaciones de tipo descriptivo no requieren formular hipótesis; es suficiente plantear algunas preguntas de investigación que, como ya se anotó, surgen del planteamiento del problema, de los objetivos y, por supuesto, del marco teórico que soporta el estudio” (Bernal, 2010, p. 136). La investigación que se desarrollara es de tipo descriptivo, por lo que no se

pretende pronosticar, hallar o verificar lo planteado en los objetivos, se optó por no plantear hipótesis.

3.4 Población y muestra

A. Población

Todos los cortafuegos a nivel de filtrado de paquetes en entornos Open Source.

B. Muestra

Cortafuego Nftables basado en el kernel de Linux.

3.5 Definición conceptual de las variables

Variable de estudio 1

a. Nftables.

"Nftables es una combinación de diversos elementos en el kernel de Linux, y representan una gran utilidad a nivel de línea de comandos en la interfaz de usuario" (Magnus, 2009)

Dimensiones

a. Ipv4.

"La dirección IPv4 es una cantidad numérica con longitud de 32 bits mediante la que se puede identificar de modo único una interfaz de red en cualquier sistema, el cual se basa en dígitos decimales, y se desglosa en cuatro entradas de 8 bits cada uno, separados por puntos". (IANA, 2021)

b. ARP.

"Se traduce al español como protocolo de resolución de direcciones, y es un protocolo utilizado por el protocolo de la capa de red del protocolo de internet, IP. Para poder definir las direcciones de red IP a las direcciones de hardware empleadas por un protocolo de enlace de datos". (Universidad de Aberdeen, 2019)

c. Ethernet

"Es la tecnología tradicional para conectar dispositivos en una red de área local o una red de área amplia por cable, lo que les permite comunicarse entre sí a través de un protocolo". (Burke, 2021)

Variables de estudio 2

a. Filtrado de paquetes.

"Cuando el tráfico de red atraviesa una interfaz configurada con ACL, el router compara la información dentro del paquete con cada ACE para determinar si el paquete coincide con una de las ACE. Este proceso se denomina filtrado de paquetes". (Interpolados, 2017)

Dimensiones

a. Open Source.

"Inicialmente fue un término que hacía referencia al software de código abierto. Siendo dicho software un código elaborado con el propósito de ser de acceso libre al público; es decir, cualquier usuario puede trabajr a libre albedrío con el código según sus necesidades". (Redhat, 2021)

3.6 Definición operacional de las variables

Variable de estudio 1

a. Nftables.

Dimensiones

a. Ipv4.

b. ARP.

c. Ethernet.

Variables de estudio 2

a. Filtrado de paquetes.

Dimensiones

a. Open Source.

3.7 Técnicas e instrumentos

A. Técnicas e instrumentos de recolección de datos

Técnicas. Análisis documental.

Instrumentos. Entrevista a expertos.

B. Técnicas de procesamiento y análisis de datos

Procesamiento en hojas de cálculo Excel. Análisis mediante estadística descriptiva.

CAPÍTULO IV

Implementación del cortafuego (firewall) con Nftables en la entidad

4.1 Antecedentes de la entidad

La Dirección Regional de Educación de Ayacucho - DREA, entidad de ámbito regional, y de carácter público, se fundó en el año 1970, bajo el D.S. N° 036 emitido el 31 de diciembre de 1969.

“Tiene por finalidad regir conducción del sector educación, a nivel regional, en el marco de las políticas nacionales y sectoriales. En ese sentido, entre otras, cumple las siguientes funciones: Aplicar, ejecutar la política educativa nacional emitida por el MINEDU y evaluar su implementación en la jurisdicción de Ayacucho; diseñar y proponer al MINEDU, planes de intervención en Ayacucho, en concordancia con la política educativa nacional; supervisar los servicios brindados por las UGEL de Ayacucho referidos a la educación básica y técnico-productiva, en concordancia con la política educativa nacional emitida por el MINEDU, etc.” (DREA, s.f.)

4.1.1 Estructura organizacional

La entidad presenta una estructura organizacional de tipo vertical, que consta de cinco (05) órganos de línea:

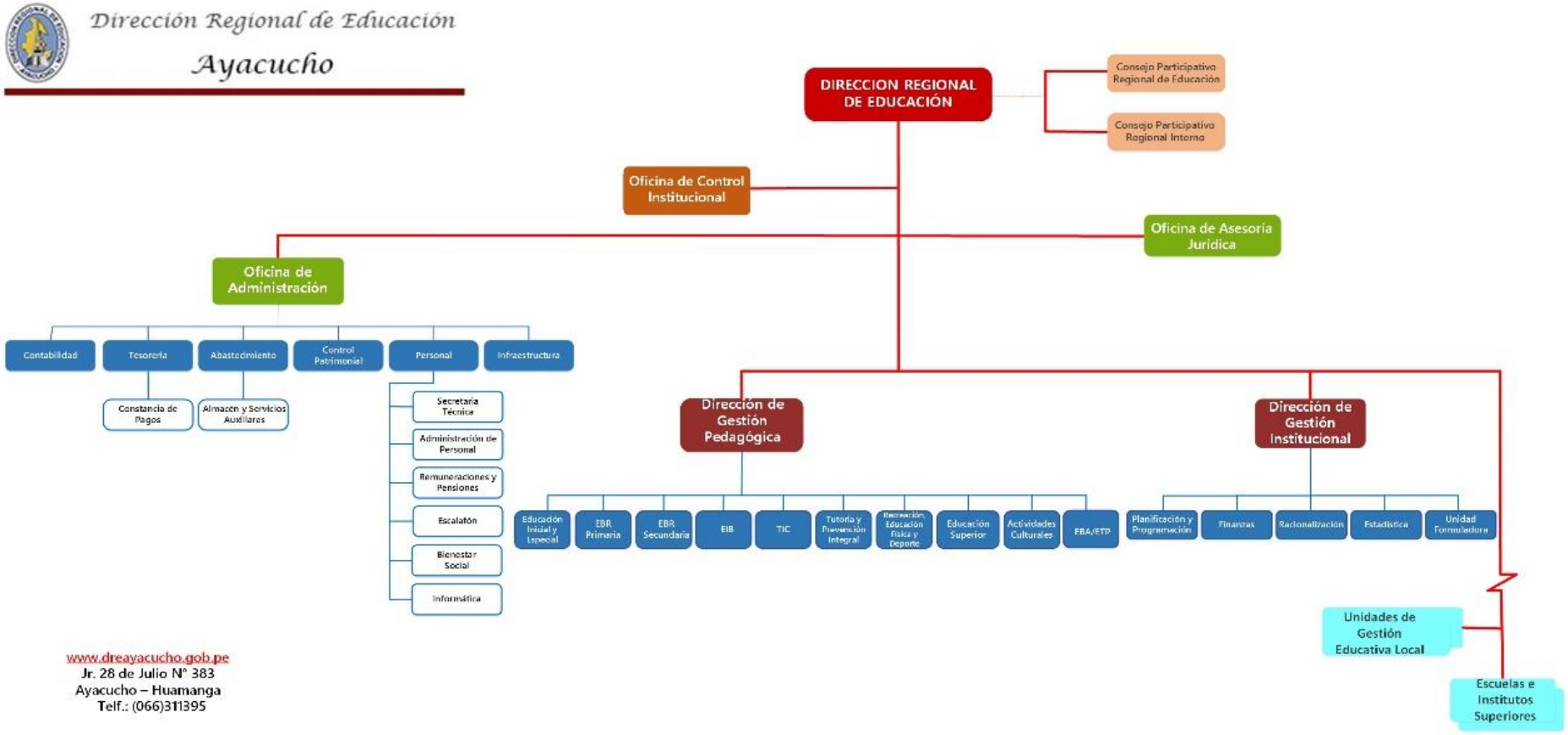
a) Dirección,
b) Dirección de Administración,
c) Órgano de Control Institucional,
d) Dirección de Gestión Pedagógica y
e) Dirección de Gestión Institucional.

Por su parte, la Oficina de Informática, cuenta como órgano apoyo, recibiendo su personal la denominación de Equipo de Informática, estando conformada por dos (02) personas. Jerárquicamente, la secuencia es: Dirección General - Dirección de Administración – Área de Personal – Oficina de Informática.

Debido a esa dependencia jerárquica, se genera una dependencia del tipo económico, siendo el principal limitante para temas de innovación y/o mejora en cuanto a temas de tecnología y seguridad informática.

Figura 16

Organigrama institucional de la Dirección Regional de Educación de Ayacucho



4.1.2 Situación actual de la red institucional

Maneja una topología en estrella, centrada en un router principal, al cual están conectados directamente los servidores principales, así como los router secundarios, los cuales brindan la conexión a los demás equipos de la red.

Se encuentra en estado vulnerable, carece de planos de la red misma, y no cuenta con una estructura definida, toda vez que la mayor parte del cableado fue realizado de manera inadecuada y de manera gradual.

Por su parte, recibe datos a través de un equipo Mikrotik, el cual, si bien es configurable, es propiedad del proveedor de acceso a internet, lo cual deja a la red vulnerable por carecer de un medio propio bajo su administración que le permita realizar las configuraciones de seguridad según sus requerimientos.

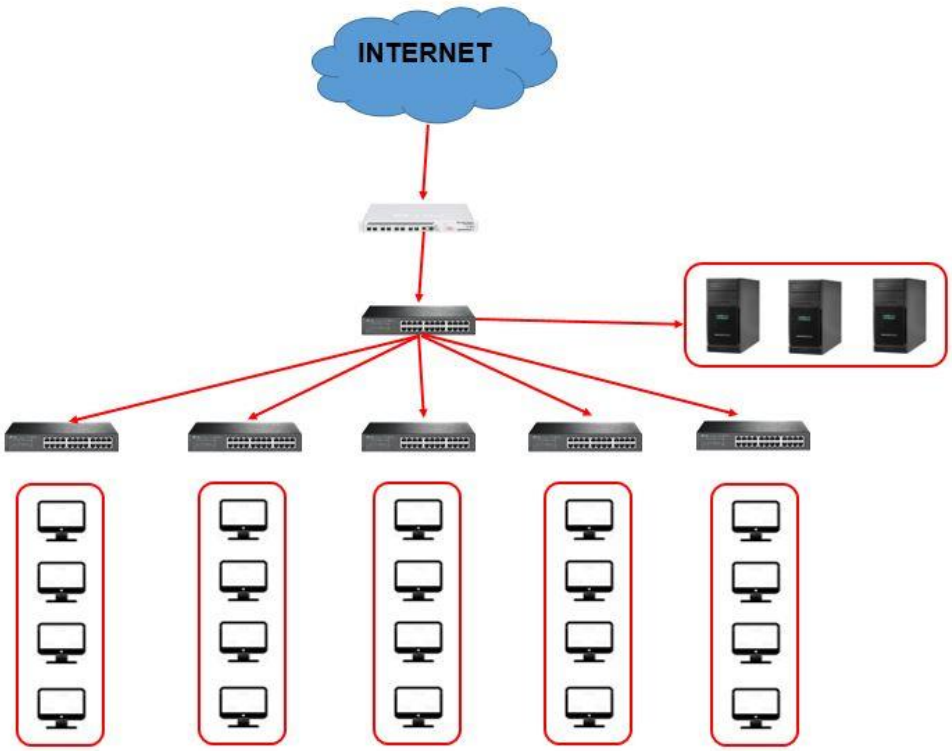
4.2 Diseño actual de la estructura de red basada en Cortafuego tradicional

Según la estructura actual, se percibe la distribución descrita de los equipos, con una topología en estrella, centrada en un solo equipo, a partir del cual se realiza la interconexión de la red. Se puede advertir que, al no contar con un filtro dedicado, toda la red queda vulnerable a las amenazas existentes a nivel interno y externo.

Por otra parte, se constata la dependencia del equipo mikrotik para el filtrado de paquetes, el cual, al no ser propiedad de la entidad, no se puede configurar de acuerdo a las necesidades existentes, quedando sin mayor utilidad que la de brindar el servicio de acceso a internet.

Figura 17

Diseño actual de la estructura de red



Nota. La imagen muestra la topología en “estrella” existente en la entidad. Elaboración propia.

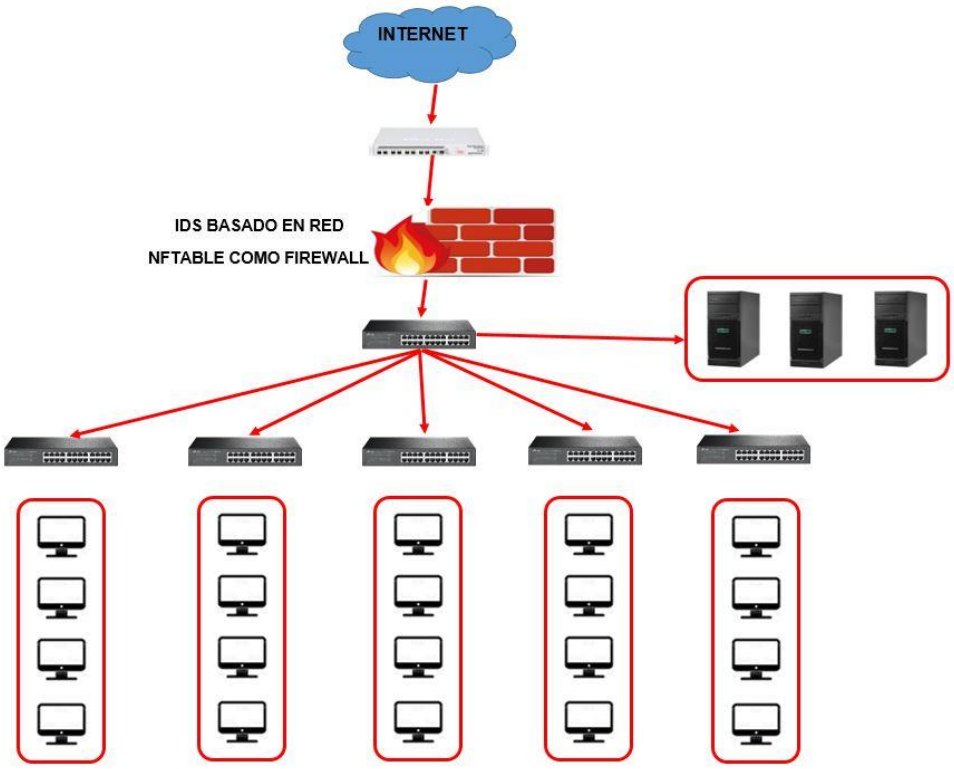
4.3 Diseño propuesto de la estructura de red basada en Cortafuego Nftables

A fin de brindar un medio de protección fiable, fácil de configurar y propio, se propone la configuración de Nftables como firewall en la red, asumiendo el rol de un IDS que garantice seguridad a nivel comunicativo de dicha red. Así, al lograr configurar el firewall, se tiene un medio no solamente propio, sino también alternativo para hacer frente a las amenazas internas y externas existentes.

Para tal objetivo, se propone la implementación bajo el esquema de ***IDS basado en red***, el cual actúa como filtro ante paquetes de información provenientes de fuera de la red, a la vez que realiza el filtrado de paquetes en la comunicación a nivel interno, otorgando protección a los terminales comunes y los servidores.

Figura 18

Diseño propuesto para la estructura de red



Nota. Descripción de la propuesta, con enfoque de IDS basado en red. Actúa a nivel interno y externo. Elaboración propia.

4.4 Configuración del IDS como Cortafuego Nftables

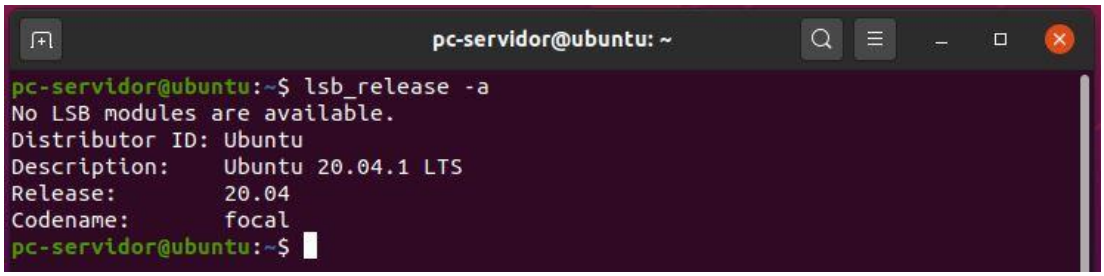
4.4.1 Instalación de Nftables en entorno Linux

Antes de proceder a instalar Nftables, tenemos que instalar el sistema operativo en el cual vamos a realizar la implementación del firewall.

Dado que el entorno de trabajo debe ser de naturaleza open source, se vio por conveniente la instalación del sistema operativo Linux Ubuntu 20.04. En ese sentido, una vez realizada la instalación del sistema, se ingresa en la terminal el comando ***lsb_release –a***, a fin de verificar que, efectivamente, se trata de dicho sistema operativo y es reconocido por el intérprete de comandos.

Figura 19

Uso de comando lsb_release –a para verificación de instalación

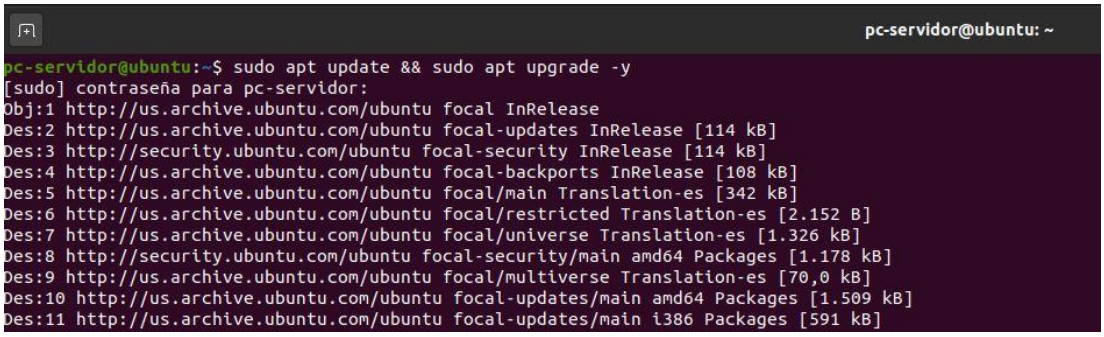


El siguiente paso previo antes de instalar nftables es actualizar el sistema operativo instalado, con la finalidad de obtener las últimas características de seguridad del sistema, así como otras funcionalidades que pudieran ser útiles para los objetivos planteados.

Para tal efecto, ingresamos en la terminal el comando ***sudo apt update && sudo apt upgrade –y***, lo cual iniciará la descarga e instalación automática de las actualizaciones más recientes.

Figura 20

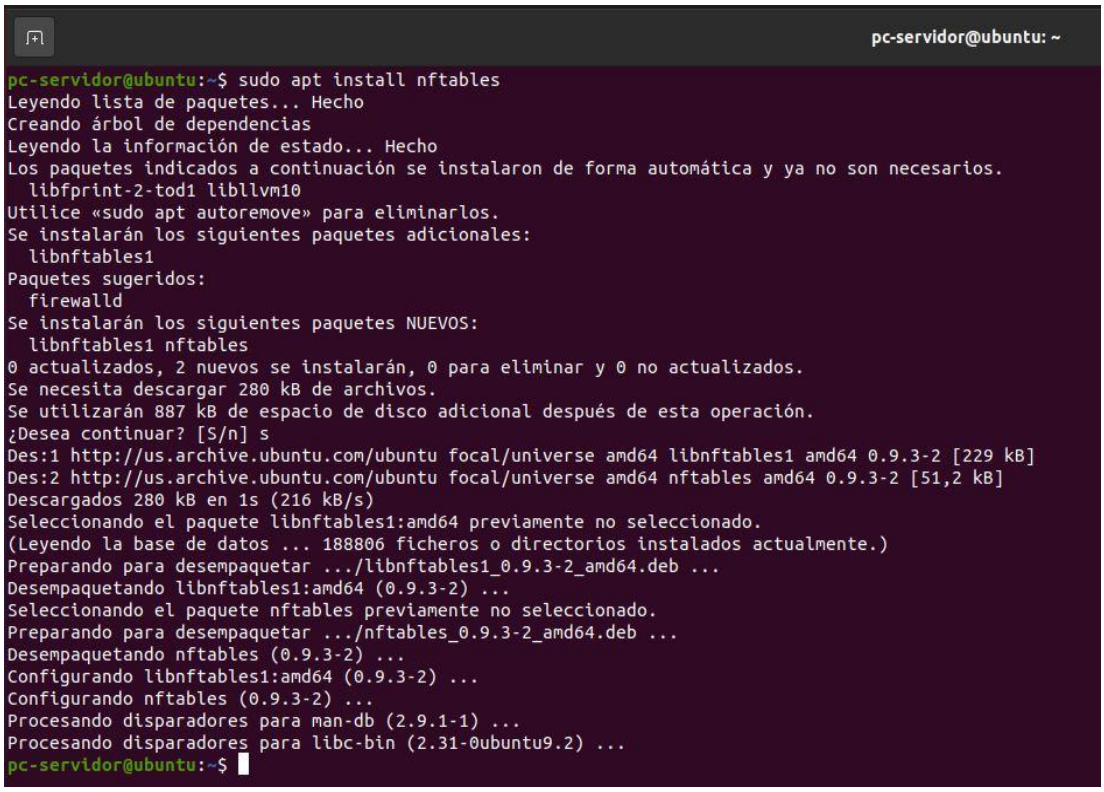
Actualización del sistema operativo Ubuntu 20.04



Tras haber culminado la parte previa de requisitos para nftables, procedemos a insertar el comando ***sudo apt install nftables***, para poder obtener la configuración de sus librerías, así como la máquina virtual para la traducción de instrucciones con las cuales se generarán los medios de seguridad. Procedemos con la instalación propiamente dicha, la cual se da de manera automática, previa confirmación por parte del usuario (con privilegios de administrador).

Figura 21

Instalación de nftables mediante comando sudo apt install nftables



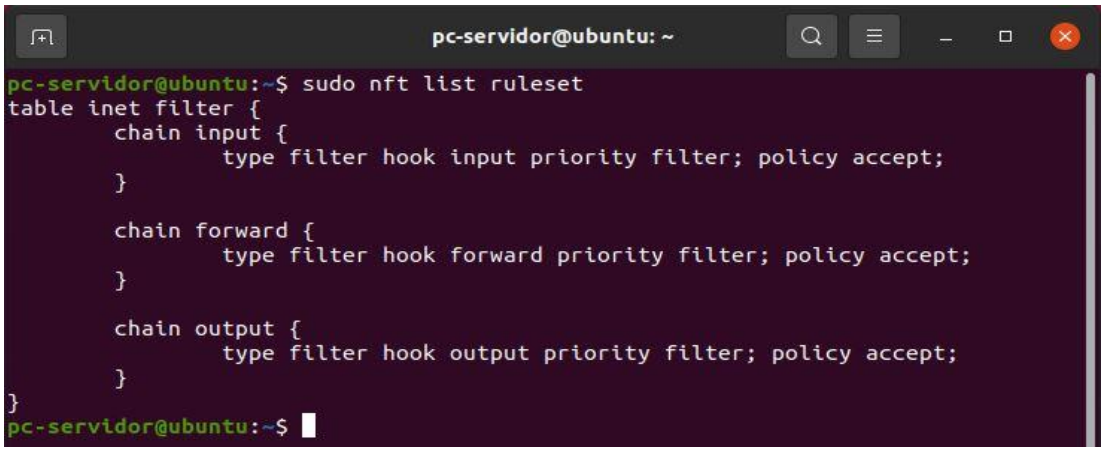
Nota. La imagen nos permite apreciar el conjunto de paquetes instalados, correspondiente a nftables. Elaboración propia.

Tras la instalación, se recomienda ingresar el comando por segunda vez, a fin de poder verificar que se descargaron e instalaron todos los paquetes.

Procedemos a verificar la instalación, utilizando ahora el comando ***sudo nft list ruleset***, el cual nos debe mostrar las reglas instaladas (en este caso solo se muestran las instaladas “por defecto”).

Figura 22

Verificación de instalación de nftables



4.4.2 Configuración de red para establecer conexión

Para poder realizar la demostración del funcionamiento de las reglas nftables, se vio por conveniente trabajar en un entorno virtual, por medio de dos máquinas virtuales (ambas con sistema operativo Ubuntu 20.04) bajo la denominación de **pc_cliente** y **pc_servidor**. Con el fin de lograr la comunicación entre ambas máquinas, se procede a la asignación de las ip, siendo pc_servidor **192.168.1.23/24** y pc_cliente **192.168.1.92/24**, ambas se comprueban con el comando ***ifconfig*** en la terminal.

Figura 23

Verificación de ip en equipo "pc_servidor"

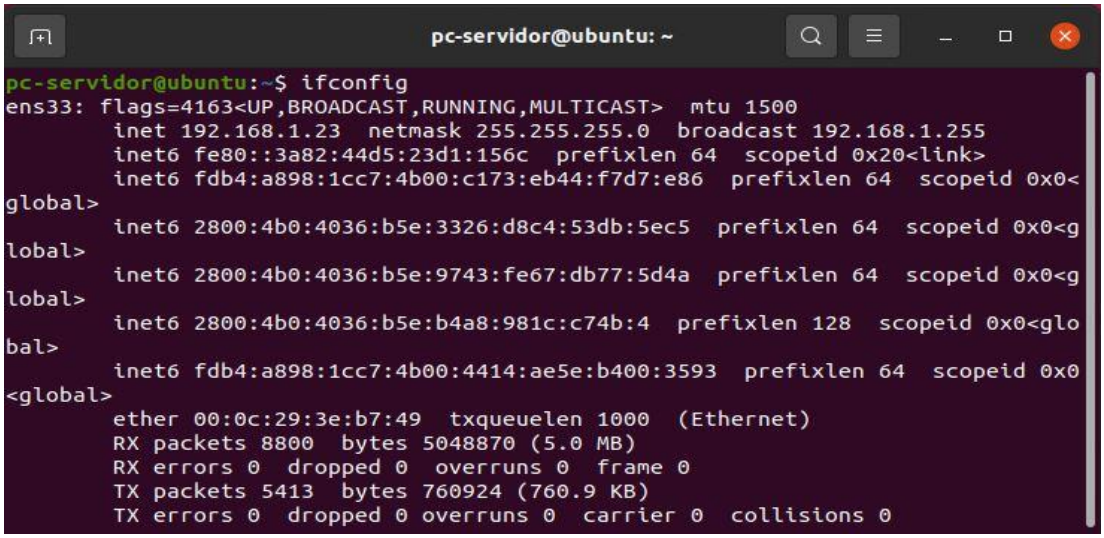
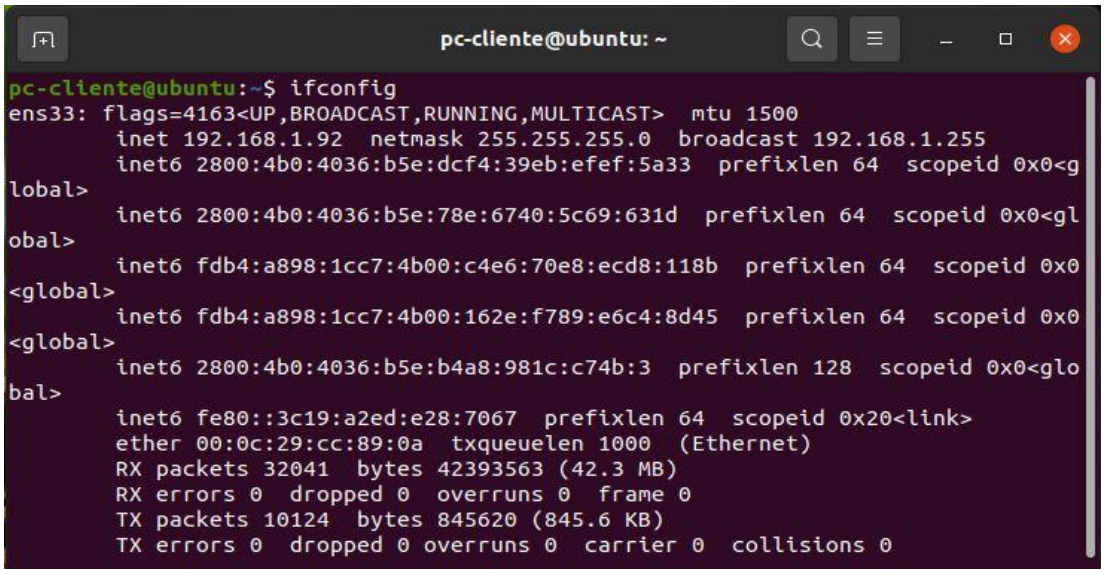


Figura 24

Verificación de ip en equipo "pc_cliente"



4.4.3 Administración de tablas, cadenas y reglas requeridas

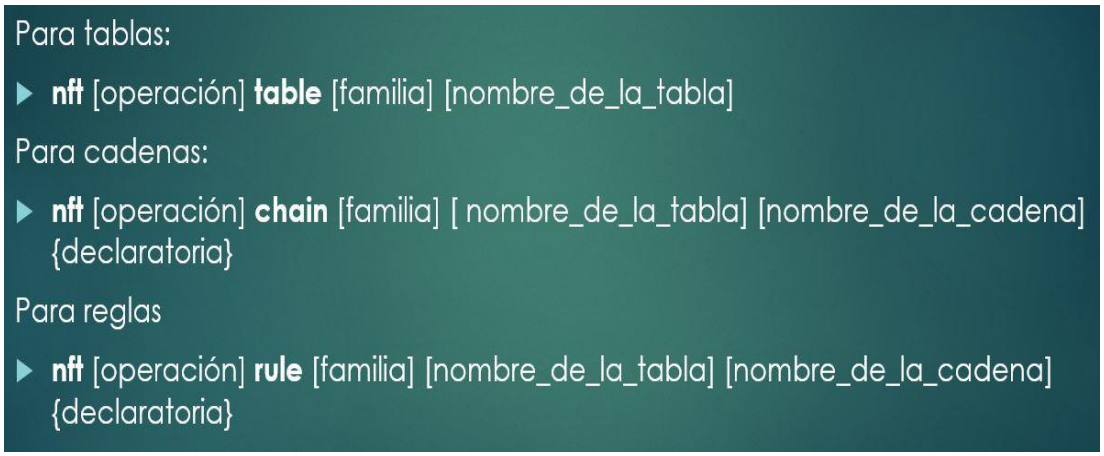
Para poder entender el funcionamiento de nftables, debemos prestar atención a la configuración y sintaxis, las cuales podemos consultar, junto a otros aspectos relacionados, en su página oficial (https://wiki.nftables.org/).

Para trabajar con nftables podemos hacerlo de dos maneras: ingresando las órdenes de manera directa en la terminal, línea por línea, o a través de scripts; cada una de ellas con su propia sintaxis y reglas.

Es así que, para ingresar las instrucciones a través de la terminal, la sintaxis es:

Figura 25

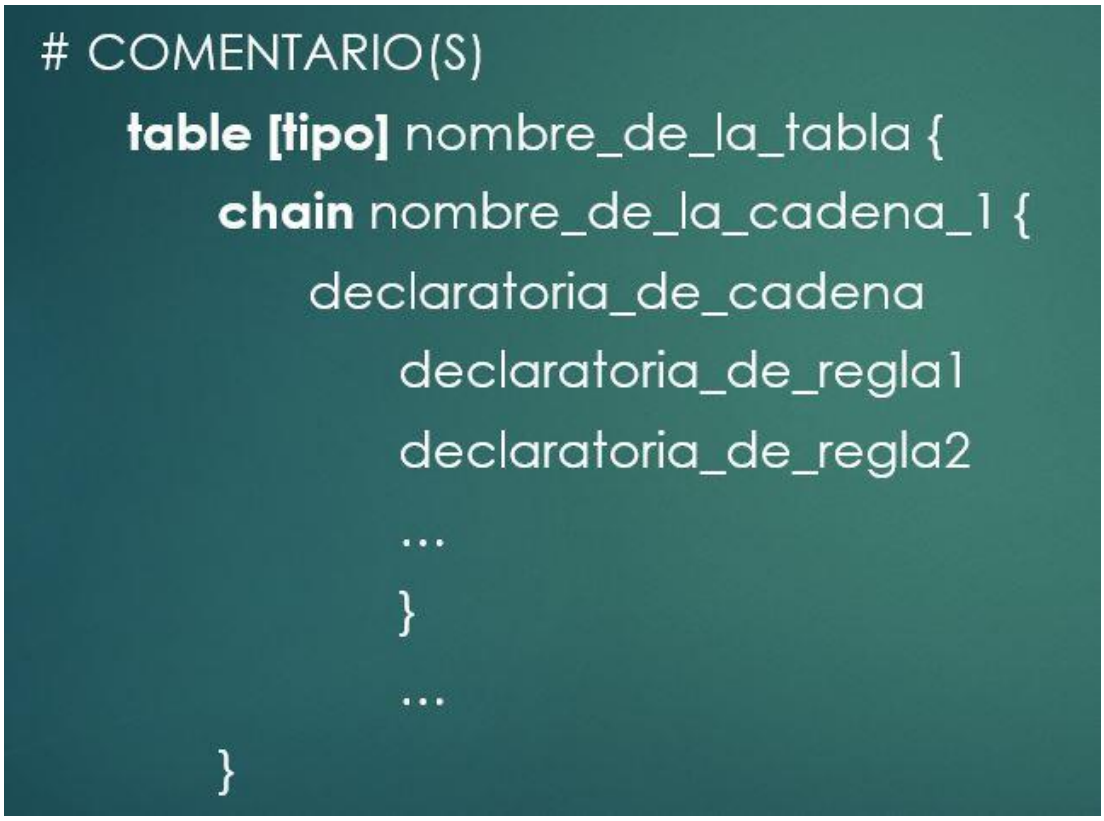
Sintaxis de nftables en terminal



Por su parte, para un script o editor de texto, se sigue la sintaxis:

Figura 26

Sintaxis de nftables en script o editor de texto



Nota. En la imagen, los tres puntos (…) hacen referencia a la posibilidad de incrementar la cantidad de reglas en cada cadena; o la cantidad de cadenas en cada tabla, según corresponda. Elaboración propia.

Cabe resaltar que la estructura de trabajo de nftables es la siguiente:

1. Tablas contienen una o más cadenas.
2. Cadenas contienen una o más reglas.
3. Las reglas trabajan de manera individual; es decir, se declaran una a una.

La sintaxis de la terminal nos obliga a ingresar línea por línea cada uno de los comandos requeridos, ya sea para crear, modificar o eliminar las instrucciones; lo cual se vuelve un proceso más prolongado y, para usuarios principiantes en su mayoría, más complicado.

Por otra parte, el uso de un editor de texto nos permite ingresar las instrucciones de manera conjunta, brindándonos además la oportunidad de analizarlas y/o corregirlas según sea necesario.

4.4.4 Pruebas de funcionamiento y análisis

A fin de cumplir con los objetivos planteados, se seleccionaron un conjunto de instrucciones relacionadas a Ethernet, ARP e IPv4.

En ese sentido, se vio por conveniente hacerlo mediante el uso de un editor de texto. En este caso el editor ***nano***, que viene integrado al sistema operativo. Para ello, se ingresó en la terminal la instrucción ***sudo nano /etc/nftables.conf*** que nos lleva, a través del editor de texto ***nano***, al fichero donde se guardan las instrucciones de nftables (debemos ingresar la contraseña del equipo para acceder).

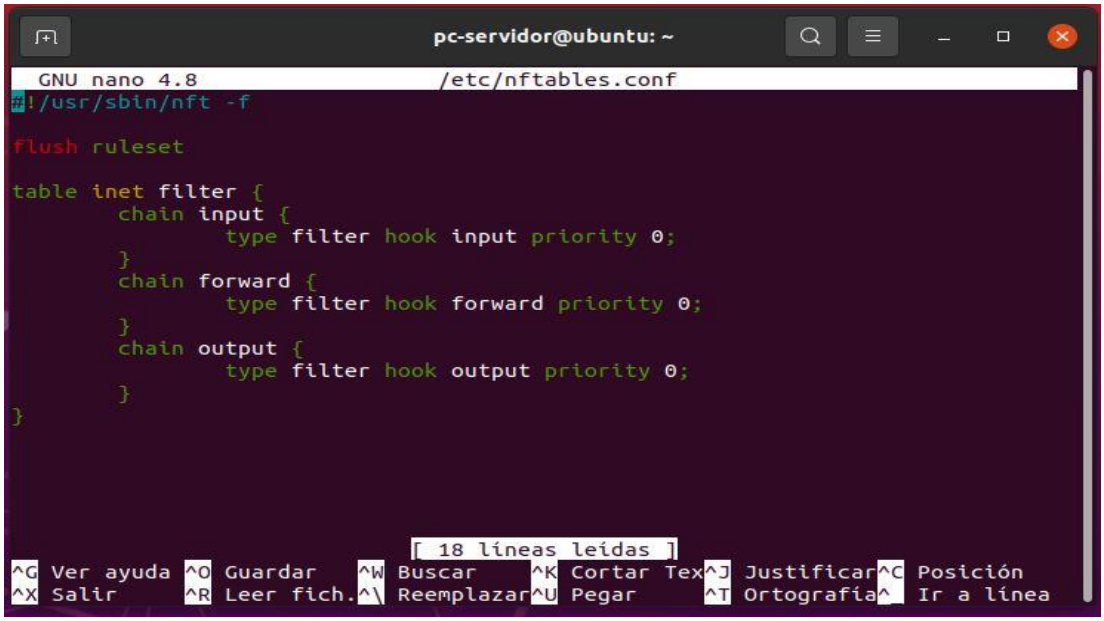
Figura 27

Ingreso al fichero nftables.conf a través del editor nano

Puesto que solo hemos instalado nftables y no hemos empleado ninguna regla hasta el momento, nos aparece el fichero original, el cual nos da la estructura de trabajo de nftables.

Figura 28

Contenido original del fichero nftables.conf



Nota. La imagen nos muestra el fichero original de nftables. En la parte inferior se observan los comandos rápidos del editor de texto.

Con esto, ya nos encontramos en el fichero, con la posibilidad de trabajar con las instrucciones de manera directa.

Para lograr que las instrucciones puedan ser reconocidas y aplicadas por la máquina virtual de nftables, solo basta con guardar el archivo/fichero (Ctrl+O) y salir (Ctrl+X), una vez hecho esto, hay que hacer que el servicio de nftables se reinicie, para que reconozca las modificaciones hechas en el fichero original. Esto se logra con el comando ***sudo systemctl restart nftables.service.***

Una vez dentro, se agregó la tabla ***accesoarp*** de la familia **arp** con el fin de habilitar dicho protocolo en nuestro firewall.

Figura 29

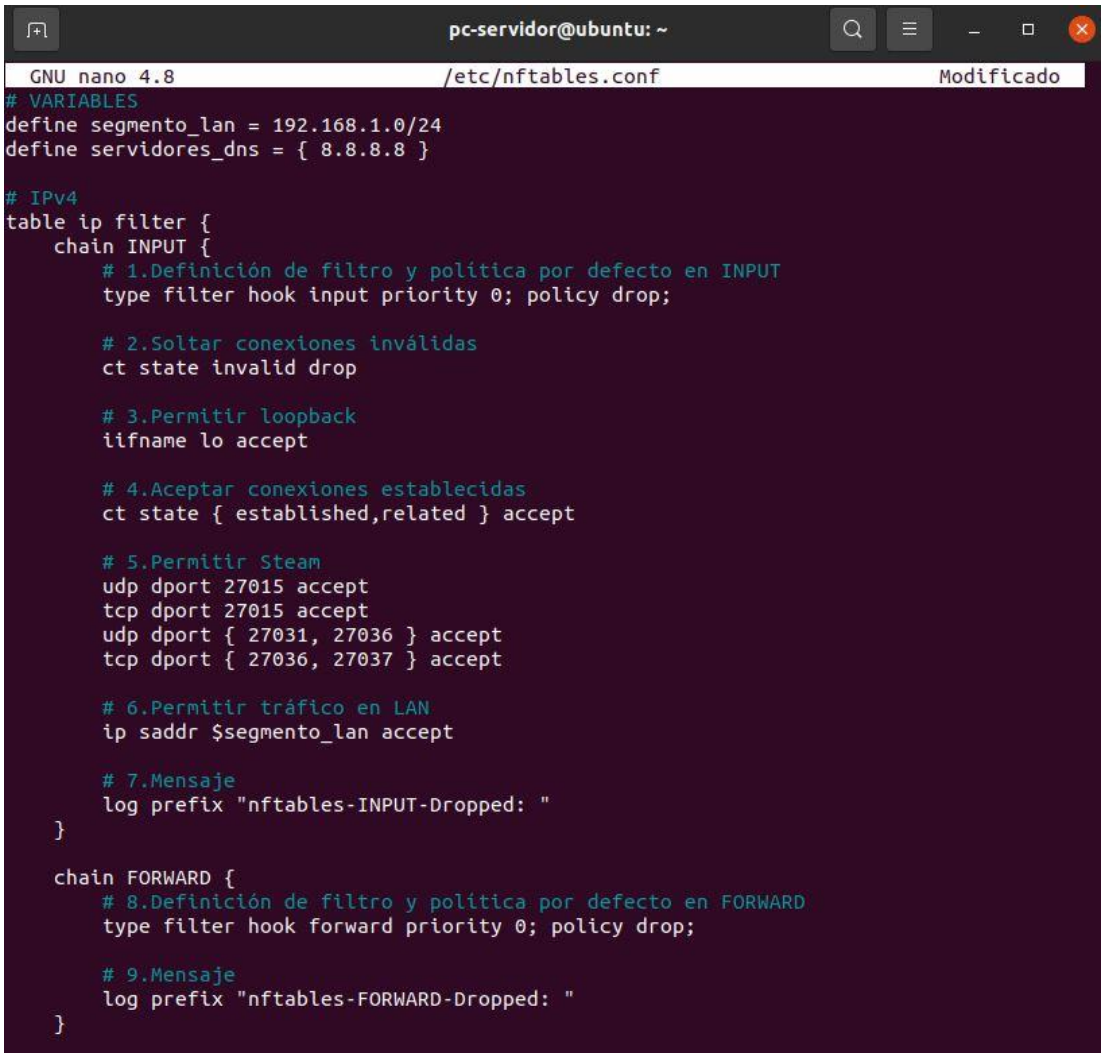
Creación de la tabla accesoarp, perteneciente a la familia arp

Nota. En la presente imagen se la tabla individual accesoarp, conteniendo la cadena entrada, así como sus respectivas reglas de trabajo.Elaboración propia.

Además de ello, se generó la tabla ***filter*** de la familia ***ip*** (para IPv4), en la cual se incluyen las cadenas y reglas necesarias para el filtrado del tráfico de red a nivel de IP en nuestro equipo; asimismo, se incluyeron las reglas y filtros para los puertos correspondientes. Cabe resaltar que, con fines demostrativos y con el afán de un trabajo más adecuado, se definieron previamente dos variables: ***segmento_lan*** y ***servidores_dns***, ambas con sus valores correspondientes.

Figura 30

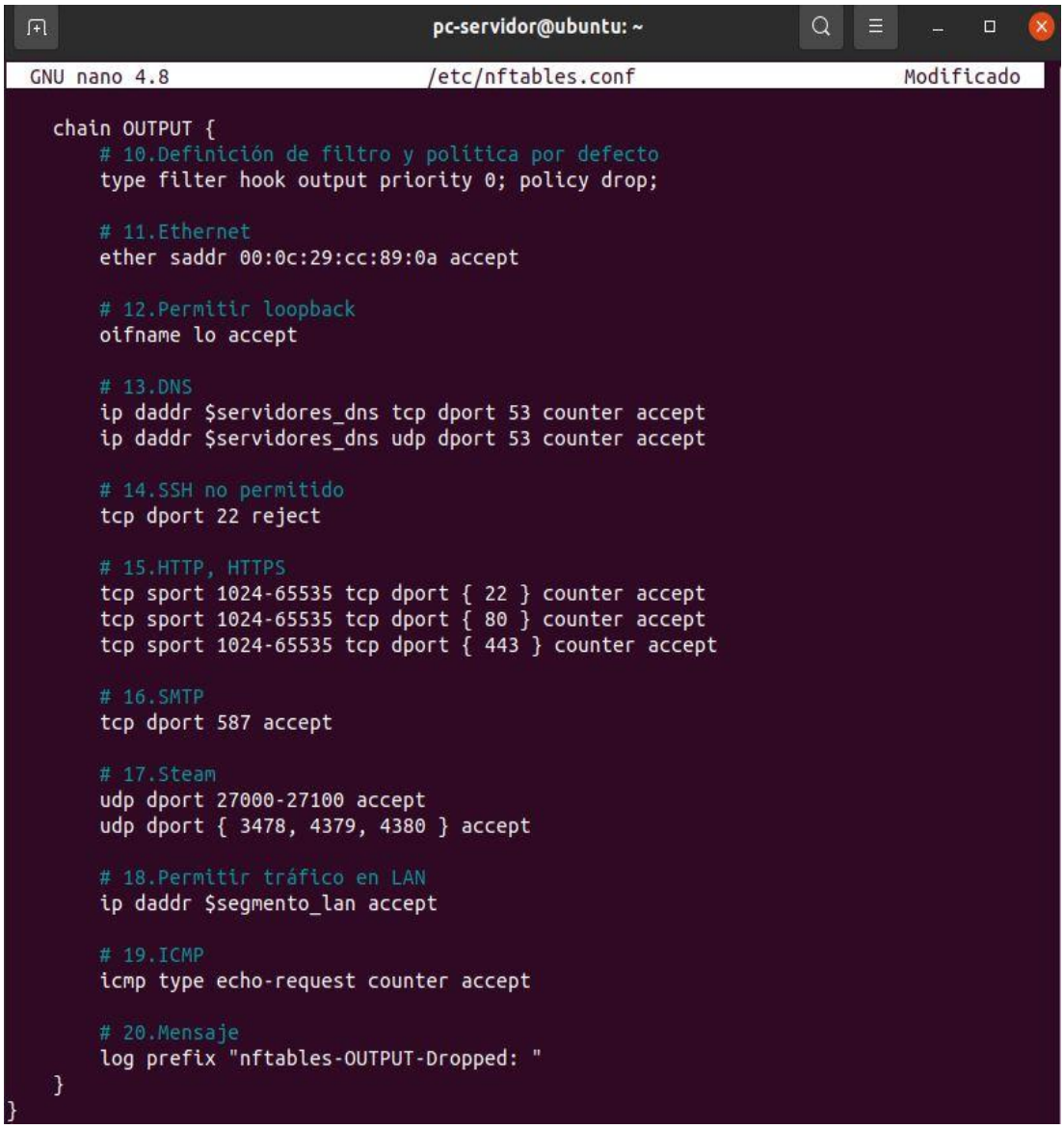
Creación de la tabla filter, perteneciente a la familia ip



Nota. En la presente imagen se aprecia las dos primeras cadenas: INPUT y FORWARD, cada una con sus respectivas reglas. Cada uno de los numerales (#) indican el inicio de un comentario de línea, lo cual significa que no serán interpretados por la máquina virtual de nftbles. Elaboración propia.

Figura 31

Creación de la cadena OUTPUT



Nota. En la presente imagen se aprecia la tercera cadena, la cadena OUTPUT, con sus respectivas reglas. Elaboración propia.

A continuación, se procede a explicar cada una de las reglas aplicadas, según el número de comentario de las figuras 30 y 31:

1. Se define el filtro en INPUT, y se agrega el gancho (hook) de entrada (input) además de la prioridad con valor cero (priority 0) que nos indica ejecución inmediata, así mismo, se indica por política la palabra clave ***drop.***
2. Obviamos las conexiones inválidas.
3. Permitimos el loopback de entrada iifname para, por ejemplo, utilizar el localhost.

4. Aceptamos todas las conexiones establecidas que sean permitidas por nftables.
5. Permitimos los puertos steam udp y tcp para asegurar la conexión de entrada.
6. Permitimos el tráfico en nuestra LAN (a nivel de entrada).
7. Dejamos un mensaje por defecto en la máquina virtual de nftables.
8. En FORWARD se define el filtro, y se agrega el gancho (hook) de tránsito (forward) además de la prioridad con valor cero (priority 0) que nos indica ejecución inmediata, así mismo, se indica por política la palabra clave drop. No habilitamos reglas; esto se debe a que el trabajo de la máquina virtual de nftables se dará en los ganchos (hook) INPUT y OUTPOUT.
9. Dejamos un mensaje por defecto en la máquina virtual de nftables.
10. En OUTPUT se define el filtro, y se agrega el gancho (hook) de salida (output) además de la prioridad con valor cero (priority 0) que nos indica ejecución inmediata, así mismo, se indica por política la palabra clave drop.
11. Establecemos la dirección del Ethernet para que la máquina virtual de nftables la reconozca y trabaje sobre ella.
12. Permitimos el loopback de salida oifname.
13. Habilitamos el puerto 53 en tcp y udp; además, establecemos counter para habilitar el contador de paquetes.
14. Rechazamos las conexiones ssh (puerto 22).
15. Habilitamos los contadores de paquetes para los puertos 22, 80 (HTTP) y 443 (HTTPS). Si bien es cierto no se permiten las conexiones en el puerto 22, se habilita el contador ante posibles intrusiones no registradas.
16. Habilitamos puerto 587 (SMTP) para correo.
17. Permitimos los puertos steam udp en el rango de 27000-271000, los puertos udp 3478, 4379 y 4380 en la salida.
18. Permitimos el tráfico en nuestra LAN (a nivel de salida).
19. Habilitamos el ICMP con echo-request (ping de comunicación) .
20. Dejamos un mensaje por defecto en la máquina virtual de nftables.

Guardamos los cambios y salimos.

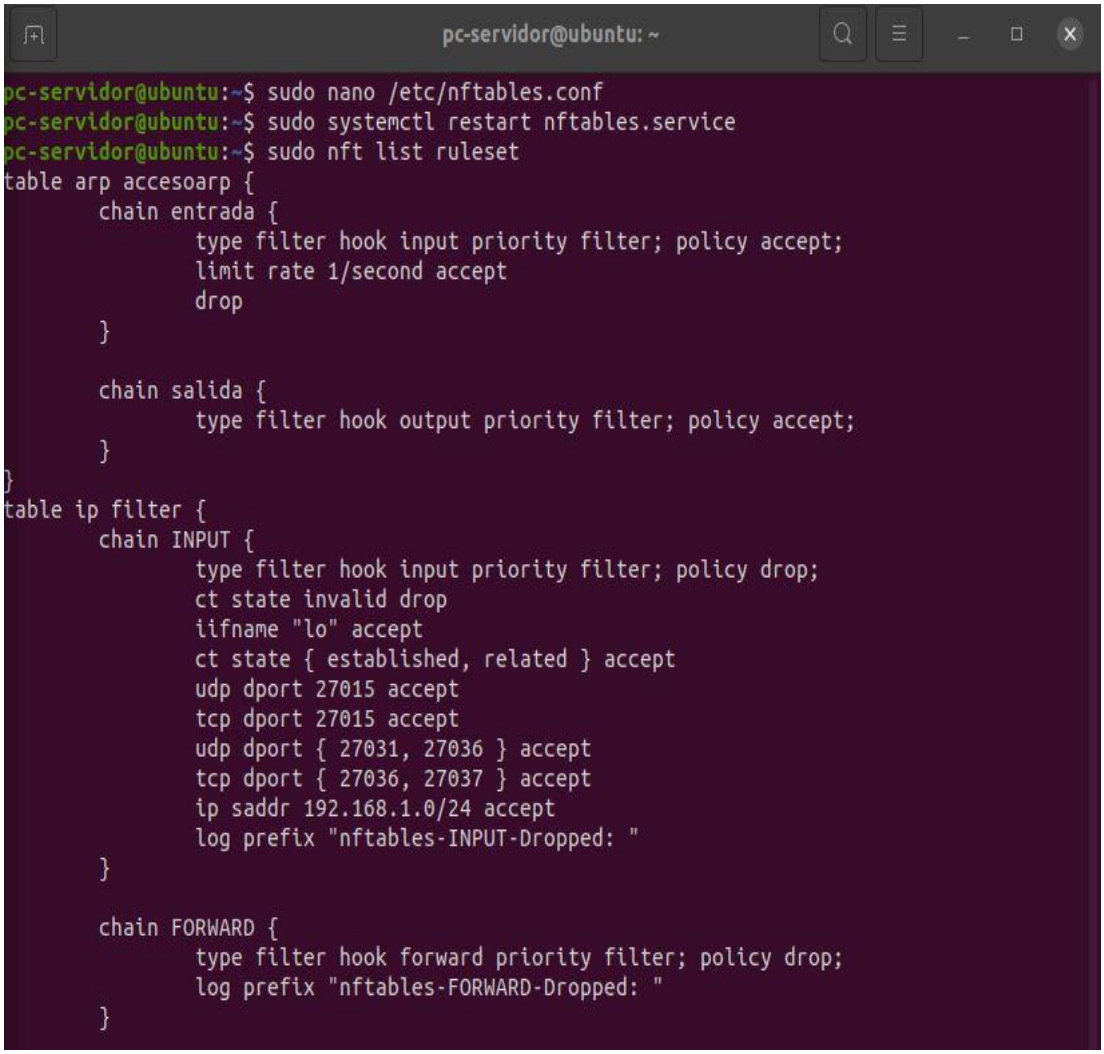
Lo que acabamos de hacer es actualizar el contenido del fichero original de nftables, por el contenido de las instrucciones de nuestro firewall.

Ejecutamos ***sudo systemctl restart nftables.service*** para validar los cambios hechos con el editor nano al fichero de nftables.

No nos aparece ningún mensaje adicional, lo cual nos indica que las reglas insertadas no poseen errores a nivel de reconocimiento por parte de la máquina virtual de nftables.

Figura 32

Visualización superior de reglas insertadas

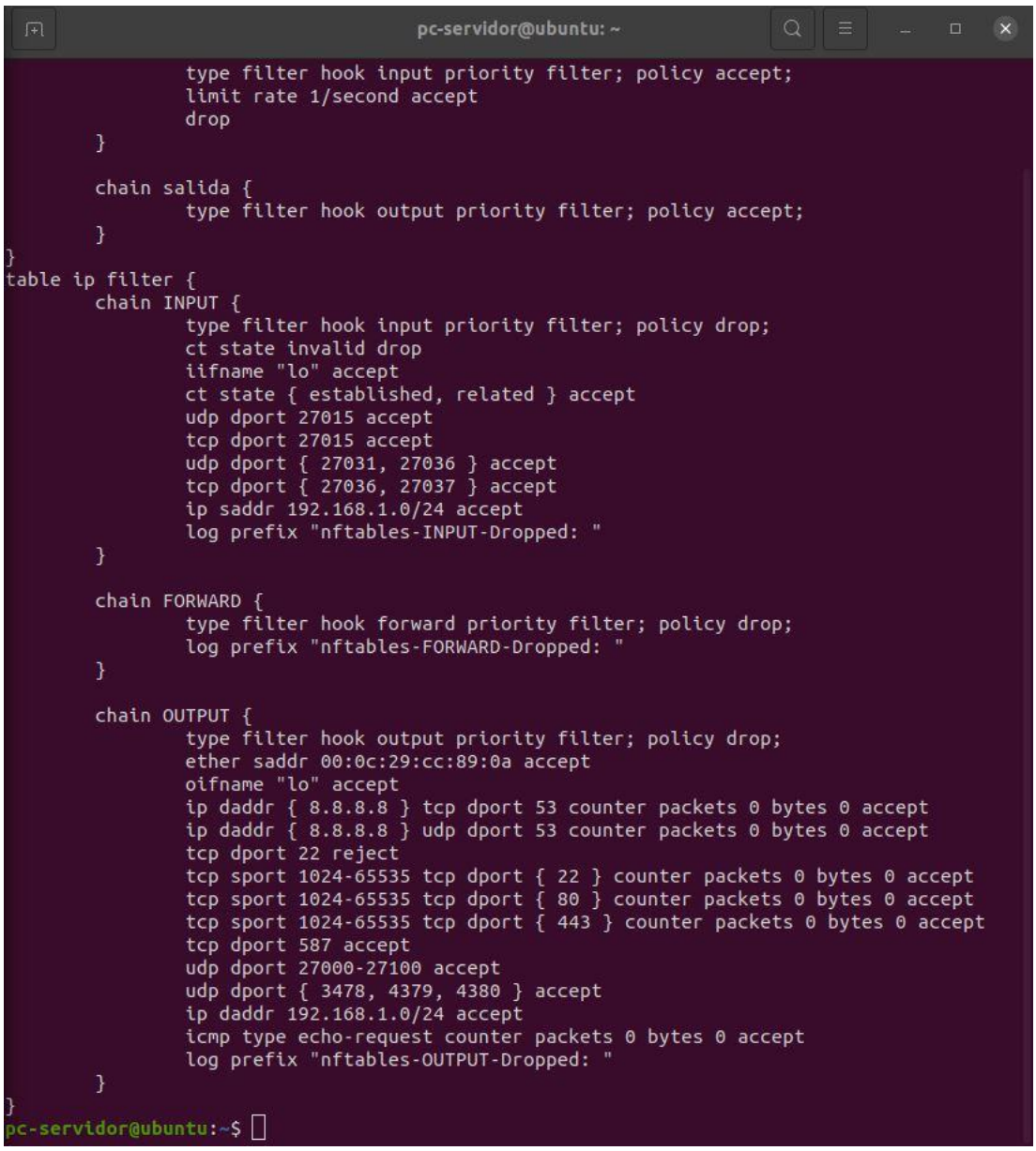


De manera seguida, ingresamos ***sudo nft list ruleset***, con el fin de poder visualizar las reglas que acabamos de ingresar en nftables.

Nótese, en la parte final (figura 33), que los contadores habilitados están en cero (packets 0 bytes 0) debido a que ya están activos, pero no registran actividad alguna.

Figura 33

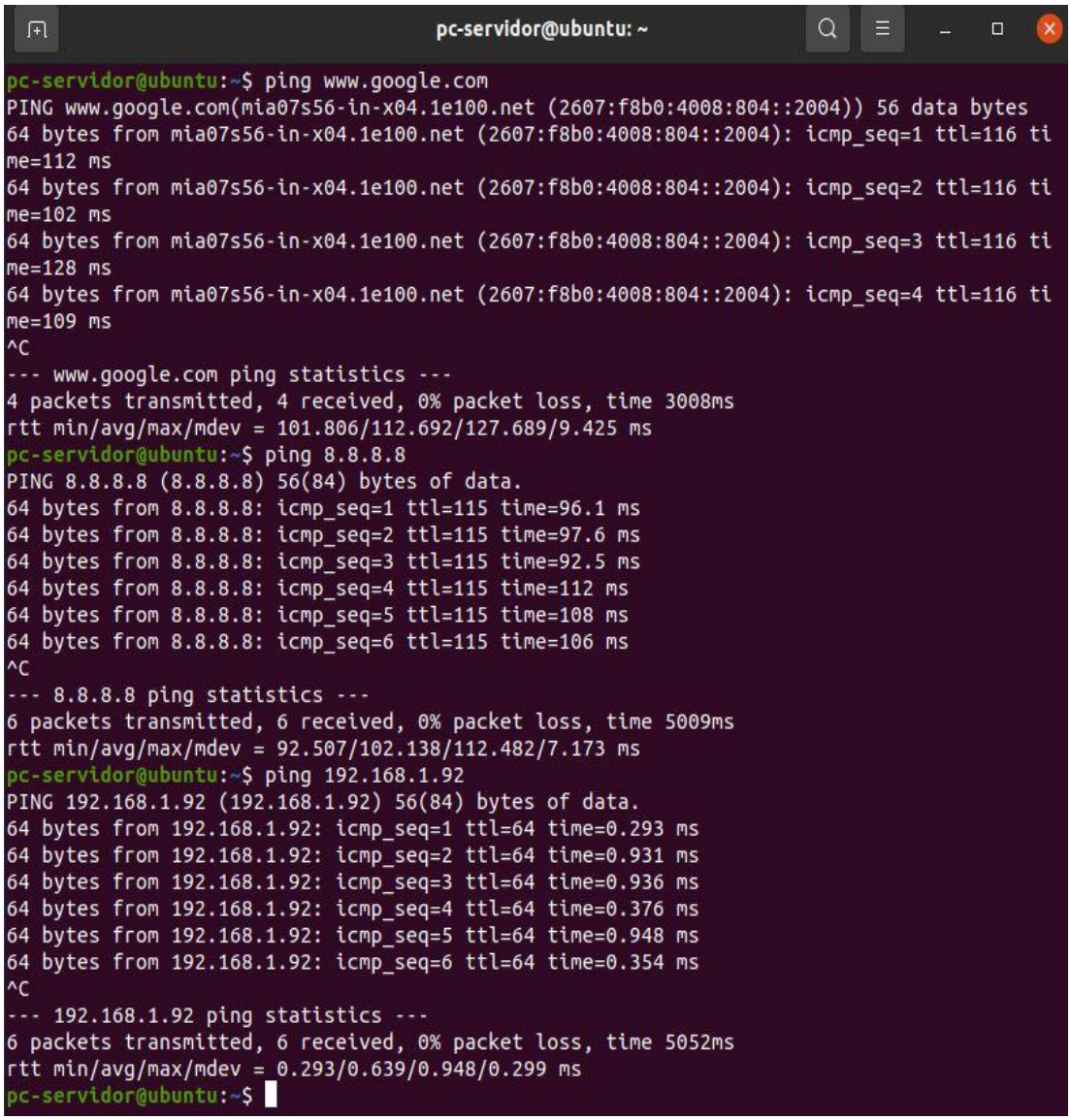
Visualización inferior de reglas insertadas



Hacemos ping, por ejemplo, a ***www.google.com*** para verificar la comunicación. Lo mismo con la dirección ***8.8.8.8*** para ver el acceso a internet y, finalmente, con ***192.168.1.92*** que es nuestra máquina virtual “pc_cliente”. En los tres casos se aprecia la comunicación exitosa.

Figura 34

Verificación de comunicación



Ingresamos a la página web de la entidad elegida (DRE AYACUCHO) y a páginas habituales como Youtube y Facebook. Se puede navegar con normalidad.

Esta acción se realiza con el fin de marcar un registro de actividad a nivel de los protocolos HTTP (puerto 80) y HTTPS (puerto 443), los cuales puedan llegar a ser detectados por el firewall que acabamos de implementar.

Figura 35

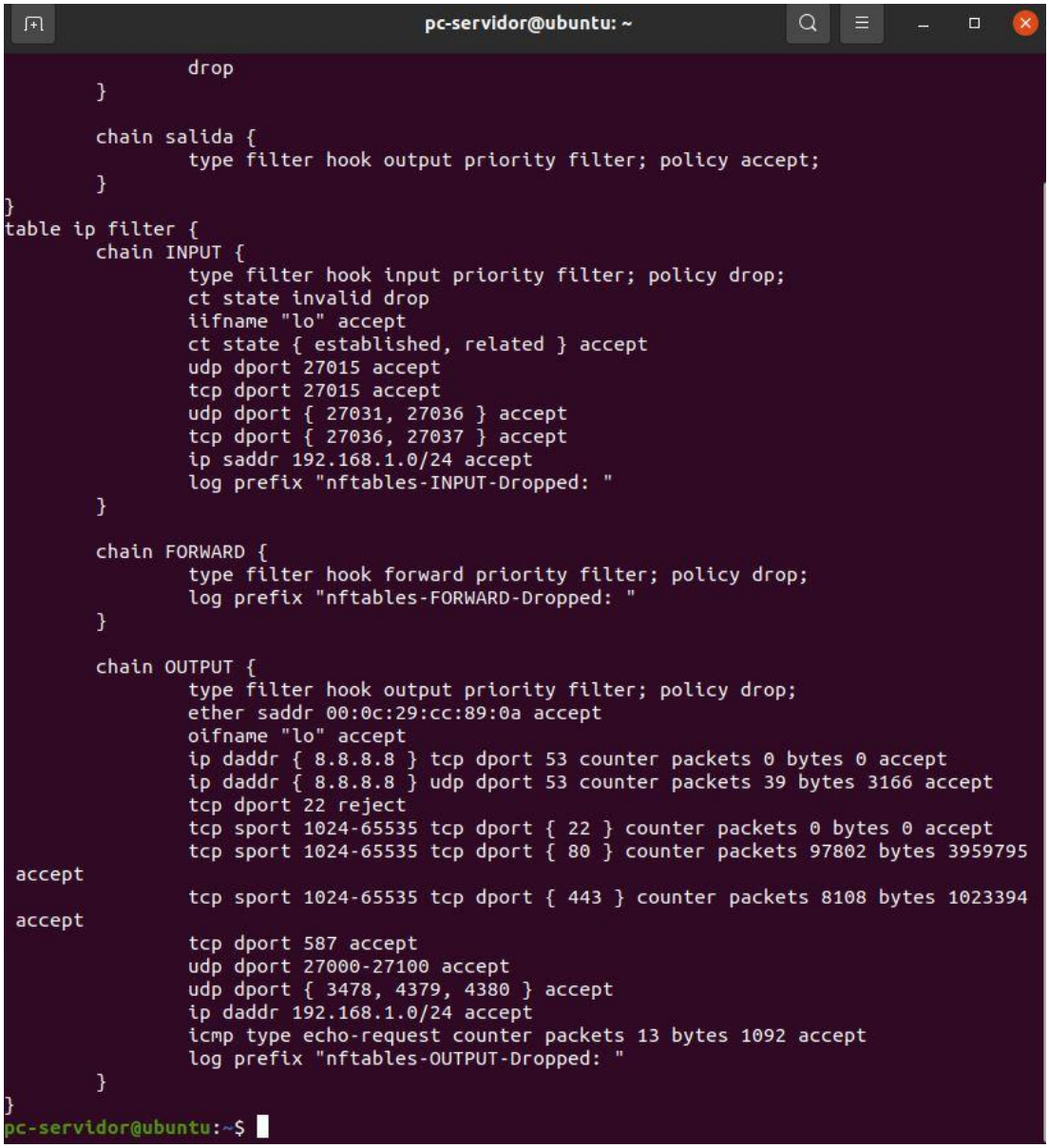
Navegación en internet

Nuevamente ingresamos ***sudo nft list ruleset***, y revisamos otra vez las reglas que habíamos habilitado en nftables.

En esta oportunidad, debido a las acciones de ping y navegación en internet, los contadores habilitados ya no están en cero, lo cual es indicativo de un monitoreo de paquetes efectivo.

Figura 36

Variación de contadores

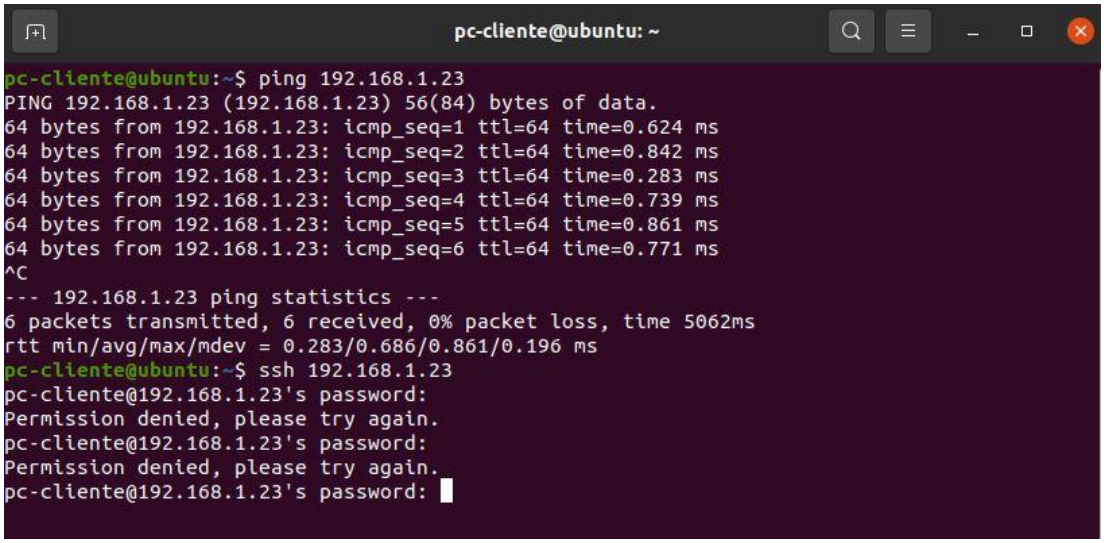


Haciendo una comprobación adicional, hacemos ping a pc_servidor (192.168.1.23) desde la máquina virtual pc_cliente para verificar la comunicación, la cual resulta positiva.

De manera seguida intentamos realizar una conexión ssh mediante ***ssh 192.168.1.23***, la cual es rechazada múltiples veces debido a la configuración de nuestro firewall, lo cual nos indica que funciona correctamente.

Figura 37

Comunicación entre pc_cliente y pc_servidor, y conexión ssh



CAPÍTULO V

Conclusiones y recomendaciones

5.1 Conclusiones

Tras la realización del presente trabajo, podemos concluir que el nivel de seguridad ofrecida por Nftables configurado como cortafuego (firewall) en la entidad seleccionada, aún configurado de manera básica, es igual al nivel ofrecido por medios de paga tradicional, pudiendo llegar a ser superior, según se incremente la complejidad de los mecanismos de protección.

Nftables no solo brinda una alternativa funcional en los puntos seleccionados, sino que también muestra una múltiple variedad de opciones, las mismas que pueden ser agregadas, modificadas y/o eliminadas según sea necesario dada la realidad de cada usuario.

Un aspecto importante a resaltar tras el uso de Nftables, es el hecho de la versatilidad que posee al poder abarcar diversas características de seguridad, así como su carácter evolutivo pues, a la fecha, sigue incrementado las librerías disponibles con lo cual, se puede concluir, es una herramienta con diversas aplicaciones y de larga vida útil.

En cuanto a temas de economía, se puede afirmar que resulta viable, pues basta contar con un equipo en la red que soporte el sistema operativo Linux, el cual, debido a su característica de ser libre y gratuito, no requiere de muchos requisitos, volviéndose así una alternativa accesible no solo a nivel económico, sino también a nivel de operatividad por su fácil configuración.

5.2 Recomendaciones

Tras realizar la implementación correspondiente, se recomienda actualizar de manera periódica el conjunto de reglas nftables, pues dada la naturaleza variable de las amenazas informáticas, el hecho de dejar estático un conjunto determinado de reglas, ocasionará que inevitablemente en algún momento dado nuevamente la red quede vulnerable.

A la fecha, Nftables es una herramienta adecuada para la seguridad informática; sin embargo, se encuentra aún en desarrollo, lo cual nos ofrece, según se actualice, la posibilidad de nuevos medios de protección, motivo por el cual se recomienda revisar periódicamente las nuevas reglas habilitadas y, según corresponda, su implementación en el cortafuegos implementado.

Asimismo, a la par de la actualización de las nuevas reglas existentes, es recomendable actualizar, también, la versión del sistema operativo, pues al margen de temas de compatibilidad que siempre están presentes, las buenas prácticas y la experiencia nos indican que mantener actualizado el sistema operativo también nos garantiza obtener las últimas soluciones en cuanto a seguridad informática.

Dado su grado de operatividad y facilidad de uso, se recomienda, de ser factible, la utilización de Nftables conjuntamente con otros medios de protección, lo cual garantizaría una protección aún mayor.

Referencias bibliográficas.

Bernal, C. (2010). *Metodología de la Investigación. Administración, Economía, Humanidades y Ciencias Sociales*. Tercera Edición. Editorial Pearson: Colombia.

Bradley, T. (2013). *Introduction to Packet Sniffing and. Net Security.* Londres, Inglaterra: McGrawHill, Inc.

Burke, J. (2021). Definition Ethernet. TechTarget. https://searchdatacenter.techtarget.com/es/definicion/Ethernet

Carrasco, S., (2019). *Metodología de la Investigación Científica. Pautas Metodológicas para Diseñar y Elaborar el Proyecto de Investigación*. Editorial San Marcos EIRL: Perú.

Castillo, J. (2018). Virtual Box vs VMWare. 05 de noviembre 2018. Disponible en: https://www.profesionalreview.com/2018/11/05/virtualbox-vs-vmware/

Cohn, D. (2008). *Análisis, Diseño e Implementación de una Aplicación para la Administración de las Herramientas de Seguridad en una Red Local*. Tesis de pregrado. Pontificia Universidad Católica del Perú.

Data Security Council of India (2011) *Cyber Crime Investigation: The Sequence of a Targeted Cyber Attack.* Delhi.

Davis, K., Turner, J.W. y Yocom, N. (2004). *The Definitive Guide To Linux Network Programming.* Inglaterra, APress.

Diario Gestión (2020). Ciberseguridad: *¿Cómo proteger tu empresa?* Recuperado de: https://gestion.pe/publirreportaje/ciberseguridad-como-proteger-tu-empresa-noticia/

Digital Guide IONOS. (16 de setiembre de 2021). *Trama Ethernet: definición, estructura y variantes.* https://www.ionos.mx/digitalguide/servidores/know-how/trama-ethernet/

Dimitrova, M. (2015). *Types of trojan attacks. Network, Browser Exploits and Security Essentials.* Sensors TechForum.

División de Delitos de Alta Tecnología de la Policía Nacional del Perú - DIVINDAT (2021). *Informe N° 04 Ciberdelincuencia: Pautas para una Investigación Fiscal Especializada.* Disponible en: https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%2020%PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20%2015%20FEBRERO%202021.pdf

EcuRed (s.f.). VMWare. Disponible en: https://www.ecured.cu/VMware

ESET (2021). *Security Report Latinoamérica 2021.* Disponible en: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Graves, K. (2010). *CEH: Certified Ethical Hacker Study Guide.* Indianapolis, Indiana: Wiley Publishing, Inc.

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la Investigación*. Sexta Edición. Mc Graw Hill Education: México.

Huebner, E. y Zanero, S. (2010). *Open Source Software fo Digital Forensics.* Inglaterra, Londres: Springer London.

Internet Assigned Numbers Authority - IANA (25 de setiembre 2021). Guía General de Protocolos de Internet. Disponible en: https://web.archive.org/web/20170905051853/https://www.iana.org/numbers

Interpolados (2017). Redes. Filtrado de Paquetes. Disponible en: https://interpolados.wordpress.com/2017/05/11/filtrado-de-paquetes/

KernelNewbies. (16 de setiembre de 2021). *Nftables, the Successor of Iptables. https://kernelnewbies.org/Linux_3.13#head-f628a9c41d7ec091f7a62db6a49b8da506 59ec88*

Koranne, S. (2010). *Handbook of Open Source Tools*. Estados Unidos, Nueva York: Springer New York.

Kwangjo, K., Muhamad Erza, A. y Chandra Tanuwidjaja, H. (2018). *Network Intrusion Detection Using Deep Learning: A Future Learning Approach.* Singapur: Springer Singapore.

Liska, A. (2003). *Network security: understanding types of attacks.* Pearson Inform. Revisado: junio 13, 2018.

Magnus, N. (2009). New Kernel Firewall Nftables to Succeed Netfilter. Linux Magazine. Disponible en: https://www.linux-magazine.com/Online/News/New-Kernel-Firewall-Nftables-to-Succeed-Netfilter

Netfilter. (16 de setiembre 2021). *Netfilter firewalling, NAT, and packet mangling for Linux.* https://netfilter.org/projects/nftables/

Neumann, P.G. (2000). *Denial-of-service attacks. Commun ACM 136*. Academic OneFile.

Pacheco, J. y Matínez, K. (2009). *Diseño e implementación de un servidor firewall en linux.* Tesis de pregrado. Universidad Tecnológica de Bolívar Cartagena de Indias. Colombia.

Pérez, I. (s.f.). *Software Libre (Ubuntu).* Universidad Autónoma del Estado de Hidalgo. Recuperado de: https://www.uaeh.edu.mx/scige/boletin/prepa4/n2/e4.html

Prasad, R.y Rohokale, V. (2020*). Cyber Security: The Lifeline of Information and Communication Technology.* Springer International Publishing.

Ramírez, I. (2020). *Máquinas Virtuales*. Actualizado 31 Enero 2020. Disponible en: https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Redhat (2021). Open Source: What is Open Source?. Disponible en: https://www.redhat.com/en/topics/open-source/what-is-open-source

Simsolo, Y. (2016). COMSEC *Consulting, the art of Securing Your Business*. India, OWSAP Top Ten.

Smith-Spark, L. (2017). *CNN, Global ransomware attack: 5 things to know*, Revisado: mayo 13, 2017.

Stallman, R. (2004). *Software libre para una sociedad libre*. Edición Traficantes de Sueños. Madrid: España.

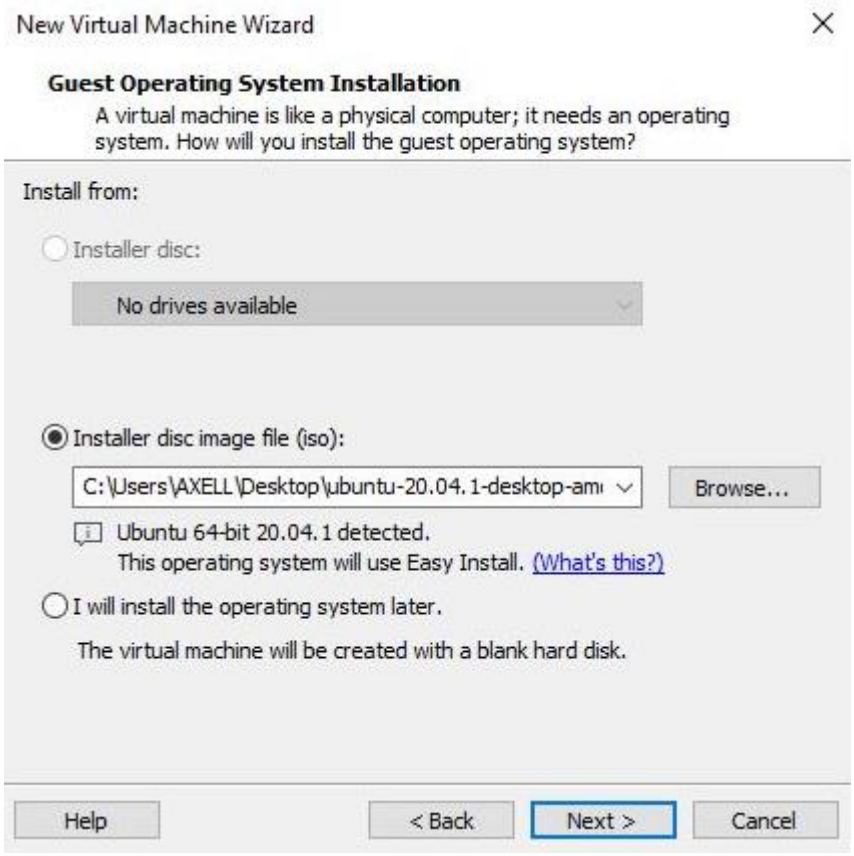
Universidad de Aberdeen (2019). Address Resolution Protocol (ARP). Escocia.

Velasco, R. (2017). Características Vmware. https://www.softzone.es/2017/03/14/comparativa-vmware-virtualbox/ Rubén Velasco 14 marzo 2017.

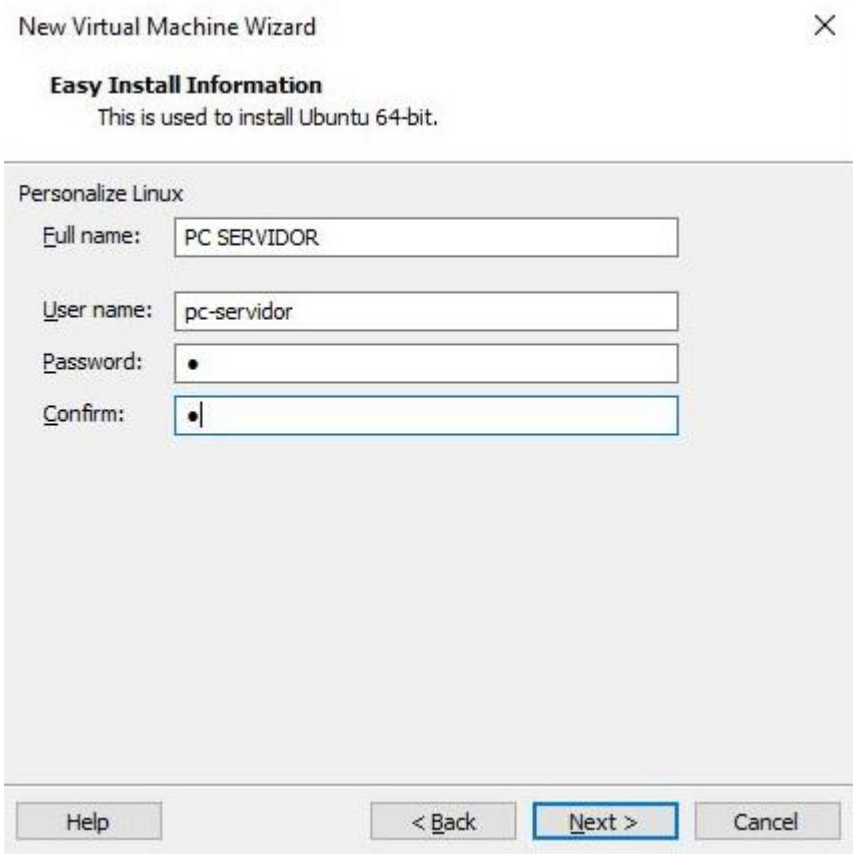
Villanueva, A. (2021). Ventajas *y desventajas de Linux*. Actualizado el 08 de diciembre 2021. Disponible en: *https://www.internetizado.com/linux/ventajas-y-desventajas*

ANEXO

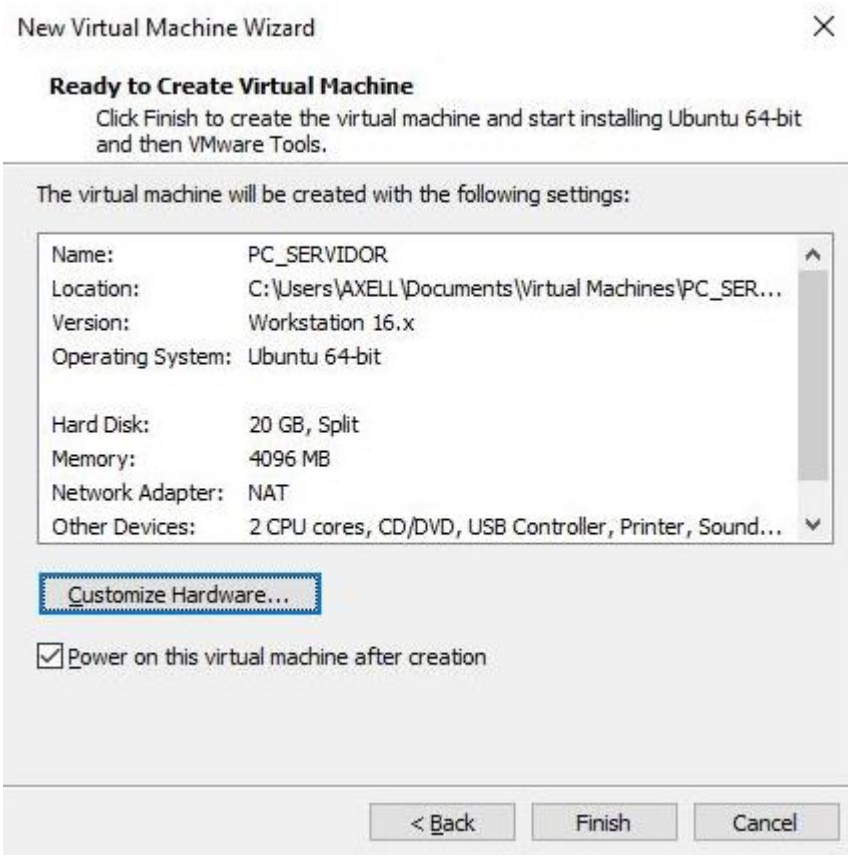
Instalación de máquina virtual, utilizando el programa VMWare, con el sistema operativo Ubuntu 20.04



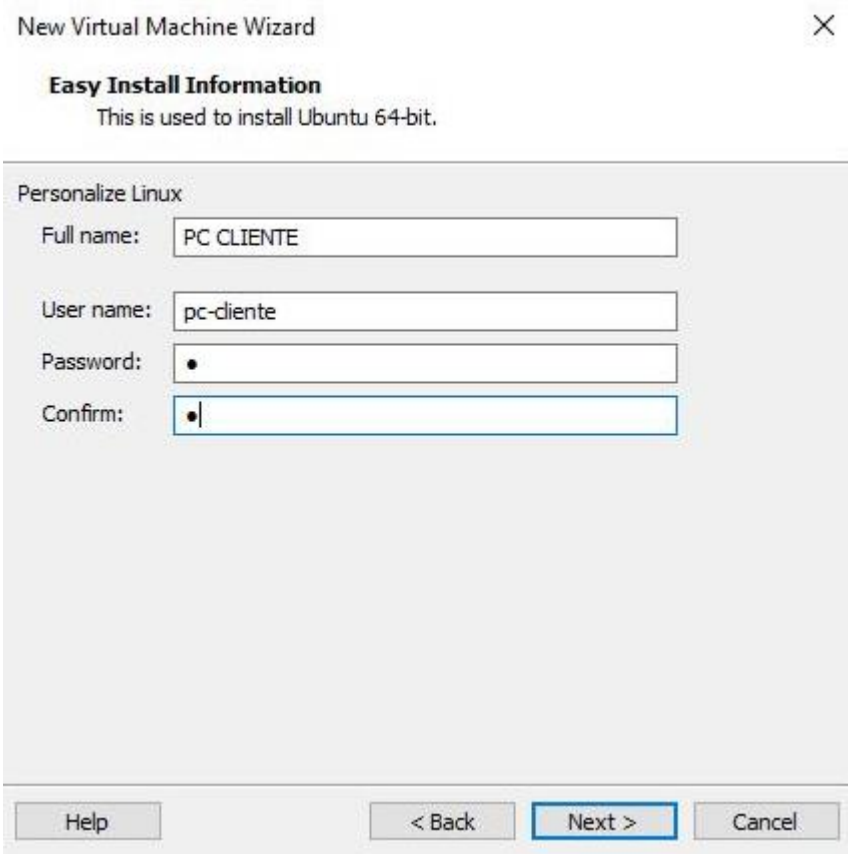
Creación de la máquina virtual “pc_servidor” y sus respectivas credenciales de acceso



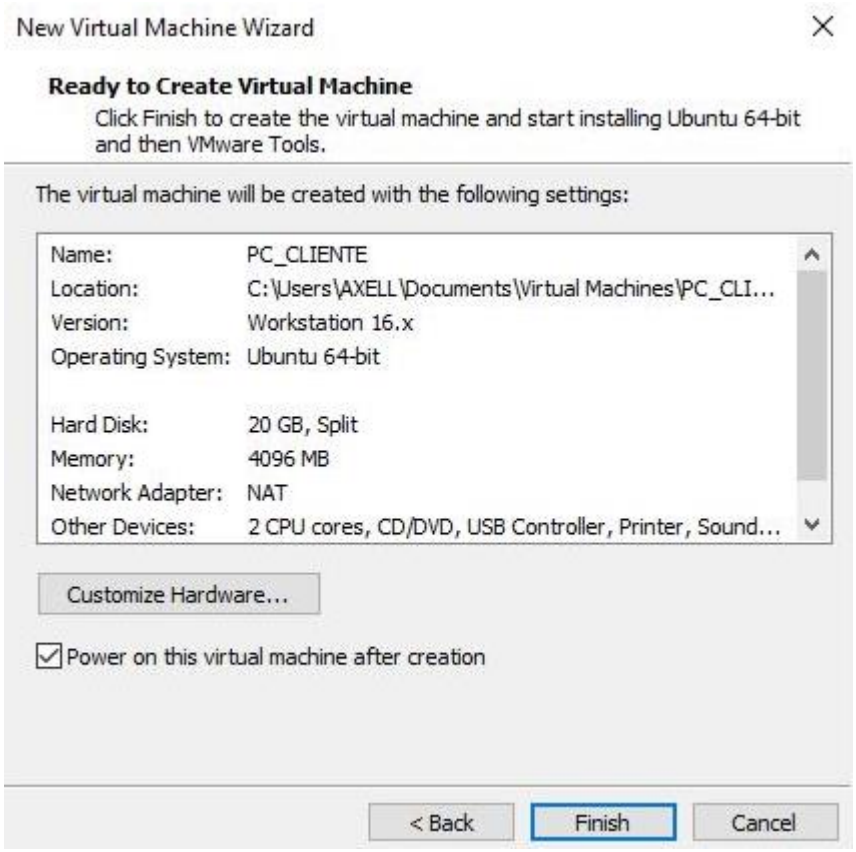
Asignación de recursos a la máquina virtual “pc_servidor”



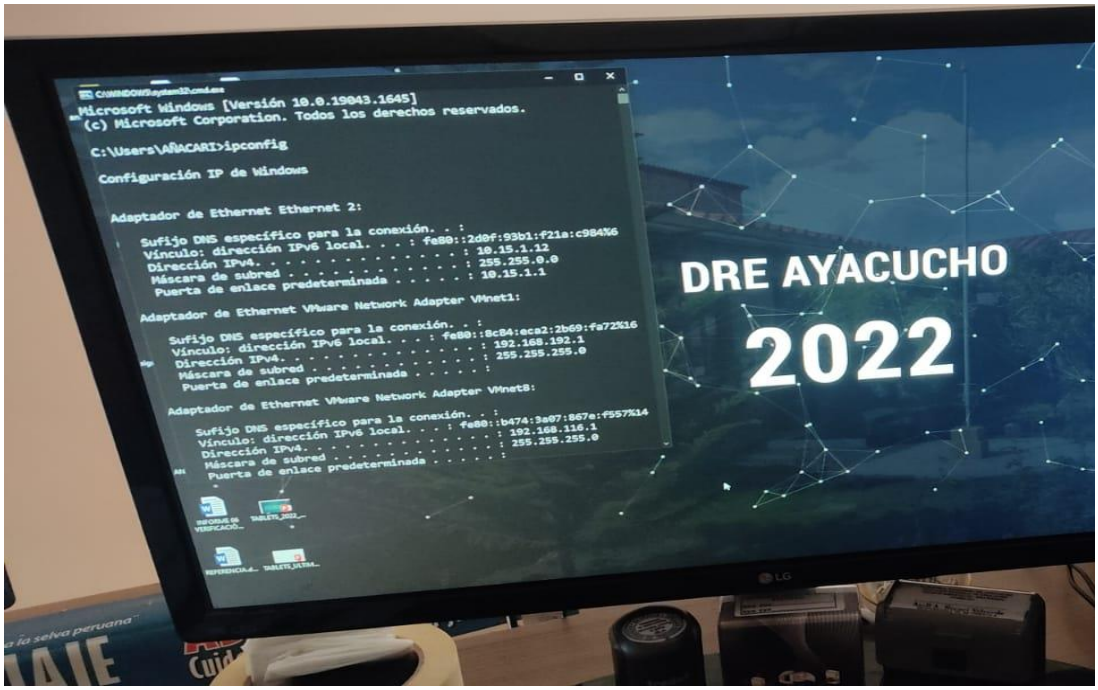
Creación de la máquina virtual “pc_cliente” y sus respectivas credenciales de acceso



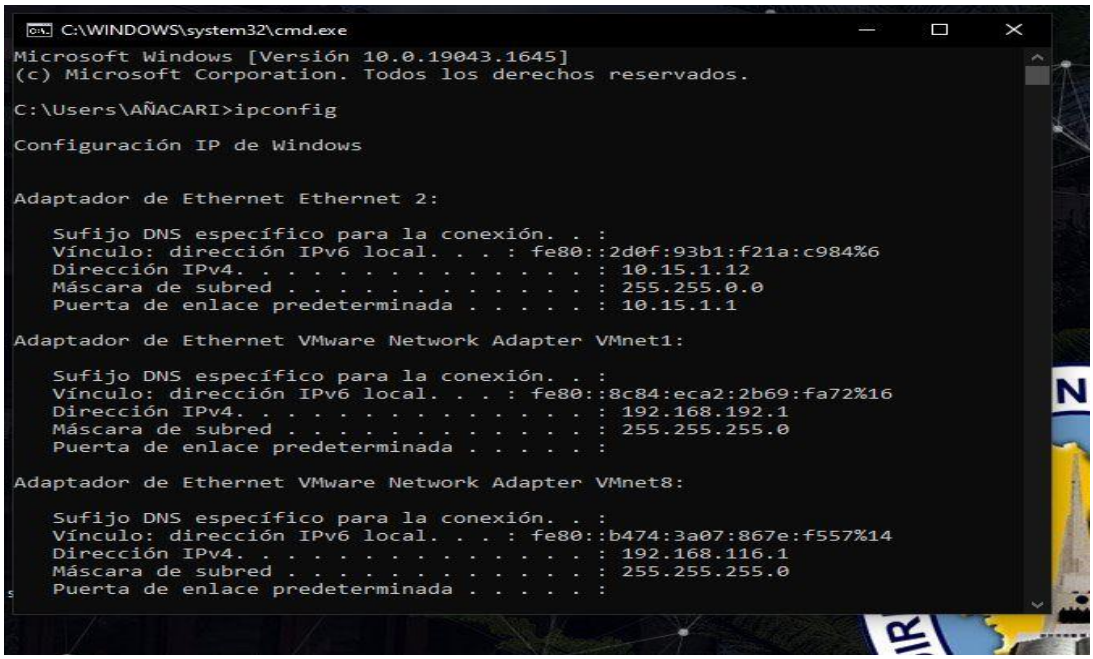
Asignación de recursos a la máquina virtual “pc_cliente”



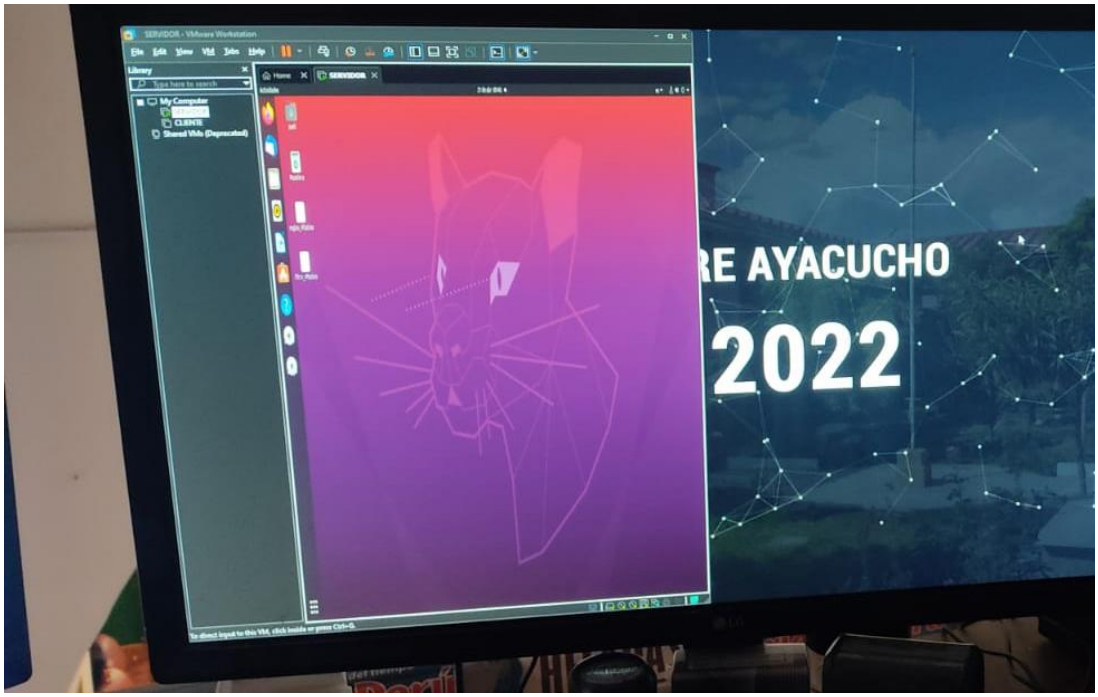
Equipo de la Dirección Regional de Educación de Ayacucho, en entorno Windows, con IP 10.15.1.12/16



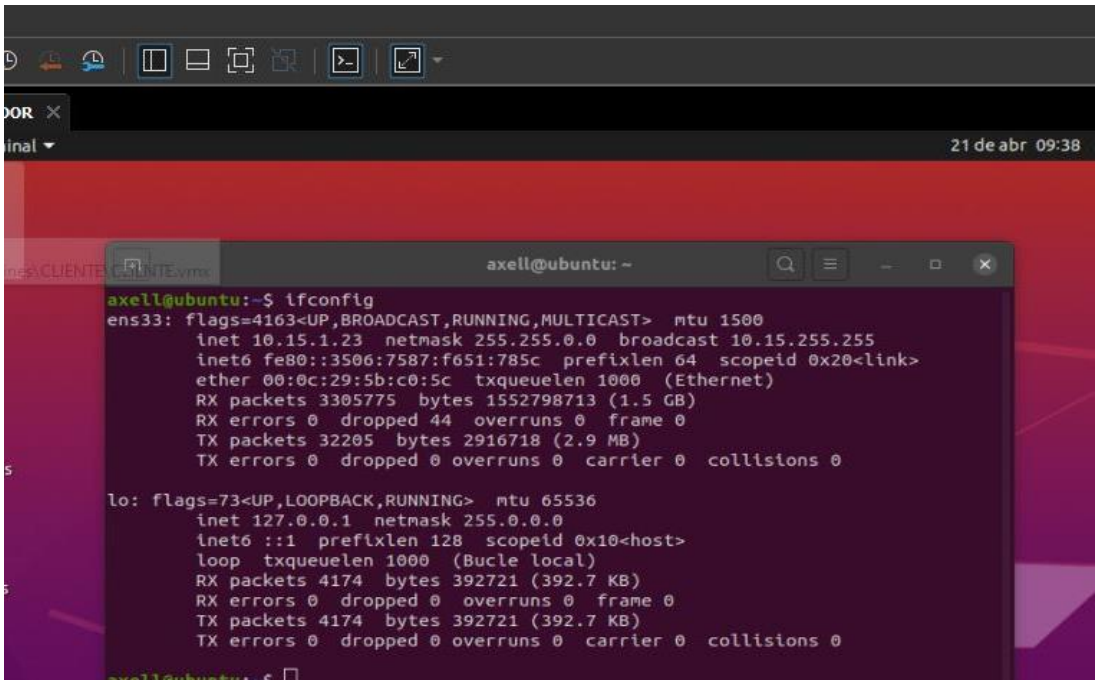
Visualización de ip asignado al equipo de Consulta de Trámites.



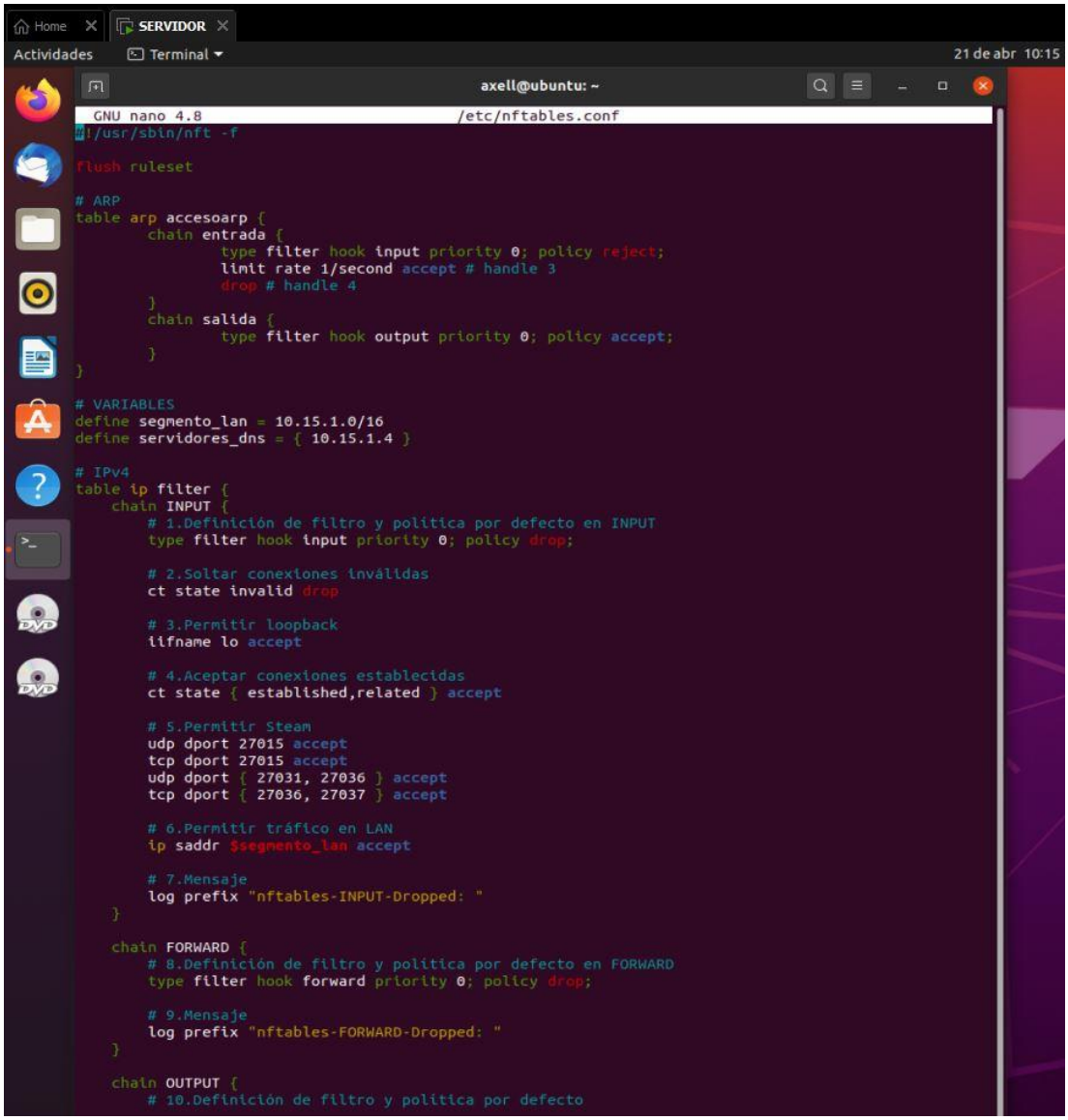
Equipo de la Dirección Regional de Educación de Ayacucho, en entorno real, con entorno Linux Ubuntu



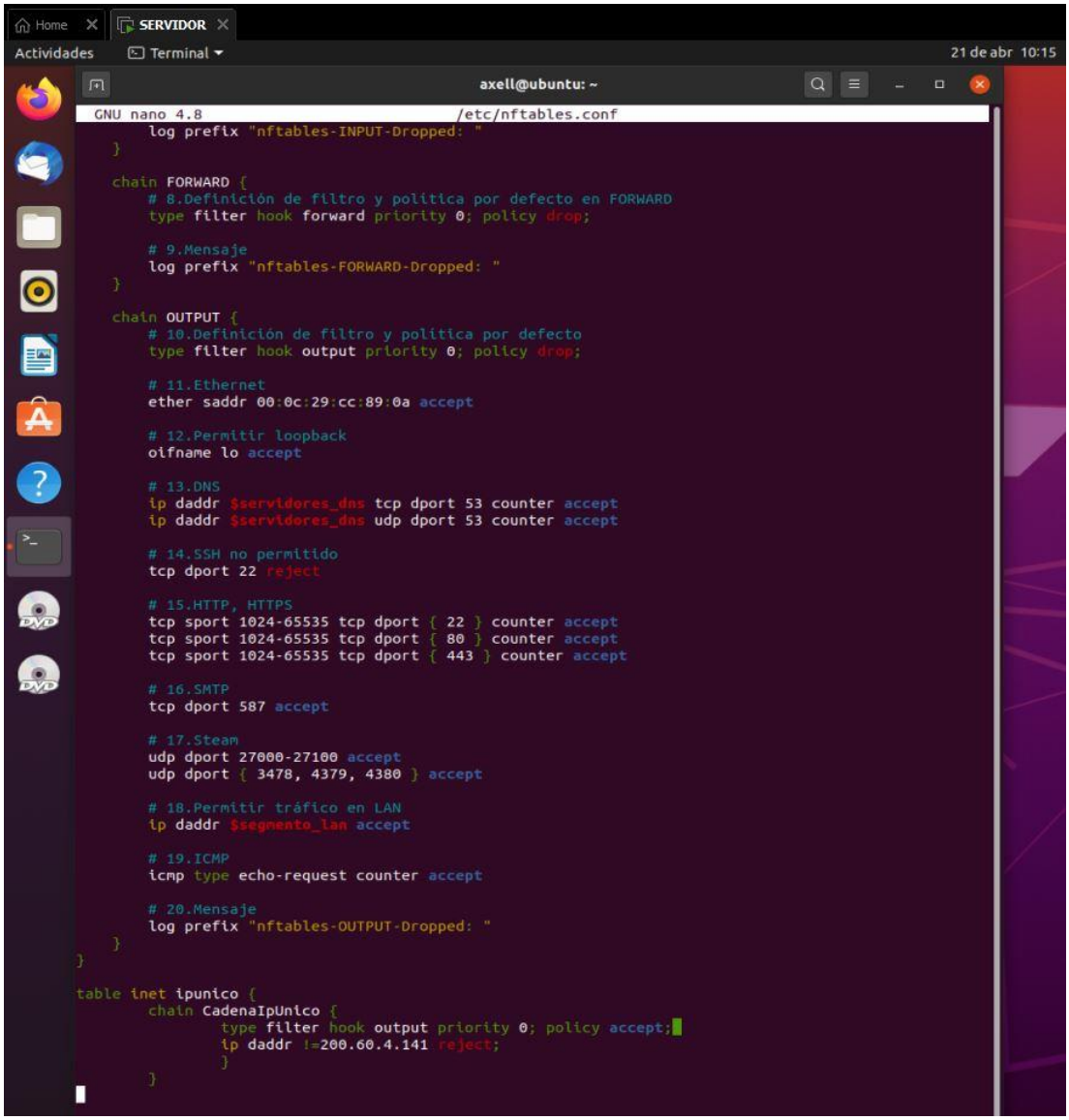
Equipo de la Dirección Regional de Educación de Ayacucho, en entorno Ubuntu, con IP 10.15.1.23/16



Reglas nftables configuradas en entorno Linux, trabajando a nivel de IDS (parte superior).



Reglas nftables configuradas en entorno Linux, trabajando a nivel de IDS (parte inferior).



Debido al filtro, se aprecia el bloqueo de toda página que no sea la ip 200.60.4.141 (Sistema de Gestión Documentaria - SISGEDO). En el ejemplo, Facebook.com.

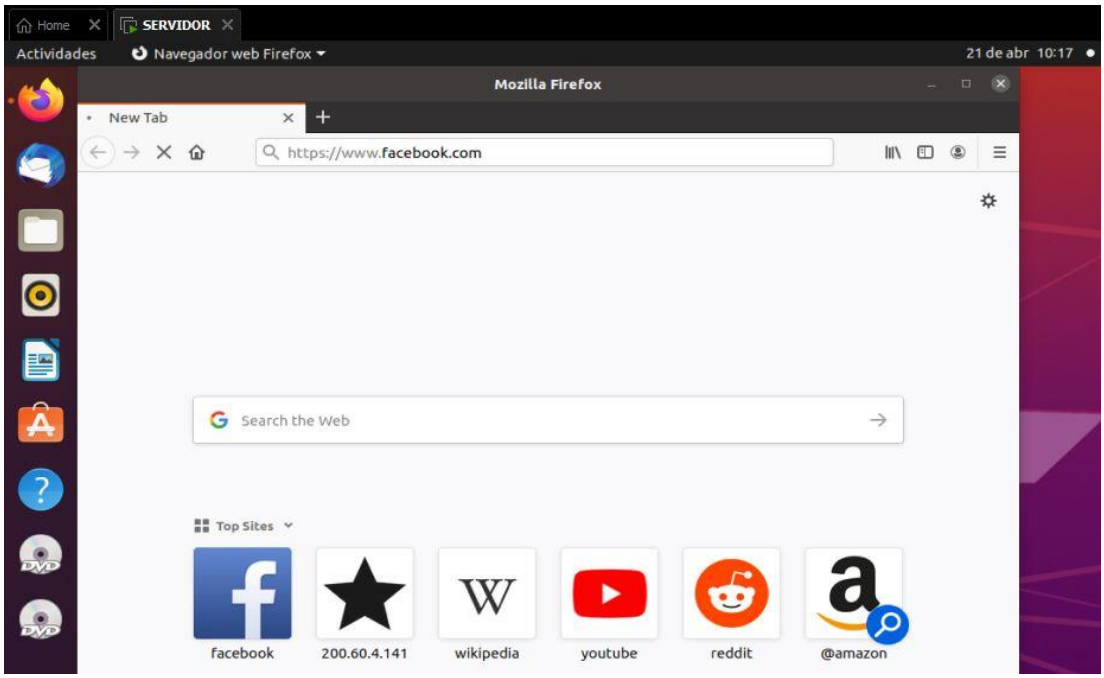
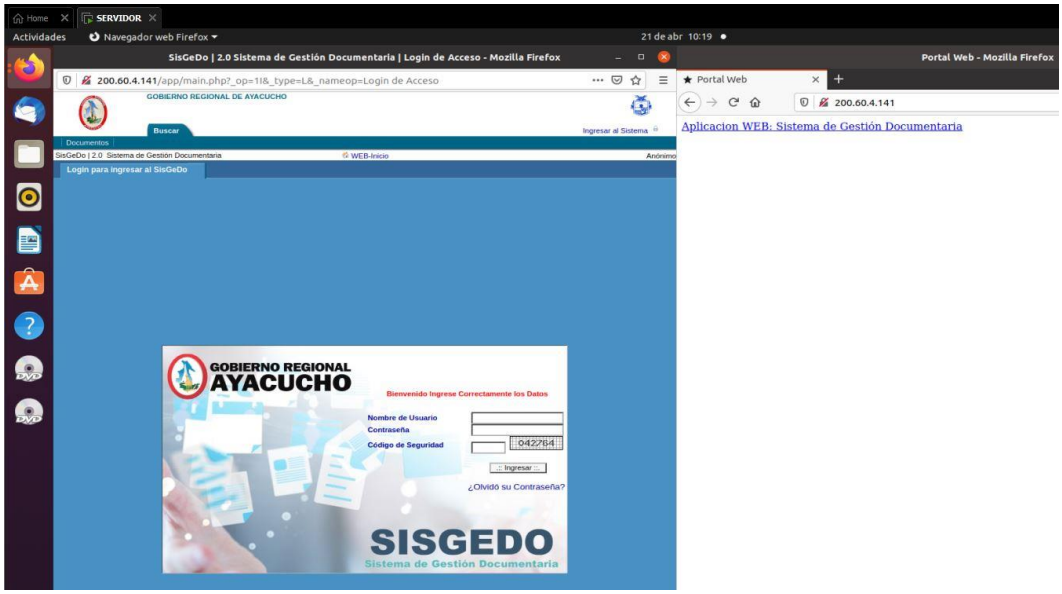


Imagen demostrativa conjunta, entre la página permitida y la página de prueba de acceso denegado.



ACTA DE SUSTENTACIÓN DE TESIS

ACTA N° 040-2022-FIMGC

En la ciudad de Ayacucho, en cumplimiento a la **RESOLUCIÓN DECANAL N° 163-2022-FIMGC-D**, siendo los veintitrés días del mes de junio del 2022, a horas 11:00 a.m.; se reunieron los jurados del acto de sustentación, en el Auditórium virtual google meet del Campus Universitario de la Universidad Nacional de San Cristóbal de Huamanga.

Siendo el Jurado de la sustentación de tesis compuesto por el presidente el **Dr. Ing. Efraín Elías PORRAS FLORES,** Jurado el **Dr. Ing. Manuel Avelino LAGOS BARZOLA,** Jurado el **Mg. Ing. Celia Edith MARTINEZ CORDOVA,** Jurado - Asesor el **Mg. Ing. Hubner JANAMPA PATILLA** y secretario del proceso el **Mg. Ing. Christian LEZAMA CUELLAR,** con el objetivo de recepcionar la sustentación de la tesis denominada **"NFTABLES COMO FIREWALL A NIVEL DEL KERNEL DE LINUX PARA EL FILTRADO DE PAQUETES EN ENTORNOS OPEN SOURCE, 2021",** sustentado por el Señor **Axell Alberto ÑACARI VALVERDE,** Bachiller en **Ingeniería de Sistemas**.

El Jurado luego de haber recepcionado la sustentación de la tesis y realizado las preguntas, el sustentante al haber dado respuesta a las preguntas, y el Jurado haber deliberado; califica con la nota aprobatoria de **15 (Quince).**

En fe de lo cual, se firma la presente acta, por los miembros integrantes del proceso de sustentación.

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE INGENIERÍA DE MINAS GEOLOGÍA Y CIVIL
Dr. Efraín Elías Porras Flores
DECANO

Firmado digitalmente por Dr. Ing. Efraín Elías Porras Flores
Fecha: 2022.06.28 08:25:50 -09'00'

Dr. Ing. Efraín Elías PORRAS FLORES
Presidente

Dr. Ing. Manuel Avelino LAGOS BARZOLA
Jurado

Mg. Ing. Hubner JANAMPA PATILLA
Jurado Asesor

Mg. Ing. Celia Edith MARTINEZ CORDOVA
Jurado

Firmado digitalmente por LEZAMA CUELLAR CHRISTIAN

Mg. Ing. Christian LEZAMA CUELLAR
Secretario del Proceso

c.c.:
Bach. Axell Alberto ÑACARI VALVERDE
Jurados (4)
Archivo

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA N° 037-2022-FIMGC

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la Resolución de Consejo Universitario N° 039-2021-UNSCH-CU, Reglamento de Originalidad de Trabajos de Investigación de la UNSCH y Resolución Decanal N° 158-2021-FIMGC-UNSCH-D, deja constancia que Sr./Srta.

Apellidos y Nombres	:	ÑACARI VALVERDE, Axell Alberto
Escuela Profesional	:	INGENIERÍA DE SISTEMAS
Título de la Tesis	:	"Nftables como firewall a nivel del kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021"
Evaluación de la Originalidad	:	**3 %** Índice de Similitud
Identificador de la entrega	:	1860567608

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

Ayacucho, 20 de junio del 2022

Firmado digitalmente por LEZAMA CUELLAR CHRISTIAN

Mg. Ing. Christian LEZAMA CUELLAR
Verificador de Originalidad de Trabajos de Tesis de Pregrado de la FIMGC

(X) Con depósito para Sustentación y Tramite de Titulo

FACULTAD DE INGENIERÍA
DE MINAS, GEOLOGÍA Y CIVIL
Av. Independencia S/N
Ciudad Universitaria
Central Tel 066 312510
Anexo 151

“Nftables como firewall a nivel del kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021”

por Axell Alberto Ñacari Valverde

Fecha de entrega: 20-jun-2022 11:39p.m. (UTC-0500)
Identificador de la entrega: 1860567608
Nombre del archivo: Tesis_Axell_Alberto_ACARI_VALVERDE_ok.pdf (3.2M)
Total de palabras: 19359
Total de caracteres: 108555

“Nftables como firewall a nivel del kernel de Linux para el filtrado de paquetes en entornos Open Source, 2021”

INFORME DE ORIGINALIDAD

3%	2%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	2%
2	likegeeks.com Fuente de Internet	<1%
3	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	<1%
4	repositorio.unsch.edu.pe Fuente de Internet	<1%

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		