FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:
Bach. Piñashca Huerta Roger Jhoel

ORCID: https://orcid.org/0000-0003-4123-1916

Asesor:
Mg. Caldas Núñez Jesús Manuel
ORCID: https://orcid.org/0000-0001-6051-0284X

Línea de Investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2022

APROBACIÓN DEL JURADO

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA

Presentado por:

Roger Jhoel Piñashca Huerta
AUTOR

Mg. Caldas Núñez Jesús Manuel
ASESOR

Aprobado por:

Mg. Bances Saavedra David Enrique
Presidente del jurado

Mg. Bravo Ruiz Jaime Arturo
Secretario del jurado

Mg. Sialer Rivera Maria Noelia
Vocal del jurado

DEDICATORIA

Este trabajo está dedicado a mi querida madre, que siempre me brindó apoyo para lograr mis metas. A mi familia, por ser siempre mi soporte y a mis profesores de los que aprendí día tras día y la motivación continua que me brindaron para el desarrollo de mi formación profesional.

AGRADECIMIENTO

Mi agradecimiento principalmente está dirigido Dios y mi familia por ser el motor que siempre me motivó a cumplir mis metas, también mi agradecimiento a todos los profesionales que me acompañaron durante este camino, orientándome en todo momento

RESUMEN

La presente investigación realizada tiene como objetivo la evaluación de las técnicas de hacking ético sobre la seguridad informática que permitan diagnosticar las vulnerabilidades, en la Municipalidad distrital de los Olivos, Lima. Es de tipo cuantitativo y de diseño no experimental. Tuvo como población las ocho técnicas de Hacking ético más utilizadas y como muestra solo tres técnicas; la DDOS, escaneo y ataque por fuerza bruta. Como primer punto se realizó un análisis de las Vulnerabilidades de los servidores que tenemos como muestra. Se recopiló la información de los puertos y protocolos para identificar los servicios que se ejecutan. Se trabajó directamente con un equipo autorizado con acceso directo a toda la red, Los resultados indicaron la existencia de vulnerabilidades en la red actual de trabajo. Llegó a la conclusión que la actual situación de la seguridad informática de la Municipalidad de los Olivos es deficiente, dado que en su estructura lógica y física presenta muchas falencias, estando expuesto a ataques y la evaluación del sistema indica que el servidor se encuentra activo según el escaneo al host. El servidor se encuentra activo (Host is up) y se muestran latencias tiempo que tarda en transmitirse un paquete de datos dentro de la red) son variadas en las diversas IP y los puertos se muestran cerrados. Se encontró 6 vulnerabilidades de los cuales la mayor cantidad es CVE-2007-6750

Palabras clave; Técnicas de Seguridad, Sistemas Operativos, Hacking ético, Seguridad informática, Vulnerabilidad.

ABSTRAC

The objective of this research carried out is the evaluation of ethical hacking techniques on computer security that allow diagnosing vulnerabilities, in the district Municipality of Los Olivos, Lima. It is of a quantitative type and of a non-experimental design. It had as a population the eight most used ethical Hacking techniques and as a sample only three techniques; the DDOS, scan and brute force attack. As a first point, an analysis of the vulnerabilities of the servers that we have as a sample was carried out. Port and protocol information was collected to identify the services that are running. We worked directly with an authorized team with direct access to the entire network. The results indicated the existence of vulnerabilities in the current work network. It came to the conclusion that the current situation of computer security in the Municipality of Los Olivos is deficient, given that in its logical and physical structure it has many shortcomings, being exposed to attacks and the evaluation of the system indicates that the server is active according to scanning to host. The server is active (Host is up) and latencies are shown (time it takes for a data packet to be transmitted within the network) they are varied in the different IPs and the ports are shown closed, scanning and brute force, 6 vulnerabilities were found, of which the largest number is CVE-2007-6750

Keywords; Security Techniques, Operating Systems, Ethical Hacking, Computer Security, Vulnerability.

INDICE DE CONTENIDOS

DEDICATORIA iii
AGRADECIMIENTO iv
RESUMEN v
ABSTRAC vi
INDICE DE CONTENIDOS vii
ÍNDICE DE TABLAS viii
INDICE DE FIGURAS viii
I. INTRODUCCION 10
1.1. Realidad Problemática 10
1.2. Antecedentes de estudio 13
1.3. Teorías relacionadas al tema. 19
1.4. Formulación del Problema 30
1.5. Justificación e importancia del estudio 30
1.6. Hipótesis 31
1.7. Objetivos 32
II. MATERIAL Y METODOS 33
2.1. Tipo y diseño de Investigación 33
2.2. Población y muestra 33
2.3. Variables y operacionalización 34
2.4. Técnicas e instrumentos de recolección de datos 35
2.5. Procedimiento de análisis de datos 38
2.6 Criterios éticos 39
2.7. Criterios de rigor científico 39
III. RESULTADOS 40
3.1. Resultados 40
3.2. Discusión de los resultados 71
3.3. Aporte científico 72
IV. CONCLUSIONES Y RECOMENDACIONES 75
REFERENCIAS 77

ÍNDICE DE TABLAS

Tabla 1 Servidores de la municipalidad de los Olivos evaluados 40

Tabla 2 Evaluación de parámetros de la propuesta implementada…… 67

INDICE DE FIGURAS

Figura 1 Nivel de vulnerabilidad de información en América Latina …….. 12

Figura 2 Fases del Hacking …….. 26

Figura 3 Diseño de investigación ……. 33

Figura 4 Fases de la metodología ISSAF …….. 36

Figura 5 Resultado de comando nmap --script dos -Pn 192.168.90.48 40

Figura 6 Resultado de comando nmap --script dos -Pn 192.168.90.49…. 41

Figura 7 Resultado de comando nmap --script dos -Pn 192.168.90.33… 41

Figura 8 Resultado de comando nmap --script dos -Pn 192.168.90.74….. 42

Figura 9 Resultado de comando nmap --script dos -Pn 192.168.90.5….. 42

Figura 10 Resultado de comando nmap --script dos -Pn 192.168.90.47…. 43

Figura 11 Resultado de comando nmap --script dos -Pn 192.168.90.23… 43

Figura 12 Resultado de comando nmap --script dos -Pn 192.168.90.29…. 44

Figura 13 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.48…….. 45

Figura 14 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.49…….. 46

Figura 15 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.33……. 47

Figura 16 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.74…… 48

Figura 17 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.5……. 49

Figura 18 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.47……. 50

Figura 19 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.23……. 51

Figura 20 Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.29……. 52

Figura 21 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.48…….. 53
Figura 22 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.49…… 54
Figura 23 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.33……. 55
Figura 24 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.74……. 56
Figura 25 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.5 …….. 57
Figura 26 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.47……. 58
Figura 27 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.23…… 60
Figura 28 Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.23 …….. 61
Figura 29 Presentación y detalle de Resultados usando Métricas CVSS… 60
Figura 30 Vulnerabilidades…….. 63
Figura 31 Análisis de servidores……. 64
Figura 32 Vulnerabilidad CVR-2007-6750……. 65
Figura 33 Vulnerabilidad CVR-2009-3103……. 65
Figura 34 Vulnerabilidad CVR-2012-0002…… 66
Figura 35 Vulnerabilidad CVR-2012-0152…… 66
Figura 36 Vulnerabilidad CVR-2014-3566…… 67
Figura 37 Vulnerabilidad CVR-2017-0143…… 67
Figura 38 Modelo propuesto para la seguridad informática de la municipalidad distrital de los Olivos……. 69
Figura 39 Resultados de evaluación de parámetros de seguridad informática……. 71

I. INTRODUCCION

1.1. Realidad Problemática

Las amenazas a la red de datos y las infraestructuras de servidores de las entidades comerciales, sufrieron un cambio con el pasar del tiempo.

Alrededor del planeta Cuando hablamos sobre la seguridad informática y sus diversas técnicas de hacking ético, las personas sin conocimiento acerca de este tema consideran que son términos que no tienen relación. Piensan que es imposible para un hacker ser ético o tener un noble propósito, pero los profesionales capacitados en la ciberseguridad saben que no todo es malo. Si precedemos el término, pirata informático se refiere a cualquier persona con conocimiento avanzado de todos los procedimientos y técnicas centrados en el campo de la computadora y el funcionamiento de los sistemas de información, independientemente del uso que se haga de ese conocimiento.

Sin embargo, los crackers son piratas informáticos maliciosos cuyo objetivo es dañar, ocultan malas intenciones oscuras en cada una de sus actividades en las redes informáticas, esto incluye la red de datos y los servidores. Al principio cualquier amenaza era de una magnitud mínima, debido a la ralentización de los equipos; con el paso del tiempo sistemas completos se empezaron a descomponer, borrando archivos o extrayendo información confidencial de las instituciones. Por lo tanto, para proteger estos sistemas, el administrador limita el acceso de los equipos, lo cual llevo a la creación de crackers los cuales son amenazas más destructivas y estructuradas.

Para ellos no hay ética y generalmente trabajan solos o para organizaciones criminales con quienes pueden intercambiar los datos confidenciales obtenidos en el desarrollo o despliegue de su intrusión, para extorsionar a la víctima si quieren que todo vuelva a la normalidad.

Hubo muy pocos ataques o penetraciones iniciales porque se lograba la ralentización del equipo; luego comenzaron a deteriorar el sistema completamente, luego se borraba se extraía información muy confidencial o se borraban archivos de las empresas. En vista de esto, para proteger el sistema, el administrador debe jugar un papel muy importante al restringir el acceso a los equipos informáticos, tanto como sea posible. por lo tanto, los crackers iniciaron lanzaron ataques. Más destructivo y estructurados.

Los hackers informáticos, no tienen ninguna mala intención, generalmente hay casos de hacking ético en el sentido de penetrar o infiltrarse deliberadamente en las redes de datos de una organización para detectar y analizar sus debilidades, y así poder mejorar la seguridad en esos puntos. y evitar posibles ataques cibernéticos en el futuro que puedan comprometer la seguridad de la infraestructura.

El término "hacking ético" tiene muchos enfoques positivos y negativos. Siendo una de las razones la unión de las palabras “ético” definido como “positivo”, y "hacking” que no lo es.

Según el artículo el laborado por Shanmugapriya. (2015). Nos define hacking como: Técnicas y procedimientos de ataques de intrusión utilizados por sujetos denominados hacker y cracker, existen dos tipos de hacker el de sombrero blanco el cual es conocido como hacker ético, su principal actividad es la de proteger la información de las personas y empresas, también encontramos a hacker de gorro negro , el cual no tiene un propósito y solo realiza ataques causando daño, sobre los cracker estos sujetos son denominados como delincuente cibernético ya que realizan ataques con fines maliciosos y lucrativos.

Según el artículo elaborado por Taiwán, Wang y Yang (2017). Afirma que de acuerdo a las noticias de CNBC sobre el panorama de amenazas, indican expertos en seguridad global de la empresa FORTINET que “cada minuto, se está realizando alrededor de medio millón de ataques en el ciberespacio, además los hackers están

lanzando ataques más sofisticados tratando de dañar o burlar el sistema de seguridad.

Gran cantidad de empresas sienten la preocupación, quieren evitar ser parte de un fraude. Estos casos generalmente se dan por infecciones de malware, siendo de menor preocupación a diferencia de los ataques de denegación de servicios.

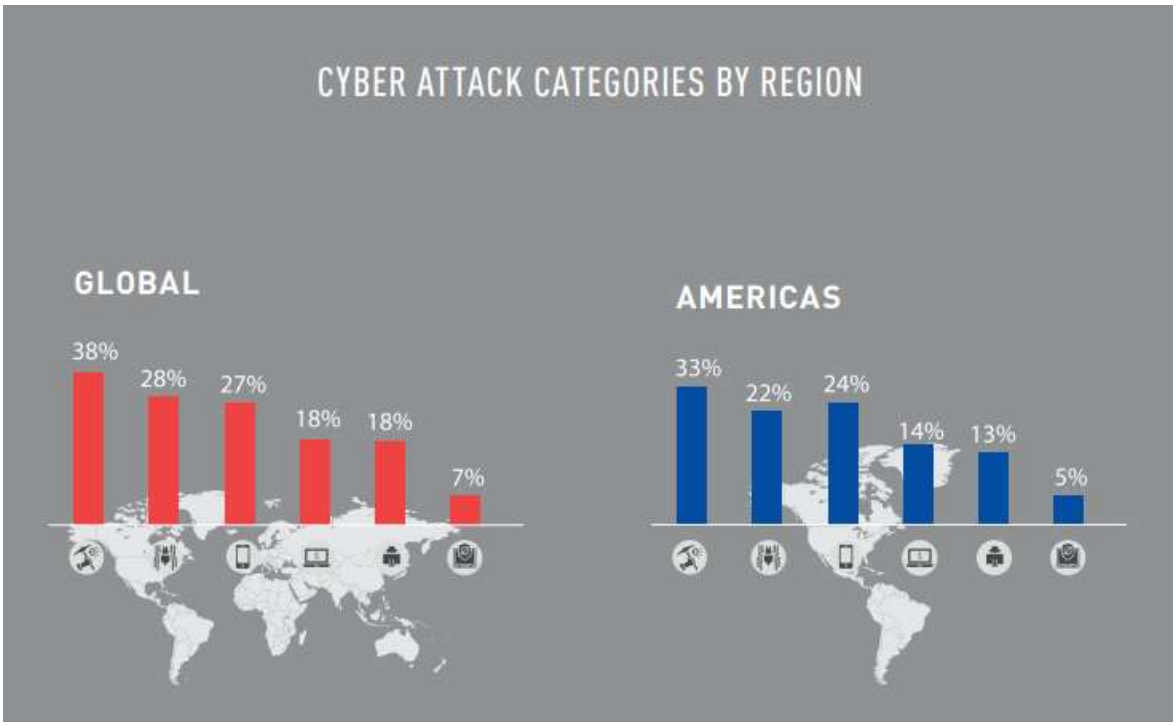


Figura 1: Nivel de Vulnerabilidad de información a nivel de Latinoamérica
Fuente: Symantec Security Response, 2020

A nivel nacional el uso de las técnicas hacking ético en el Perú abre de manera continua nuevas puertas en el campo y la seguridad informática y resulta cada vez más importante para las empresas medianas y pequeñas contar con el servicio de seguridad informática. Es así que es necesario aplicar Técnicas de Hacking Ético, Prueba de Intrusión o análisis de Penetración, el cual es una práctica habitual que cuenta con distintos procedimientos para conocer el nivel de seguridad y vulnerabilidad que posee una institución, organización o entidad estatal o gubernamental. El trabajo de los hackers éticos no deja de ser una especie de consultoría de ciberseguridad o análisis de vulnerabilidades, porque tienen que acceder a las redes y sistemas informáticos de cada empresa, con la finalidad de

buscar y analizar las vulnerabilidades, luego diseñar una estrategia eficiente para lograr mitigar el impacto que pueda causar. Un hacker ético cumple la función de hallar las vulnerabilidades antes que un cibercriminal, evitando el robo o la malversación de datos. Estando pasos delante de profesionales en ciberdelitos. Utilizando todas las herramientas o instrumentos para encontrar y resolver problemas de riesgo potencial en los sistemas informáticos.

Con la finalidad de equilibrarlo aparece el Ethical Hacking o Hacking ético, el cual tiene la función de determinar las debilidades. Permitiendo a las instituciones poder prepararse con anticipación para no sufrir ataques masivos a sus sistemas en el momento que estos se exponen. Mientras que cada mínima debilidad es la oportunidad para que estos atacantes organicen sus perpetuaciones e intervenciones. De este modo se obtiene información delicada de las diferentes empresas, siendo utilizadas con intenciones maliciosas. Los hackers éticos utilizan escenarios de práctica conocidos como pen-testing, para poder salvaguardar la información, provocando una mayor atención en los sistemas de seguridad de las instituciones.

A nivel local – institucional, en la actualidad se ha visto afectado muchas entidades públicas y privadas la mayoría son del departamento de Lima. Debido a los constantes ataques informáticos que realizan los ciberdelincuentes.

Por lo cual se realizó un análisis de las herramientas del hacking ético, para que se realice una evaluación y diagnóstico de los puntos de riesgo en la seguridad del sistema. Así se logre determinar la eficacia, clasificación y mitigación de las técnicas que se han utilizado para defender a las redes de datos.

1.2. Antecedentes de estudio

Existen varios trabajos de investigación relacionados al tema como:

Según Oñate & Martínez (2017), investigó la seguridad que ofrecía los sistemas de información del Gobierno Provincial de Imbabura. Habiendo utilizado la norma

ISO/IEC 27001:2005, siendo en la que se basó la investigación del presente trabajo. La norma determino 3 requerimientos primordiales para lograr realizar un análisis eficiente de los modelos para establecer información segura, el primero fue la recopilación de los datos del Gobierno Provincial de Imbabura. Además, se utilizó el Hacking Ético, basada en el black-box (caja negra), detectando múltiples debilidades en su sistema, en el Gobierno el desinterés por la seguridad cibernética puede resultar en una ola de problemas de vulnerabilidad informática. El hacking ético se puede realizar desde cualquier parte del planeta y con diferentes intenciones dependiendo únicamente de la persona. Luego de la identificación de los problemas se determinó los controladores más eficientes según la norma ISO/IEC 27001:2005, También se realizó un planteamiento del riesgo potencial de la información del Gobierno Provincial de Imbabura, implementando controladores que garanticen una protección reforzada de los datos.

Yien Wang, Jianhua Yang (2017) Institución O Journal. - Ieee Xplore, El Tema Que Aborda “Ethical Hacking And Network Defense: Choose Your Best Network Vulnerability Scanning Tool”, problema que enfrentó fue las Amenazas a la infraestructura de red de ordenadores, se realizó el análisis de vulnerabilidades en una red diseñada en un laboratorio virtual, Los resultados del análisis de vulnerabilidades incluyen tipo de vulnerabilidad, gravedad y el tipo de puerto disponible, después de reunir las direcciones ip, y puertos abiertos y la información del sistema operativo. De acuerdo con el artículo, el software openvas es una herramienta adecuada para el hacking ético realizando análisis de vulnerabilidades.

Patil, Jangra, Bhale,y Raina (2017) en su investigación Institución O Journal Ieee Xplore, El Tema Que Aborda “Ethical Hacking: The Need For Cyber Security”, problema que enfrentó fue Las organizaciones pueden ser dañados por software o intrusos ocasionando perdida de información, se tuvo que aprender conceptos de piratería informática y su aplicación para asegurar los sistemas de cualquier organización, resultados que se obtuvo reconocimiento, se recopilo información preliminar, máquinas activas, puertos abiertos puntos de acceso a so, visualizar todos los servicios según el puerto de red. Escaneo y recuento, en el segundo paso se realiza pruebas de penetración haciendo uso de técnicas de análisis,

conclusiones de acuerdo con el artículo, el hacking ético debe ser practicada, con un conocimiento básico de las redes y la seguridad cibernética.

López (2017) Institución O Journal Ieee Xplore, Aborda el tema de “Pentesting On Web Applications Using Ethical Hacking”, donde las organizaciones priorizaban la velocidad y el software de las apelaciones web, sin tomarle atención a la seguridad. En el cual se determinó las técnicas de penetración, y usando instrumentos de software se establecieron los puntos vulnerables. Que se hizo, describir las diferentes técnicas y pruebas de penetración, utilizando diferentes herramientas basadas en software para establecer posibles vulnerabilidades en una aplicación web, resultados obtuvo después de realizar el análisis de la información, que ninguna aplicación web es perfectamente segura y libre de ataques, pero con el uso de técnicas y test de intrusión, pentestin y herramientas de hacking ético, las vulnerabilidades pueden ser superadas evitando futuros ataques. Conclusiones relevantes, cómo nos indica el artículo, en la actualidad la información que se maneja es muy amplia que dependemos de los sistemas en gran medida, también indica que muchas empresas se preocupan por el desarrollo, pero mas no por la seguridad de sus sistemas.

Lehrfeld y Guest (2016) Institución O Journal Ieee Xplore, Tema Que Aborda “Building An Ethical Hacking Site For Learning And Student Engagement”, problema que enfrentó ataques de acceso no autorizado, robo de credenciales de inicio de sesión. se realizó la creación de escenarios realista con el objetivo de realizar ataques y tener acceso a los datos de los usuarios y clientes de una página web, resultados en la prueba de penetración, la vulnerabilidad principal que se encontró es inyección sql. Conclusiones, según el artículo usar técnicas de hacking ético nos ayuda, identificar los tipos de ataque comunes en los sitios web y los métodos para corregir las vulnerabilidades descubiertas, crear plataformas de ataque para el aprovechamiento de las tecnologías basadas en la web, evaluar cómo un determinado ataque puede ser mitigado para prevenir la explotación futura.
Zouheir y Ibrahim (2013) Institución O Journal Ieee XploreTema Que Aborda “Teaching Ethical Hacking In Information Security Curriculum: A Case Study” problema que enfrentó, Ataques DDOS que intenta inhabilitar el sistema o ralentizar

para los usuarios legítimos por la sobrecarga de los recursos para que nadie más pueda acceder. se realizó un ejercicio práctico en un entorno de laboratorio aislado sobre los ataques más comunes de denegación de servicios resultados obtuvo, los ataques DDOS son muy comunes en las pruebas realizadas en el laboratorio se muestra cómo afecta el ataque en el tráfico de red y colapsar el servidor mientras dura el ataque conclusiones relevantes, según el artículo la implementación de ejercicios prácticos en laboratorios sobre ataques de denegación de servicios, permiten a los estudiantes comprender mejor las formas en las que los sistemas de seguridad fallan por lo tanto es necesario aprender técnicas y métodos para ser capaz de aplicar soluciones de seguridad adecuadas y proteger de manera más eficiente una organización.

Sambasiva, Naveen , Swetha y Bhanukiran (2014) Institución O Journal Ieee Xplore Tema Que Aborda “Security Assessment Of Computer Networks –An Ethical Hacker’s Perspective” Problema Que Enfrentó, seguridad en la red de computadoras que se hizo, analizar y evaluar la seguridad de las redes informáticas, usando técnicas de seguridad de código abierto resultados los problemas de seguridad de la red pueden ser revelados usando herramientas de seguridad como nmap, nessus y sqlmap, con el nmap se escanea los puertos utilizados por los servicios que están en uso en la red de computadoras, se ejecutó la herramienta nmap obteniendo información detallada sobre los puertos con los protocolos tcp y udp que se encuentran abiertos, también se realizó el uso de nessus encontrando vulnerabilidades en los servicios de los sistemas, en este caso al explorar las vulnerabilidades de un computador encontramos que el navegador y reproductor flash no se encuentran actualizados y nos indica que tiene un alto grado de vulnerabilidad, también se realizó ataque de inyección sql haciendo uso de la herramienta sqlmap realizando el ataque de inyección sql revela, los datos de usuarios, id y la forma has de las contraseñas. Conclusiones, Los ataques a la seguridad están en aumento, haciendo uso de herramientas sofisticadas, al realizar la evaluación de la seguridad de las redes informáticas usando nmap, nessu y sqlmap junto con técnicas, revelo la información de los servicios de parche no cumplieron con la seguridad, los resultados del trabajo de evaluación de la seguridad ayudan a mejorar la seguridad informática

Shanmugapriya (2013) Institución O Journal Ieee Xplore Tema Que Aborda “A Study Of Network Security Using Penetration Testing” Problema Que Enfrentó, Robo de información (correo electrónico, cuentas de tarjeta de crédito, sitios de compras en línea, transmitir información de las organizaciones al internet) que se hizo, describe métodos de hacking ético y la forma en que se lleva a cabo en la red y como ayudan a resolver los agujeros de seguridad resultados, es común los ataques usando métodos de penetración, pero con el uso del hacking ético uno conoce el proceso y funcionamiento de los métodos de hacking, de esta manera para estar prevenidos revisar si las direcciones de correo que recibimos son de entidades confiables en el tema del ataque de fuerza bruta, los sistemas han mejorado el método de inicio de sesión aumentando la longitud de la contraseña y añadiendo símbolos y la cantidad de intentos en el inicio de sesión. Conclusiones; según el artículo es necesario conocer los métodos de hacking para aprender y conocer la realidad, el hacking ético no es un crimen, pero el que hace mal uso del conocimiento comete un crimen.

Shetty, Rithika, Tanisha y Souza (2018) Institución O Journal. - Ieee Xplore Tema Que Aborda “Survey Of Hacking Techniques And It's Prevention” problema que enfrentó, actividades de intrusión no autorizada por acceder y manipular los datos a través de la red que se hizo, uso de técnicas de hacking ético, de forma correcta para encontrar fallas resultados, el uso de ataques con técnicas de hacking, nos ayuda a comprender desde varias perspectivas los conocimientos básicos para la aplicación de técnicas de hacking, con la finalidad de garantizar la seguridad de los datos confidenciales, es importante proteger la red de piratas informáticos la mejor manera es pensar como ellos. Conclusiones el hacking ético está tomando forma a medida que las empresas crecen y también dependen de la tecnología, es importante tomar medidas preventivas el hacking ético es una opción para mitigar el riesgo de un ataque.

Giannone, Martins, Amatriain, Rodríguez y Merlino (2016) realizaron una investigación que Aborda el tema “Survey Of Hacking Techniques And It's Prevention”, problema que enfrentó vulnerabilidades residuales hacen ineficaz la

seguridad de la información que se hizo, evaluación de la seguridad de un sistema tiene que cumplir con responder lo siguiente
¿En los sistemas atacados que podría ver un intruso?, ¿Qué podría hacer con esa información el intruso?, ¿En el sistema alguien se podría dar cuenta de los éxitos o ataques del intruso?
Buscando la implementación del hacking ético para evitar amenazas futuras. el aporte a los encargados de testing de instrumentos de ayuda técnica con los cuales se contrarrestarán los problemas actuales. Conclusiones, de acuerdo con el artículo, vemos que es necesario contar con profesionales que tengan conocimiento en seguridad informática, también es necesario realizar el testeo de software para encontrar las posibles vulnerabilidades haciendo uso de herramientas de hacking ético.

Hidalgo, Tupiza, Sánchez y Tarquino (2016) realizaron una investigación sobre "Security Policies Of Corporate Multiservice Network; Employing Ethical Hacking" problema que enfrento, la red de datos y voz de la entidad de multiservicios no cumple con los estándares de calidad de servicio, falta de políticas de seguridad en los servidores, personal técnico sin capacitación en seguridad informática, mínimos mecanismos de seguridad en los servidores, no hay políticas de seguridad, cableado estructurado deteriorado, carencia de organización física, inadecuados medios de comunicación entre los cuartos de comunicaciones, rediseño de intranet, determinar parámetros de seguridad existente - utilizar técnicas de hacking ético para evaluar la red. Resultados, al realizar ataques: haciendo uso de footprinting maltego determinó los accesos ocultos o puertas traseras (backdoors), dominios ligados a la entidad quito.gob.ec se encuentran expuestos en el internet, cuenta con 26 dominios que pueden ser blanco de ataques. la segunda herramienta scanning haciendo uso de nmap, se encontró puertos abiertos en los servidores de la institución. Con la herramienta enumeración dnsmap se encontraron subdominios que podrían ser explotados mediante técnicas de ataque basados en dominio para escalar privilegios dentro de la red, troyanos haciendo uso de ettercap no se pudieron obtener datos ya que el antivirus bloqueo el ataque la ultima el cual es hacer uso de la ingeniería social se llegó obtener información de los switch y router. Conclusiones, de acuerdo con el artículo, es necesario hacer uso de las

buenas prácticas en los servidores , cerrar todos los puertos y luego abrir los que son necesarios, también mantener los sistemas operativos actualizados para tener un mayor grado de seguridad, también se recomienda cambiar las credenciales de acceso en un periodo de 30 días también es necesario mantener un cronograma de backups y respaldo de información y estar en constante monitoreo de los servidores para evitar cualquier perdida de información, la información es sensible y crítica por lo que es necesario protegerla de los ataques de intrusos con este fin se hace uso del hacking ético.

Según Aguilar & De la Cruz (2015), definen que las empresas del mercado fueron competidoras de las de las grandes entidades financieras. Esto se debe a la baja en los intereses, y su magnífica atención al cliente. Donde utilizó sistemas web y tecnológicos, por lo cual se recomendó usar una red informática privada debido a que se necesita minimizar los riesgos, ya que su objetivo es mejorar la seguridad de los datos.

Según Fernández (2017), determinó que la finalidad fue probar la seguridad y el rendimiento de la transferencia de información, procediendo por el análisis de los registros o los patrones VPN. Por lo que con las ejecuciones RPV, es de mucha ayuda tanto en la seguridad, confianza y en lo económicos, generando usuarios de conexiones remotas, por lo que la sobrecarga de las redes VPN no afectaran de gran manera a las redes de datos.

1.3. Teorías relacionadas al tema.

1.3.1 Hacking Ético

Se define como un profesional ético, con habilidades generales para la elaboración de evaluación en los sistemas, utilizando un criterio transversal. Aunque, también se describe como un servicio de auditoria tecnológica de información ofrecida por compañías dedicadas.

Según Astudillo (2017), La importancia radica en defenderse de todas las maneras posibles puesto que la finalidad del Ethical Hacking, es proteger los sistemas de información de las instituciones y repeler amenazas.

Por otro lado, Astudillo (2017) manifiesta que el Ethical Hacking busca evaluar las amenazas a los que pueden estar expuestos los sistemas, realizando prácticas con la finalidad de analizar la seguridad de la base de datos, redes, aplicaciones, entre otras.

A). Tipos de Hacking ético

Según Hurtado & Mendaño (2016) existen diversos tipos de pruebas frente a las penetraciones del Ethical Hacking, siendo:

- Pruebas de penetración con objeto: Analiza las debilidades de los sistemas.
- Pruebas de penetración sin objeto: Analiza todos los elementos del sistema de información
- Pruebas de penetración ciega: Es de carácter público y puede ser usada por cualquier institución.
- Pruebas de penetración informadas: De carácter privado y cuentan con acceso especial otorgado por su misma institución.
- Pruebas de penetración externas: Realizadas dentro de las empresas con la finalidad de analizar las políticas y los mecanismos externos.
- Pruebas de penetración internas: Realizadas dentro de las empresas con la finalidad de analizas las políticas y los mecanismos internos.

B). Técnicas de Hacking Ético

a. Técnica De DDOS

Denominada también denegación de servicio realiza ejecución de ataque para aprovecha las vulnerabilidades de diferentes capacidades específicas que son aplicadas a cualquier recurso de red uno del servicio es la web que ejecuta una entidad en su infraestructura. Al ejecutar ataque DDOS envía un conjunto de solicitudes en simultaneo al recurso web atacado con la intención de saturar, desbordar la máxima capacidad del servicio web que almacena el sitio web con la finalidad de realizar y proceso de gestión con varias solicitudes para ocasionar y evitar el funcionamiento correcto.

Los objetivos al ejecutar el ataque DDOS más común es:

- Sitios de compras por Internet también denominado mercado online.
- Casinos en línea o casa de apuestas online
- Empresas u organizaciones que dependa de la prestación de servicios en línea para la actividad diaria.

Cómo funciona la Técnica de ataque DDoS

Los servicios que ejecutan recursos de red como los servidores web. Cuentan con un límite máximo definido de cantidad solicitudes simultáneos que pueden dar respuesta, entregar la información en un mismo tiempo. Además, la ejecución de la máxima capacidad del servidor, el servicio de internet que tiene conexión con el aplicativo web a través del servicio de internet tiene el ancho de banda limitado. Cuando la ejecución del número de solicitudes excede los límites permitidos de la capacidad de los componentes de la infraestructura también se ve afectada, probablemente la ejecución del nivel de servicio se vea afectado de alguna forma:

- La ejecución de la respuesta junto a solicitudes estará con mucha lentitud y más lenta de lo normal.
- Algunas o todas las ejecuciones de solicitudes de los usuarios pueden ser rechazados.

Como política o regla general, la principal intención del atacante al ejecuta DDOS es evitar por completo el proceso del funcionamiento normal del recurso que cuenta con el servicio web, logrando un bloqueo total del servicio. El atacante quien ejecuta el proceso también puede solicitar un pago para detener el proceso del ataque en ejecución. En otros casos, el objetivo principal del ataque DDOS es la de dañar la Imagen de in competidor realizando ataques que afectan la vulnerabilidad del servicio en ejecución.

La ejecución y proceso de uso de una RED ZOMBI denominado botnet que permite realizar el ataque DDoS

Para ejecutar y enviar una cantidad considerable y grande de solicitudes al recurso de la víctima.

El cibercriminal ejecuta a menudo con el propósito de establecer una RED ZOMBIE de computadoras infectadas.
Según la ejecución del ataque a medida que se desarrolla el criminal informático tiene la capacidad de controlar los procesos y acciones de cada computadora infectada que se encuentre en la red zombie. La gran cantidad de ataques informáticos puede saturar la conexión dejando sin servicio a los usuarios.

La naturaleza amenazas DDOS en la actualidad

Entre los principios la ejecución en la década de 2000 habla sobre esta actividad criminal era bastante común hacer uso de técnicas de DDOS. Sin embargo, la ejecución ataques DDoS exitosos ha reducido en los últimos años. Esta disminución la cantidad de ataques DDoS probablemente se logró resolver el problema.
- Investigaciones policiales realizadas que culminaron con el arresto de criminales en todo el mundo.

Desbordamiento UDP

En este caso, el atacante usaría paquetes IP que contienen datagramas UDP para inundar puertos de víctimas aleatorios. La víctima busca servicios relacionados y, cuando no hay nada, devuelve un paquete de "destino inaccesible". Por lo que mientras más reciba y responda empieza a saturarse la red de los demás clientes.

b. Ataques de amplificación basados en UDP

El proceso de realizar este tipo de ataque se basa en saturar otros servicios, como DNS (traducción de nombres en Internet a IP), NTP (servicio de sincronización de reloj basado en la hora internacional del dispositivo a través de servicios de Internet) o SSDP (busque UPnP en dispositivos de servicios de red) enviando una gran cantidad de paquetes UDP. Se llama De Amplificación al

envío de paquetes de datos usando técnicas para exagerar el tamaño de los paquetes UDP desarrollando un proceso muy poderoso para el ataque.

Ping de la muerte

En este caso, el atacante utiliza un simple comando ping para enviar paquetes ICMP con formato incorrecto (ligeramente por encima del límite estándar de 65 535 bytes). Cuando el servidor de la víctima intenta reconstruir estos paquetes, consume una gran cantidad de recursos; cuando la cantidad de paquetes enviados a través de ping aumenta exponencialmente, el servidor se congela.

Hay otros ataques, como NUKE y SMURF (pitufo), que también utilizan vulnerabilidades del protocolo IP y mensajes ICMP para provocar la saturación de la red y eventuales desbordes.

c. Técnica Ataque Por Fuerza Bruta

Técnica que posibilita probar la totalidad de las combinaciones hasta que se encuentre un texto o palabra para obtener una contraseña. Imagínese que no es más que una caja negra, donde se conoce la salida y el proceso NPI (no tengo información), y todo lo que se sabe es que debe recibir una entrada legible para ser encriptada.

Los ataques de fuerza bruta ocurren cuando los atacantes usan ciertas técnicas para probar combinaciones de contraseñas para descubrir las credenciales de víctimas potenciales y así obtener acceso a cuentas o sistemas. Hay muchos tipos de ataques de fuerza bruta, como, ataques de diccionario, ataques de fuerza bruta inversa o ataques de rociado de contraseñas. En los casos en que la contraseña es débil o relativamente fácil de predecir, los ataques de fuerza bruta suelen tener más éxito.
El término "fuerza bruta" asociado con los incidentes de seguridad informática está relacionado con el intento de encontrar una o más contraseñas. Estos se pueden vincular para acceder a servicios en línea o archivos y mensajes

encriptados. En cualquier caso, el atacante probará varias combinaciones hasta encontrar la combinación correcta. Para ello, se basa en software, hardware y el uso de algoritmos y diccionarios de palabras.

Un ataque de fuerza bruta, también conocido como búsqueda exhaustiva, es un truco criptográfico que se basa en adivinar las posibles combinaciones de una contraseña específica hasta que se descubra la contraseña correcta. Cuanto más larga sea la contraseña, más combinaciones necesitará probar. Un ataque de fuerza bruta puede llevar mucho tiempo, es difícil de realizar si se utilizan métodos como la ofuscación de datos y, en ocasiones, es imposible. Sin embargo, si la contraseña es débil, podría tomar segundos sin apenas esfuerzo. Las contraseñas débiles son como disparar peces en un barril para los atacantes, por lo que todas las organizaciones deben aplicar una política de contraseña segura en todos los usuarios y sistemas.

d. Técnica De Escaneo de la red

El escaneo de puertos es una técnica utilizada por piratas informáticos y administradores (no para hacer distinciones) para auditar máquinas y redes con el fin de saber qué puertos están abiertos o cerrados, los servicios que se ofrecen, verificar la existencia de un cortafuego y verificar su operación y algunas otras cosas. Es la técnica más utilizada al ingresar a un sistema y realizar un análisis preliminar del sistema.

El escaneo de red es el proceso de identificar hosts activos en la red para atacarlos o evaluar la seguridad de la red. Los escáneres (como los escaneos de ping y los escaneos de puertos) devuelven información sobre las direcciones IP asignadas a los hosts activos en Internet o la red local y los servicios que brindan. Otro método de escaneo, como el mapeo inverso, devuelve información sobre las direcciones IP que aún no se han asignado al host, lo que permite al atacante asumir direcciones viables para otras actividades.

El escaneo es uno de los tres componentes de la colección de inteligencia para un atacante. En la fase de huella, el atacante crea un perfil de la organización objetivo, que contiene información como su sistema de nombres de dominio (DNS) y servidor de correo electrónico o su rango de direcciones IP. La mayor parte de la información está disponible en línea. Durante la fase de análisis, el atacante busca información sobre una dirección IP específica a la que se puede acceder a través de Internet, su sistema operativo, la arquitectura del sistema y los servicios que se ejecutan en cada computadora. En la fase de enumeración, el atacante recopila información como nombres de usuarios de red y nombres de grupos, tablas de enrutamiento y datos del Protocolo simple de administración de redes (SNMP).

C). Fases del Hacking ético

Mieres (2010), para realizar un Hacking Ético, es necesario enmarcar los procedimientos en cinco pasos o fases, éstas fases ya son reconocidas por Certified Ethical Hacker, que es una acreditación para los profesionales de seguridad informática que es reconocida a nivel internacional que es otorgada por la compañía EC-Council.

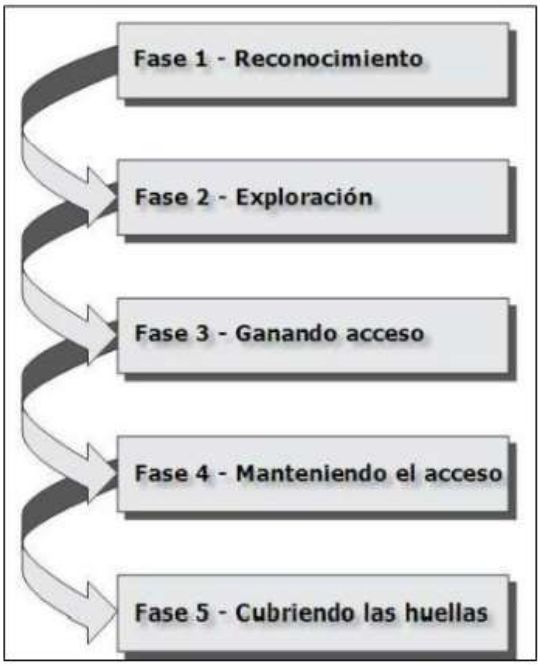


Figura 2. Fases del Hacking
Fuente: Certified Ethical Hacker Review Guide

Reconocimiento (Fase 1):

Esta es la fase inicial de una consultoría de Ethical hacking, ya que, en esta fase, el profesional Ethical Hacker se centrará en obtener la mayor cantidad de información de la empresa objetivo, esta búsqueda de información la realiza sin tener contacto directo con la organización, y para ello emplea todos los recursos de búsqueda disponibles en Internet. En este proceso la meta del profesional auditor, es recabar la mayor cantidad de información que posteriormente le servirá para perfilar y obtener un mayor porcentaje de éxito al momento de realizar el Hacking Ético.

Exploración (Fase 2):

En esta fase, el profesional que realiza la consultoría de Ethical Hacking, abarca un poco más y emplea una recopilación de información más agresiva, ya que, en esta fase el profesional interactuará directamente con la empresa objetivo en la búsqueda de servidores, direcciones IPs, y toda la información que le pueda ser útil al momento de realizar el análisis de vulnerabilidades y le permita tener un mayor porcentaje de éxito al momento de penetrar la seguridad de la empresa a través de una falla en la configuración y/o la existencia de una vulnerabilidad de sistema.

Ganando Acceso (Fase 3):

Es la fase donde se ponen a prueba los conocimientos del Hacker Ético, ya que, en esta fase se encargará de probar manualmente la explotación de las diferentes vulnerabilidades halladas en la fase de Escaneo de Vulnerabilidades. Dependiendo de los tipos de ataques que se realicen, el Hacker Ético podrá escalar privilegios y obtener un control total del sistema comprometido.

Mantener el Acceso (Fase 4):

Después de lograr el acceso a un sistema informático, ya sea a través de la explotación de una vulnerabilidad, fuerza bruta y/o ingeniería social, es importante mantener el acceso en el sistema, para lo cual el Hacker Ético dispone de una amplia variedad de herramientas y entre las más empleadas se encuentra la instalación de Troyanos, lo que le permite al Hacker ético disponer

de una puerta trasera para el acceso remoto al sistema informático comprometido.

Cubriendo Huellas (Fase 5):

Después de haber logrado el acceso al sistema informático, el hacker ético recopilará las evidencias necesarias para formular un reporte de entrega. También deberá realizar el borrado de huellas que pudieran dar indicios de que el sistema informático fue comprometido.

Prueba de Penetración Externa

El análisis que se realiza a través de pruebas de intrusión externa para validan las fortalezas y debilidades de la organización de forma externa a través del servicio de Internet.

Pasos para realizar una Prueba de Penetración Externa:

Pasos para realizar una prueba de penetración de red externa

1°- Se gestiona la topología de la red y se administra un inventario de manera completa de la estructura exterior.

2°- Se identifica las direcciones IP de cada elemento de la organización se va a evaluar (páginas web, servidor de correo, de web, etc)

3°- Se identifica la localización física de cada servidor, Neo trace, validando su uso.

4°- Se busca la información del registro de dominio de la empresa.

5°- Búsqueda de la información IP de la empresa en listas negras de internet.

Pasos para prueba de Penetración a la Red Interna

1**-** Se analiza la red interna para la identificación del número de subredes, número de equipos y el sistema operativo de ejecución.

2. escanea miento de los equipos de la red interna activos.

3. Escaneo individual de los equipos para la identificación de puertos vulnerables.

4. Obtención de accesos explotando vulnerabilidades que se conozcan en los equipos con el uso de herramientas hacking para comprometerlos.

5- Establecimiento de null sessions en los equipos, C:/net use //192.168.8/PC¨7u¨

6 Enumeración de usuarios e identificación de dominios en la red-

7- Realización de sniffing a la red.

8-Realización de sniffing a las contraseñas de POP3, FTP y Telnet

9. Realización de sniffing a los mensajes de email. Realización de ataques reproduciendo los LM Manager Heshes para el uso de la contraseña obtenida

10. Realizar ARP poisoning y MAC Flooding a los switches de la red.

11. Ejecutar el ataque man-in-the-middle

12. Pretender el ingreso a las consolas de los equipos, con el uso de las contraseñas por default. Dar inicio a los equipos con el uso de un Live CD para el robo del archivo SAM.

13. Intentar instalar keylogger en cada equipo para el robo de contraseñas

14. Intentar instalar keylogger en hadware en cada equipo para el hurto de contraseñas.

15. Tratar de instalar un spyware en los equipos, para el monitoreo de información de los usuarios de internet.

1.3.1.1. Seguridad informática

Según (López, 2015). La definió como la protección de los sistemas de información de los computadores y los dispositivos móviles, para administrar los aspectos vulnerables para poder defenderse ante ataques violentos.

Se relaciona con los conceptos básicos de seguridad, sin embargo, va encaminado hacia la información. Por lo que busca utilizar maneras, métodos, técnicas para proteger los datos de privacidad de las diferentes compañías. Debido a la gran importancia que tiene resguardar estos datos, lo que conlleva a que las empresas determinen políticas de seguridad convenientes.
Así mismo su finalidad es mitigar las amenazas tanto para las estructuras y toda la información almacenada.

Elementos de la Seguridad de la Información

Caracterizado por sus tres aspectos principales, siendo:
- **La Confidencialidad**
Limita la información únicamente a personas a las personas autorizadas, lo cual aumenta la privacidad de los datos y recursos.
- **La Integridad**
Garantiza información verídica y confiable para ser empleadas por las instituciones, asegurando que no se realizaran modificaciones de terceras personas.
- **La Disponibilidad**
Permite el acceso libre a cualquier información n que sea necesaria para los usuarios autorizados. Así se evita las interrupciones o un mal funcionamiento del sistema.

Los Riesgo en la seguridad Informática

En este aspecto nos podemos ver afectados por amenazas posibles, las cuales aprovechan las debilidades, haciendo que perdamos información o datos importantes.

La vulnerabilidad en la seguridad informática

Son las ventanas en los diversos sistemas por donde las amenazas logran cruzar, se pueden dividir en arquitectura, diseño o de configuraciones.

Objetivo de la Seguridad Informática

Busca proteger la información privada o personal en los hardware y software de las diversas instituciones. Adaptando métodos para facilitar la seguridad, resguardan sistemas, legales o económicos.

1.4. Formulación del Problema

¿Cómo la evaluación de las técnicas de Hacking ético influye en el análisis de vulnerabilidades de la seguridad informática en la municipalidad distrital de los Olivos?

1.5. Justificación e importancia del estudio

Justificación académica

Permitirá conocer las técnicas de hacking ético de la seguridad informática, de la Municipalidad distrital de los Olivos, evaluarlas y con nuestros conocimientos evaluarlas para mejorar la seguridad informática.

Justificación tecnológica

Actualmente la información física de la infraestructura de telecomunicaciones y los recursos informáticos (archivos, imágenes, base de datos, sistemas institucionales y transaccionales) son los activos de mayor importancia de una institución. Gran parte de estos activos se manejan haciendo uso de sistemas informáticos computarizados de uso constante por todos los usuarios de la sociedad (ciudadanos, empresas, organizaciones y sistemas de información). Un mal uso o de manera indebida de estos sistemas, por empleados que no se encuentran debidamente capacitados, son parte de un punto débil en las instituciones o empresas.

La seguridad en la infraestructura de red y los servidores, es necesario de una evaluación constante y permanente durante el funcionamiento sea por un periodo corto o largo. Dependiendo del rubro del negocio o industria a la que se dedica la institución o empresa, tendrá mayores o menores riesgo de ser posible víctima de ataques informáticos.

Esta investigación permitirá precisar ideas relacionados al impacto de una posible intrusión y con la evaluación de las Técnicas de Hacking ético se proporcionará o evidenciará soluciones para evitarlas, en diversos casos que se presenten.

Justificación social

La municipalidad, en el campo de las telecomunicaciones, contará con la seguridad informática de calidad para que las áreas y los usuarios accedan a información actualizada y se comuniquen de manera segura y rápida, coadyuvando a su desarrollo e integración como sociedad productiva.

Justificación tecnológica

Esta investigación permitirá conocer que las técnicas de hacking ético son parte de las herramientas modernas en seguridad informática para mitigar, resguardar y fortalecer a las organizaciones y corporaciones, evitando la acción de posibles intrusos que busquen las vulnerabilidades no se pueden tomar con rapidez; es muy importante que los actores de ciberespacio sean conscientes de los riesgos que se esconden en la red, porque están expuestos permanentemente. Es importante

Justificación teórica

Acorde a los antecedentes previos a la investigación, estos generaran discusión y reflexión a la vez, estas investigaciones hacen referencia sobre la evaluación de técnicas de Hacking ético en áreas y escenarios investigados como precedentes al que se les aplicó conocimientos teóricos de ingeniería.

Justificación metodológica

El presente trabajo aportará un nuevo modelo de seguridad informática en la siguiendo el proceso del método científico, el cual podrá ser utilizado por diversas empresas.

1.6. Hipótesis

La evaluación de Técnicas de Hacking ético influirá para mejorar la seguridad informática en la Municipalidad distrital de los Olivos, Lima.

1.7. Objetivos

1.7.1. Objetivo General.

Evaluar las técnicas de hacking ético sobre la seguridad informática que permitan diagnosticar las vulnerabilidades, en la Municipalidad distrital de los Olivos, Lima

1.7.2. Objetivos Específicos.

- **OE1;** Conocer la situación de vulnerabilidad de la seguridad informática, implementando técnicas sobre la red de datos de la Municipalidad distrital de los Olivos, Lima.

- **OE2;** Clasificar las vulnerabilidades detectadas sobre la seguridad informática en la municipalidad distrital de los Olivos.

- **OE3;** Proponer un modelo de mejora que permita garantizar la confidencialidad, integridad y disponibilidad de la red informática de la Municipalidad distrital de los Olivos, con medidas que mitiguen las vulnerabilidades ya clasificadas.

- **OE4;** Validar la propuesta de implementación de la red de informática de la Municipalidad distrital de los Olivos por especialistas en seguridad informática.

II. MATERIAL Y METODOS

2.1. Tipo y diseño de Investigación

Enfoque; La investigación presenta un foque cuantitativo, porque busca la interpretación numérica de los resultados en base a los datos recolectados.

Tipo; Presenta un descriptivo. Según Sabino (2015) la investigación descriptiva se basa en realidades de los hechos otorgando una interpretación precisa en un rango explicativo causal

Diseño; Es una investigación no experimental, las variables no se manipularon y solo se observó el fenómeno en un contexto natural para luego proceder con el análisis.

El diseño de la investigación se gráfica:

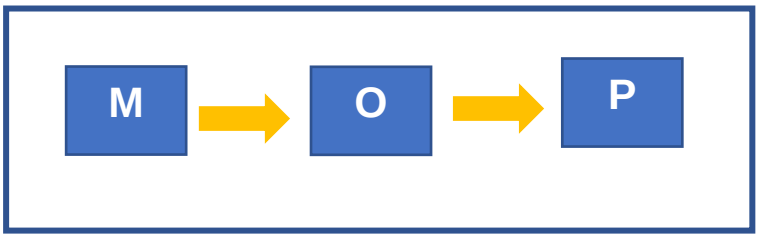


Figura 3: Diseño de investigación
Fuente: Elaboración del autor

Donde:

M = Muestra
O = Observación
P = Propuesta

2.2. Población y muestra

2.2.1. Población

Se consideró como población las 08 técnicas de Hacking ético más utilizadas actualmente para la detección de vulnerabilidades y fundamentada teóricamente:

1. Ataque por fuerza bruta (BRUTE FORCE)
2. Denegación de servicio (DOS/DDOS)
3. Técnica de escaneo de la red
4. Ataques de amplificación basado en el protocolo UDP
5. White-box
6. Análisis estático de código o auditoria de código fuente
7. Pruebas de penetración
8. Pruebas pasivas:

2.2.2. Muestra

El muestreo fue de tipo no probabilístico por conveniencia y se trabajó con una muestra representativa de 03 técnicas de hacking ético

1- Técnica DDOS
2- Técnica de escaneo
3- Técnica de ataque por fuerza bruta

2.3. Variables y operacionalización

2.3.1. Variables

Variable Independiente

- Técnicas de hacking ético

Variable Dependiente

- Seguridad informática

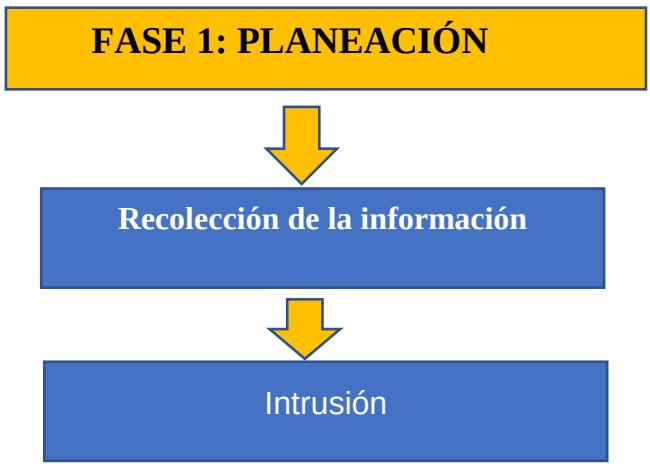
2.3.2. Operacionalización

Variable Independiente	Dimensiones	Indicadores	Unidad de medida	Instrumentos
Técnicas de Hacking ético	Métrica básica	Métricas para clasificar las técnicas de Haching ético		Tabla de Métricas de Técnicas cvss de Hacking Ético
Variable Dependiente	**Dimensiones**	**Indicadores**	**Unidad de medida**	**Instrumentos**
Seguridad informática	Nivel de riesgo	$NRV = \frac{N_v}{NTV} X100\%$	Nivel porcentual	Ficha de repostes del sistema
	Reconocimiento de puerto	Número de puertos abiertos con exposición a cyber ataques	Ordinal	Ficha de repostes del sistema
	Confidencialidad	$C = \frac{AE - AR_D}{AE} \text{ x } 100\%$	%	Ficha de repostes del sistema

2.4. Técnicas e instrumentos de recolección de datos

2.4.1. Técnica:

En la investigación para el recojo de la información se utilizó las fases del Hacking ético que permitió la evaluación, diagnóstico y detección de las vulnerabilidades a la seguridad informática aplicando la metodología ISSAF, con sus fases:



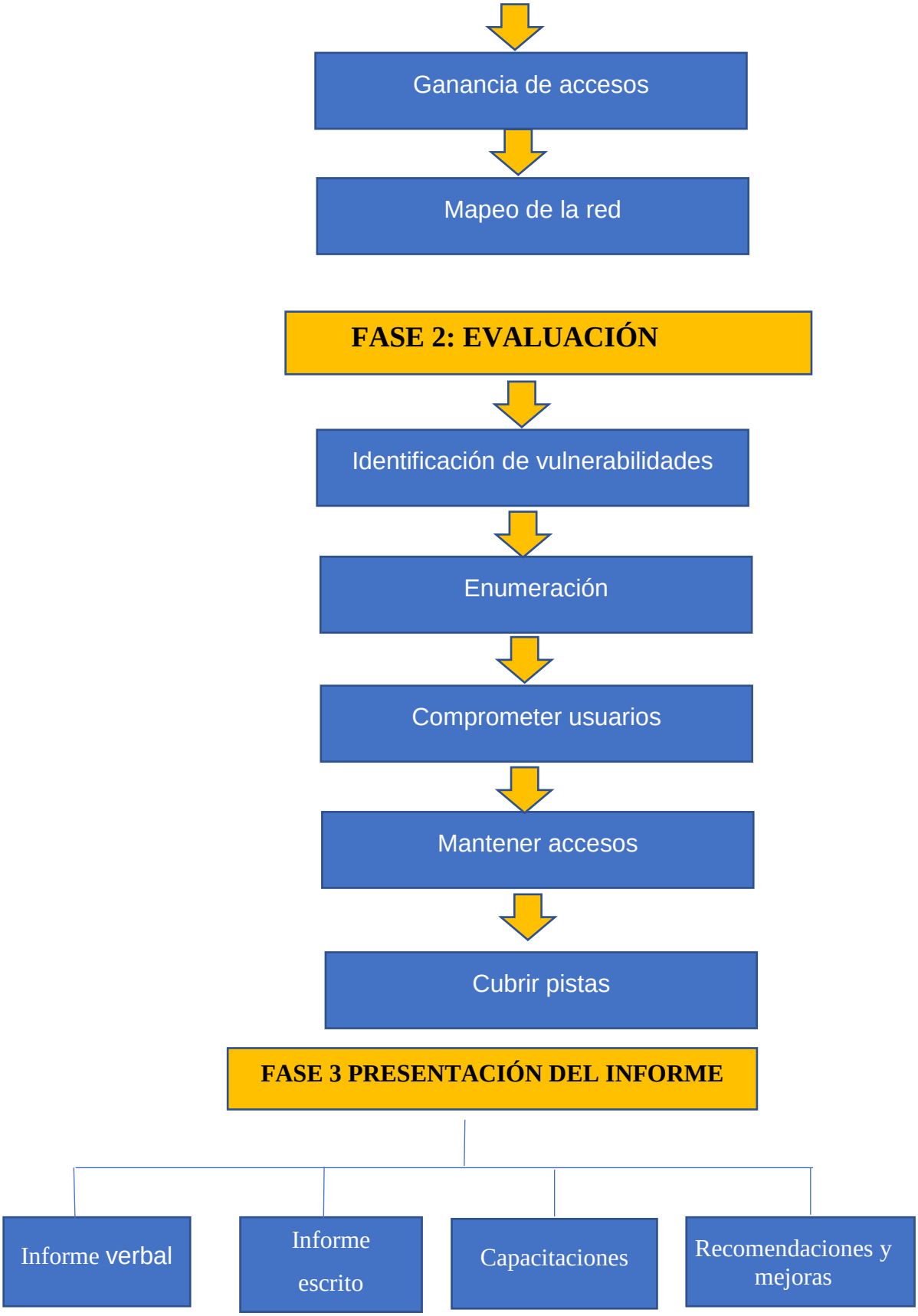


Figura 4: Fases de la metodología ISSAF
Fuente: Elaboración del autor

Fase 1 Planeación y preparación: Se realizó el proceso de recolectar información:

1. Recolección de información: es un método que se utilizó para recolectar la información de datos, fase fundamental de control que vela por la seguridad de la información
2. Intrusión; Se obtiene acceso no autorizado o ataque wifi con la finalidad de llegar al mayor acceso y evitar las medidas de seguridad, es necesario la búsqueda de códigos disponibles de preferencia públicos para las pruebas y poder aprobar o desaprobar las vulnerabilidades.
3. Ganando accesos, es el acceso a los dispositivos en la red, permite la confirmación y documenta todas las intrusiones a la difusión de los ataques automatizados, lo cual permite ingresar a mayor alcance a la administración del sistema.
4. Mapeo de la red; tiene que ver con toda la red de datos y su información se Adquiere del elemento de recopilación y se difunde produciendo diferentes tipologías.

FASE II; Evaluación

Esta fase es caracterizada por que realiza la prueba de penetración, el cual es considerada como “el enfoque por capas”, ya que cada capa expresa igual que representa los niveles de acceso.

Identificación de vulnerabilidades; en esta fase se seleccionan los elementos específicamente con la finalidad de ser comprobados y posterior aprobación.

De hecho, con este método el desarrollado y los auditores deben utilizar actividades como detectar elementos o servicios vulnerables, predecir impacto, ajustar rutas de ataque, verificar falsos positivos y falsos negativos, todo lo cual se utiliza para identificar, detectar y clasificar las Vulnerabilidades del sistema en su funcionamiento

Enumeración; Para la obtención de las contraseñas en esta fase se hace el encriptamiento, usando la técnica sniffing.

Comprometiendo usuarios; Se da la comprobación de los escritorios remotos vulnerables, también se da la exposición de toda la red, por lo cual los elementos del sistema son claves para la comunicación de las redes empresariales y los usuarios, por ello el dato encontrado no sea modificado mientras viaje a través de la red.

Mantener el acceso; Se pone a consideración su uso para tener privilegios en el sistema, teniendo y manteniendo acceso a la integridad. Siendo frecuente su utilidad.

Cubrir pistas; Se especifican los detalles y se realizan los registros por un auditor, en esta prueba se pueden ocultar archivos y borrar registros, con la finalidad de no dejar pistas en la intrusión.

FASE III: Presentación de informes

Consiste en la realización de un informe de todo lo que se encontró en el sistema durante la intrusión, explicando los problemas, además se incluyen alternativas de solución o recomendaciones

2.4.2. Instrumentos

Los instrumentos o técnicas para la recolección de información fueron:

Hojas de reporte del sistema: se generaron a través de las diferentes técnicas utilizadas

Observación: Se utilizó la técnica de observación, la misma que consistió en registrar sistemáticamente y confiable el problema.

2.5. Procedimiento de análisis de datos

Con los resultados obtenidos de las técnicas, se aplicó la estadística descriptiva. diseñando tablas para un entendimiento mucho más sencillo de la situación de la red de información.

Se realizó la tabulación respectiva y el análisis de los resultados que se obtuvieron

2.6 Criterios éticos

Los criterios los cuales han sido considerados en esta investigación fueron del Código Deontológico del Colegio de Ingenieros del Perú en su Capítulo III "Faltas Contra la Ética Profesional y Sanciones" y su Sub Capítulo II "De la Relación con El Público "en su Artículo 106 expresa: Los ingenieros, al momento de expresarse sobre sus investigaciones, deberán presentar convicción y seriedad del caso, procurando la generación de conflictos con los intereses de los demás, para profundizar el conocimiento de la sociedad. Esta investigación se manifiesta de manera clara y sencilla su información, con la finalidad de ser una contribución a las redes informáticas están disponible para las diferentes empresas.

Objetividad

La investigación y sus análisis se apoyó en criterio imparciales y técnicos.

Originalidad

Las referencias bibliográficas fueron citadas para evidenciar que no existe copia intelectual en la investigación.

Veracidad

Los datos mostrados son verdaderos, teniendo presente la confidencialidad de los mismos.

2.7. Criterios de rigor científico

Validez

Los instrumentos de validaron por juicio de especialistas en el tema. (Morales, 2015). Así como el modelo de propuesta.

Confiabilidad

La realización de estadísticas para la determinación de la confiabilidad de los instrumentos (Morales, 2015)

Investigación metódica

Aplicación de una metodología con rigor científico para su desarrollo y solución al problema.

III. RESULTADOS

3.1. Resultados

Los resultados obtenidos al evaluar la vulnerabilidad de los servidores fueron:

De acuerdo al objetivo específico 1; Conocer la situación de vulnerabilidad de la seguridad informática, utilizando técnicas de hacking ético, en la Municipalidad distrital de los Olivos, Lima.

Tabla 1:

Servidores evaluados

N°	SERVICIO	DIRECCION IP	SISTEMA-OPERATIVO	TIPO DE SERVIDOR
1	SERVIDOR DE BASE DE DATOS	192.168.90.48	WINDOWS SERVER 2008 R2 DATACENTER 64-BIT	SERVIDOR DE BASE DE DATOS SQL-SERVER
		192.168.90.49	WINDOWS SERVER 2008 R2 DATACENTER 64-BIT	SERVIDOR DE BASE DE DATOS SQL-SERVER
2	SERVIDOR WEB	192.168.90.33	UBUNTU 14.04.2 LTS \N \L	SERVIDOR WEB
		192.168.90.74	UBUNTU 14.04 SERVER	SERVIDOR WEB
3	SERVIDOR FTP	192.168.90.5	LINUX-NETBOX	SERVIDOR DE WEB
		192.168.90.47	WINDOWS SERVER 2008 R2 DATACENTER 64-BIT	SERVIDOR DE ARCHIVO
4	SERVIDOR SSH	192.168.90.23	UBUNTU 14.04.4 LTS \N \L	SERVIDOR WEB
		192.168.90.29	UBUNTU 14.04.4 LTS \N \L	SERVIDOR WEB

Pruebas Con la Técnica de DDOS:

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.48

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:30 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 5: Resultado de comando nmap --script dos -Pn 192.168.90.48
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.48
PROCESO	Ingreso al sistema operativo Kali Linux, continuamente se procede a la ejecución del comando, de acuerdo al ataque a realizar.
RESULTADOS	Escaneando el host con la ip 192.168.90.48, este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.49

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:33 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 6: Resultado de comando nmap --script dos -Pn 192.168.90.49
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.49
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.49, este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.33

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:35 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 7: Resultado de comando nmap --script dos -Pn 192.168.90.33
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.33
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.33, este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.74

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:37 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 8: Resultado de comando nmap --script dos -Pn 192.168.90.74
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.74
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.74, este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.5

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:42 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 9: Resultado de comando nmap --script dos -Pn 192.168.90.5
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.5
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.5, este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102. Con identificación RHSA-2011:0436

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.47

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:43 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 10: Resultado de comando nmap --script dos -Pn 192.168.90.47
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.47
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.74, el servidor se encuentra activo y este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.23

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:45 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 11: Resultado de comando nmap --script dos -Pn 192.168.90.23
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.23
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.23, el servidor se encuentra activo y este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

```
root@instaladores:~/freevulnsearch# nmap --script dos -Pn 192.168.90.29

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-18 01:46 PET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.50.2
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Figura 12: Resultado de comando nmap --script dos -Pn 192.168.90.29
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script dos -Pn 192.168.90.29
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Escaneando el host con la ip 192.168.90.29, el servidor se encuentra activo y este no presenta vulnerabilidad a un ataque DDOS CVE-2011-102

Pruebas con la Técnica De Escaneo

El escaneo de vulnerabilidades es el proceso de descubrir e identificar vulnerabilidades en una red.

Este proceso generará mucho tráfico y también puede causar una denegación de servicio al equipo de red. La herramienta que puede realizar el escaneo de vulnerabilidades es Nmap, a través de su poderosa y flexible función llamada NSE (Nmap Script Engine). Permite a los usuarios escribir (y compartir) scripts simples para automatizar varias tareas de red.

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.48
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 09:38 -05
Nmap scan report for 192.168.90.48
Host is up (0.0050s latency).
Not shown: 65517 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
517/tcp   filtered talk
518/tcp   filtered ntalk
1433/tcp  open     ms-sql-s
2383/tcp  open     ms-olap4
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
47001/tcp open     winrm
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49156/tcp open     unknown
49157/tcp open     unknown
60408/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 26.38 seconds
```

Figura 13: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.48
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap n -Pn -sS -p- 192.168.90.48
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0050s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65517 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	80 protocolo Tcp Estado Abierto Servicio http
	135 protocolo Tcp Estado Abierto Servicio msrpc
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	1433 protocolo Tcp Estado Abierto Servicio ms-sql-s
	2383 protocolo Tcp Estado Abierto Servicio ms-olap4
	3389 protocolo Tcp Estado Abierto Servicio ms-wbt-server
	5357 protocolo Tcp Estado Abierto Servicio wsdapi
	47001 protocolo Tcp Estado Abierto Servicio winrm
	49152 protocolo Tcp Estado Abierto Servicio desconocido
	49153 protocolo Tcp Estado Abierto Servicio desconocido
	49154 protocolo Tcp Estado Abierto Servicio desconocido
	49155 protocolo Tcp Estado Abierto Servicio desconocido
	49156 protocolo Tcp Estado Abierto Servicio desconocido
	49157 protocolo Tcp Estado Abierto Servicio desconocido
	60408 protocolo Tcp Estado Abierto Servicio desconocido

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.49
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 09:39 -05
Nmap scan report for 192.168.90.49
Host is up (0.0079s latency).
Not shown: 65517 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
517/tcp   filtered talk
518/tcp   filtered ntalk
1433/tcp  open     ms-sql-s
2383/tcp  open     ms-olap4
3389/tcp  open     ms-wbt-server
12000/tcp open     cce4x
47001/tcp open     winrm
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49156/tcp open     unknown
49157/tcp open     unknown
49624/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 24.57 seconds
```

Figura 14: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.49
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.49
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0079s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65517 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	80 protocolo Tcp Estado Abierto Servicio http
	135 protocolo Tcp Estado Abierto Servicio msrpc
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	1433 protocolo Tcp Estado Abierto Servicio ms-sql-s
	2383 protocolo Tcp Estado Abierto Servicio ms-olap4
	3389 protocolo Tcp Estado Abierto Servicio ms-wbt-server
	12000 protocolo Tcp Estado Abierto Servicio cce4x
	47001 protocolo Tcp Estado Abierto Servicio winrm
	49152 protocolo Tcp Estado Abierto Servicio desconocido
	49153 protocolo Tcp Estado Abierto Servicio desconocido
	49154 protocolo Tcp Estado Abierto Servicio desconocido
	49155 protocolo Tcp Estado Abierto Servicio desconocido

	49156 protocolo Tcp Estado Abierto Servicio desconocido
	49157 protocolo Tcp Estado Abierto Servicio desconocido
	49624 protocolo Tcp Estado Abierto Servicio desconocido

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.33
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15
Nmap scan report for 192.168.90.33
Host is up (0.011s latency).
Not shown: 65527 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
517/tcp   filtered talk
518/tcp   filtered ntalk
3306/tcp  open     mysql
5432/tcp  open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 17.73
```

Figura 15: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.33

Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.33
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0011s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65527 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	22 protocolo Tcp Estado Abierto Servicio ssh
	80 protocolo Tcp Estado Abierto Servicio http
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	3306 protocolo Tcp Estado Abierto Servicio mysql
	5432 protocolo Tcp Estado Abierto Servicio postquestl

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.74
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15
Nmap scan report for 192.168.90.74
Host is up (0.011s latency).
Not shown: 65531 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
517/tcp  filtered talk
518/tcp  filtered ntalk

Nmap done: 1 IP address (1 host up) scanned in 17.61 s
```

Figura 16: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.74
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.74
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0011s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65531 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	22 protocolo Tcp Estado Abierto Servicio ssh
	80 protocolo Tcp Estado Abierto Servicio http
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15
Nmap scan report for 192.168.90.5
Host is up (0.0095s latency).
Not shown: 65523 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
517/tcp   filtered talk
518/tcp   filtered ntalk
3000/tcp  open     ppp
3010/tcp  open     gw
4001/tcp  open     newoak
5432/tcp  open     postgresql
7262/tcp  open     cnap
8000/tcp  open     http-alt
```

Figura 17: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.5
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.5
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0095s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65523 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	22 protocolo Tcp Estado Abierto Servicio ssh
	80 protocolo Tcp Estado Abierto Servicio http
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	3000 protocolo Tcp Estado Abierto Servicio ppp
	3010 protocolo Tcp Estado Abierto Servicio gw
	4001 protocolo Tcp Estado Abierto Servicio newoak
	5432 protocolo Tcp Estado Abierto Servicio postgresql
	7262protocolo Tcp Estado Abierto Servicio cnap
	8000 protocolo Tcp Estado Abierto Servicio http-alt

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.47
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 0
Nmap scan report for 192.168.90.47
Host is up (0.013s latency).
Not shown: 65517 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
517/tcp   filtered talk
518/tcp   filtered ntalk
1433/tcp  open     ms-sql-s
1434/tcp  open     ms-sql-m
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49156/tcp open     unknown
49157/tcp open     unknown
50469/tcp open     unknown
```

Figura 18: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.47
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.47
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0013s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65517 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	21 protocolo Tcp Estado Abierto Servicio ftp
	80 protocolo Tcp Estado Abierto Servicio http
	135 protocolo Tcp Estado Abierto Servicio msrpc
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	1433 protocolo Tcp Estado Abierto Servicio ms-sql-s
	1434 protocolo Tcp Estado Abierto Servicio ms-sql-m
	3389 protocolo Tcp Estado Abierto Servicio ms-wbt-server
	5357 protocolo Tcp Estado Abierto Servicio wsdapi
	49152 protocolo Tcp Estado Abierto Servicio unknown
	49153 protocolo Tcp Estado Abierto Servicio unknown
	49154 protocolo Tcp Estado Abierto Servicio unknown
	49155 protocolo Tcp Estado Abierto Servicio unknown
	49156 protocolo Tcp Estado Abierto Servicio unknown
	49157 protocolo Tcp Estado Abierto Servicio unknown
	50469 protocolo Tcp Estado Abierto Servicio unknown

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.23
Starting Nmap 7.80 ( https://nmap.org ) at 2019-1
Nmap scan report for 192.168.90.23
Host is up (0.016s latency).
Not shown: 65523 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
443/tcp   open     https
517/tcp   filtered talk
518/tcp   filtered ntalk
5432/tcp  open     postgresql
7070/tcp  open     realserver
8084/tcp  open     unknown
8085/tcp  open     unknown
8086/tcp  open     d-s-n
9089/tcp  open     sqlexec-ssl
9418/tcp  open     git
46321/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 18.
```

Figura 19: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.23
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.23
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0016s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65517 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	80 protocolo Tcp Estado Abierto Servicio http
	443 protocolo Tcp Estado Abierto Servicio https
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	5432 protocolo Tcp Estado Abierto Servicio postgresql
	7070 protocolo Tcp Estado Abierto Servicio realserver
	8084 protocolo Tcp Estado Abierto Servicio unknown
	8085 protocolo Tcp Estado Abierto Servicio unknown
	8086 protocolo Tcp Estado Abierto Servicio d-s-n
	9089 protocolo Tcp Estado Abierto Servicio sqlexec-ssl
	9418 protocolo Tcp Estado Abierto Servicio git
	46321 protocolo Tcp Estado Abierto Servicio unknown

```
root@control:~# nmap -n -Pn -sS -p- 192.168.90.29
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15
Nmap scan report for 192.168.90.29
Host is up (0.0081s latency).
Not shown: 65525 closed ports
PORT       STATE    SERVICE
80/tcp     open     http
139/tcp    open     netbios-ssn
443/tcp    open     https
445/tcp    open     microsoft-ds
517/tcp    filtered talk
518/tcp    filtered ntalk
3306/tcp   open     mysql
9089/tcp   open     sqlexec-ssl
9090/tcp   open     zeus-admin
46321/tcp  open     unknown

Nmap done: 1 IP address (1 host up) scanned in 18.89
```

Figura 20: Resultado de estado de puertos del comando nmap -n -Pn -sS -p- 192.168.90.29
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap -n -Pn -sS -p- 192.168.90.29
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0081s y de los 65536 puertos, numerados del 0 al 65535 nos indica que 65525 puertos están cerrados
PUERTOS ABIERTOS ENCONTRADOS	80 protocolo Tcp Estado Abierto Servicio http
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	443 protocolo Tcp Estado Abierto Servicio https
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	517 protocolo Tcp Estado Abierto Servicio talk
	518 protocolo Tcp Estado Abierto Servicio ntalk
	3306 protocolo Tcp Estado Abierto Servicio mysql
	9089 protocolo Tcp Estado Abierto Servicio sqlexec-ssl
	9090 protocolo Tcp Estado Abierto Servicio zeus-admin
	46321 protocolo Tcp Estado Abierto Servicio unknown

Pruebas con la Técnica de Fuerza Bruta

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.48

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 11:45 PET
Nmap scan report for 192.168.90.48
Host is up (0.00076s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
80/tcp    open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
| ms-sql-brute:
|   [192.168.90.48:1433]
|_    No credentials found
2383/tcp  open  ms-olap4
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb-brute:
|_  No accounts found

Nmap done: 1 IP address (1 host up) scanned in 166.07 seconds
```

Figura 21: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.48
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.48
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0076s el resultado nos muestra los principales puertos encontrados
	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml - fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 138 protocolo Tcp Estado Abierto Servicio msrpc
	Puerto 139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	Puerto 445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	Puerto 1433 protocolo Tcp Estado Abierto Servicio ms-sql-s - ms-sql-brute al intentar ingresar al servicio del puerto 1433 no funciona las credenciales
	Puerto 2383 protocolo Tcp Estado Abierto Servicio ms-olap4
	Puerto 3389 protocolo Tcp Estado Abierto Servicio ms-wbt-server
	Puerto 5357 protocolo Tcp Estado Abierto Servicio wsdapi

	Puerto 49152 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49153 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49154 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49155 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49156 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49157 protocolo Tcp Estado Abierto Servicio unknown

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.49

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 11:48 PET
Nmap scan report for 192.168.90.49
Host is up (0.00074s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
80/tcp    open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
| ms-sql-brute:
|   [192.168.90.49:1433]
|_    No credentials found
2383/tcp  open  ms-olap4
3389/tcp  open  ms-wbt-server
12000/tcp open  cce4x
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb-brute:
|_  guest:<blank> => Valid credentials, account disabled

Nmap done: 1 IP address (1 host up) scanned in 180.59 seconds
```

Figura 22: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.49
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.49
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0074s el resultado nos muestra los principales puertos encontrados
	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 135 protocolo Tcp Estado Abierto Servicio msrpc

	Puerto 139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	Puerto 445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	Puerto 1433 protocolo Tcp Estado Abierto Servicio ms-sql-s - ms-sql-brute al intentar ingresar al servicio del puerto 1433 no funciona las credenciales
	Puerto 2383 protocolo Tcp Estado Abierto Servicio ms-olap4
	Puerto 3389 protocolo Tcp Estado Abierto Servicio ms-wbt-server
	12000 protocolo Tcp Estado Abierto Servicio cce4x
	49152 protocolo Tcp Estado Abierto Servicio unknown
	49153 protocolo Tcp Estado Abierto Servicio unknown
	49154 protocolo Tcp Estado Abierto Servicio unknown
	49155 protocolo Tcp Estado Abierto Servicio unknown
	49156 protocolo Tcp Estado Abierto Servicio unknown
	49157 protocolo Tcp Estado Abierto Servicio unknown

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.33

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 11:54 PET
Nmap scan report for 192.168.90.33
Host is up (0.00074s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
| mysql-brute:
|   Accounts
|     No valid accounts found
|   Statistics
|_    Performed 50005 guesses in 38 seconds, average tps: 1132
| mysql-enum:
|   Valid usernames
|     test:<empty> - Valid credentials
|   Statistics
|_    Performed 1 guesses in 5 seconds, average tps: 0
5432/tcp open  postgresql

Host script results:
| smb-brute:
|_  No accounts found

Nmap done: 1 IP address (1 host up) scanned in 68.50 seconds
```

Figura 23: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.33
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.33
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0074s el resultado nos muestra los principales puertos encontrados
	Puerto 22 protocolo Tcp Estado Abierto Servicio ssh
	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	Puerto 445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	Puerto 3306 protocolo Tcp Estado Abierto Servicio mysql-brute al intentar ingresar al servicio del puerto 3306 indica que las credenciales por defecto son validas
	Puerto 5432 protocolo Tcp Estado Abierto Servicio postgresql

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.74

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 11:55 PET
Nmap scan report for 192.168.90.74
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)

Nmap done: 1 IP address (1 host up) scanned in 3.89 seconds
```

Figura 24: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.74
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.74
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0011s el resutado nos muestra los principales puertos encontrados
	Puerto 22 protocolo Tcp Estado Abierto Servicio ssh
	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.5

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 11:56 PET
Nmap scan report for 192.168.90.5
Host is up (0.0010s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|   Accounts
|     No valid accounts found
|   Statistics
|_    Performed 23656 guesses in 600 seconds, average tps: 39
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3000/tcp open  ppp
4001/tcp open  newoak
5432/tcp open  postgresql
8000/tcp open  http-alt
| http-proxy-brute:
|_  ERROR: Proxy server did not require authentication

Nmap done: 1 IP address (1 host up) scanned in 603.09 seconds
```

Figura 25: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.5
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.5
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0010s el resutado nos muestra los principales puertos encontrados
	Puerto 22 protocolo Tcp Estado Abierto Servicio ssh

	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	Puerto 445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	Puerto 3000 protocolo Tcp Estado Abierto Servicio ppp
	4001 protocolo Tcp Estado Abierto Servicio newoak
	5432 protocolo Tcp Estado Abierto Servicio postgresql
	8000 protocolo Tcp Estado Abierto Servicio http-alt Indica que requiere autentificación

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.47

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 12:16 PET
Nmap scan report for 192.168.90.47
Host is up (0.00073s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-brute:
|   Accounts
|     No valid accounts found
|   Statistics
|_    Performed 1200 guesses in 600 seconds, average tps: 1
80/tcp    open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
| ms-sql-brute:
|   [192.168.90.47:1433]
|_    No credentials found
1434/tcp  open  ms-sql-m
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb-brute:
|_  No accounts found

Nmap done: 1 IP address (1 host up) scanned in 661.50 seconds
```

Figura 26: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.47
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.47
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0073s el resultado nos muestra los principales puertos encontrados
	21 protocolo Tcp Estado Abierto Servicio ftp al realizar el diagnostico ftp-brute indica que la cuenta por defecto no está activo
	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 135 protocolo Tcp Estado Abierto Servicio msrpc
	Puerto 139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	Puerto 445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	Puerto 1433 protocolo Tcp Estado Abierto Servicio ms-sql-s al realizar el diagnostico ms-sql-brute indica que la cuenta por defecto no está activo
	Puerto 1434 protocolo Tcp Estado Abierto Servicio ms-sql-m
	Puerto 3389 protocolo Tcp Estado Abierto Servicio ms-wbt-server
	Puerto 5357 protocolo Tcp Estado Abierto Servicio wsdapi
	Puerto 49152 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49153 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49154 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49155 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49156 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 49157 protocolo Tcp Estado Abierto Servicio unknown

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.23

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 12:28 PET
Nmap scan report for 192.168.90.23
Host is up (0.0016s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
80/tcp   open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
443/tcp  open  https
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
5432/tcp open  postgresql
7070/tcp open  realserver
8084/tcp open  unknown
8085/tcp open  unknown
8086/tcp open  d-s-n
9418/tcp open  git

Nmap done: 1 IP address (1 host up) scanned in 569.73 seconds
```

Figura 27: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.23
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.23
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0016s el resultado nos muestra los principales puertos encontrados
	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 443 protocolo Tcp Estado Abierto Servicio https citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	Puerto 5432 protocolo Tcp Estado Abierto Servicio postgresql
	Puerto 7070 protocolo Tcp Estado Abierto Servicio realserver
	Puerto 8084 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 8085 protocolo Tcp Estado Abierto Servicio unknown
	Puerto 8086 protocolo Tcp Estado Abierto Servicio d-s-n
	Puerto 9089 protocolo Tcp Estado Abierto Servicio sqlexec-ssl
	Puerto 9418 protocolo Tcp Estado Abierto Servicio git

```
root@instaladores:~# nmap --script brute -Pn 192.168.90.29

Starting Nmap 6.47 ( http://nmap.org ) at 2019-11-15 12:41 PET
Nmap scan report for 192.168.90.29
Host is up (0.0026s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
139/tcp  open  netbios-ssn
443/tcp  open  https
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-brute:
|_  Path "/" does not require authentication
| http-form-brute:
|_  ERROR: No passvar was specified (see http-form-brute.passvar)
445/tcp  open  microsoft-ds
3306/tcp open  mysql
| mysql-brute:
|   Accounts
|     No valid accounts found
|   Statistics
|_    Performed 20773 guesses in 600 seconds, average tps: 33
| mysql-enum:
|   Valid usernames
|     guest:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|   Statistics
|_    Performed 5 guesses in 6 seconds, average tps: 0
9090/tcp open  zeus-admin
| informix-brute:
|   Accounts
|     No valid accounts found
|   Statistics
|_    Performed 310 guesses in 626 seconds, average tps: 0

Host script results:
| smb-brute:
|_  No accounts found

Nmap done: 1 IP address (1 host up) scanned in 646.81 seconds
```

Figura 28: Resultado de estado de puertos del comando nmap --script brute -Pn 192.168.90.23
Fuente: Elaboración del autor

COMANDO EJECUTADO	nmap --script brute -Pn 192.168.90.23
PROCESO	Primero realizamos el ingreso al sistema operativo Kali Linux luego procedemos con la ejecución del comando, según el tipo de ataque que realizaremos.
RESULTADOS ENCONTRADOS	Nos indica que el servidor se encuentra activo (Host is up) con una latencia (tiempo que tarda en transmitirse un paquete de datos dentro de la red) de 0,0016s el resultado nos muestra los principales puertos encontrados

	Puerto 80 protocolo Tcp Estado Abierto Servicio http citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	139 protocolo Tcp Estado Abierto Servicio netbios-ssn
	Puerto 443 protocolo Tcp Estado Abierto Servicio https citrix-brute-xml -fallo indica que no especifica el dominio para el ingreso al servicio http no requiere autentificación
	445 protocolo Tcp Estado Abierto Servicio microsoft-ds
	Puerto 3306 protocolo Tcp Estado Abierto Servicio mysql
	Puerto 9089 protocolo Tcp Estado Abierto Servicio sqlexec-ssl
	Puerto 9090 protocolo Tcp Estado Abierto Servicio zeus-admin
	Puerto 46321 protocolo Tcp Estado Abierto Servicio unknown

Interpretación

Al realizar las pruebas con las técnicas que elegimos cada uno de ellos nos muestra diferentes resultados por cada servidor, los detalles que muestra en el informe son de gran ayuda ya que nos muestra el estado de los servicios y los principales accesos que tiene activo cada servidor, de esta manera nos permite verificar el tipo de vulnerabilidad que tiene los servidores para realizar el diagnostico que nos permitirá mejorar la seguridad de un servidor.

De acuerdo al objetivo específico 2; Clasificar las vulnerabilidades detectadas sobre la seguridad informática en la municipalidad distrital de los Olivos

Presentación y detalle de Resultados usando Métricas CVSS

N°	TECNICA DE HACKING	SERVICIO	DIRECCION IP	VULNERABILIDAD	PUNTUACION	Impacto de confidencialidad
1	DDOS, ESCANEO,FUERZA BRUTA	SERVIDOR DE BASE DE DATOS	192.168.90.48	CVE:CVE-2014-3566	3.4	Bajo
				CVE:CVE-2012-0152	4.3	Medio
				CVE:CVE-2012-0002	9.3	Alto
				CVE:CVE-2017-0143	8.1	Alto
			192.168.90.49	CVE:CVE-2014-3566	3.4	Bajo
2		SERVIDOR WEB	192.168.90.33	CVE:CVE-2007-6750	5	Medio
				CVE:CVE-2014-3566	3.4	Bajo
			192.168.90.74	CVE:CVE-2007-6750	5	Bajo
3		SERVIDOR FTP	192.168.90.5	CVE:CVE-2007-6750	5	Bajo
			192.168.90.47	CVE:CVE-2009-3103	10	Alto
4		SERVIDOR SSH	192.168.90.23	CVE:CVE-2007-6750	5	Bajo
				CVE:CVE-2014-3566	3.4	Bajo
			192.168.90.29	CVE:CVE-2007-6750	5	Bajo

Figura 29: Presentación y detalle de Resultados usando Métricas CVSS
Fuente: Elaboración del autor

Según la tabla N° 2 se observa que después de hacer uso de las técnicas de hacking ético ddos, escaneo y fuerza bruta en el primer servidor se encontró que cuenta con 4 vulnerabilidades de las cuales 2 tienen un impacto alto ya que pueden afectar directamente al servidor, y los otros dos son de medio y bajo impacto.

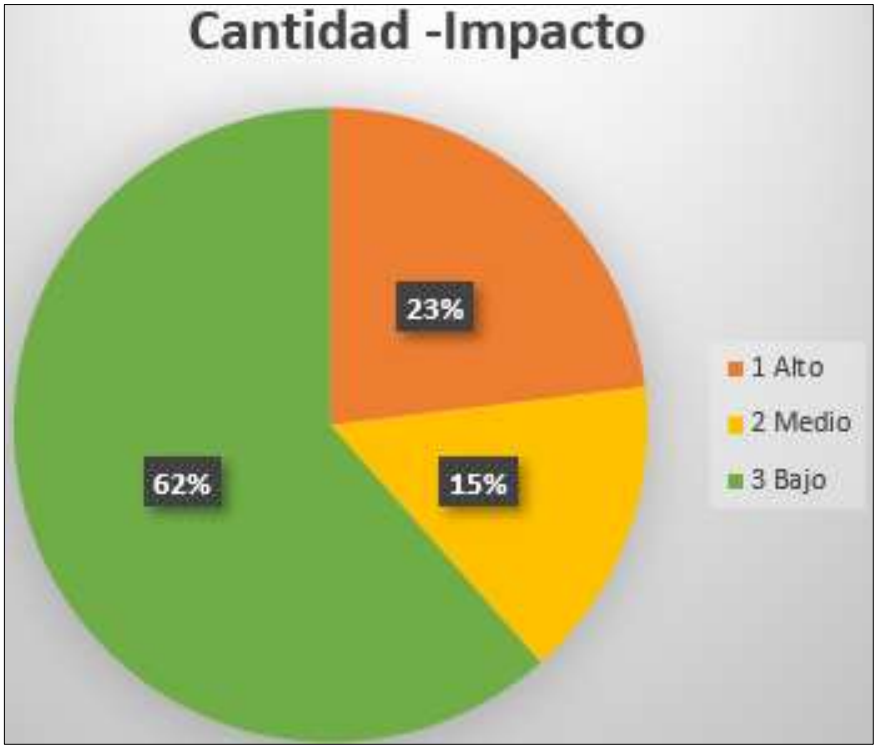


Figura 30: Vulnerabilidades
Fuente: Elaboración del autor

Según la figura 30 visualizamos que los servidores evaluados que pertenecen al grupo de la muestra, indica que el impacto de vulnerabilidad de tipo Bajo presenta

un 62%, la vulnerabilidad alta es de un 23% y la vulnerabilidad media es de un 15%
.

OE3; Analizar los servidores de la Municipalidad Distrital de los Olivos

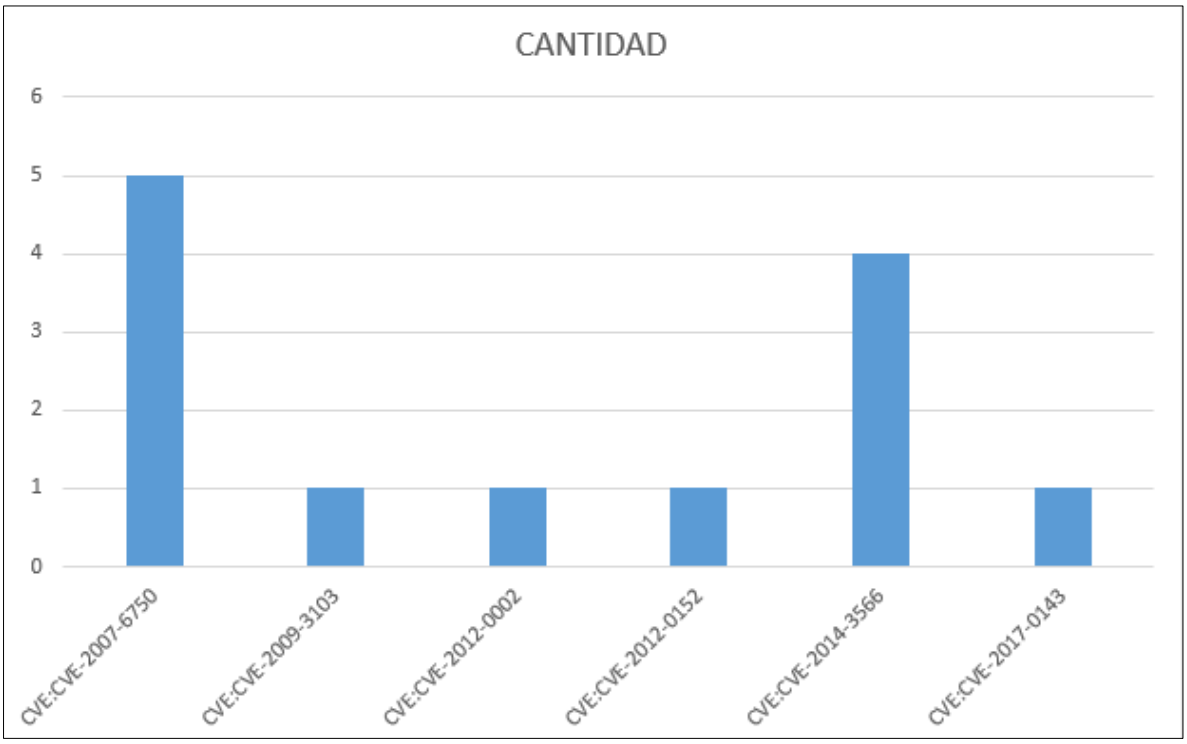


Figura 31: Análisis de servidores
Fuente: Elaboración del autor

Según la figura 31 visualizamos que en los 8 servidores que analizamos haciendo uso de las técnicas de hacking ético ddos, escaneo y fuerza bruta encontramos 6 vulnerabilidades de los cuales la mayor cantidad es CVE-2007-6750

Figura 32: Vulnerabilidad CVR-2007-6750
Fuente: Elaboración del autor

Vulnerabilidad CVR-2007-6750.- El servidor con el servicio HTTP Apache versiones 1.X-2.X permite a los atacantes de conexiones remotas provocar un ataque de denegación de servicio (caída del servicio) a través de una solicitud al protocolo HTTP (puerto 80), relacionado por la falta del módulo mod_reqtimeout que pertenece al servicio de apache.

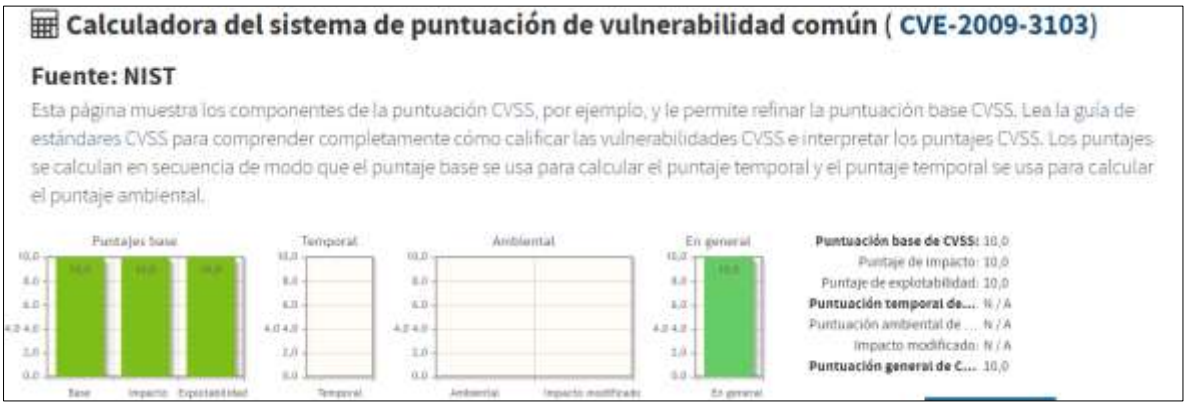


Figura 33: Vulnerabilidad CVR-2009-3103
Fuente: Elaboración del autor

Vulnerabilidad CVE-2009-3103.- El servidor con el protocolo samba (compartir archivos) es afectado con un error en el índice de la matriz, en el proceso de la implementación del protocolo SMBv2 (samba versión 02) en srv2.sys en las versiones de Microsoft Windows Vista Gold, service pack(1-2) y Windows Server 2008 Gold- service pack 2, y Windows 7 RC esto permite a los atacantes a través del servicio remoto poder ejecutar código con intenciones maliciosas el cual puede causar una denegación de servicio (bloqueo del sistema por exceso de solicitudes

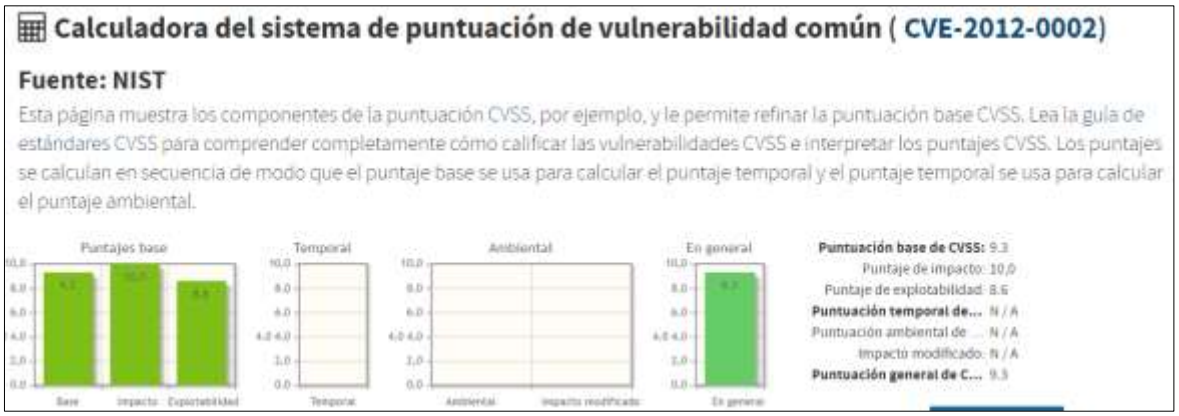


Figura 34: Vulnerabilidad CVR-2012-0002
Fuente: Elaboración del autor

Vulnerabilidad CVE-2012-0002.- La implementación del servicio del Protocolo de conexión del escritorio remoto (RDP) usado en Microsoft Windows XP service pack 2 y service pack 3, Windows Server 2003 service pack 2, Windows Vista service pack 2, Windows Server 2008 service pack 2, R2 y R2 service pack 1, y Windows 7 Gold y service pack 1 no procesa correctamente el envío de los paquetes en la memoria, esto permite que los atacantes e intrusos que realizan conexión remota ejecutar código arbitrario enviando paquetes usando el protocolo RDP, el cual desencadenara el acceso a un objeto que no se inicializó correctamente o se elimina, este tipo de vulnerabilidad es también conocido como "Vulnerabilidad de protocolo de escritorio remoto".

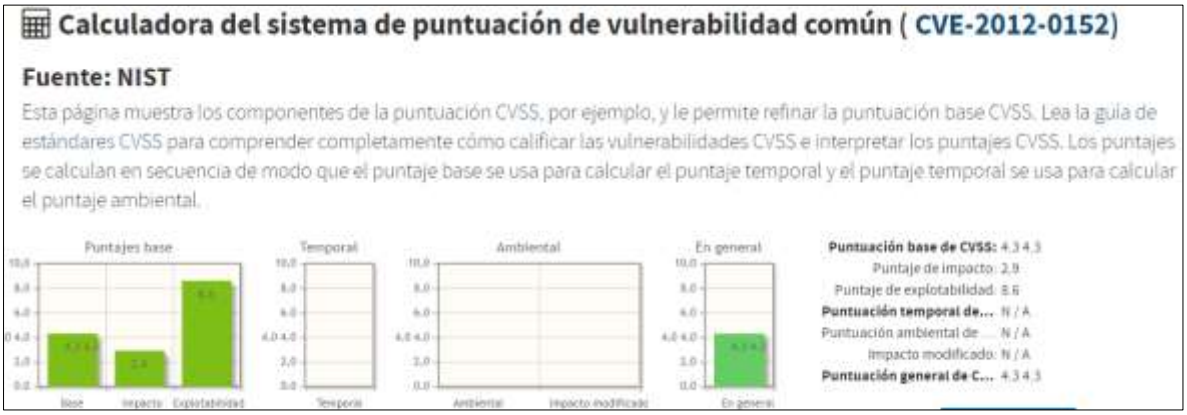


Figura 35: Vulnerabilidad CVR-2012-0152
Fuente: Elaboración del autor

Vulnerabilidad CVE-2012-0152.- El servicio del Protocolo de conexión de escritorio remoto (RDP) en Microsoft Windows Server 2008 R2 y R2 service pack 1 y Windows 7 Gold y service pack 1 permite a los atacantes e intrusos remotos

causar una denegación de servicio RDP (bloqueo de la aplicación RDP) a través de una serie de envió de paquetes diseñados, esta vulnerabilidad también es conocida como "Denegación de servicio de Terminal Server Vulnerabilidad."

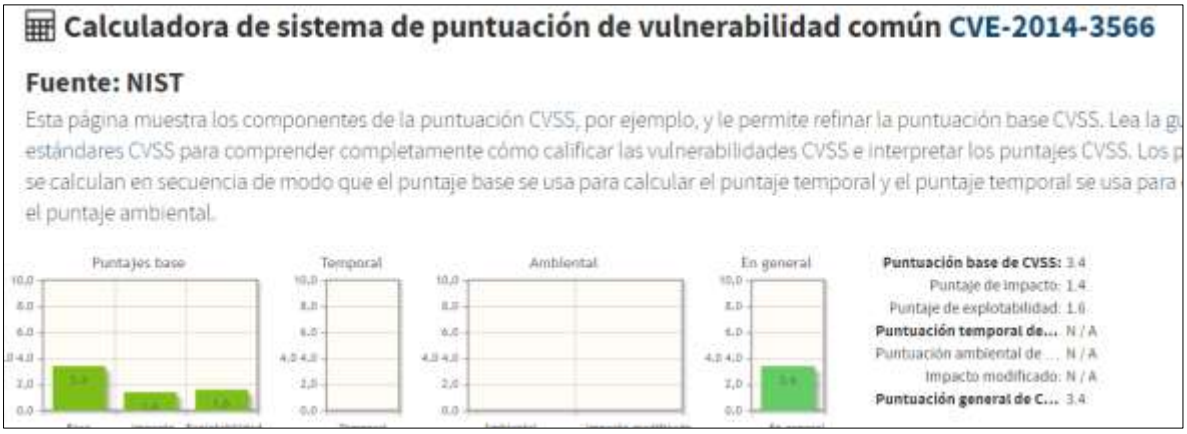


Figura 36: Vulnerabilidad CVR-2014-3566
Fuente: Elaboración del autor

Vulnerabilidad CVE-2014-3566.- El protocolo SSL con la versión 3.0, tal como es utilizado en Open SSL a través de 1.0.1 y otros productos.

Utiliza relleno CBC no determinista, lo que facilita a los atacantes e intrusos intermedios obtener datos del texto sin cifrar a través de un ataque de oráculo de relleno, también conocido como "POODLE " problema.

Figura 37: Vulnerabilidad CVR-2017-0143
Fuente: Elaboración del autor

Vulnerabilidad CVE-2017-0143.- El servidor Samba (SMB) versión 1 en Microsoft Windows Vista SP2 (service pack 2); Windows Server 2008 SP2 y R2 SP1 (service pack 1); Windows 7 SP1(service pack 1); Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a los atacantes e intrusos a través de la conexión remota ejecutar código arbitrario a través de envío de paquetes diseñados, también conocido como "Vulnerabilidad de ejecución remota de código SMB(samba) de Windows". Esta vulnerabilidad es diferente de las descritas en CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

De acuerdo al objetivo específico 3**;** Proponer un modelo de mejora que permita garantizar la confidencialidad, integridad y disponibilidad de la red informática de la Municipalidad distrital de los Olivos, con medidas que mitiguen las vulnerabilidades ya clasificadas.

Figura 38: Modelo propuesto para la seguridad informática de la municipalidad distrital de los Olivos.
Fuente: Elaboración propia

1.- Búsqueda de Técnicas de Hacking Ético
Proceso inicial para realizar la búsqueda de las principales técnicas de hacking que se puede usar de forma práctica y rápida.
2.- Seleccionar las Técnicas
De las técnicas encontradas seleccionamos las más usadas de fácil manejo y los más usados.
3.- Evaluación de las Técnicas
Procedemos a ejecutar las técnicas para evaluar el estado de los servicios de cada uno de los servidores o aplicativos a evaluar
4.- Registrar las Pruebas
Registro detallado de los resultados según muestra del software
5.- Presentación de Resultados usando Métricas CVSS
Al finalizar se muestra los resultados realizando una evaluación usando las métricas CVSS el cual nos indica el tipo de vulnerabilidad y el impacto que puede causar en un servicio si es explotado.

De acuerdo al objetivo específico 4; Validar la propuesta de implementación de la red de informática de la Municipalidad distrital de los Olivos por especialistas en seguridad informática.

Tabla 2:
Parámetros de la propuesta implementada

Criterios de seguridad informática	**Especialistas**					**Promedios**
	E1	***E2***	***E3***	***E4***	***E5***	
Integridad	5	5	5	5	5	**5**
Confiabilidad	5	5	5	5	5	**5**
Disponibilidad	5	5	4	5	5	**4.8**
Total de puntos	15	15	14	15	15	**-----**
PROMEDIO POR ESPECIALISTA	5	5	4.6	5	5	-----

Fuente: Elaboración propia

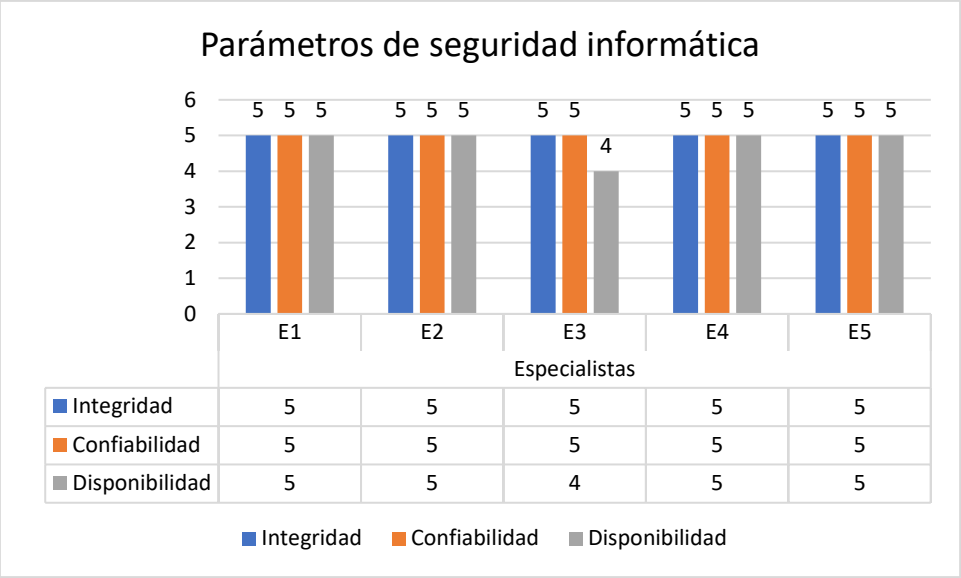


Figura 39 : Resultados de evaluación de parámetros de seguridad informática
Fuente: Elaboración propia

En la tabla 8 y figura 39 según la valoración de los criterios de la propuesta de seguridad informática por los 5 especialistas, podemos observar que el criterio integridad tiene un promedio de 5, confiabilidad de 5 y disponibilidad de 4.8. Esto indica que se la propuesta se validó con un nivel alto.

3.2. Discusión de los resultados

Los resultados indican que la actual situación de la seguridad informática de la Municipalidad de los Olivos es deficiente, dado que en su estructura lógica y física presenta muchas falencias, estando expuesto a ataques y la evaluación del sistema indica que el servidor se encuentra activo según el escaneo al host. El servidor se encuentra activo (Host is up) y los puertos se muestran cerrados. Al analizar los 8 servidores de la red usando las técnicas de hacking ético ddos, escaneo y fuerza bruta se encontró 6 vulnerabilidades de los cuales la mayor cantidad es CVE-2007-6750. La investigación coincide en lo que respecta a evaluación de seguridad informática con el método utilizado por Patil, Jangra, Bhale, Raina y Kulkarmi (2017) sobre hackers éticos, la investigación resolvió el problema de las necesidades de seguridad de la red, analizando los hackers de procesos éticos y 05 Fase 1: Reconocimiento es el mismo. Fase 2: Escaneo. Fase 3: Obtenga acceso. Fase 4: Mantener los derechos de acceso. Etapa 5:

Cubra la pista. Además, se describen las herramientas utilizadas en cada etapa. Es por esto que nuestra investigación, la comparamos con esta investigación seria, porque hemos podido utilizar un método para evaluar la tecnología y poder diagnosticar la vulnerabilidad de la empresa proveedora, este es nuestro escenario principal, de esta manera también hemos haber podido conocer el estado de la red y si está protegida de cualquier ataque de intrusos

El impacto de vulnerabilidad de la red informática de la municipalidad distrital de los Olivos presenta una prevalencia de nivel bajo con un 62%, nivel alto con un 23% y vulnerabilidad media con un 15%, esto tiene similitud con la investigación realizada por Giannone, Martins, Amatriain, Rodríguez y Merlino (2016) que Abordaron el tema “Survey Of Hacking Techniques And It's Prevention”, problema que enfrentó vulnerabilidades residuales hacen ineficaz la seguridad de la información que se hizo, buscando la implementación del hacking ético para evitar amenazas futuras. el aporte a los encargados de testing de instrumentos de ayuda técnica con los cuales se contrarrestarán los problemas actuales. Concluyendo que es necesario contar con profesionales que tengan conocimiento en seguridad informática, también es necesario realizar el testeo de software para encontrar las posibles vulnerabilidades haciendo uso de herramientas de hacking ético.

3.3. Aporte científico

Descripción de la empresa

La Municipalidad Distrital de los Olivos, es uno de los distritos de la provincia de Lima. Es un distrito de carácter "popular" con predominio de clase media a baja.

La gestión de servicios y trámites los viene trabajando actualmente en un sistema de escritorio hecho en lenguaje .Net y con la base de datos SQL Server 2008, la cual, tiene que cancelar por licencia de software y en la actualidad tiene errores como falta de integridad de datos, diseño deficiente generando demoras en los procesos.

Métricas para el diagnóstico de vulnerabilidades

Se definen nuevas métricas para iniciar el diagnostico de vulnerabilidades de hacking ético en la red de datos de Municipalidad distrital de los Olivos. Se explica de la siguiente manera:

AV: VECTOR DE ACOSO: se define como el objetivo a diagnosticar o explotar la vulnerabilidad, desde cualquier red.

- AC: COMPLEJIDAD DE ACCESO: dificultades que se presentan al momento de realizar el diagnóstico de la vulnerabilidad, es decir baja.
- AU: AUTENTICACIÓN: es decir, el usuario o cualquier tipo de privilegio de acceso al objetivo a diagnosticar.

IMPACTO EN EL NIVEL DE RIESGO: nivel de vulnerabilidades detectadas (Alto = Crítico, Medio=Alto, Bajo= Normal).

- RP: IMPACTO EN EL RECONOCIMIENTO DE PUERTOS: nivel de riesgo en puertos abiertos innecesarios.
- C: IMPACTO EN LA CONFIDENCIALIDAD: Transmisión de datos en un entorno seguro. En este caso el impacto es total.
- FC: FACILIDAD DE CORRECIÓN: Nivel de complejidad para aplicar una solución al problema encontrado. –

IV: FIABILIDAD DEL INFORME DE VULNERABILIDAD: Aplicación de soluciones en un entorno real, en tiempo real y para futuros ataques en la empresa

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

Visión en seguridad informática

En el 2025, el Gobierno Municipal Distrital de Los Olivos será reconocido como líder en seguridad informática, manteniendo la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información.

. Objetivos Institucionales:

- Ofrecer un servicio y atención de calidad.
- Controlar en tiempo real los servicios y trámites que requieran los usuarios

- Tener especialistas para la detección y mitigación de ataques en tiempo real en la seguridad informática de la Municipalidad.
- Obtener buenas referencias de los usuarios por el servicio brindado.

IV.CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Se concluye que la actual situación de la seguridad informática de la Municipalidad de los Olivos es deficiente, dado que en su estructura lógica y física presenta muchas falencias, estando expuesto a ataques y la evaluación del sistema indica que el servidor se encuentra activo según el escaneo al host. El servidor se encuentra activo (Host is up) y se muestran latencias tiempo que tarda en transmitirse un paquete de datos dentro de la red) son variadas en las diversas IP y los puertos se muestran cerrados. Al analizar los 8 servidores de la red usando las técnicas de hacking ético ddos, escaneo y fuerza bruta se encontró 6 vulnerabilidades de los cuales la mayor cantidad es CVE-2007-6750

Se concluye que el impacto de vulnerabilidad de la red informática de la municipalidad distrital de los Olivos presenta una prevalencia de nivel bajo con un 62%, nivel alto con un 23% y vulnerabilidad media con un 15%

Se Propuso lineamientos de seguridad que garantice la confidencialidad y reducción del nivel de riesgo, así como la reducción del número total de puertos abiertos, porque esto se convierte en múltiples puertas de acceso para atacantes externos, y finalmente el planteamiento de medidas de mitigación para las vulnerabilidades de clasificación.

La propuesta de implementación de la red informática al ser validada por los especialistas en los parámetros que comprende la seguridad de una red informática presenta un nivel MUY ALTO

4.2. Recomendaciones

Realizada la investigación se recomienda:

- Implementar las técnicas de Ethical Hacking, evaluadas en la presente investigación, las cuales permitirán minimizar los riesgos de vulnerabilidades ya detectadas en la red de datos de la Municipalidad.

- Rediseñar la estructura física de la red de la Municipalidad de los Olivos y así reducir tiempos en la transferencia de la información de manera unidireccional, aplicando una topología para la obtención de agilidad en la transmisión de datos y evitar ataques externos.

- Gestionar de manera adecuada el acceso de los usuarios a las redes municipales, con control de la seguridad de las conexiones de redes públicas o privadas y revisión de los eventos y actividades críticas que realizan los usuarios.

- Actualizar permanentemente el firmware en el hardware de red, de esta forma se detecte nuevas debilidades críticas o corregirlas inmediatamente.

- Actualizar las respectivas licencias de los firewalls, versiones, etc. de cada servicio.

- Obtener software para el análisis continuo de vulnerabilidades con propuesta de seguridad y confidencialidad para simular ataques comprobados y proponer mecanismos de mitigación para prevenir atacantes externos

REFERENCIAS

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

Ariel gañones, sebastian Martina, Ernán Amatriain, Darío rodríguez, Hernán merlino. (2016). inclusión de Hacking ético en el proceso de testing de software. 2016, de repositorio institucional de la universidad nacional de la plata sitio web: http://sedici.unlp.edu.ar/bitstream/handle/10915/67898/documento_completo.pdf-pdfa.pdf?sequence=1

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

Gatta sambasiva rao,p.naveen kumar,p. swetha, g. bhanukiran. (2014). problemas de seguridad en la red de computadoras. 2014, de ice explore sitio web: https://ieeexplore.ieee.org/document/7066756/

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

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

Hidalgo y. Jessica, Tupiza l. diana, Sánchez a. tarquino. (2016). políticas de seguridad de una red multiservicios corporativa; utilizando hacking ético. 2016, de laccei sitio web: http://www.laccei.org/laccei2016-sanjose/refereedpapers/rp251.pdf

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

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

Michael lehrfeld, Philip Guest. (2016). hacking ético para el aprendizaje y participación de los estudiantes. 2016, de ieee xplore sitio web: https://ieeexplore.ieee.org/document/7506746/

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

R. Shanmugapriya. (2013). estudio de seguridad de la red mediante pruebas de penetración. 2013, de ieee explore sitio web: https://ieeexplore.ieee.org/abstract/document/6508375

Rina Elizabeth López de Jiménez. (2017). pentesting de aplicaciones web utilizando hacking ético. 2017, de ieee explore sitio web: https://ieeexplore.ieee.org/abstract/document/7942364

Sabino Reyes, (2015) La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta.

Shreya s Shetty, Rithikar Shetty, Tanisha Shetty, Dvya Jennifer D'Souza. (2018). encuesta de técnicas de hacking y su prevención. 2018, de ieee explore sitio web: https://ieeexplore.ieee.org/document/8392053

Sonali Patil, Ankur Jangra, Mandar Bhale, Akshay Raina. (2017). hacking ético: la necesidad de la seguridad cibernética. 2017, de ieee explore sitio web: https://ieeexplore.ieee.org/document/8391982

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

Yien Wang, jianhua Yang. (2017). ethical hacking y la red de defensa. 2017, de ieee xplore sitio web: https://ieeexplore.ieee.org/document/7929663

Zouheir Trabelsi, Walid Ibrahim. (2013). la enseñanza de hacking ético en seguridad de la información. 2013, de ieee xplore sitio web: https://ieeexplore.ieee.org/abstract/document/6530097

ANEXO 1 Resolución de aprobación del proyecto de investigación

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°1200-2021/FIAU-USS

Pimentel, 27 de diciembre de 2021

VISTO:
El Acta de reunión N°1312 - 2021, remitida mediante oficio N°0395-2021/FIAU-IS-USS de fecha 14 de diciembre de 2021 por la Escuela profesional de INGENIERÍA DE SISTEMAS, para la ejecución de la Tesis: **"EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA"**, presentado por **PIÑASHCA HUERTA ROGER JHOEL,** del Programa de estudios de **INGENIERÍA DE SISTEMAS**, y;

CONSIDERANDO:
Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a la letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de Grados y Títulos, en su artículo 28° establece: "El jurado evaluador será designado mediante resolución emitida por la facultad o por la Escuela de Posgrado, el mismo que estará conformado por tres docentes, quienes cumplirán las funciones de presidente, secretario y vocal. El presidente será el docente de la especialidad que ostente el mayor grado académico.";

Que, mediante documento de vistos, el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acordó proponer a los siguientes docentes miembros del Jurado evaluador de la Tesis: "EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA", presentado por PIÑASHCA HUERTA ROGER JHOEL, egresado(s) del Programa de estudios de INGENIERÍA DE SISTEMAS:
PRESIDENTE: MG. BANCES SAAVEDRA DAVID ENRIQUE
SECRETARIO: MG. BRAVO RUIZ JAIME ARTURO
VOCAL: MG. CACHAY MACO JUNIOR EUGENIO

Que, mediante Resolución de Facultad se aprueba el Tema de la Tesis en referencia.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:
ARTÍCULO 1°: DESIGNAR, como miembros del Jurado Evaluador de la Tesis ***"EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA"***, presentada por **PIÑASHCA HUERTA ROGER JHOEL**, egresado(s) del Programa de estudios **INGENIERÍA DE SISTEMAS,** a los siguientes docentes:
PRESIDENTE: MG. BANCES SAAVEDRA DAVID ENRIQUE
SECRETARIO: MG. BRAVO RUIZ JAIME ARTURO
VOCAL: MG. CACHAY MACO JUNIOR EUGENIO

ARTÍCULO 2°: DISPONER, que los Miembros del Jurado, así como el aspirante al Título profesional, deberán ajustarse a lo normado en el Reglamento de Grados y Títulos de la USS.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Mg. Víctor Alexei Tuesta Montoya
Decano (e) / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

MBA. María Noelia Zúñiga Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesados, Archivo

ANEXO 2. Autorización de la institución para recojo de información

LOS OLIVOS

Gerente de Tecnología de la Información y Comunicaciones

Los Olivos, 03 de febrero de 2020

Quien suscribe:

Ing. Ricardo Gustavo Alvarado Bustos.
Gerente de Tecnología de la Información y Comunicaciones

AUTORIZA:

Permiso para recojo de información pertinente en función del proyecto de investigación, denominado: "**EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA**"

Por el presente, el que suscribe, Ing. Ricardo Gustavo Alvarado Bustos, Gerente De Tecnologías De La Información Y Comunicaciones de la Municipalidad Distrital de Los Olivos, Autorizó al alumno: Roger Jhoel Piñashca Huerta, identificado con DNI N°46156461, estudiante de la escuela Profesional de Ingeniería de Sistemas, y autor de trabajo de Investigación denominado: "**EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA**", al uso de la infraestructura tecnológica que conforma, servidores y equipos de comunicación entre otros, para efectos exclusivamente académicos de la elaboración de tesis, enunciada líneas arriba de quien solicite se garantice la absoluta confidencialidad de la información solicitada.

Atentamente,

MUNICIPALIDAD DISTRITAL DE LOS OLIVOS

Ing. Ricardo Gustavo Alvarado Bustos
GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Ing. Ricardo Gustavo Alvarado Bustos

Gerente De Tecnologías De La Información Y Comunicaciones

ANEXO 3. INSTRUMENTOS

FICHA PARA EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO USANDO MÉTRICAS CVSS

TESIS: Evaluación de técnicas de hacking ético para analizar la seguridad informática de la Municipalidad Distrital de los Olivos, Lima

N°	Técnica de Hacking	Servicio	Dirección IP	Vulnerabilidad	Puntuación	Impacto de confidencialidad
1	TÉCNICA	Servidor de base de datos				
2		Servidor web				
3		Servidor FTP				
4		Servidor SSH				

FICHA PARA EVALUAR EL ESTADO DE PUERTOS DEL COMANDO NMAP - .....

TESIS: Evaluación de técnicas de hacking ético para analizar la seguridad informática de la Municipalidad Distrital de los Olivos, Lima

COMANDO EJECUTADO	
PROCESO	
RESULTADOS ENCONTRADOS	

ANEXO 4. VALIDACIÓN DE INSTRUMENTO POR EXPERTOS

VALIDACIÓN DE INSTRUMENTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres AYBAR CORONEL JORGE LUIS

2.2. Grado del validador INGENIERO DE SISTEMAS E INFORMATICA

III. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	VALORACIONES				
		Deficiente	Regular	Bueno	Muy bueno	Excelente
CLARIDAD	Los ítems son claros y exactos.			X		
RELEVANCIA	Los ítems son apropiados para representar a las dimensiones específicas del constructo.			X		
PERTINENCIA	Los ítems corresponden al concepto teórico formulado			X		
SUFICIENCIA	Cubre todas las dimensiones de la variable de estudio.			X		
INTENCIONALIDAD	Adecuado a los propósitos de la investigación.			X		
SUBJETIVIDAD	Permite registrar información exacta sobre las variables que se investigan.			X		
METODOLOGÍA	Se hace posible el acopio de información con rigor científico.			X		

IV. OPINIÓN DE APLICABILIDAD

APLICABLE (X) APLICABLE DESPUES DE CORREGIR ( ) NO APLICABLE ( )

V. VALIDACIÓN FINAL DEL INSTRUMENTO

Muy alto	Alto	Medio	Bajo	Muy bajo
	X			

DNI: 40064319

FIRMA

VALIDACIÓN DE INSTRUMENTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres Damian Rojas Javier

2.2. Grado del validador Ingeniero de Sistemas

III. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	VALORACIONES				
		Deficiente	Regular	Bueno	Muy bueno	Excelente
CLARIDAD	Los ítems son claros y exactos.			X		
RELEVANCIA	Los ítems son apropiados para representar a las dimensiones específicas del constructo.			X		
PERTINENCIA	Los ítems corresponden al concepto teórico formulado			X		
SUFICIENCIA	Cubre todas las dimensiones de la variable de estudio.			X		
INTENCIONALIDAD	Adecuado a los propósitos de la investigación.			X		
SUBJETIVIDAD	Permite registrar información exacta sobre las variables que se investigan.			X		
METODOLOGÍA	Se hace posible el acopio de información con rigor científico.			X		

IV. OPINIÓN DE APLICABILIDAD

APLICABLE (X) APLICABLE DESPUES DE CORREGIR ( ) NO APLICABLE ( )

V. VALIDACIÓN FINAL DEL INSTRUMENTO

Muy alto	Alto	Medio	Bajo	Muy bajo
	X			

DNI: 47775397

FIRMA

VALIDACIÓN DE INSTRUMENTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres Peña Auticona Cesar Doyvi

2.2. Grado del validador Ingeniero Informático

III. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	VALORACIONES				
		Deficiente	Regular	Bueno	Muy bueno	Excelente
CLARIDAD	Los ítems son claros y exactos.			X		
RELEVANCIA	Los ítems son apropiados para representar a las dimensiones específicas del constructo.			X		
PERTINENCIA	Los ítems corresponden al concepto teórico formulado			X		
SUFICIENCIA	Cubre todas las dimensiones de la variable de estudio.			X		
INTENCIONALIDAD	Adecuado a los propósitos de la investigación.			X		
SUBJETIVIDAD	Permite registrar información exacta sobre las variables que se investigan.			X		
METODOLOGÍA	Se hace posible el acopio de información con rigor científico.			X		

IV. OPINIÓN DE APLICABILIDAD

APLICABLE (X) APLICABLE DESPUES DE CORREGIR ( ) NO APLICABLE ( )

V. VALIDACIÓN FINAL DEL INSTRUMENTO

Muy alto	Alto	Medio	Bajo	Muy bajo
	X			

DNI: 41456859

FIRMA

ANEXO 5. EVALUACIÓN DEL MODELO PROPUESTO POR ESPECIALISTAS

ESPECIALISTA 1

EVALUACIÓN DEL MODELO PROPUESTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres AYBAR CORONEL JORGE LUIS

2.2. Grado INGENIERO DE SISTEMAS E INFORMATICA

III. ASPECTOS DE VALIDACIÓN

CRITERIOS DE EVALUACIÓN DE LAS TÉCNICAS					
CRITERIO / RANGO	1	2	3	4	5
Integridad					X
Confiabilidad					X
Disponibilidad					X
TOTAL	15				

IV. OPINIÓN DE ESPECIALISTA SOBRE EL MODELO PROPUESTO

V. VALIDACIÓN FINAL DEL MODELO PROPUESTO

Alto	Medio	Bajo
X		

DNI: 40064319

FIRMA

ESPECIALISTA 2

EVALUACIÓN DEL MODELO PROPUESTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres: Limaco Rojas Jaime

2.2. Grado: Ingeniero de Sistemas

III. ASPECTOS DE VALIDACIÓN

CRITERIOS DE EVALUACIÓN DE LAS TÉCNICAS					
CRITERIO / RANGO	1	2	3	4	5
Integridad					X
Confiabilidad					X
Disponibilidad					X
TOTAL	15				

IV. OPINIÓN DE ESPECIALISTA SOBRE EL MODELO PROPUESTO

Que sea aplicado en el proyecto de Investigación.

V. VALIDACIÓN FINAL DEL MODELO PROPUESTO

Alto	Medio	Bajo
X		

DNI: 47779347

FIRMA

ESPECIALISTA 3

EVALUACIÓN DEL MODELO PROPUESTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres: Juan Diego Solanus Chozo

2.2. Grado: Ingeniero de Sistemas

III. ASPECTOS DE VALIDACIÓN

CRITERIOS DE EVALUACIÓN DE LAS TÉCNICAS					
CRITERIO / RANGO	1	2	3	4	5
Integridad					✓
Confiabilidad					✓
Disponibilidad				✓	
TOTAL					14

IV. OPINIÓN DE ESPECIALISTA SOBRE EL MODELO PROPUESTO

El modelo propuesto cumple con lo establecido para un análisis de calidad

V. VALIDACIÓN FINAL DEL MODELO PROPUESTO

Alto	Medio	Bajo
X		

DNI: 80778417

FIRMA

ESPECIALISTA 4

EVALUACIÓN DEL MODELO PROPUESTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres Peña Auticona Cesar Deyvi

2.2. Grado Ingeniero Informático

III. ASPECTOS DE VALIDACIÓN

CRITERIOS DE EVALUACIÓN DE LAS TÉCNICAS					
CRITERIO / RANGO	1	2	3	4	5
Integridad					X
Confiabilidad					X
Disponibilidad					X
TOTAL			15		

IV. OPINIÓN DE ESPECIALISTA SOBRE EL MODELO PROPUESTO

_____

_____

V. VALIDACIÓN FINAL DEL MODELO PROPUESTO

Alto	Medio	Bajo
X		

DNI: 41456859

FIRMA

ESPECIALISTA 5

EVALUACIÓN DEL MODELO PROPUESTO

I. TÍTULO DE LA TESIS:

EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA.

II. DATOS GENERALES:

2.1. Apellidos y nombres Díaz Díaz Anghi Marjorie

2.2. Grado Ingeniero de Sistemas

III. ASPECTOS DE VALIDACIÓN

CRITERIOS DE EVALUACIÓN DE LAS TÉCNICAS					
CRITERIO / RANGO	1	2	3	4	5
Integridad					X
Confiabilidad					X
Disponibilidad					X
TOTAL					15

IV. OPINIÓN DE ESPECIALISTA SOBRE EL MODELO PROPUESTO

El modelo propuesto presenta eficacia para analizar la calidad informatica.

V. VALIDACIÓN FINAL DEL MODELO PROPUESTO

Alto	Medio	Bajo
X		

DNI: 73147664

FIRMA

ANEXO 6

MANUAL DE INSTALACIÓN DE KALI LINUX

1. Cuando el archivo .iso que contiene la imagen haya sido cargada y se proceda al encendido de la nueva máquina virtual con las características mínimas que sugiera https://www.kali.org/docs/virtualization/ la pantalla de inicio será la imagen que se muestra a continuación, para lo cual se debe escoger la primera opción, un arranque de Graphical instal.

Pantalla arranque S.O de Kali Linux

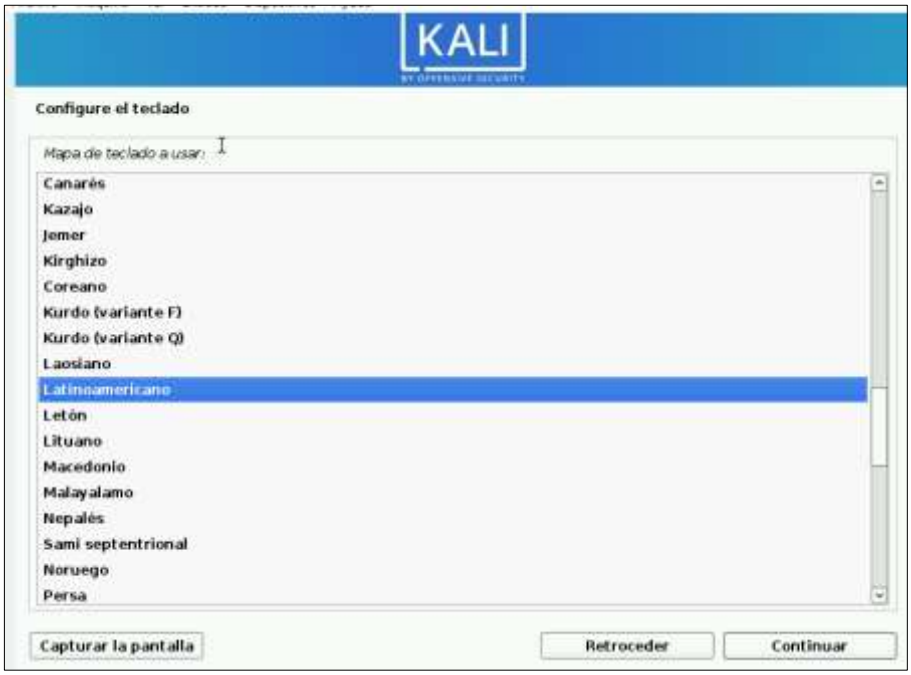
2. Una vez que el sistema arranque, visualizaremos en el escritorio el idioma a elegir en nuestro caso elegimos español.

Selección de idioma de Kali Linux

3. Procedemos a seleccionar la zona horario y región de ubicación en este caso Perú.

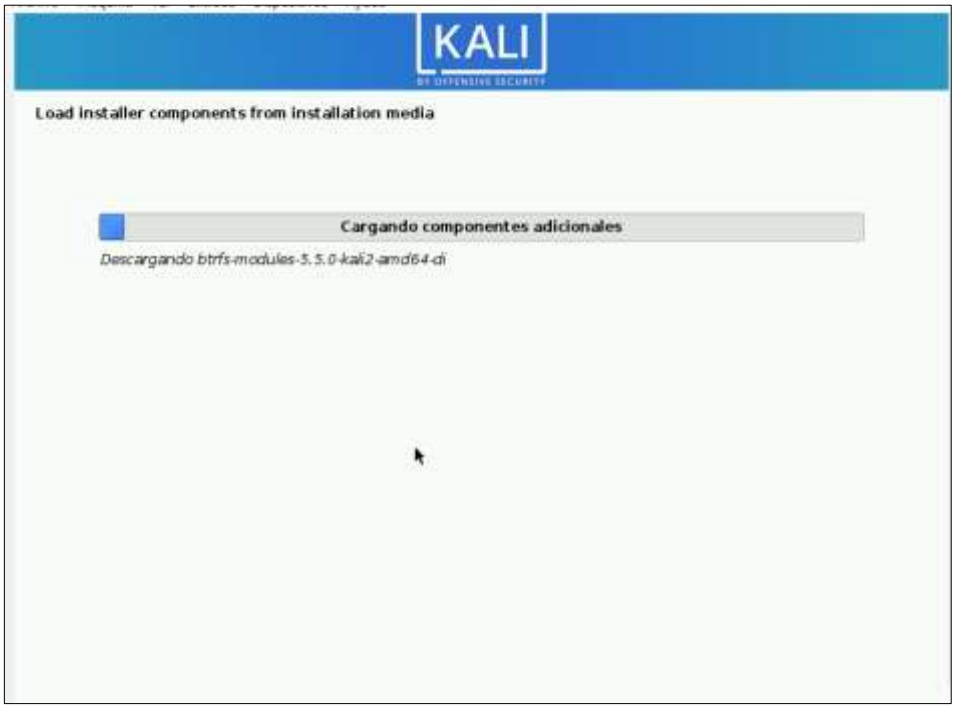
Selección de zona horaria.

4. Escogemos la distribución de teclado correspondiente en este caso vamos a elegir latinoamericano.



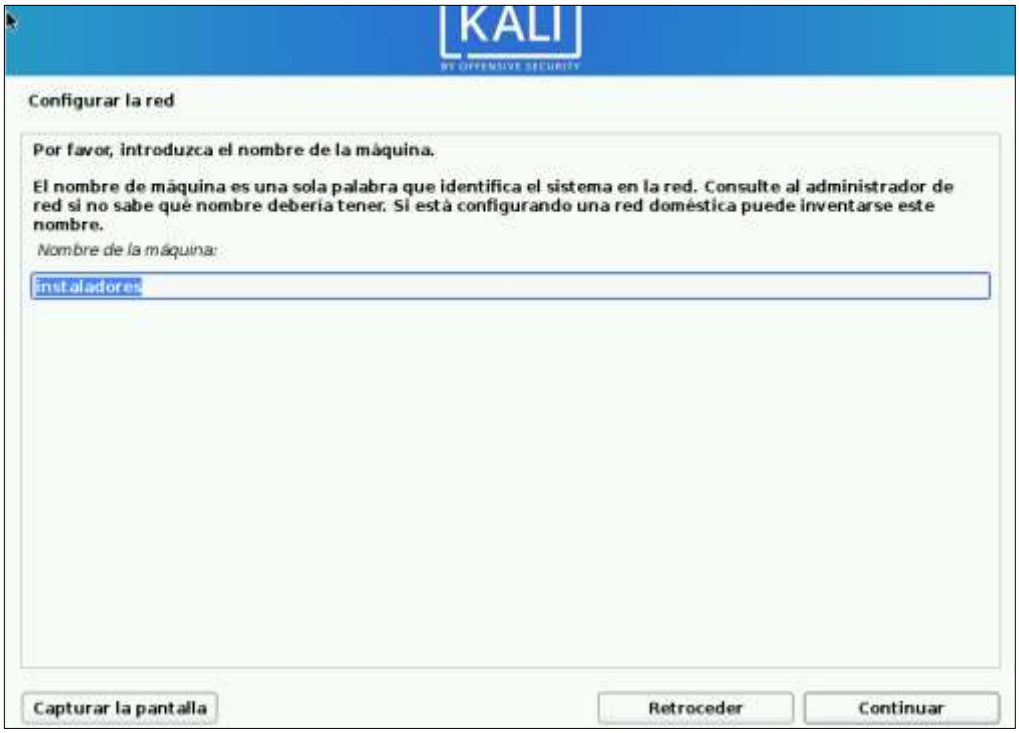
Selección del teclado

5. Esperamos el proceso de instalación que realizara el cargado de los componentes que requiere el sistema operativo.



Cargando Componentes

6. Colocamos el nombre de la maquina en este caso elegimos instaladores.

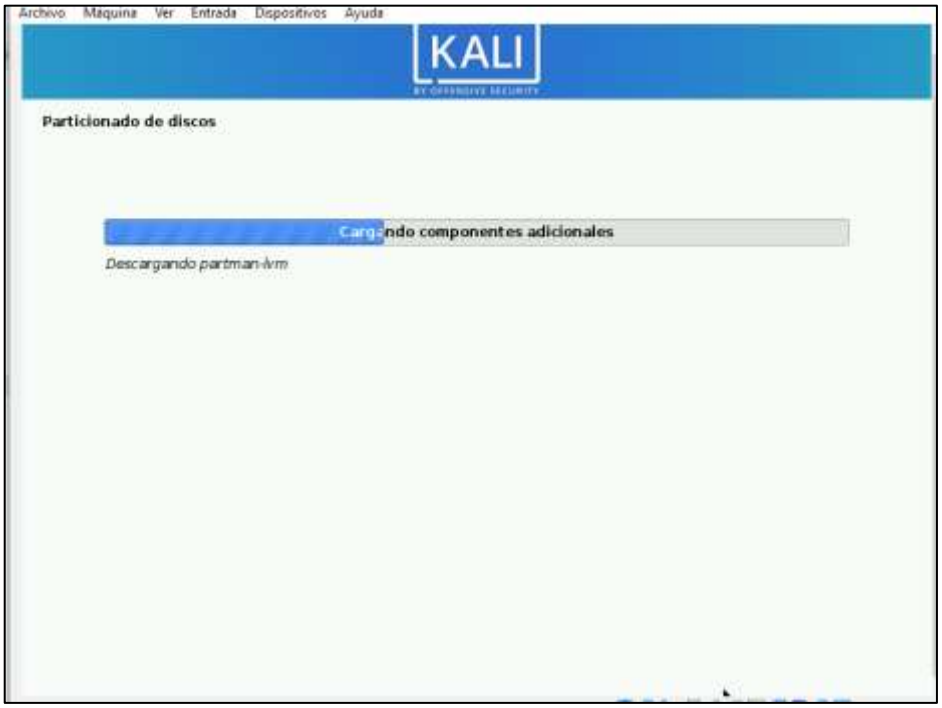


Nombre de la maquina

7. Procedemos con asignar un nuevo usuario en este caso se asigna el usuario control.

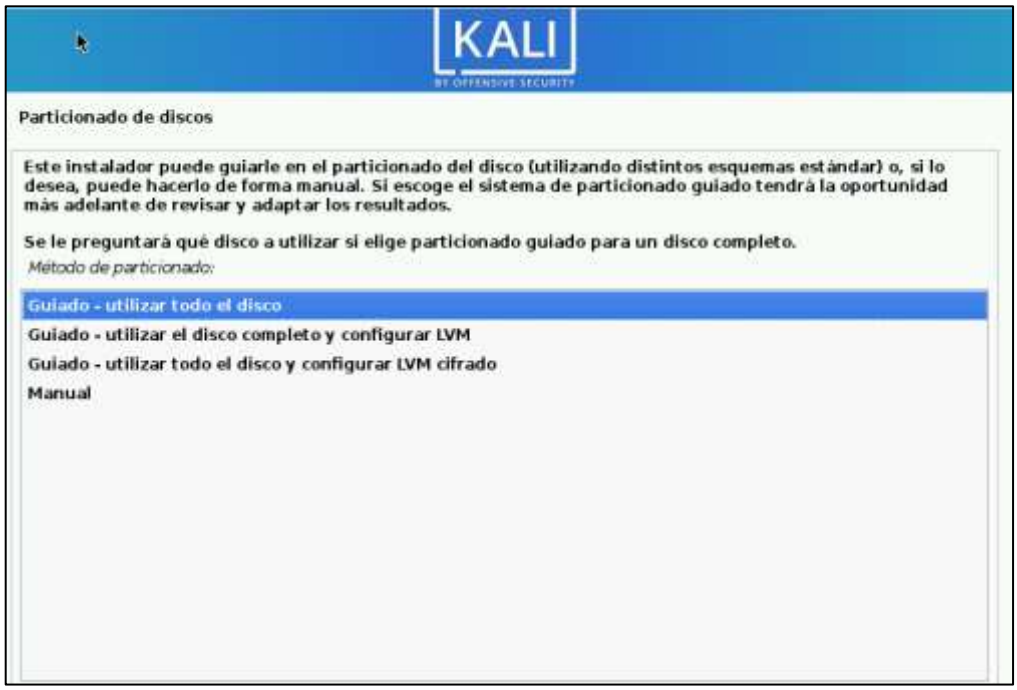
Nuevo usuario

8. Esperamos el proceso de cargado de componentes adicionales para el proceso de partición del disco duro.



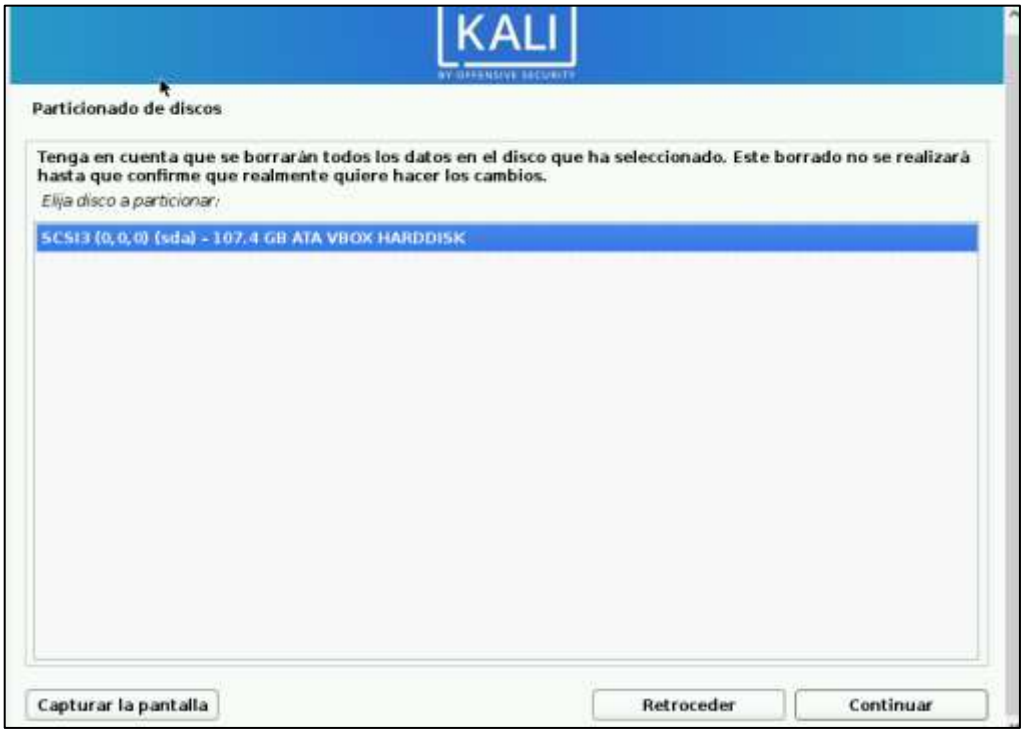
Cargado de componentes

9. Procedemos con la partición de las unidades de almacenamiento, en este caso vamos a utilizar toda la unidad que asignamos a la máquina virtual.



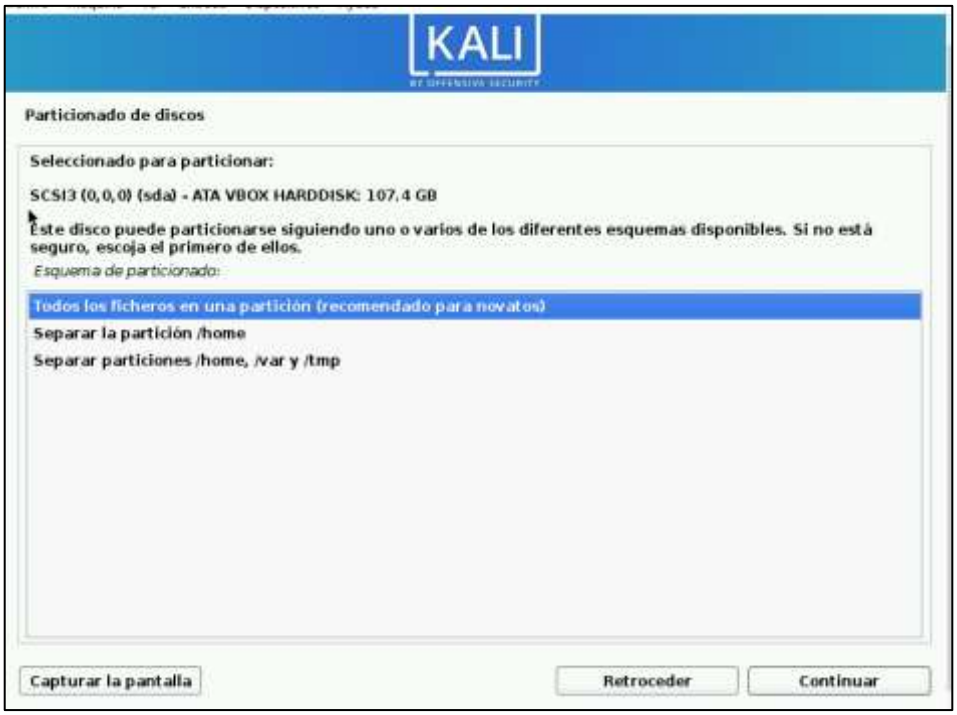
Partición de Disco Duro

10. Seleccionamos la unidad virtual para la instalación del sistema operativo según el proceso.



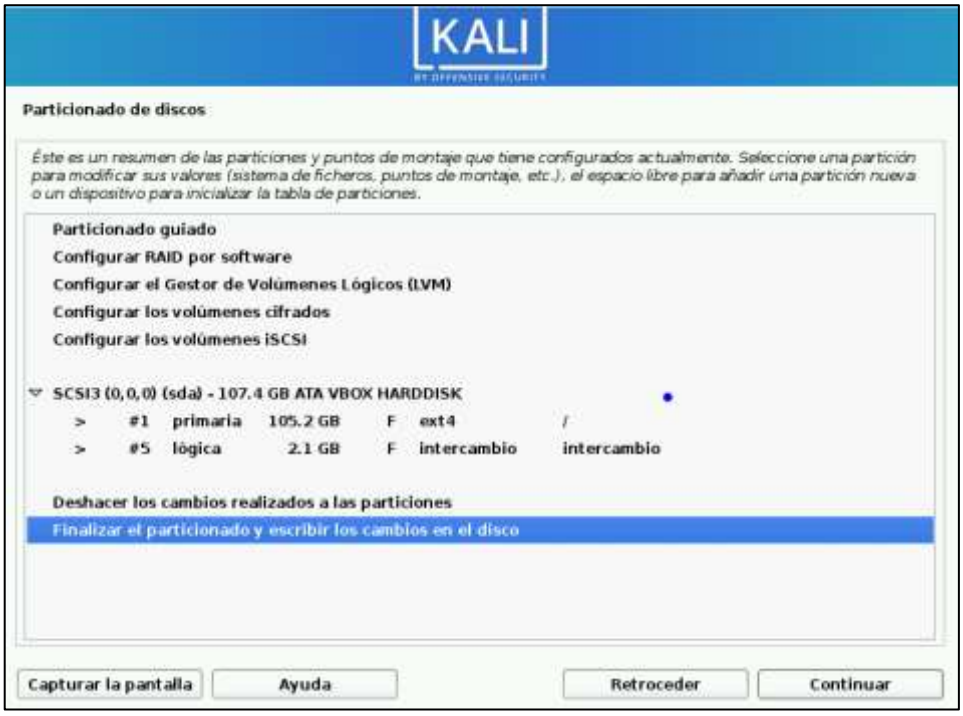
Partición de Disco Duro

11. Vamos a seleccionar toda la unidad para ser asignado al sistema operativo.



Partición de Disco Duro

12. Visualizamos que se realizó la partición por defecto asignando los 105.2 Gb a la raíz / y los 2.1 Gb al área de intercambio.



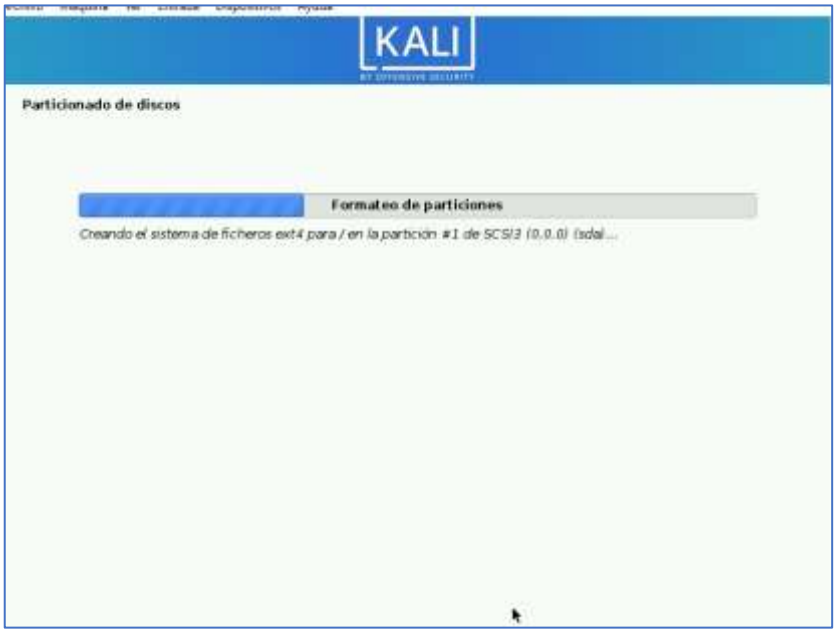
Partición de Disco Duro

13 . Procedemos con la opción de escribir los cambios según el proceso de instalación con este paso se realizará el formateo de la unidad de

almacenamiento virtual generando la particiona de la unidad según los procesos anteriores.

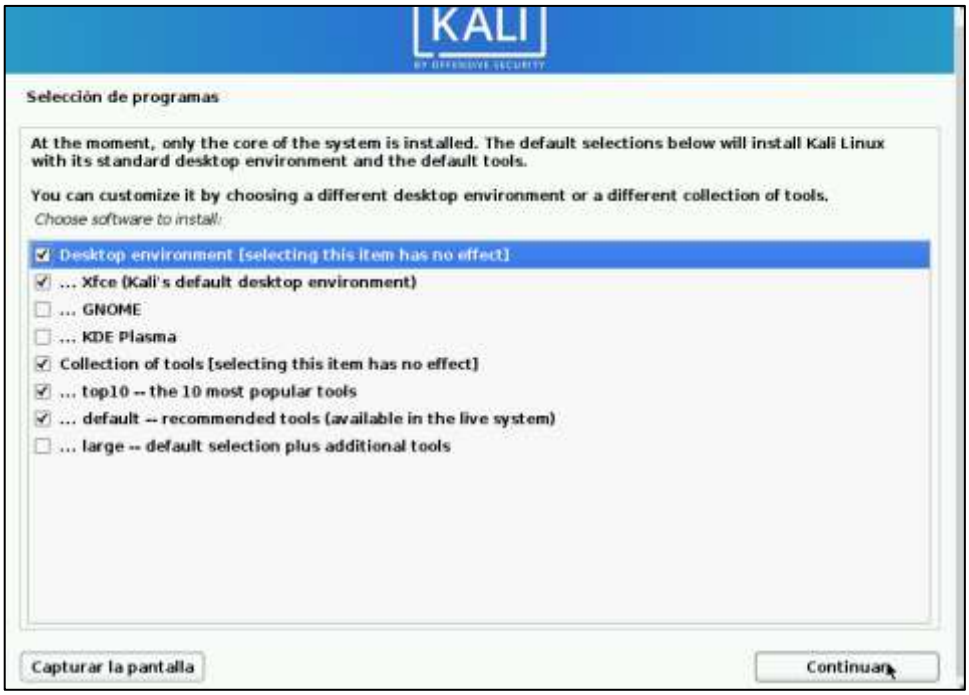
Partición de Disco Duro

14. Esperamos el proceso de particionar la unidad.



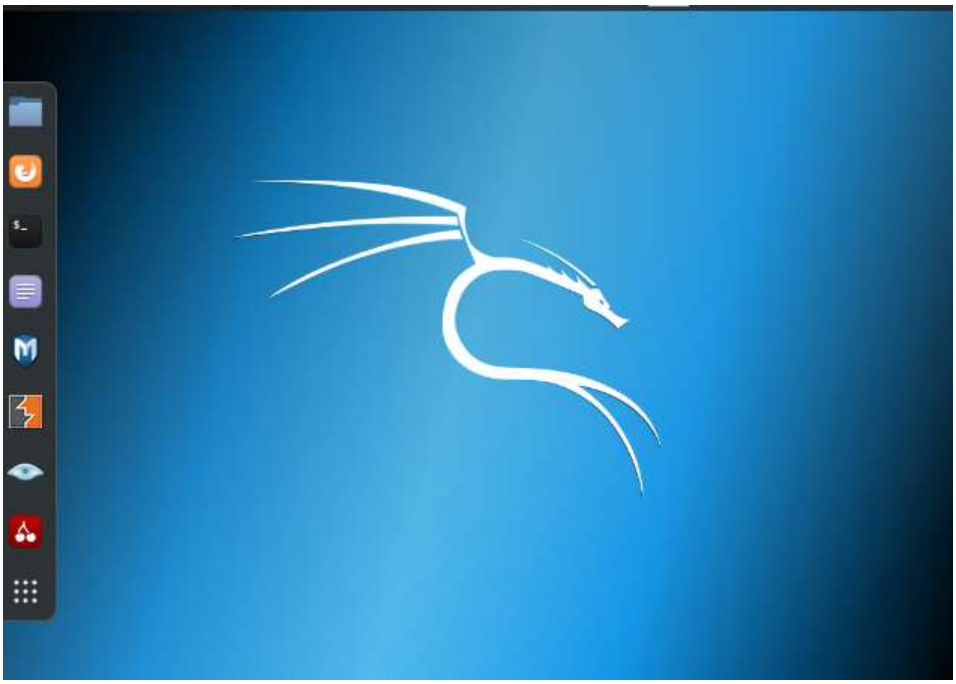
Partición de Disco Duro

15. Seleccionamos los programas a utilizar y la interfaz gráfica.



Selección grafica

16. Interfaz gráfica del escritorio de Kali linux.



```
root@control: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
```