UNIVERSIDAD CATÓLICA LOS ÁNGELES

CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ETHICAL HACKING CON KALI LINUX HACIA WINDOWS SERVER 2008 R2 PARA LA EMPRESA INFONET SOLUCIONES EIRL. - SULLANA; 2020.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL

DE INGENIERO DE SISTEMAS

AUTOR

CRIOLLO ORTIZ PAUL

ORCID: 0000-0002-5787-285X

ASESOR

MORE REAÑO RICARDO EDWIN

ORCID: 0000-0002-6223-4246

SULLANA – PERÚ

2020

EQUIPO DE TRABAJO

AUTOR

CRIOLLO ORTIZ PAUL

ORCID: 0000-0002-5787-285X

Universidad Católica Los Ángeles de Chimbote, Estudiante de Pregrado

Piura, Perú.

ASESOR

MORE REAÑO RICARDO EDWIN

ORCID: 0000-0002-6223-4246

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistemas, Piura, Perú.

JURADO

SULLÓN CHINGA JENNIFER DENISSE

ORCID: 0000-0003-4363-0590

SERNAQUÉ BARRANTES MARLENY

ORCID:0000-0002-5483-4997

GARCÍA CÓRDOVA EDY JAVIER

ORCID:0000-0001-5644-4776

HOJA DE FIRMA DEL JURADO Y ASESOR

MGTR. JENNIFER DENISSE SULLÓN CHINGA

PRESIDENTE

MGTR. MARLENY SERNAQUÉ BARRANTES

MIEMBRO

MGTR. EDY JAVIER GARCÍA CÓRDOVA

MIEMBRO

MGTR. RICARDO EDWIN MORE REAÑO

ASESOR

DEDICATORIA

Dedico toda mi investigación a mi Señora Madre Carmen Amelia Ortiz Maza de Criollo, que, en esta época terrible de pandemia, se fue de mi lado al llamado de nuestro Señor Jesucristo, esta memorable dama, siempre fue y será mi gran motivación para estudiar con ahínco y trabajar con honestidad.

También dedico mi trabajo a mi Señor Padre: Andrés Criollo García, mis hijos: Kervin Paul, Paul Andrés y Luis Sebastián y a mi señora esposa Leslie Janet García Zabaleta Suarez.

Paul Criollo Ortiz.

AGRADECIMIENTO

Un agradecimiento especial a mí asesor de todos los procesos de García mi investigación, me refiero al Ing. Ricardo More Reaño, parte del equipo y miembro de jurado de la Universidad Católica los Ángeles de Chimbote.

A todos los grupos y comunidades de seguridad, Ethical Hacking, Pentesting, Kali Linux que existen en Internet, así como foros, listas, wikis liderados y administrados por investigadores y hackers éticos en el mundo.

Toda la información encontrada me ha valido mucho para obtener información real y precisa, me permitió comparar con otros casos en otras realidades tecnológicas y sociales.

Agradezco a todas las personas cercanas que me apoyaron en todo momento con sus palabras positivas, para seguir logrando los proyectos profesionales y de vida.

Paul Criollo Ortiz.

RESUMEN

La presente investigación es desarrollada bajo la línea de investigación de Tecnología de Redes de Datos e Información, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; tuvo como objetivo Ejecutar un Ethical Hacking con Kali Linux para un Servidor con Windows 2008 Server R2 de la empresa Infonet Soluciones EIRL – Sullana 2020. El tipo de la investigación fue cuantitativa, nivel descriptivo, diseño no experimental y de corte transversal.; con una muestra de 10 personas; obteniendo como resultado en la dimensión: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2, se obtuvo que el 80% de los trabajadores expresaron que NO sienten segura su información con MS Windows 2008 Server R2 obsoleto. En la siguiente dimensión: Nivel del servicio en red para tener datos disponibles y exactos, se obtuvo que el 70% de los encuestados expresaron que SI hay un nivel alto de seguridad en los servidores de la empresa cundo los sistemas operativos y aplicaciones están actualizados. En la dimensión: Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables, se alcanzó que el 80% de los encuestados expresaron que, SI es necesario tener medidas de prevención y análisis, para minimizar los nivele de riesgos en seguridad de la información. que llegan a tener una similitud con la hipótesis planteada de la investigación.

Palabras claves: Hacking, Kali, Seguridad, Servidor, Windows.

ABSTRACT

The present investigation is developed under the line of investigation TIC Networks, of the Professional School of Engineering of Systems of the Catholic University Los Angeles de Chimbote; Its objective was to Execute an Ethical Hacking with Kali Linux for a Server with Windows 2008 Server R2 of the company Infonet Soluciones EIRL - Sullana 2020. The type of research was quantitative, descriptive level, non-experimental design and cross-sectional .; with a sample of 10 people; Obtaining as a result in the dimension: User satisfaction level regarding the use of secure systems and applications with MS Windows Server 2008 R2, it was obtained that 80% of the workers expressed that their information did NOT feel secure with MS Windows 2008 Server R2 obsolete. In the following dimension: Level of network service to have available and accurate data, it was obtained that 70% of the respondents expressed that there is a high level of security in the company's servers when the operating systems and applications are updated. In the dimension: Information Security Level, in order to have complete, timely and reliable data, it was reached that 80% of the respondents expressed that it IS necessary to have prevention and analysis measures, to minimize the levels of security risks of information. that come to have a similarity with the hypothesis raised from the research.

Keywords: Hacking, Kali, Security, Server, Windows

ÍNDICE DE CONTENIDOS

EQUIPO DE TRABAJO ii
HOJA DE FIRMA DEL JURADO Y ASESOR iii
DEDICATORIA iv
AGRADECIMIENTO v
RESUMEN vi
ABSTRACT vii
ÍNDICE DE CONTENIDOS viii
ÍNDICE DE GRÁFICOS x
ÍNDICE DE TABLAS xii
I. INTRODUCCIÓN 1
II. REVISIÓN DE LA LITERATURA 2
2.1 Antecedentes 2
2.1.1 Antecedentes a nivel nacional 2
2.1.2 Antecedentes a nivel nacional 3
2.1.3 Antecedentes a nivel regional 4
2.2 Bases teóricas 5
2.2.1 Información de “Infonet Soluciones E.I.R.L” 5
2.2.2 Información 7
2.2.3 Seguridad Informática 7
2.2.4 Ciberseguridad 8
2.2.5 Ciberseguridad y Tecnología 9
2.2.6 Ciberguerra 9
2.2.7 Hacking etico 10
2.2.8 Test de penetracion 11

2.2.9 Analisis de vulnerabilidades 12
2.2.10 EXPLOIT 13
2.2.11 KALI LINUX 15
III. HIPÓTESIS 16
IV. METODOLOGÍA 17
4.1 Diseño de la Investigación 17
4.2 Población y muestra 18
4.3 Definición de operacionalización de variables 19
4.4 Técnicas de instrumentos 20
4.5 Plan de análisis de datos 20
4.6 Matriz de consistencia 22
4.7 Principios éticos 24
V. RESULTADOS 25
5.1 Resultados 25
5.1.1 Dimensión 01: Nivel de acceso a la información 25
5.1.2 Dimensión 02: Nivel de seguridad de red 32
5.1.3 Dimensión 03: Nivel de diseño de Red Privada 39
5.2 Análisis de resultados 48
5.3 Propuesta de mejora 50
VI. CONCLUSIONES 69
RECOMENDACIONES 69
REFERENCIAS BIBLIOGRÁFICAS 70
ANEXOS 77
ANEXO I: Cronograma de actividades 78
ANEXO II: Presupuesto 79
ANEXO III: CUESTIONARIO 80
ANEXO IV: FICHA DE VALIDACIÓN PARA JUECES EXPERTOS 83

ÍNDICE DE GRÁFICOS

Gráfico Nro. 1: Logo Institucional Infonet Soluciones EIRL.....5
Gráfico Nro. 2: Organigrama de la Empresa.....6
Gráfico Nro. 3: 4 retos inaplazables de la seguridad informática.....8
Gráfico Nro. 4: Líderes IT de empresas medianas y grandes en México.....9
Gráfico Nro. 5: Ataques de malware en dispositivos móviles en América Latina.....9
Gráfico Nro. 6: Arquitectura de acceso seguro.....10
Gráfico Nro. 7: ¿Por qué el hacking ético es un recurso esencial para una pyme?.....12
Gráfico Nro. 8: Penetration Test (PENTEST).....13
Gráfico Nro. 9: Exploit.....14
Gráfico Nro. 10: Kali Linux 2020.3.....15
Gráfico Nro. 11: Resultado de la Dimensión 01 Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2.....31
Gráfico Nro. 12: Resultado de la Dimensión 02 Nivel del servicio en red para tener datos disponibles y exactos.....38
Gráfico Nro. 13: Resultado de la Dimensión 03 Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.....45
Gráfico Nro. 14: Resumen general de dimensiones.....47
Gráfico Nro. 15: Especificaciones del hardware.....50
Gráfico Nro. 16: Programas a Utilizar.....51
Gráfico Nro. 17: Instalación de vagrant.....51
Gráfico Nro. 18: Instalación de Plugin.....52
Gráfico Nro. 19: Descarga de metasploitable 3.....52
Gráfico Nro. 20: Descomprimir carpeta zip.....52
Gráfico Nro. 21: Instalación de virtual box.....53
Gráfico Nro. 22: Máquina virtual.....53
Gráfico Nro. 23: Instalacion de extensión de virtualbox.....54
Gráfico Nro. 24: Instalación exitosa de la extensión.....54
Gráfico Nro. 25: Descomprimir packer_1.5.0.....54
Gráfico Nro. 26: Copiar archivo packer.exe en la carpeta meetsploitable3.....55
Gráfico Nro. 27: Desactivar windows defender.....56
Gráfico Nro. 28: Instalacion de windows.....56
Gráfico Nro. 29: Instalación de windows exitoso.....57
Gráfico Nro. 30: Instalación Automática de aplicaciones.....57

Gráfico Nro. 31: Login de Windows 2008 Server R2 58
Gráfico Nro. 32: Escritorio de Windows 2008 Server R2 58
Gráfico Nro. 33: Avance del proceso de instalación de Metasploitable3 59
Gráfico Nro. 34: Agregar la máquina compilada a Vagrant 59
Gráfico Nro. 35: Iniciar nuestra máquina virtual 60
Gráfico Nro. 36: VirtualBox – MV Metasploitable3 60
Gráfico Nro. 37: MV Metasploitable3 – Windows 2008 Server R2 61
Gráfico Nro. 38: Ingresar Preferencias de red en VirtualBox 61
Gráfico Nro. 39: Cambiar modo de red 62
Gráfico Nro. 40: Status de dispositivo de red principal 62
Gráfico Nro. 41: Web de descargas Kali Linux para VirtualBox 63
Gráfico Nro. 42: Importar el servicio desde el archivo Ovx de KaliLinux 2020.3 63
Gráfico Nro. 43: Listado de MV de VirtualBox 64
Gráfico Nro. 44: Login de MV de KaliLinux 2020.3 64
Gráfico Nro. 45: Escritorio KaliLinux 2020.3 65
Gráfico Nro. 46: Consola de Comandos KaliLinux 2020.3 65
Gráfico Nro. 47: Escanear con nmap desde Kali Linux la máquina victima 66
Gráfico Nro. 48: Verificar la ejecución de un servidor web por el puerto 80, en equipo víctima 66
Gráfico Nro. 49: Ataque por fuerza bruta para Servidor FTP 67
Gráfico Nro. 50: Descomprimir rockyou.txt .gz 67
Gráfico Nro. 51: Crear nuevo diccionario passwd.txt 67
Gráfico Nro. 52: Descargar la aplicación FTP-Brute-Forcer 68
Gráfico Nro. 53: Ejecutar programa fuerza bruta 68
Gráfico Nro. 54: Conexión ftp 68

ÍNDICE DE TABLAS

Tabla Nro. 1: Definición Operacional 19
Tabla Nro. 2: Matriz de consistencia.....22
Tabla Nro. 3: Datos guardados están seguros en el servidor 25
Tabla Nro. 4: Utilizando MS Windows en Servidor los datos son seguros 26
Tabla Nro. 5: MS Windows 2008 Server R2 es robusto, fiable y seguro 27
Tabla Nro. 6: Utilizan sistemas operativos de red en Windows, por su facilidad de uso y popularidad 28
Tabla Nro. 7: Recomendaría MS Windows 2008 Server R2 29
Tabla Nro. 8: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2. 30
Tabla Nro. 9: Existen muchos ataques para MS Windows Server 2008 R2 32
Tabla Nro. 10: Falla del sistema operativo de un servidor, generará caos en los usuarios finales 33
Tabla Nro. 11: Datos almacenados en NTFS o FAT32, generan tranquilidad.....34
Tabla Nro. 12: MEF no debe recomendar OS Windows 2008 Server R2 para el SIAF 35
Tabla Nro. 13: La mejor decisión es migrar hacia Windows 2019 Server para minimizar las fallas de seguridad.....36
Tabla Nro. 14: Dimensión Nivel del servicio en red para tener datos disponibles y exactos. 37
Tabla Nro. 15: Utilizando un sistema operativo como MS Windows 2008 Server R2, las fallas de seguridad, vulnerabilidades, bugs, etc, son mínimas o escasas. 39
Tabla Nro. 16: Es necesrio realizar un ethical hacking anual para descubrir las fallas de seguridad en un servidor con un sistema operativo como Windows Server 2008 R2.....40
Tabla Nro. 17: Al realizar un ethical hacking en un sistema operativo se descubre las fallas y los niveles de seguridad actual, es necesario realizar procedimientos, levantamiento de observaciones o solo es para informarse. 41
Tabla Nro. 18: Utilizando Kali Linux actualizado, podemos realizar unos procesos de pentesting muy profesionales y profundos. 42
Tabla Nro. 19: Los servicios como AD, File Server, DNS, SiAF, SIGA, en cualquier institución están seguros, estando estos sistemas instalados en sistemas como MS Windows Server R2. 43
Tabla Nro. 20: Dimensión Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables. 44
Tabla Nro. 21: Resumen de Dimensiones 46

I. INTRODUCCIÓN

Según Tori (1) en su libro titulado Hacking Ético, hace algún tiempo, cuando algunas de las organizaciones apenas comenzaban a incrementar los procesos informatizados dentro de su sistema de información, sus propios administradores y analistas técnicos eran los encargados de buscar claras falencias o brechas de seguridad en el escenario para solucionarlas como podían. En ese entonces, la mayoría no tenía una noción madura acerca de la seguridad de la información o de las intrusiones de terceros no autorizados en sus sistemas. A medida que pasó el tiempo, estas organizaciones se multiplicaron de manera notable y se informatizaron aún más, incluso tomando a Internet como plataforma de sus movimientos de información. De ese modo, se hicieron fluidas las comunicaciones interpersonales, intersucursales, transacciones o flujo digital de todo tipo y nivel de importancia, dejando, al mismo tiempo, muchos más datos expuestos a terceros, como nunca antes había sucedido.

La presente investigación es desarrollada bajo la línea de investigación de Tecnología de Redes de Datos e Información. La investigación se realizó en la empresa Infonet Soluciones EIRL – Sullana, para descubrir vulnerabilidades de seguridad en el sistema operativo y aplicaciones del servidor con Windows 2008 Server R2. ¿ Con el Ethical Hacking ejecutado al Servidor Windows 2008 Server R2 de la empresa Infonet Soluciones EIRL – Sullana, se descubrirán las vulnerabilidades, riesgos y el nivel de exposición de los datos almacenados en el sistema operativo?

La investigación tiene como objetivo ejecutar un Ethical Hacking con Kali Linux para un Servidor con Windows 2008 Server R2 de la empresa Infonet Soluciones EIRL - Sullana.

La investigación se justifica económicamente porque al realizar el análisis de vulnerabilidades y reparación de las fallas a la brevedad posible, se lograa evitar pérdidas económicas, que aparecen cuando existe fuga de información, credenciales, transferencias, etc.

La investigación se justifica tecnológicamente porque hablamos lograremos implementar tecnología de punta, con altos niveles de ciberseguridad y esto va permitir que usuarios y clientes estén satisfechos en el uso de la misma.

II. REVISIÓN DE LA LITERATURA

2.1 Antecedentes

2.1.1 Antecedentes a nivel internacional

Rendon y Raza (2), en el 2019, en su investigación titulada "Análisis de Vulnerabilidades en Sistemas Informáticos Web desde la Red de Internet utilizando Herramientas de Hacking Ético y la Metodología Owasp." Se estableció que a través de estos se logra rastrear y evaluar las vulnerabilidades en los sistemas de información. El procedimiento planteado reside en realizar un levantamiento de información, luego se procede al análisis identificando los activos que evidencia riesgos. En conclusión, se obtuvo que el planteamiento propuesto sea efectivo y permite identificar y evaluar las vulnerabilidades, ayudando a que los que administran las pequeñas empresas (Pymes) mejoren los riegos reales que se presentan permitiendo mitigar la vulnerabilidad de seguridad, estas herramientas son muy prácticas.

Benítez (2), en el 2019, en su investigación titulada "Análisis de Riesgo en Redes Wifi Aplicando Técnicas de Hacking Ético". El presente trabajo de titulación tiene como objetivo realizar un análisis de riesgos a nivel de redes inalámbricas en una empresa cuyo modelo de negocio es la venta y comercialización de productos en el área turística por lo que su especialidad es totalmente ajena al de la tecnología, por lo tanto, no están tan familiarizados con atacantes, métodos y técnicas que involucren la apropiación de información a través de dispositivos electrónicos o software por parte de usuarios no autorizados. Para este trabajo se utilizarán dos metodologías la primera de ellas permitirá identificar los activos críticos, determinar si cuentan con procesos o una documentación robusta que les permita mitigar riesgos y amenazas de seguridad informática en sus activos, conocer si sus empleados saben cómo actuar frente alguna amenaza y sobre todo identificar si existen vulnerabilidades críticas en todas sus áreas.

Huilca (3), en el 2012, en su investigación titulada "Hacking Ético para detectar vulnerabilidades en los Servicios de la Intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos". El tema investigativo es hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado Municipal del Cantón Cevallos.

2.1.2 Antecedentes a nivel nacional

Bernal y Echevarría (4), en el 2019, en su investigación titulada "Modelo de Niveles de Seguridad para Pruebas de Intrusión en Aplicaciones Web para Pymes en el Perú". El presente proyecto de tesis se realizó con el propósito de determinar el nivel de seguridad de las aplicaciones web y detectar las vulnerabilidades a tiempo, para mitigar los posibles ciberataques antes de que las aplicaciones se encuentren en el entorno de producción.

Guillinta y Merino (5), en el 2016, en su investigación Titulada "Modelo de Prevención y Defensa contra Ataques Cibernéticos basado en Estándares de Seguridad Internacionales para IT-Expert". En la Encuesta global de Seguridad de la Información 2014, muestra que los incidentes de seguridad detectados se han incrementado en un 25% respecto al año anterior y los costos financieros de los incidentes han aumentado un 18%, es claro que cada día las organizaciones se encuentran más expuestas a riesgos que podrían representar grandes pérdidas económicas, así como la pérdida de la imagen corporativa ante sus clientes.

Cruz (6), en el 2014, en su investigación titulada "Aplicación de Auditoría Penetration Testing para contribuir con la Seguridad de la Información en los Sistemas Informáticos de la Empresa Data Business SAC, Trujillo". Debido a la creciente necesidad de utilización de poderosas computadoras conectadas en red para poder mantener una empresa en funcionamiento, y para poder realizar seguimientos de nuestra información personal, se han desarrollado

industrias enteras dedicadas a la práctica de la seguridad de redes y computadoras. Numerosas empresas han solicitado la pericia y el conocimiento de expertos en seguridad para poder controlar correctamente sus sistemas, y para que diseñen soluciones adecuadas a los requerimientos operativos de la organización. Debido a la naturaleza dinámica de muchas de estas organizaciones, donde los trabajadores deben tener acceso a los recursos informáticos, ya sea en forma local o remota, la necesidad de entornos de computación seguros se ha hecho más pronunciada.

2.1.3 Antecedentes a nivel regional

López (7), en el 2019, en su investigación titulada "Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú". Hoy en día los ataques a organizaciones privadas, como a una planta industrial automatizada de ensamblaje de misiles, y a entidades públicas, como la alteración de los resultados en un proceso electoral en el sistema de base de datos de la Oficina Nacional de Procesos Electorales (ONPE), generan gran impacto. Estas intrusiones, que los agresores utilizan, son cada vez más sofisticadas, organizadas e ingeniosas. Los indicios de posibles actividades maliciosas pueden ser difíciles de observar y pueden llegar a pasar desapercibidas. Se hace necesario por tanto revisar los eventos en varias herramientas de seguridad correlacionadas entre sí que monitoreen la red para encadenar y entender una serie de acciones que conlleven a la posibilidad real de detectar una intrusión en los sistemas.

Ancajima (8), en el 2019 "Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016." La presente tesis se desarrolló bajo la línea de investigación en tecnologías de información y comunicación (TIC) para la mejora continua de la calidad de las organizaciones del Perú de la escuela profesional de Ingeniería de sistemas, la cual estuvo basada en realizar una Propuesta de Implementación de Seguridad

Informática en las Tic de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.

Sandoval (9), en el 2017, en su investigación titulada "Diseño de un Plan de Seguridad de la Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, período 2015-2018". El contenido de esta tesis ayudará a las organizaciones y/o empresas ya sean grandes o pequeñas a tener una concienciación permanente de mantener seguros sus activos, teniendo en cuenta que la palabra activo son todos los recursos informáticos o relacionados con este para que la organización funcione correctamente y alcance los objetivos propuestos.

2.2 Bases teóricas

2.2.1 Información de "Infonet Soluciones E.I.R.L"

Reseña histórica

Infonet Soluciones EIRL es una empresa que da consultoría de seguridad informática, implementación y configuraciones de servidores, asesorías, charlas. Contamos con más de 10 años de experiencia. Somos especializados, contamos con muchos años de experiencia, nuestros clientes nos respaldan.

Ubicación

Av. José de Lama Sullana 149 – Sullana – Piura.

Logo Institucional

Gráfico Nro. 1: Logo Institucional Infonet Soluciones EIRL

Fuente: Infonet Soluciones EIRL

Misión

Nuestra misión es concientizar y segurizar a las empresas a mejorar sus servidores, aplicaciones web, Sistemas, con asesorías y Análisis Pen test, Hacking Ético, mejorando su infraestructura, evitar filtraciones de datos, documentos y alteración de dicho. Dándole una mejor solución en Seguridad para las empresas.

Visión

Alcanzar y prevenir múltiples ataques que perjudiquen a las empresas. La prevención es el arma para un Hackeo y que cada día sea un reto más en proteger la seguridad de la empresa. Que nuestros clientes queden satisfechos, por contactar a Infonet Soluciones.

Organigrama

Gráfico Nro. 2: Organigrama de la Empresa

Fuente: Elaboración Propia

Hardware

- Server Compatible: i3 1.7Ghz, 32 GB Ram, SSD 128 Gb, HD 1 Tb
- Server Compatible: i5 2.8 Ghz, 16 GB Ram, SSD 02 HD 1 Tb
- HP Server Proliant XEON G7, 16 Ram, HD 2 Tb

Sofware

- Windows Server 2008 Server R2
- Proxmox 6
- Nethserver 7
- Centos 6
- Centos 7

2.2.2 Información

La información es el centro del poder de una empresa, en el mundo moderno se consideran activos de la organización. La información se estructura de datos que provienen de diferentes fuentes y que circulan a través de las bases y las redes cibernéticas, transformando las velocidades y espacialidades de su acceso y utilidad, pero que a su vez, la expone a niveles de riesgo (10).

Acciones que requieren cada vez, unos niveles óptimos de seguridad, pues implican la disponibilidad de datos tanto personales como empresariales de alta privacidad. La seguridad que se ofrezca es determinante en la construcción de confianzas que se reflejan necesariamente en la rentabilidad y el crecimiento de una empresa (10).

2.2.3 Seguridad Informática

Actualmente la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y en muchos casos más compleja de manejar, ya que los procesos en muchos casos no son tan visibles para los involucrados (11).

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando (11).

Gráfico Nro. 3: 4 retos inaplazables de la seguridad informática

Fuente: Prodwareblog (12)

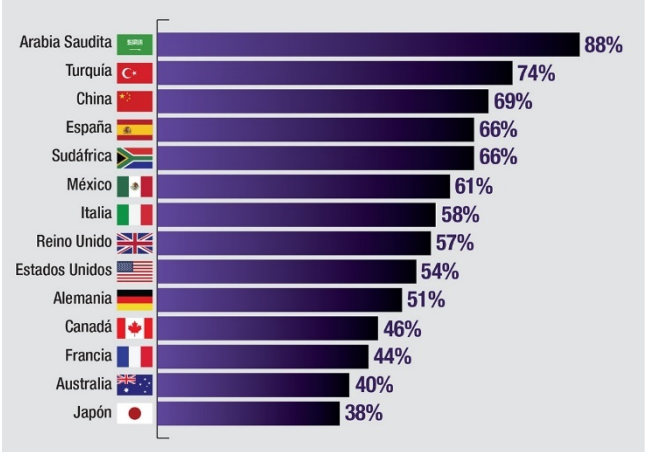
2.2.4 Ciberseguridad

EL 76,19% de las empresas ha tenido un incidente con consecuencias significativas en los últimos 6 meses, según se pone de manifiesto en el reciente estudio "Las preocupaciones de los CISOs" (13).

Datos como este explican el peso que está ganando la ciberseguridad en las empresas españolas, así como la relevancia progresiva que el director de Ciberseguridad está alcanzando en las organizaciones, donde su mensaje está calando en la alta dirección, cada vez más consciente de la necesidad de estar protegido frente a ciberamenazas (13).

El estudio pone de manifiesto que existe una relación directa muy pronunciada entre la inversión en ciberseguridad y la minimización de los ciberataques reportados. Por consiguiente, entender la ciberseguridad como parte de la estrategia de negocio, en todo tipo de empresas, con independencia de su tipología, resultará clave para la toma de medidas eficientes (13).

Gráfico Nro. 4: Líderes IT de empresas medianas y grandes en México



Fuente: Safety Detectives (14)

2.2.5 Ciberseguridad y Tecnología

Las tendencias apuntan a que la evolución tecnológica debería demandar mayores revisiones de seguridad, entornos cloud y aplicaciones tecnológicas (13).Sin embargo, el estudio revela que las revisiones siguen siendo insuficientes, la tecnología blockchain sigue estando ausente en casi todos los departamentos de Ciberseguridad de las empresas y solo el 30% de los sectores está apostando por la IA para potenciar su ciberseguridad. A diferencia de otras tecnologías más disruptivas, la IoT sí que está presente en la estrategia de ciberseguridad de las empresas (13).

Gráfico Nro. 5: Ataques de malware en dispositivos móviles en América Latina

Fuente: Statista (15)

2.2.6 Ciberguerra

La ciberguerra es asimétrica. El bajo costo de los equipos informáticos puede implicar que los eventuales adversarios no tengan necesidad de fabricar armamento sofisticado y de altos costos para suponer una amenaza significativa a las capacidades militares, ya sea afectando la planificación operacional o anulando los sistemas de inteligencia, de mando y control (16).

Junto a la ciberguerra se establece todo un panel de amenazas cibernéticas que hacen plausible, viable, y probable, como un Pearl Harbor cibernético. Esto implica un riesgo cuyo origen (país u organización) no será posible conocer. De lo que no cabe la menor duda es que el riesgo es real, y que, como ocurriera en un día, en la forma de un ataque aéreo, pueda trasladarse a otro tipo de ataque, por sorpresa, con la abierta intención de producir daño (16).

Luego, cabe pensar que una operación de ciberataque de una envergadura considerable puede conllevar importantes riesgos para quien las vaya a sufrir. Esta es la razón de que los países se preparen con la creación de estructuras orgánicas, como es el caso de Alemania, que el 1 de abril del 2017, dio inicio al funcionamiento oficial de su Cyber and Information Space Command (CIR), el cual constituye una fuerza de trabajo mixta entre civiles y militares, compuesta por aproximadamente 13.500 personas (16).

Gráfico Nro. 6: Arquitectura de acceso seguro

Fuente: FORTINET (17)

2.2.7 Hacking ético

Acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole en algunos casos acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente (18).

2.2.8 Test de penetración

Es un procedimiento de auditoría de seguridad activa en el que con autorización del propietario de un sistema de información, el auditor de seguridad analiza el susodicho sistema buscando de forma proactiva agujeros de seguridad vulnerables (19).

El test puede terminar al encontrar una vulnerabilidad, aunque solo sea explotable teóricamente; puede precisar el desarrollo de una prueba de concepto para validar que la vulnerabilidad encontrada es explotada, o puede incluso llegar a requerir que se demuestre la vulneración llegando a explotar la vulnerabilidad (19).

El test de intrusión no está enfocado a una máquina, sino a un sistema de información concreto, esto involucra los servidores, los ordenadores de sobremesa y el software de sistemas, pero y esto se olvida con frecuencia, involucra también al personal, a las mecánicas y los procedimientos de la empresa y a la gestión de la información en su sentido más amplio (19).

Gráfico Nro. 7: ¿Por qué el hacking ético es un recurso esencial para una pyme?

Fuente: ESIC (20)

2.2.9 Análisis de vulnerabilidades

Mantenerse al día con las amenazas de seguridad cibernética y el cumplimiento reglamentario no es fácil. Muchas empresas contratan la ayuda de asesores fiables para comprender mejor su seguridad cibernética y su postura de cumplimiento, aprender las prácticas recomendadas y perseguir sus objetivos de negocio frente a la incertidumbre cibernética. Con un asesor confiable, usted puede anticipar mejor la disrupción, adaptarse a un escenario de seguridad cambiante y ver nuevas innovaciones a fin de obtener una ventaja competitiva sin perder de vista la seguridad (21).

Las organizaciones líderes buscan referencias precisas de dónde se encuentran y desarrollan planes para gestionar mejor el riesgo, el cumplimiento y la gobernanza. Estas evaluaciones pueden incluir cuantificación de riesgos, identificación de riesgos de seguridad de terceros; pruebas de penetración para encontrar debilidades en el sistema propio de uno; así como simulaciones de violaciones cibernéticas para poner a prueba al personal y a la tecnología,

identificar requisitos y generar memoria muscular para prepararse para los ataques cibernéticos (21).

Cada vez más, los rangos cibernéticos se están convirtiendo en parte de las estrategias de gestión de riesgos de las organizaciones líderes. Permiten que las organizaciones reúnan sus equipos de seguridad y ejecutivos clave para experimentar una violación de seguridad simulada en un entorno contenido. Una experiencia de rango cibernético puede ayudar a las organizaciones a evaluar las brechas en su plan de respuesta ante incidentes y evaluar en forma crítica cómo sus equipos de seguridad y cumplimiento deberían integrar la respuesta ante incidentes en toda su organización (16).

Gráfico Nro. 8: Penetration Test (PENTEST)

Fuente: Open IT (22)

2.2.10 EXPLOIT

Existen ciertas vulnerabilidades que pueden ser aprovechadas a través del uso de herramientas desarrolladas exclusivamente para ese fin, que se denominan exploits. Dicho software suele estar desarrollado para afectar específicamente a una vulnerabilidad en particular. Su fin puede ser el de permitir ejecutar código arbitrario o, simplemente, de tirar abajo un sistema (23).

Los exploits pueden ser escritos empleando una diversidad de lenguajes de programación aunque suele usarse el lenguaje C aunque en la actualidad podemos encontrar C++, C#, Python, Perl, etc. También pueden valerse de distintos tipos de ataques, tales como desbordamiento de búfer, Cross Site Scripting, Format Strings e Inyección SQL, entre otros (23).

Gráfico Nro. 9: Exploit

Fuente: GuayoyoMedium (24)

2.2.11 KALI LINUX

Kali Linux es una distribución basada en GNU/Linux Debian, destinado a auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas, las cuales están destinadas hacia varias tareas en seguridad de la información, como pruebas de penetración, investigación en seguridad, forense de computadoras, e ingeniería inversa. Kali Linux ha sido desarrollado, fundado y mantenido por Offensive Security, una compañía de entrenamiento en seguridad de la información (25).

Kali Linux fue publicado en 13 de marzo del año 2013, como una reconstrucción completa de BackTrack Linux, adhiriéndose completamente con los estándares del desarrollo de Debian (25).

Gráfico Nro. 10: Kali Linux 2020.3

Fuente: Kali (26)

III. HIPÓTESIS

La propuesta de ejecutar los procedimientos de un Ethical Hacking para un Servidor Microsoft Windows Server 2008 R2, de la empresa Infonet Soluciones E.I.R.L - Sullana; permitirá que los datos almacenados se salvaguarden adecuadamente, minimizando las vulnerabilidades y riesgos informáticos.

IV. METODOLOGÍA

4.1 Diseño de la Investigación

Tipo de investigación

Esta investigación es una investigación cuantitativa, por lo tanto, Fernández, P. y Díaz, P. (27), define que trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede.

Nivel de investigación

De acuerdo a la naturaleza del estudio de la investigación, reúne por su nivel, las características de un estudio descriptivo. Según Tamayo y Tamayo M. (28), en su libro Proceso de Investigación Científica, la investigación descriptiva "comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente".

Según Sabino (29), "La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta. Para la investigación descriptiva, su preocupación primordial radica en descubrir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento. De esta forma se pueden obtener las notas que caracterizan a la realidad estudiada".

Diseño de la investigación

El diseño de esta investigación fue de tipo no experimental el mismo que define Shadish W. (30), afirma que: "Los Diseños no

experimentales, son aquellos en los que se identifica un conjunto de entidades que representan el objeto del estudio y se procede a la observación de los datos. En cuanto a la dimensión temporal, la investigación además de ser no experimental también es de corte transversal como lo define Seehorn (31), implica la recogida de datos una vez durante una cantidad de tiempo limitada. La investigación transversal suele ser descriptiva más que experimental.

4.2 Población y muestra

Población

La Población conjunto de elementos que tengan una o más propiedades en común definidas por el investigador y que puede ser desde toda la realidad, hasta un grupo muy reducido de fenómenos (32).

La población se conforma por 10 trabajadores en el área de Soporte y Redes, quienes están involucrados en el uso del Servidor Windows 2008 Server R2, en la en la empresa “Infonet Soluciones E.I.R.L.”.

Muestra

La muestra la obtenemos de la composición de toda la población, se desea obtener resultados más precisos, ya que están relacionados directamente con los procesos propios del estudio e investigación.

4.3 Definición de operacionalización de variables

Tabla Nro. 1: Definición Operacional

Variable	Descripción Conceptual	Dimensiones	Indicadores	Definición Operacional
Ethical Hacking Con Kali Linux hacia Windows Server 2008 R2	**Hacking Ético** Acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas (14). **Kali Linux** Kali Linux es una distribución basada en GNU/Linux Debian, destinado a auditorias de seguridad y pruebas de penetración avanzadas (18).	Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2. Nivel del servicio en red para tener datos disponibles y exactos. Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.	• Administración de los datos. • Compartición de recursos. • Personal especializado en seguridad. • Minimización de tiempos de caída de sistema por fallas de seguridad. • Levantamiento de observaciones de seguridad en los riesgos del sistema operativo de red.	El Ethical Hacking son un grupo de procedimientos que se llevan a cabo con el OS Kali Linux hacia un Servidor de Red con MS Windows 2008 Server R2 de la empresa Infonet Soluciones E.I.R.L", para detectar las fallas de seguridad que presenta el sistema operativo y sus aplicaciones.

4.4 Técnicas de instrumentos

Técnicas

En el presente trabajo de investigación se utilizará la técnica de la encuesta y como instrumento para la elaboración de ésta, será el cuestionario. La técnica que se utilizó en esta investigación será la encuesta que, según Mayntz citado por Díaz de Rada, describen que es la búsqueda sistemática de información en la que el investigador pregunta a los investigados sobre los datos que desea obtener, y posteriormente reúne estos datos individuales para obtener durante la evaluación datos agregados (33).

Instrumento

El instrumento que se utilizó es el cuestionario que según Casas es un documento que recoge en forma organizada los indicadores de las variables implicadas en el objetivo de la encuesta (34).

4.5 Plan de análisis de datos

A partir de los datos que se obtuvieron, se creó una base de datos temporal en el software Microsoft Excel 2016 y se procedió a la tabulación de los mismos. Se realizó el análisis de datos con cada una de las preguntas establecidas dentro del cuestionario dado permitiendo así resumir los datos en un gráfico que muestra el impacto porcentual de las mismas.

Este procedimiento se utilizó para agrupar los datos por medio de computadoras, a tabular, ponderar e interpretar los datos usando una hoja de cálculo en Excel, se presentó la información recopilada por medio de encuestas que fueron transcritas a su posterior análisis, en

este caso el indicador estadístico fue presentado como información en forma de cuadros y gráficos.

4.6 Matriz de consistencia

TÍTULO: ETHICAL HACKING CON KALI LINUX HACIA WINDOWS SERVER 2008 R2 PARA LA EMPRESA INFONET SOLUCIONES EIRL. - SULLANA; 2020.

Tabla Nro. 2: Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	METODOLOGÍA
¿Las organizaciones peruanas gubernamentales que utilizan el sistema operativo de red Windows 2008 Server R2, se encuentran seguras, están libres de fuga de información, ¿presentan manipulación de datos y ejecutan procedimientos para prevenir estos riesgos informáticos?	**OBJETIVO GENERAL** Ejecutar un Ethical Hacking con Kali Linux para un Servidor con Windows 2008 Server R2 de la empresa Infonet Soluciones EIRL - Sullana. **OBJETIVOS ESPECÍFICOS** 1. Descubrir vulnerabilidades de seguridad en el sistema operativo y aplicaciones del servidor con Windows 2008 Server R2. 2. Explotar vulnerabilidades encontradas en el sistema operativo y	La propuesta de ejecutar los procedimientos de un Ethical Hacking para un Servidor Microsoft Windows Server 2008 R2, de la empresa Infonet Soluciones E.I.R.L - Sullana; permitirá que los datos almacenados se salvaguarden adecuadamente, minimizando las vulnerabilidades y riesgos informáticos.	Tipo: Cuantitativa Nivel: Descriptiva Diseño: No experimental, de corte transversal.

	aplicaciones del servidor con Windows 2008 Server R2. 3. Registrar y recomendar la eliminación de vulnerabilidades sistema operativo y aplicaciones del servidor con Windows 2008 Server R2.		

4.7 Principios éticos

Para el desarrollo de esta investigación denominada “Ethical Hacking Con Kali Linux Hacia Windows Server 2008 R2 Para La Empresa Infonet Soluciones EIRL. - Sullana; 2020.”, se ha considerado muy estrictamente el cumplimiento de los principios éticos que permitan asegurar la originalidad de toda la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas.

Por otro lado, considerando que una gran parte de la información utilizada son de carácter público, y pueden ser conocidos y empleados por diversos analistas, sin mayores restricciones, se ha incluido su contenido sin modificaciones, salvo aquellas necesarias por la aplicación de la metodología para el análisis requerido en esta investigación.

La presente investigación se está realizando acatando el código de ética versión 002, el cual tiene por finalidad establecer los principios y valores éticos, de la misma forma del reglamento de sanción por infracción al ejercicio de la investigación científica y se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

V. RESULTADOS

5.1 Resultados

5.1.1 Dimensión 01: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2.

Tabla Nro. 3: Datos guardados están seguros en el servidor

Distribución de frecuencias y respuestas relacionadas si los datos guardados están seguros en el servidor; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cree Ud. que los datos guardados de la empresa en el servidor MS Windows Server 2008 R2 están muy seguros?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 3 se puede observar que el 80% de los trabajadores encuestados expresaron que NO creen que los datos guardados en el servidor están seguros; mientras que el 20% indicaron que SI.

Tabla Nro. 4: Utilizando Windows en Servidor los datos son seguros

Distribución de frecuencias y respuestas relacionadas si utilizando MS Windows en Servidor los datos son seguros; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que utilizando el sistema operativo MS Windows para servidor de red, los datos son más seguros y disponibles con respecto a otros sistemas operativos?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 4 se puede observar que el 80% de los trabajadores encuestados expresaron que NO creen que utilizando MS Windows en el servidor los datos están seguros; mientras que el 20% indicaron que SI.

Tabla Nro. 5: Windows 2008 Server R2 es robusto, fiable y seguro

Distribución de frecuencias y respuestas relacionadas si considera la versión MS Windows 2008 Server R2, robusta, estable y fiable; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa “Infonet Soluciones E.I.R.L”, Sullana; para responder a la pregunta: ¿Cree Ud. que esta versión de MS Servidor Windows es la más robusta, segura y fiable?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 5 se puede observar que el 60% de los trabajadores encuestados expresaron que NO creen que la versión MS Windows Server 2008 R2, sea robusta, segura y fiable; mientras que el 40% indicaron que SI.

Tabla Nro. 6: Utilizan sistemas operativos de red en Windows, por su facilidad de uso y popularidad

Distribución de frecuencias y respuestas relacionadas si considera utilizan sistemas operativos de red en Windows, por su facilidad de uso y popularidad; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que se utilizan sistemas operativos de red en Windows, por su facilidad de uso y popularidad?, en la empresa Infonet Soluciones E.I.R.L-Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 6 se puede observar que el 20% de los trabajadores encuestados expresaron que NO creen que utilizan sistemas operativos de red en Windows, por su facilidad de uso y popularidad; mientras que el 80% indicaron que SI.

Tabla Nro. 7: Recomendaría MS Windows 2008 Server R2

Distribución de frecuencias y respuestas relacionadas si recomendaría el uso de MS Windows 2008 Server R2 en empresas; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Ud. Recomendaría el uso de MS Windows 2008 Server R2 en otras empresas comunes?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 7 se puede observar que el 80% de los trabajadores encuestados expresaron que NO recomendarían MS Windows 2008 Server R2 a otras empresas; mientras que el 20% indicaron que SI.

A. Resumen de la Dimensión 01

Tabla Nro. 8: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2.

Distribución de frecuencias relacionadas con la dimensión 01: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2, la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

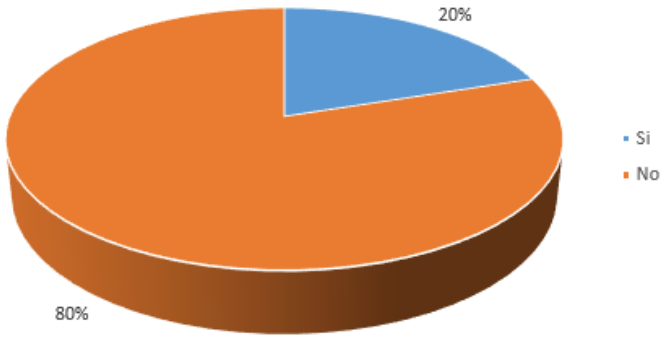
Fuente: Aplicación del instrumento para medir la Dimensión 01: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2, basado en 5 preguntas aplicadas a los trabajadores de la empresa Infonet Soluciones E.I.R.L-Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 8 se puede observar que el 80% de los trabajadores que se encuestaron expresaron que NO están seguros que los datos en el Servidor con MS Windows 2008 Server R2, que no recomendarían esa versión con otras empresas; mientras que el 20% indicaron que SI.

Gráfico Nro. 11: Resultado de la Dimensión 01 Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2.

Distribución porcentual de frecuencia y respuestas relacionadas con la dimensión 01: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2; para la Propuesta de Implementación de una Red Privada Virtual Segura Corporativa con Linux en una Plataforma Virtualizada Mixta para la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.



Fuente: Tabla N° 8

5.1.2 Dimensión 02: Nivel del servicio en red para tener datos disponibles y exactos.

Tabla Nro. 9: Existen muchos ataques para MS Windows Server 2008 R2

Distribución de frecuencias y respuestas relacionadas si piensa que existen muchos ataques para MS Windows Server 2008 R2; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que los ataques informáticos de cualquier tipo a un servidor como MS Windows Server 2008 R2, son muchos?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 9 se puede observar que el 20% de los trabajadores encuestados expresaron que NO existen muchos ataques para MS Windows Server 2008 R2; mientras que el 80% indicaron que SI.

Tabla Nro. 10: Falla del sistema operativo de un servidor, generará caos en los usuarios finales

Distribución de frecuencias y respuestas relacionadas si piensa que la caída de un sistema operativo de un servidor, generará caos en los usuarios finales; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que la caída de un servidor con el sistema operativo, logrará pérdida de datos, falta disponibilidad de los datos y mucho caos en los usuarios finales?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 10 se puede observar que el 20% de los trabajadores encuestados expresaron que NO creen que la caída de un sistema operativo de un servidor, generará caos en los usuarios finales; mientras que el 80% indicaron que SI.

Tabla Nro. 11: Datos almacenados en NTFS o FAT32, generan tranquilidad

Distribución de frecuencias y respuestas relacionadas si piensa que los datos almacenados en los sistemas de archivos NTFS o FAT32, generan tranquilidad; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud., que los datos almacenados en un sistema de archivos como NTFS o FAT32, genera tranquilidad, ya que son sistemas de archivos muy seguros?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 11 se puede observar que el 80% de los trabajadores encuestados expresaron que NO creen que los datos almacenados en los sistemas de archivos NTFS o FAT32, generan tranquilidad; mientras que el 20% indicaron que SI.

Tabla Nro. 12: MEF no debe recomendar OS Windows 2008 Server R2 para el SIAF

Distribución de frecuencias y respuestas relacionadas si piensa que el MEF no debe recomendar OS Windows 2008 Server R2 para el SIAF; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud., que los organismos gubernamentales peruanos como el MEF, son irresponsables al recomendar para el uso de su sistema SIAF el uso de OS Windows 2008 Server R2??, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 12 se puede observar que el 80% de los trabajadores encuestados expresaron que NO creen el MEF no debe recomendar OS Windows 2008 Server R2 para el SIAF; mientras que el 20% indicaron que SI.

Tabla Nro. 13: La mejor decisión es migrar hacia Windows 2019 Server para minimizar las fallas de seguridad.

Distribución de frecuencias y respuestas relacionadas si la mejor decisión es migrar hacia Windows 2019 Server para minimizar las fallas de seguridad.; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que la mejor decisión es migrar hacia Windows 2019 Server para minimizar las fallas de seguridad ?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 13 se puede observar que el 80% de los trabajadores encuestados expresaron que NO creen que la mejor decisión es migrar hacia Windows 2019 Server para minimizar las fallas de seguridad.; mientras que el 20% indicaron que SI.

B. Resumen de la Dimensión 02

Tabla Nro. 14: Dimensión Nivel del servicio en red para tener datos disponibles y exactos.

Distribución de frecuencias relacionadas con la dimensión 02: Nivel del servicio en red para tener datos disponibles y exactos, la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

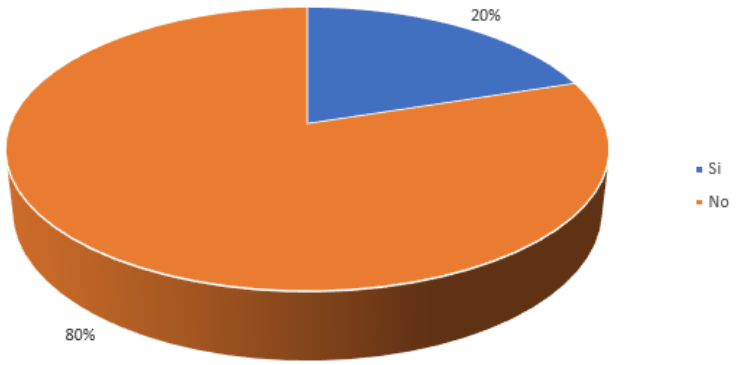
Fuente: Aplicación del instrumento para medir la Dimensión 02: Nivel del servicio en red para tener datos disponibles y exactos, basado en 5 preguntas aplicadas a los trabajadores de la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 14 se puede observar que el 80% de los trabajadores encuestados expresaron que NO hay un Nivel del servicio en red para tener datos disponibles y exactos, mientras que el 20% indico que SI.

Gráfico Nro. 12: Resultado de la Dimensión 02 Nivel del servicio en red para tener datos disponibles y exactos.

Distribución porcentual de frecuencia y respuestas relacionadas con la dimensión 02: Nivel del servicio en red para tener datos disponibles y exactos; para la Propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.



.

Fuente: Tabla N° 14

5.1.3 Dimensión 03: Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.

Tabla Nro. 15: Utilizando un sistema operativo como MS Windows 2008 Server R2, las fallas de seguridad, vulnerabilidades, bugs, etc., son mínimas o escasas.

Distribución de frecuencias y respuestas relacionadas si utilizando un sistema operativo como MS Windows 2008 Server R2, las fallas de seguridad, vulnerabilidades, bugs, etc., son mínimas o escasas.; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Piensa Ud. Qué utilizando un sistema operativo como MS Windows 2008 Server R2, las fallas de seguridad, vulnerabilidades, bugs, etc., son mínimas o escasas?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 15 se puede observar que el 80% de los trabajadores encuestados expresaron que NO creen que utilizando un sistema operativo como MS Windows 2008 Server R2, las fallas de seguridad, vulnerabilidades, bugs, etc., son mínimas o escasas.; mientras que el 20% indicaron que SI.

Tabla Nro. 16: Es necesario realizar un ethical hacking anual para descubrir las fallas de seguridad en un servidor con un sistema operativo como Windows Server 2008 R2.

Distribución de frecuencias y respuestas relacionadas si es necesario realizar un ethical hacking anual para descubrir las fallas de seguridad en un servidor con un sistema operativo como Windows Server 2008 R2; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que es necesario realizar un ethical hacking anual para descubrir las fallas de seguridad en un servidor con un sistema operativo como Windows Server 2008 R2?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 16 se puede observar que el 80% de los trabajadores encuestados expresaron que SI creen que es necesario realizar un ethical hacking anual para descubrir las fallas de seguridad en un servidor con un sistema operativo como Windows Server 2008 R2.; mientras que el 20% indicaron que NO.

Tabla Nro. 17: Al realizar un ethical hacking en un sistema operativo se descubre las fallas y los niveles de seguridad actual, es necesario realizar procedimientos, levantamiento de observaciones o solo es para informarse.

Distribución de frecuencias y respuestas relacionadas si al realizar un ethical hacking en un sistema operativo se descubre las fallas y los niveles de seguridad actual, es necesario realizar procedimientos, levantamiento de observaciones o solo es para informarse.; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree. Ud. que al realizar un ethical hacking en un sistema operativo se descubre las fallas y los niveles de seguridad actual, es necesario realizar procedimientos, levantamiento de observaciones o solo es para informarse?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 17 se puede observar que el 80% de los trabajadores encuestados expresaron que SI creen que al realizar un ethical hacking en un sistema operativo se descubre las fallas y los niveles de seguridad actual, es necesario realizar procedimientos, levantamiento de observaciones; mientras que el 20% indicaron que NO.

Tabla Nro. 18: Utilizando Kali Linux actualizado, podemos realizar unos procesos de pentesting muy profesionales y profundos.

Distribución de frecuencias y respuestas relacionadas si utilizando Kali Linux actualizado, podemos realizar unos procesos de pentesting muy profesionales y profundos.; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	8	80
No	2	20
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud. que utilizando Kali Linux actualizado, podemos realizar unos procesos de pentesting muy profesionales y profundos?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 18 se puede observar que el 80% de los trabajadores encuestados expresaron que SI creen que utilizando Kali Linux actualizado, podemos realizar unos procesos de pentesting muy profesionales y profundos.; mientras que el 20% indicaron que NO.

Tabla Nro. 19: Los servicios como AD, File Server, DNS, SIAF, SIGA, en cualquier institución están seguros, estando estos sistemas instalados en sistemas como MS Windows Server R2.

Distribución de frecuencias y respuestas relacionadas si los servicios como AD, File Server, DNS, SIAF, SIGA, en cualquier institución están seguros, estando estos sistemas instalados en sistemas como MS Windows Server R2; la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	10	100

Fuente: Origen del instrumento aplicado a los trabajadores de la empresa "Infonet Soluciones E.I.R.L", Sullana; para responder a la pregunta: ¿Cree Ud., que los servicios como AD, File Server, DNS, SIAF, SIGA, en cualquier institución están seguros, estando estos sistemas instalados en sistemas como MS Windows Server R2?, en la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 19 se puede observar que el 80% de los trabajadores encuestados expresaron que SI creen que utilizando Kali Linux actualizado, podemos realizar unos procesos de pentesting muy profesionales y profundos.; mientras que el 20% indicaron que NO.

C. Resumen de la Dimensión 03

Tabla Nro. 20: Dimensión Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.

Distribución de frecuencias relacionadas con la dimensión 03: Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables., la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Alternativas	n	%
Si	2	20
No	8	80
Total	5	100

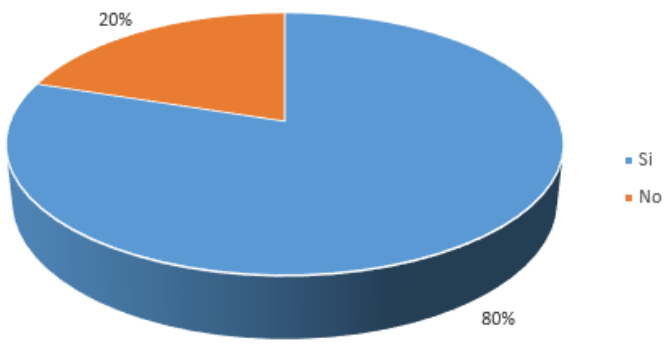
Fuente: Aplicación del instrumento para medir la Dimensión 03: Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables, basado en 5 preguntas aplicadas a los trabajadores de la empresa Infonet Soluciones E.I.R.L- Sullana; 2020.

Aplicado por: Criollo, P.; 2020.

En la Tabla Nº 20 se puede observar que el 80% de los trabajadores encuestados expresaron que SI es necesario el Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables; mientras que el 20% indicaron que NO.

Gráfico Nro. 13: Resultado de la Dimensión 03 Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.

Distribución porcentual de frecuencia y respuestas relacionadas con la dimensión 03: Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.; para la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.



Fuente: Tabla N° 20

D. Resumen de las Dimensiones

Tabla Nro. 21: Resumen de Dimensiones

Distribución de frecuencia y respuesta relacionada al resumen de las 3 dimensiones la cual son el Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2, Nivel del servicio en red para tener datos disponibles y exactos, Nivel de Seguridad de la información para tener datos completos, oportunos y fiables; para la propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Dimensiones	SI		NO		TOTAL	
	n	%	n	%	n	%
Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2.	2	20	8	80	10	100
Dimensión Nivel del servicio en red para tener datos disponibles y exactos.	2	20	8	80	10	100
Dimensión Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.	2	20	8	80	10	100

Fuente: El instrumento aplicado para el conocimiento de los trabajadores encuestados sobre las tres dimensiones definidas en la investigación; de la Empresa Infonet Soluciones E.I.R.L - Sullana; 2020.

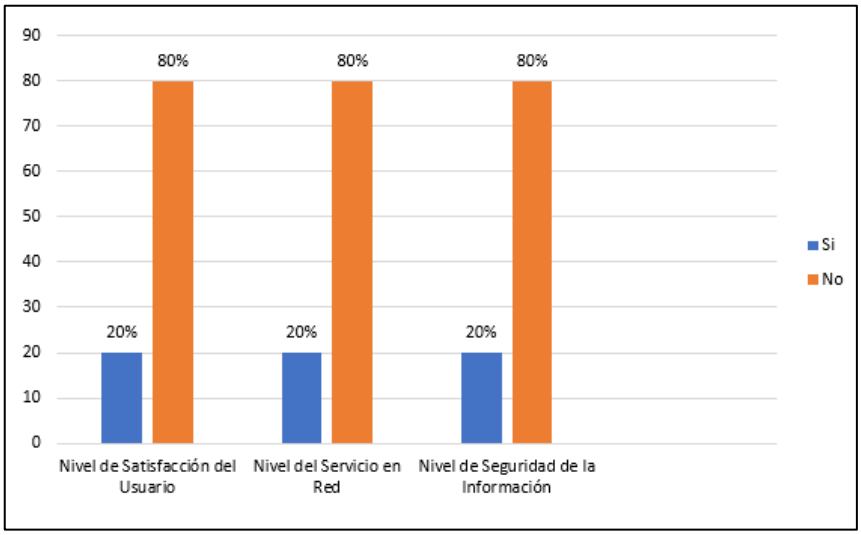
Aplicado por: Criollo, P.; 2020.

En la Tabla N° 21, en la primera dimensión se observa que el 80% de los encuestados NO están satisfechos en el uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2; mientras que el 20% indico que SI. En la segunda dimensión el 80% de los trabajadores encuestados expresaron que NO están seguros que con estos sistemas operativos exista un buen servicio de red para tener datos disponibles y exactos, mientras que el 20% indico que SI. En

la tercera dimensión el 80% de los trabajadores encuestados expresaron que NO se tiene un buen sistema de operativo con buena e Seguridad de la información para tener datos completos, oportunos y fiables; mientras que el 20% indicaron que SI.

Gráfico Nro. 14: Resumen general de dimensiones

Distribución porcentual de frecuencia y respuestas relacionadas con los resultados del resumen general de las tres dimensiones escogidas en la investigación; para la Propuesta de Ethical Hacking con Kali Linux hacia Windows Server 2008 R2 para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.



Fuente: Tabla N° 21

5.2 Análisis de resultados

El objetivo de la investigación es: Ejecutar un Ethical Hacking con Kali Linux para un Servidor con Windows 2008 Server R2 de la empresa Infonet Soluciones EIRL - Sullana; que descubra vulnerabilidades, fallas, de seguridad que tienen hoy este tipo sistema operativo y esto genere exposición de los datos privilegiados de la empresa; en este sentido para poder cumplir con este objetivo es preciso realizar una apreciación del escenario actual con el fin de que este método identifique claramente las necesidades de seguridad y se puedan dar las recomendaciones y ajustes de las aplicaciones y sistema operativo.

Por lo cual realizaremos un análisis de los resultados obtenidos de esta investigación de la siguiente manera:

1. En lo que respecta a la dimensión: Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2, en la Tabla Nº 8 se puede observar que el 80% de los trabajadores que se encuestaron expresaron que NO están seguros que los datos en el Servidor con MS Windows 2008 Server R2, que no recomendarían esa versión con otras empresas; mientras que el 20% indicaron que SI, este resultado es similar al resultado que ha obtenido Ancajima (8), en su investigación donde obtuvo como resultado en una dimensión similar a la nuestra, un resultado de 70% insatisfacción con respecto al acceso de la información. Esta similitud en los resultados se justifica porque en las empresas investigadas cada una tiene una red local aisladas de las demás, es decir cada una existía una configuración local que no necesariamente era compatible con las otras configuraciones de la empresa.
2. Con relación a la dimensión: Dimensión Nivel del servicio en red para tener datos disponibles y exactos, en la Tabla Nº 14 se puede observar que el 80% de los trabajadores encuestados expresaron que NO hay un Nivel del servicio en red para tener datos disponibles y exactos, mientras que el 20% indico que SI, este resultado no coincide con el obtenido por Ancajima (8), donde en una investigación similar obtuvo como deducción que el 73,33% de los trabajadores manifestaron que había seguridad de red en la empresa en la que laboraban.

3. Asimismo de acuerdo a los resultados obtenidos en la dimensión: Dimensión Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables, en la Tabla Nº 20 se puede observar que el 80% de los trabajadores encuestados expresaron que SI es necesario el Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables; mientras que el 20% indicaron que NO. Este resultado coincide con los resultados obtenidos por Muñoz (9), donde en su investigación indica que el 100% de los trabajadores SI están de acuerdo en el diseño e implementación de una red privada virtual, generando la urgente necesidad de un diseño y propuesta de implementación de red privada virtual la cual se ve reflejada en las respuestas de los trabajadores encuestados en busca de cumplir con los objetivos organizacionales propuesto por la empresa.

5.3 Propuesta de mejora

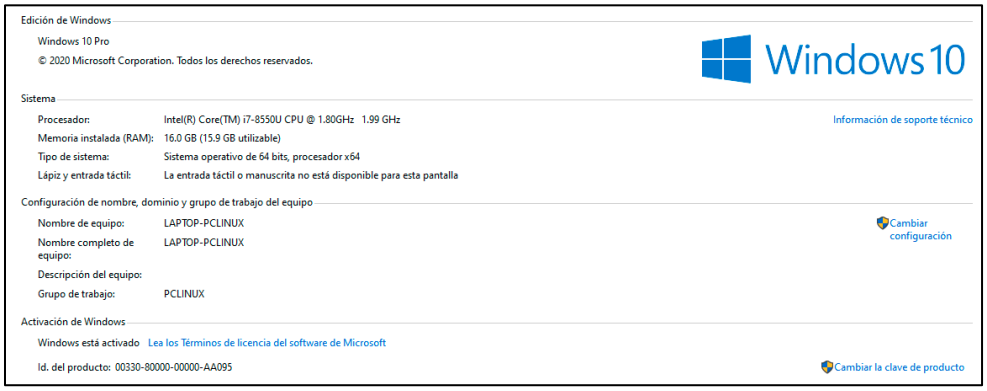
Ethical Hacking hacia un Server con MS Windows 2008 Server R2 con Kali Linux

Hardware:

Laptop HP ProBook 450 G5

- Procesador i7-8550U 1.8GHz.
- 16 Gb RAM DDR4.
- Disco M2 500Gb.
- Disco SATA 1Tb.

Gráfico Nro. 15: Especificaciones del hardware



Software:

- OS Anfitrión: MS Windows 10 Pro.
- VirtualBox 6.1
- MV: Metasploitable3 – MS Windows Server 2008 R2
- MV: Kali Linux 2020.3

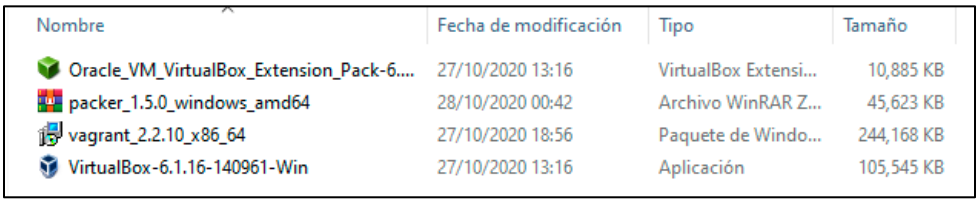
Procedimientos de Pre-requisitos:

1. **Crear la MV de MetaSploitable3**

   Software a descargar

a. **Vagrant:** https://releases.hashicorp.com/vagrant/2.2.10/vagrant_2.2.10_x86_64.msi
b. **Vagrant reload plugin** (Se instalará por comandos, después de instalar Vagrant)
c. **Packer:** https://releases.hashicorp.com/packer/1.5.0/packer_1.5.0_windows_amd64.zip
d. **Virtual Box:** https://www.virtualbox.org/wiki/Downloads

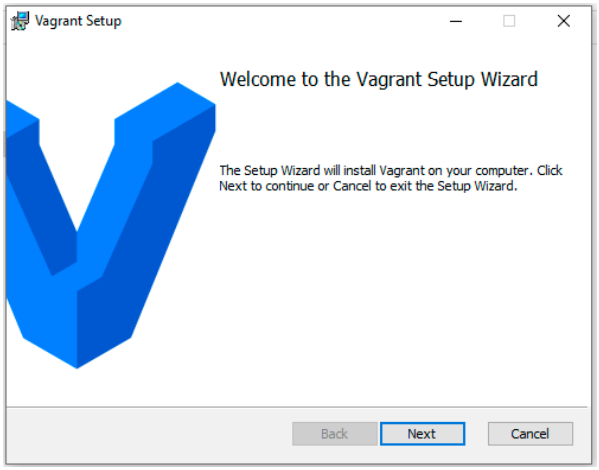
Gráfico Nro. 16: Programas a Utilizar



Instalación de software y máquinas virtuales

- Instalar Vagrant 2.2.10

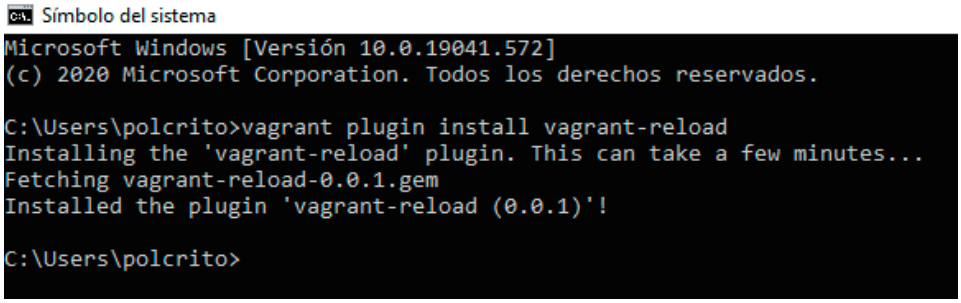
Gráfico Nro. 17: Instalación de vagrant



- Instalar plugin vagrant-reload para Windows (desde cmd)

  vagrant plugin install vagrant-reload

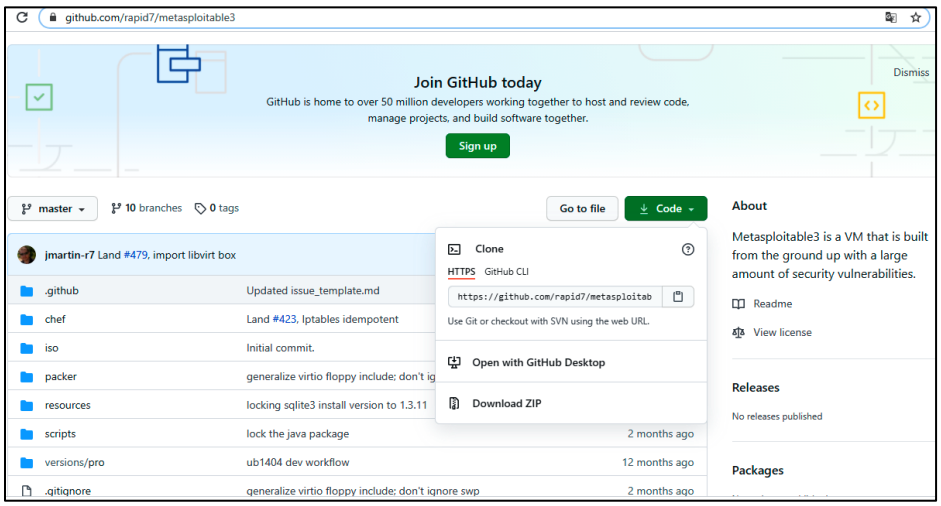
Gráfico Nro. 18: Instalación de Plugin



- Descargar Metasploitable 3 desde el repositorio de Github:

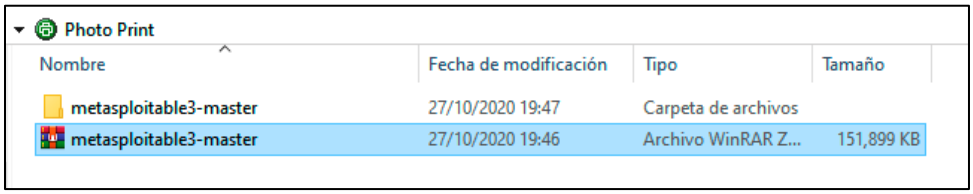
  https://github.com/rapid7/metasploitable3

Gráfico Nro. 19: Descarga de metasploitable 3



- Crear una carpeta en D, descargar el zip de metasplotable3 y descomprimimos.

Gráfico Nro. 20: Descomprimir carpeta zip



- Instalar VirtualBox-6.1.16 + Extensión

Gráfico Nro. 21: Instalación de virtual box

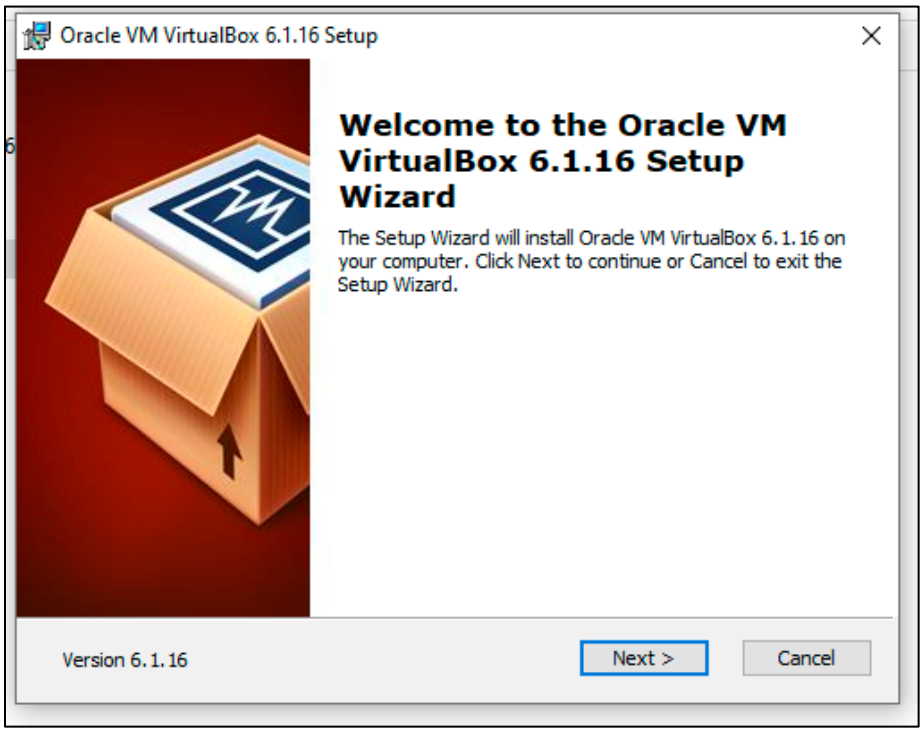


Gráfico Nro. 22: Máquina virtual

- Instalar Extensión de VirtualBox 6.1.16

Gráfico Nro. 23: Instalación de extensión de virtualbox

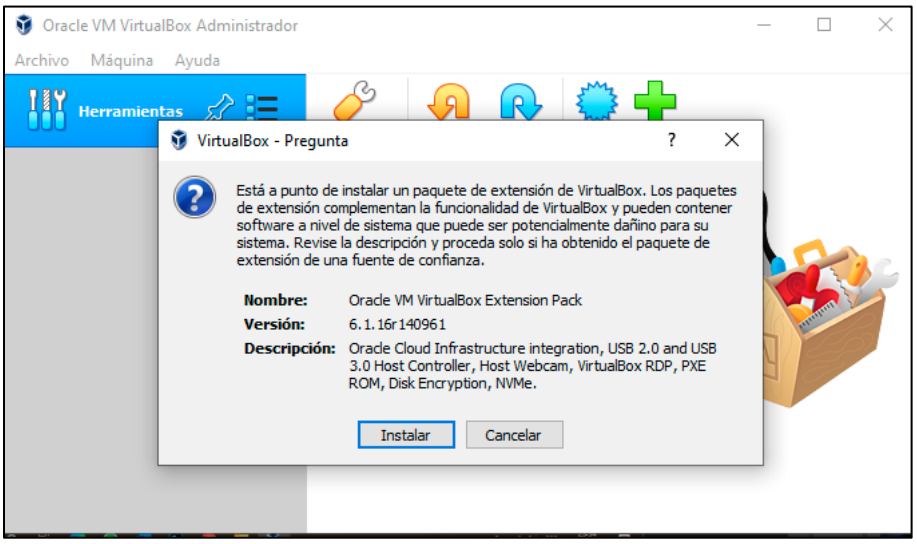
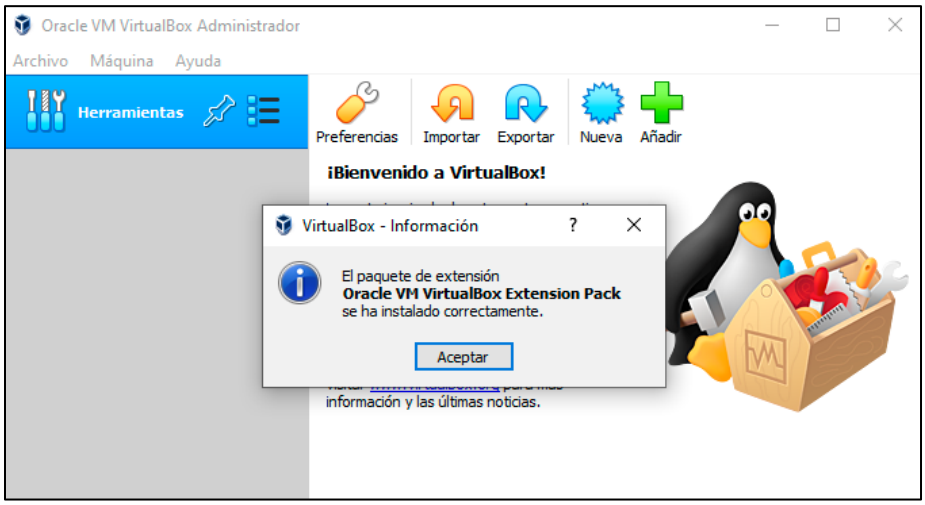
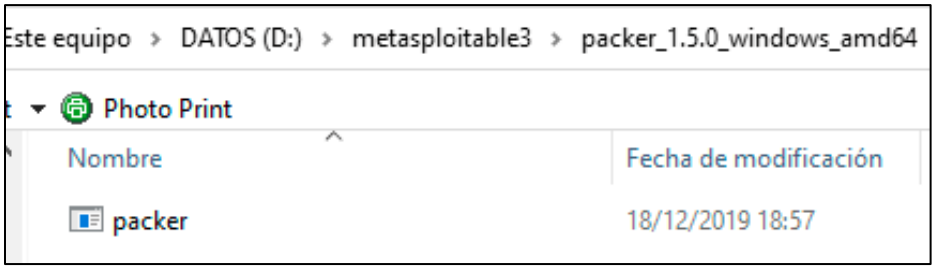


Gráfico Nro. 24: Instalación exitosa de la extensión



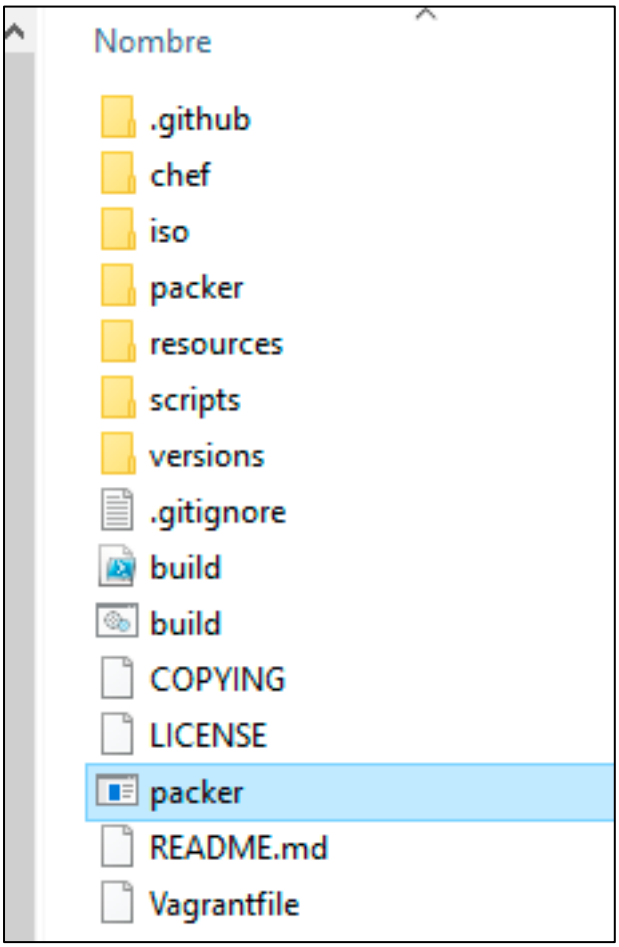
- Descomprimimos packer_1.5.0_windows_amd64.zip

Gráfico Nro. 25: Descomprimir packer_1.5.0



- Copiamos el archivo packer.exe en la carpeta meetsploitable3

Gráfico Nro. 26: Copiar archivo packer.exe en la carpeta meetsploitable3

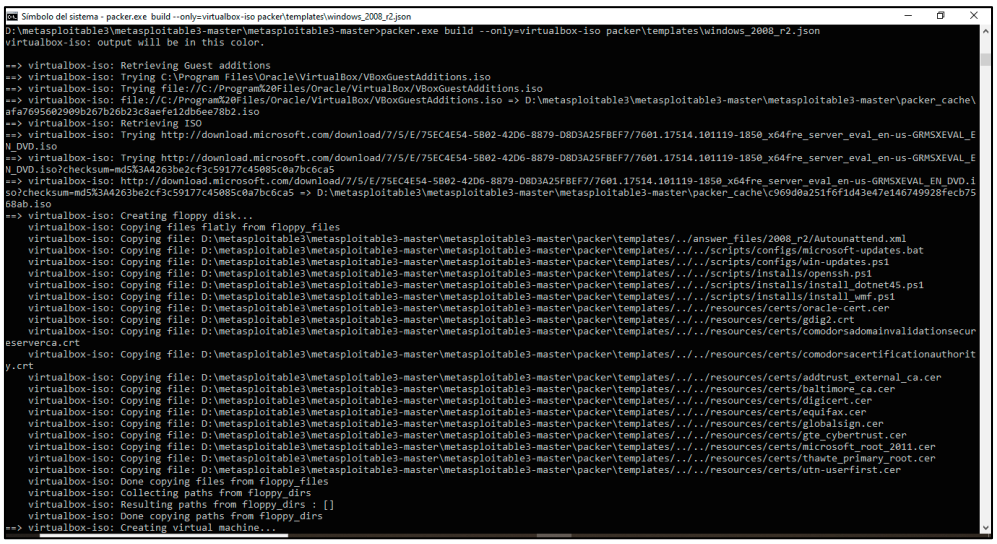


- Instalar Metasploitable 3, a través del script windows_2008_r2.json

/// DESACTIVAR WINDOWS DEFENDER Y OTROS ANTIVIRUS

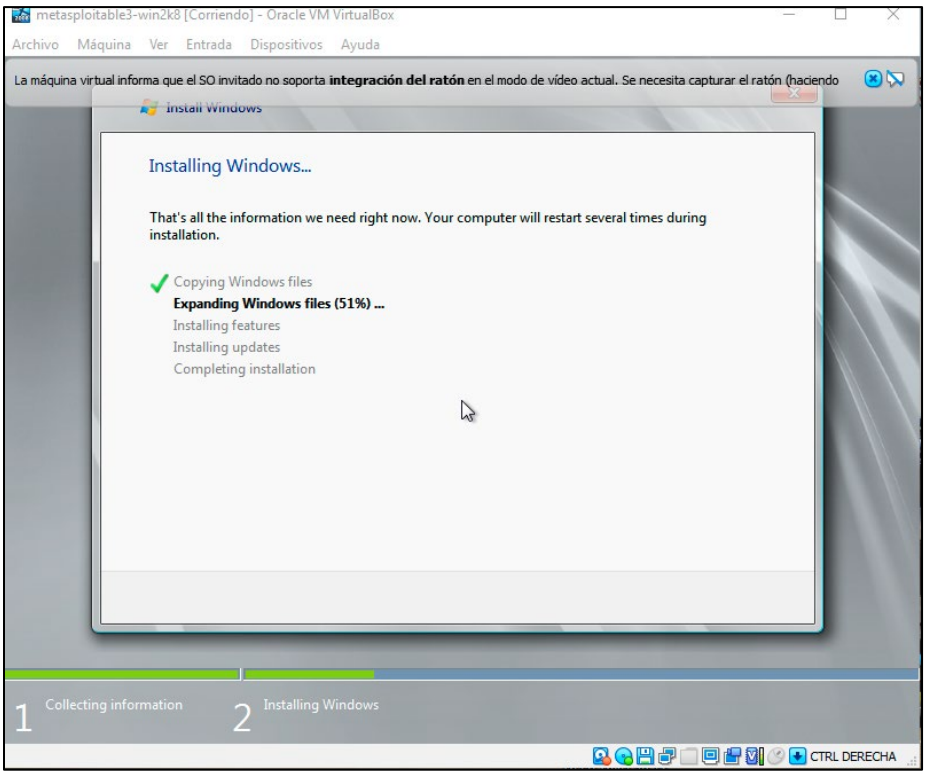
packer.exe build --only=virtualbox-iso packer\templates\windows_2008_r2.json

Gráfico Nro. 27: Desactivar Windows defender



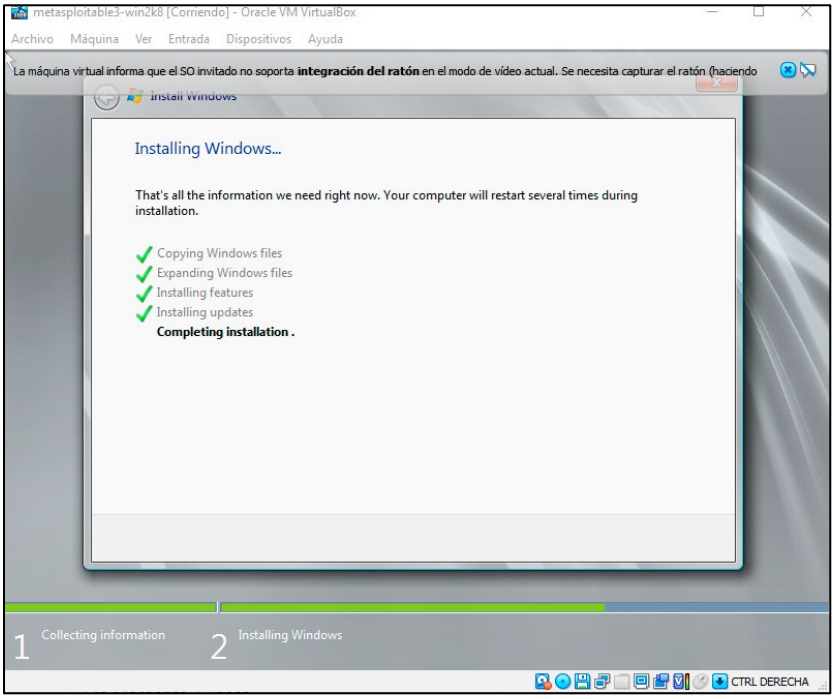
- Instalación de Windows

Gráfico Nro. 28: Instalación de Windows



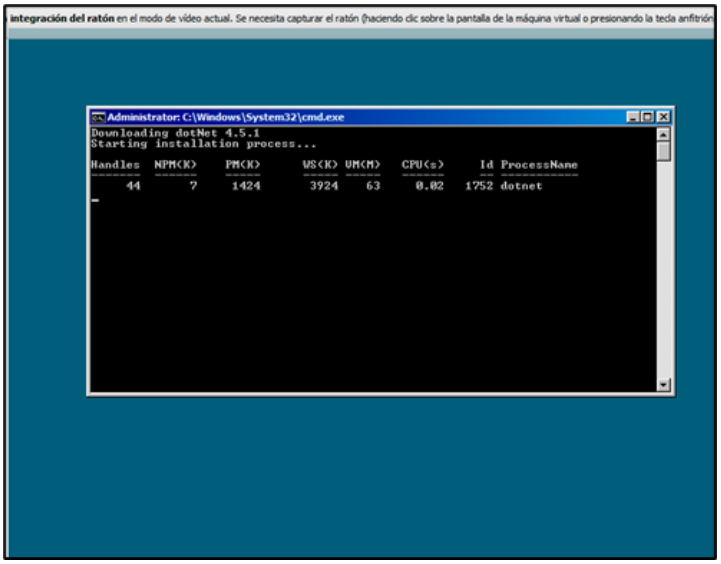
- Instalación de Windows (completado)

Gráfico Nro. 29: Instalación de Windows exitoso



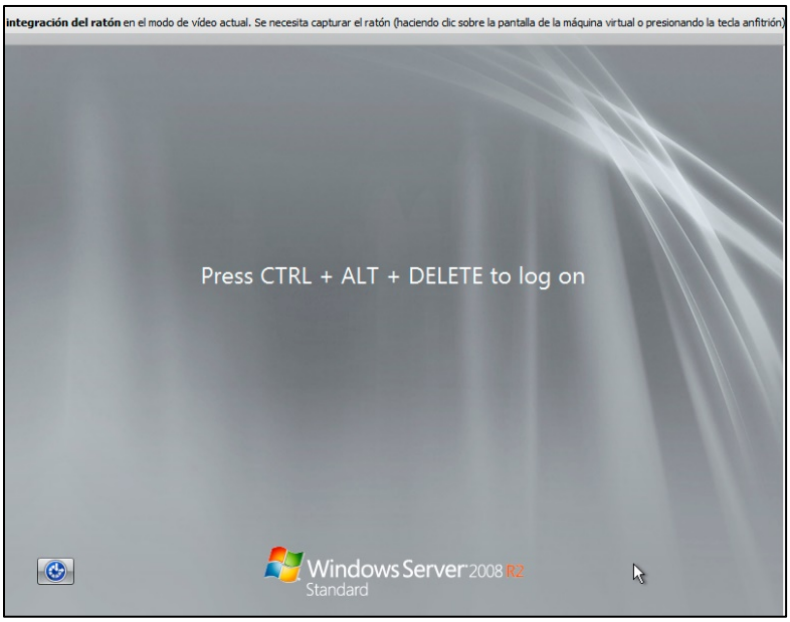
- Instalación automática de aplicaciones

Gráfico Nro. 30: Instalación Automática de aplicaciones



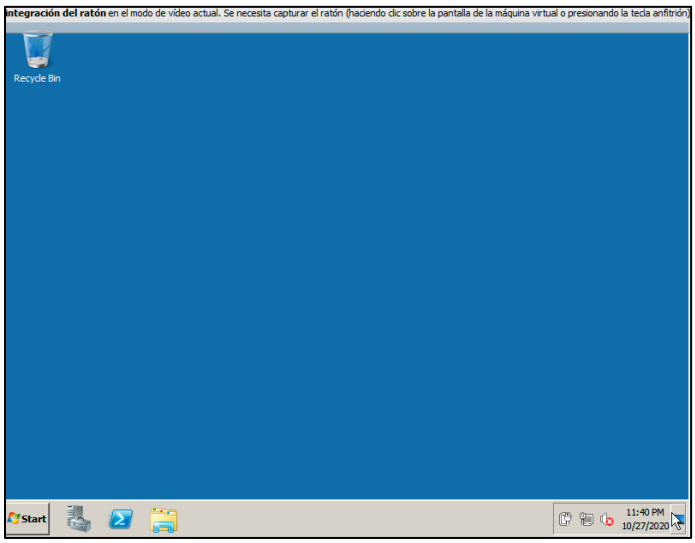
- Login de Windows 2008 Server R2

Gráfico Nro. 31: Login de Windows 2008 Server R2



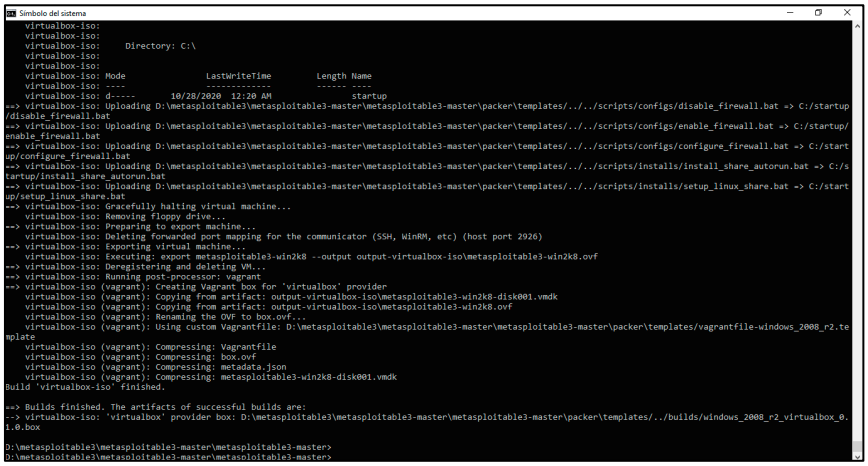
- Escritorio de Windows 2008 Server R2

Gráfico Nro. 32: Escritorio de Windows 2008 Server R2



- Avance del proceso de instalación de Metasploitable3

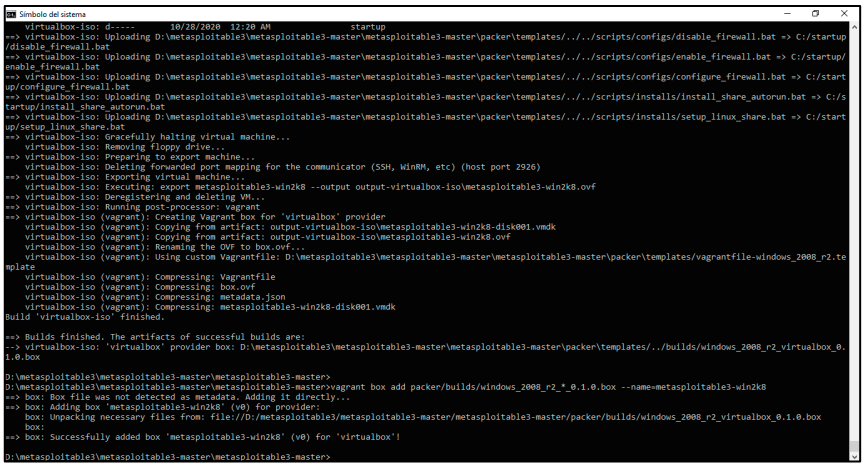
Gráfico Nro. 33: Avance del proceso de instalación de Metasploitable3



- Agregar la máquina compilada a Vagrant:

vagrant box add packer\builds\windows_2008_r2_virtualbox_0.1.0.box --name=rapid7/metasploitable3-win2k8

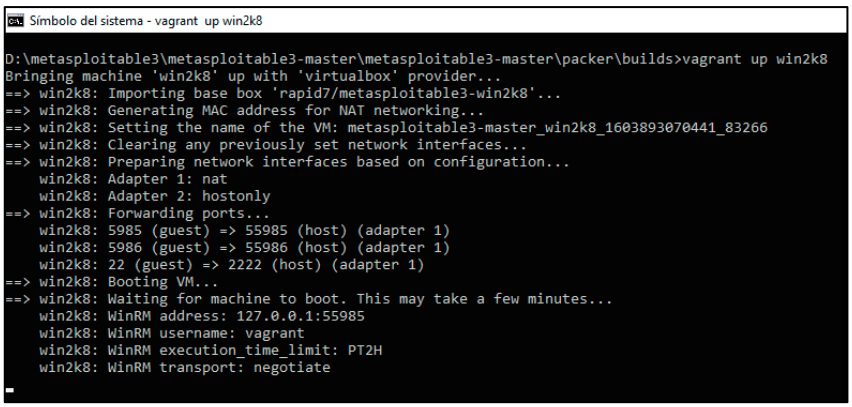
Gráfico Nro. 34: Agregar la máquina compilada a Vagrant



- Iniciar nuestra máquina virtual:

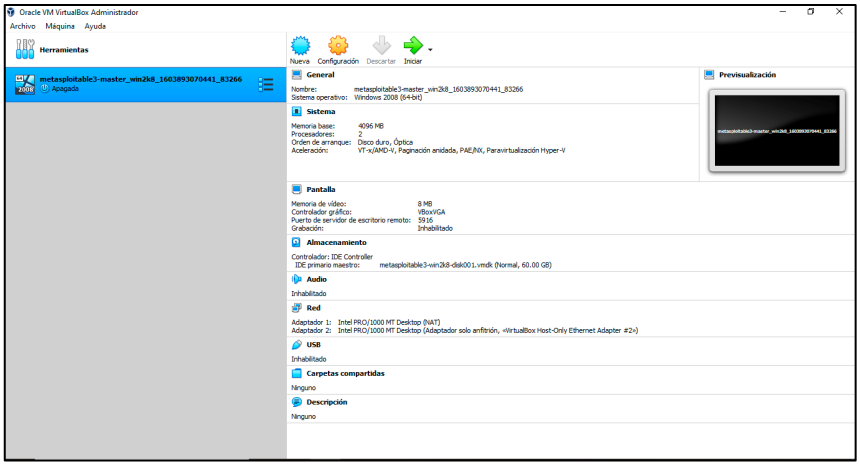
vagrant up win2k8

Gráfico Nro. 35: Iniciar nuestra máquina virtual



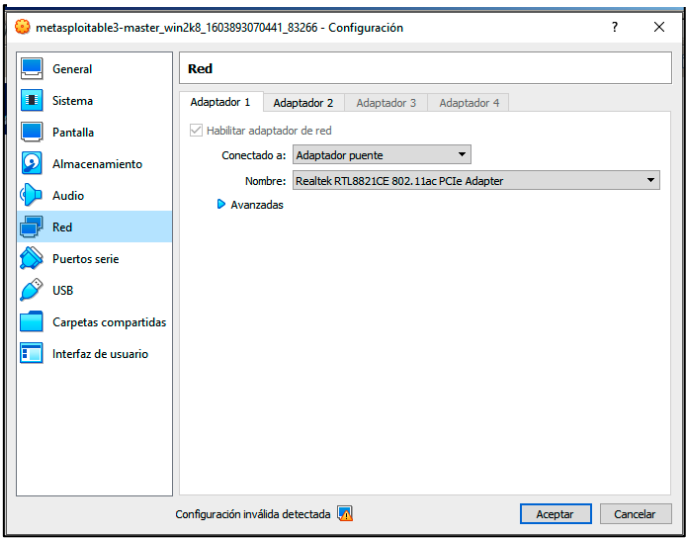
- VirtualBox – MV Metasploitable3

Gráfico Nro. 36: VirtualBox – MV Metasploitable3



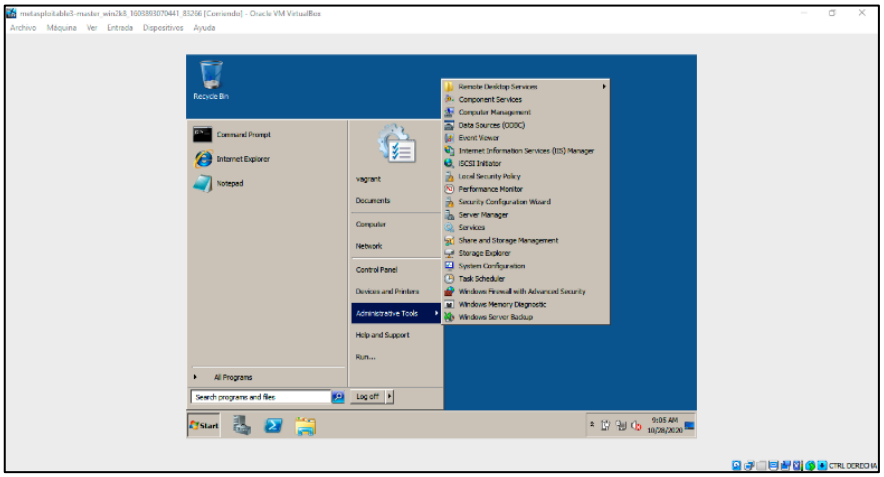
- MV Metasploitable3 – Windows 2008 Server R2

Gráfico Nro. 37: MV Metasploitable3 – Windows 2008 Server R2



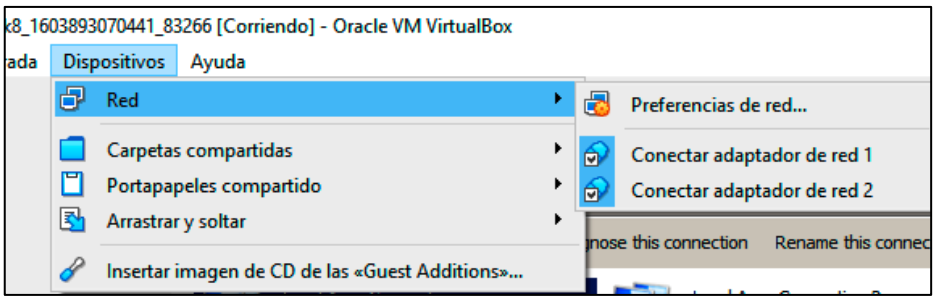
- Ingresar Preferencias de red en VirtualBox (02 tarjetas de red)

Gráfico Nro. 38: Ingresar Preferencias de red en VirtualBox



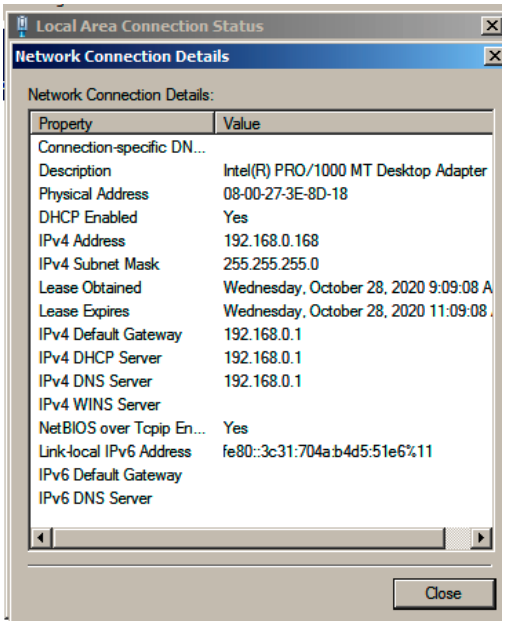
- Cambiar modo de red (Tipo Puente) en VirtualBox para cada adaptador

Gráfico Nro. 39: Cambiar modo de red



- Status de dispositivo de red principal (valores ip/mascara/gateway)

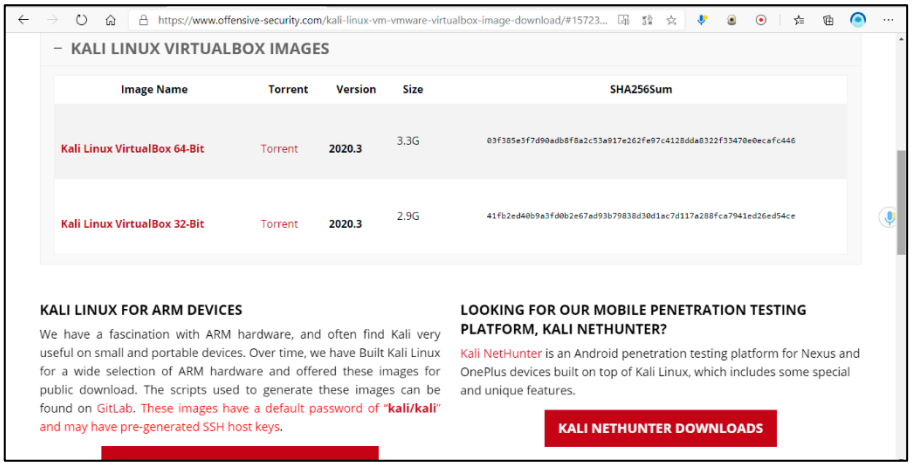
Gráfico Nro. 40: Status de dispositivo de red principal



2. Descargar la MV de Kali Linux 2020.3 en para VirtualBox

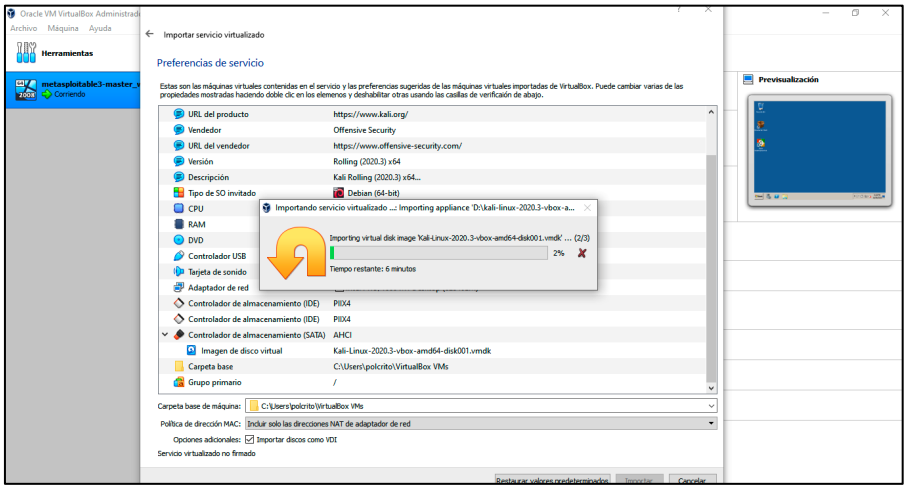
- Web de descargas Kali Linux para VirtualBox

Gráfico Nro. 41: Web de descargas Kali Linux para VirtualBox



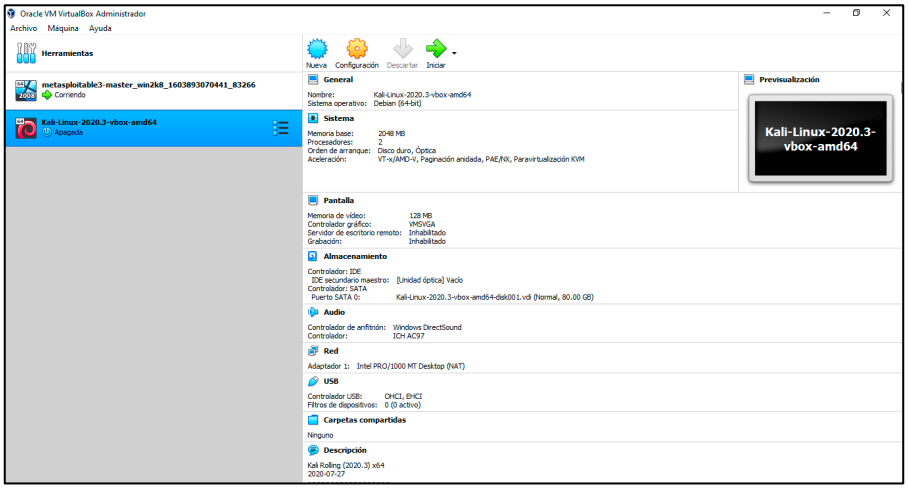
- Importar el servicio desde el archivo Ovx de KaliLinux 2020.3

Gráfico Nro. 42: Importar el servicio desde el archivo Ovx de KaliLinux 2020.3



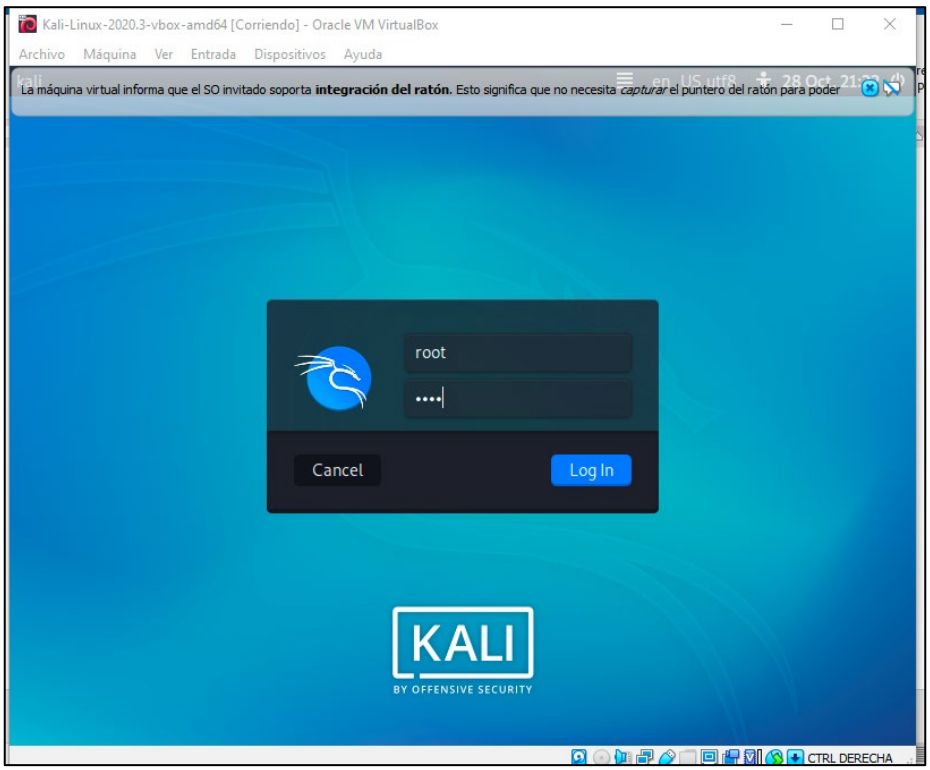
- Listado de MV de VirtualBox

Gráfico Nro. 43: Listado de MV de VirtualBox



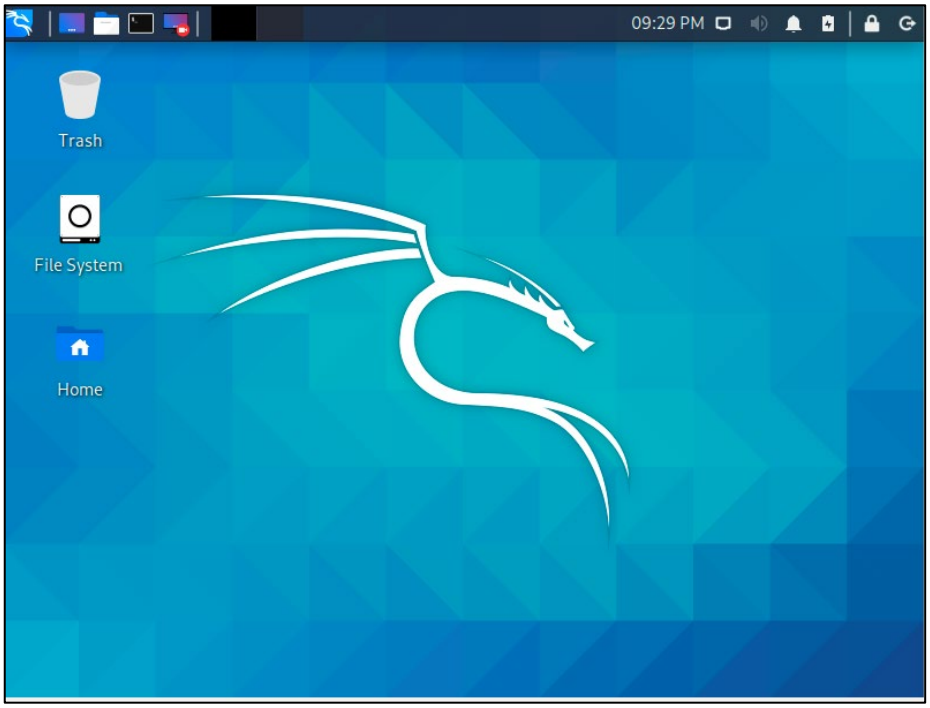
- Login de MV de KaliLinux 2020.3 en VirtualBox

Gráfico Nro. 44: Login de MV de KaliLinux 2020.3



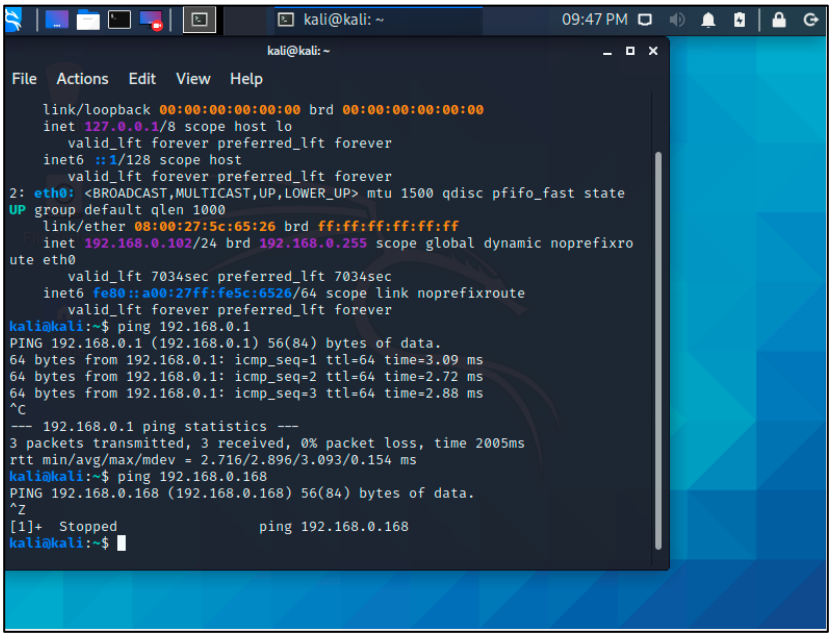
- Escritorio KaliLinux 2020.3 en VirtualBox

Gráfico Nro. 45: Escritorio KaliLinux 2020.3



- Consola de Comandos KaliLinux 2020.3:

Gráfico Nro. 46: Consola de Comandos KaliLinux 2020.3

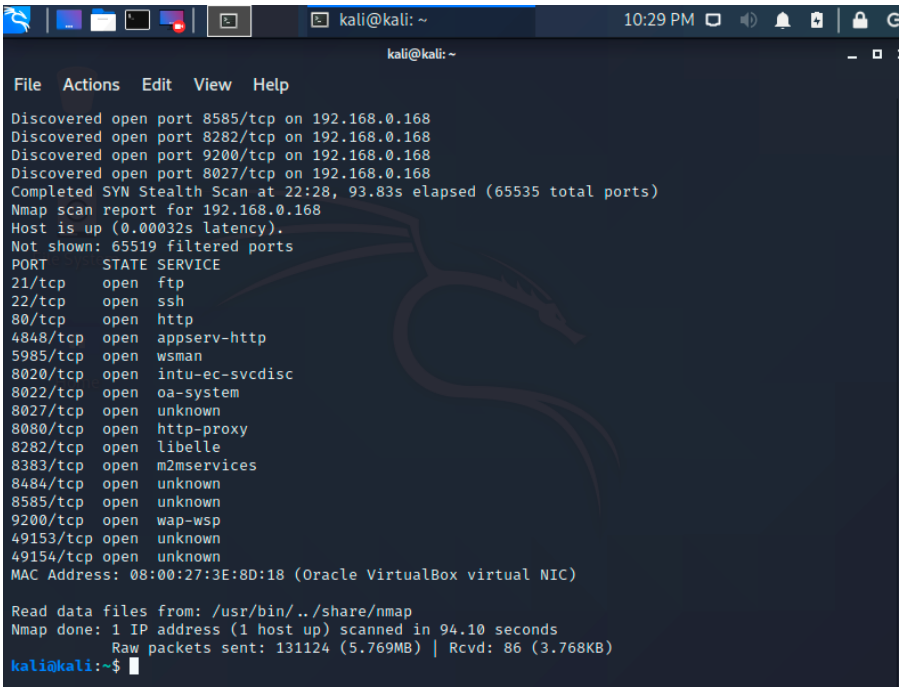


Procedimientos de Ethical Hacking

1. **Escanear con nmap desde Kali Linux la máquina victima 192.168.0.168 (Windows 2008 Server R2)**

sudo nmap -sS -p 1-65535 -T4 -v 192.168.0.168

Gráfico Nro. 47: Escanear con nmap desde Kali Linux la máquina victima



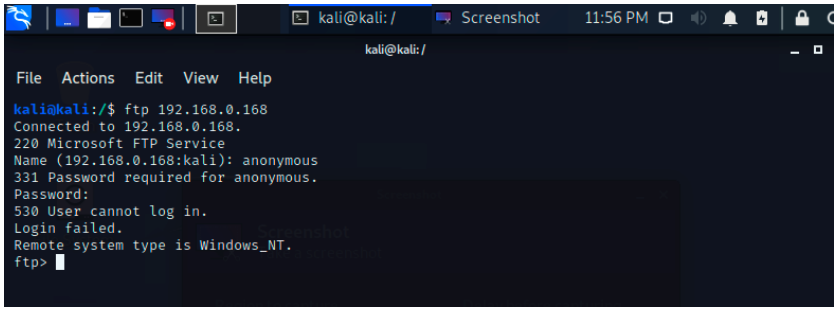
2. **Verificar la ejecución de un servidor web por el puerto 80, en equipo víctima.**

Gráfico Nro. 48: Verificar la ejecución de un servidor web por el puerto 80, en equipo víctima

3. Ataque por fuerza bruta para Servidor FTP de Microsoft en el puerto 21

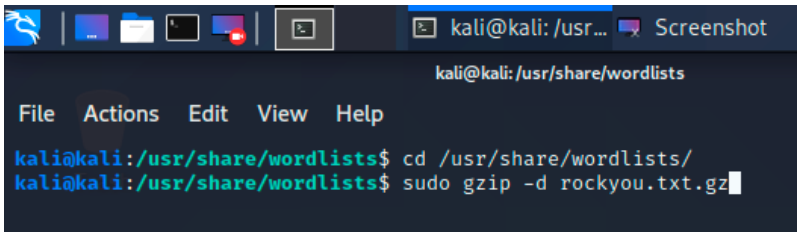
- El Microsoft FTPD está en ejecución, lograremos conexión utilizando una autenticación anónima, no logramos éxito.

Gráfico Nro. 49: Ataque por fuerza bruta para Servidor FTP



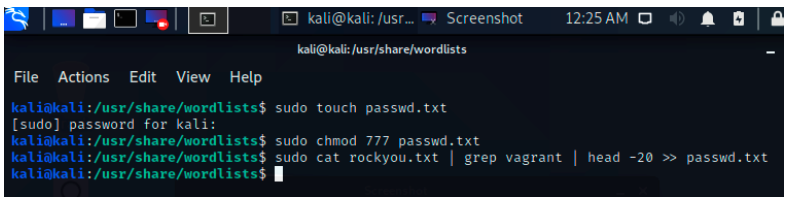
- Crear un diccionario para fuerza bruta
- Accedemos al directorio worldlists, que contiene rockyou.txt.gz
- Se descomprime el archivo del diccionario rockyou.txt .gz

Gráfico Nro. 50: Descomprimir rockyou.txt .gz



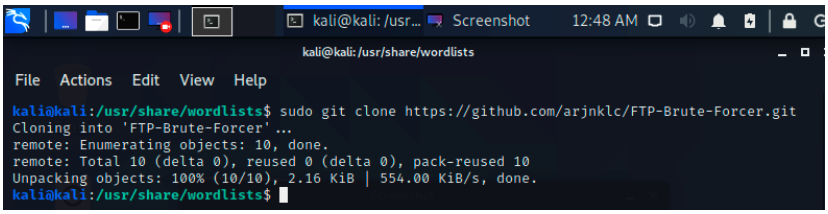
- Crear un archivo passwd.txt, este será nuevo diccionario
- Otorgar permiso 777 al archivo passwd.txt
- Crear nuevo diccionario passwd.txt, en base al rockyou.txt

Gráfico Nro. 51: Crear nuevo diccionario passwd.txt



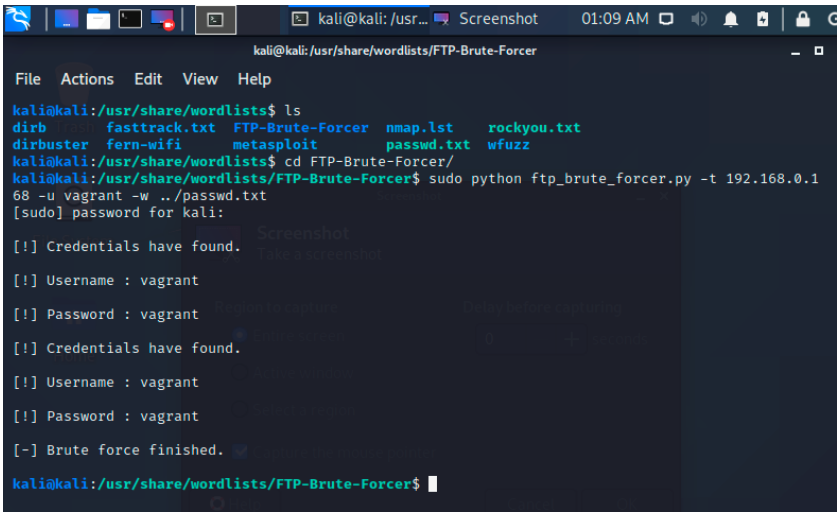
- Descargar la aplicación FTP-Brute-Forcer

Gráfico Nro. 52: Descargar la aplicación FTP-Brute-Forcer



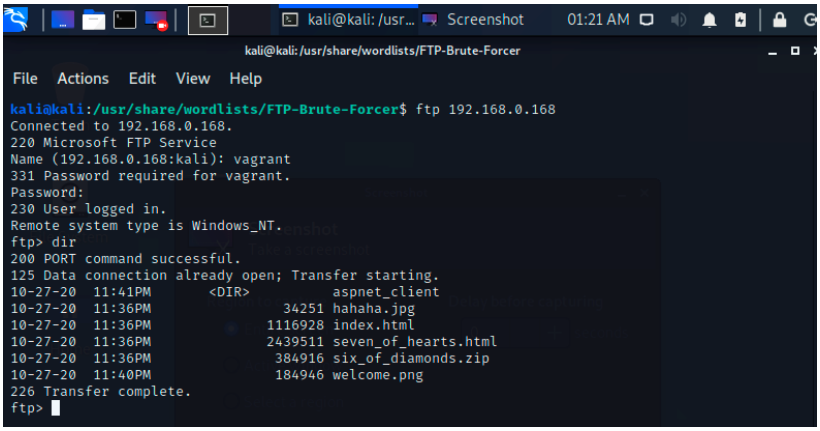
- Cambiar a directorio FTP-Brute-Forcer.
- Ejecutar programa fuerza bruta, se obtienen resultados.

Gráfico Nro. 53: Ejecutar programa fuerza bruta



- Conexión ftp, con usuario y pasword descubiertos.

Gráfico Nro. 54: Conexión ftp



VI. CONCLUSIONES

1. La mayoría de empresas peruanas, no tienen un plan de prevención de ataques
2. informáticos, realizando procesos de ethical hacking para probar sus niveles de seguridad.
3. En el año 2020, el MEF todavía sigue utilizando un sistema obsoleto como el SIAF,
4. que te obliga a usar sistemas de red Windows Server.
5. Hoy en día la versión MS Windows 2008 Server R2, es muy vulnerable.
6. La mayoría de instituciones del gobierno peruano lo siguen usando.
7. El bajo conocimiento en seguridad informática/información de los profesionales en IT en Perú es alarmante.
8. Los ataques informáticos a Windows Server 2008 R2 es muy alto.

RECOMENDACIONES

1. La Escuela Profesional de Ing. Sistemas de la Uladech, como semillero de los futuros ingenieros de sistemas del Perú, deben organizar eventos de ciberseguridad, grupos de investigación, comunidades de hacking ético, etc.
2. Los profesionales de IT peruanos deben mínimo gestionar la NTP 27001 en Seguridad de la Información en sus organizaciones, para allí gestionar los ethical hacking en sus redes.
3. En una red mínimo deben tener un Firewall, Proxy, Filtro, IDS, para prevenir ataques, si no hay para altas inversiones y colocar Palo Alto, Checkpoint,
4. Cisco, etc., pueden usar Nethserver o Pfsense

REFERENCIAS BIBLIOGRÁFICAS

1. Rendón J. , Raza J. Analisis de Vulnerabilidades en Sistemas Informáticos Web desde la Red de Internet utilizando herramientas de Hacking Etico y la Metodología Owasp.”. Tesis. Ecuador: Universidad De Guayaquil, Facultad De Ciencias Matemáticas Y Físicas Carrera De Ingeniería En Networking Y Telecomunicaciones; 2019.

2. Benítez A. “Análisis de Riesgo en Redes Wifi Aplicando Técnicas de Hacking Ético”. Tesis. Quito: Udla, Facultad De Ingeniería Y Ciencias Aplicadas; 2019.

3. Huilca G. Hacking Ético para detectar vulnerabilidades en los Servicios de la Intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos”. Tesis. Ambato - Ecuador: Universidad Técnica De Ambato, Facultad De Ingeniería En Sistemas Electrónica E Industrial - Carrera De Ingeniería En Sistemas Computacionales; 2012.

4. Bernal Yong Y. “Modelo de Niveles de Seguridad para Pruebas de Intrusión en Aplicaciones Web para Pymes en el Perú”. Tesis. Lima: Universidad Peruana De Ciencias Aplicadas, Facultad De Ingeniería - Programa Académico De Ingeniería De Sistemas De Información; 2019.

5. Guillinta Chavez , Merino Rivera. “Modelo de Prevención y Defensa contra Ataques Cibernéticos Basado en Estándares de Seguridad Internacionales para It-Expert”. Tesis. Lima: Universidad Peruana de Ciencias Aplicadas, Facultad de Ingeniería - Escuela de Ingeniería de Sistemas y Computación - ; 2016.

6. Cruz Saavedra. “Aplicación de Auditoría Penetration Testing para contribuir con la Seguridad de la Información en los Sistemas Informáticos de la Empresa Data Business SAC, Trujillo”. Tesis. Trujillo: Universidad Privada Del Norte, Facultad De Ingeniería - Carrera De Ingeniería En Sistemas

Computacionales; 2014.

7. López Torres Herrera R. “Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú”. Tesis. Piura: UNIVERSIDAD DE PIURA, FACULTAD DE INGENIERÍA; 2019.

8. Ancajima Mendoza A. “Propuesta de Implementación de Seguridad Informática en las TIC de la I.E. San Miguel Arcángel, Catacaos - Piura; 2016.”. Tesis. Piura: Uladech, Facultad De Ingeniería - Escuela Profesional De Ingeniería De Sistemas; 2019.

9. Sandoval Quino JP. “Diseño de un Plan de Seguridad de la Informacion para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, período 2015-2018”. Tesis. Piura: Universidad Nacional De Piura, Facultad De Ingenieria Industrial - Escuela Profesional De Ingenieria Informática; 2017.

10. Lopéz RA. Sistema de Gestión de la Seguridad Informática. Primera Edición Bogotá: Fundación Universitaria del Área Andina; 2017.

11. Romero Castro MI, Figueroa Morán GL, Vera Navarrete DS, Álava Cruzatty JE, Parrales Anzúles GR, Álava Mero CJ, et al. Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades. 2018th ed. Alicante: Editorial Área de Innovación y Desarrollo,S.L.; 2018.

12. ProdwareBlog. 4 retos inaplazables de la seguridad informática. [Online].; 2016. Available from: https://blog.prodware.es/4-retos-inaplazables-de-la-seguridad-informatica/#.X5TJyEeg_IU.

13. LIMA MOD. La Ciberseguridad en el 2019. Cuadernos de Seguridad. 2019 Octubre;(347).

14. Eric C. Ransomware Facts, Trends & Statistics for 2020. [Online].; 2020. Available from: https://www.safetydetectives.com/blog/ransomware-

statistics/.

15. Marina Pasquali. [Online].; 2020. Available from: https://es.statista.com/grafico/20748/ataques-de-malware-en-latinoamerica/.

16. Huidobro CB. LA DIMENSIÓN DEL CIBERESPACIO: UNA PROPUESTA DE CIBERSEGURIDAD. CUADERNO DE TRABAJO N°1-2019. 2019 Enero;(01).

17. Pacheco SS. Fortinet Secure Access ofrece seguridad y conectividad para proteger las redes inalámbricas empresariales. [Online].; 2018. Available from: https://revistaitnow.com/fortinet-secure-access-ofrece-seguridad-y-conectividad-para-proteger-las-redes-inalambricas-empresariales/.

18. B. KA. HACKING ÉTICO 101 Cómo hackear profesionalmente en 21 días o menos! Primera Edición ed. http://www.SeguridadInformaticaFacil.com , editor.: http://www.SeguridadInformaticaFacil.com; 2013.

19. Orcero DS. Pentesting con Kali. 2017120198th ed. Coronado E, editor. España: Ed. Coronado — Impreso por Amazon; 2019.

20. ESIC Business & Marketing School. ¿Por qué el hacking ético es un recurso esencial para una pyme? [Online].; 2017. Available from: https://www.esic.edu/rethink/tecnologia/hacking-etico-recurso-esencial-una-pyme.

21. IBM. Estrategias para la gestión de riesgos en seguridad cibernética. 2020th ed. Corporation I, editor. NY - Estados Unidos de América: IBM Security; 2020.

22. IT O. CIBERSEGURIDAD Penetration Test (PENTEST). [Online].; 2020. Available from: https://www.openit.com.ar/ciberseguridad/penetration-test-pentest/.

23. Maldonado D. ¿Qué es un exploits? [Online].; 2020 [cited 2020 Octubre 10. Available from: https://danielmaldonado.com.ar/diccionario-de-hacking/que-

es-un-exploits/.

24. Guayoyo. Conceptos básicos de Seguridad Informática que debes conocer: exploits. [Online].; 2017. Available from: https://medium.com/guayoyo/conceptos-b%C3%A1sicos-de-seguridad-inform%C3%A1tica-que-debes-conocer-exploits-6a5caa387397.

25. Quezada AEC. Hacking con Kali Linux - Una Perspectiva Práctica. 29th ed. www.ReYDeS.com , editor. Trujillo: www.ReYDeS.com; 2019.

26. Offensive Security. Kali. Kali Linux 2020.3 Release (ZSH, Win-Kex, HiDPI & Bluetooth Arsenal). [Online].; 2020. Available from: https://www.kali.org/news/kali-2020-3-release/.

27. Fernández P. y Díaz P. Investigación Cuantitativa. Primera ed.; 2015.

28. Toscano F. Metodologia de la Investigacion. Primera ed.; 2014.

29. Sabino. La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta. Primera ed.; 2015.

30. Shadish W CTCD. Tipo de Estudio y diseño. Primera ed.; 2014.

31. Seehorn A. Métodos de investigación de corte transversal. Primera ed.; 2014.

32. P. J. Tesis de Investigación. [Online].; 2015 [cited 2018 Noviembre 09. Available from: http://tesisdeinvestig.blogspot.com/2013/06/poblacionmuestraejemplo.html.

33. D D. Diseño y elaboración de cuestionarios para la investigación comercial. Primera ed. España; 2014.

34. Casas J. la encuesta como técnica de investigación. [Online].; 2015 [cited 2018 Noviembre 09. Available from: http://external.doyma.es/pdf/27/27v31n08a13047738pdf001.pdf.

35. Wikipedia. Penetration Testing. [Online].; 2018. Available from: https://es.wikipedia.org/wiki/Examen_de_penetraci%C3%B3n.

36. Schneier B. CiberGuerra. [Online].; 2018. Available from: https://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica.

37. Mendoza M. Ciberseguridad. [Online].; 2015. Available from: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/.

38. CERTUnam. Ethical Hacking. [Online].; 2011. Available from: https://www.cert.org.mx/historico/documento/index.html-id=7.

39. EcuRed. Ataque Informático. [Online].; 2018. Available from: https://www.ecured.cu/Ataque_inform%C3%A1tico.

40. Muñoz Villanueva A, Sánchez Méndez. "Modelo Referencial de Aprendizaje para la Implementación de Hacking Ético". Tesis. BOGOTÁ D.C: UNIVERSIDAD LIBRE DE COLOMBIA, FACULTAD DE INGENIERÍA - PROGRAMA DE INGENIERÍA DE SISTEMAS; 2015.

41. INCIBE INDC. PROTECCIÓN DE LA INFORMACIÓN España MdAEyTD, editor. Madrid: COLECCIÓN - PROTEGE TU EMPRESA; 2019.

42. Baca Urbina. Introducción a la Seguridad Informática. PRIMERA EDICIÓN EBOOK ed. México D. F.: GRUPO EDITORIAL PATRIA; 2016.

43. Teléfonica F. Ciberseguridad, la protección de la información en un mundo digital. 2016th ed. Madrid - España: Editorial Ariel, S.A., 2016; 2016.

44. Estrada AC. “Ciberseguridad” (Una Estrategia Informático/Militar). Primera Edición ed. Madrid - España: DarFe Learning Consulting S.L; 2017.

45. Parrales WMA, Tania Cecibel Cañarte Rodríguez , María Elena Villamarin Cevallos , Henry Luis Mezones Santana , Ángel Rolando Delgado Pilozo ,

Franklin Jhimmy Toala Arias , et al. La Ciberseguridad Práctica Aplicada A Las Redes, Servidores Y Navegadores Web. Primera Edición ed. Alicante - España: Editorial Área de Innovación y Desarrollo,S.L.; 2019.

46. Tori C. Hacking Etico. Primera Edición ed. Tori CS, editor. Rosario - Argentina; 2008.

47. PROSIC UdCR. Ciberseguridad en Costa Rica. Primer Edición ed. PROSIC , editor. San José - Costa Rica: PROSIC; 2010.

48. Vega E. Planificación Y Ejecución De Evaluaciones De Seguridad Nformática Desde Un Enfoque De Ethical Hacking. Primera Edición ed. Alicante - España: 3Ciencias - Editorial Área de Innovación y Desarrollo,S.L.; 2020.

49. UniversalBlog. Hacking con kali linux. [Online].; 2018 [cited 2020 Octubre 20. Available from: https://hackingkalinux.com/.

50. Matthews M. Microsoft Windows Server 2008 Guia Del Administrador México: Mc Graw Hill; 2009.

51. J C. Universidad Nacional Autónoma de México. [Online].; 2014 [Cited 2018 Noviembre 09. Available From: www.ingenieria.unam.mx/industriales/descargas/documentos/catedra/apuntesdsp.doc.

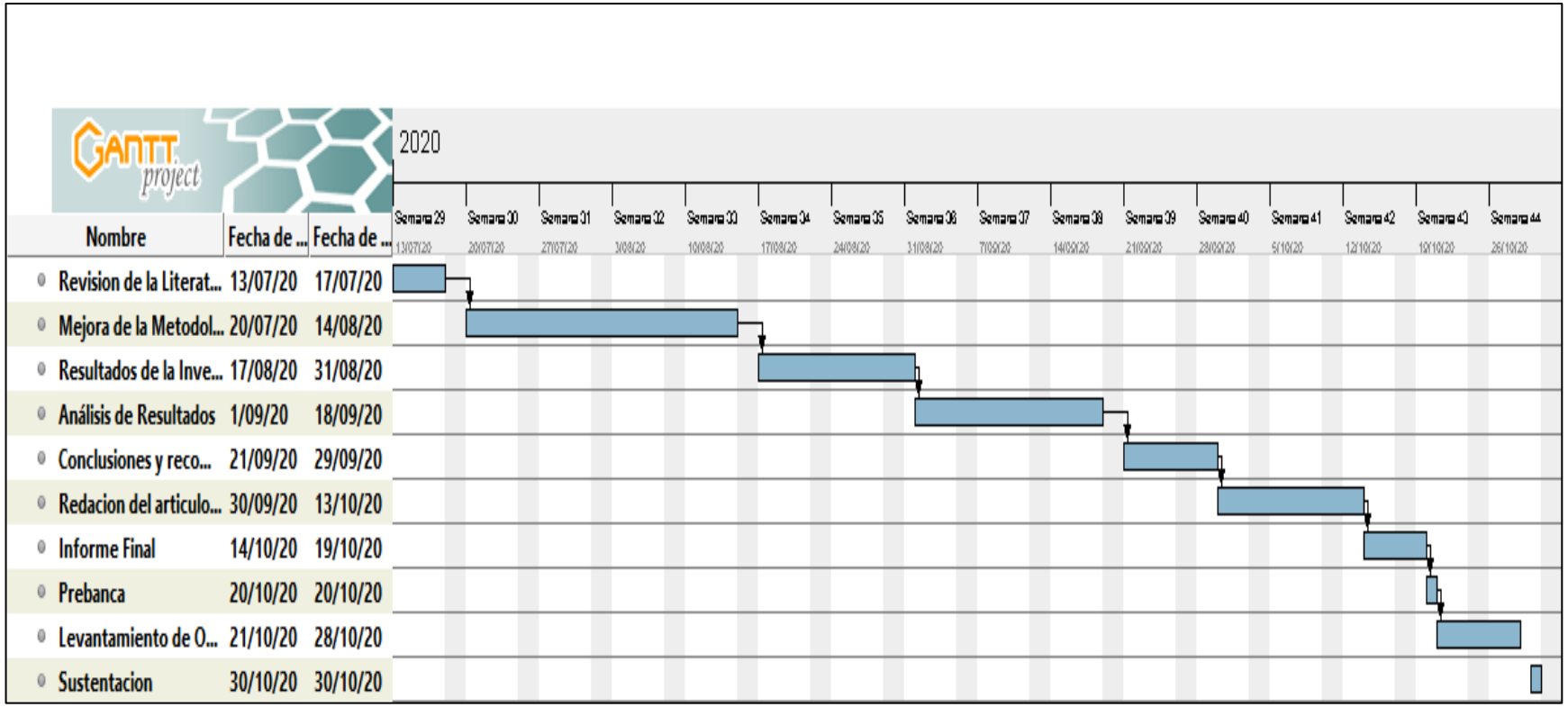
52. Margaret R. Techtarget. [Online].; 2016 [Cited 2018 Noviembre 09. Available From: http://searchenterprisewan.techtarget.com/definition/virtual-private-network.

53. Zavala F. Reingeniería De La Infraestructura De La Red De Datos Administrada Con Windows Server En Consorcio Supervisor Educa. Tesis. Piura: Universidad Católica Los Ángeles De Chimbote, Departamento De Ingeniería; 2020.

54. Castillo J.S. Propuesta De Reingeniería De Una Red De Datos Para La Municipalidad Distrital De Salitral. Tesis. Morropón : Universidad Católica Los Ángeles De Chimbote, Facultad De Ingeniería; 2018.

ANEXOS

ANEXO I: Cronograma de actividades



Fuente: Elaboración propia

ANEXO II: Presupuesto

Presupuesto desembolsable (Estudiante)			
Categoría	**Base**	**Costo Unitario**	**Total (S/.)**
Suministros			
• Impresiones	0.15	180	27.00
• Fotocopias	0.10	80	8.00
• Empastado	30	2	60.00
• Agenda	15	1	15.00
• Lapiceros	3	4	12.00
• HD USB	1	200	200.00
Servicios			
• Uso de Turnitin	100	1	100.00
• Uso de Internet	50	4	200.00
Gastos de Viaje			
• Pasajes Interprovinciales	40	4	160.00
• Pasajes Locales	5	8	40.00
Total de Presupuesto Desembolsable			822.00
Presupuesto no desembolsable (Universidad)			
Categoría	**Base**	**Costo Unitario**	**Total (S/.)**
Servicios			
Uso de Internet Laboratorio de Aprendizaje Digital - LAD	30	4	120.00
Búsqueda de información en base de datos	35	2	70.00
Soporte informático (Modulo de Investigación del ERP University - MOIC)	40	4	160.00
Publicación de articulo en repositorio institucional	50	1	50.00
Recurso Humano			
Asesoría Personalizada (5 horas por semana)	63	16	1,008.00
Total de Presupuesto No Desembolsable			1408.00
Total (S/.)			2230.00

Fuente: Elaboración Propia.

ANEXO III: CUESTIONARIO

El presente cuestionario forma de la investigación, Ethical Hacking con Kali Linux hacia MS Windows Server 2008 R2, para la Empresa Infonet Soluciones EIRL. - Sullana; 2020.

Por lo que solicitamos su participación, respondiendo cada pregunta de manera objetiva y veraz, la información a proporcionar es de carácter confidencial, los resultados serán utilizados sólo para la presente investigación.

Instrucciones:

A continuación, se le presenta 15 preguntas en 3 diferentes dimensiones en la que deberán contestar, marcando con un aspa "X" en el recuadro correspondiente (Si o No) según considere la alternativa correcta.

ÍTEM	PREGUNTAS	ALTERNATIVA	
		SI	NO
Dimensión 01: **Nivel de satisfacción del usuario con respecto al uso de sistemas y aplicaciones seguras con MS Windows Server 2008 R2.**			
1	¿Cree Ud. que los datos guardados de la empresa en el servidor MS Windows Server 2008 R2 estan muy seguros?		
2	¿Cree Ud. que utilizando el sistema operativo MS Windows para servidor de red, los datos son mas seguros y disponibles con respecto a otros sistemas operativos?		
3	¿Cree Ud. que esta versión de MS Servidor Windows es la mas robusta, segura y fiables?		
4	¿Cree Ud. que se utilizan sistemas operativos de red en Windows, por su facilidad de uso y popularidad?		
5	¿Ud. Recomendaría el uso de MS Windows 2008 Server R2 en otras emprsas comunes?		

Dimensión 02: **Nivel del servicio en red para tener datos disponibles y exactos.**			
6	¿Cree Ud. que los ataques informáticos de cualquier tipo a un servidor como MS Winows Srver 2008 R2, son muchos?		
7	¿Cree Ud. que la caída de un servidor con el sistema operativo, logrará pérdida de datos, falta disponibilidad de los datos y mucho caos en los usuarios finales?		
8	¿Cree Ud. que los datos almacenados en un sistema de archivos como NTFS o FAT32, genera tranquilidad, ya que son sistemas de archivos muy segurios?		
9	¿Cree Ud., que los organismos gubernamentales peruanos como el MEF, son irresponsables al recomendar para el uso de su sistema SIAF el uso de OS Windows 2008 Server R2??		
10	¿Cree Ud. que la mejor decisión es migrar hacia Windows 2019 Server para minimizar las fallas de seguridad ?.		

Dimensión 03: Nivel de Seguridad de la información, para tener datos completos, oportunos y fiables.			
11	¿Piensa Ud. Qué utilizando un sistema operativo como MS Windows 2008 Server R2, las fallas de seguridad, vulnerabilidades, bugs, etc, son mínimas o escasas?		
12	¿Cree ud. que es necesario realizar un ethical hacking anual para descubrir las fallas de seguridad en un servidor con un sistema operativo como Windows Server 2008 R2?		
13	¿Creee. Ud. que al realizar un ethical hacking en un sistema operativo se descubre las fallas y los niveles de seguridad		

	actual, es necesario realizar procedimientos, levantamiento de observaciones o solo es para informarse?		
14	¿Cree Ud. que utilizando Kali Linux actualizado. podemos realizar unos procesos de pentesting muy profesionales y profundos?		
15	¿Cree Ud, que los servicios como AD, File Server, DNS, SiAF, SIGA, en cualquier institución están seguros, estando estos sistemas instalados en sistemas como MS Windows Server R2?		

Fuente: Elaboración propia

ANEXO IV: PROTOCOLO DE CONSENTIMIENTO INFORMADO

UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS
(Ingeniería y Tecnología)

La finalidad de este protocolo en Ingeniería y tecnología es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador y usted se quedarán con una copia.

La presente investigación se titula **ETHICAL HACKING CON KALI LINUX HACIA WINDOWS SERVER 2008 R2 PARA LA EMPRESA INFONET SOLUCIONES EIRL. - SULLANA; 2020** y es dirigido por Paul Criollo Ortiz, investigador de la Universidad Católica Los Ángeles de Chimbote.

El propósito de la investigación es: **Realizar un Ethical Hacking a un Servidor de Windows 2008 Server R2 con Kali Linux 2020.3.**

Para ello, se le invita a participar en una encuesta que le tomará 02 minutos de su tiempo. Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través de su **correo electrónico**. Si desea, también podrá escribir al correo polcrito@hotmail.com para recibir mayor información. Asimismo, para consultas sobre aspectos éticos, puede comunicarse con el Comité de Ética de la Investigación de la universidad Católica los Ángeles de Chimbote.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: CARMEN AMELI ORTIZ MAZ

Fecha: 30 SEPTIEMBRE DEL 2020

Correo electrónico: cursos@infonetperu.com

Firma del participante:

INFONET SOLUCIONES E.I.R.L. TITULAR GERENTE GENERAL INFONET

Carmen A. Ortiz Maza
Titular - Gerente General
Infonet Soluciones EIRL

Firma del investigador (o encargado de recoger información): PAUL CRIOLLO ORTIZ

COMITÉ INSTITUCIONAL DE ÉTICA EN INVESTIGACIÓN – ULADECH CATÓLICA

ANEXO V: FICHA DE VALIDACIÓN PARA JUECES EXPERTOS

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : JESUS PARI FLORES

1.2 Cargo e institución donde labora : RESPONSABLE INFORMATICA - BIBLIOTECA CENTRAL UNA PUNO

1.3 Nombre del instrumento evaluado : CUESTIONARIO

1.4 Autor del instrumento : PAÚL CRIOLLO ORTIZ

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	☐	☐	☒	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	☐	☒	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	☐	☐	☒	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	☐	☐	☒	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	☒	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☐	☒	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☒	☐	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☐	☒	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☐	☒	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	☐	☒	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)			2	27	
		C	B	A	Total

Coeficiente de validez : $\frac{A+B+C}{30} = 0.96$

Intervalos	Resultado
0,00 – 0,49	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

VALIDEZ MUY BUENA

Piura, 2020

ING. JESUS PARI FLORES
AREA INFORMATICA
BIBLIOTECA CENTRAL UNA - PUNO

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : .....DANIEL ALONSO FLORES CÓRDOVA .....
1.2 Cargo e institución donde labora : VOCAL DEL CAPÍTULO DE ING. MECAÁNICOS Y ELÉCTRICOS CIP CD PIURA
1.3 Nombre del instrumento evaluado : CUESTIONARIO
1.4 Autor del instrumento : PAÚL CRIOLLO ORTIZ

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	☐	☐	☒	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	☐	☒	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	☐	☒	☐	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	☐	☐	☒	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	☒	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☐	☒	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☐	☒	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☐	☒	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☐	☒	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	☐	☒	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)			2	27	
		C	B	A	Total

Coeficiente de validez : $\frac{A+B+C}{30}$ = 0.96

Intervalos	Resultado
0,00 – 0,49	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

VALIDEZ MUY BUENA

Piura, 2020

Daniel Alonso Flores Córdova
ING. ELECTRÓNICO Y TELECOMUNICACIONES
CIP :120598

FICHA DE VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Nombres y apellidos del validador : RICARDO SIANCAS CULQUICONDOR

1.2 Cargo e institución donde labora : GERENTE DE PRODUCCIÓN - GCTIC – ESSALUD PERÚ

1.3 Nombre del instrumento evaluado : CUESTIONARIO

1.4 Autor del instrumento : PAÚL CRIOLLO ORTIZ

II. ASPECTOS DE VALIDACIÓN

Revisar cada uno de los ítems del instrumento y marcar con un aspa dentro del recuadro (X), según la calificación que asigna a cada uno de los indicadores.

1. Deficiente (Si menos del 30% de los ítems cumplen con el indicador).
2. Regular (Si entre el 31% y 70% de los ítems cumplen con el indicador).
3. Buena (Si más del 70% de los ítems cumplen con el indicador).

Aspectos de validación del instrumento		1	2	3	Observaciones
Criterios	Indicadores	D	R	B	Sugerencias
• PERTINENCIA	Los ítems miden lo previsto en los objetivos de investigación.	☐	☐	☒	
• COHERENCIA	Los ítems responden a lo que se debe medir en la variable y sus dimensiones.	☐	☐	☒	
• CONGRUENCIA	Los ítems son congruentes entre sí y con el concepto que mide.	☐	☐	☒	
• SUFICIENCIA	Los ítems son suficientes en cantidad para medir la variable.	☐	☐	☒	
• OBJETIVIDAD	Los ítems se expresan en comportamientos y acciones observables.	☐	☐	☒	
• CONSISTENCIA	Los ítems se han formulado en concordancia a los fundamentos teóricos de la variable.	☐	☐	☒	
• ORGANIZACIÓN	Los ítems están secuenciados y distribuidos de acuerdo a dimensiones e indicadores.	☐	☐	☒	
• CLARIDAD	Los ítems están redactados en un lenguaje entendible para los sujetos a evaluar.	☐	☐	☒	
• FORMATO	Los ítems están escritos respetando aspectos técnicos (tamaño de letra, espaciado, interlineado, nitidez).	☐	☐	☒	
• ESTRUCTURA	El instrumento cuenta con instrucciones, consignas, opciones de respuesta bien definidas.	☐	☐	☒	
CONTEO TOTAL (Realizar el conteo de acuerdo a puntuaciones asignadas a cada indicador)				30	
		C	B	A	Total

Coeficiente de validez : $\frac{A+B+C}{30}$ = 1

Intervalos	Resultado
0,00 – 0,49	• Validez nula
0,50 – 0,59	• Validez muy baja
0,60 – 0,69	• Validez baja
0,70 – 0,79	• Validez aceptable
0,80 – 0,89	• Validez buena
0,90 – 1,00	• Validez muy buena

III. CALIFICACIÓN GLOBAL

Ubicar el coeficiente de validez obtenido en el intervalo respectivo y escriba sobre el espacio el resultado.

VALIDEZ MUY BUENA

Piura, 2020