CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

WILSON ANDRES SILVA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
BOGOTÁ D.C.
2021.

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

WILSON ANDRES SILVA FERREIRA

JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
BOGOTÁ D.C.
2021.

CONTENIDO

RESUMEN

El informe presenta los temas desarrollados durante el seminario especializado: Equipos estratégicos de ciberseguridad: Blue Team y Red Team, está dividido en cuatro etapas las cuales inicia con la presentación de la normatividad vigente en cuanto a leyes que regulan la seguridad de la información y la protección de datos, la ley 1273 de 2009 y se presentan algunos documentos conpes que hacen parte de las propuestas del gobierno nacional por mejorar la ciberseguridad en Colombia. La segunda etapa comprende el actuar de los red y Blue Team desde el ámbito ético, presentando un caso de estudio en el cual se da respuesta a unos interrogantes para ser desarrollados tenido en cuenta código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y cómo se vulnera la ley 1273 especificando los artículos.

Como tercera parte está la descripción de un ataque a un sistema informático por parte de Red Team en el cual se aprovecha la vulnerabilidad en una File Server que está instalado en la máquina Windows x64 en una de sus versiones. La etapa se constituye de las medidas de contención que aplica el Blue Team para esos ataques en tiempo real que detecta, las medidas de hardenización que se deben aplicar para evitar futuro ataques y la descripción de algunas herramientas de contención de ataques que ayudan a estar alertas ante posibles intrusiones.

LISTA DE IMAGENES

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ACUERDO DE CONFIDENCIALIDAD: La forma de legal de comprometerse a no divulgar la información, procedimientos, temas y demás términos que en este se plasme, se maneja mediante un contrato

ACTIVO: aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos. [1]

ATAQUE: un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control de este.[2]

BLUE TEAM: es un equipo que está enfocado en la contención de ataques y propone mejoras para la ciberseguridad de la organización. .

EXPLOIT: Ios exploit son códigos maliciosos diseñados para aprovechar una vulnerabilidad informática. Se emplean en las herramientas de test de intrusión.[3]

FUERZA BRUTA: consisten en probar todas las combinaciones posibles de caracteres hasta encontrar la clave que permite acceder al sistema.[4]

METASPLOIT: framework con licencia BDS. Permite desarrollar y ejecutar exploit contra máquinas remotas.[5]

METERPRETER: Es un mecanismo incluido en la msfconsole (Consola de Metasploit), que permite realizar actividades de explotación en un host remoto como escalar privilegios, hacer capturas de pantalla y teclado, activar cámara y micrófono del objetivo, obtener hash entre otras cosas.

NMAP: Herramienta para escaneo de puertos, vulnerabilidades versiones de sistema operativo en maquinas objetivo.

PAYLOAD: el payload es la carga útil que esta adjunta al exploit, que se ejecuta tan pronto haya una explotación exitosa.[6]

REDRABBIT: Herramienta para recolección de información, es utilizada por Red Team para la fase inicial que consiste en el reconocimiento de la organización.

---

[1] Escrivá Gasco G. Seguridad informática [En línea]. Macmillan Iberia, S.A.; 2013. 218 p. Disponible en: https://elibro.net/es/lc/unad/titulos/43260.
[2] Ibid. p.11.
[3] Ibid. p.189.
[4] Ibid. p.49.
[5] Castro Vásquez CA. Pruebas de Penetración e Intrusión [En Línea]. Technological innovations. Bogotá D.C: Facultad de Ingenierías; 2019. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6273.
[6] Fried SD. Penetration testing. Inf Secur Manag Handbook, Sixth Ed. 2007;1005-17.

RED TEAM: es un grupo independiente de personas, puede estar conformado al menos por dos personas, quienes desafían a la organización para que mejore sus defensas. Es un hacking ético que permite demostrar qué tan bien lo hace la organización frente a un ataque real[7].

TCP_PING: Es una herramienta que emula la función del ping, función que permite determinar si un host está activo. La diferencia con el ping que se hace normalmente para comprobar conexión es el uso del protocolo, tcp-ping utiliza el protocolo TCP, mientras que el ping normal utiliza ICMP.

TEST DE INTRUSIÓN: consiste en un método de auditoría mediante el cual se intenta acceder a los sistemas para comprobar el nivel de resistencia a una intrusión no deseada.[8]

VULNERABILIDAD: en el campo de la seguridad informática se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático.[9]

[7] Tamboli A. Cybersecurity: Supervising Your AI With The Red Team. Electron You [En Línea]. 2020 Jun 20; Disponible en: https://search.proquest.com/docview/2415851338?accountid=48784.
[8] ibid., p.190.
[9] ibid., p. 9.

INTRODUCCIÓN

El presente informe es una recopilación de lo que se trabajó durante el seminario especializado: Equipos Estratégicos en ciberseguridad: Red Team y Blue Team. La primera etapa se constituye con la identificación de leyes que rigen la ciberseguridad y la protección de datos personales en Colombia, el código de ética para el ejercicio de la ingeniería en general y sus profesiones afines. La segunda etapa se basa en el actuar en el ámbito ético y legal de los Red Team y blue Team basados en un caso de estudio en el cual se hace un acuerdo de confidencialidad en el cual se presentan situaciones que atentan contra la ética profesional y vulnera algunas leyes de protección de datos.

Continúa con la tercera etapa que consiste en la descripción de un ataque a un sistema informático desde el Red Team aprovechando una vulnerabilidad en una maquina Windows con arquitectura x64 cuyo ataque se presenta mediante las fases del pentesting y el uso y descripción de herramientas para cada fase con los comandos utilizados y el resultado obtenido, llegando a la creación de un usuario con privilegios de administrador. Finalmente, la cuarta etapa presenta las medidas de contención que aplica el Blue Team para evitar daños graves en el sistema informático atacado, algunas herramientas de contención y las diferencias entre un Blue Team y un equipo de respuesta a incidentes.

1 DEFINICIÓN DEL PROBLEMA

De acuerdo con el informe sobre tendencias cibercrimen en Colombia 2019-2020[10], el principal interés de los cibercriminales el económico, el delito más denunciado es el hurto por medios informáticos con 31.058 casos, generalmente a cuentas bancarias, en segundo lugar está la violación de datos personales con 8.037 casos, y afirman que esta segunda amenaza, robo de identidad, aplica para empresas y personas, en tercer lugar se encuentra con 7.994 casos el Acceso abusivo a sistema informático, en este tipo de ataques el ciberdelincuente busca en primera instancia comprometer los sistemas informáticos obteniendo acceso a ellos; con 3.425 casos, en cuarto lugar, se encuentra la transferencia no consentida de activos, esto hace referencia a la sustracción de dinero o de activos de información. Y finalmente en quinto lugar con 2.387 casos se encuentra el uso de software malicioso.

Los ataques mencionados, aplican para empresas de todos los tamaños y personas en general, el estudio del BID[11], afirma que estos están centrados en la Pymes, entidades financieras y grandes compañías ubicadas en ciudades principales.

Ahora bien, ¿cómo proteger a las MiPymes de estos ciberataques? Existen estándares, metodologías, equipos especializados en seguridad Blue Team y Red Team, empresas de pentesting con años de experiencia y conocimientos sobre el actuar de los ciberdelincuentes, entre otras.

FORMULACIÓN DEL PROBLEMA

¿Por qué las empresas necesitan a los Red Team y Blue Team?

[10] CCIT. Policía Nacional de Colombia. Tendencias cibercrimen Colombia 2019-2020. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf.
[11] BID. MinTic. OEA. Impacto de los Incidentes de Seguridad en Colombia 2017. Organ los Estados Am [En Línea]. 2017;66(2-3):130. Disponible en: https://publications.iadb.org/es/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf.

2 JUSTIFICACION

Kaspersky[12] afirma que las pequeñas empresas son las más deseadas por los hackers, estos se basan en la información que manejan, como datos de proveedores, clientes, que suelen ser empresas grandes, y la poca seguridad informática que frecuentan. Esto las convierte en objetivos comunes ya que por allí podría un atacante llegar a una compañía mayor y obtener mayores frutos para su deseo maligno.

Por tanto, el presente informe se justifica en la importancia de invertir en seguridad informática en todas las empresas sin importar su tamaño, los hackers solo les interesa lo económico en primera instancia o hacer daños que pueden ocasionar hasta el cierre de la compañía. Se presenta basados en las etapas que se han estudiado durante el seminario especializado con la identificación de la normatividad, los actuares éticos que deben tener los Red y Blue Team en las organizaciones y el actuar de de cada equipo desde un ataque aprovechando una vulnerabilidad hasta las medidas de contención para evitar ataques futuros.

[12] Kaspersky. ¿Quién le espía? Ninguna empresa está a salvo del ciberespionaje [En Línea]. Kaspersky; 2020. p. 18. Disponible en: https://media.kaspersky.com/es/business-security/Cyber_Espionage_WhitePaper_FINAL_ES.pdf.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Presentar el informe de lo realizado en las etapas que componen el desarrollo del seminario especializado equipos estratégicos en Ciberseguridad: Red Team y Blue Team.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la legislación “leyes, decretos” que existen actualmente y las características principales de cada ley sobre ciberseguridad y protección de datos.
- Conocer las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Describir la intrusión a un sistema informático desde el Red Team mostrando la vulnerabilidad a partir de uso de técnicas de intrusión.
- Formular estrategias de contención mediante la solución a interrogantes orientados a los ataques en tiempo real, el ataque del Red Team, e identificación de diferencias entre Bule Team y Equipos e respuesta a incidentes.

4 METODOLOGIA

Para el desarrollo de este informe, se tendrá el siguiente diseño metodológico:

Tipo

Se realiza una consulta de tipo documental informativa de acuerdo con el tema tratado en cada etapa en el seminario especializado.

Enfoque de la investigación

El enfoque que se tendrá para este informe es de tipo cualitativo.

Fuentes de investigación

Secundarias: se consultarán fuentes de diferentes autores, páginas web, artículos de revistas, trabajos de grado, todos relacionadas con temas de ciberseguridad, Red Team, Blue Team.

Técnicas de recolección y análisis de información

Como técnica de recolección se utilizará la consulta de documentos de diferentes autores, páginas web, artículos de revistas, trabajos de grado, todos relacionadas con temas de ciberseguridad, Red Team y Blue Team. El análisis de la información será de tipo subjetiva de acuerdo con la comprensión e interpretación de las referencias consultadas.

Población y muestras

La población objetivo son las empresas de cualquier sector y tamaño en las que se pueden aplicar las técnicas ejecutadas por los Red Team como ejercicios de ataque a la seguridad de información y ejercicios de defensa ejecutados por los Blue Team.

5 DESARROLLO DEL INFORME

5.1 LEGISLACIÓN EN CIBERSEGURIDAD Y PROTECCIÓN DE DATOS.

La ley 1273 de 2009[13]**:** Se refiere a los delitos informáticos, las penalidades económicas y de prisión asociadas a cada tipo de delito informático. Describe los principales delitos relacionados con la protección de la información y las comunicaciones en cuanto a su integridad, disponibilidad y confidencialidad

Presenta delitos asociados con la intrusión ilegitima a sistemas de información, bloqueo sin autorización de dispositivos de Red, tratamiento de información sin los permisos correspondientes, más basado en la interceptación. La pena de prisión máxima que establece la ley 1273 de 2009 es de 96 meses, la mínima es de 36 meses, en el delito de interceptación de datos informáticos, para los demás delitos estipulados en la norma, la pena mínima es de 48 meses. En cuanto a multa la mínima es de 100 Salarios.

Ley 1341 DE 2009[14]**:** Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Contiene el marco general de TIC y establece el régimen de habilitación general para la provisión de redes y servicios de telecomunicaciones. Dentro del ordenamiento de las TIC, habla del régimen de competencia, la protección de derechos de los usuarios, las potestades que tiene el estado en cuanto a la prestación eficiente del servicio.

Ley 1581 de 2012[15]: Por la cual se desarrolla el derecho constitucional de las personas por conocer, actualizar y rectificar la información que ha recogido las empresas en bases de datos o archivos.

---

[13] Colombia. Congreso de la República “Ley 1273 de 2009” Diario Oficial No. 47.223 de 5 de enero de 2009, [En Línea] 2009. Dsiponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[14] Colombia. Congreso de la República. LEY 1341 DE 2009. Diario Oficial No 47426 de 30 de julio de 2009 [En Línea]. 2009;28. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html.

[15] Colombia. Congreso de la República. Ley 1581 de 2012. Diario Oficial No 48587 de 18 de octubre de 2012 [En Línea]. 2012; Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Ley 1978 de 2019[16]: Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones. Es ley simplifica y moderniza el marco institucional del sector TIC. Focaliza las inversiones en TI para el cierre de brechas digitales. Modifica varios artículos y numerales de la ley 1341 de 2009. Otra de las modificaciones que tiene con respecto a la ley 1341 es que no habla de la protección de los derechos de los usuarios, sino que habla directamente de la protección del usuario.

Ley 599 DE 2000[17]: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

Ley 1928 de 2018[18]**:** Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Este convenio trata sobre los delitos informáticos como la pornografía infantil, los fraudes informáticos, y violaciones a la seguridad de las redes; con el acceso ilegal a las redes informáticas, de allí, se busca que a nivel mundial se tipifiquen los delitos informáticos y se castiguen igual en todas las naciones. El objetivo principal del tratado de Budapest es "La protección de la sociedad de la ciberdelincuencia".

CONPES 3995[19]: Tiene por objetivo fortalecer las capacidades de las partes interesadas para mitigar, gestionar, tratar, los riesgos de seguridad digital en cada una de las actividades económicas. Estos para permitir el crecimiento de la economía digital, que permitirá una mayor prosperidad económica y social del país. Se basa en los siguientes frentes de acción:

- Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos.

[16] Colombia. Congreso de la República. Ley 1978 de 2019. Diario Oficial No 51025 de 2019 [En Línea]. 2019;23. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=85632.
[17] Colombia. Congreso de la República "Ley 599 de 2000" Diario Oficial No. 44.097 de 24 de julio de 2000, [En Línea]. 2000.Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html.
[18] Colombia. Congreso de la República. Ley 1928 2018. Diario Oficial No 50664 de 24 de julio de 2018 [En Línea]. 2018;13. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html.
[19] Colombia. Presidencia de la República. Documento Conpes 3995. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL [En Línea]. 2016;51. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf».

- Crear las condiciones para que las partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y generen confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional.

CONPES 3707[20]: Tiene como objetivo fortalecer las capacidades que tiene el Estado para la defensa en contra de las amenazas que atenten contra la seguridad en el ámbito cibernético.
Se basa en los siguientes frentes de acción:

- Promover la capacitación en seguridad de la información que permita fortalecer capacidades para poder afrontar las amenazas y los incidentes cibernéticos.
- Fortalecer la legislación, promover el desarrollo de herramientas jurídicas para que haya una efectiva prevención investigación y judicialización de los delitos informáticos.

Código de ética[21]**:** Este código presenta un conjunto de normas que guían el deber y la normalidad que deben cumplir los profesionales de ingeniería, sus profesiones afines y auxiliares. Habla del comportamiento que deben tener los ingenieros, la importancia de enaltecer y honrar la profesión, actuar con ética, honradez y lealtad.

5.2 RED TEAM Y BLUE TEAM ACCIONES ÉTICAS Y LEGALES

Teniendo en cuenta que la etapa comprende el caso de estudio en el cual se presenta un acuerdo de confidencialidad en el cual se presentan anomalías en las cláusulas en cuanto al proceder de manera ética. A continuación, se identifican las cláusulas del acuerdo que presentan inconsistencias.

[20] Colombia. Presidencia de la República. Documento Conpes 3701. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA [En Línea]. 2011;43. Disponible en: https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011
[21] Colombia. Copnia. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Consejo Profesional Nacional de Ingeniería [En Línea]. 2014;1(CODIGO DE ETICA):20. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Tabla 1. Cláusulas Acuerdo Confidencialidad con Inconsistencias

Clausula	Contenido	Acción Ilegal
Clausula Primera. Objeto	En virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.	Se puede apreciar que si la empresa tiene o hace procesos ilegales nadie podrá divulgar la información para dar a conocer a las autoridades lo que esté sucediendo. Esto sería un acto no ético, ya que se debe denunciar todo proceso o acto ilícito del que se tenga conocimiento.
Clausula Segunda. Definición de información confidencial, numeral 2:	se entiende como **Información Confidencial**, para los efectos del presente acuerdo: 2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".	Habla de información de chuzadas, acceso abusivo a sistemas informáticos e interceptación de información. Esto evidencia que hay procesos ilegales para obtener información y la clasifican como confidencial, se están cometiendo delitos informáticos que son castigados por la ley 1273 de 2009 y el componente ético en cuanto las prohibiciones de los profesionales del código de ética articulo 32 literal B "Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley".
Clausula Cuarta. Obligaciones del aparte Receptora, numeral 3 y numeral 4:	Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a: 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. 4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.	Dice de no denunciar las actividades sospechosas ante las autoridades que tengan que ver con espionaje u otros procesos que lleven a obtener información de terceros. Esto evidencia que se obtiene información de manera ilegal y se busca que los trabajadores de la empresa no hagan las denuncias respectivas de acuerdo con la ley y el código de ética.

Fuente: elaboración propia

Tabla 2. (Continuación)

Clausula Cuarta. Obligaciones del aparte Receptora, numeral 7 y 8:	7. Responder por el mal uso que le den sus representantes a la **información confidencial.** 8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.	Numeral 7: el receptor, debe responder por el mal uso que den a la información confidencial sus representantes, ilegal teniendo en cuenta que no depende del quien recibe la información el uso que los demás le den y que también tiene acceso a ella. Se evidencia falta de ética profesional. Numeral 8: Es algo ilegal, ya que es información que recibió directamente de la compañía o recopiló en el ejercicio de sus funciones. Por tanto, la responsabilidad de recaer en la representación leal de la empresa como responsable de los procesos que allí se ejecuten.
Cláusula Octava. Solución de Controversias:	Las partes se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.	Menciona que se deben hacer esfuerzos por solucionar las controversias que se presenten entre las partes de la mejor manera, pero si encuentran información ilegal en manos del receptor deberá acudir a un abogado privado y liberar de cualquier responsabilidad a la empresa. Esto parecer estar en el ámbito no ético, ya que si se tiene información ilegal es por los procesos que realiza la empresa y puede estar en las funciones del trabajador el recopilar información sin saber que es o no ilegal. La empresa debe apoyar al trabajador en caso de asuntos legales y este no tiene por qué buscar abogados externos.

Fuente: Elaboración propia.

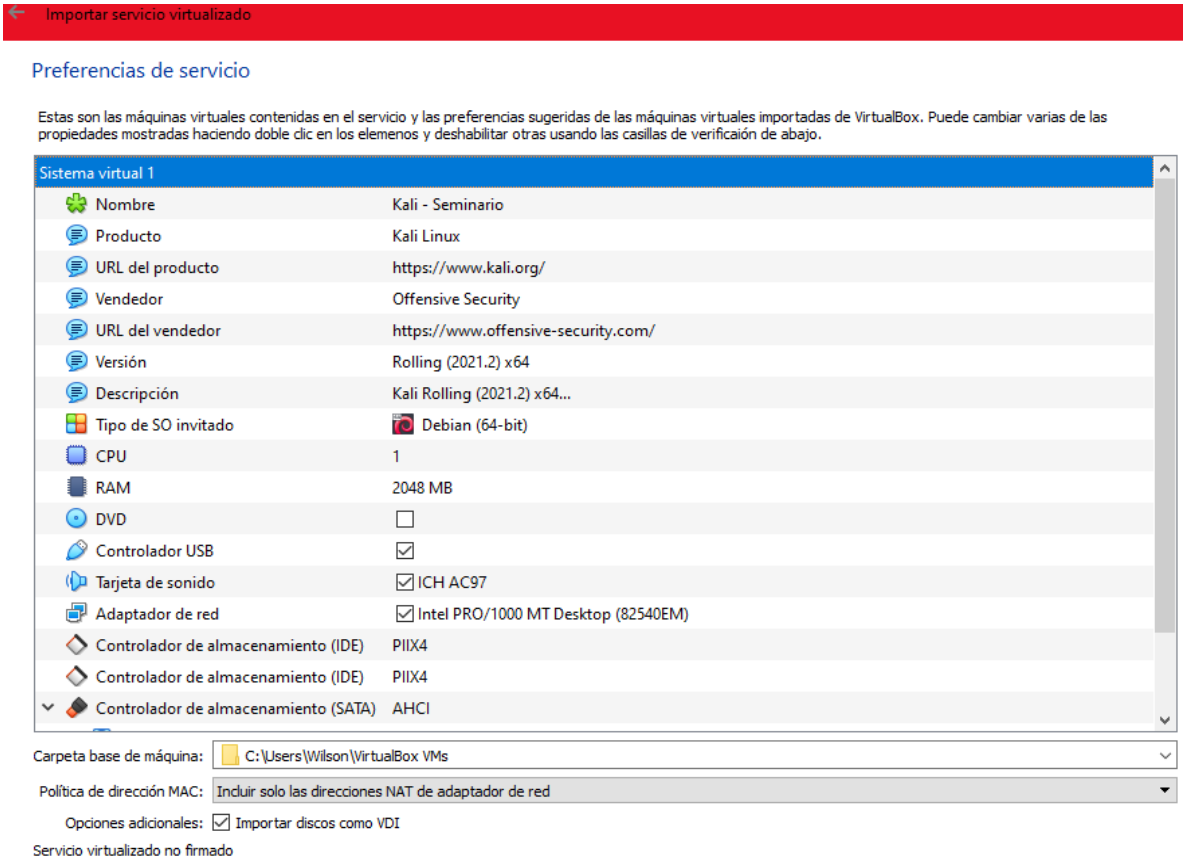
La tabla anterior presenta los argumentos no éticos que se deben tener en cuenta cuando se va a trabajar en una empresa de cualquier sector haciendo parte del Red Team o el Blue Team, no interesa de qué lado vaya a estar, atacando o defendiendo, siempre se debe hacer de manera ética y acorde a las leyes nacionales e internacionales.

5.3 INTRUSIÓN A UN SISTEMA INFORMÁTICO DESDE EL RED TEAM

Para iniciar con la descripción de una intrusión a un sistema informático desde el Red Team, primero se da a conocer las características de la máquina atacante y la maquina objetivo.

La máquina utilizada para para el ataque es Kali Linux, (Linux Kali 5.10.0-kali9-amd64 #1 SMP Debian 5.10.46-4kali1 (2021-08-09) x86_64 GNU/Linux) una distribución basada en Debian actualmente está en la versión 2021.3. Kali Linux por ser una distribución debían permite los mismos comandos de cualquier distribución de este tipo, actualizaciones permanentes y está disponible para arquitecturas x86 y x64, más o menos desde 2017 está disponible para Rasperi pi y algunos dispositivos Android. Se puede utilizar en VMWare, Virtual box y hasta en modo live para tenerla cuando se requiera.

Imagen 1. Características de Hardware Kali Linux



Fuente: elaboración propia.

Se observan las características de la maquina Kali, los controladores activados y la ubicación donde quedará el disco creado. Una vez se verifican hace la importación del servicio virtualizado.

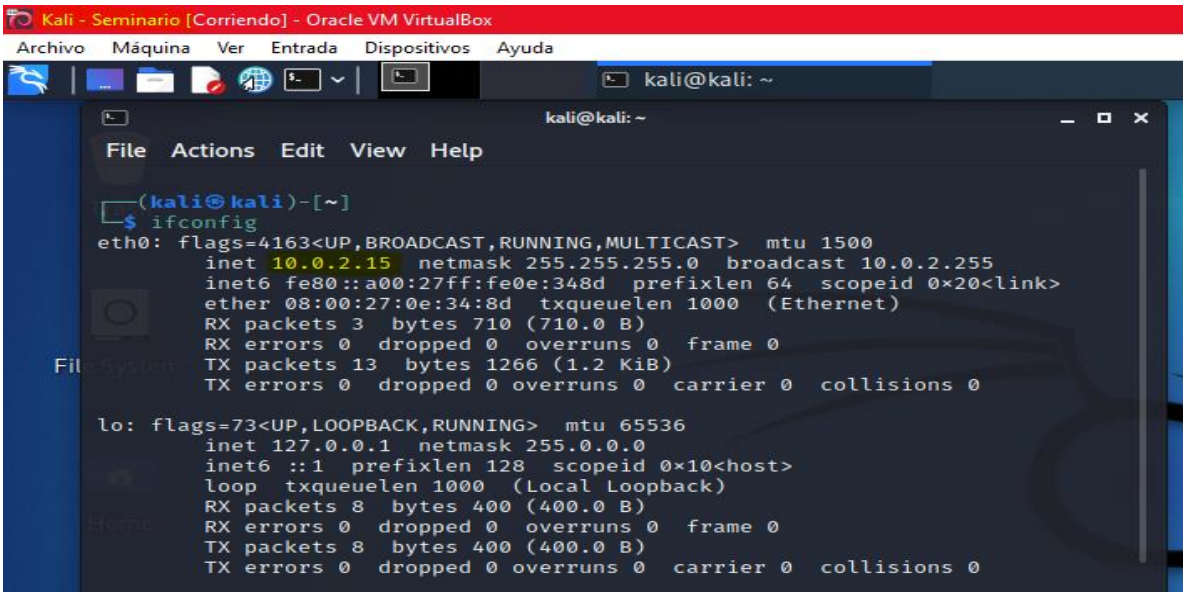
Imagen 2. Kali Linux Instalado e Iniciado

Fuente: elaboración propia.

Cuando termina el proceso de importación, la máquina se inicia, es necesario ingresar las credenciales, para el caso de Kali se inicia con las siguientes:

Usuario: Kali
Password: Kali

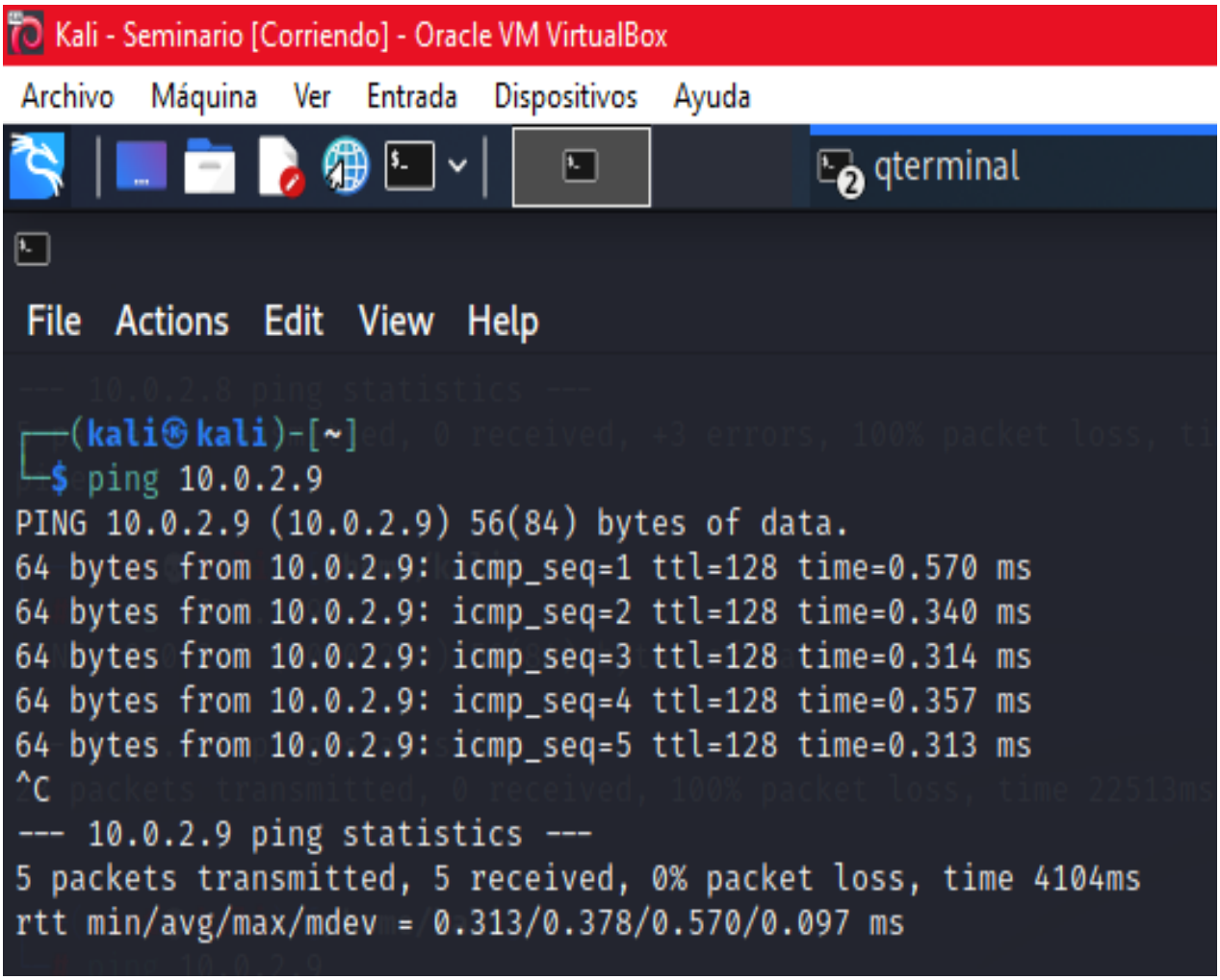
Imagen 3. Comprobando direccionamiento Ip en Kali Linux



Fuente: elaboración propia.

Se verifica la dirección Ip que se ha asignado a Kali Linux, para este caso es la 10.0.2.15

Imagen 4. Ping a Máquina Windows x64

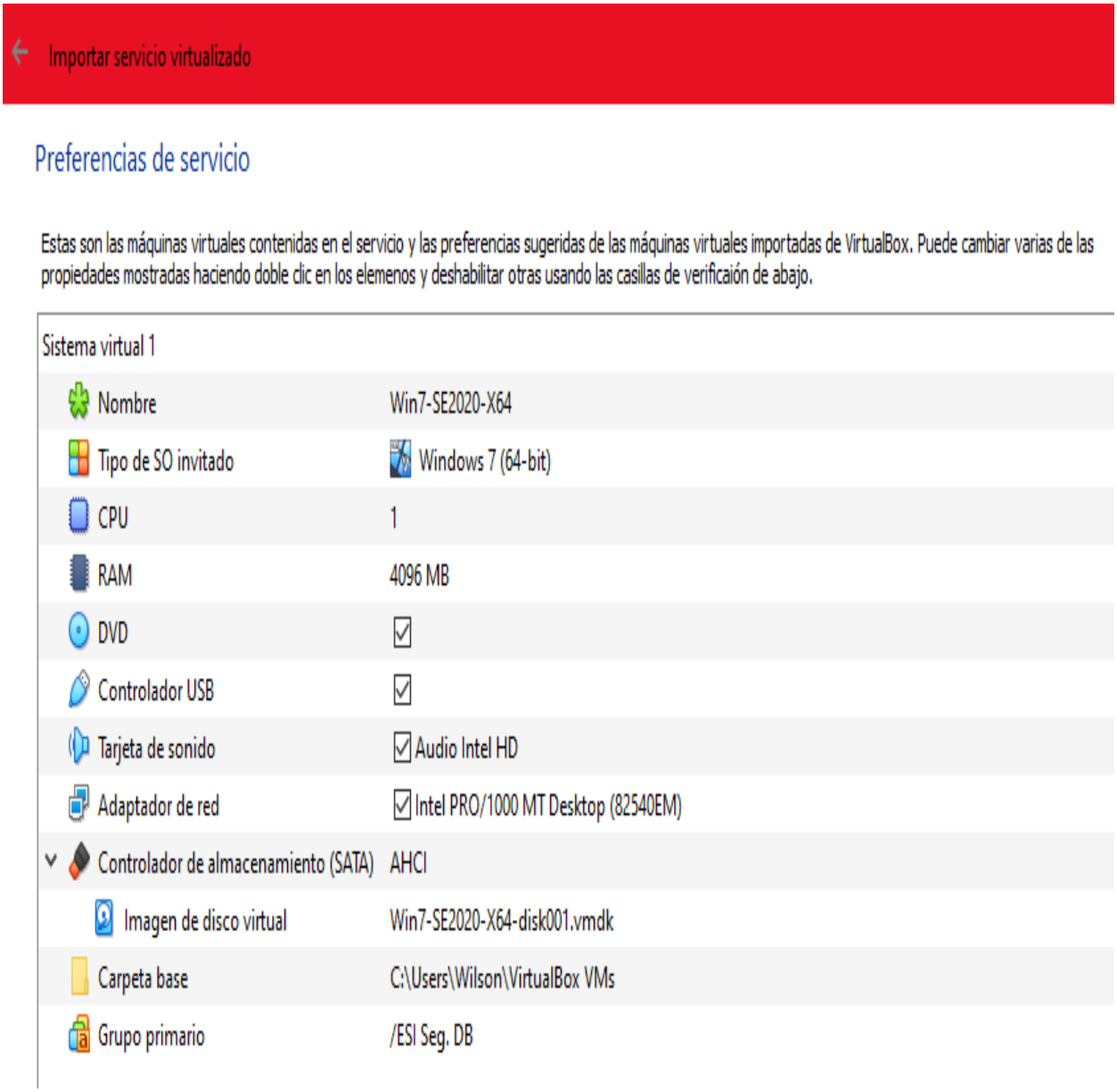


Fuente: elaboración propia.

Se realiza un ping a la maquina Windows x64 10.0.2.9, para comprobar conexión, y es exitosa.

Se inicia la importación de la maquina Win x64

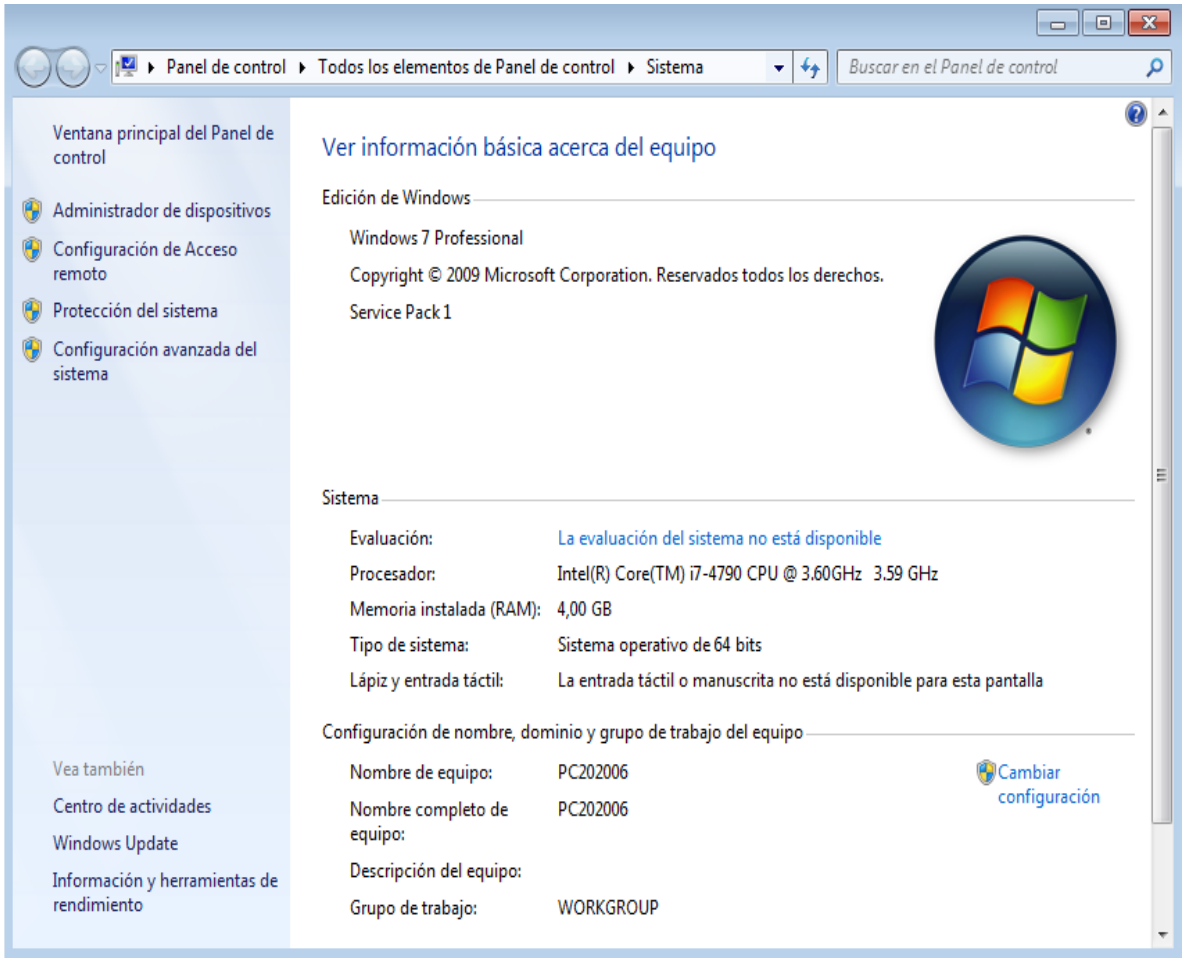
Imagen 5. Importando Máquina Win x64



Fuente: elaboración propia.

Se observan los controladores activados, la versión de Windows y la ubicación donde quedará el disco creado. Una vez se verifican se continua con la importación.

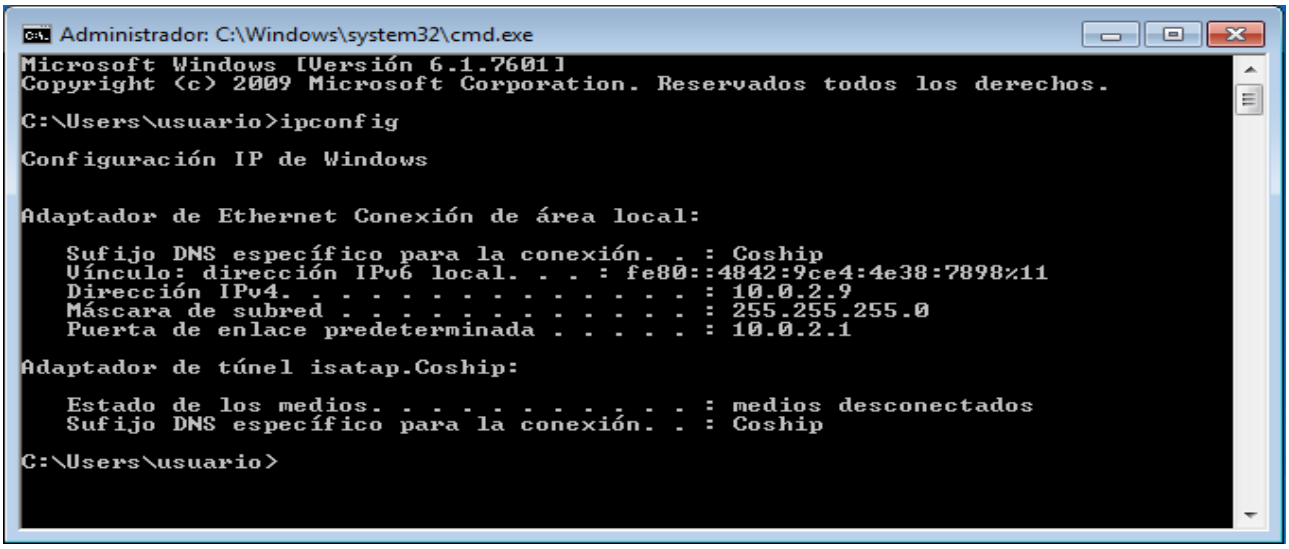
Imagen 6. Características físicas de la Máquina Win x64



Fuente: elaboración propia.

- Hardware maquina Windows x64
- Procesador: Intel® Core i7 3.60GHz
- Memoria RAM: 4.00 GB
- Disco Duro: 50GB

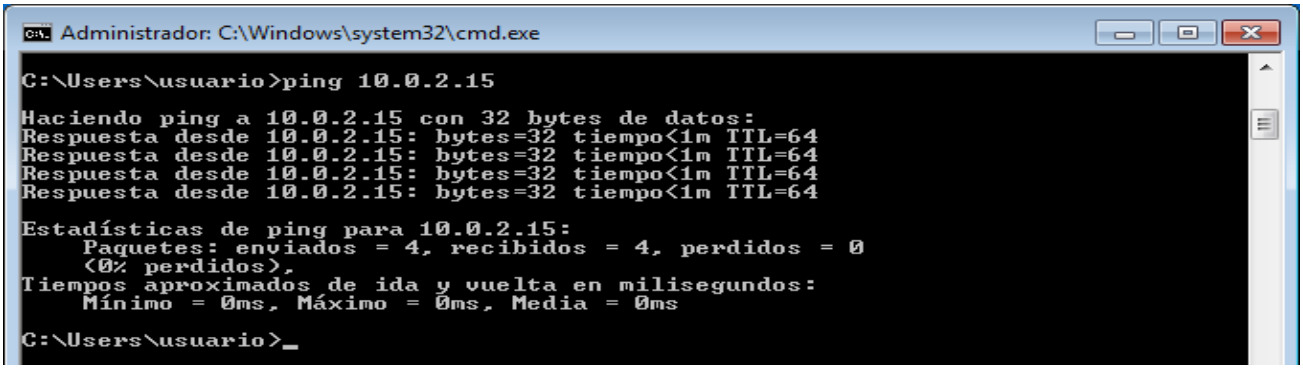
Imagen 7. Comprobando dirección Ip Windows x64



Fuente: elaboración propia.

Se realiza la comprobación de la dirección Ip asignada, para este caso es la 10.0.2.9

Imagen 8. Ping a Máquina Kali Linux



Fuente: elaboración propia.

Se realiza ping a la maquina Kali 10.0.2.15, para comprobar conexión, es exitosa.

Una vez se ha comprobado la conexión y las características físicas de cada una de las maquinas, se procede con la intrusión basados en las fases del pentesting.

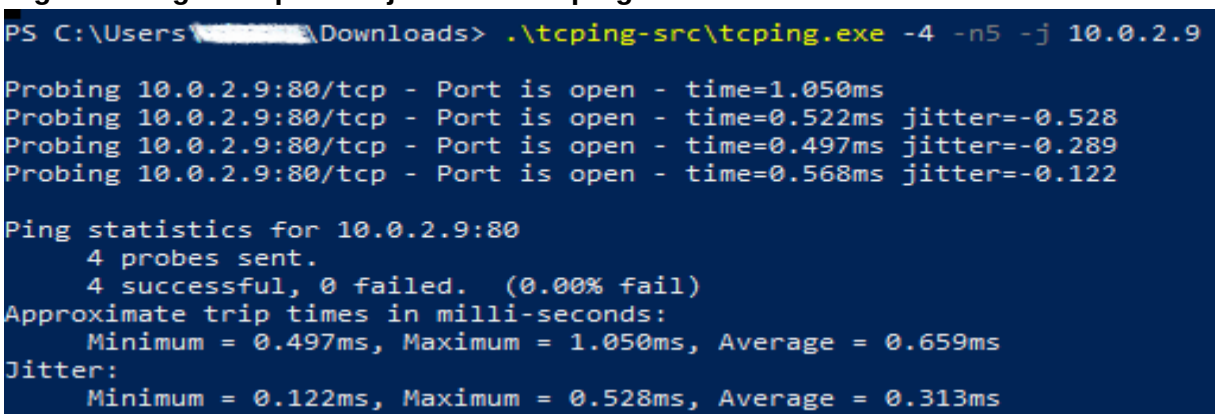
5.3.1 Fases del Pentesting

- **Recolección De Información**

Para esta fase del pentesting se utilizó la herramienta tc ping.

TCPING es una herramienta que sirve para identificar si un host esta activo y que puertos tiene abiertos, cuando se hace un ping normal para ver si un host está en la red se hace con el protocolo ICMP TCPING se basa en el protocolo TCP para realizar es escaneo del objetivo[22].

Imagen 9. Ping a máquina objetivo con TCping



Fuente: elaboración propia.

Comandos utilizados:

- Tcping-src: es el nombre de la carpeta que está ubicada en Downloads
- Tcping.exe: es el ejecutable de la herramienta TCPING
- -4: es para indicar que se utilice el protocolo Ipv4 para la conexión
- -n: es para indicar el número de solicitudes que la herramienta realizar para el caso se indicó el número 5.
- -j: muestra el jitter de la conexión que indica la variación en el retardo de paquetes.
- 10.0.2.9: es la dirección Ip de la maquina objetivo.

[22] Luz S de. Cómo realizar un escaneo de puertos en Windows con TCPing [En Línea]. RedesZone. 2021 [citado: 2021 Sep 21]. Disponible en: https://www.redeszone.net/tutoriales/configuracion-puertos/tcping-escaner-puertos-windows/.

- **Modelado de Amenazas**

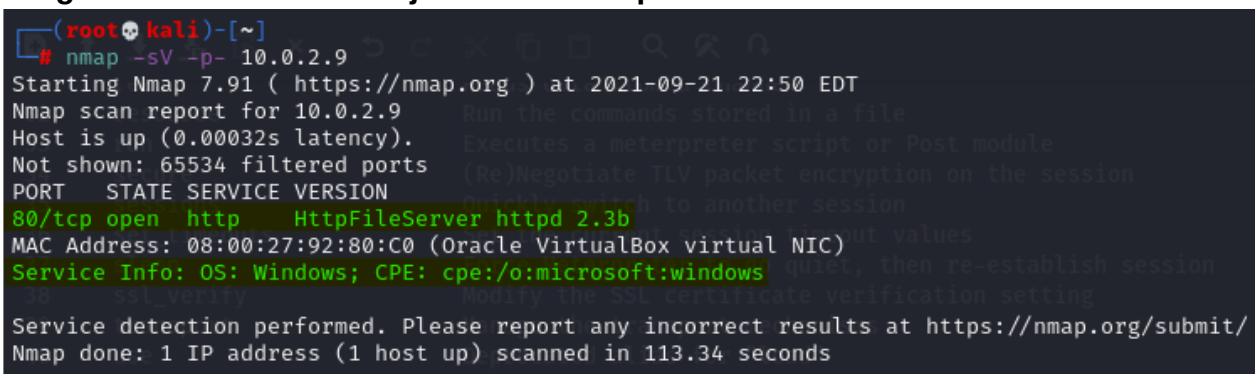
Para esta fase del pentesting se utilizó la herramienta Nmap.

Nmap: es una herramienta que permite el reconocimiento de puertos en el segmento de red que se asigne, cuenta con varios tipos de escaneo según la necesidad que se tenga y los comandos que se indiquen[23]. También permite ver la versión de los servicios o aplicaciones que se encuentran habilitados en los puertos que están abiertos.

Comandos utilizados:

- Nmap: ejecuta la herramienta utilizada
- -sV: busca en los puertos que encuentra abiertos e intenta descubrir la versión de los servicios que se alojan en esos puertos[24].
- -p: Especifica el rango de puertos a analizar -p- escanea todos los puertos, si se agrega U escanea solo UDP, T, solo los TCP y S solo SCTP.
- 10.0.2.9: es la dirección Ip de la maquina objetivo.

Imagen 10. Escaneo del objetivo con Nmap



Fuente: elaboración propia.

Como se puede observar, el texto resaltado en verde presenta el puerto 80 abierto, servicio http, y versión HttpFileServer httpd 2.3b, lo que quiere decir que tiene un file Server que puede ser vulnerable de acuerdo con su versión 2.3b. También muestra que el objetivo es un sistema operativo Windows.

[23] Ortega Candel JM. Hacking ético con herramientas Python [En Línea]. RA-MA Editorial; 2018. 291 p. Disponible en: https://elibro.net/es/lc/unad/titulos/106513.
[24] CSIRT-cv. Nmap 6: Listado de comandos. 2018;1–6. Disponible en: http://www.csirtcv.gva.es.

- **Análisis de Vulnerabilidades**

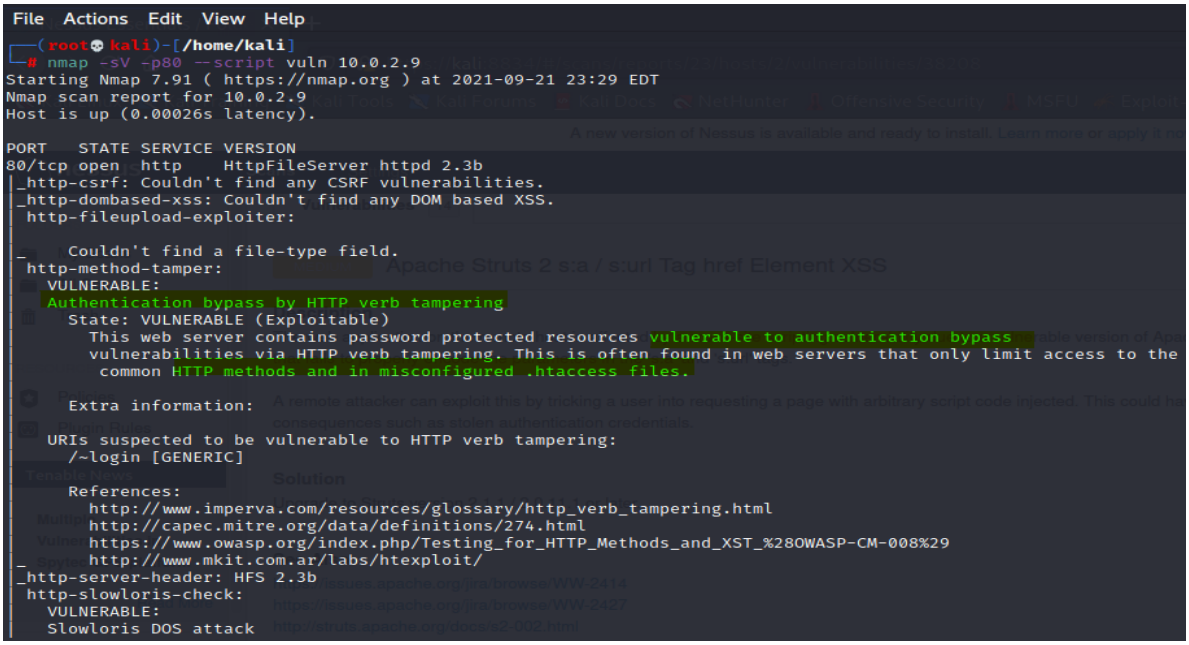
Para esta fase del pentesting se utilizó la herramienta Nmap.

Nmap, es una herramienta que también permite la identificación de vulnerabilidades, una vez que se ha detectado el o los puertos abiertos, el servicio y la versión que se encuentran activos, entonces se procede a buscar vulnerabilidades de acuerdo con la versión encontrada.

Comandos utilizados:

- Nmap: ejecuta la herramienta utilizada.
- -sV: busca en los puertos que encuentra abiertos e intenta descubrir la versión de los servicios que se alojan en esos puertos[25].
- -p80: especifica que el escaneo se realice únicamente en el puerto 80
- --script: define el script que se utiliza en el escaneo, para este caso se utilizó *vuln*, que realiza escaneo de vulnerabilidades en el puerto y servicios especificados.
- 10.0.2.9: es la dirección Ip de la maquina objetivo.

Imagen 11. Análisis de Vulnerabilidades con Nmap

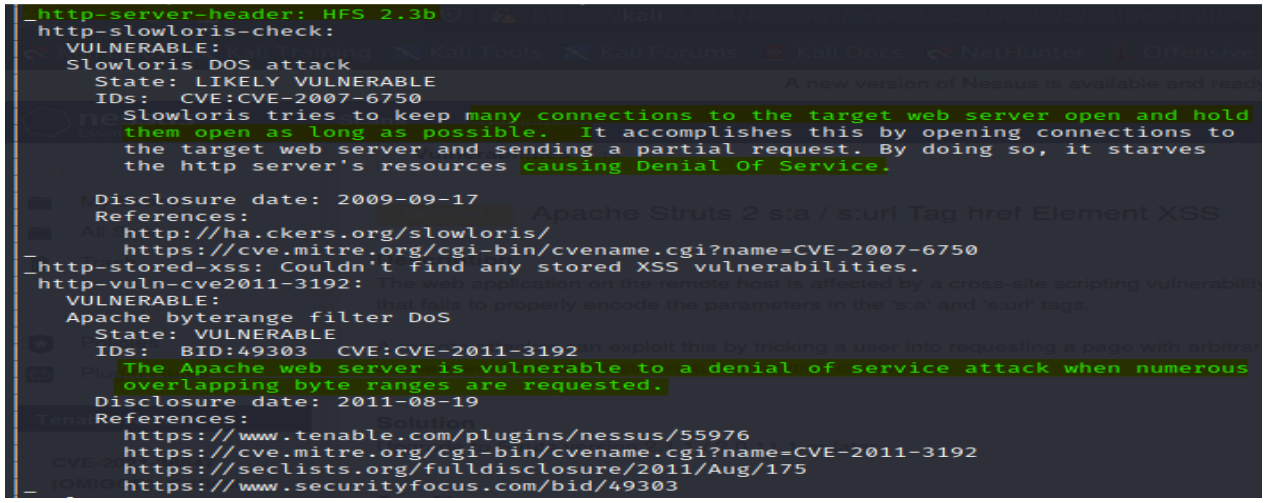


Fuente: elaboración propia.

[25] Ibíd. p3.

En los resultados obtenidos se evidencia el puerto, la versión y el servicio activos, y seguidamente un lista de vulnerabilidades con referencias e información adicional, la primera que se resalta en verde es una vulnerabilidad de autenticación generada por mala configuración del archivo .htacces.

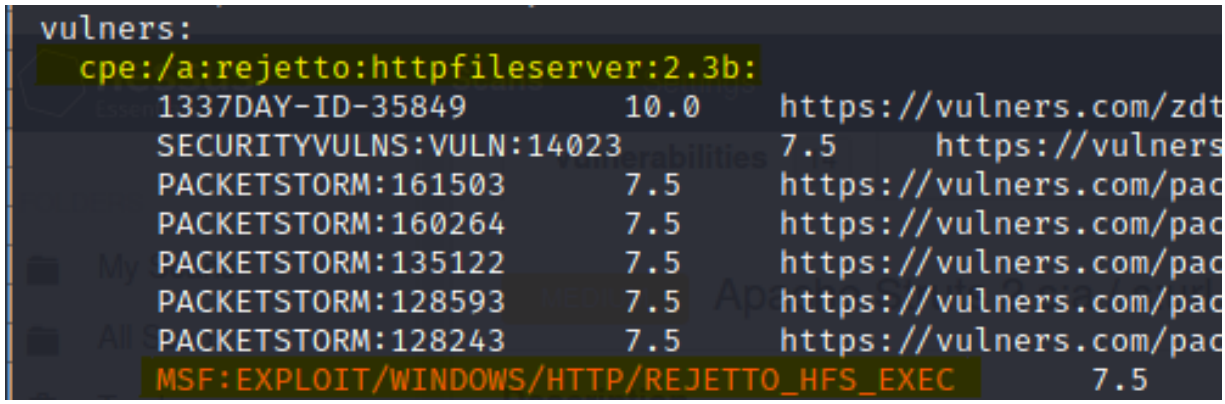
Imagen 12. (Continuación)



Fuente: elaboración propia.

Siguiendo con los resultados, la imagen anterior presenta resaltado en verde una vulnerabilidad de Denegación de servicio DoS, generada por las múltiples conexiones que el servicio permite activas por largo tiempo.

Imagen 13. (Continuación)



Fuente: elaboración propia.

Finalmente, presenta el resultado de una vulnerabilidad en la aplicación rejetto, resaltada en amarillo y se puede observar que es el servicio y la versión que se encontró en el

puerto 80 httpfileserver 2.3b. resaltado en naranja se evidencia que Nmap presenta un exploit que se puede utilizar para aprovechar esta vulnerabilidad encontrada.

- **Explotación**

Para esta fase del pentesting, se utilizó la herramienta metasploit.

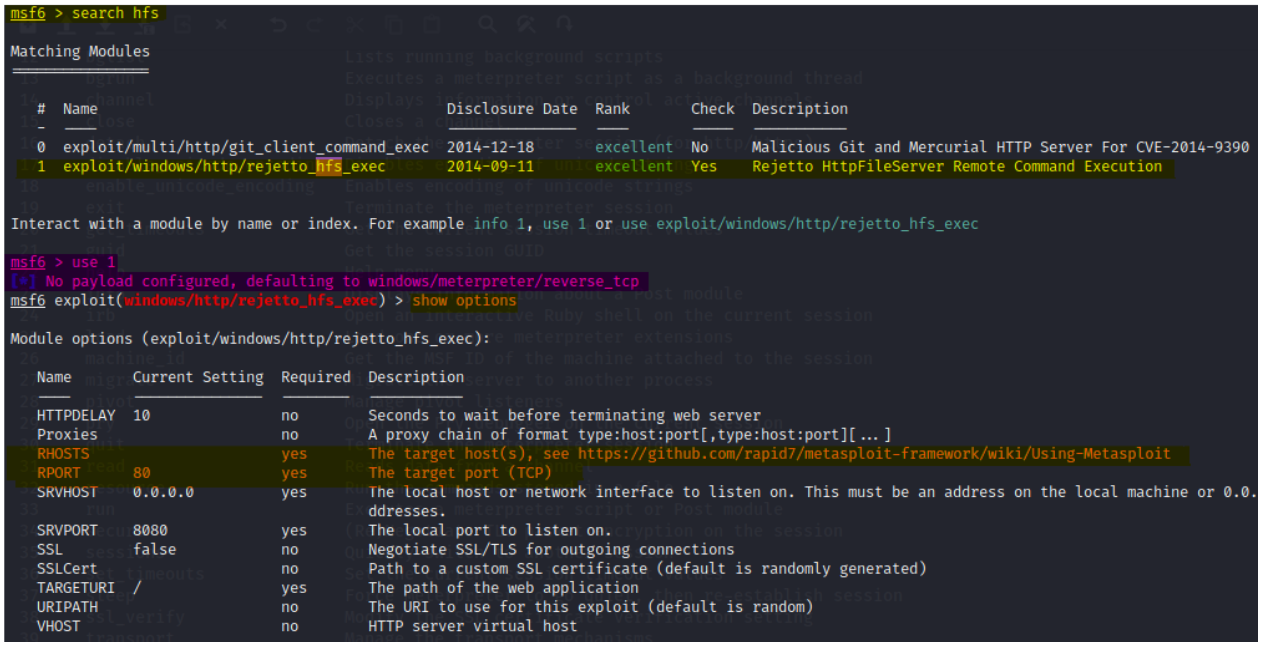
Metasploit, es una herramienta de explotación de vulnerabilidades y es de las que más utilizan los auditores de seguridad, contiene módulos auxiliares, exploits, payloads que permiten la explotación de vulnerabilidades, interactúa con Nmap y Nessus[26].

Comandos utilizados:

- Search: permite buscar en la lista de exploits que contiene metasploit, para el caso se buscó con las letras hfs como indicaba en los resultados de análisis de vulnerabilidades.
- Use: permite utilizar el exploit que se ha encontrado, para el caso se seleccionó (windows/http/rejetto_hfs_exec).
- Show options: permite ver las opciones de configuración que tiene el exploit y el payload.
- Set rhost: permite ingresar la dirección Ip del objetivo, para el caso fue 10.0.2.9
- Exploit: es el comando que inicia la explotación, si todo está correcto, genera una Shell meterpreter.

[26] Rizaldos Héctor. Qué es Metasploit framework [En Línea]. OpenWebinars. 2018 [citado 2021 Sep 21]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/.

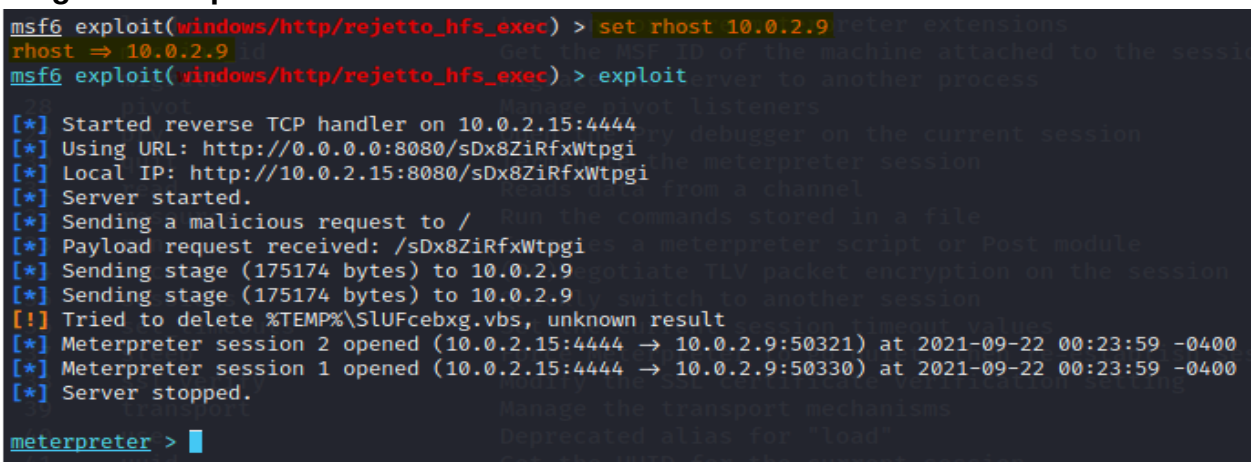
Imagen 14. Explotación con Metasploit



Fuente: elaboración propia.

En los resultados se puede evidenciar resaltado en color amarillo el comando search y el resultado de la búsqueda (windows/http/rejetto_hfs_exec). El comando use 1 en color rojo, que es para utilizar el exploit número 1 dentro de los resultados de la búsqueda, y en naranja el comando show options que muestra las opciones del exploit entre ellas el rhost que es la dirección Ip objetivo y rport que es el puerto que tiene el servicio vulnerable, para este caso el 80.

Imagen 15. Explotación de la Vulnerabilidad



Fuente: elaboración propia.

Finalmente, se muestra en color naranja como se configura el rhost y en color azul el comando exploit para que se ejecute y se muestre el acceso a la maquina objetivo mediante una Shell meterpreter.

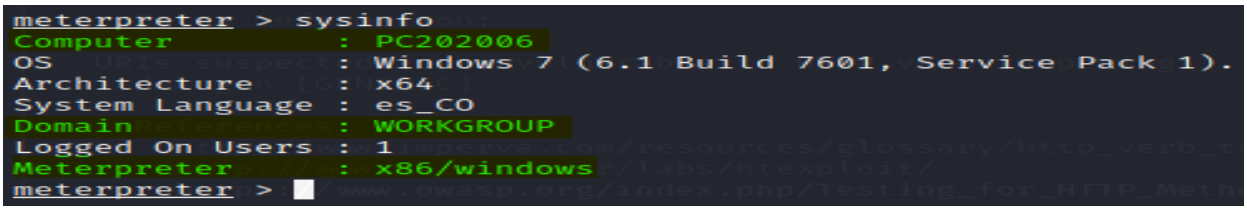
- **Post-Explotación**

Para esta fase del pentesting, se utiliza la herramienta Metasploit con la Shell meterpreter para la ejecución de comandos. Se obtiene mediante la carga de un payload que se ejecuta con el exploit que se ha utilizado, para sistemas Windows se suele utilizar Windows/meterpreter/reverse_tcp. Lo que hace es que la víctima inicia sesión mediante una Shell hacia el equipo del atacante y este la puede controlar remotamente[27].

Comandos utilizados:

- Sysinfo: permite ver la información del sistema que fue atacado, como el nombre del host, sistema operativo, arquitectura, usuarios logueados.
- Getuid: permite ver el tipo de usuario que esta logueado
- Shell: permite el ingreso a la Shell de comandos del sistema cmd
- Dir: lista los archivos y directorios que están en la carpeta

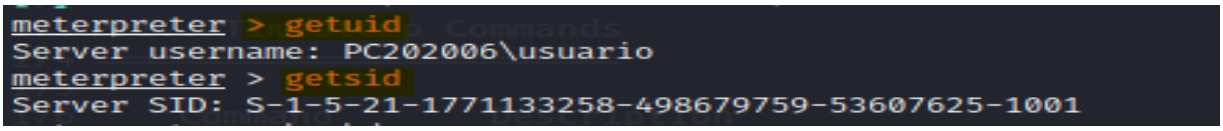
Imagen 16. Identificando el Sistema Operativo Atacado



Fuente: elaboración propia.

Se procede a realizar la verificación del sistema operativo atacado y sus principales características.

Imagen 17. Verificando privilegios de acceso

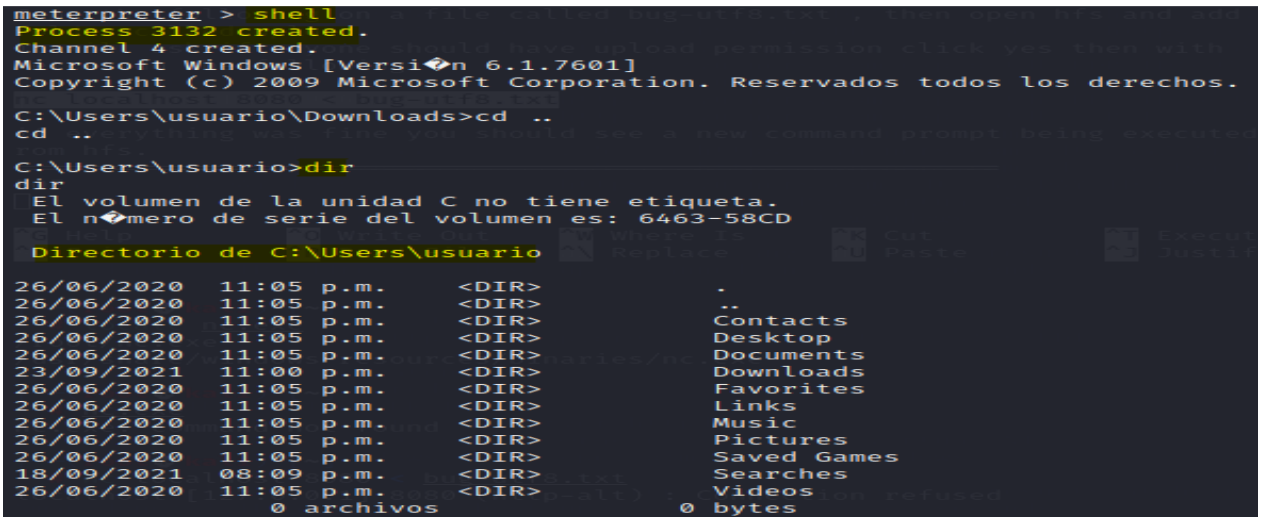


Fuente: elaboración propia.

[27] 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. 3Ciencias, editor. Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L.; 2018. 124 p.

Se continua con la verificación de los privilegios con los cuales se ha logrado tener acceso, para el caso fue con usuario sin privilegios **PC202006\usuario.**

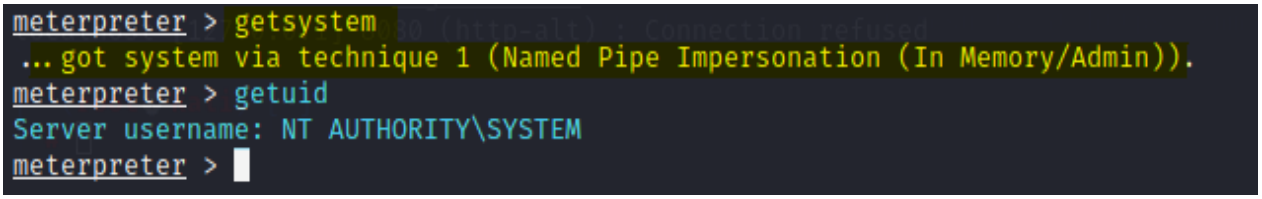
Imagen 18. Recopilando información del usuario en su PC



Fuente: elaboración propia.

Se procede a revisar que tipo de información guarda el usuario y si se encuentra algo que interese al atacante. Se ingresa el comando Shell para acceder a la consola de comandos CMD de la maquina Windows x64 y revisar los directorios en busca de información confidencial.

Imagen 19. Escalando Privilegios

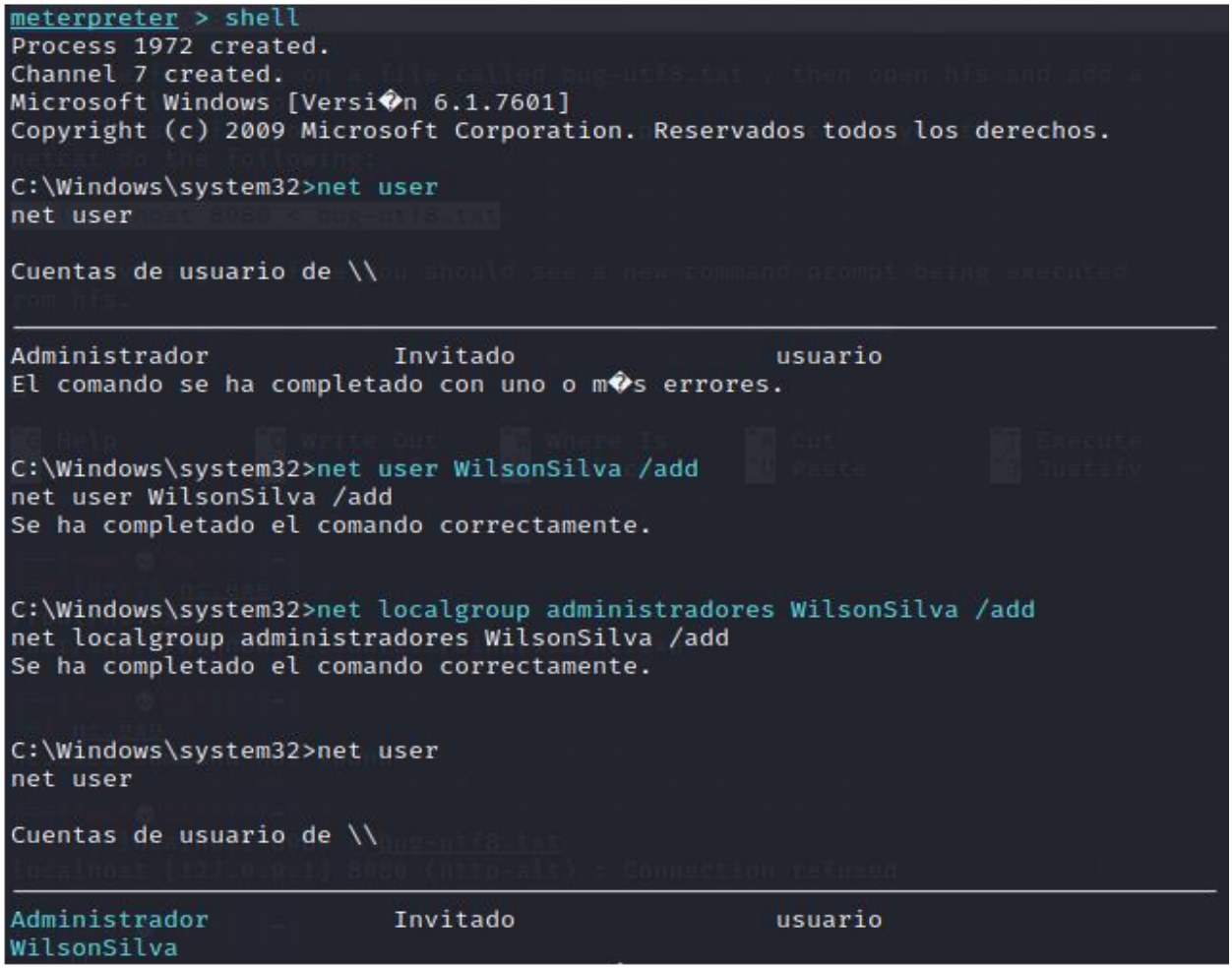


Fuente: elaboración propia.

Se realiza mediante el comando getsystem, escalada privilegios para poder ingresar a la maquina windowsx64 como usuario administrador. Se ha logrado escalar privilegios, la parte resaltada de amarillo indica el comando utilizado y la confirmación de que se ha obtenido el sistema. La parte resaltada de azul muestra el nombre de usuario **NT AUTHORITY/SYSTEM**, es decir, se ha ingresado como usuario administrador.

1. Se procede a la creación de un usuario, primero se ingresa mediante el comando **Shell** a la consola de comandos CMD de la maquina Windowsx64, se comprueba que usuarios existen con el comando **net user.**

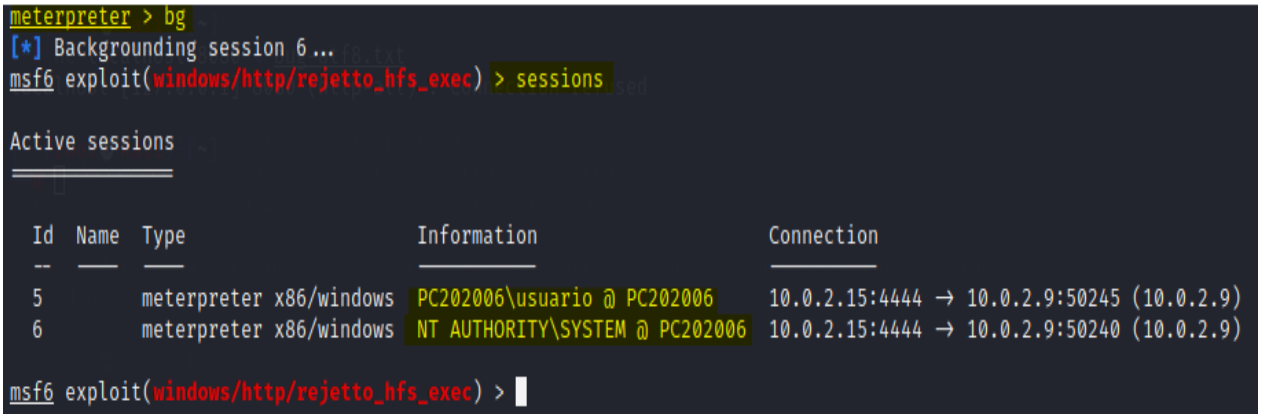
Imagen 20. Creando usuario Administrador



Fuente: Elaboración propia.

Seguido, se procede con la creación del usuario mediante el siguiente comando net user WilsonSilva /add. Una vez se ha creado satisfactoriamente, se otorgan los privilegios de administrador mediante el comando net localgroup administradores WilsonSilva /add. Se comprueba que el usuario ha sido creado como administrador

Imagen 21. Verificando sesiones abiertas



Fuente: Elaboración propia.

Con el comando bg se vuelve a metasploit y se verifican las sesiones que se tienen abiertas, una como usuario estándar **(PC202006\usuario),** y la otra con usuario administrador **(NT AUTHORITY\SYSTEM).**
Esto demuestra, que se ha logrado tener el control total de una maquina Windows con arquitectura x64 debido a una falla en una aplicación File Server que utilizaba una versión vulnerable.

5.4 ESTRATEGIAS DE CONTENCIÓN

5.4.1 Ataque en tiempo real

Al encontrarse un ataque en tiempo real, es necesario desconectar de la red el, o los equipos que pueda identificar o cree han sido afectados. Se debe considerar que posiblemente ya se ha podido extraer información, afectar algún activo critico o hacer algún daño a un equipo, por tanto, se debe iniciar la valoración de los activos y la valoración del impacto de lo sucedido.

En cuanto a indagación se debe iniciar por encontrar el punto débil, saber dónde ingreso el ataque, qué llevo a que se pudiera ejecutar, cómo se realizó, quién permitió que se produjera el ataque. En cuanto a lo que se debe hacer es:

- Preservar la máquina o activos afectados: esto para hacer copia de los Discos, volcado de RAM, y aplicación de técnicas forenses para identificar el o los atacantes.

- Documentar: se debe realizar la documentación de las evidencias recolectadas, esto se puede hacer mediante el uso de cadena de custodia[28].
- No instalar herramientas remotas u otras que puedan afectar el sistema atacado.
- Revisión de Logs de sistema, se debe realizar por parte de un experto con las herramientas adecuadas para no afectar la integridad del activo afectado.
- Revisión de copias de seguridad (Backups): se deben revisar las ultimas copias de seguridad que se hayan realizado del sistema para su posterior recuperación

5.4.2 Medidas ante el ataque del Red Team

Debido a que el ataque se ejecutó por la vulnerabilidad que presenta una aplicación instalada en la maquina Windows X64, las medidas de hardenización propuestas para que el ataque no se repita serían las siguientes:

- Actualización del Sistema Operativo: Mantener actualizado con la última versión el sistema operativo, ya que cada actualización va presentando mejoras en rendimiento y en seguridad.
- Actualización de Aplicaciones: Las aplicaciones que se instalan en las máquinas para cualquier actividad, a menudo sus desarrolladores van realizando cambios en rendimiento, seguridad, presentación y otros aspectos, por tanto, se debe estar al día con las actualizaciones y más si se conoce alguna versión con vulnerabilidades asociadas a ejecución remota de comandos u otro tipo de vulnerabilidad.
- Control de puertos TCP/UDP: se debe controlar que puertos están abiertos, y a que servicios están asociados, solo debe estar abierto el puerto necesario para el servicio requerido, se recomienda cambiar los puertos por defecto utilizando otros poco frecuentes pero que sean reconocibles al servicio. Si una aplicación para su funcionamiento requiere un puerto, generalmente abre uno por defecto, lo recomendable es cambiar este puerto.
- Control de Acceso Remoto: Se debe habilitar únicamente si el administrador lo requiere, debe tener un usuario sin privilegios de administrador para que no lo pueda habilitar.
- Gestión de usuarios: se debe tener en cada maquina un usuario administrador con acceso mediante contraseña robusta y cambios periódicos para la administración del equipo. Un usuario invitado con acceso mediante contraseña robusta, cambios

[28] Colombia. MINTIC. Guía para la Implementación de Seguridad de la Información en una MIPYME. Seguridad y Privacidad de la Información [En Línea]. 2016; Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

periódicos y privilegios mínimos que solo permitan la realización del trabajo asignado.

- Antivirus: contar con un antivirus con licencia y actualizado a diario.
- Firewall: mantener activado el firewall de cada máquina con las reglas de filtrado acordes a las necesidades del usuario.

5.4.3 Diferencias Blue Team Vs Equipo Gestión de Incidentes

La siguiente tabla presenta las diferencias entre un Blue Team y un equipo de respuesta y gestión de incidentes.

Tabla 3. Blue Team Vs Equipo de Respuesta a Incidentes

BLUE TEAM	EQUIPO RESPUESTA INCIDENTES
• Gestión de vulnerabilidades	• Gestión de incidentes
• Remediación de Vulnerabilidades	• Remediación de incidentes
• Crear plan de remediación de Vulnerabilidades	• Crear un plan de remediación de incidentes
• Recolección y análisis de las vulnerabilidades encontradas	• Recolección y análisis de evidencia digital
• Detección de ataques avanzados: Estar al tanto de los avances y nuevos ataques, evitar APT (Amenaza avanzada persistente)	• Auditoria y trazabilidad de Seguridad Informática: analizar brechas de seguridad

Fuente: elaboración propia.

5.4.4 Funciones y Características de un SIEM

SIEM (Gestión de Eventos e Información de Seguridad) es una herramienta que permite recolectar de forma centralizada toda esa información que envían los dispositivos de seguridad o inclusive los dispositivos de red. Se encarga de analizar, normalizar, correlacionar y alertar, de tal forma que se puedan medidas frente a esas posibles amenazas que están pasando en la red[29].

[29] Avansis. SIEM Qué es, funcionamiento y cómo integrarlo con éxito [En Línea]. Ciberseguridad. 2020 [citado 4 de octubre de 2021]. Disponible en: https://www.avansis.es/ciberseguridad/siem-que-es/?cn-reloaded=1.

Características básicas de un SIEM

- **Recolectar información**: recibe información de diferentes tipos de dispositivos y diferentes logs
- **Normalizar la información**: la información debe tener la misma fecha y hora de modo que permita realizar una búsqueda de manera más fácil.
- **Analizar la información**: hacer correlación, es decir, analizar la relación que existe entre una o dos variables o datos de los logs
- **Módulo de gestión**: permite administrar la solución y visualizar en tiempo real las alertas generadas.

Funciones avanzadas de un SIEM:

- **Análisis de comportamiento y aprendizaje**: consiste en aprender el comportamiento normal de la red y de un usuario en específico y en caso de detectar algún tráfico diferente generar una alerta que permita tomar las medidas necesarias para detectar la amenaza.
- **Respuesta inteligente**: hacer la integración con varios dispositivos de seguridad y tener acciones automáticas sobre los dispositivos los cuales nos permitan contener los ataques que se están generando.
- **Monitoreo de integridad de archivos y registros**: consiste en realizar un monitoreo constante a los archivos que transitan por la red para garantizar su integridad.
- **Módulo de gestión de casos**: D permite visualizar alertas y también ver y gestionar los logos de todas las acciones que se realizan durante el proceso de mitigación de alertas.
- **Integración con dispositivos de colección profunda**: permite llegar un poco más allá de la información que nos pueden entregar los dispositivos de red.

5.4.5 Herramientas de Contención de ataques informáticos

1. **Proxy:** es un software el cual se instala en una máquina servidor y éste es generalmente lo que haces configurarse para que controle todo lo que viaja por el navegador web se puede hacer filtrados para acceso a una página cifrar la información comunicación de canales y se puede garantizar que los usuarios naveguen por sitios seguros y confiables para la organización[30].

[30] Bellido Quintero E. Equipos de interconexión y servicios de red (UF1879) [En Línea]. IC Editorial; 2016. 313 p. Disponible en: https://elibro.net/es/lc/unad/titulos/44151.

2. **IDS/IPS**: son dispositivos que se encargan de verificar el tráfico en la red y analizar su comportamiento en el momento en que identifican alguna anomalía generan una alerta y de acuerdo con su configuración pueden hasta corregirla existen varios tipos de IDS, es por ejemplo el de red (NIDS). Una vez que captura y analiza los paquetes verifica y busca patrones que puedan suponer algún ataque analizar el tráfico de la red y buscan opciones no permitidas de acuerdo a las reglas que se le han configurado además emiten alertas cuando hay intentos de acceso o se prevé alguna vulnerabilidad[31].
3. **Firewall o Cortafuegos:** son herramientas tanto de hardware como software en las cuales se configuraron una serie de reglas de filtrado tanto de paquetes como de direcciones IP para controlar el tráfico que entra y sale de la red. los hay de red que van dentro de la red y los hay perimetrales que están más hacia el tráfico que entra hacia la organización que viene desde internet. Un farol realiza varias funciones entre ellas accesos no autorizados por ejemplo a través de conexiones eh intentos fallidos de inicio de sesión analiza y comprueba fallos de autentificación bloquea el tráfico de direccionamiento IP no usado con frecuencia y generar reportes sobre accesos sospechosos[32].

[31] Chicano Tejada E. Gestión de incidentes de seguridad informática (MF0488_3) [En Línea]. IC Editorial; 2015. 317 p. Disponible en: https://elibro.net/es/lc/unad/titulos/44101.
[32] Guijarro Rodríguez AA, Mendoza Moran V, Veloz Rodríguez AH. Guía de Administración de Servicios GNU/Linux CentOS7 [En Línea]. Editorial Universitaria; 2020. 175 p. Disponible en: https://elibro.net/es/lc/unad/titulos/151759.

CONCLUSIONES

- El conocer que leyes aplican y existen sobre ciberseguridad y protección de datos personales, es muy importante para un profesional dedicado preservar los pilares de la información en una empresa cualquiera que sea; esto, le permitirá actuar conforme a estas leyes y de paso su actuación estará ligada al código de ética de la ingeniería y sus profesiones afines. Por tanto, se concluye que todo profesional no solo en el ámbito de la seguridad informática sino de todas las áreas, debe conocer la legislación para estar al tanto del alcance de sus actuaciones profesionales.
- El previo conocimiento de la legislación permite que al momento de encontrarse firmando un contrato o un acuerdo de confidencialidad como el caso de estudio, se pueda tener la seguridad de lo que va a hacer, el desconocimiento de la norma no exime de la culpa, por tanto, una vez se firme, se actúa en contra del código de ética y se hace acreedor de sanciones que pueden llevar hasta a perder la oportunidad de ejercer la profesión de la ingeniería. Para los Red Team y Blue Team, es de vital importancia estar al día en materia legislativa y asesorados en acuerdos de confidencialidad para que sus funciones dentro de las compañías se puedan llevar a cabalidad en entornos éticos y bajo criterios legales, conociendo el alcance desde su posición en la defensa y ataque de sistemas informáticos que ayuden a mitigar la perdida de información por parte de ciberdelincuentes.
- Comprender la manera como se realiza un ataque a un sistema informático mediante las fases del pentesting y con el uso de herramientas por parte del Red Team, permite identificar claramente el alcance que puede tener si lo realiza un agente externo con fines maliciosos, en el ataque que se describió, se pudo evidenciar que se puede extraer información y hasta la creación de un usuario con privilegios de administrador que podrá acceder a otros equipos en la red y causar daños más grandes para la compañía, acción que puede generar hasta el cierre definitivo de esta si no se tiene un plan de contingencia definido y una respuesta a incidentes clara y actuando enseguida se da a conocer la intrusión.
- Una vez se logra la identificación de un ataque en tiempo real, se debe iniciar el proceso de aislamiento de la red de los posibles sistemas informáticos afectados, se debe activar la respuesta a incidentes e iniciar el proceso de recolección de evidencias garantizando la cadena de custodia para lograr hallar a los culpables y la manera como accedieron a los sistemas de la compañía. Es importante revisar las configuraciones de seguridad, iniciar el proceso de hardenizacion que consiste en incrementar las medidas de seguridad mediante la actualización a su última versión de los sistemas operativos que ya traen modificaciones de seguridad, actualización de aplicaciones que se utilizan en las actividades diarias y desinstalar las que no se utilizan. El Blue Team realiza un análisis de vulnerabilidades genera informes con las posibles remediaciones y estas deben ser atendidas lo antes posible para evitar nuevos ataques. El equipo de respuesta a incidentes se encarga del análisis y recolección del incidente. Se puede

evidenciar que sus funciones son diferentes, pero están encaminadas a mantener segura la información.

RECOMENDACIONES

- Estar al tanto de la legislación, constantemente cambia, se modifican artículos o la ley completa, se crean decretos reglamentarios que ayudan a entender e interpretar mejor la norma y actuar conforme esta lo estipule para evitar sanciones.
- Estar siempre enalteciendo la profesión de la ingeniería y sus profesiones afines conforme lo estipula el código de ética. Leer detenida y juiciosamente los acuerdos de confidencialidad antes de firmar, no dejarse presionar por afanes o por convencimiento de la contraparte, tener en cuenta que después de firmar no hay excusas y se debe cumplir lo estipulado, lo cual, podría generar sanciones por faltas leves, graves, gravísimas y hasta cárcel dependiendo el actuar.
- Ser consciente de lo que puede generar el sufrir un ataque a un sistema informático por un hacker con intenciones maliciosas, se deben intensificar los controles y aprovechar a los Red Team para conocer las tendencias en ataques informáticos y los Blue Team para conocer las ultimas amenazas y vulnerabilidades que deben afrontar.
- El incluir a los equipos red y Blue Team como parte integral del equipo de seguridad de la información en las empresas generará un impacto positivo hacia los clientes y proveedores, quienes podrán evidenciar que hacen transacciones con una empresa protegida ante ciberataques. Este impacto también acarrea que la empresa se mantenga en el tiempo, una transformación digital permitirá que se abran nuevos mercados en línea con operaciones y transacciones seguras, estas serían atacadas por los Red Team y monitoreadas por los Blue Team para garantizar los pilares de la seguridad de la información, integridad, disponibilidad y confidencialidad.
- Invertir en seguridad informática, en ocasiones, resultaría más económico esta inversión que tener que levantarse de un ataque, no se debe tomar como un gasto sino como una inversión; los Red y Blue Team pueden ayudar en la generación de proyectos de inversión que permitan crecer en materia de seguridad informática en las empresas.

ANEXO 1

Link Video Sustentación

https://youtu.be/inDXURcaE3A

BIBLIOGRAFÍA

Alcaldía de Bogotá. *Guardianes de La Información Penetration Testing*. *Alcaldía de Bogotá*. Bogotá D.C: Alcaldía de Bogotá, 2018. https://doi.org/10.17148/ijarcce.2014.31023

Avansis. "SIEM Qué Es, Funcionamiento y Cómo Integrarlo Con Éxito." Ciberseguridad, 2020. https://www.avansis.es/ciberseguridad/siem-que-es/?cn-reloaded=1

Bellido Quintero, Enrique. *Equipos de interconexion y servicios de red (UF1879)*. IC Editorial, 2016. https://elibro.net/es/lc/unad/titulos/44151

BID. MinTic. OEA. "Impacto de Los Incidentes de Seguridad En Colombia 2017." *Organización de Los Estados Americanos* 66, no. 2–3 (2017): 130. https://doi.org/10.1007/s11159-020-09831-4

Castro Vásquez, Carlos Arturo. "Pruebas de Penetración e Intrusión." *Technological Innovations*. Bogotá D.C: Facultad de Ingenierías, 2019. http://repository.unipiloto.edu.co/handle/20.500.12277/6273

CCIT. Policía Nacional de Colombia. "Tendencias Cibercrimen Colombia 2019-2020." n.d. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Chicano Tejada, Ester. *Gestion de incidentes de seguridad informatica (MF0488_3)*. IC Editorial, 2015. https://elibro.net/es/lc/unad/titulos/44101

Colombia. Congreso de la República. "Ley 1341 DE 2009." *Diario Oficial No. 47.426 de 30 de Julio de 2009*, 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Colombia. Congreso de la República "Ley 1581 de 2012." *Diario Oficial No. 48.587 de 18 de Octubre de 2012*, 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Colombia. Congreso de la República "Ley 1928 2018." *Diario Oficial No. 50.664 de 24 de Julio de 2018*, 2018. http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

Colombia. Congreso de la República "Ley 1978 de 2019." *Diario Oficial No. 51025 de 2019*, 2019. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=85632

Colombia. Congreso de la República “Ley 599 de 2000” Diario Oficial No. 44.097 de 24 de julio de 2000, 2000. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Colombia. Congreso de la República “Ley 1273 de 2009” Diario Oficial No. 47.223 de 5 de enero de 2009, 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Colombia. Copnia. “Código de ÉTICA Para El Ejercicio de La Ingeniería En General y Sus Profesiones Afines y Auxiliares.” *Consejo Profesional Nacional De Ingenieria* 1, no. CODIGO DE ETICA (2014): 20. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

Colombia. MINTIC. “Guía Para La Implementación de Seguridad de La Información En Una MIPYME .” *Seguridad y Privacidad de La Información*, 2016. http://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf

Colombia. Presidencia de la República. “Documento Conpes 3701.” *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA*, 2011. https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

Colombia. Presidencia de la República. “Documento Conpes 3995.” *Politica Nacional de Confianza y Seguridad Digital*, 2016. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf.

CSIRT-cv. “Nmap 6: Listado de Comandos,” 2018, 1–6. http://www.csirtcv.gva.es.
Escriva Gasco, Gema. *Seguridad informatica*. Macmillan Iberia, S.A., 2013. https://elibro.net/es/lc/unad/titulos/43260

Guijarro Rodriguez, Alfonso Anibal, Veronica Mendoza Moran, and Angel Humberto Veloz Rodriguez. *Guia de Administracion de Servicios GNU/Linux CentOS7*. Editorial Universitaria, 2020. https://elibro.net/es/lc/unad/titulos/151759

Kaspersky. “¿Quién Le Espía? Ninguna Empresa Está a Salvo Del Ciberespionaje.” kaspersky, 2020. https://media.kaspersky.com/es/business-security/Cyber_Espionage_WhitePaper_FINAL_ES.pdf

Luz, Sergio de. “Cómo Realizar Un Escaneo de Puertos En Windows Con TCPing.” RedesZone, 2021. https://www.redeszone.net/tutoriales/configuracion-puertos/tcping-escaner-puertos-windows/.

Ortega Candel, Jose Manuel. *Hacking etico con herramientas Python*. RA-MA Editorial, 2018. https://elibro.net/es/lc/unad/titulos/106513.

Rizaldos Héctor. “Qué Es Metasploit Framework.” OpenWebinars, 2018. https://openwebinars.net/blog/que-es-metasploit/

Romero Castro, Martha Irene, Grace Liliana Figueroa Morán, Denisse Soraya Vera Navarrete, José Efraín Álava Cruzatty, Galo Roberto Parrales Anzúles, Christian José Álava Mero, Ángel Leonardo Murillo Quimiz, and Miriam Adriana Castillo Merino. *Introducción a La Seguridad Informática y El Análisis de Vulnerabilidades*. Edited by 3Ciencias. *Introducción a La Seguridad Informática y El Análisis de Vulnerabilidades*. Editorial Área de Innovación y Desarrollo,S.L., 2018. https://doi.org/10.17993/ingytec.2018.46

Tamboli, Anand. “Cybersecurity: Supervising Your AI With The Red Team.” *Electronics for You*, June 20, 2020. https://search.proquest.com/docview/2415851338?accountid=48784

.