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

RAUL ALBERTO GUAPACHO LAGUNA

UNAD – Universidad Nacional Abierta y a Distancia
ECBTI - Escuela de Ciencias Básicas, Tecnología e Ingeniería.
Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team
Bogotá DC
2020

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

RAUL ALBERTO GUAPACHO LAGUNA

Presentar informe técnico

.

DIRECTOR DE CURSO: JOHN FREDDY QUINTERO

UNAD – Universidad Nacional Abierta y a Distancia
ECBTI - Escuela de Ciencias Básicas, Tecnología e Ingeniería.
Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team
Bogotá DC
2020

CONTENIDO

RESUMEN

En el presente documento se esbozan las principales leyes y decretos existentes en Colombia frente a delitos informáticos, de igual manera que es el pentesting y cuál es la forma como se realiza y las diferentes herramientas que se pueden emplear para tal propósito.

Además, mostrar las facetas de un actuar ético enmarcado en la legalidad, mostrando las diferentes facetas de un profesional al momento de aceptar o no labores que implican recibir una buna cantidad de dinero o mantenerse en su postura de un profesional recto, honesto y legal.

Junto a la recreación de pasos o etapas que permiten identificar las vulnerabilidades de un sistema por medio de herramientas que acompañen procesos que enmarcados dentro de metodologías y técnicas que permiten de forma intrusiva atacar un sistema vulnerable.

Mostrando de igual manera algunas herramientas empleadas para poder contener de la mejor manera posible ataques informáticos contra infraestructuras de información, o por lo menos atenuar el impacto de estos frente a la organización.

PALABRAS CLAVE: Leyes contra delitos informáticos, pentesting, pruebas de penetración, herramientas de ciberseguridad, ética, ilegalidad, confidencialidad, información, divulgación, acuerdo, Intrusión, vulnerabilidad, framework, victima, explotación, Hardening, Blue team, SIEM, CIS, CSIRT, contención, ataques.

GLOSARIO

Pentesting: También reconocido como *test de penetración* está proyectado para establecer la gravedad de los defectos de seguridad de un sistema. además, es la practica principal y de mayor demanda hoy por hoy, porque con estas pruebas, las compañías logran develar los riesgos a que se expone y cuál es el grado de validez y robustez de sus escudos de seguridad.[1]

Ética profesional: La ética profesional hace referencia al conjunto de normas y valores que mejoran el desarrollo de las actividades profesionales. Es la encargada de determinar las pautas éticas que deben regir dentro del ambiente laboral. Estas pautas están basadas en valores universales que poseen los seres humanos.[2]

Hardening: También llamado endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema. Esto se consigue, estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático. Este consiste en endurecer el sistema, con el fin de reducir y evitar las amenazas y los peligros de este.[3]

Delito informático: Los delitos informáticos son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc.[4]

[1] https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting
[2] https://concepto.de/etica-profesional/#ixzz6b2lZIJCK
[3] https://www.ciset.es/publicaciones/blog/746-hardening
[4] https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

INTRODUCCIÓN

El auge, evolución y preponderancia de la tecnología en todos los espacios de la sociedad y sobre todo en el nivel empresarial, han hecho emerger conductas ilegales llamados delitos informáticos, generando un espectro amplio de peligros informáticos, es donde diversas disciplinas como la legal y técnicas, han generado la regularización de estas actividades y su catalogación como ilícitas para así puedan ser penalizadas.

Estas situaciones han conducido a las organizaciones a buscar medidas para protegerse frente a esta ilegalidad, y es de allí donde han surgido las pruebas de penetración, dado que las organizaciones necesitan conocer su estado real frente a vulnerabilidades del tipo sistemas de información y así tomar medidas de contención frente a estos fallos.

Para ello se pueden usar herramientas de toda índole pagas, gratuitas, online, etc. Cada una ofrece diferentes ámbitos de trabajo, y cada una de ellas apunta a determinar diferentes vulnerabilidades, pero estas deben funcionar como un conjunto una suite para realizar pruebas de penetración lo más robusto y acertado posible para así lograr identificar las falencias que este aspecto tiene una organización.

El creciente uso de la tecnología en todas las labores cotidianas del ser humano ha permitido que las ocasiones de ser atacados por delincuentes que con mucho sigilo logran descubrir la manera de irrumpir en un sistema informático que por omisión u error se encuentre vulnerable. Las organizaciones deben tener las suficientes herramientas y técnicas implementadas para contener estos ataques y ofrecerles a las organizaciones la tranquilidad frente al manejo y conservación de la información como activo principal del funcionamiento de esta.

OBJETIVOS

OBJETIVO GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

- Construir un informe técnico donde se presenten las estrategias RedTeam & BlueTeam.

DESARROLLO DEL INFORME

Aspectos relevantes actividad 1.

En Colombia existen leyes que propenden por la protección de datos personales y penalizar los delitos informáticos entres estas están:

- Ley 1273 de 2009: Modificación del código penal, y preservación de los sistemas informáticos. [5]
- Ley 1581 de 2012: Brindar la garantía y seguridad a cualquier clase de dato pertenecientes a los individuos que son recopilados por las empresas. [6]
- Decreto 1317 de 2013: Reglamentación parcial y definición la ley 1581 de 2012. [7]
- Ley 1928 de 2018: Aprobación el convenio europeo sobre ciberdelincuencia. [8]

El pentesting es una colección de procesos definidos que como metodología se centra en arremeter contra entornos o sistemas con el propósito de descubrir y mitigar potenciales fallas en el mismo, es la practica principal y de mayor demanda hoy por hoy, porque con estas pruebas, las compañías logran develar los riesgos a que se expone y cuál es el grado de validez y robustez de sus escudos de seguridad.

Se puden identificar 3 clases de Pentesting de acuerdo all tipo de información con que se cuenta:

Pentesting de caja blanca "White Box"
Estas pruebas se hacen al interior de la organización, y conoce a profundidad la composición y estructura de los sistemas a testear.

Pentesting de caja negra "Black Box"
Estas pruebas no pertenecen a la organización, y se debe asumir el rol de delincuente informático, y se debe tener la destreza y habilidad para identificar amenazas dentro de la estructura de red de la organización.

Pentesting de caja gris "Grey Box"
Estas pruebas son una combinación de los 2 anteriores, ya que no se parte de la nada, pero no se tiene toda la información atinente a la estructura informática de la empresa.

La labor de un Pentester se organiza en pasos definidos y delimitados, para así alcanzar el éxito en cuanto a los hallazgos de riesgos de seguridad, y se pueden enumerar de la siguiente manera:

Determinar Auditoría
Esta etapa permite determinar con que información se cuenta, que tipo de pentest se debe realizar.

[5] https://www.habitatbogota.gov.co/transparencia/marco-legal/normatividad/ley-1273-2009
[6] https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf
[7] https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf
[8] http://www.suin-juriscol.gov.co/viewDocument.asp?id=30035501

Recogida de información
Esta etapa identificada como de reconocimiento, se exploran diversas situaciones, como el proceder de los empleados, el funcionamiento del entorno, etc. Entre mayor sea el detalle mejor. Nmap (escaneo de puertos), FOCA (análisis de metadatos), PassiveRecon (para webs) son algunos programas que se pueden usar en esta.

Acceso al sistema

En esta etapa se puede reconocer dos niveles de desarrollo secuenciales y que se realizan una vez se identifique plenamente el sistema, y se tenga recopilada una cantidad alta de información:

- **Búsqueda de vulnerabilidades.** Identifica los posibles fallos de seguridad buscando dentro de la información obtenida, esta fase es mejor de forma manual, Acunetix, Nessus son algunos programas que se pueden usar en esta.

- **Explotación de vulnerabilidades.** Después de identificar las posibles fallas de seguridad, se intenta explotarlas usando herramientas como: SQL injection, Metasploit.

Elaboración del informe
En esta etapa se plasma el detalle de los hallazgos, cuales vulnerabilidades fueron encontradas, como fueron explotadas, que alcance tienen y como impactan a la empresa, además de las herramientas usadas durante el desarrollo de las pruebas, que técnicas se emplearon y las recomendaciones respectivas para minimizar y/o suprimir los riesgos de seguridad. [9]

Las herramientas de seguridad son de vital importancia y aquí algunas de ellas:

- **Metasploit:** Marco de trabajo open source, para la realización de pruebas de penetración, ofrece herramientas para ser utilizados dentro de cada fase, permitiendo el desarrollo de nuevos exploits y automatizar tareas.[10]
- **Nmap**: Herramienta free y open source para explorar vulnerabilidades y detectar redes, es básicamente un scanner de puertos que recopila información de estos abiertos, cerrados y/o asegurados.[11]
- **OpenVas**: Agrupación de servicios y funcionalidades de escaneo y detección de fallos de seguridad. Es gratuita y permite analizar y gestionar riesgos de seguridad.[12]

Servicios en línea:

- **ExploitDB**: Sitio Web donde hackers publican vulnerabilidades conocidas de aplicaciones y como explotarlas, entregando detalles específicos. Estas pueden ser descargados desde línea de comandos y usando un backup del sitio, efectuar búsquedas fuera de línea.[13]

---

[9] https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting
[10] https://eliezermolina.net/que-es-y-para-que-sirve-metasploit-framework/
[11] https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/
[12] https://www.ecured.cu/OpenVas
[13] https://hackingpills.blogspot.com/2018/06/exploit-db-buscando-exploits-desde-la_23.html

- **CVE**: Listado estándar de vulnerabilidades y fallos de seguridad comunes, este es sostenido bajo la colaboración y esfuerzo común de representantes de organizaciones asociadas a la seguridad informática en el mundo.[14]

Aspectos relevantes actividad 2.

Dentro de las ramas de la seguridad informática es necesario contar con personal capacitado e idóneo, es por ello que los profesionales deben enmarcar su actuar dentro de procesos éticos y legales de manera constante y decidida, por convicción y no por la existencia de leyes, estatutos y/o códigos que así lo impongan, máxime cuando en nuestro país se requiere de un compromiso serio y decidido por parte de la sociedad para cambiar las costumbres nefastas que han generado un ambiente de zozobra generalizado, donde comúnmente se conoce como la ley del más vivo, es necesario desde lo profundo de los valores del ser humano tener un sentir diferente y así lograr que nuestro país tome un diferente y renovado rumbo que permita mostrar el verdadero potencial y la clase de personas que somos.

Conocer la legislación y saber interpretarla es fundamental por ello es necesario siempre estar muy seguros de como enfrentar las diversas y muy variadas situaciones que este devenir profesional prepara, los procesos y acuerdos enmarcados dentro de la ilegalidad están a la orden del día, el conocimiento y la interiorización de los postulados éticos como por ejemplo los establecidos en el **código de ética para ingenieros** de COPNIA, en los artículos 29, 35 literal B, que nos permiten asegurar que un ingeniero no es solo un profesional o una persona con un título es un ser humano que dentro de su quehacer debe aplicar una serie de postulados éticos y actuaciones que propendan por cumplir en toda la extensión de la palabra ETICA con todas las exigencias sociales y legales que enaltezcan su profesión, no cambiando dinero por integridad o posición social por rectitud de proceder.

Aspectos relevantes actividad 3.

Basados en el banco de trabajo montado como evidencia de la situación presentada en The Whitehouse Security, se realizan las fases o etapas del pentesting, así:

Determinar Auditoría: Fase llevada a cabo usando 2 máquinas virtuales bajos las mismas características de las usadas en la organización, ninguna de ellas tiene aplicada la actualización MS17_010, y sospechando de tener dentro de ellas el fallo de seguridad con identificador CVE-2017-0144. Estas imágenes suministradas son montadas, cada una por separado, pero dentro de un mismo segmento de red, usando la Herramienta Virtual Box.

[14] https://www.redhat.com/es/topics/security/what-is-cve

Recogida de información: Adicional dentro del mismo segmento de red se monta una maquina con SO Kali Linux, usando la Herramienta NMAP que viene dentro de las utilidades del mismo SO. Se determina la existencia de la vulnerabilidad dentro de las máquinas windows.

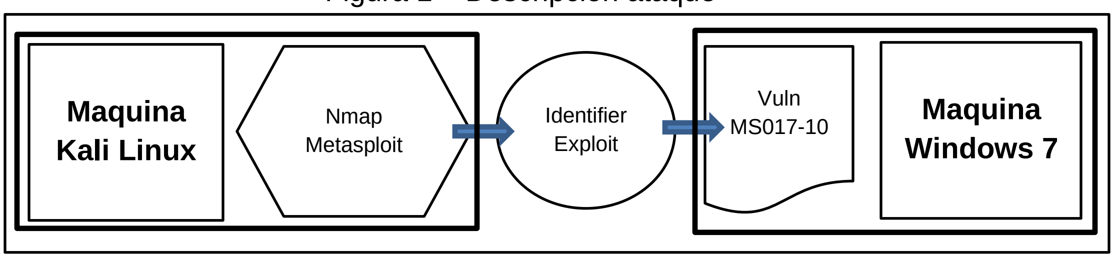
Acceso al sistema: Dentro de esta fase se utiliza el framework metaexploit que se encuentra dentro de la maquina Kali Linux, y siguiendo una serie de pasos estructurados se logra la intrusión y explotación de la vulnerabilidad.

Elaboración del informe: se logra determinar que las dos máquinas tienen el fallo de seguridad con identificador CVE-2017-0144, para la maquina X64 se explota usando el framework metasploit abriendo una Shell en el equipo víctima, la maquina víctima acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión. La máquina X86 no permite la explotación de la vulnerabilidad debido a su arquitectura.

La vulnerabilidad se resuelve instalando la actualización de seguridad de Windows del 14 de marzo de 2017 que resuelve el problema a través del parche de seguridad MS17-010.

La descripción del ataque en forma gráfica sería algo como lo siguiente:

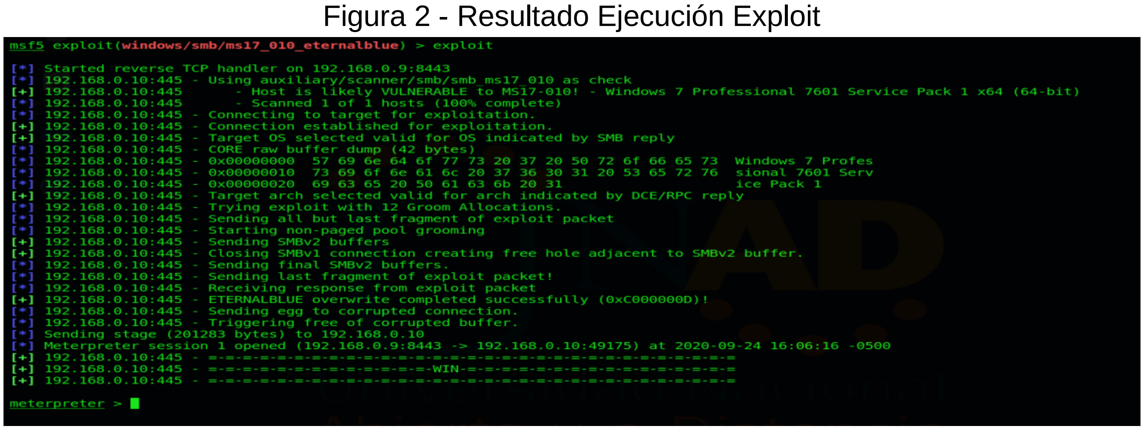
Figura 1 – Descripción ataque



Fuente: El autor

El resultado después de lograr explotar la vulnerabilidad es el siguiente, lograr por medio de un shell:

Figura 2 - Resultado Ejecución Exploit



Fuente: El autor

Figura 3 - Shell abierta maquina atacada

Fuente: El autor

Aspectos relevantes actividad 4.

Para minimizar el impacto al enfrentar un ataque informático, es necesario emprender una serie de acciones entre las cuales se pueden enumerar e identificar las siguientes:

- Hardenizacion: tiene como fin entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad. [15]

- Creación de equipo Blue Team: está conformado por expertos en seguridad especializados en analizar cómo se comportan los sistemas informáticos de una empresa estudiando los comportamientos y determinando cualquier vulnerabilidad que pudo ser omitida por los demás sistemas de seguridad, observando de forma minuciosa la circulación de datos, la conducta de sus sistemas, la raíz y nodos de las conexiones y las labores que los usuarios realizan de forma usual. [16]

- Creación de equipo de respuesta a incidentes informáticos: recibe informes sobre incidentes de seguridad presentado, analiza estas situaciones y responde sobre cómo actuar frente a estas amenazas, reaccionando para eludir casi que el 100% de los riesgos existentes.[17]

- Implementación de CIS (Center For Internet Security): fuente de información alimentada y nutrida con ataques reales y acciones auténticas son una excelente base documental de respaldo para las implementaciones futuras de seguridad al interior de la empresa. [18]

- Implementación de un SIEM: sistema usado para anticipar respuestas y contrarrestando las amenazas de seguridad, combinando funciones de un sistema **GIS** (**Gestión de Información de Seguridad**) y un **GES** (**Gestión de Eventos de**

[15] https://blog.smartekh.com/que-es-hardening
[16] https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja
[17] https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT
[18] https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

Seguridad) estableciendo una adecuada correlación entre las eventualidades suscitadas y la notificación de estas. [19]

- Ejecución de herramientas de contención: entre muchas otras Firewall, Proxy e IDS(Sistema de Detección de intrusos).

[19] https://sofecom.com/que-es-un-siem/

CONCLUSIONES

Las leyes colombianas, aunque existen, y desde ya hace algún tiempo, son laxas y se pueden considerar como letra muerta porque, aunque son un gran esfuerzo por castigar este tipo de actuaciones no generan la confiabilidad necesaria como para indicar que cuando estas situaciones ilegales se presenten los delincuentes informáticos van a ser castigados dado que existe un desconocimiento total por parte de los entes legales frente a esta jurisprudencia.

Las pruebas de penetración permiten a las empresas tomar decisiones acertadas, correctas y en el momento adecuado frente a las vulnerabilidades o fallos de seguridad existentes en los sistemas de información de la organización.

Las herramientas de ciberseguridad son el respaldo y el apoyo adecuado para que las pruebas de seguridad y los ataques de hacking ético arrojen los resultados adecuados del real estado de las falencias de seguridad existentes en la empresa.

El desarrollo de la actividad profesional siempre debe estar y estará enmarcado dentro de procesos éticos y legales que buscan enaltecer el ejercicio de una labor en este caso particular el de la ingeniería por lo tanto siempre como personas que nos desempeñamos dentro de la sociedad en busca de propósitos y bienestar común y general, siempre debemos conocer la legislación y los códigos éticos que regulan la labor en la cual hemos adquirido conocimiento y generado destrezas como profesionales.

Dentro de las organizaciones se hace de vital importancia implementar medidas de contención para que de forma proactiva se prevean posibles situaciones que atenten contra los pilares fundamentales de la seguridad de la información, pero también tener guías y planes de actuación en caso de sufrir un ataque de tipo informático y así no tener que pasar por traumatismos en la operación normal de las organizaciones. Se debe pensar siempre que, aunque no se haya pasado por este tipo de situaciones en cualquier momento se pueden vivir y es necesario listos y preparados.

Existen herramientas Software y Hardware que intentan asegurar las condiciones adecuadas para la información dentro de una empresa y que por medio de la correcta utilización de estas podremos mitigar los impactos de ataques informáticos, pero debemos tener siempre presente que nunca estaremos 100% seguros y nunca serán demasiadas al implementarlas para lograr el propósito vital de la organización en cuanto a su funcionamiento.

Con la creciente oportunidad por parte de agentes que desean genera caos y pánico por medio de herramientas informáticas que atacan a los sistemas de cómputo, es imperioso mantener el sistema operativo actualizado y con los últimos parches de seguridad

suscitando una fundamental importancia dentro de las organizaciones ya que solo de este modo es posible evitar o por lo menos bajar a porcentajes bajos los problemas de vulnerabilidad y de funcionamiento óptimo del sistema operativo y por ende del conglomerado informático a que este pertenece, y así alejar las formas de querer vulnerar y atacar nuestros sistemas.

RECOMENDACIONES

Los equipos Red Team & Blue Team deben estar conformados por personas con un alto sentido ético y profesional, que sepan documentar y comunicar todos los procesos y los resultados en cuanto a vulnerabilidades encontradas. Y para cumplir con su misión y tener éxito en sus labores puede seguir las siguientes recomendaciones:

Informar sus conclusiones a la alta dirección

Además del área de TI o del CISO de la compañía, los Red Team deben tener comunicación directa con el CEO y la junta directiva, logrando así eliminar ciertos errores embarazosos en la gestión de la seguridad de la compañía que puede llevar a conclusiones de 'falsa protección.

Las compañías requieren de Red Teams externos

Aun contando con un grupo de defensa intrusiva dentro de la planta de personal, las compañías deben hacer uso de externos que no se vean permeados por la organización y sus políticas. la cultura interna no afecta el equipo externo que tiene un alcance definido, pero sin límites artificiales.

Los Red Team deben tener escenarios lo más real posible

Un problema de los equipos rojos es que la utilización de técnicas avanzadas que no son del todo acordes con la manera de atacar de los ciberdelincuentes más comunes. Por lo general, los Red Team tienen un líder que conoce más que los defensores y este debe utilizar herramientas muy populares, sino se presenta pérdida de la realidad.

Ahorra dinero definir claramente el alcance del ataque

Hay que definir qué está al alcance y qué no del Red Team. Esto es fundamental. Ya que así el equipo rojo no va a realizar actividades que no han sido definidas por parte de la compañía.

Acoplar al equipo rojo con el azul

El Blue Team debe intensificar su defensa cada vez que el equipo rojo actúa el azul está en funcionamiento, dado que el azul es el especializado en analizar el proceder de los sistemas de una organización y de los usuarios.[20]

[20] https://cso.computerworld.es/tendencias/pasos-para-que-los-red-team-tengan-exito-en-las-companias

ENLACE DEL VIDEO

https://drive.google.com/file/d/120L511CEZDRrLl1qhjcGxF_OuervmPNO/view?usp=sharing

BIBLIOGRAFÍA

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, 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: Presidencia de la república de Colombia. Bogotá D.C. 2009.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Presidencia de la república de Colombia. Bogotá D.C. 2012.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2013. En: Ministerio de comercio, industria y turismo. Bogotá D.C. 2013.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1928 (24, julio, 2018). Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. En: Presidencia de la república de Colombia. Bogotá D.C. 2018.

JASON FIRCH. Artículo. [Sitio WEB]. [27, septiembre, 2019]. Disponible en: https://purplesec.us/red-team-vs-blue-team-cyber-security/

GERARDO ELIASIB. Artículo. [Sitio WEB]. [2, abril, 2019]. Disponible en: https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

HÉCTOR RIZALDOS. Artículo. [Sitio WEB]. [22, octubre, 2018]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/

MARIN DE LA FUENTE. Artículo. [Sitio WEB]. [29, abril, 2019]. Disponible en: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

LEOPOLDO ÁLVAREZ HUERTA. Artículo. [Sitio WEB]. [30, mayo, 2014]. Disponible en: https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

CALEB BUCKER. Artículo. [Sitio WEB]. [5, septiembre, 2012]. Disponible en: https://www.exploit-db.com/docs/spanish/22954-[spanish]-penetration-testing---analisis-web---evaluacion-de-vulnerabilidades---explotacion.pdf

JEREMY TRINKA. Artículo. [Sitio WEB]. [15, abril, 2018]. Disponible en: https://medium.com/@jeremy.trinka/five-pentesting-tools-and-techniques-that-sysadmins-should-know-about-4ceca1488bff

GRUPO SMARTEKH. Artículo. [Sitio WEB]. [3, mayo, 2012]. Disponible en: https://blog.smartekh.com/que-es-hardening

IT DIGITAL SECURITY. Artículo. [Sitio WEB]. [30, mayo, 2018]. Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

MARGARET ROUSE. Artículo. [Sitio WEB]. [15, noviembre, 2019]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT

DANIEL FUERTES. Artículo. [Sitio WEB]. [28, noviembre, 2019]. Disponible https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html

IMF BUSINNESS SCHOOL. Artículo. [Sitio WEB]. [13, agosto, 2018]. Disponible en: https://blogs.imf-formacion.com/blog/tecnologia/que-significa-siem-y-como-funciona-201808/

YÚBAL FM. Artículo. [Sitio WEB]. [17, octubre, 2012]. Disponible en: https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

DANIEL CUNHA BARBOSA. Artículo. [Sitio WEB]. [2, enero, 2020]. Disponible en: https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

SILVIA EUGENIA MESA CORREA. Artículo. [Sitio WEB]. [4, agosto, 2016]. Disponible en: http://redesysegu.blogspot.com/p/tipos-de-proteccion-para-una-red.html

DANIEL MIESSLER. Artículo. [Sitio WEB]. [4, abril, 2020]. Disponible en: https://danielmiessler.com/study/red-blue-purple-teams/

JEFF PETTERS. Artículo. [Sitio WEB]. [15, junio, 2020]. Disponible en: https://www.varonis.com/blog/what-is-siem/

MARGARET ROUSE. Artículo. [Sitio WEB]. [11, junio, 2019]. Disponible en: https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT