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

JAVIER ANDRÉS ACOSTA IZARIZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA
TUNJA BOYACA
2020

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

JAVIER ANDRÉS ACOSTA IZARIZA

Director curso seminario especializado:
M.sc John Freddy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA
TUNJA BOYACA
2020

RESUMEN

La realización del presente trabajo relaciona la normatividad vigente del margen legal en Colombia sobre delitos informáticos y protección de datos personales, conceptos y metodologías de pruebas de intrusión a una organización junto con medidas de hardenización para evitar la vulneración a un sistema.

ÍNDICE

GLOSARIO

Activo de información: Cualquier información o sistema relacionado con el tratamiento de datos que tenga un valor para la organización. Desde procesos de negocio, aplicaciones, equipos informáticos, bases de datos, hasta redes o instalaciones, son objetos susceptibles de ser atacados para la organización.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Antispam: Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus: Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Backup: Copia de seguridad que se realiza sobre la información, con la finalidad de recuperar los datos en el caso de que los sistemas sufran daños o pérdidas accidentales de los datos almacenados.

CERT/CSIRT: Es el Centro de Respuesta a Incidentes de Seguridad Informática. Su función es prevenir, detectar y mitigar ataques a los sistemas informáticos.

Ciberdelito: El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Ciberseguridad: Conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, computadoras, programas y datos de ataques, daños o accesos no autorizados. En un contexto informático, incluye seguridad cibernética y física.

Cortafuegos (Firewall): Sistema de seguridad de software y/o de hardware colocados en los límites de la red empresarial con el objetivo de permitir o denegar

el tráfico de Internet, de acuerdo a un conjunto de normas y políticas de ciberseguridad.[1]

Exploit: Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

Firewall: Aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Hacker: Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

Informática Forense: Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Lista blanca o Whitelisting: La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software.

[1] Blog Grupo Atlas (Página Web). Diccionario: términos de seguridad de la información que debes manejar [En Línea] Recuperado de: < https://blog.atlas.com.co/diccionario-seguridad-de-la-informacion >

Parche de seguridad: Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.

Pen Testing: En español se conocen como "pruebas de penetración", en donde se intenta de múltiples formas burlar la seguridad de la red para robar información sensitiva de una organización, para luego reportarlo a dicha organización y asi mejorar su seguridad. En Atlas te ayudamos a hacer este tipo de pruebas.

Phishing: Es conocido también como suplantación de identidad o simplemente suplantador, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Ransomware: Un ransomware (del inglés ransom, 'rescate', y ware, por software) es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.[2]

Spam: Los términos correo basura y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al recepto

Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

[2] DINEROENIMAGEN (Página Web). 62 términos que tienes que conocer para mejorar tu seguridad informática [En Línea] Recuperado de: < https://www.dineroenimagen.com/hacker/62-terminos-que-tienes-que-conocer-para-mejorar-tu-seguridad-informatica/100039 >

Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro.

Vulnerabilidad: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

Permitir que un atacante ejecute comandos como otro usuario.
Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
Permitir a un atacante hacerse pasar por otra entidad.
Permitir a un atacante realizar una negación de servicio.

Zero-day: Vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes, son desconocidas por los fabricantes y usuarios. No existe un parche de seguridad para solucionarlas y son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.[3]

[3] Welivesecurity.com (Página Web). Qué es un 0-day? Explicando términos de seguridad [En Línea] Recuperado de: < https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/ >

INTRODUCCIÓN

La construcción del informe técnico en el Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, me permitirá demostrar el trabajo realizado, conociendo sus aciertos y desaciertos encontrados en el mismo. Así mismo nos permitirá entregar un informe donde se describa lo realizado en los escenarios propuestos por The WhiteHose Security de acuerdo con las acciones realizadas de Red Team & Blue Team y aspectos legales.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Generar un informe técnico que contenga las conclusiones generales y relevantes del desarrollo del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

1.2 OBJETIVOS ESPECÍFICOS

- Incluir en el informe las conclusiones y recomendaciones del desarrollo del Seminario que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

- Incluir Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

- Uso de mínimo 15 referentes bibliográficos, mínimo 5 en idioma inglés.

- Realizar la sustentación del seminario especializado a través de un video con duración de 8 minutos

2. DESARROLLO DEL INFORME

2.1 ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

El mundo con el pasar de los días está experimentando una exponencial digitalización de la información, nosotros como expertos en seguridad de la información, debemos estar a la vanguardia de todas las herramientas de ciberseguridad, y mecanismos que nos permitan detectar a tiempo y actuar frente a las vulnerabilidades que está expuesta una organización.

Con el pasar del tiempo, los avances, nuevos descubrimientos y teniendo como punto fundamental que uno de los activos más importantes en esta época es la Información, la legislación debe ir a la par para poder prevenir y combatir fenómenos que atenten contra la misma.

Si bien en Colombia empezó a incluir dentro de su legislación a partir de 1980 y con el pasar del tiempo ha realizado más aportes. La Ley 1273 de 2009, nos describe puntualmente los delitos informáticos y las penas correctivas a que conllevan por su incumplimiento, y van de la mano con la Ley 1266 de 2008 de habeas data, pero ya han pasado 11 años aproximadamente y mi punto de vista es que se están quedando cortos en cuanto a legislación, ya que la tecnología está revolucionando y nos está haciendo más fácil la vida, pero al mismo tiempo nos está dejando en riesgo inminente.

2.2 ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

El actuar del ser humano siempre estará enmarcado dentro de unos principios éticos y legales, el ámbito contractual juega un papel fundamental a la hora de desempeñar nuestros roles como profesionales, y debemos tener claro estos aspectos los cuales a la hora de una investigación nos podrían salvar si desde el

comienzo de un trabajo se dejan estipulados y enmarcados dentro de los ámbitos jurídicos actuales. Como profesionales debemos estar a la par investigando y siempre rigiéndonos por nuestro código de Ética que enmarca el ser y el saber cómo profesionales.

Como experto en ciberseguridad no aceptaría un trabajo que este en contra de la ley o en contra de terceros, teniendo en cuenta que estaría incurriendo en una falta del código Penal Ley 599 del 2000 como ya se mencionó en el punto 2, así mismo en lo referente al código de Ética de COPNIA el cual moralmente es nuestra biblia como ingenieros, que nos orienta a actuar con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de nuestra profesión y en su artículo 35. Literal b y c "DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES. b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones; c) Velar por el buen prestigio de estas profesiones.

De nada sirve el dinero si desde el comienzo no se estipulo un contrato que cumpla y este acorde con la normatividad legal y vigente, siempre he tenido este concepto "lo que empieza mal, tarde que temprano terminara mal", y no estamos hablando de un simple despido, estamos hablando de la suspensión temporal o definitiva de nuestras licencias o una pena de prisión desde 36 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes como lo establece la ley actual.

Como buen ejemplo tenemos el caso de la "OPERACIÓN ANDROMEDA BUGGLY" que me permite discernir y ayudar a tomar las mejores decisiones a la hora de firmar un contrato con cualquier empresa, siempre a estar pendiente y optar como punto principal en todo contrato las clausulas y alcances del contrato siempre anteponiendo mi ética y profesionalismo.

2.3 ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

Una vez realice las pruebas de penetración en ambas maquinas Windows 7 X86 y Windows 7 X64, se puede determinar que la maquina en la cual se estaba presentando la vulneración de seguridad que se relacionan en el Anexo 4 – Escenario 3, donde describe que se está generando una serie de fuga de información al interior de la organización, determino que el sistema vulnerado es el equipo de cómputo de sistema operativo Windows 7 X64, el cual al realizarle las diferentes pruebas de penetración, se determina que la falla se encuentra asociada a el ataque ransomware WannaCrypt y que está relacionada al framework EternalBlue por la falta de instalación de la actualización MS17-010, y que de la cual la hace más vulnerable que los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red.

La vulnerabilidad permite a los atacantes ejecutar código arbitrario a través de paquetes creados, esta vulnerabilidad también es conocida como “Vulnerabilidad de ejecución remota de código de Windows SMB”.

En relación con el sistema operativo Windows 7 X86 no fue posible la intrusión teniendo en cuenta la información del anexo 4 – escenario 3, que relaciona que los equipos de cómputo son antiguos, no se encuentran actualizados, y al verificar no tiene actualizaciones instaladas ni tampoco el Service Pack 1, lo que no permite el acceso al equipo de cómputo Windows 7 X86 Home Premium.
Al no tener esta opción de escritorio remoto cada vez que trataban de vulnerar el equipo de cómputo le salía la pantalla azul como modo de protección del sistema operativo.

Cada día las amenazas cibernéticas están evolucionando de forma exponencial, como profesional en esta área debo estar preparado, la emulación de escenarios de amenazas me prepara para poder enfrentar diversidad de retos, analizando la

seguridad desde la perspectiva de quienes pretendan realizar algún ataque, y así darle la posibilidad al equipo BLUE TEAM contar con herramientas y conocimientos dispuestos a contrarrestar cualquier situación.

2.4 ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

Con el pasar del tiempo nos hemos vuelto dependientes a la tecnología, la mayoría tenemos un equipo de cómputo con acceso a internet, toda empresa ya está a la vanguardia de la utilización de internet para comercializar sus productos, bajo esta premisa la tecnología para contener amenazas y vulnerabilidades de seguridad informática debe avanzar a la par.

Al momento no hay herramienta que nos proteja al 100 % de todas las vulnerabilidades y fallos que crecen de forma exponencial. Mirando esta perspectiva tenemos que estar a la vanguardia pendiente de las nuevas amenazas con el fin de implementar medidas que contengan estos fallos de seguridad a través de buenas prácticas y herramientas fundamentales que nos permitirán disfrutar de la tecnología sin exponer nuestro activo más valioso, la información.

En la realización de la etapa 4, una de las contenciones más importantes a los ataques informáticos se basa en mantener nuestros sistemas operativos actualizados y contar con un equipo de trabajo que se encargue de estar a la vanguardia de los ataques informáticos con el fin de desplegar unas políticas de seguridad que nos permita detectar cualquier vulnerabilidad a tiempo.

3. SUSTENTACIÓN MEDIANTE VIDEO

Sustenta el desarrollo de seminario especializado mediante video donde se pueda evidenciar rostro de le estudiante con una duración mínima de 8 minutos, el estudiante deberá hacer público el vídeo haciendo uso de alguna plataforma Cloud o en YouTube.

Se realiza la publicación del video de la sustentación en la plataforma de YouTube en el siguiente enlace https://youtu.be/_B4UHzxsr5E

Sustentación Seminario Especializado Red Team & Blue Team Javier Acosta

4. CONCLUSIONES

Con la realización del presente Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, me permitió adquirir nuevos conocimientos, los cuales los voy a poder implementar en mi organización como en el cargo actual como Analista de Seguridad de la información del Departamento de Policía de Boyacá.

Estamos dentro de un mundo que cada día nos hace mas dependientes a los sistemas informáticos, los cuales a medida que nos hace más dependientes también nos deja más expuestos a vulnerabilidades y ataques que día a día crecen de forma exponencial, gracias a los conocimientos adquiridos nos va permitir enfrentarlos con herramientas y fundamentos de peso que nos abre las puertas a investigar y proponer dentro de nuestras organizaciones.

5. RECOMENDACIONES

- Una de las recomendaciones que yo creería mas importante, seria que el seminario durara mas tiempo con el fin de realizar más ejercicios prácticos.

- Los acompañamientos sincrónicos vía web deberían ser mas tiempo y de ser posible se traten temas en el manejo de herramientas de vulneración así mismo de contención de ataques.

- Se debería realizar trabajos de forma grupal con el fin de compartir conocimientos y plantear soluciones más estructuradas.

- Las videoconferencias o acompañamientos sincrónicos deberías de realizarse al inicio de la actividad con el fin de aclarar dudas e inquietudes y no en los días finales como se pudo observar en el presente seminario.

REFERENCIAS BIBLIOGRÁFICAS

SUIN-JURISCOL.GOV.CO. (Página Web). Decreto 100 DE 1980. [En Línea] Recuperado de: < http://www.suin-juriscol.gov.co/viewDocument.asp?id=1705120 > [Consultado 28 de agosto de 2020]

RÉGIMEN LEGAL DE BOGOTÁ D.C. (Página Web). Ley 23 de 1982 [En Línea] Recuperado de: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431 > [Consultado 28 de agosto de 2020]

RED JURISTA. (Página Web). DECRETO 1360 DE 1989 [En Línea] Recuperado de:<https://www.redjurista.com/Documents/decreto_1360_de_1989_ministerio_de_gobierno.aspx > [Consultado 28 de agosto de 2020]

MINTIC.GOV.CO. (Página Web). Ley 72 de 1989 [En Línea] Recuperado de: < https://www.mintic.gov.co/portal/604/articles-3720_documento.pdf> [Consultado 28 de agosto de 2020]

MINTIC.GOV.CO. (Página Web). Decreto 1900 de 1990 [En Línea] Recuperado de:<https://www.mintic.gov.co/portal/604/articles-3568_documento.pdf> [Consultado 28 de agosto de 2020]

BOGOTÁ JURIDICA. (Página Web). Acuerdo 279 de 2007 [En Línea] Recuperado de:<http://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=23574> [Consultado 28 de agosto de 2020]

SECRETARIA SENADO. (Página Web). Ley 1266 de 2008 [En Línea] Recuperado de: < http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html> [Consultado 28 de agosto de 2020]

POLICIA.GOV.CO. (Página Web). LEY 1273 DE 2009 [En Línea] Recuperado de: < https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos> [Consultado 28 de agosto de 2020]

SECRETARIA SENADO. (Página Web). Ley 1341 de 2009 [En Línea] Recuperado de:http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html#:~:te

xt=Por%20la%20cual%20se%20definen,y%20se%20dictan%20otras%20disposiciones. [Consultado 28 de agosto de 2020]

SECRETARIA SENADO. (Página Web). Decreto 1873 de 2015 [En Línea] Recuperado de: < https://www.mintic.gov.co/portal/604/articles-3568_documento.pdf> [Consultado 29 de agosto de 2020]

DIARIO OFICIAL. (Página Web). Resolución 5050 de 2016 [En Línea] Recuperado de:http://www.suin-juriscol.gov.co/imagenes//24/09/2019/1569335843344_anexo%20resoluci%C3%B3n%205050%20de%202016.pdf [Consultado 29 de agosto de 2020]

PROCURADURIA.GOV.CO. (Página Web). Resolución 670 de 2017 [En Línea] Recuperado de: < https://www.procuraduria.gov.co/portal/media/file/190124_politica_proteccion_datos_pgn.pdf> [Consultado 29 de agosto de 2020]

INFORMATICAJURIDICA.CO. (Página Web). Ley 1918 de 2018 [En Línea] Recuperado de: < http://www.informatica-juridica.com/anexos/convenio-del-consejo-de-europa-sobre-la-cybercriminalidad-budapest-23-noviembre-2001/> [Consultado 29 de agosto de 2020]

SEGURIDAD CULTURA DE PREVENCION PARA TI (Página Web). Pruebas de penetración para principiantes: 5 herramientas para empezar [En Línea] Recuperado de: < https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar > [Consultado 30 de agosto de 2020]

HACKING PARA NOVATOS (Página Web). Fases de una auditoría (pentesting) [En Línea] Recuperado de: < https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar > [Consultado 31 de agosto de 2020]

SECRETARIA SENADO (Página Web). LEY 599 DE 2000 [En Línea] Recuperado de:http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr018.html#451 > [Consultado 08 de septiembre de 2020]

POLICIA.GOV.CO. (Página Web). LEY 1273 DE 2009 [En Línea] Recuperado de: < https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos> [Consultado 08 de septiembre de 2020]

COPNIA (Página Web). CODIGO DE ÉTICA [En Línea] Recuperado de:< https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf> [Consultado 09 de septiembre de 2020]

EL TIEMPO (Página Web). Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue [En Línea] Recuperado de:< https://www.eltiempo.com/archivo/documento/CMS-15141236 > [Consultado 11 de septiembre de 2020]

ELESPECTADOR (Página Web). De Andrómeda a los 'hackers' [En Línea] Recuperado de:< https://www.elespectador.com/noticias/investigacion/de-andromeda-a-los-hackers/ > [Consultado 11 de septiembre de 2020]

RADIO NACIONAL DE COLOMBIA (Página Web). La operación Andrómeda: El proceso chuzado [En Línea] Recuperado de:< https://www.radionacional.co/linea-tiempo-paz/la-operacion-andromeda-proceso-chuzado > [Consultado 11 de septiembre de 2020]

SECRETARIA SENADO (Página Web). LEY 599 DE 2000 [En Línea] Recuperado de:http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr018.html#451 > [Consultado 16 de septiembre de 2020]

INSIDER THREAT SECURITY BLOG (Página Web). WHAT IS SMBV1 AND WHY YOU SHOULD DISABLE IT [En Línea] Recuperado de: < https://blog.stealthbits.com/what-is-smbv1-and-why-you-should-disable-it/ > [Consultado 16 de septiembre de 2020]

TECHLANDIA (Página Web). Protocolo puerto 135 [En Línea] Recuperado de: < https://techlandia.com/protocolo-puerto-135-hechos_94265/ > [Consultado 16 de septiembre de 2020]

TECHLANDIA (Página Web). Protocolo puerto 139 [En Línea] Recuperado de: < https://techlandia.com/puerto-139-info_235022/ > [Consultado 16 de septiembre de 2020]

TECHLANDIA (Página Web). Protocolo puerto 445 [En Línea] Recuperado de: < https://techlandia.com/diferencia-ssl-tls-hechos_393334/ > [Consultado 16 de septiembre de 2020]

ADMIN SUB.NET (Página Web). Protocolo puerto 554 TCP [En Línea] Recuperado de: < https://es.adminsub.net/tcp-udp-port-finder/554 > [Consultado 17 de septiembre de 2020]

Wikipedia (Página Web). Remote Desktop Protocol [En Línea] Recuperado de: < https://es.wikipedia.org/wiki/Remote_Desktop_Protocol > [Consultado 17 de septiembre de 2020]

VULDB (Página Web). CVE-2017-0143 [En Línea] Recuperado de: < https://vuldb.com/es/?id.98018 >[Consultado 17 de septiembre de 2020]

KALI TRAINIG (Página Web). INTRODUCCIÓN A KALI LINUX REVELADA [En Línea] Recuperado de: < https://kali.training/lessons/introduction/ >[Consultado 17 de septiembre de 2020]

CVE (Página Web). CVE-2017-0143 [En Línea] Recuperado de: < https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 > [Consultado 19 de septiembre de 2020]

GUAYOYO (Página Web). Los grandes también caen: El ciberataque masivo que afectó a grandes empresas e instituciones [En Línea] Recuperado de: < https://medium.com/guayoyo/los-grandes-tambi%C3%A9n-caen-el-ciberataque-masivo-que-afect%C3%B3-a-grandes-empresas-e-instituciones-d7196bdddeb1 > [Consultado 21 de septiembre de 2020]

.SEGURIDAD (Página Web). Los grandes también caen: El ciberataque masivo que afectó a grandes empresas e instituciones [En Línea] Recuperado de: < https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra > [Consultado 21 de septiembre de 2020]

INCIBE-CERT_ (Página Web). Vulnerabilidad en SMBv1 en múltiples productos de Micorsoft Windows (CVE-2017-0144) [En Línea] Recuperado de: <

https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144 > [Consultado 21 de septiembre de 2020]

VIAFIRMA (Página Web). Hacking ético: identificación de servicios con nmap [En Línea] Recuperado de: < https://www.viafirma.com/blog-xnoccio/es/identificacion-servicios-nmap/ > [Consultado 21 de septiembre de 2020]

RZREDESZONA (Página Web). Microsoft recomienda deshabilitar SMBv1 para evitar el malware [En Línea] Recuperado de: < https://www.redeszone.net/noticias/seguridad/microsoft-deshabilitar-protocolo-smbv1/ > [Consultado 22 de septiembre de 2020]

NULLSECTOR (Página Web). Explotar Vulnerabilidad EternalBlue con Metasploit [En Línea] Recuperado de: < https://nullsector.co/explotar-vulnerabilidad-eternalblue-con-metasploit/ > [Consultado 21 de septiembre de 2020]

EXPLOIT DATABASE (Página Web). MS17-010 [En Línea] Recuperado de: < https://www.exploit-db.com/ > [Consultado 21 de septiembre de 2020]

CISET (Página Web). HARDENING [En Línea] Recuperado de: https://www.ciset.es/publicaciones/blog/746-hardening > [Consultado 28 de septiembre de 2020]

EL ECONOMISTA (Página Web). 7 estrategias para sobrevivir un ciberataque [En Línea] Recuperado de: < https://www.eleconomista.com.mx/tecnologia/7-estrategias-para-sobrevivir-un-ciberataque-20170629-0093.html / > [Consultado 29 de septiembre de 2020]

DELOITTE (Página Web). Pasos a seguir ante un ataque informático [En Línea] Recuperado de: < https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html > [Consultado 29 de septiembre de 2020]

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/ [Consultado 29 de septiembre de 2020]

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html [Consultado 29 de septiembre de 2020]

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27)Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf [Consultado 29 de septiembre de 2020]

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas [Consultado 29 de septiembre de 2020]

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf [Consultado 30 de septiembre de 2020]

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf [Consultado 30 de septiembre de 2020]

Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf [Consultado 3 de octubre de 2020]

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf [Consultado 3 de octubre de 2020]

HELPSYSTEM (Página Web). ¿Qué es un SIEM? [En Línea] Recuperado de: < https://www.helpsystems.com/es/blog/que-es-un-siem >[Consultado 5 de octubre de 2020]