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

BRAYAN ALEXANDER BELEÑO GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA - HUILA
2020

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

BRAYAN ALEXANDER BELEÑO GARCÍA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

Director de Curso
MSc. JOHN FREDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA - HUILA
2020

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

El objeto de este trabajo es plantear, construir y sustentar informes técnicos y gerenciales que contengan el despliegue de las estrategias y acciones desarrolladas por los equipos Blue Team y Red Team, basadas en metodologías para el mejoramiento de la seguridad en una organización, y que permitan hacer frente a eventos o incidentes informáticos sobre una infraestructura de TI, teniendo en cuenta el cumplimiento de la normatividad ética y legal vigente.

Palabras claves: Blue Team, Ciberseguridad, Eventos, Incidentes, Información, Infraestructura TI, Metodología, Pentesting, Red Team, Vulnerabilidades.

GLOSARIO

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis forense: Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

Antivirus: 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.

Ataque: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio.

Blue Team: Equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva

Ciberdelincuente: Persona que realiza acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

CIS - Center For Internet Security: Organización que facilita lineamientos y buenas prácticas de ciberseguridad para protección de sistemas y activos de TI contra amenazas emergentes.

Confidencialidad: Propiedad de la información que determina que esté disponible a personas autorizadas

Contención: Actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI,

Contingencia: Actividad que busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI

CVE - Common Vulnerabilities and Exposures: Diccionario de vulnerabilidades y exposiciones de ciberseguridad divulgadas públicamente que se puede buscar, usar e incorporar en productos y servicios.

Delitos informáticos: Acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Ethical Hacking: Acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

Eventos: Presencia o cambio de un conjunto particular de circunstancias.

Exploit: Técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Exploit DataBase: Directorio web de vulnerabilidades publicadas por hackers, y en donde se pueden consultar exploits disponibles de una vulnerabilidad identificada.

Firewall: Aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno.

Framework: Conjunto de clases cooperativas que construyen un diseño reutilizable para un tipo específico de software.

Habeas Data: Recurso legal a disposición de todo individuo que permite acceder a un banco de información o registro de datos que incluye referencias informativas sobre sí mismo.

Hacker: Programador que, gracias a sus conocimientos técnicos, puede estudiar la seguridad de un software.

Hardening: Conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo.

IDS - Intrusion Detection System: Servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada.

Incidente: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

IPS - Intrusion Prevention System: Dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades.

Kali Linux: Distribución GNU/Linux basada en Debian que agrupa herramientas para poner a prueba la seguridad de sistemas informáticos.

Malware: Programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.

Metasploit: Suite o framework de herramientas que proporciona información sobre vulnerabilidades y permite hacer pruebas de explotación.

Meterpreter: Interprete de comandos que permite obtener una gran cantidad de información sobre un objetivo comprometido, así como también manipular procesos del sistema y/o terminarlos.

MSPI - Modelo de Seguridad y Privacidad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

NAT - Network Address Translation: Sistema que funciona bajo el protocolo IP y que permite el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP incompatibles.

NGFW - Next Generation Firewall: Sistema de seguridad para redes dentro de un dispositivo de Hardware o en una versión basada en software que es capaz de detectar y prevenir ataques sofisticados a través de forzar políticas de seguridad a nivel de aplicación, así como a nivel de puertos o protocolos de comunicación.

Nmap: Herramienta utilizada para identificar equipos de una red, escanear puertos de un equipo, e identificar servicios que se ejecutan a partir de ellos.

OpenVAS: Suite o framework utilizado para la evaluación de vulnerabilidades a través de pruebas de vulnerabilidad de red, contenidas por la herramienta en una colección y que se actualiza constantemente.

Payload: Carga que se ejecuta para aprovechar una vulnerabilidad.

Pentesting: Intento autorizado de identificar y examinar sistemas, redes y equipos de cómputo, con el fin de hallar brechas, probar vulnerabilidades, y evaluar y fortalecer su seguridad.

Red Team: Equipo de seguridad que realiza ataques controlados a un objetivo definido anteriormente por parte del cliente y bajo un contrato de confidencialidad y de alcance de este.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Sandbox: Mecanismos o herramientas que proveen entornos controlados que permiten aislar virus, malware o aplicativos sospechosos, analizando su comportamiento, ejecución y efectos, de forma que no se vean afectados otros equipos ni sistemas vinculados a la misma red, y que se generen mejoras en la seguridad de las organizaciones.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Shell: Programas que proveen una interfaz de usuario para acceder a los servicios del sistema operativo.

SIEM - Security Information and Event Management: Software que permite obtener información y datos desde diferentes sistemas disponibles como firewall, antivirus, IDS/IPS, entre otros, y proteger de intrusiones y amenazas de seguridad.

SMB - Server Message Blocks: Protocolo de red de capa de aplicación que se utiliza principalmente para ofrecer acceso compartido a archivos, impresoras, puertos serie y otros tipos de comunicaciones entre nodos de una red.

Tecnologías de la Información - TI: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Vector de ataque: Formas o medios que permiten el acceso a un sistema o a una red para transmitir códigos maliciosos, con el propósito expreso de obtener algún beneficio a cambio.

VirtualBox: Software de virtualización de sistemas operativos.

Virtualización: Tecnología que simula la funcionalidad de hardware para crear servicios de TI basados en software como servidores de aplicaciones, almacenamiento y redes.

Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Zero-day: Nueva vulnerabilidad para la cual no se crearon parches o revisiones, y que se emplea para llevar a cabo un ataque.

INTRODUCCION

La información es el activo más importante de cualquier organización, ya que es la materia prima para proveer servicios y/o productos, y poder cumplir con las exigencias y expectativas de los clientes. Vemos que en todos los ámbitos, se hacen siempre grandes esfuerzos porque la información sea mantenida y administrada de la mejor forma posible, evitando que se presenten situaciones que afecten las herramientas y activos tecnológicos de la actualidad.

Así las cosas, la seguridad se convierte en un concepto que brinda una organización, herramientas de tipo normativo, legal y técnico para lograr que la información que poseen o que les ha sido suministrada y confiada por parte de sus clientes y/o usuarios, sea destinada para los fines descritos y empleada de forma responsable, y que no se vean afectados los diferentes procesos que con ésta se desarrollan.

Teniendo en cuenta lo anterior, las organizaciones tienden a adoptar y/o desarrollar prácticas de prevención de incidentes y eventos de seguridad, propiciando el uso responsable de la información y de los activos que la gestionan, con el fin de evitar que sea usada para las situaciones fuera lo ética y legalmente correcto. De esta forma, garantizan a clientes, usuarios y terceros la calidad de sus procesos, productos y/o servicios.

Para llevar a cabo el robustecimiento de la infraestructura tecnológica de una organización, los equipos Red Team deben analizar y simular de la forma más exacta posible, situaciones de vulnerabilidad de los sistemas de una organización, para efectuar pruebas de intrusión que permitan identificar fallas de seguridad específicas, probando posibles vectores de ataque a partir de las vulnerabilidades presentes y usando herramientas especializadas para desarrollar cada una de las fases de un *pentesting*.

Posteriormente los equipos BlueTeam deben tener claridad sobre los procesos y herramientas a utilizar para el fortalecimiento y *hardening* de la seguridad de las organizaciones, fortaleciendo las capacidades de prevención y respuesta ante eventos e incidentes de seguridad, relacionados con ataques y fallas de seguridad, y gestionando y analizando la mayor cantidad disponible de información para tal fin. De esta forma, se debe ser cuidadoso al obtener información de análisis, que eventualmente se traduzca en medidas efectivas y oportunas de seguridad informática, recuperación y restablecimiento de servicios de la organización.

OBJETIVOS

OBJETIVO GENERAL

Planificar estrategias basadas en metodologías de ciberseguridad defensivas y ofensivas, que permitan hacer frente a un evento o incidente informático en una infraestructura TI, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

OBJETIVOS ESPECÍFICOS

- Identificar el marco normativo y legislación relacionada con delitos informáticos y protección de datos personales, que permita evaluar las acciones de los equipos Red Team y Blue Team de una organización en el marco de los criterios éticos y legales.
- Identificar las diferentes etapas del *pentesting* y las herramientas asociadas para su desarrollo.
- Implementar un banco de trabajo en una herramienta de virtualización, para realizar pruebas y ejercicios funcionales de *pentesting*.
- Identificar problemas específicos en temas técnicos que se ejecutan en equipos Red Team, demostrando vulnerabilidades en un sistema informático a partir del uso de metodologías, técnicas y herramientas especializadas de intrusión y solución de fallas de seguridad.
- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura de TI, para la identificación de problemas específicos en temas técnicos que se ejecutan en equipos Blue Team, aplicando medidas de *hardening*, aseguramiento y respuesta a eventos de seguridad.
- Construir y presentar informes técnicos y ejecutivos sobre el despliegue de las estrategias relacionadas con el mejoramiento de las técnicas y acciones desarrolladas por equipos Red Team y Blue Team en una organización.

DESARROLLO DEL INFORME

1. CONCEPTOS DE EQUIPOS DE SEGURIDAD

En esta primera etapa de análisis de las situaciones y escenarios planteados en materia de ciberseguridad de la organización “The WhiteHose Security”, se realizó en primer lugar una exploración y análisis pertinente de la legislación relacionada con seguridad de la información y delitos informáticos asociados, que se encuentra establecida en Colombia, identificando en orden cronológico entre otras, las siguientes:

- Ley 1266 de 2008 “Habeas Data Financiero”, con la cual se dio inicio al marco normativo de la protección y el derecho de los ciudadanos a conocer la información contenida en bases de datos personales, inicialmente en materia financiera, crediticia, comercial, y de servicios, y cuya utilidad radica principalmente en el cálculo de riesgo crediticio de una persona por parte de entidades financieras, en base a información relacionada como hábitos de pago, créditos tomados anteriormente, y salario o ingresos promedios[1].
- Ley 1273 de 2009 "Delitos Informáticos", la cual complementa el código Penal, brindando herramientas al tipificar los delitos que se pueden presentar en materia informática, para facilitar la denuncia ante las autoridades competentes, el uso inadecuado y no autorizado de información provista a organizaciones y empresas[2].
- Ley 1581 de 2012 “Protección de datos personales", que permite a las personas tener un fundamento legal para el derecho a las personas a conocer la información que se haya recogido sobre ellas y contenidas en bases de datos o archivos de cualquier entidad pública o privada, en todo tipo de ámbitos, y no solo financiero y comercial[3].
- Decreto 886 de 2014. “Registro Nacional de Bases de Datos”, por el cual se asignan las funciones de la Superintendencia de Industria y Comercio respecto

[1] Colombia Legal Corporation: Asesores Legales Especialistas. 2019. ¿Conoces el Derecho de Habeas Data en Colombia? [En línea] 10 de septiembre de 2019. https://www.colombialegalcorp.com/blog/derecho-de-habeas-data/#:~:text=El%20Derecho%20de%20Habeas%20Data%20consiste%20en%20Colombia%20por%20permitir,bases%20de%20datos%20del%20pa%C3%ADs.

[2] Daccach T., José Camilo. s.f. Delta Asesores. Ley de Delitos Informáticos en Colombia. [En línea] s.f. [Citado el: 30 de 08 de 2020.] https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D.

[3] Congreso de la República de Colombia: Senado de la República. 2012. Ley Estatutaria No. 1581 de 17 de octubre de 2012. Por el cual se dictan disposiciones generales para la protección de datos personales. [En línea] 17 de octubre de 2012. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

al Registro Nacional de Bases de Datos, un directorio público de bases de datos sometidas a tratamiento que operan en el país[4].

- Ley 1712 del 2014 "Transparencia y Acceso a la Información Pública", que regula el acceso a la información pública y las excepciones existentes respecto a su publicidad, en base al derecho fundamental de acceso a la información pública, y define además tipos de información de acuerdo con su nivel de confidencialidad, formas de acceso a la misma, y aspectos de publicidad de información especial[5].
- Decreto 2573 de 2014 "Estrategia de Gobierno en línea", que establece lineamientos generales de la Estrategia de Gobierno en línea y sus componentes, entre los que se encuentra el relacionado con la Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información (MSPI)[6].
- Decreto 1008 de 2018 "Política de Gobierno Digital", actualización de la Estrategia de Gobierno en Línea, enfocándola ahora a la construcción y desarrollo de ciudades y territorios inteligentes, para generar valor en la gestión y administración de los recursos públicos, y el mejoramiento de la interacción ciudadano-Estado[7].

Posterior a este análisis de legislación existente en materia de seguridad de la información, se realizó análisis de un ejercicio importante en materia de ciberseguridad, como lo es el *pentesting*, identificando en el examen autorizado de sistemas, redes y equipos de cómputo, el medio por el cual se determinan brechas y vulnerabilidades antes que las realice un ciberdelincuente, y fortalecer los mecanismos de protección necesarios para mitigar o solucionar los riesgos identificados[8], teniendo la posibilidad de usar para esto diferentes herramientas en

[4] Ministerio de Comercio, Industria y Turismo. 2014. Decreto Número 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. [En línea] 13 de mayo de 2014. http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf.

[5] Presidencia de la República de Colombia. 2014. Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En línea] 06 de marzo de 2014. http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/ley-1712.pdf.

[6] Ministerio de Tecnologías de la Información y las Comunicaciones. 2014. Decreto Número 2573 de 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de diciembre de 2014. https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf.

[7] Ministerio de Tecnologías de la Información y las Comunicaciones. 2019. Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital. [En línea]. Abril de 2019. https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf.

[8] Catoira, Fernando. 2012. Penetration Test, ¿en qué consiste? We live Security by ESET. [En línea] 24 de julio de 2012. https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/.

cada una de sus fases[9] (recopilación de información, búsqueda y explotación de vulnerabilidades, post explotación de vulnerabilidades, y la elaboración de informes), y que faciliten la toma de decisiones a futuro que subsane las vulnerabilidades encontradas. Entre otras, las principales herramientas identificadas para uso en las fases del *pentesting* se encuentran:

- Nmap, que permite recopilación de información y búsqueda de vulnerabilidades de equipos en red, a través de los puertos y servicios disponibles[10].
- Metasploit, que proporciona información sobre vulnerabilidades, o exploits, y permite hacer pruebas de explotación usando payloads o código de explotación[11].
- OpenVAS, que se utiliza para la evaluación de vulnerabilidades a través de red, utilizando diferentes herramientas integradas[12].
- ExploitDB, que consiste en un directorio web de vulnerabilidades publicadas por diferentes hackers, y los exploits asociados a estas[13].
- CVE, que es un listado de vulnerabilidades y exposiciones comunes de seguridad informática que se encuentra publicado en la web[14].

Por último en esta etapa se realizó el montaje de un banco de trabajo, basado en herramientas OpenSource, con el fin de que el personal que se postuló a la organización The Whitehouse Security, realice una serie de ejercicios y prácticas que permitan dar solución a escenarios y problemas que se presentan al interior.

En esta caso se realizó configuración del banco de trabajo utilizando la herramienta virtualizadora VirtualBox, y realizando la instalación de las imágenes de maquinas virtuales correspondientes a sistemas operativos Kali Linux, Windows 7 X86, y Windows 7 X64, ajustando las preferencias para optimizar el uso de recursos de hardware del host, y la configuración de red necesaria para validar comunicación entre ellas, seleccionando al opción Red NAT en VirtualBox, con el fin de crear la red internamente entre las máquinas y mantener acceso a internet.

---

[9] Eliasib, Gerardo. 2017. Fases de un pentesting. Hacking Professional with HTB. [En línea] 04 de septiembre de 2017. https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/.

[10] De Luz, Sergio. 2019. Nmap: Descarga, instalación y manual de uso paso a paso. Redeszone. [En línea] 21 de enero de 2019. https://www.redeszone.net/analisis/routers/asus-rt-ax86u-ax5700/.

[11] Curso de Hackers.com. s.f. MetaSploit, tomar control de equipos remotos. [En línea] s.f. http://www.cursodehackers.com/metasploit.html.

[12] We live security by ESET. 2014. Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. [En línea] 18 de noviembre de 2014. https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/.

[13] DragonJAR. s.f. Repositorio Exploit-DB. [En línea] s.f. https://www.dragonjar.org/repositorio-exploit-db.xhtml.

[14] Red Hat. s.f. El concepto de CVE. [En línea] s.f. https://www.redhat.com/es/topics/security/what-is-cve.

2. ACTUACIÓN ÉTICA Y LEGAL

Para esta etapa se planteó como escenario, la entrega de contratos y acuerdos de confidencialidad para la realización de análisis de este último tipo de documentos desde el punto de vista legal colombiano y desde el punto de vista ético, identificando faltas que atenten contra la ética profesional, y estipuladas en el Código de Ética establecido por el Consejo Profesional Nacional de Ingeniería, como las que van en contra de los deberes generales de los profesionales y contra los deberes para con los clientes y público en general, entre otras faltas gravísimas establecidas en este código y en la Ley 842 de 2003[15].

Posteriormente se realizó el análisis legal del documento de acuerdo de confidencialidad provisto por la organización The Whitehouse Security, de modo que se identifiquen vulneraciones y procesos ilegales establecidos en el éste, según la Ley 1273 de 2009 de Delitos Informáticos, encontrando procesos ilegales que correspondían a violaciones de datos personales, interceptaciones de datos informáticos, acceso abusivo a sistemas informáticos, y varias circunstancias de agravación punitiva, como el aprovechamiento de la confianza depositada por los propietarios de la información en calidad de administrador de ésta[16].

Este tipo de análisis sobre situaciones y escenarios planteados, facilitaron el análisis de casos y situaciones complejas presentadas en años anteriores, como es el de la Operación Andrómeda, desarrollada en el sitio Buggly Ethical Hacking Community, el cual sirvió de fachada para una Central de Inteligencia Militar para esta operación que presentaron interceptaciones ilegales, violaciones de datos personales, uso de software malicioso, acceso abusivo informático, entre otros delitos, con el fin de acceder a información confidencial de personas del gobierno nacional y relacionadas. Además, desde el punto de vista ético, fuera de las sanciones disciplinarias impuestas a los involucrados relacionadas con el incumplimiento de deberes y funciones (relevos y separaciones de cargos, entre otros[17]), se identificó que no se realizó un debido control por parte de las entidades participantes (Ejercito, Policía, Armada, Fuerza Aéreas) para la prevención y detección de delitos informáticos al interior de las instituciones de orden público.

[15] COPNIA Consejo Profesional Nacional de Ingeniería. 2015. Código de ética. [En línea] 2015. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

[16] Ministerio de Tecnologías de la Información y las Comunicaciones. 2009. Ley 1273 de 2009. [En línea] 04 de enero de 2009. https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009.

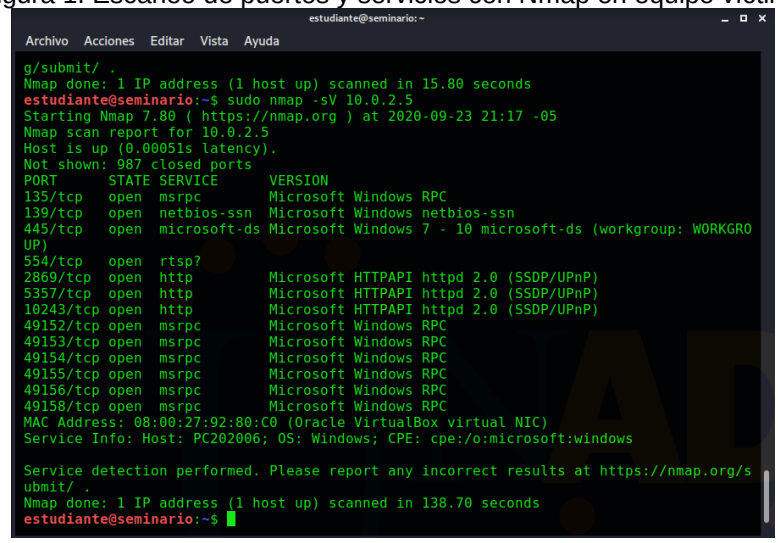
[17] Revista Semana. 2015. El informe que sacudió el caso de la fachada Andrómeda. [En línea] 24 de enero de 2015. https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3.

3. EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

En esta etapa, siguiendo el escenario propuesto en la organización The Whitehouse Security, se analizan las funciones y características de un equipo de Red Team, aplicando la metodología *pentesting* para la identificación y explotación de vulnerabilidades y fallas de seguridad de un sistema, y teniendo en cuenta la información disponible sobre el escenario establecido, la cual abarca desde información relacionada con el sistema operativo y su versión, protocolos de red utilizados, hasta actualizaciones de seguridad para corrección de fallas y vulnerabilidades *zero-day*.

En el escenario propuesto en la organización The Whitehouse Security, se identificó que uno de los equipos está afectado con fallas de seguridad relacionadas con la ejecución remota de código SMB de Windows (CVE-2017-0144), que permite recepción de paquetes en varias versiones de Windows, a través de los cuales se puede incluir ejecución de códigos maliciosos[18], y sin contar con las actualizaciones del sistema operativo que contrarrestan esta falla (MS17-010). Al realizar la inspección necesaria al sistema operativo a través de la herramienta Nmap, se identificaron los puertos 139 y 445 correspondientes a servicios de red, para comunicaciones entre software y aplicaciones con hardware de red LAN, y para compartir recursos de red como impresoras y archivos, respectivamente (protocolo SMB)[19].

Figura 1. Escaneo de puertos y servicios con Nmap en equipo víctima



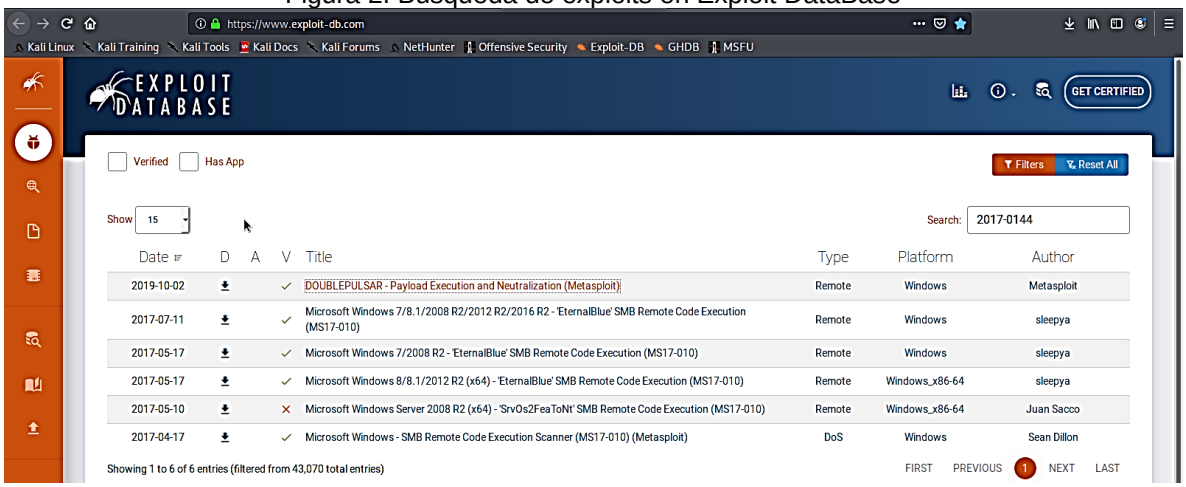
Fuente: el autor

[18] Incibe. (2018). Vulnerabilidad en SMBv1 en múltiples productos de Microsoft Windows (CVE-2017-0144). [En Línea]. 2018. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144.

[19] PcHardwarePro. (s.f.). ¿Qué es un puerto SMB? ¿Para qué se utilizan los puertos 445 y 139? [En Línea]. https://www.pchardwarepro.com/que-es-un-puerto-smb-para-que-se-utilizan-los-puertos-445-y-139/

Con base en lo anterior, se realiza la búsqueda de exploits relacionados con la falla de seguridad descrita (CVE-2017-0144) y el protocolo SMB, en la base de datos *ExploitDataBase*, a fin de aplicarlos sobre el equipo víctima a través del framework Metasploit, y de los payloads asociados a estos exploits.

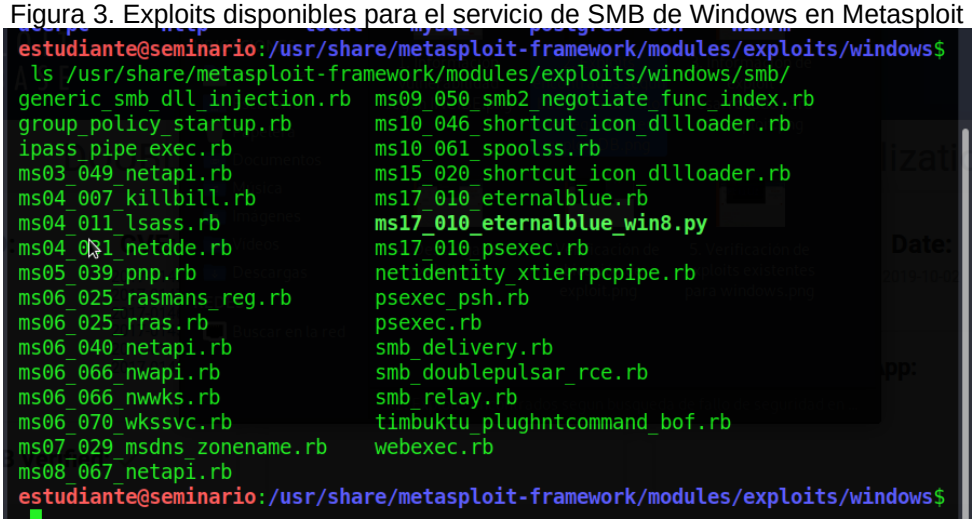
Figura 2. Búsqueda de exploits en Exploit DataBase



Fuente: el autor

En este caso se identificó el exploit "*ms17_010_eternalblue.rb*" entre los propuestos por ExploitDataBase y los disponibles en Metasploit, con lo que se seleccionó éste para ejecución a través de éste framework, y se realizó la configuración pertinente de las opciones de éste (direccionamiento de equipos víctima, puertos disponibles, cargue del payload correspondiente, entre otros).

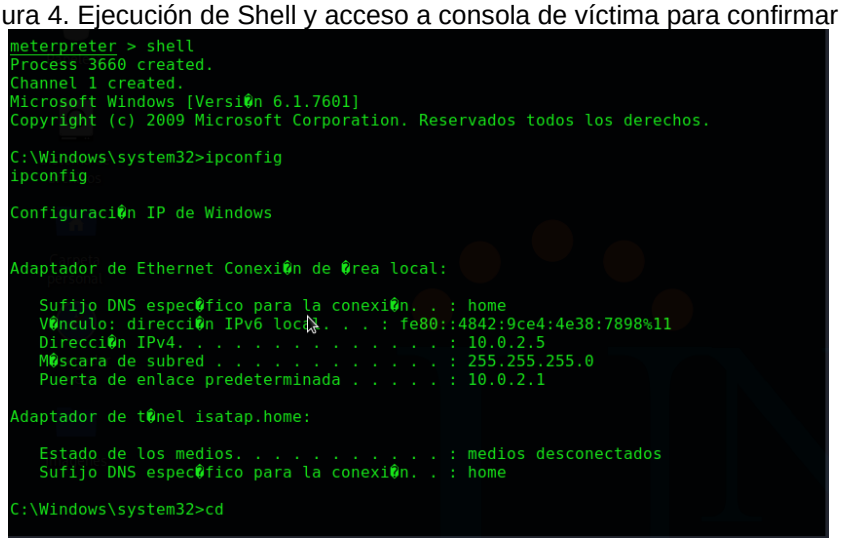
Figura 3. Exploits disponibles para el servicio de SMB de Windows en Metasploit



Fuente: el autor

Una vez se confirma la ejecución exitosa del payload, se habilita el intérprete *meterpreter* para acceso al sistema objetivo, validando que es el equipo víctima, a través de la ejecución del comando Shell, con el que es posible acceder al equipo víctima, dirigiéndonos a la ubicación "*C:\Windows\System32*" y confirmamos que es nuestra víctima, y con el comando "*ipconfig*" se verifica la IP.

Figura 4. Ejecución de Shell y acceso a consola de víctima para confirmar IP



Fuente: el autor

Por último, y siguiendo con la utilización de *meterpreter* desde el host, se efectúa el proceso de post-explotación, accediendo y ejecutando el archivo deseado. En este punto, el archivo que se ejecuta puede activar virus que faciliten acceso a información o control remoto del equipo, entre otros tipos de denegaciones de servicios y accesos.

4. CONTENCIÓN DE ATAQUES INFORMÁTICOS

En esta última etapa se analizan las medidas necesarias para la prevención y contención de ataques informáticos, partiendo de la base de la aplicación de acciones de respuesta enmarcadas en lo posible dentro de un procedimiento de respuesta a ataques e incidentes, como parte de un plan de contingencia general para la organización, que incluya el desarrollo de una serie de fases y actividades a ejecutar en caso de un ataque o evento de seguridad informática[20], que van desde las alertas emitidas respecto al ataque presentado, la verificación del estado de la

[20] FREIRE FAJARDO, Franklin Faried. 2017. Plan de Contingencia ante Ciberataques. *Escuela Superior Politécnica del Litoral*. [En Línea]. https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf

infraestructura y servicios de TI, la evaluación de daños, y la realimentación del plan de contingencia que tenga establecido la organización.

Cabe anotar que después de este plan de contingencia, es posible continuar con un análisis forense[21] realizado por autoridades competentes en la materia, ejecutando una serie de acciones para descubrir indicios del ataque, como el estudio de la situación de partida, el análisis y diagnóstico del escenario con las evidencias recopiladas del ataque, evaluando posteriormente el impacto, las consecuencias del ataque, así como también la definición de controles sobre las vulnerabilidades explotadas en los sistemas afectados, y su respectiva documentación técnica y ejecutiva sobre resultados y recomendaciones[22].

Teniendo como base el escenario propuesto para esta etapa, se analizó el alcance de las acciones de un equipo Blue Team frente ataques informáticos, las cuales abarcan desde la prevención de incidentes mediante la evaluación de amenazas y vulnerabilidades, y monitoreo de la infraestructura de TI, pasando por la detección y respuesta a incidentes, hasta llegar al análisis forense sobre vectores de ataque ejecutados, y propuestas de solución y mejora a las vulnerabilidades encontradas[23].

Para el desarrollo de estas acciones, se involucra el uso de estrategias de hardening: actualizaciones de seguridad, bloqueo de puertos[24], instalación de antivirus, copias de seguridad[25], instalación de IDS e IPS[26], y el uso de herramientas como una sandbox -utilizada para aislar virus, malware y entornos sospechosos[27]-, un firewall de nueva generación NFGW -para filtrado e inspección dinámico de

---

[21] GRUPO ACMS CONSULTORES. (s.f.). ANÁLISIS FORENSE INFORMÁTICO – CIBERSEGURIDAD. [En Línea]. https://www.grupoacms.com/analisis-forense-informatico-ciberseguridad

[22] INFOLAFT. (s.f.). ¿Qué hacer antes, durante y después de un ataque informático? [En Línea]. https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

[23] VAQUERO, Daniel. 2020. ¿CÓMO PUEDE AYUDAR EL BLUE TEAM A PROTEGER LA EMPRESA? *Ingecom*. [En Línea]. 10 de julio de 2020. https://www.ingecom.net/es/blog/45/como-puede-ayudar-el-blue-team-a-proteger-la-empresa/

[24] TORRES, Miguel. 2017. 9 RECOMENDACIONES Y PARCHES PARA PROTEGERTE DE WANNACRY. *Blog Smartekh*. [En Línea]. 18 de mayo de 2017. https://blog.smartekh.com/wannacry-9-recomendaciones-parches

[25] JIMENEZ, Javier. 2019. EternalBlue no deja de infectar equipos, pese a que puedes evitarlo fácilmente. *Redes Zone*. [En Línea]. 20 de septiembre de 2019. https://www.redeszone.net/tutoriales/seguridad/como-proteger-equipo-eternalblue/

[26] Industrial Cybersecurity by Logitek. 2017. Recomendaciones y buenas prácticas para Ransomware WannaCry. [En Línea]. 16 de mayo de 2017. https://www.ciberseguridadlogitek.com/recomendaciones-y-buenas-practicas-para-ransomware-wannacry/

[27] SANZ ROMERO, Marta. 2019. ¿Qué es Sandbox y en qué consiste? *Computer Hoy*. [En Línea]. 16 de noviembre de 2019. https://computerhoy.com/reportajes/tecnologia/que-es-sandbox-529177

paquetes y aplicaciones web[28]-, o una herramienta de contención de aplicativos DAC, para protección ante malware zero-day, y bloqueo de acciones[29]-.

Igualmente se incluyen los sistemas integrados de gestión de eventos e información de seguridad -SIEM- como herramientas basadas en software que permite obtener información sobre posibles amenazas de seguridad que pueden afectar la organización, integrando varios sistemas (firewall, antivirus, IDS/IPS, entre otros), para proteger las organizaciones de intrusiones y amenazas diversas, de manera automatizada y predictiva[30], y se realiza un análisis general de la utilidad de lineamientos establecidos por CIS -Center For Internet Security- en materia de ciberseguridad[31], definida por la efectividad de los controles establecidos y probados en entornos de simulación y situaciones reales, robusteciendo de esta manera la infraestructura de TI y mejorando la seguridad de una organización[32].

5. SUSTENTACIÓN INFORME EJECUTIVO

El siguiente es el enlace de la sustentación del informe ejecutivo:

https://drive.google.com/drive/folders/18qT80VCFLPEQbkmb5TB8LQ1k2HsKNoWh?usp=sharing

[28] BRODBECK, Cassio. (s.f.). Firewall UTM y NGFW, conozca las principales diferencias. OSTEC Blog. [En Línea]. https://ostec.blog/es/seguridad-perimetral/firewall-utm-ngfw-diferencia

[29] McAfee. 2018. Guía de módulo de producto Protección adaptable frente a amenazas de McAfee Endpoint Security 10.5.0 (McAfee ePolicy Orchestrator) – Windows. [En Línea]. 04 de mayo de 2018. https://docs.mcafee.com/bundle/endpoint-security-10.5.0-adaptive-threat-protection-product-guide-epolicy-orchestrator-windows/page/GUID-F8CE8A74-826D-41BB-9D6A-9CC70C434070.html?_LANG=eses

[30] ROUSE, Margaret. 2017. Gestión de eventos e información de seguridad (SIEM). *SearchDataCenter*. *TechTarget*. [En Línea]. Agosto de 2017. https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

[31] CIS Center for Internet Security. (s.f.). About us. [En Línea]. https://www.cisecurity.org/about-us/

[32] CIS Center for Internet Security. (s.f.). Test Your Security Configuration [En Línea]. https://learn.cisecurity.org/cis-cat-lite

CONCLUSIONES

El marco normativo y legislativo en materia de delitos informáticos y protección de datos personales en nuestro país es amplio, con varias leyes que establecen las funciones y alcances de las empresas y entidades involucradas en el tratamiento de información de las personas en la actualidad. Sin embargo, hace falta aún mayor reglamentación basada en dichas leyes, de forma que brinde lineamientos técnicos precisos para el cumplimiento de dicha reglamentación. Cabe resaltar que en algunos casos, se requieren fuertes destinaciones de recursos, no solo financieros, sino humano y materiales, para que las organizaciones puedan dar cumplimiento detallado de la reglamentación actual, lo cual ha limitado las exigencias al respecto por parte del Estado.

Debido a la complejidad para gestionar la confidencialidad en las organizaciones, se hacen necesarios modelos de confidencialidad completos que permitan adoptarse y adaptarse a las necesidades de cada organización y que estén alineados con los diferentes lineamientos, legislación, normatividad y reglamentación relacionadas, como por ejemplo las directrices dadas por el Ministerio TIC, en su modelo de seguridad y privacidad de la Información -MSPI-, las cuales incluyen aspectos relevantes como la definición de acciones requeridas cuando se termina un acuerdo de confidencialidad, derechos de actividades de auditoría y seguimiento al uso de información confidencial, y procesos de notificación y reportes ante incumplimientos del acuerdo, entre otros aspectos de relevancia[33].

Desde el punto de vista ético, se hace necesario alinear siempre los principios organizacionales y competencias comportamentales de cargos y funciones de las organizaciones, con los códigos de ética profesional establecidos para el ejercicio de las diferentes profesiones incluidas en los perfiles definidos. Esto, con el fin de evitar el desarrollo y ejecución de procesos, procedimientos o actividades ilegales, incurrir en omisiones o violación de la ley, penas y delitos relacionados con seguridad de la información, o con cualquier otra sanción o multa que comprometa la ética profesional de los funcionarios, empleados y aspirantes a empleos.

Para los empleados y aspirantes es importante tener en cuenta el código de ética profesional en el momento de, ya sea aspirar a un cargo, o ejecutar funciones de este, para identificar aspectos, situaciones, escenarios y casos reales que pueden incurrir en faltas o incumplimientos a los lineamientos establecidos en dichos

[33] Ministerio de Tecnologías de la Información y las Comunicaciones. 2017. Instrumento de Evaluación MSPI - MinTIC. [En línea] 09 de Junio de 2017. https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx.

códigos y que, si bien pueden no transformarse en sanciones penales, pueden incurrir en multas y sanciones de tipo administrativo y disciplinario.

Desde el punto de vista técnico, el *pentesting* como ejercicio práctico, permite identificar oportunidades de mejora para la disminución de amenazas y mitigación de riesgos, a partir de la identificación vulnerabilidades, teniendo en cuenta para ello, las diferentes etapas de este proceso, las herramientas y servicios que se pueden usar en ciberseguridad. Cabe añadir que no solamente con la información que se genera de la aplicación de las diferentes herramientas especializadas, se puede realizar un buen pentesting, ya que se requiere además, un análisis detallado de escenarios y condiciones actuales de debilidades y vulnerabilidades, que permitan orientar las demás fases de este proceso.

Así mismo, es importante resaltar en el desarrollo y efectividad de las actividades realizadas por los equipos Red Team, el conocer en detalle las diferentes vulnerabilidades y debilidades que se presentan y que pueden ser aprovechadas por atacantes, para inhabilitar servicios y sistemas de una organización, lo cual permite fortalecer las capacidades de contención y respuesta ante este tipo de ataques e incidentes de seguridad por parte de los equipos Blue Team, siendo este uno de los objetivos y propósitos de éstos en una organización, y teniendo en cuenta que se desarrolla basado, no solo en acciones preventivas o de detección, sino que también en un análisis detallado de los diferentes sistemas y plataformas de seguridad disponibles. Esto, con el fin de que, al tener más información de éstas, sea posible analizar los datos obtenidos para el desarrollo de medidas de *hardening* y respuestas a eventos e incidentes de seguridad.

Así mismo, para el éxito de estas medidas desarrolladas por los equipos BlueTeam, es necesario que la información recopilada para mejorar la seguridad de las organizaciones sea producto de situaciones reales de ataques y riesgos de seguridad, o lo más cercanas a la realidad posible, con el fin de que las estrategias planteadas sean efectivas y eficientes. De esta forma, es necesario su interacción con los equipos RedTeam de manera articulada en escenarios que permitan simular situaciones y eventos de seguridad, y fortalecer conjuntamente la plataforma de seguridad de las organizaciones.

De esta articulación se resalta la importancia de que la identificación y análisis efectivo de vectores de ataque, que permita contener y dar respuesta a ataques informáticos que se presenten, teniendo en cuenta las capacidades del equipo de trabajo disponible y con funciones de seguridad asignadas, para recuperar y restaurar los servicios en el momento indicado, a sabiendas de que al hacerlo se puede perder información valiosa para fortalecer y endurecer la infraestructura de TI y los sistemas de seguridad.

RECOMENDACIONES

Los profesionales de los equipos Blue Team y Red Team deben tener claridad sobre la legislación nacional en materia de seguridad y privacidad de la información, y los códigos de ética profesional establecido por los consejos profesionales para el ejercicio de la ingeniería en nuestro país, con el fin de evitar la acusación por delitos de carácter informático y omisiones en el desarrollo de su profesión o funciones establecidas en una empresa u organización, ya que de esto afecta, además de la continuidad de su profesión, el entorno social, ambiental, cultural y económico que lo rodea.

Es importante resaltar que, de acuerdo con el medio en el que se desenvuelve una organización para la que un profesional de seguridad presta sus servicios, se debe realizar la priorización de estrategias de simulación de ataques e incidentes de seguridad que deben probar los equipos de Red Team. De esta forma, la identificación de vectores de ataque será ajustada a posibles situaciones reales, cumpliendo con los objetivos para los que se establecen estos equipos de trabajo, y por consiguiente, las medidas de prevención y mitigación de riesgos de seguridad que posteriormente sean establecidas por los equipos de Blue Team.

A nivel nacional, entidades como el Ministerio de Tecnologías de la Información y las Comunicaciones, la Policía Nacional a través del Centro Cibernético Policial, y el Ministerio de Defensa a través del ColCERT -Grupo de Respuesta a Emergencias Cibernéticas-, informan y facilitan continuamente sobre vulnerabilidades y ataques que se presentan cotidianamente en sistemas y en entornos sociales y organizacionales, compartiendo información de empresas y organizaciones a nivel mundial del medio de la seguridad de la información, así como recomendaciones y medidas a tener en cuenta para prevenir y detectar incidentes relacionados. Por lo anterior, es primordial que un profesional de seguridad informática y miembro de equipos Blue Team y Red Team esté en permanente contacto con autoridades nacionales, e incluso internacionales, a fin de estar al tanto de las noticias y novedades relacionadas con la seguridad de la información y la ciberseguridad.

Desde el punto de vista técnico, es importante que los profesionales de seguridad desarrollen capacidades en el uso de herramientas especializadas para cada una de las fases de un *pentesting*. Sin embargo debe ser cuidadoso de los entornos en donde realice ejercicios prácticos para mejorar sus habilidades, evitando aplicarlos sobre entornos públicos y reales. Para esto existen los sistemas de virtualización como VirtualBox y VMWare entre los más reconocidos, en los cuales es posible utilizar imágenes de sistemas operativos que deben configurarse para realizar las pruebas y ejercicios que se requieran. Sin embargo existen algunas herramientas como DVWA (Damn Vulnerable Web Application), que cuentan con entornos de

prueba preconfigurados para realizar estos ejercicios de hacking y pentesting, y que corresponden a entornos seguros y legales, con diferentes niveles de seguridad parametrizables y con diferentes guías y tutoriales de uso de diferentes tipos de vulnerabilidades y ataques que se pueden probar[34].

Finalmente, es importante que los profesionales de seguridad desarrollen capacidades de análisis para seleccionar las metodologías y herramientas que más se ajusten a las necesidades de seguridad de una organización, de modo que los resultados de los ejercicios de pentesting, auditorías, hacking, entre otros, además de facilitar el hardening de los sistemas de seguridad, brinden información que permitan agregar valor a la organización, desde la ciberseguridad, alineándose de esta forma, con la estrategia y los objetivos de una organización, y que de esta forma, sea tenida en cuenta por la alta dirección.

[34] Bortnik, Sebastian. 2018. Pruebas de penetración para principiantes: 5 Herramientas para empezar. Revista Seguridad. Número 18. Universidad Nacional Autónoma de México. [En línea]. 2018. https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

BIBLIOGRAFIA

Bortnik, Sebastian. 2018. Pruebas de penetración para principiantes: 5 Herramientas para empezar. Revista Seguridad. Número 18. Universidad Nacional Autónoma de México. [En línea]. 2018. https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Brodbeck, Cassio. (s.f.). Firewall UTM y NGFW, conozca las principales diferencias. OSTEC Blog. [En Línea]. https://ostec.blog/es/seguridad-perimetral/firewall-utm-ngfw-diferencia

Catoira, Fernando. 2012. Penetration Test, ¿en qué consiste? We live Security by ESET. [En línea] 24 de Julio de 2012. https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/.

CIS Center for Internet Security. (s.f.). About us. [En Línea]. https://www.cisecurity.org/about-us/

CIS Center for Internet Security. (s.f.). Test Your Security Configuration [En Línea]. https://learn.cisecurity.org/cis-cat-lite

COPNIA Consejo Profesional Nacional de Ingeniería. 2015. Código de ética. [En línea] 2015. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

Congreso de la República de Colombia: Senado de la República. 2012. Ley Estatutaria No. 1581 de 17 de octubre de 2012. Por el cual se dictan disposiciones generales para la protección de datos personales. [En línea] 17 de octubre de 2012. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

Curso de Hackers.com. s.f. Metasploit, tomar control de equipos remotos. [En línea] s.f. http://www.cursodehackers.com/metasploit.html.

Daccach T., José Camilo. s.f. Delta Asesores. Ley de Delitos Informáticos en Colombia. [En línea] s.f. [Citado el: 30 de 08 de 2020.] https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D.

De Luz, Sergio. 2019. Nmap: Descarga, instalación y manual de uso paso a paso. Redeszone. [En línea] 21 de enero de 2019. https://www.redeszone.net/analisis/routers/asus-rt-ax86u-ax5700/.

DragonJAR. s.f. Repositorio Exploit-DB. [En línea] s.f. https://www.dragonjar.org/repositorio-exploit-db.xhtml.

Eliasib, Gerardo. 2017. Fases de un pentesting. Hacking Professional with HTB. [En línea] 04 de septiembre de 2017. https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

FREIRE FAJARDO, Franklin Faried. 2017. Plan de Contingencia ante Ciberataques. Escuela Superior Politécnica del Litoral. [En Línea]. https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf

Grupo ACMS Consultores. (S.F.). Análisis Forense Informático – Ciberseguridad. [En Línea]. https://www.grupoacms.com/analisis-forense-informatico-ciberseguridad

INCIBE, 2018. Vulnerabilidad en SMBv1 en múltiples productos de Microsoft Windows (CVE-2017-0144). [En línea]. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

Industrial Cybersecurity by Logitek. 2017. Recomendaciones y buenas prácticas para Ransomware WannaCry. [En Línea]. 16 de mayo de 2017. https://www.ciberseguridadlogitek.com/recomendaciones-y-buenas-practicas-para-ransomware-wannacry/

INFOLAFT. (s.f.). ¿Qué hacer antes, durante y después de un ataque informático? [En Línea]. https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

Jiménez, Javier. 2019. EternalBlue no deja de infectar equipos, pese a que puedes evitarlo fácilmente. Redes Zone. [En Línea]. 20 de septiembre de 2019. https://www.redeszone.net/tutoriales/seguridad/como-proteger-equipo-eternalblue/

McAfee. 2018. Guía de módulo de producto Protección adaptable frente a amenazas de McAfee Endpoint Security 10.5.0 (McAfee ePolicy Orchestrator) – Windows. [En Línea]. 04 de mayo de 2018. https://docs.mcafee.com/bundle/endpoint-security-10.5.0-adaptive-threat-

protection-product-guide-epolicy-orchestrator-windows/page/GUID-F8CE8A74-826D-41BB-9D6A-9CC70C434070.html?_LANG=eses

Ministerio de Comercio, Industria y Turismo. 2014. Decreto Número 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. [En línea] 13 de mayo de 2014. http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones. 2014. Decreto Número 2573 de 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de diciembre de 2014. https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf.

-. 2017. Instrumento de Evaluación MSPI - MinTIC. [En línea] 09 de junio de 2017. https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

—. 2009. Ley 1273 de 2009. [En línea] 04 de enero de 2009. https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009.

—. 2019. Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital. [En línea] abril de 2019. https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf.

PCHardwarePro. s.f. ¿Qué es un puerto SMB? ¿Para qué se utilizan los puertos 445 y 139? [En línea]. https://www.pchardwarepro.com/que-es-un-puerto-smb-para-que-se-utilizan-los-puertos-445-y-139/

Presidencia de la República de Colombia. 2014. Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En línea] 06 de marzo de 2014. http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/ley-1712.pdf.

Red Hat. s.f. El concepto de CVE. [En línea] s.f. https://www.redhat.com/es/topics/security/what-is-cve.

Revista Semana. 2015. El informe que sacudió el caso de la fachada Andrómeda. [En línea] 24 de enero de 2015. https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3.

Rouse, Margaret. 2017. Gestión de eventos e información de seguridad (SIEM). SearchDataCenter. TechTarget. [En Línea]. Agosto de 2017. https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Sanz Romero, Marta. 2019. ¿Qué es Sandbox y en qué consiste? Computer Hoy. [En Línea]. 16 de noviembre de 2019. https://computerhoy.com/reportajes/tecnologia/que-es-sandbox-529177

Torres, Miguel. 2017. 9 Recomendaciones y parches para protegerte de Wannacry. Blog Smartekh. [En Línea]. 18 de mayo de 2017. https://blog.smartekh.com/wannacry-9-recomendaciones-parches

We live security by ESET. 2014. Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. [En línea] 18 de noviembre de 2014. https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

Vaquero, Daniel. 2020. ¿Cómo Puede Ayudar el Blue Team a Proteger la Empresa? Ingecom. [En Línea]. 10 de julio de 2020. https://www.ingecom.net/es/blog/45/como-puede-ayudar-el-blue-team-a-proteger-la-empresa/