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

JORGE FABIÁN BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
VALLEDUPAR
2020

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

AUTOR:
JORGE FABIÁN BRACHO

Trabajo: Etapa 5 Socialización de Informe Técnico

Director:
John Freddy Quintero
Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
VALLEDUPAR
2020

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ATAQUE: intento de acceder, modificar, eliminar, divulgar información sin consentimiento del propietario.

DELITO: acceder a un sistema informático con el fin de destruir, modificar, suspender su funcionamiento normal.

KALI: distribución de Linux, usada para proteger los equipos pertenecientes a una red de computadores.

PENTESTING: acción de descubrir vulnerabilidades en equipos de red de computadores mediante ataques controlados buscando resolver dichas vulnerabilidades.

RED: equipos de cómputo conectados entre sí con el fin de compartir recursos.

RIESGO: probabilidad que existe en que una amenaza se convierta en un incidente real.

SEGURIDAD: estado ideal de los equipos y la información pertenecientes a un sistema informático.

VULNERABILIDAD: fallo de un sistema de información, el cual puede ser explotado pudiendo afectar la información.

RESUMEN

La información es el activo más importante en todo tipo de organización actualmente. Es por ello que los procesos de transporte, transformación y conservación de dicha información, deben estar lo más blindados posible con el fin de no tener incidentes que puedan afectar negativamente el funcionamiento de las empresas e incluso, dejar en riesgo a sus clientes.

Es así como los equipos Red Team y Blue Team, mediante técnicas y diversas aplicaciones buscan identificar los riesgos que pueden generar o están generando algún tipo de fuga de información a personas que pueden hacer uso indebido de esta para cualquier tipo de acción ilegal; así mismo, una vez identificados los riesgos, se puede aplicar controles necesarios con el fin de aumentar la seguridad a la información y recursos informáticos para garantizar en gran parte la privacidad de dicha información que implica a usuarios y clientes de las empresas, buscando siempre la mejora contínua teniendo como objetivo principal mantener la confiablidad, integralidad y disponibilidad de la información en sus procesos productivos.

Las acciones anteriores deben ser ejecutadas bajo parámetros legales como son contratos con delimitaciones claras de acción que evidencie hasta dónde puede llegar el accionar de los equipos Red Team y Blue Team, regidos por las leyes y decretos que buscan proteger los datos personales, así mismo, ayudar en generar información que pueda ser útil a los encargados de penalizar a quienes incurran en delitos informáticos tipificados en las leyes nacionales, como los son la Ley 1273 del 2009, adicionado el Título VII Bis denominado “De la protección de la información y de los Datos”[1], y la Ley 1581, el cual dicta “…desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos…[2] .

Palabras claves: Activo, Blue Team, delito, información, proceso, Red Team,

[1] **COLOMBIA. CONGRESO DE LA REPÚBLICA.** Ley 1273 (05 de Enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

[2] **COLOMBIA. CONGRESO DE LA REPÚBLICA.** Ley 1581 (17 de Octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales.

INTRODUCCIÓN

La legislación colombiana, según descripción anterior, tiene definida las leyes y decretos que rigen los delitos informáticos y también apuntan al buen uso y protección de los datos personales que recopilan las empresas en los procesos que requieran de ello. Por otro lado, el ejercicio de las carreras de Ingenierías y afines, también tiene pautas que deben ser tenidas en cuenta desde el punto de vista ético. El COPNIA, (Consejo Profesional Nacional de Ingeniería) busca proteger a la sociedad del inadecuado ejercicio profesional por medio del Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares[3].

El uso de máquinas virtuales puede generar un ambiente adecuado para ejecutar diferentes técnicas propias de equipos Red Team como es el pentesting, con el fin de encontrar, identificar y explotar vulnerabilidades, y así dar paso a las técnicas del equipo Blue Team para poder detectar y controlar incidentes en forma oportuna según su Plan de Respuesta a Incidentes (IRP).

Las medidas de hardenización buscan endurecer las medidas de seguridad y cerrar más las brechas para que las vulnerabilidades en los equipos informáticos tanto a nivel personal como los que suelen estar presentes en las redes de las organizaciones.

El uso de CIS (Centro de Seguridad para Internet) con la implementación de mejores prácticas de ciberseguridad, en la acción de Blue Team y SIEM (Gestión de la Información de Seguridad de Eventos) para asegurar los sistemas y plataforma de redes, y por otro lado la detección, contención y recuperación de incidentes, son factores determinantes para brindar mayor protección a los sistemas informáticos en las organizaciones.

[3] **COLOMBIA. Consejo Profesional Nacional de Ingeniería.** Código de Ética. Recuperado de: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Plasmar informe técnico del proceso de los escenarios propuestos en cada una de las acciones como Red Team y Blue Team, dentro del período de prueba en la organización The WhiteHouse Security.

1.2. OBJETIVOS ESPECÍFICOS

- Conocer el ámbito ético y legal de los equipos Red Team y Blue Team.
- Identificar procesos para ejecutar análisis de vulnerabilidades.
- Conocer métodos de contención y hardenización.

2. DESARROLLO DEL INFORME

Entre las labores en el periodo de prueba en la organización The WhiteHouse Security se ejecutaron técnicas propias de Red Team y Blue Team, bajo un laboratorio virtualizado, donde se montan dos (2) máquinas con sistema operativo Windows (x86 y x64), las cuales cumplen el rol de víctimas y una (1) con Kali, la cual cumple el rol de atacante.

El presente informe también puede ser consultado en el link[4] https://youtu.be/vlHjBxhdeYY

2.1. AMBITO ÉTICO Y LEGAL DE LOS EQUIPOS RED TEAM Y BLUE TEAM

Es importante tener claro que las técnicas usadas como Red Team y Blue Team para la organización The WhiteHouse Security son ejecutadas bajo lineamientos descritos en el código de ética para el ejercicio de las carreras de Ingenierías y afines, código suministrado por El COPNIA, (Consejo Profesional Nacional de Ingeniería), quienes buscan proteger a la sociedad colombiana del inadecuado ejercicio profesional de los ingenieros, profesionales afines y auxiliares[5], los cuales deben estar adscritos a este Consejo para poder avalar las facultades propias del ejercicio profesional y ejercer legalmente en el territorio nacional. Adicional al código de ética de EL COPNIA, las técnicas ejecutadas por Red Team y Blue Team en estos procesos, se rigen teniendo en cuenta la legislación nacional en lo que tiene que ver con los delitos informáticos para no incurrir en alguno de ellos, o bien informar a los encargados, en caso de identificar incidentes o acciones que atenten contra la confiabilidad, disponibilidad e integridad de la información descritas en la Ley 1273 del 2009[6], para que así puedan tomar decisiones en lo que tiene que ver con las acciones judiciales que pudieran iniciar.

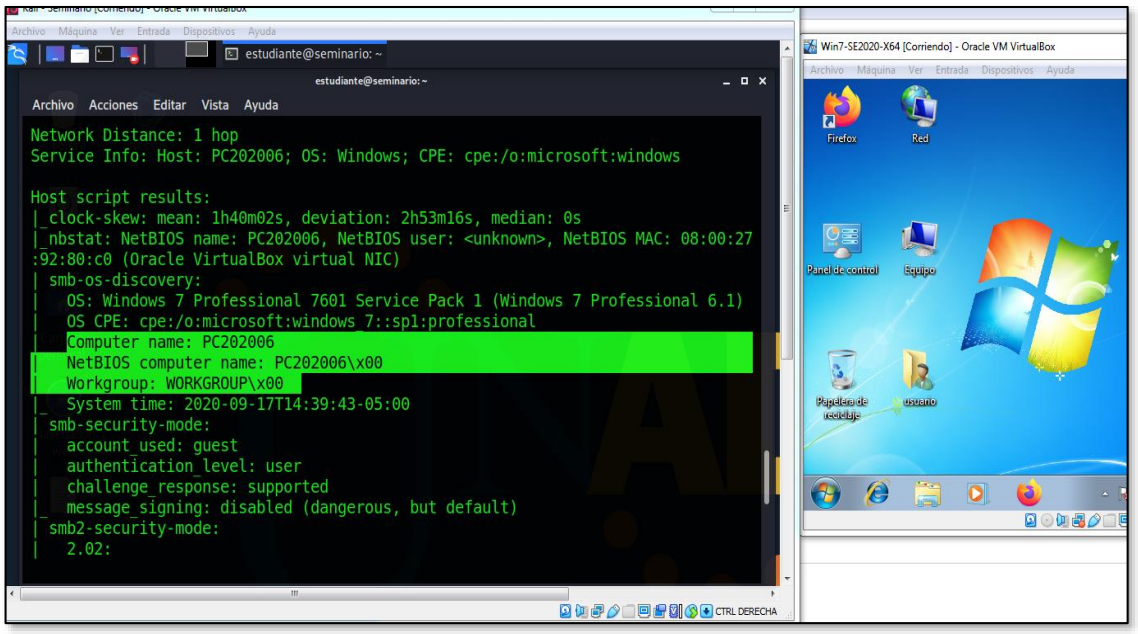
2.2. TÉCNICAS EQUIPO RED TEAM

Teniendo montadas las máquinas virtuales y comunicándose entre ellas, se procede desde la máquina Kali, a buscar información sobre los equipos conectados en red. Apoyados con la herramienta **NMAP** ("Network Mapper")[7], la cual es una utilidad

[4] **COLOMBIA. UNAD - Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. Recuperado de:** https://youtu.be/vlHjBxhdeYY
[5] **COLOMBIA. Consejo Profesional Nacional de Ingeniería.** Misión. Recuperado de: https://www.copnia.gov.co/nuestra-entidad/quienes-somos
[6] **COLOMBIA. Ministerio de las TIC.** LEY 1273 DE 2009. [En línea]. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html
[7] **NMAP.** Open Source Tool. Recuperado de: https://nmap.org/

gratuita para descubrimiento de redes y auditoria de seguridad, se inicia proceso de “pentesting” respetando el orden en sus fases, desde la recolección de información, la cual arroja que una máquina tiene instalado sistema operativo Windows 7 de 32 bits (x86) y la otra Windows 7 de 64 bits (x64), también se identifican los puertos abiertos, servicios y versión.

Figura 1. Identificación equipo víctima



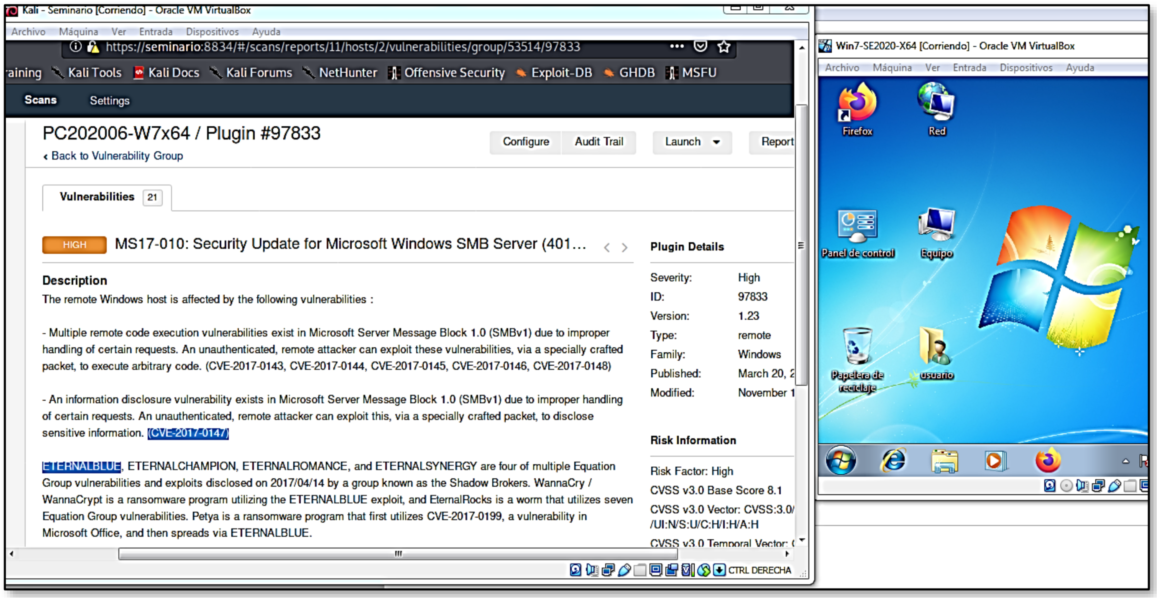
Fuente: El Autor

Con la mayor información recolectada, se procede con la fase de análisis, usando la herramienta **NESSUS**[8] para ejecutar el análisis de vulnerabilidades en cada equipo víctima, teniendo desde la fase anterior las direcciones IP’s de cada equipo.

Entre las vulnerables encontradas por **NESSUS**, se identifica la vulnerabilidad llamada EternalBlue, la cual se ha generado bajo registro (CVE-2017-0147).

[8] **NESSUS.** Operating System Vulnerability Scan Tool. Recuperado de: https://www.tenable.com/products/nessus

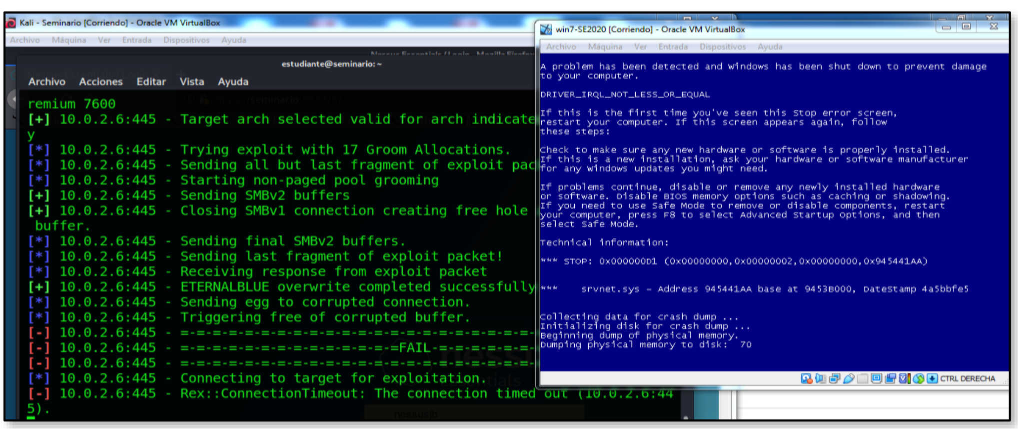
Figura 2. Vulnerabilidad CVE-2017-0147



Fuente: El Autor

Con la fase de análisis completa, se sigue a la fase de explotación con la herramienta **Metasploit Framework**[9], lanza el exploit a dicha vulnerabilidad teniendo como resultado pantalla azul y reinicio de sistema en la máquina Windows 7 de 32 bits (x86). El pantallazo azul es generado en la máquina Windows 7 x86, porque el exploit se está ejecutando desde la máquina Kali de 64 bits, lo cual genera el error por la diferencia entre las arquitecturas de estos dos equipos.

Figura 3. Máquina Windows 7 x86 - Pantalla azul

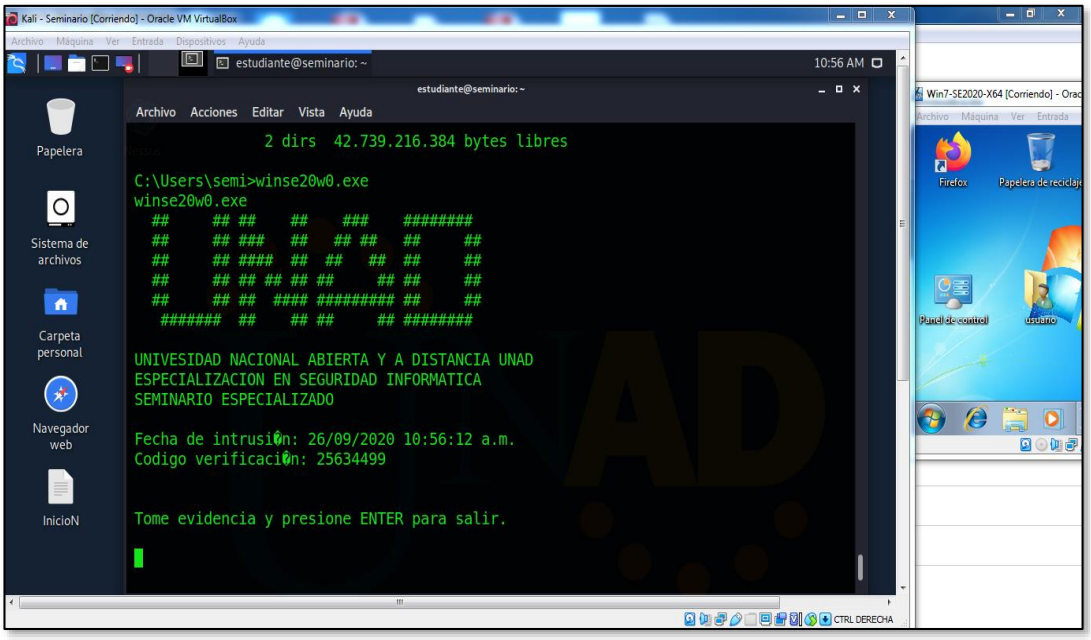


Fuente: El Autor

[9] **METASPLOIT FRAMEWORK.** The world’s most used penetration testing framework. Recuperado de: https://www.metasploit.com/

En el caso de la máquina con Windows 7 x64, se identifica la misma vulnerabilidad y se procede a lanzar el exploit, teniendo éxito en la intrusión. Ya estando dentro de la máquina víctima, se procede a localizar el archivo “winse20w0.exe”, indicado según Anexo 4 – Escenario 3. El archivo fue encontrado en el directorio “C:\users\semi el cual se ejecutó en forma invisible a la víctima.

Figura 4. Archivo ejecutado



Fuente: El Autor

Teniendo documentado el análisis de vulnerabilidades, la identificación y ejecución de las mismas, se determinan acciones para solucionar esta y otras vulnerabilidades. Para este caso, la actualización del sistema operativo con los parches de seguridad para tal fin, cierran brechas que ya están documentadas para las organizaciones no sigan viéndose afectados desde ese punto de vista.

2.3. TÉCNICAS EQUIPO BLUE TEAM

Un equipo BLUETEAM puede pertenecer a la empresa o ser un aliado externo (minimizar costos), el cual tendrá la responsabilidad de conocer en detalle el comportamiento cotidiano de la empresa y así estar alerta frente a un comportamiento fuera de lo normal con el fin de dar respuesta oportuna según su

Plan de Respuesta a Incidentes (IRP) teniendo en cuenta los activos informáticos de la misma empresa.

Las alertas de incidentes pueden ser generados por los usuarios o por equipos tecnológicos dentro de la red para tal fin. Ante la alerta de detección de un incidente, el quipo Blue Team, debe tener tiempos definidos para ejecutar acciones tendientes contener el ataque para que los equipos y la información no se vean afectados por intento o accesos no autorizados o modificación, destrucción o divulgación igualmente sin autorización.

Para ello se hace necesario la identificación y evaluación del incidente de seguridad informática con el fin de tener claro la severidad del impacto al cual se estaría enfrentado (Alto, Medio, Bajo)[10] y las posibles consecuencias que pudieran existir por la ejecución del ataque.

Para un equipo Blue Team es pertinente trabajar con CIS (Centro para la Seguridad de Internet) teniendo en cuenta que ofrece actualización en identificación y perfeccionamiento continuo de medidas de seguridad efectivas estandarizadas a nivel global y, su uso es gratuito.

Las redes de cómputo y los equipos conectado a ellas, son frecuentemente afectados por incidentes de seguridad informáticos, por lo cual CIS Benchmarks establece las pautas comprobadas para protegerlos de ataques cibernéticos[11].

El equipo Blue Team también realiza búsqueda activa de amenazas usando SIEM (Gestión de la Información de Seguridad de Eventos), los cuales se caracterizan por recolectar información de los dispositivos y la forma como los usuarios realizan sus procesos frecuentemente, normalizar y analizar dicha información, administrar la solución y visualizar en tiempo real las alertas generadas.

El hardening es otra actividad ejecutada desde el equipo Blue Team, esta se realiza con el fin de robustecer las medidas de seguridad, incluso teniendo en cuenta todo el proceso que permitió la intrusión al equipo víctima (aprender sobre las acciones tomadas hasta contener alertas anteriores).

Entre las medidas de hardening tomadas están: la instalación de antivirus, instalar actualizaciones del sistema operativo con el fin de cerrar vulnerabilidades ya

---

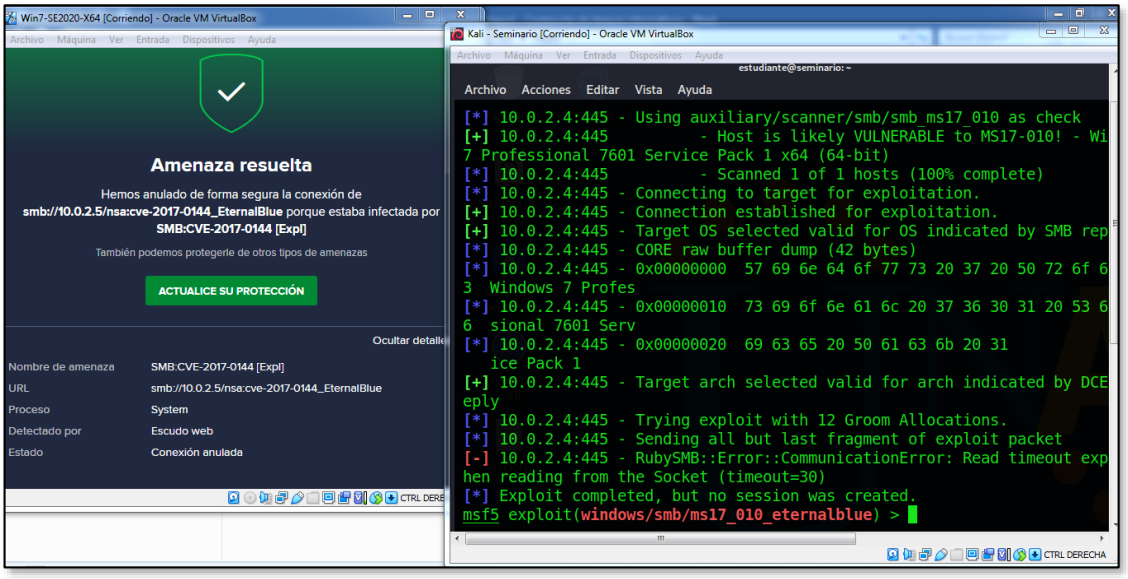
[10] **Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información**. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[11] **Center for Internet Security**. Recuperado de: https://www.cisecurity.org/cybersecurity-best-practices/

solucionadas en cada sistema operativo (como la Eternalblue), se deben cerrar los puertos y desactivar servicios no usados, activar el firewall del sistema operativo para los tres perfiles (público, privado y dominio), en los usuarios se debe capacitar y concientizar sobre el uso de contraseñas fuertes.

Para el caso de los mismos equipos en la actividad de Red Team, se puede verificar el bloqueo y alerta generada por el incidente de seguridad informática.

Figura 5. Amenaza resuelta



Fuente: El Autor

CONCLUSIONES

La realización del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team permitió realizar actividades como aspirante bajo el período de prueba en el proceso de inserción al grupo de empleados de la empresa The WhiteHouse Security.

Las actividades permitieron analizar el marco legal colombiano en lo que tiene que ver con los delitos informáticos y leyes de protección de la información personal. Así mismo, profundizar el código de ética del COPNIA, el cual indica deberes y prohibiciones de los profesionales con sus colegas, con la sociedad y en general, so pena de incurrir en sanciones o llegar a la cancelación de la Tarjeta Profesional. Lo anterior se pudo aplicar ante algunas situaciones planteadas en las cláusulas del contrato para ingreso de personal a The WhiteHouse Security.

La asignación de labores por parte de The WhiteHouse Security para los aspirantes, como miembro de equipos Red Team & Blue Team, permitió evaluar las acciones de dichos equipos dentro de una organización en el marco de los criterios éticos y legales.

La ejecución de labores de equipos Red Team, logró demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Desde el rol de equipo Blue Team, se formularon estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Se abordó la opción de trabajar como miembro de equipo Blue Team, endurecer los aspectos de seguridad, también trabajar con CIS, con los cual se planteó utilizar el CIS Benchmarks como medida de mejores prácticas para cerrar las vulnerabilidades tanto en los sistemas como en la plataforma de red.

Se elaboró video presentación en PowerPoint documentando en esa forma el informe técnico presente. El cual puede ser consultado ingresando con el link https://youtu.be/vlHjBxhdeYY

RECOMENDACIONES

Teniendo en cuenta las actividades realizadas durante el Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, donde se abordaron temas relacionados al campo de acción de equipos Read Team y Blue Team dentro del marco ético y legal, se hace necesario relacionar algunas recomendaciones tendientes a brindar mayor seguridad a los sistemas de información y sus procesos en las organizaciones con el fin de mantener la integridad, confiabilidad y disponibilidad en su información.

- La necesidad en las organizaciones de contar con equipos Red Team y Blue Team, es cada vez mayor. Muchas organizaciones desconocen el nivel real de vulnerabilidad que presentan sus activos informáticos, tampoco saben cómo protegerlos. Por ello, se recomienda contar con personal dedicado a labores de Red Team y Blue team, buscando así tener un panorama claro sobre las vulnerabilidades a las que está expuesta la organización, reducir dichas vulnerabilidades, analizar y normalizar el uso con los equipos informáticos de la organización, tener un plan de acción y mitigación frente a alertas de incidentes que se puedan presentar.

- Sabiendo que los servicios de equipos Red Team y Blue Team no son económicos, las organizaciones pueden hacer alianzas estratégicas o contractuales con empresas dedicadas a estas actividades, disminuyendo considerablemente los costos que le puedan generar a las organizaciones.

- Actividades de hardening buscan endurecer las medidas de seguridad en los sistemas de información y las plataformas que implementan los procesos para el tráfico, tratamiento y salvaguarda de la información. Entre las actividades que deben ser tenidas en cuenta para disminuir las vulnerabilidades en las organizaciones, que no solo se deben a la parte tecnológica, sino también el factor humano; están: capacitar a los usuarios con temas relacionados a las buenas prácticas de uso, la necesidad de implementar contraseñas fuertes, exigir el uso exclusivo de correo institucional, identificación de modalidades de robo de información por diferentes formas, socializar plan de acción frente a alertas de incidentes de seguridad informática, contar con software licenciado, mantener actualizados los sistemas operativos, antivirus y demás programas. No menos importante, contar con IPS´s y firewall activado para todos los equipos endurece las acciones contra los delincuentes informáticos. Entre otras actividades.

- Para las pequeñas y medianas empresas, los CIS (Centro de Seguridad para Internet) se convierten en una buena opción con la implementación de mejores prácticas de ciberseguridad, teniendo en cuenta que es una comunidad colaborativa que busca cerrar el campo de acción a la ciberdelincuencia, en forma gratuita.

BIBLIOGRAFIA

Alcaldía de Ibagué. Plan Gestión de Incidentes. [En línea]. Recuperado de: https://www.ibague.gov.co/portal/admin/archivos/publicaciones/2019/26850-DOC-20190822.pdf

CCNA SEC: Router Hardening. Recuperado de: https://www.ciscopress.com/articles/article.asp?p=1750219

Center for Internet Security - CIS. Recuperado de: https://www.cisecurity.org/cybersecurity-best-practices/

Consejo Profesional Nacional de Ingeniería. Código de Ética. Recuperado de: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Congreso de la República. Ley 1273 (05 de Enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Congreso de la República. Ley 1341 (30 de Julio de 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Bogotá D.C.

Congreso de la República. Ley 1581 (17 de Octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales

Impacto Mundo. (2020, Abril 18). Los delitos informáticos aumentaron en la Cuarentena | Impacto TDN [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=X2KLIg2G2dE

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

Jorge B. (2020, Octubre 16) UNAD - Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. Informe Técnico. [Archivo de video] Recuperado de: https://youtu.be/vlHjBxhdeYY

METASPLOIT FRAMEWORK. The world's most used penetration testing framework. Recuperado de: https://www.metasploit.com/

Ministerio de las TIC. LEY 1273 DE 2009. [En línea]. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

Ministerio de las TIC. LEY 1341 DE 2009. Ministerio de las TIC. [En línea]. Recuperado de: https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009

NMAP. Open Source Tool. Recuperado de: https://nmap.org/

NESSUS. Operating System Vulnerability Scan Tool. Recuperado de: https://www.tenable.com/products/nessus

QUINTERO, John Freddy (2020). Imagen OVA máquinas virtuales. [En línea]. Recuperado de: https://drive.google.com/drive/folders/10k-TcnJYINZ9q4I9csNBdS49EdCo0sWx?usp=sharing

Secretaría del Senado. LEY 1581 DE 2012. [En línea]. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html