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

ANA MARÍA MONTOYA BURITICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2020

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

ANA MARÍA MONTOYA BURITICA

ACTIVIDAD ETAPA 5

M.Sc. JOHN FREDDY QUINTERO
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2020

CONTENIDO

RESUMEN

“En el 2019 fueron reportados más de 28.000 casos de ciberataques en Colombia, incrementaron en un 54% en comparación con el 2018 y los más comunes están relacionados con ransomware, phishing, suplantación de identidad, envío de malware y fraudes en medios de pago en línea” (Tecnosfera, 2019).

“En la actualidad grandes y medianas empresas están expuestas a múltiples ciberataques que pueden impactar negativamente su operación, imagen y reputación, el 90% de estos ataques están relacionados a ingeniería social, sin embargo, la Ciberseguridad se ha convertido en una pieza clave, dado que involucra diferentes técnicas y herramientas que permiten salvaguardar la información contenida en servidores, dispositivos móviles, redes, entre otros y se cuentan con equipos expertos que se encargan de la seguridad ofensiva y defensiva: RedTeam y BlueTeam”(Crowdstrike, 2020).

GLOSARIO

Activos de información: "*Son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección"*(SGSI, 2017) .

BlueTeam: *"Es un equipo conformado por profesionales de la seguridad que tienen una visión de adentro hacia afuera de la organización. Su tarea es proteger los activos críticos de la organización contra cualquier tipo de amenaza, conocen bien los objetivos comerciales y la estrategia de seguridad de la organización. Por lo tanto, su tarea es fortalecer los muros del castillo para que ningún intruso pueda comprometer las defensas"*(Purplesec, 2020).

Ciberataque: *"Los ciberataques son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet"*(Auditool, 2017)

Ciberseguridad*: "Es la práctica de proteger las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos*"(Kaspersky, 2020) (Cisco, 2020).

Malware: *"Es un software diseñado para causar daño a dispositivos, sistemas de información, personas e incluye muchos tipos de programas, como spyware, ransomware, caballos troyanos, rootkits, entre otros"* (Softwarelab, 2020).

RedTeam: *"Es un equipo conformado por profesionales de la seguridad que actúan como adversarios para superar los controles de seguridad cibernética. Estos equipos suelen estar formados por piratas informáticos éticos independientes que evalúan la seguridad del sistema de manera objetiva y utilizan todas las técnicas disponibles (que se describen a continuación) para encontrar debilidades en las personas, los procesos y la tecnología para obtener acceso no autorizado a los activos. Como resultado de estos ataques simulados, los equipos rojos hacen recomendaciones y planes sobre cómo fortalecer la postura de seguridad de una organización"*(Purplesec, 2020).

Vulnerabilidad: (INCIBE, 2017) *"Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad*

de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos"

INTRODUCCIÓN

En este documento se presentará un informe técnico a la compañía WHITEHOUSE SECURITY, donde se relacionarán los aspectos evaluados en las actividades de la etapa dos, tres y cuatro, mencionando las recomendaciones que permitan mejorar las estrategias utilizadas por los equipos BlueTeam y RedTeam.

OBJETIVOS

2.1 OBJETIVO GENERAL

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

2.2 OBJETIVOS ESPECÍFICOS

- *“Presentar un informe técnico donde relacione los aspectos relevantes del desarrollo de las actividades anteriores”*
- *“Plantear recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam”.*

INFORME TÉCNICO

3.1 ASPECTOS ETICOS Y LEGALES

3.1.1 De acuerdo con la evaluación realizada al documento “anexo 2 – escenario 2”, se identificó que la compañía WhiteHouse Security realizó la contratación de los profesionales para conformar los equipos BlueTeam y RedTeam, sin revisar el contrato y los acuerdos de confidencialidad; y entregando como prueba de admisión situaciones internas de la compañía.

Lo anterior podría ocasionar pérdida de confidencialidad de la información de la compañía.

Recomendaciones:

- ✓ Revisar los contratos del personal, teniendo en cuenta el código sustantivo del trabajo
- ✓ Revisar las políticas de contratación y los acuerdos de confidencialidad con los empleados.

3.1.2 De acuerdo con la evaluación realizada al documento “anexo 3 - Acuerdo”, se identificaron las siguientes irregularidades descritas en la actividad dos entregada en el campus (MONTOYA, 2020):

a. *“En la cláusula primera, indica que la parte receptora se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados”*
b. *“Hay cuatro numerales en la cláusula cuarta “Obligaciones de la parte receptora”:*

    3. *“No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros”*
    4. *“Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas”*
    7. *“Responder por el mal uso que le den sus representantes a la información confidencial”.*

c. “En la cláusula octava. Solución de controversias, indica que en caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security”
d. “En la cláusula novena. Legislación aplicable, indica que este acuerdo de confidencialidad se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas”.

Lo anterior podría ocasionar el incumplimiento de los artículos *269C y 269F de la “Ley 1273 de 2009”* (MINTIC, 2009), *y el Artículo 67 del código penal* (Leyes, 2020).

Recomendaciones:

Ajustar los acuerdos de confidencialidad y obligaciones de la parte receptora (en este caso experto de Ciberseguridad), sin incumplir los mencionado en la Ley 1273 de 2009 (MINTIC, 2009)., código penal (Leyes, 2020), código de ética de COPNIA (COPNIA, 2020) y *“Ley 842 de 2003”* (Estatuto Tributario, 2020), teniendo en cuenta lo descrito en la actividad dos entregada en el campus (MONTOYA, 2020):

1. *“La información no puede ser divulgada, ni entregada a terceros que no corresponden, pero se deben llevar a cabo los protocolos de operación definidos por la compañía en el caso de que uno de sus empleados identifique actividades sospechosas de espionaje u otro delito”*
2. *“La parte receptora está en la obligación de proteger la información confidencial y de terceros, pero en caso de detectar actividades ilegales de espionaje, deberá llevar a cabo los protocolos de operación definidos por la compañía”*
3. *“Cada miembro de la compañía debe responder por sus actos ilícitos y no éticos, y se deben establecer unas políticas y acuerdos de confidencialidad acordes con los objetivos del negocio y la legislación colombiana”*
4. *“La parte receptora no es la única responsable en caso de encontrarse información ilegal, dado que la compañía debe ser responsable de las acciones que se presentan dentro de la misma”*

3.2 DESARROLLO DE ACTIVIDADES REDTEAM Y BLUETEAM

3.2.1 De acuerdo con la evaluación realizada por el equipo RedTeam, se llevó a cabo la ejecución de las etapas de pentesting sobre dos máquinas Windows que presentaban sospecha de fuga de información, para lo cual se identificaron los siguientes hallazgos:

a. La máquina “win7 se2020x64”, cuenta con el sistema operativo Windows 7 Professional 7601 Service pack 1 6.1 64 bits, el cual es una versión desactualizada y no cuenta actualmente con soporte por parte de Microsoft
b. La máquina “win7 se2020”, cuenta con el sistema operativo Windows 7 Home Premium 7600 6.1 32 bits, el cual es una versión desactualizada y no cuenta actualmente con soporte por parte de Microsoft
c. Se identifica la vulnerabilidad crítica “CVE-2017-0143 / smb_ms17-010” en las dos máquinas Windows
d. Se realiza la explotación exitosa de la vulnerabilidad “smb_ms17-010” en la máquina “win7 se2020x64”.

Lo anterior podría ocasionar pérdida de confidencialidad, integridad y disponibilidad de la información y posibles ataques de ramsonware.

Recomendación:

Realizar la aplicación del parche MS17-010 para las dos máquinas Windows “win7 se2020x64” y “win7 se2020”.

3.2.2 De acuerdo con la evaluación realizada por el equipo BlueTeam, se llevaron a cabo las actividades de contención de un ataque informático y de hardening para la máquina Windows “win7 se2020x64”, evidenciando los siguientes hallazgos:

a. No contaba con antivirus instalado
b. El firewall se encontraba desactivado
c. El Windows defender se encontraba desactivado y, por lo tanto, no tenía actualizaciones instaladas
d. La máquina no contaba mecanismos de autenticación activos.

Lo anterior podría ocasionar pérdida de disponibilidad, confidencialidad e integridad de la información y posibles ataques de ramsonware.

Recomendaciones:

- ✓ Realizar la instalación del agente de antivirus
- ✓ Realizar la activación del Firewall y Windows Defender
- ✓ Crear la contraseña para el usuario
- ✓ Descargar y aplicar las actualizaciones de Windows

- ✓ Definir actividades y responsables para monitoreo periódico a las estaciones de trabajo que permitan mantener y fortalecer la seguridad de las mismas.

ANÁLISIS ESTRATEGIAS REDTEAM Y BLUETEAM

A continuación, se detallan las estrategias recomendadas para los equipos RedTeam y BlueTeam, las cuales permitirán fortalecer las habilidades de dichos equipos y mejorarán los aspectos de seguridad en la compañía “WHITEHOUSE SECURITY”, las cuales se mencionan en (Crowdstrike, 2020)(Eccouncil, 2020)(Amy Hargreaves and James Chamberlain, 2018)(Jelen, 2018):

4.1 ESTRATEGIAS REDTEAM

- ✓ *“Un profundo conocimiento de los sistemas y protocolos informáticos, así como de las técnicas, herramientas y salvaguardias de seguridad”*
- ✓ *“Fuertes habilidades de desarrollo de software para desarrollar herramientas personalizadas para eludir los mecanismos y medidas de seguridad comunes”*
- ✓ *“Experiencia en pruebas de penetración, que ayudaría a explotar vulnerabilidades comunes y evitar actividades que a menudo se monitorean o detectan fácilmente”*
- ✓ *“Habilidades de ingeniería social que permiten al miembro del equipo manipular a otros para compartir información o credenciales”*
- ✓ *“Reconocimiento inicial: inteligencia de código abierto (OSINT) para recopilar información sobre el objetivo”*
- ✓ *“Implementar servidores de comando y control para establecer comunicación con la red del objetivo”*
- ✓ *“Usar señuelos para despistar al equipo BlueTeam”*
- ✓ *“Aplicar técnicas de ingeniería social y phishing para manipular a los empleados para que expongan o revelen información que ponga en peligro sus máquinas”*
- ✓ *“Pruebas de penetración física y digital”.*

4.2 ESTRATEGIAS BLUETEAM

- ✓ *“Una comprensión completa de la estrategia de seguridad de la organización en personas, herramientas y tecnologías”*
- ✓ *“Habilidades de análisis para identificar con precisión las amenazas más peligrosas y priorizar las respuestas en consecuencia”*
- ✓ *“Fortalecimiento de técnicas para reducir la superficie de ataque, particularmente en lo que se refiere al sistema de nombres de dominio (DNS) para prevenir ataques de phishing y otras técnicas de violación basadas en web”*
- ✓ *“Gran conocimiento de las herramientas y sistemas de detección de seguridad existentes de la empresa y sus mecanismos de alerta”*
- ✓ *“Revisión y análisis de datos de registro”*

- ✓ *“Utilizar una plataforma de gestión de eventos e información de seguridad (SIEM) para la visibilidad y detección de intrusiones en vivo y para clasificar alarmas en tiempo real”*
- ✓ *“Recopilar nueva información de inteligencia sobre amenazas y priorizar las acciones adecuadas en contexto con los riesgos”*
- ✓ *“Realizar análisis de tráfico y flujo de datos”.*

VIDEO SUSTENTACIÓN

A continuación, se relaciona el enlace de la sustentación del informe técnico:

https://youtu.be/do5dQrRW2ZI

CONCLUSIONES

En primera medida la Ciberseguridad debe enfocarse a la estrategia del negocio, debe ser una parte fundamental para la operación de las empresas con el fin de que puedan implementarse, mantenerse y/o fortalecer actividades y controles que permitan mitigar los riesgos de la organización.

En la actualidad uno de los activos más importante es la información y, por lo tanto, se deben definir e implementar estrategias de seguridad de la información que estén a la vanguardia de los cambios y avances tecnológicos, para ello se puede contar con dos grandes equipos “RedTeam” y “BlueTeam”, conformados por profesionales en seguridad quienes protegen y aseguran los activos críticos de las organizaciones contra cualquier amenaza, llevando a cabo evaluaciones de seguridad en los sistemas.

BIBLIOGRAFÍA

Amy Hargreaves and James Chamberlain. (2018). *The Roles of Red, Blue and Purple Teams*. https://www.itlab.com/blog/understanding-the-roles-of-red-blue-and-purple-security-teams

Auditool. (2017). *¿Qué es un ciberataque?* 2015. https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque

Cisco. (2020). *What Is Cybersecurity? - Cisco*. Cisco.Com. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

COPNIA. (2020). *Código de ética | Copnia*. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Crowdstrike. (2020). *Red Team VS Blue Team in Cybersecurity | CrowdStrike*. https://www.crowdstrike.com/epp-101/red-team-vs-blue-team/?utm_campaign=dsa&utm_content=latam&utm_medium=sem&utm_source=goog&utm_term=&gclid=CjwKCAjw_Y_8BRBiEiwA5MCBJoS0IOAe38iU55x6L7_t4aB2FBjjHv4SpHZPATIxrcQGtOFFVejCyhoCr_wQAvD_BwE

Eccouncil. (2020). *Red Team vs Blue Team _ EC-Council Official Blog.pdf*. https://blog.eccouncil.org/red-team-vs-blue-team/

Estatuto Tributario. (2020). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [CODIGO_CIVIL]*. http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003_pr001.html

INCIBE. (2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? | INCIBE*. Web. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Jelen, S. (2018). *Cybersecurity Red Team Versus Blue Team — Main Differences Explained*. Securitytrails.Com. https://securitytrails.com/blog/cybersecurity-red-blue-team

Kaspersky. (2020). *¿Qué es la ciberseguridad? | Kaspersky*. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Leyes, C. (2020). *Art. 67 Código de Procedimiento Penal Deber de denunciar Artículo 67 (CPP) - Legislación colombiana 2020*. https://leyes.co/codigo_de_procedimiento_penal/67.htm

MINTIC. (2009). *Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones*. https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MONTOYA, A. M. (2020). *Act_Etapa 2_Ana María Montoya.pdf*. https://campus102.unad.edu.co/ecbti81/pluginfile.php/2925/assignsubmission_file/submission_files/553/Act_Etapa 2_Ana María Montoya.pdf?forcedownload=1

Purplesec. (2020). *Red Team VS Blue Team: What's The Difference? | PurpleSec*. https://purplesec.us/red-team-vs-blue-team-cyber-security/

SGSI. (2017). *¿Cómo realizar un inventario de activos de información?* https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Softwarelab. (2020). *¿Qué es un virus informático? La definición y los 5 tipos*

principales. https://softwarelab.org/es/que-es-malware/
Tecnosfera. (2019). En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. *El Tiempo*, 1–3. https://protecdatalatam.com/ciberseguridad-en-2019-se-reportaron-mas-de-28-000-casos-de-ciberataques-en-colombia/