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

RAFAEL ORLANDO DOMINGUEZ SIERRA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2020

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

RAFAEL ORLANDO DOMINGUEZ SIERRA

Tutor:
JHON FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2020

RESUMEN

Las organizaciones de nuestro mundo actual basan la toma de decisiones en la información que son capaces de obtener producto de su normal desempeño en el mercado, el protegerla de personas no deseadas se vuelve cada día más difícil por la misma tecnología naciente, por los ataques que puede tener, la falta de ética de personas que trabajan conjuntamente con las empresas o puntualmente la falencia del factor humano que la deja vulnerable, estas vulnerabilidades son identificadas por personas externas y tratan de todas las formas posibles de explotarlas para lograr su cometido, de esta manera se puede identificar los dos equipos tratados en el curso, Red Team y Blue Team.

Lo que le compete a Red Team son las personas que se encargan de aplicar todas aquellas prácticas de hacking ético que por medio de simulaciones y entornos controlados permiten conocer las vulnerabilidades que presenta una red de datos y a su vez los equipos que pertenecen a ella, explotarlas de tal manera que sea posible conocer las vías de acceso y los recursos comprometidos, de tal manera que la organización pueda dirigir sus esfuerzos en mitigar estas vulnerabilidades y puedan mantener la información y los activos de la empresa a salvo.

Por otro lado, lo que le corresponde al Blue Team son las personas que se encargan de defender a las organizaciones de los diferentes ataques que se le pueden llegar a presentar a la red de comunicaciones o equipos, este equipo busca realizar la evaluación de todas las posibles amenazas que pueden llegar a afectar la organización y realizar las recomendaciones necesarias para la correcta mitigación de las mismas, razón por la cual es muy importante conocer y dar aviso pronto cuando se estime un ataque, además este equipo permite dar respuesta cuando se presenta un inminente ataque conforme a procedimientos establecidos.

Teniendo en cuenta lo anterior, en el documento es posible apreciar el desarrollo de actividades de aplicación y contención de ataques informáticos en un entorno controlado, los procedimientos realizados y la normatividad vigente que enmarca la situación.

CONTENIDO

1. GLOSARIO

- Ley: Regla o norma dictada por la autoridad competente en que se manda o prohíbe algo.

- Información: Conjunto de datos ordenados de manera lógica y con sentido.

- Seguridad: Conjunto de reglas determinadas para la protección de un objeto.

- Proceso: Conjunto de actividades ordenadas determinadas a un propósito general donde se encuentra un producto.

- Contrato laboral: Acuerdo escrito o verbal en el que dos partes se comprometen a respetar y cumplir las condiciones dadas.

- Delito informático: Acciones que se llevan a cabo para cometer una acción en contra de la ley y que interviene en el campo de la información.

- Ataque informático: Acciones ejecutadas aprovechando la vulnerabilidad de un equipo informático buscando que la información pierda su integridad.

- Herramienta: Instrumento software o hardware utilizado en los procesos de la empresa u organización.

- Contención: Situación donde proceso detiene la ejecución de otro que generalmente causa daño a la propiedad de la organización.

- Hardening: Acciones realizadas por un sistema para generar mayor robustez y no permitir los ataques de ningún tipo.

- Falla de seguridad: Error lógico o físico que compromete la integridad de la información de una organización.

- Equipo de cómputo: Estación de trabajo utilizada por un usuario final en la ejecución de un proceso.

2. OBJETIVOS

2.1 Objetivo general

Analizar el proceso de ejecución y contención de un ataque informático en un entorno real.

2.2 Objetivos específicos

- Mostrar la legislación relacionada con los delitos informáticos.
- Puntualizar el tema de acuerdo laboral de seguridad de la información.
- Observar las acciones relacionadas con el pentesting.
- Resumir un ataque real a la seguridad de la información en un entorno controlado como miembro de un equipo Red Team
- Sintetizar las acciones necesarias para la contención del ataque como miembros de un equipo Blue Team

3. INFORME TÉCNICO RED TEAM Y BLUE TEAM

Desde los inicios de la constitución de cualquier empresa una mirada latente siempre es hacia la información que se maneja, por supuesto que la información se convierte en un activo más para la empresa ya que entre otras muchas cosas permite la toma de decisiones que son tan importantes en cualquier plano empresarial, pero, como es un activo hay que buscar la manera de salvarla y protegerla de ataques que puedan comprometer la integridad de la misma, cuando esto ocurre se concibe el tema de la seguridad de la información, y por este mismo camino inicia el tema de cómo llegar a proteger al 100% la información que se cuenta en la empresa.

Llegar al sistema perfecto no es tarea fácil, ya que a diario surgen nuevas propuestas y entre ellas herramientas las cuales hacen que la persona encargada de la seguridad de la información esté en continua formación y adquiera capacidades para afrontar cualquiera que sea la situación, pero, cuando no se cuenta con personal capacitado en ese perfil se acude a solicitar con personas capaces y con los conocimientos adecuados una prueba de pentesting, la cual nos proporciona la situación actual en temas de vulnerabilidad que posee la empresa.

El producto anterior es de gran importancia para la gerencia, ya que abarca puntualmente las vulnerabilidades presentadas y los objetivos a trazar para mitigar y proteger uno de los activos más importantes de la empresa y que en la práctica apoya cualquier proceso y genera valor agregado frente a otras similares.

3.1 Actuación legal

Uno de los factores más importantes que se deben tener en cuenta cuando se propone realizar un ataque de seguridad informática es el marco legal vigente que actúa en cada país, ya que actúa como guía normativa y se fundamenta en cada uno de los delitos contemplados en su actuar, para el tema de la seguridad de la información se conocen leyes y decretos que nos acogen desde el año 1968 y que han abarcado temas de derechos de autor, pactos internacionales, tratamiento de la propiedad intelectual entre otros.

En lo que compete a la normativa colombiana se debe tener en cuenta la ley 1273 de 2009 que se encamina a los atentados que puede sufrir la información y datos almacenados en sistemas informáticos, y el código de ética del Copnia que enfoca sus esfuerzos en conductas que debe tener el ingeniero o profesional afín con su ejercicio normal de la profesión, ya que son las que puntualmente rigen el tema de la seguridad de la información y los delitos que pueden cometer personas afines a la actividad, esto cobra relevancia porque todas las actuaciones que una persona realice deben estar encaminadas a las buenas prácticas y el mejoramiento de la empresa y no en buscar provecho para cometer delitos previamente conocidos producto de vulnerabilidades conocidas.

3.2 Los acuerdos laborales

Todas las personas en su afán de tener un empleo que permita una mejor calidad de vida dejan a un lado el observar minuciosamente lo contenido en los contratos, muchas veces llenos de vicios y hasta con cláusulas que afectan esa estabilidad laboral que se busca, para el ejercicio se incluyó un acuerdo de contrato para una persona en donde se pudo evidenciar que desde la persona quién realizo la redacción inicial hasta las cláusulas que se encontraban allí hacían parte de un grupo de vicios que iban en contravención a la ley y al código de ética, razón por la cual pudo ser evidente que este contrato no podía ser aplicado a ninguna persona que quiera ser parte de la organización y mucho menos aplicado al comportamiento interno de la persona ya que de inmediato se estará cometiendo un delito a ojos de la ley y una prohibición a la luz del código de ética.

3.3 El pentesting

Los conocimientos que se adquieren todos los días deben siempre aplicarse para temas útiles y no buscar el mal ajeno, basado en esto es posible observar que con el uso del pentesting es posible actuar buscando un impacto negativo en las empresas, esto sucede cuando lo que se busca es la información que almacena esta empresa, sin embargo la palabra encierra mucho más que eso, el pentesting es una actividad adoptada por las empresas que buscan obtener un resultado de la seguridad de su infraestructura, de tal manera que les permita observar todas las vulnerabilidades que presentan para corregirlas y mantener el sistema lo más seguro posible.

El actuar bajo el pentesting es hablar del hacking ético, el cual apropia herramientas que permiten visibilizar las vulnerabilidades propias de un equipo puntual, el cual se convierte en el objetivo y el atacante hace uso de todas las posibilidades disponibles para conocer, explotar y obtener lo que se busca, de esta manera es posible reconocer las vulnerabilidades que se tienen y mostrar las acciones que son aplicables para mitigar el riesgo.

3.4 Red Team

El Red Team hace referencia a los temas de ataque a vulnerabilidades presentadas por una empresa, específicamente las amenazas que pueden enfrentar en su normal desarrollo de actividades, las cuales son producidas por los mismos equipos e infraestructura con la que cuentan.

El Red Team se enmarca en el hacking ético y busca la emulación de amenazas en entornos controlados para representar la seguridad que se tiene frente al punto de vista de los atacantes, lo que muestra la capacidad real que tiene una empresa para proteger sus activos más importantes como lo es la información.

Tomando en cuenta la actividad desarrollada para Red Team, es posible ver como desde el escaneo de una máquina propuesta es inevitable conocer sus vulnerabilidades, puesto que desde este punto se puede establecer las vulnerabilidades presentadas, ya que el reporte de las vulnerabilidades arroja como resultado el origen del problema, y es aquí donde apreciamos que una actualización sin realizar es la puerta de acceso para un ataque.

Esa vulnerabilidad presentada es el origen del ataque exhibido en la actividad que permitió obtener el archivo buscado, las empresas generalmente no se preocupan por mantener sus equipos actualizados por los tiempos que permanecen inactivos, el costo que genera la interrupción de un empleado o el consumo de ancho de banda para ejecutar la actualización, pero a la larga son muy efectivas para mitigar accesos no autorizados y proteger la información contenida allí.

3.5 Blue Team

El Blue Team es el equipo de personas capaces de identificar y mitigar una vulnerabilidad o ataque que se presenta en los activos de una organización, generalmente buscando tener acceso a la información que se contiene allí, realizan el análisis de los diferentes sistemas y componentes con el fin de garantizar la seguridad informática.

El Blue Team dentro de las acciones que le son posible realizar se encuentra el Hardening, que no es más que el endurecimiento del sistema operativo y el hardware encargado de dar protección a la información, este endurecimiento es una actividad que se lleva a cabo en cada una de las máquinas que pertenecen a la empresa ya que la más vulnerable puede ser el acceso para los atacantes.

Estas propuestas deben estar encaminadas a dar la mayor robustez posible para evitar que cualquiera pueda ingresar y tomar el control de la información contenida, pasando desde acciones que el mismo usuario final puede llegar a hacer, pasando por la implementación de software necesario y llegando hasta la creación de reglas para cada procedimiento, de todo esto lo más importante que se debe observar

siempre es el tema de la actualizaciones que de manera nativa ofrecen protección a vulnerabilidades globales aportando el tema de parches de seguridad.

Algunas veces no es posible considerar tener un equipo Blue Team en la empresa, para ello se debe conocer que es posible contratar un servicio SIEM o un CIS, el primero que es un software que proporciona información acerca de las principales y más comunes amenazas, identificarlas, responderlas y neutralizarlas, la segunda son un conjunto de acciones priorizadas que agrupadas forman un conjunto de prácticas de defensa que identifican, controlan y mitigan los ataques más comunes a las redes de datos, todo esto muestra y deja en evidencia que mantener el sistema protegido no es tarea fácil, pero hay opciones que se pueden adoptar para que funcione y tenga la robustez buscada.

Una vez terminado el tema referente al seminario especializado, adjunto en enlace de la sustentación realizada, se encuentra alojada en el servidor de YouTube en el siguiente enlace:

https://www.youtube.com/watch?v=uAwpTfmx6Pg&ab_channel=RAFAELORLANDODOMINGUEZSIERRA

4. RECOMENDACIONES

- Mantener al equipo de trabajo de la organización en constante capacitación que permita mitigar cualquier vulnerabilidad por parte del usuario final.

- Establecer un equipo de trabajo ya sea interno o externo que permita identificar y controlar las amenazas a las que está expuesta la organización.

- Tener en la organización un equipo de trabajo encargado de la parte legal y la legislación vigente en temas de seguridad de la información.

- Procurar realizar acciones de pruebas de penetración y hacking ético a la infraestructura de redes y equipos de cómputo para observar su comportamiento y posibles vulnerabilidades encontradas.

- Mantener la buena práctica del uso de contraseñas para los equipos de cómputo de la organización.

- Mantener siempre actualizados los equipos de cómputo con la última actualización enviada por el proveedor del sistema operativo.

- Evitar dejar puertos abiertos a comunicaciones que no tengan ningún uso.

- Utilizar infraestructura software o hardware que permita el control de acceso desde fuera de la red de datos y de esta manera proteger los recursos de la empresa

- Mantener una documentación actualizada en temas de ataques informáticos y acciones pertinentes para proteger los recursos de la empresa.

5. CONCLUSIONES

- Se evidenció que la legislación vigente debe estar siempre a la vista de aquellas personas que obedecen a la actividad de la seguridad de la información.

- El código de ética hace parte fundamental para el actuar de los ingenieros y afines que trabajan con la seguridad de la información.

- Se establece el pentesting como método de intrusión para la verificación de vulnerabilidades que presenta la organización.

- Se mostraron las características legales que debe tener una empresa bajo las normas de las leyes de seguridad de la información vigentes.

- Se evidenció como desde el Red Team existe la posibilidad de tratar una vulnerabilidad de la organización como una ventaja para los atacantes.

- Se comprobó como el Blue Team se convierte en el grupo necesario en la organización que permite la mitigación de un ataque informático.

- Se expusieron las alternativas que tiene la organización para tratar y mitigar un ataque informático.

6. BIBLIOGRAFÍA

Comstor, S. (26 de febrero de 2016). *LAS 10 MEJORES PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN*. Obtenido de https://blogmexico.comstor.com/las-10-mejores-practicas-de-seguridad-de-la-informacion

Corponet. (12 de juinio de 2015). *La importancia de la información para la toma de decisiones en una empresa*. Obtenido de https://blog.corponet.com.mx/la-importancia-de-la-informacion-para-la-toma-de-decisiones-en-la-empresa#:~:text=La%20importancia%20de%20la%20informaci%C3%B3n%20para%20la%20toma%20de%20decisiones%20en%20la%20empresa&text=La%20importancia%20de%20la%20informa

DesdeLinux. (s.f.). *Seguridad de la Información: Historia, Terminología y Campo de acción*. Obtenido de https://blog.desdelinux.net/seguridad-informacion-historia-terminologia-campo/

España, C. (12 de noviembre de 2019). *Pasos para que los Red Team tengan éxito en las compañías*. Obtenido de https://cso.computerworld.es/tendencias/pasos-para-que-los-red-team-tengan-exito-en-las-companias

Gestión, B. e. (12 de octubre de 2017). *ISO 27001 ¿Cuáles son las buenas prácticas que se utilizan en seguridad de la información?* Obtenido de https://www.pmg-ssi.com/2017/10/iso-27001-buenas-practicas-seguridad-informacion/

Group, S. (22 de noviembre de 2018). *LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA*. Obtenido de https://www.serban.es/la-importancia-de-la-seguridad-de-la-informacion-en-la-empresa/

Halon, J. (30 de agosto de 2018). *So You Want To Be a Pentester?* Obtenido de https://jhalon.github.io/becoming-a-pentester/

imperva. (s.f.). *Penetration Testing*. Obtenido de https://www.imperva.com/learn/application-security/penetration-testing/

Ingeniería., C. P. (2016). *RÉGIMEN COLOMBIANO DEL EJERCICIO ÉTICO PROFESIONAL DE LA INGENIERÍA*. Obtenido de https://xperta.legis.co/visor/copnia

Isabella Gandini, A. I. (s.f.). *Ley de Delitos Informáticos en Colombia*. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Jelen, S. (s.f.). *Top 30+ Best Blue Team Tools*. Obtenido de https://securitytrails.com/blog/blue-team-tools

MediaCloud. (s.f.). *Ataque cibernético: consecuencias, cómo actuar y cómo protegerse*. Obtenido de https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/

MINTIC. (6 de noviembre de 2016). *mintic.gov.co.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

SecurityTrails. (7 de diciembre de 2018). *Cybersecurity red team versus blue team - main differences explained*. Obtenido de https://securitytrails.com/blog/cybersecurity-red-blue-team

ZDNet. (14 de october de 2015). *How to launch an effective Red team enterprise hack*. Obtenido de https://www.zdnet.com/article/top-tips-to-launch-an-effective-red-team-enterprise-hack/