Capacidades técnicas, legales y de gestión para equipos de blue team y red team

Luis Velandia Almeida

Universidad Abierta Y A Distancia - Unad
Escuela De Ciencias Básicas, Tecnológicas e Ingeniería
Especialización En Seguridad Informática

Bogotá Colombia
Noviembre de 2024

Capacidades técnicas, legales y de gestión para equipos de blue team y red team

Luis Velandia Almeida

Universidad Abierta Y A Distancia - Unad
Escuela De Ciencias Básicas, Tecnológicas e Ingeniería
Especialización En Seguridad Informática
Docente: Ever Luis Arroyo Baron

Bogotá Colombia
Noviembre de 2024

Resumen

Las necesidades emergentes de la sociedad y los constantes desarrollos tecnológicos impactan a los profesionales de la informática, especialmente a aquellos involucrados en la gestión de riesgos de seguridad informática, porque a mayor tecnología, significa más riesgos, más amenazas y, por lo tanto, una mayor necesidad de implementación en acciones, proceso y herramientas que ayude a gestionar todos los riesgos que una organización enfrenta en todas las áreas y recursos. por lo que es necesario utilizar todas las herramientas y recursos humanos altamente calificados para brindar un seguimiento y mejora continua para el aseguramiento integral de los procesos y actividades de la organización, esto implica que la gestión de recursos de TI, estén alineados con las políticas y objetivos del negocio.

Red Team y Blue Team proporcionan dos escenarios de ciberseguridad, ya que Red Team tiene como objetivo explotar vulnerabilidades para exponer debilidades en los sistemas de información o la infraestructura tecnológica, impactando así el contexto de seguridad en tiempo real, todo este proceso debe estar bajo control siempre proporcionando en un entorno que no llegue a afectar la operación de la organización. En lo que respecta al equipo Blue Team, tiene como labora centralizar el monitoreo continuo de la seguridad utilizando herramientas, técnicas y las mejores prácticas que puedan mitigar el impacto de los incidentes que se puedan presentar, es así como estos equipos trabajan de manera articulada y sincronizada, para mantener el e equilibrio y la estabilidad en los procesos de la organización desarrollando a su vez los planes de acción para mejora continua los componentes de la infraestructura tecnológica, dando cumplimiento a los lineamientos normativos que aplican de acuerdo a la legislación Colombiana y demostrando la importancia de implementación e inversión en seguridad, como un postulado de crecimiento y estabilidad empresarial, bajo los parámetros y principios éticos que deben tener los profesionales se de seguridad, promoviendo el cumplimiento de las acciones legales en relación al tratamiento de datos, para cumplir con la confidencialidad, integridad y disponibilidad de la información.

Índice

Lista De Imágenes

Glosario

Acceso No Autorizado: Acceso a servicios web, ordenadores y/o datos confidenciales mediante suplantación de credenciales de usuarios o de manera abrupta.

Activo De Información: Se refiere a información, datos o dispositivos que tenga valor para la organización, datos, aplicaciones, equipos informáticos, redes, servidores, los cuales son susceptible de ser atacados por un ciberdelincuente.

Amenazas: Es la explotación o aprovechamiento de una vulnerabilidad, buscando acceso a información y recursos sensibles, causando daños.

Análisis De Riesgos: Proceso para identificar los activos dentro de una organización, así mismo analiza su vulnerabilidad, amenazas y las probabilidades de ocurrencia e impacto en la organización.

Autenticación: Procedimiento para validar la identidad que requiere un usuario mediante una admisión en un sistema de control de acceso.

Blue Team: Equipos de defensa informática los cuales evalúan la seguridad, detectan amenazas y realizan una mitigación o control en un tiempo oportuno.

Ciberseguridad: Toda buena práctica orientada a proteger los recursos de una infraestructura tecnológica, incluye redes, aplicaciones y datos, estas buscan salvaguardarlos y protegerlos de amenazas y accesos no autorizados.

CIS: Conjunto de buenas prácticas en seguridad informática, guía para alcance de meta en la gestión de los objetivos de las organizaciones.

Criptografía: Son técnicas que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado, que resulta difícil de leer para todo aquel que no tenga las claves o el sistema mediante el cual ha sido cifrado.

Delito Informático: Son las acciones u omisiones realizadas a través de medios informáticos y que son penados por la Ley.

Ethical Hacking: Acciones y herramientas para localizar vulnerabilidades y debilidades en los sistemas de información y ordenadores duplicando las acciones y la intención de los ciberdelincuentes malintencionados que buscan eludir la seguridad y buscar brechas en los sistemas que pueden explotarse.

Exploit: Código o parte de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de explotar una vulnerabilidad de seguridad de un sistema de información para conseguir un procedimiento no deseado del mismo.

Hardenizacion: Conjunto de actividades enfocadas en reforzar la seguridad de los sistemas, con el fin de reducir las amenazas y vulnerabilidades, buscando una infraestructura mas segura y eficiente.

IDS/IPS: Sistemas software, diseño para detección de intrusos informáticos en tiempo real y detecta y bloque amenazas.

Pentesting: Técnicas de seguridad, basadas en la ejecución de pruebas simuladas para detección de vulnerabilidades en los sistemas de información, redes y aplicaciones.

Red Team: Son equipos de ciberseguridad, encargados de realizar pruebas y simulación de ataques informáticos, con el fin de validar la seguridad de un sistema u equipo, y así mismo validar su impacto.

SIEM: Solución de seguridad, apoya la gestión de información y eventos en seguridad.

Vulnerabilidad: son las falencias que puede tener un sistema o estructura tecnológica, la cual puede ser utilizada por un atacante y comprometer su seguridad.

Introducción

La ciberseguridad es hoy en día una de las disciplinas mas activas dentro de las organizaciones, ya que es el conjunto de acciones, normas, leyes. protocolos y herramientas enfocadas en la protección de los sistemas, redes y datos, esto en relación con las creciente amenazas y riesgos a as que se exponen diariamente, en este sentido alcanza el nivel mas alto de relevancia dentro de los proceso organizacionales, toda vez que la era digital conlleva a que sea un proceso transversal de apoyo para la gestión y cumplimiento de los objetivos que plantea el negocio, ya que la actividad, toda actividad empresarial produce constante mente la demanda de servicio digitales y por ende la producción de información, la cual requiere un tratamiento seguro, y en concordancia con las políticas empresariales y las leyes imputables que rigen la sociedad.

Las acciones ofensivas y defensivas de los equipos de seguridad Red Team y Bue Team, aparte de ser parte integral de la seguridad en las organizaciones, deben documentar su actuar, de manera que la alta dirección de la organización, pueda tomar las decisiones resultado de auditorías y acciones defensivas realizadas posterior a las incidencia o ataques presentados que afectan la seguridad de la información, por ende y en relación al proceso desarrollado mediante loas casos y escenarios planteado a largo del seminario especializado en desarrollo, por ende debemos presentar el informe técnico, que permita describir el proceso desarrollado y plantee a su vez ejecuta las acciones necesarias a fin de reforzar los proceso de seguridad, mediante la implementación de equipos de seguridad y los proyectos de apoyo que estos deben administrar.

Objetivos

1.1 objetivos general

Generar, diseñar e implementar las estrategias de seguridad enfocadas en la contención de amenazas y riegos, mediante procesos de análisis de la infraestructura tecnológica, a partir la experiencia en los casos aplicados, esto con el apoyo de las acciones, guías, normas y herramientas especializadas.

1.2 Objetivos Específicos

Describir los procesos ejecutados en la ejecución de pruebas de seguridad y contención realizadas por los equipos de seguridad Red Team y Blue Team.

Conocer las acciones y normas legales aplicables a los procesos de hacking ético como apoyo al proceso de seguridad informática.

Proponer acciones de mitigación y control de riesgos, mediante implementación de políticas, acciones y herramientas especializadas.

Presentar las recomendaciones y medidas de control propuestas para mejorar y reforzar la seguridad en las organizaciones.

Documentar las estrategias resultado del aprendizaje y contexto legal aplicable, mediante un informe técnico que permita dar a conocer y justificar los proyectos a ejecutar y las guías de implementación sugeridas.

2. Desarrollo del Informe Técnico

Dentro de los procesos realizados por los equipos de seguridad Red Team y Blue Team, a continuación se describen las acciones y apreciaciones mas relevantes a los largo del desarrollo del ejercicio aplicado, en aras e poder evidenciar no solo el proceso técnico, sino lo el marco legal y ético que esta estrictamente ligado a la implementación de las políticas y actividades propias de la ciberseguridad en las organizaciones, en este contexto y en relación con los escenarios propuestos para el desarrollo de las pruebas de intrusión y contención, se describe de manera general cada acción de acuerdo al caso aplicado y su importancia dentro del marco de la gestión e implementación para el mejoramiento de la seguridad dada por los equipos de seguridad.

2.1 Etapa 1

En el inicio del ejercicio de la seguridad y con enfoque en equipos Red Team, encontramos como primera medida, el contexto de la normatividad aplicable para la aplicación de medidas de control judicial en relación con los delitos informáticos, para el caso tenemos como referente a la ley 1273 de 2009 la cual compone los pilares fundamentales de la normativa colombiana en relación con los delitos informáticos. Esta ley provee de los tipos penales aplicables, y estableció un marco jurídico para la protección de la información y los datos, esta ley colombiana cobija un amplio contexto de delitos informáticos, con lo cual busca generar una respuesta integral a las diversas amenazas cibernéticas y los riesgos asociados a estas.

Así mismo la ley 1581 de 2012, aporta lineamientos específicos y muy relevantes frente a la protección de datos personales, cuya responsabilidad de la organización es un cumplimiento estricto, buscando proteger al generador de datos y ofreciendo al seguridad dentro de las cadena de custodia y tratamiento que pueda recibir su información, así mismo es responsabilidad de la organización establecer sus políticas, y resoluciones que alineada a la legislación puedan garantizar el cumplimiento legal y generar la confianza a sus clientes, empleados y proveedores.

Para este escenario, además pudimos evaluar las fases que componen un proceso de pentesting, enfocado en la acción ética y legal para aplicación de pruebas de penetración, cuyo objetivo es identificar las brechas de seguridad existentes en la organización, mediante ataques simulados y controlados, permitiendo un despliegue seguro que aporte a la construcción de las medidas de seguridad y control de acuerdo con el nivel se protección evaluado y evidenciado.

Recordemos que pentesting no solo es un proceso técnico, toda vez que este debe estar previamente conciliado, definiendo alcance y responsabilidades, bajo documentación de proceso y en relación con las fases, las cuales se define:

Reconocimiento – Recopilación de información y definición de objetivos.

Análisis de vulnerabilidades – Identificación del entorno de trabajo y búsqueda de brechas en seguridad.

Explotación – Posterior a los resultados del escaneo anterior se realizan las explotaciones de acuerdo con las vulnerabilidades identificadas y su explotación.

Escala e privilegios – Una vez realizada la explotación y con acceso al sistema objetivo, se escalan los privilegios para contar con un control total y sostenido.

Informe – Para esta fase de realiza la documentación de los procesos realizado, y los resultados obtenidos, para ser contrarrestados con el equipo Blue Team.

Así mismo estos procesos deben ser llevado a cabo mediante un acuerdo de confidencialidad, el cual define el alcance y garantiza protección en caso de omisiones o excesos dentro de la ejecución de las acciones que realiza el equipo ofensivo Red Team, a su vez este es el responsable de la implementación y construcción del banco de trabajo, el cual permite contar con las herramientas y diseño estructural para llevar a cabo las auditorias de seguridad dentro del contexto técnico.

El banco de pruebas establecido para un proceso posterior de explotación, se compone de la instalación de dos sistemas operativos, estos sobre un servicio virtualizado, en el cual contamos con una maquina Kali Linux, especializada para procesos de ciberseguridad y pruebas de penetración, esta cuenta con una suite muy avanzada, dentro de la cual podemos encontrar software como Nmap, utilizado para el escaneo de puertos, redes y vulnerabilidades, así mismo en este escenario tenemos Metasploid, herramienta muy eficiente para la explotación de vulnerabilidades y así mismo tener el acceso a la maquina objetivo, y en este sentido para el ejercicio propuesto contamos con otro sistema, el cual es un Windows 7, el cual cuenta con un aplicación vulnerable sobre la cual se podrán realizar pruebas posteriores.

Los datos técnicos se relacionan a continuación:

- El software de virtualización Virtual Box en su versión 7.0.18, la cual se monta sobre una maquina host Lenovo que cuenta con 8 GB de memoria RAM procesador Intel Core i5 12th Gen y unidad de almacenamiento de 500 GB en estado sólido.

- Sistema operativo basado en Lunix, y especializado en procesos de ciberseguridad, para el caso usaremos Kali Linux versión 2024.3 para ambiente de 64 bits

- Máquina instala es un Windows 7 64 bits, Versión 6.1 compilación 7601 Service Pack 1

Como recomendación dentro del contexto de la etapa 1, se requiere documentar, publicar y socializar una política de estricto cumplimiento y eficiente frente al desempeño normativo, relacionado con el tratamiento de datos personales y las consecuencias legales ante incumplimientos éticos y profesionales relacionados con el tratamiento de la información, su cadena de custodia y la integridad que se requiere en estos procesos empresariales.

2.2 Unidad 1 Etapa 2

Continuando con el desarrollo de las actividades establecidas para aplicación de resultados sobre los ejercicios propuestos nos encontramos con los escenario para analizar el actuar ético y legal que enmarca las actividades de los profesionales en seguridad, esta etapa nos permite evaluar las condiciones en las cuales de debe desarrollar las actividades de un proceso de auditoria y los marcos legales aplicables, así mismo pudimos evaluar las fallas de gestión de recursos humanos, toda vez que la seguridad es un proceso transversal que involucra a todos los actores de la operación y en este sentido a los calanes de contratación, quienes deben ser garantes e los proceso contractuales a finde contar con personal no solamente altamente calificado, sino además éticos, y son antecedentes que pueden afectar el nombre y la integridad de los datos y recurso dispuestos, es así como debemos para el caso de los ingenieros lideres de seguridad verla por el cumplimiento de los lineamientos establecidos por la legislación colombiana vigente.

Es de precisar que para esta etapa se busca contextualizar la importancia de contar con proceso ajustado a la normatividad y el contexto ético necesario para operar, conociendo de fondo las implicaciones legales que conlleva el actuar fuera de lo ético y legal, así mismo como fue definido en la etapa anterior, vemos como debemos articular un proceso de pentesting mediante un proceso de hacking ético.

Este es un contexto que implica, herramientas avanzadas y grandes conocimientos en informática, ramas como la programación, manejo de sistemas basados en Linux y buen manejo de redes, lo cual les proporciona unas cualidades que pueden explotar a alto nivel.

Todo esto debe estar dentro del contexto ético ya que son encaminadas a poder apoyar proceso de seguridad, realizando pruebas controladas y respetando las políticas de tratamiento de datos y la confidencialidad necesaria para operar.

A continuación, recordaremos las premisas de un acuerdo de confidencialidad que permitirá a los profesionales de seguridad ejercer y cumplir con los objetivos propuestos si afectaciones a la operación y dentro del marco legal.

Imagen 1 Acuerdo de Confidencialidad

Fuente: https://blog.hubspot.es/sales/que-es-acuerdo-confidencialidad-nda

Si bien el actuar ético, moral y profesional de todo colaborador, corresponde a su formación y trayectoria, si debe ser una responsabilidad empresarial, las buenas prácticas de contratación y selección del personal, toda vez que se esta entregando no solo funciones sino además activos importantes para una administración, en este sentido se requiere un proceso de interventoría a nivel directivo que permita monitorear cada proceso de incorporación para contar con el personal idóneo no solo a nivel técnico si no ético, que aporte al crecimiento y seguridad de la organización.

2.3 Unidad 2 Fase 3

Para esta etapa como profesionales en ciberseguridad, debemos analizar y demostrar las capacidades técnicas evidenciando la ejecución de fases de pentesting mediante la activación del banco de trabajo estructurado en la primera etapa, para esto nos basamos en el escenario # 3 el cual nos plantea una situación de perdida de información, resultado de un acceso no autorizado, explotando vulnerabilidades identificadas en aplicaciones bajo ejecución en un ordenador con sistema operativo Windows 7.

En el laboratorio realizado, pudimos ejecutar y documentar las fases llevadas a cabo por profesionales hacking ético, ejecutando a la medida las fases de pentesting, lo cual nos permitió evidenciar las acciones que ejecutan los delincuentes cibernéticos, y las brechas de seguridad que presentaba la organización y consecuencia de esta la perdida reportada, con esto se puede determinar las causales, las debilidades y el impacto que esta genera no solo en el momento de la intrusión, sino además a largo plazo, toda vez que se pierde la custodia de la información, que puede tener destinos de carácter extorsivos y suplantación.

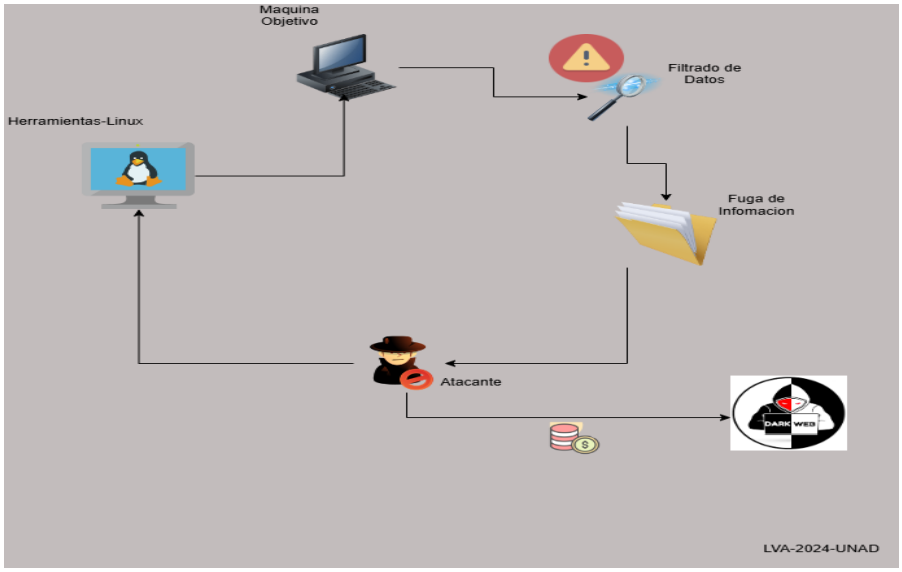
En consecuencia a los anterior , se realiza el proceso de escaneo de vulnerabilidades con la herramienta Nmap, l cual se ejecuta desde la terminal de Kali Linux, la cual busca conexión con la maquina objetivo, en la cual se encuentra la aplicación vulnerable, posteriormente con la ayuda de la herramienta Mestasploid, se ejecutan las acciones de intrusión y elevación de privilegios para acceder remotamente y poder cargar el contenido malicioso o simplemente la extracción de datos allí contenidos, como resultado de este proceso de pentesting, se genera el reporte correspondiente, el cual permite evidenciar fallas a nivel de seguridad, como lo son, malas configuraciones dentro de las reglas de firewall, ausencia de sistemas IDS para el monitoreo de red, falta de actualizaciones de parches de seguridad en sistema operativo y compilación del software, fallas en el levantamiento de matrices de riesgos, procesos de auditoria deficientes y falta de capacitación de los usuarios finales.

En conclusión, general la organización no cuenta con un control de seguridad ni equipos encargados de mantener y garantizar una operación segura y continua, fue muy sencillo demostrar las falencias que deben ser inmediatamente controlados y comunicar a la alta dirección para toma de decisiones que puedan reforzar la seguridad.

Por el desarrollo anteriormente descrito, vemos la importancia de la implementación de equipos de seguridad en las organizaciones en una actividad que hace parte de las buenas prácticas que deben ser política para garantizar la seguridad de la información y así proteger los activos a nivel de datos e infraestructura tecn0logica, es vital comprender la importancia de invertir no solamente en infraestructura si no en recurso humano altamente calificado, para que este se encargue de la administración ética de los sistemas de información corporativos.

Para el ejercicio realizado, a continuación, se describe de manera general como se plantea el proceso de intrusión realizado, desde la óptica de un atacante dentro del sistema, lo cual origino las fugas de información, posteriormente se complementará con la descripción grafica del proceso de pentesting que está inmerso en la ejecución del laboratorio y que define las fasea aplicada por el equipo Red Team.

Imagen 2. Esquema de ataque informático.



Fuente: Propia, Luis Velandia 2024.

De igual manera em la simulación realizada por Red Team se aplican los principios generales de las fases definidas en pentesting a fin de lograr la misma acción desde el enfoque de aprendizaje en seguridad para un posterior proceso defensivo.

Teniendo en cuenta la situación presentada y expuesta mediante la auditoria prueba de penetración, es clara la necesidad de implementación de los equipos de seguridad, que permitan de mare continua la ejecución de acciones controladas a fin de evaluar el estado de seguridad y contrarrestar de igual manera los riesgo y amenazas identificadas para lograr una gestión de recursos TI que pueda dar un valor agregado a la organización.

Imagen 3. Fases del Pentesting.

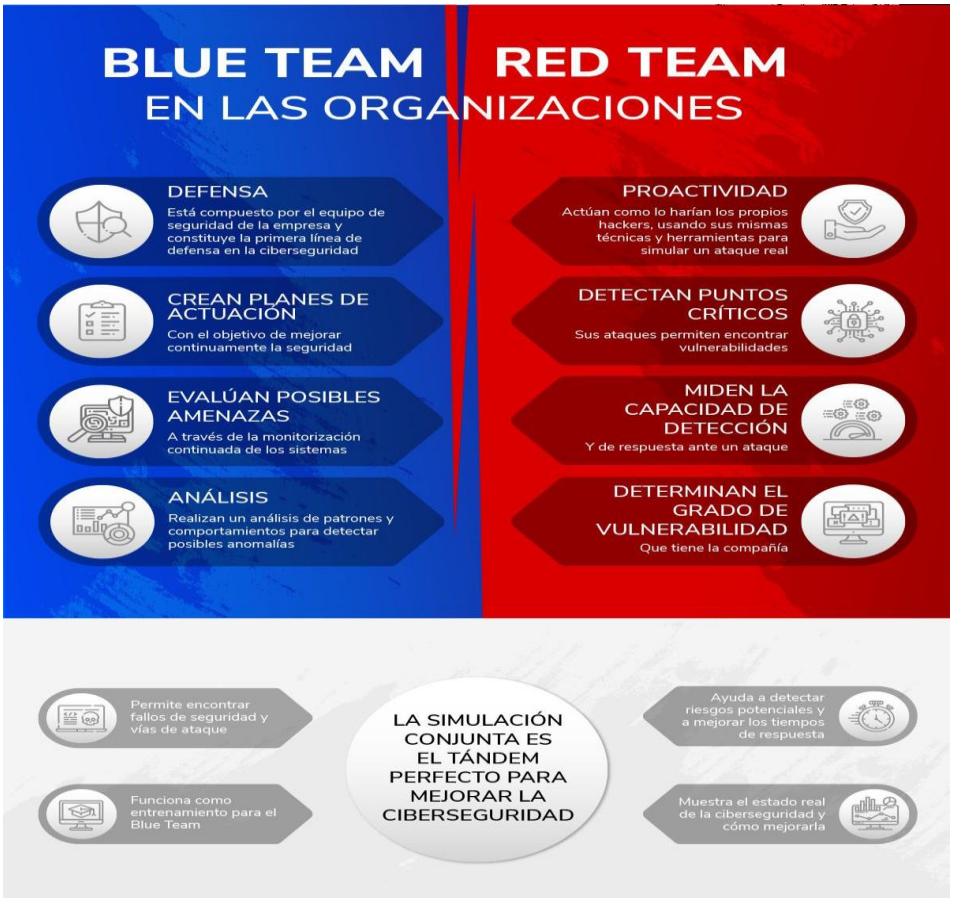
Fuente: https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/

2.4 Unidad 3 Etapa 4

Para la siguiente etapa y en consecuencia al laboratorio realizado por el equipo Red Team, encontramos un escenario que nos plantea la necesidad de articular procesos defensivos y actividades de control para atender los incidentes presentado y promover la prevención para reducir la tasa de ocurrencia y de esta manera reforzar la seguridad de la organización.

Antes de entrar en detalles frente a los descrito en este ultimo proceso, debemos tener muy claro el esquema comparativo para identificare las acciones que ejecuta cada equipo de seguridad y poder conocer la importancia de su implementación y las estrategias que estos ofrecen para el concepto general de seguridad informática.

Imagen 4. Red Team vs Blue Team.



Fuente: https://globalt4e.com/infografia-blue-team-red-team-organizaciones/

Para el proceso defensivo, es importante tener en cuenta muchas variables de las cuales depende el éxito de la implementación de estrategias Blue Team, y diferenciar este concepto de los equipos de respuesta a incidentes, que si bien están orientados a proceso defensivo, estos actúan en consecuencia de la identificación de la materialización de una amenaza, en este sentido son de gran utilidad, para la atención inmediata, controlando y asilando el escenario para mitigar el impacto, aun así este no contempla acciones de control evolutivo y constante que garanticen promover una postulación defensiva más avanzada.

En este sentido la organización debe promover como estrategia la implementación de un plan de seguridad informática, el cual pueda dar respuesta a la necesidad de protección, control y mitigación de riesgos, este plan debe contemplar tres acciones principales.

- ✓ Establecer las acciones necesarias, dentro del contexto digital para la protección de datos de la organización, aliando a las políticas y cumplimiento normativo aplicable.

- ✓ Debe tener la capacidad de enfrentar e implementar controles para soportar cualquier tipo de ataque realizado por ciberdelincuentes, garantizando contención y respuesta inmediata.

- ✓ Impedir la fuga o exposición de la información sensible y privada de la organización, sin omitir las responsabilidades asociadas, contemplando el accionar jurídico aplicable en referencia a la protección de datos y sus políticas.

Dentro del plan de seguridad debe estar inmerso el equipo de respuesta a incidentes, el cual debe estar preparado, realizar el análisis y detección de amenazas, realizar contención del ataque y activar el plan de recuperación, así mismo apoyara la gestión para definir mediante la experiencia las acciones necesarias post incidente.

En este sentido es vital la adopción de normas estandarizadas en relación a proceso de seguridad, y puntualmente a la gestión de incidentes, tal como se establece en la ISO/IEC 27035, la cual provee el ciclo de gestión, donde encontraremos: Preparación -Identificación – Contención – Erradicación - Recuperación y Aprendizaje, todos estos pasos son la base de la respuesta oportuna para una atención de incidentes eficiente y con soporte legal ante la responsabilidad legal que se pueda derivar de una intrusión detectada que afecte datos e información sensible.

Es muy importante tener presente que todas las medidas de contención en seguridad son importantes, validas y eficiente, pero las acciones de Blue Team son particularmente un postulado de medidas continuas y evolutivas, tal como se resume a continuación.

Imagen 5. Objetivos Blue Team

Fuente: https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/

Es muy importante que en la organización se establezcan políticas de control y adopción de recomendaciones CIS, la cuáles son parte de una alternativa de controles y pruebas para reforzar la seguridad de la organización, así mismo están los sistema de seguridad SIEM, las cuales son herramientas para aumenta niveles de seguridad, dentro de estas se encuentra procesos de monitoreo, y muy importante la documentación de los registros asociados que a su vez apoyan el cumplimiento de normas y leyes vigentes que hacen parte de los objetivos que debe cumplir toda organización en relación a las seguridad y confianza que se debe dar a clientes, usuarios y proveedores.

Finalmente es muy importante conocer el alcance de los equipos de seguridad Blue Team está enfocado en poder ejecutar un plan director que permita la proposición, y priorización para implementar proyectos que apoyen la seguridad, como lo puede ser un escenario de hardenizacion, la cual busca contar con proceso de apoyo como lo son:

Auditorias, en este sentido debemos realizar revisión de todos los sistemas, aplicaciones y entorno de red, de esta manera podremos contar con una visión de las capacidades de la infraestructura, validando los riesgo, amenazas y vulnerabilidades que cada uno de los compontes de la infraestructura tecnológica tiene, en este caso debemos contar con nuestra matriz de riesgo, la cual nos permita ponderar y priorizar las áreas críticas para intervenir y así implementar medidas y herramientas de control.

Eliminación de servicios no esenciales, se deben eliminar los servicios, software y hardware que no se requieren en la operación, así mismo se debe controlar el acceso a sitios en internet que no estén relacionados con la operación, así mismo debemos controlar las actualizaciones.

Guías de implementación técnicas en seguridad, la adopción de estas guías establecidas por el ministerio de defensa de los Estados Unidos son documentos de lineamientos específicos y controles de seguridad de productos y versiones para apoyar a las organizaciones a cumplir con las políticas de seguridad necesarias, estas guías contemplan:

- Configuraciones seguras, política de gestión de contraseñas.
- Controles de acceso, definición de roles y doble factor de autenticación.
- Actualizaciones de los sistemas y aplicaciones, orientados a los parches de seguridad.
- Registro y monitoreo de redes y sistemas, mediante control de eventos.
- Fortalecimiento de seguridad en la red, segmentación, mejoras de firewall e implementación de sistemas IDS.
- Política de Backup y recuperación, integrando servicios fuera de la red.

- Protección de datos mediante cifrado de información y retención.

- Educación y toma conciencia para los actores del sistema, esto en relación con gestión de riesgos y seguridad.

Dentro del proceso de Hardening encontramos diversas herramientas de apoyo, para e caso puntual veremos tres opciones que son de licencia GPL y apoyaran la gestión de seguridad.

1. **OSSEC**: Este es un sistema para intrusiones (IDS) que apoya el proceso de análisis de seguridad, revisando los registros de la red.

2. **Rkhunter**: Herramienta utilizada en la verificación ante presencia de rootkits, backdoors y exploits locales, gestionado la identificación de vulnerabilidades en el sistema.

3. **OpenVAS**: Una herramienta para análisis de vulnerabilidades que se basa en el escaneo de sistemas buscando debilidades y genera los informes detallados para el hardening.

Si bien la inversión de seguridad puede ser un elemento para evaluar por parte de algunas organizaciones, toda vez que esto tiene injerencia en sus proceso administrativo y financiero, existen alternativas para apoyar la gestión de seguridad mediante herramientas de apoyo que se pueden implementar sin necesidad de licenciamiento, y tiene una respuesta efectiva, ofreciendo seguridad en su despliegue.

Por lo anterior se pueden recomendar como alternativas de apoyo las siguientes herramientas a nivel software, sin dejar de lado el postula más importante que se relaciona con la capacitación del personal en materia de seguridad, ya que este es claramente el mayor riesgo para toda organización y desde donde se debe asegurar una gestión segura ética y confidencial para proteger el flujo de datos a los que se tiene acceso para dar un tratamiento adecuado.

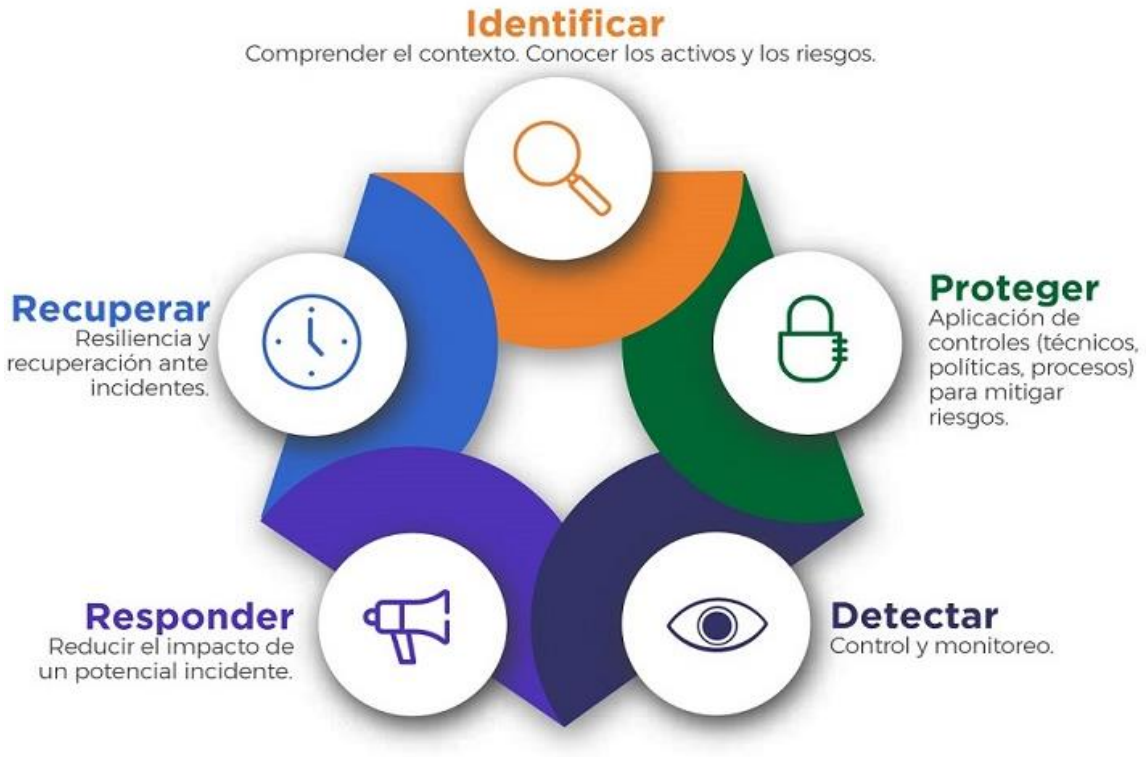
- **Sistemas de Detección de Intrusos (IDS)** y **Sistemas de Protección contra Intrusos (IPS) -SURICATA:** Este es un gran motor para la detección de intrusos, software especializado en ciberseguridad el cual se utiliza para la identificación de actividades maliciosas en la red, esta herramienta es muy conocida por su gran capacidad, para realizar el examen del tráfico de la red en tiempo real.

- **KeePass:** Esta herramienta es un software gestor de contraseñas, para nuestros sistemas de información, sitios web y correo electrónico, el cual permite centralizar todas las contraseñas de manera controlada.

- **Firewalls open-source – Pfsense:** Si bien los sistemas operativos traen por defecto un firewall, el cual e una herramienta de control, utilizada para el filtrado del tráfico de red, es importante reforzar las medidas de seguridad, implementado dentro de nuestro entorno y arquitectura de red, un firewall que nos permita duplicar la capa de filtrado, esta herramienta, de uso libre continua kernel que permite su instalación en cualquier sistema.

Finalmente, como recomendación general debemos llevar a consenso, aprobación e inversión plan de acción debe siempre estar alineado a las políticas y objetivos de la organización, esto de acuerdo con los lineamientos del marco de seguridad.

Imagen 6. Marco de Ciberseguridad



Fuente: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

3. Conclusiones

El análisis de problemáticas, necesidades y riesgos de seguridad que pudimos encontrar en nuestro entorno empresarial, nos apoyó para aplicar las acciones y controles que ejercieron los equipos de seguridad a fin de que estas garantizar un resultado eficiente y seguro para los involucrados y en aras de dar cumplimiento a los objetivos del negocio, todo esto también con la relevancia que tuvo el documentar y retroalimentar en su momento cada acción, así mismo se pudo contextualizar y adoptar el uso de herramientas que pudo ejecutar cada equipo, las cuales siempre se implementaron buscando estar a la vanguardia de las necesidades sociales y empresariales, y aplicaron para el sector público y privado.

En base a la compresión que se logró y con las características y aplicaciones de los equipos de seguridad Red Team y Blue Team, y conociendo previamente las amenazas y riesgos de un entorno empresarial se pudo plantear soluciones de seguridad y desarrollar las estrategias aplicables a fin de poder mitigar y/ o controlar el impacto ante incidentes o ataques que se analizaron y se pudieron presentar. Así mismo se logró evaluar el estado de la organización para así cerrar las brechas encontradas y fortalecer las áreas más críticas, según lo aplicado por cada equipo en la auditoria y posterior plan de mejora.

Es vital que las organizaciones protejan sus activos informáticos, y si bien esto implico validar una inversión en recursos financieros, tiempo y cumplimientos normativos, esto sin dudar nos dejó ver que tuvo un valor agregado a su actividad comercial, toda vez que implementar procesos, modelos y equipos de seguridad, aportaron un plus para dar confianza a los clientes e inversionistas, por ende se pudo evidenciar la gran necesidad de adopción de profesionales que velen por la seguridad de la información y permitan una administración de recursos de manera estructurada y en constante monitoreo.

Si bien la seguridad al 100 % no es ponderado posible, el haber realizado este análisis no permitió conocer los beneficios de la articulación de equipos de seguridad, las amenazas, los riesgo, las estrategias y materialización de acciones, sin duda lograron fortalecer a todas la áreas de la organización y así mismo tener un cumplimiento de requisitos u objetivos en alineación con las políticas empresariales, aportando un valor empresarial y de alto impacto para clientes e inversionistas que pudieron evidenciar más respaldo y confianza del negocio.

4. Recomendaciones

- ✓ Realizar valuaciones periódicas usando la actualización o construcción de la matriz de riesgos, el estado de la organización, a fin de poder justificar la inversión necesaria, para apoyar procesos seguros en informática.

- ✓ Efectuar la ponderación de los riesgos, con el fin de poder determinar las necesidades y prioridades en la gestión de recursos, y así poder identificar los activos que por su evaluación son clasificados como más críticos y que estos tengan un tratamiento adecuado.

- ✓ Adoptar e implementar las herramientas para control de tráfico de red (IDS) y proteger siempre sistemas (software) con la constante actualización y desde los medios certificados.

- ✓ Promover la toma de conciencia en todos los miembros de la organización sobre temas de seguridad, ingeniería social y control de activos informáticos, tanto físicos como digitales e información sensible, a fin de poder definir las medidas de control para con el usuario final, quien podría ser más sensible a ataques y procesos de ingeniería social.

- ✓ Implementar el recurso humano y técnico de los equipos de seguridad vistos, para la administración de activos informáticos, a fin de poder evaluar, y controlar de manera permanente posibles incidentes que afecten la normal operación del negocio.

- ✓ Aplicar las pruebas pentesting, bajo entornos controlados de manera periódica y documentarlas, a fin de realizar la evaluación a fondo de las vulnerabilidades que pueda presentar la infraestructura de red de la organización.

- ✓ Mantener una actualización constante de las herramientas de seguridad y actualizar las bases de información relacionadas con vulnerabilidades y nuevas amenazas de seguridad, tanto físicas como digitales, así mismo conocer nuevas tendencias en ciberdelincuencia para estar preparados y actuar ante de una posible materialización.

5. Bibliografía

Blog Hubspot, Plan de seguridad informática: qué es, elementos clave y ejemplo, https://blog.hubspot.es/website/plan-de-seguridad-informatica

https://www.comptia.org/content/articles/what-is-ethical-hacking#:~:text=Ethical%20hackers%20are%20tasked%20with,that%20protect%20organizations%20from%20attacks.

Crowdstrike, Red Team vs Blue Team in Cybersecurity, https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/red-team-vs-blue-team/#:~:text=Red%20Team%20vs%20Blue%20Team%20Defined,to%20the%20red%20team%20attack.

Deloitte, Global Future of Cyber Survey, 4th Edition, https://www.deloitte.com/global/en/services/risk-advisory/research/global-future-of-cyber.html?id=gx:2ps:3gl:4cyber:5:6con:20241021::2024focs-paidsearch-southamerica&gad_source=1&gclid=CjwKCAiA3ZC6BhBaEiwAeqfvytn_HWJoi_JeUgHkAs5tGhTxtr8IHbqEVx6Y5rfP7Dy0wHd2puSUVBoCPyIQAvD_BwE

El Campus Internacional de Ciberseguridad, ¿Qué es el Pentesting?, https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

Foundrez, Todo sobre el blue team en ciberseguridad, https://founderz.com/es/blog/blue-team-seguridad-cibernetica/

Función Pública, Políticas de Operación Proceso de Tecnologías de la Información, https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672

Hacker Mentor, El límite de lo ético y lo no ético en el Hacking, https://www.hacker-mentor.com/blog/la-etica-en-el-hacking

Intelequia, Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad, https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Mytra, ¿Qué es un SIEM?, https://www.mytra.es/blog-post/siem-gestion-de-eventos-e-informacion-de-seguridad

Ninjaone, Complete Guide to Systems Hardening [Checklist], https://www.ninjaone.com/blog/complete-guide-to-systems-hardening/

Keepcoding, ¿Qué es Suricata en ciberseguridad?, https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

Ninjaone, Guía completa para el hardening de sistemas, https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

Opirani, Guía para la Gestión de Incidentes de Seguridad, https://www.piranirisk.com/es/blog/guia-para-la-gestion-de-incidentes-de-seguridad

Redes zone, Los mejores Firewall open-source para proteger tu red, https://www.redeszone.net/tutoriales/seguridad/mejores-firewall-open-source-proteger-red/

Secretaria del senado, Ley 1273 de 2009, http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

S2 Grupo, Red team: definición, funciones y diferencias con blue team, https://s2grupo.es/red-team-definicion-funciones-y-diferencias-con-blue-team/

Universidad Nacional Abierta y a Distancia, Campus virtual, seminario especializado equipos de seguridad Red Team-Blue Team, especialización en seguridad informática.

6. Anexo

Enlace videos sustentación: Capacidades Técnicas, Legales Y De Gestión Para Equipos De Blue Team Y Red Team.mp4