Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

JOHN FREDY BENAVIDES SANTAMARIA

Socialización informe técnico

DIRIGIDO POR:

INGENIERO JOHN FREDDY QUINTERO

Universidad Nacional Abierta y a Distancia

Vicerrectoría Académica y de Investigación

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Bogotá D.C. Colombia

2020

Resumen

El desarrollo de este informe ofrece una síntesis del seminario especializado equipos estratégicos en Ciberseguridad red team y blue team, se da a conocer las características y funcionalidades dentro de un equipo blue team y un red team, esto nos permite tener una visión generalizada de cada uno de estos roles, dentro de este informe se relacionada cada una de estas características su alcance debilidades y fortalezas, también como alinear estos roles al estatuto legal y ético que se permite ejecutar dentro de esos lineamientos.

El enfoque que da este trabajo es tanto técnico como analítico, y por medio de unos puntos de vista doy orientación a cada respuesta que se dio en el desarrollo del seminario, dentro de este se incluye la apreciación de las 4 etapas del seminario por medio de un video resumiendo en mis palabras cada contexto de cada etapa, por último, argumento mis posturas por medio de conclusiones que permiten definir una relación profesional con el curso.

A lo largo de estas 4 etapas se desarrollaron conceptos, se compartieron experiencias tanto de parte del tutor como del equipo y utilizando criterios propios e investigativos se dio un análisis personal a cada una de las preguntas y ejercicios desde el punto de vista de cada equipo estratégico.

Contenido

Glosario

Ciberseguridad: Seguridad informática

Pentestet: Pruebas de penetración a un sistema informático

Backdoor: En seguridad informática refiere a una puerta trasera conocida de ingreso a un sistema

IDS: Sistema de detección de intrusos por sus siglas en ingles

Vulnerabilidad: Debilidad o fallo de sistema.

DB: Base de datos por sus siglas en ingles

Exploit: Parte de un software para aprovechar una vulnerabilidad

Metadata: Información acerca de datos

Cmd: Símbolo del sistema o consola de comandos de Windows.

Comando find: Comando de búsqueda dentro de la consola de comandos

Telnet: Protocolo de comunicación sobre el puerto TCP 23

HTTP: Protocolo de comunicación WEB

RDP: Protocolo de comunicación orientado a control remoto de windows

Introducción

Miles de ataques se perpetúan diariamente sin que muchos de los afectados si quiera se den cuenta, la justificación de contar con equipos de seguridad dentro de una organización resultaría vital e innegable sin embargo la realidad es que esto no ocurre, y esto no solo a nivel país si no que es un comportamiento generalizado, sin embargo, el desarrollo de este informe permite dar a conocer desde un punto profesional la importancia de estos.

En el mundo actual tener equipos especializados en diferentes roles de seguridad informática resulta casi una obligación pues a partir de este se desglosa una serie de respuestas que permiten estar alineados a los estándares de seguridad dentro de una organización. Y es que contar con un equipo capacitado permite dar varias ventajas frente a organizamos o individuos que intentan vulnerar un sistema con un propósito.

En el desarrollo del informe de este seminario se expone en un ambiente controlado el análisis y puesta en operación de un equipo Red Team con la ejecución de un ataque buscando la manera de como un atacante logra obtener acceso a información argumentando la fuga de la misma, además desde el enfoque de un equipo Blue Team que herramientas y mecanismos usar para evitar y contener este ataque, con esto se logra dar un análisis profundo de manera tal que permita detallar y justificar el uso de estos roles dentro de un equipo de ciberseguridad.

Objetivos

General

Comprender el comportamiento de roles de equipos estratégicos de seguridad desde 2 posiciones diferentes en los cuales tienen como objetivo común de mejorar los conocimientos y estrategias acerca de vulnerabilidades y ataques informáticos.

Específicos

- Establecer las reglas claras de juego de cada equipo desde la base legal y ética de cada organización o país
- Fortalecer los conocimientos en estrategias de seguridad que le permita al equipo blue team tener bases para soportar el análisis de amenazas y riesgos.
- Motivar a los estudiantes de seguridad de la información a comprender desde cada equipo sus fortalezas y debilidades y definir un rol al cual quiera ser parte como especialista.

1. Desarrollo del informe

1.1. Etapa 1 Conceptos equipos de Seguridad

Las leyes siempre están ligadas a una acción o labor, generalmente asociado con reglas de juego para ejecutar estas acciones, los profesionales en seguridad no somos la excepción y si bien las reglas de juego están bien definidas algunas acciones que se ejecuten en el diario vivir pueden tener consecuencias y estar arraigados a actos ilícitos.

En esta etapa se hizo énfasis en algunas leyes y artículos importantes sin embargo la que en mi opinión me parece más importante es la ley 1273 del 09 la cual voy a enunciar:

Ley 1273 de 2009, refiere al poder del bien tutelar denominado la protección de la información y de los datos y se preservan integralmente los elementos que utilicen las tecnologías de la información.

Esta ley si bien no es la primera ya que, desde la constitución del 91 se recalca lo de la protección a la propiedad intelectual y los derechos de autor, si retoma todas las anteriores incluyendo la fijada en la constitución y la relaciona con los manejos de datos de las tecnologías de la información y agrega lo que corresponde a delitos informáticos y la recalco por el auge de transformación digital en el que vive el mundo. En el crecimiento exponencial del uso de la virtualidad como medio de comunicación en el mundo se apertura una gran cantidad de datos sobre Internet lo que permite lograr acciones que anterior a la virtualidad no es posible. Este crecimiento de uso de medio virtuales y digitales a su vez crea un ambiente propicio delincuencial donde el crecimiento este a su vez depende intrínsicamente del uso y desconocimiento de los usuarios.

1.1.1. Análisis el ejercicio del pentesting

Una prueba de pentesting consiste en utilizar una metodología en base a pruebas ofensivas con el fin de evaluar los mecanismos de defensas existentes en un entorno especifico, este entorno puede estar constituido por un software, un hardware o un conjunto de ellos. La finalidad de esta prueba es identificar vulnerabilidades para posteriormente evaluar dar un análisis y posteriormente mitigar y/o corregir.

Existen 5 fases para este ejercicio definidas de la siguiente manera:

- Fase de reconocimiento, el objetivo de esta fase es realizar la mayor recolección de información que nos permita tener una mejor visión del objetivo.

- Fase Análisis de Vulnerabilidades, con esta fase se busca analizar toda la información colectada en la fase inicial y posteriormente evaluar para identificar las vulnerabilidades que se pueden explotar para lograr obtener una posición privilegiada.

- Fase explotación de Vulnerabilidades, esta fase es muy importante ya que básicamente con la información obtenida en las anteriores fases se procede a explotar estas vulnerabilidades

- Fase posterior a la explotación, refiere básicamente a luego de explotar esa vulnerabilidad y lograr ganar acceso se permite encontrar backdoors para mantener el acceso dentro del sistema y continuar explotando otras vulnerabilidades.

- Fase de Informe, aquí lo que se busca es crear un informe de lo realizado en las anteriores fases en lo cual deben documentar los pasos realizados la información encontrada, herramientas usadas, sistemas analizados y técnicas usadas para validar como se explotó lo encontrado.

Cada una de estas fases generalmente están acompañadas con una serie de herramientas y se ejecuta como una metodología ya que es considera bajo los mismos pasos en orden descendente.

Algunas de estas herramientas usadas para este fin en una o varias fases son las siguientes:

• Metasploit

Es una poderosa herramienta muy usadas por diferentes profesionales de la ciberseguridad, pero también por delincuentes. Esta herramienta consiste en un código que puede ser modificado dependiendo de la vulnerabilidad explotada o a explotar. Este código es inyectado en la red de la cual se logró acceso y de esta manera probar puntos débiles por ejemplo usar un mecanismo de fuerza bruta para lograr acceder a otros sistemas diferentes por donde se logró acceso para ejecutar este código.

• Nmap

Es una de las herramientas más importantes a la hora de realizar una búsqueda de información, esta herramienta realiza un escaneo de un sistema llámese hardware software e inclusive a una página web para identificar los puertos que se encuentran abiertos para luego tratar de explotar el sistema sobre ese puerto que se encuentra abierto. Esta herramienta al permitirse identificar los puertos que se encuentran abiertos en una red es posible evaluar los puertos más inseguros como telnet, http o RDC.

• OpenVas

Es una excelente herramienta cuya principal funcionalidad es proporcionar mecanismos para evaluación de vulnerabilidades, esta herramienta se integra a la red donde se encuentra los sistemas a obtener información realiza un escaneo de vulnerabilidades y lo compara con su base de datos, al final elabora un informe detallando las vulnerabilidades encontradas y las mejores prácticas para corregir en caso de que aplique.
Servicios en línea:

• ExploitDB

Son una serie de activos WEB en los cuales personas denominados hackers enriquecen una base de datos con acceso público donde se encuentra información relacionada con vulnerabilidades de todo tipo de software, esta herramienta al estar en un dominio público y abierta a cualquier persona que busque información relacionada con la seguridad permite detallar las vulnerabilidades de cada software y de esta manera permitirse actuar en base a un hallazgo detectado en una prueba pentesting.

• CVE

Por sus siglas en ingles refiere a vulnerabilidades comunes expuestas, son los conjuntos de exploitDB que enriquece información y generalmente comercializada con la información recopilada para lograr identificar programa maligno y/o virus además detectada en una red, generalmente estos CVE se usan en IDS e IPS como antimalware de fabricantes comercial tales como Palo Alto, Cisco entre otros.

De esta etapa resalto la importancia de conocer y aplicar a cada una de las leyes que esta vigentes y que nos competen para llevar a cabo nuestras funciones como profesionales de seguridad este debe ser el patrón de la línea base de inicio de nuestra labor.

Por último el ejercicio de pentest está alineado con una metodología definido y dividido en varias fases dependiendo del organismo o las pruebas a ejecutar estos ejercicios son importantes y vitales a la hora de auditar un sistema pues estos nos ponen a prueba de que tan seguro es un sistema o varios en una organización, como recomendación incluir dentro de los procesos periódicos ejecutar ejercicios de pentest antes y después de la implementación de un elemento y/o aplicación a un sistema, esto nos permite conocer como estábamos y si este elemento o aplicación fue incluida correctamente.

1.2. Etapa 2 Actuación ética y legal

En esta etapa se nos expone un documento asociado a un anexo el cual expresa bajo un contrato laboral y acuerdo de confidencialidad de una organización dedicada a servicios y actividades de ciberseguridad asociadas al gobierno, este documento evidente muestra actividades ilícitas en las cuales como parte del equipo de seguridad y de la organización se expone como cohecho de estas actividades.

Si bien el estatuto del contrato no atenta contra el bien de la compañía si lo hace con las practicas ejecutadas adicional que esta tiene un precedente negativo ya que fue encontrado evidencias de actividades ilícitas por un abogado. Al linearse a prácticas corruptas quien acate y acepte este contrato será participe y coautor de las actividades implícitas dentro de la empresa.

1.2.1. Análisis de este comportamiento bajo la ley 1273 del 09

En la segunda cláusula del contrato de confidencialidad en el numeral 2 de la parte receptora indica que dentro de las actividades realizadas dentro del equipo pueden tratar

información o datos producto de interceptación de información y accesos abusivos a sistemas informáticos, la práctica de estas actividades se infringen los siguientes artículos de la ley 1273 del 2009, bien el acuerdo de confidencialidad expresa dicha información adicional que en caso de una investigación la persona que esté a cargo de esa información deberá hacerse responsable de esta y afrontar un proceso legal ante la justicia con medios propios y como responsabilidad única e individual por infringir los artículos 269 (A,B y C) de la ley 1273

Como lo mencioné la práctica de las actividades que ejecuta la compañía atenta totalmente con las leyes del estatuto que refiere a la seguridad de la información, pues esta reconoce el estar involucrado con accesos abusivos a los sistemas informáticos y obstaculicen ilegitima de un sistema informático intenta contra un bien particular. Y si bien esta organización trabaja directamente con el gobierno esto no la inhibe de actuar con integridad y bajo las leyes que lo rigen como actuador de este tipo de servicios.

1.2.2. Análisis de propuesta laboral desde lo ético y legal

Como profesional de ciberseguridad al identificar los reglamentos citados en el documento como acuerdo de confidencialidad y limitaciones debo declinar del contrato, ya que con esto atenta en primera medida a la ley 1273 del 2009 y al código de ética del cual acepte bajo juramento ante la Republica de Colombia y ante el consejo Profesional Nacional de ingeniería que al recibir mi tarjeta como profesional acepto alinear el ejercer mi profesión bajo los lineamientos inscritos y que al incumplir uno o varios de estos lineamientos conllevara a la imposición de las sanciones que allí se indiquen, en donde uno de estos códigos expresamente se reseña en el capítulo 2 articulo 31 numeral b y corresponde acorde a una de las actividades expresadas en el anexo, El custodio de bienes incluido la documentación e información ocultar o utilizaciones indebidas de los mismos bienes, atenta contra el código de ética quien cataloga este acto como muy grave.

Este tipo de acuerdos generalmente están acompañados de contratos millonarios los cuales resultan ser atractivos sin embargo como profesional de seguridad debo regir mi profesión a lo legal y la moral como ciudadano integro y no de intereses particulares.

1.2.3. Análisis del caso operación Andrómeda

El estado en este caso en específico representado por las fuerzas militares toma practicas con el cual buscan obtener ventaja para tener un paso adelante, frente a los grupos al margen de la ley, estas actividades en la práctica son totalmente validas y normales en estatuto gubernamental colombiano.

En la operación Andrómeda el ejercito tripulado por varios generales y el ministro de justicia buscaban obtener información privilegiada que les diera acceso a datos con los cuales acontecer actividades legitimas, sin embargo, esto fue solo parte de una actividad con fines ilícitos pues el objetivo final era el de interceptar información y comunicaciones de

funcionarios del gobierno especialmente quienes hacían parte de los negociadores de la paz con las FARC llevada a cabo en Cuba.

Las actividades realizadas en esta operación infringieron tanto ético, como legalmente violando los artículos de la ley 1273 de 2009 ya que no se tenía una orden judicial para llevar a cabo estos procesos, estas actividades debieran estar acompañadas con la fiscalía que son el único organismo en Colombia para llevar acabo interceptaciones por orden de un juez.

Un proceso licito de este tipo bajo de un marco legal dentro y fuera del gobierno siempre debe estar acompañado por entes públicos como Fiscalía y la procuraduría, adicionalmente alineado a actividades licita, documentando la información obtenida y a obtener además realizando un proceso documental de las personas que iban a relacionarse con las actividades a realizar, alinear los valores que rigen las instituciones y utilizar las mejores prácticas para obtener información, de acuerdo a los resultados obtenidos en la investigación claramente se observa que nada de lo antes expuesto se tomó como practica en la realización de estas actividades.

Si bien las actividades realizadas no comprometieron la seguridad de un individuo, grupo o nación, estas si deben ser castigadas bajo la normatividad expresa en los artículos que contemplan la ley 1273 de Colombia, así como las leyes de la seguridad de la información que obtuvieron por las interceptaciones en otro país en este caso leyes cubanas.

Finalmente, estas actividades al involucrar políticas que atentan directamente a la nación no pueden ser juzgadas por la justicia penal militar si no por la justicia ordinaria.

Los implicados directa e indirectamente relacionados con estas actividades y que eran conscientes de las actividades que se practicaba en este sitio debieron actuar con legitima ética denunciando ante las autoridades el tipo de labor que se ejercía ya fuese con o sin ánimo lucrativo y/o didáctico. Estas personas serán procesadas de igual manera por la justicia ordinaria.

1.3. Etapa 3 Ejecución pruebas de intrusión

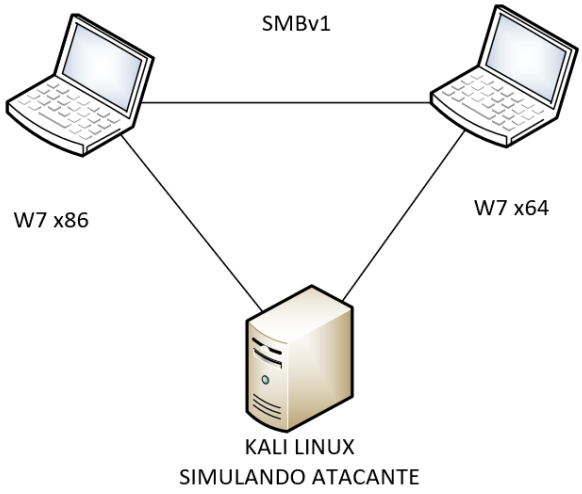
Para iniciar con este informe quiero exponer la diferencia entre un equipo Red Team y un equipo Blue Team.
El red team (Equipo rojo) es un equipo humano integrado por diferentes miembros que a su vez cada miembro cuenta con múltiples habilidades en seguridad pero que a su vez se especializa en un aspecto en específico, su función principal es la de llevar a cabo un propósito con un objetivo el cual ha sido definido y cuenta con un criterio y unas reglas de juego las cuales han sido expresas por el cliente u organización. El red team con su objetivo trazado y por medio de metodologías intenta lograr llegar al punto que se requiere, ejemplo conseguir recrear un escenario en el cual se presenta un ataque interno con acceso al servidor de base de datos, el equipo red team en este caso se le asigna una regla de juego de identificar el servidor y lograr alcanzar el mismo objetivo que el atacante.
El blue team (Equipos azul) es un equipo humano que al igual que el red team cuenta con habilidades enfocadas a seguridad alguno especializados en temas como aplicaciones, firewall perimetral, la nube, etc. Tal cual, como el equipo rojo, la diferencia radica que este

equipo se le define el objetivo de lograr contener un ataque o mitigar una vulnerabilidad con base en evidencias con ayuda de sistemas que permitan identificar estas amenazas y ejecutar el plan de riesgo, ejemplo evidenciar un log de ataque al servidor de base de datos intentar contener y/o mitigar el impacto que se está recreando.

Otra diferencia grande de estos dos equipos es que generalmente el equipo azul está contratado por la compañía y el equipo rojo es contratado fuera de la compañía, generalmente las auditorias del equipo rojo se realizan para analizar qué tan preparado está el equipo azul para contener o mitigar un ataque, por ende, estos análisis de fallos son ejecutados por el equipo rojo sin ningún conocimiento por personas dentro de la compañía.

Parte del desarrollo del seminario estuvimos realizando ejercicios desde el lado del equipo rojo, donde se encuentra desde un banco de pruebas con una situación de fuga de información se colecta y se tiene el siguiente diagrama:

Figura 1 Diagrama banco de pruebas



Fuente: Propia, etapa 3 del curso Equipos Estratégicos en Ciberseguridad

Se observan 2 máquinas las cuales se comunican a través del protocolo SMBv1 para compartir dispositivos o directorios a través de una red LAN. Adicional a ellos nos entregan la información de una vulnerabilidad conocida y el tipo de comportamiento de las maquinas durante el registro del ataque.

El equipo rojo comienza a colectar esta información y procede a ejecutar la fase de explotación de vulnerabilidades para se hace uso de la herramienta metasploit un código incluido dentro del sistema operativo Kali Linux, allí se procede a usar el mecanismo de explotación eternalblue que está diseñado para explotar la vulnerabilidad CVE-2017-0144, información que también estaba incluida en el anexo de la fase de levantamiento de información.

Se procede a ejecutar el código y se detecta el reinicio de una de ellas la máquina virtual con S.O. W7 x86 y el metasploit mostraba un error, luego se ejecutó sobre la maquina W7 con arquitectura x64 no ocurría ninguna acción sobre la maquina y el metasploit mostraba un error, por último se exploró la opción de modificar el payload del encabezado de la trama del código con un TCP reverse, de esta manera el código tiene éxito y se logra ganar tener acceso al sistema operativo:

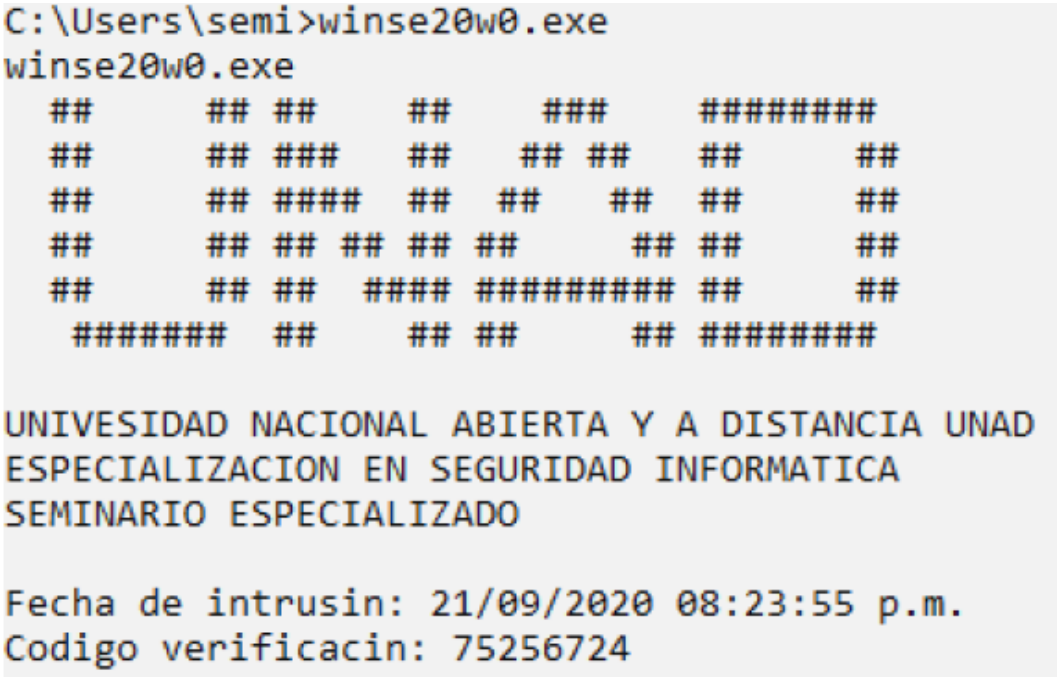
Figura 2 Acceso a equipo con falla de seguridad W7x64

```
[+] 192.168.0.109:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.109:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.109:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=



C:\Windows\system32>

C:\Windows\system32>ipconfig
ipconfig

Configuracin IP de Windows


Adaptador de Ethernet Conexin de rea local:

   Sufijo DNS especfico para la conexin. . : www.nexxtwifi.com
   Vnculo: direccin IPv6 local. . . : fe80::4842:9ce4:4e38:7898%11
   Direccin IPv4. . . . . . . . . . . . . . : 192.168.0.109
   Mscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1

Adaptador de tnel isatap.www.nexxtwifi.com:

   Sufijo DNS especfico para la conexin. . : www.nexxtwifi.com
   Vnculo: direccin IPv6 local. . . : fe80::5efe:192.168.0.109%12
   Puerta de enlace predeterminada . . . . . :

C:\Windows\system32>
```

Fuente: Propia, etapa 3 del curso Equipos Estratégicos en Ciberseguridad

De este punto solo resta hacer la búsqueda del archivo del cual funciona como mecanismo para la extracción de la data que no por más al ejecutar un find desde el lugar de acceso cmd se logra ubicar ejecutándolo encontramos el siguiente mensaje:

Figura 3 Evidencia acceso equipo con falla se seguridad



Fuente: Propia, etapa 3 del curso Equipos Estratégicos en Ciberseguridad

Las funciones de un equipo rojo siempre resultan estresantes para un profesional que hace parte del equipo azul pues no sabes en qué momento o a que sistema pueden ejecutar su prueba de pentest sin embargo en un ataque real tampoco se saben estos dos aspectos por eso a pesar de que resulte retador e intimidante esto te prepara para llevar a cabo corrección de errores y estar mejor preparado en el caso de una eventualidad real.

1.4. Etapa 4 Contención de ataques informáticos

Esta etapa hace énfasis a la respuesta de una serie de preguntas las cuales permiten dar mi punto de vista y mi criterio para dar una serie de conclusiones del lado del equipo azul o blue team.

Una de las primeras preguntas que piden es conocer que sería lo primero a indagar y haría de llegar a encontrase en un ataque en tiempo real.

Para responder esta pregunta primero debo definir cuál es mi papel o rol dentro del equipo de seguridad, luego quisiera saber es conocer si es un ataque real, muchas veces las organizaciones implementan sistemas IDS (Sistema de detección de Intrusos) los cuales

también arrojan falsas alarmas, una vez confirmado que el ataque si es real significa que no se pudo contener por lo cual debería conocer si está logrando tener éxito el ataque, evaluar si se presenta perdida de información e indisponibilidad de algún sistema y/o servicio, con base a la información colectada proceder a ejecutar un plan de mitigación por ejemplo redirigir el tráfico cambiando direcciones IP del servicio, deshabilitar temporalmente el sistema que está siendo atacado para así permitir la recuperación del mismo, ejecutar puntos de restauración de información que permita recuperar el estado previo al ataque ejemplo copias de respaldo de bases de datos y/o aplicaciones.

Posterior a esto, quiero saber cuál es la gravedad de lo ocurrido y la actividad por la cual se alertó el ataque esto define como parte de la documentación del cómo actuar en caso de volver a repetirse cuando se ejecute la recuperación del sistema en el punto de restauración.
Para la colección de información en la investigación debería como primera medida conocer si el ataque fue interno o externo, si el ataque tuvo éxito por qué fallaron las medidas de seguridad que se implementaron, adicionalmente reportar el incidente a las autoridades competentes. Por último, definir las lecciones aprendidas para de esta manera tomar acción y endurecer las políticas tanto internas como externas con base a lo ocurrido.

Luego me preguntan sobre las medidas de hardening con base al ejercicio ejecutado desde el rol de red team.

El propósito principal de un plan de hardening a un sistema es el de mitigar y dar tiempo para tomar medidas en caso de presentarse un ataque con el fin de minimizar las consecuencias, tal como se presentó en el ejercicio el cual presentaba un caso grave de fuga de información.

Dentro de las medidas que a mi criterio se deben implementar como proceso de hardening son las siguientes:

- Plan de protección posibles ataques físicos en el hardware
- Instalación segura del sistema operativo
- Configuración de servicios de actualizaciones periódicas
- Configuración de servicios y protocolos de Red
- Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema

Pues con la adecuada implementación de estas medidas se previene ataques como el documentado en este informe y adicional otros los cuales están relacionados en una serie de vulnerabilidades con una mala instalación y ejecución de los sistemas operativo, así como la ausencia de algunos mecanismos de hardware y software en un ambiente.

La siguiente pregunta va relacionada con la diferencia entre un equipo blue team y un equipo de respuesta a incidentes.

Esta pregunta resulta muy importante ya que hace parte de la definición de roles dentro de una organización orientado al equipo de seguridad y en conclusión, con referencia a un

equipo de respuesta de incidentes puede ser un equipo que cumpla una o varias de estas funcionalidades, generalmente este equipo está compuesto por diferentes roles dentro de una organización incluidos los del equipo de blue team. Por ende, cuando se habla de un equipo de respuesta a incidentes o CSIRT hace referencia a un grupo de gestión de incidentes y cuando se habla de un grupo blue team hace referencia a un grupo especializado de un nivel superior que permite garantizar los sistemas de seguridad incluido la gestión de incidentes.

Por último, la pregunta de qué fin le daría a la herramienta CIS (Center for Internet Security) dentro del blue team.

El CIS es una organización que presta ayuda de consultoría de servicios de seguridad a organizaciones basado en planes de diseño ofreciendo herramientas de ciberseguridad.

El uso de CIS lo utilizaría para implementar soluciones de seguridad de cara a Internet basados en las mejores prácticas desarrolladas por la organización, esto permite a la compañía estar alineado a los estándares de la industria de seguridad y proteger a la organización a la cual pertenece el equipo Blue team. Adicionalmente estar constantemente actualizado en mis sistemas en base a las practicas que tome esta organización con las herramientas puestas en funcionamiento.

Hacer uso de los servicios de CIS permitiría además mantener los controles de seguridad de la compañía organizados con los estándares usados por esta organización (CIS) usando herramientas desarrolladas por ellos que me permita la automatización de ciertos proceso, como por ejemplo la implementación de políticas de seguridad en un sistema basado en las vulnerabilidades encontradas recientes en un aplicación de uso común, ejemplo aplicar parches de seguridad sobre la aplicación Google Chrome de manera masificada en el dominio de la organización con la evaluación previa del uso dentro de la compañía.

Aquí se hace también el uso de SIEM para el equipo de blue team con sus funcionalidades y características para ello voy a dar mi apreciación:

SIEM es software el cual es una combinación entre SIM administrador de seguridad de la información por sus siglas en inglés y SEM administrador de eventos de seguridad por sus siglas en ingles los cuales a su vez entregan de manera integral y en tiempo real análisis de alertas de seguridad generadas por aplicaciones y dispositivos de seguridad, este software se alimenta a su vez de bases de datos de diferentes recursos los cuales integran amenazas presentadas y analizadas en otros ambientes.

Dicho de otra manera (SIEM) está diseñado para proporcionar a los equipos de seguridad una visibilidad centralizada de datos de seguridad de toda la empresa con conocimientos prácticos sobre las amenazas principales. Con la premisa de la solución ingiere una gran cantidad de datos en toda la empresa para proporcionar una visión completa de actividad en entornos locales (Software y Hardware) así como también para entornos alojados en la nube.

Dentro de sus funcionalidades principales está en dar inteligencia al correlacionador de eventos la integración a diferentes sistemas desde la complejidad de un proxy hasta la

simplicidad de un end point nos da esa trazabilidad que nos permite detectar de manera temprana lo posibilidad de un ataque hacia ese sistema.

Herramientas de contención de ataques.

Existen diferentes herramientas que permiten realizar procesos de contención de ataques informáticos, aquí listare algunas de ellas:

- Firewall de red perimetral: Integrado como elemento de red analiza el origen y el destino basado en las IPs y puertos que toma acción en políticas permitiendo o denegando el acceso, esta herramienta de seguridad netamente se limita a la capa 3 y 4 del modelo OSI, su administración es simple y segura.
- Servidor Proxy: Actúa como intermediario entre el navegador e internet, debido a sus funcionalidades aplica sus políticas a nivel de capa 7 del modelo OSI permitiendo o denegando acceso a contenido y/o aplicaciones.
- Antivirus: Es un software instalado en un sistema operativo que puede ser tanto en un servidor como en un end point, que por medio de una base de datos la cual se actualiza constantemente del servidor de firmas de antivirus permite integrarse con las aplicaciones del sistema permitiendo identificar y bloquear amenazas de tipo virus

2. Video del desarrollo de seminario especializado

https://www.youtube.com/watch?v=pcqKoXvEjMY

Conclusiones

- Uno de los aspectos más importantes para llevar labores bajo el título de profesional debe ser el regirse bajo los valores uno como persona y otro como ser, sin embargo, COPNIA nos entrega lineamientos con el cual podemos reafirmar estos valores con argumentos basado en lineamientos éticos.
- Tomar acción por un contrato que aparentemente se ve atractivo monetariamente tiene sus riesgos un profesional debe saber cuento puede costar su trabajo sin embargo existen ofertas laborales que si bien en principio pueden ser validas puede llevar algo oculto, lo mejor es asesorarse legalmente con un abogado antes de celebrar este tipo de contratos.
- Los contratos para empresas que trabajan para el gobierno son aun de mayor cuidado pues los alcances de estos a veces no están fijados y muchas veces son licitaciones que se cerraron por tratamiento político es ahí que uno debe entrar a intuir y el asesoramiento legal es clave para la celebración de un contrato.
- Si bien trabajar para el gobierno tiene grandes beneficios, también pueden estar alineado con prácticas ilegales, si se trabaja con el gobierno siempre las acciones deben estar alineadas con las leyes y la constitución desconfiar siempre es un asunto de un profesional de la ciberseguridad.
- Se puede ser un gran experto de la ciberseguridad realizando protección o menester sin embargo si se desconoce el alcance o las leyes que se rige un proyecto puede recaer en sanciones por esto es que un profesional de ciberseguridad siempre debe conocer las leyes y además basarse en su código de ética.
- Si bien un equipo de seguridad puede optar por algunas herramientas que son de tipo open source con licenciamiento gratuito y bastante potentes, los ambientes productivos y la industria corporativa exige contar con elementos que cuenten con soporte constante con plataformas robustas que permitan estar alineados con las mejores prácticas en seguridad
- Conocer y comprender dentro de la industria de seguridad existen herramientas plataformas y comunidades como SIEM o CIS permite que se cuente con mecanismos seguros y actualizados y sobre todo permite a los equipos de seguridad estar constantemente en aprendizaje, esto en el largo plazo permite a las empresas ahorrar tiempo y dinero lo cual es beneficioso para ambas partes.
- Las actualizaciones de los sistemas operativos son de vital importancia para cualquier sistema, a diario se conocen nuevas fallas de seguridad y por ello el hincapié en la actualización constante de cada uno de ellos.

- La implementación de mecanismos y herramientas de seguridad en las empresas permiten a estas estar mejor preparadas para incidentes o fallos de seguridad, sin embargo, no por tener mayor cantidad de estos elementos y más costosos se está más seguro, siempre hay que buscar la mejor relación costo-valor pues con ello permite contar a los equipos de seguridad con mejor presupuesto y un uso inteligente implementando herramientas de seguridad acorde al core de negocio.
- Conocer el alcance de los equipos de seguridad permite delimitar las actividades por las cuales se desempeña, vimos que un equipo Blue Team puede hacer parte de otras dependencias como rol de seguridad dentro de una organización sin embargo ese equipo debe estar respaldado y apoyado por las demás áreas para realizar un proceso integro dentro la misma.
- El conocimiento las leyes contra delitos informáticos es de vital importancia para un profesional en seguridad informática pues argumenta la manera por la cual podemos proteger nuestra labor, así como tener las herramientas legislativas que nos permitan exponer ante un tribunal nuestras evidencias en caso de detectar una violación a nuestra información.
- Las pruebas de penetración es un conjunto de fases con las cuales utilizamos mecanismos para detectar vulnerabilidades en nuestros proyectos tecnológicos. Estas pruebas nos permiten tomar acciones para mitigar vulnerabilidades que podamos presentar y actuar de manera preventiva.
- Las herramientas de ataque son indispensables para la ejecución y labor de un equipo red team, sin embargo, las herramientas del equipo blue team debe ser más avanzadas y con mayores funcionalidades que le permitan evaluar y tomar acción frente a un evento de seguridad.
- Hablar de red team y blue team resulta dispendioso y a veces tedioso esto se ve reflejado en la presentación del video sin embargo es útil tomarse el tiempo necesario para dar un mensaje, hablar claro es una de las virtudes de un profesional en ciberseguridad.

Recomendaciones

La participación en este seminario dio lugar a diferentes criterios relacionados con los conocimientos previos a este, en ese sentido se encontraron debates con los cuales la participación individual fue fundamental ya que desde la perspectiva individual se da como objeto el logro de los objetivos que fue el de identificar cada fase desde cada uno de los equipos, el uso adecuado de las herramientas nos permitió desarrollar este curso de una forma ágil y organizada.

Recomendaciones para resaltar:

1. El conocimiento legislativo antes y después del desarrollo de las preguntas
2. Las reglas de juega para cada equipo siempre deben ser definidas, de aquí parte el éxito de cada una de las actividades a ejecutar
3. El seguimiento de cada actividad llevada a cabo permite tener una correcta documentación de esta, esto permite tener el control de los procesos de los equipos.
4. Fortalecer el conocimiento de un equipo de seguridad permite tener ventaja sobre los riesgos y vulnerabilidades a los que se expone un sistema.
5. Las herramientas avanzadas tales como SIEM y equipos estratégicos tales como CIS son cada día mas necesarios pues permiten a los equipos de seguridad contar con un mayor criterio y análisis para mitigar y contener un ataque informático.

Bibliografía

ClamAV Malware, T. (s.f.). *About Clamav*. Obtenido de clamav.net: https://www.clamav.net/about

CLAMWIN. (s.f.). *CLAMWIN*. Obtenido de CLAMWIN: http://es.clamwin.com/content/view/71/63/

LogRhythm. (s.f.). *LogRhythm Overview*. Obtenido de LogRhythm: logrhythm.com/about/

OPNsense, p. (s.f.). *About OPNSense*. Obtenido de opnsense.org/: https://opnsense.org/about/about-opnsense/

Pfsense, T. (s.f.). *Getting Started*. Obtenido de Pfsense: www.pfsense.org/getting-started/

Security, C. f. (s.f.). *Partnerships and Associations*. Obtenido de Center for Internet Security: https://learn.cisecurity.org/partnerships

Security, I. (Febrero de 2019). *IBM QRadar SIEM.* Obtenido de IBM: www.ibm.com/downloads/cas/RLXJNX2G

Smartekh, G. (03 de 05 de 2012). *Smartekh*. Obtenido de TIPS TECNOLÓGICOS, DE CONFIGURACIÓN Y NEGOCIO QUE COMPLEMENTAN TU SEGURIDAD: blog.smartekh.com/que-es-hardening

Splunk, T. (s.f.). *About*. Obtenido de Splunk.com: www.splunk.com/en_us/about-splunk.html

Squid: Optimising Web Delivery. (s.f.). Obtenido de squid-cache.org: http://www.squid-cache.org/

SWIPERPROXY. (s.f.). *SWIPERPROXY*. Obtenido de SWIPERPROXY: https://swiperproxy.github.io/index.html

Caballero, R. A. (04 de septiembre de 2018). reydes. Obtenido de reydes.com: www.reydes.com/d/?q=Fundamentos_de_Metasploit_Framework_para_la_Explotacion

Chandel, R. (19 de 07 de 2017). 3-ways-scan-eternal-blue-vulnerability-remote-pc. Obtenido de Hacking Articles: www.hackingarticles.in/3-ways-scan-eternal-blue-vulnerability-remote-pc/

Elias, G. (02 de Abril de 2019). Hacking Professional. Obtenido de GitHub: https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/

Gómez, J., & Franco, W. (noviembre de 2015). Universidad de Manizales. Obtenido de ridum u manizales: http://ridum.umanizales.edu.co/xmlui/bitstream/handle/20.500.12746/2452/INFORME_FINAL_JORGE_MARIO_-_WILLIAM.pdf?sequence=5

Kuvobic, O. (10 de mayo de 2018). exploit EternalBlue. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2018/05/10/exploit-eternalblue-registra-mayor-actividad-ahora-que-durante-brote-wannacryptor/

Peters, J. (29 de 03 de 2020). What is Metasploit. Obtenido de Varonis: https://www.varonis.com/blog/what-is-metasploit/

Consejo Profesional Nacional de Ingeniería. (s.f.). código de etica. Obtenido de copnia.gov.co: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Redonda, J. L. (09 de diciembre de 2015). detras de buggly detras de la fachada andromeda. Obtenido de enter.co: https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Gómez, J., & Franco, W. (noviembre de 2015). *Universidad de Manizales.* Obtenido de ridum u manizales: http://ridum.umanizales.edu.co/xmlui/bitstream/handle/20.500.12746/2452/INFORME_FINAL_JORGE_MARIO_-_WILLIAM.pdf?sequence=5

Pratt, M. (28 de noviembre de 2017). What is SIEM software? How it works and how to choose the right tool. Obtenido de enter.co: https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

Ogden, J. (21 de mayo de 2020). Why CIS Benchmarks are Critical for Security and Compliance Obtenido de enter.co: https://www.cimcor.com/blog/why-cis-benchmarks-are-critical-for-security-and-compliance

UNAD (2020) Plantilla presentación UNAD. Tomado para presentación de video de https://drive.google.com/file/d/1ukr4-owxrWl3FyWnip9UIkMKBaogf-36/view?usp=sharing