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

DIDIMO CALA MEJIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
CEAD-FLORENCIA
FLORENCIA - CAQUETÁ
2020

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

DIDIMO CALA MEJIA

Etapa 5 - Socialización de informe técnico

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
CEAD-FLORENCIA
FLORENCIA - CAQUETÁ
2020

CONTENIDO

1. RESUMEN

Se hace necesario la aplicabilidad de las estrategias RedTeam & BlueTeam en el presente informe técnico propuesto para la revisión de los protocolos de riesgos en la infraestructura TI en la organización The Whitehouse Security ” Es por esto que se pueden presentar diferentes tipos de vulnerabilidades, tales como pérdida de información sensible ya sean por hacking o ingeniería social, o ataques informáticos de diversa índole, por lo que se debe implementar metodologías que permitan establecer límites relacionados directamente con la necesidad de preservar la información de modo que la estructura organizacional de Whitehouse Security, reconozcan la relación que existe entre la apropiada utilización de la tecnología, a través da las Tic.

2. GLOSARIO

RedTeam: es un ejercicio, el cual consiste en simular un ataque dirigido a una organización, lo que se traduce que un grupo de personas internas o externas a la empresa, comprueban la posibilidad de tener acceso a los sistemas, comprometerlos y el impacto que esto podría tener en el negocio.

BlueTeam: es un grupo de especialistas que analizan, rastrean investigan y buscan toda clase de vulnerabilidades para prevenirlas.

Hardening: (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

CIS o Center for Internet Security: es una entidad sin fines de lucro cuya misión es 'identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la ciberdefensa'.

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management): es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas.

McAfee LiveSafe: Este es un cortafuego que protegerá tu computadora contra virus y ransomware.

Access Rights Manager: nos permite un control de los accesos a toda la infraestructura TIC importante para la seguridad general de las empresas.

SERVIDOR PROXY: Herramienta generalmente se usan como un puente entre el origen y el destino de una solicitud.

3. INTRODUCCIÓN

El siguiente informe técnico se presentan las estrategias RedTeam & BlueTeam planteadas en el seminario especializado, en el marco de la opción de grado de la especialización en seguridad informática de la universidad nacional abierta ya distancia – UNAD. Realizada mediante diferentes etapas y planteamientos de escenarios en las cuales se abordaron temas como: Conceptos equipos de Seguridad, Actuación ética y legal, Ejecución pruebas de intrusión y Contención de ataques informáticos.

Dando como resultado un informe técnico con las estrategias, recomendaciones que permitan endurecer los aspectos de seguridad en una organización.

4. OBJETIVO

Diseñar estrategias de contención mediante el análisis de riesgos y vulnerabilidades de la infraestructura TI de la Whitehouse Security.

4.1 ESPECÍFICOS

- Formular estrategias de contención mediante el análisis de riesgos para la organización.

- Identificar y evaluar las vulnerabilidades en una infraestructura TI.

- Diseñar estrategias de prevención y contención de ataques en el desarrollo de sus diferentes procesos en la organización.

5. DESARROLLO DE LA ACTIVIDAD

Durante el desarrollo del seminario especializado en red Team y BlueTeam se revisaron diferentes escenarios prácticos y teóricos mediante 5 etapas para dar como resultado un informe técnico de las etapas y recomendaciones. Se realizó una investigación con diferentes softwares especializados según las etapas del pentesting

Metasploit: es una herramienta que ayuda en estos casos ideales para realizar este tipo de pruebas posee una base de exploits que puede aprovecharse, lo que quiere decir que en lugar de buscar una vulnerabilidad ejecuta directamente el exploit que podría aprovecharlas y simula las consecuencias en caso de que se ejecute con éxito, utiliza una línea de comandos msfconsol y cuenta con una interfaz gráfica puede ejecutarse tanto en Windows como en Linux

Nmap: esta es una herramienta de escaneo de redes que permite identificar los servicios que están en ejecución en un dispositivo remoto, la identificación de equipos que se encuentran activos, sistemas operativos que se encuentran instalados en los equipos, la utilización de firewall entre otros.

OpenVas: Se trata de un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management).

Servicios en línea:

Explotad: Es un directorio web donde muchos hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones específicas, todos los días es actualizado generando gran cantidad de información.

CVE: Los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de fallas de seguridad informática que se encuentra disponible al público. Por

lo general, cuando alguien habla de un CVE, se refiere al número de identificación de CVE que se le asigna a una falla de seguridad. Las entradas de CVE son breves y no incluyen datos técnicos ni información sobre riesgos, efectos o soluciones.

se evaluaron las diferentes acciones de los equipos Red Team & Blue Team de la organización en el marco de los criterios éticos y legales; En la parte jurídica para los delitos informáticos, en Colombia se cuenta con varios recursos, sin embargo, uno de los más significativos es la ley 1273 de 2009, la cual complementa el Código Penal Colombiano con base en el concepto de la protección de la información y de los datos, con el cual se busca preservar los sistemas que utilicen tecnologías da la información y las comunicaciones en Colombia.

La ley 1273 de 2009 no es más que el mecanismo mediante el cual se definen los tipos penales que tienen relación con delitos informáticos, la protección de la información y los datos de todos los colombianos. En dicha ley se tipifican los diferentes delitos informáticos, y las diferentes penas aplicables a quienes incurran en cualquiera de ellos.

Otro punto importante es la actuación ética y legal del contrato y el personal que laboraba realizando los contratos del nuevo personal equipos estratégicos en ciberseguridad: red team & blue team y de la operación “OPERACIÓN ANDRÓMEDA BUGGLY” en la ciudad de Bogotá, En el acuerdo se evidencia un acto ilegal en el Cuarto punto.

Obligaciones de la parte receptora: Se obliga al receptor a guardar silencio si encuentra procesos ilegales a no dar aviso a las autoridades, también se le hace responsable si los representantes hacen mal uso de la información confidencial si al momento de algún allanamiento tiene información y la más grave de todas lo hacen responsable ante las autoridades de la información que tenga en su poder.

Pero lo más grave es que, según la Ley de Protección de Datos 1273 de la Constitución Política de Colombia se infringieron varios artículos como: utilizar

software malicioso para captar información de terceros, Hurto por medios informáticos y semejantes y venderla al mejor postor cometiendo delitos.

Considero que todo lo que se realizó estuvo mal hecho por parte de las personas que dirigían la operación, porque no llevaron un registro de las cosas que allí se realizaban ni del personal que entraba en las instalaciones menos de lo que realizaban con toda esta tecnología.

La firma de un contrato con la organización que al momento de analizarlo se encuentran muchas anomalías como ocultar, suplantar o asumir responsabilidades de otras personas y en un apartado del acuerdo menciona textualmente: No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros; se puede ver involucrado en problemas legales.

Ya pasando al marco de las vulnerabilidades en el sistema informático de la organización Whitehouse Security a partir del uso de metodologías y técnicas de intrusión. Realizando el análisis al escenario 3 se encontraron diferentes falencias:

- Fuga de información la cual se presenta al interior de la organización en
- dos de sus equipos de cómputo en la dependencia.
- Equipos de cómputo sospecha cuentan con Windows 7 X86 y X64 y
- tienen un sistema operativo antiguo.
- Fuga de información (10 de junio de 2020) los S.O. no se encontraban
- actualizados.
- Fallo de seguridad con identificador CVE-2017-0144.
- No tienen instalada la actualización MS17-010.

Se realizó un ataque con EXPLOIT a las máquinas virtuales buscando las “vulnerabilidad en la implementación del protocolo del Bloque de Mensaje de Servidor (SMB, por sus siglas en inglés) de Microsoft, a través del puerto 445”[1] esto

[1] https://www.welivesecurity.com/la-es/2019/05/17/detecciones-eternalblue-alcanza-nuevo-pico-desde-wannacry/

con la falla que presentan los dos sistemas operativos que se encuentran sin una actualización nueva lo cual los vuelve vulnerables a este ataque.

Para contener estos ataques informáticos, se formuló estrategias de contención de riesgos y vulnerabilidades en la infraestructura TI de la organización que se encontraron en la fase anterior

- Actualizar los sistemas operativos de las máquinas.
- Eliminaría el SMBv1 el cuan es protocolo que permite acceder y modificar a archivos de un servidor remoto, así como a otros recursos, la última actualización fue en el 216[2]
- Recomiendo instalar el parche MS17-010 para eliminar la vulnerabilidad que presenta la falla de seguridad con identificador CVE-2017-0144.
- Crear un equipo de respuesta a incidentes, responsabilidades.
- Crear procedimientos de recuperación y restauración de sistemas SIN eliminación de posibles evidencias del ataque.
- Monitorear periódicamente a toda la red para identificar posibles fallas.

Al momento de revisar todas las vulnerabilidades, se recomienda instalar el SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas.[3]

Las funciones principales del sistema es recopilar información de registros para verificar el cumplimiento de ciertas normas de seguridad en las compañías detención y bloqueo de actividades sospechosas.

[2] https://www.nerion.es/blog/protocolo-smb1/
[3] https://www.helpsystems.com/es/blog/que-es-un-siem

Una de las características y la más importante es que podemos monitorear en tiempo real todo el tráfico de información de nuestra compañía y activar las alertas de posibles ataques.

6. LINK DE VIDEO SUSTENTACIÓN

https://youtu.be/w7hWGi__QuI

7. RECOMENDACIONES

Teniendo como base el diagnóstico que arrojo la organización Whitehouse Security equipos actualizados, se sugiere poner en práctica el Manual de funciones que maneja la organización en funciones y políticas de privacidad que se requieren para salvaguardar la información generada.

Actualizar el SMBv1 el cual es un protocolo obsoleto que permite acceder y modificar a archivos de un servidor remoto, así como a otros recursos de la infraestructura TI.

Se recomienda la instalación del parche MS17-010 para eliminar la vulnerabilidad que presenta la falla de seguridad con identificador CVE-2017-0144 todo esto con el propósito de mejorar la ciberseguridad en la organización.

Revisando el nivel de conocimiento que muestran los empleados de los procesos seguridad se recomienda diseñar un plan de capacitar al personal en cuanto a la seguridad TIC la ética y la ley que rigen los diferentes delitos de cibernéticos.

8. CONCLUSIONES

Se diseñaron diferentes estrategias de contención arrancando desde el análisis de riesgos y vulnerabilidades en la infraestructura TI de la organización WhiteHouse Security.

Desde el marco legal se realizó una evaluación de las acciones de los equipos Red Team & Blue Team dando como resultado un informe técnico con las recomendaciones y procedimientos a seguir para realizar las mejoras.

Mediante la instalación de diferentes programas se demostró las vulnerabilidades en escenario de prueba la organización con el uso de metodologías y técnicas de intrusión arrojando como resultado un informe técnico con todas las falencias encontradas y las posibles soluciones al respecto.

9. REFERENCIAS BIBLIOGRAFÍA

R. (2020, 22 septiembre). Center for Internet Security (CIS) Benchmarks - Microsoft Compliance. Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-cis-benchmark?view=o365-worldwide

Microsoft Windows SMB escalada de privilegios. (2020, 7 octubre). MICROSOFT WINDOWS HASTA XP SP3 SMB ESCALADA DE PRIVILEGIOS. https://vuldb.com/es/?id.98019#:%7E:text=Una%20vulnerabilidad%20fue%20encontrada%20en,es%20afectada%20por%20esta%20vulnerabilidad.&text=El%20advisory%20puede%20ser%20descargado,como%20CVE%2D2017%2D014

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado

de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

.

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

R. (2020, 22 septiembre). Center for Internet Security (CIS) Benchmarks - Microsoft Compliance. Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-cis-benchmark?view=o365-worldwide

Microsoft Windows SMB escalada de privilegios. (2020, 7 octubre). MICROSOFT WINDOWS HASTA XP SP3 SMB ESCALADA DE PRIVILEGIOS. https://vuldb.com/es/?id.98019#:%7E:text=Una%20vulnerabilidad%20fue%20encontrada%20en,es%20afectada%20por%20esta%20vulnerabilidad.&text=El%20advisory%20puede%20ser%20descargado,como%20CVE%2D2017%2D0144

[Anónimo]. Pentesting con OWASP Zed Attack Proxy. Available http://www.tic.udc.es/~nino/blog/psi/2012/pentestingZAP2.pdf

Ortiz Aristizábal, D. (2019). Desarrollo De Metodología Para Hallazgos De Vulnerabilidades En Redes Corporativas E Intrusiones Controladas. https://repository.libertadores.edu.co/bitstream/handle/11371/342/DiegoFernandoOrtizAristizabal.pdf?sequence=2&isAllowed

You are being redirected... (2017). infolaft.com. https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

Carisio, E. (2019, 26 septiembre). Ataque cibernético: consecuencias, cómo actuar y cómo protegerse. #ADNCLOUD. https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/

Smartekh, G. (2012). *¿QUÉ ES HARDENING?* Blog-GrupoSmartekh. https://blog.smartekh.com/que-es-hardening

T., J. (2019). Ley de Delitos Informáticos en Colombia - DELTA Asesores. [online] DELTA Asesores. Available at: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Toro, R. (2019). ISO 27005: Seguridad de la Información y de las comunicaciones. [online] PMG SSI - ISO 27001. Available at: https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE GRADO. {En línea}. {Consultado junio 2009}. Disponible en: http://www.ICONTEC.org/BancoConocimiento/C/compendio_de_tesis_y_otros_trabajo