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

RICARDO FERNANDEZ ARBOLEDA

JOHN FREDDY QUINTERO
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2020

RESUMEN

En el desarrollo de cada una de las etapas del seminario, brinda la oportunidad para entender el marco normativo colombiano referente a delitos informáticos (ley 1273 de 2009) y protección de datos personales (ley 1581 de 2012), de la misma manera el código de ética emitido por el COPNIA y la forma de entender basado en casos de uso en el cual se presentan supuestos en los cuales se debió realizar el discernimiento si era procedente o no lo propuesto. Como punto inicial se debe realizar la verificación de los postulados éticos y normativos vigentes con el fin de desarrollar las actividades técnicas y resaltando la importancia de las actividades desarrolladas por el Red Team y el Blue Team (basados en el marco legal). De la misma manera se brinda la oportunidad de conocer herramientas útiles para el proceso de pruebas de penetración, monitoreo y documentación en línea con el fin de conocer las vulnerabilidades conocidas y metodologías para pruebas de penetración y propias del Red Team y Blue Team. Por último, se desarrollan actividades practicas con el fin de brindar un entendimiento de las operaciones que se deberán desarrollar por los equipos.

Se puede encontrar la sustentación en:
https://www.youtube.com/watch?v=NepjbsOQN9M

ÍNDICE

Lista de Tablas

LISTA DE GRAFICAS

GLOSARIO

Activo Informático[1]***:*** Es cualquier componente, dispositivo o dato del entorno que apuntala actividades afines con la generación de información. Incluyen generalmente software, hardware e información.

Ataque Informático[2]***:*** Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red.

Blue Team[3]***:*** Es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva.

Ciberataque[4]***:*** Los ciberataques pueden implicar un equipo muy unido de hackers de élite que trabajan bajo el mandato de un estado nación. Su intención es crear programas que aprovechen fallas previamente desconocidas en el software. Así consiguen filtrar datos confidenciales, dañar infraestructura clave o desarrollar una base para futuros ataques***.***

Ciberseguridad[5]***:*** La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Confidencialidad[6]***:*** Consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que, si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo

---

[1] Ciberseguridad sin miedo [Consultado 16 de octubre 2020] Disponible en URL: https://www.widefense.com/recursos/ciberseguridad/activo-informatico-gerente-cuidar/

[2] EcuRed [Consultado 16 de octubre 2020] Disponible en URL: https://www.ecured.cu/Ataque_inform%C3%A1tico

[3] UNIR (La Universidad en Internet) [Consultado 16 de octubre 2020] Disponible en URL: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[4] Tecnologias para los negocios [Consultado 16 de octubre 2020] Disponible en URL: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/

[5] Ciberseguridad [Consultado 16 de octubre 2020] Disponible en URL: https://sites.google.com/site/jezabelydyddra/concepto

[6] Seguridad Informatica[Consultado 16 de octubre 2020] Disponible en URL: https://infosegur.wordpress.com

de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio, entre otros.

Disponibilidad*[7]*: Se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

Exploit*[8]*: Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Integridad*[9]*: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

Pentesting*[10]*: Es una abreviatura de las palabras inglesas “penetration” y “testing”, que significa test. Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

Purple Team*[11]*: Existen para asegurar y maximizar la efectividad de los equipos rojo y azul. Lo hacen integrando las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team. Idealmente, no debería ser un equipo, sino una dinámica de cooperación entre los equipos rojo y azul***.***

---

[7] Seguridad Informatica[Consultado 16 de octubre 2020] Disponible en URL: https://infosegur.wordpress.com

[8] Dragoit [Consultado 16 de octubre 2020] Disponible en URL: https://dragoit.com/blog/definicion-de-exploit/

[9] Seguridad Informatica[Consultado 16 de octubre 2020] Disponible en URL: https://infosegur.wordpress.com

[10] Openwebinars [Consultado 16 de octubre 2020] Disponible en URL: https://openwebinars.net/blog/que-es-el-pentesting/

[11] UNIR (La Universidad en Internet) [Consultado 16 de octubre 2020] Disponible en URL: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Red Team*[12]*: Es un servicio en el cual, el scope o alcance es muchísimo más amplio y rico en relación con los activos y el tiempo para modelar los escenarios de ataque. Un servicio gestionado de Red Team no suele estar limitado en tiempos ni en infraestructura y aplicaciones a probar, y normalmente la ejecución de este suele ser tanto externo como interno, dando como resultado que el testeo de la postura de seguridad de la compañía sea mucho más real y completa que un penetration test tradicional.

[12] BlackmantiSecurity [Consultado 16 de octubre 2020] Disponible en URL: https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

INTRODUCCIÓN

Los múltiples cambios a los que se ve enfrentado el mundo ha creado la necesidad inminente de que todas las organizaciones locales e internacionales se adapten a ellos, estableciendo de esta forma tecnologías relacionadas con los novedosos conocimientos en ciberseguridad implementados a fin de conocer el modo en que los atacantes operan aprovechando las vulnerabilidades presentes en los sistemas informáticos, convirtiéndose así en el punto crítico de investigación del presente informe: la prevención y minimización de estos ataques.

En este sentido, es fundamental resaltar que la gestión en ciberseguridad que seguirá esta línea de investigación consiste en identificar todos y cada uno de los ámbitos de protección, detección y posibles respuestas ante potenciales ataques, enmarcados todos ellos en un aseguramiento continuo de los sistemas informáticos que garanticen el correcto funcionamiento de las empresas afectadas. Ante este hecho, se ha evidenciado que las operaciones basadas en Red Team se han postulado como uno de los mejores procesos que siguen altos esquemas de revisión y aseguramiento para identificar de este modo la seguridad de los sistemas informáticos empleados en la operatividad de las organizaciones y las diversas actividades usadas para evidenciar potenciales vulnerabilidades y las posibles protecciones, detecciones y respuestas hacia ellas. De la misma manera, el concepto Blue Team complementa el objetivo del Red Team en su uso como mecanismo para dar respuesta frente a la detección y la mitigación de las vulnerabilidades halladas.

OBJETIVOS

Objetivo General

Con este informe se busca englobar los enfoques de Red Team y Blue Team para atender las necesidades de ciberseguridad en las organizaciones con la finalidad de conseguir altos niveles de protección de los datos informáticos, además de la detección oportuna de posibles vulnerabilidades y/o ataques y su respuesta oportuna frentes a los mismos.

Objetivos Específicos

1. Analizar la normativa vigente en Colombia en lo que respecta a delitos informáticos y protección de datos personales
2. Describir el proceso de pentesting elaborado para la compañía WhiteHouse Security
3. Definir las herramientas empleadas en los procesos de contención de ataques informáticos
4. Enumerar las recomendaciones estratégicas en seguridad informática.

1. INFORME TÉCNICO

El presente documento brinda el detalle de lo asimilado referente a las etapas desarrolladas en los postulados por parte de WhiteHouse Security, con un enfoque critico de lo desarrollado para dar análisis de las estrategias a desarrollar por el Red Team y por el Blue Team, por último, brindar las recomendaciones de las mejores estrategias por estos equipos y como la ciberseguridad está tomando fuerza tomando como base el hecho de que el activo más importante en estos años es la información.

1.1. Marco Normativo en Colombia y Código de Ética

Actualmente en Colombia se le dio la importancia a la información y a la revolución del uso cotidiano de infraestructura tecnológica para dar respuesta y mejorar la eficiencia de los diferentes procesos desarrollados por las empresas privadas, publicas, mixtas o personas naturales; con la inclusión de este componente y tomando en cuenta que con el desarrollo de nuevas herramientas tecnológicas esta la posibilidad de la vulneración a cada uno de los componentes de la infraestructura tecnológica que soporta el almacenamiento y custodia de la información, por lo anterior, se hace necesario brindar herramientas jurídicas con el fin de generar acciones legales en caso de presentarse algún delito informático o el uso no adecuado para el tratamiento datos personales. Por lo anterior se realiza la emisión de dos (2) leyes que modifica el código penal y agrega un nuevo apartado sobre delitos informáticos y otro para reglamentar el correcto manejo de datos personales el cual en su momento original nació como la ley 527 de 1999.

Respecto al código de ética se hace importante conocerlo, puesto que, como profesionales del área de seguridad informática, más específicamente el área de ingeniería informática o de sistemas están regidos por el Consejo Profesional Nacional de Ingeniería (COPNIA), el cual dicta el código de ética[13] para la ejecución de actividades de la profesión, los cuales en caso de incumplir puede conllevar sanciones y revocación de la tarjeta profesional, el cual avala las actividades del profesional; se debe tener en cuenta que no se debe por ningún motivo incumplir la ley o aceptar condiciones que puedan llegar a contrariar lo normado y legislado, de igual manera, lo importante es desarrollar actividades de la profesión y de la vida cotidiana basado en un correcto desarrollo de las actividades sin generar ventajas o elementos que apoyen el fraude o incumplimiento de la ley.

[13] Código de ética, para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, emitido por el Consejo Profesional Nacional de Ingeniería (COPNIA) [Consultado 15 de octubre 2020] Disponible en URL:
(Copnia, 2020)

Es de resaltar que es de suma importancia conocer las legislaciones vigentes en estos temas con el fin de:

1. Conocer el alcance a nivel legal que se puede dar a las pruebas de penetración o generación de métodos de defensa.
2. En caso de presentarse algún tipo de ataque o explotación de una vulnerabilidad, tener claro que se debe contener y posterior realizar la denuncia correspondiente ante los órganos correspondientes.
3. De la misma manera, es de importancia para que todo empresa busque la manera de implementar el aseguramiento físico y lógico para el acceso a sus sistemas de información, bases de datos o infraestructura tecnológica, puesto que en caso de presentarse afectación por alguna vulneración o fuga de información genera desprestigio o daño al buen nombre, pérdidas económicas, robo de información, secuestro de información y tomando como base la ley de protección de datos personales, siendo los custodios de dicha información puede conllevar sanciones a la empresa vulnerada por no tener implementado buenas prácticas para evitar estas acciones.

A continuación, se detallan las leyes y decretos que se encuentran vigentes:

Ley 1273 de 2009[14]: la presente ley dispuso la modificación del código penal reglamentando el “bien jurídico tutelable de la protección de la información y de los datos”, dicho proceso se legislo por el incremento de uso de las tecnologías de la información y comunicación, viéndose cada día la implementación y tecnificación de procesos, pasando del resguardo de información sensible y confidencialidad en carpetas, archivadores o bodegas, a equipos de cómputo, infraestructura tecnológica o al modelo de cloud computing; por lo anterior se debió legislar de tal manera que si una persona natural o jurídica atenta contra la confidencialidad, integridad y disponibilidad de los datos de sistemas informáticos tal como el acceso a sistemas informáticos sin el debido permiso, obstaculización en el correcto funcionamiento de un sistema informático o red de comunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, suplantación de sitios web para la captura de datos personales tendría implicaciones legales y punitivas, de igual manera se definen como atentados informáticos u otras infracciones realizar algún proceso de captación de información sin autorización, intrusión a un sistema informático sin el debido permiso, robo de bienes intangibles a través de medios informáticos.

[14] Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, emitido por el congreso de Colombia [Consultado 15 de octubre 2020] Disponible en URL: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Ley 1581 de 2012[15]: la ley derogo lo que corresponde a la ley 1266 de 2008, dando un espectro más amplio y no limitado únicamente a la información de tipo financiero, crediticio, comercial, de servicios y lo proveniente de terceros países; la ley busco generalizar el concepto de protección de datos personales, manteniendo los principios rectores de la Ley 1266 de 2008 y anteriormente la ley 527 de 1999, en el cual se fundamenta el cumplimiento de tratamiento de datos personales, legalidad en materia de tratamiento de datos, uso para los fines dispuestos, libertad de aceptación y autorización del uso, veracidad de la información almacenada, transparencia, de acceso y circulación restringida, de seguridad y confidencialidad; un cambio respecto a las anteriores leyes es el hecho de categorizar los datos como datos sensibles y definición de que dato se puede considerar sensible, el tratamiento que se debe dar y disposiciones referente a la información de menores de edad. Se plantean los derechos y deberes en el proceso del tratamiento de datos personales por cada uno de los actores que resguarden este tipo de información. La SIC se mantiene como la entidad encargada de hacer cumplir las disposiciones de la presente ley y generar auditorias para la verificación del cumplimiento de lo dispuesto. Un punto importante de la ley 1581 de 2012 es la creación del Registro Nacional de Bases de Datos (RNBD), definiéndose como el directorio público en donde toda entidad que resguarde datos personales deberá realizar un registro de sus bases de datos y las políticas estipuladas a nivel interno para salvaguardar el cumplimiento de los datos personales.

Decreto 1377 de 2013[16]: por medio del cual se reglamenta de manera parcial la ley 1581 de 2012 y a través de la cual se estipula la disposiciones para el proceso de recolección de los datos personales, buscando dar cumplimiento a los principios rectores y hacer uso de la información únicamente para la finalidad por lo cual fue entregado, deberá existir una autorización explicita del titular de los datos personales para su tratamiento, teniendo el titular la capacidad de retirar la autorización y solicitar en cualquier momento las pruebas de dicha autorización. Uno de los elementos principales del presente decreto es la reglamentación de que toda entidad pública o privada que realice tratamiento de datos personales debe implementar una política de tratamiento de datos personales, divulgarla al interior de cada organización, darle cumplimiento, hacerlo parte de la cultura organizacional, en la política debe estar contenido el proceso de tratamiento de datos personales, los derechos, los deberes y responsabilidades del tratador de los datos.

[15] Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales, emitido por el congreso de Colombia [Consultado 15 de octubre 2020] Disponible en URL: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

[16] Decreto 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012, emitido por el presidente de la República de Colombia [Consultado 15 de octubre 2020] Disponible en URL: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

1.2. Red Team y Blue Team

El concepto original fue introducido hace mucho tiempo durante la Primera Guerra Mundial y como muchos términos utilizados en la seguridad de la información, se originó en el ejército. La idea general era demostrar la efectividad de un ataque a través de simulaciones. La efectividad de las simulaciones basadas en tácticas reales que podría utilizar el adversario es bien conocido y utilizado en el campo militar y de seguridad cibernética.

1.2.1. Red Team

Se define como una prueba de intrusión mediante el cual se lleva a cabo una búsqueda de posibles vulnerabilidades al interior de los sistemas informáticos y las fallas en la estructura tecnológica de una empresa[17]. Para ello, se contrata un equipo de expertos en ciberseguridad para que realice ataques a los sistemas en estudio de forma intencional. Esto es logrado emulando los comportamientos y técnicas de los posibles atacantes de la manera más realista posible. La práctica es similar, pero no idéntica, a las pruebas de penetración e implica la consecución de uno o más objetivos.

Este grupo designado prueba la postura de seguridad de la organización para ver cómo será su comportamiento contra ataques en tiempo real, antes de que ocurran. En el campo de la seguridad informática, la adopción del enfoque del Red Team también ayuda a las organizaciones a mantener sus activos más seguros. Esto requiere de un personal altamente capacitado dotados con diferentes conjuntos de habilidades y deben ser plenamente conscientes de la amenaza actual y el panorama general de la organización. En este punto es sumamente importante que el Red Team este al tanto de las tendencias del mercado en el cual opera la organización contratante para comprender de este modo como se están produciendo los ataques hacia ella. Incluso en algunas circunstancias y dependiendo de los requisitos de la organización, los miembros del equipo deben tener habilidades de codificación para crear su propio exploit y personalizarlo para aprovechar mejor las vulnerabilidades relevantes que podrían afectar a la empresa.

1.2.1.1. Metodología Pentesting

Para el caso propuesto por WhiteHouse Security se usó como metodología la siguiente:

Planificación: Durante el proceso de planificación se realizó entendimiento de la solicitud del cliente en la cual se exponía claramente que los equipos a revisar eran de sistema operativo windows 7, con actualizaciones de sistema operativo

[17] Red Team, emitido por redteams.net [Consultado 15 de octubre 2020] Disponible en URL: https://redteams.net/redteaming/2013/what-is-a-red-team

obsoletas y sin aplicar el parche MS17-010 el cual solventa la vulnerabilidad CVE-2017-0144. Tomando en cuenta lo anterior, se realiza uso de la herramienta OpenVAS para ejecutar el escaneo de vulnerabilidades sobre las dos máquinas con IPs 192.168.1.12 y 192.168.1.13. como resultado se obtuvo la siguiente información referente a vulnerabilidades:

Tabla 1. Vulnerabilidades evidenciadas en máquinas Windows 7

Name	Severity	Quality of Detection	Hosts	Descripción
OS End Of Life Detection	10.0 (High)	80%	1	La vulnerabilidad radica en el hecho de que el sistema operativo ya no es soportado por el fabricante
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	1	Vulnerabilidad que si se llega a explotar permitirá al atacante generación de código arbitrario o en otro caso denegación de servicios.
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	2	Vulnerabilidad que permite al atacante obtener control de la maquina con los privilegios del usuario que se encuentre con login, afecta el protocolo smb v1.0 por el puerto 445
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	2	Vulnerabilidad que permite al atacante conseguir más conocimiento sobre el host remoto o host atacado.
Fuente el autor. Verificación de vulnerabilidades a través de OpenVAS				

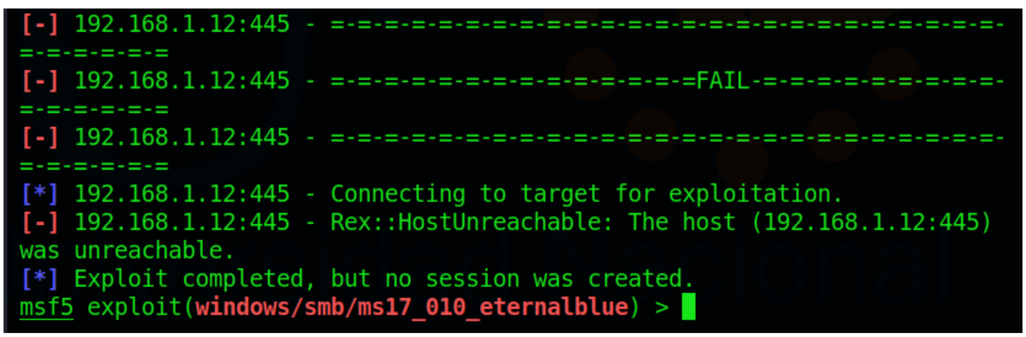
Referente a los CVEs relacionados están enfocados a la vulnerabilidad de SMB.V1.0, los cuales se relacionan a continuación:

- Microsoft Windows SMB Server NTLM Multiple Vulnerabilities(971468): CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231
- Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389): CVE-2017-0143, **CVE-2017-0144**, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 y CVE-2017-0148

Explotación: Utilizando la información obtenida del proceso de planificación, en el cual se logra evidenciar una clara oportunidad para un atacante de hacer explotación de la vulnerabilidad MS17-010, el cual permite realizar acceso no permitido de manera remota a la maquinada atacada y realizar ejecución de código arbitrario, obtener información, eliminar información, agregar cuentas, insertar código malicioso, buscar afectar otros equipos que se encuentren en la misma red del equipo atacado.

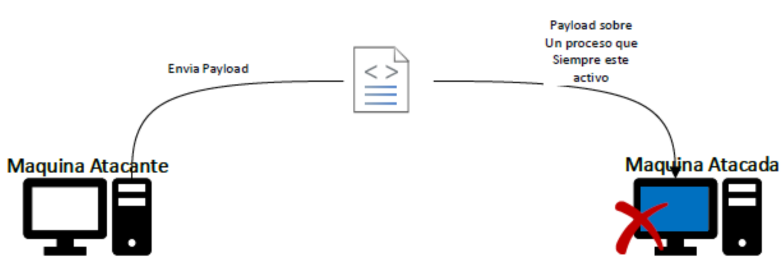
Se realiza la explotación a través de la herramienta MetaSploit de la maquina 192.168.1.12, la cual cuenta con sistema operativo Windows 7 home premium build 7600 x86, esta máquina al intentar realizar el proceso de explotación y falla del mismo se genera un crash sobre el sistema operativo, lo cual revisando la documentación en exploit-db, se evidencia que en caso de fallar la explotacion este puede generar un crash al Sistema operativo "*The exploit might FAIL and CRASH a target system (depended on what is overwritten)*"[18], obligando al mismo a realizar un reinicio para recuperarse, se realizó uso de la misma carga útil que en el de 64 bits, como la maquina realiza reinicio no se logra obtener acceso a la misma, pero cada intento de explotación genera el crash de la máquina, evidenciándose que la maquina con constantes pantallazos azules es la 192.168.1.12 con hostname win7.

Figura 1. Ejecución explotacion de maquina 192.168.1.12



Fuente: el autor

Figura 2. Diagrama explotación maquina 192.168.1.12



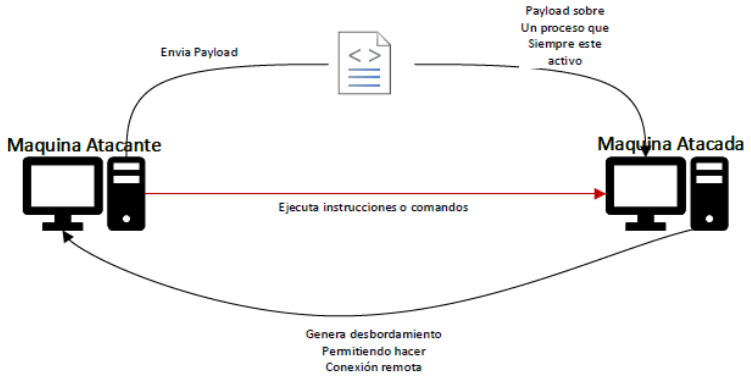
---

[18] EternalBlue crash Windows 7 x86, emitido por exploit-db [Consultado 15 de octubre 2020] Disponible en URL: https://www.exploit-db.com/exploits/42031

Fuente: el autor

Referente a la maquina 192.168.1.13 se evidencia según el análisis de vulnerabilidades que tiene como sistema operativo Windows 7 profesional build 7601 service pack 1 de 64 bits (revisando el CVE-2017-0144, se evidencia que es un sistema operativo vulnerable a explotaciones de este tipo), con hostname PC202006. Al momento de realizar la explotación se logra conseguir acceso de manera remota a la maquia, permitiéndose la ejecución de código arbitrario y búsqueda del archivo en el cual el atacante estaba almacenando la información. Basándose en este hecho, desde esta máquina se puede generar adición de código malicioso a la misma u otras que se encuentren en la misma red.

Figura 3. Diagrama explotación maquina 192.168.1.13



Fuente: el autor

Reporte: Con la premisa de que el proceso de explotación fue exitoso se realiza la sugerencia al Blue Team, con el fin de que realice la verificación de cómo se puede realizar defensa para esta vulnerabilidad, entregando el detalle del proceso de pentesting, de igual manera se realiza entrega de reporte ejecutivo a la parte directiva para el conocimiento y levantar la alerta de esta brecha de seguridad.

1.2.2. Blue Team

Hace referencia al equipo interno cuya función primordial es defender los ataques llevados a cabo por parte del Red Team[19].

El Blue Team debe distinguirse de los equipos de seguridad estándar empleados en la mayoría de las organizaciones, puesto que la mayoría de los equipos de operaciones de seguridad no tienen una mentalidad de vigilancia constante contra el ataque, que es la misión y la perspectiva de un verdadero Blue Team. El Blue

[19] Blue Team, emitido por coresecurity [Consultado 15 de octubre 2020] Disponible en URL: https://www.coresecurity.com/penetration-testing/red-team

Team debe asegurarse de que los activos estén seguros y en caso de que el Red Team encuentre vulnerabilidad y la explota, necesitan remediarla y documentarla rápidamente como parte de las lecciones aprendidas.

1.2.2.1. Contención de Ataques Informáticos

Tomando en cuenta lo evidenciado referente al pentesting realizado por el Red Team, se hace necesario que el Blue Team comience a trabajar en buscar la manera de mitigar la brecha de seguridad y posterior la generación de un plan de trabajo para realizar monitoreo y contención de vulnerabilidades.

Para el caso de eternal blue se debe realizar alguna de las siguientes acciones:

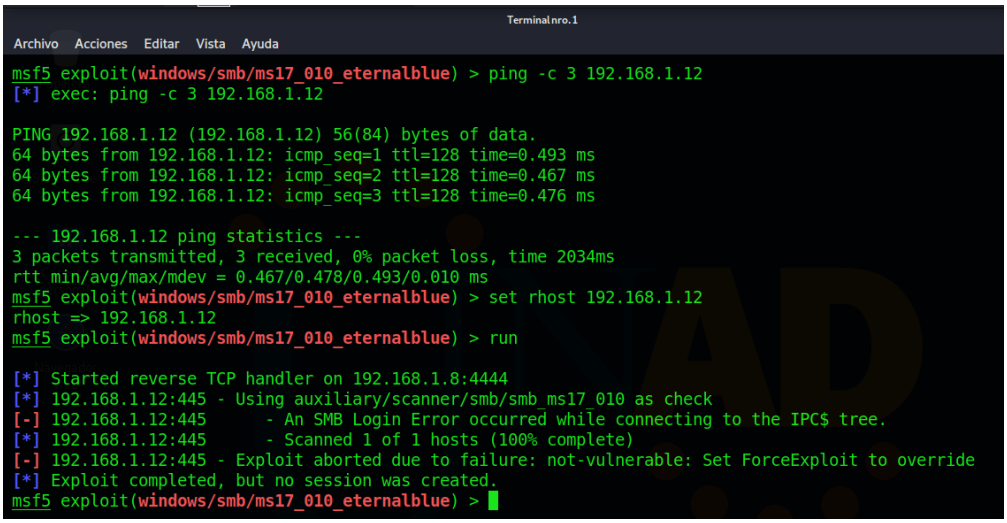
Aplicación de parche MS17-010: Se debe realizar la descarga y aplicación del parche de seguridad MS17-010[20] el cual arregla la brecha de seguridad conocida como eternal blue sobre las maquinas afectadas

Actualización de parches de seguridad hasta lo soportado por fabricante: un elemento importante en todo plan de seguridad es que los equipos conectados a la red estén con las actualizaciones de fabricante y principalmente los cumulativos de seguridad, con el fin de mitigar el riesgo de ser afectado por alguna brecha de seguridad conocida.

Realizar inactivación del protocolo SMBv1: Para mitigar lo evidenciado por el Red Team, se debe realizar el aislamiento de las maquinas o en su defecto, si se conoce ya la vulnerabilidad, buscar la manera de cerrar la brecha de seguridad, a continuación, se da un ejemplo del proceso realizado para mitigar la vulnerabilidad conocida como eternal, tomando como base la información obtenida en el benchmark del sistema operativo windows 7, se evidencia que para el protocolo SMBv1 se debe ejecutar la siguiente sentencia - `Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force` - por powershell con privilegios de administrador para inactivar dicho protocolo; al momento de realizar este proceso se mitiga la vulnerabilidad encontrada.

[20] Parche MS17-010, emitido por Microsoft [Consultado 15 de octubre 2020] Disponible en URL: Microsoft https://support.microsoft.com/es-co/help/4013389/title

Figura 4. Intento de ataque fallido



Fuente: el autor

Hardening al sistema operativo: El hardening se define como un proceso mediante el cual se elabora un mapeo general de los sistemas informáticos con la finalidad de identificar las potenciales vulnerabilidades presentes al interior de estos y que fueron configurados con anterioridad. En este punto, es importante señalar que las vulnerabilidades halladas dependerán directamente de la cantidad de entornos en que se ejecutarán los sistemas empleados. Posterior a ello, se puede realizar uso de los Benchmark del Center for Internet Securiy (CIS), en el cual se podrán descargar las diferentes guías, las cuales permiten a cualquier persona del área de seguridad informática realizar el análisis de las buenas prácticas o referentes de seguridad que se deben realizar sobre un sistema operativo, un sistema de gestión de base de datos, una herramienta de capa media, dispositivos de red, Firewall, herramientas de virtualización entre otras.

por lo anterior podemos inferir que puede ser un excelente punto inicial para la verificación de si los dispositivos electrónicos cumplen elementos mínimos ya conocidos y documentados para evitar o mitigar cualquier tipo de riesgo que pueda desencadenar en un ataque informático a través de los controles propuestos.

En el caso de lo evidenciado en la etapa 3 del seminario, se evidencia en el documento CIS para el sistema operativo Windows 7 en su numeral "*18.3.2 (L1) Ensure 'Configure SMB v1 client' is set to 'Enabled: Bowser, MRxSmb20, NSI' (Scored)"* se menciona la descripción de que este elemento debe estar inactivo, el método de cómo se puede auditar y en dado caso los controles que se pueden implementar para evitar esta vulnerabilidad. En conclusión, CIS permite tener una guía y realizar procesos de hardenización.

Implementación de herramientas de contención y monitoreo: Blue Team debe proponer y buscar la implementación de herramientas de monitoreo y contención para evitar que las brechas de seguridad se lleguen a materializar, en el mercado se encuentran diferentes herramientas de licencia tipo GPL.

1.2.2.2 Ataque en Tiempo Real

En caso de no tener alguna herramienta de monitoreo o detección de intrusos en nuestra red o sistema se hace necesario ejecutar acciones de manera inmediata sobre la red, los equipos de cómputo, servidores, dispositivos electrónicos o sistemas informáticos que posiblemente se encuentren comprometidos. A continuación, se enumeran los elementos para tener en cuenta en caso de tener un ataque en tiempo real:

1. Realizar aislamiento de conexión hacia internet (bloqueo de entrada y salida a internet de todos los dispositivos electrónicos), con el fin de
    a. Identificar si el atacante está realizando su actividad de manera local (inhouse) o desde redes externas
    b. En caso de estar sobre redes externas, se bloqueará el ataque
    c. Siguiendo la premisa que el atacante este por fuera, se evitara que siga sustrayendo información
    d. En el peor de los casos si el atacante realiza la adición de código malicioso sobre una de las maquinas es importante tener instalado protección antimalware para evitar la infección y propagación de un virus
2. Aislar completamente los equipos, servidores, dispositivos electrónicos que contengan información confidencial, sensible o necesaria para el funcionamiento correcto de la empresa.
3. Identificar los equipos susceptibles o vulnerables a algún ataque o inyección de código malicioso conocido, esto a través de:
    a. estado de los equipos en sus bases de datos de firmas de código malicioso de su protección antivirus
    b. Sistema operativo instalados, verificando y priorizando los no soportados por fabricante (obsoletos)
    c. actualizaciones no instaladas que puedan ser susceptibles a permitir ataques informáticos conocidos
    d. equipos con permisos brindados para permitir cumplir funciones y no generar interrupción de las operaciones, pero que dicho permiso pueda generar una brecha de seguridad, como tener habilitado el protocolo smb v1
4. Posterior a la identificación de estos equipos, se debe realizar aislamiento de estos equipos vulnerables y verificar si fueron comprometidos, por lo anterior se debe realizar ejecución de análisis de antivirus, cierre de brechas de seguridad basados en métodos de hardenización para el sistema operativo existente o para software de capa media.

5. Se debe realizar análisis de la red a través de una herramienta de monitoreo como OpenVAS buscando que equipos son susceptibles o estén comprometidos, con el fin de tomar acciones sobres los mismos
6. Verificar intentos fallidos de login de manera repetitiva
7. En caso de encontrarse un equipo comprometido se debe realizar desconexión de la red hasta el momento en el cual se encuentre desinfectado y con aplicación de buenas prácticas en términos de seguridad Informática sobre el mismo
8. Posterior al aislamiento y en caso de encontrarse fallas en la integridad de la información, se debe realizar restauración de Backup para permitir el funcionamiento de los sistemas informáticos.
9. Posterior a la mitigación se debe realizar una evaluación de riesgos y ver la manera de generar planes de trabajo buscando la disminución de la probabilidad y del impacto en caso de que se vuelva a materializar el riesgo
10. Realizar la implementación de una herramienta de monitoreo del estado de la red y los dispositivos conectados a ella, con el fin de realizar evaluación de vulnerabilidades y evitar la materialización con la implementación de detección de intrusos y adicional aplicación de medidas de hardening sobre lo detectado como vulnerable

1.2.3. Cooperación Blue Team Y Red Team

El trabajo del Red Team y el Blue Team no termina cuando el Red Team puede comprometer el sistema. Hay mucho más por hacer en este proceso, lo que crea la necesidad de colaboración entre ambos equipos[21].

La utilidad del enfoque Red Team vs Blue Team radica en la interacción y retroalimentación, en su capacidad de convertir el desafío en una forma de mejorar la capacidad de detectar y contrarrestar amenazas. Tal cooperación debe esforzarse por lograr una mejora continua, el Blue Team debe ver las actividades realizadas por parte del Red Team como una oportunidad para comprender las tácticas, técnicas y procedimientos.

El ataque del Red Team puede exponer las debilidades de los sistemas informáticos antes de que los delincuentes reales se aprovechen de ellos. Como cada equipo tiene diferentes propósitos, sus medios también serán diferentes.

Se espera que el Red Team domine el uso de herramientas ofensivas (por ejemplo, Meterpreter o Metasploit), saber qué es una inyección SQL, emplear herramientas de escaneo de red (Nmap), utilizar lenguajes de secuencias de comandos para

[21] Cooperación Red Team y Blue Team, emitido por securityaffairs [Consultado 15 de octubre 2020] Disponible en URL: https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html

reconocer los comandos del enrutador y del firewall, etc. Por otro lado, se supone que el Blue Team debe comprender cualquier fase de un Incidente.

Dar respuesta oportuna ante estos hechos, para dominar su propia cuota de herramientas e idiomas, para detectar patrones de tráfico sospechosos, identificar los indicadores de compromiso, utilizar adecuadamente un IDS, realizar análisis y pruebas forenses en diferentes sistemas operativos.

Se debe crear un informe final para resaltar los detalles sobre cómo ocurrió la infracción, proporcionar una cronología documentada del ataque, los detalles de las vulnerabilidades explotadas para obtener acceso y elevar privilegios (si corresponde), y el impacto generado en la empresa u organización.

1.2.4. Herramientas utilizadas

En el desarrollo de las actividades del Red Team como el Blue Team, se hace necesario el uso de herramientas informáticas usadas en sitio o basados en documentación en línea. A continuación, se detallan herramientas usadas para realizar pruebas de penetración el cual concierne al Red Team, herramientas de monitoreo y contención de vulnerabilidades el cual concierne a Blue Team y por ultimo documentación de vulnerabilidades y guías de buenas practicaspara ejecución o realización de proceso de hardening el cual es de importancia para ambos equipos, puesto que el uno requiere que no se materialice el riesgo y el otro estará encargado de verificar que ese riesgo no se materialice tomando la labor de pentester.

1.2.4.1. Herramientas Red Team

Metasploit[22]: Se define como una herramienta informática empleada para realizar auditorías de seguridad, con el objeto de identificar las posibles debilidades de los sistemas y hallar la mejor manera de protegerlos, la herramienta permite a los usuarios con conocimientos en el tema realizar pruebas de penetración, brindando un kit de herramientas para realizar explotación de vulnerabilidades en diferentes conceptos.

Nmap[23]: la herramienta Nmap permite realizar escaneo a nivel de red obteniendo información importante para realizar reconocimiento de los dispositivos conectados a una red, basado en la premisa de mapeo en todos y cada uno de los puertos, aplicaciones, identificándose información como sistema operativo usado por un host, puertos abiertos, de igual manera se puede programar un monitoreo para que se realice recolección de información, identificándose elementos que permitirán a

[22] Metasploit. [Consultado 15 de octubre 2020] Disponible en URL: https://www.metasploit.com/
[23] Nmap. [Consultado 15 de octubre 2020] Disponible en URL: https://nmap.org/

un usuario que audite o que intente realizar algún ataque las vulnerabilidades dentro de toda la información capturada.

OpenVas[24]: Esta herramienta ofrece un escenario de trabajo cuya finalidad consiste en integrar los instrumentos esenciales para realizar un escaneo oportuno de las posibles vulnerabilidades de los sistemas informáticos evaluados. La herramienta tiene como base el escaneo de vulnerabilidades a nivel de red y posterior a su configuración y captura de información, se puede realizar la verificación de vulnerabilidades de un host especifico y posterior corrección, es una herramienta que puede permitir al grupo definido de seguridad informática para atacar dichas vulnerabilidades y realizar mitigación de estos.

1.2.4.2. Herramientas Blue Team

Snort[25]: esta herramienta funciona tanto como sistema de detección de intrusos y sistema de prevención de intrusos, la ventaja que tiene es que se encuentra funcional desde 1998, lo cual genera confianza en la estabilidad y en la posibilidad de encontrar documentación gracias a la comunidad existente; esta herramienta es basada en la verificación de red. La desventaja es que se debe realizar la implementación de un ambiente grafico para dar manejo de una manera más intuitiva.

Untangle NG Firewall[26]: herramienta de tipo software para la implementación con el fin de realizar actividades de firewall y aseguramiento perimetral, tomando como premisa el aseguramiento o acceso únicamente a los puertos y aplicaciones que son requeridos por la organización, acceso controlado a través de segmentos de red.

Suricata[27]: esta herramienta realiza labores de sistema de detección de intrusos (IDS), de sistema de prevención de intrusos (IPS) y monitoreo de seguridad de red (NSM), su funcionamiento se basa en la verificación del tráfico de red.

1.2.4.3. Sitios de consulta en Línea Red Team y Blue Team

ExploitDB[28]: Un exploit se define como un código informático que se sirve de la detección de ciertas vulnerabilidades en un sistema y se aprovecha de este para atacar. Teniendo en cuenta esto, el sitio web exploit Db es un repositorio donde muchos expertos en ataques a la seguridad informática publican sus hallazgos de las vulnerabilidades en los sistemas y aplicaciones y como aprovecharse de ellas;

---

[24] OpenVas. [Consultado 15 de octubre 2020] Disponible en URL: https://www.openvas.org/
[25] Snort. [Consultado 15 de octubre 2020] Disponible en URL: https://www.snort.org/
[26] Untangle NG Firewall. [Consultado 15 de octubre 2020] Disponible en URL: https://www.untangle.com/untangle-ng-firewall/
[27] Suricata. [Consultado 15 de octubre 2020] Disponible en URL: https://suricata-ids.org/
[28] ExploitDB. [Consultado 31 de agosto 2013] Disponible en URL: https://www.exploit-db.com/

es otras palabras es como un instructivo que hacen viral para explicar sus técnicas. Esta plataforma permite obtener información que se puede usar para probar si la organización cuenta o no con las medidas para protegerse de algún tipo de ataque o explotación de vulnerabilidades.

CVE[29]: Se trata de un listado que contiene todas las fallas de seguridad informática a disposición del público en general. Dentro de esta lista se enumera cada vulnerabilidad con su respectivo código de identificación.

Center for Internet Security (CIS)[30]: es un sitio en el cual se pueden encontrar guías de buenas practicas para diferentes elementos, tales como sistemas operativos, gestores de bases de datos, elementos de capa media, etc., esto permitía al equipo de Red Team cuales vulnerabilidades se pueden llegar a explotar y son conocidos para uno de los elementos anteriores o en su defecto al Blue Team para saber cuáles son los métodos o procesos a desarrollar para mitigar el riesgo de materialización.

[29] CVE. [Consultado 31 de agosto 2013] Disponible en URL: https://cve.mitre.org/

[30] Center for Internet Security (CIS), Benchmark. [Consultado 15 de octubre 2020] Disponible en URL (Exploit Database, 2020) (MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017, 2020) (Rapid Metasploit, 2020) (NMAP.ORG, 2020)/

CONCLUSIONES

La ciberseguridad debe gestionar diferentes riesgos, no sólo proteger la información sino también contra ataques a los servicios: como sistemas, redes e infraestructuras críticas; entre otros puesto que está en juego la identidad y reputación del sector empresarial y quienes lo conforman.

Para proteger a las organizaciones contra estas amenazas, se aprendió en este diplomado sobre los factores claves que pueden ser de gran ayuda para mejorar la postura acerca de la seguridad. El Red Team ataca y el Blue Team defiende; sin embargo, el objetivo principal es compartido entre ellos: mejorar la postura de seguridad de la organización. Idealmente, el Red/ Blue Team trabajan en perfecta armonía entre sí, como dos manos que forman la capacidad de aplaudir. Para eso, el uso de Red y Blue Team se vuelve imperativo y el proceso de respuesta a incidentes es primordial para que las empresas obtengan mejor detección y respuesta ante ciber amenazas.

RECOMENDACIONES

Antes de iniciar con las recomendaciones para poder llegar a realizar un reforzamiento en la estrategia de seguridad informática en la organización, es importante tener en cuenta que estos procesos son exitosos si desde la dirección o gerencia de la organización están comprometidos con la seguridad, no es solo implementar herramientas y estrategias, es que la organización este comprometida y este proceso debe iniciar desde las altas directivas. Tomando en cuenta lo anterior, se comenta que basado en la práctica realizada a través de la solicitud de WhiteHouse Security se ve necesario que:

1. Se debe contemplar la implementación de los equipos Red Team y Blue Team, o en su defecto Purple Team (dependerá de la capacidad de adquisición y administración de costos de cada organización), con el fin de que cumplan la premisa de su funcionar, es decir, Red Team Ataca y Blue Team defiende; claramente esta actividad será a nivel interno.
2. Cumplir con la normatividad vigente en el país, en el caso de Colombia no llegar a generar alguna infracción sobre la ley 1273 de 2009 o la 1581 de 2012, en el marco de las pruebas de penetración deben ir enfocadas en nunca generar alguna infracción de estas leyes.
3. Cumplir con el código de ética para las actividades realizadas a nivel de Red Team y Blue Team.
4. Realizar un proceso de hardening sobre cada uno de los elementos informáticos que puedan llegar a ser comprometidos y buscar la manera de implementar cada una de las recomendaciones.
5. Tomar como base la documentación existente para buenas practicas que se encuentra disponible como lo es el benchmarking de Center of Internet Security o la información divulgada a través de CVE o Exploit-db.
6. Generar un plan de pruebas de penetración al menos dos veces en el año basado en escucha a través de red, o cuando se llegue a divulgar una vulnerabilidad que pueda llegar a afectar algún elemento informático de la organización.
7. Se debe realizar la implementación de seguridad perimetral a través de un firewall ya sea físico o lógico y permitir únicamente acceso a cada usuario a lo que requiere, buscando no dar más de lo que requiere.
8. Implementación de software antimalware en todo dispositivo que este conectado a la red institucional.
9. En caso de tener información divulgada a internet generar un plan de verificación exhaustiva con el fin de evitar cualquier tipo de ataque informático.
10. Generar la implementación de herramientas de monitoreo y contención para vulnerabilidades, se pueden encontrar diferentes herramientas en el mercado con licencias GPL o privadas.

11. Un punto importante, generar capacitación sobre los usuarios finales, darles a conocer todos los riesgos que se pueden llegar a tener y como pueden mitigar el riesgo.

REFERENCIAS BIBLIOGRAFICAS

Academia. (2014). Recuperado el 6 de Octubre de 2020, de Seguridad y Hardening en y Hardening en ServidoresServidores LinuxLin: https://www.academia.edu/33024222/Seguridad_y_Hardening

Arame. (s.f.). Recuperado el 6 de Octubre de 2020, de LA GUÍA DEFINITIVAPARA EL ROBUSTECIMIENTO (HARDENING)DE SERVIDORES: SUPERANDO LA BRECHA EN SEC-OPS: https://www.arame.com.mx/wp-content/uploads/2019/04/Whitepaper-Hardening-de-Servidores.pdf

BlackmantiSecurity. (16 de 10 de 2020). Obtenido de BlackmantiSecurity: https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

BlogdelCISO. (6 de Octubre de 2020). Obtenido de BlogdelCISO: https://blogdelciso.cl/2018/06/25/que-es-un-bluered-y-purple-team/

Center for Internet Security. (6 de Octubre de 2020). Obtenido de Benchmarks: https://www.cisecurity.org/cis-benchmarks/

Ciberseguridad. (16 de 10 de 2020). Obtenido de Ciberseguridad: https://sites.google.com/site/jezabelydyddra/concepto

CIS Microsoft Windows 7 Workstation Benchmark. (6 de Octubre de 2020).

Computer Science Columbia. (6 de Octubre de 2020). Obtenido de A Red Team/Blue Team Assessment of FunctionalAnalysis Methods for Malicious Circuit Identification: http://www.cs.columbia.edu/~simha/preprint_dac14.pdf

Copnia. (15 de 10 de 2020). *Código de Etica para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.* Obtenido de Código de Etica para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Core Security. (15 de 10 de 2020). Obtenido de Core Security: https://www.coresecurity.com/penetration-testing/red-team

Dragoit. (16 de 10 de 2020). Obtenido de Dragoit: https://dragoit.com/blog/definicion-de-exploit/

EcuRed. (15 de 10 de 2020). Obtenido de EcuRed: https://www.ecured.cu/Ataque_inform%C3%A1tico

esecurityplanet. (7 de Octubre de 2020). Obtenido de 10 Open Source Security Breach Prevention and Detection Tools: https://www.esecurityplanet.com/network-security/10-open-source-security-breach-prevention-and-detection-tools.html

ESED. (6 de Octubre de 2020). Obtenido de Pasos a seguir ante un ataque informático en tu empresa: https://www.esedsl.com/blog/pasos-a-seguir-ante-un-ataque-informatico-empresa

Exploit Database. (15 de 10 de 2020). Obtenido de Exploit Database: https://www.exploit-db.com/exploits/42031

InfoLaft. (6 de Octubre de 2020). Obtenido de ¿Qué hacer antes, durante y después de un ataque informático?: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

MinTIC. (7 de Octubre de 2020). Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017. (15 de 10 de 2020). Obtenido de MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017: https://support.microsoft.com/es-co/help/4013389/title

Netsparker. (6 de Octubre de 2020). Obtenido de Red Team Vs Blue Team Testing for Cybersecurity: https://www.netsparker.com/blog/web-security/red-team-vs-blue-team/

NMAP.ORG. (15 de 10 de 2020). Obtenido de NMAP.ORG: https://nmap.org/

OpenVas. (15 de 10 de 2020). Obtenido de OpenVas: https://www.openvas.org/

OpenWebinars. (16 de 10 de 2020). Obtenido de OpenWebinars: https://openwebinars.net/blog/que-es-el-pentesting/

Proteger Mi PC. (7 de Octubre de 2020). Obtenido de Mejores IDS Opensource para Detección de Intrusiones: https://protegermipc.net/2018/02/22/mejores-ids-opensource-deteccion-de-intrusiones/

Rapid Metasploit. (15 de 10 de 2020). Obtenido de Rapid Metasploit: https://www.metasploit.com/

Ribera, G. (15 de 10 de 2020). *Seguridad Informatica*. Obtenido de Seguridad Informatica: https://infosegur.wordpress.com/

Ribera, G. (s.f.). *Seguridad Informatica*. Obtenido de https://infosegur.wordpress.com/

Security Affairs. (15 de 10 de 2020). Obtenido de Security Affairs: https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html

SNORT. (15 de 10 de 2020). Obtenido de SNORT: https://www.snort.org/

Sofecom. (s.f.). (Sofecom) Recuperado el 6 de Octubre de 2020, de Sofecom: https://sofecom.com/que-es-un-siem/

Suricata. (7 de Octubre de 2020). Obtenido de Suricata: https://suricata-ids.org/

Tecnologia para los negocios. (16 de 10 de 2020). Obtenido de Tecnologia para los negocios: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/

Unir (La Universidad en Internet). (16 de 10 de 2020). Obtenido de Unir (La Universidad en Internet): https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Untangle. (15 de 10 de 2020). Obtenido de Untangle: https://www.untangle.com/untangle-ng-firewall/

What is a red Team. (15 de 10 de 2020). Obtenido de What is a red Team: https://redteams.net/redteaming/2013/what-is-a-red-team

Widefense. (16 de 10 de 2020). *Ciberseguridad sin miedo*. Obtenido de Ciberseguridad sin miedo: https://www.widefense.com/recursos/ciberseguridad/activo-informatico-gerente-cuidar/