CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Hamilton Felipe Quintero Monsalve

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN

CURSO SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM

MEDELLÍN

2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Hamilton Felipe Quintero Monsalve

Asesor Temático

John Freddy Quintero Tamayo

Asesor Metodológico

John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

VICERRECTORIA ACADEMICA Y DE INVESTIGACIÓN

CURSO SEMINARIO ESPECIALIZADO EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM

Medellín

2023

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Medellín,15 de Junio de 2023

DEDICATORIA

Papá donde quiera que estés, fuiste una inspiración. Que Dios te tenga en su gloria.

AGRADECIMIENTOS

A John Freddy Quintero Tamayo, M.Sc, docente y Analista de Ciberseguridad CSIRT UNAD. Quien con sus conocimientos y paciencia aporto al desarrollo de este trabajo.

Universidad UNAD, por todo el contenido bien preparado su logística que garantizaron una eficiente educación virtual.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

SCOPE: "Alcance" o "ámbito". En el contexto de un proyecto, el scope se refiere al conjunto de objetivos, entregables, tareas y limitaciones que se definen al inicio del proyecto y que se deben cumplir para que este sea exitoso

OSSTMM: Open Source Security Testing Methodology Manual. es un manual de pruebas de seguridad de código abierto, que proporciona una metodología sistemática y detallada para llevar a cabo pruebas de seguridad

FIREWALL: Herramienta de seguridad que permite la protección contra eventos malintencionados puede ser en una red (fisico) o logico en una estación o nodo.

CIS: Centro para la seguridad en internet. Se trata de una organización sin ánimo de lucro que busca mejorar la seguridad cibernética en todo el mundo.

SIEM: Security Information and Event Management; se trata de una plataforma que centraliza todas las alertas integrando diferentes fuentes en una organización. con el propósito de monitorear, alertar y reaccionar ante potenciales amenazas.

EDR: siglas de Endpoint Detection and Response. Se trata de sistemas de usuario final que se encargan de proteger los dispositivos alertando y aplicando la contención cuando sea requerida.

CVSS: (Common vulnerability Scoring System), (Sistema Común de Puntuación de Vulnerabilidades, en español) y es un marco estándar de la industria para clasificar y puntuar la gravedad de las vulnerabilidades de seguridad informática.

BOTNET: se refiere a una red de computadoras comprometidas por un atacante para realizar actividades maliciosas.

EXPLOIT: Se refiere a un código o técnica que se utiliza para aprovechar una vulnerabilidad en un sistema o aplicación.

PHISHING: Se refiere a un tipo de ataque en el que un atacante intenta engañar a una persona para que revele información confidencial como contraseñas, números de tarjeta de crédito o datos personales.

INTRODUCCIÓN

En la actualidad, la ciberseguridad se ha convertido en un tema de gran importancia para cualquier organización que maneje información crítica o confidencial. Es por eso que se han desarrollado equipos especializados en ciberseguridad, como los equipos Red Team y Blue Team, que tienen la tarea de proteger los sistemas de información de una organización y prevenir posibles ataques cibernéticos.

Para que estos equipos puedan llevar a cabo su trabajo de manera efectiva, es necesario que cuenten con una serie de capacidades técnicas, legales y de gestión específicas. En este sentido, es fundamental que los profesionales que forman parte de los equipos Blue Team y Red Team tengan una comprensión profunda de los procesos, metodologías, herramientas y marco legal que se aplican en el ámbito de la ciberseguridad.

En este contexto, es importante destacar la importancia de la formación y capacitación constante de estos profesionales, con el fin de mantenerse actualizados en las últimas tendencias y tecnologías en ciberseguridad. De esta manera, podrán estar preparados para enfrentar y prevenir posibles amenazas informáticas que puedan afectar la seguridad de la organización.

En este trabajo, se explorará en detalle las capacidades técnicas, legales y de gestión necesarias para los equipos Blue Team y Red Team, con el fin de brindar una visión general sobre cómo estos equipos pueden proteger los sistemas de información de una organización y prevenir posibles ataques cibernéticos.

OBJETIVOS

1.1 OBJETIVO GENERAL

Explicar las capacidades técnicas, legales y de gestión necesarias para que los equipos Blue Team y Red Team puedan proteger los sistemas de información de una organización y prevenir posibles ataques cibernéticos.

1.2 OBJETIVOS ESPECIFICOS

- Conocer el marco legal y ético que rige en el ámbito de la ciberseguridad.

- Explicar las habilidades técnicas para el uso de herramientas de seguridad informática y técnicas de pruebas de penetración.

- Comprender los procesos, metodologías y herramientas que se aplican en el ámbito de la ciberseguridad.

- Desarrollar habilidades de gestión y presentación de proyectos e informes de ciberseguridad que van de la mano con las habilidades de liderazgo para los equipos Blue Team y Red Team.

1. DESARROLLO DE LA ACTIVIDAD

Teniendo en cuenta en anexo 6 – escenario 5 usted debe presentar un informe técnico donde relacione los aspectos relevantes del desarrollo de las actividades anteriores y plantee recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam:

A. CONSTRUYA UN INFORME TÉCNICO DONDE SE PRESENTEN LAS ESTRATEGIAS REDTEAM & BLUETEAM PLANTEADAS EN EL SEMINARIO ESTE DEBE CONTENER:

DESARROLLO DEL INFORME

Para que un profesional en seguridad informática pueda proteger la información y la privacidad de una organización debe hacerlo mediante la implementación de estrategias de ciberseguridad eficaces y éticas tal como se presenta en las siguientes etapas:

A. Etapa 1: Conceptos equipos de Seguridad

Como profesionales de seguridad de la información si queremos poder proteger de manera efectiva la información y los sistemas de una organización. ***Es muy importante comprender los conceptos clave*** de la ciberseguridad, y así se ***facilita la identificación de las amenazas potenciales*** y las vulnerabilidades en los sistemas de información, para poder tomar las medidas preventivas y correctivas adecuadas que puedan minimizar los riesgos de seguridad.

Además, ***tener una comprensión sólida de la ciberseguridad*** puede ayudar a las organizaciones a cumplir con las normas y regulaciones de seguridad de la información y a ***mantener la confianza de sus clientes y socios comerciales***. En resumen, tener claros los conceptos de ciberseguridad es fundamental para la ***protección efectiva de la información y los sistemas en una organización***. Conceptos que se especifican a continuación y algunos también contenidos en el framework **OSSTMM** [1]y nombrados a continuación:

- **Red Team:** Se refiere a una práctica en la que un equipo de expertos se encarga de simular un ataque o escenario adverso contra un sistema u organización con el fin de identificar vulnerabilidades y mejorar las defensas. El término "red team" proviene de la estrategia militar, donde los equipos que representan al enemigo se designan como "rojos" para diferenciarlos de las fuerzas amigas[2].
- **Blue Team:** Se refiere a un grupo de profesionales de seguridad informática y defensa cibernética que se encargan de proteger un sistema o una organización contra los ataques de los adversarios. En contraposición al equipo Red (Red Team), que simula los ataques y explota las debilidades, el equipo Blue se enfoca en la detección, respuesta y mitigación de los ataques reales[3].
- **Firewall:** Es un software o hardware que se encarga de proteger una red informática de posibles amenazas externas, permitiendo o bloqueando el tráfico de red según políticas de seguridad establecidas. Actúa como una barrera entre la red protegida y el mundo exterior, controlando el acceso a los recursos de la red y protegiendo la información y los sistemas de la organización[4].

[1] ISECOM. (2008). Open Source Security Testing Methodology Manual (OSSTMM) Versión 3.0. Retrieved from https://www.isecom.org/OSSTMM.3.pdf
[2] Candau, J. (2019). Red Team: Cómo funciona y por qué lo necesitas. Ra-Ma Editorial.
[3] Bitdefender. (2019, 26 de julio). ¿Qué es el equipo Blue? Bitdefender Business Insights. https://www.bitdefender.com/business/what-is-blue-team/
[4] Barrera, J. A. (2017). Firewall: A Network Security System. International Journal of Computer Science and Information Security, 15(1), 72-80. [En línea]: https://www.researchgate.net/publication/316695216_Firewall_A_Network_Security_System

- **Scanning:** El escaneo en seguridad informática se refiere al proceso de exploración de una red, sistema o aplicación en busca de vulnerabilidades o puntos débiles que puedan ser explotados por atacantes malintencionados. Los escaneos pueden realizarse de forma manual o con herramientas automatizadas, y pueden ser utilizados para identificar posibles brechas de seguridad que necesiten ser corregidas[5].
- **Vulnerability**: Una vulnerabilidad en seguridad informática se refiere a una debilidad o fallo en un sistema, aplicación o infraestructura que puede ser explotado por un atacante malintencionado para causar daño o acceder a información confidencial. Las vulnerabilidades pueden surgir debido a errores de diseño, programación, configuración o mantenimiento, y pueden ser explotadas mediante diferentes tipos de ataques informáticos[6].
- **Penetration Testing:** Un pentest (o Penetration Test) es una prueba de seguridad de sistemas en la que se simulan ataques de ciberseguridad para identificar vulnerabilidades en la seguridad de un sistema o red[7].
- **Discovery**: Es una actividad de ciberseguridad que implica identificar activamente dispositivos, sistemas o aplicaciones en una red o entorno de computación determinado. El objetivo de esta actividad es descubrir posibles vulnerabilidades o debilidades de seguridad que puedan ser explotadas por atacantes malintencionados.
- **Enumeration:** Es el proceso de identificar activamente usuarios, cuentas, recursos y servicios en una red o sistema informático. La enumeración Verification (verificación de enumeración) es el proceso de confirmar la existencia y accesibilidad de los recursos y servicios identificados durante el proceso de enumeración.

[5] Gupta, A., & Singh, N. (2018). Scanning Techniques in Network Security. International Journal of Computer Applications, 180(29), 47-53. [En línea]: https://www.ijcaonline.org/archives/volume180/number29/29845-2018919082
[6] Shahzad, F., Aslam, W., & Saleem, S. (2019). A survey of vulnerabilities in computer systems. Journal of Information Security and Applications, 47, 14-27. [En línea]: https://doi.org/10.1016/j.jisa.2019.02.008
[7] Penetration testing (pentesting). (2021, October 14). IBM. Retrieved from https://www.ibm.com/topics/penetration-testing

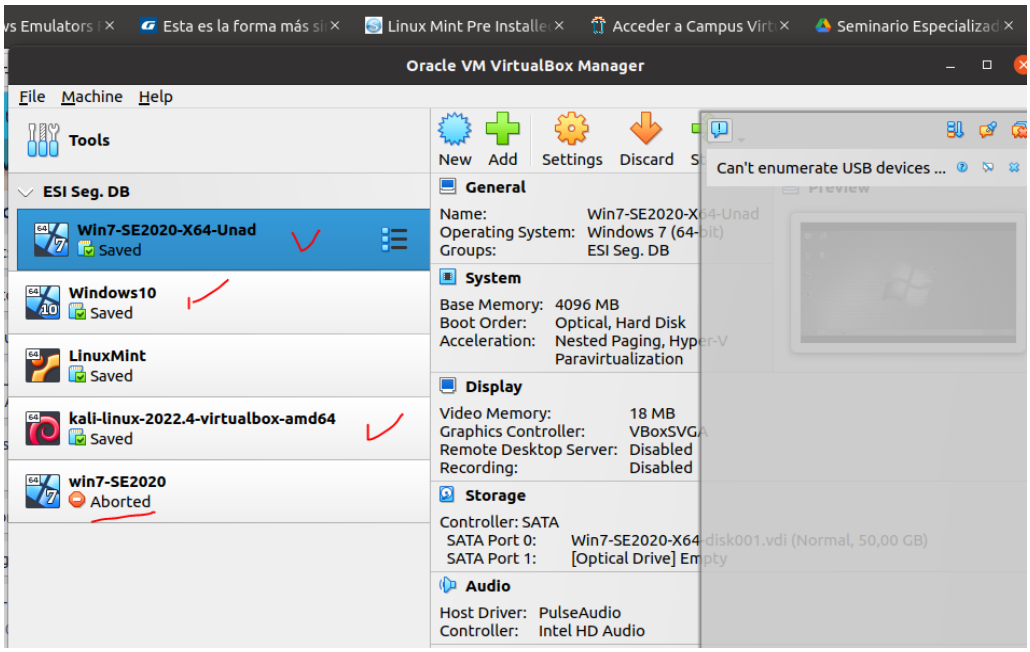
- **Security Mapping:** Se refiere al proceso de identificar y mapear todos los componentes de un sistema o red y cómo interactúan entre sí. El objetivo de la Security Mapping es comprender completamente la arquitectura y la topología de la red o sistema a evaluar, de modo que se pueda identificar y evaluar de manera efectiva las vulnerabilidades y debilidades de seguridad.
- **Risk Assessment Value:** Se refiere al valor asignado a una vulnerabilidad en función de su probabilidad de ocurrencia y su impacto en la organización. Este valor se utiliza para determinar la prioridad de las vulnerabilidades y para asignar recursos para su mitigación.
- **Reporting**: Se refiere al proceso de documentar y comunicar los resultados de una evaluación de seguridad. Esto incluye la elaboración de informes detallados sobre las vulnerabilidades identificadas, los riesgos asociados y las recomendaciones de mitigación correspondientes.
- **Phishing**: se refiere a un tipo de ataque en el que un atacante intenta engañar a una persona para que revele información confidencial como contraseñas, números de tarjeta de crédito o datos personales[8].
- **Exploit**: se refiere a un código o técnica que se utiliza para aprovechar una vulnerabilidad en un sistema o aplicación[9].
- **Botnet**: se refiere a una red de computadoras comprometidas por un atacante para realizar actividades maliciosas[10].
- **Metasploit**: Es una herramienta de pruebas de penetración de código abierto utilizada por profesionales de la seguridad para identificar y explotar vulnerabilidades en sistemas informáticos[11].

[8] Alshammari, M. R., & Dafalla, S. A. (2020). Detection and prevention of phishing attacks: A systematic review. Journal of Network and Computer Applications, 159, 102655. [En línea]: https://doi.org/10.1016/j.jnca.2020.102655
[9] Aftab, M., & Shaikh, F. K. (2021). Exploit prediction using machine learning. Journal of Information Security and Applications, 60, 102770. [En línea]: https://doi.org/10.1016/j.jisa.2021.102770
[10] Khattak, H. A., Khan, M. A., & Jadoon, M. A. (2018). A comprehensive survey of botnet: Concepts, activities and countermeasures. Future Generation Computer Systems, 82, 421-441. [En línea]: https://doi.org/10.1016/j.future.2017.12.011
[11] Offensive Security. (s.f.). Metasploit Unleashed. Recuperado el 5 de abril de 2023, de https://www.offensive-security.com/metasploit-unleashed/

- **Openvas**: Es un escáner de vulnerabilidades de código abierto que se utiliza para detectar vulnerabilidades en sistemas y aplicaciones[12]..

Para poder adecuar satisfactoriamente estas herramientas los equipos de trabajo pueden crear entornos virtuales (máquinas virtuales) como lo realizamos en la etapa 2 que veremos a continuación:

Figura 1. Máquinas Virtuales VIRTUALBOX



Fuente: El Autor

B. Etapa 2: Actuación ética y legal:

Es muy importante tener claro cuáles son las acciones de los equipos Red Team & Blue Team de una organización sobre todo el scope en el marco de los criterios éticos y legales.

[12] Greenbone Networks GmbH. (2019). OpenVAS - Open Vulnerability Assessment System. Recuperado el 1 de abril de 2023, de https://www.openvas.org/

En Colombia, existen varias normas de ciberseguridad, entre ellas se destacan:

- **La Ley 1266 de 2008:** Establece el régimen de Habeas Data en Colombia y tiene como objetivo garantizar la protección de los datos personales de las personas[13].

- **Ley 527 de 1999:** Regula el uso de mensajes de datos y firmas digitales. Obliga a las empresas a garantizar la autenticidad, integridad y confidencialidad de los mensajes de datos que se envían por medios electrónicos[14].

- **Ley 1273 de 2009**: Establece los delitos informáticos y sus sanciones. Establece penas de prisión para las personas que realicen actividades ilegales a través de medios electrónicos[15].

- **Decreto 1078 de 2015**: Regula la seguridad de la información en el sector público. Obliga a las entidades del Estado a implementar medidas de seguridad para proteger la información que manejan[16].

Por citar un ejemplo, si una empresa que realiza malos protocolos, culpa a sus empleados, los explota y expone información sensible, esta empresa estaría incumpliendo con las normas de ciberseguridad antes mencionadas. En primer lugar, estaría violando la Ley 527 de 1999, al no garantizar la confidencialidad de la información que maneja. Además, estaría incumpliendo la Ley 1273 de 2009, al

[13] Congreso de la República de Colombia. (2008). Ley 1266 de 2008. Recuperado de https://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
[14] Congreso de la República de Colombia. (1999). Ley 527 de 1999, Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5376
[15] Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Recuperado de https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[16] Presidencia de la República de Colombia. (2015). Decreto 1078 de 2015. Recuperado de https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201078%20DEL%2026%20DE%20MAYO%20DE%202015.pdf

exponer información sensible y explotar a sus empleados. Finalmente, estaría vulnerando el Decreto 1078 de 2015, al no implementar medidas de seguridad para proteger la información que maneja. Como resultado, la empresa podría enfrentar sanciones y multas por parte de las autoridades competentes en materia de ciberseguridad.

Otro escenario muy importante consiste en la realización de **actividades de red team o blue team sin el consentimiento requerido** puede ser considerado como una violación de la privacidad y seguridad de la organización objetivo, y **puede llevar a responsabilidades legales y sanciones**.

En Colombia, la normatividad que regula esta situación es la **Ley 1273 de 2009,** que establece los delitos informáticos y las sanciones correspondientes. En particular, el **artículo 269A** del Código Penal colombiano establece la prohibición de acceder a sistemas informáticos, bases de datos o redes de computadores sin autorización o excediendo la autorización dada. En este sentido, cualquier actividad realizada sin el consentimiento previo de la organización podría ser considerada como un delito informático[17].

Además, el Marco Normativo para la Seguridad y Privacidad de la Información (Resolución 20002688 de 2019) establece que todas las actividades de seguridad informática deben ser realizadas bajo un marco legal y regulatorio, y con el debido consentimiento de los propietarios de la información. En caso contrario, se podrían enfrentar a sanciones por parte de la Superintendencia de Industria y Comercio[18].

[17] Ley 1273 de 2009, recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=38729
[18] Resolución 20002688 de 2019 recuperado de https://www.mintic.gov.co/portal/604/articles-13497_documento.pdf

C. Etapa 3: Ejecución pruebas de intrusión:

Se debe demostrar las vulnerabilidades de un sistema informático a partir del uso de metodologías y técnicas de intrusión, la ejecución de pruebas de intrusión es un proceso proactivo en el que un equipo de seguridad intenta descubrir y explotar vulnerabilidades en un sistema o red para **evaluar su seguridad.** El objetivo de las pruebas de intrusión es identificar las debilidades antes de que un atacante real las encuentre y explote.

Para realizar pruebas de intrusión, se utilizan una variedad de herramientas y técnicas, incluyendo el **escaneo de puertos**, la **enumeración de servicios**, **la explotación de vulnerabilidades**, la **escalada de privilegios** y la **obtención de acceso remoto**. Las pruebas de intrusión también pueden involucrar **la ingeniería social,** que implica manipular a los usuarios para que revelen información confidencial o tomen acciones que comprometan la seguridad[19].

Nuevamente es importante destacar que las pruebas de intrusión deben ser realizadas por profesionales capacitados y éticos, ya que pueden involucrar actividades que pueden ser ilegales si se realizan sin el consentimiento del propietario del sistema o red[20].

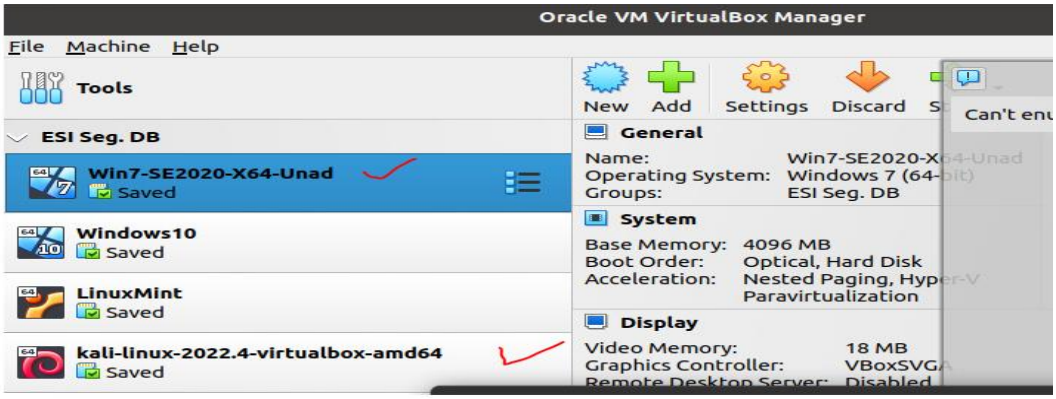
La ejecución de una prueba de intrusión típicamente sigue los **siguientes pasos[21]:**

- **Recopilación de información**: se recopila información sobre el sistema o aplicación que se va a probar, como la dirección IP, los servicios que se ejecutan y las tecnologías utilizadas. Para esto se lleva a cabo la preparación de las

[19] Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press. ISBN 978-1-59327-564-8.
[20] Kim, P. (2018). The Hacker Playbook 3: Practical Guide To Penetration Testing. Independently published. ISBN 978-1980901756.
[21] Beale, J. (2015). Penetration Testing: Procedures & Methodologies. CreateSpace Independent Publishing Platform. ISBN 978-1511901247.

herramientas en primera instancia para el ejercicio realizado se utilizaron máquinas virtuales.

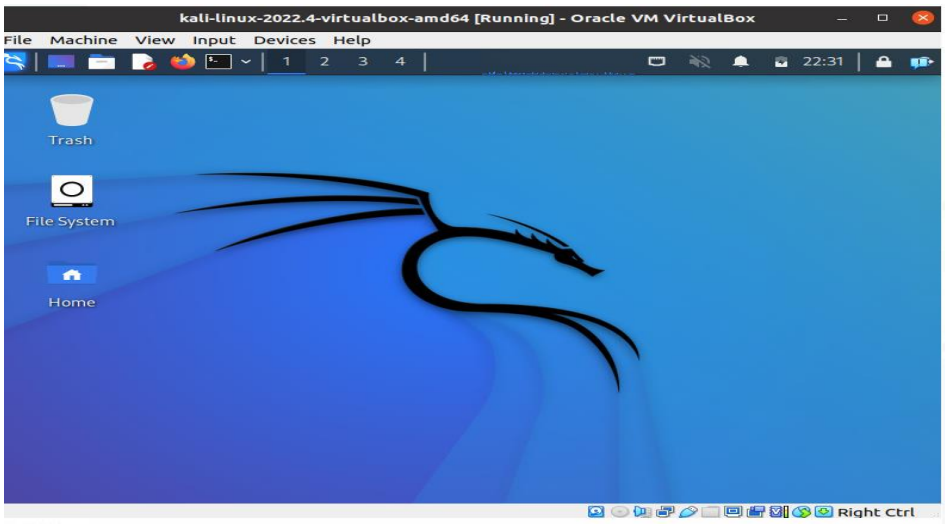
Figura 2. Máquinas virtuales VIRTUALBOX



Fuente: El Autor

- ✓ **Análisis de vulnerabilidades*:*** se utiliza un escáner de vulnerabilidades para identificar posibles vulnerabilidades en el sistema o aplicación, el escáner utilizado fue parte del kit de herramientas de Kali Linux. (nmap)

Figura 3. Máquinas virtuales KALI LINUX

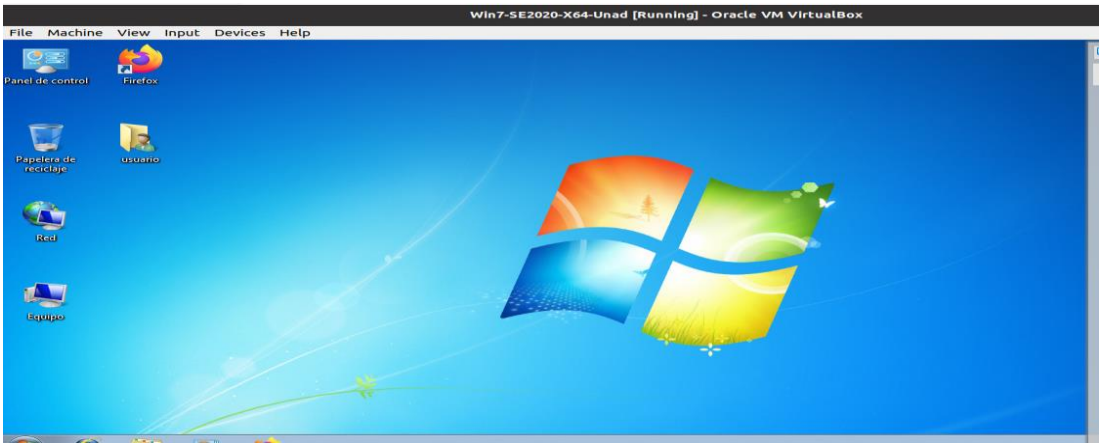


Fuente: El Autor

- **Explotación de vulnerabilidades**: se intenta explotar las vulnerabilidades encontradas para obtener acceso al sistema o aplicación. El ejercicio realizado se

llevó a cabo la explotación de brecha sobre el sistema operativo Windows 7 aplicación, rejetto v. 2.3

Figura 4. Máquinas virtuales WINDOWS 7



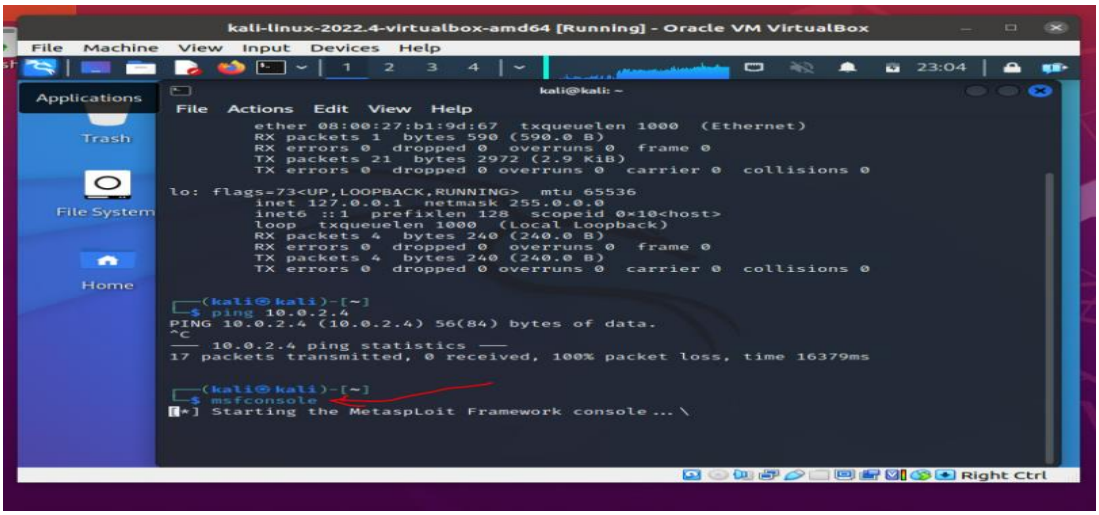
Fuente: El Autor

- **Escalamiento de privilegios*:*** una vez que se ha obtenido acceso, se intenta escalar los privilegios para obtener un mayor nivel de control sobre el sistema. Actividad realizada con la herramienta Metasploit.

  Se dio inicio a la consola de METASPLOIT a través del comando

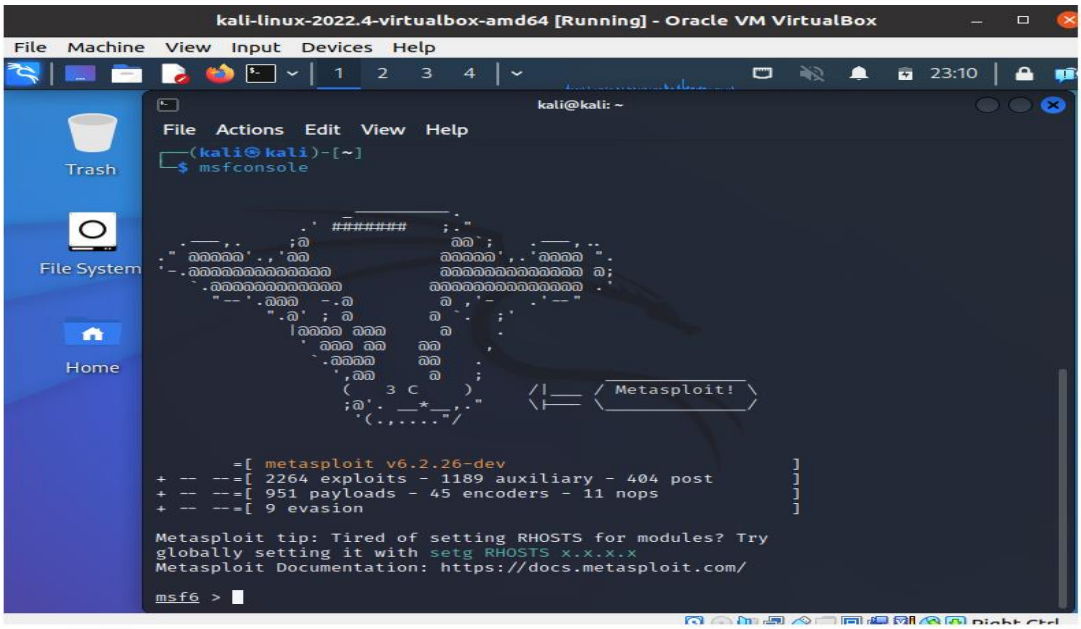
  MSFCONSOLE tal como se puede apreciar en las imágenes siguientes se inicia la consola:

Figura 5. Máquina virtual KALI LINUX – METASPLOIT



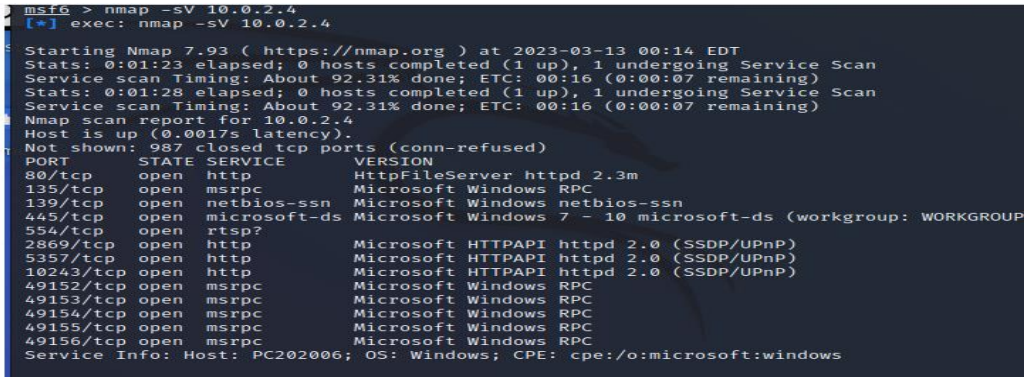
Fuente: El Autor

Figura 6. Máquina virtual KALI LINUX - METASPLOIT



Fuente: El Autor

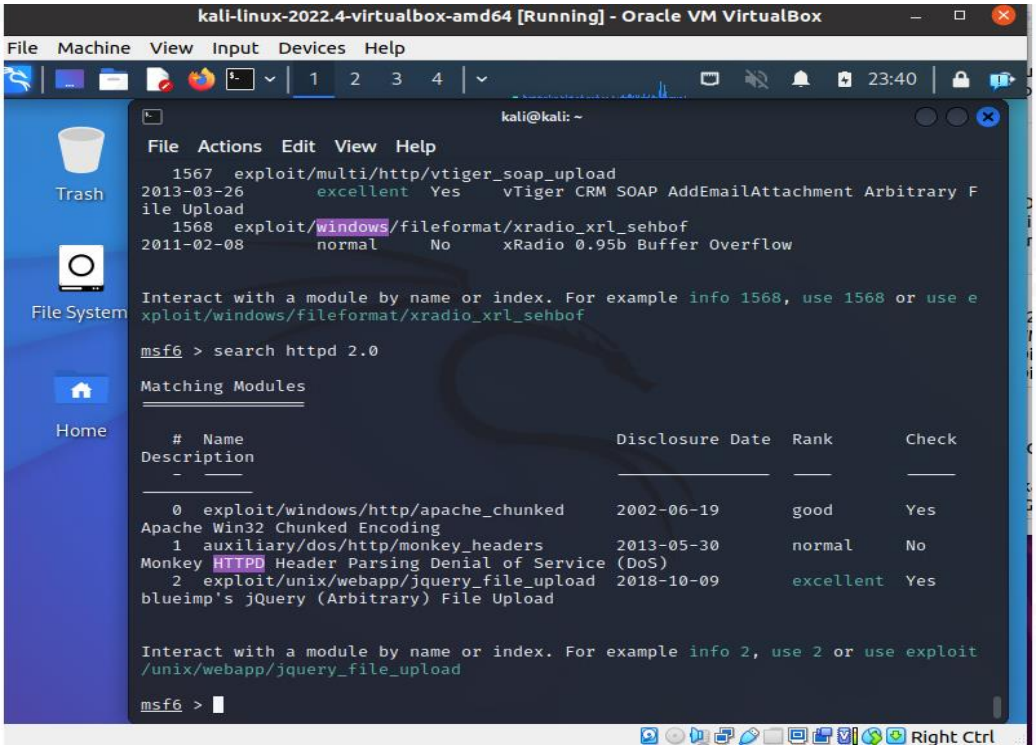
Figura 7. Máquina virtual KALI LINUX – METASPLOIT



Fuente: El Autor

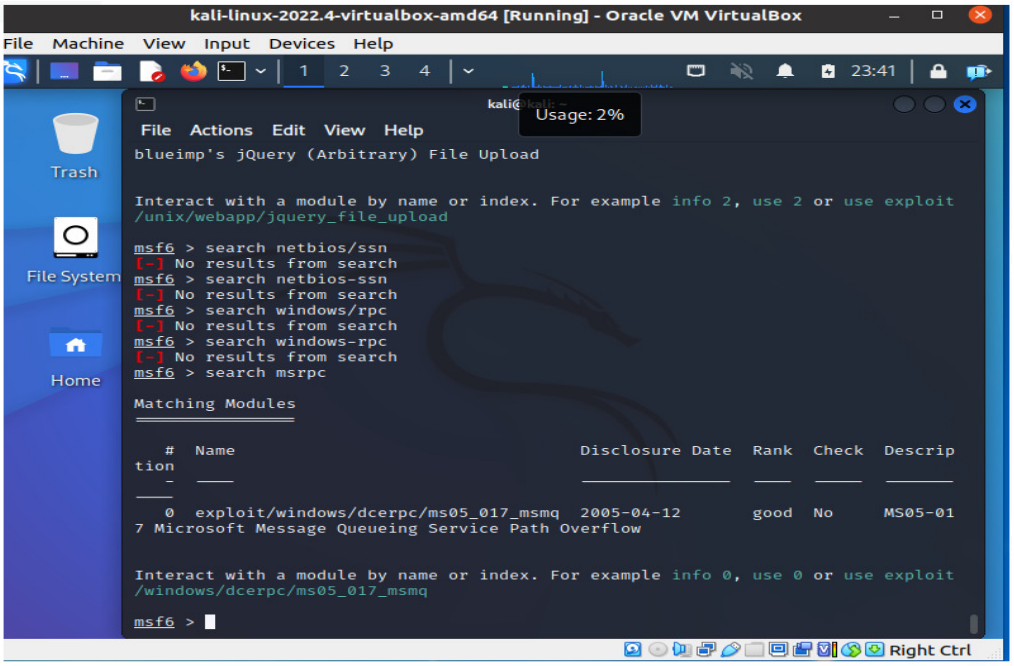
- **Mantenimiento del acceso**: se realizan esfuerzos para mantener el acceso al sistema o aplicación comprometida.

Figura 8. Máquina virtual KALI LINUX – METASPLOIT



Fuente: El Autor

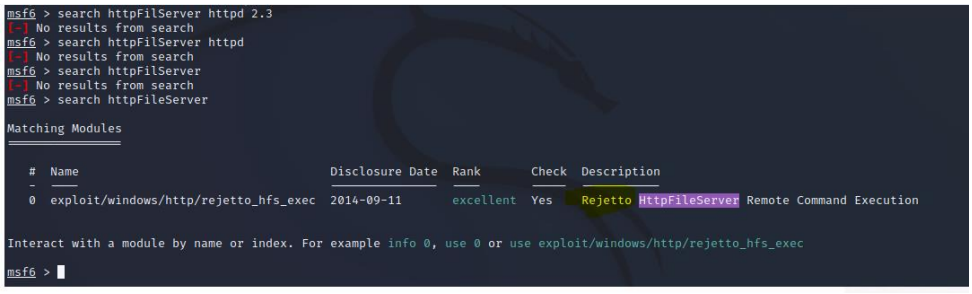
Figura 9. Máquina virtual KALI LINUX – METASPLOIT



Fuente: El Autor

- **Lanzamiento del exploit**: se realiza la ejecución del exploit

Figura 10. Máquina virtual KALI LINUX - METASPLOIT



Fuente: El Autor

- **Generación de informe**: se documenta el proceso y los hallazgos en un informe de prueba de intrusión.

La ejecución de una prueba de intrusión es un proceso complejo que requiere un ***enfoque sistemático y bien estructurado***. Los pasos típicos son los mencionados previamente e incluyen la recopilación de información, el análisis de vulnerabilidades, la explotación de vulnerabilidades, el escalamiento de privilegios, el mantenimiento del acceso y la generación de informes. **La planificación cuidadosa** y la selección adecuada de herramientas son fundamentales para garantizar la efectividad de las pruebas de intrusión y evitar impactos negativos en los sistemas o aplicaciones probados. Además, es importante que se realicen las pruebas de acuerdo con estándares reconocidos, como los proporcionados por el **OMSSTT** y el **OWASP** Testing Guide, y que se documenten cuidadosamente los hallazgos y las recomendaciones para ayudar a los equipos de seguridad a mejorar la postura de seguridad de sus sistemas y aplicaciones.

D. Etapa 4: Contención de ataques informático

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI es una cualidad que debe desarrollar todo profesional de seguridad de la información, La contención de ataques informáticos es una estrategia para ***limitar el impacto de un ataque informático*** y ***prevenir su propagación***. A continuación, se presentan los pasos típicos y los equipos que interactúan en la contención de ataques:

- **Identificación del ataque**: El primer paso es identificar el ataque y determinar su alcance y gravedad. Esto puede involucrar la revisión de registros de seguridad, análisis forense y otras técnicas de detección. Estado de red con comandos tan sencillos como NetStat -a. Al igual que el estado de procesos en memoria con el comando TaskList si se trata de un Windows.

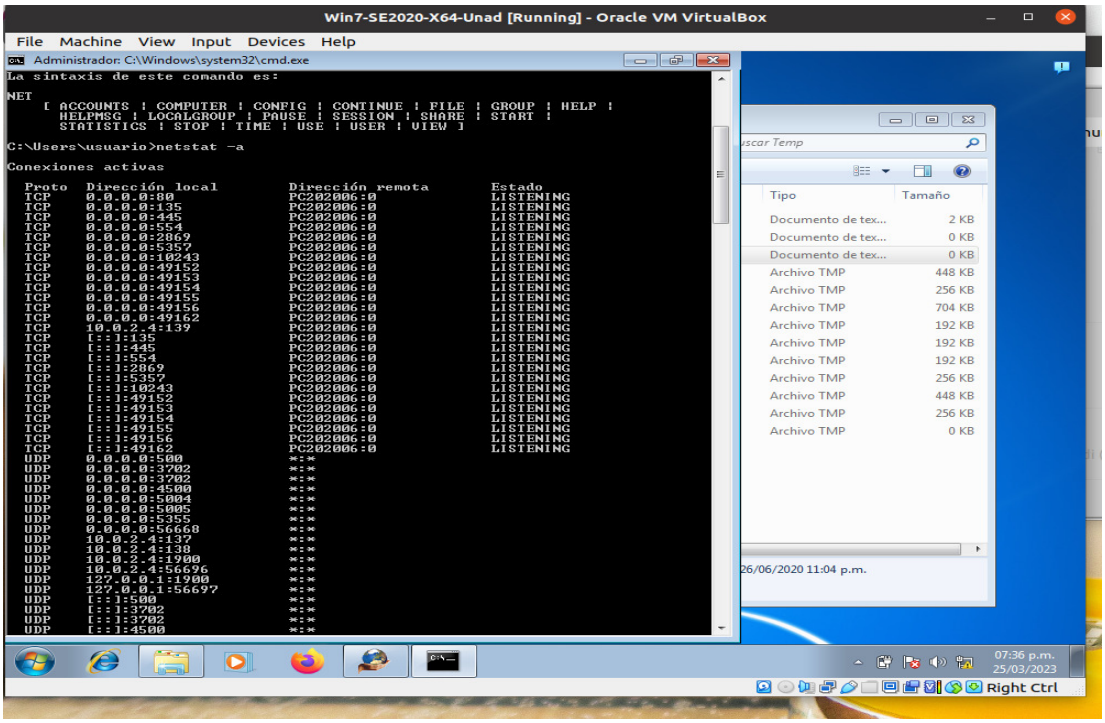
- **Aislamiento de la red:** Si el ataque está propagándose a través de la red, se puede aislar la red afectada para evitar que el ataque se propague a otras partes de la red.

- **Estado de conexiones de red:**

  ✓ Abrir la aplicación del símbolo del sistema (CMD) como administrador preferiblemente. Se puede hacer esto haciendo clic derecho en el icono de CMD y seleccionando "Ejecutar como administrador" en el menú contextual.

  ✓ Una vez que se abra el CMD, escribe el comando "netstat -a". Este comando mostrará información sobre todas las conexiones de red activas en el equipo, incluyendo el estado de la conexión, los puertos utilizados y las direcciones IP de origen y destino.

Figura 11, Máquina virtual WINDOWS 7 – Comando NetStat



Fuente: El Autor

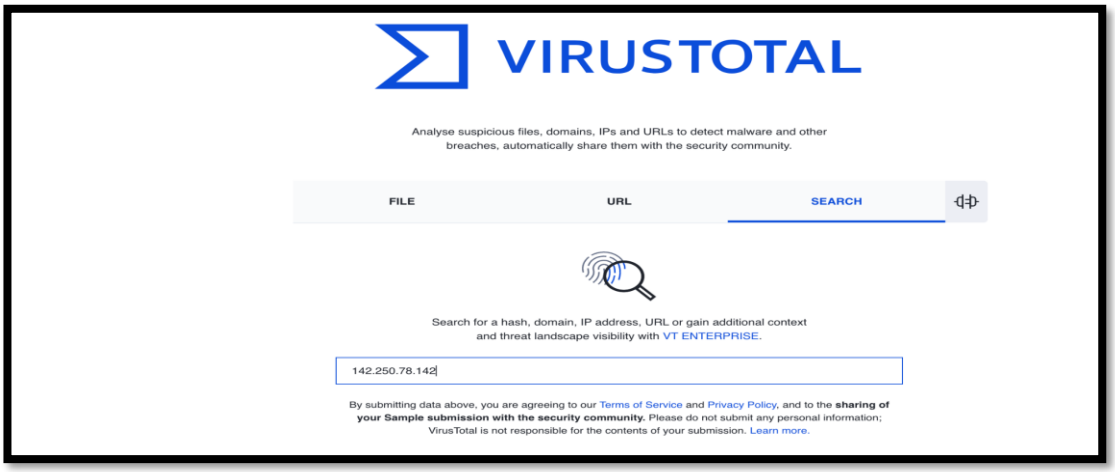
- **Conexiones entrantes no autorizadas:**

  Revisar la lista de conexiones entrantes y asegurarse de que todas sean autorizadas y correspondan a programas que estén instalados en el sistema. Si se encuentran conexiones entrantes sospechosas, es posible que se pueda rastrear el software malicioso que está causando el ataque.

- **Conexiones salientes a direcciones IP desconocidas:**

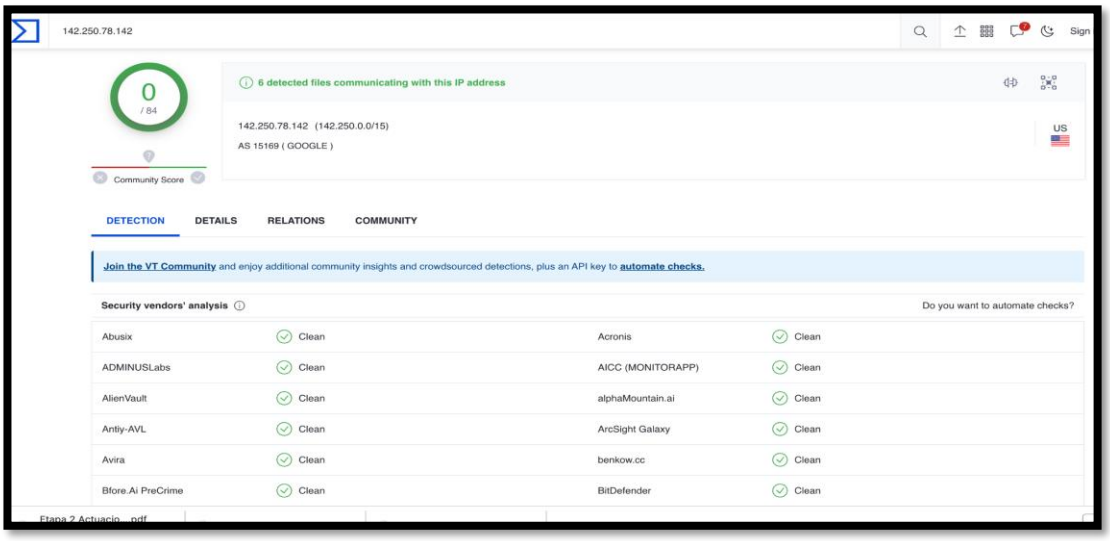
  Verificar las conexiones salientes y revisar las direcciones IP de destino (**virustotal.com**). Si se encuentran conexiones a direcciones IP desconocidas o **sospechosas**, es posible que el equipo esté siendo infectado con algún tipo de malware, para validar la seguridad de las IP con las que se está comunicando se puede realizar la consulta a la página virustotal.com ingresando a la opcion “search”, se especifica la dirección IP a consultar ver imagen 1 y el resultado en la imagen 2.

Figura 12, Plataforma WEB de consulta - virus total



Fuente: https://www.virustotal.com/gui/home/upload

Figura 13. Plataforma WEB de Consulta - virus total



Fuente: https://www.virustotal.com/gui/home/upload

Si las IP están comprometidas aparecen en color rojo y en alerta los reportes de estado de dicha IP.

- **Puertos abiertos no autorizados:**

Al comprobar los puertos abiertos en el equipo y asegurarse de que solo los necesarios están abiertos. Si se encuentran puertos abiertos no autorizados, es posible que se haya instalado el software malicioso que está siendo causal del ataque.

- **Actividad de red inusual:**

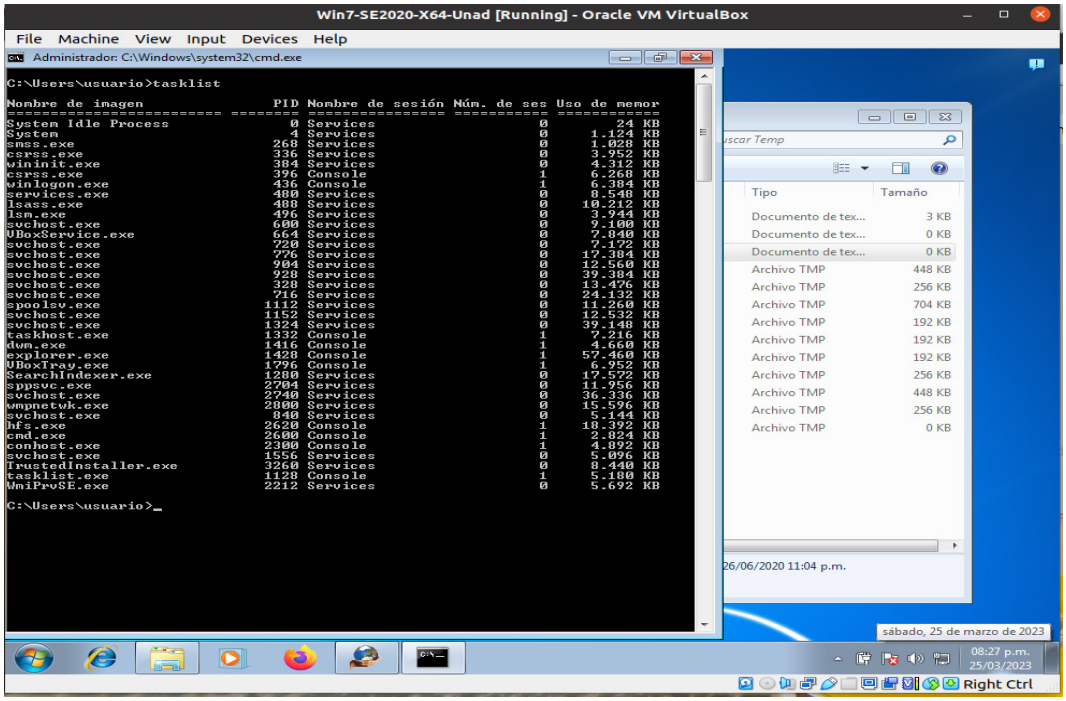
Al revisar el tráfico de red y asegurarnos de que no haya un tráfico inusual o sospechoso. Si se encuentra actividad de red inusual.

- **Estado de Memoria Volátil (Aplicar post incidente para Forense también):**

Resulta que en el proceso de atención de un incidente la memoria volátil hace parte de una de las evidencias que deben capturarse para la valoración y análisis post-incidente. Y esta debe tomarse primero antes de aplicar el “aislamiento” de la máquina sino se corre el riesgo de perder información valiosa para el análisis forense.

- ✓ Abrir la aplicación del símbolo del sistema (CMD) en el equipo.
- ✓ Escribir el comando "**tasklist**" y presionar Enter. Este comando mostrará una lista de todos los procesos en ejecución en el sistema, junto con el consumo de memoria de cada proceso.

Figura 14. Máquina virtual WINDOWS 7 – Comando TaskList



Fuente: El Autor

- ✓ Se podrá examinar la lista de procesos, buscar aquellos que estén consumiendo una cantidad **inusual de memoria**. Tener en cuenta que algunos

procesos legítimos pueden consumir mucha memoria, por lo que es importante investigar más a fondo antes de tomar medidas.

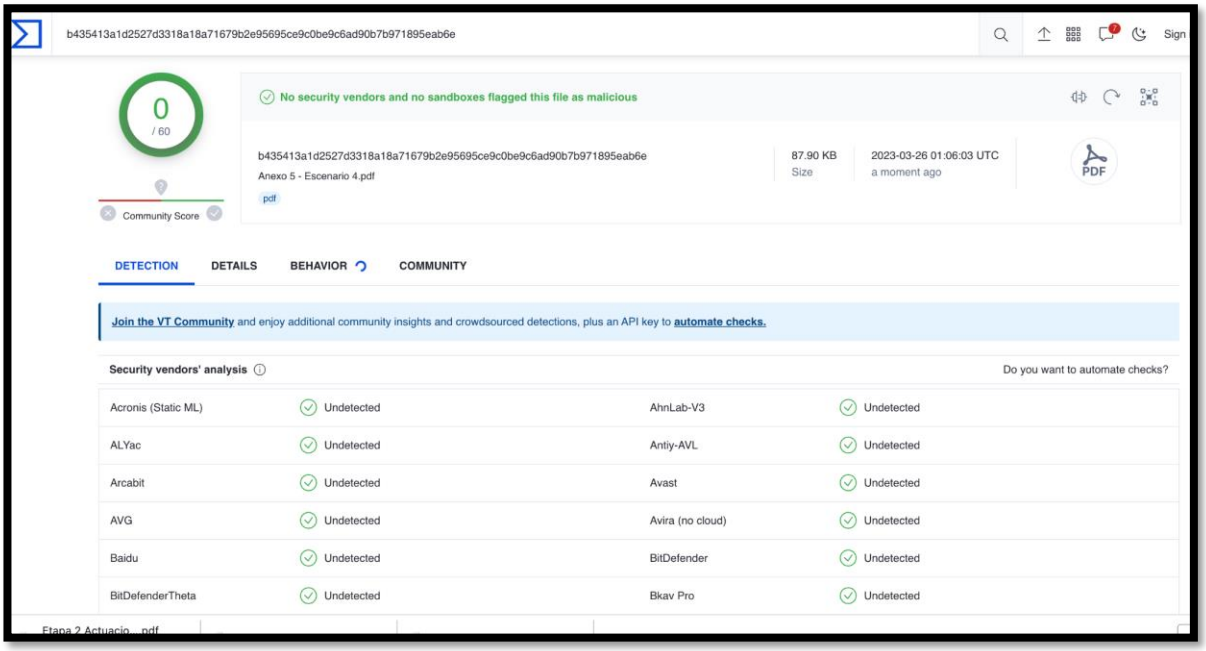
- ✓ Si se encuentra un proceso sospechoso, anotar el nombre del proceso (se encuentra en la columna "Nombre de imagen") y el ID del proceso (se encuentra en la columna "PID").

- ✓ Utilizar el comando "taskkill" para detener el proceso malicioso. Escribir el comando "taskkill /f /pid [ID del proceso]" y presionar Enter. Este comando finalizará el proceso malicioso.

- ✓ Es importante tener en cuenta que este enfoque puede no ser efectivo para todos los tipos de software malicioso. Algunos tipos de malware pueden ocultar sus procesos o utilizar nombres de proceso legítimos, lo que los hace difíciles de detectar mediante Tasklist.

- ✓ Luego de identificar el archivo malicioso se puede proceder a consultar en la web de virustotal.com, arrojará los resultados de inmediato si ya ha sido reportado desde su hash hasta ingeniería inversa del mismo.

Figura 15. Plataforma WEB de Consulta - virus total



Fuente: https://www.virustotal.com/gui/home/upload

- **Eliminación de malware**: Si el ataque implica la presencia de malware en un sistema, se puede utilizar software antivirus o herramientas de eliminación de malware para eliminar el malware de los sistemas afectados.

- **Restauración de sistemas**: Después de eliminar el malware, se deben restaurar los sistemas afectados a su estado original para que puedan volver a estar en línea.

- **Investigación del incidente**: Una vez que se haya contenido el ataque, se debe realizar una investigación completa para determinar la causa del incidente, la extensión del daño y las medidas que se pueden tomar para evitar futuros ataques.

Los equipos que interactúan en la contención de ataques incluyen equipos de seguridad informática (Red Team, Blue Team y ***equipos de respuesta a incidentes***, equipos de soporte técnico y, en algunos casos, equipos de aplicación de la ley o abogados de la empresa afectada[22].

E. Etapa 5: Socialización de informe técnico

Es fundamental que el informe sea comprensible para un público no técnico, como los gerentes y ejecutivos de la empresa, para que puedan tomar decisiones informadas sobre la asignación de recursos y la mejora de la seguridad de la información. Además, socializar un informe técnico también puede ayudar a fomentar una cultura de seguridad en la organización, donde todos los miembros comprendan la importancia de la ciberseguridad y su papel en ella.

Un informe técnico de ciberseguridad es una tarea crítica que requiere atención al detalle y una buena comprensión del público objetivo. Para presentar un informe técnico de ciberseguridad de manera exitosa, se deben seguir las siguientes pautas:

- **Conocer la audiencia:** Antes de comenzar a redactar el informe, es importante conocer al público objetivo. Si el informe se presenta a un equipo técnico, se puede incluir terminología especializada. Si el informe se presenta a un equipo

[22] CERT Coordination Center. (2016). Incident Management for Information Security. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485134

no técnico, se debe evitar el uso de jerga técnica y explicar los términos complejos en lenguaje sencillo.

- **Ser claro y conciso:** El informe debe ser claro, conciso y fácil de entender. No se debe llenar el informe con información innecesaria o redundante. Se deben incluir solo los detalles relevantes para el objetivo del informe.

- **Estructurar el informe de manera lógica:** El informe debe seguir una estructura lógica y fácil de seguir. Se recomienda incluir un resumen ejecutivo al comienzo del informe, seguido de una introducción, un cuerpo principal y una conclusión. El cuerpo principal debe ser organizado en secciones temáticas claras.

- **Incluir detalles técnicos**: El informe debe incluir detalles técnicos, como los sistemas y aplicaciones afectados, ***los vectores de ataque*** y las ***medidas de seguridad recomendadas***. Se debe presentar la información técnica de manera clara y accesible para el público objetivo.

- **Proporcionar recomendaciones prácticas:** El informe debe incluir recomendaciones prácticas para mejorar la seguridad de la empresa. Estas recomendaciones deben ser ***fáciles de implementar y realistas*** en términos de costo y recursos.

- **Utilizar gráficos y tablas:** El uso de gráficos y tablas puede ayudar a resumir la información compleja de manera clara y concisa. Los gráficos y tablas también pueden ayudar a destacar las tendencias y patrones importantes en los datos.

- **Revisar y editar el informe:** Antes de presentar el informe, es importante revisar y editar el documento para asegurarse de que sea claro, conciso y preciso.

2. CONCLUSIONES

Después de haber consultado diversos textos y normativas relacionadas con la ciberseguridad en Colombia, podemos concluir que la realización de ***pruebas de seguridad es una actividad esencial para garantizar la integridad y confidencialidad de la información en una organizació***n. Sin embargo, estas actividades deben ser llevadas a cabo dentro del marco legal y normativo establecido por el país para evitar sanciones y problemas legales.

Es importante que los equipos de Red Team y Blue Team tengan en cuenta que sus actividades deben ser autorizadas previamente y llevarse a cabo de manera ética y responsable. Es fundamental que se respeten los derechos de los empleados y que no se exponga información sensible o privada durante el proceso.

En cuanto a las pruebas de penetración, es necesario contar con conocimientos técnicos avanzados y utilizar herramientas adecuadas para poder realizarlas de manera efectiva. Además, es importante tener en cuenta que estas pruebas pueden generar un impacto en la infraestructura y sistemas de la organización, por lo que se debe contar con medidas de contención en caso de un ataque informático.

Frente a los resultados de las pruebas de seguridad, ***es importante ser claro y preciso en la información presentada*** para que los responsables de la ***toma de decisiones puedan entender la gravedad*** de las vulnerabilidades encontradas y tomar las medidas necesarias para corregirlas.

En conclusión, la ciberseguridad es una preocupación cada vez más importante en nuestra sociedad y es ***fundamental contar con medidas adecuadas para proteger la información y los sistemas de las organizaciones***. La realización de pruebas de

seguridad es una herramienta valiosa para identificar las debilidades y tomar medidas preventivas y correctivas. Sin embargo, estas actividades deben ser realizadas dentro del marco legal y normativo establecido para evitar problemas legales.

3. RECOMENDACIONES

- Es fundamental que los equipos de red team y blue team realicen sus actividades siempre con el ***consentimiento y la autorización previa*** del dueño del sistema, aplicación o red que se va a evaluar. El incumplimiento de esta norma puede ser sancionado por la ley colombiana.
- Para ***realizar pruebas de penetración***, es necesario conocer claramente los ***conceptos y las metodologías*** utilizadas. Se recomienda familiarizarse con herramientas como Metasploit, OpenVAS y otras que pueden ser útiles para llevar a cabo estas actividades.
- Es importante ***tener en cuenta la normativa colombiana relacionada con la seguridad informática*****,** como la Ley 1273 de 2009 y el Decreto 1078 de 2015. Estas leyes establecen las sanciones y penas para aquellos que violen la seguridad de los sistemas de información.
- Para contener un ataque informático, es necesario contar con un ***plan de contingencia y un equipo de respuesta a incidentes***. Este equipo debe estar capacitado para actuar de manera rápida y efectiva en caso de una violación de seguridad.
- Es importante que la ***presentación de los resultados de las pruebas de seguridad sea clara*****,** concisa y entendible para aquellos que no son expertos en el tema. Se recomienda seguir las pautas establecidas en el OSSTMM para la presentación de informes de pruebas de seguridad.
- ***Establecer un equipo red team y blue team dentro de la empresa*** para llevar a cabo pruebas de penetración y fortalecer las medidas de seguridad.

- ***Conocer y cumplir con la normativa colombiana en cuanto a seguridad informática***, para evitar sanciones y proteger la información de la empresa y sus clientes.
- ***Garantizar que los empleados de la empresa estén capacitados en seguridad*** informática y sepan cómo actuar en caso de un ataque informático.
- ***Implementar medidas de seguridad adecuadas, como firewalls, antivirus*** y autenticación de dos factores, para proteger la red y los sistemas de la empresa.
- ***Realizar pruebas de penetración regulares*** para detectar posibles vulnerabilidades en la red y los sistemas, y corregirlas antes de que sean explotadas por atacantes.
- ***Presentar los resultados de las pruebas de seguridad de manera clara y entendible*** para que la dirección de la empresa pueda tomar decisiones informadas en cuanto a la seguridad informática.

Estos objetivos ayudarán a la empresa a mejorar su seguridad informática, proteger su información y la de sus clientes, y evitar sanciones por no cumplir con la normativa colombiana en cuanto a seguridad informática. Además, permitirán a la empresa detectar y corregir posibles vulnerabilidades antes de que sean explotadas por atacantes.

- **ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM *&* BLUETEAM**.

  Para el desarrollo de estrategias de RedTeam y BlueTeam es necesario considerar varios aspectos que aporten a la eficacia de estas prácticas. Algunos de los aspectos clave son:

  1. **Conocimiento detallado del entorno:** Tanto el equipo RedTeam como el BlueTeam necesitan tener un conocimiento profundo del entorno en el que se llevarán a cabo las pruebas. Esto incluye el hardware y software utilizado, la

arquitectura de red, la infraestructura y cualquier otro aspecto relevante que pueda afectar la seguridad.

2. **Comunicación efectiva**: Es importante que ambos equipos se comuniquen de manera efectiva para garantizar que la información se comparta de manera oportuna y se puedan tomar las decisiones adecuadas en el momento adecuado.

3. **Conocimiento de técnicas de ataque y defensa**: El equipo RedTeam debe tener un conocimiento detallado de las técnicas de ataque que se utilizan comúnmente en el mundo del hacking, mientras que el BlueTeam debe conocer las mejores prácticas y técnicas de defensa para contrarrestar dichos ataques.

4. **Herramientas adecuadas**: Tanto el RedTeam como el BlueTeam deben contar con herramientas adecuadas para realizar sus tareas. Esto puede incluir herramientas de hacking y pentesting para el RedTeam, y herramientas de monitoreo y detección de amenazas para el BlueTeam.

5. **Planificación y ejecución adecuada**: Ambos equipos deben tener un plan claro y detallado antes de comenzar las pruebas. Esto incluye establecer objetivos claros y definir los roles y responsabilidades de cada miembro del equipo.

6. **Evaluación y mejora continua:** Después de cada prueba, es importante que ambos equipos evalúen su desempeño y busquen oportunidades para mejorar en futuras pruebas.

7. C**apacitación y actualización constante:** Los miembros del RedTeam y BlueTeam deben mantenerse actualizados en las últimas técnicas y herramientas de hacking y defensa, y deben recibir capacitación regular para mejorar su habilidad en la materia.

- **RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN**

1) **Identificar los activos críticos:** Identificar los activos críticos de la organización y determinar qué amenazas pueden afectarlos es fundamental para poder establecer medidas de seguridad efectivas.
2) **Establecer políticas de seguridad:** Se deben definir políticas de seguridad claras y bien definidas que aborden los aspectos críticos de la seguridad, tales como el acceso a los sistemas, el uso de contraseñas y la gestión de parches.

3) **Realizar una evaluación de riesgos:** Evaluar los riesgos de la organización y establecer medidas de seguridad para mitigarlos es clave para poder proteger los activos críticos.

4) **Implementar controles de acceso**: Los controles de acceso, tales como la autenticación multifactor, son esenciales para proteger los sistemas y datos de la organización de accesos no autorizados.

5) **Implementar la gestión de parches**: La gestión de parches es crítica para mantener los sistemas de la organización actualizados y protegidos de las vulnerabilidades conocidas.

6) **Capacitar al personal:** Capacitar al personal en cuanto a las prácticas de seguridad es esencial para que los empleados comprendan su papel en la seguridad de la organización y puedan ayudar a proteger los activos críticos.

7) **Implementar la monitorización y el análisis de amenazas (SIEM):** La monitorización y el análisis de amenazas son esenciales para detectar y responder rápidamente a los ataques.

8) **Realizar pruebas de penetración (RED TEAM):** Las pruebas de penetración son una herramienta efectiva para evaluar la efectividad de las medidas de seguridad de la organización y detectar posibles brechas.

9) **Establecer un plan de contingencia**: Un plan de contingencia bien establecido y probado es esencial para que la organización pueda responder rápidamente a un incidente de seguridad.

10) **Realizar auditorías periódicas:** Las auditorías periódicas son esenciales para evaluar la efectividad de las medidas de seguridad de la organización y detectar posibles brechas.

- **CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.**

La ciberseguridad es un tema crítico en la actualidad, ya que las amenazas cibernéticas son cada vez más sofisticadas y frecuentes. Para proteger a las organizaciones de estas amenazas, es fundamental contar con estrategias efectivas de RedTeam y BlueTeam, así como con medidas de seguridad sólidas y bien definidas.

La construcción del conocimiento en el enfoque de la ciberseguridad se basa en la comprensión detallada de las amenazas y vulnerabilidades, así como en la identificación de los activos críticos de la organización y la implementación de medidas de seguridad efectivas para protegerlos. También es fundamental contar con un equipo de profesionales capacitados y actualizados en las últimas técnicas y herramientas de seguridad.

La evaluación continua de las medidas de seguridad de la organización es esencial para detectar posibles brechas y tomar medidas para mejorar la seguridad. La monitorización y el análisis de amenazas, así como las pruebas de penetración, también son herramientas críticas para evaluar la efectividad de las medidas de seguridad y detectar posibles brechas.

En conclusión, la ciberseguridad es un tema crítico para las organizaciones en la actualidad, y requiere de estrategias efectivas, medidas de seguridad sólidas y bien definidas, así como de un equipo capacitado y actualizado en las últimas técnicas y herramientas de seguridad. La construcción del conocimiento en este enfoque es

esencial para proteger los activos críticos de la organización y responder de manera efectiva a las amenazas cibernéticas.

Además de las estrategias y medidas de seguridad mencionadas, es importante tener en cuenta la normatividad de ciberseguridad en Colombia para garantizar el cumplimiento legal en materia de seguridad de la información. Algunas de las normas más relevantes en este ámbito son:

Ley 1266 de 2008: Esta ley establece el régimen general de protección de datos personales en Colombia y establece las obligaciones y responsabilidades de los titulares de la información y los encargados de su tratamiento.

Decreto 620 de 2020: Este decreto establece las reglas para la protección de la información personal y confidencial en la administración pública colombiana, así como los procedimientos para la notificación de incidentes de seguridad.

Ley 1341 de 2009: Esta ley establece las bases para la implementación de la política pública de tecnologías de la información y las comunicaciones en Colombia.

Resolución 2646 de 2008: Esta resolución establece las medidas mínimas de seguridad que deben implementar las entidades que tratan información personal y confidencial en Colombia.

Decreto 1335 de 2012: Este decreto establece las medidas para la protección de la información personal y confidencial de los usuarios de servicios de comunicaciones en Colombia.

Resolución 1577 de 2019: Esta resolución establece los requisitos técnicos mínimos para la implementación de medidas de seguridad en las entidades que tratan información personal y confidencial en Colombia.

Es importante tener en cuenta que el incumplimiento de estas normas puede llevar a sanciones y multas por parte de las autoridades correspondientes. Por lo tanto,

es fundamental para las organizaciones colombianas tener en cuenta la normatividad de ciberseguridad al planificar e implementar sus estrategias y medidas de seguridad.

B. SUSTENTA EL DESARROLLO DE SEMINARIO ESPECIALIZADO MEDIANTE VIDEO DONDE SE PUEDA EVIDENCIAR ROSTRO DEL ESTUDIANTE CON UNA DURACIÓN MÍNIMA DE 8 MINUTOS, EL ESTUDIANTE DEBERÁ HACER PÚBLICO EL VÍDEO HACIENDO USO DE ALGUNA PLATAFORMA CLOUD O EN YOUTUBE.

Link YouTube: https://youtu.be/epJHSkHApGY

BIBLIOGRAFÍA

- ISECOM. (2008). Open Source Security Testing Methodology Manual (OSSTMM) Version 3.0. retrieve from https://www.isecom.org/OSSTMM.3.pdf

- Penetration testing (pentesting). (2021, October 14). IBM. recuperado de https://www.ibm.com/topics/penetration-testing

- Shahzad, F., Aslam, W., & Saleem, S. (2019). A survey of vulnerabilities in computer systems. Journal of Information Security and Applications, 47, 14-27. [En línea]: https://doi.org/10.1016/j.jisa.2019.02.008

- Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

- Congreso de la República de Colombia. (1999). Ley 527 de 1999, Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5376

- Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Recuperado de https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- Presidencia de la República de Colombia. (2015). Decreto 1078 de 2015. Recuperado de https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201078%20DEL%2026%20DE%20MAYO%20DE%202015.pdf

- Offensive Security. (s.f.). Metasploit Unleashed. Recuperado el 5 de abril de 2023, de https://www.offensive-security.com/metasploit-unleashed/

- Aftab, M., & Shaikh, F. K. (2021). Exploit prediction using machine learning. Journal of Information Security and Applications, 60, 102770. [En línea]: https://doi.org/10.1016/j.jisa.2021.102770

- Khattak, H. A., Khan, M. A., & Jadoon, M. A. (2018). A comprehensive survey of botnet: Concepts, activities and countermeasures. Future Generation Computer Systems, 82, 421-441. [En línea]: https://doi.org/10.1016/j.future.2017.12.011

- Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

- Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

- OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

- Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. https://repository.unad.edu.co/handle/10596/35497

- Alshammari, M. R., & Dafalla, S. A. (2020). Detection and prevention of phishing attacks: A systematic review. Journal of Network and Computer Applications, 159, 102655. [En línea]: https://doi.org/10.1016/j.jnca.2020.102655

- Gupta, A., & Singh, N. (2018). Scanning Techniques in Network Security. International Journal of Computer Applications, 180(29), 47-53. [En línea]: https://www.ijcaonline.org/archives/volume180/number29/29845-2018919082

- CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

- Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35). https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

- Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57). https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

- Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

- 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). 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). 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). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

- "Red Team vs. Blue Team: Understanding the Difference" de Dark Reading:(2016) https://www.darkreading.com/attacks-breaches/red-team-vs-blue-team-understanding-the-difference/a/d-id/1327207

- Beale, J. (2015). Penetration Testing: Procedures & Methodologies. CreateSpace Independent Publishing Platform. ISBN 978-1511901247.

- CERT Coordination Center. (2016). Incident Management for Information retrieve from Security. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485134

- National Institute of Standards and Technology (NIST). (2018). Computer Security Incident Handling Guide. retrieve from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- United States Computer Emergency Readiness Team (US-CERT). (2015). Incident Handling Process., retrieve from https://www.us-cert.gov/sites/default/files/publications/incident_handling.pdf