1. **Elección del tema y justificación**:
   * Comienza identificando por qué el análisis de vulnerabilidades y los honeypots son importantes para la administración de sistemas y redes.
   * Explica cómo este proyecto contribuirá al campo y por qué es relevante.
2. **Revisión de la literatura**:
   * Investiga la teoría y las investigaciones existentes sobre análisis de vulnerabilidades y honeypots. Esto te ayudará a definir el marco teórico y contextualizar tu proyecto.
3. **Definición de objetivos**:
   * Establece claramente los objetivos de tu TFG. Pueden incluir cosas como:
     + Diseñar y configurar un honeypot virtualizado.
     + Analizar vulnerabilidades específicas en el tráfico capturado por el honeypot.
     + Evaluar la eficacia del honeypot en la detección de amenazas.
4. **Selección de herramientas y tecnologías**:
   * Elige las herramientas y tecnologías que utilizarás para crear y gestionar el honeypot. Puedes optar por soluciones de código abierto como Honeyd, Cowrie, Dionaea, o desplegar honeypots personalizados.
5. **Diseño y configuración del honeypot**:
   * Crea un diseño detallado de cómo configurarás el honeypot virtualizado. Esto incluye la selección de sistemas operativos, la topología de red, las reglas de firewall y las políticas de seguridad.
6. **Captura de tráfico y análisis de vulnerabilidades**:
   * Implementa el honeypot y comienza a capturar el tráfico. Realiza un análisis exhaustivo de las vulnerabilidades y amenazas detectadas.
7. **Evaluación de la eficacia**:
   * Evalúa qué tan eficaz es el honeypot en la detección de amenazas. Compara tus resultados con las expectativas iniciales y discute cualquier desviación.
8. **Documentación**:
   * Mantén un registro detallado de todo lo que haces, desde la configuración hasta el análisis de datos. Esto será crucial para tu TFG.
9. **Análisis y discusión de resultados**:
   * Analiza los resultados obtenidos y discute sus implicaciones. ¿El honeypot detectó amenazas con éxito? ¿Hubo desafíos inesperados?
10. **Conclusiones y recomendaciones**:

* Resume tus hallazgos en tus conclusiones y proporciona recomendaciones basadas en tus resultados.

1. **Redacción del TFG**:

* Escribe tu trabajo, asegurándote de que tenga una estructura clara con introducción, marco teórico, metodología, resultados y conclusiones.

1. **Presentación y defensa**:

* Prepara una presentación de tu TFG y prepárate para defenderlo ante un tribunal.

1. **Bibliografía y referencias**:

* Asegúrate de citar adecuadamente todas las fuentes y referencias utilizadas.

1. **Revisión y edición**:

* Revisa y edita tu TFG para corregir errores gramaticales y de formato.

1. **Entrega y presentación**:

* Entrega tu TFG de acuerdo con los requisitos de tu institución y realiza la presentación ante el tribunal.

1. **Considera la ética**:

* Asegúrate de respetar la ética y la legalidad en tu proyecto, especialmente cuando se trata de la captura de tráfico.

Recuerda que tu asesor académico o profesor guía será de gran ayuda a lo largo de este proceso. Comunica tus avances regularmente y busca su orientación cuando sea necesario. ¡Buena suerte con tu TFG!

El análisis de vulnerabilidades y el uso de honeypots son importantes para la administración de sistemas y redes por varias razones fundamentales:

1. \*\*Identificación de Debilidades en la Seguridad\*\*:

- El análisis de vulnerabilidades permite a los administradores de sistemas y redes identificar posibles debilidades en la seguridad de sus sistemas y aplicaciones. Esto es esencial para prevenir ataques y mejorar la postura de seguridad.

2. \*\*Detección Temprana de Amenazas\*\*:

- Los honeypots son sistemas configurados intencionalmente para atraer a los atacantes. Proporcionan una forma de detectar y estudiar ataques de manera temprana antes de que comprometan sistemas críticos.

3. \*\*Mejora de la Seguridad\*\*:

- La información recopilada a través del análisis de vulnerabilidades y los honeypots puede utilizarse para tomar medidas correctivas y mejorar la seguridad de una red o sistema, como la aplicación de parches, reconfiguraciones o mejoras en las políticas de seguridad.

4. \*\*Concienciación sobre Amenazas\*\*:

- Estas prácticas ayudan a los administradores a comprender mejor las amenazas específicas que enfrentan. Con esta comprensión, pueden tomar decisiones más informadas sobre cómo proteger sus sistemas y redes.

5. \*\*Investigación y Análisis de Amenazas\*\*:

- Los honeypots permiten estudiar a fondo las tácticas y técnicas utilizadas por los atacantes. Esto es esencial para el desarrollo de contramedidas efectivas y para contribuir a la investigación de ciberseguridad.

6. \*\*Cumplimiento de Normativas y Regulaciones\*\*:

- En muchos entornos, el análisis de vulnerabilidades y la implementación de honeypots son requisitos para el cumplimiento de normativas de seguridad, como el Reglamento General de Protección de Datos (GDPR) o las regulaciones de la industria.

7. \*\*Evaluación de Riesgos\*\*:

- Ambas prácticas ayudan a evaluar y cuantificar los riesgos de seguridad a los que se enfrenta una organización. Esto es esencial para priorizar recursos y tomar decisiones informadas.

8. \*\*Capacitación y Entrenamiento\*\*:

- Los honeypots pueden servir como entornos de capacitación para el personal de seguridad. Los administradores pueden utilizar los datos recopilados para desarrollar escenarios de entrenamiento y mejorar la preparación ante incidentes.

9. \*\*Alerta Temprana de Posibles Ataques\*\*:

- Los honeypots pueden funcionar como sistemas de alerta temprana, permitiendo a los administradores identificar patrones de tráfico inusual o sospechoso que podrían indicar un ataque en curso.

En resumen, el análisis de vulnerabilidades y los honeypots son herramientas fundamentales para mantener la seguridad de los sistemas y redes en un entorno cada vez más amenazante en el ámbito de la ciberseguridad. Ayudan a prevenir ataques, mitigar riesgos y mejorar la resiliencia de las organizaciones ante las amenazas cibernéticas.

La elección del sistema operativo para virtualizar en tu honeypot dependerá en gran medida de tus objetivos y preferencias, así como de las herramientas específicas que planeas utilizar en tu proyecto. Aquí hay algunas consideraciones para ayudarte a tomar una decisión:

1. **Linux**:
   * Linux es una opción común para implementar honeypots debido a su naturaleza de código abierto y su flexibilidad.
   * Puedes elegir una distribución de Linux como Ubuntu, CentOS o Debian.
   * Algunas herramientas de honeypot, como Cowrie y Dionaea, están diseñadas para Linux.
2. **Windows**:
   * Si tu objetivo es atraer amenazas que se dirigen principalmente a sistemas Windows, puedes virtualizar un sistema Windows como Windows Server o Windows 10 como honeypot.
   * Ten en cuenta que Windows puede requerir licencias y puede ser menos común en implementaciones de honeypots.
3. **Sistemas operativos específicos**:
   * Algunos honeypots están diseñados para emular sistemas operativos específicos. Por ejemplo, Honeyd puede emular varios sistemas operativos, incluyendo versiones de Windows y Linux.
   * Esta opción te permite simular sistemas específicos para atraer amenazas que se dirigen a esos sistemas.
4. **Honeypots de red**:
   * En algunos casos, puedes implementar honeypots de red, que no ejecutan un sistema operativo en particular, sino que interceptan el tráfico y registran los intentos de acceso no autorizado.
   * Esta opción no implica virtualizar un sistema operativo en sí, sino más bien implementar hardware o software de monitoreo de tráfico.

La elección dependerá de tu enfoque de investigación y del tipo de amenazas que desees analizar. Es importante considerar que los honeypots a menudo se utilizan como señuelos, por lo que debes configurarlos de manera realista para atraer a los atacantes. Además, es crucial seguir las mejores prácticas de seguridad al implementar honeypots, ya que a menudo involucran interactuar con tráfico malicioso.

<https://blog.elhacker.net/2021/01/los-mejores-honeypots-ejemplos-y-tipos-trampas-rdp-ssh-cowrie-docker-rdpy.html>

<https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>

<https://github.com/paralax/awesome-honeypots>