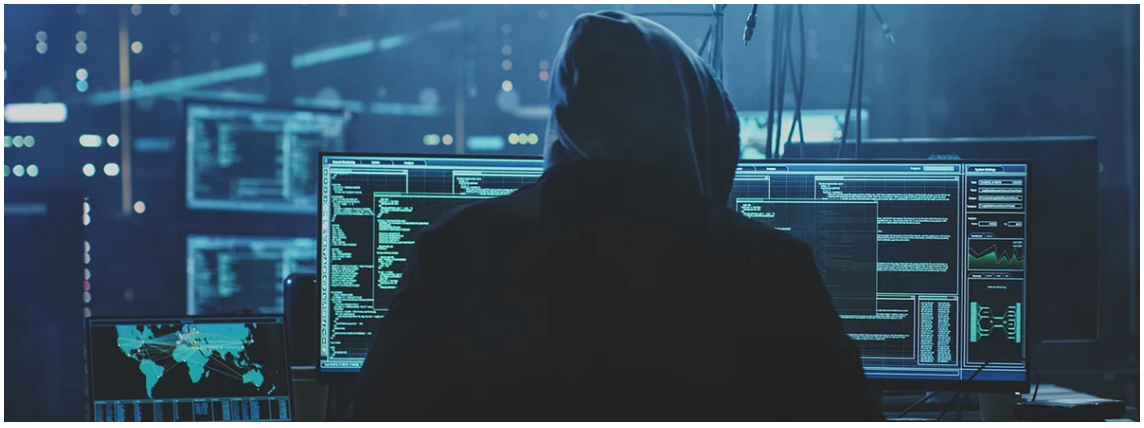
Asignatura:

Hacking Ético

Título del Documento:

Oferta - Numbers



Nombre:	Fecha:	Firma:
Mario de la Rosa García	02/04/24	
Gonzalo Pascual Romero	02/04/24	
David Lucas Sánchez	02/04/24	
Simón Armando Padrón	02/04/24	

Tabla de contenido

1. INTRODUCCIÓN

En esta propuesta de **pentesting**, abordaremos los aspectos clave relacionados con la seguridad de los sistemas de la empresa "**Number**". Nuestro objetivo es realizar una evaluación de la resiliencia de sus sistemas y aplicación web ante posibles explotaciones de vulnerabilidades que se puedan encontrar en su panorama de amenazas. La prueba estará focalizada en replicar las tácticas, técnicas y procedimientos posibles que podrían emplear atacantes externos contra la organización. El informe a presentar describirá los resultados de las pruebas de penetración además de detallar las vulnerabilidades encontradas como así también las medidas de mitigación y controles necesarios de implantar.

2. OBJETIVOS

La sección de objetivos detalla los fines primordiales y las metas específicas que se buscan alcanzar a través de la prueba de penetración. Estos objetivos son esenciales para dirigir el enfoque y los esfuerzos del equipo de seguridad durante la evaluación y para establecer los criterios contra los cuales se medirá el éxito de la prueba.

El primer objetivo es **identificar las vulnerabilidades específicas** encontradas en la máquina objetivo. Esto implica un análisis exhaustivo y detallado del sistema, utilizando diversas herramientas y técnicas para descubrir fallos de seguridad, configuraciones erróneas, o cualquier otro tipo de debilidades que podrían ser explotadas por un atacante. La identificación precisa de estas vulnerabilidades es fundamental, ya que proporciona la base para las fases subsiguientes de la prueba.

Una vez identificadas las vulnerabilidades, el siguiente objetivo es **explotarlas** para poder obtener acceso no autorizado al sistema. Esto incluye la obtención de acceso a niveles de usuario estándar, así como acceso a niveles de administrador o privilegiados. El propósito de este paso es demostrar el impacto real y el nivel de riesgo asociado con cada vulnerabilidad encontrada. No se trata simplemente de identificar teóricamente las debilidades, sino de probar en la práctica hasta qué punto estas pueden comprometer la seguridad de la máquina.

Finalmente, un **objetivo** adicional es **encontrar y capturar las "banderas" (flags)** ocultas en la máquina. Estas banderas son objetos o datos específicos colocados intencionalmente dentro del sistema como parte de la configuración de la prueba de penetración. El objetivo de localizar y capturar estas banderas es proporcionar una medida cuantitativa del éxito de la prueba, demostrando la capacidad del equipo de seguridad para descubrir y acceder a información protegida dentro del entorno evaluado.

Cada uno de estos objetivos contribuye a una comprensión completa de la postura de seguridad de la máquina y permite al equipo de seguridad y a la organización tomar decisiones informadas sobre cómo mejorar y fortalecer sus defensas.

3. ALCANCE

El pentest, en este caso, **se delimita estrictamente a la evaluación de seguridad** de la máquina servidor específicamente designada, la cual alberga la aplicación web crítica para las operaciones del cliente. Este enfoque concentrado asegura que los esfuerzos de seguridad estén dirigidos hacia el componente más crítico y potencialmente vulnerable dentro del ecosistema de TI del cliente. La evaluación se llevará a cabo específicamente en la dirección IP asignada al servidor, asegurando un análisis detallado y enfocado.

La ventana para la ejecución de esta prueba de penetración ha sido cuidadosamente seleccionada y programada **desde el 02 de abril hasta el 16 de abril**. Este período de tiempo ha sido acordado para minimizar cualquier interferencia con las operaciones normales del cliente y para proporcionar al equipo de CyberSentinel el tiempo necesario para realizar una evaluación exhaustiva.

El equipo técnico de CyberSentinel, una firma con experiencia y reconocimiento en el ámbito de la seguridad cibernética será responsable de llevar a cabo las pruebas. La combinación de herramientas avanzadas de seguridad y la profunda experiencia técnica del equipo garantizará un análisis completo y detallado de la seguridad del servidor web del cliente.

Durante el período estipulado, se realizará un **análisis profundo del servidor web**. Este análisis incluirá la evaluación de la configuración del servidor, la identificación de posibles fallos de seguridad y la detección de vulnerabilidades críticas y de alta severidad. Un enfoque particular será puesto en identificar aquellas vulnerabilidades que puedan ser explotadas a distancia, ya que representan una amenaza significativa por permitir a los atacantes comprometer el servidor sin necesidad de acceso físico.

El objetivo final de este pentest es **proporcionar al cliente un entendimiento** claro y detallado **de la postura de seguridad de su servidor web**, identificar áreas de riesgo y ofrecer recomendaciones concretas para mejorar la seguridad y protegerse contra ataques maliciosos.

4. FUERA DEL ALCANCE

Esta sección especifica los límites y exclusiones del proceso de prueba de penetración. Es importante destacar que la presente evaluación **no abarca ni incluye las pruebas relacionadas con técnicas de ingeniería social y phishing**. Estas prácticas, aunque relevantes para la seguridad integral, requieren un enfoque y metodología distintos y, por lo tanto, no se contemplan dentro del alcance de este pentest específico.

Además, se **excluye de este análisis la revisión del código fuente** de las aplicaciones halladas dentro del servidor. Tal revisión implicaría un examen detallado de las líneas de código individualmente, buscando vulnerabilidades o fallos de seguridad específicos, lo cual representa un tipo de prueba diferente y más especializada que no se incluye en los servicios proporcionados en este caso particular.

Es fundamental también señalar que cualquier elemento encontrado que no esté incluido en la máquina virtual designada para el pentest queda fuera del alcance de la prueba. Esto incluye, pero no se limita a, dispositivos físicos, sistemas externos, redes adicionales y otros activos digitales que no hayan sido específicamente señalados para la evaluación. La delimitación precisa del entorno de prueba es crucial para garantizar una evaluación clara, enfocada y efectiva.

Al establecer estos límites, buscamos asegurar una prueba de penetración concentrada y eficiente, permitiendo al equipo de seguridad centrarse en las áreas designadas y proporcionando resultados más precisos y útiles para la organización.

5. METODOLOGÍA

La metodología de esta auditoría consistirá en **distintas fases teniendo como objetivo la elaboración de un informe que detalle los hallazgos de vulnerabilidades y los controles apropiados para su mitigación**. Durante el proyecto, se simulará el procedimiento con el que actuaría una amenaza externa a la organización cubriendo todas las fases de una intrusión. Será una **investigación de caja negra** y se realizará acorde a las siguientes fases:

5.1. Fase 1. Reconocimiento:

El reconocimiento activo se realizará para recopilar información sobre el objetivo de la auditoría, como **direcciones IP de dispositivos, nombres de dominio, tecnologías utilizadas y sus versiones, etc**. Además, se utilizarán fuentes abiertas para la recopilación de datos públicos que revelen información que no debería ser pública. El enfoque estará dirigido obtener la máxima cantidad de información sobre la organización a la que pertenece el sistema objetivo. La información que se recolecta de fuentes abiertas puede incluir: datos sobre librerías, datos de los empleados, estructura de correos corporativos, dependencias y credenciales de acceso predeterminadas.

5.2. Fase 2. Inspección:

Se emplearán diversas herramientas para realizar un **inventario de los activos hardware y software**. Está información puede ser utilizada por un atacante para identificar cuáles son los dispositivos en funcionamiento o las aplicaciones ejecutadas por el sistema de la empresa **para poder identificar qué vulnerabilidades existen**. Definiremos el objetivo que se desea atacar y los puntos críticos con vulnerabilidades que se pueden llegar a explotar. En esta etapa se hace una recolección de información más específica para sacar datos como sus sistemas operativos, los servicios y sus respectivas versiones, páginas web almacenadas en el servidor, rangos de IP, información de DNS, detección de IDS e IPS o firewall.

5.3. Fase 3. Análisis de Vulnerabilidades:

Utilizaremos herramientas punteras en el mercado para encontrar las vulnerabilidades más efectivas que apliquen tanto al software como a los servicios que se encontraron en la fase previa. El propósito de esta fase es determinar la información relevante para realizar ataques que una amenaza externa sería capaz de identificar. **Esta información sería utilizada por el atacante para determinar las vulnerabilidades del sistema objetivo que deberá explotar para lograr lanzar su ataque**. Con la información obtenida podremos clasificar las posibles vulnerabilidades del sistema objetivo.

- Vulnerabilidad local: Es el tipo de vulnerabilidad en la cual se debe tener acceso físico a la máquina o sistema objetivo para explotar una vulnerabilidad y posterior a esto elevar o escalar privilegios dentro del sistema y tener acceso a él sin ninguna restricción.
- Vulnerabilidad remota: Es el tipo de vulnerabilidad en la cual se puede obtener acceso al sistema objetivo a través de la red sin necesidad de un acceso físico o local.

5.4. Fase 4. Explotación:

Utilizaremos la información obtenida en las fases previas y aprovecharemos las vulnerabilidades encontradas en el sistema objetivo para tomar control de éste y **conseguir extraer datos confidenciales en formato de "flags"** como también **escalar privilegios para conseguir el control total sobre el sistema objetivo**.

Se elegirán varias vulnerabilidades para explotar y conseguir adquirir el control del sistema. Durante esta fase también **se pondrá a prueba los sistemas de detección y de seguridad** empleados por el equipo responsable dentro de la organización. El objetivo de esta fase consiste en **simular el plan de acción de una supuesta amenaza externa una vez que ésta haya adquirido el acceso y/o control de algún sistema o red** de la infraestructura de la organización. Esta fase revelará tanto las vulnerabilidades presentes en el sistema que se deben de remediar como también fallos en los sistemas de monitorización y protección que permiten a un atacante permanecer dentro de los sistemas de la empresa una vez terminada la explotación de las vulnerabilidades.

Además, realizaremos un secuestro de datos críticos para el funcionamiento de la organización con el propósito de simular el modus operandi de una amenaza externa y probar las medidas de mitigación implantadas por el equipo de seguridad para evitar tal evento. A continuación, se explica más a fondo esta fase de la metodología.

5.5. Fase 5. Secuestro de datos:

Durante esta fase nos centraremos en **identificar y extraer información sensible de la máquina objetivo**. Utilizaremos técnicas especializadas para acceder a datos confidenciales, como, por ejemplo: **archivos, bases de datos o información confidencial de los usuarios**. Nuestro objetivo es **simular un escenario realista en el cual algún posible atacante podría comprometer la seguridad de la infraestructura y obtener acceso a datos sensibles sin autorización**. Este proceso se realizará con el máximo cuidado y respeto a la privacidad y confidencialidad de los datos, asegurando que **cualquier información obtenida se maneje de manera ética y responsable**.

5.6. Fase 6. Borrado de huellas:

En esta última fase, se eliminarán las evidencias e indicios de compromiso que delaten la presencia y actuación de un actor externo**. Se tomarán todas las medidas que un atacante utilizaría para cubrir su rastro y asegurarse de no ser localizado posteriormente al ataque**. Estas medidas podrán incluir:

- Alteración de las marcas de tiempo.
- Modificar valores de registro.
- Alteración de los registros del sistema para eliminar evidencias de las actividades realizadas.
- Cerrar todos los puertos que fueron abiertos.
- Desinstalar las aplicaciones utilizadas para lograr los objetivos.

6. RIESGOS

6.1. Apoyo Ejecutivo

Falta de apoyo por parte de la directiva. El equipo del proyecto no tiene la autoridad necesaria para lograr los objetivos del proyecto. El apoyo ejecutivo es fundamental para el éxito del proyecto.

Los conflictos entre los operarios del proyecto perturban a los miembros de la directiva o existe un desacuerdo sobre los problemas del proyecto a nivel ejecutivo.

Solución: Establecer una comunicación efectiva y continua con la dirección ejecutiva para asegurar su compromiso y apoyo en todas las etapas del proyecto. Esto implica la organización de reuniones regulares para informar sobre el progreso, discutir problemas y recalcar la importancia y los beneficios del proyecto para la organización. Asimismo, es crucial definir y comunicar claramente los roles, responsabilidades y autoridad del equipo del proyecto desde el inicio. Involucrar a los miembros de la dirección en la toma de decisiones clave y proporcionarles informes periódicos puede aumentar su compromiso y facilitar la resolución de conflictos. Además, implementar una estrategia de gestión de cambios que incluya la capacitación y sensibilización de los ejecutivos sobre los aspectos críticos y los beneficios del proyecto puede mejorar significativamente su apoyo y colaboración.

6.2. Alcance:

No se ha definido bien el alcance. El riesgo proviene de un error u omisión en el momento de la definición del alcance.

Estimaciones inexactas es un riesgo común en realidad el proyecto. Puede afectar drásticamente la programación del proyecto y también los costes.

Solución: Realizar una revisión exhaustiva del alcance del proyecto y asegurarse de que todas las partes involucradas comprendan claramente lo que se espera. Esto incluye definir criterios de éxito claros y establecer un proceso sólido para estimaciones y

pronósticos, con la participación de expertos en el área correspondiente y el uso de datos históricos siempre que sea posible.

6.3. Gestión del cambio:

Un gran número de solicitudes de cambio dramáticamente aumenta la complejidad del proyecto y quita prioridad a las características clave.

Solicitudes de cambios de baja calidad.

Solución: Implementar un proceso formal y claro para gestionar los cambios en el proyecto. Esto incluiría establecer criterios claros para evaluar y priorizar las solicitudes de cambio, así como comunicar de manera efectiva los impactos de dichos cambios en el alcance, los plazos y los costos del proyecto.

6.4. Comunicación:

Cuando los requisitos son mal interpretados por el equipo del proyecto se producirá un desfase entre las expectativas, demandas y el trabajo en su conjunto.

Los usuarios tienen expectativas inexactas.

Solución: Mejorar la comunicación a través de la clarificación constante de los requisitos y la retroalimentación regular entre todas las partes interesadas. Esto podría incluir el uso de herramientas de gestión de proyectos y reuniones regulares para garantizar que todos estén en la misma página y que las expectativas sean realistas y alineadas con los objetivos del proyecto.

6.5. Equipo:

Las debilidades de los miembros del equipo.

Problemas de rendimiento del equipo del proyecto.

Solución: Identificar las áreas de debilidad dentro del equipo y proporcionar capacitación y desarrollo adecuados para abordar esas deficiencias. Además, fomentar un ambiente de trabajo positivo y colaborativo, donde se reconozcan y se aborden los

problemas de rendimiento de manera proactiva, puede mejorar la productividad y la moral del equipo.

6.6. Técnico:

Los componentes técnicos no son escalables.

Los componentes técnicos tienen vulnerabilidades de seguridad.

Solución: Realizar una evaluación exhaustiva de los componentes técnicos utilizados en el proyecto y tomar medidas para abordar cualquier problema de escalabilidad o seguridad. Esto podría incluir la actualización de tecnologías obsoletas, la implementación de medidas de seguridad adicionales y la realización de pruebas exhaustivas para identificar y mitigar posibles vulnerabilidades.

6.7. Integración:

La imposibilidad de adaptarse a los procesos de negocio.

El proyecto interrumpe las operaciones.

Solución: Incorporar la planificación de la integración desde las etapas iniciales del proyecto, asegurándose de que se entienda y se alinee con los procesos de negocio existentes. Además, implementar estrategias de mitigación de riesgos para minimizar las interrupciones operativas durante la implementación del proyecto, como la realización de pruebas exhaustivas y la coordinación efectiva con los equipos operativos relevantes.

6.8. Requisitos:

Los requisitos son ambiguos.

Los requisitos son incompletos.

Solución: Establecer un proceso claro para la captura y documentación de requisitos, incluyendo la realización de sesiones de trabajo con las partes interesadas relevantes para aclarar cualquier ambigüedad y garantizar que todos los requisitos sean completos

y comprensibles. Además, mantener una comunicación abierta y continua con las partes interesadas puede ayudar a identificar y abordar cualquier cambio en los requisitos a medida que surjan.

6.9. Decisiones y solución de problemas:

Los proyectos en retrasos generan impacto al establecer directrices para la toma de decisión.

Las decisiones no son las adecuadas para el propósito del proyecto.

Solución: Implementar un proceso de toma de decisiones claro y eficiente que incluya la identificación y evaluación de todas las opciones disponibles, así como la consideración de las posibles consecuencias de cada decisión. Además, establecer un mecanismo para revisar y ajustar las decisiones a medida que evoluciona el proyecto puede ayudar a garantizar que se tomen las decisiones más apropiadas y oportunas.

6.10. Adquisición:

Propuesta al RFP que es inutilizable.

La infraestructura es de baja calidad.

Solución: Realizar una evaluación exhaustiva de las propuestas recibidas en respuesta a RFP (Request for Proposal) y seleccionar proveedores que puedan cumplir con los requisitos del proyecto de manera efectiva. Además, establecer estándares de calidad claros y realizar una supervisión continua de la infraestructura adquirida para garantizar que cumpla con los estándares establecidos y satisfaga las necesidades del proyecto.

6.11. Autoridad:

La falta de autoridad en el equipo para completar el trabajo y lograr los objetivos.

Solución: Empoderar al equipo del proyecto otorgándole la autoridad necesaria para tomar decisiones y llevar a cabo las tareas requeridas para cumplir con los objetivos del proyecto. Esto podría incluir la asignación de responsabilidades claras y la eliminación

de obstáculos organizativos que puedan obstaculizar el progreso del equipo. Además, establecer canales de comunicación efectivos entre el equipo del proyecto y la dirección superior puede ayudar a garantizar un flujo constante de apoyo y orientación.

7. PLANIFICACIÓN DEL PROYECTO

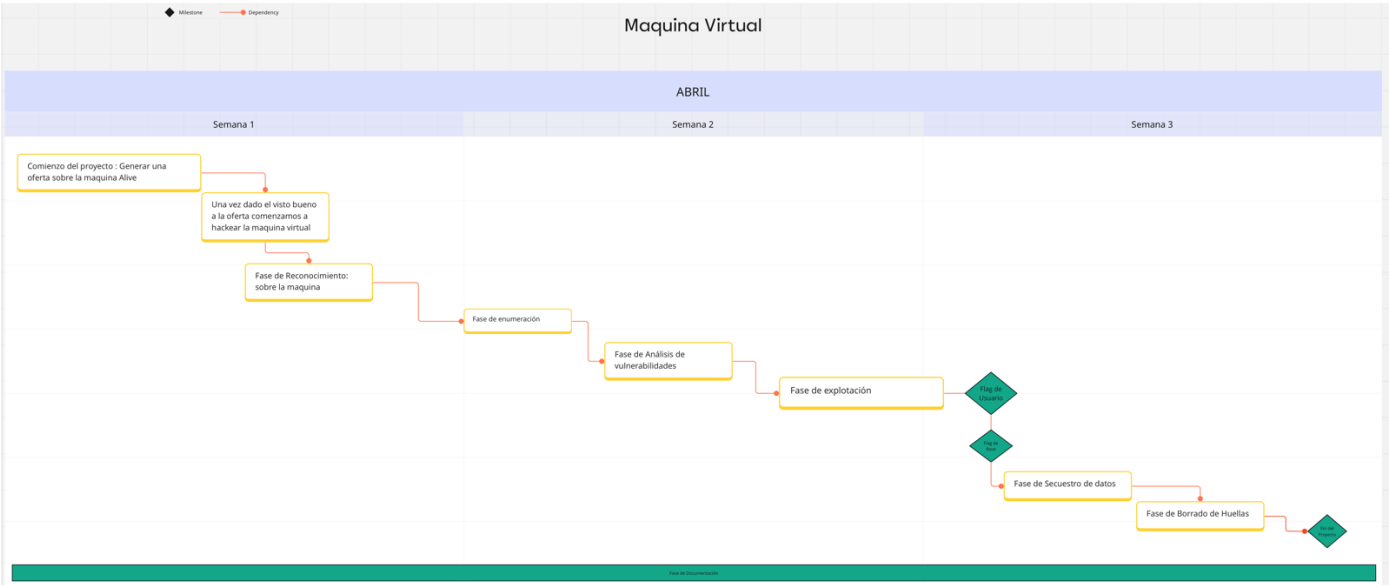
7.1. Forma de pago:

El pago se realizará en **dos partes**:

70% al inicio del pentest	4340 €
30% al finalizar el pentest	1860 €

7.2. Tiempo de entrega:

El pentest se realizará en un plazo de **15 días hábiles**.



7.3. Costes:

Realización del pentesting y explotación de la máquina objetivo	5.200 €
Realización del análisis de vulnerabilidades e informe	1.000€

7.4. Distribución:

1. **Líder de Equipo (Gestor de Proyecto):**

Presupuesto: 2000 euros

Horas laborables: 15 días * 8 horas/día = 120 horas

Tarifa por hora: 2000 euros / 120 horas ≈ **16.67 euros/hora**

2. **Pentester:**

Presupuesto: 2500 euros

Horas laborables: 15 días * 8 horas/día = 120 horas

Tarifa por hora: 2500 euros / 120 horas ≈ **20.83 euros/hora**

3. **Técnico/Experto en Sistemas:**

Presupuesto: 1200 euros

Horas laborables: 15 días * 8 horas/día = 120 horas

Tarifa por hora: 1200 euros / 120 horas ≈ **10 euros/hora**

4. **Documentalista:**

Presupuesto: 500 euros

Horas laborables: 15 días * 4 horas/día = 60 horas

Tarifa por hora: 500 euros / 60 horas ≈ **8.33 euros/hora**

* Este desglose proporciona las tarifas por hora para cada rol basado en el presupuesto asignado.

7.5. Entregables

Los **entregables** del proyecto consistirán en:

- Acta de Kick-Off
- Informe de Seguimiento del Proyecto
- Informe Técnico del Pentest que incluirá:
  - Descripción de las pruebas realizadas
  - Vulnerabilidades identificadas
  - Explotación de vulnerabilidades
  - Impacto potencial de las vulnerabilidades
  - Recomendaciones para mitigar las vulnerabilidades
- Guía burros/Manual técnico

7.6. Compras para proyecto:

No se necesitan compras adicionales para la realización del proyecto.

7.7. Contacto:

Para cualquier pregunta o comentario, no dude en contactarnos a: [correo electrónico]

5. ANEXO

a. Herramientas:

Nmap: abreviatura de Network Mapper, es una herramienta de código abierto utilizada para explorar y mapear redes informáticas. Permite a los administradores de sistemas y profesionales de seguridad escanear redes para descubrir hosts activos, servicios en ejecución, puertos abiertos y otros detalles de la topología de red. Nmap ofrece una variedad de técnicas de escaneo, como el escaneo de puertos, el escaneo de versiones de servicios, el descubrimiento de sistemas operativos remotos, entre otros. Además, puede usarse para detectar y evaluar vulnerabilidades de seguridad en sistemas y dispositivos de red. Es una herramienta poderosa y versátil que se utiliza comúnmente en auditorías de seguridad, pruebas de penetración y tareas de administración de redes.

Kali Linux: es una distribución de Linux basada en Debian, diseñada específicamente para pruebas de penetración y seguridad informática. Incorpora una amplia gama de herramientas de seguridad, incluyendo herramientas de escaneo de red como Nmap, utilidades de fuerza bruta como Hydra, herramientas de análisis forense digital como Autopsy, y muchas otras.

Msfvenom: Esta herramienta de Metasploit se utiliza para generar payloads personalizados para la explotación de sistemas vulnerables. Msfvenom permite a los operadores de seguridad crear payloads específicos para sus objetivos, como troyanos, backdoors o exploits, adaptados a diferentes plataformas y arquitecturas. Esto es esencial para la creación de herramientas de ataque efectivas en pruebas de penetración, ya que permite a los profesionales de la seguridad adaptar sus ataques a las condiciones específicas de la infraestructura objetivo.

MySQL: Este sistema de gestión de bases de datos relacional es una opción popular para el almacenamiento y gestión de datos en aplicaciones web. MySQL es conocido por su rendimiento, fiabilidad y facilidad de uso, lo que lo convierte en una opción preferida para proyectos de todos los tamaños. Su integración con PHP y otros lenguajes de programación lo hace especialmente popular en el desarrollo de aplicaciones web dinámicas, aunque la seguridad de MySQL depende en gran medida de las prácticas de administración de bases de datos implementadas.

Nmap: abreviatura de Network Mapper, es una herramienta de código abierto utilizada para explorar y mapear redes informáticas. Permite a los administradores de sistemas y profesionales de seguridad escanear redes para descubrir hosts activos, servicios en ejecución, puertos abiertos y otros detalles de la topología de red. Nmap ofrece una variedad de técnicas de escaneo, como el escaneo de puertos, el escaneo de versiones de servicios, el descubrimiento de sistemas operativos remotos, entre otros. Además, puede usarse para detectar y evaluar vulnerabilidades de seguridad en sistemas y dispositivos de red. Es una herramienta poderosa y versátil que se utiliza comúnmente en auditorías de seguridad, pruebas de penetración y tareas de administración de redes.

NetCat: También conocido como "nc", es una herramienta de línea de comandos que facilita la comunicación y transferencia de datos entre dos sistemas a través de una red utilizando los protocolos TCP/IP y UDP. Se utiliza para una variedad de propósitos, desde la simple transferencia de archivos hasta la creación de túneles de red y la realización de pruebas de penetración. NetCat puede actuar tanto como servidor como cliente, lo que lo hace extremadamente versátil en entornos de redes. Es una herramienta popular en el campo de la seguridad informática y la administración de redes, y se utiliza comúnmente para realizar pruebas de seguridad, auditorías de red y depuración de aplicaciones. Su flexibilidad y facilidad de uso lo convierten en una herramienta valiosa para cualquier persona que trabaje con redes informáticas.

PHP: Es un lenguaje de programación de código abierto diseñado específicamente para el desarrollo de aplicaciones web dinámicas. PHP se ejecuta en el servidor y se integra fácilmente con HTML, lo que permite la creación de sitios web interactivos y dinámicos. Con soporte para una variedad de bases de datos, incluido MySQL, PHP es una opción popular para la creación rápida de aplicaciones web, aunque su seguridad puede ser un desafío debido a las vulnerabilidades comunes asociadas con el código PHP mal escrito.

Python: Este lenguaje de programación de alto nivel es conocido por su sintaxis clara y legible, lo que lo hace accesible para principiantes y poderoso para profesionales. Python se utiliza en una amplia gama de aplicaciones, desde el desarrollo web y la automatización de tareas hasta la inteligencia artificial y el análisis de datos. En el ámbito de la seguridad informática, Python es popular debido a su flexibilidad y la gran cantidad de bibliotecas y herramientas disponibles, lo que facilita el desarrollo de scripts y herramientas personalizadas para tareas de pentesting.

Searchsploit: Como parte del marco Metasploit, Searchsploit permite a los investigadores de seguridad buscar exploits y payloads en la base de datos de Metasploit. Esto simplifica el proceso de encontrar exploits para vulnerabilidades conocidas en sistemas y aplicaciones, facilitando la investigación y la ejecución de pruebas de penetración. Con una interfaz de línea de comandos fácil de usar, Searchsploit proporciona acceso rápido a una amplia gama de exploits y facilita la identificación de amenazas potenciales en entornos de red.