Reporte de proyecto de explotación en pentesting en una maquina vulnerable.

Introducción.

Objetivo: El principal objetivo del proyecto es identificar y explotar vulnerabilidades en una máquina diseñada para simular entornos reales de ciberseguridad. A través de pruebas de penetración (pentesting), se busca evaluar la seguridad de la infraestructura, validar la efectividad de las medidas de protección implementadas y proporcionar recomendaciones para mitigar riesgos.

El alcance del proyecto incluye:

1. **Identificación de Vulnerabilidades:** Realizar un escaneo exhaustivo de la máquina utilizando herramientas y técnicas de pentesting para descubrir posibles debilidades en el sistema.
2. **Explotación de Vulnerabilidades:** Intentar explotar las vulnerabilidades identificadas para determinar el impacto potencial y la facilidad con la que un atacante podría comprometer la máquina.
3. **Evaluación de Seguridad:** Analizar la configuración de seguridad, políticas de acceso y controles implementados en la máquina.
4. **Documentación y Reporte:** Elaborar un informe detallado que incluya hallazgos, métodos utilizados, evidencia de explotación y recomendaciones para mejorar la seguridad.

Herramientas y técnicas utilizadas.

- **Nmap**: Utilizada para escanear redes y descubrir hosts activos, puertos abiertos y servicios en ejecución.
- **Nikto**: Herramienta de escaneo de vulnerabilidades web que identifica configuraciones inseguras y vulnerabilidades en servidores web.
- **Metasploit**: Framework muy popular para el desarrollo y ejecución de exploits. Permite automatizar la explotación de vulnerabilidades.

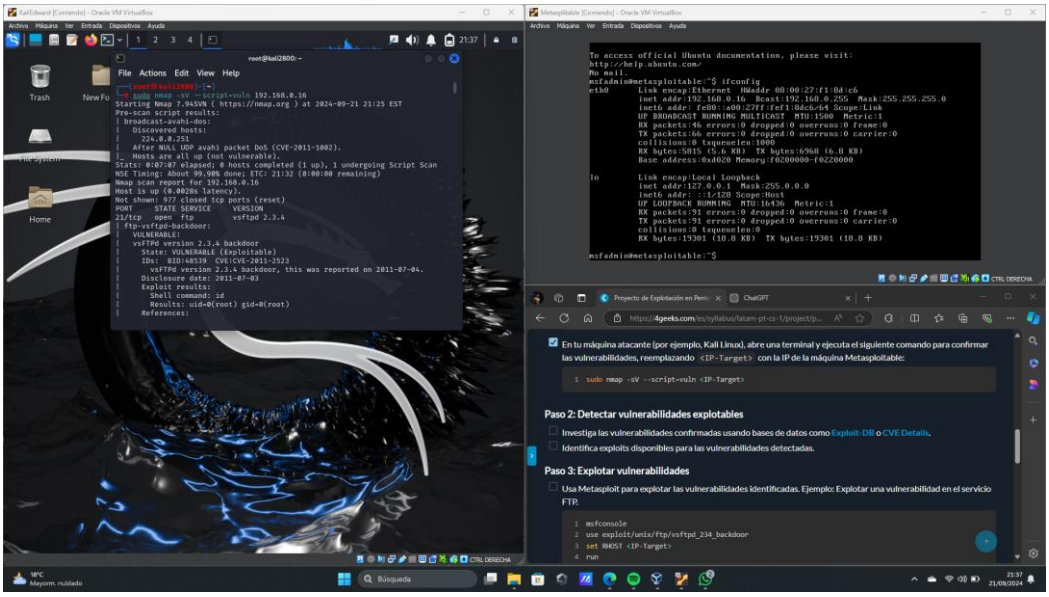
Técnicas

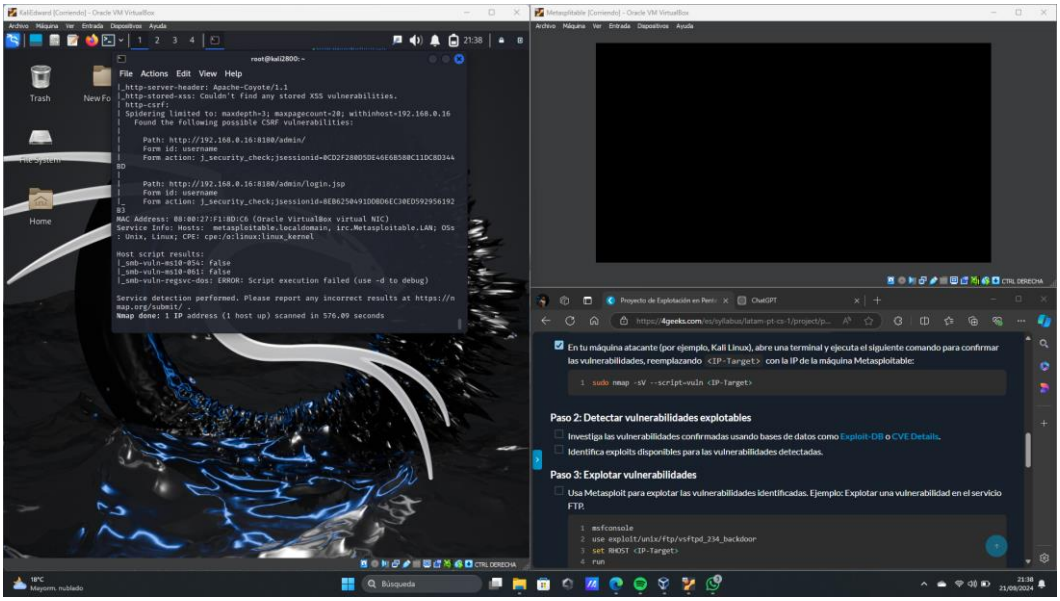
- **Reconocimiento**: Recolección de información sobre el objetivo, como direcciones IP, nombres de dominio y servicios expuestos.
- **Escaneo**: Identificación de puertos abiertos, servicios y posibles vulnerabilidades mediante escaneo de red.
- **Enumeración**: Recopilación de información detallada sobre usuarios, grupos, y configuraciones del sistema.

- **Explotación**: Uso de exploits para aprovechar vulnerabilidades y obtener acceso no autorizado.

Detalles de las vulnerabilidades explotadas.

- Como primer punto abrimos la terminal de nuestra maquina atacante y ejecutamos el comando **sudo nmap –sV –script=vuln + la direcciòn de la maquina víctima,** este comando es para confirmar las vulnerabilidades encontradas.





Detectar vulnerabilidades explotables.

Para este apartado tomamos 5 vulnerabilidades del escaneo que realizamos anteriormente.

- **Puerto 21/tcp CVE-2011-2523** estado: abierto, servicio: ftp.
  vsftpd versión 2.3.4 descargado entre 20110630 y 20110703, contiene una puerta trasera (backdoor) que abre un shell en el puerto 6200/tcp. Estatus vulnerable. (Explotable)

  Posible solución vsftpd: versión 2.3.4 posterior al 3 de julio de 2011. Si vsftpd 2.3.4 fue descargado entre el 30 de junio de 2011 y el 3 de julio de 2011, se debe descargar la nueva versión.
- **Puerto 22/tcp CVE-2023-38408** estado: abierto, servicio: ssh.
  La característica PKCS#11 en ssh-agent en OpenSSH anterior a 9.3p2 tiene una ruta de búsqueda insuficientemente confiable, lo que lleva a la ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante. (El código en /usr/lib no es necesariamente seguro para cargar en ssh-agent). NOTA: este problema existe debido a una solución incompleta para CVE-2016-10009. Estatus vulnerable de 9.8 crítico.

Para abordar las preocupaciones de seguridad asociadas con CVE-2023-38408, se proponen las siguientes estrategias de mitigación y recomendaciones:

- **Actualizar a la versión de OpenSSH**: Es esencial actualizar OpenSSH a la versión 9.3p2 o más reciente.
- **Limitar el uso de proveedores PKCS#11**: Ajusta las configuraciones de OpenSSH para aceptar solo proveedores PKCS#11 de confianza. Al restringir el acceso a una lista seleccionada de proveedores verificados, reduces la posibilidad de explotación y limitas las vías potenciales a través de las cuales los atacantes pueden obtener acceso.
- **Puerto 22/tcp CVE-2015-5600**: Vulnerabilidad en la función kbdint_next_device en auth2-chall.c en sshd en OpenSSH hasta la versión 6.9, no restringe correctamente el procesamiento de dispositivos de teclado interactivo con una única conexión, lo cual facilita a atacantes remotos ejecutar un ataque de fuerza bruta o causar una denegación de servicio (mediante el consumo de la CPU) a través de una lista larga y redundante en la opción ssh -oKbdInteractiveDevices, según lo demostrado por una modificación en el cliente que provee una contraseña diferente para cada uno de los elementos pam de la lista.

Las siguientes versiones de software se han actualizado para resolver este problema específico: Junos OS 12.1X44-D55, 12.1X46-D40, 12.1X47-D30*, 12.3R11, 12.3X48-D20*, 13.2X51-D40*, 13.2X52-D30, 13.3R8, 14.1R6, 14.2R5, 15.1F3, 15.1F2-S1, 15.1R2, 15.1X49-D20, 15.1X53-D20 y todas las versiones posteriores.

- **Puerto 25/tcp CVE-2014-3566, estado:abierto, servicio:smtp.**
  El protocolo SSL 3.0, utilizado en OpenSSL hasta 1.0.1i y otros productos, utiliza relleno (padding) CBC no determinístico, lo que facilita a los atacantes man-in-the-middle obtener datos de texto plano a través de un ataque de relleno (padding) oracle, también conocido como el problema "POODLE". Estado vulnerable (baja).
- **Puerto 53/tcp CVE-2008-0122, Estado: abierto, servicio:domain.**
  Error de off-by-one en la función inet_network en libbind en ISC BIND 9.4.2 y versiones anteriores, utilizado en libc en FreeBSD 6.2 hasta 7.0-PRERELEASE, permite a atacantes dependientes del contexto causar una denegación de servicio (fallo) y posiblemente ejecutar código arbitrario a través de una entrada manipulada que desencadena corrupción de memoria. Estado vulnerable (alta).
  Realiza una de las siguientes acciones:
  - Actualiza tu sistema vulnerable a 7.0-PRERELEASE, o 6-STABLE, o a las ramas de seguridad RELENG_7_0, RELENG_6_3 o RELENG_6_2 con fecha posterior a la fecha de corrección.
  - Para parchear tu sistema actual:
    Los siguientes parches han sido verificados para aplicarse a sistemas FreeBSD 7.0, 6.3 o 6.2.

Exploits disponibles para las vulnerabilidades encontradas.

- **CVE (Common Vulnerabilities and Exposures)**: Cada vulnerabilidad se registra con un identificador CVE. Puedes buscar en la base de datos CVE para encontrar vulnerabilidades específicas y sus exploits asociados.
- **Exploit-DB**: Este es un repositorio de exploits que contiene código y descripciones para numerosas vulnerabilidades. Puedes buscar por tipo de software o CVE.

Escalación de privilegios.

El escalamiento de privilegios es una técnica que utilizan los atacantes para obtener acceso a niveles más altos de autorización dentro de un sistema.

Algunas técnicas utilizadas en este caso son: Explotación de vulnerabilidades, Ataques de fuerza bruta, Inyección SQL.

Algunos resultados obtenidos con los casos presentados son:

- **Instalar puertas traseras:** Para mantener el acceso al servidor de forma persistente.
- **Robar datos sensibles:** Acceder a bases de datos que contienen información confidencial de los clientes, empleados o de la empresa.
- **Realizar ataques de denegación de servicio (DoS):** Inutilizar el servidor para los usuarios legítimos.
- **Moverse lateralmente:** Utilizar el servidor comprometido como punto de partida para atacar otros sistemas de la red.

Mitigación.
Para mitigar los riesgos identificados y proteger la máquina de futuras explotaciones, se recomiendan las siguientes acciones:

- **Parcheo de vulnerabilidades:**
    - Aplicar los parches de seguridad más recientes para el sistema operativo, aplicaciones y software de terceros.
- **Configuración segura:**
  Revisar y fortalecer la configuración de seguridad de la máquina, incluyendo:
    - Restricción de los servicios innecesarios.
    - Configuración de firewalls para bloquear el tráfico no autorizado.
    - Implementación de reglas de control de acceso basado en roles (RBAC).
- **Gestión de contraseñas:**
  Implementar políticas de contraseñas sólidas, incluyendo el uso de contraseñas fuertes y únicas para cada cuenta.
- **Capacitación de usuarios:**
  Concientizar a los usuarios sobre las mejores prácticas de seguridad, como evitar hacer clic en enlaces sospechosos o descargar archivos adjuntos de correos electrónicos no solicitados.

Monitoreo continuo:

- Implementar un sistema de detección de intrusos (IDS) y un sistema de prevención de intrusiones (IPS) para monitorear la actividad de la red y detectar posibles ataques.
- Realizar auditorías de seguridad periódicas para identificar nuevas vulnerabilidades y evaluar la efectividad de las medidas de seguridad implementadas.

Conclusión.

Tras la evaluación de seguridad realizada, se identificó un conjunto de vulnerabilidades críticas en la máquina [Metaspoitable]. Estas vulnerabilidades, si fueran explotadas por un actor malicioso, podrían haber resultado en posibles consecuencias, como pérdida de datos, interrupción del servicio, etc.