Reconocimiento de la Máquina

Introducción

En este informe, se documenta un proceso de pruebas de penetración (pentesting) con el objetivo de identificar y analizar las vulnerabilidades presentes en una máquina virtual vulnerable. A lo largo del ejercicio, se evaluaron los puertos abiertos y los servicios en ejecución para determinar posibles brechas de seguridad que pudieran ser explotadas. Este análisis es fundamental para comprender el impacto que estas vulnerabilidades podrían tener en la seguridad del sistema y en la integridad de la organización.

Objetivo

El objetivo de este ejercicio es demostrar el conocimiento adquirido en el módulo, en el cual se nos enseñó cómo realizar un escaneo completo de una máquina vulnerable. A través de la evaluación de los puertos y servicios, se busca desarrollar un análisis profundo de cómo las vulnerabilidades encontradas pueden impactar en la seguridad de un entorno corporativo.

Alcance

Se detallarán las vulnerabilidades encontradas de una manera clara y comprensible, con el fin de proporcionar conciencia y comprensión sobre los riesgos de seguridad, tanto para un público técnico como no técnico.

Herramientas y Técnicas Utilizadas

Para la ejecución de estas pruebas, se utilizaron dos máquinas virtuales: una máquina atacante (Kali Linux) y una máquina vulnerable (Metasploitable 2). Se realizaron escaneos básicos y avanzados de los puertos utilizando la herramienta Nmap, lo que permitió identificar qué puertos estaban abiertos y qué versiones de software estaban en ejecución. Con base en esta información, se identificaron las vulnerabilidades potenciales que podrían ser explotadas.

Vulnerabilidades

- **Puerto**: 21/tcp, **Servicio**: ftp, **Versión**: vsftpd 2.3.4, **ID CVE**: CVE-2011-2523
  Explicación: Descargar entre 20110630 y 20110703 contiene un backdoor que abre una shell en el puerto 6200/tcp
  Severidad: V4.0: (no disponible), V3.1: 9.8 CRÍTICO, V2.0: 10.0 ALTO
- **Puerto**: 22/tcp, **Servicio**: ssh, **Versión**: OpenSSH 4.7p1, **ID CVE**: CVE-2008-5161

Explicación: Error en el manejo del protocolo SSH en Tectia y OpenSSH cuando se utiliza un algoritmo de cifrado en modo Cipher Block Chaining (CBC), lo que facilita a los atacantes remotos recuperar ciertos datos en texto plano.
Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 2.6 BAJO

- **Puerto**: 53/tcp, **Servicio**: domain, **Versión**: ISC BIND 9.4.2, **ID CVE**: CVE-2008-4163
  Explicación: Vulnerabilidad no especificada en ISC BIND permite a atacantes remotos provocar una denegación de servicio a través de vectores desconocidos.
  Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 7.8 ALTO
- **Puerto**: 53/tcp, **Servicio**: domain, **Versión**: ISC BIND 9.4.2, **ID CVE**: CVE-2008-0122
  Explicación: Error "off-by-one" en la función inet_network en ISC BIND permite a atacantes dependientes del contexto causar una denegación de servicio o ejecutar código arbitrario a través de entrada manipulada que desencadena corrupción de memoria.
  Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 10.0 ALTO
- **Puerto**: 80/tcp, **Servicio**: http, **Versión**: Apache httpd 2.2.8 (Ubuntu) DAV/2, **ID CVE**: CVE-2010-1452
  Explicación: Los módulos mod_cache y mod_dav en Apache HTTP Server permiten a atacantes remotos causar una denegación de servicio (crash del proceso) a través de una solicitud sin una ruta.
  Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 5.0 MEDIO
- **Puerto**: 80/tcp, **Servicio**: http, **Versión**: Apache httpd 2.2.8 (Ubuntu) DAV/2, **ID CVE**: CVE-2011-3192
  Explicación: El filtro byterange en Apache HTTP Server permite a atacantes remotos causar una denegación de servicio (consumo de memoria y CPU) a través de un encabezado Range que expresa múltiples rangos superpuestos.
  Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 7.8 ALTO
- **Puerto**: 80/tcp, **Servicio**: http, **Versión**: Apache httpd 2.2.8 (Ubuntu) DAV/2, **ID CVE**: CVE-2009-1891
  Explicación: El módulo mod_deflate en Apache httpd comprime archivos grandes incluso después de que la conexión de red asociada se haya cerrado, lo que permite a atacantes remotos provocar una denegación de servicio (consumo de CPU).
  Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 7.1 ALTO
- **Puerto**: 111/tcp, **Servicio**: rpcbind, **Versión**: 2 (RPC #100000), **ID CVE**: CVE-2003-1070
  Explicación: Vulnerabilidad desconocida en rpcbind para Solaris permite a atacantes remotos provocar una denegación de servicio (crash de rpcbind).
  Severidad: V4.0: (no disponible), V3.x: (no disponible), V2.0: 5.0 MEDIO
- **Puerto**: 139/tcp, **Servicio**: netbios-ssn, **Versión**: Samba smbd 3.X - 4.X, **ID CVE**: CVE-2007-2447

Explicación: Samba tiene una vulnerabilidad de inyección de comandos que permite a atacantes remotos ejecutar comandos arbitrarios mediante un paquete manipulado.
Severidad: V4.0: 9.8 CRÍTICO, V3.x: 9.0 CRÍTICO, V2.0: 7.5 ALTO

- **Puerto**: 445/tcp, **Servicio**: netbios-ssn, **Versión**: Samba smbd 3.0.20-Debian, **ID CVE**: CVE-2017-7494
  Explicación: Vulnerabilidad de ejecución remota de código en Samba que permite a los atacantes cargar y ejecutar bibliotecas compartidas de forma remota.
  Severidad: V4.0: 10.0 CRÍTICO, V3.x: 9.8 CRÍTICO, V2.0: 7.5 ALTO
- **Puerto**: 512/tcp, **Servicio**: exec, **ID CVE**: N/A
  Explicación: No se encontró ninguna vulnerabilidad específica, pero ejecutar el servicio exec se considera un riesgo de seguridad, ya que puede usarse para la ejecución remota de comandos.
  Severidad: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Puerto**: 513/tcp, **Servicio**: login, **ID CVE**: N/A
  Explicación: El servicio login se utiliza comúnmente para el inicio de sesión remoto y es inherentemente arriesgado si no está asegurado. No hay vulnerabilidades específicas asociadas, pero el servicio en sí puede ser un vector de ataque.
  Severidad: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Puerto**: 514/tcp, **Servicio**: shell, **ID CVE**: N/A
  Explicación: Ejecutar el servicio rsh (shell remota) es altamente inseguro debido a la falta de cifrado. Es vulnerable a ataques de intermediarios (man-in-the-middle).
  Severidad: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Puerto**: 1099/tcp, **Servicio**: java-rmi, **Versión**: GNU Classpath grmiregistry, **ID CVE**: CVE-2011-3556
  Explicación: El registro RMI de Java puede permitir a atacantes remotos ejecutar código arbitrario o acceder a información sensible mediante ataques de deserialización.
  Severidad: V4.0: 9.8 CRÍTICO, V3.x: 9.0 CRÍTICO, V2.0: 7.5 ALTO
- **Puerto**: 1524/tcp, **Servicio**: bindshell, **Versión**: Metasploitable root shell, **ID CVE**: N/A
  Explicación: Un backdoor conocido instalado en la máquina Metasploitable, que permite acceso root a atacantes remotos.
  Severidad: V4.0: N/A, V3.x: N/A, V2.0: N/A (Backdoor)
- **Puerto**: 2049/tcp, **Servicio**: nfs, **Versión**: 2-4 (RPC #100003), **ID CVE**: CVE-2018-16871
  Explicación: Las comparticiones NFS pueden ser vulnerables al acceso no autorizado si no están configuradas correctamente, permitiendo a los atacantes montar directorios compartidos y acceder a archivos sensibles.
  Severidad: V4.0: 7.5 ALTO, V3.x: 6.5 MEDIO, V2.0: 5.0 MEDIO

- **Puerto**: 2121/tcp, **Servicio**: ccproxy-ftp, **ID CVE**: N/A
  Explicación: No se encontró ninguna vulnerabilidad específica. Sin embargo, exponer servicios FTP es inherentemente arriesgado debido a la transferencia de datos sin cifrar, lo que podría exponer las credenciales de inicio de sesión.
  Severidad: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Puerto**: 3306/tcp, **Servicio**: mysql, **ID CVE**: CVE-2012-2122
  Explicación: Vulnerabilidad de omisión de autenticación en MySQL que permite a los atacantes remotos autenticarse sin una contraseña válida.
  Severidad: V4.0: 7.5 ALTO, V3.x: 7.0 ALTO, V2.0: 5.0 MEDIO
- **Puerto**: 3632/tcp, **Servicio**: distccd, **Versión**: distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)), **ID CVE**: CVE-2004-2687
  Explicación: Vulnerabilidad de ejecución remota de código en el servicio distccd que permite a los atacantes ejecutar comandos arbitrarios de forma remota.
  Severidad: V4.0: 10.0 CRÍTICO, V3.x: 9.0 CRÍTICO, V2.0: 7.5 ALTO
- **Puerto**: 5432/tcp, **Servicio**: postgresql, **Versión**: PostgreSQL DB 8.3.0 - 8.3.7, **ID CVE**: CVE-2007-0555
  Explicación: PostgreSQL tiene un defecto de validación de entrada que permite la escalada de privilegios, lo que podría permitir a los atacantes ejecutar código SQL arbitrario.
  Severidad: V4.0: 8.5 ALTO, V3.x: 7.8 ALTO, V2.0: 6.5 MEDIO
- **Puerto**: 5900/tcp, **Servicio**: vnc, **Versión**: VNC (protocolo 3.3), **ID CVE**: CVE-2011-2523
  Explicación: VNC permite a los atacantes omitir la autenticación y acceder a escritorios remotos.
  Severidad: V4.0: 7.5 ALTO, V3.x: 7.8 ALTO, V2.0: 5.0 MEDIO
- **Puerto**: 6000/tcp, **Servicio**: X11, **ID CVE**: CVE-1999-0526
  Explicación: El servicio X11 está expuesto y permite a atacantes remotos acceder al sistema gráfico sin autenticación.
  Severidad: V4.0: 9.8 CRÍTICO, V3.x: 9.0 CRÍTICO, V2.0: 7.5 ALTO
- **Puerto**: 6667/tcp, **Servicio**: irc, **Versión**: UnrealIRCd, **ID CVE**: CVE-2010-2075
  Explicación: Backdoor en UnrealIRCd permite a los atacantes remotos ejecutar comandos arbitrarios.
  Severidad: V4.0: 10.0 CRÍTICO, V3.x: 9.8 CRÍTICO, V2.0: 7.5 ALTO
- **Puerto**: 8009/tcp, **Servicio**: ajp13, **Versión**: Apache Jserv (Protocolo v1.3), **ID CVE**: CVE-2020-1938
  Explicación: El conector AJP en Apache Tomcat es vulnerable a ataques de inclusión de archivos, lo que permite a los atacantes leer archivos arbitrarios en el servidor.
  Severidad: V4.0: 7.5 ALTO, V3.x: 8.1 ALTO, V2.0: 6.5 MEDIO

Análisis del Impacto de las Vulnerabilidades

El impacto de las vulnerabilidades encontradas durante el proceso de escaneo es significativo, ya que muchas de ellas permiten la ejecución remota de código, acceso no autorizado o denegación de servicio (DoS). Estas brechas de seguridad podrían ser explotadas por atacantes externos, poniendo en riesgo la confidencialidad, integridad y disponibilidad de los datos en la red de la organización.

Por ejemplo, las vulnerabilidades detectadas en los servicios Samba y Apache expuestos en los puertos 139, 445 y 80 son particularmente críticas. La ejecución remota de código y la inyección de comandos pueden dar a los atacantes el control completo del sistema, lo que podría permitir la propagación de malware o ransomware, la exfiltración de datos sensibles, o el acceso no autorizado a recursos críticos.

Además, servicios como rpcbind, nfs, y vnc tienen vulnerabilidades que permiten ataques de denegación de servicio y exposición de información sensible, lo cual puede comprometer la operatividad de la red.

Las vulnerabilidades en servicios clave como MySQL y PostgreSQL, por su parte, representan riesgos importantes para las bases de datos, que podrían ser explotadas para manipular datos o interrumpir la integridad de las transacciones, afectando directamente las operaciones comerciales.

Mitigación

Para mejorar la seguridad de nuestra red, es crucial verificar y corregir cada una de las vulnerabilidades expuestas en los puntos anteriores. El proceso de mitigación debe priorizar aquellas vulnerabilidades clasificadas como críticas, ya que son las que presentan mayor riesgo para la empresa.

Aplicación de Actualizaciones y Parches: Es fundamental mantener los servicios y sistemas operativos actualizados con las versiones más recientes. Servicios como Apache, Samba, y MySQL deben ser actualizados a versiones que ya no sean vulnerables a ataques de ejecución remota de código o inyección de comandos.

Restricción de Acceso: Para minimizar el riesgo de explotación, se recomienda aplicar listas de control de acceso (ACL) para limitar qué direcciones IP pueden interactuar con servicios críticos como NFS, MySQL y PostgreSQL. Además, la segmentación de la red puede reducir la exposición de servicios sensibles a atacantes externos.

Deshabilitación de Servicios Innecesarios: Servicios como **exec**, **login**, y **rsh** deben ser deshabilitados si no son necesarios, ya que presentan riesgos significativos debido a su falta de cifrado y vulnerabilidad a ataques de intermediarios (man-in-the-middle).

Configuración Segura de los Servicios: Los servicios de red como **Samba** y **Apache** deben configurarse correctamente, asegurando que los permisos de archivo y las políticas de acceso sean adecuadas. Deshabilitar características innecesarias como **Directory Indexing** en Apache y restringir el acceso a phpMyAdmin son buenas prácticas de seguridad.

Monitoreo Continuo: Implementar herramientas de monitoreo en tiempo real que permitan detectar actividades sospechosas o intentos de explotación de vulnerabilidades es clave para mantener una seguridad proactiva. Servicios como VNC y RPC deberían ser monitorizados constantemente.