Informe de Pentesting - Fase 2: Detección y Explotación

Objetivo: Escanear, detectar y explotar vulnerabilidades localizadas, lograr el compromiso total del sistema y aplicar medidas estrictas de corrección, incluyendo el cierre de puertos innecesarios.

Índice (Tabla de Contenido)

1. Detección y Proceso de Explotación (Paso 2 y 3)

1.1. Vector de Ataque: Escaneo y Servicios Expuestos

El proceso de reconocimiento inicial (escaneo con Nmap) reveló que el servidor Debian tenía los siguientes puertos TCP abiertos, lo que inmediatamente incrementó la superficie de ataque:

Puerto	**Servicio Detectado**	**Versión**	**Riesgo de Seguridad**
22/TCP	**SSH**	OpenSSH 9.2p1 Debian	**Alto**. Permite acceso remoto al sistema. Cualquier debilidad en la autenticación (como la credencial por defecto) o en la configuración de *root* lleva al compromiso total.
80/TCP	**HTTP**	Apache httpd 2.4.57	**Medio-Alto**. Aloja la plataforma web

			(WordPress). Vulnerable a ataques a la aplicación (Inyección SQL, XSS) o a fallos de configuración del servidor (como el Listado de Directorios, explotado en la Fase 1).

Explotación del Puerto 22 (SSH):

Detalle	**Observación**	**Evidencia**
Vulnerabilidad	Uso de **credenciales por defecto** (debian:debian).	Credencial débil
Proceso de Explotación	Se resolvió el error de cambio de *host key* y se accedió mediante la credencial débil.	SSH Login
Resultado	Se obtuvo una *shell* de bajo privilegio como el usuario debian.	debian@debian:~$

Proceso de Explotación: Listado de Directorios y LPE

La explotación se centró en la combinación de credenciales débiles, escalada de privilegios y una configuración laxa del servidor web:

1. **Explotación de Listado de Directorios (Apache Misconfiguration)**:
   - **Acceso (Vector Web):** Al intentar acceder a la ruta /wp-content/uploads/ sin un archivo índice (como index.html), el servidor Apache, al tener activa la directiva **Options Indexes** por defecto, respondió mostrando el **contenido completo del directorio** .
   - **Consecuencia:** Esto expuso la estructura interna de los archivos subidos, permitiendo la enumeración de archivos de *uploads*, lo cual es un riesgo significativo de divulgación de información.

¿Por qué estas vulnerabilidades son peligrosas?

- **SSH (Puerto 22):** Es la puerta de administración. Si un atacante encuentra una debilidad (como la credencial por defecto), obtiene acceso directo al sistema operativo sin tener que pasar por fallos de la aplicación web. El compromiso del puerto 22 suele ser la ruta más directa al control total del sistema.
- **HTTP (Puerto 80):** Al exponer Apache y WordPress, el atacante tiene acceso a la aplicación más compleja, que a menudo contiene vulnerabilidades de inyección RCE, inyección SQL o, como se encontró previamente, fallos de configuración que exponen directorios sensibles.

1.2. Escalada de Privilegios Local (LPE)

El usuario debian poseía permisos inadecuados que permitieron la elevación a root.

Detalle	Observación	Evidencia
Vulnerabilidad	El usuario debian pertenece al grupo sudo.	Comando id
Proceso de LPE	Se utilizó el binario sudo para ejecutar la *shell* con privilegios de root.	Ejecución sudo su
Resultado Final	Control total del sistema.	root@debian:/home/debian #

2. Medidas Correctivas (Paso 4: Hardening)

Se aplicaron medidas para corregir la vulnerabilidad de acceso explotada (SSH Inseguro) y para asegurar la vulnerabilidad HTTP anterior (Listado de Directorios).

2.1. Hardening del Firewall (Cierre de Puertos con iptables)

Para cumplir con la directiva de **cerrar puertos innecesarios/restringir accesos**, se implementó una política estricta de *firewall* con iptables, denegando por defecto todas las nuevas conexiones entrantes.

Comando Ejecutado	Descripción Técnica	Propósito de Seguridad
iptables -F	Limpia todas las reglas existentes en todas las	Asegura que las reglas antiguas (como las

	cadenas.	específicas DROP/ACCEPT) se eliminen.
iptables -X	Elimina las cadenas personalizadas (si existen).	Limpieza completa del entorno de iptables.
iptables -P INPUT DROP	**Establece la política por defecto de la cadena INPUT a DROP.**	**Restricción al puerto 22 (SSH)** y cualquier otro puerto no especificado. Máxima restricción de acceso.
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT	Acepta paquetes que pertenecen a una conexión ya establecida o relacionada.	Permite que las sesiones activas y las respuestas a solicitudes salientes sigan funcionando.
iptables -A INPUT -i lo -j ACCEPT	Acepta todo el tráfico en la interfaz de *loopback* (lo).	Necesario para la comunicación interna y salud del sistema.
iptables -A INPUT -p tcp --dport 80 -j ACCEPT	Acepta nuevas conexiones entrantes en el puerto 80 (HTTP).	Mantiene el servicio web de WordPress (Apache) accesible.

2.2. Correcciones de Autenticación y Permisos

Corrección	**Comando Ejecutado**	**Detalle de la Medida**
Credenciales Débiles	passwd debian	Se cambió la contraseña del usuario debian por una robusta, eliminando el vector de acceso inicial.
Listado de Directorios	echo "Options -Indexes" > /var/www/html/wp-content/uploads/.htaccess	Se creó el archivo de configuración .htaccess para deshabilitar la función Options Indexes, previniendo la visualización de archivos en la carpeta de *uploads* de WordPress.

3. Conclusión

La Fase 2 resultó en el compromiso total del sistema debido a la combinación de credenciales débiles y escalada de privilegios a través de sudo. Las medidas correctivas se aplicaron con éxito, cerrando el acceso externo a servicios sensibles (SSH) mediante una política estricta de iptables y asegurando la configuración del servidor web Apache, mitigando el riesgo de re-explotación.