**Plan de Respuesta a Incidentes de Seguridad según NIST SP 800-61**

1. **Identificación**

La fase de identificación es crucial para detectar de manera oportuna cualquier indicio de un incidente de seguridad y reducir su impacto. En esta fase, el equipo debe ser capaz de distinguir entre actividades normales del sistema y potenciales ataques.

Procedimientos de Identificación:

1. Uso de Herramientas de Monitoreo:

- Implementar herramientas de detección de intrusiones y monitoreo continuo, como Nmap, Lynis, Nessus, chkrootkit y rkhunter.

- Justificación: Estas herramientas permiten supervisar constantemente los servicios, puertos y vulnerabilidades activas, generando alertas automáticas si se detecta una actividad fuera de lo común.

- Ejemplo: Configurar escaneos automáticos con Nessus para evaluar vulnerabilidades en la red y correlacionar estos datos con registros de auditoría del sistema.

2. Supervisión de Registros:

- Revisar los registros de seguridad, eventos y auditoría de sistemas y aplicaciones para detectar patrones inusuales o eventos anómalos, como intentos de acceso fallidos y cambios en los permisos de archivos.

- Justificación: Supervisar registros permite identificar incidentes en tiempo real y proporciona datos precisos sobre las vulnerabilidades y actividades sospechosas.

- Ejemplo: Implementar una herramienta de administración de registros (como Splunk) para consolidar y analizar eventos de seguridad en tiempo real.

3. Evaluación del Impacto y Priorización de Amenazas:

- Clasificar las amenazas según su posible impacto en el sistema y su criticidad, considerando los servicios comprometidos y su importancia.

- Justificación: La priorización de amenazas permite enfocar los recursos en las más críticas y reducir el riesgo de impactos mayores.

- Ejemplo: Crear una tabla de clasificación para priorizar las amenazas basándose en factores como disponibilidad del servicio, confidencialidad y criticidad de los datos.

2. Contención

La fase de contención tiene como objetivo limitar el alcance y el impacto del incidente una vez detectado, permitiendo la recuperación sin que el daño se extienda al resto del sistema.

**Contención Inmediata y a Largo Plazo:**

1. Medidas de Contención Inmediata:

- Configuración del Firewall (UFW): Activar reglas de firewall estrictas para bloquear conexiones no esenciales, permitiendo solo el acceso a servicios críticos desde IPs específicas.

- Justificación: Un firewall correctamente configurado evita la propagación del incidente y restringe el acceso a servicios sensibles mientras se evalúa la amenaza.

- Ejemplo: Configurar UFW para aceptar solo conexiones seguras por SSH y denegar accesos a servicios como FTP (Puerto 21).

2. Aislamiento de la Máquina Comprometida:

- Desconectar de la red cualquier dispositivo afectado para evitar la propagación lateral del ataque.

- Justificación: Aislar el dispositivo comprometido es fundamental para contener el daño mientras se investiga la magnitud del incidente.

- Ejemplo: Usar una red de pruebas aislada o una VLAN para realizar el análisis sin exponer otros sistemas.

3. Contención a Largo Plazo:

- Restricciones de Acceso a SSH: Deshabilitar temporalmente el acceso SSH al sistema afectado o implementar autenticación de dos factores (2FA).

- Justificación: Una autenticación más robusta minimiza la posibilidad de accesos no autorizados durante y después del incidente.

- Ejemplo: Configurar SSH para aceptar solo autenticación por clave y restringir accesos a IPs específicas en el archivo sshd\_config.

4. Evaluación de los Sistemas de Soporte:

- Revisar los sistemas de respaldo o almacenamiento conectados para verificar que no hayan sido comprometidos.

- Justificación: Asegurarse de que los sistemas de respaldo están seguros evita que el atacante use estos recursos para expandirse o recuperar acceso.

- Ejemplo: Auditar accesos y permisos en dispositivos de almacenamiento y respaldos conectados a la red comprometida.

3. Erradicación

En esta etapa se eliminan todos los rastros dejados por el atacante y se reparan las configuraciones o aplicaciones vulnerables. La erradicación garantiza que el sistema recupere su estado seguro original.

**Pasos de Erradicación:**

1. Eliminación de Artefactos Maliciosos:

- Realizar un escaneo exhaustivo para detectar archivos, procesos y configuraciones introducidos por el atacante y proceder a su eliminación.

- Justificación: La eliminación de rastros de malware es clave para evitar reactivaciones o retenciones de acceso por parte del atacante.

- Ejemplo: Usar herramientas como rkhunter y chkrootkit para identificar rootkits o procesos sospechosos que podrían haber sido introducidos.

2. Actualización de Aplicaciones y Sistemas Vulnerables:

- Actualizar software, aplicaciones y configuraciones a sus versiones más recientes para cerrar posibles brechas.

- Justificación: Mantener los servicios en sus versiones más seguras ayuda a evitar la explotación de la misma vulnerabilidad en futuros ataques.

- Ejemplo: Actualizar Apache, WordPress y MySQL a versiones recientes y configurarlos para restringir accesos públicos.

3. Revisión de Configuraciones de Seguridad:

- Ajustar configuraciones de seguridad en servicios críticos, asegurando permisos y autenticación adecuados en rutas de administración y servicios de red.

- Justificación: Configuraciones de seguridad sólidas reducen la posibilidad de que la vulnerabilidad vuelva a ser explotada.

- Ejemplo: Configurar Apache para permitir accesos a directorios de administración solo mediante autenticación estricta o IP autorizadas.

4. Prueba de Validación de Seguridad:

- Realizar pruebas adicionales para asegurar que todas las fallas han sido eliminadas y que el sistema es seguro.

- Justificación: Validar las configuraciones corregidas asegura la seguridad del sistema y confirma que no existen puertas traseras.

- Ejemplo: Ejecutar un escaneo de seguridad completo con Nessus para confirmar que no hay vulnerabilidades restantes.

4. Recuperación

La fase de recuperación consiste en restaurar el sistema a un estado seguro y funcional, asegurando que los servicios comprometidos operen correctamente y bajo estrictas medidas de seguridad.

Pasos de Recuperación:

1. Restauración de Sistemas y Servicios:

- Reiniciar y verificar servicios críticos tras confirmar que las configuraciones están libres de problemas y que el sistema ha sido restaurado por completo.

- Justificación: Reiniciar los servicios permite que el sistema vuelva a operar normalmente, minimizando la interrupción para los usuarios.

- Ejemplo: Verificar la integridad de servicios como HTTP, MySQL y SSH antes de habilitarlos para el público.

2. Verificación de Integridad del Sistema:

- Realizar auditorías de integridad de datos y configuración para asegurar que no queden restos del ataque o archivos comprometidos.

- Justificación: Validar la integridad del sistema asegura que no quedan residuos del ataque y que el sistema seguirá siendo seguro.

- Ejemplo: Usar herramientas como Tripwire para verificar la integridad de archivos y configuraciones clave del sistema.

3. Revisión de Accesos y Permisos:

- Implementar permisos más estrictos en servicios comprometidos y reducir accesos innecesarios.

- Justificación: Limitar permisos y accesos disminuye las probabilidades de futuras amenazas y refuerza la seguridad del sistema.

- Ejemplo: Configurar MySQL para aceptar solo conexiones locales y restringir el acceso a SSH a IPs específicas.

4. Generación de Informe de Recuperación:

- Documentar todo el proceso, incluyendo hallazgos, medidas de contención, erradicación y acciones de recuperación.

- Justificación: Un informe completo permite llevar un registro de las acciones y facilita la evaluación de la respuesta a incidentes.

- Ejemplo: Preparar un informe detallado con lecciones aprendidas, recomendaciones y ajustes para fortalecer el plan de respuesta a incidentes.

Este plan proporciona una respuesta completa y estructurada, siguiendo el marco NIST SP 800-61, para gestionar futuros incidentes con una estrategia clara y efectiva que proteja los activos y la información de la organización.