Gestión Integral de un Incidente Crítico de Seguridad

Fase 1: Detección y análisis forense inicial

En esta primera fase, se realiza una inspección detallada del sistema en busca de signos de compromiso. Se analizan los registros del sistema, los procesos activos y cualquier modificación reciente que pudiera indicar una intrusión.

• Revisión de logs del sistema:

Se examinan los siguientes archivos y comandos:

```
cat /var/log/syslog
cat /var/log/auth.log
ls -l /var/log/apache2/
journalctl -xe
```

Se buscan entradas inusuales, intentos de acceso fallidos o conexiones desde direcciones IP no habituales.

• Búsqueda de Indicadores de Compromiso (IoC):

- IPs repetitivas con múltiples accesos fallidos.
- Presencia de scripts o binarios en directorios temporales como `/tmp` o `/dev/shm`.
- Usuarios nuevos o modificaciones en `/etc/passwd`.

• Herramientas de análisis del sistema:

```
who          # Usuarios conectados
last         # Historial de accesos
netstat -tulpn   # Conexiones de red
ss -antp         # Estado de sockets
lsof             # Archivos abiertos por procesos
```

Estas herramientas ayudan a reconstruir qué ocurrió y cuándo.

Fase 2: Aislamiento y preservación de la evidencia

Una vez identificado el compromiso, es crítico contener la amenaza y conservar la información para un análisis forense adecuado.

• Desconexión del servidor de la red:

Esto evita la propagación del ataque o la pérdida de información.

```
sudo ip link set eth0 down
sudo ufw default deny incoming
sudo ufw default deny outgoing
```

• Copia de seguridad forense del disco:

```
sudo dd if=/dev/sda of=/mnt/evidencia/disco.img bs=4M
status=progress
```

También puede usarse `dcfldd` o herramientas como Clonezilla.

• Montar la copia en modo sólo lectura:

```
sudo mount -o ro,loop /mnt/evidencia/disco.img /mnt/analisis
```

• Verificación de integridad con SHA256:

```
sha256sum /mnt/evidencia/disco.img
```

Este hash se conserva para validar que no haya sido alterada la evidencia digital.

Fase 3: Análisis profundo del ataque y cronología

En esta fase se profundiza en la naturaleza del ataque, buscando malware, técnicas de persistencia y la secuencia de acciones realizadas por el atacante.

• Análisis del entorno con herramientas de detección:

```
sudo apt install chkrootkit rkhunter clamav
sudo chkrootkit
sudo rkhunter --check
sudo clamscan -r /
```

• Búsqueda de persistencia maliciosa:

Se revisan archivos como:

- `~/.bashrc`, `~/.bash_profile`
- `/etc/crontab`, `cron.d/`
- `/etc/rc.local`

• Línea de tiempo del ataque:

Se construye con ayuda de:

```
stat archivo
ls -lt /etc/
```

y combinando timestamps obtenidos de logs para identificar el momento exacto de la intrusión y sus consecuencias.

• Detección de escalada de privilegios:

Revisar si el atacante pasó de usuario normal a root mediante logs, permisos alterados o comandos ejecutados.

Fase 4: Erradicación y reconstrucción del entorno

Tras entender el ataque, se eliminan todos los elementos sospechosos y se restaura el sistema a un estado limpio y seguro.

• Eliminar elementos comprometidos:

```
sudo deluser atacante
sudo rm -rf /tmp/malware
```

• Reinstalar servicios clave:

```
sudo apt purge apache2
sudo apt install apache2
```

• Aplicar medidas de refuerzo inmediatas:

- Modificar `/etc/ssh/sshd_config` para restringir accesos.
- Instalar `fail2ban` para proteger el SSH:

```
sudo apt install fail2ban
```

- Cambiar todas las contraseñas y claves afectadas.

• Aplicar actualizaciones:

```
sudo apt update && sudo apt upgrade
```

Es fundamental que el sistema y todas las aplicaciones estén parcheadas contra vulnerabilidades conocidas.

Fase 5: Reforzamiento y respuesta futura

Esta fase tiene como objetivo prevenir futuros ataques similares y mejorar la capacidad de respuesta ante incidentes.

• Activar autenticación en dos factores (2FA):

Especialmente en accesos SSH o VPN.

• Segmentación de red:

Separar servidores críticos de redes de usuarios mediante VLANs o firewalls internos para limitar movimientos laterales.

• Instalar un IDS como OSSEC o Wazuh:

```
curl -s https://packages.wazuh.com/install.sh | bash
```

Estas herramientas monitorizan eventos sospechosos y generan alertas en tiempo real.

• Crear un playbook de respuesta a incidentes:

Debe incluir:

- Checklist de pasos a seguir.
- Roles asignados por cada fase (detección, análisis, respuesta, recuperación).
- Herramientas recomendadas.
- Tiempos de actuación esperados según la criticidad.