Investigación Forense de un Incidente

Fase 1: Identificación y recolección de evidencias

En esta primera fase se busca asegurar toda la información útil que pueda servir como evidencia del incidente de seguridad. Es fundamental recopilar los datos lo antes posible para evitar su alteración o pérdida.

• Revisión de logs del sistema:

En sistemas Linux se consultan los archivos:

```
cat /var/log/auth.log
cat /var/log/syslog
```

En sistemas Windows, se utiliza el **Visor de eventos (Event Viewer)** para revisar registros de seguridad, sistema y aplicaciones.

• Análisis de usuarios conectados y procesos:

En Linux:

```
who
ps aux
```

En Windows:

```
tasklist
query user
```

Estos comandos permiten identificar usuarios activos y procesos potencialmente sospechosos.

• Conexiones de red activas:

En Linux:

```
netstat -tulnp
ss -tulnp
```

En Windows:

```
netstat -ano
```

Sirven para descubrir conexiones remotas activas, puertos abiertos y servicios escuchando.

• Volcado de memoria RAM:

En sistemas Linux:

```
sudo apt install linux-crashdump
sudo makedumpfile /dev/mem /root/dump.mem --dump-dmesg
```

En sistemas Windows se puede usar **FTK Imager**, **Belkasoft RAM Capturer** u otras herramientas para capturar y analizar la memoria.

Fase 2: Análisis del incidente y detección del atacante

Una vez recolectada la información, se realiza un análisis para identificar al atacante y los pasos que siguió durante el ataque.

• Identificación de IP y métodos de ataque:

Revisando los registros de logs se detectan direcciones IP sospechosas que han realizado múltiples accesos fallidos o conexiones inusuales.

• Revisión de modificaciones del sistema:

Se comprueba si se han creado usuarios nuevos o si se han modificado archivos clave como:

```
ls -lt /etc/passwd
cat /etc/sudoers
```

• Ejecución de comandos maliciosos:

Revisión de historiales (`~/.bash_history`) o procesos que ejecutan scripts desde directorios como `/tmp`.

• Búsqueda de puertas traseras (backdoors):

Comprobación de conexiones persistentes, scripts en crontab o binarios sospechosos en rutas no habituales. También se inspeccionan servicios instalados recientemente o configuraciones alteradas.

Fase 3: Extracción y análisis de archivos sospechosos

Se procede a recuperar, analizar y evaluar los archivos que puedan haber sido utilizados durante el incidente o eliminados posteriormente.

• **Recuperación de archivos eliminados:**

En Linux se pueden utilizar:

```
sudo apt install foremost
foremost -i /dev/sda1 -o /root/recovery
```

En Windows, herramientas como **Recuva** permiten escanear y restaurar archivos borrados.

• **Análisis de scripts o ejecutables:**

Todos los archivos sospechosos recuperados deben ser analizados manualmente o con herramientas de escaneo como **ClamAV** o entornos de análisis como **VirusTotal**.

• **Análisis de tráfico de red con Wireshark:**

Si se dispone de un volcado de red (`.pcap`), se puede inspeccionar la comunicación entre el equipo afectado y servidores externos:

```
wireshark
```

Esto permite detectar intentos de exfiltración de datos o conexiones con servidores de comando y control.

Fase 4: Aplicación de medidas de seguridad

Con toda la información recopilada, se aplican medidas correctivas y preventivas para evitar futuros incidentes similares.

• Deshabilitar cuentas comprometidas:

```
sudo usermod -L usuario
sudo passwd -l usuario
```

También se cambian todas las contraseñas, claves SSH y credenciales que hayan podido verse comprometidas.

• Configurar firewall con reglas estrictas:

```
sudo ufw default deny incoming
sudo ufw allow ssh
```

En Windows se deben revisar reglas del Firewall de Windows Defender.

• Implementar autenticación multifactor (2FA):

Se recomienda integrar soluciones de autenticación en dos pasos en accesos SSH, VPN, paneles web y servicios administrativos.

• Monitoreo avanzado con IDS:

Instalación y configuración de sistemas de detección de intrusos como:

```
sudo apt install snort
sudo apt install suricata
```

Estos sistemas permiten detectar patrones de ataque y generar alertas automáticas ante eventos sospechosos.