Detección, Análisis y Eliminación de Malware

Fase 1: Identificación y detección del malware

En esta fase se busca reconocer la presencia del malware en el sistema, identificando procesos y comportamientos sospechosos.

• Análisis de procesos activos:

En Linux:

```
top
ps aux
```

En Windows:

```
tasklist
```

Estos comandos permiten identificar procesos que consumen muchos recursos, tienen nombres extraños o rutas poco comunes.

• Escaneo de malware:

En Linux:

```
sudo apt install clamav
sudo freshclam
sudo clamscan -r /home
```

En Windows se utiliza **Malwarebytes** u otro antivirus avanzado para hacer un escaneo profundo del sistema.

• Revisión de logs del sistema:

En Linux:

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

En Windows se revisa el **Visor de eventos** buscando errores de seguridad, ejecución de scripts y cambios no autorizados.

• Conexiones de red abiertas:

En Linux:

```
ss -tulnp
```

En Windows:

```
netstat -ano
```

Estas herramientas permiten detectar conexiones anómalas a servidores remotos o intentos de escucha en puertos no autorizados.

Fase 2: Análisis del malware y evaluación del impacto

Una vez detectada su presencia, se analiza el comportamiento del malware y se determina su tipo y alcance dentro del sistema.

• Detección de archivos afectados:

Se buscan archivos modificados, cifrados con extensiones extrañas o eliminados recientemente mediante herramientas de logs o comandos como:

```
find /home -mtime -1
```

• Clasificación del malware:

Según el comportamiento observado, se identifica si se trata de:

- **Ransomware**: Cifra archivos.
- **Spyware**: Roba datos o contraseñas.
- **Rootkit**: Oculta procesos y accesos.
- **Virus/Troyano**: Infecta y replica código.

• **Hashes y análisis en VirusTotal:**

```
sha256sum archivo_sospechoso
```

El hash se puede subir a www.virustotal.com para ver si el archivo es reconocido por motores antivirus.

• **Análisis de código malicioso:**

```
strings archivo_sospechoso
hexedit archivo_sospechoso
```

Estas herramientas permiten ver textos incrustados, posibles URLs, comandos incrustados o llamadas al sistema.

Fase 3: Eliminación del malware y recuperación del sistema

El objetivo aquí es erradicar completamente el malware y restaurar la funcionalidad del sistema.

• **Detener procesos maliciosos:**

En Linux:

```
kill -9 PID
```

En Windows:

```
taskkill /IM malware.exe /F
```

• **Eliminación segura de archivos:**

En Linux:

```
shred -u archivo_infectado
```

En Windows:

```
sdelete archivo_infectado
```

• Restauración desde copias de seguridad:

Se deben recuperar archivos críticos desde backups limpios previos al incidente.

• Verificación de limpieza:

Se analiza nuevamente el sistema con herramientas antivirus para asegurar que no quedan rastros del malware.

Fase 4: Implementación de medidas de protección

Tras eliminar el malware, se implementan medidas de defensa para reducir el riesgo de reinfección.

• Activar antivirus en todos los equipos:

Verificar que cada equipo tenga un sistema de protección activo y actualizado.

• Aplicación de listas blancas (whitelisting):

Permitir únicamente la ejecución de programas previamente autorizados.

• Refuerzo de reglas de firewall:

En Linux:

```
sudo ufw deny out to any port 4444
```

En Windows:

Usar el Firewall avanzado para bloquear conexiones salientes hacia puertos o IPs maliciosas.

• Autenticación multifactor (2FA):

Habilitar 2FA en accesos remotos, correo electrónico, VPN y paneles administrativos.

• Políticas de acceso reforzadas:

- Prohibir el uso de cuentas sin contraseña.
- Limitar privilegios administrativos.
- Registrar todos los accesos.