✅ Checklist - Análisis Estático de Malware

## 1. Identificar la arquitectura de destino del malware

☐ Renombrar la muestra si tiene un nombre genérico o engañoso (ej. invoice.pdf.exe → malware\_sample.exe).

## 2. Tomar huellas dactilares del malware

☐ Obtener hash de la muestra (MD5, SHA1, SHA256).

☐ Herramientas: md5sum, sha256sum (Linux), HashMyFiles, Get-FileHash (Windows).

## 3. Escanear el binario sospechoso con motores antivirus

## 4. Detección de empaquetado / protección

☐ Usar herramientas como DIE, PEiD, RDG Packer Detector.

☐ Buscar pocas importaciones, secciones UPX o no estándar, diferencias entre VirtualSize y RawSize.

☐ Intentar desempaquetar con upx -d malware.exe.

☐ Si no se puede, preparar para análisis dinámico.

## 5. Identificación de ofuscación

☐ Buscar saltos inusuales (jmp, call).

☐ Verificar flujos difíciles de seguir (opaque predicates, anti-disassembly).

☐ Detectar API hashing.

## 6. Detección de técnicas anti-análisis

☐ Uso de IsDebuggerPresent, CheckRemoteDebuggerPresent.

☐ Verificación de procesos: procmon, wireshark, idaq.exe, etc.

☐ Buscar llamadas: NtQueryInformationProcess, RDTSC, GetTickCount.

## 7. Extraer cadenas y metadatos

☐ Extraer cadenas imprimibles (URLs, rutas, claves, etc.).

☐ Herramientas: exiftool, binwalk, trid.

## 8. Funciones/APIs utilizadas

☐ Revisar tabla de importación (IAT): CreateRemoteThread, VirtualAlloc, etc.

☐ Revisar tabla de exportación: ¿exporta funciones? ¿Simula ser una DLL?

## 9. Tamaño y análisis de la estructura PE

☐ Revisar headers: IMAGE\_DOS\_HEADER, IMAGE\_NT\_HEADERS.

☐ Comprobar nombres de secciones (.text, .data, .rsrc, .UPX, etc.).

☐ Comparar VirtualSize vs RawSize.

☐ Revisar permisos: R, W, X.

☐ Detectar secciones vacías o con overlays.

☐ Herramientas: PE-bear, PEview, CFF Explorer, pefile, DIE.

## 10. Desensamblado y descompilado

☐ Usar Ghidra, IDA Free, Binary Ninja, Cutter + radare2.

☐ Buscar rutinas de cifrado (XOR, ADD, ROR, etc.).

☐ Buscar llamadas a funciones clave: CreateProcess, LoadLibrary, etc.

## 11. Análisis de recursos embebidos

☐ Extraer iconos, DLLs, configuraciones C2.

☐ Herramientas: Resource Hacker, PE Explorer, rcedit, exiftool.

## 12. Análisis de firmas y YARA

☐ Buscar coincidencias con reglas YARA: yara -r rules.yar malware.exe.

☐ Comparar en VirusTotal, HybridAnalysis, Intezer.

☐ Usar reglas públicas (TheZoo, Malpedia).

## 13. Clasificación y comparación de muestras de malware

## 14. Mapeo y documentación