

حل التحدي 2

1. تحليل الملف المشبوه

أدوات التحليل:

- **VirusTotal**: لفحص الملف ضد قواعد بيانات متعددة للبرمجيات الضارة.
- **Sandboxing** (مثل **Cuckoo Sandbox**): لتشغيل الملف في بيئة معزولة ومراقبة سلوكه.
- **Wireshark**: لتحليل حركة الشبكة الناتجة عن تشغيل الملف.
- **Process Monitor (ProcMon)**: لمراقبة العمليات والملفات التي يحاول البرنامج الوصول إليها.
- **IDA Pro** أو **Ghidra**: لتحليل الشيفرة الثابتة وفك تجميع الملف.

2. تحديد نوع البرمجية الضارة

أنواع البرمجيات الضارة:

- **فيروس**: يلتصق بملفات أخرى وينتشر عند تشغيل هذه الملفات.
- **دودة**: تنتشر عبر الشبكة دون الحاجة إلى ملف مضيف.
- **تروجان**: يتظاهر بأنه برنامج شرعي ولكنه ينفذ أنشطة ضارة.
- **برنامج فدية**: يشفر الملفات ويطلب فدية لفك التشفير.

كيفية التعرف:

- **الفيروس**: يبحث عن سلوكيات مثل تعديل ملفات النظام أو نسخ نفسه إلى ملفات أخرى.
- **الدودة**: يراقب حركة الشبكة ومحاولات الاتصال بأجهزة أخرى.
- **التروجان**: يتحقق من الأنشطة الخلفية مثل فتح منافذ غير معتادة أو الاتصال بخوادم خارجية.
- **برنامج الفدية**: يراقب عمليات التشفير غير المصرح بها للملفات.

3. تحليل الشيفرة

البحث عن تعليمات مشبوهة:

- **الاتصالات الخارجية**: تعليمات الاتصال بخوادم خارجية.
- **التشفير**: استخدام مكتبات التشفير بشكل غير معتاد.
- **التنفيذ الذاتي**: تعليمات لإعادة تشغيل البرنامج أو نسخ نفسه.
- **التلاعب بالنظام**: تعليمات لتعديل ملفات النظام أو السجل.

4. طرق التخفيف

توصيات الحماية:

- **تحديث البرامج**: التأكد من أن جميع البرامج محدثة لتجنب الثغرات الأمنية.

- استخدام برامج مكافحة الفيروسات: تثبيت وتحديث برامج مكافحة الفيروسات بشكل دوري.
- التدريب والتوعية: تدريب الموظفين على التعرف على رسائل البريد الإلكتروني المشبوهة والملفات غير الموثوقة.
- النسخ الاحتياطي: إجراء نسخ احتياطي دوري للبيانات الهامة.
- تقييد الوصول: تقييد صلاحيات الوصول إلى الملفات والشبكة بناءً على الحاجة.

التقرير التحليلي

مقدمة:

- وصف الملف المشبوه: نوعه، حجمه، وتاريخ اكتشافه.

تحليل السلوك:

- نتائج الفحص باستخدام الأدوات: ما هي السلوكيات المشبوهة التي تم اكتشافها؟

تحديد النوع:

- نوع البرمجية الضارة: بناءً على السلوك والتحليل.

تحليل الشيفرة:

- التعليمات المشبوهة: تفاصيل التعليمات البرمجية التي تشير إلى سلوك ضار.

التوصيات:

- طرق الحماية: الإجراءات الموصى بها لحماية النظام والشبكة.