

سلسلة تحديات الأمن السيبراني الأسبوعية للطلاب المتوسطين والمحترفين.

التحدي الأسبوعي 2: تحليل البرمجيات الضارة

السيناريو:

لقد تم اكتشاف ملف مشبوه في شبكة المؤسسة، ويُعتقد أنه يحتوي على برنامج ضار. مهمتك هي تحليل هذا الملف لفهم سلوكه وطرق انتشاره وكيفية التخفيف من المخاطر.

المهمة:

قم بتحليل الملف المشبوه من أجل تحديد نوع البرنامج الضار وطرق الحماية منه.

تفاصيل التحدي:

- 1. تحليل الملف:**
 - افتراض أن لديك ملفًا بامتداد exe. أو doc. (يمكنك إنشاء مثال بسيط لهذا الغرض أو تحميل أحد ملفات malware التي تم التعرف عليها من خلال موقع theZoo). حاول التعرف على أي سلوك مشبوه للملف. اذكر أدوات التحليل التي يمكنك استخدامها.
- 2. تحديد نوع البرمجية الضارة:**
 - حاول تحديد نوع البرنامج الضار بناءً على سلوكه. هل هو فيروس، دودة، تروجان، أو برنامج فدية؟ اشرح كيف يمكن التعرف على هذا النوع من البرامج الضارة.
- 3. تحليل الشيفرة:**
 - إذا كان بإمكانك الوصول إلى الشيفرة المصدرة (مثلاً، من برنامج مفتوح المصدر أو شيفرة مشبوهة تم توفيرها لك)، قم بتحليل الشيفرة بحثاً عن أي تعليمات مشبوهة أو ممارسات غير آمنة. ما هي التعليمات البرمجية التي تشير إلى سلوك ضار؟
- 4. طرق التخفيف:**
 - بعد تحليل الملف وتحديد نوع البرمجية الضارة، قدم توصيات حول كيفية حماية الشبكة أو النظام من هذا النوع من الهجمات.

المطلوب:

- قم بإعداد تقرير تحليلي يوضح سلوك الملف، ونوع البرنامج الضار، وطرق الحماية الموصى بها.
- استخدم لغة واضحة ومنظمة عند تقديم النتائج.

التقييم:

- سيتم تقييمك بناءً على شمولية التقرير ووضوحه، وكذلك جودة الاقتراحات المقدمة لحماية النظام والشبكة.

تقرير تحليل البرمجيات الضارة

1. تحليل الملف المشبوه

تفاصيل الملف:

- اسم الملف: suspicious_file.exe
- الامتداد: .exe
- حجم الملف: 1.2 ميغابايت

أدوات التحليل:

- VirusTotal**: لتحليل الملف على الإنترنت باستخدام أكثر من 60 محرك كشف الفيروسات.
- Cuckoo Sandbox**: لتشغيل الملف في بيئة معزولة وتحليل سلوكه ديناميكياً.
- PEiD**: للكشف عن نوع الحماية المستخدمة في الملف (مثل الحماية من الهندسة العكسية).
- ProcMon**: لمراقبة العمليات والنشاطات الناتجة عن تشغيل الملف.
- Strings**: لاستخراج النصوص القابلة للقراءة من الملف، والتي قد تكشف عن سلوكيات مشبوهة.

سلوك الملف:

- محاولة إنشاء اتصال بشبكة خارجية.
- تعديل إعدادات السجل (Registry) لتفعيل التشغيل التلقائي.
- تحميل ملفات إضافية من الإنترنت.
- تنفيذ أوامر النظام مثل cmd.exe.

2. تحديد نوع البرمجية الضارة

استناداً إلى سلوك الملف، يمكن تصنيفه على أنه **تروجان**.

كيفية التعرف على التروجان:

- السلوك المتخفي**: لا يظهر كبرنامج ضار بوضوح، بل يتنكر كبرنامج شرعي.
- التواصل الخارجي**: يسعى لإرسال البيانات أو استقبال أوامر من المخترق.
- التأثير على النظام**: قد يتسبب في تدهور أداء النظام أو تسريب البيانات.

3. تحليل الشيفرة

يمكن تحليلها للبحث عن تعليمات مشبوهة، مثل:

- استخدام مكتبات الشبكة: مثل socket في Python.
- عمليات الإدخال/الإخراج: التي تتعلق بالتلاعب بالنظام (مثلاً، os.system).
- التلاعب بالسجل: عن طريق استخدام API مثل RegOpenKeyEx.

مثال على التعليمات البرمجية المشبوهة:

```
import socket
import os
```

```
# فتح اتصال مع خادم بعيد
(s = socket.socket
s.connect(('malicious-server.com', 12345))
```

```
# تنفيذ أمر نظام
os.system('cmd.exe /c dir')
```

4. طرق التخفيف

التوصيات لحماية الشبكة:

1. استخدام برامج مضادة للفيروسات: تحديثها بانتظام للكشف عن البرمجيات الضارة.
2. تطبيق مراقبة الشبكة: لمراقبة حركة البيانات والكشف عن الأنشطة المشبوهة.
3. تدريب المستخدمين: على كيفية التعرف على الملفات المشبوهة وعدم فتح الروابط أو المرفقات غير الموثوق بها.
4. تقييد الامتيازات: على الأنظمة لمنع البرمجيات الضارة من إجراء تغييرات على السجل أو الاتصال بالإنترنت.
5. استخدام جدران نارية: للحد من الاتصالات غير المصرح بها.

الخاتمة

هذا التقرير يوفر نظرة شاملة حول تحليل البرمجيات الضارة، بما في ذلك نوع البرنامج الضار وسلوكه، بالإضافة إلى اقتراحات لحماية الشبكة. يجب على المؤسسات تحديث استراتيجيات الأمان بشكل دوري لضمان سلامة أنظمتها.

اسم الطالبة / شهد عادل علي.

تخصص تقنية المعلومات