

تحدي الأسبوع ٢: تحليل البرمجيات الضارة

❖ السيناريو:

لقد تم اكتشاف ملف مشبوه في شبكة المؤسسة، ويعتقد 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:

♦ 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. (التحليل على النحو التالي):

✚ للقيام بتحليل شامل للملف، يمكننا الاعتماد على مجموعة من الأدوات:

✚ الأدوات المستخدمة:

✚ Virus Total: لتحليل الملف والتحقق من سجله لدى قواعد البيانات المختلفة. يمكن استخدامه لمعرفة ما إذا تم الإبلاغ عن هذا الملف كملف ضار سابقًا.

✚ PEiD و Exeinfo PE: لمعرفة ما إذا كان الملف مضغوطًا أو مشفرًا. قد يشير الضغط أو التشفير إلى محاولة من مطور البرمجية الضارة لإخفاء بعض المعلومات.

✚ IDA Pro أو Ghidra: لتحليل الشيفرة على مستوى منخفض وفك تجميع الملف، مما يتيح فهم كيفية عمله.

✚ Wireshark: لمراقبة حركة الشبكة إذا كان الملف يتصل بخادم خارجي أو يرسل بيانات، وهو ما قد يشير إلى تواصل مع خادم تحكم وتحكم (C&C)

♦ 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 (ويكون تحديد نوع البرمجية الضارة على النحو التالي):

بناءً على السلوك، يمكننا التعرف على نوع البرمجية الضارة، حيث أن لكل نوع سلوك مميز:

✚ الفيروسات: تلتصق عادةً بالملفات التنفيذية وتحاول الانتشار عبر نسخ نفسها في ملفات أخرى.

✚ الدودة: تحاول الانتشار عبر الشبكة والوصول إلى أنظمة أخرى، باستخدام بروتوكولات الشبكة.

✚ التروجان: يبدو كبرنامج عادي ولكنه يقوم بتنفيذ أنشطة ضارة في الخلفية، مثل سرقة المعلومات.

✚ برامج الفدية: تقوم بتشفير الملفات وتطلب فدية لفك التشفير.

♦ تحليل الشيفرة:

إذا كان بإمكانك الوصول إلى الشيفرة المصدرية (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؟ (ويكون البحث عن السلوكيات الضارة التالية):

- ✚ التواصل الشبكي المشبوه: يمكن البحث عن أوامر أو مكتبات تستخدم لإنشاء اتصال بخادم خارجي.
- ✚ التعديل على سجلات النظام (Registry): قد يكون الهدف هو تثبيت البرمجية الضارة لتعمل تلقائياً مع بدء تشغيل النظام.
- ✚ عمليات ضارة: مثل مراقبة نشاط المستخدم، سرقة كلمات المرور، أو تشفير الملفات.

♦ طرق التخفيف:

بعد تحليل الملف وتحديد نوع البرمجية الضارة، قدم توصيات حول كيفية حماية الشبكة أو النظام من هذا النوع من الهجمات. (تكون التوصيات على النحو التالي):

- ✚ تحديث برامج مكافحة الفيروسات باستمرار لضمان اكتشاف أي ملفات مشبوهة.
- ✚ إعداد الجدار الناري لمنع الوصول إلى عناوين خوادم مشبوهة خارجية ومنع أي اتصال غير مصرح به.
- ✚ التوعية الأمنية للمستخدمين: تجنب فتح الملفات من مصادر غير معروفة وعدم تحميل مرفقات مشبوهة.
- ✚ النسخ الاحتياطي المنتظم للبيانات لحماية المعلومات ضد برامج الفدية.
- ✚ مراقبة الشبكة باستخدام IDS/IPS (نظام كشف التسلل/نظام منع التسلل) للتحذير من أي نشاط غير طبيعي.

الاسم: صخر حامد عرب

طالب الدراسات العليا تخصص الامن السيبراني