تقرير حل تحدي FireEye Redline — TryHackMe

اسم الطالب: محمد حيدر مرشد ناصر المعمري

Task 1: Introduction — المقدمة

FireEye طوّرتها شركة (Digital Forensics) هي أداة تحليل جنائي رقمي **Redline**. تمنح المحلّل الأمني نظرة شاملة بزاوية 360 درجة على نقطة النهاية (Endpoint) المشبوهة، وذلك من خلال واجهة رسومية (GUI) سهلة الاستخدام. تحليل ملفات الذاكرة وهياكل الملفات المتعددة عبر.

لقطة الشاشة ١ — نظرة عامة على غرفة Redline وبداية التحدي

attachment:90bb0d32-69cf-4569-905e-87f0e37b222c:01-room-intro.jpg

ما الذي يمكن فعله باستخدام Redline؟

- جمع بيانات السجل (Registry) — لأجهزة Windows فقط
- جمع العمليات الجارية (Running Processes)
- جمع صور الذاكرة (Memory Images) — لما قبل Windows 10
- جمع سجل المتصفح (Browser History)
- البحث عن السلاسل المشبوهة (Suspicious Strings)
- وأكثر من ذلك بكثير!

إعداد البيئة الافتراضية

لإتمام التحدي، تم إعداد بيئة افتراضية تتضمن:

- **Attacker Machine**: جهاز المهاجم (AttackBox) — لتنفيذ العمليات
- **Lab Machine**: الجهاز المختبري — تم تشغيله والاتصال به عبر RDP

لقطة الشاشة ٢ — إعداد AttackBox وLab Machine وشرح بيئة Redline

attachment:fc583a03-5502-4091-9950-1b878b520df5:02-intro-environment.jpg

بيانات الاتصال بـ RDP:

الحقل	القيمة
Machine IP	10.10.90.149
Username	administrator
Password	letmein123!

لقطة الشاشة ٣ — تشغيل الجهاز المختبري وتفاصيل اتصال RDP

attachment:bf3ae533-fe96-4258-9f13-805e1d574e0e:03-lab-rdp-details.jpg

إجابة سؤال Task 1

س: أيّ شركة طوّرت أداة Redline؟
الجواب: FireEye

لقطة الشاشة ٤ — الإجابة الصحيحة لسؤال الشركة المطوّرة لـ Redline

attachment:0b1e9f8c-5906-4248-b6f3-bddce78d50ec:04-task1-fireeye-answer.jpg

---

Task 2: Data Collection — جمع البيانات

يوفّر Redline ثلاثة أساليب لجمع البيانات من نقطة النهاية:

1. **Standard Collector** — الجامع القياسي: الأسرع والأخف، يجمع البيانات الأساسية.

2. **Comprehensive Collector** — الجامع الشامل: يجمع أكبر قدر ممكن من البيانات.
3. **IOC Search Collector** — جامع IOC: يجمع البيانات استناداً إلى مؤشرات اختراق محددة (Domains, Hashes, IPs, Filenames...).

إجابات أسئلة Task 2

السؤال	الجواب
ما أسلوب الجمع الأسرع؟	`Standard Collector`
لتشغيل جمع دقيق بناءً على مؤشرات معروفة؟	`IOC Search Collector`
ما السكريبت المستخدم لبدء عملية الجمع؟	`RunRedlineAudit.bat`
أين يمكن العثور على بيانات الأقراص والأجزاء (Disks & Volumes)؟	`Disk Enumeration`
ما الاسم الافتراضي لملف نتيجة مسح Redline؟	`AnalysisSession1.mans`

لقطة الشاشة 0 — إجابات أسئلة جمع البيانات في Task 2

attachment:49c23faf-6193-42a5-8ef4-53b7f051a5d5:05-task2-collection-answers.jpg

---

Task 3: The Redline Interface — واجهة المستخدم

توفّر واجهة Redline رؤية تفصيلية لنقطة النهاية من خلال أقسام متعددة:

- **System Information**: معلومات النظام والمستخدمين المسجّلين
- **Processes**: العمليات الجارية وخصائصها
- **Network Connections**: الاتصالات الشبكية النشطة
- **File System**: هيكل نظام الملفات
- **Timeline**: الجدول الزمني للأحداث
- **Registry**: سجل نظام Windows

إجابة سؤال Task 3

س: أين في واجهة Redline يمكن عرض معلومات المستخدم المسجّل دخوله؟
الجواب: System Information

لقطة الشاشة ٦ — إجابة سؤال موضع معلومات المستخدم المسجّل دخوله

attachment:4dae2f8d-33ee-4d80-82be-854bd1620100:06-task3-interface-answer.jpg

---

🔬 Task 4: Standard Collector Analysis — تحليل الجامع القياسي

في هذه المرحلة، تم تحليل ملف الجلسة المُجمَّع بواسطة الأداة. كشف التحليل عن العناصر التالية:

نظام التشغيل المكتشف

Windows Server 2019 Standard — Build 17763

المهام المجدوَلة المشبوهة (Suspicious Scheduled Tasks)

تم اكتشاف مهمة مجدوَلة ضارة أنشأها المتسلل:

اسم المهمة المشبوهة: `MSOfficeUpdateFa.ke`
تنكّر المهاجم باستخدام اسم يحاكي عمليات تحديث Microsoft Office الشرعية.

الرسالة المخفية في المهمة

```
THM-p3R5IStENCe-m3Chani$m
```

تحليل سجلات الأحداث (Event Logs)

تم رصد حدث نظامي مشبوه بالتفاصيل التالية:

الخاصية	القيمة
Source Name	THM-Redline-User
Event Type	ERROR
Event ID	`546`
الرسالة	"Someone cracked my password. Now I need to rename my puppy-++-"

الملف الذي نزّله المتسلل

الخاصية	القيمة
URL المصدر	`https://wormhole.app/download-stream/gI9vQtChjyYAmZ8Ody0AuA`
المسار الكامل	`C:\Program Files (x86)\Windows Mail\SomeMailFolder\flag.txt`
محتوى الملف (Flag)	`THM{600D-C@7cH-My-FR1EnD}`

ملخص إجابات Task 4

السؤال	الجواب
نظام التشغيل	`Windows Server 2019 Standard 17763`
المهمة المجدوَلة المشبوهة	`MSOfficeUpdateFa.ke`
رسالة المهمة	`THM-p3R5IStENCe-m3Chani$m`
رقم الحدث Event ID	`546`
رسالة الحدث	`Someone cracked my password. Now I need to rename my puppy-++-`
URL تحميل الملف	`https://wormhole.app/download-stream/gI9vQtChjyYAmZ8Ody0AuA`
مسار الملف المنزّل	`C:\Program Files (x86)\Windows Mail\SomeMailFolder\flag.txt`
Flag	`THM{600D-C@7cH-My-FR1EnD}`

لقطة الشاشة ٨ — تفاصيل حدث النظام وملف التنزيل والـ Flag

attachment:c3a3db6a-d0f7-471f-bae7-c814d1c8cdb3:08-task4-event-download-flag.jpg

Task 5: IOC Search Collector — الكشف عن Keylogger

في هذه المرحلة، تم استخدام **IOC Search Collector** للبحث عن مؤشرات اختراق محددة مرتبطة بـ Keylogger مشبوه.

نتائج التحليل

تم اكتشاف Keylogger يتنكر باسم ملف شرعي!

الخاصية	القيمة
الاسم الحقيقي للملف	`psylog.exe`
الاسم الذي يتنكر به	`THM1768.exe`
مالك الملف	`WIN-2DET5DP0NPT\charles`
حجم الملف (بالبايت)	`35400`
مسار ملف IOC	`C:\Users\charles\Desktop\Keylogger-IOCSearch\IOCs\keylogger.ioc`

لقطة الشاشة ٩ — نتائج فحص IOC واكتشاف ملف Keylogger

attachment:f200395b-24ba-451e-9c10-bc9ab2ed900b:09-task5-keylogger.jpg

---

Task 6: IOC Search Collector Analysis — تحليل ملف ضار متقدم

تم تحليل ملف تنفيذي ضار تم اكتشافه عبر مطابقة مؤشرات IOC متعددة.

تفاصيل الملف الضار

الخاصية	القيمة
المسار الكامل (مع اسم الملف)	`C:\Users\Administrator\AppData\Local\Temp\8eJv8w2id6IqN85dfC.exe`
مسار المجلد	`C:\Users\Administrator\AppData\Local\Temp\`

الخاصية	القيمة
مالك الملف	`BUILTIN\Administrators`
النظام الفرعي (Subsystem)	`Windows_CUI`
مسار الجهاز (Device Path)	`\Device\HarddiskVolume2`
SHA-256 Hash	`57492d33b7c0755bb411b22d2dfdfdf088cbbfcd010e30dd8d425d5fe66adff4`

لقطة الشاشة ١٠ — مسار الملف المشبوه وخصائصه في تحليل IOC

attachment:fe651fff-43cd-4b62-b3b7-987f6cef1d56:10-task6-file-details.jpg

التعرف على الملف الحقيقي عبر Hash

بعد البحث عن Hash SHA-256 في قواعد بيانات التهديدات، تبيّن أن الملف الضار في حقيقته هو:
`PsExec.exe` — أداة إدارة نظام شرعية من Sysinternals تم إساءة استخدامها من قِبَل المهاجم للتنفيذ عن بُعد.

لقطة الشاشة ١١ — مطابقة SHA-256 وتحديد الملف الحقيقي PsExec.exe

attachment:19da5f58-a560-4786-9ffb-f3904353e5a8:11-task6-hash-psexec.jpg

---

Task 7: Endpoint Investigation — التحقيق في نقطة النهاية

في المرحلة الأخيرة، تم التحقيق في جهاز ضحية مختلف لاكتشاف هجوم Ransomware.

معلومات الجهاز

نظام التشغيل: Windows 7 Home Basic

الأدلة المكتشفة

الخاصية	القيمة
ملاحظة المهاجم على سطح المكتب	`_R_E_A_D____T_H_I_S___AJYG1O_.txt`
خدمة DLL Windows Defender	`MpSvc.dll`
ملف ZIP ضار تم تنزيله	`eb5489216d4361f9e3650e6a6332f7ee21b0bc9f3f3a4018c69733949be1d481.zip`
الملف التنفيذي الضار على سطح المكتب	`Endermanch@Cerber5.exe`
MD5 Hash للملف الضار	`fe1bc60a95b2c2d77cd5d232296a7fa4`

لقطة الشاشة ١٢ — أدلة التحقيق في الجهاز المصاب ببرنامج الفدية

attachment:abf14bf6-b107-4046-8e0c-a20ba83e748a:12-task7-ransomware-evidence.jpg

تحديد هوية برنامج الفدية

تم التعرف على برنامج الفدية: Cerber Ransomware
يُعدّ Cerber من أكثر برامج الفدية انتشاراً، يقوم بتشفير ملفات الضحية ويطلب فدية بعملة Bitcoin مقابل فك التشفير.

لقطة الشاشة ١٣ — تأكيد قيمة MD5 وتحديد Cerber كبرنامج الفدية

attachment:9c542857-b587-456d-b2f5-1e3de298e270:13-task7-md5-cerber.jpg

---

Task 8: Conclusion — الخاتمة والنتائج النهائية

تم إنهاء جميع مهام التحدي بنجاح — نسبة الإنجاز: 100%

ملخص المهام المُنجَزة

المهمة	العنوان	الحالة
Task 1	Introduction	✅ مكتملة
Task 2	Data Collection	✅ مكتملة
Task 3	The Redline Interface	✅ مكتملة
Task 4	Standard Collector Analysis	✅ مكتملة
Task 5	IOC Search Collector	✅ مكتملة
Task 6	IOC Search Collector Analysis	✅ مكتملة
Task 7	Endpoint Investigation	✅ مكتملة
Task 8	Conclusion	✅ مكتملة

لقطة الشاشة ١٤ — اكتمال جميع مهام غرفة Redline بنسبة 100%

attachment:99ec279c-25f8-43a7-8cbd-3e641244a6a5:14-completion.jpg

---