الاسم: _____ التاريخ: _____ الدرجة: _____

تحليل البرمجيات الخبيثة والحد من التهديدات دليل

أحصنة طروادة، برامج الفدية، برامج التجسس، حزم الجذر (rootkits)، بيئات العزل الافتراضية، الاحتواء

نظرة تعليمية على تحليل البرمجيات الخبيثة

مرحبًا! ترشدك حزمة الأنشطة هذه عبر تحليل البرمجيات الخبيثة والوقاية منها. ستستكشف برامج التجسس وأحصنة طروادة وحمولات برامج الفدية وأدوات الهندسة العكسية وسلوك الجذور الخفية (rootkit) واستراتيجيات الاحتواء.

نقاط التحقق في ورقة العمل

- [ ] **الجزء 1-4: أتقن الأمن السيبراني ومنع التهديدات.**
- [ ] **الجزء 5-7: حل الكلمات المتقاطعة وألغاز البحث عن الكلمات.**
- [ ] **الجزء 8-9: حل دراسات الحالة وتحدي الشيفرة.**
- [ ] **الجزء 10: راجع صفحات الأسئلة الشائعة الأساسية والمتقدمة.**
- [ ] **الجزء 11: استكشف 10 حقائق مثيرة من الواقع.**
- [ ] **إضافي: تحدّي فكّر بسرعة**

مؤمَّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

افتح دليل VPN.com للأمن السيبراني

URL: https://www.vpn.com/cybersecurity/malware/

خارطة طريقك لتعلّم الحد من البرمجيات الخبيثة

- ميّز بين أنواع البرمجيات الخبيثة: حصان طروادة والدودة والجذور الخفية (rootkit).
- طبّق تنفيذ الشيفرة في بيئة افتراضية معزولة (sandbox) لتحليلها.
- صمّم خطط احتواء وتعقيم لحمولات برمجيات الفدية النشطة.

تعليمات دليل تحليل البرمجيات الخبيثة

أجب عن أسئلة الاختيار من متعدد وأسئلة صحيح/خطأ، وأكمل الجمل الناقصة باستخدام بنك الكلمات، وطابق التعريفات، وحُلّ الكلمات المتقاطعة وبحث الكلمات. طبّق معرفتك على الحد من البرمجيات الخبيثة. واختم بالنشاط الإضافي «فكّر بسرعة».

تحليل البرمجيات الخبيثة واحتواء التهديدات (مقدمة)

تشكل الأكواد الخبيثة مثل أحصنة طروادة والديدان وبرمجيات الفدية تهديدات عالية التأثير على نقاط النهاية والخوادم. يحلل فرق الأمن البرمجيات الخبيثة داخل بيئات عزل افتراضية وينفذون ضوابط عزل سريعة للشبكة لاحتواء انتشار الحمولة.

اقرأ كل نقطة تحقق بعناية، ثم اختر الإجابة الصحيحة أو اكتبها.

نقطة التحقق 1: تحدي الاختيار من متعدد

1. 1. ما الخاصية المميزة لحصان طروادة؟
   - A. ينتحل صفة برنامج شرعي لخداع المستخدمين كي يشغّلوه
   - B. يتكاثر تلقائيًا عبر خطوط الشبكة المحلية
   - C. يصيب الملفات داخل بيئات معزولة افتراضية
   - D. يعترض حركة مزود خدمة الإنترنت

2. 2. ما نوع البرمجيات الخبيثة الذي يشفّر الملفات ويطلب مقابلًا ماليًا؟
   - A. برمجيات الفدية
   - B. برامج التجسس
   - C. Rootkit
   - D. البرمجيات الإعلانية

3. 3. ما الذي يمثل برمجيات التجسس؟
   - A. برمجيات خبيثة مصممة لمراقبة ضغطات مفاتيح المستخدم وأنشطة المتصفح سرًا
   - B. شيفرة برمجية تعمل داخل حاوية افتراضية معزولة
   - C. تحديثات مكافحة البرمجيات الخبيثة المنزّلة من سجلات قواعد البيانات
   - D. ضبط سطوع الشاشة تلقائيًا

4. 4. لماذا يستخدم مطورو البرمجيات الخبيثة الجذور الخفية (rootkits)؟
   - A. لإخفاء العمليات النشطة والملفات الخبيثة عن نظام التشغيل
   - B. لزيادة سرعة معالجة وحدة المعالجة المركزية على نقاط النهاية
   - C. لنسخ ملفات قاعدة البيانات احتياطيًا إلى خزائن سحابية آمنة
   - D. لتحسين عمر البطارية في أجهزة الكمبيوتر المحمولة

5. 5. ماذا تعني العزل في بيئة اختبار (Sandboxing) عند تحليل البرمجيات الخبيثة؟
   - A. تنفيذ الملفات المشبوهة في خزنة افتراضية معزولة لمراقبة سلوكها بأمان
   - B. فحص تجزئات الملفات مقابل قواعد بيانات التهديدات المعروفة
   - C. استعادة النسخ الاحتياطية لقواعد البيانات بعد اختراق
   - D. فصل أجهزة توجيه الشبكة المحلية عن الخطوط العامة

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. تتطلب الديدان الحاسوبية تفاعلًا بشريًا من المستخدم للانتشار عبر الشبكات المحلية.

صحيح خطأ

7 سؤال 7

7. البرمجيات الإعلانية غير ضارة دائمًا ولا تتتبع سلوك المستخدم أو سجل المتصفح.

صحيح خطأ

8 سؤال 8

8. تتيح استعادة النسخ الاحتياطية النظيفة غير المتصلة بالإنترنت للضحايا استرداد الملفات المشفرة دون دفع الفدية.

صحيح خطأ

9 سؤال 9

9. يوقف برنامج مكافحة الفيروسات المعتمد على التواقيع برمجيات اليوم الصفر الخبيثة بشكل موثوق قبل وجود أي توقيع لها.

صحيح خطأ

10 سؤال 10

10. تنفّذ البرمجيات الخبيثة بلا ملفات سكربتات خبيثة في ذاكرة النظام، متجنبةً الكتابة على القرص.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

اقرأ كل جملة أدناه وأكمل الفراغ بالمصطلح الصحيح من بنك الكلمات.

1. البرمجية الخبيثة المتنكرة في هيئة أداة آمنة هي حصان _____ .
2. تمثل الحمولات الخبيثة التي تقفل أنظمة قواعد البيانات مقابل المال برمجيات _____ .
3. تمثل البرامج التي تسجل ضغطات المفاتيح لالتقاط كلمات المرور سرا برمجيات _____ .
4. يتطلب الاختباء في أعماق أنوية أنظمة التشغيل برمجية تعرف باسم _____ .
5. يتم تحليل الملفات المشبوهة في خزنة معزولة باستخدام _____ افتراضي.
6. يتطلب إيقاف انتشار حمولات البرمجيات الخبيثة النشطة إجراء _____ فوريا للشبكة.

بنك كلمات المفردات

الاحتواء | التجسس | الدودة | الفدية | بلا ملفات | روتكيت | صندوق الرمل | طروادة

اكتب إجاباتك هنا:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

نقطة التحقق 4: مطابقة مفاهيم الأمان

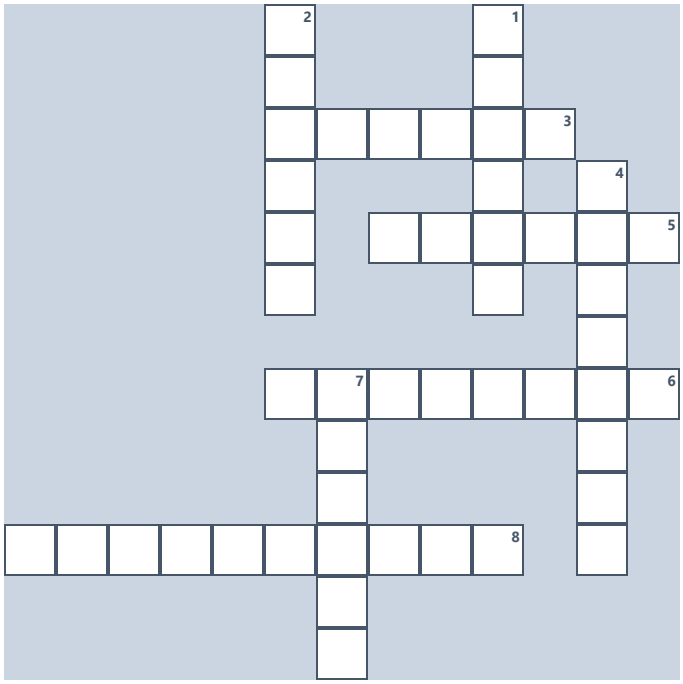
مطابقة التعريفات

طابق كل مصطلح مفردات على اليمين مع تعريفه الصحيح على اليسار بكتابة الحرف المقابل (A-H) في مربع الإدخال القابل للتعبئة.

1. حصان طروادة	A	برنامج مصمم لمراقبة نشاط المستخدم ومدخلاته وتسجيلها سرًا.
2. برامج الفدية	B	برمجية خبيثة تُنفَّذ مباشرة في الذاكرة RAM لتفادي الكشف بواسطة ماسحات القرص.
3. برمجيات التجسس	C	عزل نقاط النهاية المصابة لمنع انتشار حمولات التهديد.
4. الجذور الخفية	D	برمجية خبيثة متنكرة في هيئة أداة مساعدة حميدة أو مفيدة.
5. صندوق الرمل	E	برمجية خبيثة ذاتية التكاثر تنتشر عبر الشبكات دون تدخل بشري.
6. الاحتواء	F	برمجية خبيثة تشفّر وحدة تخزين النظام وتطلب دفع مبلغ مقابل تسليم المفتاح.
7. الدودة	G	بيئة افتراضية معزولة تُستخدم لتحليل الملفات الخبيثة بأمان.
8. بلا ملفات	H	برمجية خبيثة متخفية تختبئ في أعماق نوى الأنظمة للحفاظ على التحكم الإداري.

نقطة التحقق 5: لغز الكلمات المتقاطعة

حلّ الكلمات المتقاطعة بكتابة الحروف في المربعات البيضاء النشطة. تتوافق الأرقام مع الدلائل أدناه.



أفقي

3. برمجية خبيثة متخفية في أعماق أنوية النظام للحفاظ على سيطرة إدارية (6)

5. برمجية خبيثة تشفر وحدة تخزين النظام وتطلب دفعا مقابل تسليم المفتاح (6)

6. حصر نقاط النهاية المصابة لمنع انتشار حمولات التهديد (8)

8. بيئة افتراضية معزولة تستخدم لتحليل الملفات الخبيثة بأمان (10)

عمودي

1. برنامج خبيث متنكر في هيئة أداة حميدة أو مفيدة (6)

2. برنامج مصمم لمراقبة نشاط المستخدم ومدخلاته وتسجيلها سرا (6)

4. برمجية خبيثة تنفذ مباشرة في الذاكرة العشوائية لتفادي كشفها بماسحات الأقراص (8)

7. برمجية خبيثة ذاتية النسخ تنتشر عبر الشبكات دون تدخل بشري (6)

نقطة التحقق 5 – نشاط بديل: أدلة الكلمات المتقاطعة الميسَّرة

يمكن لمستخدمي قارئ الشاشة ولوحة المفاتيح كتابة إجابات الكلمات المتقاطعة مباشرة في حقول النص أدناه.

أفقي

3 أفقي: برمجية خبيثة متخفية في أعماق أنوية النظام للحفاظ على سيطرة إدارية (6 حروف):

5 أفقي: برمجية خبيثة تشفر وحدة تخزين النظام وتطلب دفعا مقابل تسليم المفتاح (6 حروف):

6 أفقي: حصر نقاط النهاية المصابة لمنع انتشار حمولات التهديد (8 حروف):

8 أفقي: بيئة افتراضية معزولة تستخدم لتحليل الملفات الخبيثة بأمان (10 حروف):

عمودي

1 عمودي: برنامج خبيث متنكر في هيئة أداة حميدة أو مفيدة (6 حروف):

2 عمودي: برنامج مصمم لمراقبة نشاط المستخدم ومدخلاته وتسجيلها سرا (6 حروف):

4 عمودي: برمجية خبيثة تنفذ مباشرة في الذاكرة العشوائية لتفادي كشفها بماسحات الأقراص (8 حروف):

7 عمودي: برمجية خبيثة ذاتية النسخ تنتشر عبر الشبكات دون تدخل بشري (6 حروف):

نقطة التحقق 6: البحث عن الكلمة المخفية

ابحث عن 8 مصطلحات مفردات رئيسية مخبأة في الشبكة أدناه. يمكن أن تكون الكلمات أفقية أو رأسية أو قطرية.

ت	ل	س	ز	د	ع	ك	ط	ق	ي	ك	ف	ت	ن	م
م	ح	س	ص	س	ب	ا	ب	ط	ت	ف	ة	ص	ش	ة
ص	ي	ج	ن	ش	ج	ك	ط	س	ر	ج	ز	ع	ع	ش
ك	ق	ت	ة	ي	د	ف	ل	ا	ر	و	ط	ط	ك	ل
ت	م	ل	ن	ن	ص	ر	ت	ت	م	ق	ا	ف	ز	ل
ا	ب	ا	و	ج	ن	م	ا	ء	ي	ه	ت	د	ء	و
ف	د	ش	ر	ء	ج	د	ع	ل	ج	ك	ك	ي	ة	ق
ل	ت	ن	ب	ا	و	ء	ع	ج	ا	ص	ت	ا	ج	ف
م	ج	ح	ر	ز	ق	ج	ل	ك	ط	ح	ح	و	ز	ل
ا	ء	م	ح	ك	ا	ا	ه	ح	ا	ا	ت	ك	ر	ف
ل	ع	ق	ن	ي	ل	ل	ك	ش	ل	ن	ل	و	ت	ع
ب	ة	ب	د	ل	ر	د	ي	و	س	ا	ل	ء	ا	ة
ة	ص	د	ز	ط	م	و	ك	ش	ط	ط	م	ف	ر	ء
ق	ك	ر	ء	ا	ل	د	ف	ه	د	ه	ب	ة	ل	ة
ب	ر	ط	ء	ر	ش	ة	ف	ق	ع	ي	ت	ط	ء	ة

قائمة كلمات المفردات

طروادة الفدية التجسس روتكيت صندوقالرمل الاحتواء الدودة بلاملفات

نقطة التحقق 6 – نشاط بديل: مطابقة المفردات الميسَّرة

طابق كل مصطلح من المصطلحات الـ 8 في البحث عن الكلمات مع تعريفه الصحيح بكتابة الحرف (A-H) في الفراغ.

مصطلحات المفردات
A. طروادة
B. الفدية
C. التجسس
D. روتكيت
E. صندوقالرمل
F. الاحتواء
G. الدودة
H. بلاملفات

التعريفات وحقول المطابقة
1. برمجية خبيثة متخفية في أعماق أنوية النظام للحفاظ على سيطرة إدارية.
2. حصر نقاط النهاية المصابة لمنع انتشار حمولات التهديد.
3. برمجية خبيثة تنفذ مباشرة في الذاكرة العشوائية لتفادي كشفها بماسحات الأقراص.
4. برمجية خبيثة ذاتية النسخ تنتشر عبر الشبكات دون تدخل بشري.
5. برمجية خبيثة تشفر وحدة تخزين النظام وتطلب دفعا مقابل تسليم المفتاح.
6. برنامج مصمم لمراقبة نشاط المستخدم ومدخلاته وتسجيلها سرا.
7. برنامج خبيث متنكر في هيئة أداة حميدة أو مفيدة.
8. بيئة افتراضية معزولة تستخدم لتحليل الملفات الخبيثة بأمان.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن المفاهيم والمصطلحات الأساسية في الأمن السيبراني. اكتب إجاباتك في مربعات الإدخال المخصصة.

1. و ط ا د ة ر
2. س ا ت س ج ل
3. ص ا م ل ن ق ل و ر د
4. ة و د د ا ل
5. د ف ة ا ي ل
6. ي ك ر ت ت و
7. ا ء ت و ا ل ح ا
8. م ل ل ت ب ا ف ا

نشاط إضافي: فكّر بسرعة

اكتب 3 إجابات لكل فئة. يفوز أول من يكمل القائمة.

1	أماكن لتنزيل تطبيقات آمنة		
2	أجهزة يمكن اختراقها		
3	أشياء تحتفظ بنسخة احتياطية منها		
4	علامات تحذيرية في البريد الإلكتروني		
5	علامات إصابة الهاتف ببرمجية خبيثة		
6	أنواع البرمجيات الخبيثة التي تعرفها		
7	أنواع ملفات تتوخى الحذر منها		
8	طرق وصول البرمجيات الخبيثة إلى الحاسوب		
9	عادات آمنة يمكنك البدء بها اليوم		
10	كلمات متعلقة بالأمن السيبراني		
11	أشياء تفعلها بعد تسرّب البيانات		
12	أسباب لتحديث البرامج		
13	حيوانات أو شخصيات بأسماء تشبه البرمجيات الخبيثة		
14	أشياء يمكن أن تسرقها البرمجيات الخبيثة		
15	أشياء تفعلها إذا نقرت على الرابط الخطأ		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: احتواء حمولة برمجيات الفدية في المؤسسات



السيناريو: تعرضت الشبكة المحلية لشركة لاختراق من برمجية فدية نشطة. بدأت خوادم الملفات الرئيسية بعرض امتدادات ملفات بصيغة .locked. ضع سياسات الاحتواء.

سؤال للنقاش: فصّل خطوات الاحتواء، ولخّص بروتوكول استعادة البيانات.

دراسة الحالة 2: حقن الذاكرة بالبرمجيات الخبيثة عديمة الملفات



السيناريو: يرصد محلل أنماط برمجة نصية مشبوهة تُنفَّذ مباشرة في ذاكرة RAM المتطايرة للنظام باستخدام أدوات إدارية قياسية، لكن لا توجد ملفات خبيثة على القرص.

سؤال للنقاش: اشرح استراتيجية تحليل الذاكرة، وحدّد الأدوات اللازمة لحظر التنفيذ الذي لا يعتمد على الملفات.

نقطة التحقق 9: فك الشيفرة

يحمي متخصص الأمن السيبراني أصول الشبكة من الجهات التهديدية عبر الإنترنت. استخدم مفتاح الحرف إلى الرقم أدناه لفك تشفير الرسالة بكتابة الحروف المطابقة في الفراغات.

مفتاح التشفير من الحرف إلى الرقم

ا=1 ب=2 ت=3 ث=4 ج=5 ح=6 خ=7 د=8 ذ=9 ر=10 ز=11

س=12 ش=13 ص=14 ض=15 ط=16 ظ=17 ع=18 غ=19 ف=20 ق=21 ك=22

ل=23 م=24 ن=25 هـ=26 و=27 ي=28 ة=29 ى=30 ء=31 ؤ=32 ئ=33

16	1	21	25		3	1	23	27	24	6		20	13	3	22	1

29	2	21	1	10	24	2		29	28	1	26	25	23	1

22	27	23	12	23	1

الرسالة بعد فك التشفير:

نصيحة: يمثل كل رقم حرفًا عربيًا واحدًا من المفتاح أعلاه.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء A)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q1: ما البرمجيات الخبيثة؟

برمجيات خبيثة صممها جهات تهديد لإتلاف البيانات من الأجهزة والشبكات أو اختطافها أو سرقتها.

Q2: ما الفرق بين الفيروس والدودة؟

يتطلب الفيروس إجراءً بشريًا (مثل فتح ملف) لينتشر، بينما تنتشر الدودة تلقائيًا عبر الشبكات.

Q3: كيف يصيب حصان طروادة الحاسوب؟

يخدع المستخدمين بالتنكر في هيئة برنامج غير ضار أو آمن، مخفيًا حمولته الخبيثة بداخله.

Q4: ما برامج الفدية؟

نوع من البرمجيات الخبيثة يشفّر الملفات على النظام المستهدف ويطالب بدفع مبلغ مالي مقابل مفتاح فك التشفير. [1]

Q5: ما برامج التجسس؟

برمجية خبيثة تسجل سرًا ضغطات مفاتيح المستخدم وكلمات المرور وعادات التصفح لإرسالها إلى المهاجمين.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء B)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: ماذا يعني العزل في بيئة معزولة (sandboxing)؟

تشغيل الملفات المشبوهة في بيئة افتراضية آمنة ومعزولة لمراقبة سلوكها دون خطر على أنظمة الإنتاج.

Q7: ما البرمجيات الخبيثة بلا ملفات (fileless malware)؟

برمجية خبيثة تعمل مباشرة في ذاكرة النظام (RAM) باستخدام أدوات مشروعة، وتتجنب كتابة الملفات على القرص لتجاوز الماسحات الأساسية.

Q8: كيف تحمي الجذور الخفية (rootkit) البرمجيات الخبيثة؟

يخفي العمليات والملفات الخبيثة، غالبًا بالتحايل على نواة نظام التشغيل، لذا قد تفوتها ماسحات مكافحة الفيروسات.

Q9: ما المراقبة السلوكية الديناميكية؟

فحص مضاد الفيروسات الذي يراقب العمليات النشطة في الوقت الفعلي لمنع الإجراءات المعتادة للبرمجيات الخبيثة، مثل تشفير عدد كبير من الملفات دفعة واحدة.

Q10: لماذا يكون الاحتواء عاجلًا أثناء الاستجابة للحوادث؟

يمنع عزل نقاط النهاية المخترقة انتشار حمولات البرمجيات الخبيثة النشطة إلى أجهزة الشبكة الأخرى.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء C)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q1: كيف يتجاوز مطورو البرمجيات الخبيثة ماسحات مكافحة الفيروسات المعتمدة على التواقيع؟

تستخدم تعدد الأشكال، فتغيّر تجزئة الملف وبنية شيفرته مع كل إصابة مع بقاء السلوك الخبيث نفسه.

Q2: ما خطر الأدوات مزدوجة الاستخدام في حملات البرمجيات الخبيثة؟

يستخدم المهاجمون أدوات إدارية مشروعة (مثل PowerShell أو Sysinternals) للاندماج مع حركة مرور الشبكة العادية، مما يصعّب الكشف عنهم.

Q3: كيف ينفّذ تفريغ العمليات (process hollowing) الحمولات الخبيثة؟

يشغّل عملية نظام شرعية في حالة تعليق، ويستبدل شيفرتها في الذاكرة ببرمجية خبيثة، ثم يستأنف التنفيذ.

Q4: ما دور خادم القيادة والتحكم (C2)؟

خادم بعيد يشغّله المخترقون لإرسال التعليمات والحمولات إلى البرمجيات الخبيثة العاملة على الأجهزة المخترقة.

Q5: لماذا يصعب اكتشاف تسجيل ضغطات المفاتيح (keylogging)؟

تستهلك برامج تسجيل ضغطات المفاتيح الأساسية الحد الأدنى من موارد المعالج المركزي وتخفي عملياتها داخل أدوات مشروعة في فضاء المستخدم.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء D)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q6: كيف يؤخر تعتيم الشيفرة البرمجية تحليل البرمجيات الخبيثة؟

يشفّر الشيفرة المصدرية أو يعيد ترتيبها، فتصبح غير مقروءة لأدوات المحللين والماسحات الأمنية.

Q7: ما وظيفة برنامج الإقلاع الخبيث (bootkit)؟

برمجية جذرية (rootkit) تصيب عملية الإقلاع (MBR أو قطاع الإقلاع أو البرنامج الثابت UEFI)، فتعمل قبل تحميل نظام التشغيل.

Q8: كيف يحدد الفحص الاستدلالي تهديدات اليوم الصفري؟

يفحص أنماط الشيفرة المشبوهة والأوامر الإدارية بدلًا من البحث عن تجزئة مطابقة في قاعدة البيانات.

Q9: ما تهديد اختطاف مكتبات DLL؟

إجبار تطبيق شرعي على تحميل مكتبة ارتباط ديناميكي (DLL) خبيثة بوضعها في مسار دليل التطبيق.

Q10: كيف تستخدم خطوط تحليل البرمجيات الخبيثة الآلية المحاكاة الافتراضية؟

تشغّل الملفات المشبوهة عبر عدة أجهزة افتراضية بأنظمة تشغيل مختلفة، وتنشئ تلقائيًا سجلات سلوك وملفات PCAP للشبكة.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

لا تزال أحصنة طروادة طريقة إصابة شائعة لأنها تخفي شيفرة خبيثة داخل برامج تبدو بريئة.

2. نظرة على الأمن

تلقى مركز IC3 التابع لمكتب FBI أكثر من 3,600 شكوى تتعلق ببرامج الفدية في عام 2025، مع خسائر مبلّغ عنها تتجاوز 32 مليون دولار. [3]

3. نظرة على الأمن

يمكن للديدان أن تنتشر بسرعة عبر الشبكات باستغلال ثغرات البروتوكولات غير المصحّحة، مثل EternalBlue في SMB.

4. نظرة على الأمن

يصعب اكتشاف البرمجيات الخبيثة بلا ملفات لأنها تعمل في الذاكرة عبر أدوات شرعية وتترك آثارًا قليلة على القرص.

5. نظرة على الأمن

تعود بيئات الاختبار المعزولة للتحليل عادةً إلى لقطة نظيفة بعد كل تشغيل، بحيث يبدأ كل اختبار من حالة معروفة.

6. نظرة على الأمن

يمكن لبرمجيات Rootkit تعديل استدعاءات نواة النظام، فتبلغ ماسحات البرمجيات الخبيثة بنتائج تشخيص كاذبة.

7. رؤية حول الأمان

يستخدم تعتيم الشيفرة أدوات التعبئة لضغط بنية الحمولة الثنائية الحقيقية للبرمجيات الخبيثة وإخفائها.

8. رؤية حول الأمان

تغيّر البرمجيات الخبيثة متعددة الأشكال شيفرتها، وبالتالي بصمة ملفها، مع كل نسخة جديدة للتهرب من فحوص التواقيع.

9. رؤية حول الأمان

يستغل اختطاف DLL إعدادات ترتيب البحث في أنظمة التشغيل القياسية مثل Windows.

10. نظرة على الأمن

يرصد موردو الأمان أعدادًا ضخمة من عينات البرمجيات الخبيثة الجديدة يوميًا، لذا تحتاج التوقيعات إلى تحديث مستمر.

المراجع والمصادر التقنية

أُعد دليل الدراسة والألغاز التفاعلية استنادًا إلى معايير NIST وOWASP العالمية ومعايير الامتثال لخصوصية البيانات.

المراجع الأكاديمية والصناعية

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1

الإجابة الصحيحة: A

ملاحظة للمعلم

ما الخاصية المميزة لحصان طروادة؟ ← ينتحل صفة برنامج شرعي لخداع المستخدمين كي يشغّلوه

2 السؤال 2

الإجابة الصحيحة: A

ملاحظة للمعلم

ما نوع البرمجيات الخبيثة الذي يشفّر الملفات ويطلب مقابلًا ماليًا؟ ← برمجيات الفدية

3 السؤال 3

الإجابة الصحيحة: A

ملاحظة للمعلم

ما الذي يمثل برمجيات التجسس؟ ← برمجيات خبيثة مصممة لمراقبة ضغطات مفاتيح المستخدم وأنشطة المتصفح سرًا

4 السؤال 4

الإجابة الصحيحة: A

ملاحظة للمعلم

لماذا يستخدم مطورو البرمجيات الخبيثة الجذور الخفية (rootkits)؟ ← لإخفاء العمليات النشطة والملفات الخبيثة عن نظام التشغيل

5 السؤال 5

الإجابة الصحيحة: A

ملاحظة للمعلم

ماذا تعني العزل في بيئة اختبار (Sandboxing) عند تحليل البرمجيات الخبيثة؟ ← تنفيذ الملفات المشبوهة في خزنة افتراضية معزولة لمراقبة سلوكها بأمان

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: تنسخ الديدان نفسها ذاتيًا وتنتشر عبر الشبكات دون أي إجراء من المستخدم.

7 السؤال 7

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: ليست برمجيات الإعلانات المتطفلة (adware) غير ضارة دائمًا؛ فكثير منها يتتبع التصفح لاستهداف الإعلانات.

8 السؤال 8

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

صحيح: تستعيد النسخ الاحتياطية النظيفة غير المتصلة الملفات المشفرة دون دفع، رغم أن البيانات المسروقة قد تتسرب مع ذلك.

9 السؤال 9

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: تحتاج الماسحات المعتمدة على التواقيع إلى عينة معروفة، لذا يمكن للبرمجيات الخبيثة الجديدة كليًا من اليوم الصفر أن تفلت منها.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تنفّذ البرمجيات الخبيثة بلا ملفات سكربتات خبيثة في ذاكرة النظام، متجنبةً الكتابة على القرص.

مفاتيح المفردات ومعيار التقييم

معيار التصحيح للمعلم: امنح 1 نقطة لكل مطابقة صحيحة (المجموع 8 نقطة) ولكل مصطلح سياق (المجموع 6 نقطة).

نقطة التحقق 4: مفتاح الإجابة – مطابقة المفاهيم

D 1. حصان طروادة	F 2. برامج الفدية	A 3. برمجيات التجسس	H 4. الجذور الخفية
G 5. صندوق الرمل	C 6. الاحتواء	E 7. الدودة	B 8. بلا ملفات

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 طروادة	2 الفدية	3 التجسس	4 روتكيت
5 صندوق الرمل	6 الاحتواء		

نقطة التحقق 6 – نشاط بديل: مفتاح الإجابة – مطابقة المفردات

1 D – روتكيت	2 F – الاحتواء	3 H – بلاملفات	4 G – الدودة
5 B – الفدية	6 C – التجسس	7 A – طروادة	8 E – صندوقالرمل

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح حصان طروادة وبرامج الفدية وبرمجيات التجسس بكلماتهم الخاصة وإعطاء مثال على كل منها.

دراسات الحالة:
اطلب من الطلاب أن يدعموا توصياتهم بحقائق من ورقة العمل لا بآرائهم.

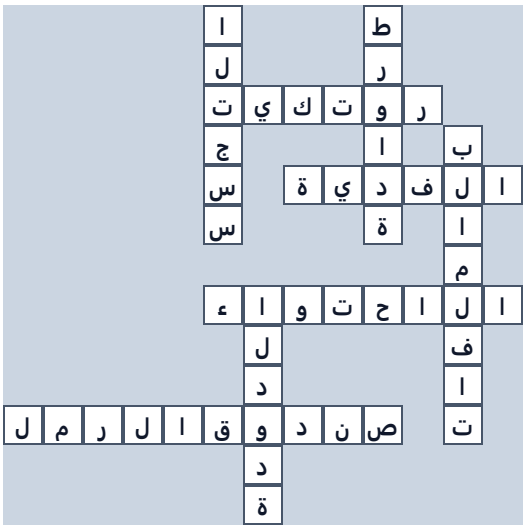
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

ت	ل	س	ز	د	ع	ك	ط	ق	ي	ك	ف	ت	ن	م
م	ح	س	س	ب	ا	ب	ط	ت	ف	ة	س	ش	ة
س	ي	ج	ن	ش	ج	ك	س	ر	ج	ز	ع	ع	ش
ك	ق	ت	ة	ي	د	ف	ل	ا	ر	و	ط	ك	ل
ت	م	ل	ن	ن	س	ر	ت	م	ق	ا	ف	ز	ل
ا	ب	ا	و	ج	ن	م	ا	ء	ي	ه	ت	د	ء	و
ف	د	ش	ر	ء	د	ج	ل	ج	ع	ك	ي	ة	ق
ل	ت	ن	ب	ا	و	ء	ع	ج	ا	س	ت	ا	ج	ف
م	ج	ح	ر	ز	ق	ج	ك	ط	ح	ح	و	ز	ل
ا	ء	م	ح	ك	ا	ا	ه	ا	ا	ت	ك	ر	ف
ل	ع	ق	ن	ي	ل	ل	ك	ش	ل	ن	ل	و	ت	ع
ب	ة	ب	د	ل	ر	د	ي	و	س	ا	ل	ء	ا	ة
ة	س	د	ز	ط	م	و	ك	ش	ط	ط	م	ف	ر	ء
ق	ك	ر	ء	ا	ل	د	ف	ه	د	ه	ب	ة	ل	ة
ب	ر	ط	ء	ر	ش	ة	ف	ق	ع	ي	ت	ط	ء	ة

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

3 أفقي: روتكيت برمجية خبيثة متخفية في أعماق أنوية النظام للحفاظ على سيطرة إدارية (6 حروف)

5 أفقي: الفدية برمجية خبيثة تشفر وحدة تخزين النظام وتطلب دفعا مقابل تسليم المفتاح (6 حروف)

6 أفقي: الاحتواء حصر نقاط النهاية المصابة لمنع انتشار حمولات التهديد (8 حروف)

8 أفقي: صندوقالرمل بيئة افتراضية معزولة تستخدم لتحليل الملفات الخبيثة بأمان (10 حروف)

عمودي

1 عمودي: طروادة برنامج خبيث متنكر في هيئة أداة حميدة أو مفيدة (6 حروف)

2 عمودي: التجسس برنامج مصمم لمراقبة نشاط المستخدم ومدخلاته وتسجيلها سرا (6 حروف)

4 عمودي: بلاملفات برمجية خبيثة تنفذ مباشرة في الذاكرة العشوائية لتفادي كشفها بماسحات الأقراص (8 حروف)

7 عمودي: الدودة برمجية خبيثة ذاتية النسخ تنتشر عبر الشبكات دون تدخل بشري (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. وطادةر ← **طروادة**
2. ساتسجل ← **التجسس**
3. صاملنقلورد ← **صندوقالرمل**
4. ةوددال ← **الدودة**
5. دفةايل ← **الفدية**
6. يكرتتو ← **روتكيت**
7. اءتوالحا ← **الاحتواء**
8. مللتبافا ← **بلاملفات**

مفتاح تحدي الشيفرة السرية

"اكتشف حمولات نقاط النهاية بمراقبة السلوك"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: احتواء حمولة برمجيات الفدية في المؤسسات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: اخترقت برمجية فدية نشطة الشبكة المحلية لشركة. بدأت خوادم الملفات الرئيسة تعرض امتدادات ملفات بالصيغة .locked. ضع سياسات الاحتواء.
- الاستراتيجية والحل الموصى بهما: افصل جميع الخوادم المتأثرة عن الشبكة المحلية. أنهِ جلسات الإدارة النشطة. استعد الملفات غير المخترقة من نظام نسخ احتياطي آمن غير متصل ومقفل ضد الكتابة.

B دراسة الحالة 2: حقن الذاكرة بالبرمجيات الخبيثة عديمة الملفات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يكتشف محلل أنماط برمجة نصية مشبوهة تُنفَّذ مباشرةً في ذاكرة RAM المتطايرة للنظام باستخدام أدوات إدارية قياسية، لكن لا توجد ملفات خبيثة على القرص.
- الاستراتيجية والحل الموصى بهما: اعزل نقاط النهاية المتأثرة والتقط صورة للذاكرة أولًا. راجع سجلات PowerShell وWMI، واحظر البرامج النصية غير المعتمدة باستخدام AppLocker، ثم أعد التشغيل لإزالة الحمولة.