خطوات حل التمرين التقيمي

حلّ تمرين 11.4 — دليل إجراءات الحوادث الرقمية + إجراءات الأدلة الجنائية (شرح وافي)

مقدمة سريعة: المطلوب تكتب دليل عملي يتعامل مع تكرار حادث أمني: كيف تكشف/تعزل/تجمع أدلة/تحلل/وتقدّم إجراءات جنائية إن لزم. الحل المقترح هنا يغطي كل خطوة بترتيب عملي مع قوالب جاهزة.

(1مرجعية المعايير (كيف يربط الحلّ بالـD.P8, D.M4, CD.D2)

- D.P8 ← اطّلب إنك "تطبّق إجراءات عملية في المؤسسة" ← اشرح خطة الاستجابة، من أدوار، خطوات احتواء، جمع أدلة، وتدريبات. أظهر أمثلة تطبيقية.
- D.M4 ← يتطلّب "تحليل وتقييم" ← قدّم تقييم فاعلية التدابير، جدول تقييم المخاطر (احتمال×أثر)، وثبت كيف تتخذ أولويات.
- CD.D2 ← يركّز على "الإجراءات الجنائية/الجنائية الرقمية" ← نوّه لسلسلة الحيازة، طرق عمل نسخة فورنسيك، توثيق قابل للمحكمة، والتوافق القانوني.

إذا كتبت الدليل بهذه العناصر ورفقت نماذج/سجلات، تكون غطيت الثلاث معايير.

(2هيكل الدليل (محتوى مقترح — كل قسم شو بدّه(

1. **النطاق والتعريفات** :أي أنظمة/بيانات مشمولة، تعريف حادث أمني، تعريف الأدلة الرقمية.
2. **الأدوار والمسؤوليات** :من يبلغ، مين قائد الفريق، من يتواصل مع القانون، من مسؤول التخزين.
3. **تصنيف الحوادث)** :مثلاً: مستوى 1 — حادث محدود، مستوى 2 — اختراق بيانات، مستوى 3 — رانسوموير/تسريب كبير.(
4. **خطة الاستجابة خطوة بخطوة)** :التحضير ← الكشف ← الاحتواء ← جمع الأدلة ← التحليل ← الاستعادة ← الدروس المستفادة.(
5. **إجراءات جمع الأدلة الجنائية الرقمية** :أدوات، طرق التصوير، حفظ السجلات، سلسلة الحيازة.
6. **قوالب وسجلات** :نموذج تبليغ، نموذج سلسلة الحيازة، سجل الأدلة، تقرير حادث.
7. **متطلبات قانونية/امتثال** :إشعار للجهات، حفظ سجلات، حقوق المستخدمين، إشراف قانوني.
8. **اختبار ومراجعة** :جدول لاختبار الدليل مرة سنوياً أو بعد كل حادث.

(3دليل خطوة بخطوة (عملي جداً — ماذا تفعل فوراً(

1. **الإبلاغ والتوثيق الفوري**
   - كل ملاحظة غير عادية تُبلّغ فوراً لقائد الاستجابة.
   - سجّل: تاريخ/وقت الاكتشاف، من بلّغ، وصف أولي، الأجهزة المتأثرة.
2. **العزل(Containment)**
   - افصل الجهاز/الخادم عن الشبكة فوراً (إن أمكن دون مسح الأدلة).
   - إن عزل الجهاز قد يوقف الانتشار؛ لا تطفئ الجهاز إلا إذا كان ذلك ضروريًا) قد تفقد ذاكرةRAM ، المفيدة للتحقيق.(
3. **جمع الأدلة(Evidence Collection)**
   - اعمل صورة فورنسية (Forensic Image) للقرص الصلب. أمثلة أوامر شائعة:
     - على لينكس dd if=/dev/sda of=/mnt/usb/image.dd bs=4M : conv=noerror,syncثم md5sum image.ddلتوثيق.
     - استخدم أدوات مصممة.FTK Imager, Guymager, EnCase :
   - احفظ سجلات النظام(syslog, auth.log) ، سجلات الجدار الناري، سجلات السيرفرات والتطبيقات، سجلات البريد.
   - التقط لقطة لذاكرة النظام (memory dump) إن كان الهجوم حديثاً) أدوات.(DumpIt, FTK Imager :
4. **سلسلة الحيازة(Chain of Custody)**
   - لكل قطعة دليل: مَن أخذها، متى، أين خزّنت، حالة الوسيط، توقيع. سجل كل حركة لاحقة. (القالب أدناه).
5. **التحليل**
   - تحليل الملفات/برمجيات الخبيثة في بيئة معزولة.(sandbox)
   - تحليل السجلات لتحديد نقطة الدخول، الحسابات المستخدمة، الأوامر المنفذة، الملفات المنسوخة/المعدلة.
6. **الإزالة والتعافي**
   - ازالة البرمجيات الخبيثة، استعادة من نسخ احتياطية نظيفة، إعادة بناء الأنظمة إن لزم، إعادة تعيين كلمات المرور.
7. **الدروس والتقارير**
   - إعداد تقرير كامل: ملخص الحادث، الأصول المتأثرة، سبب الاختراق، التدابير المتخذة، التوصيات.
   - تحديث السياسات وإجراء تدريب للموظفين.

(4قوالب جاهزة (انسخها وخليها عندك(

نموذج سلاّلة الحيازة — (Chain of Custody) الحقول الأساسية:

- معرف الدليل_____ :
- وصف الدليل) نوع: هارد/USB/سجل/صورة_____ :(
- التاريخ والوقت الذي جُمِع فيه_____ :
- المجمّع/الآخذ: الاسم والتوقيع_____ :
- حالة التعبئة/الختم_____ :
- موقع التخزين_____ :
- أي تحويل/نقل (التاريخ، من/إلى، التوقيع): سجل هنا...
- ملاحظات إضافية_____ :

نموذج تقرير حادث (مختصر):

- عنوان الحادث_____ :
- تاريخ/وقت الاكتشاف_____ :
- من أبلغ_____ :
- مستوى الحادث(1/2/3) :
- الأنظمة المتأثرة_____ :
- ملخص موجز لوقائع الهجوم_____ :
- الإجراءات الفورية المتخذة_____ :
- الأدلة المجمعة: (قائمة + معرف)
- نتيجة التحليل_____ :
- توصيات عاجلة ومتوسطة وطويلة الأمد_____ :

نموذج جدول حفظ السجلات:(Timeline)

- وقت | حدث | من | ملاحظة

(5أمثلة أدوات مفيدة (دفاع/تحقيق) — للاستخدام المشروع فقط

- جمع/تصوير dd, Guymager, FTK Imager :

- تحليل الذاكرةVolatility :
- تحليل برمجيات خبيثة) Cuckoo sandbox :في بيئة معزولة(
- سجلات ومراقبة (ELK (Elasticsearch, Logstash, Kibana :أو أيSIEM

ملاحظة: لا تستخدم الأدوات للهجوم — الغرض دفاعي وتحقيقي.

(6كيفية العرض في الامتحان/التقييم (صيغة مختصرة للكتابة(

اكتب فقرة منظمة على هذا النحو (مناسب للامتحان):

1. تعريف الحادث ونطاقه.
2. خطوات الاستجابة: التبليغ → العزل → جمع الأدلة) تصوير Forensic Image + حفظ السجلات → (تحليل → إزالة → استرداد.
3. إجراءات جنائية: الحفاظ على سلسلة الحيازة، استخدام أدوات فورنسية موثوقة، توثيق كل خطوة لضمان قبول الدليل قضائياً.
4. بعد الحادث: تقرير مفصل وتحديث السياسات والتدريب.

مثال جاهز للنسخ (سطرين/ثلاثة):

عند تكرار حادث أمني، نتبع خطة استجابة موثقة: نبلغ ونعزل الأجهزة المصابة فوراً، ثم نجمع الأدلة عبر تصوير فورنسيك للأقراص وسجلات النظام مع توثيق سلسلة الحيازة. يُحلّل الفريق الأدلة في بيئة معزولة لتحديد مصدر الاختراق، ثم تُستعاد الأنظمة من نسخ نظيفة وتُطبق توصيات للوقاية. تُحفظ كل الإجراءات للتقديم القانوني عند الحاجة.

(7نقاط تقييم عادةً تُقَيّم عليها الأسئلة — كيف أتأكّد أن إجابتي "كاملة"؟

- وضّحت خطوات عملية ومترابطة → Evidence → Containment → Detection → (Preparation Analysis → Recovery → Lessons).
- أضفت إجراءات فنية محددة (تصوير الأقراص، حفظ السجلات، حفظ الذاكرة).
- أدرجت سلسلة الحيازة ونموذج حفظ الأدلة (مهم للقضايا الجنائية).
- قدمت توصيات ومرحلة متابعة (تدريب، تحديث سياسات).
- لو طُلب تقييم: أعطيت جدول مخاطر أو وصفت كيفية ترتيب الأولويات.

هذي النقاط ترضي) D.P8 تنفيذ الإجراءات(،) D.M4التحليل والتقييم(،) CD.D2الإجراءات الجنائية الرقمية.(

(8نصائح ذكية (عشان تجيب علامة كاملة وتبين إنك فاهمة(

- لا تذكر أسماء أو تفاصيل تقنية مرفوضة — ركّز على المنهج والالتزام القانوني.
- أستخدم أمثلة قصيرة) مثال: بريد تصيّد تسبب دخول ← كيف جمعنا logs ومتى لقينا الأثر.(
- إذا في سؤال يطلب "أذكر" — أعط 4 خطوات واضحة. إذا يطلب "ناقش" — وضّح لماذا كل خطوة مهمة وربطها بالمخاطر.
- لو عندك وقت زد: رسم مصغر يبيّن مراحل الاستجابة (مخطط سير). المعلمين يحبوها.

(9خلاصة قصيرة تسليم الامتحان (نسخة نهائية لتضعها(

عند تكرار حادث أمني، تُطبق خطة الاستجابة التالية: (1) التبليغ والتوثيق الفوري، (2) العزل لمنع الانتشار، (3) جمع الأدلة عبر تصوير فورنسيك للقرص وحفظ سجلات النظام ولقطات الذاكرة، مع الحفاظ على سلسلة الحيازة، (4) تحليل الأدلة في بيئة معزولة لتحديد طريقة الدخول والجهات المتورطة، (5) إزالة البرمجيات الخبيثة واستعادة الأنظمة من نسخ احتياطية نظيفة، و(6) استخراج الدروس وتحديث السياسات. تُراعى طوال العملية المتطلبات القانونية لضمان قبول الأدلة أمام الجهات القضائية.
