الاسم: _____ التاريخ: _____ الدرجة: _____

الويب المظلم مقابل الويب العميق: الأمان و الفروق

فهرسة محركات البحث، وقواعد بيانات الويب العميق، وتوجيه البصل في Tor، وإخفاء هوية الشبكة ومخاطرها

نظرة تعليمية عامة على الويب المظلم مقابل الويب العميق

مرحبًا! ترشدك حزمة الأنشطة هذه عبر الفروق بين الويب العميق والويب المظلم. ستستكشف قواعد البيانات غير المفهرسة والتوجيه البصلي في متصفح Tor ونطاقات .onion التشفيرية ومخاطر الأمان في إخفاء الهوية.

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/dark-web-vs-deep-web/

خارطة طريقك لتعلّم استراتيجية الويب العميق والمظلم

- قارن الويب العميق (قواعد البيانات غير المفهرسة) بالويب المظلم (خدمات onion).
- افهم كيف يشفّر التوجيه البصلي حركة مرور الشبكة ويرحّلها.
- قيّم المخاطر الأمنية للوصول إلى مواقع شبكة Tor غير الموثقة.
- انشر سياسات البوابة الآمنة والعزل التجريبي (sandboxing) لزحف استخبارات التهديدات.
- حلّل صيغة العناوين التشفيرية لنطاقات خدمات onion.

تعليمات دليل الويب العميق والمظلم

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 الخصوصية في الويب العميق والمظلم. واختم بالنشاط الإضافي «فكّر بسرعة».

قواعد بيانات الويب العميق مقابل توجيه البصل في الويب المظلم (مقدمة)

يتكون الويب العميق من صفحات غير مفهرسة خلف كلمات مرور وتسجيلات دخول، مثل رسائل البريد الإلكتروني الخاصة أو بوابات البنوك المؤسسية. أما الشبكة المظلمة فهي مجموعة فرعية من الويب العميق مخفية عمدًا، وتتطلب متصفحات متخصصة (مثل Tor) وشبكات onion للوصول إليها دون الكشف عن الهوية.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما الذي يميز الويب العميق عن الويب السطحي؟
   - A. صفحات الويب العميق غير مفهرسة في محركات البحث العامة
   - B. حركة الويب العميق غير قانونية وتراقبها الجهات المختصة بإنفاذ القانون
   - C. تتطلب مواقع الويب العميق متصفحات متخصصة مثل Tor للوصول إليها
   - D. صفحات الويب العميق تُحمَّل دائمًا أسرع من صفحات الويب السطحي

2. كيف يُوصَل إلى الويب المظلم؟
   - A. عبر متصفحات متخصصة تستخدم شبكات التوجيه البصلي
   - B. بضبط إعدادات DNS مخصصة على الموجّهات القياسية
   - C. عبر وحدات تحكم بحث الويب السطحي الخاصة بالدعوة فقط
   - D. بتثبيت إضافة متصفح قياسية لحظر الإعلانات

3. ما البنية التي تشكل الجزء الأكبر من الويب العميق؟
   - A. قواعد بيانات المستخدمين المحمية بكلمة مرور والحسابات الخاصة
   - B. منتديات سوق سوداء غير قانونية تتاجر بسلع محظورة
   - C. بروتوكولات مشاركة الملفات بين الأقران غير المشفرة
   - D. قواعد بيانات الذاكرة المؤقتة لمحركات البحث العامة

4. ماذا يفعل التوجيه البصلي بحركة الشبكة؟
   - A. يشفّر الحزم ويوجّهها عبر عدة مرحّلات
   - B. يزيد سرعات التنزيل بتجاوز عقد مزود خدمة الإنترنت
   - C. يربط الأرقام التسلسلية لعتاد الجهاز بسجلات IP
   - D. يحذف ملفات تعريف الارتباط في متصفح الويب بعد كل نقرة

5. ما لاحقة النطاق المستخدمة حصريًا على شبكات Tor؟
   - A. امتداد النطاق العلوي التشفيري .onion
   - B. الامتداد التجاري القديم القياسي .com
   - C. امتداد Web3 اللامركزي .eth على البلوكتشين
   - D. امتداد التقنية .ai برمز البلد

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال tf 6

6. يشير الويب العميق والشبكة المظلمة إلى الجزء نفسه من الشبكة.

صحيح خطأ

7 سؤال tf 7

7. بوابات الشبكات الداخلية للشركات جزء من الويب العميق.

صحيح خطأ

8 سؤال tf 8

8. يفك التوجيه البصلي تشفير حزم البيانات بالكامل في كل عقدة عبور.

صحيح خطأ

9 سؤال tf 9

9. يعرّض الوصول إلى الويب المظلم الأجهزة لمخاطر عالية من البرمجيات الخبيثة.

صحيح خطأ

10 سؤال tf 10

10. تزحف محركات البحث القياسية على مواقع onion وتفهرسها.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. توجد بوابات البنوك الخاصة في الجزء _____ غير المفهرس.
2. تستضيف عقد Tor المتخصصة خدمات _____ المخفية.
3. تستخدم مواقع Tor امتداد المستوى الأعلى التشفيري _____ .
4. يسمى مسار الحركة المشفرة متعدد الطبقات _____ .
5. تزحف محركات بحث الويب السطحي إلى الصفحات _____ علناً.
6. تشفر شبكات Onion عناوين IP للعملاء للحفاظ على _____ المستخدم.

بنك كلمات المفردات

onion. البصل التوجيه القاعدة المفهرسة الويب العميق الويب المظلم مجهولية

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

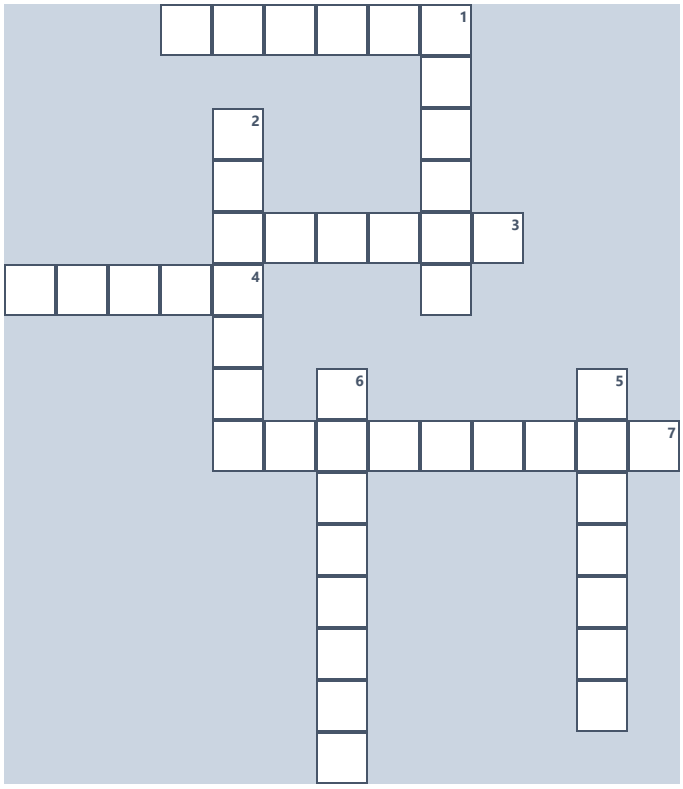
مطابقة التعريفات

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

1. جزء من الويب العميق	A	جزء شبكة مشفّر لا يمكن الوصول إليه إلا عبر متصفحات خاصة.
2. بوابة الويب المظلم	B	تشفير البيانات في طبقات وتمريرها عبر ثلاث عقد.
3. امتداد Onion	C	تخزين خلفي آمن يستضيف سجلات النظام غير المفهرسة.
4. توجيه Tor	D	لاحقة نطاق من المستوى الأعلى تشفيرية تُستخدم على شبكات Tor.
5. الصفحات المفهرسة	E	عقدة نقطة الدخول المستخدمة للوصول إلى شبكة Tor.
6. إخفاء هوية المستخدم	F	محتوى الويب السطحي المفهرس والقابل للبحث في Google.
7. قاعدة بيانات خاصة	G	إبقاء عناوين IP العامة للعملاء مخفية عن الخوادم.
8. بوابة الدخول	H	محتوى ويب غير مفهرس مثل تسجيلات الدخول الخاصة ورسائل البريد الإلكتروني وسجلات قواعد البيانات.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

1. عقدة نقطة البداية المستخدمة للوصول إلى شبكة Tor (6)

3. محتوى ويب غير مفهرس مثل تسجيلات الدخول الخاصة والبريد وسجلات قواعد البيانات (6)

4. لاحقة نطاق أعلى تشفيرية تُستخدم في شبكات Tor (5)

7. إبقاء عناوين IP العامة للعملاء مخفية عن الخوادم (9)

عمودي

1. جزء شبكي مشفر لا يمكن الوصول إليه إلا عبر متصفحات خاصة (6)

2. تخزين خلفي آمن يستضيف سجلات النظام غير المفهرسة (7)

5. تشفير البيانات على طبقات وتمريرها عبر ثلاث عقد (7)

6. محتوى الويب السطحي المجمع والقابل للبحث في Google (8)

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

1 أفقي: عقدة نقطة البداية المستخدمة للوصول إلى شبكة Tor (6 حروف):

3 أفقي: محتوى ويب غير مفهرس مثل تسجيلات الدخول الخاصة والبريد وسجلات قواعد البيانات (6 حروف):

4 أفقي: لاحقة نطاق أعلى تشفيرية تُستخدم في شبكات Tor (5 حروف):

7 أفقي: إبقاء عناوين IP العامة للعملاء مخفية عن الخوادم (9 حروف):

عمودي

1 عمودي: جزء شبكي مشفر لا يمكن الوصول إليه إلا عبر متصفحات خاصة (6 حروف):

2 عمودي: تخزين خلفي آمن يستضيف سجلات النظام غير المفهرسة (7 حروف):

5 عمودي: تشفير البيانات على طبقات وتمريرها عبر ثلاث عقد (7 حروف):

6 عمودي: محتوى الويب السطحي المجمع والقابل للبحث في Google (8 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	م	م	س	د	ف	ل	ط	ك	ظ	ك	ف	ت	ه	م
ن	ح	ل	ص	ش	ب	ا	ب	ش	ص	ل	ح	ن		
ص	ظ	ظ	ه	ص	ج	ل	ع	ش	ل	ج	س	ع	ع	ص
ك	ق	م	ق	ي	م	ع	ل	ا	ر	ق	ع	ع	ك	ل
م	ه	ل	ن	ر	ا	ت	م	ل	ك	ف	ا	ز	م	ب
ه	ي	ا	ج	ن	ل	خ	ا	و	و	ت	خ	ع	ي	د
ي	ص	ز	خ	ج	م	ع	ج	ل	ل	خ	ظ	ق	د	ت
ج	ه	ب	ا	خ	ج	ف	ج	ص	م	ا	د	ج	ف	ة
و	ج	د	ر	س	ه	ج	ل	ك	ع	ف	ح	ل	س	م
ت	خ	ن	د	ل	و	ا	و	ح	ا	ا	ه	ل	ا	ق
ل	ع	ك	ه	ظ	ل	ل	ك	ش	م	ه	م	ر	ت	ع
ا	ة	ب	د	م	ي	ب	ظ	ي	س	ا	ل	خ	س	ة
ة	ص	ر	س	ع	ة	ص	ل	ش	ط	ط	ن	ق	ر	ة
ك	ل	ر	خ	ا	ف	ل	و	د	و	ب	ة	م	ة	ب
ر	ط	خ	ر	ش	ف	ك	ف	ي	ت	ط	خ	ة	د	ة

قائمة كلمات المفردات

العميق المظلم البصل التوجيه المفهرسة المجهولية القاعدة الدخول

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. العميق
B. المظلم
C. البصل
D. التوجيه
E. المفهرسة
F. المجهولية
G. القاعدة
H. الدخول

التعريفات وحقول المطابقة
1. إبقاء عناوين IP العامة للعملاء مخفية عن الخوادم.
2. تخزين خلفي آمن يستضيف سجلات النظام غير المفهرسة.
3. تشفير البيانات على طبقات وتمريرها عبر ثلاث عقد.
4. محتوى ويب غير مفهرس مثل تسجيلات الدخول الخاصة والبريد وسجلات قواعد البيانات.
5. جزء شبكي مشفر لا يمكن الوصول إليه إلا عبر متصفحات خاصة.
6. لاحقة نطاق أعلى تشفيرية تُستخدم في شبكات Tor.
7. عقدة نقطة البداية المستخدمة للوصول إلى شبكة Tor.
8. محتوى الويب السطحي المجمع والقابل للبحث في Google.

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. ع ا م ي ق ل
2. ا ل ص ب ل
3. ف ل ا ه ر ة س م
4. ة ل ع ا د ا ق
5. ظ م م ا ل ل
6. ي ت ج ا و ه ل
7. و ا ي ة ل ج ل ه م
8. د ل ا و خ ل

نشاط إضافي: فكّر بسرعة

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

1	أسباب للابتعاد عن الشبكة المظلمة		
2	أشياء لا يستطيع محرك البحث العثور عليها		
3	أجهزة يمكن اختراقها		
4	أسباب قانونية لاستخدام Tor		
5	أسباب لتحديث البرامج		
6	علامات تحذيرية في البريد الإلكتروني		
7	أشياء تُباع بصورة غير قانونية على الشبكة المظلمة (dark web)		
8	أشخاص يمكنك طلب مساعدة تقنية منهم		
9	عادات آمنة يمكنك البدء بها اليوم		
10	أشياء تفعلها بعد تسرّب البيانات		
11	أشياء تنتمي إلى الشبكة العميقة (deep web)		
12	مواقع تستخدمها بتسجيل الدخول		
13	كلمات متعلقة بإخفاء الهوية		
14	معلومات لا ينبغي أن تشاركها أبدًا		
15	أشياء تقع "تحت السطح"		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: تحديد تسرب البيانات



السيناريو: يكتشف تدقيق أمني مؤسسي أن سجلات قاعدة بيانات العملاء الحساسة يجري تداولها في سوق onion. البيانات غير مفهرسة في Google.

سؤال للنقاش: اشرح أي أجزاء الويب معنية وكيف حدث هذا التسريب.

دراسة الحالة 2: إخفاء الهوية مقابل مخاطر البرمجيات الخبيثة



السيناريو: يريد محلل التحقق من موجزات استخبارات التهديدات على موقع Tor. ينزّل متصفح Tor ويدخل إلى الموقع.

سؤال للنقاش: قيّم فوائد إخفاء الهوية ولخّص خطوات الحد من البرمجيات الخبيثة.

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

29	28	23	27	26	5	24		30	23	18		17	20	1	6

23	14	2	23	1		26	28	5	27	3	2		24	8	7	3	12	24	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 الويب العميق؟

يتكون الويب العميق من جميع صفحات الويب التي لا تستطيع محركات البحث فهرستها، بما فيها الخدمات المصرفية عبر الإنترنت وقواعد بيانات البريد الإلكتروني والمجلات المدفوعة.

Q2: ما الويب المظلم؟

الشبكة المظلمة مجموعة فرعية صغيرة من الويب العميق، مخفية عمدًا ولا يمكن الوصول إليها إلا عبر متصفحات متخصصة تستخدم شبكات onion.

Q3: كيف تفهرس محركات البحث الصفحات؟

تشغّل المحركات برامج آلية (زواحف) لتتبع الروابط العامة وفهرسة الصفحات التي لا تحجب الزحف عبر توجيهات الروبوتات.

Q4: لماذا تُعد الخدمات المصرفية عبر الإنترنت جزءًا من الويب العميق؟

تقع بوابات المصارف خلف جدران تسجيل الدخول وكلمات المرور، مما يمنع محركات البحث العامة من فهرسة صفحات كشوف الحساب.

Q5: ما التوجيه البصلي (Onion Routing) في متصفح Tor؟

التوجيه البصلي طريقة نقل تشفّر حركة المرور على طبقات وتمررها عبر مرحّلات متعددة لإخفاء عناوين IP للمستخدمين.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: هل الوصول إلى الويب المظلم غير قانوني؟

لا. فالوصول إلى الويب المظلم قانوني في معظم الدول، رغم أن الانخراط في الأسواق غير القانونية أو الأنشطة السيبرانية محظور.

Q7: لماذا تتباطأ مواقع الويب المظلم في التحميل؟

تُوجَّه حركة المرور وتُفكّ تشفيراتها عبر ثلاث عقد ترحيل عالمية على الأقل (الدخول والوسيط والخروج)، مما يزيد زمن الاستجابة في الإرسال.

Q8: ماذا تعني لاحقة النطاق .onion؟

هو لاحقة نطاق علوي متخصصة تُستخدم على شبكات Tor، وتشير إلى عناوين مولّدة تشفيريًا بدلًا من خوادم DNS القياسية.

Q9: ما المخاطر المرتبطة بروابط الويب المظلم؟

المواقع لا تخضع لأي فحص أمني، مما يعرّض المستخدمين لمعدلات إصابة مرتفعة بالبرمجيات الخبيثة وبرامج التصيّد النصية واحتيال المعاملات.

Q10: من أنشأ بروتوكول توجيه شبكة Tor؟

طُورت التقنية في الأصل في تسعينيات القرن الماضي (1990s) على يد مختبر الأبحاث البحرية الأمريكي لحماية الاتصالات الحكومية.

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

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

Q1: كيف تحمي العقد الوسيطة إخفاء الهوية في Tor؟

تفك كل عقدة تشفير طبقة واحدة فقط من بيانات التوجيه، فلا تعرف سوى القفزة السابقة والقفزة التالية، ولا تعرف المصدر والوجهة معًا أبدًا.

Q2: ما دور عقدة الخروج؟

تفك عقدة الخروج الطبقة الأخيرة من التشفير، وترسل حركة المرور إلى خادم الوجهة العام أو خادم onion.

Q3: ما بوابة جسور Tor؟

الجسور هي مرحّلات دخول Tor غير مدرجة تُستخدم لتجاوز حجب مزود خدمة الإنترنت والرقابة في المناطق التي تقيّد الوصول إلى متصفح Tor.

Q4: كيف يستغل فاعلو الويب المظلم العملات المشفرة؟

يستخدم الفاعلون عملات مشفّرة مجهولة لتنفيذ صفقات مالية في الأسواق المظلمة، متهربين من فحوص المعاملات المصرفية القياسية.

Q5: لماذا تفشل محركات البحث القياسية في زحف قواعد البيانات العميقة؟

لا تستطيع الزواحف إدخال بيانات تسجيل الدخول أو حل اختبارات CAPTCHA الأمنية أو تشغيل نصوص استعلامات SQL الخلفية اللازمة للوصول إلى قواعد البيانات العميقة.

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

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

Q6: ما خادم الدليل (directory server) في شبكات Tor؟

هو خادم موثوق يحتفظ بقائمة مرحّلات الدخول والوسط والخروج النشطة التي يستخدمها العملاء لبناء مسارات التوجيه.

Q7: كيف ينفّذ الفاعلون الخبيثون التنصت على عقدة الخروج؟

يمكن لمشغّلي عقد الخروج المارقة اعتراض حركة HTTP غير المشفرة عند خروجها من شبكة Tor، وسرقة أسماء المستخدمين وملفات تعريف الارتباط.

Q8: ما الفرق بين Tor وI2P؟

يستخدم Tor دليل ترحيل مركزيًا وعقد خروج للوصول إلى الويب العام، بينما يستخدم I2P بنية لامركزية من نظير إلى نظير للاستضافة الداخلية.

Q9: كيف تتتبع وكالات إنفاذ القانون أسواق الويب المظلم؟

تستخدم الجهات تحليل البلوكتشين، وتحدد مواقع إعدادات استضافة الخوادم الفعلية، وتنفذ عمليات خداع لتحديد المشغّلين.

Q10: كيف يُضعف تسريب DNS إخفاء هوية العميل؟

يحدث تسرّب DNS عندما تُرسَل استعلامات DNS الخاصة بالمتصفح مباشرة عبر مزوّد خدمة الإنترنت المحلي بدلًا من توجيهها عبر شبكة Tor المشفّرة.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

الويب العميق أكبر بكثير من الويب السطحي القابل للبحث، إذ يقع معظم المحتوى خلف تسجيلات الدخول وقواعد البيانات.

2. نظرة على الأمن

الشبكة المظلمة جزء صغير مخفي عمدًا من الويب العميق، يُوصل إليه بأدوات مثل Tor.

3. نظرة على الأمن

يشفّر توجيه Tor حزم البيانات ثلاث مرات، ويُزيل طبقات التشفير كما تُقشّر البصلة عند كل عقدة ترحيل.

4. نظرة على الأمن

نشأ Tor من مشروع التوجيه البصلي (onion routing) الذي أدارته مختبرات الأبحاث البحرية الأمريكية، وأُطلقت شيفرته كبرنامج حر. [1]

5. نظرة على الأمن

عناوين Onion سلاسل أبجدية رقمية من 56 حرفًا تُولَّد تشفيريًا من أزواج المفاتيح العامة.

6. نظرة على الأمن

يمكن لعقد الخروج قراءة حركة المرور النصية الواضحة، ما يعني أن TLS/HTTPS لا يزال مطلوبًا على Tor لحماية بيانات الجلسة.

7. رؤية حول الأمان

تمثل مواقع الإنترانت ومحركات التخزين السحابية وقواعد البيانات الخاصة أكبر شرائح تخزين البيانات على الويب العميق.

8. رؤية حول الأمان

تشغّل محركات البحث المتخصصة مثل DuckDuckGo بوابات onion للسماح بعمليات بحث مجهولة على شبكات Tor.

9. رؤية حول الأمان

يتصل أكثر من 2 مليون مستخدم بشبكة Tor يوميًا لتجاوز الرقابة والحفاظ على خصوصية الاتصالات.

10. نظرة على الأمن

تغلق عمليات إنفاذ القانون العالمية (مثل عملية Bayonet) أسواقًا مظلمة كبرى بالاستيلاء على أجهزة الاستضافة.

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-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 **الفهرسة في البحث** الويب العميق
الإجابة الصحيحة: **A**

ملاحظة للمعلم

تقع صفحات الويب العميق خلف جدران تسجيل الدخول وقواعد البيانات، ما يمنع زواحف البحث من فهرستها. المصدر: IETF RFC 3986.

2 **الوصول إلى Tor** الويب المظلم
الإجابة الصحيحة: **A**

ملاحظة للمعلم

تتكون الشبكة المظلمة من خدمات onion مخفية لا يمكن الوصول إليها إلا عبر متصفحات مثل Tor. المرجع: IETF RFC 3986.

3 **قواعد البيانات العميقة** قواعد البيانات
الإجابة الصحيحة: **A**

ملاحظة للمعلم

تشكّل الحسابات المحمية بكلمات مرور والسجلات المؤسسية أكبر شريحة من الويب العميق. المرجع: NIST Digital Identity.

4 **التوجيه البصلي** شبكة TOR
الإجابة الصحيحة: **A**

ملاحظة للمعلم

يشفّر التوجيه البصلي حزم البيانات على طبقات ويمررها عبر عقد متعددة لإخفاء الهوية. المرجع: IETF RFC 3986.

5 **نطاق Onion** اللاحقة
الإجابة الصحيحة: **A**

ملاحظة للمعلم

تُوجّه اللاحقة التشفيرية للنطاق.onion حركة المرور داخليًا على Tor دون DNS عام. المرجع: IETF RFC 3986.

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 قطاعات الويب — البنية — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

يشمل الويب العميق جميع الصفحات غير المفهرسة، بينما الشبكة المظلمة جزء فرعي صغير مشفر من شبكات onion. المرجع: IETF RFC 3986.

7 الشبكات الداخلية للشركات — الويب العميق — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

مواقع الإنترانت خلف بوابات كلمات المرور وغير مفهرسة، أي أنها تنتمي إلى الويب العميق. المصدر: NIST Digital Identity.

8 تشفير الطبقات — المرحّلات — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

لا تفك مرحّلات Onion تشفير سوى طبقة توجيه واحدة لحماية إخفاء هوية المستخدم، ولا تفك الحزمة بأكملها أبدًا. المرجع: IETF RFC 3986.

9 التعرض للبرمجيات الخبيثة — التهديدات — الإجابة الصحيحة: صحيح

ملاحظة للمعلم

لا تخضع أسواق الويب المظلم لأي تصفية أمنية، ما يحمل مخاطر شديدة للإصابة بالبرمجيات الخبيثة. المصدر: Center for Internet Security (CIS).

10 السؤال 10 — الإجابة الصحيحة: خطأ

ملاحظة للمعلم

لا تستخدم برامج زحف محركات البحث العادية Tor، لذا لا تستطيع الوصول إلى مواقع .onion أو فهرستها.

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

H 1. جزء من الويب العميق	A 2. بوابة الويب المظلم	D 3. امتداد Onion	B 4. توجيه Tor
F 5. الصفحات المفهرسة	G 6. إخفاء هوية المستخدم	C 7. قاعدة بيانات خاصة	E 8. بوابة الدخول

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 الويب العميق	2 الويب المظلم	3 onion.	4 التوجيه
5 المفهرسة	6 مجهولية		

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

1 F – المجهولية	2 G – القاعدة	3 D – التوجيه	4 A – العميق
5 B – المظلم	6 C – البصل	7 H – الدخول	8 E – المفهرسة

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح جزء من الويب العميق وبوابة الويب المظلم وامتداد Onion بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

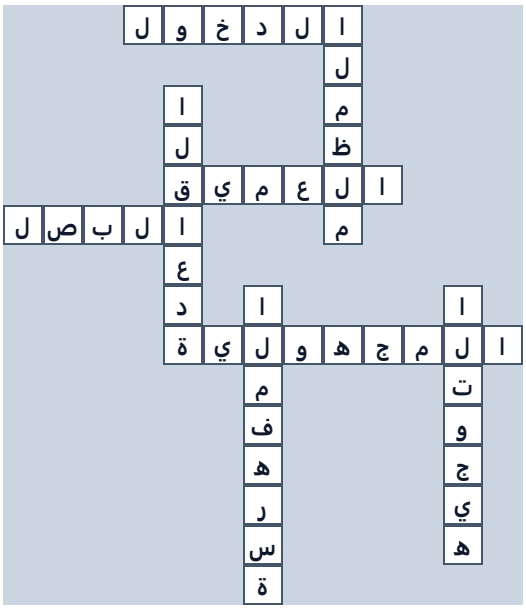
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

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

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

1 أفقي: الدخول عقدة نقطة البداية المستخدمة للوصول إلى شبكة Tor (6 حروف)

3 أفقي: العميق محتوى ويب غير مفهرس مثل تسجيلات الدخول الخاصة والبريد وسجلات قواعد البيانات (6 حروف)

4 أفقي: البصل لاحقة نطاق أعلى تشفيرية تُستخدم في شبكات Tor (5 حروف)

7 أفقي: المجهولية إبقاء عناوين IP العامة للعملاء مخفية عن الخوادم (9 حروف)

عمودي

1 عمودي: المظلم جزء شبكي مشفر لا يمكن الوصول إليه إلا عبر متصفحات خاصة (6 حروف)

2 عمودي: القاعدة تخزين خلفي آمن يستضيف سجلات النظام غير المفهرسة (7 حروف)

5 عمودي: التوجيه تشفير البيانات على طبقات وتمريرها عبر ثلاث عقد (7 حروف)

6 عمودي: المفهرسة محتوى الويب السطحي المجمع والقابل للبحث في Google (8 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. عاميقل — **العميق**
2. الصبل — **البصل**
3. فلاهرةسم — **المفهرسة**
4. ةلعاداق — **القاعدة**
5. ظممالل — **المظلم**
6. يتجاوهل — **التوجيه**
7. وايةلجلهم — **المجهولية**
8. دلاوخل — **الدخول**

مفتاح تحدي الشيفرة السرية

"حافظ على مجهولية المستخدم بتوجيه البصل"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: تحديد تسرب البيانات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يكتشف تدقيق أمني في شركة أن سجلات قاعدة بيانات عملاء حساسة تُتداول في سوق onion والبيانات غير مفهرسة في Google.
- الاستراتيجية والحل الموصى بهما: الأجزاء المعنية: تنتمي قاعدة البيانات الخاصة إلى الويب العميق (غير مفهرسة لكنها آمنة). أما السوق الذي يتاجر بالبيانات المسروقة فهو على الويب المظلم (شبكة onion). كيف حدث ذلك: تجاوز المخترقون دفاعات الخادم، وسرقوا قاعدة البيانات من الويب العميق، وأدرجوها بشكل مجهول على الويب المظلم للإفلات من تتبع جهات إنفاذ القانون.

B دراسة الحالة 2: إخفاء الهوية مقابل مخاطر البرمجيات الخبيثة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يريد محلل فحص موجزات استخبارات التهديدات على موقع Tor. فينزّل متصفح Tor ويصل إلى الموقع.
- الاستراتيجية والحل الموصى بهما: الفوائد: يوجّه Tor الحركة عبر ثلاث عقد، فيخفي عنوان IP الخاص بشركة المحلل. المخاطر وسبل التخفيف: لا تخضع روابط الويب المظلم لأي فحص للسمعة. وعلى المحللين تشغيل Tor داخل أجهزة افتراضية (VMs) معزولة، وتعطيل JavaScript في إعدادات Tor، وتجنب تنزيل أي ملفات لحماية شبكة الشركة.