ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

เว็บมืดเทียบกับเว็บลึก: ความปลอดภัยและความแตกต่าง

การจัดทำดัชนีของเครื่องมือค้นหา ฐานข้อมูลดีพเว็บ การกำหนดเส้นทางหัวหอมของ Tor การปกปิดตัวตนบนเครือข่ายและความเสี่ยง

ภาพรวมการเรียนรู้ดาร์กเว็บเทียบกับดีปเว็บ

ได้รับการรักษาความปลอดภัย

การเข้ารหัสข้อมูล

มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด

มาตรฐานสากล

กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์

นโยบายการเข้าถึง

การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับความแตกต่างระหว่างดีปเว็บและดาร์กเว็บ คุณจะได้สำรวจฐานข้อมูลที่ไม่ได้จัดทำดัชนี Onion Routing ของ Tor browser โดเมนเข้ารหัส .onion และความเสี่ยงด้านความปลอดภัยของการไม่เปิดเผยตัวตน

จุดตรวจสอบของใบงาน

- [ ] **ส่วนที่ 1-4: เรียนรู้ความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามให้เชี่ยวชาญ**
- [ ] **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- [ ] **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- [ ] **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- [ ] **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- [ ] **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความปลอดภัยไซเบอร์ของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/dark-web-kap-deep-web/

เส้นทางการเรียนรู้กลยุทธ์ดีปเว็บและดาร์กเว็บของคุณ

- เปรียบเทียบดีปเว็บ (ฐานข้อมูลที่ไม่ถูกจัดทำดัชนี) กับดาร์กเว็บ (บริการ onion)
- ทำความเข้าใจว่า Onion Routing เข้ารหัสและส่งต่อทราฟฟิกเครือข่ายอย่างไร
- ประเมินความเสี่ยงด้านความปลอดภัยของการเข้าถึงเว็บไซต์ในเครือข่าย Tor ที่ไม่ได้รับการยืนยัน
- ติดตั้งเกตเวย์ที่ปลอดภัยและนโยบายแซนด์บ็อกซ์สำหรับการรวบรวมข้อมูลภัยคุกคาม
- วิเคราะห์รูปแบบที่อยู่เข้ารหัสของโดเมนบริการ Onion

คำแนะนำคู่มือเว็บลึกและเว็บมืด

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ ความเป็นส่วนตัวบนดีพเว็บและดาร์กเว็บ ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

ฐานข้อมูลเว็บลึกเทียบกับการกำหนดเส้นทางแบบหัวหอมของเว็บมืด (บทนำ)

ดีปเว็บประกอบด้วยหน้าที่ไม่ถูกทำดัชนีซึ่งอยู่หลังรหัสผ่านและการเข้าสู่ระบบ เช่น อีเมลส่วนตัวหรือพอร์ทัลธนาคารขององค์กร ดาร์กเว็บเป็นส่วนย่อยของดีปเว็บที่ซ่อนไว้โดยเจตนา ต้องใช้เบราว์เซอร์เฉพาะ (เช่น Tor) และเครือข่าย onion เพื่อเข้าถึงอย่างไม่เปิดเผยตัวตน

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1 **1. อะไรที่ทำให้ดีพเว็บแตกต่างจากเซอร์เฟซเว็บ?**

- A. หน้าดีพเว็บไม่ได้ถูกทำดัชนีโดยเสิร์ชเอนจินสาธารณะ
- B. ทราฟฟิกบนดีพเว็บผิดกฎหมายและถูกเจ้าหน้าที่บังคับใช้กฎหมายเฝ้าติดตาม
- C. เว็บไซต์ดีพเว็บต้องใช้เบราว์เซอร์เฉพาะทางอย่าง Tor จึงจะเข้าถึงได้
- D. หน้าดีปเว็บโหลดเร็วกว่าหน้าเซอร์เฟซเว็บเสมอ

2 **2. เข้าถึงดาร์กเว็บได้อย่างไร?**

- A. ผ่านเบราว์เซอร์เฉพาะที่ใช้เครือข่ายการกำหนดเส้นทางแบบหัวหอม
- B. ด้วยการกำหนดค่า DNS แบบกำหนดเองบนเราเตอร์มาตรฐาน
- C. ผ่านคอนโซลค้นหาบนเซอร์เฟซเว็บแบบเซิญเท่านั้น
- D. ด้วยการติดตั้งส่วนขยายเบราว์เซอร์บล็อกโฆษณามาตรฐาน

3 **3. โครงสร้างใดที่เป็นส่วนใหญ่ที่สุดของดีพเว็บ?**

- A. ฐานข้อมูลผู้ใช้และบัญชีส่วนตัวที่ป้องกันด้วยรหัสผ่าน
- B. ฟอรัมตลาดมืดผิดกฎหมายที่ซื้อขายสินค้าผิดกฎหมาย
- C. โปรโตคอลแชร์ไฟล์แบบเพียร์ทูเพียร์ที่ไม่เข้ารหัส
- D. ฐานข้อมูลแคชของเสิร์ชเอนจินสาธารณะ

4 **4. Onion Routing ทำอะไรกับทราฟฟิกเครือข่าย?**

- A. เข้ารหัสแพ็กเก็ตและส่งผ่านรีเลย์หลายตัว
- B. เพิ่มความเร็วดาวน์โหลดโดยข้ามโหนดของ ISP
- C. จับคู่หมายเลขซีเรียลของฮาร์ดแวร์อุปกรณ์กับระเบียน IP
- D. ลบคุกกี้ของเว็บเบราว์เซอร์หลังการคลิกทุกครั้ง

5 **5. คำต่อท้ายโดเมนใดที่ใช้เฉพาะบนเครือข่าย Tor?**

- A. นามสกุลระดับบนสุด .onion แบบเข้ารหัส
- B. นามสกุลเชิงพาณิชย์ .com แบบดั้งเดิมมาตรฐาน
- C. นามสกุลบล็อกเชน .eth แบบกระจายศูนย์ของ Web3
- D. นามสกุลเทคโนโลยี .ai ตามรหัสประเทศ

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถามจริง/เท็จ 6

6. ดีปเว็บและดาร์กเว็บหมายถึงส่วนเครือข่ายเดียวกัน

จริง เท็จ

7 คำถามจริง/เท็จ 7

7. พอร์ทัลอินทราเน็ตขององค์กรเป็นส่วนหนึ่งของดีปเว็บ

จริง เท็จ

8 คำถามจริง/เท็จ 8

8. การกำหนดเส้นทางแบบหัวหอมถอดรหัสแพ็กเก็ตข้อมูลทั้งหมดที่ทุกโหนดที่ผ่าน

จริง เท็จ

9 คำถามจริง/เท็จ 9

9. การเข้าถึงดาร์กเว็บทำให้อุปกรณ์เสี่ยงต่อมัลแวร์สูง

จริง เท็จ

10 คำถามจริง/เท็จ 10

10. เครื่องมือค้นหาเว็บทั่วไปรวบรวมและจัดทำดัชนีไซต์ onion

จริง เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. พอร์ทัลธนาคารส่วนตัวอยู่ในส่วนของ _____ ที่ไม่ได้จัดทำดัชนี
2. โหนด Tor เฉพาะทางโฮสต์บริการที่ซ่อนของ _____
3. เว็บไซต์ Tor ใช้นามสกุลระดับบนสุดแบบเข้ารหัสลับ _____
4. การเข้ารหัสทราฟฟิกหลายชั้นเรียกว่าการจัด _____ แบบหัวหอม
5. เสิร์ชเอนจินบนพื้นผิวรวบรวมหน้าเว็บที่ _____ แบบสาธารณะ
6. เครือข่ายโอเนียนเข้ารหัสไอพีของไคลเอนต์เพื่อรักษา _____ ของผู้ใช้

คลังคำศัพท์

จัดทำดัชนี | ฐานข้อมูล | ดาร์กเว็บ | ดีปเว็บ | นิรนาม | เส้นทาง | โหนดทางเข้า | โอเนียน

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

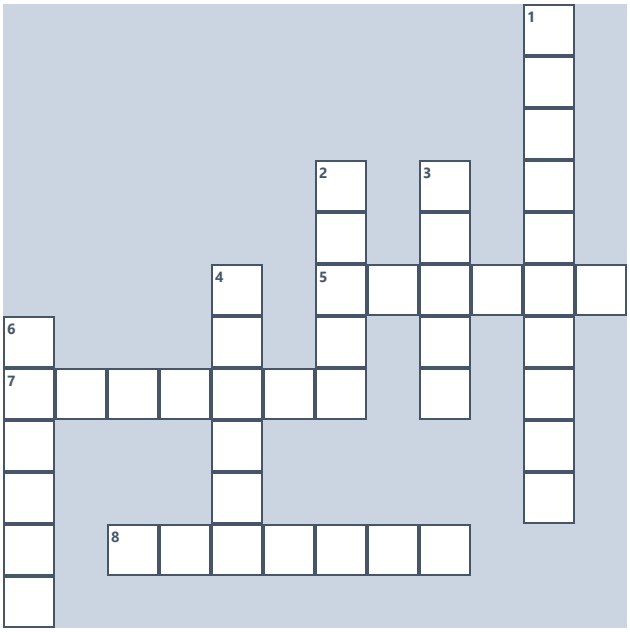
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. ส่วนของดีปเว็บ**	**A**	ส่วนของเครือข่ายที่เข้ารหัสซึ่งเข้าถึงได้ผ่านเบราว์เซอร์พิเศษเท่านั้น
☐	**2. พอร์ทัลดาร์กเว็บ**	**B**	การเข้ารหัสข้อมูลเป็นชั้นๆ และส่งต่อผ่านสามโหนด
☐	**3. นามสกุล Onion**	**C**	ที่เก็บข้อมูลแบ็กเอนด์ที่ปลอดภัยซึ่งเก็บบันทึกระบบที่ไม่ได้จัดทำดัชนี
☐	**4. การกำหนดเส้นทาง Tor**	**D**	ส่วนต่อท้ายโดเมนระดับบนสุดที่ใช้เข้ารหัสบนเครือข่าย Tor
☐	**5. หน้าที่ถูกทำดัชนี**	**E**	โหนดจุดเข้าที่ใช้เข้าถึงเครือข่าย Tor
☐	**6. การไม่เปิดเผยตัวตนของผู้ใช้**	**F**	เนื้อหาเว็บผิวน้ำที่ถูกรวบรวมและค้นหาได้บน Google
☐	**7. ฐานข้อมูลส่วนตัว**	**G**	การปกปิดที่อยู่ IP สาธารณะของไคลเอนต์จากเซิร์ฟเวอร์
☐	**8. เกตเวย์ทางเข้า**	**H**	เนื้อหาเว็บที่ไม่ได้จัดทำดัชนี เช่น หน้าเข้าสู่ระบบส่วนตัว อีเมล และระเบียนฐานข้อมูล

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

5. การเข้ารหัสข้อมูลเป็นชั้นๆ แล้วส่งต่อผ่านสามโหนด (6)

7. ส่วนของเครือข่ายที่เข้ารหัสซึ่งเข้าถึงได้ผ่านเบราว์เซอร์พิเศษเท่านั้น (7)

8. ที่จัดเก็บส่วนหลังที่ปลอดภัยซึ่งเก็บบันทึกของระบบที่ไม่ได้จัดทำดัชนี (7)

แนวตั้ง

1. โหนดจุดเข้าที่ใช้เข้าถึงเครือข่าย Tor (10)

2. เนื้อหาเว็บที่ไม่ได้จัดทำดัชนี เช่น การเข้าสู่ระบบส่วนตัว อีเมล และบันทึกฐานข้อมูล (5)

3. การปกปิดไอพีสาธารณะของไคลเอนต์จากเซิร์ฟเวอร์ (5)

4. คำต่อท้ายโดเมนระดับบนสุดแบบเข้ารหัสลับที่ใช้บนเครือข่าย Tor (6)

6. เนื้อหาเว็บบนพื้นผิวที่ถูกรวบรวมและค้นหาได้บน Google (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

5 แนวนอน: การเข้ารหัสข้อมูลเป็นชั้นๆ แล้วส่งต่อผ่านสามโหนด (6 ตัวอักษร):

7 แนวนอน: ส่วนของเครือข่ายที่เข้ารหัสซึ่งเข้าถึงได้ผ่านเบราว์เซอร์พิเศษเท่านั้น (7 ตัวอักษร):

8 แนวนอน: ที่จัดเก็บส่วนหลังที่ปลอดภัยซึ่งเก็บบันทึกของระบบที่ไม่ได้จัดทำดัชนี (7 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: โหนดจุดเข้าที่ใช้เข้าถึงเครือข่าย Tor (10 ตัวอักษร):

2 แนวตั้ง: เนื้อหาเว็บที่ไม่ได้จัดทำดัชนี เช่น การเข้าสู่ระบบส่วนตัว อีเมล และบันทึกฐานข้อมูล (5 ตัวอักษร):

3 แนวตั้ง: การปกปิดไอพีสาธารณะของไคลเอนต์จากเซิร์ฟเวอร์ (5 ตัวอักษร):

4 แนวตั้ง: คำต่อท้ายโดเมนระดับบนสุดแบบเข้ารหัสลับที่ใช้บนเครือข่าย Tor (6 ตัวอักษร):

6 แนวตั้ง: เนื้อหาเว็บบนพื้นผิวที่ถูกรวบรวมและค้นหาได้บน Google (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ร	ต	อ	า	นี	า	น	นี	ส	ช	มี	ฟ	บ	า	า
ห	นี	ม	า	ม	กี	จ	า	โ	า	ดี	รี	ต	ว	ย
ง	ก	า	ค	จ	น	ตี	ว	ร	อ	ป	ตี	ว	า	ล
ล	ด	น	นี	ช	ดั	ทำ	ด	จั	า	เ	อ	ย	ซ	ฟ
ก	ก	ร	ล	ม	โ	า	ป	อ	อ	ว็	นี	ม	เ	มี
ล	า	นิ	ล	ล	ห	ป	ด	จ	า	บ	นี	ย	ส้	กี
มู	พ	ร	ง	า	น	ซ	า	า	า	ลี	จ	ดี	น	า
อ	น	ล	ผ	ดี	ด	ซ	ก	ด	ร์	า	ต	า	ท	จ
ข้	า	ค	ก	ดี	ท	า	ช	ว	ก	ก	ด	กี	า	ด
น	ท	ผ	ฟ	ซ	า	มี	ม	อ	ต	ฟ	เ	ร	ง	ดี
า	า	ท	า	ส	ง	ท	ข	ข	า	น	ก	ว็	า	ล
ฐ	า	ม	ร	มี	เ	า	ร	ช	ก	ด	ง	น	บ	ร
ต	สี	ย	ข	มี	ข้	ดี	ด	ด	ว	บ	ฟ	อ	า	ร
ห	ห	รี	น	ผ	า	นี	ม	ผ	ดี	ข	กี	ส	บ	ลี
ง	ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ

รายการคำศัพท์

ดีปเว็บ ดาร์กเว็บ โอเนียน เส้นทางโหนดทางเข้า จัดทำดัชนี นิรนาม ฐานข้อมูล

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. ดีปเว็บ

B. ดาร์กเว็บ

C. โอเนียน

D. เส้นทาง

E. จัดทำดัชนี

F. นิรนาม

G. ฐานข้อมูล

H. โหนดทางเข้า

คำนิยามและช่องจับคู่

1. การปกปิดไอพีสาธารณะของไคลเอนต์จากเซิร์ฟเวอร์
2. ที่จัดเก็บส่วนหลังที่ปลอดภัยซึ่งเก็บบันทึกของระบบที่ไม่ได้จัดทำดัชนี
3. การเข้ารหัสข้อมูลเป็นชั้นๆ แล้วส่งต่อผ่านสามโหนด
4. เนื้อหาเว็บที่ไม่ได้จัดทำดัชนี เช่น การเข้าสู่ระบบส่วนตัว อีเมล และบันทึกฐานข้อมูล
5. ส่วนของเครือข่ายที่เข้ารหัสซึ่งเข้าถึงได้ผ่านเบราว์เซอร์พิเศษเท่านั้น
6. คำต่อท้ายโดเมนระดับบนสุดแบบเข้ารหัสลับที่ใช้บนเครือข่าย Tor
7. โหนดจุดเข้าที่ใช้เข้าถึงเครือข่าย Tor
8. เนื้อหาเว็บบนพื้นผิวที่ถูกรวบรวมและค้นหาได้บน Google

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ว็ เ ด็ บ ป
2. น โ เ ย นื อ
3. จั ทำ ดั นี ช ด
4. ล า อ ข้ มู ฐ น
5. เ บ ก ร์ ด ว็ า
6. า ท เ น ง ส้
7. า ม นิ น ร
8. ข้ ด า า โ ท ห ง เ น

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	เหตุผลที่ควรอยู่ห่างจาก **Dark Web**			
2	สิ่งที่เสิร์ชเอนจินค้นหาไม่พบ			
3	อุปกรณ์ที่ถูกแฮกได้			
4	เหตุผลที่ชอบด้วยกฎหมายในการใช้ **Tor**			
5	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
6	สัญญาณเตือนในอีเมล			
7	สิ่งที่ขายอย่างผิดกฎหมายบน **Dark Web**			
8	บุคคลที่คุณขอความช่วยเหลือด้าน IT ได้			
9	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
10	สิ่งที่ควรทำหลังข้อมูลรั่วไหล			
11	สิ่งที่อยู่ใน **Deep Web**			
12	เว็บไซต์ที่คุณใช้โดยต้องเข้าสู่ระบบ			
13	คำที่เกี่ยวข้องกับการไม่เปิดเผยตัวตน			
14	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
15	สิ่งที่อยู่ "ใต้ผิวน้ำ"			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การระบุข้อมูลรั่วไหล



สถานการณ์: การตรวจสอบความปลอดภัยขององค์กรพบว่าระเบียนฐานข้อมูลลูกค้าที่ละเอียดอ่อนถูกซื้อขายในตลาด onion ข้อมูลนี้ไม่ได้ถูกทำดัชนีบน Google

คำถามอภิปราย: จงอธิบายว่าส่วนใดของเว็บที่เกี่ยวข้อง และการรั่วไหลนี้เกิดขึ้นได้อย่างไร

กรณีศึกษาที่ 2: การไม่เปิดเผยตัวตนเทียบกับความเสี่ยงจากมัลแวร์



สถานการณ์: นักวิเคราะห์ต้องการตรวจสอบฟีดข้อมูลภัยคุกคามบนเว็บไซต์ Tor เขาดาวน์โหลดเบราว์เซอร์ Tor และเข้าถึงไซต์

คำถามอภิปราย: จงประเมินประโยชน์ด้านการไม่เปิดเผยตัวตน และสรุปขั้นตอนลดความเสี่ยงจากมัลแวร์

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ปกป้องทรัพย์สินเครือข่ายจากผู้ก่อภัยคุกคามออนไลน์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ั=48
า=49 ำ=50 ิ=51 ี=52 ึ=53 ื=54 ุ=55 ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ็=62 ่=63 ้=64 ๊=65 ๋=66 ์=67

35	48	1	41	49		4	39	49	33		25	51	35	25	49	33	
20	64	39	34		57	42	64	25	23	49	7		43	48	39	43	45	33

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: ดีปเว็บคืออะไร?

ดีปเว็บประกอบด้วยหน้าเว็บทั้งหมดที่เสิร์ชเอนจินไม่สามารถทำดัชนีได้ รวมถึงธนาคารออนไลน์ ฐานข้อมูลอีเมล และวารสารที่มีระบบเพย์วอลล์

Q2: ดาร์กเว็บคืออะไร?

ดาร์กเว็บเป็นส่วนย่อยเล็กๆ ของดีปเว็บที่ถูกซ่อนไว้โดยเจตนา และเข้าถึงได้ผ่านเบราว์เซอร์เฉพาะที่ใช้เครือข่าย onion เท่านั้น

Q3: เสิร์ชเอนจินทำดัชนีหน้าเว็บอย่างไร?

เอนจินรันโปรแกรมอัตโนมัติ (สไปเดอร์) เพื่อตามลิงก์สาธารณะและทำดัชนีหน้าที่ไม่ได้บล็อกการรวบรวมข้อมูลด้วยคำสั่ง robot

Q4: ทำไมธนาคารออนไลน์จึงถือเป็นส่วนหนึ่งของดีพเว็บ?

พอร์ทัลธนาคารอยู่หลังหน้าล็อกอินและรหัสผ่าน จึงบล็อกเสิร์ชเอนจินสาธารณะไม่ให้จัดทำดัชนีหน้าใบแจ้งยอดบัญชี

Q5: Onion Routing ของ Tor browser คืออะไร?

การกำหนดเส้นทางแบบหัวหอมเป็นวิธีส่งข้อมูลที่เข้ารหัสทราฟฟิกเป็นชั้นๆ และส่งผ่านรีเลย์หลายตัวเพื่อซ่อนที่อยู่ IP ของผู้ใช้

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: การเข้าถึงดาร์กเว็บผิดกฎหมายหรือไม่?

ไม่ การเข้าถึงดาร์กเว็บถูกกฎหมายในส่วนใหญ่ของประเทศ แต่การเข้าร่วมตลาดผิดกฎหมายหรือกิจกรรมไซเบอร์ผิดกฎหมายเป็นสิ่งต้องห้าม

Q7: ทำไมเว็บไซต์บนดาร์กเว็บจึงโหลดช้า?

ทราฟฟิกถูกกำหนดเส้นทางและถอดรหัสผ่านรีเลย์ทั่วโลกอย่างน้อยสามตัว (ขาเข้า กลาง ขาออก) ซึ่งเพิ่มความหน่วงในการส่งข้อมูล

Q8: ส่วนต่อท้ายโดเมน .onion หมายความว่าอย่างไร?

เป็นส่วนต่อท้ายโดเมนระดับบนสุดเฉพาะที่ใช้บนเครือข่าย Tor ชี้ไปยังที่อยู่ที่สร้างด้วยการเข้ารหัสลับแทนเซิร์ฟเวอร์ DNS มาตรฐาน

Q9: ลิงก์ดาร์กเว็บมีความเสี่ยงอะไรบ้าง?

ไซต์ไม่มีการคัดกรองความปลอดภัย ทำให้ผู้ใช้เสี่ยงต่ออัตราการติดมัลแวร์สูง สคริปต์ฟิชชิง และการหลอกลวงในธุรกรรม

Q10: ใครสร้างโปรโตคอลกำหนดเส้นทางของเครือข่าย Tor?

เทคโนโลยีนี้พัฒนาขึ้นครั้งแรกโดยห้องปฏิบัติการวิจัยกองทัพเรือสหรัฐฯ ในทศวรรษ 1990 เพื่อปกป้องการสื่อสารของรัฐบาล

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: โหนดตัวกลางปกป้องการไม่เปิดเผยตัวตนของ Tor ได้อย่างไร?

แต่ละโหนดถอดรหัสข้อมูลการกำหนดเส้นทางเพียงชั้นเดียว รู้เพียงฮอปก่อนหน้าและฮอปถัดไป ไม่เคยรู้ทั้งต้นทางและปลายทางพร้อมกัน

Q2: โหนดขาออกมีบทบาทอย่างไร?

โหนดทางออกถอดรหัสชั้นสุดท้ายของการเข้ารหัส แล้วส่งทราฟฟิกออกไปยังเซิร์ฟเวอร์ปลายทางสาธารณะหรือเซิร์ฟเวอร์ onion

Q3: เกตเวย์บริดจ์ของ Tor (Tor bridges) คืออะไร?

Bridges คือรีเลย์ทางเข้า Tor ที่ไม่ได้ระบุไว้สาธารณะ ใช้หลบเลี่ยงการบล็อกจาก ISP และการเซ็นเซอร์ในภูมิภาคที่จำกัดการเข้าถึงเบราว์เซอร์ Tor

Q4: ผู้ไม่หวังดีบนดาร์กเว็บใช้ประโยชน์จากสกุลเงินดิจิทัลอย่างไร?

ผู้ก่อภัยคุกคามใช้สกุลเงินดิจิทัลแบบนิรนามเพื่อทำธุรกรรมทางการเงินในตลาดมืดออนไลน์ เลี่ยงการตรวจสอบธุรกรรมธนาคารมาตรฐาน

Q5: ทำไมเสิร์ชเอนจินทั่วไปจึงรวบรวมข้อมูลฐานข้อมูลเชิงลึกไม่ได้?

โปรแกรมครอว์เลอร์ไม่สามารถป้อนข้อมูลเข้าสู่ระบบ แก้ CAPTCHA ด้านความปลอดภัย หรือรันสคริปต์คิวรี SQL ฝั่งแบ็กเอนด์ที่จำเป็นต่อการเข้าถึงฐานข้อมูลดีปเว็บได้

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: เซิร์ฟเวอร์ไดเรกทอรีในเครือข่าย Tor คืออะไร?

เป็นเซิร์ฟเวอร์ที่เชื่อถือได้ซึ่งดูแลรายการรีเลย์ขาเข้า ตรงกลาง และขาออกที่ใช้งานอยู่ ซึ่งไคลเอนต์ใช้สร้างเส้นทางการกำหนดเส้นทาง

Q7: ผู้ไม่หวังดีดักข้อมูลที่โหนดขาออก (exit node sniffing) ได้อย่างไร?

ผู้ดำเนินการโหนดทางออกที่ไม่น่าไว้ใจสามารถดักจับทราฟฟิก HTTP ที่ไม่เข้ารหัสขณะออกจากเครือข่าย Tor เพื่อขโมยชื่อผู้ใช้และคุกกี้

Q8: Tor และ I2P ต่างกันอย่างไร?

Tor ใช้ไดเรกทอรีรีเลย์แบบรวมศูนย์และโหนดทางออกสำหรับเข้าถึงเว็บสาธารณะ ส่วน I2P ใช้โครงสร้างเพียร์ทูเพียร์แบบกระจายศูนย์สำหรับการโฮสต์ภายใน

Q9: หน่วยงานบังคับใช้กฎหมายติดตามตลาดดาร์กเว็บอย่างไร?

หน่วยงานต่างๆ ใช้การวิเคราะห์บล็อกเชน ระบุตำแหน่งการตั้งค่าโฮสต์เซิร์ฟเวอร์จริง และดำเนินปฏิบัติการล่อเพื่อระบุตัวผู้ดำเนินการ

Q10: การรั่วไหลของ DNS ทำลายการไม่เปิดเผยตัวตนของไคลเอนต์ได้อย่างไร?

การรั่วไหลของ DNS เกิดขึ้นเมื่อคำขอ DNS ของเบราว์เซอร์ถูกส่งตรงผ่าน ISP ในพื้นที่ แทนที่จะถูกส่งผ่านเครือข่าย Tor ที่เข้ารหัส

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ดีปเว็บใหญ่กว่าเซอร์เฟซเว็บที่ค้นหาได้มาก เพราะเนื้อหาส่วนใหญ่อยู่หลังการเข้าสู่ระบบและฐานข้อมูล

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ดาร์กเว็บเป็นส่วนเล็กๆ ของดีปเว็บที่ถูกซ่อนไว้โดยเจตนา เข้าถึงได้ด้วยเครื่องมืออย่าง Tor

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การกำหนดเส้นทางของ Tor เข้ารหัสแพ็กเก็ตข้อมูลสามชั้น โดยลอกชั้นการเข้ารหัสออกทีละชั้นเหมือนหัวหอมที่รีเลย์แต่ละโหนด

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

Tor พัฒนามาจากโครงการ onion routing ของห้องปฏิบัติการวิจัยกองทัพเรือสหรัฐฯ และโค้ดถูกเผยแพร่เป็นซอฟต์แวร์เสรี [1]

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ที่อยู่ Onion เป็นสตริงตัวอักษรและตัวเลข 56 ตัวที่สร้างด้วยวิธีเข้ารหัสจากคู่กุญแจสาธารณะ

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

โหนดขาออกอ่านทราฟฟิกที่ไม่เข้ารหัสได้ ซึ่งหมายความว่ายังต้องใช้ TLS/HTTPS บน Tor เพื่อข้อมูลเซสชันที่ปลอดภัย

7. ข้อมูลเชิงลึกด้านความปลอดภัย

เว็บไซต์อินทราเน็ต คลาวด์ไดรฟ์ และฐานข้อมูลส่วนตัวเป็นส่วนจัดเก็บข้อมูลที่ใหญ่ที่สุดในดีพเว็บ

8. ข้อมูลเชิงลึกด้านความปลอดภัย

เครื่องมือค้นหาเฉพาะทางอย่าง DuckDuckGo ให้บริการพอร์ทัลหัวหอมเพื่อให้ค้นหาแบบไม่เปิดเผยตัวตนบนเครือข่าย Tor

9. ข้อมูลเชิงลึกด้านความปลอดภัย

ผู้ใช้กว่า 2 ล้านคนเชื่อมต่อเครือข่าย Tor ทุกวันเพื่อหลีกเลี่ยงการเซ็นเซอร์และรักษาความเป็นส่วนตัวของการสื่อสาร

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ปฏิบัติการของหน่วยงานบังคับใช้กฎหมายทั่วโลก (เช่น Operation Bayonet) ปิดตลาดมืดรายใหญ่ด้วยการยึดฮาร์ดแวร์โฮสติ้ง

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 **การจัดทำดัชนีของเครื่องมือค้นหา** เว็บลึก — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

หน้าเว็บลึกอยู่หลังหน้าล็อกอินและฐานข้อมูล ทำให้สไปเดอร์ของเสิร์ชเอนจินคลานเข้าไปไม่ได้ แหล่งอ้างอิง: IETF RFC 3986.

2 **การเข้าถึง Tor** ดาร์กเว็บ — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

ดาร์กเว็บประกอบด้วยบริการ onion ที่ซ่อนอยู่ ซึ่งเข้าถึงได้ผ่านเบราว์เซอร์อย่าง Tor เท่านั้น อ้างอิง: IETF RFC 3986.

3 **ฐานข้อมูลลึก** ฐานข้อมูล — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

บัญชีที่ป้องกันด้วยรหัสผ่านและบันทึกขององค์กรเป็นส่วนที่ใหญ่ที่สุดของดีปเว็บ อ้างอิง: NIST Digital Identity.

4 **การกำหนดเส้นทางแบบหัวหอม** เครือข่าย Tor — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

การกำหนดเส้นทางแบบหัวหอมเข้ารหัสแพ็กเก็ตข้อมูลเป็นชั้นๆ แล้วส่งต่อผ่านหลายโหนดเพื่อการไม่เปิดเผยตัวตน อ้างอิง: IETF RFC 3986.

5 **โดเมนหัวหอม** นามสกุลโดเมน — **คำตอบที่ถูกต้อง: A**

หมายเหตุสำหรับผู้สอน

ส่วนต่อท้ายโดเมน.onion แบบเข้ารหัสลับส่งทราฟฟิกภายใน Tor โดยไม่ต้องใช้ DNS สาธารณะ อ้างอิง: IETF RFC 3986.

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **ส่วนเว็บ** โครงสร้าง **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

ดีปเว็บครอบคลุมหน้าที่ไม่ถูกทำดัชนีทั้งหมด ส่วนดาร์กเว็บเป็นส่วนย่อย onion ที่เข้ารหัสขนาดเล็ก อ้างอิง: IETF RFC 3986.

7 **อินทราเน็ตองค์กร** เว็บลึก **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

เว็บไซต์อินทราเน็ตอยู่หลังพอร์ทัลรหัสผ่านและไม่ถูกทำดัชนี หมายความว่าเป็นส่วนหนึ่งของดีพเว็บ การอ้างอิง: NIST Digital Identity.

8 **การเข้ารหัสแบบหลายชั้น** รีเลย์ **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

รีเลย์ Onion ถอดรหัสเพียงชั้นการกำหนดเส้นทางเดียวเพื่อปกป้องการไม่เปิดเผยตัวตนของผู้ใช้ ไม่ใช่ทั้งแพ็กเก็ต อ้างอิง: IETF RFC 3986.

9 **ความเสี่ยงจากมัลแวร์** ภัยคุกคาม **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

ตลาดบนเว็บมืดไม่มีการกรองด้านความปลอดภัย จึงมีความเสี่ยงสูงมากที่จะติดมัลแวร์ แหล่งอ้างอิง: Center for Internet Security (CIS).

10 **คำถาม 10** **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

โปรแกรมครอว์เลอร์ของเสิร์ชเอนจินทั่วไปไม่ใช้ Tor จึงเข้าถึงหรือทำดัชนีเว็บไซต์ .onion ไม่ได้

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

H 1. ส่วนของดีปเว็บ	A 2. พอร์ทัลดาร์กเว็บ	D 3. นามสกุล Onion	B 4. การกำหนดเส้นทาง Tor
F 5. หน้าที่ถูกทำดัชนี	G 6. การไม่เปิดเผยตัวตนของผู้ใช้	C 7. ฐานข้อมูลส่วนตัว	E 8. เกตเวย์ทางเข้า

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ดีปเว็บ	2 ดาร์กเว็บ	3 โอเนียน	4 เส้นทาง
5 จัดทำดัชนี	6 นิรนาม		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 F – นิรนาม	2 G – ฐานข้อมูล	3 D – เส้นทาง	4 A – ดีปเว็บ
5 B – ดาร์กเว็บ	6 C – โอเนียน	7 H – โหนดทางเข้า	8 E – จัดทำดัชนี

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย ส่วนของดีปเว็บ พอร์ทัลดาร์กเว็บ และ นามสกุล Onion ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

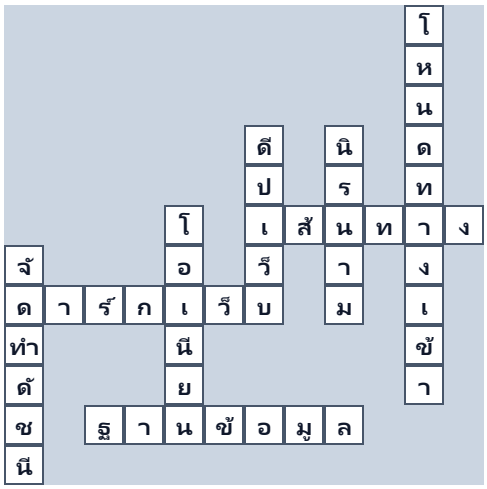
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ร	ต	อ	า	นี	า	น	นี	ส	ช	มี	ฟ	บ	า	า
ห	นี	ม	า	ม	กี	จ	า	โ	า	ดี	รี	ต	ว	ย
ง	ก	า	ค	จ	น	ตี	ว	ร	อ	ป	ตี	ว	า	ล
ล	ด	น	นี	ช	ดั	ทำ	ด	จั	า	เ	อ	ย	ช	ฟ
ก	ก	ร	ล	ม	โ	า	ป	อ	อ	วิ	นี	ม	เ	มี
ล	า	นิ	ล	ล	ห	ป	ด	จ	า	บ	นี	ย	ส้	กี
มู	พ	ร	ง	า	น	ช	า	า	า	ลี	จ	ดี	น	า
อ	น	ล	ผ	ดี	ด	ช	ก	ด	ร์	า	ต	า	ท	จ
ข้	า	ค	ก	ดี	ท	า	ช	ว	ก	ก	ด	กี	า	ด
น	ท	ผ	ฟ	ช	า	มี	ม	อ	ต	ฟ	เ	ร	ง	ดี
า	า	ท	า	ส	ง	ท	ข	ข	า	น	ก	ว็	า	ล
ฐ	า	ม	ร	มี	เ	า	ร	ช	ก	ด	ง	น	บ	ร
ต	สี	ย	ข	มี	ข้	ดี	ด	ด	ว	บ	ฟ	อ	า	ร
ห	ห	รี	น	ผ	า	นี	ม	ผ	ดี	ข	กี	ส	บ	ลี
ง	ด	ร	ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

5 แนวนอน: เส้นทาง การเข้ารหัสข้อมูลเป็นชั้นๆ แล้วส่งต่อผ่านสามโหนด (6 ตัวอักษร)

7 แนวนอน: ดาร์กเว็บ ส่วนของเครือข่ายที่เข้ารหัสซึ่งเข้าถึงได้ผ่านเบราว์เซอร์พิเศษเท่านั้น (7 ตัวอักษร)

8 แนวนอน: ฐานข้อมูล ที่จัดเก็บส่วนหลังที่ปลอดภัยซึ่งเก็บบันทึกของระบบที่ไม่ได้จัดทำดัชนี (7 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: โหนดทางเข้า โหนดจุดเข้าที่ใช้เข้าถึงเครือข่าย Tor (10 ตัวอักษร)

2 แนวตั้ง: ดีปเว็บ เนื้อหาเว็บที่ไม่ได้จัดทำดัชนี เช่น การเข้าสู่ระบบส่วนตัว อีเมล และบันทึกฐานข้อมูล (5 ตัวอักษร)

3 แนวตั้ง: นิรนาม การปกปิดไอพีสาธารณะของไคลเอนต์จากเซิร์ฟเวอร์ (5 ตัวอักษร)

4 แนวตั้ง: โอเนียน คำต่อท้ายโดเมนระดับบนสุดแบบเข้ารหัสลับที่ใช้บนเครือข่าย Tor (6 ตัวอักษร)

6 แนวตั้ง: จัดทำดัชนี เนื้อหาเว็บบนพื้นผิวที่ถูกรวบรวมและค้นหาได้บน Google (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. วีเดีบป → ดีปเว็บ
2. นโยเนือ → โอเนียน
3. จัทำดันีชด → จัดทำดัชนี
4. ลาอข้มูฐน → ฐานข้อมูล
5. เบกร์ดวิา → ดาร์กเว็บ
6. าทเนงส้ → เส้นทาง
7. ามนินร → นิรนาม
8. ขัดาาโทหงเน → โหนดทางเข้า

เฉลยภารกิจรหัสลับ

"รักษา ความ นิรนาม ด้วย เส้นทาง หัวหอม"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การระบุข้อมูลรั่วไหล

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: การตรวจสอบความปลอดภัยขององค์กรพบว่าข้อมูลฐานข้อมูลลูกค้าที่ละเอียดอ่อนถูกซื้อขายในตลาด onion ข้อมูลนั้นไม่ถูกจัดทำดัชนีบน Google
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ส่วนที่เกี่ยวข้อง: ฐานข้อมูลส่วนตัวอยู่ใน deep web (ไม่ถูกจัดทำดัชนีแต่ปลอดภัย) ส่วนตลาดที่ซื้อขายข้อมูลที่ถูกขโมยอยู่บน dark web (เครือข่าย onion) เกิดขึ้นได้อย่างไร: แฮกเกอร์ข้ามการป้องกันของเซิร์ฟเวอร์ ขโมยฐานข้อมูลจาก deep web และลงขายแบบไม่เปิดเผยตัวตนบน dark web เพื่อหลบการติดตามของเจ้าหน้าที่บังคับใช้กฎหมาย

B กรณีศึกษาที่ 2: การไม่เปิดเผยตัวตนเทียบกับความเสี่ยงจากมัลแวร์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: นักวิเคราะห์ต้องการตรวจสอบฟีดข่าวกรองภัยคุกคามบนเว็บไซต์ Tor เขาดาวน์โหลดเบราว์เซอร์ Tor และเข้าถึงเว็บไซต์
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ประโยชน์: Tor กำหนดเส้นทางทราฟฟิกผ่านสามโหนด ซ่อน IP ขององค์กรของนักวิเคราะห์ ความเสี่ยงและการลดความเสี่ยง: ลิงก์ดาร์กเว็บไม่มีการคัดกรองชื่อเสียง นักวิเคราะห์ต้องรัน Tor ภายในเครื่องเสมือน (VM) ที่แยกต่างหาก ปิด JavaScript ในการตั้งค่า Tor และหลีกเลี่ยงการดาวน์โหลดไฟล์ใดๆ เพื่อปกป้องเครือข่ายขององค์กร