



กิจกรรมการแข่งขันด้านความปลอดภัยทางไซเบอร์ Zero Day Quest CTF

รายละเอียดการแข่งขันการแก้โจทย์ปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์

วันอังคารที่ 13 มกราคม 2569

วัตถุประสงค์

- เพื่อส่งเสริมและสนับสนุนให้ผู้เข้าร่วมได้พัฒนาทักษะและความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านการแก้ปัญหาในรูปแบบ Capture The Flag
- เพื่อเปิดโอกาสให้ผู้มีความสามารถได้แสดงศักยภาพและฝึกฝนทักษะทางด้านความมั่นคงปลอดภัยไซเบอร์
- เพื่อสร้างความตระหนักรู้ถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์และส่งเสริมการใช้งานเทคโนโลยีอย่างมีจริยธรรม
- เพื่อเป็นเวทีในการแลกเปลี่ยนความรู้และสร้างเครือข่ายระหว่างผู้ที่สนใจในสายงานความมั่นคงปลอดภัยไซเบอร์

กติกาการแข่งขัน

- เวลาที่ใช้ในการแข่งขัน 3 ชั่วโมง (19:30-21:30 น.)
- ขณะทำการแข่งขันไม่อนุญาตให้ผู้เข้าแข่งขันออกนอกสถานที่แข่งขัน หากมีความจำเป็นให้คณะกรรมการพิจารณาอนุญาตเป็นราย ๆ ไป
- อนุญาต
 - ใช้ทุกวิถีทางที่ไม่ขัดแย้งกับกฎเพื่อหามาซึ่งคำตอบของโจทย์ข้อนั้น
 - สามารถสื่อสารกับสมาชิกในทีมเดียวกันที่เข้าแข่งขันได้
 - สามารถใช้อุปกรณ์คอมพิวเตอร์พกพาส่วนตัว (laptop) ในการแข่งขันได้
 - ระหว่างแข่งขัน ผู้เข้าแข่งขันสามารถใช้เครื่องมือช่วยเหลือใด ๆ ก็ได้ในการแข่งขัน
 - เพื่อจะแก้โจทย์ข้อนั้น เช่น Google search, Generative AI & AI Tools, Cyberchef, Log Analyzer, Linux, Decompiler , อื่น ๆ
- ไม่อนุญาต
 - ห้ามสื่อสารกับผู้เข้าแข่งขันทีมอื่นระหว่างทำการแข่งขัน หากฝ่าฝืนจะมีบทลงโทษคือให้ทีมที่ฝ่าฝืนหมดสิทธิในการแข่งขันต่อ
 - ห้ามใช้งานอุปกรณ์สื่อสาร (มือถือ, แท็บเล็ต) หรือ โปรแกรมที่สามารถสื่อสารกับผู้อื่น หรือ website Social Media ระหว่างการแข่งขัน จะถือว่าเป็นการสื่อสารกับทีมอื่น และจะหมดสิทธิในการแข่งขันต่อ
 - ห้ามสื่อสารกับ staff ในเชิง ขอช่วยเหลือ, ขอวิธีทำ, ขอคำตอบ, ขอคำใบ้ หรือ ส่อในเชิงทุจริต เพื่อให้มีความได้เปรียบเหนือผู้เข้าแข่งขันทีมอื่น หากฝ่าฝืนจะมีบทลงโทษคือ ให้ทีมที่ฝ่าฝืนหมดสิทธิในแข่งขันต่อ
 - ห้ามทำการส่งคำตอบ หรือ วิธีการได้มาซึ่งคำตอบ หรือ ส่วนใดส่วนหนึ่งของคำตอบ แก่ผู้เข้าแข่งขันทีมอื่น หากฝ่าฝืนจะมีบทลงโทษคือ ให้ทีมที่ฝ่าฝืนหมดสิทธิในแข่งขันต่อ



กิจกรรมการแข่งขันด้านความปลอดภัยทางไซเบอร์ Zero Day Quest CTF

- ห้ามทำการโจมตี(Attack), การดักจับข้อมูล(Sniffing), การปลอมแปลงข้อมูล(Spoofing) หรือการโจมตีเครือข่ายทั้งแบบ สาย(Wired) และ ไร้สาย(Wireless) จนเป็นเหตุให้ผู้เข้าแข่งขันทีมอื่นได้รับผลกระทบ บทลงโทษคือ ให้ทีมที่ฝ่าฝืนหมดสิทธิในแข่งขันต่อ
- ห้ามขัดขวางการแข่งขันของทีมอื่น บทลงโทษคือให้ทีมที่ฝ่าฝืนหมดสิทธิในแข่งขันต่อ
- ห้ามโจมตี Website ที่ใช้ในการจัดการแข่งขัน หากฝ่าฝืนจะมีบทลงโทษคือ ให้ทีมที่ฝ่าฝืนหมดสิทธิในแข่งขันต่อ
- การโจมตีไปยัง Website ที่เป็นโจทย์ในการแข่งขัน จะถือว่าเป็นการโจมตีไปยัง Website ที่ใช้จัดการแข่งขัน
- ห้ามทำการสุ่มคำตอบแล้วส่งคำตอบไปยัง website ที่ใช้แข่งขัน โดยใช้โปรแกรม หรือ สคริปต์ (Brute Force) จะถือว่ามีความผิดในการพยายามโจมตี โจทย์ website ที่ใช้ในการแข่งขัน (ยกเว้นว่าโจทย์ข้อนั้นอนุญาตให้ทำการ Brute Force ได้)
- หากผู้เข้าแข่งขันประมาทไปโหลด tools ที่แฝง malware, worm ผลกระทบที่เกิดขึ้นกับการแข่งขัน จะถือว่าเป็นผลกระทบมาจากทีมดังกล่าวโดยไม่สามารถปฏิเสธได้
- ห้ามทำการโจมตีเว็บไซต์ zdqctf.lol หรือ เว็บไซต์ที่ใช้ในการแข่งขัน การใช้งานช่องโหว่ซึ่งทำให้ website ได้รับผลกระทบไปด้วย จะถือว่ามีความผิดตามกฎหมาย

รูปแบบการแข่งขัน

- ในการแข่งขันโจทย์จะมีทั้ง ภาษาอังกฤษ และ ภาษาไทย ผู้เข้าแข่งขันสามารถใช้เครื่องมือเพื่อช่วยในการแปลภาษาได้
- เป็นการแข่งขัน Cyber Security ในรูปแบบการชิงธง (Capture The Flag)
- Platform แข่งขันเป็น Website สามารถเข้าถึงได้จาก Network ภายในขณะเท่านั้น
- ในการแข่งขันโจทย์ทุกข้อจะถูกปล่อยให้ทำพร้อมกัน
- เวลาแข่งขัน 3 ชั่วโมง ตั้งแต่เวลา 19:30 น. เป็นต้นไป และ สิ้นสุด ณ เวลา 21.30 น.
- โจทย์มีทั้งหมด 3 ประเภทคือ
 - Static file โจทย์จะเป็นลักษณะไฟล์ที่ให้ทำการดาวน์โหลดลงในเครื่อง แล้วทำการหาคำตอบจากโจทย์ข้อนั้นมาให้ได้
 - Website โจทย์ที่จะทำการเปิด instance website ภายนอกให้เข้าไปทำโจทย์
 - Virtual Machine โจทย์ที่จะให้ไฟล์ Virtual machine มาให้ไปสืบเหตุการณ์ที่เกิดขึ้นจากเครื่องแล้วนำมาเป็นคำตอบของโจทย์
- หัวข้อของโจทย์ประกอบไปด้วย Web Exploitation, Reverse Engineering, Digital Forensics, Cryptography, Network Security, Programming, Mobile Security
- ผู้เข้าแข่งขันสามารถเลือกทำข้อใดก่อนก็ได้ไม่จำเป็นต้องทำตามลำดับ หรือ หัวข้อ/ประเภท ของโจทย์
- แต่ละหัวข้อ จะมีจำนวนโจทย์ไม่เท่ากัน
- โจทย์แต่ละข้อจะมีคะแนนไม่เท่ากันซึ่งขึ้นอยู่กับระดับความยาก



กิจกรรมการแข่งขันด้านความปลอดภัยทางไซเบอร์ Zero Day Quest CTF

- การส่ง flag หรือ คำตอบ สามารถส่งได้ไม่จำกัดจำนวนครั้ง
- Tools ที่ใช้สำหรับการแก้โจทย์หา Flag หรือ คำตอบ จะไม่ตายตัวผู้เข้าแข่งขันสามารถใช้เครื่องมือ และ วิธีการใดก็ได้เพื่อให้ได้ Flag หรือ คำตอบ ออกมา ซึ่งวิธีการ และ เครื่องมือ ดังกล่าวต้องไม่ส่งผลกระทบต่อการแข่งขัน ผู้เข้าร่วมทีมอื่น หรือ ระบบอื่นที่ไม่เกี่ยวข้องกับการแข่งขัน
- ในการแข่งขันนี้จะใช้ระบบให้คะแนนแบบ Dynamic Scoring คะแนนที่ได้จากข้อที่ทำผ่านแล้วจะขึ้นอยู่กับจำนวนทีมที่ทำผ่านในข้อนั้นด้วย แต่จะลดต่ำสุดไม่เกิน 80% ของคะแนนของข้อนั้น
- สำหรับทีมที่แก้โจทย์ข้อใดได้เป็นทีมแรก จะได้คะแนนจากข้อนั้น จะเพิ่มขึ้น 5%
- สำหรับทีมที่แก้โจทย์ข้อใดได้เป็นทีมที่ 2 จะได้คะแนนจากข้อนั้น จะเพิ่มขึ้น 3%
- ในโจทย์แต่ละข้อจะมีคำใบ้ หรือ ไม่ก็ได้ และ โจทย์บางข้ออาจมีได้มากกว่า 1 คำใบ้
- การเปิดดูคำใบ้จะไม่เสียคะแนน
- การแข่งขันไม่จำเป็นต้องเขียน DFIR / Wrap-Up ส่ง

เกณฑ์การตัดสินคะแนน

- มีการใช้งานสัญลักษณ์ดาว ในการบอกระดับความยาก มีตั้งแต่ 0 - 5 ดาว แสดงถึงระดับความยากตั้งแต่ ง่าย ไป ถึง ยาก โดยคะแนน แต่ละข้อจะขึ้นอยู่กับความยากของข้อนั้น
- หากรางวัลใดที่มีทีมที่ได้รางวัลเดียวกันมากกว่า 1 ทีม เพราะมีคะแนนรวมเท่ากัน ให้พิจารณาช่วงเวลาที่ได้คะแนน แทนโดยให้พิจารณาทีมที่ทำคะแนนได้เร็วกว่าเป็นฝ่ายชนะ
