CTF

Capture The Flag

CTF คืออะไร

CTF ย่อมาจาก Capture The Flag เป็นรูปแบบการแข่งขันด้านความปลอดภัยคอมพิวเตอร์ (Cybersecurity Contest) ที่ผู้เข้าแข่งขันจะต้อง “ค้นหา” และ “เก็บธง” (Flag) ซึ่งก็คือรหัสหรือข้อความที่ซ่อนอยู่ในโจทย์ต่างๆ ให้ได้เร็วที่สุดและถูกต้องที่สุด โดยทั่วไปแบ่งออกเป็นสองรูปแบบหลัก

- Jeopardy-Style
- Attack-Defense

Jeopardy-Style CTF

โจทย์ถูกแบ่งเป็นหมวดหมู่ย่อย ๆ เช่น

- Cryptography - ถอดรหัส ข้อความที่ถูกเข้ารหัส
- Reverse Engineering - วิเคราะห์ Binary หรือโปรแกรมเพื่อค้นหา Flag
- Web Exploitation - หาช่องโหว่บนเว็บแอปพลิเคชัน
- Steganography - การซ่อนข้อมูลลับ เช่น ไฟล์ภาพ เสียง วิดีโอ หรือเอกสาร
- Networking - วิเคราะห์หรือดักจับข้อมูลที่วิ่งผ่านเครือข่าย
- Forensics - วิเคราะห์ไฟล์ภาพ การ์ดข้อมูล หรือเครือข่าย เพื่อตามหาเบาะแส
- Binary Exploitation (Pwn) - เขียน Exploit เพื่อเจาะโปรแกรมระดับบิต

และอื่นๆ ซึ่งแต่ละโจทย์มีคะแนนไม่เท่ากัน ขึ้นกับความยากง่าย ผู้แข่งขันสะสมคะแนนจากการเก็บ Flag

Attack-Defense CTF

ทีมแต่ละทีมจะมี Server หรือระบบของตัวเองที่มีช่องโหว่เหมือนกัน เป้าหมายคือ ป้องกันระบบตัวเองจากการโจมตี และในขณะเดียวกันก็ต้อง โจมตีระบบของทีมอื่น เพื่อขโมย Flag ทีมที่สามารถ ป้องกันได้ดี และโจมตีได้สำเร็จ จะได้คะแนนสูงสุด โดยต้องใช้ทั้งทักษะการวิเคราะห์ช่องโหว่, การเขียน Exploit, การ Patch ระบบ, และการตั้งรับเครือข่าย

Platform สำหรับฝึกซ้อม CTF

- SECPlayground: เรียนรู้และฝึกเจาะระบบ และมีจัด CTF ฟรีตามเทศการต่างๆ เช่น ช่วงปีใหม่, สงกรานต์
- TryHackMe: มี Learning paths, Challenges และ CTF แบบกำหนดเอง สำหรับทุกระดับความสามารถ
- HackTheBox: มีโจทย์ CTF หลากหลาย พร้อม Platform ใหม่ที่ปรับปรุงให้ใช้งานได้ดีขึ้น
- picoCTF: Platform ที่เป็นมิตรกับผู้เริ่มต้น พัฒนาโดยมหาวิทยาลัย Carnegie Mellon มาพร้อมเนื้อเรื่องและโจทย์ที่ค่อยๆ ยากขึ้น

ทักษะที่ใช้ในการแข่ง CTF

- พื้นฐานระบบปฏิบัติการ Linux, Windows และการใช้ Terminal (Command Line)
- พื้นฐานการเขียนโปรแกรม (C, C++, Python, Java, JavaScript, Bash)
- ความเข้าใจระบบไฟล์, Network protocols
- พื้นฐานการวิเคราะห์ Binary และ Reverse engineering
- พื้นฐาน Crypto และคณิตศาสตร์
- การสังเกตและการค้นหาข้อมูล

Challenges

- Cryptography
- Steganography
- Network
- Web Application
- Reverse Engineering
- Programming

Cryptography

Cryptography คือศาสตร์และเทคนิคในการ ปกป้องข้อมูล ด้วยวิธีการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถเข้าใจได้โดยผู้ไม่ได้รับอนุญาต (เช่น การเข้ารหัส) และการรับรองความถูกต้องของข้อมูล

จุดประสงค์หลักของ

Confidentiality (ความลับ): ป้องกันไม่ให้ข้อมูลถูกอ่านโดยคนที่ไม่ใช่เจ้าของ

Integrity (ความถูกต้อง): ตรวจสอบว่า ข้อมูลไม่ได้ถูกเปลี่ยนแปลงระหว่างทาง

Authentication (การพิสูจน์ตัวตน): ยืนยันตัวตนของผู้ส่งหรือผู้รับข้อมูล

Non-repudiation (ปฏิเสธไม่ได้): ป้องกันไม่ให้ผู้ส่งปฏิเสธการส่งข้อมูล

Cryptography - คำศัพท์

- Encoding: การแปลงข้อมูลบางอย่างจากรูปหนึ่งไปเป็นรูปหนึ่ง
- Cipher: Algorithm สำหรับการเข้ารหัสหรือถอดรหัส
- Plaintext: ข้อความที่ยังไม่ได้เข้ารหัสหรือข้อความต้นฉบับ
- Ciphertext: ข้อความที่ถูกเข้ารหัส (โดยปกติจะดูเหมือนเป็นตัวอักษรที่ไม่สามารถเข้าใจได้)
- Frequency Analysis: วิธีทางสถิติในการ crack ซึ่งถือว่าตัวอักษรที่พบบ่อยที่สุดในข้อความเข้ารหัสจะตรงกับตัวอักษรที่พบบ่อยที่สุดในภาษา plaintext
- Key: ข้อมูลที่ใช้ระบุการเปลี่ยนแปลงหรือก็คือกุญแจ
- Symmetric Cipher: ใช้ key เดียวกันในการเข้ารหัสและถอดรหัสข้อความ เช่น ROT13
- Asymmetric Cipher: ใช้ key สองตัวคือ ตัวแรกใช้เข้ารหัส ตัวที่สองใช้ถอดรหัส เช่น RSA

Cryptography - Bin, Octal, Dec, Hex and ASCII

ASCII (American Standard Code for Information Interchange) คือมาตรฐานการแทน ตัวอักษร, ตัวเลข และสัญลักษณ์ ด้วย รหัสตัวเลข 7 บิต (0-127)

ตัวอย่าง

"abc ABC" -> "97 98 99 32 65 66 67"

"123" -> "49 50 51"

Binary (ฐาน 2): ระบบเลขที่ใช้แค่ สองตัวเลข คือ 0 และ 1 เช่น: 1011 = 11 (ฐาน 10)

Octal (ฐาน 8): ใช้ตัวเลข 0-7 เท่านั้น เช่น: 31 = 25 (ฐาน 10)

Decimal (ฐาน 10): ระบบเลขที่ใช้ทั่วไป มีตัวเลข 0-9

Hex (Hexadecimal, ฐาน 16): ใช้ตัวเลข 0-9 และ A-F เช่น: 0x1A = 26 (ฐาน 10)

Cryptography - Base

การเข้ารหัส Base (เช่น Base32, Base64) คือการแปลงข้อมูลให้เป็นรูปแบบที่สามารถอ่านและส่งผ่านระบบที่รองรับเฉพาะตัวอักษรและตัวเลขได้ โดยการใช้ชุดตัวอักษรที่มีขนาดจำกัดเพื่อแทนข้อมูลไบต์ (binary data) ซึ่งนิยมใช้ในการส่งข้อมูลผ่านช่องทางที่ไม่รองรับข้อมูลไบต์โดยตรง

ตัวอย่าง

Base32 “Hello” -> “JBSWY3DP”

Base32 “#!/usr/bin/bash” -> “EMQS65LTOIXWE2LOF5RGC43I”

Base64 “Hello” -> “SGVsbG8=”

Base64 “#!/usr/bin/bash” -> “IyEvdXNyL2Jpbi9iYXNo”

Cryptography - URL Encoding

URL Encoding คือการแปลงอักขระพิเศษใน URL ให้อยู่ในรูปแบบที่สามารถส่งผ่านอินเทอร์เน็ตได้อย่างถูกต้อง โดยใช้เครื่องหมาย % ตามด้วยรหัสเลขฐาน 16 (Hex) ของอักขระ

ตัวอย่าง

"ค่ะ" -> "%E0%B8%84%E0%B9%88%E0%B8%B0"

"A B C" -> "A%20B%20C"

Cryptography - Substitution, ROT13

Substitution (การแทนที่) คือเทคนิคการเข้ารหัสที่ แทนแต่ละตัวอักษรในข้อความต้นฉบับ (plaintext) ด้วยตัวอักษรอื่นตามกฎที่กำหนดไว้

ตัวอย่าง

Plaintext: HELLO WORLD

Rule: ABCDEFGHIJKLMNOPQRSTUVWXYZ -> XYZABCDEFGHIJKLMNOPQRSTUVW

Ciphertext: EBIIL TLOIA

ROT13 คือการเลื่อนตัวอักษรใน A ถึง Z ไปข้างหน้า 13 ตำแหน่ง เช่น A เป็น N ถ้าเข้ารหัสซ้ำอีกครั้งจะได้ข้อความเดิม ใช้ซ่อนข้อความง่ายๆ

ตัวอย่าง

“HELLO WORLD” -> “URYYB JBEYQ”

Cryptography - Vigenère Cipher

Vigenère Cipher คือการเข้ารหัสแบบ Polyalphabetic Substitution ใช้คีย์เป็นคำหรือข้อความ เพื่อเลื่อนตัวอักษรใน plaintext ทีละตัวตามตัวอักษรในคีย์ ทำให้มีความปลอดภัยมากกว่า Caesar cipher เพราะเปลี่ยนการเลื่อนตามคีย์ที่ยาวและซับซ้อน

ตัวอย่าง

Key “key” : “HELLO WORLD” -> “RIJVS UYVJN”

Key “hello” : “ab12ce45fg” -> “hf12np45tn”

Cryptography - RSA

RSA (Rivest-Shamir-Adleman) เป็น Algorithm เข้ารหัสแบบ อสมมาตร (Asymmetric Cryptography) ซึ่งใช้คู่กุญแจ 2 ชุด ได้แก่

Public Key (กุญแจสาธารณะ) ใช้สำหรับเข้ารหัสข้อมูล

Private Key (กุญแจส่วนตัว) ใช้สำหรับถอดรหัสข้อมูล

Cryptography - Hash

ฟังก์ชันแฮช (Hash function) เป็นกระบวนการแปลงข้อมูลทุกขนาดให้กลายเป็นค่าแฮชที่มีความยาวคงที่ (Fixed length) เป็น one-way function คือ แปลงข้อมูลต้นฉบับเป็นค่าแฮช แต่ไม่สามารถย้อนกลับไปหาเนื้อหาเดิมได้ ซึ่งใช้สำหรับตรวจสอบความถูกต้องของข้อมูล, เก็บรหัสผ่าน, การทำ Index ข้อมูล เป็นต้น

ตัวอย่าง

MD5:

"hello" -> "5d41402abc4b2a76b9719d911017c592"

SHA256:

"hello" -> "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"

Cryptography - Tools

CyberChef - https://gchq.github.io/CyberChef/

Web app for encryption, encoding, compression and data analysis.

RsaCracker - https://github.com/skyf0l/RsaCracker

Powerful RSA cracker for CTFs. Supports RSA, X509, OPENSSH in PEM and DER formats.

Crack Station - https://crackstation.net/

Free Password Hash Cracker

Steganography

Steganography คือเทคนิค ซ่อนข้อมูลลับไว้ในสื่ออื่น ๆ เช่น ภาพ เสียง หรือวิดีโอ โดยที่ผู้สังเกตไม่รู้เลยว่ามีข้อมูลซ่อนอยู่

จุดประสงค์หลัก

ซ่อนการมีอยู่ของข้อมูล ไม่ให้ถูกตรวจจับ

แตกต่างจาก Cryptography ที่ทำให้ข้อมูลอ่านไม่ได้ แต่ยังเห็นว่ามีข้อมูลอยู่

Steganography ทำให้ข้อมูลดูเหมือนธรรมดา ไม่มีใครสงสัย

Network

การสื่อสารข้อมูลระหว่างคอมพิวเตอร์ผ่านเครือข่าย เช่น TCP/IP โดยการวิเคราะห์ข้อมูล หรือ กิจกรรมของระบบ เป้าหมายคือการหาหลักฐานที่ซ่อนอยู่ในการสื่อสาร หรือพฤติกรรมของระบบ

หมวดโจทย์ที่เกี่ยวกับ การดักจับ วิเคราะห์ หรือแก้ไขข้อมูล ที่วิ่งในเครือข่าย

ผู้เล่นมักได้รับไฟล์ .pcap (packet capture) หรือให้เชื่อมต่อไปยัง server

วิเคราะห์ Log File

Web Application

โปรแกรมหรือระบบที่ทำงานบนเว็บเบราว์เซอร์ผ่านอินเทอร์เน็ตหรือเครือข่าย ตัวอย่างเช่น เว็บไซต์, ระบบจัดการข้อมูลออนไลน์, เว็บบอร์ด, เว็บแอปพลิเคชันต่างๆ

หมวดหมู่โจทย์ที่เกี่ยวกับความปลอดภัยของเว็บแอป เช่น

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Authentication Bypass
- File Upload Vulnerabilities

Reverse Engineering

กระบวนการ วิเคราะห์และเข้าใจซอฟต์แวร์หรือโปรแกรม โดยไม่ได้มีซอร์สโค้ด ใช้ศึกษาวิธีการทำงาน, โครงสร้าง, หรือค้นหาช่องโหว่ในโปรแกรม

หมวดโจทย์ที่ให้ไฟล์ไบนารี เช่น โปรแกรม EXE, ELF, หรือไฟล์อื่นๆ

ผู้เล่นต้องถอดรหัส, วิเคราะห์ logic, หา key, รหัสผ่าน, หรือ flag จากโปรแกรมนั้น

มักใช้เครื่องมือ เช่น Ghidra, IDA Pro, Radare2, strings, objdump

Programming

การเขียนโปรแกรมคอมพิวเตอร์ เป็นการสั่งให้คอมพิวเตอร์ทำงานตามลำดับขั้นตอน ที่มนุษย์ออกแบบไว้ โดยใช้ภาษาคอมพิวเตอร์ (เช่น Python, C, Java) เพื่อแก้ปัญหา คำนวณ ควบคุม หรือประมวลผลข้อมูลให้ได้ผลลัพธ์ตามที่ต้องการ

หมวด เขียนโปรแกรม เพื่อแก้โจทย์ที่ใช้ตรรกะหรือคณิตศาสตร์

ไม่ใช่การเจาะระบบโดยตรง แต่ใช้ทักษะ คิด วิเคราะห์ และเขียนโค้ด

โจทย์มักต้องการให้เขียนสคริปต์เพื่อคำนวณ ถอดรหัส หรือแก้ปัญหาอัตโนมัติ