Written by Dr. Thapanapong Rukkanchanunt

15 Security 2

OUTLINE

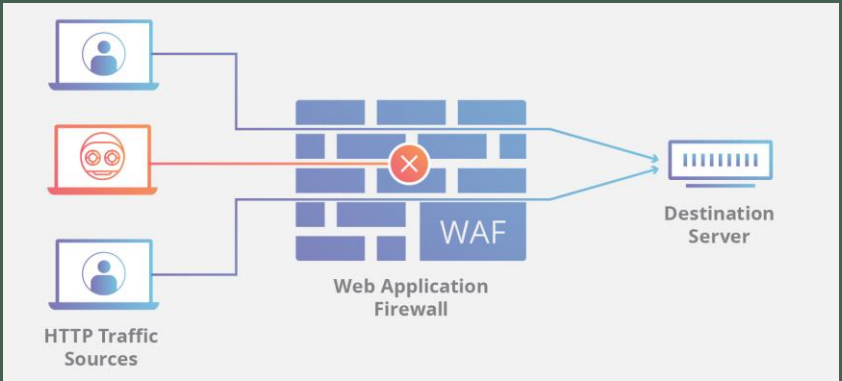
- Defensive Protocol
  - Common Approaches
    - Resource Assignment
    - Web Scanning
  - WAF
  - DDoS Mitigation
  - DNSSEC Protection

Defense against Hacking

- การป้องกันการโจมตีจากแฮกเกอร์สามารถทำได้หลายวิธีมาก วิธีที่มักจะใช้กันทั่วไปมีดังต่อไปนี้ (อาจจะเรียกเป็น Best Practice หรือ Common Approach)
  - ใช้ Up-to-date Encryption
  - ใช้ Authentication ให้ถูกต้อง
  - ติดตามข่าวการรั่วไหลของข้อมูลแล้วตรวจสอบว่าเว็บแอพของเราตกอยู่ในสถานการณ์เดียวกันหรือไม่
  - Resource Assignment คือการเชื่อมโยงทรัพยากรของเว็บแอพไปยังระบบแจ้งเตือน ทำให้เมื่อมีความพยายามเข้าถึงทรัพยากรดังกล่าว ผู้พัฒนาเว็บจะได้รับคำเตือนก่อนและสามารถป้องกันอันตรายได้ทันที
  - Web Scanning คือการใช้ Tools/Software ในการสแกนหาช่องโหว่ของระบบ แม้ว่าจะเป็นวิธีอัตโนมัติแต่ก็สแกนหาได้แค่ Threats ในอดีต

Web Application Firewall

- ไม่ต่างจากระบบปฏิบัติการ เว็บแอพก็มี Firewall เป็นของคนเอง
- Web Application Firewall (WAF) ใช้ป้องกันการโจมตีที่เกิดจากการใช้ HTTP Request
  - Cross Site Forgery, Cross Site Scripting, SQL Injection
- เช่นเดียวกับ Proxy Server ที่เป็นเหมือนโล่กำบังป้องกันตัวตนของ Client WAF เป็นเหมือน Reverse-Proxy ป้องกันการเข้าถึง Server โดยตรงจาก Client



Whitelist and Blacklist

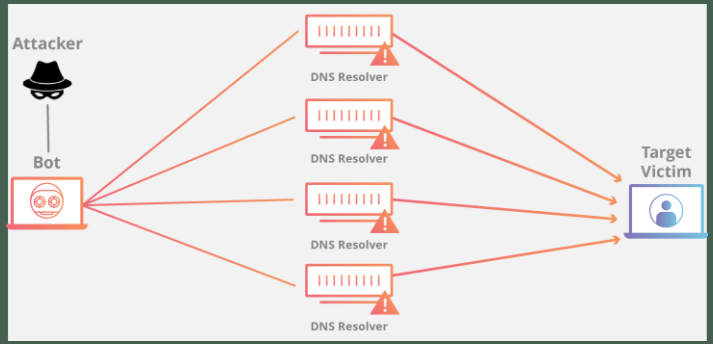
- WAF ทำงานตามกรอบที่กำหนดให้ โดยกรอบสามารถเป็นได้ทั้ง Whitelist และ Blacklist หรือใช้ทั้งสองกรอบร่วมกันได้
- Blacklist คือรายชื่อการกระทำที่ไม่อนุญาตให้ทำได้ ถ้า Client พยายามจะทำการกระทำนั้นก็จะถูกปฏิเสธ ในบางกรณี หากถูกปฏิเสธครั้งแรกแล้วก็อาจจะถูกปฏิเสธในครั้งถัดไป การกระทำที่ไม่อนุญาตอาจจะรวมจำนวนครั้งในการทำอะไรบางอย่าง
- Whitelist ตรงข้ามกับ Blacklist คืออนุญาตให้ทำสิ่งที่กำหนดไว้หรือการกระทำที่การประทับตราว่าปลอดภัย (Pre-approved) แฮกเกอร์ต้องใช้ความพยายามมากในการปลอมแปลงการประทับตราเมื่อต้องต่อสู้กับ Whitelist

WAF Implementations

- Network-based WAF ใช้วิธีการติดตั้ง WAF บน Hardware ที่อยู่ติดกับ Server ที่ต้องการป้องกัน ข้อดีคือไม่มี Latency ข้อเสียคือราคาแพงและต้องบำรุงรักษาอยู่ตลอดเวลา
- Host-based WAF ติดตั้งร่วมกับ Software เลย ข้อดีคือราคาถูกกว่าแบบแรกและ Customize ได้เยอะกว่า ข้อเสียคือใช้ทรัพยากรร่วมกับ Server ทำให้ประสิทธิภาพลดลง
- Cloud-based WAF ใช้บริการ Cloud Service ข้อดีคือใช้งานง่าย มีบริษัทดูแลระบบให้ ค่าบริการตามจำนวน Traffic ที่เข้ามา ข้อเสียคือเป็นบริการภายนอก ข้อมูลผู้ใช้ต้องผ่านมือที่สามก่อนจะมายังเว็บแอพของเรา

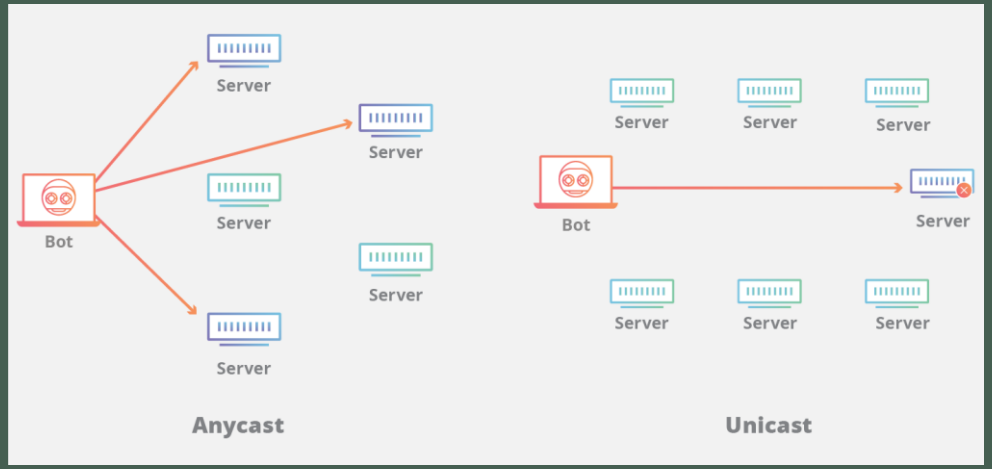
Distributed Denial-of-Service Mitigation

- Distributed Denial-of-Service (DDoS) เป็นรูปแบบการโจมตีที่ถูกใช้รบกวนระบบบ่อยที่สุด
- แฮกเกอร์ใช้ Bot ยิง Request จำนวนมากไปยัง DNS ทำให้ผู้ใช้อื่นที่พยายามจะเข้าเว็บแอพของเราไม่สามารถเข้ามาได้
- วิธีแก้ไขคือการสลับเส้นทาง Request จริงไปยัง Server ที่ถูกต้อง



Anycast

- Anycast คือวิธีการสับเปลี่ยน Network Address ไปยังปลายทางได้หลาย ๆ ที่
- โดยปกติแล้วถ้าเรามี Server หลายที่ Anycast จะส่งต่อ Request ไปยัง Data Center ที่ใกล้ที่สุด
- ในกรณีที่มีหลาย Request ส่งไปยัง Server เดียว Anycast สามารถส่งต่อ Request ไปยัง Server อื่นที่ว่างอยู่แม้จะทำให้ Latency เยอะขึ้นก็ตาม



DNS Security – DNSSEC Protection

- DNS เปรียบเสมือนสมุดโทรศัพท์ของอินเทอร์เน็ต
- Web Browser ส่งข้อมูล Domain Name ไปยัง DNS เพื่อรับข้อมูล IP Address
- แฮกเกอร์สามารถโจมตี DNS ด้วยวิธีการต่าง ๆ เช่น DNS Cache Poisoning, Man-in-the-middle Attack ทำให้ DNS ไม่สามารถเลือก IP Address ที่ถูกต้องได้
- DNSSEC แก้ปัญหาโดยการใช้ Digital Signature ในทุกระดับของ Domain แม้แฮกเกอร์สับเปลี่ยน IP ได้แต่เขาไม่สามารถปลอม Digital Signature ได้ (Public-Key Encryption)

Other Methods

- นอกจากวิธีที่กล่าวมาแล้วเรายังสามารถทดสอบความปลอดภัยของเว็บแอพได้ด้วย Tools ต่าง ๆ เช่น
  - Black Box Testing Tools ทดสอบได้กับระบบทุกรูปแบบ
  - Fuzzing Tools ทดสอบการกรอกข้อมูลผิด ๆ
  - White Box Testing Tools ตรวจสอบโค้ดภายในเช่นโครงสร้างโปรแกรม
  - Password Cracking Tools เราควรศึกษาการทำงานของ Tools เหล่านี้เพื่อใช้ในการป้องกัน

แม้ว่าเราจะป้องกันแต่ละส่วนดีเพียงใด แฮกเกอร์ที่ฉลาดก็ยังสามารถเจาะระบบได้ ดังนั้นระบบความปลอดภัยโดยรวมจึงเป็นสิ่งสำคัญ

Thank you for the semester

- สอบปลายภาค 30%
  - Take Home Exam (23 เมษายน 12:00 – 23:59) ส่งผ่านเว็บ ระบุไว้ในข้อสอบ
  - SQL 15%
  - NoSQL 15%
  - Web Dev 45%
  - Security 35%