SC362006 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY
การโจมตี HTTP FLOODING
GROUP 21

หลักการและเหตุผล

ในปัจจุบันเทคโนโลยีเข้ามามีบทบาทอย่างมากการโจมตีทางไซเบอร์ประเภทหนึ่งที่ใช้ปริมาณการรับส่งข้อมูลอย่างล้นหลามเพื่อทำลายเว็บไซต์หรือเซิร์ฟเวอร์ โดยปกติแล้ว การรับส่งข้อมูลจะถูกส่งผ่านอุปกรณ์ที่ถูกไฮแจ็กจำนวนมาก เช่น คอมพิวเตอร์ สมาร์ทโฟน หรืออุปกรณ์ IOT

วัตถุประสงค์

- ทดสอบ HTTP Flooding บนเว็บไซต์ที่ไม่มีการป้องกัน
- การตรวจดูบันทึกการโจมตี และสถานะเมื่อถูกโจมตี

ทฤษฎีที่เกี่ยวข้อง

HTTP Floodเป็นการโจมตีแบบ Distributed Denial of Service (DDoS) ซึ่งผู้โจมตีจัดการคำขอ HTTP และ POST ที่ไม่ต้องการเพื่อโจมตีเว็บเซิร์ฟเวอร์หรือแอปพลิเคชัน การโจมตีเหล่านี้มักจะใช้คอมพิวเตอร์ที่เชื่อมต่อกันที่ได้ดำเนินการไปด้วยความช่วยเหลือของมัลแวร์ เช่น ม้าโทรจัน แทนที่จะใช้แพ็กเก็ตที่มีรูปแบบไม่ถูกต้อง เทคนิคการปลอมแปลงและการสะท้อนกลับ HTTP Flood ต้องการแบนด์วิดท์น้อยลงในการโจมตีไซต์หรือเซิร์ฟเวอร์เป้าหมาย

ในการฟลัด HTTP ไคลเอ็นต์ HTTP เช่นเว็บเบราว์เซอร์โต้ตอบกับแอปพลิเคชันหรือเซิร์ฟเวอร์เพื่อส่งคำขอ HTTP คำขออาจเป็น "GET" หรือ "POST" จุดมุ่งหมายของการโจมตีคือเมื่อต้องบังคับให้เซิร์ฟเวอร์จัดสรรทรัพยากรให้มากที่สุดเท่าที่จะมากได้เพื่อให้บริการโจมตี ซึ่งจะเป็นการปฏิเสธไม่ให้ผู้ใช้ที่ถูกต้องเข้าถึงทรัพยากรของเซิร์ฟเวอร์

คำขอ GET ใช้เพื่อดึงเนื้อหาคงที่เช่นรูปภาพ โดยทั่วไปแล้วสิ่งนี้จะทำให้เซิร์ฟเวอร์มีภาระงานค่อนข้างต่ำต่อคำขอ

คำขอ POST มักจะต้องการให้เซิร์ฟเวอร์ดำเนินการประมวลผลบางอย่าง เช่น ค้นหารายการในฐานข้อมูล ดังนั้น การโจมตี HTTP POST แบบฟลัดมักจะกำหนดให้มีโหลดที่สูงกว่าบนเซิร์ฟเวอร์ต่อคำขอ

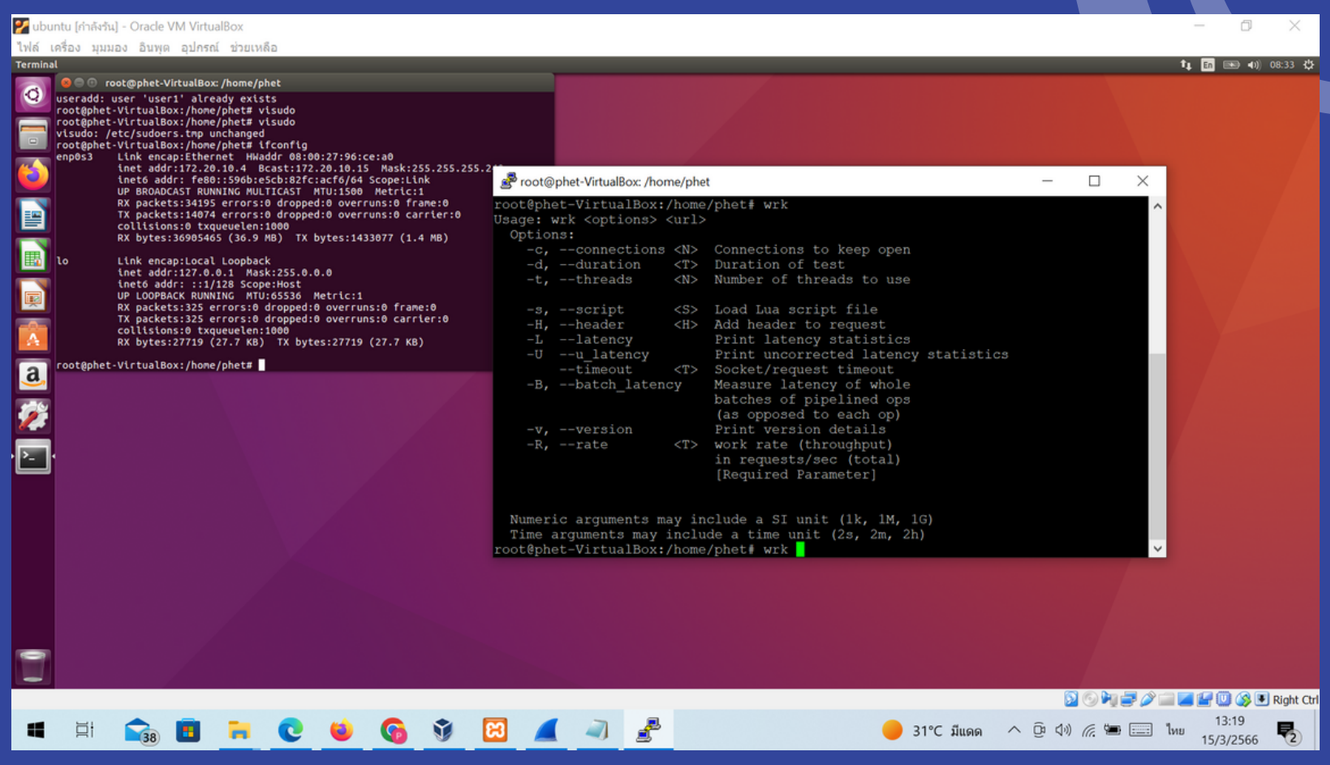
เนื่องจากการโจมตี HTTP Flood ใช้คำขอ URL มาตรฐาน ดังนั้นจึงค่อนข้างท้าทายที่จะแยกความแตกต่างจากการรับส่งข้อมูลที่ถูกต้อง วิธีการบรรเทาผลกระทบที่มีประสิทธิภาพมากที่สุดวิธีหนึ่งคือการรวมกันระหว่างวิธีการสร้างโปรไฟล์การรับส่งข้อมูลซึ่งส่วนใหญ่รวมถึงการระบุชื่อเสียงของ IP การติดตามการกระทำที่ผิดปกติและการใช้ความท้าทายในสถานที่ศักดิ์สิทธิ์ที่ก้าวหน้า

วิธีการทำงาน

หาหน้าเว็ปที่อยากโจมตี และเปิด PAGE SOURCE เพื่อดู CODE และดูว่า ส่งไปที่ ADDRESS อะไรและใช้ MEDTHOD อะไรในการส่ง และใช้ VALUE อะไรบ้างในการส่ง

ขอบเขตการทำงาน

โจมตีเว็ปไซน์ที่อยากโจมตี และ ดูว่าโจมตียังไง และตัวที่โดนโจมตีทำงานยังไง



สรุปผลการดำเนิน

สามารถยิงเว็ปและดูสถานะของทั้ง TARGET และ ATTACKER

SEC 5

1.) 643020581-2 นางสาววิชาภรณ์ กลิ่นจันทน์
2.) 643020589-6 นายอนันต์ยศ ทุมมาลา
3.) 643021296-6 นางสาวกชพร จันทร์เหลือง
4.) 643021307-7 นายภาณุรักษ์ พลดงนอก

รศ.ดร.จักรชัย โสอินทร์
ภาควิชาเทคโนโลยีสารสนเทศ
วิทยาลัยการคอมพิวเตอร์