ชื่อเรื่อง : การป้องกันการโจมตีแบบ Denial of Service

เรียบเรียงโดย : ภูวดล ด่านระหาญ

เผยแพร่เมื่อ : 30 มกราคม 2545

การโจมตีแบบ Distributed Denial of Service (DDoS) มักจะนำเครื่องมือที่จะใช้ในการโจมตีไปติดตั้งบนเครื่องที่ถูกเจาะไว้แล้ว ซึ่งมีจำนวนพอสมควร จากนั้นจึงจะระดมส่งข้อมูลในรูปแบบที่ควบคุมได้โดยผู้ควบคุมการโจมตีไปยังเหยื่อหรือเป้าหมายที่ต้องการ ซึ่งการโจมตีรูปแบบนี้มักจะก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้อื่นไม่สามารถใช้งานได้ตามปกติ หรือทำให้ระบบที่ถูกโจมตีไม่มีทรัพยากรเหลือพอที่จะให้บริการผู้ใช้ธรรมดาได้

การป้องกันการโจมตีแบบ DoS นั้น จะสามารถทำได้ก็ต่อเมื่อทราบวิธีของการโจมตีก่อน และการป้องกันการโจมตีในบางครั้งก็ไม่สามารถทำได้ในครั้งเดียว ขึ้นอยู่กับรูปแบบการโจมตี สถาปัตยกรรมของเป้าหมายที่ถูกโจมตี ซึ่งการป้องกันอาจจะได้ผลหรือล้มเหลวก็ขึ้นอยู่กับปัจจัยเหล่านี้คือ

- การมีคู่มือหรือเอกสารการใช้งานของระบบเป้าหมายที่ถูกโจมตี
- การตรวจจับการโจมตีสามารถทำได้อย่างรวดเร็วและสามารถค้นหาต้นตอที่แท้จริงได้
- มีวิธีดำเนินการสนองตอบเหตุการณ์ละเมิดความปลอดภัยอย่างเป็นขั้นตอน (incident response)
- และการป้องกันรูปแบบอื่นที่สามารถทำได้

รูปแบบการโจมตีและการป้องกัน

เครื่องมือที่ใช้โจมตีแบบ DDoS มีใช้กันอย่างแพร่หลายมานานหลายปีแล้ว และบรรดาผู้ผลิตเองต่างก็มีวิธีป้องกันการโจมตีเช่นเดียวกัน รูปแบบการโจมตีที่นิยมใช้กันก็มีอย่าง SYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น ซึ่งจะได้ศึกษาในรายละเอียดและวิธีป้องกันกันต่อไป

1. **SYN Flood**
    - **รายละเอียด**
      เป็นการโจมตีโดยการส่งแพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง source ip address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source ip address ไม่ให้ส่งข้อมูล

ตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย

- **การป้องกัน**
  - Cisco Router

    เราเตอร์ของ Cisco มีฟังก์ชันการทำงานชื่อ TCP Intercept ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood โดย TCP intercept software จะพยายามสร้างการเชื่อมต่อกับ client หากสำเร็จการเชื่อมต่อดังกล่าวก็จะถูกส่งไปให้กับเครื่องให้บริการต่อไป ดังนั้นการโจมตีแบบ SYN flood จะไม่สามารถเข้าไปถึงเครื่องเป้าหมายจริงๆ ได้ และเราเตอร์ก็ถูกออกแบบให้รองรับการเชื่อมต่อได้มากกว่าเครื่องให้บริการ (server) อีกด้วย แต่ก็มีข้อเสียคือจะทำให้เราเตอร์ใช้ทรัพยากรมากกว่าปกติ รายละเอียดเพิ่มเติมศึกษาได้จาก http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm

    นอกจากนี้เราเตอร์ของ Cisco ยังมีฟังก์ชันชื่อ Committed Access Rate (CAR) ซึ่งใช้ในการจำกัดแบนด์วิดธ์ที่ใช้สำหรับแต่ละบริการได้ (แก้ไขได้ผ่านทาง extended access control list) ซึ่งไม่เพียงแต่ป้องกันการโจมตีแบบ SYN flood ยังป้องกันการเชื่อมต่อที่ถูกต้องไม่ให้ใช้แบนด์วิดธ์มากเกินไป ซึ่งข้อเสียในการนำไปใช้งานคือในขณะที่เครื่องเป้าหมายถูกโจมตีจะทำให้การเชื่อมต่อจากผู้ใช้ธรรมดาไม่สามารถทำได้ เทคนิคหนึ่งในการนำ CAR ไปใช้งานคือ การจำกัดการเข้าถึงโดยระบุเป็นจำนวน client ที่สามารถเข้าใช้งานได้

  - Checkpoint FW-1

    FW-1 มีฟังก์ชั่นชื่อ SYN Defender ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood โดยใช้หลักการเช่นเดียวกันกับ Cisco's TCP Intercept ซึ่งจะทำให้ SYN packet ถูกหยุดยั้งไว้ที่ FW-1 เช่นเดียวกันกับ Cisco's TCP Intercept ตัว FW-1 เองก็จะใช้ทรัพยากรมากกว่าปกติในการทำงานในลักษณะดังกล่าว

- ไฟร์วอลล์และเราเตอร์ยี่ห้ออื่น
  ส่วนใหญ่จะมีฟังก์ชันที่ป้องกันการโจมตีคล้ายๆ กัน โปรดศึกษาจากคู่มือการใช้งาน

2. **ICMP Flood**
   - **รายละเอียด**
     เป็นการส่งแพ็คเก็ต ICMP จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่
   - **การป้องกัน**
     ระบบส่วนใหญ่สามารถทำงานได้โดยไม่ต้องใช้ ICMP Echo Request ซึ่งสามารถป้องกันการใช้งานได้โดยใช้คำสั่งที่เราเตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ

3. **UDP Flood**
   - **รายละเอียด**
     เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่และ/หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)
   - **การป้องกัน**
     เราเตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop แพ็คเก็ตที่มุ่งโจมตีมายัง port ที่ไม่เป็นที่ต้องการได้ เช่น โจมตีมายัง port ที่ไม่ได้ให้บริการใน port ดังกล่าว ในกรณีที่เป็นการโจมตีเฉพาะ port ที่เปิดให้บริการ เช่น port 53 ก็สามารถป้องกันระบบเป้าหมายได้โดยใช้ CAR เพื่อจำกัดจำนวนข้อมูล

4. **Smurf**
   - **รายละเอียด**
     ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast address ในเครือข่ายที่เป็นตัวกลาง(ปกติจะเรียกว่า amplifier) โดยปลอม source ip address เป็น ip address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง ip address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่
   - **การป้องกัน**
     เช่นเดียวกันกับการโจมตีแบบ ICMP flood เราเตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop ICMP Echo Reply ซึ่งในกรณีนี้ควร drop ICMP Echo Reply ที่ส่งเข้ามาโดยไม่ได้มี

การส่ง ICMP Echo Request ออกไปก่อน ซึ่งการทำงานลักษณะนี้อาจจะทำให้อุปกรณ์ packet filtering ใช้ทรัพยากรเพิ่มขึ้น และในกรณีที่เกิดการโจมตีขึ้นแล้วยังสามารถบล็อก source ip address ของ ICMP Echo Reply ได้ เพราะผู้โจมตีไม่สามารถเปลี่ยนแปลงข้อมูลส่วนนี้ได้

สำหรับผู้ดูแลระบบทั่วไปควรป้องกันไม่ให้ระบบของตัวเองถูกใช้เป็น amplifier โดยการไม่ตอบสนองต่อแพ็คเก็ตที่ส่งเข้ามายัง broadcast address ซึ่งมีวิธีการแก้ไขแยกตามระบบที่ http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

5. **Fraggle**
   - **รายละเอียด**

     เป็นอีกรูปแบบหนึ่งของการโจมตีแบบ Smurf โดยผู้โจมตีจะส่ง UDP Echo Request (UDP port 7) ไปยัง broadcast address ของ amplifier network โดยปลอม source ip address ไปเป็น ip address ของเป้าหมาย ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่ และ/หรือทำให้มีการใช้ทรัพยากรของเป้าหมายจนหมดไป ซึ่งการโจมตียังสามารถใช้ได้กับ UDP, TCP services อื่น เช่น Chargen อีกด้วย

   - **การป้องกัน**

     สามารถป้องกันได้คล้ายๆ กับการป้องกันการโจมตีแบบ Smurf attack โดยใช้เราเตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ drop แพ็คเก็ต UDP/TCP ที่ใช้โจมตีเข้ามา หรืออาจจะใช้วิธีบล็อก source ip address ได้เช่นเดียวกัน

     สำหรับผู้ดูแลระบบทั่วไปควรป้องกันไม่ให้ระบบของตัวเองถูกใช้เป็น amplifier โดยการไม่ตอบสนองต่อแพ็คเก็ตที่ส่งเข้ามายัง broadcast address ซึ่งมีวิธีการแก้ไขแยกตามระบบที่ http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

     อย่างไรก็ตามผู้ดูแลระบบควรยกเลิกการใช้งาน UDP, TCP service บางตัวเช่น Echo, Chargen, Discard ซึ่งไม่มีความจำเป็นในการใช้งานอีกแล้ว ซึ่งสำหรับเราเตอร์ของ Cisco แล้ว สามารถใช้คำสั่งด้านล่างนี้เพื่อยกเลิกบริการดังกล่าว

     no service udp-small-servers

     no service tcp-small-servers

6. **การโจมตีรูปแบบอื่นๆ**
   การโจมตีรูปแบบอื่นๆ สามารถเกิดขึ้นได้ จำเป็นต้องมีการตรวจสอบและป้องกันแก้ไขตามเหตุการณ์ที่เกิดขึ้น

จะทำอย่างไรเมื่อถูกโจมตี

- การโจมตีที่เกิดขึ้นมักจะทำให้เกิดการใช้งานแบนด์วิดธ์จนเต็มที่ เช่น SYN flood ถ้าหากทำการกรองแพ็คเก็ตที่ ISP ได้ ก็จะสามารถลดผลกระทบที่จะเกิดขึ้นได้

- ติดตั้ง hardware ที่มีขีดความสามารถสูงไว้ระหว่างเครือข่ายของ ISP กับของระบบที่ต้องการป้องกัน เช่น การติดตั้งเราเตอร์ประสิทธิภาพสูง ที่สามารถทำ filtering ได้

- โดยปกติการโจมตีแบบ DoS ผู้โจมตีมักจะโจมตีไปยังเป้าหมายโดยระบุเป็น ip address โดยตรง ไม่ได้ผ่านการทำ DNS lookup มาก่อน ดังนั้น เมื่อเกิดการโจมตีขึ้น ยังสามารถหาหนทางหลบหลีกการโจมตีดังกล่าวได้ 2 วิธีคือ 1. เปลี่ยน ip address เมื่อเกิดการโจมตี 2. เปลี่ยน ip address ไปเรื่อยๆ แม้จะไม่มีการโจมตี ซึ่งการกระทำทั้งสองรูปแบบก็มีข้อดีข้อเสียต่างกัน ในรูปแบบแรกจะต้องมีระบบตรวจจับที่ดี สามารถแจ้งเตือนผู้ดูแลระบบให้สามารถปรับเปลี่ยน ip address ได้อย่างรวดเร็ว จะเห็นว่ามีช่องว่างระหว่างการดำเนินงานอยู่ แต่ก็มียังมีข้อดีที่ผู้โจมตีจะไม่สามารถรู้แทกติกนี้จนกว่าจะเริ่มโจมตี ในขณะที่วิธีที่สองจะมีความยากลำบากในการเริ่มโจมตีมากกว่า

  มีวิธีปฏิบัติที่ใช้ได้จริงซึ่งต้องการการแก้ไขเพียงเล็กน้อย และพยายามลดผลกระทบที่จะเกิดขึ้นกับผู้ใช้ให้น้อยที่สุด ดังนี้

  1. **การแก้ไข DNS**
     การแก้ไข DNS entries โดยเปลี่ยน ip address ของระบบที่กำลังถูกโจมตีไปเป็น ip address ใหม่ ให้พยายามลดค่า TTL ของ DNS record ให้น้อยที่สุดเท่าที่จะเป็นไปได้ และพิจารณาว่าควรย้าย DNS server ไปยังลิ้งค์อื่นที่ไม่ใช่ลิ้งค์เดียวกันกับระบบที่กำลังถูกโจมตี โดยพิจารณาได้จาก traffic ที่จะเกิดขึ้นจาก DNS server เครื่องนี้ นอกจากนี้ควรตรวจสอบ secondary DNS server ด้วยว่ามีความพร้อมในการทำงานหรือไม่หาก primary DNS server มีปัญหา

  2. **Network Address Translation**
     หากระบบที่ถูกโจมตีสามารถใช้งาน NAT ได้ ก็จะทำให้ง่ายในการเปลี่ยน ip address หาก

ไม่มี NAT ถูกติดตั้งในระบบไว้แล้ว ก็ควรติดตั้งเพิ่มเติม โดยปกติแล้วเราเตอร์ก็มีความสามารถนี้ นอกจากนี้ควรพิจารณาถึงระบบที่สามารถทำ load balancing ได้ เพื่อกระจายภาระงานให้ทั่วถึง

3. **filter ค่า ip address เดิม**

   traffic ที่เข้ามายัง ip address ตัวเดิมจะมีแค่ traffic ที่เกิดจากการโจมตี และจากผู้ใช้ที่ยังใช้ค่า DNS entry เก่าเท่านั้น(ซึ่งเกิดจากการกระจายตัวของ DNS entry นั้นจะต้องใช้เวลาซักระยะ) ดังนั้นจึงสามารถบล็อก traffic สำหรับ ip address นี้ได้ หากไม่ต้องการให้ traffic ของ ip address ชุดเดิมเข้ามาภายในระบบก็สามารถทำได้โดยการยกเลิก routing สำหรับ ip address เดิมเสีย

4. **ใช้ ip address ชุดใหม่และลิ้งค์ที่แตกต่าง**

   มีวิธีแก้ไขที่ได้ผลอีกวิธีคือ การเปลี่ยนไปใช้ลิ้งค์ชุดใหม่และ ip address บล็อกใหม่ทั้งหมด หากผู้โจมตีหยุดการโจมตีและเปลี่ยนเป้าหมายเป็น ip address ชุดใหม่ ผู้ดูแลระบบก็สามารถเปลี่ยน ip address และลิ้งค์กลับไปเป็นลิ้งค์เดิมได้

5. **การป้องกันการโจมตี DNS server**

   การป้องกันการโจมตีที่กล่าวมาด้านบนนี้ อาศัยฟังก์ชันการทำงานของ DNS server เพื่อกระจายข่าวการเปลี่ยน ip address ชุดใหม่ ดังนั้นผู้โจมตีอาจจะเปลี่ยนเป้าหมายมาเป็น DNS server ก็เป็นได้ โดยสามารถโจมตีมายัง port 53 ทั้ง UDP flood หรือ SYN flood ได้ มีวิธีป้องกันดังต่อไปนี้

   - วางเครื่อง primary DNS server ไว้ในลิ้งค์ที่แยกต่างหาก
   - สำรองข้อมูลของ primary DNS server ไปยังที่ตั้งแห่งใหม่
   - สร้าง secondary DNS server ไว้ในหลายๆ จุด บนลิ้งค์ที่แตกต่างกัน
   - ใช้ primary DNS server ที่ผู้อื่นมองไม่เห็น (unadvertised) และเชื่อมโยงไปยัง secondary DNS server โดยลิ้งค์ที่แยกต่างหาก
   - สร้าง non-advertised secondary DNS server ที่สามารถพร้อม advertise ได้ตลอดเวลา

6. ผู้โจมตี

   หากผู้โจมตีเปลี่ยนเป้าหมายมาเป็น ip address ใหม่ตามที่กำหนด จะทำให้สามารถประมาณการณ์การตั้งรับได้ เช่น

        - เมื่อผู้โจมตีซึ่งควบคุมการโจมตีเปลี่ยนแปลงคำสั่ง ก็จะทำให้เพิ่มโอกาสในการตามจับตัวได้ง่ายขึ้น
        - หากมีการจับตาดู traffic จะทำให้เพิ่มโอกาสในการตามจับตัวได้ง่ายขึ้น

- **URL redirect**

  หากผู้โจมตีทำการโจมตี web server อาจจะพิจารณาใช้การ redirect เพื่อแก้ไขปัญหาได้ โดยการแก้ไข DNS entry เพื่อเปลี่ยน ip address ไปเป็น server ที่ตั้งไว้เพื่อแก้ปัญหาโดยเฉพาะ ซึ่งจะทำ redirection ไปยัง web server ที่แท้จริงไว้ ซึ่งจะทำให้ incoming request ที่เป็นของผู้ใช้ปกติถูก redirect ไปยัง web server ตัวจริง ในขณะที่ traffic ที่เป็นการโจมตีจะไม่ถูก redirect ไป แต่ผู้โจมตีก็สามารถค้นหา ip address ที่แท้จริงของ web server ได้ ดังนั้นจึงควรใช้ network address translation ซึ่งจะช่วยแก้ไขปัญหานี้ได้เป็นอย่างดี

- อาจจะมีการพิจารณาสร้างเส้นทางเชื่อมต่อพิเศษสำหรับ client ที่มีความสำคัญกว่าปกติ เพื่อไม่ให้ได้รับผลกระทบจากเหตุการณ์การโจมตีที่อาจจะเกิดขึ้น

- **คำแนะนำทั่วไป**
    - จัดหาแบนด์วิดธ์ให้มากกว่าความต้องการใช้งานยามปกติ
    - สร้างระบบสำรองทั้งระบบเครือข่ายและระบบของเครื่องให้บริการ
    - ถ้าเป็นไปได้พยายามแยก traffic ให้ออกจากกันให้ได้ เช่น ใช้ ISP คนละแห่งกันสำหรับลิ้งค์ไปยัง web server และลิ้งค์เพื่อใช้งานอินเทอร์เน็ต
    - ติดต่อ network service provider ในเรื่อง
        - นำระบบป้องกันการโจมตีแบบ DoS มาใช้
        - ระบบป้องกัน DoS ที่มีอยู่
        - ข้อมูลติดต่อในกรณีฉุกเฉิน
        - ผู้ให้บริการ upstream
    - ให้กรองข้อมูลที่ไม่มีประโยชน์ทิ้ง เช่น
        - กรอง private ip addresses เช่น 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
        - กรอง broadcast address ซึ่งปกติจะลงท้ายด้วย .255 หรือ .0
        - กรอง loopback address (127.0.0.0/8)
        - ป้องกันการปลอมแปลง ip address โดยกรองแพ็คเก็ตที่มาจากภายนอกและมี source ip address ตรงกันกับ ip address ในระบบเครือข่ายของตนเอง