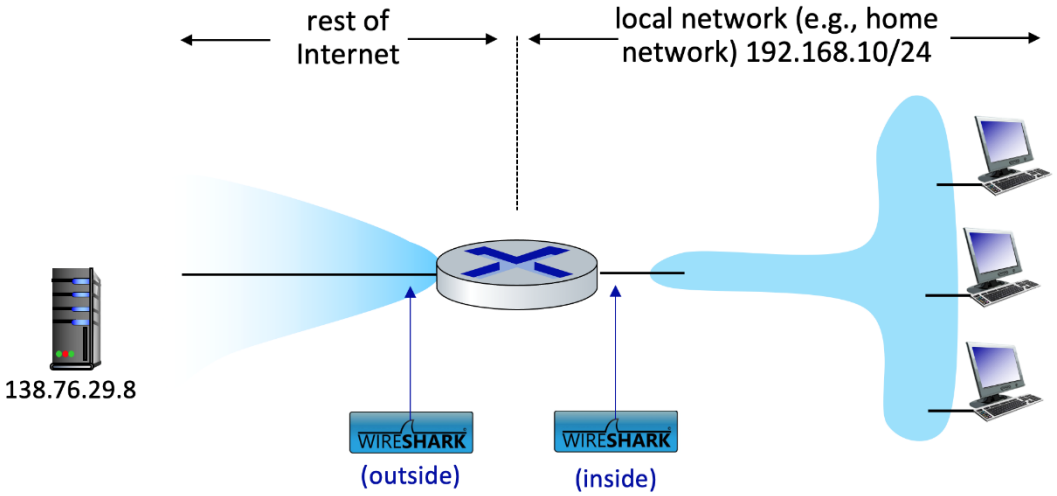
Lab 09: Network Address Translation

ปฏิบัติการในครั้งนี้เราจะมาสำรวจพฤติกรรมการทำ Network Address Translation (NAT) ของ router โดยปฏิบัติการครั้งนี้จะแตกต่างจากครั้งอื่นที่ปกติเราจะดักจับ packets จากจุดเดียว เนื่องจากเราสนใจใน packets ที่ดักจับได้จากทั้งสองจุด นั่นคือทั้งด้านที่เป็น input และ output ของอุปกรณ์ NAT ซึ่งการดักจับ packets จากสภาพแวดล้อมจริงไม่สามารถทำได้โดยง่ายนัก ดังนั้นในปฏิบัติการครั้งนี้ผู้เรียนจะได้ศึกษาและวิเคราะห์ข้อมูลจากไฟล์ที่ได้จัดเตรียมไว้ให้

A. NAT Measurement Scenario

ในปฏิบัติการครั้งนี้ เราได้เตรียมไฟล์ที่ดักจับ packet ซึ่งส่ง HTTP GET message จากเครื่อง client ซึ่งอยู่ใน home network ไปยัง remote server และดักจับ packet ซึ่งเป็น response จาก server นั้น โดยมี router เป็นอุปกรณ์ที่ให้บริการ NAT โดยเราจะดักจับ packets จากสองตำแหน่ง จึงทำให้มีไฟล์ trace อยู่สองไฟล์ ได้แก่

- nat-inside-wireshark-trace1-1.pcapng ซึ่งเป็นไฟล์ที่ดักจับ packets จากฝั่ง local area network (LAN) ของ NAT router โดยอุปกรณ์ใน LAN มี network address เป็น 192.168.10.0/24
- nat-outside-wireshark-trace1-1.pcapng ซึ่งเป็นไฟล์ที่ดักจับ packets จากอีกฝั่งของ router ใกล้กับส่วนที่เชื่อมต่อออกไปยัง Internet ซึ่งเป็นฝั่งด้านซ้ายตาม รูป 1 โดย packets ที่ถูกส่งจาก host ที่อยู่ด้านขวาไปยัง server ที่อยู่ด้านซ้ายจะผ่านการทำ NAT มาแล้วก่อนที่จะมาถึงจุดที่ถูกดักจับ



รูป 1 สถานการณ์ที่ใช้ในการดักจับ NAT packets

ในสถานการณ์ตามที่แสดงใน รูป ๑ มี host นึงจากฝั่ง LAN ส่ง HTTP GET request ไปยัง web server ซึ่งใช้หมายเลข IP เป็น 138.76.29.8 ซึ่ง web server ดังกล่าวได้ส่ง packet ตอบกลับมายัง host ในกรณีนี้เราไม่ได้มุ่งความสนใจไปที่ HTTP GET request นัก แต่เรามุ่งความสนใจไปที่การทำงานของ NAT router ที่เปลี่ยนหมายเลข IP ของ datagram จากฝั่ง LAN (ฝั่งด้านใน) ไปยังหมายเลขในฝั่งที่ใกล้กับการเชื่อมต่อออกสู่ Internet (ฝั่งด้านนอก) ของ NAT router

Questions (A)

ขั้นแรกให้ผู้เรียนเปิดไฟล์ nat-inside-wireshark-trace1-1.pcapng ซึ่งผู้เรียนจะจะพบ HTTP GET request ที่ส่งออกไปยังหมายเลข IP 138.76.29.8 และพบ HTTP response message (“200 OK”) ซึ่ง messages ทั้งสองถูกดักจับจากฝั่ง LAN ของ router ให้ผู้เรียนศึกษา packets ดังกล่าวและตอบคำถามต่อไปนี้

1) เครื่อง client ที่ส่ง HTTP GET request ในไฟล์ nat-inside-wireshark-trace1-1.pcapng ใช้หมายเลข IP address หมายเลขใด? TCP segment ที่นำส่ง HTTP GET request ระบุหมายเลข source port เป็นเลขอะไร? HTTP GET request ถูกส่งไปยังหมายเลข destination IP หมายเลขใด? TCP segment ที่นำส่ง HTTP GET request ระบุหมายเลข destination port เป็นเลขอะไร?

   Source IP: 192.168.10.11
   Source Port: 53924
   Destination IP: 138.76.29.8
   Destination Port: 80
   Packet detail pane

2) เมื่อเวลาเท่าไร (สำหรับคำถามเวลานับจากนี้ โปรดระบุเวลานับจากเริ่มต้นไฟล์ trace ไม่ใช่เวลา wall-clock) ที่ HTTP 200 OK message จาก web server ถูกส่งต่อจาก NAT router ไปยังเครื่อง client ซึ่งอยู่ในฝั่ง LAN

   t = 0.030672101s
   packet list pane

3) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP 200 OK message มีค่าเป็นเท่าใดบ้าง?

   Source IP: 138.76.29.8
   Source Port: 80
   Destination IP: 192.168.10.11
   Destination Port: 53924
   Packet detail pane

ในลำดับถัดมาเราจะสำรวจ HTTP messages ทั้งสอง (GET และ 200 OK) ซึ่งดักจับจากฝั่งที่ใกล้กับส่วนเชื่อมต่อ Internet ระหว่าง router และเครือข่ายของผู้ให้บริการอินเทอร์เน็ต เนื่องจาก packets ที่ถูกดักจับกำลังถูกส่งไปยัง server จะได้รับการส่งต่อออกมาจาก NAT router หมายเลข IP address และ/หรือ หมายเลข port อาจจะมีการเปลี่ยนแปลงจาก NAT

ให้เปิดไฟล์ nat-outside-wireshark-trace1-1.pcapng ค้นหา HTTP GET message ซึ่งเป็น packet ที่ตรงกับ HTTP GET message ที่ถูกส่งจาก client ไปยัง server ที่ใช้หมายเลข IP 138.76.29.8 ที่เวลา t = 0.27362245 จงใช้ของมูลจาก header ของ packet ดังกล่าวเพื่อตอบคำถามต่อไปนี้

4) เมื่อเวลาเท่าไร ที่ HTTP GET message ปรากฏขึ้นในไฟล์ nat-outside-wireshark-trace1-1.pcapng?

   t = 0.027356291s
   packet list pane

5) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP GET มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-outside-wireshark-trace1-1.pcapng)

   Source IP: 10.0.1.254
   Source Port: 53924
   Destination IP: 138.76.29.8
   Destination Port: 80
   Packet detail pane

6) จากข้อ 5) ค่าของ field ทั้ง 4 มี field ใดบ้างที่แตกต่างจากข้อ 1) ?

   Source IP

7) จากการตรวจสอบ HTTP GET message เทียบระหว่างไฟล์ทั้งสอง มี field ใดใน HTTP header ที่เปลี่ยนแปลงหรือไม่? ถ้าหากมีพบว่าเป็น field ใดบ้าง?

   ไม่มีการเปลี่ยนแปลง

   นำ hex stream ไปเทียบกัน

8) ใน IP datagram ที่นำส่ง HTTP GET จาก datagram ที่ดักจับได้ในฝั่ง LAN (ฝั่งด้านใน) กับ datagram ที่ถูกส่งต่อออกมายังฝั่งที่ใกล้กับการเชื่อมต่อ Internet (ฝั่งด้านนอก) ของ NAT router มีค่าของ field ใดที่เปลี่ยนแปลงไปบ้างจากรายชื่อ field ใน IP header ต่อไปนี้: Version, Header Length, Flags, Checksum, Time to Live? หากมีการเปลี่ยนแปลงค่า โปรดระบุค่าเดิมและค่าใหม่

   Checksum: 0x64dc → 0x2492
   Time to Live: 64 → 63
   Packet detail pane

ลำดับถัดไปเราจะศึกษาไฟล์ nat-outside-wireshark-trace1-1.pcapng ต่อ โดยให้ค้นหา HTTP reply ที่นำส่ง “200 OK” message ซึ่งเป็นการตอบ HTTP GET request ที่ผู้เรียนได้สำรวจไปในคำถามข้อ 4) ถึงข้อ 8) ก่อนหน้านี้ ให้ศึกษา packet ดังกล่าวเพื่อตอบคำถามต่อไปนี้

9) เมื่อเวลาเท่าไร ที่ HTTP 200 OK message ปรากฏขึ้นในไฟล์ nat-outside-wireshark-trace1-1.pcapng?

   t = 0.030625966s
   packet list pane

10) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP reply (“200 OK”) มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-outside-wireshark-trace1-1.pcapng)

   Source IP: 138.76.29.8
   Source Port: 80
   Destination IP: 10.0.1.254
   Destination Port: 53924
   Packet detail pane

ส่วนสุดท้ายมาพิจารณาว่าเกิดอะไรขึ้นเมื่อ NAT router รับ diagram ที่ผู้เรียนสำรวจไปในคำถามที่ 9) และ 10) จากนั้นนำ packet ดังกล่าวมาผ่าน Network Address Translation และส่งต่อไปยัง host ซึ่งอยู่ฝั่ง LAN จากคำถามที่ผู้เรียนได้ตอบไปตั้งแต่ 1) ถึงข้อ 10) ผู้เรียนควรจะสามารถตอบคำถามข้อต่อไปนี้โดยไม่จำเป็นต้องดูข้อมูลจาก packet จริงๆ เสียด้วยซ้ำ

11) หมายเลข source IP และ destination IP และหมายเลข TCP source port และ destination port ของ IP datagram ที่นำส่ง HTTP reply (“200 OK”) ซึ่งถูกส่งจาก router ไปยัง host ปลายทางที่อยู่ด้านขวาตาม รูป 1 มีค่าเป็นเท่าใดบ้าง? (โปรดระบุค่าตามที่บันทึกได้ในไฟล์ nat-inside-wireshark-trace1-1.pcapng)

   Source IP: 138.76.29.8
   Source Port: 80
   Destination IP: 192.168.10.11
   Destination Port: 53924
   Packet detail pane

12) หากมีให้เพียงไฟล์ trace จำนวนสองไฟล์ซึ่งดักจับ packets จากสองฝั่งของ NAT device ผู้เรียนสามารถระบุได้หรือไม่ว่าฝั่งใดเป็นฝั่งเริ่มต้นส่งข้อมูลก่อนที่จะเกิดการ NAT ขึ้น? สามารถสังเกตได้จากอะไร? จงอธิบาย

เนื่องจากไม่แน่ใจว่า “ฝั่งใด” หมายถึง inside/outside หรือ client/server ดังนั้นจึงตอบทั้งคู่

สามารถสังเกตได้จากใครเป็นคนเริ่มTCP Connection, Timing, TTLที่ลดลง

เมื่อมีการเริ่ม TCP Connection ถ้าเริ่มจับเวลาพร้อมกันจะสังเกตได้ว่าเมื่อจะส่งยกตัวอย่างHTTP GETเวลาที่ถูกจับได้ใน outside จะช้ากว่าเนื่องจากต้องส่งจากเครื่องในLANไปที่routerแล้วจึงส่งไปที่Server และTTLเมื่อผ่านhopแรกก็ต้องมีค่าลดลงด้วย

Submission

จงตอบคำถามในส่วนที่ระบุหัวข้อ Questions (A) ซึ่งมีคำถามร่วมทั้งหมด 12 ข้อ โดยในคำตอบของแต่ละข้อด้วยให้อธิบายด้วยว่าหาคำตอบมาได้อย่างไร ตัวอย่างเช่น อธิบายว่าสามารถค้น packet ตามที่โจทย์ระบุได้ด้วยวิธีการใด หรือค่าที่นำมาตอบ นำมาจาก field ใดของ header ตาม protocol ใด

ในกรณีที่คัดลอกคำตอบของคนอื่นมา ให้ระบุชื่อของบุคคลที่เป็นต้นฉบับมาด้วย หากตรวจพบว่ามีการลอกมาแต่ไม่มีการระบุชื่อบุคคลที่เป็นต้นฉบับ ผู้สอนจะถือว่าทุจริตและอาจพิจารณาลงโทษให้ตกเกณฑ์รายวิชาในทันที

การส่งงาน ให้เขียนหรือพิมพ์หมายเลขข้อและคำตอบของข้อนั้นๆ และส่งเป็นไฟล์ PDF เท่านั้น กรุณาตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab09 ตามตัวอย่างต่อไปนี้ 64019999_sec20_lab09.pdf