**Lab 6: Network Address Translation (NAT)**

เปิดไฟล์ **NAT\_home\_side.pcap** ที่ดาวน์โหลดมาแล้วตอบคำถามดังต่อไปนี้

เนื่องจากว่า Client นั้นจะติดต่อกับ Google Server หลายๆ ตัวเพื่อเป็นการใช้งาน Safe Browsing หรือเพื่อเพิ่มความปลอดภัยสำหรับการใช้งานเวป ซึ่งเราต้องการดูแค่ Server หลักของ Google ซึ่งก็คือ 64.233.169.104 ในที่นี้เราต้องการดูเฉพาะ packet ที่ติดต่อกับเซิฟเวอร์หลักของ Google โดยการกรอง Packet โดยการใส่

“http && ip.addr == 64.223.169.104”

ลงไปในช่อง Filter เพื่อกรองให้เหลือแต่ Packet ที่เราต้องการเท่านั้น

จงตอบคำถามดังต่อไปนี้

1. IP Address ของ Client คืออะไร

* 192.168.1.100

1. ให้ดูว่า Packet ที่เป็น HTTP GET ที่ส่งมาจาก Client ไป Google Server (Destination IP: 64.233.169.104 ณ.ที่เวลา 7.109267) มี Source IP Address คืออะไร

* 192.168.1.100

1. หมายเลขพอร์ตของ Source และ Destination ของ IP Datagram ที่ส่ง HTTP GET ออกไปนั้นคือหมายเลขอะไร

* Source 4335
* Destination 80

1. ที่ณ.เวลาเท่าใดที่ได้รับข้อความ HTTP OK (200) มาถึง Client (ที่ตอบกลับมาจาก Google Server)?

* 7.158797

1. Source และ Destination IP Address ของข้อความที่ตอบกลับมาจาก Server นั้นคือหมายเลขอะไร

* Source 64.233.169.104
* Destination 192.168.1.100

1. หมายเลขพอร์ตชอง Source และ Destination ของข้อความที่ตอบกลับมาจาก Server นั้นคือหมายเลขอะไร

* Source 80
* Destination 4335

ในช่อง Filter ให้ใส่ “tcp” ลงไปแทนที่ข้อความเก่าเพื่อกรองข้อมูลเฉพาะ Packet ที่ใช้งานโปรโตคอล TCP

1. การงาน TCP นั้นจะต้องมีการทำ Three-way SYN/ACK Handshake ก่อนคำถามคือ ณ.เวลาที่เท่าใดที่ Client และ Server ได้ทำการสร้าง Connection เสร็จแล้ว (ซึ่งจะเป็นเวลาก่อนที่ Client จะเริ่มส่งข้อความ GET ไปยัง Server)

* 1.572228

1. Source และ Destination IP Address ของ TCP SYN Segment นั้นคือหมายเลขอะไร

* Source 192.168.1.100
* Destination 74.125.106.31

1. หมายเลขพอร์ตของ Source และ Destination ของ TCP SYN Segment นั้นคือหมายเลขอะไร

* Source 4335
* Destination 80

1. ที่ณ.เวลาเท่าใดที่ Client ได้รับ TCP ACK Segment (TCP SYN,ACK ซึ่งก็คือ ACK ของ SYN) มาจาก Server

* 1.572197

1. Source และ Destination IP Address ของ TCP ACK Segment นั้นคือหมายเลขอะไร

* Source 74.125.106.31
* Destination 192.168.1.100

1. หมายเลขพอร์ตของ Source และ Destination ของ TCP ACK Segment นั้นคือหมายเลขอะไร

* Source 80
* Destination 4335

คำถามก่อนหน้านั้นเราดัก Packet ที่ส่งออกและรับเข้ามาในเครื่องเราเท่านั้น ซึ่งก็คือข้อความ HTTP และ TCP SYN และ ACK นั้นเอง ต่อจากนี้ไปเราจะมาดู Packet ที่ดักมาได้ที่ NAT Router ซึ่งเป็น Gateway ของเครื่องคอมเรา ซึ่งไฟล์ที่ดัก Packet ที่ NAT Router นั้นจะชื่อว่า **NAT\_ISP\_side.pcap**

ข้อความที่ถูกบันทึกอยู่ในไฟล์นี้นั้นเป็นข้อความที่ NAT Router ติดต่อกับ ISP ซึ่งเราจะได้เห็นการทำงานของ NAT Router ว่ามันมีการแปลงหมายเลขของ IP และ พอร์ตในการสื่อสารอย่างไร

(หมายเหตุ เวลาที่ถูกบันทึกในไฟล์นี้ไม่ตรงกับไฟล์ที่บันทึกได้ในฝั่ง Client เนื่องจากว่าทั้งสองเครื่องไม่ได้เริ่มการทำงานพร้อมกัน)

จงตอบคำถามดังต่อไปนี้โดยใช้ไฟล์ Trace จาก NAT Router

1. ใช้ข้อมูลจากไฟล์ NAT\_ISP\_side, จงหาว่าณ.เวลาที่เท่าใดที่ข้อความ HTTP GET ที่ Client ส่งมานั้น ถึงที่ NAT Router (ข้อความที่ Client ส่ง HTTP GET ออกมาณ.เวลา 7.109267)

* 6.069168

1. Source และ Destination IP Address ของ IP Datagram ที่ส่ง HTTP GET มานั้นคือหมายเลขอะไร

* Source 71.192.34.104
* Destination 64.233.169.104

1. หมายเลขพอร์ตของ Source และ Destination ของ IP Datagram ที่ส่ง HTTP GET นั้นคือหมายเลขอะไร

* Source 4335
* Destination 80

1. ให้เปรียบเทียบระหว่าง IP และหมายเลขพอร์ตของ IP Datagram ที่ส่ง HTTP GET ที่ดักได้จาก Client (จากไฟล์ NAT\_home\_side) ต่างจาก IP Datagram ที่ดักได้จาก NAT Router (จากไฟล์ NAT\_ISP\_side) ว่ามีข้อมูลอะไรที่เหมือนกัน และมีข้อมูลอะไรที่ต่างกันบ้าง

* IP ของ SERVER เหมือนกัน
* IP ของ Client ไม่เหมือนกัน

1. จงหาข้อแตกต่างระหว่างข้อความ HTTP GET ที่ดักได้ที่ Client และ NAT Router ว่าในแต่ละ Field (Version, Header Length, Flags, Checksum) นั้นมีค่าเหมือนกันหรือแตกต่างกันอย่างไร หากแตกต่างจงบอกว่าเพราะอะไรจึงแตกต่าง

* ไม่ต่าง

1. ใช้ข้อมูลจากไฟล์ NAT\_ISP\_side, จงหาว่าณ.เวลาที่เท่าใดที่ NAT Router ได้รับข้อความ HTTP OK มาจาก Server

* 6.117570

1. Source และ Destination IP Address ของข้อความ HTTP OK มาจาก Server นั้นคือหมายเลขอะไร

* Source 64.233.169.104
* Destination 71.192.34.104

1. หมายเลขพอร์ตของ Source และ Destination ของข้อความ HTTP OK มาจาก Server นั้นคือหมายเลขอะไร

* Source 80
* Destination 4335

1. ให้เปรียบเทียบระหว่าง IP และหมายเลขพอร์ตของข้อความ HTTP OK ที่ดักได้จาก Client และ ที่ดักได้จาก NAT Router ว่ามีข้อมูลอะไรที่เหมือนกัน และมีข้อมูลอะไรที่ต่างกันบ้าง
2. ใช้ข้อมูลจากไฟล์ NAT\_ISP\_side, จงหาว่าณ.เวลาที่เท่าใดที่ได้รับข้อความ TCP SYN มาจาก Client

* 6.067775

1. และเวลาที่เท่าใดที่ NAT Router ส่ง TCP ACK กลับไปให้ Client

* 6.068754

1. Source และ Destination IP Address ของทั้งสอง TCP SYN และ TCP ACK เหมือนหรือแตกต่างกันอย่างไร

* เหมือนกัน

1. หมายเลขพอร์ตของ Source และ Destination ของทั้งสอง TCP SYN และ TCP ACK เหมือนหรือแตกต่างกันอย่างไร

* เหมือนกัน

1. **Lab 5: Network Address Translation (NAT)**

**Lab 5: Network Address Translation (NAT)**

Google Server

NAT Router

Client

**NAT Translation Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **LAN** | | **WAN** | |
| **IP Address** | **Port** | **IP Address** | **Port** |
| 192.168.1.100 | 4335 | 71.192.34.104 | 4335 |

HTTP OK

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 64.233.169.104 | 80 |
| Dest | 71.192.34.104 | 4335 |

HTTP GET

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 71.192.34.104 | 4335 |
| Dest | 64.233.169.104 | 80 |

HTTP OK

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 64.233.169.104 | 80 |
| Dest | 192.168.1.100 | 4335 |

HTTP GET

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 192.168.1.100 | 4335 |
| Dest | 64.233.169.104 | 80 |

TCP ACK

TCP ACK

TCP SYN, ACK

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 64.233.169.104 | 80 |
| Dest | 71.192.34.104 | 4335 |

TCP SYN

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 71.192.34.104 | 4335 |
| Dest | 64.233.169.104 | 80 |

TCP SYN

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 192.168.1.100 | 4335 |
| Dest | 64.233.169.104 | 80 |

TCP SYN, ACK

|  |  |  |
| --- | --- | --- |
|  | IP | Port |
| Src | 64.233.169.104 | 80 |
| Dest | 192.168.1.100 | 4335 |