Lab 05: UDP and TCP Basics

ในปฏิบัติการครั้งผู้เรียนจะได้ศึกษาพฤติกรรมการทำงานเบื้องต้นของ User Datagram Protocol (UDP) และ Transmission Control Protocol (TCP) ซึ่งทั้งสอง protocols ถูกจัดว่าทำงานอยู่ในชั้น Transport-Layer

A. User Datagram Protocol (UDP)

จากที่ได้เรียนรู้ไปแล้วในรายวิชาทฤษฎีว่า UDP ถูกออกแบบมาให้มีความคล่องตัว มีการทำงานไม่ซับซ้อน การทดลองในส่วนนี้จึงสามารถทำเสร็จได้ภายในเวลาไม่นาน

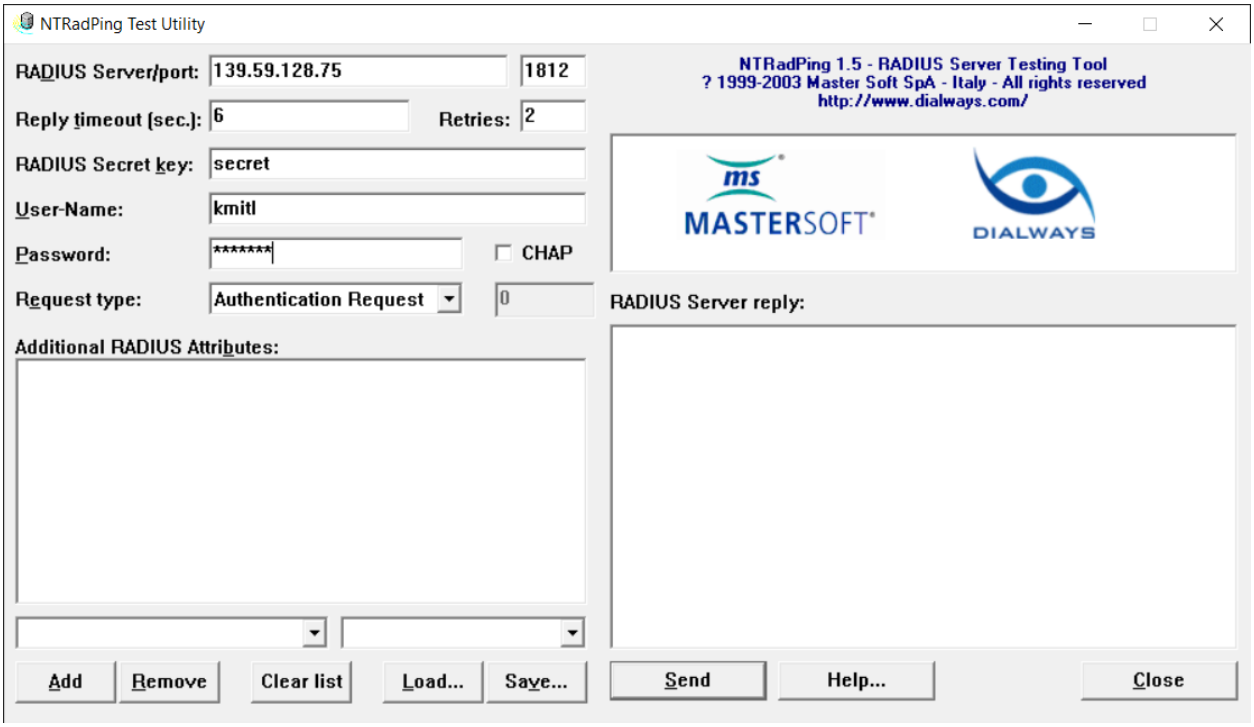
ลำดับในการทดลองนี้เริ่มจากการดักจับ packets ด้วย Wireshark และทำบางสิ่งที่ทำให้เครื่องของผู้เรียนส่งและได้รับ UDP packets จำนวนหนึ่ง ซึ่งก็มีโอกาสเป็นไปได้ว่าถึงแม้นจะไม่ได้ทำอะไร (นอกเหนือจากการสั่ง Wireshark ให้ดักจับ) เครื่องของผู้เรียนก็จะยังมีการส่ง UDP packets ออกไปบ้างเป็นปกติอยู่แล้ว โดยเฉพาะในการทำงานของ DNS ซึ่งจะส่ง DNS query และรับ DNS response ซึ่งรับส่งโดยใช้ UDP ดังนั้นจึงเป็นไปได้สูงที่ผู้เรียนจะพบ UDP packets ใน การดักจับ

อย่างไรก็ดี เพื่อให้สามารถระบุเจาะจง UDP segment ที่เราจะศึกษา ในปฏิบัติการนี้จะให้ผู้เรียนทดลองโดยการใช้ protocol ในชั้น Application Layer ที่ชื่อ Remote Authentication Dial-In User Service (RADIUS) ซึ่งจะประกอบโดย RADIUS client และ RADIUS server โดยให้ทำตามขั้นตอนต่อไปนี้

1. เปิด web browser และเข้าไปที่ URL ต่อไปนี้ https://idblender.com/tools/public-radius ซึ่งเป็นเว็บไซต์ที่เปิดให้บริการ public RADIUS server เพื่อใช้สำหรับทดสอบ โดย RADIUS server ดังกล่าวทำงานที่หมายเลข IP address 139.59.128.75 และ port หมายเลข 1812
2. จากในหน้าเพจให้เลื่อนลงมาที่ส่วน Created identities เพื่อตรวจสอบว่ามี User-Name และ Cleartext-Password ใดๆ กำหนดไว้แล้วหรือไม่ หากยังไม่มี ให้กรอกข้อมูลต่อไปนี้และกด Submit

User-Name	kmitl
Cleartext-Password	CEkmitl

3. ดาวน์โหลดซอฟต์แวร์ที่จะทำหน้าที่เป็น RADIUS client ซึ่งมีชื่อว่า NTRadPing จาก link ต่อไปนี้ https://community.microfocus.com/cfs-file/__key/communityserver-wikis-components-files/00-00-00-01-70/ntradping.zip
4. ให้แตกไฟล์ ntradping.zip ออกมาจะพบไฟล์ชื่อ NTRadPing.exe ให้คลิกขวาที่ไฟล์ดังกล่าวและเลือก Run as administrator ซึ่งจะทำให้หน้าต่างของ NTRadPing Test Utility ปรากฏขึ้นมาดังภาพ รูป 1



รูป ๑ หน้าต่าง NTRadPing Test Utility

5. ในหน้าต่าง NTRadPing Test Utility ให้กรอกข้อมูลดังต่อไปนี้

RADIUS Server	139.59.128.75
RADIUS port	1812
Reply timeout (sec.)	6
Retries	2
RADIUS Secret key	Secret
User-Name	kmitl
Password	CEkmitl
Request type	Authentication Request

6. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
host 139.59.128.75 and udp port 1812
```

7. สลับกลับมาที่หน้าต่าง NTRadPing Test Utility และกดปุ่ม Send หากทำถูกต้องควรจะมีบรรทัด response: Access-Accept ปรากฏขึ้นใน RADIUS Server reply
8. ทดลองเปลี่ยนค่า Password เป็นค่าอื่นที่ไม่ตรงกับค่าที่ตั้งไว้ก่อนหน้า จากนั้นให้กดปุ่ม Send เพื่อส่ง Access Request อีกครั้ง
9. ทดลองเปลี่ยนค่า Password กลับเป็นค่า CEkmitl อีกครั้ง จากนั้นกดปุ่ม Send เพื่อส่ง Access Request อีกครั้ง
10. สลับไปหน้า Wireshark และสั่งให้หยุด capture
11. ให้ save ไฟล์ไว้ด้วยชื่อ Lab05-A.pcapng

Questions (A)

หลังจากทำตามขั้นตอนข้างต้นแล้ว ให้ใช้ไฟล์ packet capture ที่ save เอาไว้ในการตอบคำถามต่อไปนี้

1) จาก packets ที่ดักจับได้ จงค้นหาว่า UDP segment แรก มีหมายเลขลำดับ packet เป็นหมายเลขอะไร? และประเภทของ Application-Layer payload หรือ protocol ที่ถูกนำส่งด้วย UDP segment เป็น Application-Layer protocol ใด?

   packet number 0
   Application-Layer protocol RADIUS
   ดูได้จาก packet detail pane

2) ที่ Menu bar เลือก Edit -> Preferences เพื่อให้ Preferences ปรากฏขึ้นมา ในหน้าต่างดังกล่าว ให้เลือก หัวข้อ Appearance -> Layout จะพบว่ามีให้ปรับต่าง Layout หน้าจอ Wireshark โดยให้ปรับ Pane 3 ให้เป็น Packet Diagram และกดปุ่ม OK เพื่อปิดหน้าต่าง Preferences จากนั้นจึงมาพิจารณาข้อมูลใน Packet Detail Pane ของ packet ดังกล่าวและหาว่าใน UDP header มี field อยู่ทั้งหมดกี่ fields? และแต่ละ field มีชื่อว่าอะไรบ้าง?

   4 fields 1) Source Port 2) Destination Port 3) Length 4) Checksum
   ดูจาก Packet diagram

3) จากการศึกษาข้อมูลในแสดงใน Packet Diagram ของ UDP แต่ละ field ใน UDP header มีความยาวเท่าไรในหน่วย bytes?

   แต่ละfieldมีขนาด2bytes ดูได้จากจำนวนบิตที่เป็น16บิตใน Packet Diagram

4) ค่าของ field ที่ชื่อว่า Length ใน UDP header เป็นความยาวของอะไร? ทดลองตรวจสอบค่าความยาวกับ UDP packet ที่ผู้เรียนดักจับมาได้ว่ามีค่าเท่ากับที่ตอบหรือไม่

   เท่ากันเพราะ ค่าlengthในUDP HeaderคือขนาดของUDP Header+UDP Payload และตัวUDP packetมีขนาด 8 bytes + payload 45 bytes

5) ขนาดสูงสุดที่เป็นไปได้ของ UDP payload มีขนาดเป็นกี่ bytes? (คำใบ้: โปรดพิจารณาคำตอบของคำถามก่อนหน้า)

65527 bytes เนื่องจาก max-length ที่ 65535 และหัก UDP header 8 bytes

6) ค่าต่ำสุดและค่าสูงสุดที่เป็นไปได้ของหมายเลข source port มีค่าเป็นเท่าใด?

0-65535 คล้ายกับข้อ 5)

7) หมายเลข Protocol สำหรับ UDP คือหมายเลขใด? ให้ผู้เรียนตอบเป็นเลขฐาน 10 โดยในการหาคำตอบของคำถามนี้ ให้ผู้เรียนค้นหาและตรวจสอบค่าของ field ที่ชื่อว่า Protocol ใน header ของ Internet Protocol (IP) ของ packet

17 ดูจาก field Protocol ใน IP

8) ค้นหาคู่ UDP packets คู่ใดคู่หนึ่ง ซึ่งประกอบด้วย UDP packet ที่ส่งออกจาก host ฝั่งเครื่องของผู้เรียนและ packet ที่ host ฝั่งเครื่องคู่สนทนาตอบกลับมายังเครื่องผู้เรียน (ข้อสังเกต: ใน Packet List Pane ที่คอลัมน์ No. จะมีลูกศรแสดง UDP packets ที่เข้าคู่กันระหว่างส่งออกไปและตอบกลับ โดยหมายเลข IP ของผู้ส่งใน packet แรกจะเป็นหมายเลขเดียวกับ IP ของผู้รับใน packet ที่สอง) โปรดระบุว่า packet แรก มีหมายเลข packet เป็นหมายเลขใด? และ packet ที่สองมีหมายเลข packet เป็นหมายเลขใด? หมายเลข port ของ packets ทั้งสองมีความสัมพันธ์กันอย่างไร? จงอธิบาย

Packet number 1, 2 source port and destination port จะสลับกันระหว่าง packetที่hostส่งไปและ packetที่hostได้รับเนื่องจากเป็น protocol UDP ส่งออกไปจากportไหนก็จะส่งกลับคืนที่นั้น

9) จาก trace ไฟล์ พบว่ามีการส่ง Access-Request ออกไปทั้งหมดกี่ครั้ง? แต่ละครั้งใช้ source port หมายเลขใดบ้าง? เครื่องคอมพิวเตอร์ของผู้เรียนซึ่งทำหน้าที่เป็น host ต้นทางใช้หลักการใดในการเลือกหมายเลข source port? จงอธิบาย

3 ครั้ง 59564, 60236, 49687

ใช้Dynamic portคือosสุ่มเลือกportที่ไม่มีการใช้งานอยู่ในตอนนั้น

10) ในรอบที่ RADIUS client ส่ง Access Request ไปพร้อมกับ Password ที่ผิดนั้น พบว่าได้รับ packet ตอบกลับมาจาก RADIUS server หรือไม่? ผู้เรียนสามารถบอกได้ชัดเจนหรือไม่ว่าเกิดอะไรขึ้นบ้าง? Access Request ที่ส่งไปถึง RADIUS server หรือไม่? RADIUS server ตอบกลับมาหรือไม่? หรือว่า packet ที่ RADIUS server ส่งกลับมาหายไประหว่างทาง?

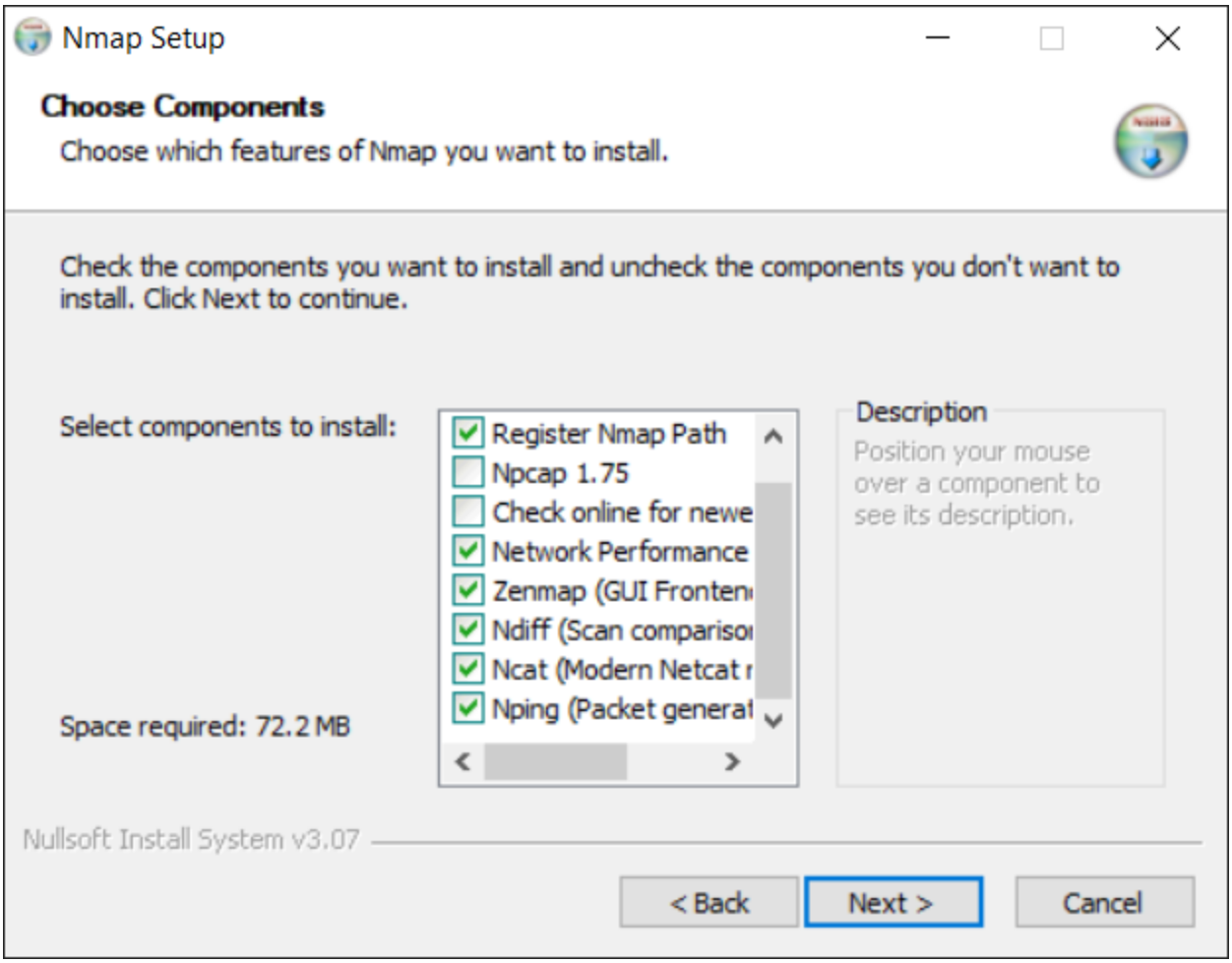
ไม่ได้รับpacketที่ตอบกลับมาทำให้ไม่สามารถระบุได้ว่าเกิดอะไรขึ้น

B. Transmission Control Protocol (TCP)

ในปฏิบัติการส่วนนี้เราจะสำรวจพฤติกรรมการทำงานของ TCP มากขึ้นในรายละเอียด เนื่องจาก TCP มีรายละเอียดหลายส่วน เราจะไม่สามารถศึกษาทุกแง่มุมของ TCP ได้ในปฏิบัติการเพียงครั้งเดียว ในครั้งนี้เราจะเน้นไปที่การศึกษาเรื่องการสร้างการเชื่อมต่อ (TCP connection setup) ซึ่งเราจะศึกษาโดยการวิเคราะห์จากบันทึกร่องรอยการสร้างการเชื่อมต่อและในการร้องขอข้อมูลจากบริการ Quote of the Day (QOTD) เปรียบเทียบระหว่างกรณี TCP เทียบกับ UDP ซึ่งผู้เรียนสามารถศึกษาการทำงานของ protocol ดังกล่าวได้จากเอกสาร RFC 865

เพื่อความสะดวกในการทดลองตามปฏิบัติการในครั้งนี้ เพื่อให้ไม่จำเป็นต้องเขียนโปรแกรมเพื่อติดต่อสื่อสารกับฝั่ง server ผู้เรียนจะได้ใช้ command line utility ที่ชื่อว่า ncat ซึ่งพัฒนาขึ้นมาโดยเลียนแบบการทำงานของเครื่องมือดั้งเดิมที่ชื่อว่า netcat โดยสามารถติดตั้ง ncat พร้อมกับซอฟต์แวร์ที่ใช้ในการทำ port scan ที่ชื่อว่า Nmap ในการทดลองให้ทำตามขั้นตอนต่อไปนี้

1. เปิด web browser และเข้าไปที่ URL ต่อไปนี้ https://nmap.org/download.html เพื่อดาวน์โหลดไฟล์ติดตั้ง Nmap โดย ณ เวลาที่จัดทำเอกสารสำหรับปฏิบัติการนี้ ไฟล์ติดตั้ง Nmap เวอร์ชั่นล่าสุดคือไฟล์ชื่อ nmap-7.94-setup.exe
2. หลังจากดาวน์โหลดไฟล์ติดตั้งเรียบร้อยแล้ว ให้รันไฟล์ดังกล่าวเพื่อทำการติดตั้ง โดยให้ระบุตัวเลือกติดตั้ง components Ncat และ Nping รวมถึง component อื่นๆ ตามรูปที่ปรากฏต่อไปนี้



รูปที่ 2 การติดตั้ง component ของ Nmap

3. หลังจากติดตั้งเสร็จสิ้น ให้ทดสอบว่า ncat พร้อมใช้งานหรือไม่โดยเปิด command prompt และพิมพ์คำสั่งต่อไปนี้

```
ncat -help
```

หากติดตั้งสำเร็จพร้อมใช้งาน หน้าจอ command prompt จะแสดงคำอธิบายการใช้งาน ncat

4. เปิด Wireshark และเริ่มทำการ capture packet โดยใช้ Capture filter ต่อไปนี้

```
tcp port 17 or udp port 17
```

5. สลับกลับไปหน้า command prompt และพิมพ์คำสั่งต่อไปนี้ เพื่อเป็นการร้องขอไปยัง QOTD server ที่ชื่อ djxmmx.net ซึ่งให้บริการด้วย TCP ที่ port หมายเลข 17 โดยหลังจากพิมพ์คำสั่ง ให้กด Enter สองครั้งเพื่อให้กลับมาที่ prompt

```
ncat djxmmx.net 17
```

6. ทำตามขั้นตอนในข้อที่แล้วอย่างน้อย 3 ครั้งเพื่อขอ quote ต่างๆ กัน
7. พิมพ์คำสั่งต่อไปนี้ เพื่อเป็นการร้องขอไปยัง QOTD server ที่ชื่อ djxmmx.net ซึ่งให้บริการด้วย UDP ที่ port หมายเลข 17 ซึ่งการใส่ -u เป็นการระบุว่าใช้ UDP โดยหลังจากพิมพ์คำสั่ง ให้กด Enter อย่างน้อย 2-3 ครั้ง โดยจะพบว่าหลังจากกด Enter แต่ละครั้ง จะปรากฏ quote ใหม่ขึ้นมาเรื่อยๆ หากต้องการหยุดและกลับมาที่ prompt ให้กด Ctrl + Z แล้วกด Enter (สำหรับกรณีของ macOS และ Linux ให้กด Ctrl + D แล้วกด Enter)

```
ncat -u djxmmx.net 17
```

8. สลับไปหน้า Wireshark และสั่งให้หยุด capture
9. ให้ save ไฟล์ไว้ด้วยชื่อ Lab05-B.pcapng

Questions (B)

11) จากการร้องขอ quote ผ่าน TCP โปรดระบุว่า quote แรกที่ได้มีข้อความว่าอะไร? จงค้นหาว่า packet ใดจากไฟล์ capture ที่เนื้อความ quote แรกปรากฏอยู่ในเนื้อหาของ packet โปรดระบุหมายเลข packet

"Why do you build me up, buttercup baby, just to let me down, and mess me around?
And then worst of all, you never call baby when you say you will, but I love you still.
I need you, more than anyone darling, you know that I have from the start.
So build me up, buttercup, don't break my heart..."
packet no 4

12) จากหมายเลข packet ในข้อที่แล้ว ให้คลิกขวาที่ packet ดังกล่าวแล้วเลือก Follow -> TCP Stream ซึ่งจะมีผลให้ Wireshark สร้างและใช้ Display filter เพื่อแสดงเฉพาะ packets ของ TCP connection เดียวกัน จงตรวจสอบว่า Wireshark สร้าง Display filter อะไรให้? โปรดระบุ Display filter ดังกล่าวในคำตอบ

tcp.stream eq 0

13) หลังจากใช้ Follow -> TCP Stream เหลือ packets ที่แสดงผลใน Packet List Pane จำนวนกี่ packets? Packet ที่มีเนื้อความ quote ที่ server ส่งมาเป็น packet ลำดับที่เท่าไรจาก packets ทั้งหมดใน TCP connection นี้ (ไม่ใช่ packet No. แต่ให้นับว่าเป็นบรรทัดที่เท่าไร หลังจากจัดเรียงตามคอลัมน์เวลาแล้ว)

8 packets quote เป็น packet ที่ 4

14) ตอนเริ่มต้นของ TCP connection ในคอลัมน์ Info ของ 3 packets แรกมีข้อมูลอะไรปรากฏอยู่บ้าง นำข้อมูลเหล่านั้นมาเขียนในคำตอบ

Source Port
Destination Port
Sequence Number
Sequence Number (raw)
Acknowledgment Number
Acknowledgment Number (raw)
Header Length
Window
Checksum
Urgent Pointer
Option

ดูจาก detail ของ TCP

15) หากต้องการกรองให้ Packet List Pane แสดงผลเฉพาะ 3 packets แรกของ TCP connection จะต้องเขียน Display filter ว่าอย่างไร

(tcp.flags.syn == True) || (tcp.seq == 1 && tcp.ack == 1 && !(tcp.flags.push == True))
หาได้จากการดูfieldที่มีค่าเหมือนกัน

16) จากที่ผู้เรียนได้ทราบจากรายวิชาทฤษฎีแล้วว่าในการส่งข้อมูลแบบเชื่อถือได้ (Reliable Data Transfer) มีการใช้ Timer เพื่อรอการตอบกลับเป็นระยะเวลาที่เหมาะสม ซึ่งระยะเวลาดังกล่าวมีความสัมพันธ์กับ RTT ระหว่างคู่สนทนา จงอธิบายว่า ฝั่ง client สามารถใช้ประโยชน์จากการรับส่ง packets ทั้ง 3 เพื่อหาค่า RTT ได้อย่างไร? ในทำนองเดียวกัน จงอธิบาย ฝั่ง server สามารถใช้ประโยชน์จากการรับส่ง packets ทั้ง 3 เพื่อหา RTT ได้อย่างไร?

Client สามารถนำpacket1และ2มาคำนวณหาRTTได้

Server สามารถนำpacket2และ3มาคำนวณหาRTTได้

17) ค่าใน field ใดที่ Wireshark ได้คำนวณและแสดงผลค่า RTT ระหว่าง client และ server จงหาค่าดังกล่าวใน Packet Details Pane จาก 3 packets แรก และระบุชื่อ field ดังกล่าวในคำตอบ

tcp.analysis.ack_rtt เป็นfieldที่ไม่ได้อยู่ในpacketดั้งเดิม แต่wiresharkวิเคราะห์ให้

18) ให้ล้าง Display filter เพื่อให้กลับมาแสดงผลทุก packets ที่ดักจับได้อีกครั้ง และค้นหาว่าในแต่ละอย่างที่ร้องขอ quote ผ่าน TCP เครื่องของผู้เรียนใช้ port หมายเลขอะไรบ้าง? โปรดระบุหมายเลขเหล่านั้นในคำตอบ

63944 63946 63950 ดูจาก source port ใน tcp

19) จากข้อ 18) เครื่องของผู้เรียนมีหลักการยังไงในการเลือกหมายเลข port ที่จะใช้งาน? จงอธิบาย

ใช้Dynamic portคือosสุ่มเลือกportที่ไม่มีการใช้งานอยู่ในตอนนั้น

20) ให้ล้าง Display filter เพื่อให้กลับมาแสดงผลทุก packets ที่ดักจับได้อีกครั้ง และเขียน Display filter ใหม่ให้แสดงผลเฉพาะ packet ที่มีการใช้งาน UDP และตรวจสอบว่ามี UDP จำนวนกี่ packets? เป็น packet ที่ client ส่งไปยัง server กี่ packets? และเป็น packets ที่ server ตอบกลับมาที่ client กี่ packet? จำนวน UDP segment ที่ส่งไปและได้รับตอบกลับมีจำนวนเท่ากันหรือไม่?

UDP 6 packets
Client → Server 3 packets
Server → Client 3 packets
ส่งและรับจำนวนเท่ากัน

21) ในบรรดา UDP segment ที่ server ตอบกลับมาหา client จงค้นหาว่ามี packets ที่เป็นการแลกเปลี่ยน control information โดยที่ไม่บรรจุเนื้อหา quote หรือไม่? ถ้าหากมี packets เหล่านั้นมี control information อะไร?

ไม่มี

Submission

จงตอบคำถามในส่วนที่ระบุหัวข้อ Question ตั้งแต่ (A) ไปจนถึง (B) ซึ่งมีคำถามร่วมทั้งหมด 21 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 _lab05 ตามตัวอย่างต่อไปนี้ 64019999_sec20_lab05.pdf