<u>กิจกรรมที่ 5 : FTP และ DNS</u>

กิจกรรมครั้งนี้จะเป็นการทำความเข้าใจกับโปรโตคอล FTP (File Transfer Protocol) และ DNS (Domain Name System) เพื่อเสริมสร้างความเข้าใจในการทำงานของโปรโตคอลทั้ง 2 ตัว

FTP (File Transfer Protocol)

โปรโตคอล FTP จะใช้ 2 พอร์ต คือ พอร์ต 21 ใช้เป็น command channel คือเป็นช่องทางสำหรับรับส่งคำสั่ง และ พอร์ต 20 ใช้เป็น data channel ซึ่งใช้ในการรับส่งไฟล์

1. เปิดโปรแกรม wireshark ให้กำหนดให้ capture เฉพาะ host test.rebex.net
2. เรียก Command Prompt แล้วป้อนคำสั่ง ftp test.rebex.net โดยให้ใส่ user เป็น demo และใช้ password เป็น password
3. ใช้คำสั่ง **dir** ในโปรแกรม ftp และ capture ภาพของผลการทำงานของคำสั่ง dir จากนั้นกลับมาที่ Wireshark แล้วใช้ display filter เป็น ftp ให้เปรียบเทียบระหว่าง<u>แต่ละคำสั่ง</u>ของ ftp ว่าตรงกับ packet ใดของ Wireshark ที่ดักจับ โดยให้ capture ภาพของ packet list pane ที่แสดงคำสั่งมาแสดงด้วย

   _____

   _____

   _____

   _____

4. ให้ค้นหา packet ที่ได้ดักจับไว้ ที่มีชื่อไฟล์ readme.txt (ซึ่งเป็นข้อมูลที่ ftp server ส่งมา) ว่าส่งมาทาง port ใด และอยู่ใน packet ใด จากนั้นให้เปิดดูที่ Statistics –> Flow graph และนำมาอธิบายขั้นตอนการทำงานของคำสั่ง dir โดยละเอียด โดยอ้างอิงจาก Flow graph

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

5. ใช้คำสั่ง get readme.txt เพื่อรับไฟล์ readme.txt จาก ftp server จากนั้นให้เปิดไฟล์ใน notepad และ capture มาแสดง และ capture ข้อมูลใน Wireshark ส่วนที่เป็นการส่งไฟล์ readme.txt มาเปรียบเทียบ

6. ให้คลิกขวาที่ packet ที่เป็นข้อมูลของ readme.txt และเลือก Follow TCP Stream และ Save as... เป็นไฟล์ ให้ตั้งชื่ออะไรก็ได้ จากนั้นเปิดไฟล์ด้วย notepad แล้วเปรียบเทียบกับไฟล์ readme.txt ว่ามีอะไรแตกต่างกันหรือไม่

   _____

   _____

7. ให้เปิดไฟล์ ftp-clientside101.pcapng คลิกขวาที่ Packet 6 (USER anonymous) และเลือก Follow TCP Stream ให้ **Capture** หน้าต่างของ Follow TCP Stream ที่แสดงการโต้ตอบของ FTP ให้อธิบายว่ามีคำสั่งของ FTP Protocol อะไรบ้าง (คำสั่งของ Protocol ไม่ใช่คำสั่งของโปรแกรม)

   _____

   _____

8. จากนั้นที่หน้าต่างของ Follow TCP Stream ให้เลือก Filter Out this Stream และให้ดูที่ display filter ว่าแสดงว่าอะไร จากนั้นคลิกขวาที่ Packet 16 และเลือก Follow TCP Stream อีกครั้งและเลือก Filter Out this Stream อีกครั้ง
9. จากนั้นคลิกที่ packet ใดก็ได้และเลือก Follow TCP Stream คลิก Save as ให้ตั้งชื่อ pantheon.jpg โดยเลือกชนิดเป็น raw และให้เปิดภาพขึ้นมาดูว่าเป็นภาพอะไร

_____

_____

10. ให้อธิบายว่าการทำงานในข้อ 8 ทำเพื่ออะไร

_____

_____

11. ให้เปิดไฟล์ ftp-download-good2.pcapng ให้หาคำตอบว่าเวลาที่ใช้ในการโหลดไฟล์ “SIZE OS Fingerprinting with ICMP.zip” เท่ากับเท่าไร อธิบายวิธีการ

_____

_____

_____

_____

_____

_____

_____

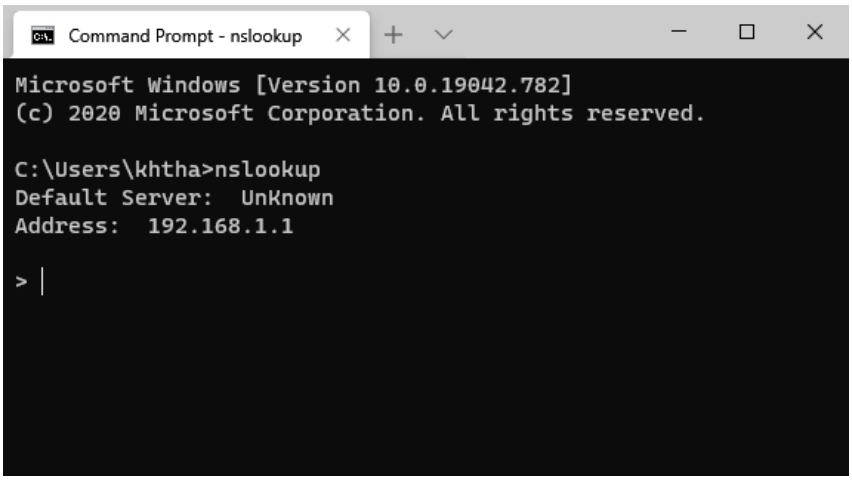
_____

_____

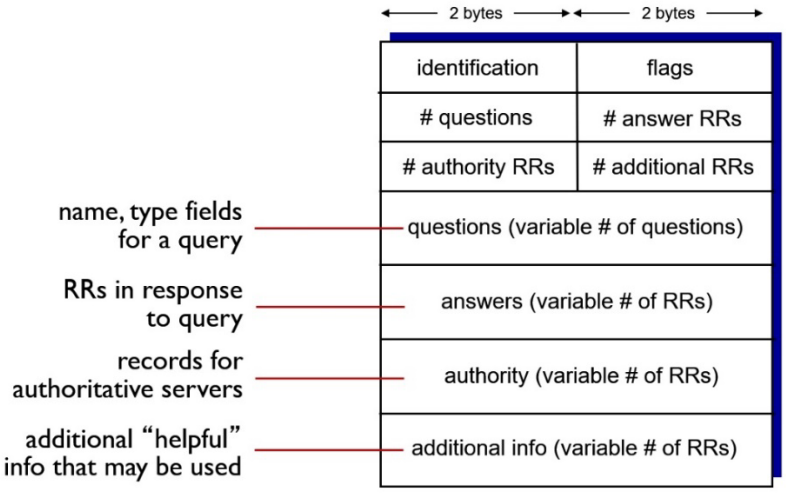
_____

DNS (Domain Name System)

โปรโตคอล DNS จะใช้พอร์ต 53 โดยระบบปฏิบัติการส่วนใหญ่จะมีโปรแกรมที่ติดต่อกับ DNS ได้ มีชื่อว่า nslookup กรณีของ Windows ให้เรียก Command Prompt จากนั้นให้เรียกโปรแกรม nslookup (หากใช้ระบบปฏิบัติการอื่นก็ทำคล้ายกัน) จะปรากฏหน้าจอดังรูป



12. ให้เปิดโปรแกรม Wireshark กำหนดเงื่อนไขให้ Capture เฉพาะโปรโตคอล DNS พิมพ์ server 161.246.52.21 ลงไป (เป็นการกำหนดให้เชื่อมต่อกับ DNS Server ที่มี IP Address 161.246.52.21 แทน Default Server) ให้ตอบว่า 161.246.52.21 มีชื่อ Domain Name อะไร _____



13. ให้พิมพ์ www.ce.kmitl.ac.th และหยุด Capture ให้ตอบคำถามดังนี้

- ใน DNS Query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

_____

_____

- ใน DNS Response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

  _____

  _____

- มี query และ response กี่ packet ให้ Capture ส่วนของ Packet Details Pane ด้วย

  _____

  _____

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

_____

_____

14. ทำตามข้อ 13 อีกครั้ง แต่ใช้ 161.246.4.119 แทนที่จะใช้ www.ce.kmitl.ac.th

- ใน DNS Query มี # questions เท่าไร และข้อมูลใน questions คืออะไร type เป็นค่าอะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

_____

_____

- ใน DNS Response มี # answer เท่าไร และข้อมูลใน answer คืออะไร ให้ Capture ส่วนของ Packet Details Pane ประกอบด้วย

_____

_____

- มี query และ response กี่ packet ให้ Capture ส่วนของ Packet Details Pane ด้วย

  _____

  _____

- มีข้อมูลส่วน authority และ additional info หรือไม่ เป็นข้อมูลอะไร

  _____

  _____

15. ให้ใช้โปรแกรม nslookup แล้วตั้ง server เป็น 199.7.91.13 จากนั้นให้ ป้อน 199.7.91.13 โปรแกรมแสดงผลอะไรมาบ้าง ให้ capture มาแสดง นักศึกษาคิดว่า 199.7.91.13 เป็น server อะไร

_____

16. ให้ป้อน query www.ce.kmitl.ac.th แสดงผลอะไรมาบ้าง ให้ capture มาแสดง จากนั้นให้ใช้ IP Address ของ ns.thnic.net เป็น server จากนั้นให้ป้อน ac.th, kmitl.ac.th และ ce.kmit.ac.th ตามลำดับ ให้ capture มาแสดง และให้นักศึกษาวาดรูปการทำ name resolution ของ www.ce.kmitl.ac.th โดยสมมติให้เครื่องที่ request เป็นเครื่องที่อยู่ต่างประเทศ

17. ให้เปิดไฟล์ tr-dns-slow.pcapng แล้วหา packet response ของ DNS แล้วขยายส่วนที่เป็น DNS หาข้อมูลเวลา จากนั้นให้สร้างเป็นคอลัมน์ ตั้งชื่อเป็น DNS Delta
18. ให้ Sort แล้วดูว่ามี DNS Query/Response ใด ที่ใช้เวลาเกิน 1 วินาที ให้ capture ผลการค้นหามาแสดง

    _____

19. ให้เริ่ม capture ใหม่เฉพาะข้อมูล DNS จากนั้นให้ใช้โปรแกรม nslookup และกำหนด server เป็น 161.246.4.3 จากนั้นให้ query www.ce.kmitl.ac.th จากนั้นเปลี่ยน server เป็น 161.246.52.21 และ 8.8.8.8 ตามลำดับ ให้เปรียบเทียบ DNS Delta ที่ได้จากแต่ละ Server (แสดงตัวเลขที่ได้) จากนั้นให้วิเคราะห์ผล

    _____

    _____

    _____

    _____

งานครั้งที่ 5

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งโดยเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา และ _Lab5 เช่น 63010789_Lab5.pdf
- กำหนดส่ง ภายในวันที่ 16 กุมภาพันธ์ 2565