**Task 1.1: Sniffing Packets**

**Task 1.1A**

Run as root:

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

Compare to run as user seed:

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, เอกสาร

คำอธิบายที่สร้างโดยอัตโนมัติ

จาก Error: PermissionError: [Errno 1] Operation not permitted คือ แม้ว่าจะเปลี่ยน permission ไฟล์ให้ execute ได้ด้วย chmod แล้ว แต่ไม่สามารถ execute ไฟล์ได้ เนื่องจาก sniff ต้องการสิทธิ์ระดับ root เท่านั้น

**Task 1.1B**

**• Capture only the ICMP packet**

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

**• Capture any TCP packet that comes from a particular IP and with a destination port number 23.**

- ฝั่ง action

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

- ฝั่ง sniffing

รูปภาพประกอบด้วย ข้อความ, ตัวอักษร, ภาพหน้าจอ

คำอธิบายที่สร้างโดยอัตโนมัติ

**• Capture packet(s) comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to.**

- ฝั่ง ping

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

- ฝั่ง sniffing

รูปภาพประกอบด้วย ข้อความ, ตัวอักษร, ภาพหน้าจอ, ข้อมูล

คำอธิบายที่สร้างโดยอัตโนมัติ

**Task 1.2: Spoofing ICMP Packets**

**Demonstrate that you can spoof an ICMP echo request packet with an arbitrary source IP address.**

- ฝั่ง spoofing

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, จำนวน, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

- ฝั่ง sniffing

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

**Task 1.3: Traceroute**

Command for sending packet

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

จากการทดสอบ ping ผลมีค่า TTL =1 แล้วได้รับ echo-reply ทันที เนื่องจาก router รู้จัก IP เหล่านี้แล้ว

**Task 1.4: Sniffing and-then Spoofing**

Code สำหรับ sniff แล้ว spoof กลับไป หลอกว่าเป็นเครื่องปลายทาง

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

* ping 1.2.3.4 # a non-existing host on the Internet

- ฝั่งส่ง ping โดยไม่โดน spoofing

รูปภาพประกอบด้วย ข้อความ, ตัวอักษร, ภาพหน้าจอ, ขาว

คำอธิบายที่สร้างโดยอัตโนมัติ

- ฝั่ง spoofing - ฝั่ง ping

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

ฝั่ง spoofing ประพฤติเป็น 1.2.3.4 ที่ไม่มีจริง ทางฝั่ง ping จึงได้รับ packet echo-reply สำเร็จ

* ping 10.9.0.99 # a non-existing host on the LAN

- ฝั่งส่ง ping โดยไม่โดน spoofing

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, อัลจีบรา

คำอธิบายที่สร้างโดยอัตโนมัติ

- ฝั่ง spoofing - ฝั่ง ping

รูปภาพประกอบด้วย ข้อความ, ตัวอักษร, ภาพหน้าจอ

คำอธิบายที่สร้างโดยอัตโนมัติ

เนื่องจากในวง local subnet จะมี ARP ช่วย map MAC เครื่องกับ IP ในวง แต่ ARP ไม่รู้จัก 10.9.0.99 จึงตอบกลับมาเป็น Unreachable Host ดังนั้นจึงไม่โดนผลกระทบจาก spoofing

* ping 8.8.8.8 # an existing host on the Internet

- ฝั่งส่ง ping โดยไม่โดน spoofing

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

- ฝั่ง spoofing - ฝั่ง ping

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

ทางฝั่ง ping ได้รับ echo-reply packet ที่เขียนว่า DUP! เพราะว่าเกิด packet ซ้ำ ซึ่งมาจากทั้งเครื่อง spoofing และต้นทางจริง (8.8.8.8) echo-reply ทั้งคู่