

## **Lesson 4. Understanding the bettercap tool**

### **GOAL**

This lesson shows how bettercap enables the attacker machine in becoming the man-in-the-middle.

### **TASK A.**

From your Windows machine, try to ping the below remote server

google.com

Ex., ping google.com

What output did you get?

```
C:\Users\sandh>ping google.com

Pinging google.com [2607:f8b0:4009:81b::200e] with 32 bytes of data:
Reply from 2607:f8b0:4009:81b::200e: time=43ms
Reply from 2607:f8b0:4009:81b::200e: time=39ms
Reply from 2607:f8b0:4009:81b::200e: time=34ms
Reply from 2607:f8b0:4009:81b::200e: time=33ms

Ping statistics for 2607:f8b0:4009:81b::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 43ms, Average = 37ms
```

We see Alice can ping google.com, which means Ubuntu VM is forwarding Alice's traffic.

### **TASK B.**

On the Ubuntu machine, Mallory should be able to intercept the packets from the victim machine.

Run the command.

*net.sniff on*

On the Windows machine, open the browser and navigate to any HTTP website such as

Unicornitems.com

Click on 'My account' and type any username and password and log in.

Go to the bettercap terminal on the Ubuntu machine (Mallory). You should be able to see each of the requests sent from the victim machine (Alice). You should also be able to see the username and password that you typed.