Man-in-the-Middle Attack

1. Setting up a virtual lab environment for the MITM lab
   (i) Download the following VMs
      - **Kali Linux** (please choose an older version, e.g. 2018.2 which is available here)
      - **Windows 10 VM as target 1** https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
      - **Metasploitable2 as target 2** reuse the VM from Lab 1

   (ii) Import the VMs as appliance , please pay attention to the following settings
      - Kali Linux: Select USB 1.1 only in settings->USB
      - Windows 10: Specify type (Microsoft Windows) and version (Windows 10 64-bit) in general

   (iii) Setup a global NAT network
      - File->Preferences
         1. Create a new NAT network called "MITM network"
         2. Assign an IP address range to it, e.g. 192.168.56.0/24
         3. Select "Setup for DHCP"
      - Kali Linux
         1. Virtual box manager, go to Settings->network of Kali
         2. Change to NAT Network "MITM network"
      - Windows 10
         1. Virtual box manager, go to Settings->network of Win 10
         2. Change to NAT Network "MITM network"
      - Metasploitable2
         1. Virtual box manager, go to Settings->network of Metasploitable2
         2. Change to NAT Network "MITM network"
      - Test the connectivity between all host machines by using the ping command

   (iv) After the Kali system is ready, enable IP forwarding by using the command
      - `echo „1“ > /proc/sys/net/ipv4/ip_forward`

   Hint: You might want to use the Webserver of the Metasploitable2 machine as example and demo system (several running web applications have weak passwords configured, e.g. the DVWA web site).

2. Use **Ettercap** (*http://ettercap.sourceforge.net/*) to launch a MITM attack based on ARP poisoning. Ettercap is part of Kali Linux and can be found under applications->09 - sniffing & spoofing

   (i) Start with capturing ICMP messages between two hosts
   (ii) Observe and note the arp caches of both target systems, what is changing as soon as Ettercap is active
   (iii) Capture the traffic of another internet connection and find the user/password login credentials to access a web page that is protected by a basic authentication mechanism only.

3. Explore the available options for MITM attacks that can be launched with the Ettercap tool.