Exercises on Man-in-the-Middle Attacks

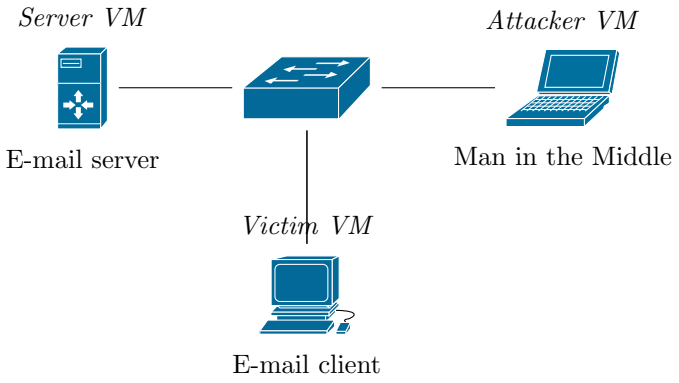
Solve the following exercises and submit them until the communicated date.

Reminder: All VMs must be running at the same time and your host machine **must** be disconnected from the Internet at any time during the subsequent exercises unless explicitly noted otherwise. For details, refer to the respective VM tutorials and the instructions on the previous exercise sheet.

LB-MA 00.

a) As the user *Victoria Victim* in the *Victim VM*, start *Mozilla Thunderbird* and ensure that you can send e-mails from your pre-configured e-mail account (`victoria.victim@lab-unterweger.it-security`) to another user, e.g., `maintenance@lab-unterweger.it-security`. The recipient can see its e-mails by logging into the *Server VM* with its user name, e.g., `maintenance`, and the corresponding password. In the provided setup, the *Server VM* acts as the e-mail server with its user accounts.

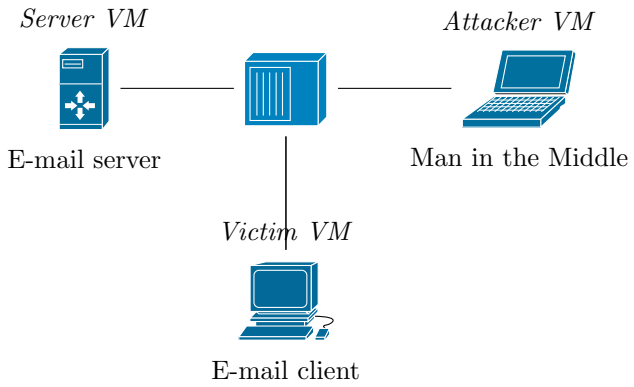
b) As the e-mail recipient user from a), use the `mail` command on the *Server VM* to read see the user's e-mails and verify that the e-mail from a) has been successfully received. Reply to the e-mail and make sure that the response e-mail can be received and read by the user *Victoria Victim* in the *Victim VM* from within *Mozilla Thunderbird*.
Usage note: `mail` is an interactive command line utility for reading and writing e-mails. Type the `h` command to list messages, the `t` command, followed by the listed message number, to show the respective message, `R` to reply to the shown message and `x` or `q` (archives all read messages) to exit. Confirm each command with the return key. The command `help` shows a list of available commands. When replying (or writing e-mails, in general), indicate the end of the message by hitting return and afterwards pressing `Ctrl+D` twice. Note that new incoming e-mails are not shown automatically, but require `mail` to be exited and restarted.



LB-MA 01.

a) In the *Attacker VM*, start *Wireshark* and try to capture any IMAP or SMTP traffic between the e-mail client and the e-mail server, as shown in the network diagram above. For simplicity, capture only while the client sends and receives new e-mails. Describe which data can be captured and how sensitive it is. Explain why the rest cannot be captured. A tutorial on how to use *Wireshark* is available in the How to use *Wireshark* Section.

b) Without shutting down the virtual machine, go to the network configuration of the *Attacker VM* in *VirtualBox* and set the *Promiscuous mode* of the VM's only network adapter to *Allow all VMs* (you may have to expand the advanced properties to see this setting). This simulates a network that is not switched, i.e., a network where all VMs are connected to a single central hub, as illustrated in the figure below.
After first **stopping** the capturing process within *Wireshark*, repeat a). Explain the differences in the results by elaborating on the differences between switched and non-switched networks.



LB-MA 02.

a) Revert the promiscuous mode setting (to *Deny*), like in exercise 01. b). After restoring the switched network through this change, use *Ettercap* (see How to use *Ettercap*) to perform an ARP poisoning attack so that all network traffic between the e-mail server and the e-mail client is passed through the man in the middle. While the attack is ongoing, repeat exercise 01. a). Describe which information, especially message content, can be intercepted by the man in the middle. Explain which content is encrypted, e.g., via TLS, and which security implications this has.

b) Use the command `arp -a` in **all** VMs but the *Attacker VM* to see their ARP caches before, during and after a successful ARP poisoning attack. Explain why and how this information helps to detect an ongoing attack.

How to use *Wireshark*

Wireshark can be started from the command line through the `wireshark` command. Alternatively, it can be started through the program menu of the operating system.
A new capturing process can be started by double-clicking the network interface name, e.g., `enp0s3` (hovering the mouse over the name shows the interface IP address for verification). Until the capturing process is stopped through the corresponding symbol in the toolbar, all packets being sent from or received at the selected network interface are captured and listed so that they can be analyzed.
The text box at the top can be used for filtering. For example, the filter `imap` exclusively shows packets which use the IMAP protocol. Each of the packets listed after filtering can be examined layer by layer in the middle portion of the windows upon selection. The protocol layers are displayed from bottom to top, i.e., the top-most protocol layer (e.g., IMAP) is at the bottom-most position in the list. Details can be accessed by expanding the corresponding fields of each protocol layer or any of its expandable fields.
If a new capturing process is to be started, the current list of captured packets can be discarded by clicking the *Close* item in the *File* menu. In the appearing prompt, the option *Continue without saving* has to be chosen. A new capturing process can then be started as described above.

How to use *Ettercap*

The graphical user interface of *Ettercap* can be started from the command line by calling `sudo ettercap -G`. Alternatively, it can be started through the program menu of the operating system.
In the initial setup, make sure that the selected primary (network) interface is the same that has been used previously in *Wireshark*, e.g., `enp0s3`. Click the *Accept* button (check mark symbol) to proceed.
Next, click the *Scan for hosts* button (magnifying glass symbol), wait for the scan to finish and subsequently click the *Hosts List* button (Web hosting symbol). In the appearing list, select the first of the two IP addresses between which all communication should be intercepted and click the *Add to Target 1* button. Do the same for the second address, but with the *Add to Target 2* button.
To start a man-in-the-middle attack, click the *MITM* button (Internet symbol), select *ARP poisoning...* in the appearing menu and confirm by clicking *OK*. The ARP poisoning attack is now active until the *Stop MITM* button (cancellation symbol) is clicked.