Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Import the VM provided in the file HackingLab.ova into your local Virtual Box lab (select the option “Include all network adapter MAC addresses” when importing). Make sure your own Kali Linux VM can communicate with all the other VM in the lab by means of the internal network (try nmap -sn 192.168.0.0/24, because inbound pings are filtered out by default in Windows). Then, answer the questions below, giving an explanation of how or why even if not explicitly asked.

Reference tutorial: <https://www.hackers-arise.com/post/2017/08/28/mitm-attack-with-ettercap>

Part A: Checking the environment

1. Capture a screenshot of the nmap command showing all 3 machines in the network.
2. Open a browser in the Debian client and access the URL http://baloon/herzing. Capture a screenshot.
3. Try with http://baloon/herzing/private. What kind of authentication was set in IIS? Check it out in the IIS Manager in the Windows server.

Part B: Preparing an ARP poising attack

1. Open the graphical interface for ettercap, available by default in Kali under the Sniffing & Spoofing category. Make sure you select the internal network interface that has connectivity with the other machines in the lab. Then, click on the “Accept” button on the top right. Copy & paste here all messages in the bottom frame.
2. Click on the “Host List” button on the top left corner. If the list is empty, click on the “Scan for hosts” button. Once you get them, capture a screenshot.
3. Execute a ping from the Windows server to the Debian client. Then, check the ARP table in both. What command did you use? The MAC addresses are different. However, the first 6 octets are equal. Why?
4. Back in ettercap, right click on 192.168.0.31 (the server) and set it as Target1; then, 192.168.0.101 (the client) as Target2. Finally, click on the “MITM menu” button on the top right corner and select “ARP poisoning”. Capture a screenshot including the bottom frame.
5. Check again the ARP tables and explain in your own words what is happening. Support your explanation with screenshots if necessary.

Part C: Performing the MITM attack

1. Now, all communication will pass through Kali. To demonstrate it, browse to http://baloon/herzing/private from the Debian client. Use any credentials, such as “abc” for username and password. Then, check the messages frame in ettercap. Capture a screenshot.
2. When done, always click on the “Stop MITM” button. How can you protect against MITM attacks? How could you try this protection in the present lab?
3. Using filters, you can interfere with the communication. As root, move to the folder /usr/share/ettercap in Kali. Copy the file etter.filter to myfilter.txt and, then, modify it so that “Herzing” is substituted by your first name. Also, the message to be logged is “Hacked”. Show the content of the new file.
4. The filter needs to be compiled to a new file, for instance myfilter.comp. What command would you use?
5. Repeat the attack but loading the filter you created and, then, browsing to http://baloon/herzing. Capture a screenshot of the message frame.
6. Execute the command “wget http://baloon/herzing/index.html” as well (you might need to press Ctrl+C to return to the shell prompt). What is the content of the file?

Part D: Reasoning

1. Explain why this attack would not be effective if you are in a different network segment than the victim.
2. Your co-worker advised the IT Manager to use encryption to prevent ARP poisoning attacks. What is your opinion?