1. What is the men in the middle attack and what does the attacker gain with it? **(4p)** Describe a men in the middle attack that can be performed on the local area network! Use a sequence diagram to show the steps of the attack! **(6p)**

2. Suppose, we have a captive portal protected wireless network. Describe, how an evil attacker can perform a successful ARP poisoning attack! Draw a time sequence diagram with the attacker, a victim and all other involved parties! **(6p)** What kind of damages can the attacker make after a successful attack? **(4p)**

3. Describe step by step, how you can perform an ARP poisoning attack! **(4p)** What are the benefits you can gain through this attack? **(4p)** Is it possible to make this attack work for arbitrary victims over the Internet? **(2p)**

4. Describe step by step, how someone can perform a man in the middle attack on the local network! **(6p)** How is it possible to protect against this attack from the user's side? **(2p)** How is it possible to protect against this attack from the network's side? **(2p)**

5. Describe step by step, how you can perform an MAC flooding attack against a switch, and what can you gain! **(3p)** What mechanisms make this attack possible in the switch? **(3p)** How to protect your switch against these attacks? **(4p)**

6. Bob's company is a software developer startup that has a web (port 80) site to offer their latest products and their drivers. Plus they have their own proprietary authentication service running on port 88. Both servers are on the company's site and the developers should be able to access them. The Internet access should be disabled for all employee and services, so they should not initiate connections to the Internet! The only exception is a single machine, which should be connected to the internet, but not to the local network! How would you create the defense of the company's network in order to prevent attack from the Internet? Create a sketch! In the case, if you would use firewalls, describe the ACL in table format! **(10p)**

7. Describe the similarities and differences between the packet filter and application proxy firewalls! Which are the pros and cons for the given firewall type? Which firewall is stronger and why? **(6p)** Describe an arbitrary packet filter firewall rule and give explanation to all parameters, what does it mean, how does it work! **(4p)**

8. What is the DMZ, and why is it good or bad for administrators? **(2p)** Create a network with DMZ zone and put the following servers into your network: company's public web server, company's public ftp server, company's internal web server! **(4p)** Put firewalls into your configuration and describe the basic rules in a table for them! **(4p)**

9. To defend you company's network against attacks from the Internet, you plan to setup firewalls. The company has a public web page and a public ftp server that should be available from the Internet. The protection should be efficient, but should use packet filters as firewalls! Design the protection. Depict the place of the protection and the servers and the networks! Explain your configuration! **(5p)** Give the firewall rules (ACLs) when only these two services should be available from the Internet! **(5p)**

10. You have a firewall with 3 zones: Internet, intranet and DMZ. Describe what DMZ is and what you should put into DMZ! **(4p)** Assume that your web server should be reached from the Internet and the administrator’s PC (it is inside the intranet), but should not be accessible from the rest of the intranet hosts. Also, the web server should not initiate any connections. Create the firewall’s Access Control List (ACL)! Describe the ACL table! **(6p)**

11. You have a firewall with 3 zones: Internet, intranet and DMZ. Describe what DMZ is and what you should put into DMZ! **(4p)** In the same environment, your web server can be reached from the Internet and the administrator’s PC (which is inside the intranet), but it is not accessible from the rest of the intranet hosts. Also, the web server should not initiate any outgoing connections. Create the Access Control List (ACL) of the firewall(s)! Describe them line by line! **(6p)**

12. Your task is to deploy security elements within your company network to protect running services. Indicate the threats and their attack points! **(5p)** Design the protection! What should be used, why and where? **(5p)**

13. You are the network security architect of a medium sized company. The boss ordered a secure network with web and ftp servers (not necessarily the same servers) for both public and internal access, plus an email server. Plus there are some workers who occasionally would like to work from home. Design the layout of the network, and place the servers inside it. Use only the most secure solutions! Sketch the network plan with servers and describe them! Write down, why do you use that particular solution and why don’t you use something else! **(10p)**

14. There is an intruder in your network, who can control one of your host machines. It is possible that the intruder will try to gain access on all the communications in the network. Assuming a small LAN with a few servers, hosts and switches, how could the intruder do that? **(5p)** How could you spot and stop these attacks? **(5p)**

15. You would like to run your company’s Web server that Internet customers can reach, and also a Web server for your internal employees. How can you place these web servers and firewalls in your network, to protect yourself against threats coming from the Internet? Sketch your network configuration! **(5p)** The web service is running on port 80. Please give the rules of your firewalls that block all traffic coming from Internet and going to your machines, except the web traffic to the company’s web server. **(5p)**

16. Tell 3 different kinds of attacks that can be detected using a Network IDS! **(3p)** Tell 3 different kinds of attacks that can be detected using a Host IDS! **(3p)** What are the difficulties of NIDS-es? **(4p)**

17. You have a WEP compatible WiFi stick. Describe what is wrong with WEP in terms of security! Describe all the problems! **(4p)** How is it possible to fix WEP? Describe the algorithms that create a secure WiFi reusing the WEP engine! Beside the description, depict them using a block scheme! **(3+2p)**

18. Describe the TKIP protocol, mentioning the WEP problems that were fixed. **(7p)** If TKIP is still using the WEP engine, why it is considered as a secure solution? **(3p)**

19. Describe the change from the WEP WiFi protection to the WPA protection! What were the mistakes and how are they fixed now? Mention the related attacks as well! **(7p)** If TKIP is still using the WEP engine, why it is considered as a secure solution? **(3p)**

20. Depict the WPA (WPA-TKIP) and WPA2 (AES-CCMP) protocols using a block diagram! **(2x2p)** Compare the two solutions! What are the similarities and differences? What are the pros and cons of the different solutions? **(6p)**

21. Draw and compare the block diagrams of WPA-TKIP and WPA-CCMP! **(6p)** Describe, the differences between the protocols, algorithms and their parameters! **(4p)**

22. Create a block diagram and show how WPA-TKIP utilizes the WEP engine to transmit the packets! **(7p)** Describe, why WPA-TKIP is more secure than WEP! Give at least 3 different reasons with explanations! **(3p)**

23. Besides the firewalls, you plan to strengthen the WiFi network protection as well, upgrading it from WEP protection. Show at least 3 different problems of the WEP protocol! **(3p)** Describe a protocol that is safer than WEP, compare the solution to the WEP protocol in all possible aspects. **(7p)**

24. There is a project to cover your enterprise with an enterprise level wireless network. The network access should be as safe as possible! Focusing only on the network access, describe your approach, how this access is organized efficiently and securely! Describe every devices and servers that are required for the operation! Describe the protocols that you use! **(10p)**

25. There is a project to cover whole Budapest with free wireless network. For this reason one company gives thousands of APs and also provides the Internet backhaul. Your task is to organize the wireless network in Budapest. The network should be accessible for the most citizens, regardless their computer skills! However, the network should be safe as well! Describe your approach, how this network is organized efficiently and securely! Describe every devices and servers that are required for the operation! Describe the protocols that you use! **(6p)** In your network, describe the potential problems regarding the security of the network and the security of the users! **(4p)**

26. Compare the TKIP and the AES-CCMP solutions by sketching their internal blocks! **(5p)** Why has TKIP a relatively complex key mixing? How is the key mixing accelerated in this case? **(5p)**

27. Give a complete description, what problems of Wired Equivalent Privacy (WEP) was solved by the WiFi Protected Access (WPA) TKIP (Temporal Key Integrity Protocol) mechanism! Write down what was the problem and what was the solution! **(8p)** TKIP reuses the WEP engine in the interface. What is the reason behind it? **(2p)**