Komunikacijski protokoli in omrežna varnost
2013/14
First midterm

This test must be taken individually. Any and all literature may be used while taking this test. Answer diligently *all* questions.

Bonus points might be awarded if you at least partially correctly answer each question.

Duration of the test: 60 minutes.

We wish you a lot of success – veliko uspeha!

TASK	POINTS	MAX. POINTS	TASK	POINTS	MAX. POINTS
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Peter has just landed a job as the network system administrator in some company. Veronika, Peter's friend, also recently started working as a system administrator, only at a different company.

VPRAŠANJA:

1. Veronika noticed, that all devices in the company have pre-set IPs within the range 192.168.12.0/24 – in other words, the company does not use the DHCP protorol. After consulting Peter she decided to implement the DHCP protocol. This means that each device would get the IP during bootup and that the IPs would not always be the same. Most users never noticed the change, but a few complained that they always want to have the same IP. Describe *two* ways for Veronica to give them what they want.

2. One of the employees, Cefizelj, was especially angered by Veronica's improvement and has decided to disable the system for assigning IP addresses by using a DHCP server. (i.) Describe two ways for Cefizelj to disable the DHCP server so that it is no longer able to assign IPs and (ii.) how can Veronika protect the server against each of these two attacks.

    HINT: You can assume that you have access to the DHCP source code and are able to fix it in any way neccessarry.

3. Veronika would like to set the date on each computer during bootup using the bootp protocol. (i.) Which field can she use to transfer the information about the date? (ii.) Would she need to change/update anything on the client to actually set the date? Explain your answer.

2. naloga:

VPRAŠANJA: Addressing is a basic concept which can be met anywhere content has to be transfered from a source to some destination.

VPRAŠANJA:

1. In the IP standard definition, the addresses are divided into two large groups according to their function (method of delivery): *unicast* and *multicast*. (i.) Describe how the two groups differ regarding their functionality? (ii.) List the IPv6 ranges used for each of the groups. (iii.) When talking about multicast, we mentioned the IGMP and PIM protocols. Which of these actually transfers the multicast packets? Explain your answer.

2. Peter noticed that his predecessor set the IPs of the devices on the network to a range between 192.1.1.1 and 192.1.1.100. Peter immediately recommended his boss to change the addresses. The boss did not agree with the

recommendation because the Internet at the company works fine. (i.) Who is right, the boss or Peter? Explain your answer. (ii.) Suggest a way to check, whether the boss or Peter is right. Write which programs to use and how to use them in order to check who was right.

HINT: You can get bonus points for a complete answer.

3. During lectures, we mentioned the importance and role of protocols. (i.) What is the purpose of a protocol? (ii.) Explain with an actual example.

4. NON-OBLIGATORY An important role in transfering packets (postage packets, not IP packets) could have been played by an improvement suggested by Lovrenc Košir from Spodnja Luša near Škofja Loka who sent his suggestion to the Austro-Hungarian postal service in 1835 but was denied. What did Lovrenc suggest five years before this improvement was implemented by the Postal Service of the United Kingdom?

3. naloga:

VPRAŠANJA:

1. At his new job, Peter wants to control a number of devices. To make the overview of what is going on with the devices easier, he has written a program which uses the command snmpget[1] to read a value and then plot it as a point on a graph. Peter now has to somehow specify, which value snmpget should read. (i.) Can Peter read the chosen value without having an entry for it in the MIB? Explain your answer - if he can, explain how the value can be chosen; if not, explain why the MIB entry is neccessarry.

2. The SNMP uses UDP as the transport layer protocol. (i.) Why do you think UDP is used? (ii.) For the protocol to work, the manager and the agent have to establish a session. Describe how a session is established in SNMP. Describe the package contents and the order of steps taken during the establishment of the session. (iii.) Security is the most dire problem regarding SNMPv2. Describe how SNMPv3 solves this problem. Describe the content of the packages and the steps taken in communication.

   You are not expected to know the exact names and sizes for each field, only which fields are used and how.

3. Peter's server has received the following sequence of bytes (first the one on the far right, all values are decimal):

---

[1]The program is similar to the program snmpwalk, only it reads just a single value

33 73 82 70 04 02 33 73 82 70 04 04

What is the meaning of the received sentence? Explain your answer. If you think one of the values represents an ASCII character and do not know which character that is, write that down in the answer.

4. naloga:

VPRAŠANJA:

1. The service for setting the network time uses the NTP. (i.) Which protocol does NTP use at the transport layer and why?

   One of the problems NTP must solve is the transfer delay. (ii.) Describe in as much detail as possible all the delays present in using the protocol and how the protocol solves each problem.

2. In the RTP protocol, a stream source (SSRC) sends data to a receiver. How can the receiver determine what the sender is (a camera, a microphone, ...)? Describe the solution.

3. Peter went further with the time and entered the new world of clouds. He is renting a server but without administrative rights and he wants to use a program called `MojProg`. He downloaded a package with the program to the server and unpacked it in sub-directory of his home directory called `~/mojProg`. The program itself is in the file `~/mojProg/bin/mojprog`.

   Peter wants to run his program by simply writing `mojprog` at the shell prompt, regardless of the directory he is in. (i.) Which environment variable should he change? (ii.) How?