Komunikacijski protokoli in omrežna varnost
2012/13
Pisni izpit

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: 75 minutes.

A lot of success – veliko uspeha!

TASK	POINTS	MAX. POINTS	TASK	POINTS	MAX. POINTS
1			4		
2			5		
3					

IME IN PRIIMEK: ______________________________

ŠTUDENTSKA ŠTEVILKA: ______________________________

DATUM: ______________________________

PODPIS: ______________________________

1. naloga:

VPRAŠANJA:

1. This time, Peter is concerned with the bootp protocol. Actually, he is concerned about a bothersome boss who sometimes wants to boot his computer into Linux and sometimes into FreeBSD. Peter always has his computers boot over the network. How can he have the bosses computer boot over the network in a way that will allow the boss to choose the operating system when the computer starts?

   NAMIG: The more detailed the description of each step during boot, the more points you will get.

2. One of the most commonly used protocols is NFS. Which transport layer protocol does it use? Why?

   Name three risks encountered by Peter when he adds the following line to his exports file:

   ```
   /boot    -network 192.168.12.0/25
   ```

   Explain the reasoning behind your answer.

3. The IP and network address of computer A is 192.168.12.7/25. Which addresses (including *broadcast*) may be used inside this network?

4. Peter has decided to use 192.168.12.161 as the IP address of the gateway in his network. Is this even allowed? Explain the reasoning behind your answer.

2. naloga: This task is about multicasting.

VPRAŠANJA:

1. In the lectures, we learned about two protocols which are related to multicast: IGMP and PIM. Describe the role of each protocol it has in multicast. Be careful of the different tasks related to multicast: joining a group, packet delivery, ...

2. Peter Zmeda has run the following command `netstat -g`:

   ```
   Group                     Link-layer Address      Netif
   224.0.0.251               <none>                  lo0
   224.0.0.1                 <none>                  lo0
   224.0.0.251               1:0:5e:0:0:fb           en0
   ```

```
224.0.0.1              1:0:5e:0:0:1           en0
224.0.0.251            1:0:5e:0:0:fb          en1
224.0.0.251            1:0:5e:0:0:fb          vmnet8
224.0.0.1              1:0:5e:0:0:1           vmnet8
224.0.0.251            1:0:5e:0:0:fb          vmnet1
224.0.0.1              1:0:5e:0:0:1           vmnet1
```

Comment on the output.

3. Peter would like to re-transmit a recording of a TV program where they often play baroque suites. Because the only people who still listen to such music are Peter, his mother and some of their friends, he has decided to only stream the recording inside his home network. To do this, he intends to use the following command line:

```
cvlc --"sout=#transcode{vcodec=h264,vb=200,scale=0.5}: \
  rtp{dst=233.252.0.63,port=5004,mux=ts,ttl=1}" \
  --sout-keep peter.mp4
```

   How should he change the command line if suddenly, thousands upon thousands of people who like this sort of music wished to listen to it and see the musicians play in HD? Explain the reasoning behind your answer.

   How should he change the command line if their neighbor has just bought a coffee grinder from 1976 with worn-out brushes and Peter's mother only wishes to listen to her son's favorite concerts on a tablet computer. Do not worry if you do not know all the VLC command-line switches by hand – you can get full points for each of the questions if your explanation is correct and sufficient.

4. NON-OBLIGATORY Name three movements of a French baroque suite.

3. naloga:

VPRAŠANJA:

1. Peter has become involved in a dispute with his friend Simon. Peter claims that RADIUS is a safe protocol because he remembers that a radius packets contain an authenticator among other things. Explain the role of the authenticator in the RADIUS protocol.

2. Describe three possible attacks on the RADIUS protocol and the damage each attack can cause.

3. How does the CHAP protocol prevent replay attacks?

4. naloga:

VPRAŠANJA:

1. Traffic security can be ensured on different network layers. Write down all the layers and how traffic security may be handled on each layer (also write down the names of respective securtity protocols on each layer).

2. The IPsec protocol can work in one of two modes – either in transport or tunnel mode. Describe how packets are transformed between a source and a destination device if tunnel mode is used and only the authentication of a packet is required. Be careful when describing the heads of each packet.

3. What is a content of a PTR DNS record for the domain `d.c.b.a.in-addr.arpa`?

   One of the possible attacks on the security of the Internet is an attack on the root DNS servers. Comment on the possible damage caused by an attacker gaining control over one of the root DNS servers.

5. naloga: IEEE 802.

VPRAŠANJA:

1. During the lectures, we mentioned the IEEE 802.1x standard and the EAPOL protocol. How are they related? Describe the function and purpose of both the standard and the protocol.

2. Recently, the IEEE has approved a new standard – IEEE 802.11ad, also known as *WiGig*:

   > *The IEEE Standards Association has approved WiGig, a very fast, short-range networking technology that operates in the 60-GHz band. WiGig, also known as 802.11ad, has the potential to eliminate the tangled bundle of wires at the back of PCs, and could start appearing in routers as early as the second or third quarter this year. The technology would transfer data at 7 Gbits per seconds, compared to current routers using 802.11g technology that transfer data at 50 Mbits/s and 802.11n at 100 Mbits/s.*

   When Peter Zmeda learned about this news, he panicked. He is afraid that he will have to replace all the switches and bridges in his company's network. Is his fear well grounded? Explain the reasoning behind your answer.

   NAMIG: The link layer in IEEE 802 is not monolithic.

3. The IEEE 802.1d protocol handles MAC bridges. Among other things it specifies a protocol for building a spanning tree inside a network. Why is a spanning tree necessary?