Communication Protocols and Network Security 2020/21
Written exam 3. Sol-mōnaþ 2020

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

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

Duration of the test: 105 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. task: Basics. Strange things were happening on the Butale network, and in search of the source of the problems, Peter Zmeda recorded traffic on the network on Figure 1.

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: ba:ba:fa:fa:de:ca (ba:ba:fa:fa:de:ca), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: ba:ba:fa:fa:de:ca (ba:ba:fa:fa:de:ca)
    Sender IP address: 10.0.11.71
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.11.1
```

Figure 1: Network traffic trace.

QUESTIONS:

A) (i.) Which protocols are presented in the trace on Figure 1 and on which network layers are they? (ii.) Who is the sender and to whom is the frame sent and what does the sender want?

B) Peter has set up computers at the company to run over a network. He provides them with all the information needed to boot from a computer that has all the necessary programs. Unfortunately, he started to run out of space on this computer. (i.) Which piece of software do you suggest moving elsewhere to free up as much disk space as possible? Justify the answer. (ii.) If he is still running out of disk, what is the second piece of software to move? Justify the answer.

   HINT: Write down which data is provided by the first and which by the second piece of software.

C) In describing the services and protocol, we mentioned *entity pairs*. (i.) Take the TCP service as an example of a service. What does the TCP service offer? (ii.) How does the entity pair ensure the offered service?

   HINT: Start with describing a case when failure of the lower layer service prevents the TCP service provider from providing its service and resulting in an appropriate resolution response from the entity pair.

   (iii.) Let's say we use the UDP service on a transport layer and one member of an entity pair on the application layer asks another member a question. In

order for the latter to be able to answer the question, both the question and the answer must contain what? Justify the answer.

2. task: Time and video. Peter Zmeda wants to set up a video conferencing system on his network.

QUESTIONS:

A) He heard that the right way to transfer audio and video between participants was to use multicasting. (i.) In which case would this not make sense? Justify the answer. (ii.) He also built in the videoconferencing system a possibility of using polls. Should he also transmit data for this by means of multicasting? Justify the answer? (iii.) What about chat? Justify the answer. (iv.) What about obscuring the content at each of the points (i.) to (iii.)? Justify the answer.

B) In addition, he heard that in multicast there is a rendezvous point. (i.) What is a rendezvous point (RP)?

   (a) A server where we can get information about different multicast groups.
   (b) A router that is a part of two subnets and forwards multicast traffic.
   (c) A router that plays a role of the root of distribution tree.
   (d) A node that is a part of multiple multicast groups.

   (ii.) Describe an example of using a rendezvous point.

C) Peter has set up his own DHCP server using Debian GNU/Linux and the ISC-DHCP-SERVER package. He has added the following to his /etc/dhcp/dhcpd.conf:

```
host pxelinux.0
    hardware ethernet ba:dc:0d:e5:d0:0d;
    filename "peter.si";
```

   (i.) What is the hostname? Justify your answer. (ii.) Which bootloader is he using? Justify your answer. (iii.) Apart from a DHCP server, what else does he need in order to get the bootloader to load? Give an example program (package) providing it.

3. task: My network and its management. Network management includes hardware and software management as well as user management.

QUESTIONS:

A) To set up IP addresses on the network, Peter set up a DHCP server. He determined the pool from which to assign addresses. When he connected a few dozen computers, problems started - some computers no longer got the address. Peter suspects that the server has run out of addresses, so he will add another DHCP server. Justify the answers to the following questions. (i.) Is his approach correct? (ii.) How should he configure a new server? (iii.) How else could he solve his problem?

B) When logging network events, the message in the `syslog` protocol contained the record:

```
Jan 31 09:21:19 kajtimar dhcpd[61626]:
  uid lease 192.168.126.164 for client ac:cc:8e:bb:17:bd
  is duplicate on internaMreza
```

(i.) Which program requested the record?

(a) `dhcpd`
(b) `kajtimar`
(c) `uid`
(d) `lease`

(ii.) What does the record say? Describe what happened.

C) In network management, we mentioned management: of errors, of configurations, of security, and of access logs. Users are also among the three factors we manage. (i.) For each of the four mentioned managements, describe an example of user management. (ii.) For each of the management examples, please provide software or protocol that allows the mentioned management.

HINT: Be specific when describing a management example – describe the specific situation and how we manage users in it.

4. task: Security.

QUESTIONS:

A) Let's say we use the LDAP database for authorization. Sometimes, one may wish to find objects based on complicated queries. For example, one might want to find every person in Maribor named either Janez or Borut. Are such queries against LDAP databases even possible by just using the query language these databases support?

(a) This is supported. The conditions are chained using an infix notation.

(b) Such complicated queries are not supported by the LIGHT-WEIGHT Directory Access Protocol. The data must be filtered manually.
(c) This is supported. The conditions are chained using a prefix notation.
(d) This is supported. The conditions are chained using reverse polish notation.

B) The TLS/SSL protocol can be used to secure Internet traffic. We define three phases of operation: session set-up, data transmission and session breakdown. (i.) Which data in the IP packet (all layers) identify a session?

HINT: This question could be in the basics task, as the session is defined outside the TLS protocol itself.

(ii.) Describe how the integrity of the transmitted data is ensured in the TLS protocol? (iii.) What kind of attack could Cefizelj stage if the TLS protocol did not include a special session-breaking packet? Describe an example.

C) Peter Zmeda would like to connect to his company's VPN using OpenVPN. He has created two files using Easy-RSA: peter.csr and peter.key and has sent both files to the network administrator. (i.) Which files, created using data in his files, can he expect to get back? (ii). Which additional files will he need in order to connect to the VPN? (iii.) Has he done everything correctly? Has he forgotten something? Explain why.