Communication Protocols and Network Security 2019/20
Written exam 11. 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: 90 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 of Networking.

QUESTIONS:

A) (i) Draw an IPv4 and IPv6 packet and pair the fields that serve the same purpose in both packets. Why and how they serve the same purpose? (ii) The network layer provides basically a single service. Which one is this? (iii) How the source address is used for this service? Justify the answer.

HINT: The answer to this question is in the specific form of routing that we mentioned lectures about multicasting.

B) Can a device with an IP address 192.168.2.10 send a network packet to a device with an IP address 1.2.3.4? Justify the answer.

HINT: If you think it can not, why not? If you think it can, why yes? If you think sometimes yes and sometimes no – justify both options.

C) Peter wants to connect his computer to the Internet. He connected to a wireless network. The `ifconfig` command indicates that he got the address 192.168.1.110. (i) With which command can he verify that the default gateway is set? (ii) With which command can he verify that he can access the server at the address `www.arnes.si`? (iii) Suppose he successfully receives a response from server 8.8.8.8, but he always receives the following message from the web browser: "*Server not found - can't find the server at ...*". What else does he have to check? Justify the answer.

2. task: My network and its management.

QUESTIONS:

A) Which protocol is used for username and password authentication when entering FRI online classroom (*spletna učilnica*)?

- MIME,
- LDAP,
- TLS or
- DNS.

Justify the answer by drawing the architecture of services around the online classroom. Obviously, the online classroom is a central service that uses other services.

B) Peter would like to start the computer over the network, with a nice startup menu. The computer will boot from the menu to the DOS operating system. It has an USB installer (*Live USB* stick) with Linux Mint available. (i) Which files on the USB stick will come in handy? Justify the answer by describing the data contained in each of these files. (ii) What other files will he need to display the startup menu and where can he get them?

C) To attack passwords, meaning that an attacker wants to get user passwords, *rainbow tables* are used. Besides the tables he also needs records from the password table (on FreeBSD this is the file `/etc/master.passwd`). A record looks like this (three dots present an abbreviation):

```
peter:UZs...4sm:1002:1002::0:0:Peter Zmeda:/home/peter:/bin/bash
```

(i) What are rainbow tables – what do they contain and how do we use them to crack passwords?

HINT: Describe specifically how Cefizelj can use rainbow tables to get Peter's password.

(ii) Passwords can be further protected by a salt. How does this work? (iii.) Let's say that Cefizelj got not only the password file but also the salt. Does this help him with the attack using rainbow tables? Justify the answer.

3. task: Time and television. Peter Zmeda is setting up Butale TV. In doing this, he encountered the following issues, which you are helping him to solve.

QUESTIONS:

A) He set the current time on the central Butale TV server with the following command:

```
Peter> rdate ntp1.arnes.si
```

(i) What protocol is used for this query? (ii) How big a mistake can he expect? What does it depend on? (iii) How would he further (and in the long run) increase the accuracy of his system clock? (iv) Describe two situations in which it is important that the system time is set correctly. Justify the answer.

B) Peter's Butale TV use IP protocol to broadcast the program. Peter Zmeda noticed a REGISTER packet of PIM-SM protocol on his network. Who is sending it to whom?

- client that wants to join group to the client that is already member of a group;

- arbitrary router to the router to which the source of the data stream is connected;
- router to which the source of the data stream is connected to some other router; or
- client that wants to join group to its router.

Justify the answer by explaining what does it mean to send a REGISTER packet.

C) He spent quite a bit of time figuring out that it is crucial for the viewer to create his own session in which he watches the program. (i) Describe what a session is and what its three phases are. (ii) During the lectures we learned about two protocols for setting up a session. Which two? (iii) Describe briefly each of them. (iv) Suggest which one Peter should use. Justify your answer.

HINT: The justification must describe why the chosen one is appropriate and the other is not. If it doesn't include both viewpoints, you only get half points.

4. task: Network operation and security.

QUESTIONS:

A) We added an entry to the `/etc/inetd.conf` file for some service

```
http stream tcp nowait root /usr/sbin/httpd
    in.httpd -r /etc/httpd.conf
```

(i) Which program receives requests and sends replies via the network? (ii) Which program generates the reply for each request? (iii) On which port is the service accessible? (iv) What file contains our service settings? (v) What is the (general) function of `inetd`? What it offers us?

B) (i) Describe how ESP prevents replay attacks. (ii) And describe how AH prevents replay attacks. (iii) Which cryptographic service does AH offer and which ESP does? Justify the answer.

C) When describing firewalls, we mentioned the three levels of operational security offered by firewalls. (i) What are they? (ii) For example, let's say that we want to use the firewall to prevent someone from injucting virus in our network using the TFTP protocol. What type of firewall would you use and why the others are not good enough?