Komunikacijski protokoli in omrežna varnost 2015/16 Pisni izpit 5. kimovca 2016

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke.

Čas pisanja izpita je 90 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: ______________________________

ŠTUDENTSKA ŠTEVILKA: ______________________________

DATUM: ______________________________

PODPIS: ______________________________

1. naloga: Zagon in DHCP.

VPRAŠANJA:

A) Peter was preparing for the KPOV exam. In the lessons regarding operating system booting, he learned that the `bootp` protocol mentions an intermediate server (*proxy* or *gateway*). (1) Describe it's function in detail.

NAMIG: It would be best if you described how messages are sent between devices.

(ii) He also learned that the operating system itself is loaded by using the `tftp` protocol. He has heard that there is no need for an intermediate server when using `tftp`. Explain why.

B) Peter has downloaded a file called `delajdenar.tgz` from the web. The file is supposed to contain a program which, when run, creates money on the user's current account. When Peter unpacked the file using `tar`, a subdirectory called `delajdenar` was created in his current directory. This subdirectory contained two more subdirectories called `bin` and `data`. There was a file called `mula` in the `bin` subdirectry which he is unable to run because he does not have the neccessarry permissions. (i) What must Peter do to be able to run the program? Assume that the program works on Peter's computer.

NAMIG: Write the exact commands. If he has too many or too few rights, you will not get full points.

(ii) How can he run the program without moving from the directory where he *initially unpacked the .tgz file*?

C) With IPv4 packets, fragmentation can occur in transfer. This can cause problems. How can Cefizelj use fragmentation to attack Peter's server? The more precise the description, the more points you will get.

2. naloga: Network management. Peter has finally set up a complete SNMP environment in his company. This enables him to effectively manage the network and all devices attached to it. But after a few days of operation, he realized that Cefizelj is able to successfully intercept all the traffic on the network.

VPRAŠANJA:

A) Peter has decided to encrypt the SNMP traffic, but he knows that he can not use SSL. (i) Why can he not use SSL? (ii) He has therefore decided to use chaining for encryption. Name all the pieces of software on his network will he have to change to implement the encryption of SNMP packets using chaining. Explain your answer.

B) Peter Zmeda is a Linux fanatic. Athough he works at a company which uses Microsoft's Active Directory, he does not want to swith operating systems on his computer. Peter's boss, however, demands that Peter allow all users from AD to log in to his computer. Is this even possible? If not – why and which pieces of software would Peter need to write to enable the users to log in? If yes – which pieces of software should Peter install?

C) We sometimes wish to find objects based on more complicated queries. We could, for example, look for all people from Maribor who are named Janez or Borut. The question is, does the query language which is used to get data from an LDAP database, support such queries? Explain your answer.

3. naloga: Time and web services.

VPRAŠANJA:

A) Security in the RTP (Real-time protocol) is defined by its secure version - SRTP. The latter introduces security through the use of a stream cipher. (i) Does this ensure the integrity of the messages? Explain your answer.

A key piece of information is the common secret. (ii) Could you use the IKE protocol to receive it? Explain your answer.

NAMIG: If you beleive that IKE can be used, explain the steps. If you beleive it can not, explain why.

B) Peter has written a program which is supposed to act as a `rdate` server. The program is written in Python and Peter uses `inetd` to run it. The program looks something like this:

```
import time
import struct
import sys
t = time.time() # time since the Epoch in seconds
# i -> signed integer, ! -> network byte order
sys.stdout.write(struct.pack("!i", int(t)))
```

Which mistakes has Peter made? What has he forgotten? Explain your answer..

C) Peter's superiors were very displeased with the sound quality during their Monday morning on-line conference. They usually start the week with the conference which is attended by department heads in Butale, Višnja Gora and Abdera. Peter has inspected the system thoroughly and has found that a lot of packets are getting lost. To avoid data loss, he has decided to use TCP instead of UDP. (i) Comment on the sensibility of his solution. Explain your comments. (ii) Would the situation change if only the heads of Butale and Abdera attended the meeting? Explain your answer.

4. naloga: Data link, network layer and network secutiry.

VPRAŠANJA:

A) When talking about security, we mention multiple components. Two of these are encryption and data integrity. Which two mathematical approaches or mechanisms are used to implement each of these? Describe them. (ii) How can you enable both encryption and data integrity on the third layer of the OSI model? Describe both mechanisms. (iii) Can VLANs on the second layer provide either of the two components? Explain your answer.

B) Peter and Konrad have set up a virtual network using OpenVPN. This is Konrad's configuration file:

```
proto tcp
dev tap
remote 193.2.167.13
secret AAAA
```

(i) What does Peter's config file look like? (ii) Who is running the OpenVPN server? Explain your answer. OpenVPN strežnik? Utemeljite odgovor. (iii) Can the line containing `secret` be different on Peter's computer? Explain your answer. (iv) Peter is afraid that such a secret is not safe. Konrad does not agree. Who is right? Explain your answer. What is the length of the secret in bits? Explain your answer.

C) Cefizelj has arrived at a company where they use the IEEE 802.1x to secure the wired network. He would like to connect to the network. Which approach can he use?

- He can connect to one of the unused ethernet ports; exploit a vulnerability on the RADIUS server to gain access.
- He should give up – IEEE 802.1x is a secure and well-written standard. This means that security holes which would work on network equipment from different vendors are not known.
- He can add an ethernet switch between an authenticated computer and the network; he can then use this switch to access the network.
- He can intercept the traffic from one of the computers on the network and perform a replay attack.

Explain your answer. Also explain why the other answers are not applicable.