Komunikacijski protokoli in omrežna varnost
2014/15
Drugi kolokvij

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

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

Duration of the test: 60 minutes.

Much success – veliko uspeha!

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

IME IN PRIIMEK: ______________________________

ŠTUDENTSKA ŠTEVILKA: ______________________________

DATUM: ______________________________

PODPIS: ______________________________

1. naloga: AAA and RADIUS.

1. This time, Peter is caught-up in some bitter-sweet affairs. He has started selling coffee and chocolate bars from vending machines. Do you think he could use the RADIUS protocol for that? Explain your answer.

   HINT: A schematic of the system would help.

2. Peter has set up a RADIUS server and created some users. He is now afraid that Cefizelj might be able to sneak onto his server and steal (read) the file /etc/freeradius/users with the passwords of all users. How can Peter prevent any possible damage in the case of such a theft? How can he make sure that the passwords are not stored on his RADIUS server in plain-text form? Describe at least 2 solutions.

3. Can we have an FTP server `abc.primer` on IP X, and at the same time an e-mail server for addresses `...@abc.primer` on IP address Y? Explain your answer.

2. naloga: Directories and LDAP.

VPRAŠANJA:

1. With the LDAP protocol, the security of transferred data can be ensured in multiple ways. One of them is to start the LDAP server on a special port which already uses SSL (ldaps). (i) What if we do not do this? How can we protect the communication? (ii) With protocols, it is often possible to systematically add new commands. Is this possible with LDAP? Explain your answer.

2. Peter has an extensive phone directory of friends. He stores this directory in a relational database (MySQL). He stores the name, surname and telephone number of each friend. He would now like to create a username and set a password for each friend so they can access his webpage. He also wants to have them use the same usernames and passwords to log into his computers. (i) Suggest two protocols he could use to log in? (ii) What would he have to set up / configure for the authentication to work with MySQL directly?

3. Name at least two important differences between LDAP v2 and LDAP v3.

3. naloga: Security elements

VPRAŠANJA:

1. Peter Zmeda has set up a VPN between his office in Zgornje Butale and the mayor's office in Spodnje Butale. He is using OpenVPN. Since the weekend was rainy, he spent most of the time at home reading through the handouts for KPOV an has learned that IPsec also exists. (i) Can he set up OpenVPN over IPsec or the other way around? Explain your answer. (ii) Does any one of these options make sense? Explain your answer.

2. Peter and Konrad have set up a VPN using OpenVPN. They are using the configurations below: Peter:

   ```
   proto tcp
   remote vpn.pavel.net
   dev tap
   secret skrivnost.key
   ```

   and Konrad:

   ```
   proto tcp
   dev tap
   secret skrivnost.key
   ```

   Now, they also want to connect Polona to their network. (i) How can they do this? Can they use the same secret with Polona?

   (ii) Draw a schematic of the network if Peter and Konrad keep their current settings and also connect Polona. (iii) Then draw a schematic of the network if in addition to Polona, 7 of her female friends also join the network. (iv) Describe everything that Polona and her friends will need on their computers in order to sign onto the network.

3. What should be the minimal password length if the passwords consist of lowercase letters of the English alphabet (26 letters) and digits 0-5 if we want to have security equal (or greater) than that provided by a 192-bit key?

4. naloga: Miscellaneous.

VPRAŠANJA:

1. The IEEE 802.1x is used between three types of devices. (i) Draw a minimal schematic containing the devices, describe what the connections between them are like and describe the role of each device.

   Peter Zmeda has received a strange client which can only use PAP for authentication in order to access the network. (ii) What and where can Cefizelj attack? Think about what kind of damage he can do. (iii) Can you suggest a way to guard against such attacks?

2. Peter uses his free time to herd sheep and loves to watch movies about sheep [1] peacefully grazing on the meadows. At the moment, he is streaming the movies from a server running VLC. VLC is streaming an endless loop of sheep-themed videos.

   Peter is a bit annoyed by the fact that when he logs onto the server, he almost never catches the start of the video. He would also like to set up Video-on-demand. (i) Which piece of software can he use to achieve this? (ii) Can he provide both services (live video streaming and video-on-demand)? (iii) Can he set both of them up on the same address? Explain your answers!

3. How does the CHAP protocol prevent replay attacks? Describe the steps it takes and how it uses them to prevent attacks.

[1] Taking into consideration the sheep from our neighboring faculty, we might get to meet our Peter Zmeda in person