

Izpit RK 21.6.2010

- 1) V podjetju, ki ima dve podružnici, podatke med njima prenaša kurir s pomočjo prenosnega diska, velikega 80 GB. Če sede na kolo, pot od ene do druge podružnice prevozi v 20 minutah. Tako na nek način opravlja funkcijo popolnoma dvosmerne komunikacijske povezave. Kakšno kapaciteto v vsako smer bi imela ekvivalentna popolnoma dvosmerna povezava?
- 2) Na katero plast po TCP/IP modelu sodijo naslednji protokoli in storitve?

a) IEEE 802.11 n	f) amplitudna modulacija
b) IRC	g) izogibanje kolizijam
c) enkapsulacija in dekapulacija	h) EIGRP, RIP in BGP
d) ICMPv6	i) https
e) izogibanje zamažitvam	j) SMTP
- 3) Katera polja najdemo tako v glavi UDP datagrama kot tudi TCP segmenta? Čemu so namenjena?
- 4) Kaj je čas obhoda ali vrnitve (RTT), v katerem protokolu je pomemben in zakaj ga potrebujemo?
- 5) Opišite mehanizem napada smurf in opišite, kaj se zgodi žrtvi napada. Kaj lahko storimo za preprečevanje takega napada?
- 6) Zakaj uporabljamo pri kriptiranju veriženje (chaining) in kaj je sploh to?
- 7) Rdeča Kapica bi rada Babici sporočila, da je njen najljubši predmet RK. Glede na to, da je Volk zadnje čase zelo aktiven pri prisluškovanju, bi rada Kapica sporočilo zašifrirala (tako da ga Volk ne bo mogel prebrati tudi, če ga prestreže). Kapica bo za šifriranje uporabila algoritem RSA. Na voljo ima naslednje podatke:
 - Babičin javni ključ: (7, 33)
 - Kapičin privatni ključ: (7, 41)
 - Kapičin javni ključ: (11, 41)

Besedilo RK pretvorite v številke tako, da vzamete kar zaporedno številko črke v slovenski abecedi, za velikost bloka pa vzemite **1 črko**.

- 8) S programom Wireshark smo zajeli paket:

```
IEEE 802.11 Data, Flags: .....F.
  Type/Subtype: Data (0x20)
  [x] Frame Control: 0x0208 (Normal)
    Duration: 149
    Destination address: Cisco-Li_59:a7:91 (00:0c:41:59:a7:91)
    BSS Id: Cisco-Li_f3:f1:c9 (00:0c:41:f3:f1:c9)
    Source address: Xircom_0e:37:b8 (00:10:a4:0e:37:b8)
    Fragment number: 0
    Sequence number: 2788
  [x] Logical-Link Control
  [x] Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.100 (192.168.1.100)
  [x] Transmission Control Protocol, Src Port: 20 (20), Dst Port: 1041 (1041), Seq: 39097, Ack: 1, Len: 1448
  [x] FTP Data
```

In paket:

```
Ethernet II, Src: VMware_a7:73:f1 (00:0c:29:a7:73:f1), Dst: Cisco_be:20:cb (00:16:47:be:20:cb)
  [x] Destination: Cisco_be:20:cb (00:16:47:be:20:cb)
  [x] Source: VMware_a7:73:f1 (00:0c:29:a7:73:f1)
    Type: IP (0x0800)
  [x] Internet Protocol, Src: 192.168.12.199 (192.168.12.199), Dst: 212.235.189.158 (212.235.189.158)
  [x] Internet Control Message Protocol
```

8.1. Kateri protokol je prisoten na povezavni plasti prvega paketa?

8.2. Kateri protokol je prisoten na povezavni plasti drugega paketa?

8.3. Kako se ta dva protokola razlikujeta med seboj? Primerjajte polja enega in drugega po pomenu, ne po vsebini!

8.4. V kakšnih omrežjih srečamo prvi protokol in v kakšnih drugega?

9) S programom Wireshark smo zajeli spodnji odgovor na poizvedbo DNS:

```
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 3650 (3650)
⊞ Domain Name System (response)
  [Request In: 289]
  [Time: 0.002414000 seconds]
  Transaction ID: 0x000a
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 3
    Additional RRs: 4
  ⊞ Queries
    ⊞ uni-lj.si: type MX, class IN
  ⊞ Answers
    ⊞ uni-lj.si: type MX, class IN, preference 20, mx kanin.arnes.si
    ⊞ uni-lj.si: type MX, class IN, preference 10, mx unis3.uni-lj.si
  ⊞ Authoritative nameservers
    ⊞ uni-lj.si: type NS, class IN, ns kanin.arnes.si
    ⊞ uni-lj.si: type NS, class IN, ns metulj.uni-lj.si
    ⊞ uni-lj.si: type NS, class IN, ns ns.uni-lj.si
  ⊞ Additional records
    ⊞ unis3.uni-lj.si: type A, class IN, addr 193.2.64.82
    ⊞ kanin.arnes.si: type A, class IN, addr 193.2.1.87
    ⊞ ns.uni-lj.si: type A, class IN, addr 193.2.64.45
    ⊞ metulj.uni-lj.si: type A, class IN, addr 193.2.64.46
```

9.1. Po katerem tipu zapisa DNS smo poizvedovali?

9.2. Kakšen je strežnikov odgovor na našo poizvedbo?

9.3. Kaj se nahaja v delu odgovora Additional records? Zakaj je to pomembno?

9.4. Ali ima kakšen od strežnikov navedenih v Additional records naveden tudi zapis za naslov IPv6?

10) Naš računalnik ima naslov IP nastavljen na 10.0.2.93, masko podomrežja pa na 255.255.255.160.

10.1. Izračunajte naslov podomrežja.

10.2. Izračunajte najmanjši naslov naprave v tem podomrežju.

10.3. Izračunajte največji naslov naprave v tem podomrežju.

10.4. Koliko naprav lahko priklopimo v to podomrežje?

10.5. Kako bi zapisali naslov našega računalnika in masko podomrežja v notaciji CIDR?