

RK VSP drugi kolokvij 1. junij 2010

- 1) V spletni brskalnik (web browser) smo vnesli naslov <http://www.google.com/>. S programom Wireshark smo zajeli spodnji promet:

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3) Gecko/20100401
Firefox/3.6.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
```

```
HTTP/1.1 302 Found
Location: http://www.google.si/
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Date: Tue, 01 Jun 2010 08:04:09 GMT
Server: gws
Content-Length: 218
X-XSS-Protection: 1; mode=block
```

```
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.si/">here</A>.
</BODY></HTML>
```

- Kaj pomeni strežnikov odgovor?
- Kakšno bo naslednja zahteva HTTP našega brskalnika in kam jo bo brskalnik poslal?
- Kateri spletni brskalnik smo uporabili za pošiljanje zahteve?
- Kaj pomeni vrstica Keep-Alive v glavi zahteve?

- 2) S programom Wireshark smo zajeli spodnji promet:

Št. Čas	Izvorni IP	Ponorni IP	Vsebina
11 3.419393	212.235.189.155	212.235.189.139	HTTP GET /videofiles/RK-Vaje11.mp4 HTTP/1.1
12 3.419751	212.235.189.139	212.235.189.155	TCP [ACK] Seq=1 Ack=433
13 3.441692	212.235.189.139	212.235.189.155	TCP [ACK] Seq=1461 Ack=433
14 3.441854	212.235.189.139	212.235.189.155	TCP [ACK] Seq=2921 Ack=433
15 3.441856	212.235.189.139	212.235.189.155	TCP [ACK] Seq=4381 Ack=433
16 3.441885	212.235.189.155	212.235.189.139	TCP [ACK] Seq=433 Ack=4381

- Katere pakete potrjuje paket številka 16? Upoštevajte, da paket številka 11 potrjuje vse pakete, ki so prispeli pred tem paketom.
- Koliko bajtov se prenese v paketu številka 13?

- 3) Naloga

Zlobni heker si je ogledal zadnje vaje in sedaj že hiti ponarejati e-pošto. Pogledal je MX zapis za domeno fri.uni-lj.si in se s programom Telnet povezal na vrata 25 na strežniku SMTP. Izvedel je ukaze, ki jih kaže spodnja seja in ugotovil, da si snovi iz vaj ni najboljše zapomnil.

```
220 ns.fri.uni-lj.si ESMTP Postfix (Debian/GNU)
EHLO fri.uni-lj.si
250-ns.fri.uni-lj.si
250-PIPELINING
250-SIZE 60000000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: <mojca.ciglaric@fri.uni-lj.si>
250 2.1.0 Ok
DATA
554 5.5.1 Error: no valid recipients
```

- a. Zakaj strežnik javi napako?
 - b. Kateri ukaz (in na katerem mestu) bi moral napadalec uporabiti, da se strežnik ne bi pritožil?
 - c. Ali sta ukaz MAIL FROM in polje From: v glavi sporočila povezana? Ali lahko to napadalec izkoristi?
- 4) V katero od plasti po ISO OSI modelu in v katero po TCP/IP modelu sodijo naslednje storitve:
 - a. usmerjanje paketov
 - b. iskanje z googlom
 - c. zanesljiv prenos podatkov od procesa do procesa
 - d. kriptiranje
 - e. vodenje evidence o seji
 - f. ugotavljanje IP naslova za www.fri.uni-lj.si
 - g. pretvorba bitov v signale
 - h. okvirjanje
 - i. rušenje virtualne zveze
 - j. prenos datoteke iz omrežja torrent
- 5) Kakšen je pomen podatka sprejemno okno (Receive window) v glavi TCP segmenta? Navedite ime mehanizma, ki ta podatek uporablja. Kakšna je korist tega mehanizma?
- 6) Zakaj je potrebna ocena RTT in zakaj je potrebna ocena odmika?
- 7) Aplikacijska plast:
 - a. Zakaj pravimo, da je http protokol brez stanj?
 - b. Ali veste za kak protokol aplikacijske plasti, ki ima stanja?
 - c. Pojasnite razlike med njima.
 - d. Navedite, kaj so na splošno prednosti protokola brez stanj in kaj s stanji
 - e. Ali lahko v http protokol uvedemo stanja in če da, kako?
- 8) Kaj je zastrupljanje DNS-ja in kako nam napadalec s tem lahko škodi? (Pojasnite tudi nekaj delovanja DNS protokola – kolikor je potrebno, da lahko razložite zastrupljanje.)
- 9) Avtentikacija:
 - a. Za kakšen namen se uporablja protokol Diffie- Hellman?
 - b. Kaj je napad z vrivanjem (man in teh middle)? Ali je protokol Diffie- Hellman ranljiv za ta napad?
 - c. Kaj pridobi napadalec, če ga uporabi v protokolu Diffie-Hellman? (Ni treba opisovati celotnega postopka izvedbe napada, če je ta seveda sploh možen)
- 10) RSA: za p in q izberemo 11 in 5, za d in e pa 13 in 37.
 - a. Ali smo izbrali za d in e števili, ki ustrezata pogojem za ključ?
 - b. Ne glede na odgovor pod točko a kriptirajte število 15.
 - c. Ne glede na odgovor pod točko a dekriptirajte število 16.