|  |
| --- |
| **Ime:**  **Priimek:**  **Vpisna št:**  **Datum:** |

**Povezavnost s protokolom TCP**

# Namen

Namen vaje je preveriti delovanje nekaterih mehanizmov protokola TCP na praktičnem primeru transportne seje. Poudarek bo na: signalizaciji za vzpostavitev in rušenje seje TCP.

# Potek vaje

V orodju Wireshark zajemite in shranite novo sled prometa, ki vsebuje komunikacijo ob nalaganju strani [http://test.ltfe.org/.](http://test.ltfe.org/) Potek zajema:

1. Orodje Wireshark mora biti pognano preden začnete s shranjevanjem;
2. V brskalniku odprite stran;
3. Ustavite zajem prometa v Wireshark; 4. Sled prometa shranite v lokalno datoteko.

Vsa nadaljnja navodila se nanašajo na tako zajeto sled prometa.

# Osnovna analiza zajetega prometa

## Filtriranje sledi prometa

V sledi prometa je poleg preučevanega prometnega toka še mnogo drugih prometnih tokov (=zajeli smo agregirani promet celotnega omrežnega vmesnika). Z analizo TCP konverzacij (***Statistics > Conversations***), poiščite in izločite preučevalno sled.

Pojasnite, s katerimi štirimi parametri je opredeljen posamezen prometni tok TCP (namig: transportni naslovi), in njihove vrednosti zapišite za ta izbrani prometni tok. Zapišite tudi Wireshark prikazni filter, ki izloči samo ta prometni tok (filtriranje samo po IP naslovih ni dovolj!).

|  |
| --- |
| Ip1,ip2,port1,port2 |

Ali je prometni tok enosmeren ali dvosmeren? Odgovor po potrebi komentirajte:

|  |
| --- |
| Prometni pretok je dvosmeren saj imamo povezavo in strežnik pričakuje odgovor |

# Seja TCP

## Vzpostavitev seje s trojnim dogovorom

V sledi prometa s ***Statistics > Flow Graph*** izrišite časovno zaporedje izmenjave sporočil in poiščite sporočila, ki tvorijo trojni dogovor (angl. Three-way Handshake). Pri iskanju si lahko pomagate tudi s prikaznimi filtri (angl. Display Filter) in tako poiščete pakete, namenjene vzpostaviti seje:

1. Narišite graf izmenjave sporočil (angl. Message Sequence Chart) za vzpostavitev te konkretne TCP seje (naslovi IP, sporočila, sekvenčne številke, zastavice). Konkretno zapišite, kakšne vrednosti sekvenčnih števil, potrditvenih števil sta komunicirajoči entiteti pri tem uporabili;

|  |
| --- |
| Naslovi IP:  Zastavice:Ack |

## Prekinitev seje

V sledi prometa z orodjem ***Statistics > Flow Graph*** izrišite časovno zaporedje izmenjave sporočil:

1. Poiščite sporočila, ki predstavljajo prekinitev seje TCP, in jih zapišite. Narišite graf izmenjave sporočil (angl. Message Sequence Chart) za rušenje te konkretne TCP seje; 2. Pojasnite, s katere strani in kakšnim tipom sporočila se je začelo rušenje seje; 3. Kaj lahko ugotovite glede števila sporočil, ki so vpletena v rušenje seje?

|  |
| --- |
|  |

# Dodatni primeri

**3.1 Iztek časovnika seje TCP**

V orodju Wireshark zajemite in shranite novo sled prometa, ki vsebuje komunikacijo ob nalaganju strani [http://test.ltfe.org/.](http://test.ltfe.org/)

Preučite, kakšne so razlike v postopku rušenja seje (npr. katera stran začne z rušenjem) v sledečih primerih:

1. Ko se stran naloži, pustite brskalnik prižgan še dlje časa.
2. Ko se stran naloži, takoj ugasnete brskalnik.

Namig: uporabite prikazne filtre, ki vam prikažejo le signalizacijske segmente TCP.

|  |
| --- |
| Dobimo reset packet |