Tavasz 2016

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS

UNIVERSITY OF SZEGED

Department of Software Engineering

2. Gyakorlat mérési jegyzőkönyv

A csoport

Bordé Sándor

Név:Törőcsik Richárd Tamás

ETR azonosító:TORXABT.SZE

Hexuni.github.io/uni

1. Feladat (1 pont)

Készíts olyan **capture filter** kifejezést, amely kiszűri a *https* portról a *www.facebook.com* szervere *felé menő* forgalmat!

Megoldás

Https-8080
dst host www.facebook.com and tcp port https

2. Feladat (3 pont)

Indíts egy mérést, melyben minden HTTP protokollhoz tartozó csomagot elfogsz. Ezután nyiss meg a böngésződben egy híroldalt (ha nem látogatsz ilyet, akkor használhatod pl. az origo.hu hírportált).

Display filter segítségével keresd meg a híroldal szervere *felé menő* csomagokat, majd másold ki ide a listából az első ilyen csomag adatait: *sorszám, idő, forrás és cél IP, protocol, hossz és info*.

A megoldáshoz írd le a használt capture- és display filtereket is!

Megoldás

Capture filter
tcp port http VAGY tcp port 80 // http-80
Display filter
ip.dst == www.origo.hu

13 0.134300 192.168.0.103 84.2.32.98 TCP 66 53675 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

3. Feladat (3 pont)

Töltsd be wiresharkba a *wikipedia.pcap* fájlt. Keresd meg a listában az első olyan HTTP GET kérést, ami külső hálózatra megy. A talált csomag headerjét másoljuk be a megoldáshoz! *(A csomag adatainak kimásolása: jobb gomb a csomagon, "Copy->Bytes->Printable text only")*

A megoldáshoz írd le még röviden, hogy találtad meg a csomagot!

Megoldás

- tcp.port == 80 and http.request.method == "GET"

  továbbá lehet még:

- Find packet icon(menu)-string get

Packet
19 5.022671 192.168.1.70 www.wikipedia.org HTTP 376 GET / HTTP/1.1

Header
?I? t/hEjJ@[P
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: hu-HU
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586
Accept-Encoding: gzip, deflate
Host: www.wikipedia.org
Connection: Keep-Alive

4. Feladat (szorgalmi) (3 pont)

Olvasd be *wiresharkba* a *vatera.pcap* fájlt. Ebben egy forgalmi mérést találsz, amit akkor rögzítettem, amikor a *vatera.hu*-n kerestem egy terméket. Derítsd ki a csomagokból, hogy mire kerestem rá? A megoldásban írd le, hogy találtad meg a keresett információt.

Megoldás

Tipp: először display filterrel szűkítsd minél jobban a csomaglistát, majd pedig a keresés funkcióval megtalálhatod a kért adatot.

-folytatás-másik oldal

Display filter

http.request.method == "GET"

Find packet icon(menu)=keresés funkció

q=

q=router jelenik meg, ami azt jelenti, hogy a kereső mezőbe a router nevezetű kulcs szó lett beírva.

Hexuni.github.io/uni