Tavasz 2016

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS

SZEGED

Department of Software Engineering

5. gyakorlat mérési jegyzőkönyv

Bordé Sándor

Név:Törőcsik Richárd Tamás

ETR azonosító:TORXABT.SZE

A csoport

1. Feladat (2 pont)

Indíts egy forgalommérést Wiresharkban ***capture*** *filter* nélkül. Válassz ki egy tetszőleges, 80-as porton kommunikáló TCP csomagot, és vizsgáld meg, a **hozzáférési** rétegbe történő beágyazódást! (Itt már használhatsz display filtert.)

- Írd le lépésenként, hogy hajtottad végre a feladatot! (Ha használtál display filtert, akkor azt is írd ide.)✔
- Milyen mezők és adatok kerültek a fejlécbe és láblécbe?✔

Megoldás

Display filter:

http and tcp.port eq 80

tcp 80 port – böngésző http forgalmát vettem alapul

TCP/IP header[1]

- Forrás/Cél
- Sequence
- Méter
- TTL
- Protocol
- Verzió

2. Feladat (2 pont)

Indíts egy mérést Wiresharkban, amely az ICMP csomagokat szűri ki (mindegy, hogy milyen szűrőt használsz)! Pingeld meg az *www.u-szeged.hu* szerverét, és válaszolj a következő kérdésekre:

- Melyik ICMP csomagtípust használja a *ping* program a kommunikáció meglétének ellenőrzésére?✔
- A távoli gép milyen csomaggal jelzi a kapcsolat meglétét?✔
- Pingelj meg a hálózaton nyilvánvalóan nem létező hálózati címet (pl. 192.168.100.100, persze, ha nincs ilyen Nálad), és írd le, hogy mi változott az eddigi pingeléshez képest!✔

A megoldásodban írd le:

- a használt szűrőkifejezést
- honnan tudtad meg az ICMP csomag típusát
- a két eset közötti különbséget részletesen, 1-2 mondatban

1http://networkstatic.net/what-are-ethernet-ip-and-tcp-headers-in-wireshark-captures/

Megoldás

Display filter icmp
Info/Packet info, ICMP header(listából▼)

- Type: 8 (Echo (ping) request)
  A 8-as típusú csomagot használja(ping), a teszteléshez.
- Type: 0 (Echo reply)
  A 8-as típusú csomagra küld választ.
- nem kapott választ, 1. hálózaton belül a router felé még kiküldte a kérést amelyet a router értelmezett is, de mivel nem talált ilyen címet ezért el is dobta a kérést[2]

192.168.0.103 192.168.100.100 ICMP 98 Echo (ping) request id=0x51ad, seq=1/256, ttl=64 (**no response found!**)

*** www.u-szeged.hu = 160.114.8.5

3. Feladat (3 pont)

Indíts egy szűrő nélküli Wireshark mérést! Törölj ki egy IP cím-MAC cím párt a géped ARP táblájából! (Ha még egy bejegyzés sem volt a táblában, akkor a következő lépésben tetszőleges, létező címet választhatsz.) Ezután (miközben fut a Wireshark) *ping*eld meg a törölt címet. Figyeld meg a közlekedő ARP csomagokat. Milyen adatokat olvashatsz ki belőle? Miben különbözik a kérő és a válasz csomag?

A megoldásodban írd le:

- hogyan és milyen paranccsal törölted az ARP táblából a címet (ha nem kellett törölni, akkor azt írd le)✔
- milyen mezők voltak az ARP csomagban, mely mezők tartalmaznak lényeges információt✔
- miben különbözik a kérő és a válasz csomag✔

2 Forrás: 05gyakorlat.pdf

Megoldás

- sudo ip -s -s neigh flush all , de nem volt szükséges a törlés
    - WIN:netsh interface ip delete arpcache
- küldő(sender) címe, MAC cím, *?ethx csatlakozása?+flag*
- hosszúságban, A küldő fél (**broadcast**) csomatot küld

4. Feladat (szorgalmi, 3 pont)

Ürítsd ki a géped ARP tábláját! Ezután pingelj meg egy külső hálózatba tartozó gépet (mondjuk a 2. feladatban adott webszervert). Belekerült-e ez a cím az ARP táblába? Ha igen, akkor mi az új bejegyzés? Ha nem, akkor miért nem? A megoldásodban írd le:

- hogyan, mely paranccsal ürítetted a géped ARP tábláját
- mely címet választottad pingelésre
- ha belekerült a cím, akkor másold ide az ARP táblád adott sorát
- ha nem került bele, akkor másold ide, hogy mi került be helyette és válaszold meg, miért ez került be?

Megoldás

- sudo ip -s -s neigh flush all
  - WIN:netsh interface ip delete arpcache
- sudo ping 160.114.8.5
- nem történik váltoás, dinamikus/statikus ARP tábla [win]

Kapcsolat: 192.168.0.103 --- 0xb Internetcím Fizikai cím Típus 192.168.0.1 c8-3a-35-4f-58-78 dinamikus

**sudo parancs a Wireshark működése miatt volt szükséges