Informatika 2 – 6. gyakorlat

Jegyzőkönyv

Hallgató: Baráth László Q6KTPF

Feladatok

1 ARP címlekérés vizsgálata

1.1 A kérés csomag Ethernet kerete milyen cél címet tartalmaz és miért?

broadcast (ff-el kezdődő)

1.2 A kérés csomag ARP keretében milyen HW és IP címeket találunk?

Saját IP és HW címet

1.3 A válasz csomag Ethernet kerete milyen cél címet tartalmaz?

A host HW címe, Mac címe a válasz csomag cél címe

1.4 A válasz csomag ARP keretében milyen HW és IP címeket találunk?

A válasz csomag ARP kerete a saját, host gép IP és HW címét tartalmazza

2 Ping vizsgálata

2.1 Melyik ICMP csomag típust használja a ping program a kommunikáció ellenőrzésére?

ICMP echo (ping) request

2.2 A távoli gép milyen csomaggal jelzi a kommunikációs kapcsolat meglétét?

ICMP echo (ping) reply

3 Név feloldás vizsgálata

3.1 Milyen protokoll csomagokat küld ki és kap a gépünk a név feloldás során?

DNS

3.2 Mi a kérés csomag cél portja és a válasz csomag forrás portja?

53 és 56536

3.3 Keresse meg a kérés csomagban a lekérdezett gép nevét és a válasz csomagban a név szerver válaszát!

Kérdés quary: www.facebook.com: type A, class IN

Az answers-nél:

www.facebook.com: type CNAME, class IN, cname star-mini.c10r.facebook.com

star-mini.c10r.facebook.com: type A, class IN, addr 31.13.84.36

4 Traceroute vizsgálata

4.1 Milyen protokoll csomagokat küld a program a távoli gépnek?

ICMP (echo ping request) csomagokat

4.2 Hogyan változik a kiküldött csomagok „Time to live” értéke?

Egyesével nő 1-től kezdve, minden értékből 3-at küld a program

4.3 Honnan és milyen protokoll üzeneteket kapunk vissza?

ICMP time-to-live exceeded csomagokat az egyre távolabbi hopoktól (célcím a saját gépünk)

4.4 Hogyan deríti ki ez a mechanizmus a kommunikációs vonalban lévő egyes csomópontok címét?

Feljegyzi, hogy ki küldte vissza a time-to-live exceeded üzeneteket, innen tudja hogy ki van pontosan ttl távolságra

5 TCP kapcsolat felépülése és lebontása

5.1 Vizsgálja meg a gépünk által a szervernek küldött első csomag, a szerver válasz csomagjának, majd a gépünk viszont válasz csomagjának TCP Flags mező értékét! Hogyan változnak a Flag értékek a kapcsolat felépülése során?

0x0002 SYN – kérés flag

0x0012 SYN ACK- válasz flag

0x0010 ACK – host küldi, hogy vette, hogy vettem

5.2 Vizsgálja meg a többi csomag (a kapcsolat lebontás csomagjainak) TCP Flags értékét! Hogyan változnak a Flag értékek a kapcsolat lebontása során?

0x0011 – FIN, ACK

0x0011 – FIN, ACK

0x0010 – ACK

handshake elköszönésnél is

6 HTTP protokoll vizsgálata

6.1 Keresse meg a kliens kérését, azon belül a címet és a protokoll verziót!

GET /nar/ HTTP/1.1

6.2 Keresse meg a szerver válaszában a státuszkódot és a szöveges leírását! Mit jelez vissza a szerver?

HTTP/1.1 401 Unauthorized

Felhasználónév + jelszó nélkül nem lhet megtekinteni az oldalt

A belépés után a kliens újraküldi a **GET /nar/ HTTP/1.1**-et, ezúttal **Authorization: Basic bGV2aTpoYTd3ZW4=** headerrel, ami base64-elve, kettősponttal elválasztva tartalmazza a felhasználónevet és jelszót (ami elég insecure). A szerver erre már elküldi az oldalt.