תרגיל 2

Application Layer & Sockets

מגישות:מורז תמיר 208397455

נינל בניוש 324699826

חלק א:

(לבחור מפה 6 ולמחוק אחת)

שאלה 3:

אפליקציה אינה שקולה לפרוטוקול משום ש:

1.אפליקציה יכולה לממש מספר פרוטוקולים כלומר אפליקציה לא נועדה לשרת מטרה מסוימת אחת, אלא משררת כמה מטרות לעומת זאת פרוטוקול נועד לשרת מטרה אחת(לדוגמא פרוטקול Http שתפקידו להעביר קבצים דרך הווב)

2.אפליקציה מתקשרת לתוכנה שאפשר להשתמש בה שנותנת פונקציונליות מסויימת ולעומת זאת פרוטוקול הוא מגדיר כללים\חוקים כמו פרוטוקול TCP שמגדיר "חוקים" לתעבורה אמינה

.3

ייתכן שפרוטוקול מסוים יהיה קשור ליותר מאפליקציה אחת כמו HTTP שכל מיני אפליקציות יכולות להשתמש בו כמו ווב, ישומיים בטלפונים וכדומה.

משום שפרוטוקול הוא דרך להשגת משהו, או בעל מטרה מסוימת ולכן כל אפליקציה יכולה להשתמש בו, הוא לא כבול רק לאפליקציה אחת.

שאלה 4:

אם נשתמש בפרוטוקול TLS\SSL נוכל לדעת שההודעה בצד השני לא תתפרש כהודעה מוצפנת גם אם הנמען והפורט לא מוצפנים

ועל ידי סיומת הs בhttp נבין זאת.

שאלה 6:

שרתי השורש שומרים את המידע המועט ביותר, משום שהם מכילים את השרתים ותפקידם רק להפנות לשרת הTLD המתאים

כלומר הכל בצורה כללית יותר וכבר נראה שבTLD יש יותר מידע מפורט כמו איזה סיומת וכדומה

ובכללי ככל שיורדים בהיררכיה יש יותר מידע

על מנת למצוא כתבנו באינטרנט כתובת IP של שרתי שורש של DNS

וקיבלנו אתר עם כל ה13 חוות שרתים עם הכתובות IP

הקישור לאתר

iana
Internet Assigned Numbers Authority

Domains Protocols Numbers About

Root Servers

The authoritative name servers that serve the DNS root zone, commonly known as the "root servers", are a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities, as follows.

List of Root Servers

a.root-servers.net 198.41.0.4, 2001:503:ba3e::2:30 Verisign, Inc.
b.root-servers.net 170.247.170.2, 2801:1b8:10::b University of Southern California, Information Sciences Institute
c.root-servers.net 192.33.4.12, 2001:500:2::c Cogent Communications
d.root-servers.net 199.7.91.13, 2001:500:2d::d University of Maryland
e.root-servers.net

שאלה 7:

```
C:\Users\Nina>nslookup www.sapir.ac.il
Server:  home.home
Address:  10.0.0.138

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    ycbsrho.impervadns.net
Address:  45.223.167.122
Aliases:  www.sapir.ac.il
```

את הכתובת אפשר למצוא על ידי פקודת הnslookup שאיתו ניתן לקבל מידע על שמות

כתובות IP

משמש לעזרה עם שאילתות על DNS

אם היינו גולשים למחלקה של מדעי המחשב סביר להניח שהיינו מקבלים

שאלה 8:

2 מקומות בהם ניתן לשמור מטמון DNS שאינם שרתים בהיררכיה הם:

השרת הלוקאלי- יכול לשמור מידע ואז כל שאילתה שנשלחת לשרת הלוקאלי, הוא יכול לחפש

אם ישלו מה לתת ואם אין הוא יעשה את העבודה כדי להשיג את מה שצריך.

שרת פרוקסי -אפשר לשמור בcache של מערכת ההפעלה שלנו עותקים של אתרים בווב

ייתכן שנשאל שאילתת DNS אחת ונקבל 2 תשובות משום שיכול להיות מצב

כי לשאלה אחת נגיד אפשר לקבל כמה כתובות IP שונות לאותו שרת

אפשר לקבל שמות שונים לIP שונים

שאלה 9:

[קישור לאתר עם הסוגי תקיפות]

תקיפת zero day attack =>

כאשר הפורץ מנצל את הפגיעה שקרתה לתוכנה מסויימת לפני שמפתחי התוכנה מצאו תיקון

לכך

וניצול זה נקרא zero day attack

CHECK POINT

Zero Day Attacks

If a hacker manages to exploit the vulnerability before software developers can find a fix, that exploit becomes known as a zero day attack.

Zero day vulnerabilities can take almost any form, because they can manifest as any type of broader software vulnerability. For example, they could take the form of missing data encryption, SQL injection, buffer overflows, missing authorizations, broken algorithms, URL redirects, bugs, or problems with password security.

This makes zero day vulnerabilities difficult to proactively find—which in some ways is good news, because it also means hackers will have a hard time finding them. But it also means it's difficult to guard against these vulnerabilities effectively.

קישור לאתר

תקיפת <= cache poisoning

כאשר התוקף מרמה את הDNS כדי לאחסן מידע שקרי במטמון כמו כתובות IP מוטעות שיובילו לאתרים זדוניים וכדומה.

TechTarget | Security

DEFINITION

cache poisoning

By Rahul Awati

What is cache poisoning?

Cache poisoning is a type of cyber attack in which attackers insert fake information into a domain name system (DNS) cache or web cache for the purpose of harming users.

In DNS cache poisoning or DNS spoofing, an attacker diverts traffic from a legitimate server to a malicious/dangerous server. The perpetrator enters false information -- such as a doctored website address -- into the DNS cache, which results in the redirection of users to a wrong, unexpected or dangerous website.

DNS cache poisoning is a highly deceptive attack that not only diverts traffic from legitimate websites, but also leaves users vulnerable to many risks, including malware infections and data theft. In web cache poisoning, an attacker exploits a web server and cache to serve a malicious Hypertext Transfer Protocol (HTTP) response to users.

קישור לאתר

קישור למתקפה אמיתית => https://www.wired.com/story/github-ddos-memcached/

Github עבר מתקפת DDoS במשך 20 דקות בשנת 2018

ולמשך כל ה20 דקות הללו האתר לא יכל לתת שירות למשתמשיו הרבים.

שאלה 11:

333 => 101001101

173 => 001111011

321 => 101000001

455 => 111000111

333+173 -> 455

```
      1 1 1 1 1 1 1
+     1 0 1 0 0 1 1 0 1
      0 0 1 1 1 1 0 1 1
      1 1
  ---------------------
      1 1 1 0 0 1 0 0 0
+     1 0 1 0 0 0 0 0 1
                      1
  ---------------------
+   1 1 0 0 0 0 1 0 0 1
                      1
      1 1 1
  ---------------------
      1 0 0 0 0 1 0 1 0
+     1 1 1 0 0 0 1 1 1
                      1
  ---------------------
    0 1 1 0 1 0 0 0 1
                      1
  ---------------------
    0 1 1 0 1 0 0 1 0   - sum
  ---------------------
    1 0 0 1 0 1 1 0 1   checksum
```

חלק ב:

שאלה 1:

<u>סעיף א:</u>

על מנת לבדוק כמה זמן יידרש להקים קישור עם האתר

נציב בנוסחה הבאה:

$$\frac{\text{מס חבילות} * \text{גודל חבילה}}{\text{מהירות ההגעה}}$$

9mb=9000kb

T0(America) = $\frac{3*10kb}{9000kb} = \frac{1}{300}sec$

3mb=3000kb

T0(Israel) = $\frac{3*10kb}{3000kb} = 0.01sec$

<u>סעיף ב:</u>

דף HTML מגודל 500kb

כל תמונה באתר (1mb(1000kb

אצל לקוח אמריקאי =>

שליחת חבילה 10kb, חבילה מהשרת 500kb או 1mb, שליחה לאישור 10kb

הזמן עבור הדף html עצמו -- > $\frac{(10kb+500kb+10kb)}{9000kb} = \frac{13}{225}$

הזמן עבור תמונות -- > $\frac{(10kb+100kb+10kb)}{9000kb} = \frac{1}{75} * 5 = \frac{1}{15}$

כפלנו בחמש כי יש לנו סה"כ 5 תמונות

אז נחבר את שני הזמנים

וסך הזמן שייקח הוא T(America) = $\frac{28}{225}$

אצל לקוח ישראלי =>

ההבדל מלקוח ישראלי ללקוח אמריקאי במהירות הגעת הקובץ הוא פי 3

לכן פשוט אפשר לכפול ב3 מה שקיבלנו אצל הלקוח האמריקאי

ונקבל את סך הזמן שזה יקח אצל הלקוח הישראלי

$$\frac{1}{75} * 3 = \frac{1}{25} * 5 = \frac{1}{5}$$

$$\frac{13}{225} * 3 = \frac{13}{75}$$

סך הזמן שייקח ללקוח הישראלי => $\frac{28}{75}$

<u>סעיף ג:</u>

אם מקבלים במקביל אין צורך לכפול בכל 5 התמונות שיש לנו

כי זה אומר שבפנייה אחת נקבל ישר את כל החמש

אצל הלקוח האמריקאי =>

$$\frac{1}{75} + \frac{13}{225} = \frac{16}{225}$$

אצל הלקוח הישראלי =>

$$\frac{1}{25} + \frac{13}{75} = \frac{16}{75}$$

<u>סעיף ד:</u>

קישורים לא רציפים ולא מקבילים:

נצטרך לכפול במספר האובייקטים ופלוס 1 שזה הדף עצמו

כי נצטרך בשביל כל אחד בנפרד ליצור קישור

לכן נכפול ב6 את הזמן של יצירת קישור

אצל הלקוח האמריקאי =>

$$\frac{1}{300} * 6 + \frac{28}{225} = \frac{13}{90}$$

אצל הלקוח הישראלי =>

$$\frac{1}{100} * 6 + \frac{28}{75} = \frac{13}{30}$$

<u>סעיף ה:</u>

קישורים לא רציפים ומקבילים:

נכפול ב2 את זמן יצירת הקישור משום שפעם אחת נבקש עבור הדף html עצמו והקישור הזה

יהיה עבור התמונות שיבואו במקביל לכן 2 קישורים

עבור הלקוח האמריקאי =>

$$\frac{1}{300} * 2 + \frac{28}{225} = \frac{59}{450}$$

אצל הלקוח הישראלי =>

$$\frac{1}{100} * 2 + \frac{28}{75} = \frac{59}{150}$$

<u>סעיף ו:</u>

עבור לקוח ישראלי =>

כאשר הקישורים רציפים ללא הקבלה כלשהי יידרשו 7RTT אחד ליצירת הקישור

אחד להבאת הקובץ ואז כל קישור נוסף עבור כל אובייקט וישלנו 5 אובייקטים של תמונות

כאשר מדובר במיקבול של עד 2 בקשות וקישורים לא רציפים יהיה 4RTT

שאלה 2:

<u>סעיף א:</u>

נחשב את מקדם העומס בLAN:

$$\frac{12mb * 2}{120mbps} = 0.2$$

נחשב את מקדם העומס ברשת הגישה

$$\frac{12mb * 2}{24mbps} = 1$$

<u>סעיף ב:</u>

T(total) = t(lan-queue) + t(queue) +t(access) +t(internet)

T(total) = $\frac{12}{120} + 2500 * 0.2^8 + \frac{12}{24} + 2.4 = 3.0064$

סעיף ג:

נוספו 3 חבילות אז עכשו ישלנו סך הכל של 5 חבילות אז נחשב מחדש את מקדמי העומס

מקדם העומס בLAN =>

$$\frac{12mb * 5}{120mbps} = 0.5$$

מקדם העומס ברשת הגישה =>

$$\frac{12mb * 5}{24mbps} = 2.5$$

נראה שהעומס גדל

בעיכוב הכולל נצטרך רק לשנות את העיכוב לפי הנוסחה ושאר הערכים נשארים אותו דבר

כי מקדם העומס שלנו כרגע אחר

Total = $\frac{12}{120} + 2500 * 0.5^8 + \frac{12}{24} + 2.4 = 12.765625$

השינוי תלוי בעומס המקדמים, כלומר אם המקדמים שלנו גדולים ככה גם הזמן הכולל יגדל

סעיף ד:

נבדוק לפי בוב:

נקח מסעיף ב ונשנה במקום ה24 ל240 כי הפתרון שלו הוא שדרוג הקו לספק

$$\frac{12}{240} = 0.05$$

עכשו נציב ונחשב את הזמן הכולל (בגלל שחישבנו בסעיף ב פשוט נשנה את מה שהיה קודם למה שיש עכשו)

ונקבל:

Total = $\frac{4}{625} + 0.1 + 0.05 + 2.5 = 2.6564$

נראה שינוי מאוד מזערי של 0.35 שזה כבר לא כלכך משמעותי השינוי הזה

נבדוק לפי הצעת הפתרון של אליס:

0.5 * 3.0064 +0.5 * $\frac{12}{120} = 1.5532$

פה נראה שינוי של כמעט 50 אחוז שיפור

לכן הפתרון של אליס יותר טוב

הפחתה משמעותית בזמן

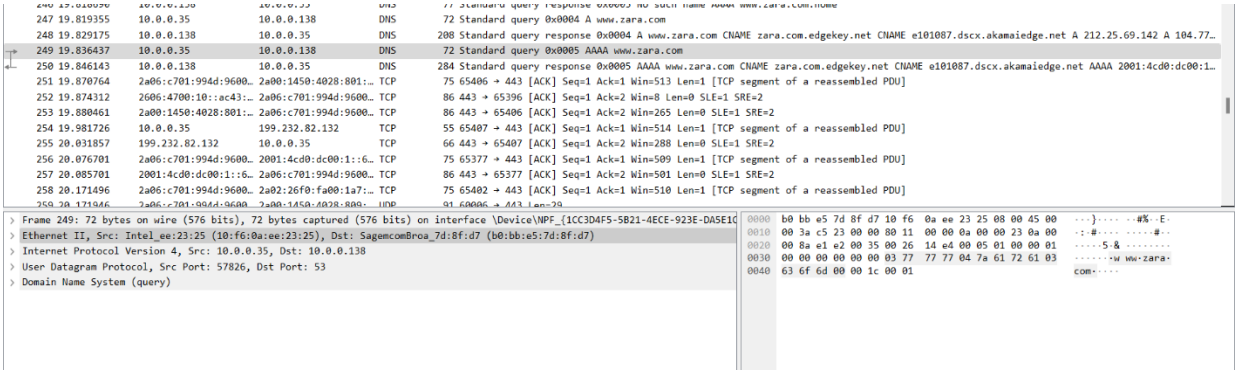
שאלה 3:

<u>סעיף א:</u>

הרצנו לאתר זארה וקיבלנו:

```
C:\Users\Nina>nslookup www.zara.com
Server:  home.home
Address:  10.0.0.138

Non-authoritative answer:
Name:    e101087.dscx.akamaiedge.net
Addresses:  2001:4cd0:dc00:1::d419:45a6
          2001:4cd0:dc00:1::d419:458e
          2001:4cd0:dc00:1::684d:ca69
          2001:4cd0:dc00:1::684d:ca59
          2001:4cd0:dc00:1::684d:ca61
          212.25.69.142
          104.77.202.98
          104.77.202.105
          212.25.69.160
Aliases:  www.zara.com
          zara.com.edgekey.net
```



Query:

```
> Frame 249: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\
> Ethernet II, Src: Intel_ee:23:25 (10:f6:0a:ee:23:25), Dst: SagemcomBroa_7d:8f:d7 (b0:bb:e5
> Internet Protocol Version 4, Src: 10.0.0.35, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 57826, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0005
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.zara.com: type AAAA, class IN
    [Response In: 250]
```

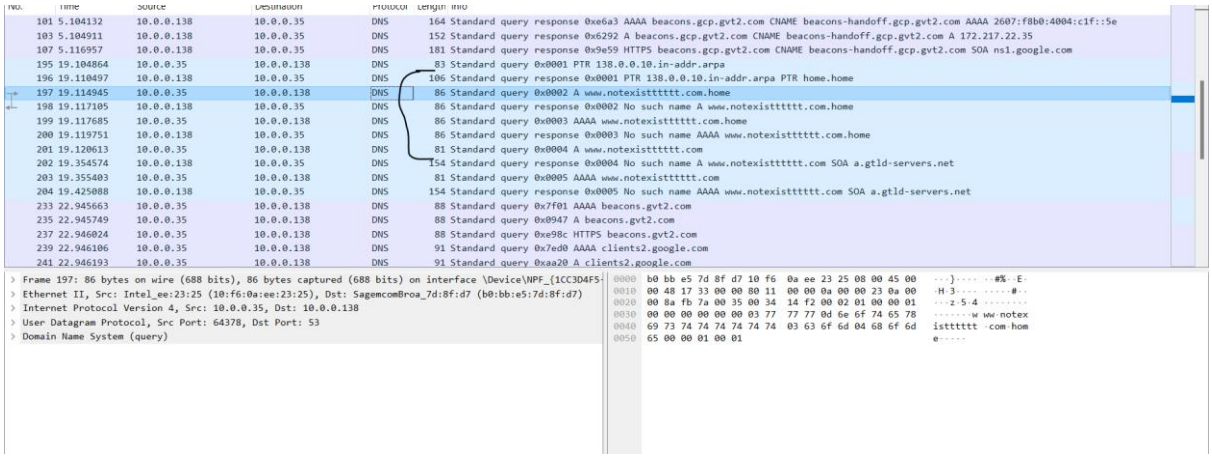
```
0000  b0 bb e5 7d 8f d7 10 f6  0a ee 23 25 08 00 45 00   ···}···· ··#%··E·
0010  00 3a c5 23 00 00 80 11  00 00 0a 00 00 23 0a 00   ·:·#···· ·····#··
0020  00 8a e1 e2 00 35 00 26  14 e4 00 05 01 00 00 01   ·····5·& ··ooooooo
0030  00 00 00 00 00 00 03 77  77 77 04 7a 61 72 61 03   ·******w ww·zara·
0040  63 6f 6d 00 00 1c 00 01                            com·····
```

Response:

```
Questions: 1
Answer RRs: 7
Authority RRs: 0
Additional RRs: 0
> Queries
v Answers
  > www.zara.com: type CNAME, class IN, cname zara.com.edgekey.net
  > zara.com.edgekey.net: type CNAME, class IN, cname e101087.dscx.akamaiedge.net
  > e101087.dscx.akamaiedge.net: type AAAA, class IN, addr 2001:4cd0:dc00:1::d419:45a6
  > e101087.dscx.akamaiedge.net: type AAAA, class IN, addr 2001:4cd0:dc00:1::d419:458e
  > e101087.dscx.akamaiedge.net: type AAAA, class IN, addr 2001:4cd0:dc00:1::684d:ca69
  > e101087.dscx.akamaiedge.net: type AAAA, class IN, addr 2001:4cd0:dc00:1::684d:ca59
  > e101087.dscx.akamaiedge.net: type AAAA, class IN, addr 2001:4cd0:dc00:1::684d:ca61
[Request In: 249]
[Time: 0.009706000 seconds]
```

```
0000  10 f6 0a ee 23 25 b0 bb  e5 7d 8f d7 08 00 45 00   ····#%·· ·}····E·
0010  01 0e aa 8c 40 00 40 11  7a a6 0a 00 00 8a 0a 00   ····@·@· z·******
0020  00 23 00 35 e1 e2 00 fa  43 c9 00 05 81 80 00 01   ·#·5···· C·******
0030  00 07 00 00 00 00 03 77  77 77 04 7a 61 72 61 03   *******w ww·zara·
0040  63 6f 6d 00 00 1c 00 01  c0 0c 00 05 00 01 00 00   com····· ********
0050  00 ea 00 16 04 7a 61 72  61 03 63 6f 6d 07 65 64   *****zar a·com·ed
0060  67 65 6b 65 79 03 6e 65  74 00 c0 2a 00 05 00 01   gekey·ne t··*····
0070  00 00 45 ec 00 1a 07 65  31 30 31 30 38 37 04 64   ··E····e 101087·d
0080  73 63 78 0a 61 6b 61 6d  61 69 65 64 67 65 c0 3b   scx·akam aiedge·;
0090  c0 4c 00 1c 00 01 00 00  00 06 00 10 20 01 4c d0   ·L****** ···· ·L·
00a0  dc 00 00 01 00 00 00 00  d4 19 45 a6 c0 4c 00 1c   ******** ··E··L··
00b0  00 01 00 00 00 06 00 10  20 01 4c d0 dc 00 00 01   ********  ·L*****
00c0  00 00 00 00 d4 19 45 8e  c0 4c 00 1c 00 01 00 00   ******E· ·L******
00d0  00 06 00 10 20 01 4c d0  dc 00 00 01 00 00 00 00   ···· ·L· ********
00e0  68 4d ca 69 c0 4c 00 1c  00 01 00 00 00 06 00 10   hM·i·L·· ********
00f0  20 01 4c d0 dc 00 00 01  00 00 00 00 68 4d ca 59    ·L***** ····hM·Y
0100  c0 4c 00 1c 00 01 00 00  00 06 00 10 20 01 4c d0   ·L****** ···· ·L·
0110  dc 00 00 01 00 00 00 00  68 4d ca 61               ******** hM·a
```

ונראה דוגמא עבור אתר שלא באמת קיים:



סעיף ב:

המשמעות של שדות A וAAAA בתשובה היא לתת את כתובת הIP

A נותן את שם הhost

וAAAA נותן מיפוי לdomain name והוא יותר ארוך מבחינת מספר הביטים

עכשו זה נובע מIPv4 או IPv6 (גרסה) ולכן משתמשים בשני האופציות כי אין לדעת באיזה גרסה יש אצל המשתמש

לכן כדי שהכל יעבוד ישר נותנים את שתי האפשריות הללו.

סעיף ג:

כדי לדעת האם קיבלנו את הIP המבוקש

סעיף ד:

כן קיימות הקלטות נוספות של DNS שלא קשורות לבקשה שלנו משום שקיימים עוד שירותי DNS ברשת, גם אם זה לא קשור לשאלה שלי

279	26.503247	10.0.0.35	10.0.0.138	DNS	103	Standard query 0xb247 A signaler-pa.clients6.google.com
280	26.503305	10.0.0.35	10.0.0.138	TCP	56	65433 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP segment of a reassembled PDU]
281	26.503330	10.0.0.35	10.0.0.138	DNS	103	Standard query 0x2f95 HTTPS signaler-pa.clients6.google.com
282	26.504799	10.0.0.138	10.0.0.35	TCP	54	53 → 65431 [ACK] Seq=1 Ack=3 Win=29312 Len=0
283	26.505178	10.0.0.138	10.0.0.35	TCP	54	53 → 65431 [ACK] Seq=1 Ack=52 Win=29312 Len=0
284	26.505178	10.0.0.138	10.0.0.35	TCP	54	53 → 65432 [ACK] Seq=1 Ack=3 Win=29312 Len=0
285	26.505739	10.0.0.138	10.0.0.35	TCP	54	53 → 65432 [ACK] Seq=1 Ack=52 Win=29312 Len=0
286	26.505739	10.0.0.138	10.0.0.35	TCP	54	53 → 65433 [ACK] Seq=1 Ack=3 Win=29312 Len=0
287	26.505739	10.0.0.138	10.0.0.35	TCP	54	53 → 65433 [ACK] Seq=1 Ack=52 Win=29312 Len=0

שאלה 5:

סעיף א:

אצל אליס:

בקישור UDP סוקט מזוהה על ידי פורט מקור וIP יעד

Source port = 2200 and ip destination=40.50.60.70

בקישור TCP צריך את כל הרביעיה

Source port = 220, source ip=1.11.2.22

Destination port= 101 and destination ip 40.50.60.70

אצל בוב:

בקישור UDP

Source port=3300 and ip destination=40.50.60.70

בקישור TCP

Source port =330 and source ip=2.33.4.55

Destination port=101 and destination ip= 40.50.60.70

אצל ססיל:

בקישור UDP:

Source port= 4400 and destination ip=49.50.60.70

בקישור TCP:

Source port=440 and source ip=3.44.5.66

Destination port=101 and destination ip=40.50.60.70

אצל אמיר:

בקישור UDP

Source port =1010 and destination ip=the ip of alice\bob\cecil

בקישור TCP:

Source port=1010 source ip=40.50.60.70

Destination port=the destination port of alice\bob\cecil and destination ip its also the ip of alice\bob\cecil

<u>סעיף ב:</u>

יתווספו סוקטים חדשים של UDP בשביל ליצור קשר עם ida

אצל אליס => source port 2200 and destination ip=140.150.160.170

אצל בוב => 3300, 140.140.160.170

אצל ססיל => 4400, 140.140.160.170

אצל אמיר => Source port =1010 and destination ip=the ip of alice\bob\cecil

אצל אידה => source port =5050, and destination ip=the ip of alice\bob\cecil

<u>סעיף ג:</u>

נוסיף את הסוקטים החדשים

אצל אליס => (220,1.11.2.22 505, 140.140.160.170)

אצל בוב => (330,2.33.4.55 505, 140.140.160.170)

אצל ססיל => (440,3.44.5.66 505, 140.140.160.170)

אצל אמיר => (101, 40.50.60.70 port of alice/bob/cecil, ip of alice\bob\cecil)

אצל אידה => (505, 140.140.160.170 port of alice/bob/cecil, ip of alice\bob\cecil)

<u>סעיף ד:</u>

יהיו שני סוקטים של UDP

והרי בTCP יוצרים סוקט ספציפי ללקוח מה שאומר שאצל אמיר יהיו 39 סוקטים של וגם לאידה 39

רק סוקטים של TCP יהיו כ78 סוקטים

ונוסיף את השני סוקטים של UDP שיש אחד לאמיר ואחד לאידה

סהכ 80 סוקטים