تمرین شماره شش + حل و بررسی

درس شبکه های کامپیوتری - فصل دوم

مدرس: دکتر هاشمی

***

۱- RFC 5321 را مطالعه کرده و بگویید که MTA کوتاه شده ی چیست؟ سپس ایمیل اسپم دریافت شده ی زیر را در نظر گرفته و کاربری را که این اسپم را ارسال کرده شناسایی کنید. (با این فرض که همه ی کاربران به جز ارسال کننده ی اسپم راستگو هستند.)

```
From - Fri Nov 07 13:41:30 2008
Return-Path: <tennis5@pp33head.com>
Received: from barmail.cs.umass.edu
(barmail.cs.umass.edu [128.119.240.3]) by cs.umass.edu
(8.13.1/8.12.6) for <hg@cs.umass.edu>; Fri, 7 Nov 2008
13:27:10 -0500


Received: from asusus-4b96 (localhost [127.0.0.1]) by
barmail.cs.umass.edu (Spam Firewall) for
<hg@cs.umass.edu>; Fri,  7 Nov 2008 13:27:07 -0500
(EST)
Received: from asusus-4b96 ([58.88.21.177]) by
barmail.cs.umass.edu for <hg@cs.umass.edu>; Fri,
07 Nov 2008 13:27:07 -0500 (EST)
Received: from [58.88.21.177] by
inbnd55.exchangeddd.com; Sat, 8 Nov 2008 01:27:07 +0700
From: "Jonny" <tennis5@pp33head.com>
To: <hg@cs.umass.edu>
Subject: How to secure your savings
```

MTA = Mail Transfer Agent

فرستنده ایمیل اش را به MTA داده و این ایمیل توسط چند MTA دست به دست می شود تا به گیرنده برسد.

یک MTA راستگو باید بگوید که ایمیل را از چه کسی گرفته است، اما اگر دقت کنید کاربر asusus-4b96 به نشانی اینترنتی 58.88.21.177 از آن چه که MTA قبلی اعلام کرده استفاده کرده است. پس این کاربر ارسال کننده ی اسپم است.[1]

۲- فرض کنید که از طریق پروتکل POP3 به ایمیل خود وصل شده اید.

الف. اگر POP mail client شما در مد download-and-delete پیکربندی شده باشد، مذاکره ی زیر را کامل کنید.

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: blah blah ...
S: .........blah
S: .
```

C: dele 1

C: retr 2

S: (blah blah …. Blah)

S: .

C: dele 2

C: quit

S: +OK POP3 server signing off

[1] درباره این پاسخ مطمئن نیستم. برای بررسی بیش تر به لینک زیر مراجعه کنید.
http://www.rahul.net/falk/mailtrack.html

ب. حال فرض کنید که در مد download-and-keep کار می کنید. مذاکره بالا را با فرض جدید کامل کنید.

C: retr 2

S: (blah blah …. Blah)

S: .

C: quit

S: +OK POP3 server signing off

پ. با این فرض که مد کاری ما download-and-keep باشد (از آن چه که در بند ب نوشته اید استفاده کنید.)، اگر پیغام های ۱ و ۲ را بازیابی کنیم، سپس از POP خارج شویم، و چند دقیقه بعد دوباره وارد POP شویم تا ایمیل های جدید را بازیابی نماییم، متن نشست (session transcript) دوم را بنویسید. (در این فاصله پیغام جدیدی به ما ارسال نشده است.)

C: list

S: 1 498

S: 2 912

S: .

C: retr 1

S: (blah blah …. Blah)

S: .

C: retr 2

S: (blah blah …. Blah)

S: .

C: quit

S: +OK POP3 server signing off

۳- الف. پایگاه داده ی whois چیست؟

پایگاه داده ای ست شامل مشخصات صاحبان دامنه های اینترنتی (نام، آدرس ایمیل، شماره تلفن و ...) و اطلاعات مربوط به آن IP مثلاً DNS آن

ب. از پایگاه های داده ی whois بر روی اینترنت استفاده کنید و نام دو سرور DNS را به دست آورید. مشخص کنید که از کدام پایگاه های whois استفاده کرده اید.

ns1.google.com (DNS Server of Google)

ns.iut.ac.ir (DNS Server of IUT)

هر دو از پایگاه who.is برداشته شده اند.

نکته ی جالب آن است که اکثر دانشجویان به یک پایگاه whois مراجعه کرده و دو DNS یکسان را نیز به دست آورده اند. (:

پ. از nslookup استفاده کرده و در خواست های DNS را به سرور محلی تان و دو سروری که در بند ب به دست آورده اید، بفرستید. در خواست های خود را برای نوع A، MX و NS فرستاده و نتایج را خلاصه وار بنویسید.

یادآوری: نوع A: IPv4 نوع MX: Mail Exchange و نوع NS: Name server

سرور محلی (ns.iut.ac.ir):

A: 176.101.52.130

```
MX:
 iut.ac.ir      mail exchanger = 20 ijpr.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 ivut.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 jcme.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 testa.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 ejgcst.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 jstnar.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 central-fax.iut.ac.ir.
 iut.ac.ir      mail exchanger = 10 mta.iut.ac.ir.
 iut.ac.ir      mail exchanger = 10 mail1.iut.ac.ir.
```

```
 iut.ac.ir      mail exchanger = 10 mail2.iut.ac.ir.
 iut.ac.ir      mail exchanger = 20 www.iut.ac.ir.
```

NS:

```
iut.ac.ir       nameserver = ns.iut.ac.ir.
iut.ac.ir       nameserver = ns2.iut.ac.ir.
```

ت. با استفاده از nslookup بررسی کنید که آیا وب سایت دانشگاه صنعتی اصفهان چندین IP address دارد؟

خیر، یک آدرس دارد: 176.101.52.130

ث. توضیح دهید که یک مهاجم چگونه می تواند از پایگاه های whois و نیز ابزار nslookup بهره ببرد تا اطلاعاتی درباره ی سازمان مورد حمله اش به دست آورد؟

می تواند اطلاعاتی در خصوص نحوه ی تماس با مدیران سایت، DNS آن سایت و سایر اطلاعاتی که می تواند برای حمله مفید باشد را به دست آورد.

ج. توضیح دهید که چرا پایگاه های داده ی whois باید در دسترس همگان باشد؟

تا در صورت وقع حمله بتوان حمله کننده را شناسایی و ردیابی کرد.

***

۴- فرض کنید که دانشگاه شما یک DNS server محلی داشته باشد. شما یک کاربر عادی هستید (مسوول شبکه یا نظیر آن نیستید.) آیا برای شما ممکن است که بفهمید یک وب سایت مربوط به خارج از دانشگاه در چند ثانیه ی گذشته توسط یکی از کاربران داخل دانشگاه بازدید شده است؟

بله، هر DNS ای آدرس صفحاتی را که کاربران به آن ها دسترسی داشته اند برای مدتی در خود ذخیره می کند. حال با استفاده از دستور dig که ارتباطات بین DNS ها برای یافتن یک آدرس را ردیابی می کند، می

توان این موضوع را بررسی کرد؛ به این صورت که اگر دستور در زمان خیلی کوتاهی به نتیجه رسید معلوم است که اخیراً یک تقاضا برای آن صفحه وجود داشته است.

***

۵- آیا می توانید مرورگر کامپیوتر خود را به گونه ای تنظیم کنید تا چندین ارتباط موازی با یک وب سایت ایجاد نماید؟ مزایا و معایب داشتن تعداد زیادی ارتباط TCP همزمان چیست؟

بله. مزایا: در صورت گم شدن بسته ها درخواست مجدد برای همان شیء داده می شود و نیازی نیست که کل محتوا دوباره فرستاده شود. – عیب: ارتباط های زیادِ TCP سربار زیادی را ایجاد می کند.

***

۶- برنامه های TCPClient، UDPClient، TCPServer و UDPServer را که به زبان پایتون نوشته شده اند در نظر بگیرید. (پیوست یک) دو برنامه ی اول (Client) بر روی یک کامپیوتر و دو برنامه ی بعدی (Server) بر روی یک کامپیوتر دیگر اجرا می شود.

الف. اگر برنامه ی TCPClient قبل از برنامه ی TCPServer اجرا شود، چه اتفاقی رخ می دهد و چرا؟

موجب خطا می گردد، چون client درخواستش را به سرور می فرستد، اما سروری وجود ندارد که پاسخ دهد.

ب. اگر برنامه ی UDPClient قبل از برنامه ی UDPServer اجرا شود، چه اتفاقی رخ می دهد و چرا؟

مشکلی پیش نمی آید، چرا که در UDP ایجاد ارتباط (handshaking) نداریم.

پ. اگر شماره پورت های متفاوتی را بر روی طرف کلاینت و سرور اجرا کنیم، چه رخ می دهد؟

موجب خطا می شود، چون در این حالت کلاینت سعی می کند با یک پروسه ی نادرست ارتباط برقرار کند.

ت. فرض کنید که در برنامه ی UDPClient بعد از ایجاد سوکت، خط زیر را اضافه کنیم. آیا نیاز هست که برنامه ی سمت سرور را تغییر دهیم؟ شماره پورت برای سوکت های UDPClient و UDPServer چند است؟

```
clientSocket.bind(('', 5432))
```

در برنامه اصلی (پیوست یک) سیستم عامل شماره پورت مناسب را پیدا می کند. اما با اضافه کردن این خط ما خودمان یک شماره پورت برای این کار در نظر می گیریم. (=۵۴۳۲)

پیوست یک

UDPClient.py

Here is the code for the client side of the application:

```
from socket import *
serverName = 'hostname'
serverPort = 12000
clientSocket = socket(socket.AF_INET, socket.SOCK_DGRAM)
message = raw_input('Input lowercase sentence:')
clientSocket.sendto(message,(serverName, serverPort))
modifiedMessage, serverAddress = clientSocket.recvfrom(2048)
print modifiedMessage
clientSocket.close()
```

UDPServer.py

Let's now take a look at the server side of the application:

```
from socket import *
serverPort = 12000
serverSocket = socket(AF_INET, SOCK_DGRAM)
serverSocket.bind(('', serverPort))
print "The server is ready to receive"
while 1:
        message, clientAddress = serverSocket.recvfrom(2048)
        modifiedMessage = message.upper()
        serverSocket.sendto(modifiedMessage, clientAddress)
```

TCPClient.py

Here is the code for the client side of the application:

```
from socket import *
serverName = 'servername'
serverPort = 12000
clientSocket = socket(AF_INET, SOCK_STREAM)
clientSocket.connect((serverName,serverPort))
sentence = raw_input('Input lowercase sentence:')
clientSocket.send(sentence)
modifiedSentence = clientSocket.recv(1024)
print 'From Server:', modifiedSentence
clientSocket.close()
```

برنامه سرور

```
from socket import *
serverPort = 12000
serverSocket = socket(AF_INET,SOCK_STREAM)
serverSocket.bind(('',serverPort))
serverSocket.listen(1)
print 'The server is ready to receive'
while 1:
   connectionSocket, addr = serverSocket.accept()
   sentence = connectionSocket.recv(1024)
   capitalizedSentence = sentence.upper()
   connectionSocket.send(capitalizedSentence)
   connectionSocket.close()
```

عکس های فوق از کتاب کروز برداشته شده اند.