

## บทที่ 5

### การทดสอบโปรแกรม

การทดสอบโปรแกรมเป็นการทดสอบผลการทำงานของโปรแกรมภายใต้สภาพแวดล้อมของระบบปฏิบัติการลินุกซ์ โดยมีจุดประสงค์ของการทดสอบ ดังนี้

1. ผลของการเข้ารหัส
2. ผลการพิสูจน์ตัวตนจริง
3. การทำงานของระบบและประสิทธิภาพของระบบ

#### 5.1 อุปกรณ์ที่ใช้ในการทดสอบ

5.1.1 เครื่องออกใบรับรอง ทำหน้าที่ออกใบรับรองทั้งของผู้ให้บริการและผู้ออกใบรับรอง ประกอบด้วย

เครื่องพีซีคอมพิวเตอร์

หน่วยประมวลผล	80486	หรือ ดีกว่า
หน่วยความจำหลัก	16	เมกะไบต์
ฮาร์ดดิสก์ (hard disk)	1.2	จิกะไบต์
ฟลอปปีดิสก์ (floppy disk)	3.5	นิ้ว 1.44 เมกะไบต์
แผงวงจรเชื่อมต่อเครือข่าย (NIC)	NE2000	Compatible
ระบบปฏิบัติการ ลินุกซ์	Redhat	Version 5.2.5

5.1.2 เครื่องให้บริการรหัสผ่าน ทำหน้าที่ให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวแก่เครื่องแม่ข่ายยูนิกซ์ ประกอบด้วย

เครื่องพีซีคอมพิวเตอร์

หน่วยประมวลผล	80486	หรือ ดีกว่า
หน่วยความจำหลัก	16	เมกะไบต์
ฮาร์ดดิสก์ (hard disk)	1.2	จิกะไบต์
ฟลอปปีดิสก์ (floppy disk)	3.5	นิ้ว 1.44 เมกะไบต์



ZXBhcnRtZW50MREwDwYDVQQDEwhDQXNlcnZlcjCBnzANBgkqhkiG9w0BAQEFAAOB  
 jQAwgYkCgYEA1GSjGce5lUEWbEjTyglP1d4G1Ji6z0115lCIWtEFuTeVFmT1ctTU  
 PzadFhV9n68/dAAI8zlxK+IQ6DB7UYZNYvYK01LXVm6yVWfo8NTT9/SqbFFv/NzP  
 0vX7cBAcncwBsqJiIOfZ3V03cSxAg98WDgxbOepsZY+L8VI3ldTsnVsCAwEAATAN  
 BgkqhkiG9w0BAQQFAAOBgQBzd9FG4FTTK8q5ZKBlblZX977WSdTNHFPd4SRsJ+3C  
 dpzt6EELmmtzWmbYDrhjrprVW/UdvnMYIQ0ThRX9xnW7SKaxk3Lbmb5zf7Zqm1rA  
 qXKEg5bQyeW6urvZ42HuUov/MmqjH7DQ5t5ucqKC+v2UuY4h6idYW4AwFnGMmvwa  
 mA==  
 -----END CERTIFICATE-----

### รูปที่ 5.1 ใบรับรองของผู้ออกใบรับรอง

-----BEGIN RSA PRIVATE KEY-----  
 Proc-Type: 4,ENCRYPTED  
 DEK-Info: DES-EDE3-CBC,28FF6FED557B0F74  
  
 pl2GJQAe0GCeUfRMb3FQLvGnnlIttRxE0mRqlDCi5t72LuqOBvtFKugaaM8B0eP  
 fLTKs0gWF6lmmqzxWmaS7LdBaol3w3D0WfzMIp8LuL6BjEu9nzmU662ueUCj2AA  
 7ne/bsJDb0CcgBHfQBBqKoiPkiwUMwV598uqDE9rv0Z85MS/4rt88Mwba+ORAG0  
 NlhvbbBRThpZobGsyBawnX1UfhAynlDuYv7vy/gI5iq6pb0qllOvZLwCPmc0eXYA  
 DvAgcvYPnlE1m7iptSiYIzq1f+yh1+FWN3Ju8j5U4krpGO9z2JKoa53lutsWzFHQ  
 C4woGLbOjflP6bA/bw8K8HJocVsFjQOFeyvud7ukfkEMeeYoB2AojycxzEvPK/PH  
 ewwGFNijKXNgt2iv/K579EXzA30s/BemuBdThezkrPIFBR48ufY1QNojl02Krebz  
 WP29NauqZBSP5xKwKdZWlgG6K+hGYn3S8YUfKzAfSsyXwdKZfdGwLXvQTTyeKrxO  
 h5QJnlu3YcAAHj2J15sRWcXQUfv/DXUzTYZsp7j0z+Y10VnYT0QYCpa+L2d7BGdZ  
 O243eETew1JDKI1ykBX6XZktdHi7YzqhtRfbuqs58caA6P9/7CVTAghxHQzmxlbb  
 ISJ88py6oL+4OGRbTctFbDwtjVAxBWXwFooHv/07ZMcS8+T91Fx+BZxiZaJl61Az  
 bxzp6kR+Xsptp+O+JjoUAjXZxK9NC3pciu4cC/57j8jAvJ6Y13MzO72QH2lks/Jw  
 iXGEVifSxzXeUFmNZdQfBBSmM+U5yFUs50S1HUG1ncOwmaK5sJxPSw==  
 -----END RSA PRIVATE KEY-----

### รูปที่ 5.2 คีย์ส่วนตัวของผู้ออกใบรับรอง

5.2.2 ติดตั้งโปรแกรมที่ใช้สร้างชุดคีย์สาธารณะ ลงบนเครื่องผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว แล้วสร้างชุดคีย์สาธารณะขึ้นที่เครื่องผู้ให้บริการ และเก็บคีย์ส่วนตัวที่ถูกเข้ารหัสด้วยวิธีคือเอส (DES : Data Encryption Standard) ดังแสดงในรูปที่ 5.3 ไว้เป็นความลับ

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,59CB02A9F1606AAA

0FsFuJRhfit+GPM1gnrzeqA2mpTwaxzCwdGxibra9wHg8O33skB0Lxvi9Lc+RE3r  
 bb3edzG1zhCmXeAS5ZfJytTRyCp5QGV7SLM2GOgx+4KSoev84hdESOs3Z/hv9NaK  
 BDiii0YkZohgKgqb7dh+NrXO4xJP7ZKMtS6N6FM8nmXvzYri46HmgFEO8kbCSiLj  
 hBDhJVfxnCcMT/SIC/xodH3MZ0rqEblSbC7TsdC0ODJytNQpiSoLCEpfAAWEM3PK  
 i+ga+JbhuLxwTuSQBtlarIFOLDMor0UiJk2TKRXxqnCfimQvK3bg6DGZbylkqis4  
 2LaCISExXYF586BUh/X+Stn+JERoJNP/EC41ajEsTgFaBjN0+PHNWgS4FeAdAUEG  
 nyi9bjp9x8vJuP67inDkerwNECiVaZ2MfwrVx2gmNvDTfo2AUBa3Xi/vqFjoWhgw  
 mO1FDRsHuP8AbbDQ2NDECYEZl4vD4GjGhXj4B6YZdsqD6/9oIaLvQGVNwXRSDqII  
 RiYg/3q5wSMliR7v9oqb33sGdZsQEOR3w1uHgXZtN5mvBxFwAc8lBdISL8NEFa60  
 5jMbw3bMTPYjUw7QbN5VzWJzHnZpGbUy1yjpcr0E0CHINKLgwpCuR+les4pmCq7V  
 wRwZ85onsO0lRhfcplpWSN25HJEACI9/IA196rpwCRPHLHoVIKvsK/pFAfziZSE  
 Q45ZwmdaFVeXOeJfwdWab2BpeO8k9mpCIV0v013D7GkRhGwyi0rrCJjlkCwcuJ/c  
 7ViHiTfhoDPckJqsO2PP/rBut1oONh2T9MfOQAXfC5E=

-----END RSA PRIVATE KEY-----

รูปที่ 5.3 คีย์ส่วนตัวของผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว

5.2.3 ทำการสำเนาส่วนของคีย์สาธารณะใส่แผ่นบันทึกข้อมูลนำส่งให้แก่ผู้ออกใบรับรอง ผู้ออกใบรับรองนำคีย์สาธารณะที่ได้มาออกใบรับรองดังแสดงในรูปที่ 5.4 โดยใช้คีย์ส่วนตัวของผู้ออกใบรับรองในการลงลายเซ็นอิเล็กทรอนิกส์ แล้วสำเนาใส่แผ่นบันทึกข้อมูลส่งคืนให้กับผู้ขอใบรับรอง (ผู้ให้บริการ) เพื่อทำการติดตั้งลงในเครื่องผู้ให้บริการรหัสผ่าน

issuer :/C=TH/SP=Bangkok/O=Chulalongkorn University/OU=Computer Engineering  
 Department/CN=CAserver  
 subject:/C=TH/SP=Bangkok/O=Chulalongkorn University/OU=Computer Engineering  
 Department/CN=OTPserver  
 serial :01

Certificate:

Data:

Version: 2 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5withRSAEncryption

Issuer: C=TH, SP=Bangkok, O=Chulalongkorn University, OU=Computer Engineering Department,  
 CN=CAserver

Validity

Not Before: Apr 27 00:53:32 1999 GMT

Not After : Apr 26 00:53:32 2000 GMT

Subject: C=TH, SP=Bangkok, O=Chulalongkorn University, OU=Computer Engineering Department,  
 CN=OTPserver

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Modulus:

00:97:90:73:fe:a8:db:35:79:5d:b2:61:8c:29:89:  
 f5:0d:8e:f8:9e:5d:e4:dc:40:14:4a:ec:c4:e9:6e:  
 1d:4a:33:aa:04:cc:83:5e:4e:f5:a9:dd:2d:11:68:  
 2a:15:6c:b0:37:96:38:1d:d9:70:ca:42:28:d1:e9:  
 03:c7:25:bc:76:c9:a7:ff:15:a4:ac:71:41:47:9c:  
 b7:56:9f:5b:91:4e:8f:55:9c:d2:60:09:8a:e0:06:  
 1c:d4:ec:67:8e:a2:08:81:b4:0f:f0:f3:d9:43:7c:  
 1b:a5:dd:9d:a2:d0:de:43:da:48:23:8d:2f:5f:66:  
 c6:e8:cc:36:b9:45:97:4d:b5

Exponent: 65537 (0x10001)

X509v3 extensions:

Netscape CA Revocation Url:

."http://orb.mincom.oz.au/ca-crl.pem

Netscape Comment:

..This is a comment

Signature Algorithm: md5withRSAEncryption

6c:67:ef:64:7b:c2:8e:7e:83:0f:81:71:40:d5:d0:80:71:23:  
af:eb:06:81:9d:aa:77:1d:79:3e:13:c4:aa:29:2b:44:c0:2e:  
51:6a:10:67:74:fe:7f:c7:5b:da:1f:5d:91:49:79:08:13:da:  
ca:23:68:9d:84:bb:32:8b:fb:c0:4c:f9:14:cc:18:14:0b:6f:  
fc:03:7f:79:a8:47:2f:40:b3:fc:c5:58:7b:71:43:96:92:a4:  
2c:73:e8:93:cc:d4:b0:3c:2c:bd:7a:f5:31:41:67:d1:80:3a:  
d1:ed:a8:7c:f1:2e:91:7c:a2:e1:5c:74:99:ff:ff:80:3a:b3:  
9c:f9

-----BEGIN CERTIFICATE-----

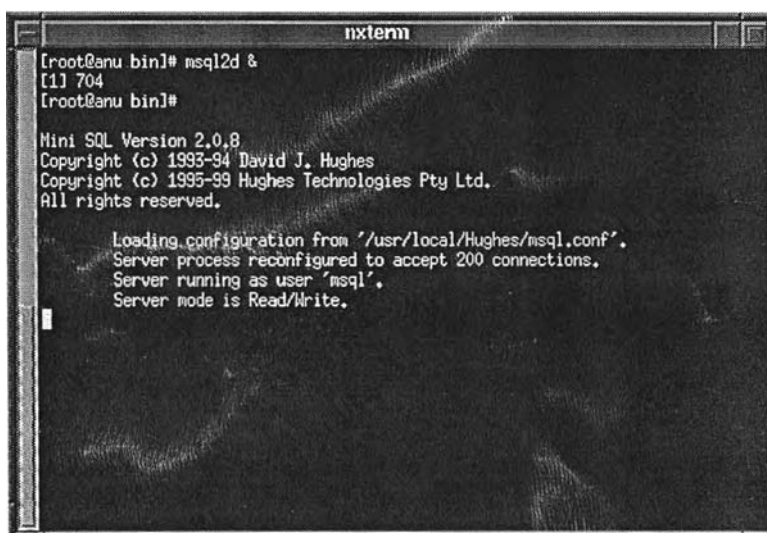
MIICzTCCAjagAwIBAgIBATANBgkqhkiG9w0BAQQFADB/MQswCQYDVQQGEwJUSDEQ  
MA4GA1UECBMHQmFuZ2tvazEhMB8GA1UEChMYQ2h1bGFsb25na29ybiBVbml2ZXJz  
aXR5MSGwJgYDVQQLEx9Db21wdXRlciBFbmdpbmVlcmluZyBEZXBhcnRtZW50MREw  
DwYDVQQDEwhDQXNlcnZlejAeFw05OTA0MjcwMDUzMzJaFw0wMDA0MjYwMDUzMzJa  
MIGAMQswCQYDVQQGEwJUSDEQMA4GA1UECBMHQmFuZ2tvazEhMB8GA1UEChMYQ2h1  
bGFsb25na29ybiBVbml2ZXJzaXR5MSGwJgYDVQQLEx9Db21wdXRlciBFbmdpbmVl  
cmluZyBEZXBhcnRtZW50MRlWEAYDVQQDEwlpVFZzZXJ2ZXIwZ8wDQYJKoZIhvcN  
AQEBBQADgY0AMIGJAoGBAJeQc/6o2zV5XbJhjCmJ9Q2O+J5d5NxAFersxOluHUoz  
qgTMg15O9andLRFoKhVssDeWOB3ZcMpCKNHpA8clvHbJp/8VpKxxQUect1afW5FO  
jlWc0mAJiuAGHNTsZ46iCIG0D/Dz2UN8G6XdnaLQ3kPaSConL19mxujMnrIFi021  
AgMBAAGjVzBVMDEGCWCGSAGG+EIBBAQkFiJodHRwOi8vb3JiLm1pbmNvbS5vei5h  
dS9jYS1jemwucGVtMCAGCWCsAGG+EIBDQQTfFhFUaGlzIGlzIGEgY29tbWVudDAN  
BgkqhkiG9w0BAQQFAAObgQBsZ+9ke8KOfoMPgXFA1dCAcSOv6waBnap3HXk+E8Sq  
KStEwC5RahBndP5/x1vaH12RSXkIE9rKI2idhLsyi/vATPkUzBgUC2/8A395qEcv  
QLP8xVh7cUOWkqQsc+iTzNSwPCy9evUxQWfRgDrR7ah88S6RfKLhXHSZ//+AOrOc  
+Q==

-----END CERTIFICATE-----

รูปที่ 5.4 ใบรับรองของผู้ให้บริการที่ถูกรอกโดยผู้ออกใบรับรอง

5.2.4 ผู้ขอใช้บริการติดต่อขอใบรับรองของผู้ออกใบรับรอง ดังแสดงในรูปที่ 5.1 มาติดตั้งลงบนเครื่องที่ขอใช้บริการ

5.2.5 ติดตั้งโปรแกรมที่ทำหน้าที่บำรุงรักษาฐานข้อมูลของระบบรหัสผ่านแบบใช้ครั้งเดียว ลงบนเครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียว ได้แก่ โปรแกรมจัดการฐานข้อมูลแบบสัมพันธ์ ชื่อ “mysql” และ โปรแกรมเครื่องเสมือนจาวา (JDK) แล้วเรียกโปรแกรม mSQL2d ขึ้นมาทำหน้าที่ให้บริการฐานข้อมูลดังแสดงในรูปที่ 5.5



```

nxterm
[root@anu bin]# msql2d &
[1] 704
[root@anu bin]#

Mini SQL Version 2.0.8
Copyright (c) 1993-94 David J. Hughes
Copyright (c) 1995-99 Hughes Technologies Pty Ltd.
All rights reserved.

Loading configuration from '/usr/local/Hughes/msql.conf'.
Server process reconfigured to accept 200 connections.
Server running as user 'msql'.
Server mode is Read/Write.

```

รูปที่ 5.5 แสดงการเริ่มดำเนินงานของโปรแกรมจัดการฐานข้อมูล

5.2.6 ลงทะเบียนเครื่องแม่ข่ายยูนิคซ์ลงในฐานข้อมูล โดยการใส่ชื่อเครื่อง ชื่อโดเมน และหมายเลขไอพี ผ่านทางโปรแกรมบำรุงรักษาฐานข้อมูลรหัสผ่านแบบใช้ครั้งเดียว ดังแสดงในรูปที่ 5.6

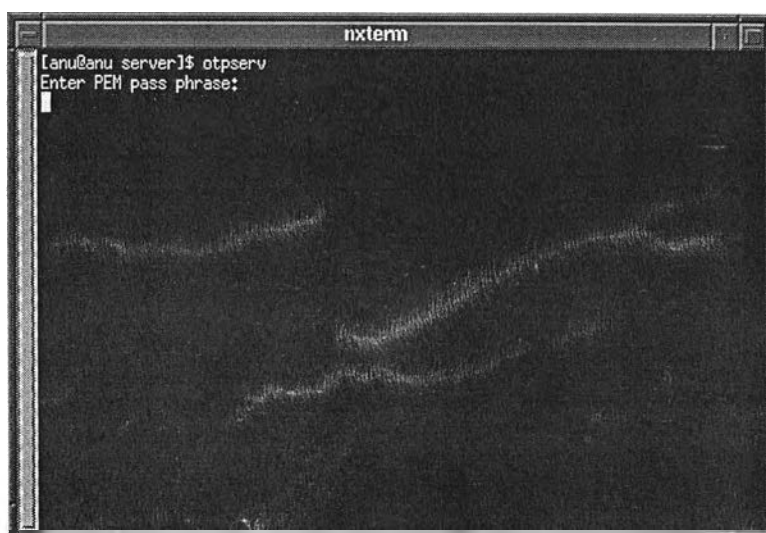
รูปที่ 5.6 หน้าจอที่ใช้ในการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์

5.2.7 เพิ่มบัญชีผู้ใช้ทั้งประเภทใช้รหัสผ่านแบบยูนิกซ์ในที่นี้คือ “anu” และผู้ใช้ประเภทใช้รหัสผ่านแบบใช้ครั้งเดียวในที่นี้คือ “anu1” โดยดำเนินการตามขั้นตอนในข้อ 3.3.3 สำหรับกรณีของผู้ใช้ประเภทใช้รหัสผ่านแบบใช้ครั้งเดียวให้เพิ่มบัญชีผู้ใช้ในฐานะข้อมูลผ่านโปรแกรมบำรุงรักษาฐานข้อมูลรหัสผ่านแบบใช้ครั้งเดียวดังแสดงในรูปที่ 5.7

รูปที่ 5.7 หน้าจอที่ใช้ในการเพิ่มบัญชีผู้ใช้เข้าสู่ระบบรหัสผ่านแบบใช้ครั้งเดียว



5.2.8 ติดตั้งโปรแกรมผู้ให้บริการ (otpserv) ลงบนเครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียว เรียกโปรแกรม otpserv หลังจากนั้นโปรแกรมจะแสดงข้อความให้คีย์วลีรหัสผ่าน (pass phase) ดังแสดงในรูปที่ 5.8 ทำการคีย์วลีรหัสผ่านตามที่กำหนดในขั้นตอนการสร้างชุดคีย์สาธารณะตามข้อ 5.2.2 หลังจากนั้นโปรแกรม otpserv จะทำหน้าที่ให้บริการรหัสผ่าน



รูปที่ 5.8 แสดงการเริ่มดำเนินงานของโปรแกรมให้บริการรหัสผ่าน

5.2.9 ติดตั้งโปรแกรมขอใช้บริการแทนที่โปรแกรม “login” ในไดเรกทอรี /bin ของเครื่องผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว (เครื่องแม่ข่ายยูนิกซ์)

### 5.3 ขั้นตอนการทดสอบระบบ

5.3.1 ทดสอบการเข้าใช้งานบนเครื่องแม่ข่ายยูนิกซ์ เมื่อผู้ใช้เป็นประเภทใช้รหัสผ่านแบบยูนิกซ์

5.3.2 ทดสอบการเข้าใช้งานบนเครื่องแม่ข่ายยูนิกซ์ เมื่อผู้ใช้เป็นประเภทใช้รหัสผ่านแบบใช้ครั้งเดียว ในกรณีต่าง ๆ ดังนี้

- กรณีที่ผู้ใช้คีย์รหัสผ่านถูกต้อง
- กรณีที่ผู้ใช้คีย์รหัสผ่านผิด
- กรณีบัญชีผู้ใช้ถูกระงับการใช้

- กรณีบัญชีผู้ใช้หมดอายุการใช้
- กรณีจำนวนรหัสผ่านใกล้หมด
- บัญชีผู้ใช้ใกล้หมดอายุ

5.3.3 ทดสอบการป้องกันการขอใช้บริการจากเครื่องแม่ข่ายยูนิกซ์ ที่ไม่ได้ลงทะเบียน

5.3.4 ทดสอบการป้องกันการปลอมตัวเป็นผู้ให้บริการ โดยการปลอมใบรับรอง ในกรณีต่าง ๆ

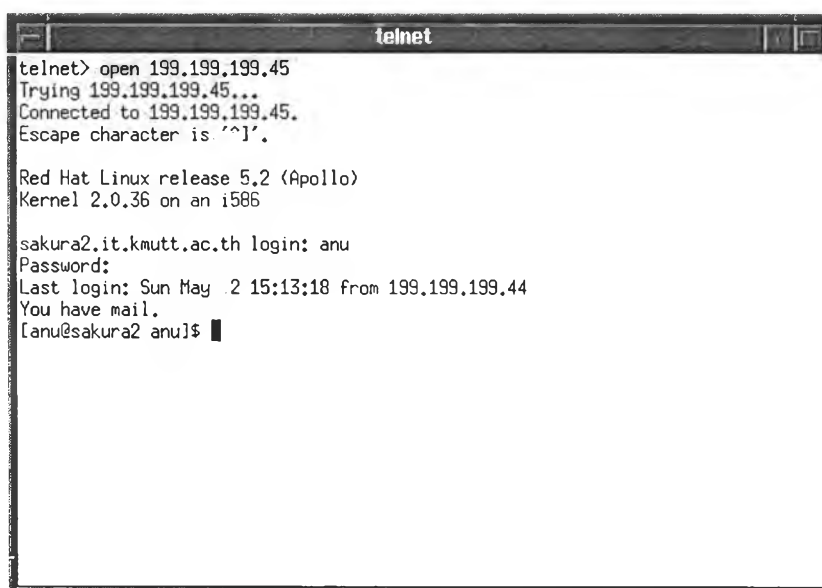
5.3.5 ทดสอบการเข้ารหัสของชั้นเอสเอสแอล

5.3.6 ทดสอบการระบุขอบเขตของบัญชีผู้ใช้

## 5.4 ผลการทดสอบระบบ

ระบบรหัสผ่านแบบใช้ครั้งเดียวสามารถทำงานได้ตามที่ออกแบบ โดยมีผลการทดสอบดังนี้

5.4.1 ผู้ใช้ของเครื่องแม่ข่ายยูนิกซ์สามารถล็อกอินเข้าใช้งานได้ตามปกติ ในกรณีที่ใช้รหัสผ่านแบบยูนิกซ์ ซึ่งในที่นี้ คือ การล็อกอินด้วยชื่อ “anu” ดังแสดงในรูปที่ 5.9



```
telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^]'.

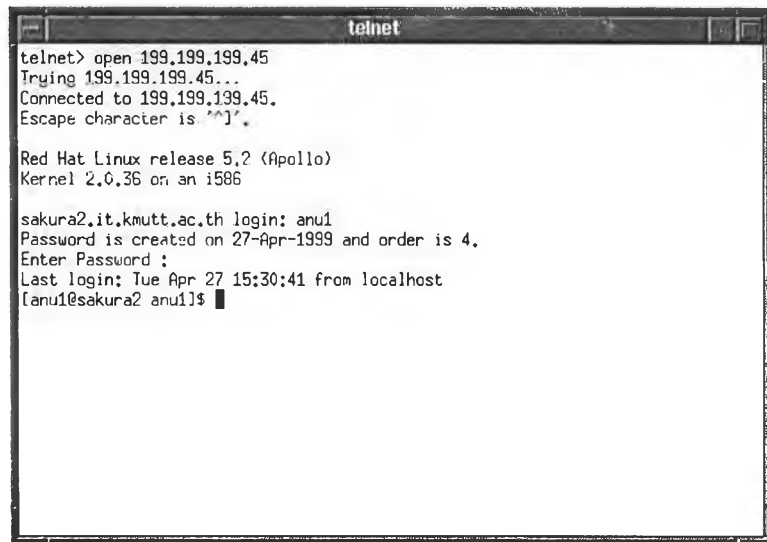
Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu
Password:
Last login: Sun May .2 15:13:18 from 199.199.199.44
You have mail.
[anu@sakura2 anu]$
```

รูปที่ 5.9 แสดงการล็อกอินของผู้ใช้ประเภทที่ใช้รหัสผ่านแบบยูนิกซ์

5.4.2 ผู้ใช้ของเครื่องแม่ข่ายยูนิคซ์สามารถล็อกอินเข้าใช้งานได้ตามปกติ ในกรณีที่ใช้รหัสผ่านแบบใช้ครั้งเดียว ซึ่งในที่นี้ คือ การล็อกอินด้วยชื่อ “anu1” ซึ่งสามารถแยกการทดสอบออกได้ 6 กรณี ดังนี้

5.4.2.1 กรณีที่ผู้ใช้คีย์รหัสผ่านถูกต้อง ระบบจะให้ข้อความพร้อมรับคำสั่ง (shell prompt) ตามปกติ ดังแสดงในรูปที่ 5.10 นอกจากนี้ยังมีการแสดงข้อความแนะนำการคีย์รหัสผ่านประกอบ ได้แก่ วันที่สร้างชุดรหัสผ่าน และลำดับที่ปัจจุบันของรหัสผ่าน



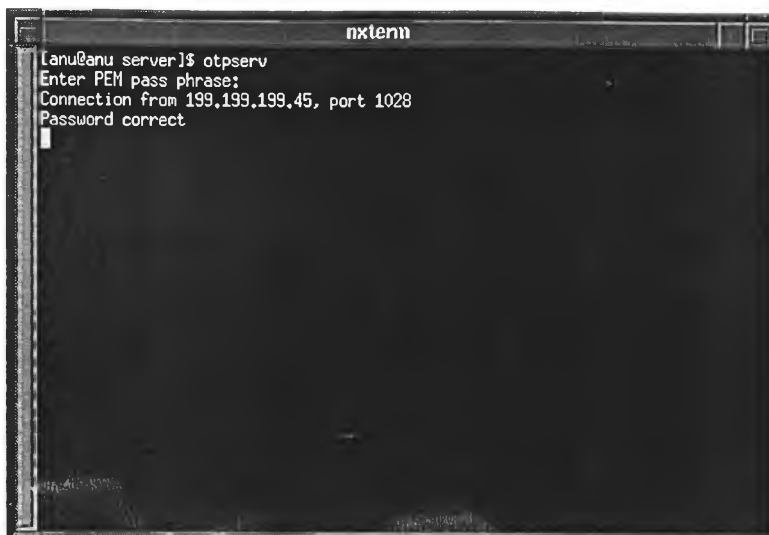
```
telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^['.

Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
Password is created on 27-Apr-1999 and order is 4.
Enter Password :
Last login: Tue Apr 27 15:30:41 from localhost
[anu1@sakura2 anu1]$
```

รูปที่ 5.10 แสดงการล็อกอินของผู้ใช้ประเภทรหัสผ่านแบบใช้ครั้งเดียว และคีย์รหัสผ่านถูกต้อง

ส่วนของผู้ให้บริการ (OTP Server) สามารถรายงานว่าหมายเลขไอพี หมายเลขพอร์ตของผู้ขอใช้บริการ และ การตรวจสอบรหัสผ่าน ดังแสดงในรูปที่ 5.11



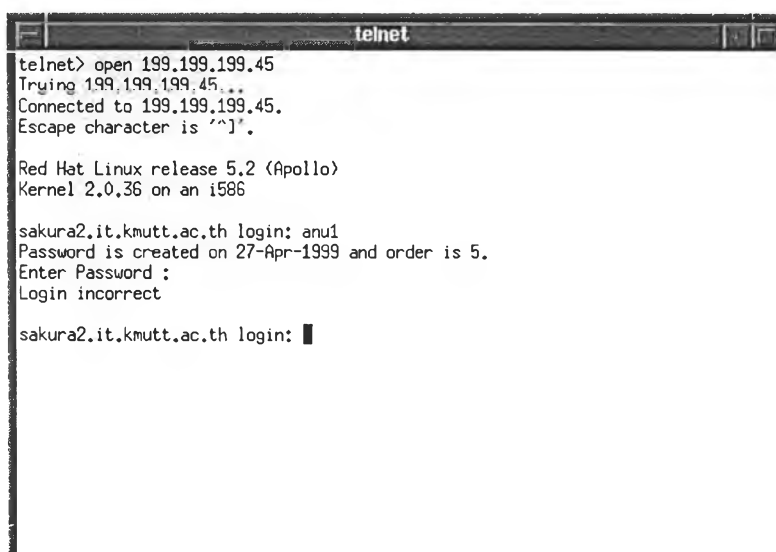
```

nxtenn
lanu@anu server]# otpserv
Enter PEM pass phrase:
Connection from 199.199.199.45, port 1028
Password correct

```

รูปที่ 5.11 แสดงการทำงานของ OTP Sever กรณีที่มีการขอตรวจสอบรหัสผ่าน  
และรหัสผ่านถูกต้อง

5.4.2.2 กรณีที่ผู้ใช้รหัสผ่านผิด ระบบจะให้คีย์ช็อล็อกอินและรหัสผ่านใหม่ โดยในการคีย์ผิดแต่ละครั้ง จะเพิ่มเวลาหน่วงมากขึ้นเรื่อย ๆ แต่อนุญาตให้คีย์รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง ดังแสดงในรูปที่ 5.12 ส่วนแสดงการทำงานของ ผู้ให้บริการ แสดงในรูปที่ 5.13



```

telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^'.

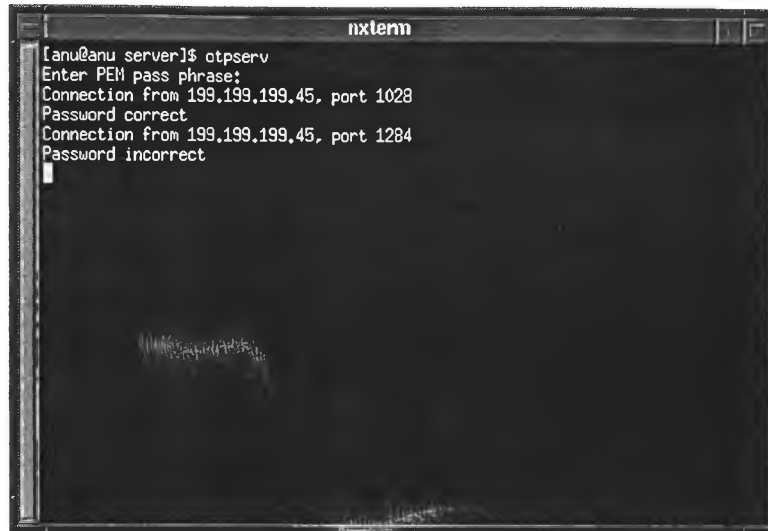
Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
Password is created on 27-Apr-1999 and order is 5.
Enter Password :
Login incorrect

sakura2.it.kmutt.ac.th login: █

```

รูปที่ 5.12 แสดงการล็อกอินเมื่อคีย์รหัสผ่านผิด



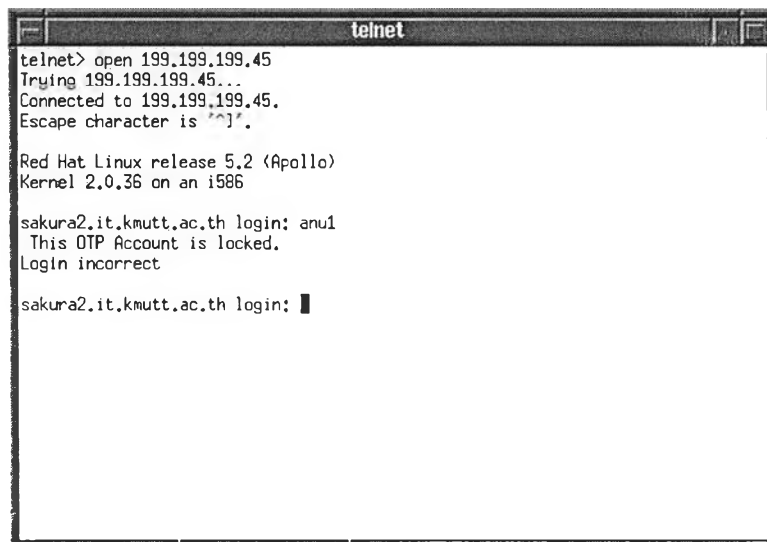
```

nxtelm
[anu@anu server]$ otpserv
Enter PEM pass phrase:
Connection from 199.199.199.45, port 1028
Password correct
Connection from 199.199.199.45, port 1284
Password incorrect

```

รูปที่ 5.13 แสดงการทำงานของ OTP Server กรณีที่มีผู้ใช้คีย์รหัสผ่านผิด

5.4.2.3 กรณีบัญชีผู้ใช้ถูกสั่งระงับการใช้ ระบบจะไม่อนุญาตให้ล็อกอินและแสดงข้อความเตือนดังรูป 5.14 แล้วให้ล็อกอินใหม่ ส่วนการทำงานของผู้ใช้บริการแสดงดังรูปที่ 5.15



```

telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^['.


Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
This OTP Account is locked.
Login incorrect

sakura2.it.kmutt.ac.th login: █

```

รูปที่ 5.14 แสดงการล็อกอินของผู้ใช้ที่ถูกสั่งระงับการใช้



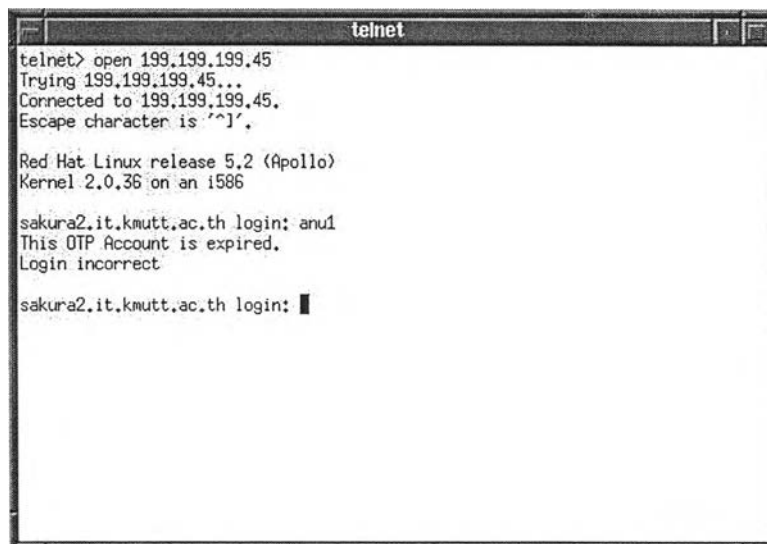
```

nxtenn
[anu@anu server]$ otpserv
Enter PEM pass phrase:
Connection from 199.199.199.45, port 20484
User account is locked!

```

รูปที่ 5.15 แสดงการทำงานของ OTP Server กรณีบัญชีผู้ใช้ถูกระงับการใช้

5.4.2.4 กรณีบัญชีผู้ใช้หมดอายุการใช้ ระบบจะไม่อนุญาตให้ล็อกอินและแสดงข้อความเตือนให้ทราบดังแสดงในรูปที่ 5.16 แล้วให้ล็อกอินใหม่ ส่วนการทำงานของผู้ใช้บริการแสดงในรูปที่ 5.17



```

telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^]'.

Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
This OTP Account is expired.
Login incorrect

sakura2.it.kmutt.ac.th login: █

```

รูปที่ 5.16 แสดงการล็อกอินของผู้ใช้กรณีบัญชีผู้ใช้หมดอายุการใช้

```

ixterm
[anu@anu server]$ otpserv
Enter PEM pass phrase:
Connection from 199.199.199.45, port 20484
User account is locked!
Connection from 199.199.199.45, port 20996
Password expire

```

รูปที่ 5.17 แสดงการทำงานของ OTP Server กรณีที่บัญชีผู้ใช้หมดอายุ

5.4.2.5 กรณีจำนวนรหัสผ่านใกล้หมด ระบบจะอนุญาตให้ล็อกอินได้ตามปกติ แต่จะแสดงข้อความเตือน ดังแสดงในรูปที่ 5.18 เพื่อให้ผู้ใช้ติดต่อขอรับใบรายงานรหัสผ่านชุดใหม่จากผู้ดูแลระบบ รูปที่ 5.19 แสดงให้เห็นการทำงานของผู้ใช้บริการซึ่งมีการสร้างรหัสผ่านชุดใหม่ให้โดยอัตโนมัติ

```

telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^]'.

Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
Password is created on 27-Apr-1999 and order is 182.
Enter Password :
Password will be empty recently.
Last login: Sun May  2 15:23:15 from 199.199.199.44
[anu1@sakura2 anu1]$

```

รูปที่ 5.18 แสดงการเตือนให้ผู้ใช้ทราบว่าจำนวนรหัสผ่านใกล้หมด

```

nxtlenn
[anu@anu server-1$ otpserv
Enter PEM pass phrase:
Connection from 199.199.199.45, port 20484
User account is locked!
Connection from 199.199.199.45, port 20996
Password expire
Connection from 199.199.199.45, port 21252
Password correct
Gen Password

```

รูปที่ 5.19 แสดงการทำงานของ OTP Server เมื่อจำนวนรหัสผ่านของผู้ใช้ใกล้หมด

5.4.2.6 กรณีบัญชีผู้ใช้ใกล้หมดอายุ ระบบจะอนุญาตให้ล็อกอินได้ตามปกติ แต่จะแสดงข้อความเตือนดังแสดงในรูปที่ 5.20 เพื่อให้ผู้ใช้ติดต่อขอต่ออายุการใช้กับผู้ดูแลระบบ

```

telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^]'.

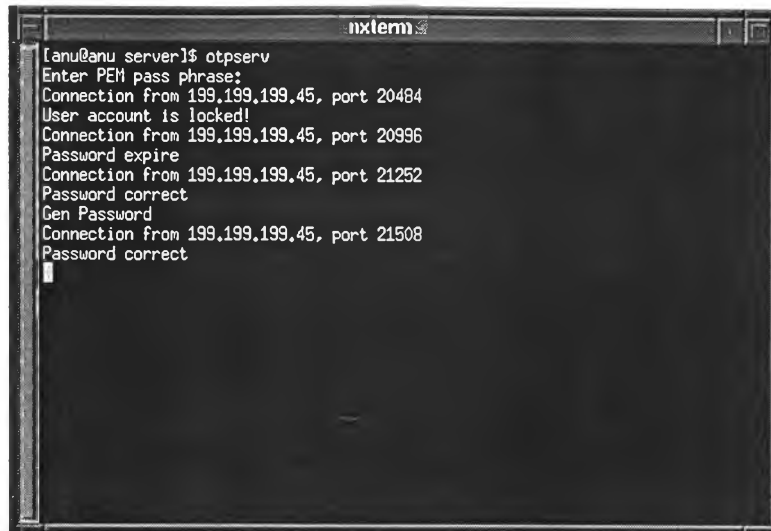
Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
Password is created on 27-Apr-1999 and order is 50.
Enter Password :
This OTP Account will be expired recently.
Last login: Sun May 2 16:58:35 from 199.199.199.44
[anu1@sakura2 anu1]$ █

```

รูปที่ 5.20 แสดงการเตือนให้ผู้ใช้ทราบว่าบัญชีผู้ใช้ใกล้หมดอายุ





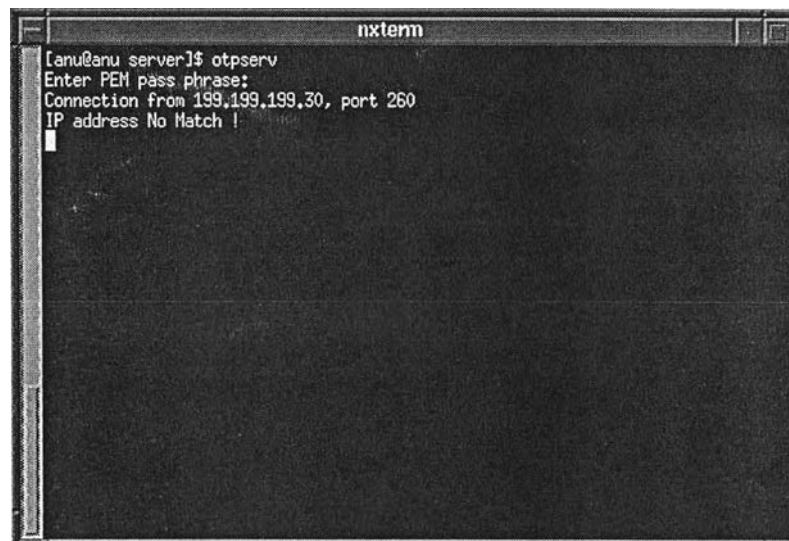
```

[anu@anu server]$ otpserv
Enter PEM pass phrase:
Connection from 199.199.199.45, port 20484
User account is locked!
Connection from 199.199.199.45, port 20996
Password expire
Connection from 199.199.199.45, port 21252
Password correct
Gen Password
Connection from 199.199.199.45, port 21508
Password correct

```

รูปที่ 5.21 แสดงการทำงานของ OTP Server เมื่อบัญชีผู้ใช้ใกล้หมดอายุ

5.4.3 ผู้ให้บริการสามารถตรวจจับเครื่องแม่ข่ายยูนิกซ์ที่ไม่มีการลงทะเบียนดังแสดงในรูปที่ 5.22 และจะทำการขอปิดการติดต่อทันที เป็นผลให้ผู้ขอใช้บริการไม่สามารถใช้บริการจากผู้ให้บริการได้ ดังแสดงในรูปที่ 5.23



```

[anu@anu server]$ otpserv
Enter PEM pass phrase:
Connection from 199.199.199.30, port 260
IP address No Match !

```

รูปที่ 5.22 แสดงการทำงานของ OTP Server ในการตรวจจับผู้ใช้บริการที่ไม่ได้ลงทะเบียน

```

telnet> o 199.199.199.30
Trying 199.199.199.30...
Connected to 199.199.199.30.
Escape character is '^]'.

Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anu1
This OTP Client isn't in the region.
Login incorrect

sakura2.it.kmutt.ac.th login: █

```

รูปที่ 5.23 แสดงการถูกปิดการติดต่อเนื่องจากเครื่องแม่ข่ายยูนิคซ์ไม่ได้ลงทะเบียน

5.4.4 ระบบพิสูจน์ตัวตนจริงสามารถป้องกันการปลอมตัวเป็นผู้ให้บริการได้ โดยทำการปลอมแปลงใบรับรองของผู้ให้บริการ 2 วิธี คือ

5.4.4.1 ใช้ใบรับรองของคนอื่นที่ออกโดยผู้ออกใบรับรองคนเดียวกันกับผู้ให้บริการตัวจริง ผู้ขอใช้บริการ (OTP Client) สามารถตรวจจับได้ว่าเป็นใบรับรองของคนอื่นที่ไม่ใช่ของผู้ให้บริการตัวจริง ดังแสดงในรูปที่ 5.24 จึงหยุดการติดต่อกับผู้ให้บริการทันที

```

telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^]'.

Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

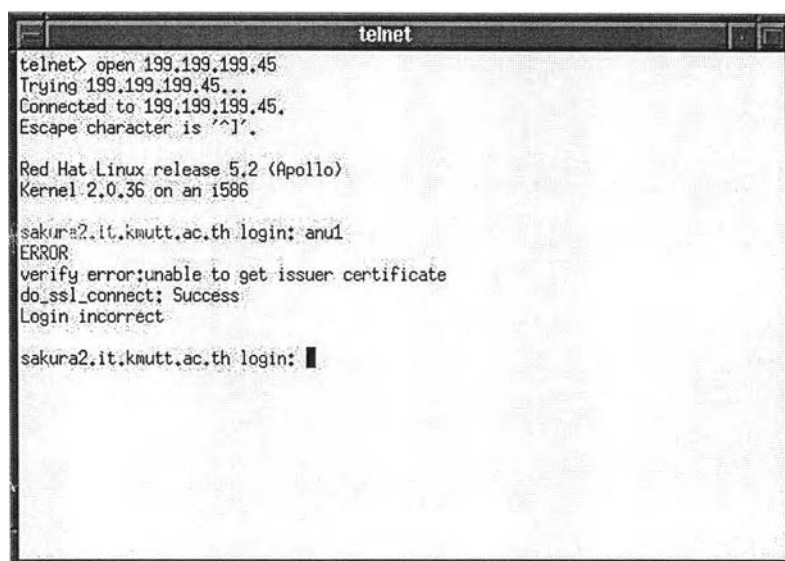
sakura2.it.kmutt.ac.th login: anu1
Server subject name is not match.
ssl_states: Success
Login incorrect

sakura2.it.kmutt.ac.th login: █

```

รูปที่ 5.24 แสดงการทำงานของ OTP Client ในการตรวจสอบใบรับรองพบว่าไม่ใช่ของผู้ให้บริการตัวจริง

- 5.4.4.2 ใช้ไบบรรองที่มีชื่อตรงกับผู้ให้บริการแต่ออกโดยผู้ออกไบบรรองที่ไม่น่าเชื่อถือ ผู้ขอใช้บริการตรวจสอบว่าผู้รับรองที่ลงลายเซ็นอิเล็กทรอนิกส์ไม่อยู่ในรายชื่อผู้รับรองที่น่าเชื่อถือ ดังแสดงในรูปที่ 5.25 จึงหยุดการติดต่อกับผู้ให้บริการทันที



```

telnet
telnet> open 199.199.199.45
Trying 199.199.199.45...
Connected to 199.199.199.45.
Escape character is '^I'.

Red Hat Linux release 5.2 (Apollo)
Kernel 2.0.36 on an i586

sakura2.it.kmutt.ac.th login: anul
ERROR
verify error:unable to get issuer certificate
do_ssl_connect: Success
Login incorrect

sakura2.it.kmutt.ac.th login: █

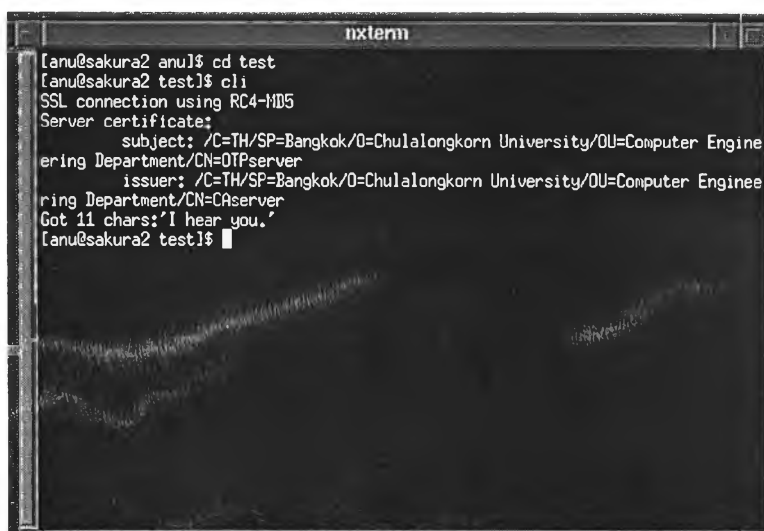
```

รูปที่ 5.25 แสดงการทำงานของ OTP Client ในการตรวจสอบไบบรรองพบว่าออกโดยผู้รับรองที่ไม่น่าเชื่อถือ

5.4.5 การเข้ารหัสของชั้นเอสเอสแอล สามารถป้องกันการดักฟังขณะส่งข้อมูลไปมาระหว่างผู้ขอใช้บริการและผู้ให้บริการ ทดสอบโดยการเขียนโปรแกรมจำลองการทำงานของผู้ให้บริการ และผู้ขอใช้บริการ ฟังผู้ให้บริการประกอบด้วย โปรแกรม serv-1 และ serv-2 และฟังผู้ขอใช้บริการ คือ โปรแกรม cli ซึ่งมีการทำงานดังนี้

- โปรแกรม serv-1 ทำหน้าที่รับข้อมูลจากโปรแกรม cli ผ่านชั้นสื่อสารเอสเอสแอล
- โปรแกรม serv-2 ทำหน้าที่รับข้อมูลจากโปรแกรม cli จากชั้นที่ซีพี โดยไม่ผ่านชั้นสื่อสารเอสเอสแอล
- โปรแกรม cli ทำการส่งข้อความ “Hello World” ผ่านชั้นสื่อสารเอสเอสแอล

ผลจากการทดลองส่งข้อความ “Hello World” โดยโปรแกรม cli ที่มีการเข้ารหัส ด้วยชั้นสื่อสารเอสเอสแอล ดังแสดงในรูปที่ 5.26 ไปยังโปรแกรม serv-1 ที่มีการถอดรหัสผ่านชั้นสื่อสารเอสเอสแอล ดังแสดงในรูปที่ 5.27 ปรากฏว่าโปรแกรม serv-1 สามารถอ่านข้อความได้ถูกต้อง



```

nxterm
[anu@sakura2 anu]$ cd test
[anu@sakura2 test]$ cli
SSL connection using RC4-MD5
Server certificate:
  subject: /C=TH/SP=Bangkok/O=Chulalongkorn University/OU=Computer Engine
  ering Department/CN=OTPServer
  issuer: /C=TH/SP=Bangkok/O=Chulalongkorn University/OU=Computer Engine
  ring Department/CN=CAserver
Got 11 chars: 'I hear you.'
[anu@sakura2 test]$
  
```

รูปที่ 5.26 แสดงการส่งข้อความ “Hello World” ของโปรแกรม cli



```

nxterm
[anu@sakura2 test]$ serv-1
Enter PEM pass phrase:
Connection from 100007f, port 540a
SSL connection using RC4-MD5
Client does not have certificate.
Got 12 chars: 'Hello World!'
[anu@sakura2 test]$
  
```

รูปที่ 5.27 แสดงการรับข้อความ “Hello World” ของโปรแกรม serv-1

ต่อมาเมื่อเปลี่ยนมาใช้โปรแกรม serv-2 ทำหน้าที่รับข้อความ "Hello World" จากโปรแกรม cli แทน ปรากฏว่าข้อความที่โปรแกรม serv-2 รับได้ไม่สามารถอ่านออกได้ เนื่องจากการถอดรหัสโดยชั้นเอสเอสแอล แสดงให้เห็นว่าถ้ามีการดักฟังทางเครือข่าย ข้อมูลที่ถูกดักฟังไม่สามารถนำเอาไปใช้ประโยชน์ได้

```

nxtlenn
[anu@sakura2 test]$ serv-2
Enter PEM pass phrase:
Connection from 100007f, port 560a
SSL connection using RC4-MD5
Client does not have certificate.
Got 30 chars: "njK02" f  m$6ã
ó20^~  &f
[anu@sakura2 test]$
  
```

รูปที่ 5.28 แสดงการรับข้อความ "Hello World" ของโปรแกรม serv-2

5.4.6 ทดสอบการระบุขอบเขตการใช้ของบัญชีผู้ใช้ทั้ง 3 วิธี คือ

- <ชื่อโฮสต์> + <ชื่อเครื่อง> + <ชื่อ โดเมน>
- <ชื่อโฮสต์> + ALL + <ชื่อ โดเมน>
- <ชื่อโฮสต์> + ALL + ALL

โดยการเพิ่มบัญชีผู้ใช้ตามกฎที่ระบุ แล้วทำการทดลองซ้ำตามข้อ 5.4.2 ปรากฏว่าสามารถทำงานได้ถูกต้องและมีลำดับความสำคัญถูกต้องตามที่กำหนดไว้