ปรับแต่ง Secure Shell (SSH) ให้ปลอดภัยมากขึ้น

นายเกรียงศักดิ์นามโคตร (Mr.Jodoi) เรียบเรียง

ก่อนที่จะปรับแต่ง Secure Shell หรือ SSH นั้น มาทำความรู้จักกันก่อนว่า SSH คืออะไร หลายท่านจะคุ้นเคยกับการ Telnet เข้าไปยังอุปกรณ์ต่างๆไม่ว่าจะเป็น Router , Switch หรือ Server ข้อเสียของ Telnet คือ จะไม่มีการเข้ารหัส (encrypted) ดังนั้นเมื่อมีการ Telnet เข้าอุปกรณ์ต่างๆมีโอกาสที่จะโดนขโมย หรือ hack ข้อมูลได้ ส่วนตัว Secure Shell จะมีการเข้ารหัส (encrypted) และต้องมีการติดตั้งโปรแกรม SSH Client ที่เครื่อง PC หรือ Notebook ด้วย เช่นโปรแกรม OpenSSH , Putty เป็นต้น จะเห็นว่า SSH มีความปลอดภัยกว่าแน่นอน ซึ่งเจ้า SSH จะมีติดตั้งอยู่ใน Unix หรือ Linux ทุกค่าย แต่ควรจะมีการปรับแต่งจึงจะมีความปลอดภัยมากขึ้น

เริ่มด้วยการตรวจสอบ service sshd ว่ามีการ run อยู่หรือไม่ ด้วย command netstat ใน Linux Server 2 ตัว ดังนี้

Linux Server ตัวที่ 1

[root@linux-jodoi ~]# **netstat -tanp|grep ssh**

tcp 0 0 :::**22** :::* LISTEN 2406/**sshd**

Linux Server ตัวที่ 2

root@jodoi-gateway:~# **netstat -tanp|grep sshd**

tcp 0 0 0.0.0.0:**2222** 0.0.0.0:* LISTEN 1550/**sshd**

จากผลที่ได้จะเห็นว่า Server ตัวที่ 1 ใช้ port 22 ซึ่งเป็น port ค่า default ของ SSH ถือว่าไม่ปลอดภัย

ในการปรับแต่งค่า config ของ SSH ใน Linux Server นั้นทำได้โดยปรับแต่งที่ file sshd_config ดังนี้

[root@linux-jodoi ~]# **vi /etc/ssh/sshd_config**

#Port 22

Port 54321 (ค่าเดิมเป็น port 22 ทำการเปลี่ยนเป็น 54321 ควรมีอย่างน้อย 5 หลัก)

#Protocol 2,1

Protocol 2 (Protocol เลือกเป็น version 2 จะมีความปลอดภัยกว่า)

#ServerKeyBits 768

ServerKeyBits 1024 (เป็นคีย์ที่ใช้ในการเข้ารหัส ควรเปลี่ยนให้มากขึ้น)

#PermitRootLogin yes

PermitRootLogin no (ไม่ควร ให้ user root login ได้ เพราะจะไม่รู้ว่า user ใดเข้ามาในระบบบ้าง และเสี่ยงเกินไปที่ admin เข้ามาได้โดยตรง)

#MaxAuthTries 6

MaxAuthTries 3 (ใส่ password ผิดได้ไม่เกิน 3 ครั้ง)

#PasswordAuthentication yes

#PermitEmptyPasswords no

PermitEmptyPasswords no (การใช้รหัสผ่านในการ log in และห้ามใช้รหัสผ่านที่ว่างเปล่า)

PasswordAuthentication yes (การใช้รหัสผ่านในการ log in และห้ามใช้รหัสผ่านที่ว่างเปล่า)

#Banner /some/path

Banner /home/jodoi/banner.txt (สร้าง Banner หรือข้อความต้อนรับก่อนเข้า Server)

:wq! (save และออกจาก file config)

ต่อไปเป็นการสร้าง file banner.txt ตามที่กำหนดไว้ใน config file

[root@linux-jodoi ~]# **vi /home/jodoi/banner.txt**

```
##################################################
##################################################
#############      Jodoi Server            ###########
############# Please do not hack Me         ###########
#############  http://www.jodoi.com         ###########
##################################################
##################################################
```

:wq!

สั่ง restart service sshd

[root@linux-jodoi ~]# **/etc/init.d/sshd restart**

Stopping sshd: [OK]

Starting sshd: [OK]

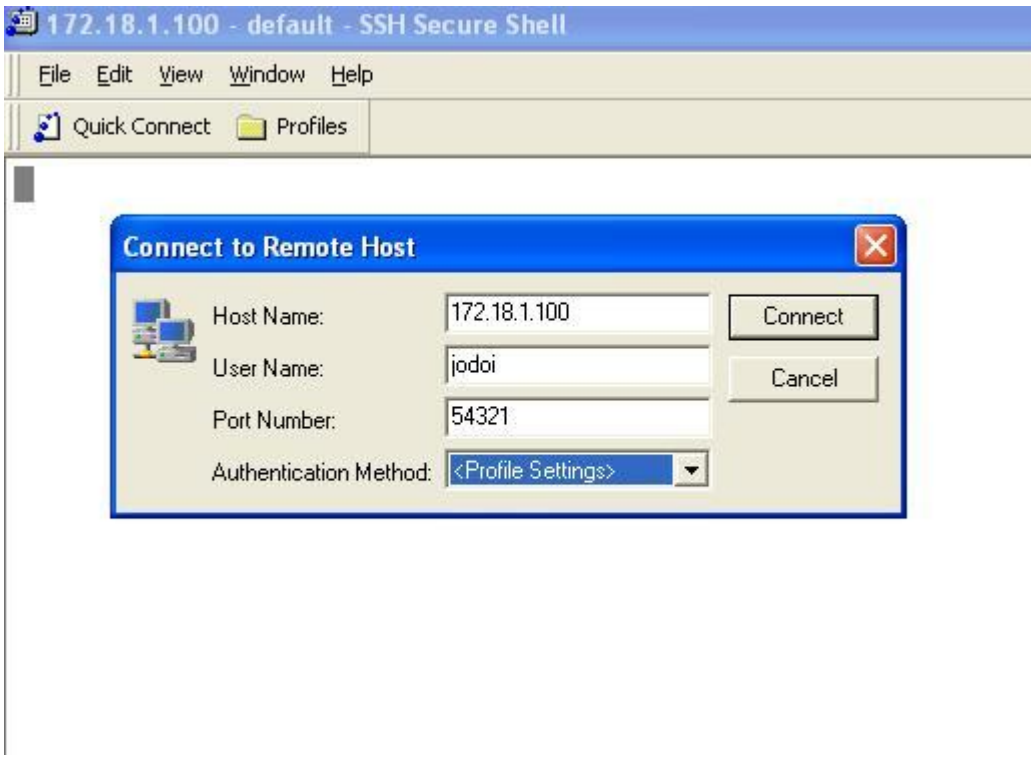
[root@linux-jodoi ~]#

ตรวจสอบ service sshd ว่า run อยู่หรือไม่และ port เปลี่ยนหรือไม่

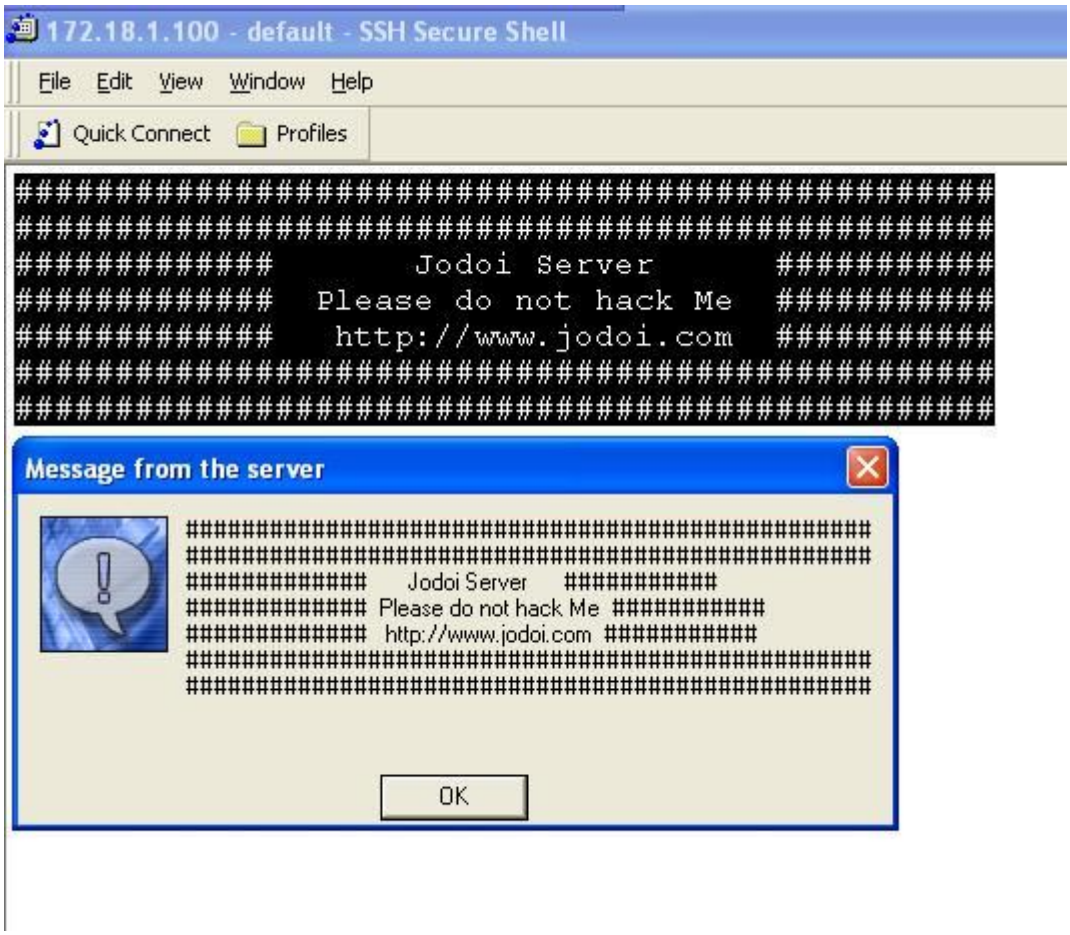
[root@linux-jodoi ~]# **netstat -tanp |grep ssh**

tcp 0 0 :::**54321** :::* LISTEN 4447/sshd

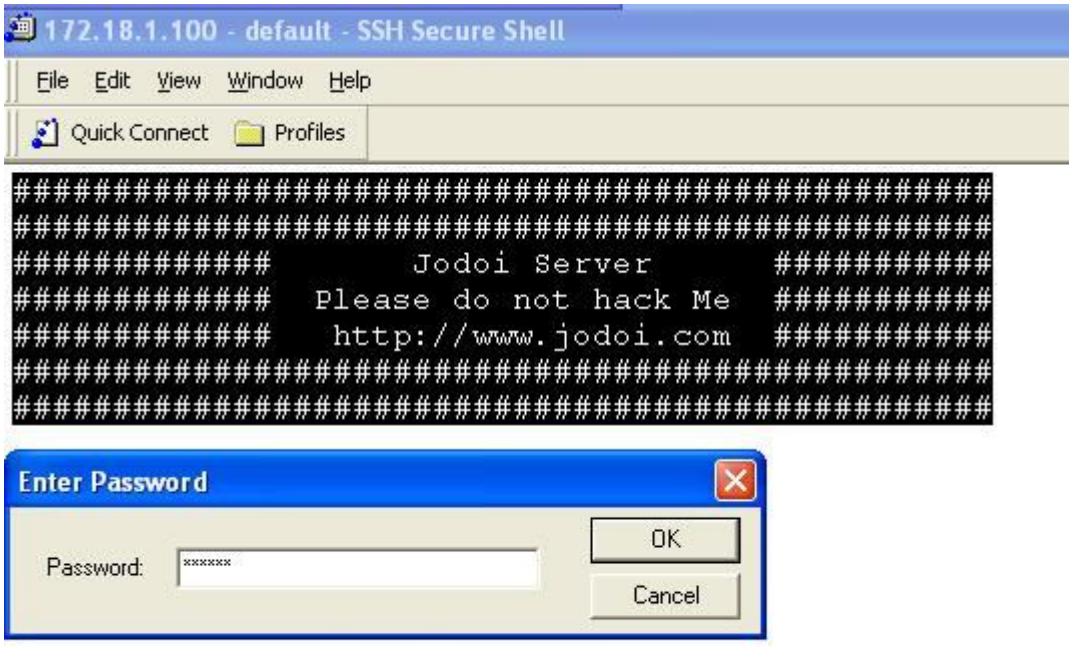
ต่อไปเป็นการทดสอบโดยการ remote ด้วย SSH Client ในที่นี้จะใช้ OpenSSH ดังรูป จะต้องมีการกำหนด IP ของ Linux Server ,User ในการ login และ port ที่ใช้ในการ connect



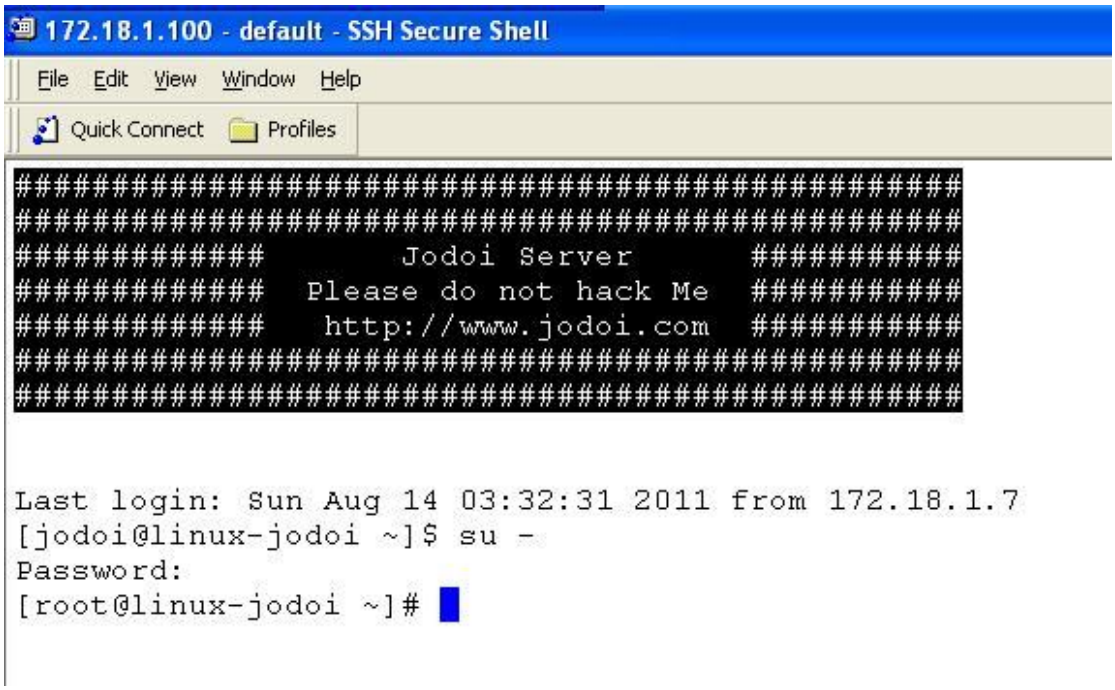
เมื่อสามารถ connect เข้า Linux Server ได้ จะมีข้อความต้อนรับดังรูปด้านล่าง



ให้ทำการใส่ password ตามรูปด้านล่าง ถ้าใส่ไม่ถูกต้องจะไม่สามารถเข้าสู่ Linux Server ได้



ในกรณีที่ใช้ user เป็น root ในการ login เข้า SSH จะไม่สามารถเข้าได้ เนื่องจากใน file config มีการห้ามไว้ และถ้าสามารถเข้าได้จะแสดงดังรูปด้านล่าง
เพียงเท่านี้ SSH Server ก็มีความปลอดภัยแล้ว



ทำการตรวจสอบว่ามีใคร login เข้ามาใน Linux Server บ้าง

[root@linux-jodoi ~]# **netstat -tanp|grep sshd**

tcp 0 0 :::54321 :::* LISTEN 4447/sshd

tcp 0 0 ::ffff:172.18.1.100:54321 ::ffff:172.18.1.7:1422 ESTABLISHED 4495/sshd: jodoi [p

[root@linux-jodoi ~]# **w**

03:36:24 up 59 min, 2 users, load average: 0.03, 0.05, 0.05

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

root tty1 - 02:40 48:38 1.33s 1.33s -bash

jodoi pts/0 172.18.1.7 03:34 1.00s 1.31s 0.49s sshd: jodoi [priv]

สรุปควรจะมีการเปลี่ยนค่า Config ที่เป็นค่า default โดยเฉพาะ port 22 และการห้าม root login เข้า SSH Server ได้ เนื่องจากผู้ที่ใช้งาน Linux Server จะรู้ว่าจะต้องมีการเปิด port 22 ไว้ และ user Admin ก็คือ user root นั่นเอง ถือว่าเสี่ยงมากถ้าไม่เปลี่ยนแปลง และถ้าตั้ง password ง่ายเกินไปก็อันตรายมาก และยังมีโปรแกรมในการสุ่มสร้าง password สำหรับไว้ hack password เข้า SSH Server อีกด้วย

หวังว่าบทความนี้คงจะก่อให้เกิดประโยชน์ไม่มากก็น้อยสำหรับผู้ที่ทำงานอยู่ในแวดวงไอทีและใช้ Linux Server อยู่นะครับ

แหล่งข้อมูลอ้างอิง

http://www.jodoi.com

สนับสนุนโดย http://www.jodoi.com