OPERATING SYSTEM 1

Lecture 11

Eng. Joud Khattab

SECURE SHELL

SSH

What is SSH?

- SSH, or Secure Shell, is a protocol used to securely log onto remote systems.
- It is the most common way to access remote Linux and Unix-like servers.

Setting Up SSH

- First of all we must know our IP address, using the following instruction:
  - **ifconfig**
- Second we must open port 22 to let SSH command execute successfully:
  - **sudo apt-get install openssh-server**

Basic Syntax

- The tool on Linux for connecting to a remote system is called ssh.
- The most basic form of the command is:
  - **ssh remote_host**
    - The *remote_host* is the IP address or domain name that you are trying to connect to.
    - This command assumes that your username on the remote system is the same as your username on your local system.
  - **ssh remote_username@remote_host**
    - If your username is different on the remote system.
- Once you have connected to the server, you will probably be asked to verify your identity by providing a password.
- To exit back into your local session, simply type:
  - exit

SSH Client Version

- Sometimes it may be necessary to identify the SSH client that you are currently running and it's corresponding version number, which can be identified as shown below.
  - **ssh -V**
    - OpenSSH_3.9p1, OpenSSL 0.9.7a Feb 19 2003
  - **ssh -V**
    - ssh: SSH Secure Shell 3.2.9.1 (non-commercial version) on i686-pc-linux-gnu

Login to Remote Host

- The First time when you login to the remotehost from a localhost, it will display the host key not found message and you can give "yes" to continue. The host key of the remote host will be added under .ssh2/hostkeys directory of your home directory, as shown below.

```
localhost$ ssh -l jsmith remotehost.example.com

Host key not found from database.
Key fingerprint:
xabie-dezbc-manud-bartd-satsy-limit-nexiu-jambl-title-jarde-tuxum
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes
Host key saved to /home/jsmith/.ssh2/hostkeys/key_22_remotehost.example.com.pub
host key for remotehost.example.com, accepted by jsmith Mon May 26 2008 16:06:50 -0700
jsmith@remotehost.example.com password:
remotehost.example.com$
```

Login to Remote Host

- The Second time when you login to the remote host from the localhost, it will prompt only for the password as the remote host key is already added to the known hosts list of the ssh client.

```
localhost$ ssh -l jsmith remotehost.example.com
jsmith@remotehost.example.com password:
remotehost.example.com$
```

File Transfer to/from Remote Host

- Another common use of ssh client is to copy files from/to remote host using scp.
  - Copy file from the remotehost to the localhost:
    - **Localhost $ scp jsmith@remotehost.example.com:/home/jsmith/remotehostfile.txt remotehostfile.txt**
  - Copy file from the localhost to the remotehost:
    - **Localhost $ scp localhostfile.txt jsmith@remotehost.example.com:/home/jsmith/localhostfile.txt**