**CH 18 OpenSSH: secure network communication**

(In the case of the questions referencing a server named plum just use the IP address of your second virtual machine)

1. What is the difference between the **scp** and **sftp** utilities?

A: The scp (secure copy) utility copies files to and from a remote system. sftp (FTP services) copies files to and from a remote system but it is a secure replacement for ftp.

2. How can you use **ssh** to find out who is logged in on a remote system?

A: The ssh utility allows you to log in on a remote system over a network. I can omit user@ from the command line if the host and remote user use the same username. Hence, I choose the same username on both systems and the command which displays the output of who run on host is

$ ssh host who

3. How would you use **scp** to copy your **~/.bashrc** file from the system named **plum** to the local system?

A: Assuming the host is zach and remote user is plum. The command is

$ scp plum@IP address: ~/.bashrc destinationDirectory

4. How would you use **ssh** to run xterm on **plum** and show the display on the local system?

A: I can omit user@ from the command line if the host and remote user use the same username. Hence, I choose the same username on both systems and an X11 server running locally, the command is

$ ssh plum xterm

5. What problem can enabling compression present when you are using **ssh** to run remote **X** applications on a local display?

A: Enabling compression can speed up communication over a low-bandwidth connection and it can increase latency to an extent that might not be desirable for an X session forwarded over high-bandwidth connections. When using ssh to run remote x11 applications on a local display, the problem that enabling compression present would be that this creates a backup feature. It should lead the computer crash.

6. When you try to connect to a remote system using an OpenSSH client and you see a message warning you that the remote host identification has changed, what has happened? What should you do?

A: This message indicates that the fingerprint of the remote system has changed and is not the same as the local system remembers it. Check with the remote system’s administrator to find out if something changed. If everything is in order, remove the remote system’s key from the file specified in the error message and try logging in on the remote system again using **ssh**. I should use **ssh-keygen** with the **–R** option followed by the name of a host to remove a hashed entry. I will be subject to first-time authentication message (page 691) again as OpenSSH verifies that I am connecting to the correct system.

7. Which scp command would you use to copy your home directory from **plum** to the local system?

A: Assuming the host is zach and remote user is plum. The command is

$ scp plum@IP address:~/. zack@IP address:

8. Which single command could you give to log in as **root** on the remote system named **plum**, if **plum** has remote **root** logins disabled?

A: Assuming I have the same username on both systems, the following command logs in on plum as root:

$ ssh -t plum su –

Running this command, I must have user’s passwords and root’s. The su utility requires that its input come from standard input; the -t option allocates a pseudo-tty (terminal) to run su.

9. How could you use **ssh** to compare the contents of the **~/memos** directories on **plum** and the local system?

A: Assuming the host is zach and remote user is plum. The command is

$ssh zack@plum cat ~/memos | diff -u ~/memos

10. How would you use rsync with OpenSSH authentication to copy the **memos12** file from the working directory on the local system to your home directory on **plum**?

A: Assuming the host is zach and remote user is plum. The command is

$ rsync zack@IP address: memos12 plum@IP address:

How would you copy the **memos** directory from the working directory on the local system to your home directory on **plum** and cause rsync to display each file as it copied the file?

A: $ rsync -av zack@IP address: memos12 plum@IP address:

**CH 26 Apache(httpd): Setting up a web server**

1. What is Apache? Very basically, how does it work (i.e., what happens when you point a browser at a Web page)?

A: Apache is the most popular Web server on the Internet. It responds to requests from Web browsers, or clients, such as Firefox, Netscape, Iynx, elinks, and Internet Explorer. When you enter the address of a Web page in a Web browser’s location bar, the browser sends a request over the Internet to the Apache server at the address. In response, the server sends (serves) the requested content back to the browser. The browser then displays or plays the content, which might be a textual document, song, picture, video clip, or other information.

2. What is the function of the document root?

A: The root of the directory hierarchy that Apache serves content from is called the document root and is controlled by the DocumentRoot directive.

Where is it located by default?

A: By default it is located at **/var/www/html**.

How would you change the location of the document root?

A: This directory locates on the server maps to / so it appears to users who are browsing a Web site as the root directory.

3. How would you tell Apache that the content is in **/usr/local/www**?

A: In the Apache config file: **/etc/httpd/conf/httpd.conf** and I will specify DocumentRoot **/usr/local/www**

4. How would you instruct an Apache server to listen on port 81 instead of port 80?

A: Listen specifies the IP address and port that Apache listens for requests on. Hence, if I want to change port 80 to port 81, I just need to change the directive Listen 80 to Listen 81in the file, **httpd.conf.**

5. How would you enable Sam to publish web pages from his ~/webiste directory but not allow anyone else to publish to the web?

A: edit the directory, /**etc/httpd/conf/httpd.conf**:

UserDir website

UserDir disabled

UserDir enabled sam

6. Apache must be started with **root** privileges. Why?

A: By default, httpd listens on port 80, which is a privileged port. Only a process with root privileges can use privileged ports, so you must start Apache with root privileges.

Why does this action not present a security risk?

A: Starting Apache with root privileges does not pose a security risk because Apache uses child processes running as Apache to serve pages and the child processes (servers) run as nonprivileged users. The original **httpd** process running with root privileges remains but does not interact over the network.

7. What is the relationship between Apache and httpd?

A: Apache is the name of a server that serves HTTP and other content. The Apache daemon is named httpd because it is an HTTP server daemon. In reference to Apache, httpd refers to the Apache HyperText Transfer Protocol (HTTP) server program which handles the requests. Thus, both the terms are also used interchangeably.

8. What does the ServerName directive do?

A: The ServerName directive establishes a name for the server.

Which value can you use as a ServerName if you want to experiment with an Apache server locally (on the server system)?

A: If you do not need to access an Apache server from other systems, you can specify a ServerName of 127.0.0.1, the address of localhost.