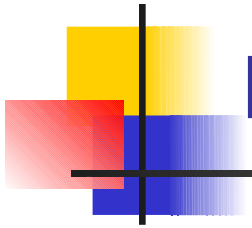
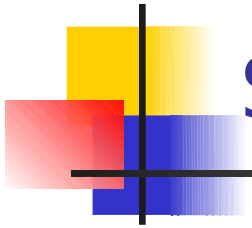
OPS235

Setup and Configure Secure Shell Services (ssh) Using Virtual Machines



Lab 7 - Topics

- **Establishing SSH Connection**
  - Install SSH
  - Configure SSH
  - SSH Public Key Authentication
  - scp, sftp
  - SSH Tunnelling
    - How to
    - Make SSH More Secure



SSH

- The concept of connecting computers via wide area networks is not new. In the Fall 1969, the forerunner to the Internet was developed by connecting 4 computer systems via communication lines.

- This lead to the development of network-based applications:
  - Telnet (1970)
  - FTP (1972)
  - Email Standard (using @ symbol - 1973)

SSH

- The problem with the Telnet and FTP applications is that they are not secure (at least the applications that were developed years ago).
- This means that Internet traffic is available for viewing and interpretations by other people (lurkers). This could pose a serious security risk – for example: account passwords.
- SSH (Secure Shell) is a method to allow secure transmission of data between two computer systems. This method uses public and private key cryptography initially theorized by Whitfield Diffy in the 70s.

SSH

- How to start ssh on all 3 Virtual Machines?
- How to establish ssh connection via Virtual Machines?
- How to establish ssh connection via Public Key Authentication
  - What is the purpose of this above method?
- How to use scp and sftp?

SSH – Tunnelling

- SSH Tunnelling allows secure communications among computer system, not only for text-based transactions, but also remote graphical applications.
- SSH Tunnelling opens up an encrypted channel (tunnel) via a ssh connection.
- Assuming you are located in the **centos1** virtual machine. What is the command using SSH tunnelling to run the **gedit** program on centos2, but display it in centos1?

SSH – Tunnelling

- SSH can be used to tunnel other types of traffic. For example, it can be used to bypass a firewall (iptables rule).

- How is this done?
  - Establish an SSH Tunnel on a local port of the remote machine. For example, here is the command to create a tunnel for accessing the World Wide Web for a remote host called “hostname”:
    - **ssh -L 20808:hostname:80 user@hostname**

- The above example assumes that incoming requests are blocked for port 80:
  - **iptables INPUT -p tcp s0/0 d0/0 –dport 80 DROP**

Making SSHd More Secure

Discuss the steps for making sshd more secure:

- More secure root passwords
- Edit **/etc/ssh/sshd_config**
  - Deny root login
  - Restrict user access
  - Change default port number
- iptables rules to reject old ssh port and accept new ssh port
- Use ssh command with -p option
- Monitor system logs (eg. **/var/log/secure**) to check for authorized access attempts.