Assignment 1 – Secure remote administration and firewalls

Part I 10%
Objective: To Study the concepts of remotely administering a server using ssh. You are to secure a Linux server by restricting remote root access by running a **separate sshd daemon**. Make the necessary changes to have the newly configured sshd daemon comply with following restrictions:

1. Daemon must start on all run levels, i.e. 2345
2. root should have remote access to this server using new sshd daemon and no others.
3. All others should be accessing the server using the existing sshd daemon; again root should not be able to access this sshd daemon.
4. Public-key authentication should be used for the root user
5. Feel free to add any configuration directives to further secure the ssh daemon

Part II 10%
Objective: To study the concepts ssh port forwarding.

You will be using ssh to port forward any port required for remote administration of a Linux server. You are to setup a gateway using ssh port forwarding facility. For example: setup an SMTP port forwarding on one instance of the CN8822 VM to act as an SMTP gateway for all internal machines.

Part III 10%
Objective: Firewall using IPTABLES

Firewall implementation using iptables. You are to setup the

appropriate iptables rules to accomplish the following:

1. Using the same VM running the newly configured sshd daemon from Part I; setup a default-deny policy to drop all inbound traffic.
2. Only allow inbound traffic to both sshd ports, port 22 for public access and privileged port for root access. Note: Privileged port is something you choose in Part I when new daemon was configured.
3. Only allow a trusted network or net-block to access the privileged sshd port.
4. Log all other dropped packets

Notes:

1. This assignment requires you to read the man pages and research how to setup multiple sshd daemons.
2. For all parts you are expected to list and explain all changes required to accomplish required tasks.
3. Report must adhere to the format of a formal report; disclaimer, cover page, table of contents, explanations and conclusions. For guidelines see: http://www.cn.ryerson.ca/discus/messages/871/1764.html?1225745536
4. Sample Disclaimer page provided in the next page.

Faculty of Engineering, Architecture and Science
Computer Networks Program

Course Number: CN8822

Course Title: Network Operating Systems

Semester/Year: W2012

Instructors:

Lab Assignment:

Assignment Title:

Submission Date:

Due Date:

Student Name:

Student ID:

Signature:

**By signing above you attest that you have contributed to this written lab report and confirm that all work you have contributed to this lab report is your own work. Any suspicion of copying or plagiarism in this work will result in an investigation of Academic Misconduct and may result in a "0" on the work, an "F" in the course, or possibly more severe penalties, as well as a Disciplinary Notice on your academic record under the Student Code of Academic Conduct, which can be found online at: www.ryerson.ca/senate/current/pol60.pdf.*