# Assignment 2: Securing system using IPTable firewall

## Due Week 8, Worth 25%

You are required to set up, configure, and test your firewall. You need to do research and reading to be able to complete this assignment.

You have to discuss the main uses, limitations, and possible security holes of your firewall and write it in your report. You should test that following packages are installed on your machines: Telnet, MySQL and Apache webserver. Start the services, and test that they are working prior to your experiments with the IPTables firewall. Include screenshots in your answers to show that the services are working and the output of your results to show that the requested filtering is performed.

**Important:**

***You need to save copies of all different configurations (for each part) that you have done. (You should include your firewall rules and the results (screenshots) in the report)***

**Configure your firewall to:**

1. Reject all incoming and outgoing **ping** packets.

2. Reject all incoming **telnet** packets and allow all outgoing **telnet** packets.

3. Reject all traffic coming to MySQL server.

4. Block incoming packets to the IP address of your virtual machine.

5. Allow packets inbound to port 80 (inbound) and reject packets going out (outbound) through port 80.

You then have to:

a. Discuss the advantages and disadvantages of firewalls with **iptables** and make suggestions to overcome the disadvantages in your report.

**Submission**

You should submit your report on the Moodle. The length of the report should be no longer than 10 pages.

# Scoring

|  |  |  |
| --- | --- | --- |
| **Question** | **Score** | **Description** |
| **Content** | | |
| 1 Ping service denial | 5 | Show that **ping** traffic is filtered |
| 2 Control telnet traffic | 10 | Show that the **telnet** service is working, incoming connections are rejected and outgoing connections are allowed |
| 3 Traffic to MySql | 10 | Show that the **Mysql** service is working, show that all traffic coming to **MySql** is rejected |
| 4 IP address access control | 10 | Demonstration of blocking traffic connection to your IP address of your virtual machine |
| 5 Control port 80 traffic | 10 | Show that **apache** service is working, show that inbound traffic to port 80 is allowed, but outbound traffic from port 80 is rejected |
| Subtotal: | **45** | Subtotal for content |
| **Presentation** |  |  |
| Experiment setup in Kali | 15 | Report should show the details how you have tested in parts: 1,2,3,4,5 with practical tests and/or with your gathered information |
| IPTable advantages and disadvantages | 15 | Include advantages and disadvantages of firewalls with **iptables** and make suggestions to overcome the disadvantages in your report. |
| Report is comprehensive | 15 | Does the report reflect an understanding of the use of the IPtables firewall? |
| Spelling, Grammar, Presentation, Style References | 10 | The report’s contents are appropriately written in English, with no spelling errors or grammar issues. The report is well presented, with diagrams, headings, tables and other visual aids. The report contains appropriate references and referencing style. |
| Subtotal: | **55** | Subtotal for presentation |
| Total: | **100** |  |
|  |  |  |