

ISEC2022-700-5115 Firewalls VPNS and Endpoints

Assignment 1 – A Basic Iptables Firewall

Preamble

The purpose of this in-class assignment is to construct a basic iptables firewall.

In this assignment, imagine that this is a firewall that is installed on a single server (whose ip or name is irrelevant to the solution) and that the firewall governs the actions of that server only. Therefore, there is no requirement (for example) to state the IP Destination address in rules that govern traffic coming into this server. The same is true for the Source Address of traffic outbound from this server.

Requirements

Complete the following tasks:

On an ubuntu linux VM create a script with an appropriate name of your choosing that will implement the following firewall rules in iptables.

Note: All of the following commands are to be issued from within your script.

1. Put comments at the top of your script containing:

- a. the filename of your script
- b. assignment number and title
- c. your name as author
- d. the original creation date of the script and the date of your last revision to the script
- e. make sure to label each so others will know what the information is

2. Start your script by flushing all previous firewall rules

3. Next in your script you are to list your current firewall rules but send the output to a file named [path]initialstate.log, where [path] can be anything of your choosing.

4. Define the following variables: (Hint: These ip addresses should only appear once in your script. In all other occurrences, the variable name is used)

- a. SERVER1 as 192.168.4.2
- b. TECHSUPPORT1 as 192.168.4.5
- c. UPDATESERVER as 192.168.4.7

5. Allow all traffic in and out of your loopback interface (hint: you need the -i for input & -o for output interfaces. The loopback interface is identified as "lo". (without the quotations of course)
6. Make your firewall stateful and allow incoming traffic for all ESTABLISHED and RELATED connections and allow outbound traffic for ESTABLISHED and NEW connections.
7. Allow incoming SSH traffic from TECHSUPPORT1.
8. Allow outgoing FTP traffic to SERVER1 and incoming FTP traffic from UPDATESERVER. Note: FTP uses more than one port.
9. Make the default policy for: INPUT DROP, OUTPUT ACCEPT and FORWARD DROP.
10. Save your firewall rules.
11. Next in your script you are to list (verbose) your current firewall rules but send the output to a file named [path]configuredstate.log, where [path] can be anything of your choosing.

Your submission will consist of the contents of your script file as well as the contents of the two output files (initialstate.log and configuredstate.log), **ALL IN A SINGLE WORD FILE..**

Submission Guidelines

Your assignment submission is to be uploaded to the Brightspace drop box on or before the due date.

You will create a document in MS Word for the content of your submission.

Your document must contain a separate title page containing the course code (ISEC), the course number (2022), The Assignment number (1) and title ("A Basic IP Tables Firewall") and your name.

The document is to be of professional quality including content, layout, font, grammar, spelling, overall appearance and structure. You should include a proper Section Title for each part of your submission (i.e. Script, Initial State, Configured State). Take care to make your work look neat and easily readable.

References are not required for original work, but if you include any then they **MUST** be properly cited in an acceptable APA format.

Document name (i.e. filename) **MUST** be of the format: YourLastName-YourFirstName@ISEC2022-As1

Rubric

This assignment is worth 20% of your final mark and it is scored out of 40 points using the following rubric.

Please note that a pass is 60% (24 points) and if all categories are "Condition Somewhat Met" then you can only score a maximum of 20 points and will therefore not receive a passing grade.

Neatness counts!

Rubric on following page...

Rubric	Condition Not Met	Condition Somewhat Met	Condition Met
Document Names and Comments are clear, complete and well formatted as required.	0	1 - 5	6 - 10
Each question and task is complete and correct.	0	1 - 12	13 - 24
Assignment submission shows obvious effort and care especially regarding original content.	0	1 - 3	4 - 6
Total Points available by column	0	20	40