CYBR 8410 – Distributed System Security – 2021 Spring

Lab 3 Part 2

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NUID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please follow the requirements and due date to submit your work.

**Lab Description**:

Students will learn how to create Linux firewall (Netfilter) rules using the iptables command line program. You need to answer the specified questions in the following lab content and steps, and submit your answers in a PDF or Word file.

During the lab, if anything is not clear to you, please contact the instructor.

**Lab Content and Steps:**

1. Reuse your virtual machine created in Lab 1
2. Start to get familiar with Netfilter and iptables by
   1. viewing the iptables manual, i.e., run "man iptables"
   2. searching Linux iptables online, for example, https://wiki.archlinux.org/index.php/iptables
3. Your virtual machine has an IP on the network. Let's explore the ways we can stop someone from finding or attacking it.
   1. List the current rules defined in all the default chains of the default firewall table.

Question 1: (10 pts)

1. What is your command? (2 pts)
2. What is the default table and what are the default chains of the default table? (4 pts)
3. What are the rules in those default chains? Explain your observation. (4 pts)
   1. Verify that you can send ICMP echo requests from your host OS to your virtual machine, and also verify that you can send ICMP echo requests from your virtual machine to an external server, e.g., [www.yahoo.com](http://www.yahoo.com)

Question 2: (10 pts)

What are your commands for these two tasks and what are the outputs of those commands?

* 1. Add firewall rules (using iptables) to your virtual machine to block both incoming and

outgoing ICMP echo requests.

Question 3: (20 pts)

1. What are your commands and what are the rules in the firewall tables after you run

your commands? (5 pts)

1. Verify the new added rules are working by pasting your verification commands and

outputs. (5 pts)

1. What commands can be used to delete your new added rules? You can verify the

commands can be successful. (5 pts)

1. If you stop and restart your EC2 instance, your new added rules will disappear.

Suggest and test a solution to address this issue, i.e., enabling firewall rules to

survive reboot. (5 pts)

* 1. Check open ports on your EC2 instance. (Hint: there are many ways to do this, e.g., you can run netstat with some special options)

Question 4: (5 pts)

What are those open TCP/UDP ports?

* 1. Execute sudo apt-get install openssh-server on your virtual machine to install an SSH server. Now you are able to connect to your virtual machine using SSH. Execute your command for Question 4 again and now you will see a port 22 is now listened by the SSH server.

There are different ways to hide SSH from attackers yet allow you to still login.

For example, assuming that your SSH daemon can accept requests from two ports: the

traditional port 22 and another hidden port 3000 (you need to change the configuration of

sshd to enable this additional port). Then you can use iptables to add firewall rules so that:

(a) requests coming to the port 22 can be accepted only from some specific IP addresses

(e.g., the public addresses of your home network)

(b) requests coming to the hidden port 3000 can be accepted from all IP addresses

(c) all requests coming to both the port 22 and port 3000 will be logged.

Question 5: (20 pts)

Either try the above example solution (you need to meet those three requiremens), or

suggest and try a better solution. Describe your experiment including: procedure (4 pts),

firewall rules (iptables commands and the content in the firewall table) (4 pts), verification

commands (4 pts), output (4 pts), and results (4 pts).

* 1. Suggest a way to prevent brute force attacks against SSH (Note: you can assume SSH port

22 is not hidden in this case. Hint, rate limiting is an acceptable solution).

Question 6: (20 pts)

Describe your experiment including: procedure (4 pts), firewall rules (iptables commands and

the content in the firewall table) (4 pts), verification commands (4 pts), output (4 pts), and results (4 pts).

* 1. Your virtual machine is still not secure enough based on your observation in the above step

(4). Please suggest and verify at least one more firewall solution to improve the security of

your virtual machine.

Question 7: (15 pts)

Describe your experiment including: procedure (3 pts), firewall rules (iptables commands and

the content in the firewall table) (3 pts), verification commands (3 pts), output (3 pts), and results (3 pts).