Configure Uncomplicated Firewall Policy in Ubuntu

|  |
| --- |
| Copyrights 2016-2017 Dr. Frank Xu, Bowie State University.  The lab manual is developed for teaching cybersecurity courses.  Comments and suggestions can be sent to wxu@bowiestate.edu |

**Introduction**

UFW, or Uncomplicated Firewall, is an interface to iptables that is geared towards simplifying the process of configuring a firewall. While iptables is a solid and flexible tool, it can be difficult for beginners to learn how to use it to properly configure a firewall. If you're looking to get started securing your network, and you're not sure which tool to use, UFW may be the right choice for you.

**Lab Environment**

1. We have created two accounts in the Seed Ubuntu. The instructions for installing Seed Ubuntu virtual image is here <http://www.cis.syr.edu/~wedu/seed/labs.html>. The usernames and passwords are listed in the following:
   * User ID: root, Password: seedubuntu.

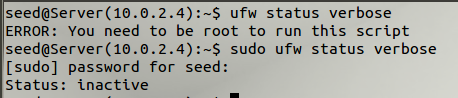
Note: Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command su to login to the root account.

* + User ID: seed, Password: dees

1. Clone the Seed Ubuntu virtual image.
   * Use the cloned virtual image as the attacker’s machine collecting the stolen cookies.
   * Configure the network of the cloned image as the same as the original image
   * Ping two Ubuntu systems each other to make sure they can communicate

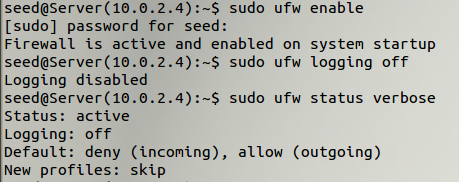
**Task 1: Check UFW Status**

1. Open a terminal in the first Seed Ubuntu virtual iamge
   1. You need to have root privilege
   2. By default, UFW is disabled



**Task 2: Enable UFW**

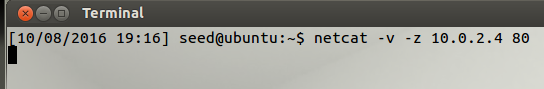
|  |
| --- |
| $ sudo ufw enable  $ sudo ufw logging off  $ sudo ufw status verbose |



1. Default policies

By default, UFW is set to deny all incoming connections and allow all outgoing connections. This means anyone trying to reach your server would not be able to connect, while any application within the server would be able to reach the outside world.

* 1. Test the default polices from the second Ubuntu virtual image by scanning the TCP port of the first Ubuntu virtual image



* 1. Questions:
     1. Describe your observation
     2. Describe the command
  2. The commands to set default policies manually

|  |
| --- |
| $ sudo ufw default deny incoming  $ sudo ufw default allow outgoing |

* 1. Disable firewall in the first Ubuntu virtual image



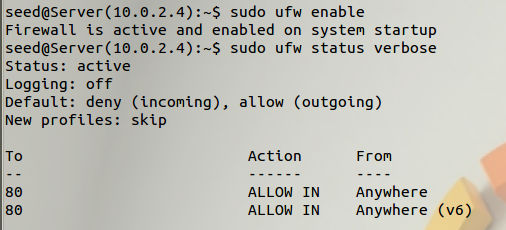
* 1. Question: Are you able to scan the port 80 from the second Ubuntu image?

**Task 3: Allow Http port 80 with Firewall Enabled**

1. Enable the first Ubuntu virtual image

|  |
| --- |
| $ sudo ufw enable  $ sudo ufw logging off  $ sudo ufw status verbose |

1. Allow Http connection



1. Question: Are you able to scan the port 80 from the second Ubuntu image?



**Task 4: Allow Specific IP Addresses**

When working with UFW, you can also specify IP addresses. For example, if you want to allow connections from a specific IP address, such as a work or home IP address of 15.15.15.51, you need to specify "from" then the IP address:

|  |
| --- |
| $ sudo ufw allow from 15.15.15.51 |

You can also specify a specific port that the IP address is allowed to connect to by adding "to any port" followed by the port number. For example, If you want to allow 15.15.15.51 to connect to port 22 (SSH), use this command:

|  |
| --- |
| $ sudo ufw allow from 15.15.15.51 to any port 22 |

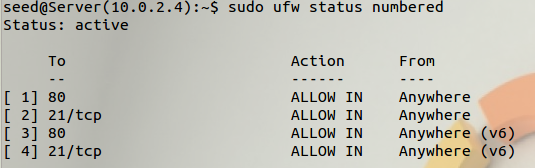
**Task 5: Deny Http Connections**

To write **deny** rules, you can use the commands that we described above except you need to replace "allow" with "deny".

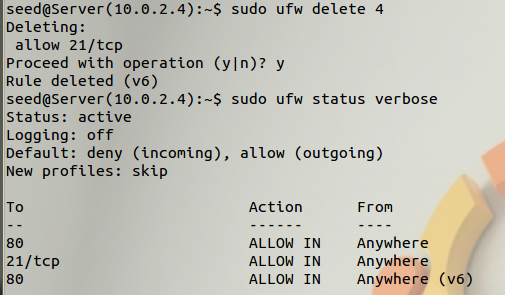
|  |
| --- |
| $ sudo ufw deny http |

**Task 6: Delete Rules**

1. Get a list of your firewall rules



1. Delete number TCP (number 4)



**Reference:**

* <https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-14-04>
* <https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf>
* https://www.youtube.com/watch?v=cscIe9fYKMU