**CY481 Network Security**

**HOS02 – Basic Firewall**

10/04/2020 Developed by Spencer (Yu Che) Liu

11/29/2023 Reviewed by Vaishnavi Mandage

01/11/2024 Updated by Asia Shvets

Center for Cybersecurity Innovation (C4Cyi)



**Before You Start**

* Version numbers may not match with the most current version at the time of writing. If given the option to choose between stable release (long-term support) or most recent, please choose the stable release rather than beta-testing version.
* This tutorial targets Windows users and MacOS users.
* There might be subtle discrepancies along the steps. Please use your best judgement while going through this cookbook style tutorial to complete each step.
* For your working directory, use your course number. This tutorial may use a different course number as an example.
* The directory path shown in screenshots may be different from yours.
* If you are not sure what to do or confused with any steps:
  + Consult the resources listed below.
  + If you cannot solve the problem after a few tries, ask a TA for help.

**Learning Outcomes**

* Understand basic commands to configure firewall.
* Understand how to block incoming traffic.
* Understand how to allow incoming traffic.

**Resources**

* Linux main page
* <https://zcom.tech/configure-iptables-linux.html/#:~:text=%20IPTables%20Tutorial%3A%20Chains%20%201%20INPUT%20%E2%80%93,It%20is%20important%20to%20note%20that...%20More%20>
* <https://phoenixnap.com/kb/iptables-tutorial-linux-firewall>

## **KNOW YOUR NETWORK**

Most of the time when network systems fail or are vulnerable, diagnosing and resolving the issues help detecting problems and fixing them before things get out of hand. In this Hands-On practice we will explore some Linux commands to understand what and how these commands can help to analyze and monitor for network security.

## **This HOS covers:**

* **Check your network**
* **ping**
* **Iptables**
* **firewall**

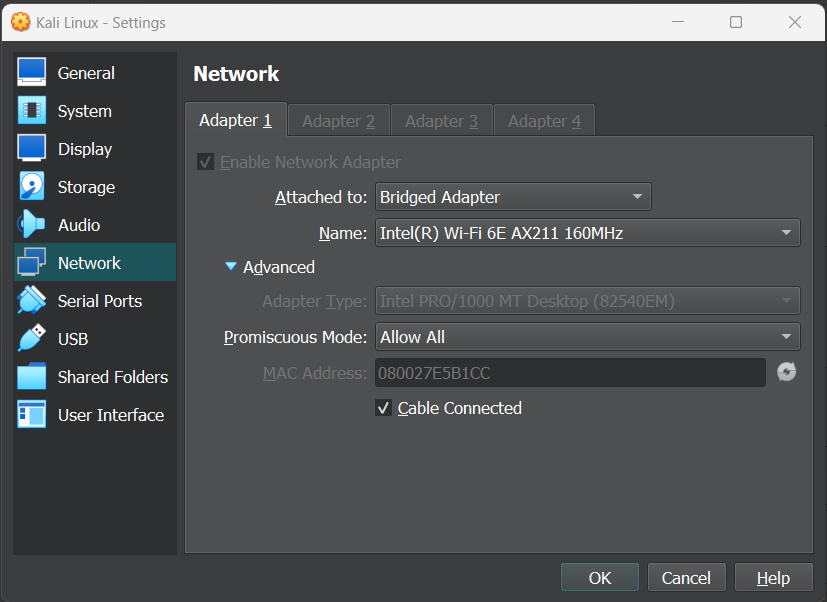
## **ping**

## The ping command sends echo requests to a designated machine to determine if communication is possible. The syntax is ping [options] targetname/address. The options include items such as name resolution, how many pings, data size, TTL counts, and more. See the firewall rule of the Kali Linux.

ping command can do:

* Test network connectivity.
* Test network interface card.
* Test DNS name resolution issues.

1. Make sure your VM is connected to the internet. Go to Virtual box, then Kali Linux Settings. Select Network and then follow the screenshot below:



Click OK.

Reference: <https://www.youtube.com/watch?v=u8BGQ5fl3Yg>

2. Go to Kali Linux. Type the following command: ping [www.cityu.edu](http://www.cityu.edu).

If you receive the message below, which means CityU website server is working and sending echo result back.

A screen shot of a computer

Description automatically generated

3. ping [www.cityu.edu](http://www.cityu.edu), if you don’t receive a message below, which means the CityU server is not working, or the firewall blocks the traffic.

A computer screen shot of a computer screen

Description automatically generated

## **Iptables command**

iptables is a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall, implemented as different Netfilter modules. The filters are organized in different tables, which contain chains of rules for how to treat network traffic packets.

## See the firewall rule of the kali Linux.

A screenshot of a computer

Description automatically generated

Explanation:

* Target: Each rule specifies what to do with a packet that matches.
* Chain: chain is a list of rules which can match a set of packets.
  + INPUT – The INPUT chain is the rule that controls incoming packets. Here you can block or allow new connections. You can do this based on port, protocol, and source IP address.
  + FORWARD – The FORWARD chain filters incoming packets that are being forwarded to a different end location. You are unlikely to use this chain unless you are routing or looking for forwarding specifically.
  + OUTPUT – The OUTPUT chain is used to manage outgoing packets and connections. It is important to note that if you ping an external host then the input chain will be used to return the data back to you.

Options:

* **-L** --list: List all rules in the selected chain.

1. Block the incoming traffic.

* sudo iptables -P INPUT DROP
* sudo iptables --list

Options:

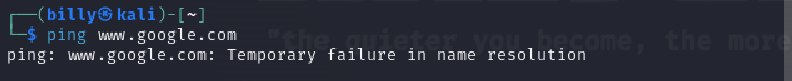
* + **-P**: Set the policy for the built-in (non-user-defined) chain to the given target. The policy target must be either ACCEPT or DROP.
  + **-L**: List all rules in the selected chain. If no chain is selected, all chains are listed.

A screenshot of a computer

Description automatically generated

1. Use ping command to check if the traffic comes in. You will get the error message that [www.google.com](http://www.google.com): Temporary failure in name resolution.

* ping [www.google.com](http://www.google.com)

\_

1. Allow INPUT traffic and use ping command to see if there is any difference.

* sudo iptables -P INPUT ACCEPT
* ping [www.google.com](http://www.google.com)

A computer screen with white text

Description automatically generated

**CHALLENGE**

Capture the screenshots to the submission doc.