

Lab Assignment 4 - Stopping Fires with Walls

CSEC 2324 - Network Security
Lab Guide v1.0

William Cox, M.S.
Visiting Assistant Professor
wcox@ualr.edu or wcox@uaptc.edu

January 2023




Contents

Lab Guide Instructions	4
Lab File Formatting	4
Markdown How-To	5
Suggested Setup	5
Lab Assignment 4 - Stopping Fires with Walls	5
Overview	5
Lab Artifacts	6
Lab Software	6
Part 1: Host-Based Firewall	6
Allowing traffic	6
Denying Traffic	7
Forwarding Traffic	8
Clearing IPTABLES	8
IPTables Questions	9

Lab Guide Instructions

The labs included in this guide will help you understand the principles of Network Security.

When you see a  you will be required to take a screenshot of that step.

Included is the requirement for a Lab Report file.

Follow the formatting instructions for full credit.

Note: Using Markdown is only required for the first lab.

Lab File Formatting

When completing your labs please follow these instructions.

1. All Labs created using Markdown & will use the Eisvogel template. Labs files created in another word processing program will use Times New Roman, 12 Font, Double Space.
Get Eisvogel here: <https://github.com/Wandmalfarbe/pandoc-latex-template>
2. Create a title page with the following details:
 1. Title of the Lab
 2. Class Name
 3. Your name
 4. Date
3. Section 2 will have all screenshots and questions/answers for the lab.
 1. Each question must be listed with its question number.
 2. Answers will be indented on the next line and start with an "a."
 3. If answer includes a picture, make sure picture is big enough for your instructor to interpret, but not too big to distract from the quality of your work.
4. Section 3 will be labeled Reflection.
 1. This is where you add any reflections needed.
 2. Make sure to quote your sources with parenthetical citations.
 3. Do not use quotes, but instead rewrite the quote in your own words. *Remember to still give credit to the author.*
5. Section 4 will be References
 1. All references should be in alphabetical order
 2. Use either APA or IEEE formatting

Markdown How-To

Below you will find a quick reference on how to use Markdown. This is not all inclusive and you may need to research steps that are particular to your situation. IE. Operating System, IDE, etc...

Suggested Setup

(You don't need to follow if you know Markdown)

1. Download and install following programs:
 1. VSCode Download
 2. Pandoc Install Instructions **Note: make sure to install all of the required dependencies**
 3. Eisvogel Template Download
2. Once you have downloaded and installed the required applications, you will need to set up your template and environments.
 1. VSCode Setup - Install following extensions:
 1. Markdown All in One, Author: Yu Zhang
 2. Dictionary Completion, Author: Yu Zhang
 3. markdownlint, Author: David Anson
 2. Setup Pandoc template Eisvogel Install Instructions
3. Basic Markdown syntax can be found at Markdown Guide
4. Convert Markdown to PDF syntax
 1. Open terminal and navigate to your markdown location
 2. Execute the following command replacing the file names with your information.

```
1 pandoc filename.md -o filename.pdf --from markdown --template  
   eisvogel --listings
```

Lab Assignment 4 - Stopping Fires with Walls

Overview

This lab will introduce you to Host and Network Firewalls. Don't just go through the motions in this lab, but try to understand what you are doing and how you could defend against these attacks.

Lab Artifacts

Build a Lab report file with the requested answers or screenshots presented in this lab. Follow the Lab file format found in the beginning of the Lab Guide Manual.

Lab Software

Programs tcpdump, Wireshark, IPTables

Operating System: Linux


Terminal Emulator: bash, shell, zsh, csh

Environment Cyber Arena

Sudo Password CSEC2324_Student!

Part 1: Host-Based Firewall

Allowing traffic

1. Log into the Cyber Arena
2. Select CSEC2324 Workout
3. List the existing iptables rules: 

```
1 iptables -L
```

This will display the current iptables rules in the following format:

```
1 Chain INPUT (policy ACCEPT)
2 target      prot opt source                destination
3
4 Chain FORWARD (policy ACCEPT)
5 target      prot opt source                destination
6
7 Chain OUTPUT (policy ACCEPT)
8 target      prot opt source                destination
```

4. Allow all outgoing FTP traffic from IP address 172.16.0.254/24: 


```
1 iptables -A OUTPUT -p tcp --sport 21 -d 172.16.0.254/24 -j ACCEPT
```

This will add a new rule to the OUTPUT chain that allows outgoing TCP packets with a source port of 21 (FTP) to the IP address range 172.16.0.254/24.

5. Save the iptables rules: 


```
1 iptables-save > /etc/iptables/rules.v4
```

This will save the iptables rules to the file /etc/iptables/rules.v4, which will be automatically loaded the next time the system boots.

6. To verify that the new iptables rule is in place, you can list the rules again using the iptables -L command. The new rule should be listed in the OUTPUT chain. 

Remember to always be careful when modifying iptables rules, as incorrect or malicious rules can disrupt network connectivity and expose your system to security risks. Make sure to thoroughly test your rules and ensure that they are working as intended before saving them.


Denying Traffic

1. Log into the Cyber Arena
2. Select CSEC2324 Workout
3. List the existing iptables rules: 

```
1 iptables -L
```

This will display the current iptables rules in the following format:

```
1 Chain INPUT (policy ACCEPT)
2 target     prot opt source                destination
3
4 Chain FORWARD (policy ACCEPT)
5 target     prot opt source                destination
6
7 Chain OUTPUT (policy ACCEPT)
8 target     prot opt source                destination
```

4. Deny all outgoing Telnet traffic from IP address 172.16.0.254/24: 


```
1 iptables -A OUTPUT -p tcp --sport 23 -d 172.16.0.254/24 -j DROP
```

This will add a new rule to the OUTPUT chain that denies outgoing TCP packets with a source port of 23 (Telnet) to the IP address range 172.16.0.254/24.


5. Save the iptables rules: 

```
1 iptables-save > /etc/iptables/rules.v4
```

This will save the iptables rules to the file /etc/iptables/rules.v4, which will be automatically loaded the next time the system boots.

6. To verify that the new iptables rule is in place, you can list the rules again using the iptables -L command. The new rule should be listed in the OUTPUT chain. 

Forwarding Traffic


1. Log into the Cyber Arena
2. Select CSEC2324 Workout
3. List the existing iptables rules: 

```
1 iptables -L
```

4. Enable IP forwarding:

```
1 echo 1 > /proc/sys/net/ipv4/ip_forward
```

This will enable IP forwarding on the system, allowing it to forward packets between different networks.

5. Forward all incoming traffic to IP address 172.16.0.254/24: 


```
1 iptables -A FORWARD -d 172.16.0.254/24 -j ACCEPT
```

This will add a new rule to the FORWARD chain that allows all incoming packets to be forwarded to the IP address range 172.16.0.254/24.

6. Save the iptables rules: 

```
1 iptables-save > /etc/iptables/rules.v4
```

This will save the iptables rules to the file /etc/iptables/rules.v4, which will be automatically loaded the next time the system boots.


7. To verify that the new iptables rule is in place, you can list the rules again using the iptables -L command. 

The new rule should be listed in the FORWARD chain.

Clearing IPTABLES

1. Log into the Cyber Arena

2. Select CSEC2324 Workout

3. List the existing iptables rules: 

```
1 iptables -L
```

4. Flush (clear) all iptables rules:

```
1 iptables -F
```

This will delete all rules in all chains and reset the policy to ACCEPT for all chains.

5. Save the iptables rules:

```
1 iptables-save > /etc/iptables/rules.v4
```

This will save the iptables rules to the file /etc/iptables/rules.v4, which will be automatically loaded the next time the system boots.

6. To verify that the iptables rules have been cleared, you can list the rules again using the iptables -L command. The list should be empty, indicating that there are no rules in place.

IPTables Questions

Answer the following questions in detail and add them to your reflections.

1. What is iptables and what is it used for?
2. How do you list the existing iptables rules on a system?
3. How do you add a new iptables rule to block all incoming traffic from a specific IP address?
4. How do you add a new iptables rule to allow all incoming traffic to a specific port?
5. How do you delete an iptables rule?
6. How do you flush (clear) all iptables rules?
7. What is the difference between the INPUT, FORWARD, and OUTPUT chains in iptables?
8. What is the difference between the -A and -I options in iptables?