Lab 7 - Proxychains and Chill: Navigating the Interwebs in Stealth Mode

CSEC 2324 - Network Security Lab Guide v1.0

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

January 2023

Cybersecurity

UA LITTLE ROCK | Department of Computer Science

Contents

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 note 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 temaplate Eisogel 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.

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

Lab Assignment 7 - Proxychains and Chill: Navigating the Interwebs in Stealth Mode

Overview

This lab will teach you about different ways to protect your data and identity. Don't just go through the motions in this lab, but try to understand what you are doing and how your 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 proxychains, Tor, SSH **Operating System:** Linux, Mac, Windows **Terminal Emulator:** bash, powershell, zsh, csh
Environment Cyber Arena
Sudo Password CSEC2324_Student!

Part 1: Create an SSH Key

Windows

To generate an SSH key using PowerShell, you can use the built-in New-SSHSession command.

1. Open PowerShell on your Windows machine.
2. Run the following command to generate a new SSH key: 📷

```
ssh-keygen
```

3. Press Enter to use the default location and file name for the key.
4. Enter a passphrase (this is optional but highly recommended).

```
PS C:\Users\Student> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Student/.ssh/id_rsa):
Created directory 'C:\Users\Student/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Student/.ssh/id_rsa.
Your public key has been saved in C:\Users\Christopher/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:/mjkrJOQbRzCAwlSPYVBNcuxntm/Ms5/MMC15dCRrMc christopher@Christopher-Win10-VM-01
The key's randomart image is:
+---[RSA 2048]----+
|oo.+o==    o.o   |
|. o +. =  o =    |
|   o .+. . B     |
|    +..+o o E    |
|     *+.S. .     |
|    o +...o      |
|     o =. .o     |
|      o.*o ..    |
|      .=+++.     |
+----[SHA256]-----+
PS C:\Users\Student>
```

5. Next, you will need start a new workout on CyberArena

   1. Log into the CSEC2324 workout
   2. Open the Web browser and Google “whats my ip”
   3. Annotate your public IP

6. From your local host, use the following command to add the public key to the authorized_keys file on the remote server:

```
ssh-copy-id -i [file_path\student.pub] student@[IP from step 5]
```

6. To check if the key is added successfully, you can use the following command: 📷

```
ssh -T [student]@[IP from step 5]
```

Note: If you are using PowerShell on Windows, you may need to install OpenSSH and add the OpenSSH executable files to your PATH environment variable before you can run the ssh-keygen and ssh-copy-id commands.

Mac/Linux

1. Open the Terminal on your Mac or Linux machine.
2. Run the following command to generate a new SSH key: 📷

```
ssh-keygen
```

3. Press Enter to use the default location and file name for the key.
4. Enter a passphrase (this is optional but highly recommended).
5. Next, you will need start a new workout on CyberArena
    1. Log into the CSEC2324 workout
    2. Open the Web browser and Google “whats my ip”
    3. Annotate your public IP
6. Use the following command to add the public key to the authorized_keys file on the remote server:

```
ssh-copy-id [student]@[IP from Step 5]
```

7. To check if the key is added successfully, you can use the following command 📷

```
ssh -T [username]@[remote host]
```

Note: If you don’t specify a file name and location while creating the key, it will be saved in ~/.ssh/id_rsa for private key and ~/.ssh/id_rsa.pub for public key.

Part 2: Tunneling with SSH

Windows

1. Open Powershell
2. Create an SSH tunnel with the following command 📷

```
ssh -D [local port] -f -C -q -N [student]@[remote host]
```

- “-D [local port]” specifies the local port to use for the tunnel
- “-f” runs ssh in the background
- “-C” enables compression
- “-q” reduces verbosity
- “-N” do not execute a remote command.

3. Configure your web browser to use a SOCKS proxy on the specified local port. 📷
4. Test that the tunnel is working properly
    1. Go to google on your host
    2. Type: whats my ip 📷
    3. Annotate the IP address
5. Stop the Tunnel with the following command:

```
Stop-SSHSession -ComputerName [remote host]
```

6. Open your Web browser
7. Go back to Google and type "whats my ip" 📷

Note: *Some web browsers have a built-in proxy configuration, while others may require additional software such as FoxyProxy.*

Linux/Mac

1. Open your terminal
2. Create an SSH tunnel with the following command: 📷

```
ssh -f -N -M -S /tmp/sshtunnel -D 1080 student@[remote IP] -p22
```

- "-D [local port]" specifies the local port to use for the tunnel
- "-f" runs ssh in the background
- "-M" places the ssh client into "master" mode
- "-N" do not execute a remote command.
- "-p" Port to connect to on the remote host
- "-S" Specifies the location of a control socket for connection sharing

3. Configure your web browser to use a SOCKS proxy on the specified local port. 📷
4. Test that the tunnel is working properly
    1. Go to google on your host
    2. Type: whats my ip 📷
    3. Annotate the IP address
5. Close your Web browser
6. Stop the Tunnel with the following command:

```
ssh -S /tmp/sshtunnel -O exit student@3[remote IP] -p22
```

6. Disable the proxy settings in your browser.
7. Open your Web browser
8. Go back to Google and type "whats my ip" 📷

Part 3: Another way to be Anonymous

In this exercise, you will research how to setup Tor and a Proxy service on your host.

References

Tor: https://community.torproject.org/onion-services/setup/install/ **Windows Proxy settings:** https://bitstobytes.org/tor **Linux:** https://geekflare.com/anonymize-linux-traffic/ **Mac:** https://dev.to/procode/anonymise-yourself-how-to-set-up-tor-in-mac-in-the-terminal-noobsec-series-pm6

ProxyChains is a tool that allows network connections to be made through a chain of proxy servers. It is often used to anonymize Internet connections and to bypass network restrictions or censorship. The tool can be configured to use a specific proxy for different types of connections, or to rotate through a list of proxies for added anonymity.

Tor (The Onion Router) is a free and open-source network that is designed to allow users to browse the internet anonymously and securely. It works by routing internet traffic through a network of volunteer-run servers (known as "nodes" or "relays") that are distributed around the world. Each time a user's traffic passes through a relay, the relay encrypts and wraps the traffic in multiple layers of encryption (hence the name "onion routing"). This makes it difficult for anyone monitoring the traffic to trace it back to the original user.

1. Install Tor (terminal/commandline/pwoershell)
2. Install Proxychains
3. In your Reflections write a step by step guide for the setup and use of Tor and the proxy service. Include the following:
    1. Detailed commands
    2. Associated Pictures
    3. References
    4. Proof that it is working
    5. Extra credit for completing in Markdown