CS 489/698 Assignment 4

TA: Ruizhe Wang (ruizhe.wang@uwaterloo.ca)

Office hours:
Thursday, Aug. 3rd 2:00 pm - 3:00 pm, DC 3333;
Tuesday, Aug. 8th 2:00 pm - 3:00 pm, DC 3333;

Due date: Aug. 11, 2023

Network Security

We briefly talked about network security in the lecture on network security. Given that network devices are common attack targets, let's give it a closer examination in this assignment. In particular, let's learn this concept by

1. [**5 * 2 pts**] breaking a network device,
2. [**5 * 1 pts**] improving the security of a network device.

Mission Description

Mako Reactors are massive structures designed and built by the **Shinra Electric Power Company (shinra.co.jp)**. These reactors extract Mako energy, a form of spiritual life energy, directly from the Lifestream. Mako energy is then processed and used as a power source, providing electricity to cities and facilitating advanced technology, including Shinra's military equipment.

Shinra's Mako harvesting damages the planet, causing it to slowly die. You are devoted to destroying the Mako Reactors as an act of rebellion against Shinra and an attempt to halt their exploitation of the Lifestream. The mission is fraught with danger, as you have to bypass Shinra's security systems and face off against the company's defensive measures – robotic enemies.

Now, eventually, you find yourself standing before the final Mako Reactor, its towering structure bathed in an eerie, luminescent glow. Your final mission, as critical as it is dangerous, is to bypass the guards, elite members of Shinra's security force, without raising the alarm. Each movement you make needs to be calculated and precise, every step a testament to your training and instinct. Stealth is your best weapon here, the shadows are your only allies.

The area is heavily fortified, monitored by advanced surveillance systems, and populated by both human personnel and robotic guards, their eyes unblinking, ever vigilant. The Shinra insignia, a glaring, omnipresent reminder of the corporation's stranglehold over the world, is emblazoned everywhere you look.

Upon successfully navigating past the guards, your next task is to open the gate to the reactor. The control panel is a labyrinth of levers and buttons, a testament to Shinra's technological prowess. It's a puzzle that you need to solve quickly and accurately, your fingers flying over the controls, guided by the information provided by your comrades – or possibly not, if you are brilliant enough to compromise the system.

Once the gate opens, the reactor's core lies exposed, a pulsating heart of Mako energy. The sight is almost hypnotic, the bright green energy humming with the life force of the planet. It is here that you'll set the charges, a blow aimed straight at the heart of Shinra's operations. It's a high-stakes gambit, a crucial step in your fight to save the planet, and everything rests on your shoulders.

Important Notice

Hacking our database is out of the scope of this assignment.

Environment Setup

You need to do the whole assignment in the Firefox browser with socks proxy through the *ugster*71*b* computer. You need to be either on campus or connected to the university VPN.

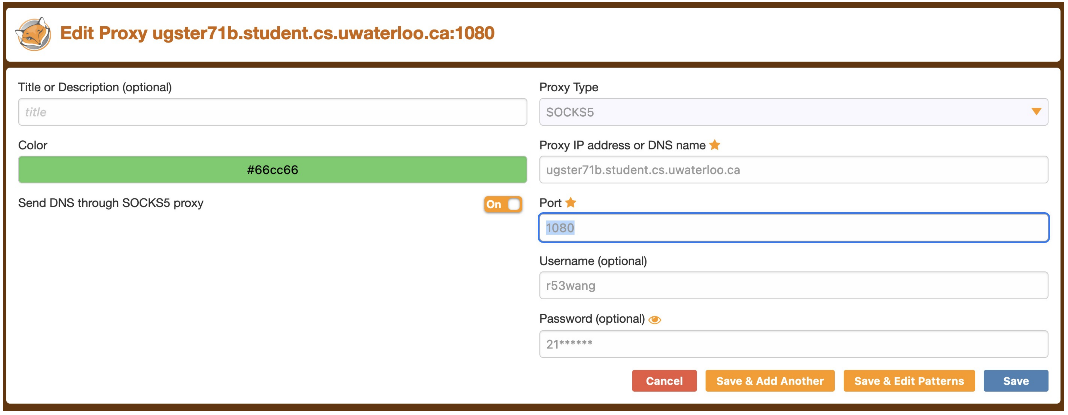
1. If you do not have Firefox installed, download and install the latest version of the Firefox Browser.

2. Open http://ugster71b.student.cs.uwaterloo.ca/ in Firefox. An error page should show up with **error code 404**.

3. Install any addon that supports authenticated **SOCKS V5**. We recommend FoxyProxy.

4. Open the addon and create a new proxy with the following configurations:

   - **Proxy Type**: SOCKS5
   - **Proxy IP address or DNS name**: ugster71b.student.cs.uwaterloo.ca
   - **Port**: 1080
   - **Username**: your_login
   - **Password**: your_student_id



Edit Proxy ugster71b.student.cs.uwaterloo.ca:1080

Title or Description (optional): title

Color: #66cc66

Send DNS through SOCKS5 proxy: On

Proxy Type: SOCKS5

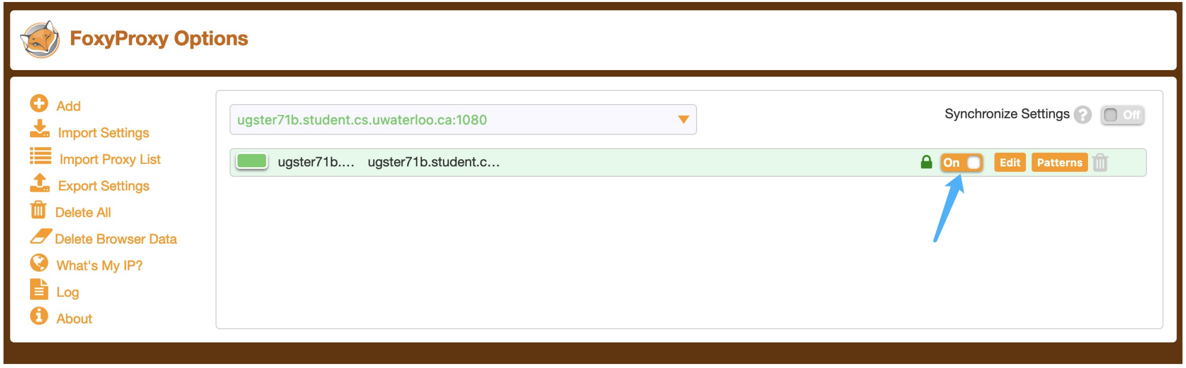
Proxy IP address or DNS name: ugster71b.student.cs.uwaterloo.ca

Port: 1080

Username (optional): r53wang

Password (optional): 21******

5. Save your proxy and turn it on



FoxyProxy Options

ugster71b.student.cs.uwaterloo.ca:1080

Synchronize Settings: Off

ugster71b.... ugster71b.student.c... On

6. Open http://ugster71b.student.cs.uwaterloo.ca/ again in Firefox. A different error page will show up stating that you are **Unable to connect**

7. Open 143.132.44.55:80. Register with your UWaterloo Login and choose a password **DIFFERENT** from your UWaterloo password. **You will lose 10 pts if we find you use your UWaterloo password.**

8. Login to your account, and you shall start doing the assignment.

Do not have your classmates logging in to their accounts on your personal devices.

Shodan

The (fake) Shodan search engine – accessible at 8.223.1.109:8647 – provides a subset of the functionality of the real shodan.io search engine. We recommend you familiarize yourself with Shodan first. There are many tutorials on the web that explain shodan search syntax. However, our minimal Shodan search engine only supports limited operations.

The search functionality works as follows:

- A search query is made up of tokens separated by a semicolon (the character ';').
- Each token specifies an AND condition for the search (so the results are at the intersection of the sets matched by the queries).
- Each token is constructed using the equal sign (the character '=') that connect a field name and a field value.
- If a filter value contains white spaces, enclose it either in single or double quotes.
- The list of fields you can filter on are as follows (refer to the Shodan documentation on what they mean)
  - hostname
  - city
  - port
  - ip_str
  - org
  - isp
  - city
  - longitude
  - latitude
  - postal_code
  - country_name
  - transport

For instance, to find all devices listening at port 80, located in the United States, you can use the query:

port=80;country_name="United States"

Grading Schema and Instruction to Deliverables

In this assignment, you are required to compromise five devices. You can check your progress at 143.132.44.55:80\gallery. You will earn two points for compromising each of the devices and will earn one point for giving one or two simple advice about improving its security. Submit your advice via the Assignment 4 **quiz** in LEARN.

Hints

Upload a File

file.io provides one-time file upload and download services for free. An uploaded file can be requested directly with the corresponding link provided at the time the file is uploaded.

Send a Request

The following script gives an example of making a request in the Firefox terminal

```
var  json = {
  url: "https://example.com"
}

var xhr = new XMLHttpRequest();
xhr.open("POST", "http://ip:port/path");
xhr.setRequestHeader("Content-Type", "application/json; charset=UTF-8")

var body = JSON.stringify(json);
xhr.onload = () => {
  console.log(`${xhr.response}`);
};
xhr.send(body);
```

Acknowledgement

This assignment is inspired by homework 5 of CS 642 at the University of Wisconsin-Madison. We used ChatGPT and DALL·E (New Bing) to generate all figures and most story scripts. The background of this assignment is derived from the world of Final Fantasy VII Remake. This assignment is made possible with multiple open-source projects. To maximize the learning procedure, their names are not going to be disclosed.