**Step 1: Clone the Phishing Lab Repository**

1. Open a terminal on your Linux machine.
2. Install Git if it's not already installed using this code
   * sudo apt update
   * sudo apt install git
3. Clone the Phishing Lab repository by running the following command:
   * git clone https://github.com/Abdi-Ahmed1/Phishing-Attacks.git

**Step 2: Install Dependencies**

1. Ensure that you have the necessary dependencies installed by running the following command:
   * sudo apt-get install php wget unzip curl
2. Navigate to the **Phishing-Attacks** directory:
   * cd Phishing-Attacks
3. Run the installation script to install the required dependencies:
   * ./phishing\_script.sh --install

**Step 3: Configure Ngrok**

1. Open a new terminal window.
2. Download Ngrok from the official website: [Ngrok Website](https://ngrok.com/).
3. Extract the downloaded Ngrok package to a directory of your choice.
4. Authenticate your Ngrok account by running the following command in the Ngrok directory and entering your authentication token when prompted:
   * ./ngrok authtoken [your-auth-token]

**Step 4: Start the Phishing Server**

1. In the terminal, navigate to the root directory of the cloned repository.
2. Start the phishing server by running the following command:
   * chmod +x phishing\_script.sh
   * ./ phishing\_script.sh
3. The script will prompt you to select a phishing page template. Enter the corresponding number for your chosen template.

**Step 5: Start a Tunnel with Ngrok**

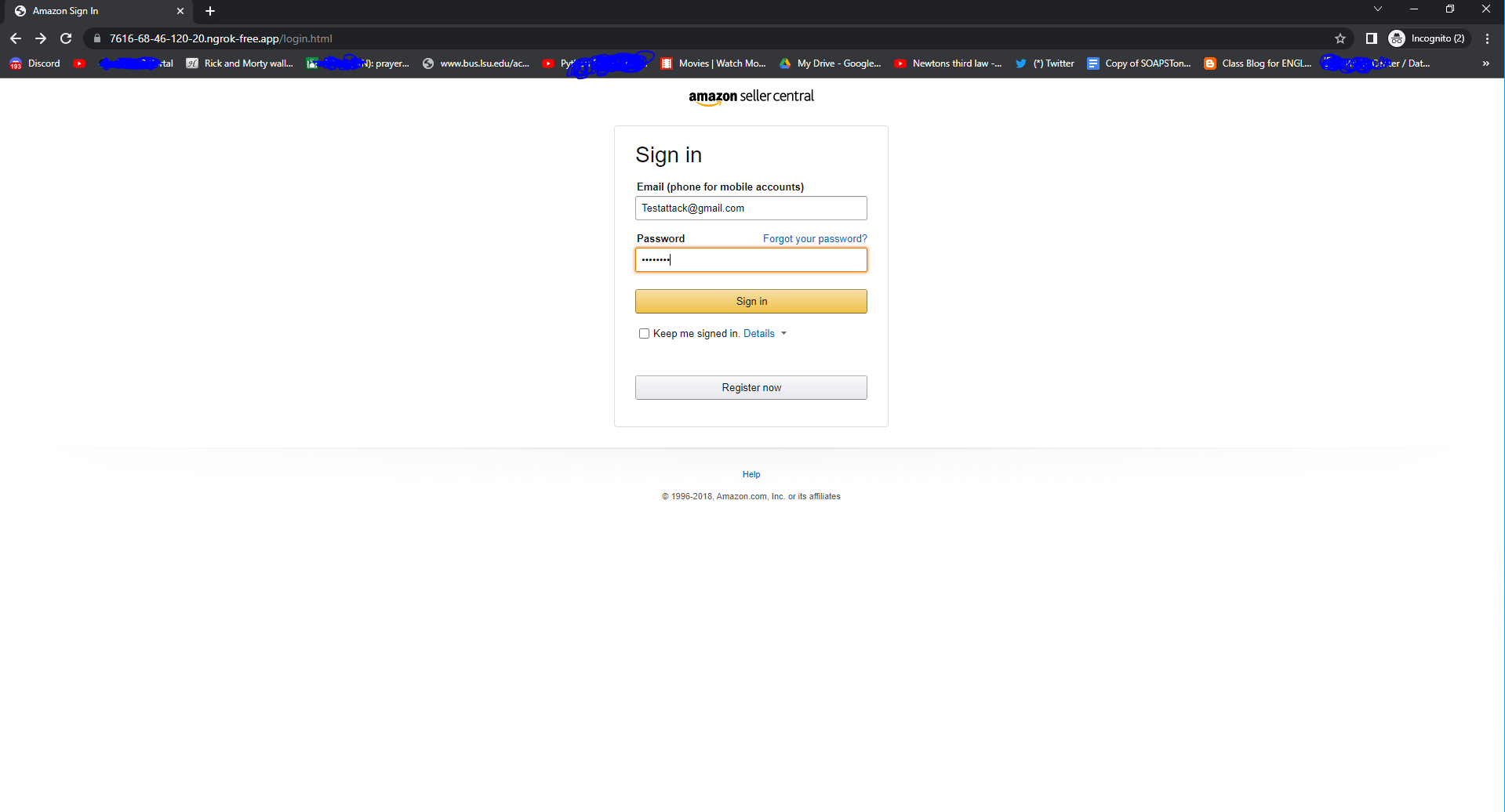
1. In the Ngrok directory, start a tunnel to your local phishing server by running the following command:
   * ./ ngrok http 3333

Note: Replace **3333** with the port number specified by the Phishing Lab script if it's different.

1. Ngrok will generate a public URL (e.g., **https://random-subdomain.ngrok.io**) that will forward traffic to your local phishing server.

**Step 6: Execute the Phishing Attack**

1. Copy the Ngrok-generated URL (e.g., **https://random-subdomain.ngrok.io**).
2. Share the URL with the target you want to perform the phishing attack on.
3. Monitor the terminal running the Phishing Lab script for incoming connections and captured credentials.

****