Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

Lab 5.2.8: Hardening a pfSense Security Appliance

From TestOut CompTIA Security+ Course

In this lab I will be hardening a pfSense security appliance within a hypothetical organization by changing the default credentials, which is an industry best practice.

The scenario for this lab is as follows:

"You work as the IT security administrator for a small corporate network. You need to secure access to your pfSense appliance, which is still configured with the default user settings.

In this lab, your task is to:

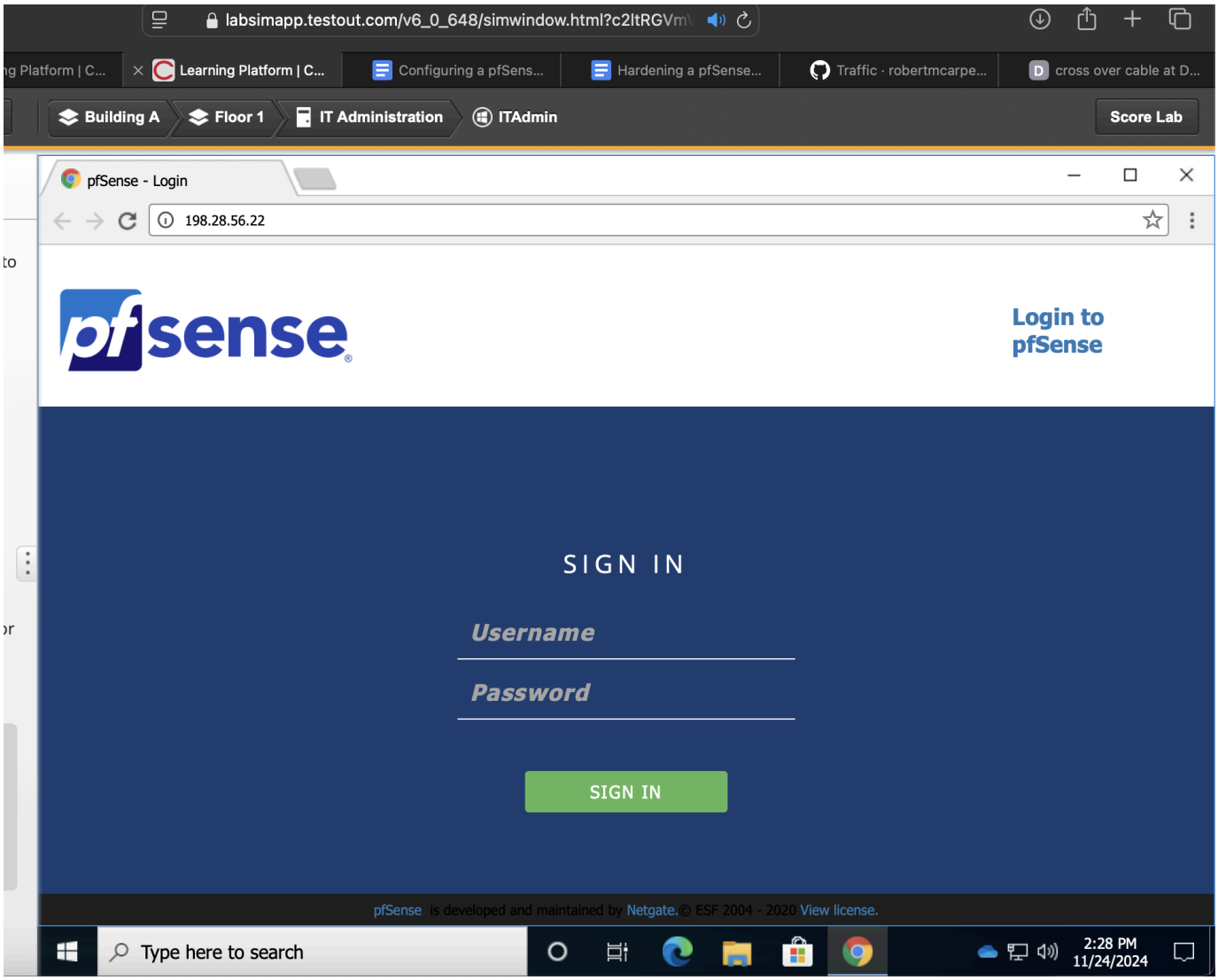
- **Change the password for the default pfSense account from P@ssw0rd to 1w0rm4b8.**
- **Create a new administrative user with the following parameters:**
  - **Username: zolsen**
  - **Password: St@yout!**
  - **Full Name: Zoey Olsen**
  - **Group Membership: admins**
- **Set a session timeout of 15 minutes for pfSense.**
- **Disable the webConfigurator anti-lockout rule for HTTP.**

Access the pfSense management console through Google Chrome using: http://198.28.56.22

- **Default username: admin**
- **Password: P@ssw0rd"**

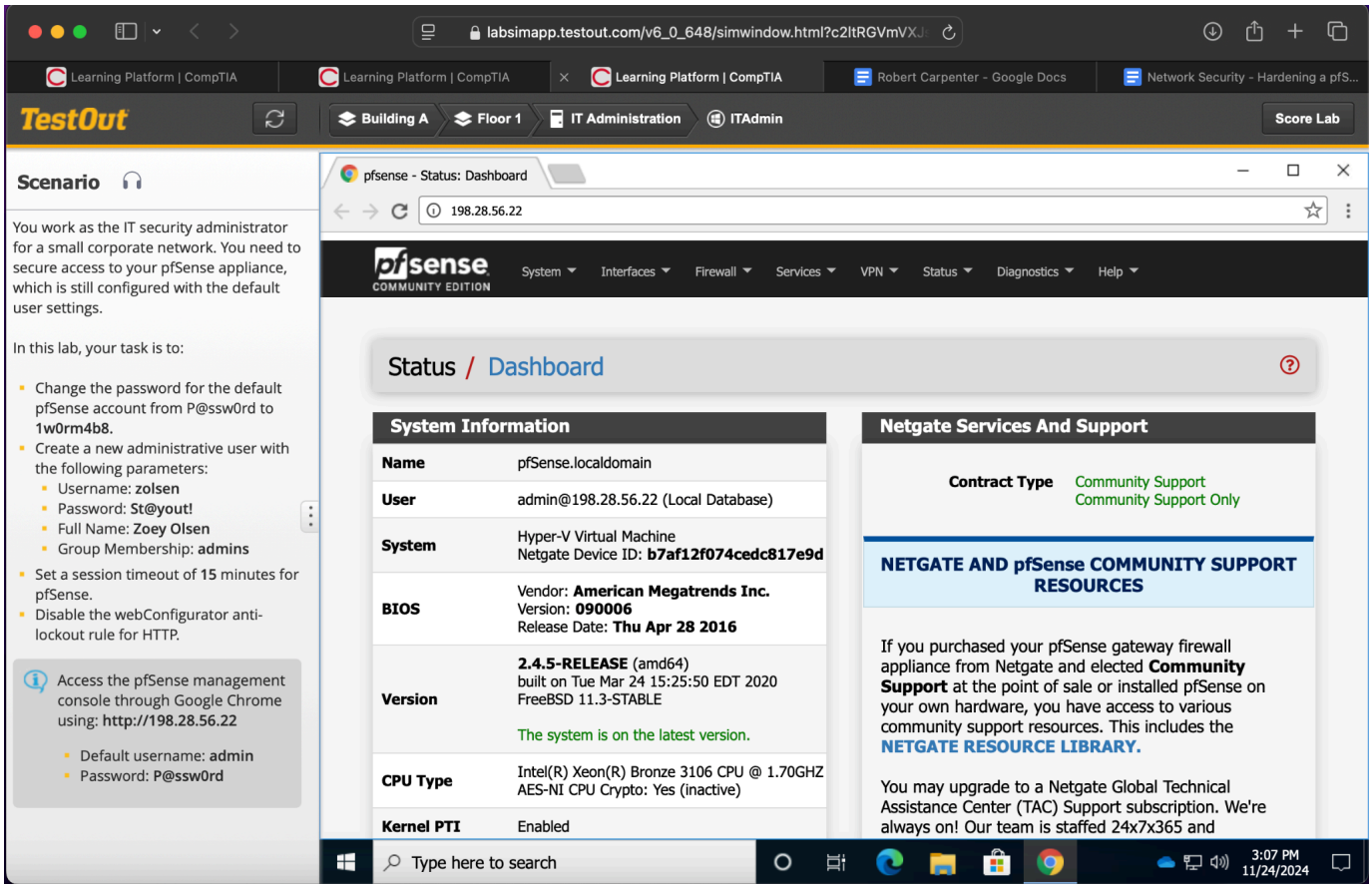
First, I'll navigate to our pfSense management portal. I will enter **198.28.56.22** in the URL field and hit Enter.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Since I know this pfSense appliance has the default credentials (as evidenced by the last pfSense lab) I can login with the username “**admin**” and password “**P@ssw0rd**”

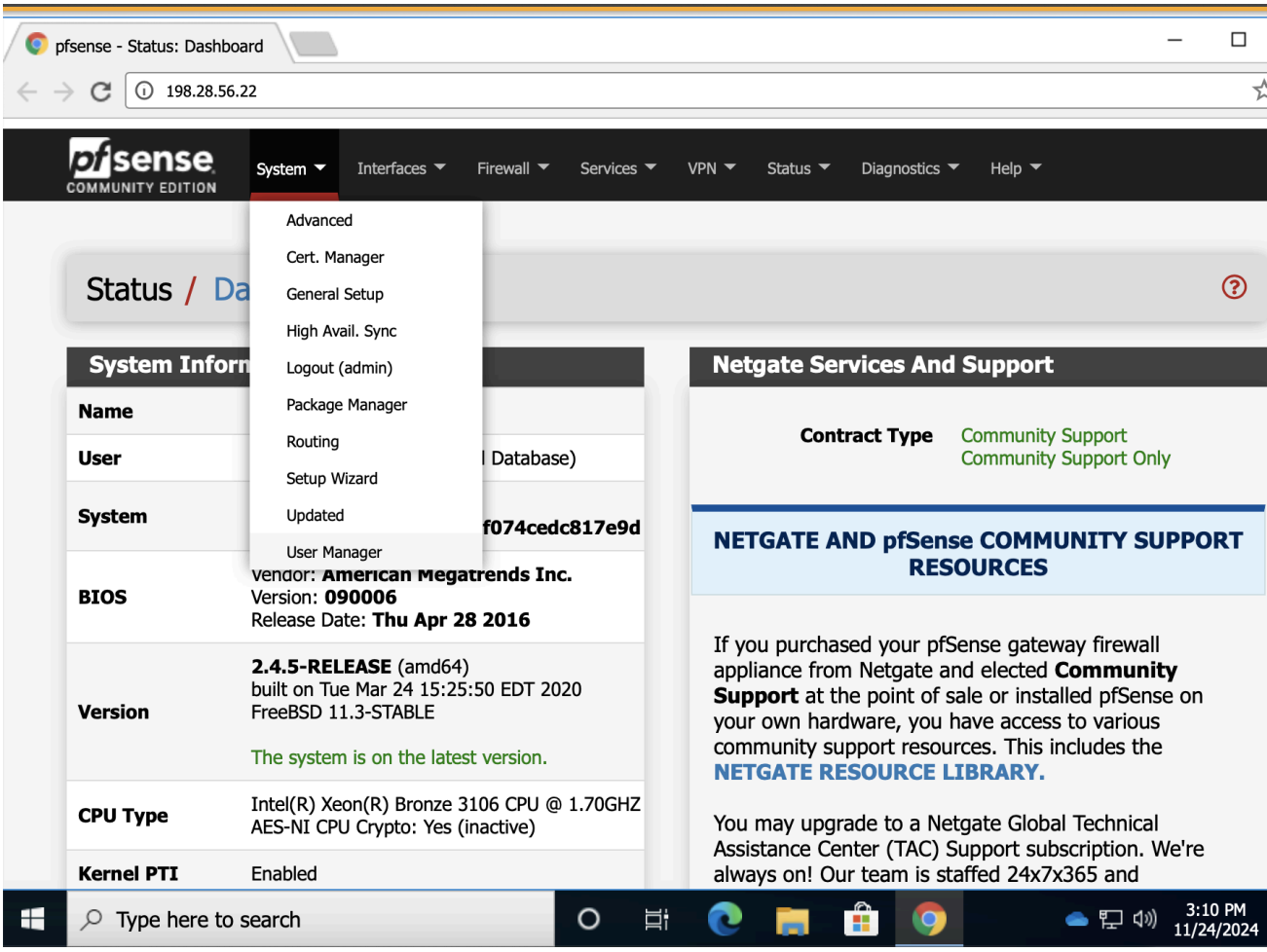
Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



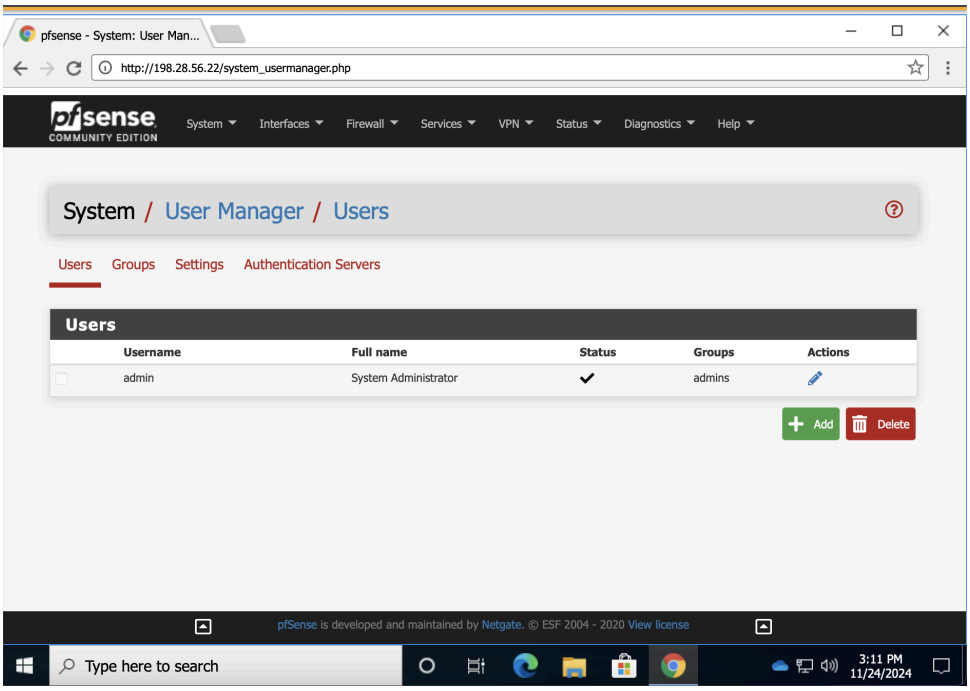
Success , we are in! We need to change the default credentials ASAP as these are well known especially amongst the “Black Hat” / Bad Actor hacking community. To change the user credentials we’ll navigate to **System > User Manager.**

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

- Group Membership: **admins”**

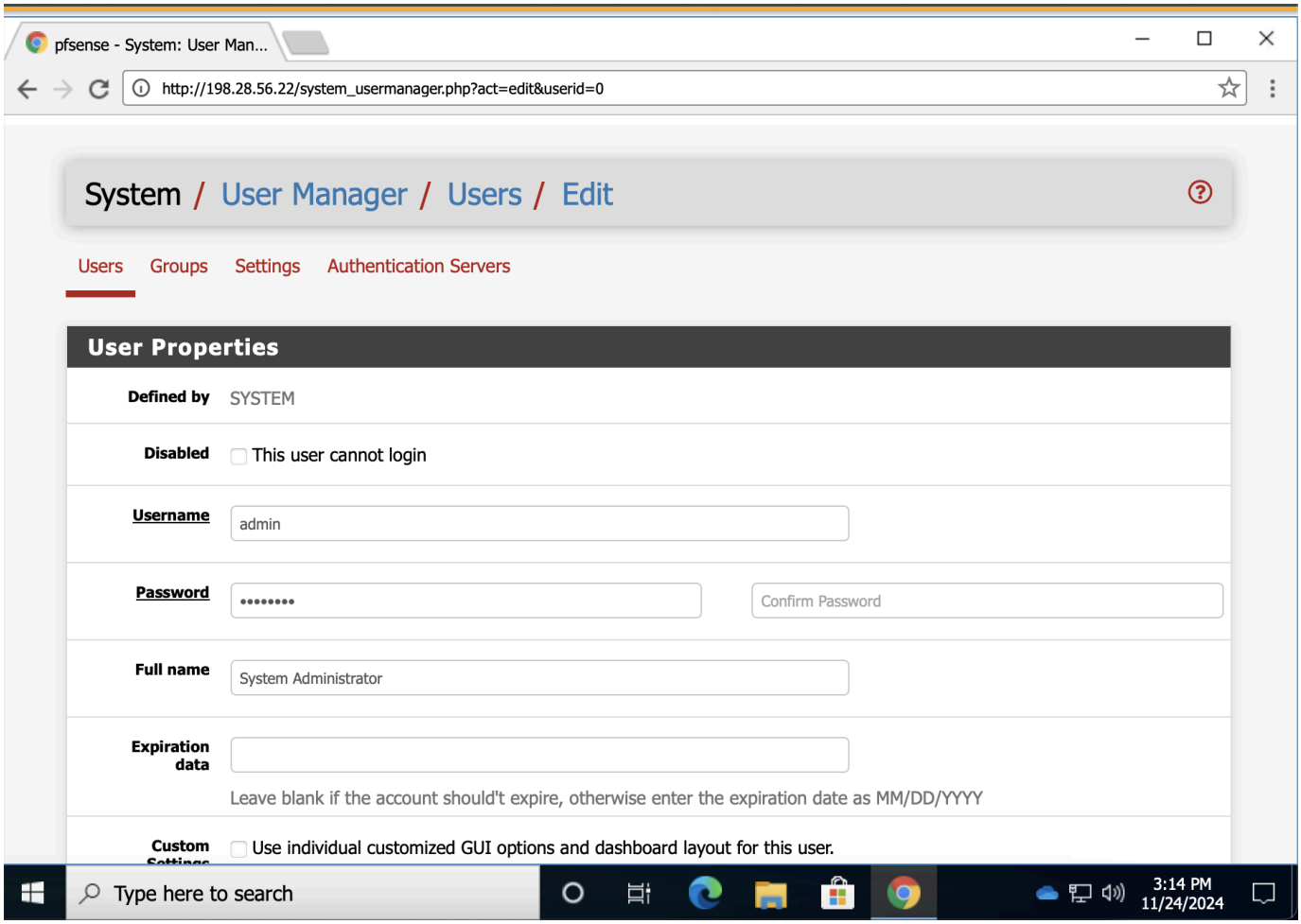


Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



On this page, we'll click the Pencil/Edit icon next to the admin user account in order to change the user's parameters.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Now, we'll delete the current password field and change it to the new password given to us by the lab which is **1w0rm4b8.**

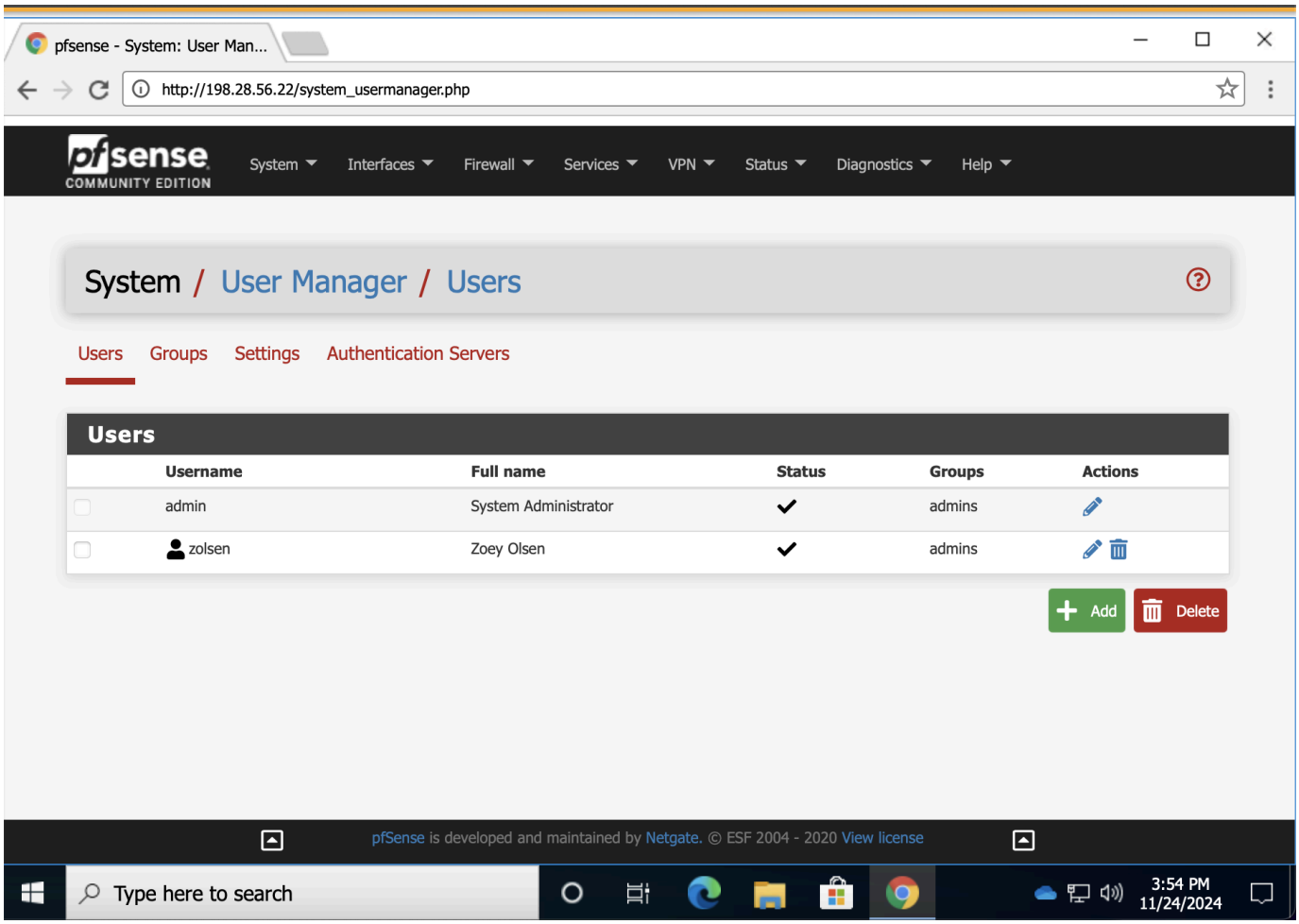
We will now enter the new password then scroll down to the very bottom of this page and hit the blue "**Save"** button.

Now that we've successfully changed the default password for our pfSense application, we can move on to the next part of the lab which is to add a new Administrative user. To do that , we'll go back to the 1st page that showed us all of our users and click the Green "**ADD"** button. A form pops up which prompts us for the configuration of this user.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

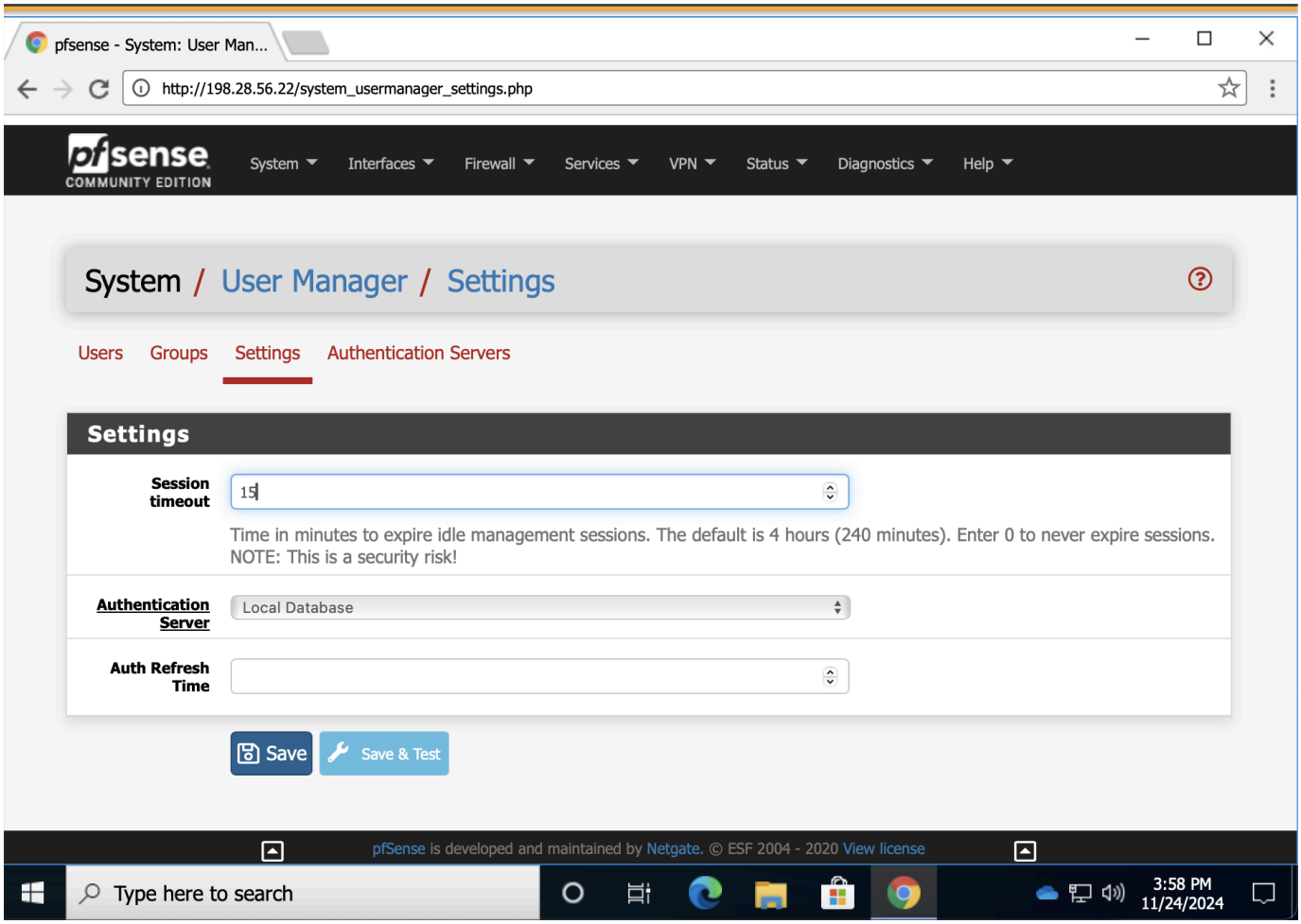
I'll set the username to the one given which is **zolsen** with a password of "**St@yout!"** I'll also need to add their full name which is **Zoey Olsen.** I'll do that now!

After entering the information, I'll hit the blue save button at the bottom and navigate back to my user page to see if the user was created.

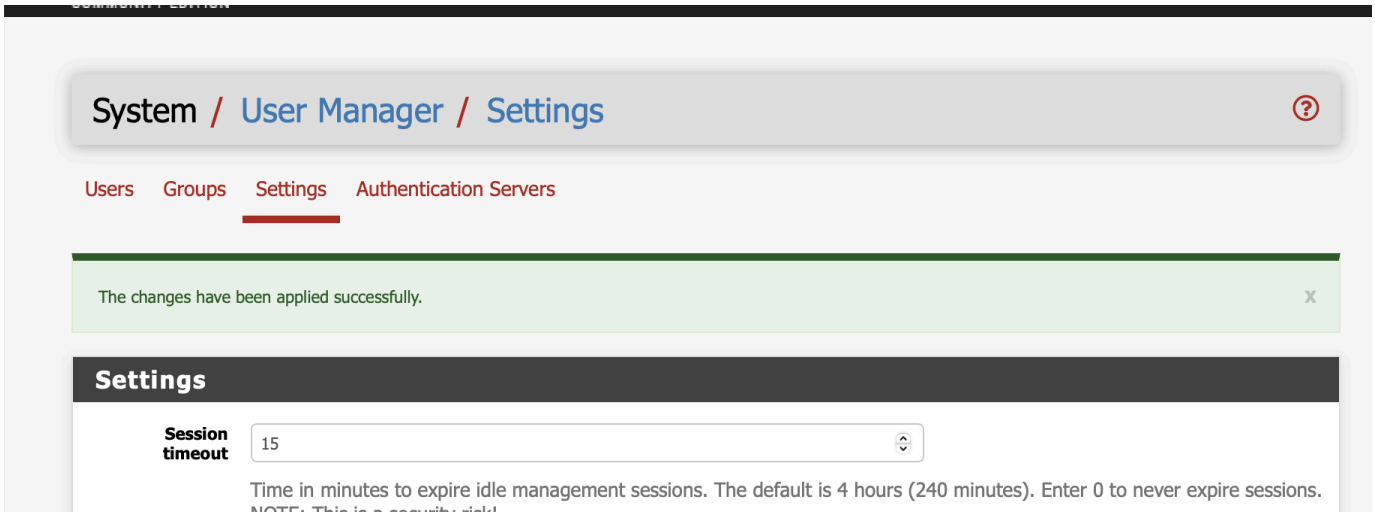


Success! Now we need to configure the logout time to be 15 minutes. To do that, I'll click the Red "Setting" breadcrumb on the same page (pictured above) within User Manager. Under Session timeout I'll enter 15 minutes.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

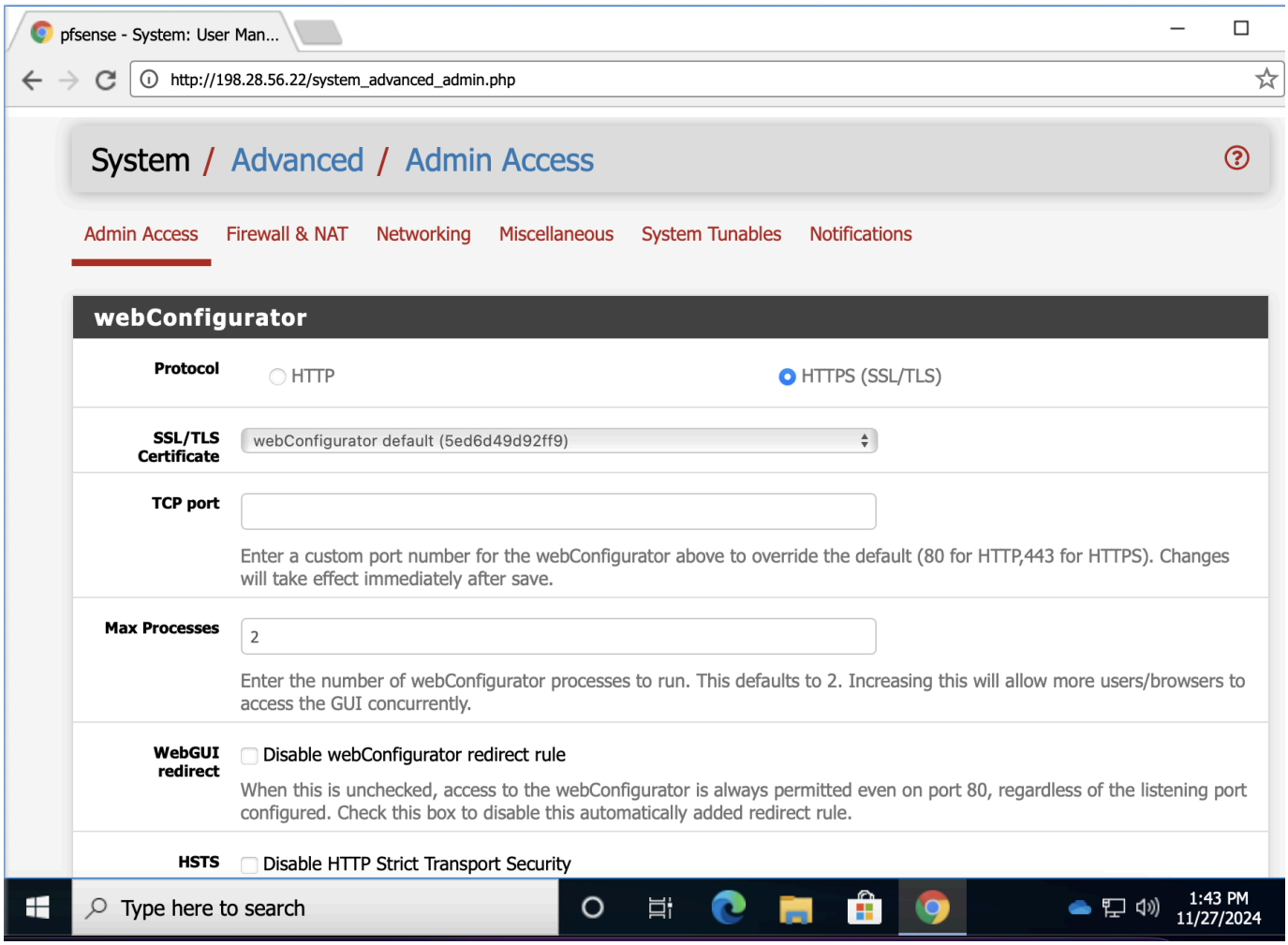


We can see a note which states that the default logout time is 4 hours. After making the change , hit the Blue “**Save”** button in order to apply these changes.



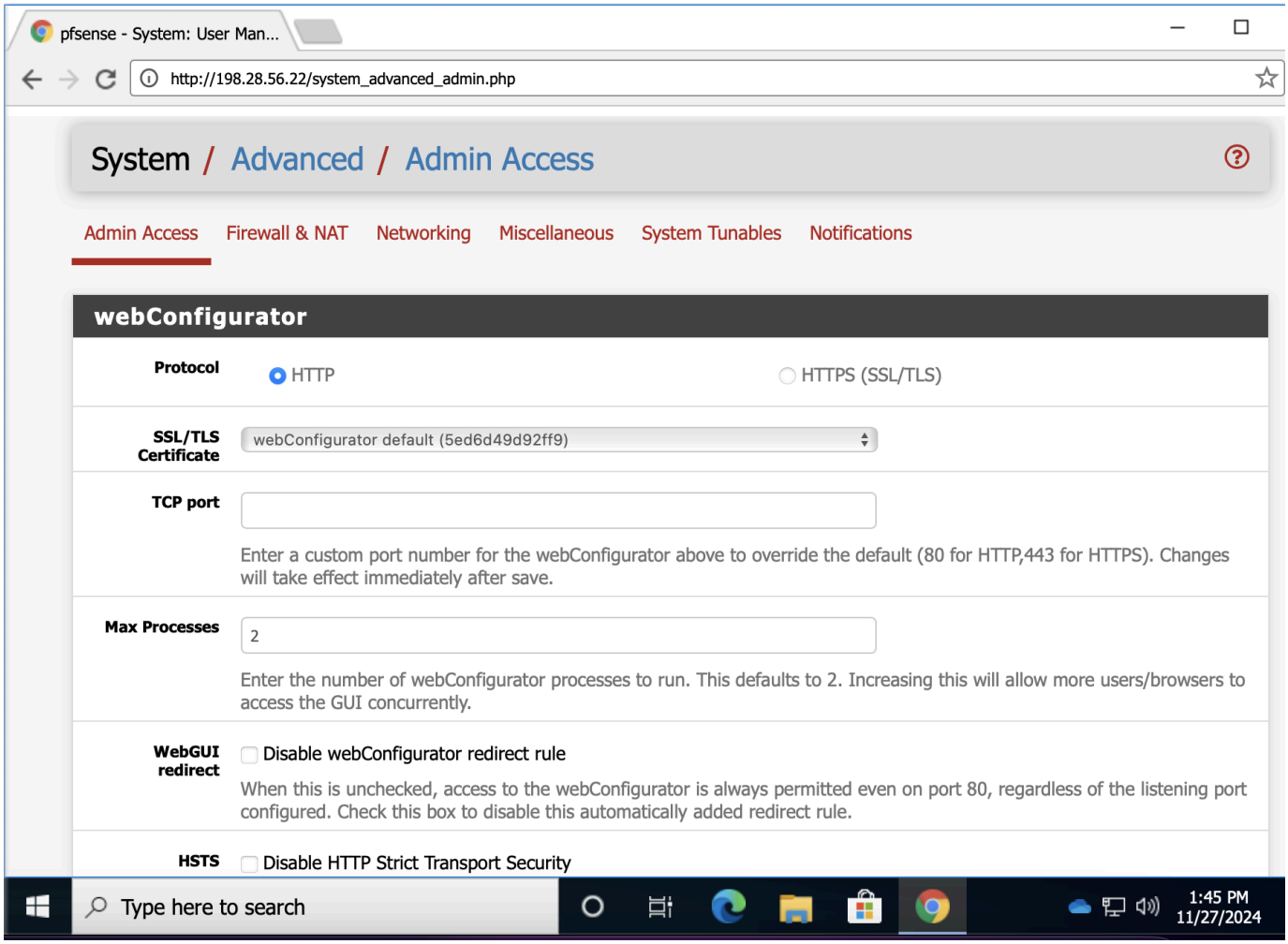
Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

Now that we've complete that, we can move on to the final part of this lab. My last task is to **"Disable the webConfigurator anti-lockout rule for HTTP."** To do this, we'll need to navigate to the Advanced section of the pfSense menus. Go to **System > Advanced** and search for the webConfigurator section:



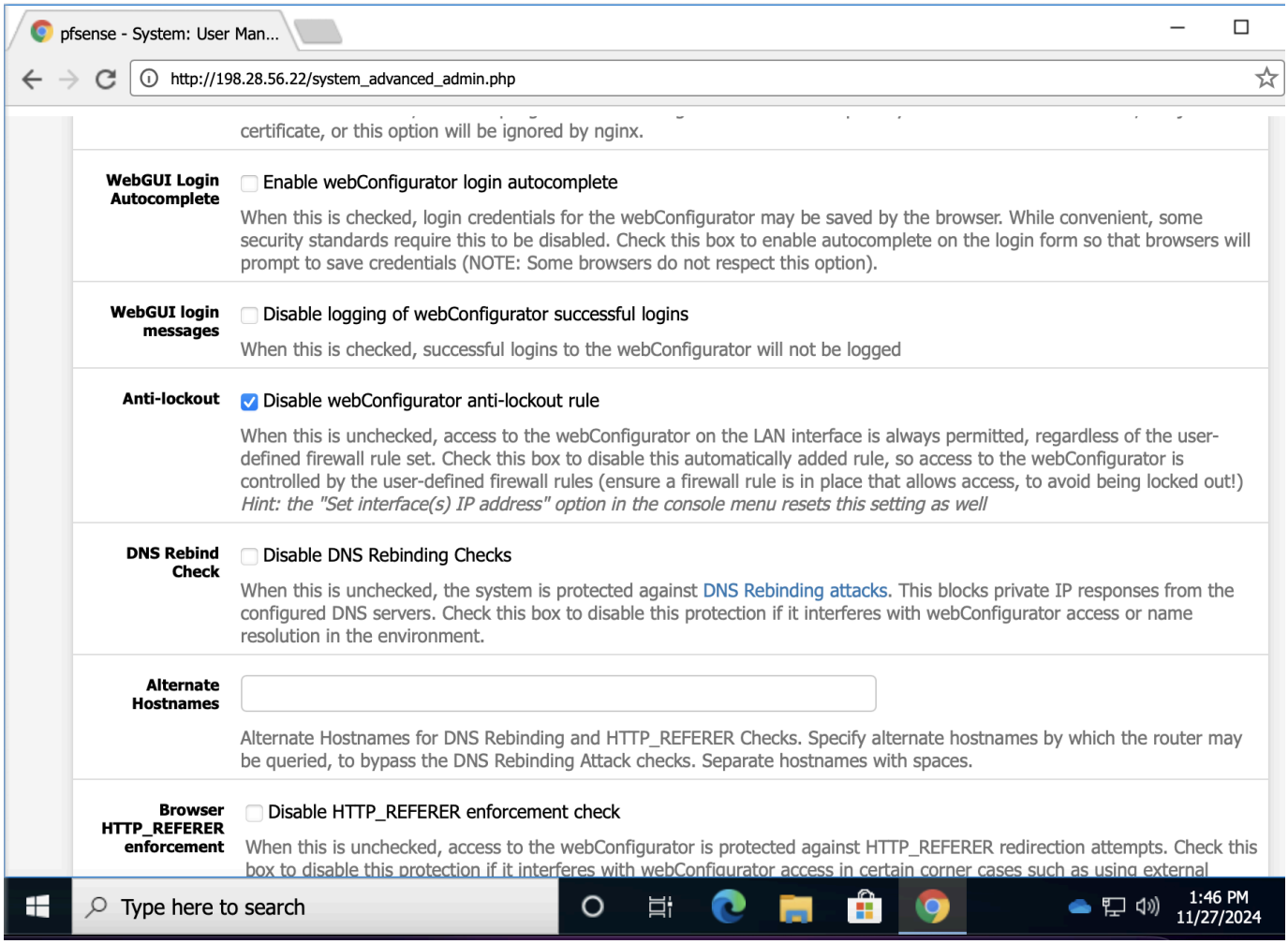
We need to disable the lockout rule for the HTTP protocol. At the top we'll need to change the selection from **HTTPS (SSL/TLS)** to **HTTP** instead.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Now, that it's selected I'll scroll down and look for the webConfigurator rule.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Now that's been checked we can click save at the bottom. This now concludes this lab.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024