

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:

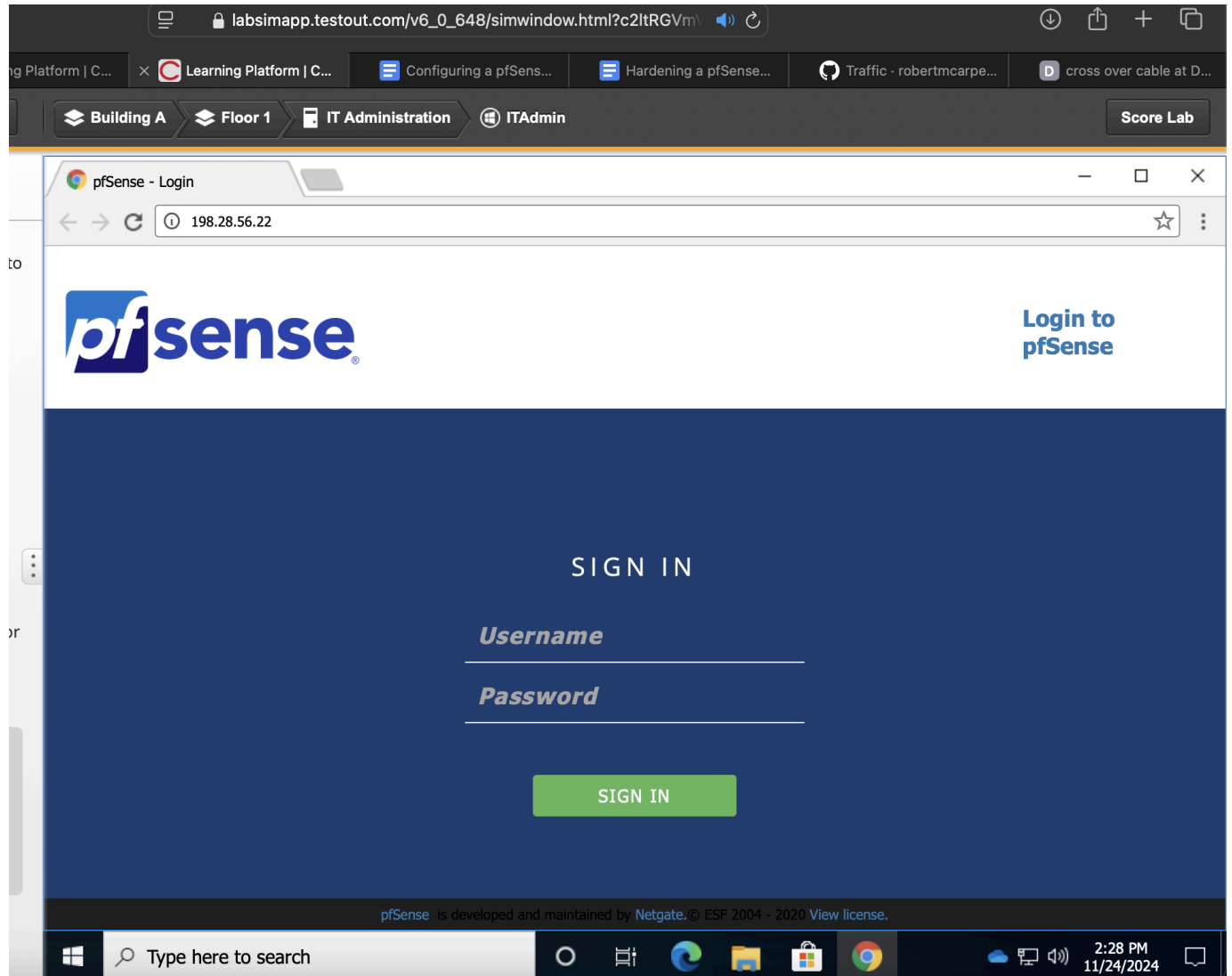
- Change the password for the default pfSense account from P@ssw0rd to 1w0rm4b8.
- Create a new administrative user with the following parameters:
 - Username: zolsen
 - Password: St@yout!
 - Full Name: Zoey Olsen
 - Group Membership: admins
- Set a session timeout of 15 minutes for pfSense.
- Disable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

The screenshot shows a web browser window within a TestOut lab environment. The browser address bar shows the URL `labsimapp.testout.com/v6_0_648/simwindow.html?c2lRGVmVXJ...`. The TestOut interface includes a sidebar with a 'Scenario' section and a main content area displaying the 'pfSense - Status: Dashboard'.

Scenario

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

pfSense - Status: Dashboard

198.28.56.22

System Interfaces Firewall Services VPN Status Diagnostics Help

Status / Dashboard

System Information	
Name	pfSense.localdomain
User	admin@198.28.56.22 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: b7af12f074cedc817e9d
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Thu Apr 28 2016
Version	2.4.5-RELEASE (amd64) built on Tue Mar 24 15:25:50 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHZ AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled

Netgate Services And Support

Contract Type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and

Success , we are in! We need to change the default credentials ASAP as these are well known 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**

pfSense - Status: Dashboard

198.28.56.22

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Status / Dashboard

System Information

Name	
User	
System	f074cedc817e9d
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Thu Apr 28 2016
Version	2.4.5-RELEASE (amd64) built on Tue Mar 24 15:25:50 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHZ AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled

Netgate Services And Support

Contract Type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

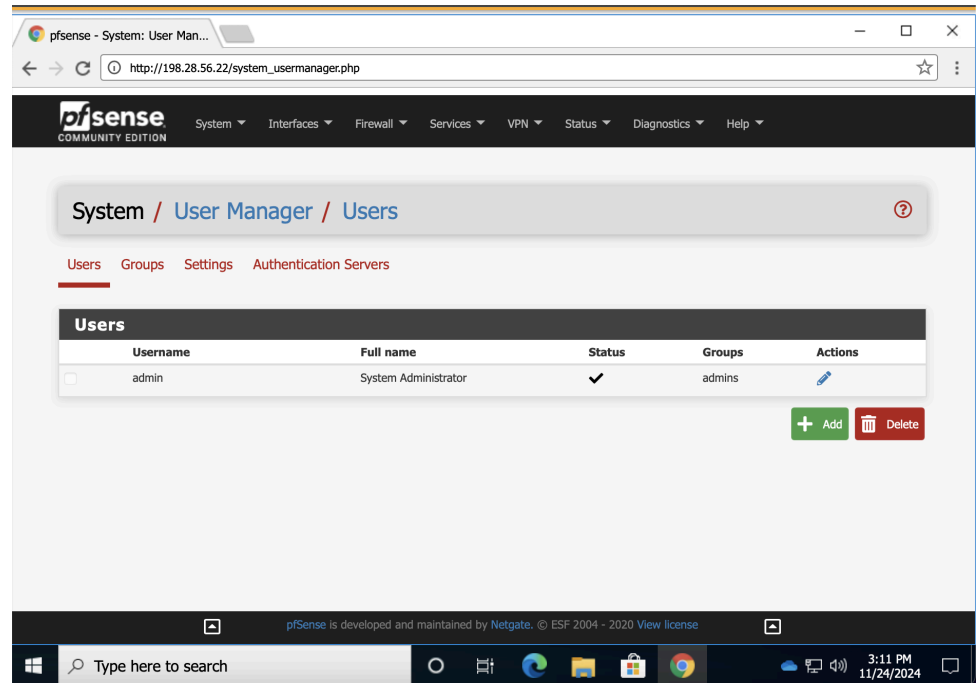
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and

Type here to search

3:10 PM 11/24/2024

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.

The screenshot shows a web browser window with the address bar displaying `http://198.28.56.22/system_usermanager.php?act=edit&userid=0`. The page title is "pfSense - System: User Man...". The breadcrumb navigation shows "System / User Manager / Users / Edit". Below this, there are tabs for "Users", "Groups", "Settings", and "Authentication Servers", with "Users" being the active tab. The main section is titled "User Properties" and contains the following fields:

- Defined by:** SYSTEM
- Disabled:** ☐ This user cannot login
- Username:** admin
- Password:** A text field with masked characters (dots) and a "Confirm Password" field.
- Full name:** System Administrator
- Expiration data:** A text field with a note below it: "Leave blank if the account should't expire, otherwise enter the expiration date as MM/DD/YYYY".
- Custom Settings:** ☐ Use individual customized GUI options and dashboard layout for this user.

The Windows taskbar at the bottom shows the search bar with "Type here to search", several application icons, and the system clock displaying "3:14 PM 11/24/2024".

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

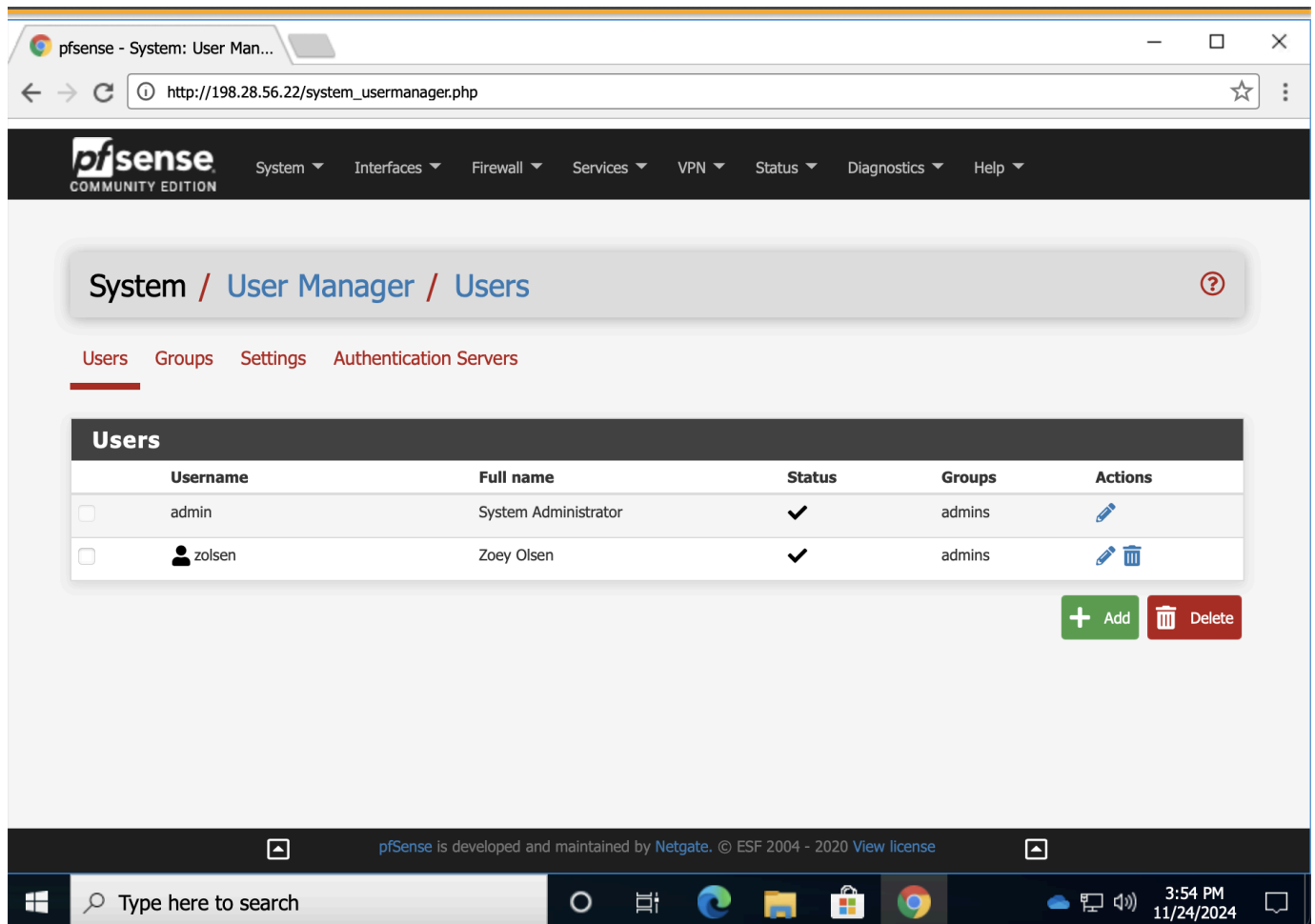
We will now enter the new password then scroll down to the very bottom of this page and hit the blue **"Save"** button.

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

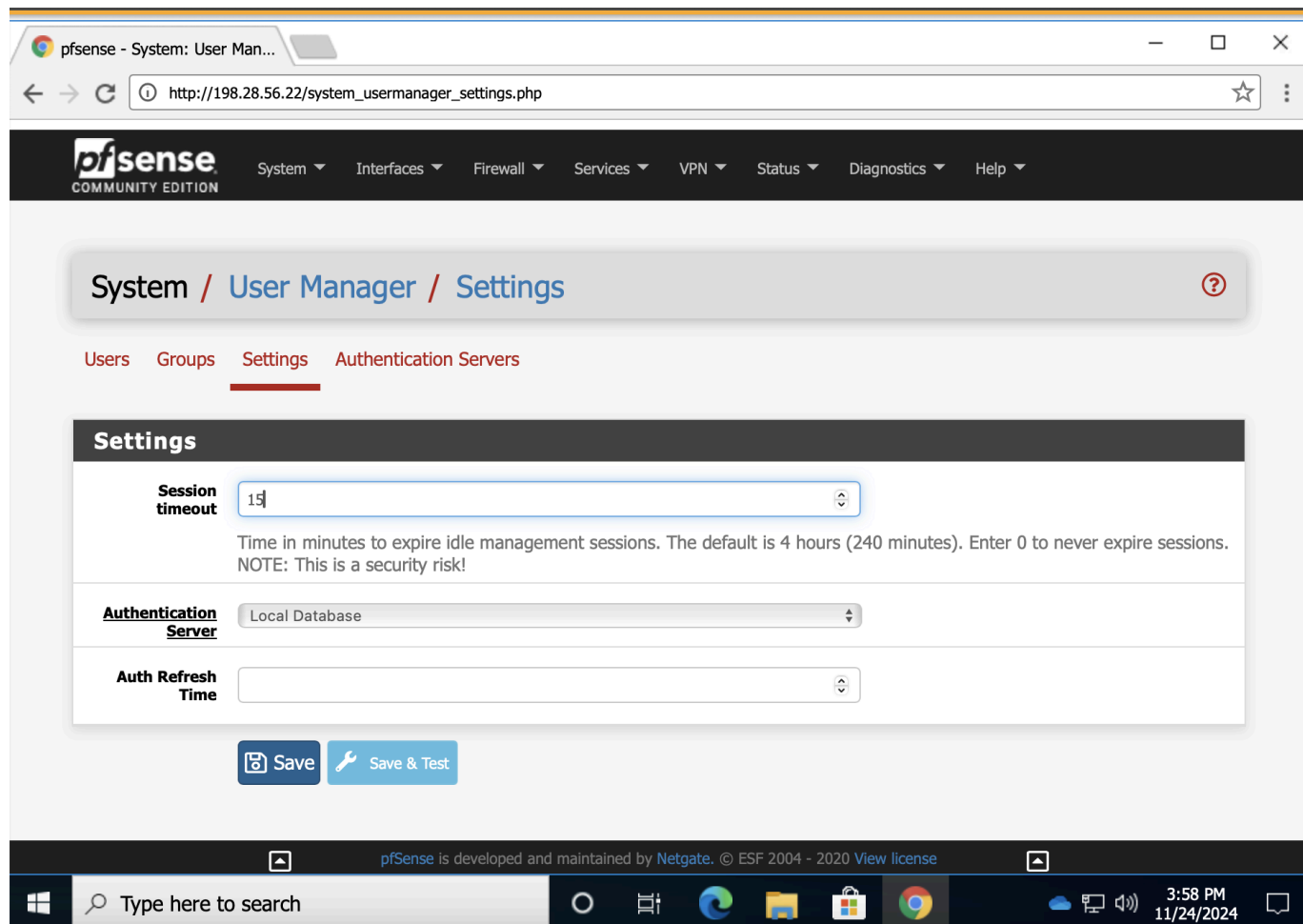
I'll set the username to the one given which is **zolsen** with a password of **"St@yout!"** I'll also need to add their full name which is **Zoey Olsen**. I'll do that now!

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.

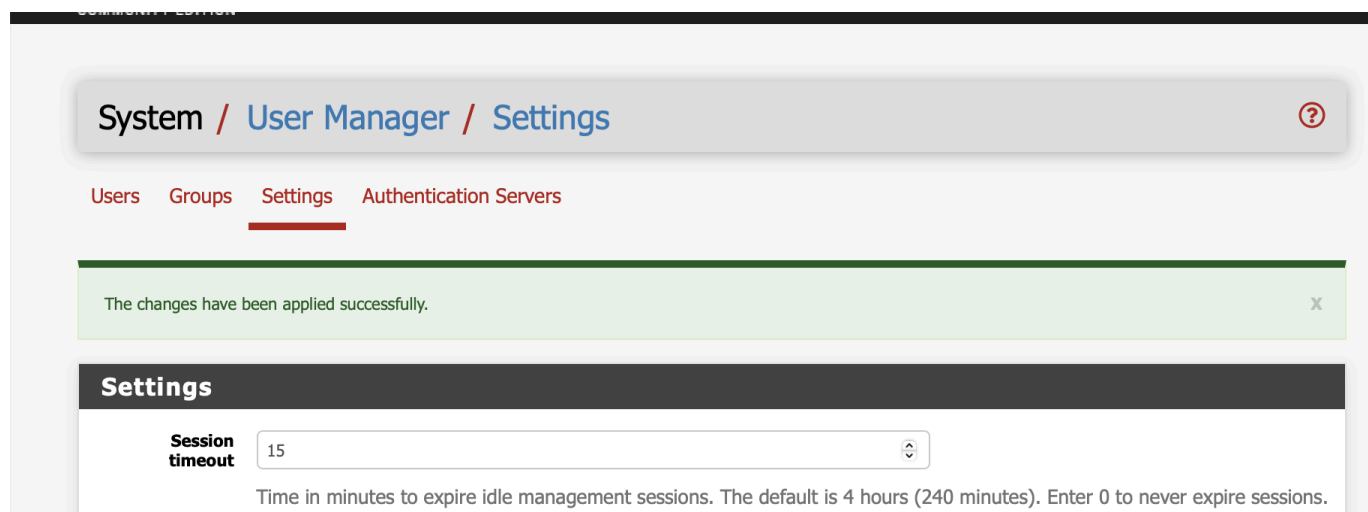


Success! Now we need to configure the logout time to be 15 minutes. To do that, I'll click the Red "Setting" breadcrumb on the same page (pictured above) within User Manager. Under Session timeout I'll enter 15 minutes.

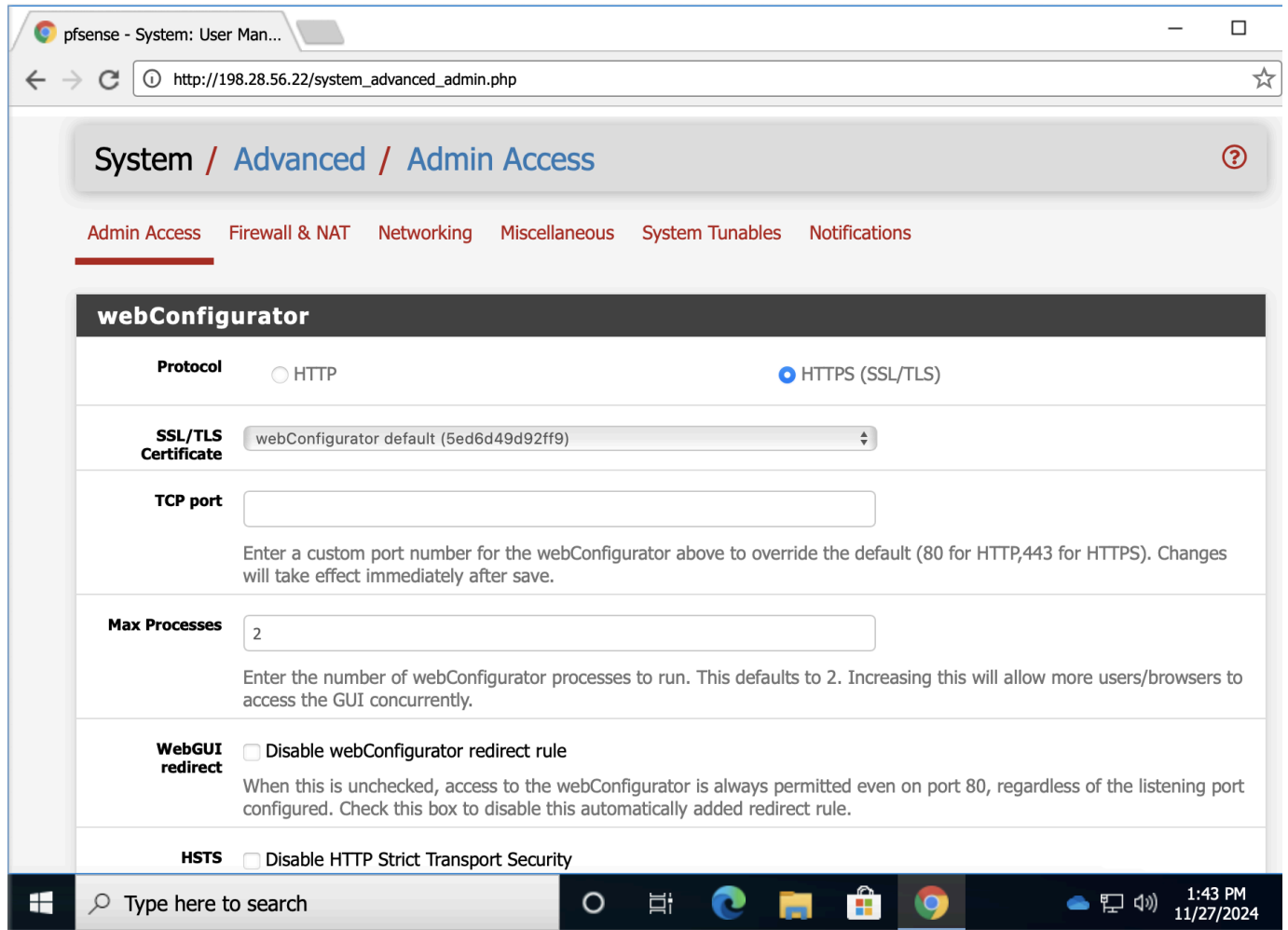
Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



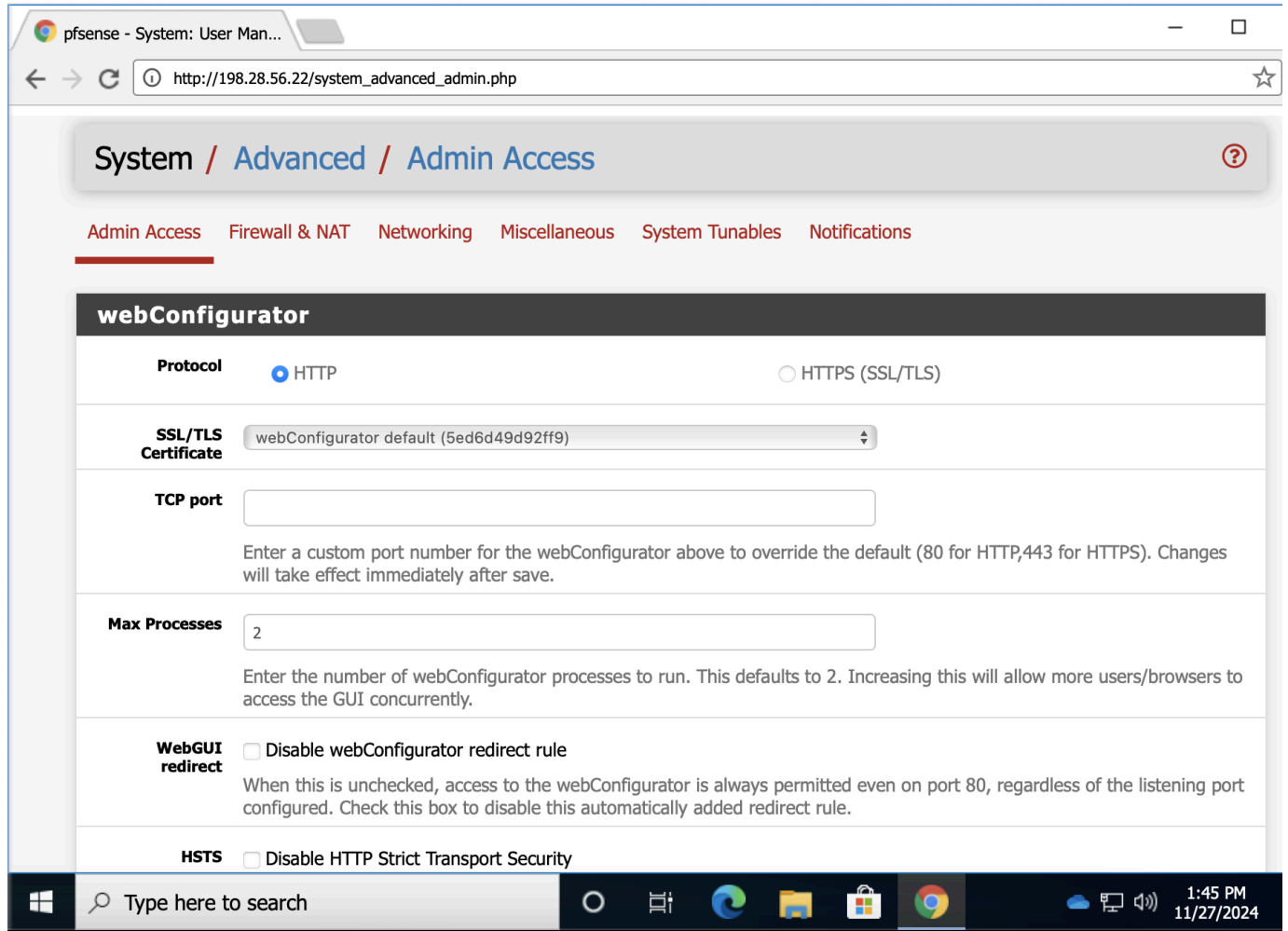
We can see a note which states that the default logout time is 4 hours. After making the change , hit the Blue “**Save**” button in order to apply these changes.



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.



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

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

The screenshot shows a web browser window with the address bar displaying `http://198.28.56.22/system_advanced_admin.php`. The page title is "pfsense - System: User Man...". The main content area contains several configuration sections:

- WebGUI Login Autocomplete**: A checkbox labeled "Enable webConfigurator login autocomplete" is unchecked. Below it, a text block explains that when checked, login credentials may be saved by the browser, but some security standards require this to be disabled. A note mentions that some browsers do not respect this option.
- WebGUI login messages**: A checkbox labeled "Disable logging of webConfigurator successful logins" is unchecked. Below it, a text block explains that when checked, successful logins will not be logged.
- Anti-lockout**: A checkbox labeled "Disable webConfigurator anti-lockout rule" is checked. Below it, a text block explains that when unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. A hint suggests that the "Set interface(s) IP address" option in the console menu resets this setting.
- DNS Rebind Check**: A checkbox labeled "Disable DNS Rebinding Checks" is unchecked. Below it, a text block explains that when unchecked, the system is protected against DNS Rebinding attacks, which block private IP responses from configured DNS servers. A note suggests checking this box to disable this protection if it interferes with webConfigurator access or name resolution.
- Alternate Hostnames**: A text input field is empty. Below it, a text block explains that alternate hostnames can be specified to bypass DNS Rebinding Attack checks, separated by spaces.
- Browser HTTP_REFERER enforcement**: A checkbox labeled "Disable HTTP_REFERER enforcement check" is unchecked. Below it, a text block explains that when unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. A note suggests checking this box to disable this protection in certain corner cases.

The bottom of the screenshot shows the Windows taskbar with the search bar and several application icons. The system clock in the bottom right corner displays "1:46 PM 11/27/2024".

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

The screenshot shows a web browser window with the URL `labsimapp.testout.com/v6_0_650/simwindow.html?c2ltRGVm...`. The browser has multiple tabs open, including 'Learning Platform | CompTIA', 'Network Security - Hardening a pfSense Secur...', and 'Robert Carpenter - Google Docs'. The 'TestOut' logo is visible in the top left corner of the browser window. The main content area shows a 'Scenario' section on the left with a description of the task: '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:'. The task list includes: '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.', and 'Disable the webConfigurator anti-lockout rule for HTTP.'. A 'Score Lab' button is in the top right corner. A 'Lab Report' modal window is open in the center, displaying 'Score: 4/4 (100%)', 'Time Spent: 12:41', and a 'TASK SUMMARY' section with 'Required Actions' listed as: 'Change the password for the admin account to 1w0rm4b8', 'Set a 15 minute session timeout for pfSense', 'Create and configure a new pfSense user (with a 'Show Details' link)', and 'Disable anti-lockout for HTTP'. The background also shows a 'pfSense - System: User Man...' window with the URL `http://198.28.56.22/system_advanced_admin.php`. The Windows taskbar is visible at the bottom with the search bar and system clock showing 1:49 PM on 11/27/2024.

Scenario

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

pfSense - System: User Man...

http://198.28.56.22/system_advanced_admin.php

Lab Report

Time Spent: 12:41

Score: 4/4 (100%)

TASK SUMMARY

Required Actions

- ✓ Change the password for the admin account to 1w0rm4b8
- ✓ Set a 15 minute session timeout for pfSense
- ✓ Create and configure a new pfSense user [Show Details](#)
- ✓ Disable anti-lockout for HTTP

Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes

Type here to search

1:49 PM 11/27/2024