# Project 13: Security Management

# Description: Learn how to start using the FirewallD tool within Red Hat Enterprise. Install and configure firewall rules, test and verify how the rules work between the two servers provided and Build a rocky8.project13.com.

# You will use your rocky8 for this project part1, 2 and 3

# Make sure your rocky8 ip:x.x.x.210 and hostname is rocky8.project13.com

# Download rhel8.project13.com from project folder of your class website, RHEL8 IP should updated to: ip:x.x.x.212

# Both static IP Address.

# Part1:

# Provision the firewall on Rocky8.

**You have two new servers in your environment that are intended to have proprietary information on them. As a result, you will control access to various services on them using a firewall.**

**Provision the firewall on** Rocky8**. Be sure that the iptables service is not running and/or is masked. Start the firewall on rocky8 and verify it is running.**

1. **Install and start the Apache web server on rocky8.**

**Run below command to install apache:**

**#dnf install httpd –y**

**#cd /var/www/html**

**And enter the line below inside of index.html file**

**“This is my first website configuration”**

1. **Start the httpd service and make sure httpd is running by run an appropriate command. The deamon is httpd.**
2. **Trying to access your website from your laptop by enter** [**http://ipdaddres**](http://ipdaddres) **of your system in your browser**

**Note: if you are not able to access your website, that is where troubleshooting start from. You need to focus on firewall and make sure http port 80 is accessible.**

1. **Now move your index.html to /app/platform/webex/index.htm and update your /etc/httpd/conf/httpd.conf directory with new /app/platform/webex/index.html**
2. **Restart your apache service and now trying to access your website again and fix any problem related to access denied.**

# Part2: On rocky8

# Print your firewall current default zone

# Create a new zone called testing

# Set default zone of your system to home zone

# List all current zone of your system

# Diplay your only current active zone

# Display all the service which is currently predefine for your firewall

# Add the Kerberos service to your firewall

# Add the source ip:x.x.x.212 to your firewall

# Remove the Kerberos service from your firewall

# Remove Kerberos service from your firewall

# Add the port tcp 9000 to your firewall

# Add the port 788 udp to your firewall

# Add port 455 tcp tour testing zone

# Part3: Using firewall rich rule

# Add to your testing zone a source x.x.x.0/24 into only x.x.x.50/32 through TCP ports 8080 through to 8090

# Configure port forwarding

# The traffic coming from centos8 on port 415/tcp should be forwarded to port 22 on your rhel8

# Use an appropriate command to view only all the rich rule set up on your rhel8

# Allow Telnet connection only from centos8. Limit this connection one per minute. Drop Telnet connection from remaining hosts.

# Allow SSH Connection from your network. Log each access with “SSH Access” prefix with notice at level.

# Allow ftp connection on centos8 from only rhel8. Reject FTP connections from remaining systems.

# Part4:

# Troubleshoot rhel8.project13.com and make sure the website display below content:

# “This is project13 homework for Linux Class” when putting IP address on browser.