**ProLUG 101**

**Unit 6 Worksheet**

# Instructions

Fill out this sheet as you progress through the lab and discussions. Hold onto all of your work to send to me at the end of the course.

# Discussion Questions:

**Unit 5 Discussion Post 1**: A ticket has come in from an application team. Some of the servers your team built for them last week have not been reporting up to enterprise monitoring and they need it to be able to troubleshoot a current issue, but they have no data. You jump on the new servers and find that your engineer built everything correctly and the agents for node\_exporter, ceph\_exporter and logstash exporter that your teams use. But, they also have adhered to the new company standard of firewalld must be running. No one has documented the ports that need to be open, so you’re stuck between the new standards and fixing this problem on live systems.

1. As you’re looking this up, what terms and concepts are new to you?

2. What are the ports that you need to expose? How did you find the answer?

3. What are you going to do to fix this on your firewall?

**Unit 5 Discussion Post 2**: A manager heard you were the one that saved the new application by fixing the firewall. They get your manager to approach you with a request to review some documentation from a vendor that is pushing them hard to run a WAF in front of their web application. You are “the firewall” guy now, and they’re asking you to give them a review of the differences between the firewalls you set up (which they think should be enough to protect them) and what a WAF is doing.

1. What do you know about the differences now?
2. What are you going to do to figure out more?
3. Prepare a report for them comparing it to the firewall you did in the first discussion.

# Definitions/Terminology

Firewall

Zone

Service

DMZ

Proxy

Stateful packet filtering

Stateless packet filtering

WAF

NGFW

# Notes During Lecture/Class:

Links:

Terms:

Useful tools:

# Lab and Assignment

Unit 6 Firewalls - To be completed outside of lecture time

* (Alternate assignment to lab, if you have no Rocky) <https://killercoda.com/het-tanis/course/Linux-Labs/205-setting-up-uncomplicated-firewall-UFW>

Begin working on your project from the Project Guide

Topics:

* + 1. System Stability
    2. System Performance
    3. System Security
    4. System monitoring
    5. Kubernetes
    6. Programming/Automation

You will research, design, deploy, and document a system that improves your administration of Linux systems in some way.

# Digging Deeper

1. Read <https://docs.rockylinux.org/zh/guides/security/firewalld-beginners/>

What new things did you learn that you didn’t learn in the lab?

What functionality of firewalld are you likely to use in your professional work?

# Reflection Questions

1. What questions do you still have about this week?
2. How does security as a system administrator differ from what you expected?