ProLUG Security Engineering Unit 1 Worksheet

# Instructions

Fill out this sheet as you progress through the lab and discussions. Hold your worksheets until the end to turn them in as a final submission packet.

# Discussion Questions:

**Unit 2 Discussion Post 1**: The first question of this course is, “What is Security?”

1. Describe the CIA Triad.

2. What is the relationship between Authority, Will, and Force as they relate to security?

3. What are the types of controls and how do they relate to the above question?

**Unit 2 Discussion Post 2:** Find a STIG or compliance requirement that you do not agree is necessary for a server or service build.

1. What is the STIG or compliance requirement trying to do?

2. What category and type of control is it?

3. Defend why you think it is not necessary. (What type of defenses do you think you could present?)

# Definitions/Terminology

CIA Triad:

RegulatoryCompliance:

HIPAA:

Industry Standards:

PCI/DSS:

Security Frameworks:

CIS:

STIG:

# Notes During Lecture/Class:

Links:

- <https://public.cyber.mil/stigs/downloads>

- <https://excalidraw.com>

- <https://www.open-scap.org>

- <https://www.sans.org/information-security-policy>

- <https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets>

Terms:

Useful tools:

* STIG Viewer 2.18
* SCC Tool (version varies by type of scan)
* OpenScap

# Lab and Assignment

Unit1\_Build\_Standards\_and\_Compliance - To be completed outside of lecture

time.

# Digging Deeper

1. Research a risk management framework. <https://csrc.nist.gov/projects/risk-management/about-rmf>

 - What are the areas of concern for risk management?

2. Research the difference between quantitative and qualitative risks.

 - Why might you use one or the other?

3. Research ALE, SLE, and ARO.

 - What are these terms in relation to?

 - How do these help in the risk discussion?

# Reflection Questions

1. What questions do you still have about this week?

2. How are you going to use what you’ve learned in your current role?