ProLUG Security Engineering Unit 2 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**: There are 401 stigs for RHEL 9. If you filter in your stig viewer for sysctl there are 33 (mostly network focused), ssh - 39, and network - 58. Now there are some overlaps between those, but review them and answer these questions

1. As systems engineers why are we focused on protecting the network portion of our server builds?
2. Why is it important to understand all the possible ingress points to our servers that exist?
   1. Why is it so important to understand the behaviors of processes that are connecting on those ingress points?

**Unit 2 Discussion Post 2:** Read this: [https://ciq.com/blog/demystifying-and-](https://ciq.com/blog/demystifying-and-troubleshooting-name-resolution-in-rocky-linux/)

[troubleshooting-name-resolution-in-rocky-linux/](https://ciq.com/blog/demystifying-and-troubleshooting-name-resolution-in-rocky-linux/) or similar blogs on DNS and host file configurations.

1. What is the significance of the nsswitch.conf file?
2. What are security problems associated with DNS and common exploits? (May have to look into some more blogs or posts for this)

# Definitions/Terminology

sysctl

nsswitch.conf

DNS

Openscap

CIS Benchmarks ss/netstat

tcpdump ngrep

# Notes During Lecture/Class:

Links:

* <https://www.sans.org/information-security-policy/>
* <https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/>
* <https://docs.rockylinux.org/gemstones/core/view_kernel_conf/>
* [https://ciq.com/blog/demystifying-and-troubleshooting-name-resolution-in-](https://ciq.com/blog/demystifying-and-troubleshooting-name-resolution-in-rocky-linux/) [rocky-linux/](https://ciq.com/blog/demystifying-and-troubleshooting-name-resolution-in-rocky-linux/)
* <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

Terms:

Useful tools:

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

# Lab and Assignment

Unit2\_Network\_Standards\_and\_Compliance - To be completed outside of lecture

time.

# Digging Deeper

1. See if you can find any DNS exploits that have been used and written up in the

diamond model of intrusion analysis format. If you can, what are the primary actors and actions that made up the attack?

# 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?