Unit 1 Lab – Build Standards and Compliance

**Required Materials**

Putty or other connection tool Lab Server

Root or sudo command access

STIG Viewer 2.18 (download from <https://public.cyber.mil/stigs/downloads/> )

# EXERCISES (Warmup to quickly run through your system and familiarize yourself)

1. mount | grep -i noexec
2. mount | grep -i nodev
3. mount | grep -i nosuid
	1. Approximately how many of your mounted filesystems have each of these values?
4. sysctl -a | grep -i ipv4
5. sysctl -a | grep -i ipv6
	1. How many of each are there?
6. sysctl -a | grep -i ipv4 | grep -i forward
	1. Does IPv4 forward on interfaces?
7. lsmod | grep -i tables
	1. What type of tables exist?

# PreLAB

Download the STIG Viewer 2.18 from - <https://public.cyber.mil/stigs/downloads/>



Download the STIG for Mariadb and the import it into your STIG viewer



# LAB

This lab is designed to have the engineer practice securing a Linux server or service against a set of configuration standards. These standards are sometimes called benchmarks, checklists, or guidelines. The engineer will be using STIG Viewer 2.18 to complete this lab.

# MariaDB Service configuration:

1. Connect to a hammer server
2. Install MariaDB
	1. dnf install mariadb-server
3. Ensure that it is running
	1. systemctl start mariadb
	2. systemctl status mariadb
	3. ss -ntulp | grep 3306
4. Check and remediate v-253666 STIG



* 1. What is the problem?
	2. What is the fix?
	3. What type of control is being implemented?
	4. Is it set properly on your system?
	5. Connect to mariadb locally
		1. mysql
		2. SELECT user, max\_user\_connections FROM mysql.user;
		3. Can you remediate this finding?



1. Check and remediate v-253677 STIG
	1. What is the problem?
	2. What is the fix?
	3. What type of control is being implemented?
	4. Is it set properly on your system?
2. Check and remediate v-253678 STIG
	1. What is the problem?
	2. What is the fix?
	3. What type of control is being implemented?
	4. Is it set properly on your system?
3. Check and remediate v-253734 STIG
	1. What is the problem?
	2. What is the fix?
	3. What type of control is being implemented?
	4. Is it set properly on your system?