Unit 4 Lab – Bastions

Required Materials

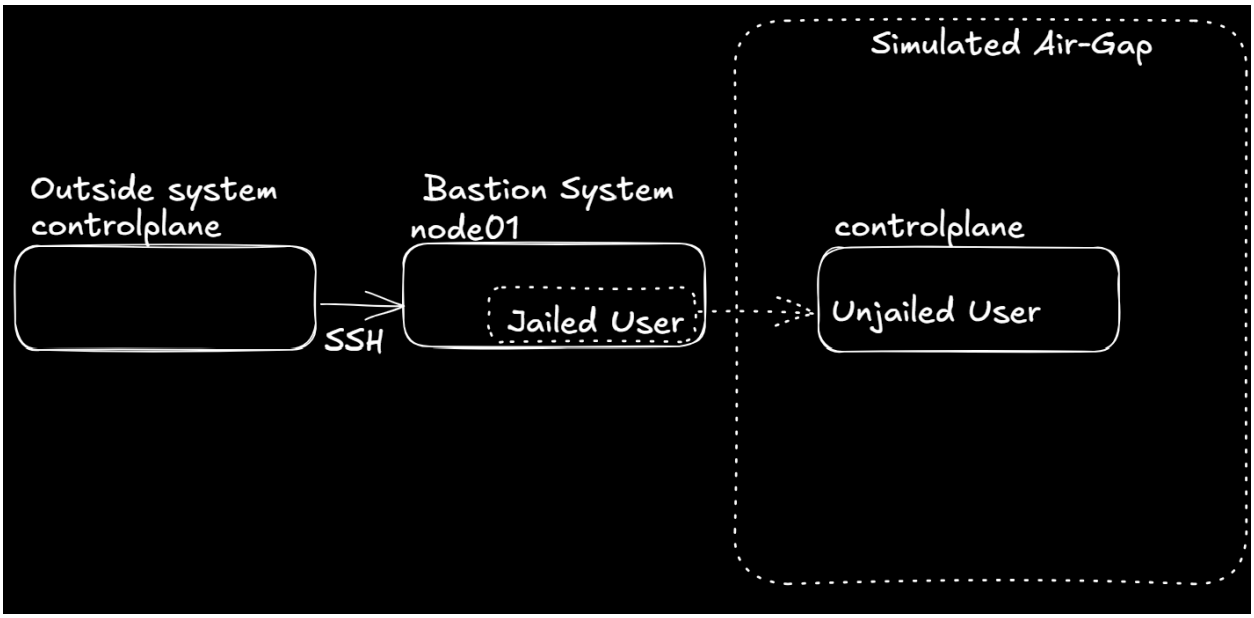
Putty or other connection tool

Lab Server

Root or sudo command access

PreLAB

Review lab diagram for the Bastion design.



LAB

This lab is designed to have the engineer practice securing a Linux environment by the use of bastion hosts and jailing users as they enter an air-gapped environment.

Jailing a user:

1. Follow the lab here answering the questions below as you progress: https://killercoda.com/het-tanis/course/Linux-Labs/204-building-a-chroot-jail
2. If you were to write out the high level steps of building a chroot jail, what would they be?

3. Think about what you did in the lab and what extra (or less) you might give a user/process.
    a. What directories are needed?
    b. What executables might you give the jailed user/process?
    c. If you give an executable, why is it important to give the link libraries that it uses?
    d. What are the special files that you made with mknod and why must they be there? (try removing them or redoing the lab without them. How does it break?)

Building a Bastion

1. Follow the lab here: https://killercoda.com/het-tanis/course/Linux-Labs/210-building-a-bastion-host
2. If you were to write out the high level steps of building a bastion host, what would they be?
3. When you jump into the bastion host, do you have any options other than the one you have given yourself?
4. How did you test that you couldn't leave the jailed environment?
    a. How effective do you think this is as a technical preventative control against user breakout in the jail, having a 20 second timeout?

Digging Deeper challenge (not required for finishing lab)

1. Fix the drawing from the lab with excalidraw and properly replace it here: https://github.com/het-tanis/prolug-labs/tree/main/Linux-Labs/210-building-a-bastion-host
2. Do a pull request and get some github street cred or something.