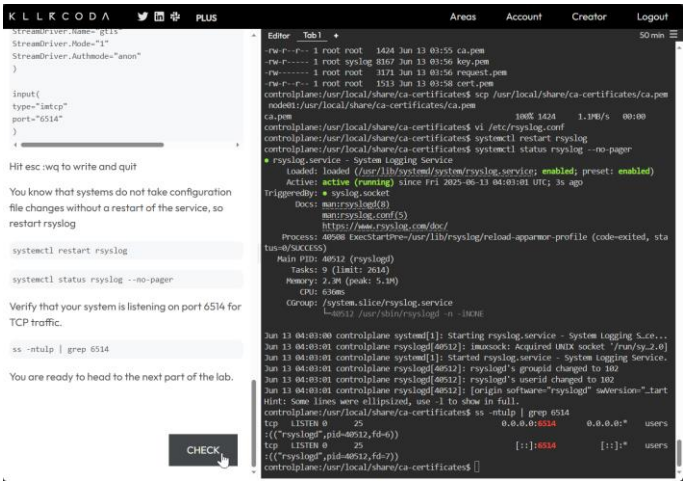
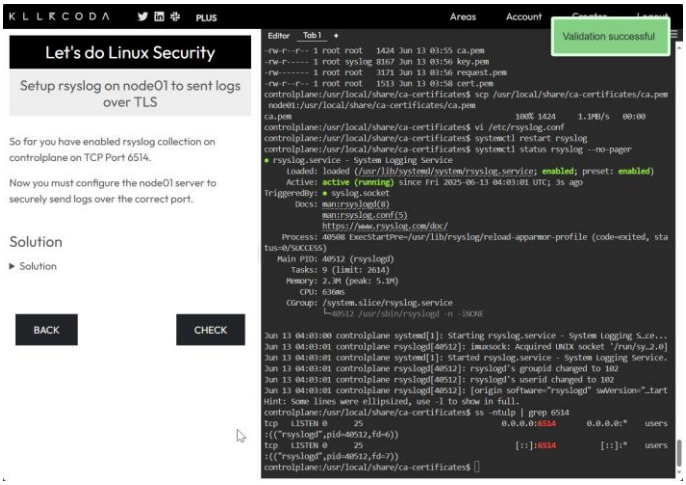
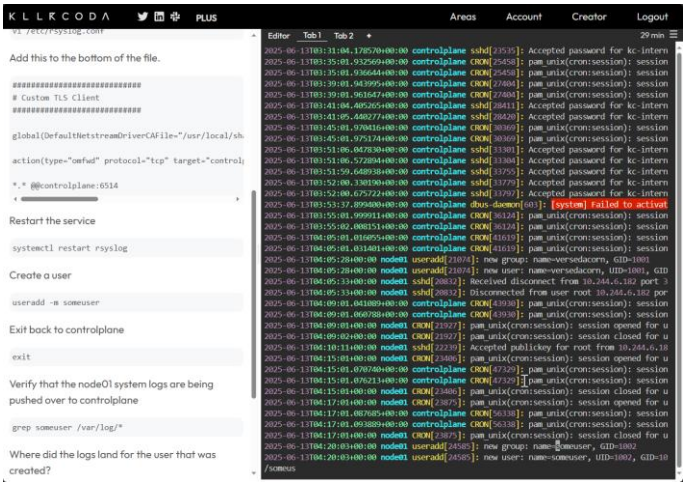
Unit 9 Lab - Certificate and Key Madness

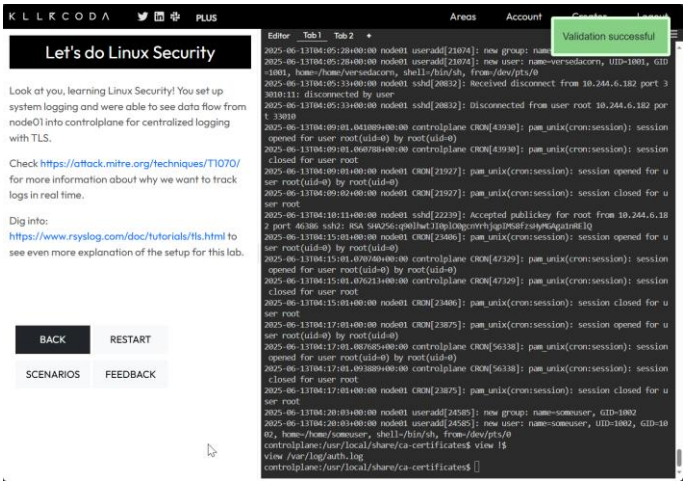
Setting up Rsyslog with TLS

Complete the lab: https://killercoda.com/het-tanis/course/Linux-Labs/211-setting-up-rsyslog-with-tls






KLLKCODA
PLUS
Areas
Account
Creator
Logout
vi /etc/rsyslog.conf
Add this to the bottom of the file.
Restart the service
systemctl restart rsyslog
Create a user
useradd -m someuser
Exit back to controlplane
exit
Verify that the node01 system logs are being pushed over to controlplane
grep someuser /var/log/*
Where did the logs land for the user that was created?
Editor
Tab 1
Tab 2
29 min


KLLKCODA
PLUS
Areas
Account
Validation successful
Let's do Linux Security
Look at you, learning Linux Security! You set up system logging and were able to see data flow from node01 into controlplane for centralized logging with TLS.
Check https://attack.mitre.org/techniques/T1070/ for more information about why we want to track logs in real time.
Dig into: https://www.rsyslog.com/doc/tutorials/tls.html to see even more explanation of the setup for this lab.
BACK
RESTART
SCENARIOS
FEEDBACK
Editor
Tab 1
Tab 2

Review Solving the Bottom Turtle

Review pages 41-48 of https://spiffe.io/pdf/Solving-the-bottom-turtle-SPIFFE-SPIRE-Book.pdf

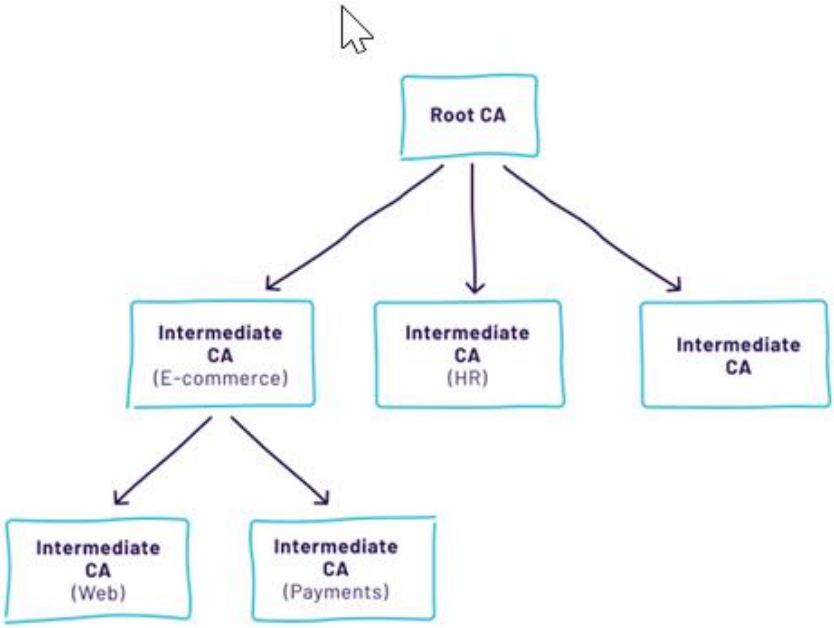
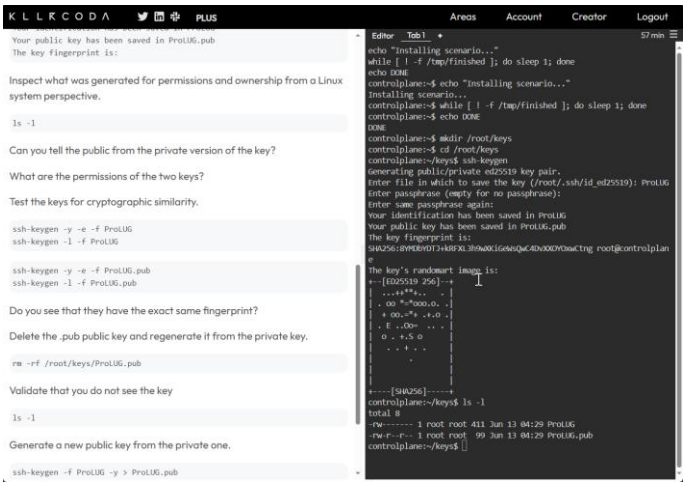


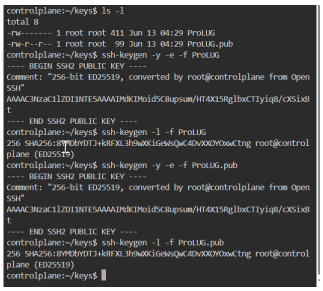
Fig. 3.3: Illustration of intermediate certificate authorities.

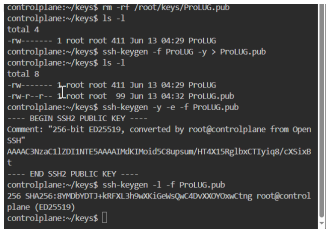
Does the diagram on page 44 make sense to you for what you did with a certificate authority in this lab?

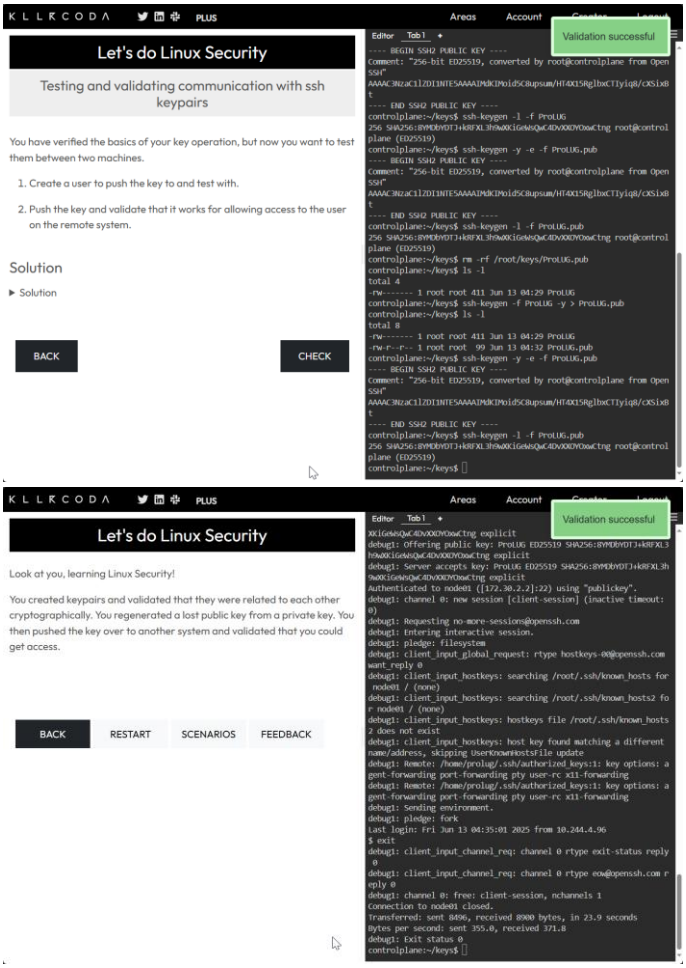
SSH – Public and Private key pairs

Complete the lab: https://killercoda.com/het-tanis/course/Linux-Labs/212-public-private-keys-with-ssh









What is the significance of the permission settings that you saw on the generated public and private key pairs?

The public key is readable to all.

The private key is readable to only the owner.