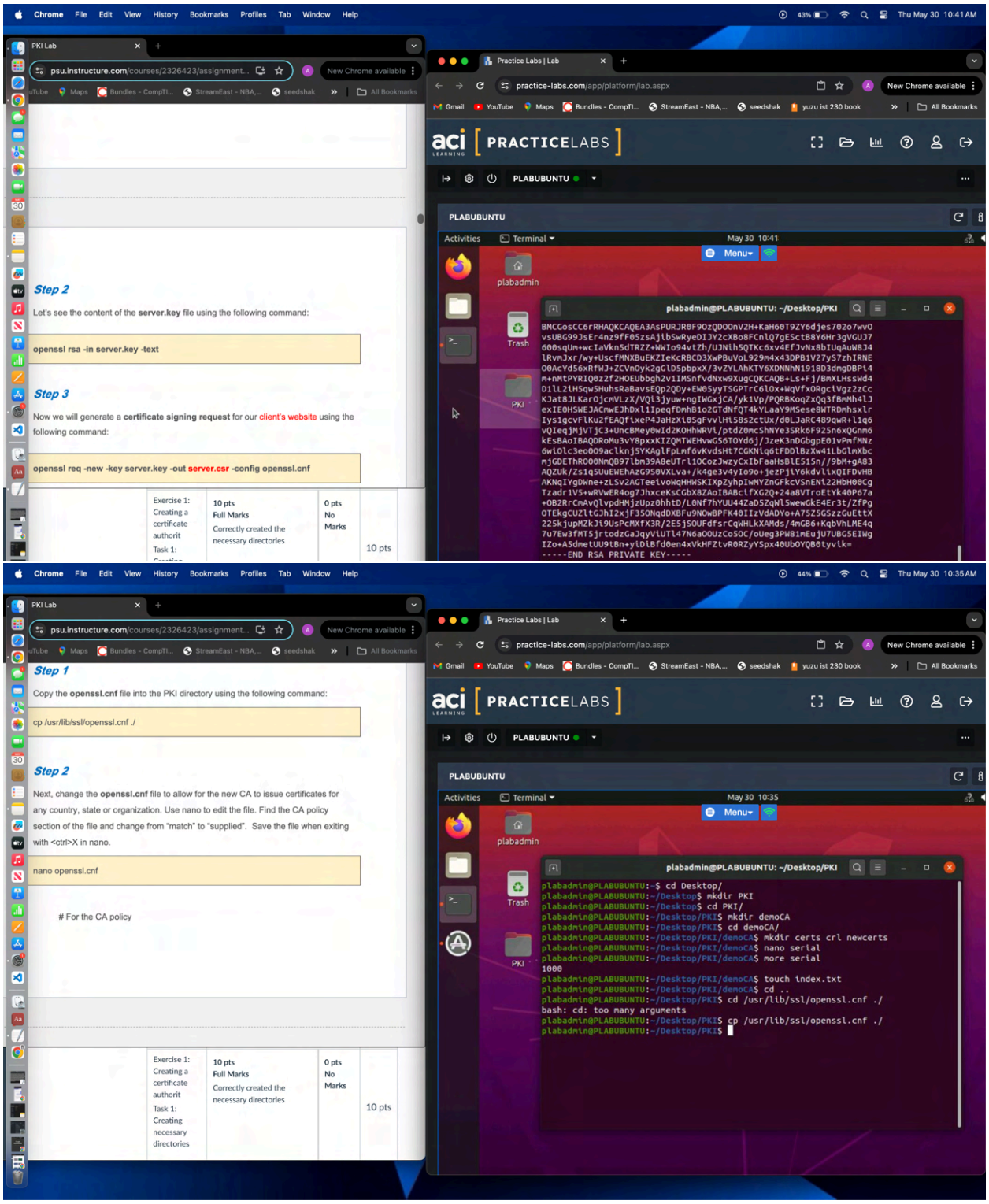
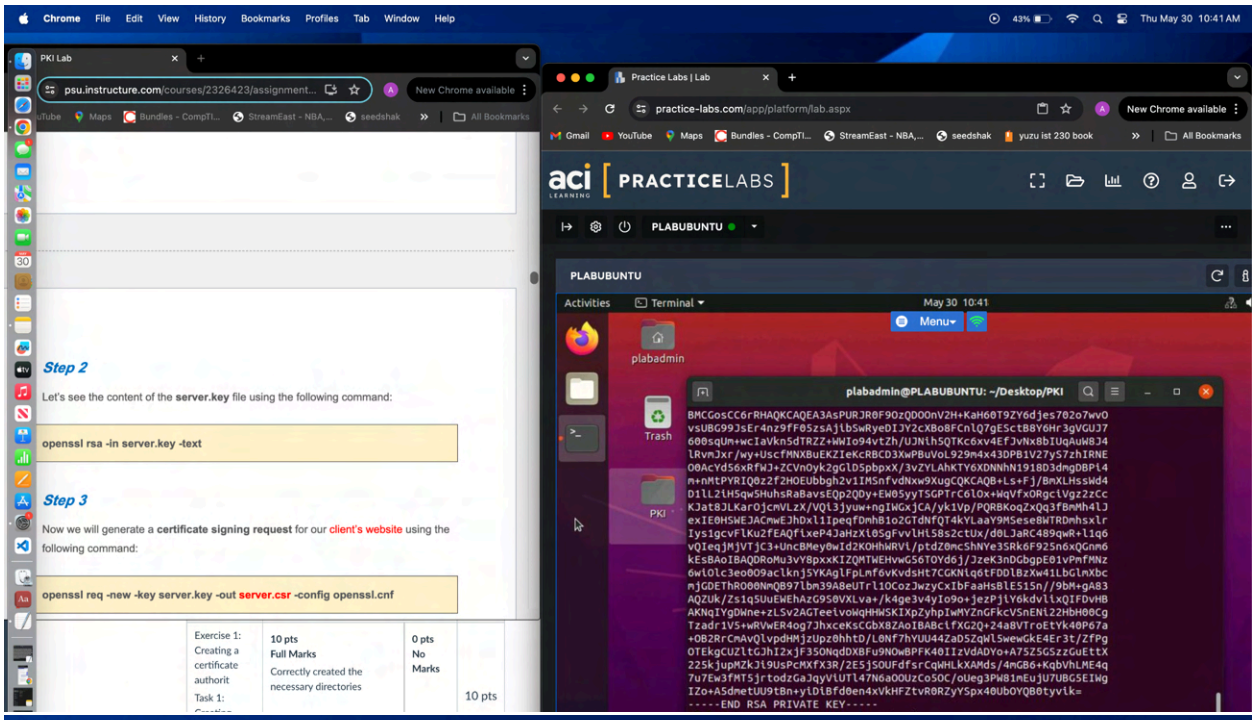
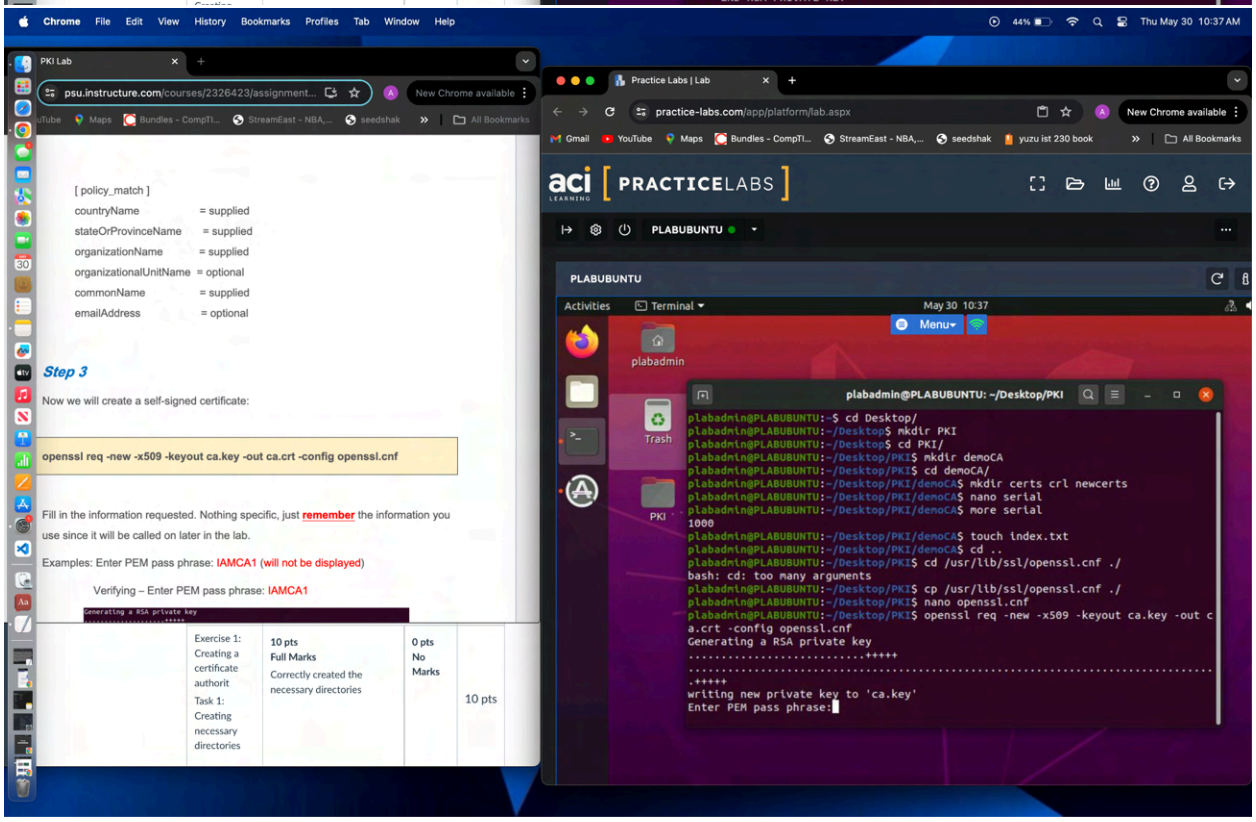
PKI Lab report by Anthony Coppolecchia



In this screenshot i changed the directory to desktop then created a PKI directory and changed the directory to desktop/pki. Then i created a new directory called demoCA and changed the directory to it. Then i created three folders called certs, crl and newcerts. Then i edited serial to put the number 1000 in it and i showed the contents of serial. I then created a new file called index.txt and saved it to the demo ca directory i made. Then switched back to the pki folder i created. I then copied the openssl.cnf file into the pki directory i made.

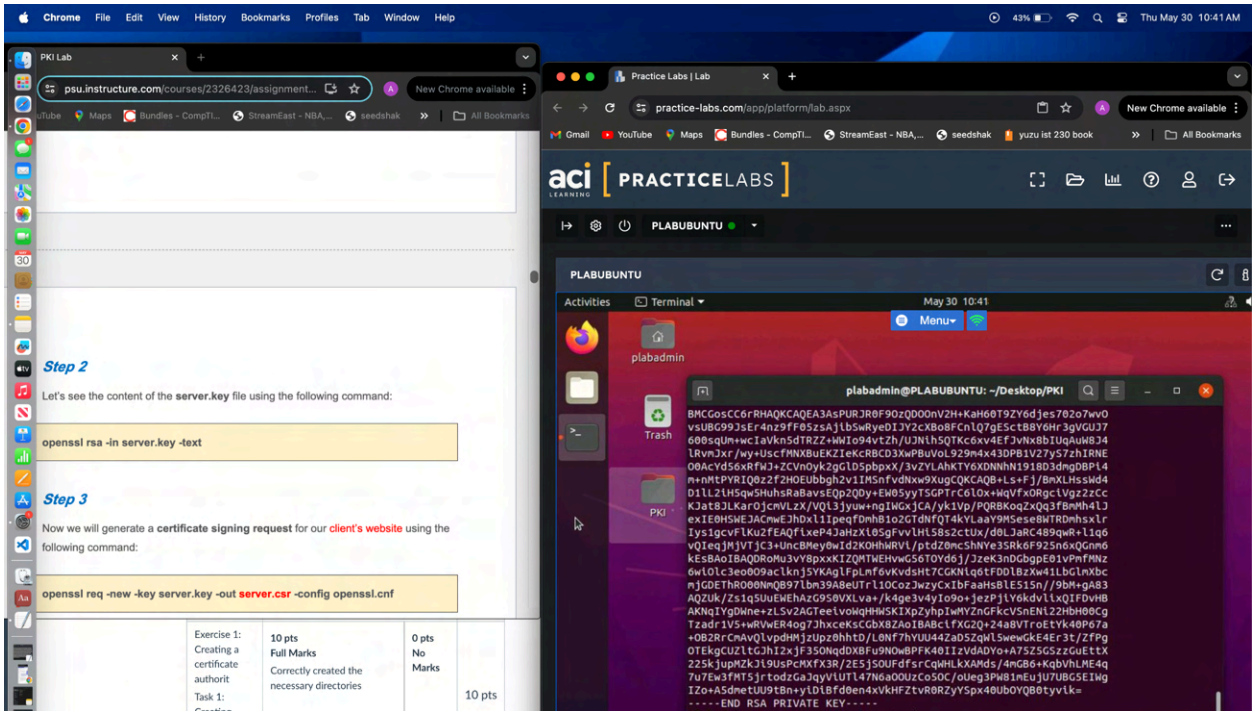
PKI Lab report by Anthony Coppolecchia



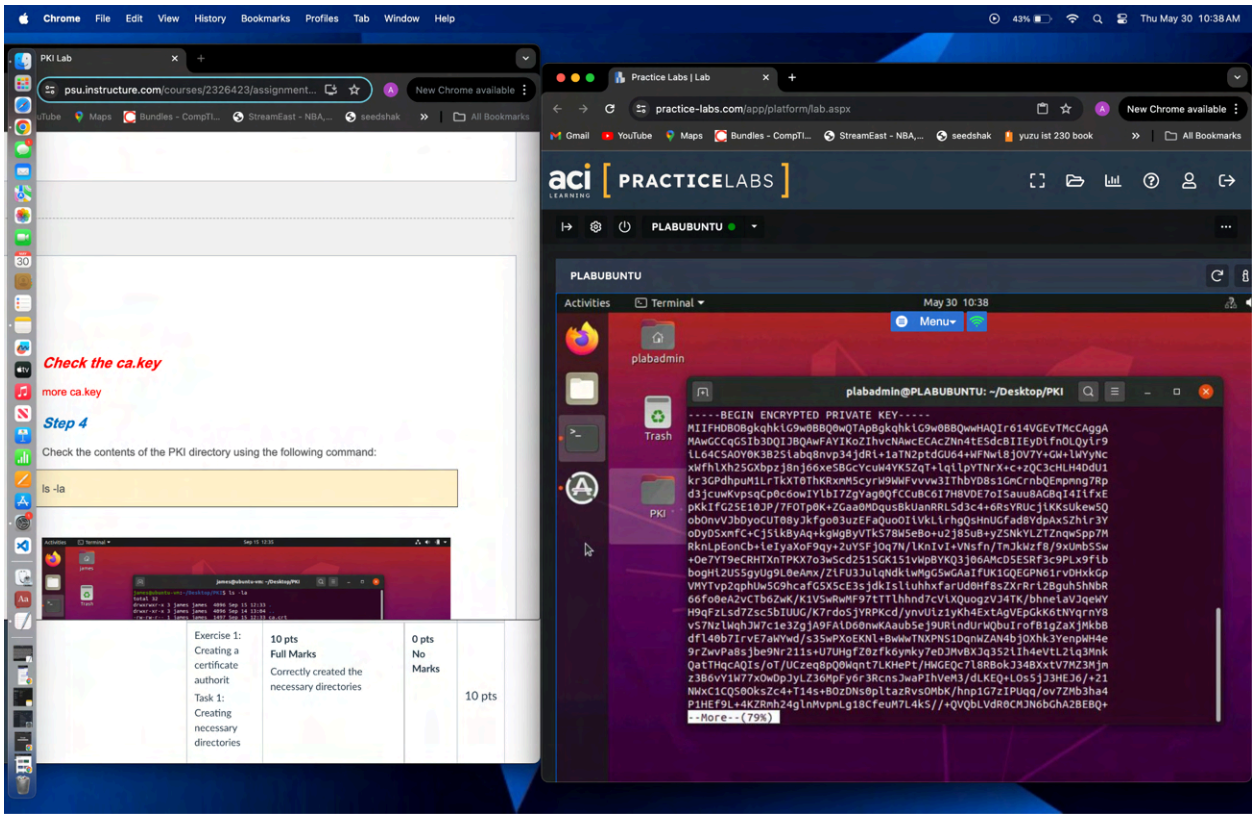


In this ss i changed openssl.cnf to allow for demo ca to issue certificates and i used nano command to edit the fileand changed match to supplied . I then created a self signed certificate.

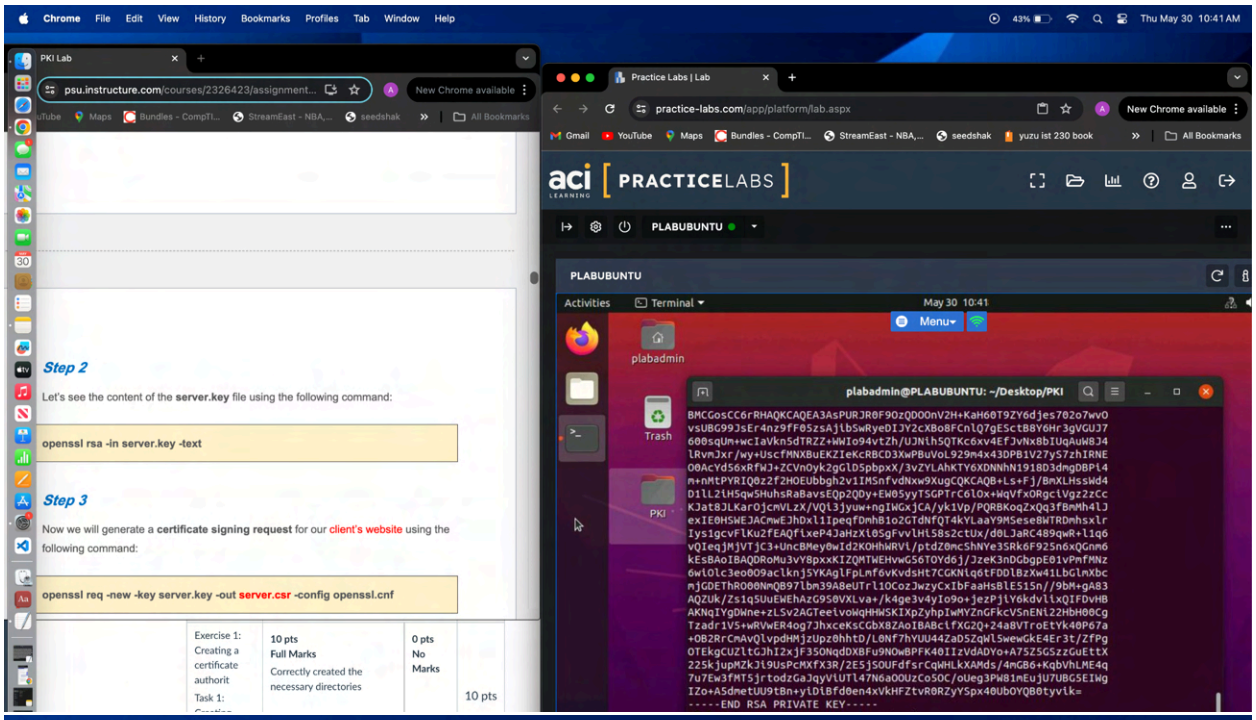
PKI Lab report by Anthony Coppolecchia



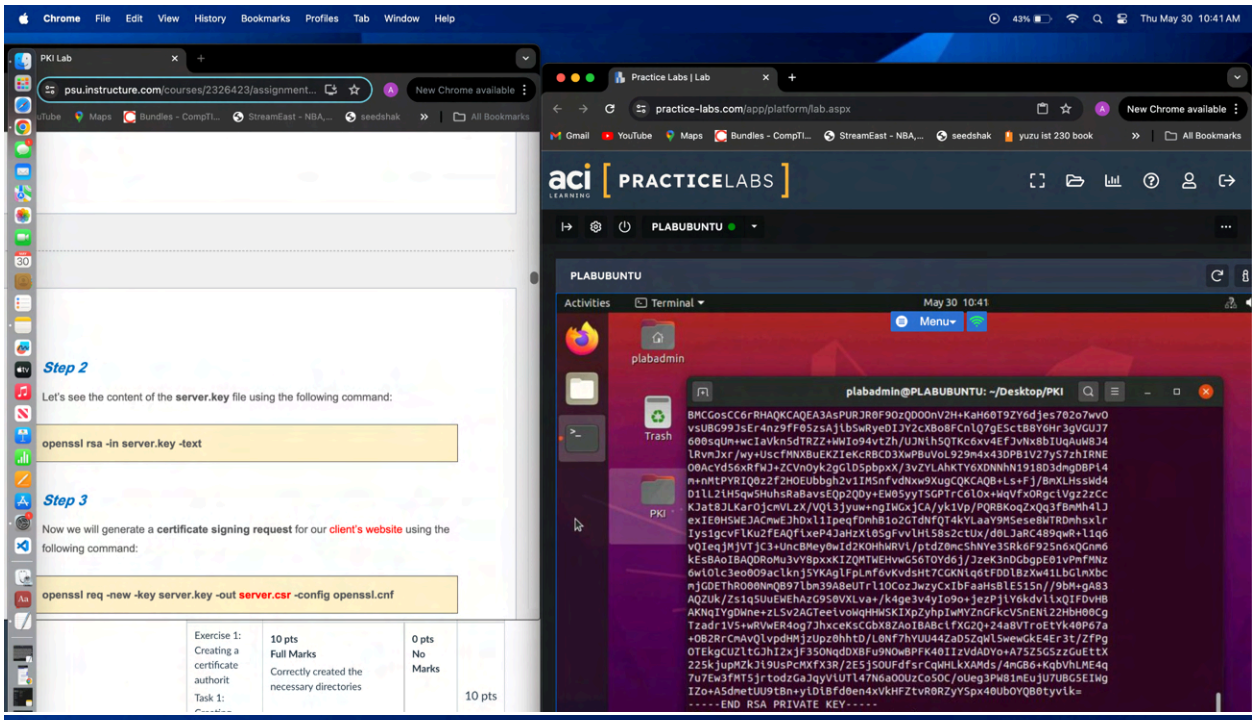
In the following ss i showed the contents of more ca.key

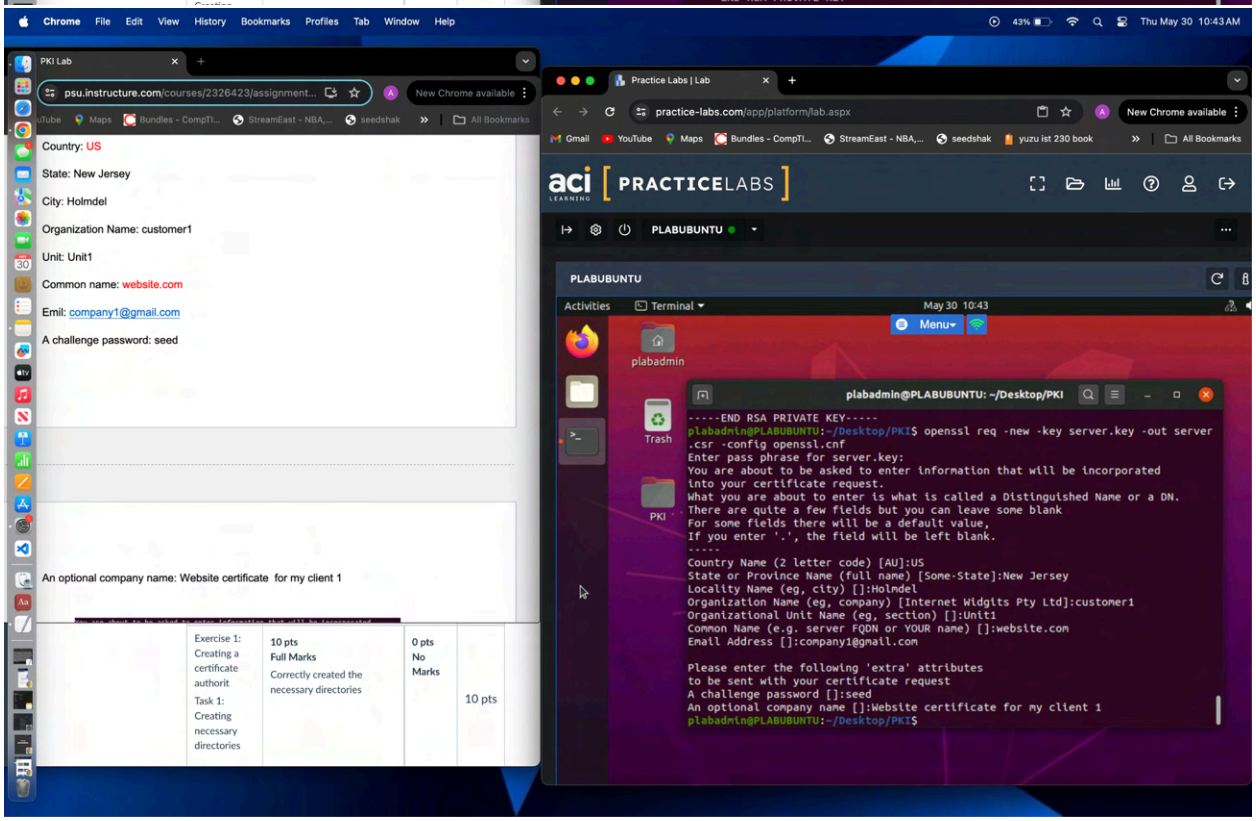


PKI Lab report by Anthony Coppolecchia

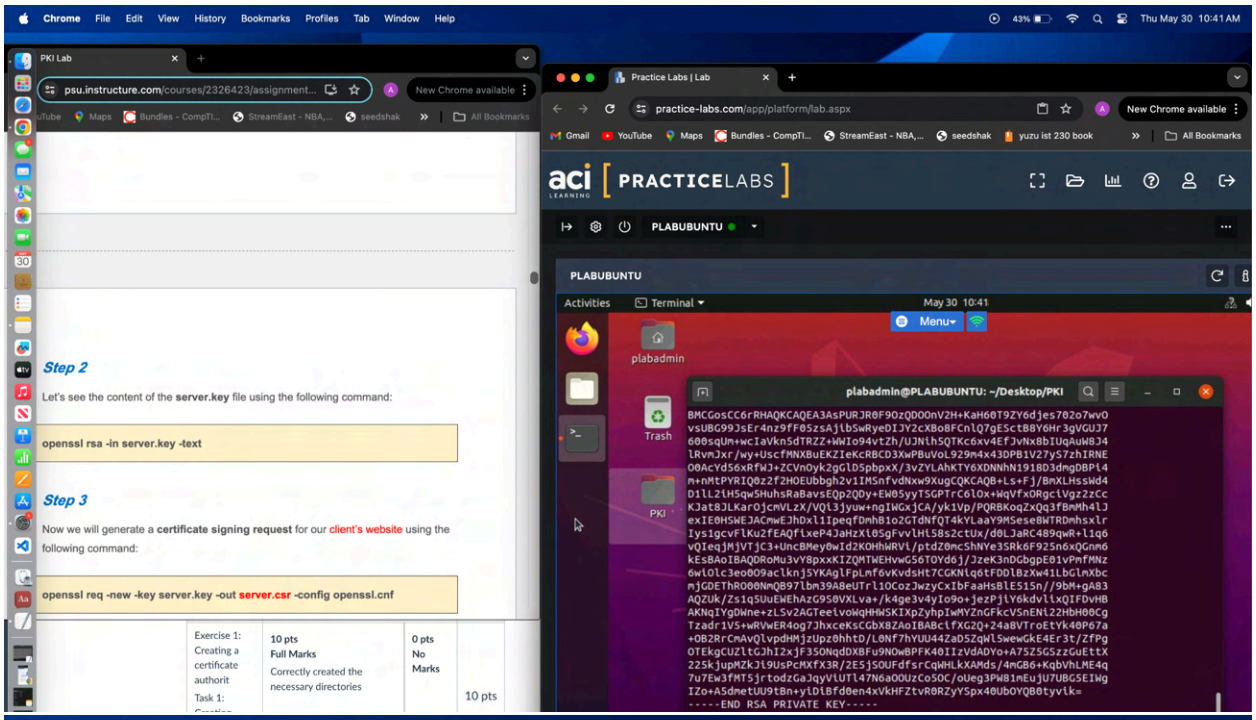


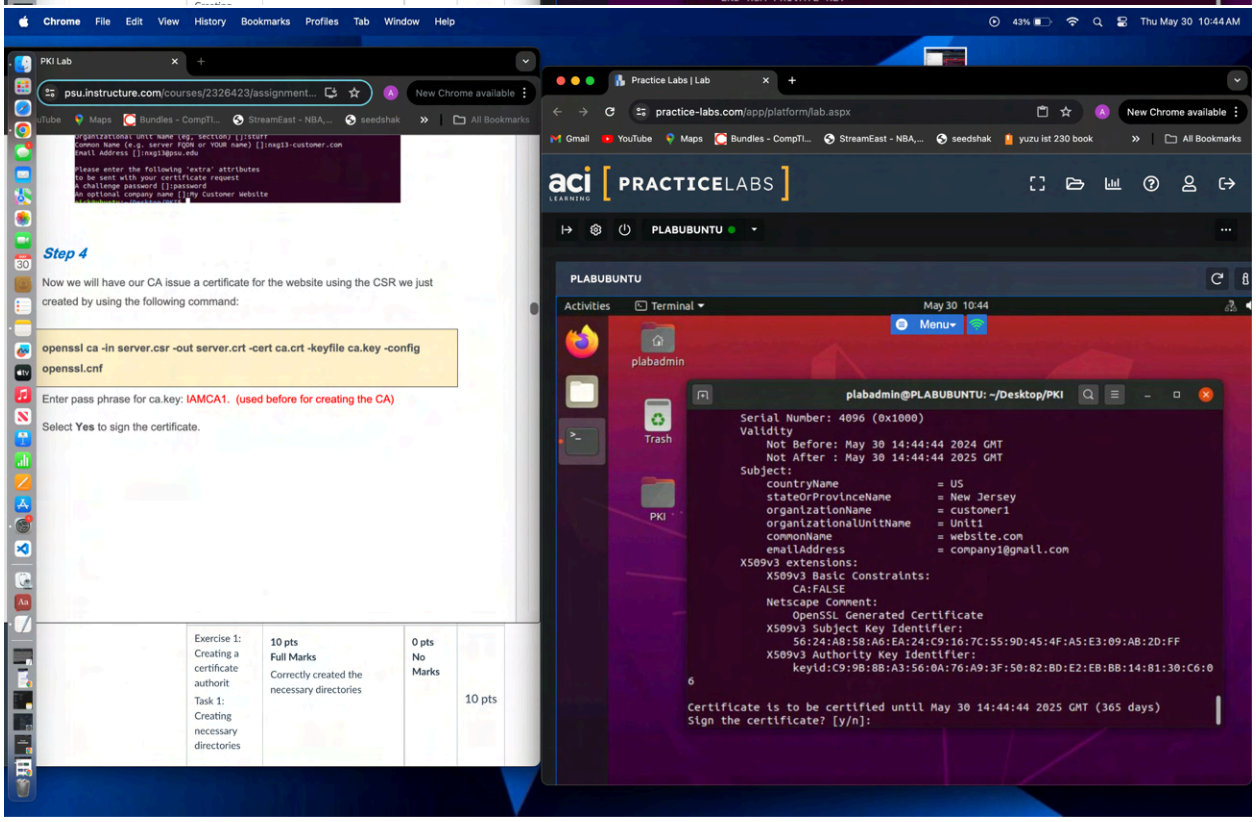
PKI Lab report by Anthony Coppolecchia



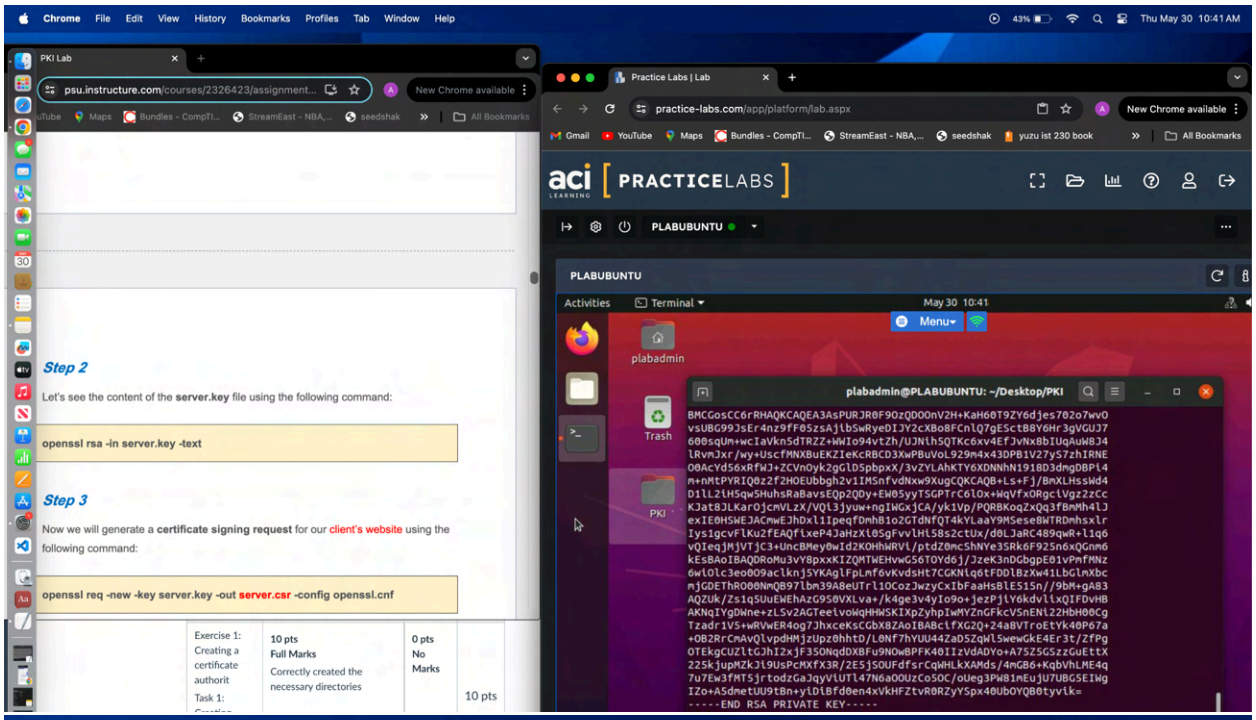


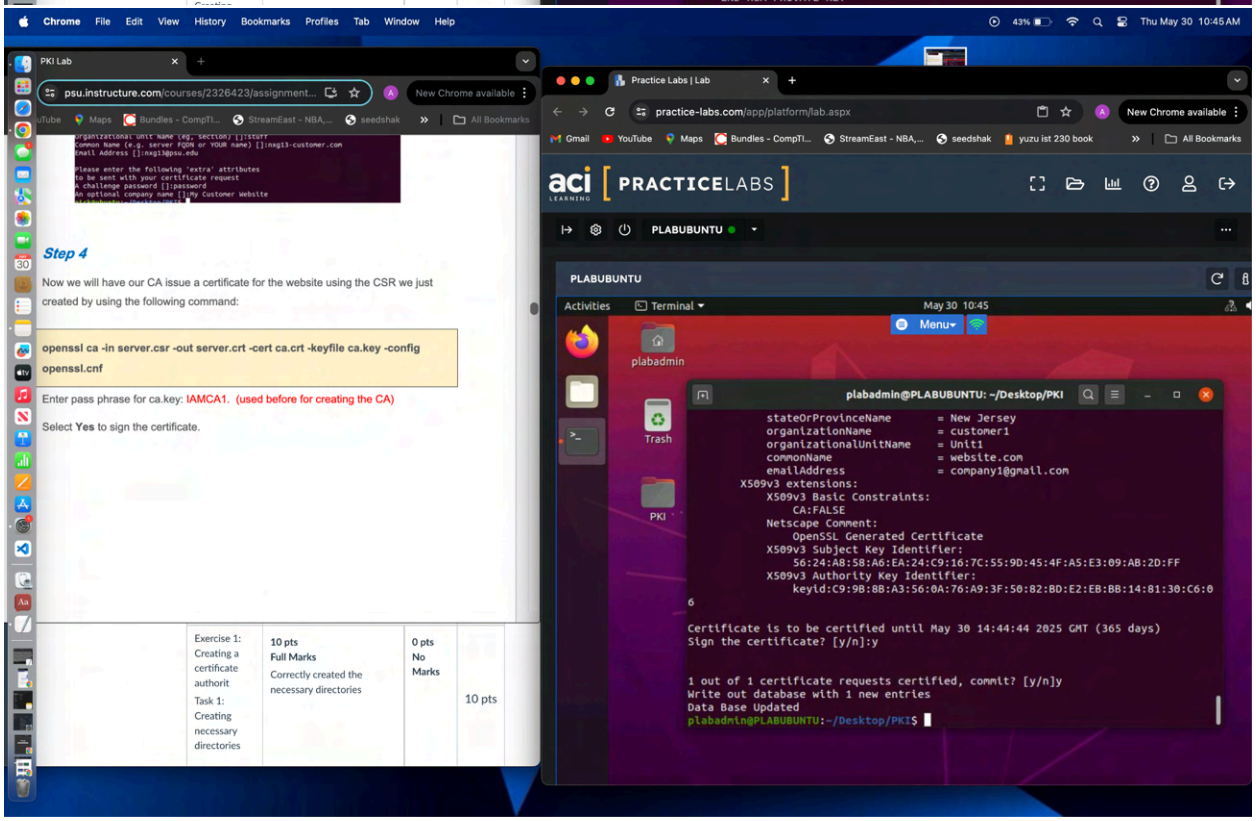
PKI Lab report by Anthony Coppolecchia



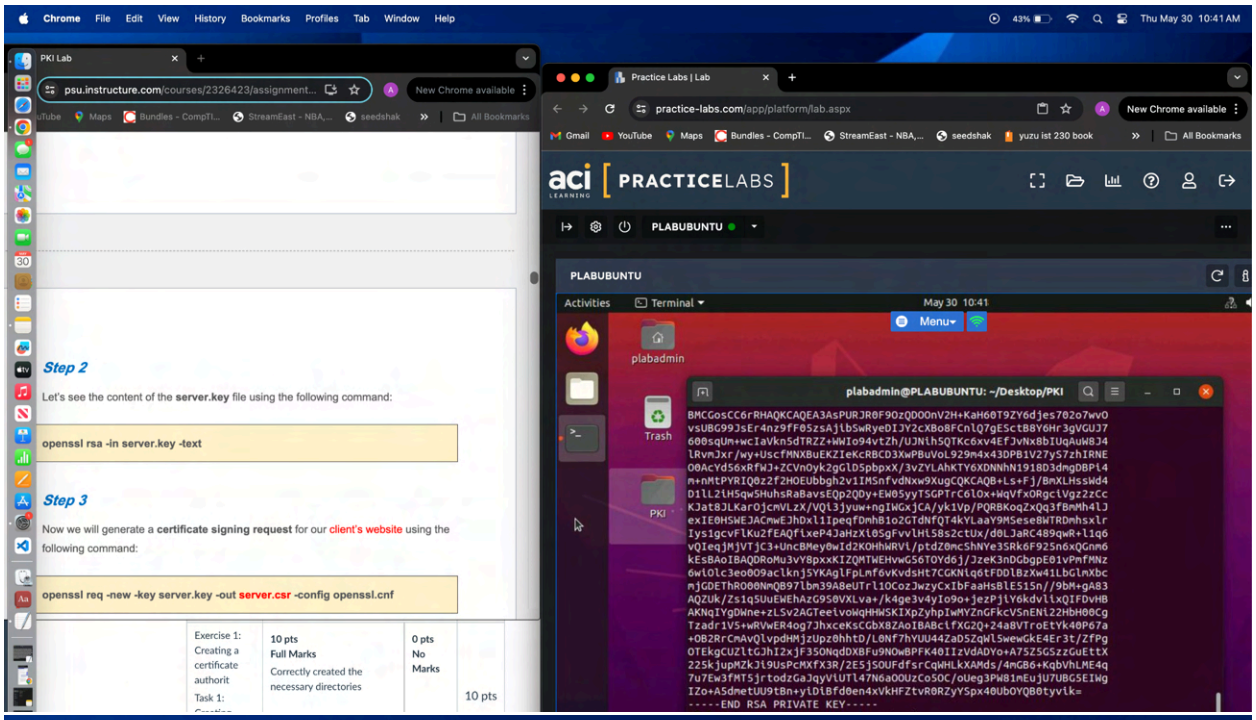


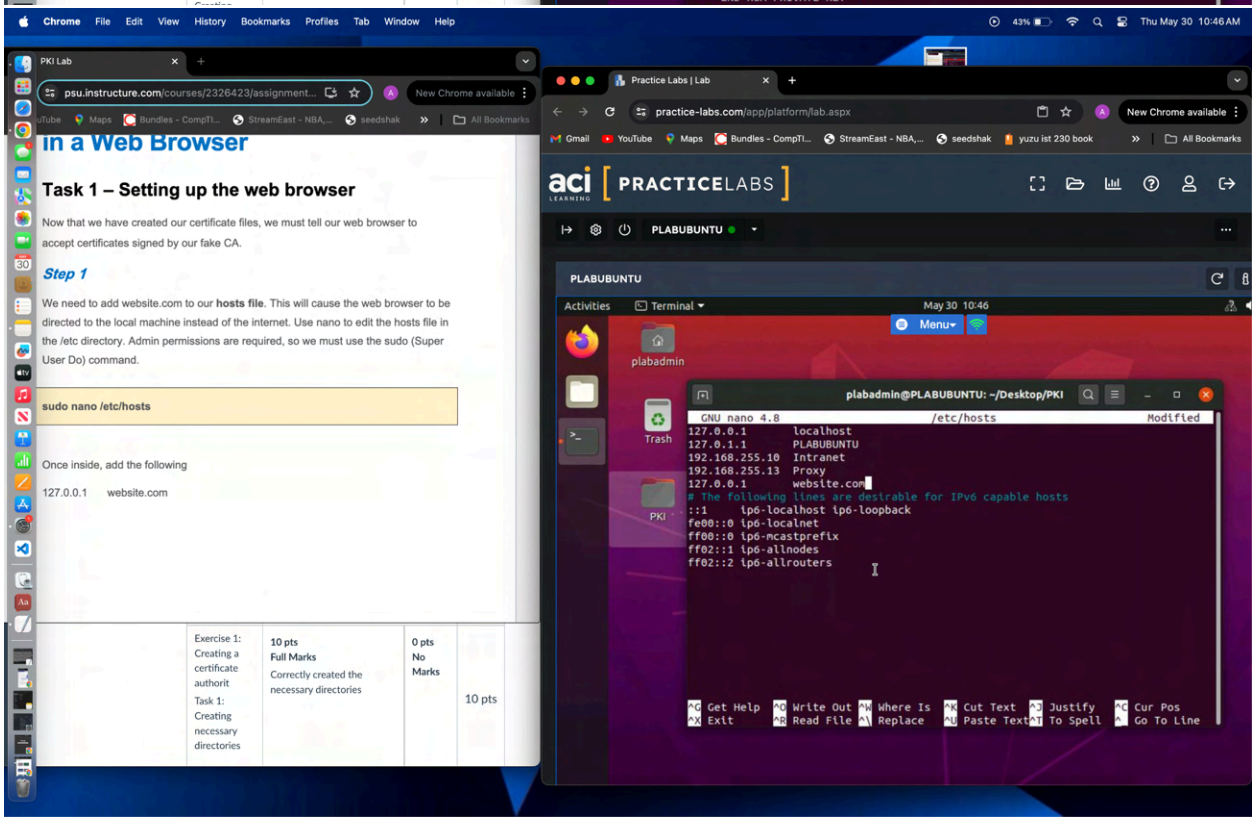
PKI Lab report by Anthony Coppolecchia



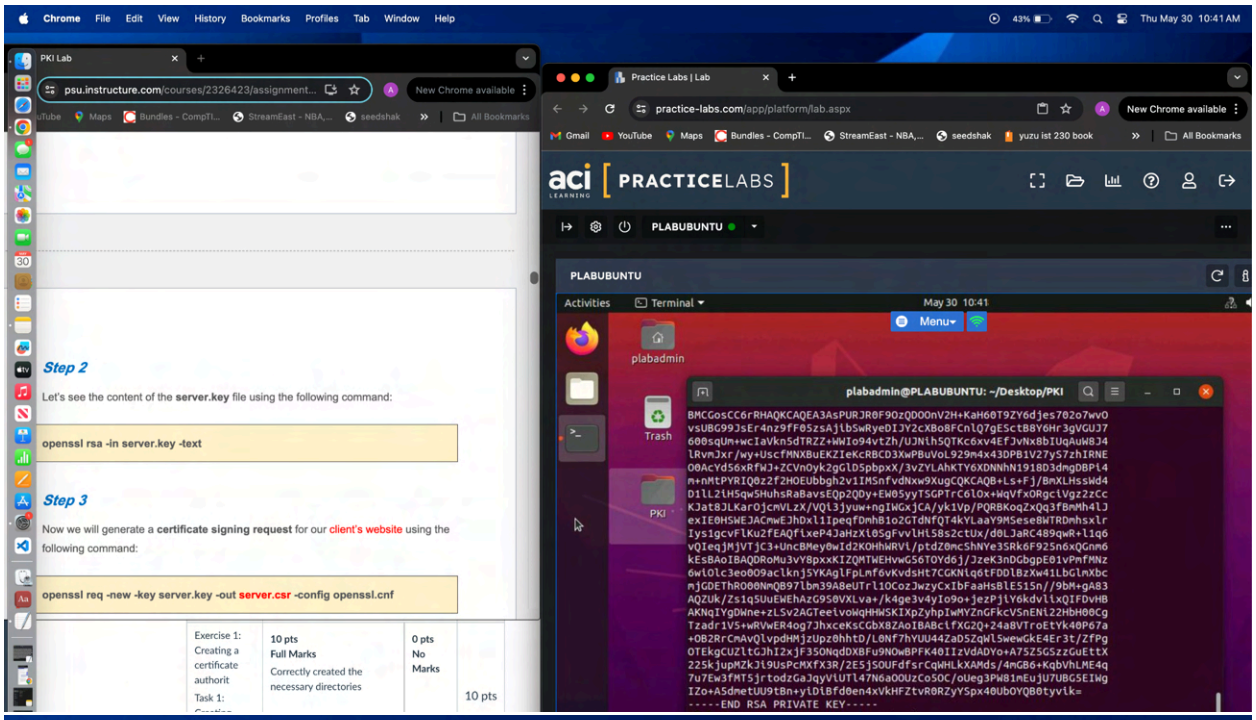


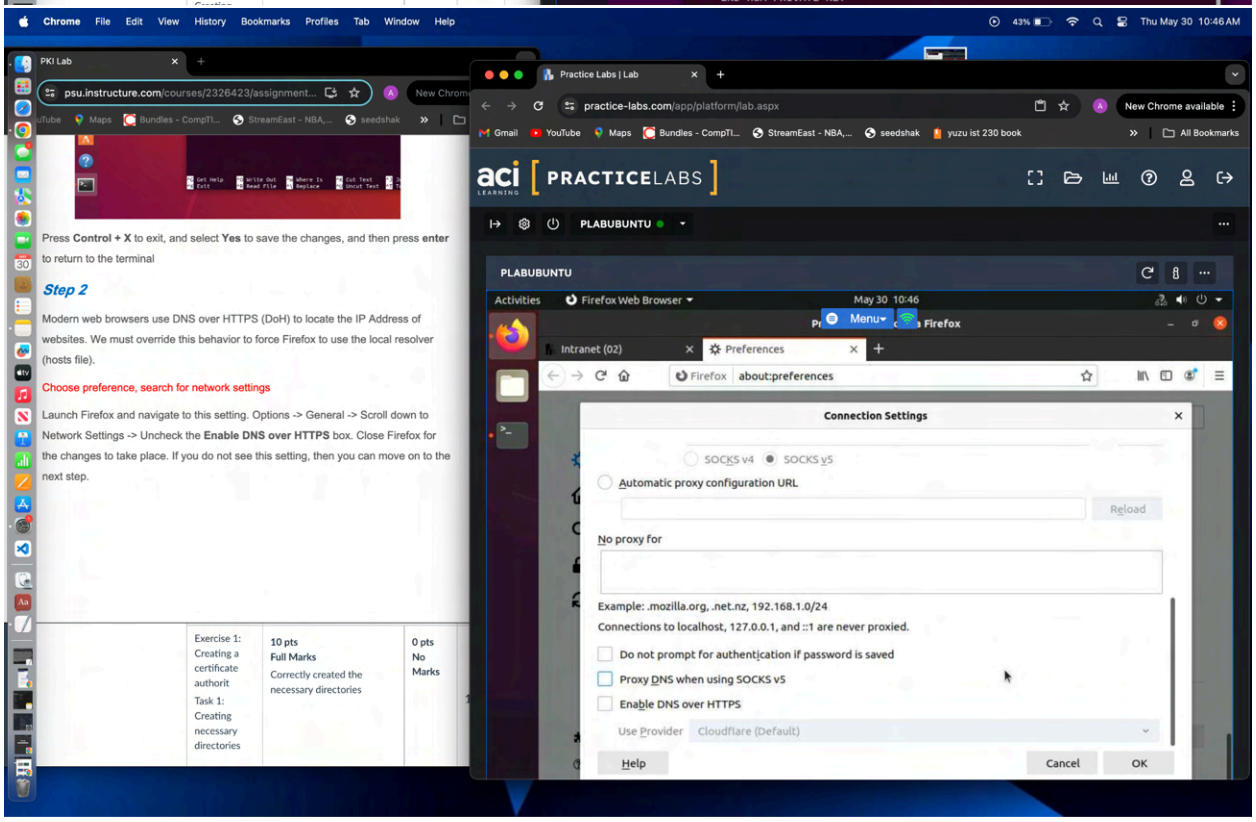
PKI Lab report by Anthony Coppolecchia



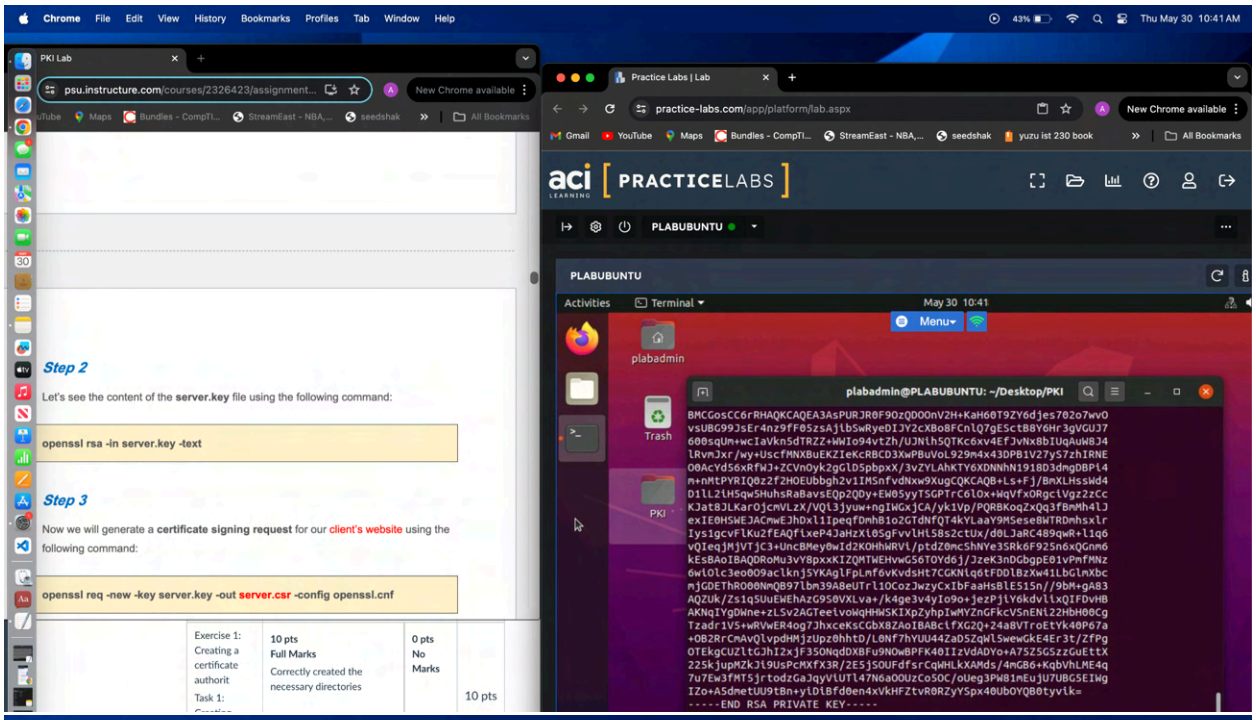


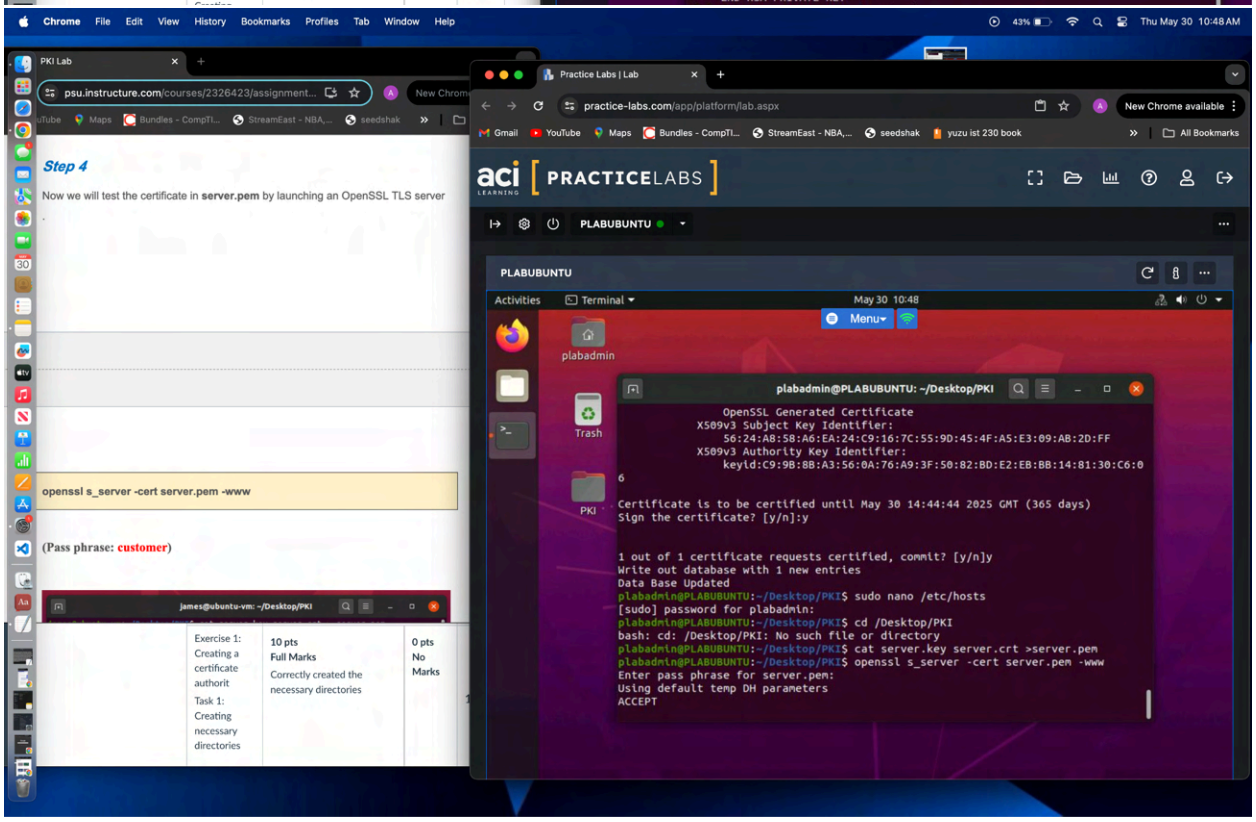
PKI Lab report by Anthony Coppolecchia



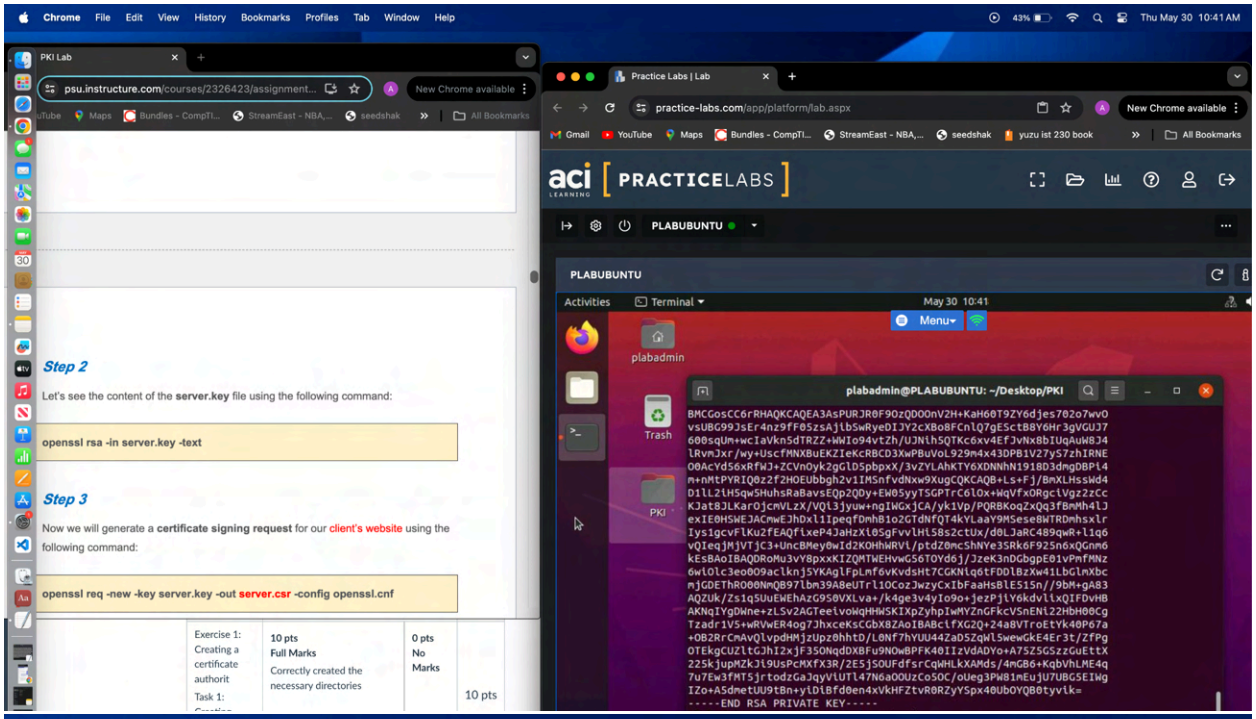


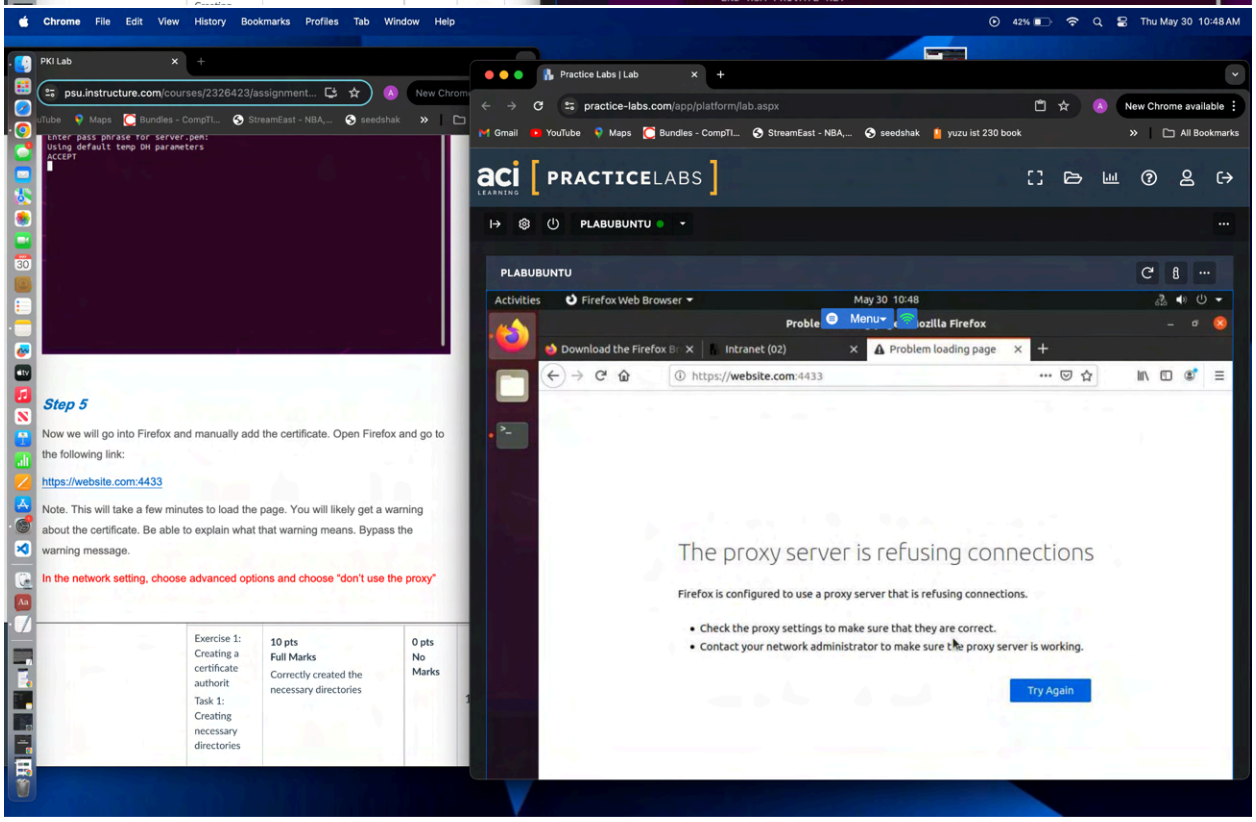
PKI Lab report by Anthony Coppolecchia



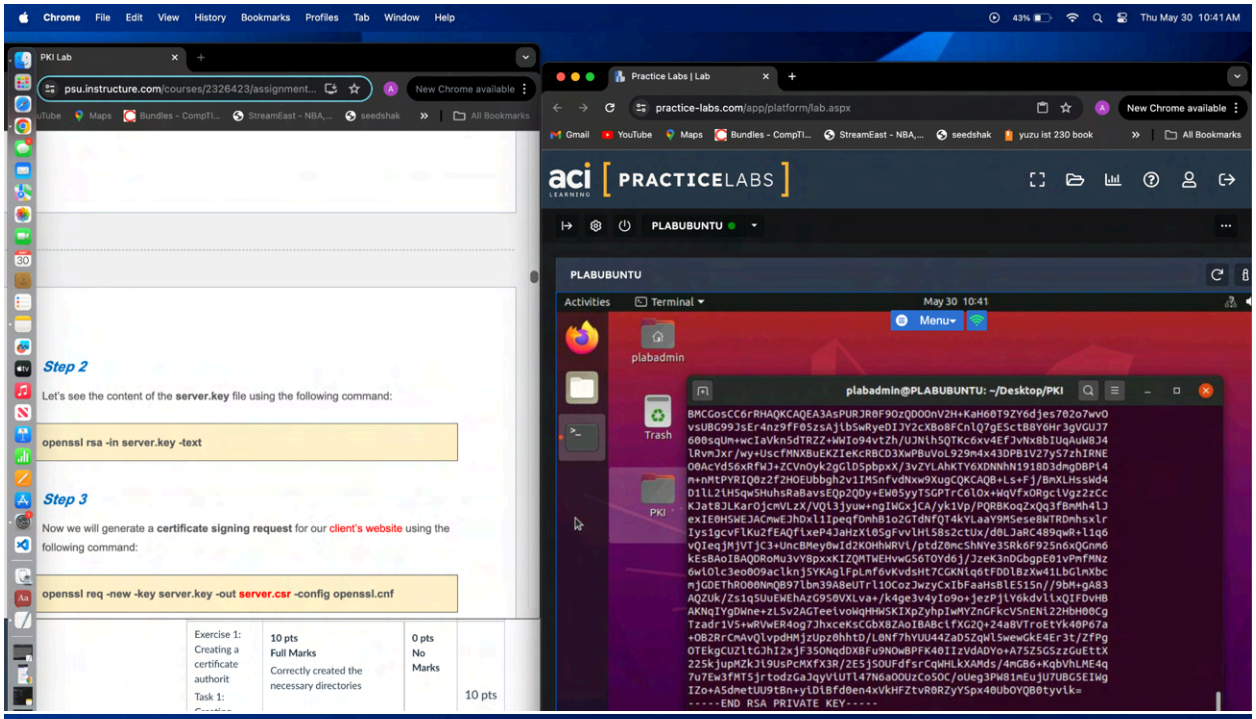


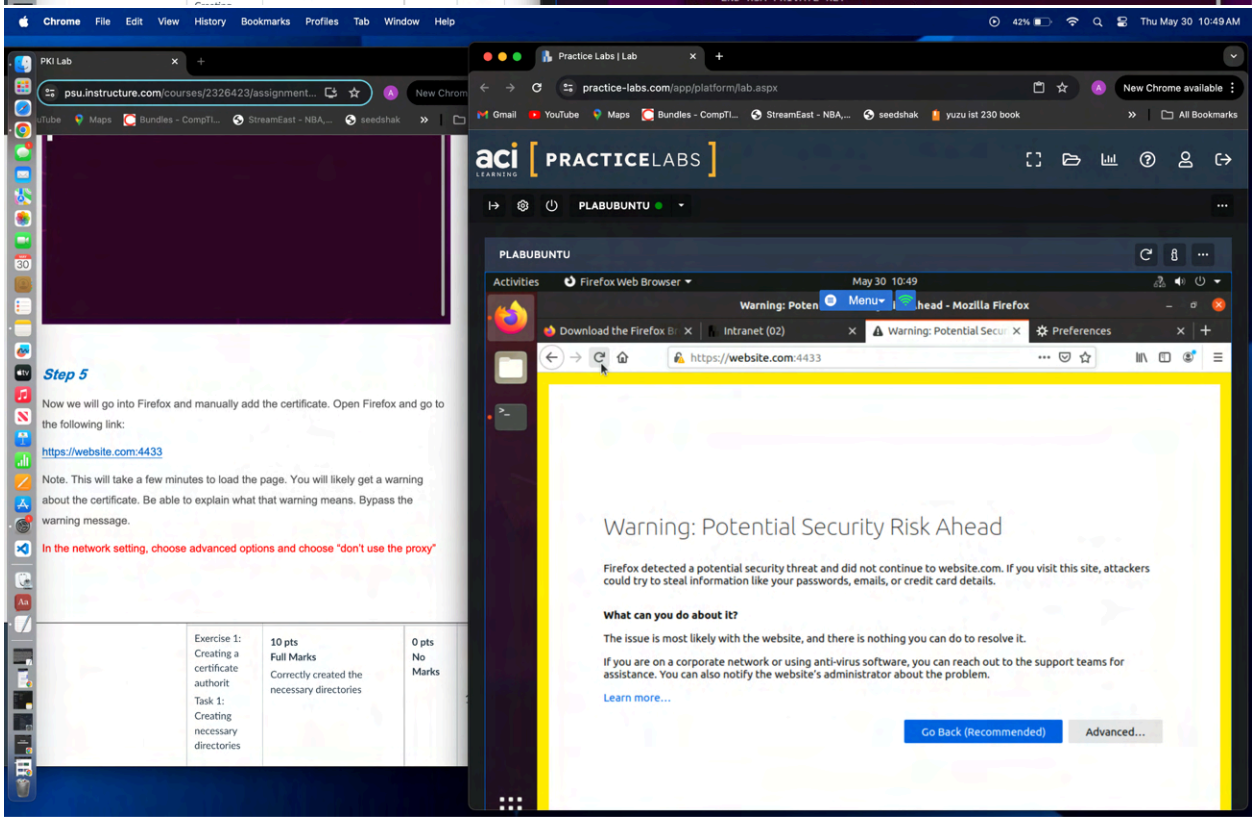
PKI Lab report by Anthony Coppolecchia



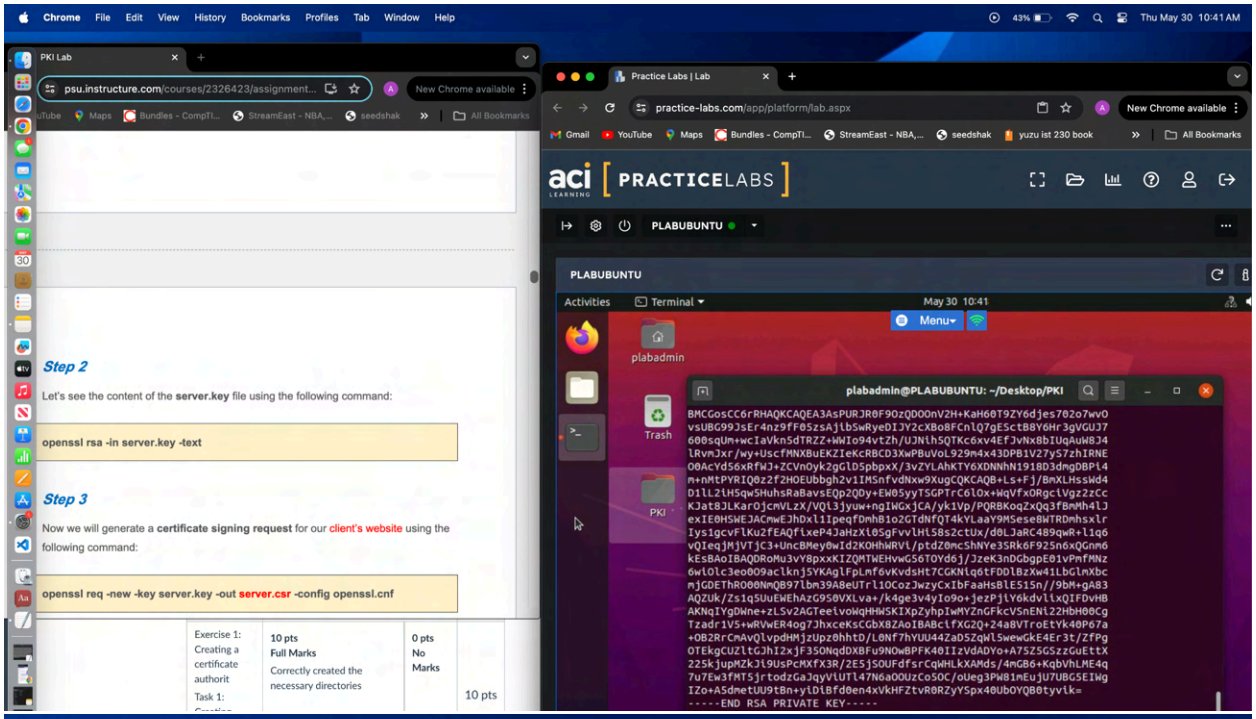


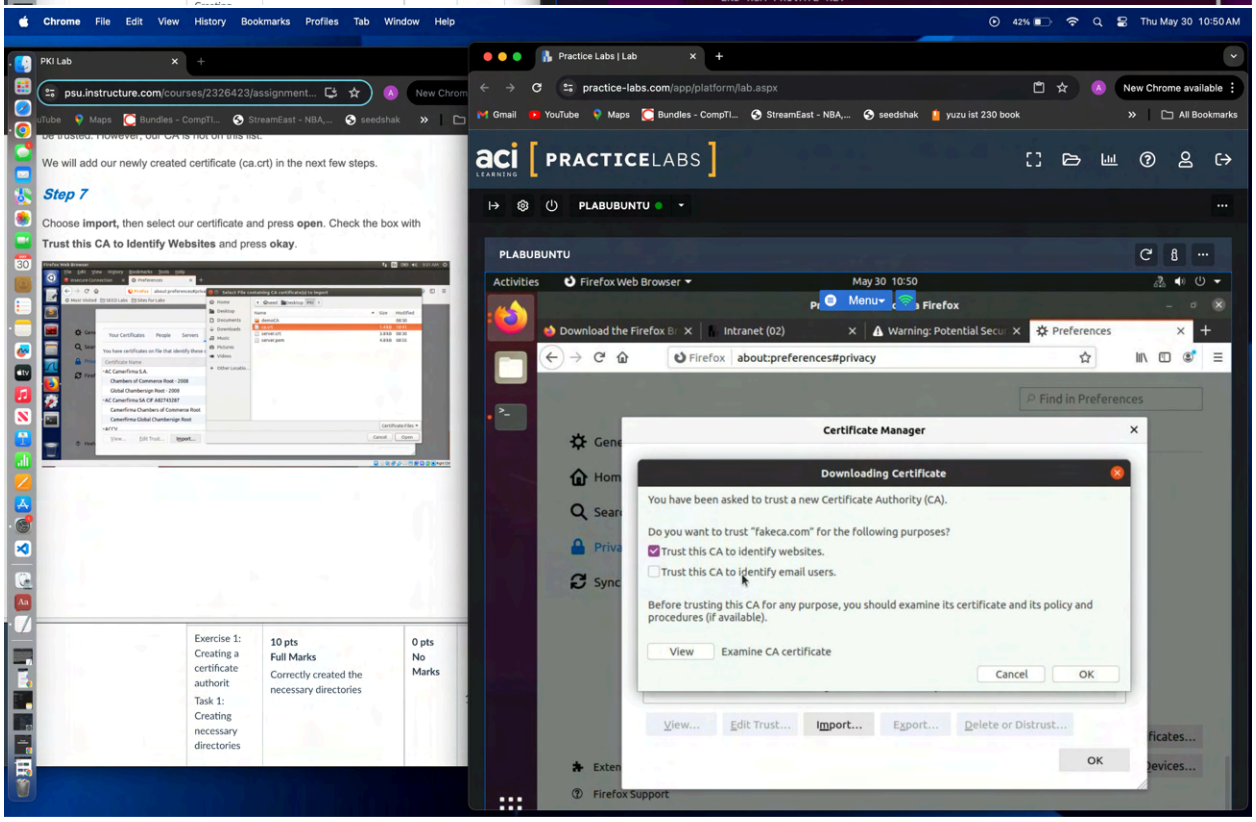
PKI Lab report by Anthony Coppolecchia



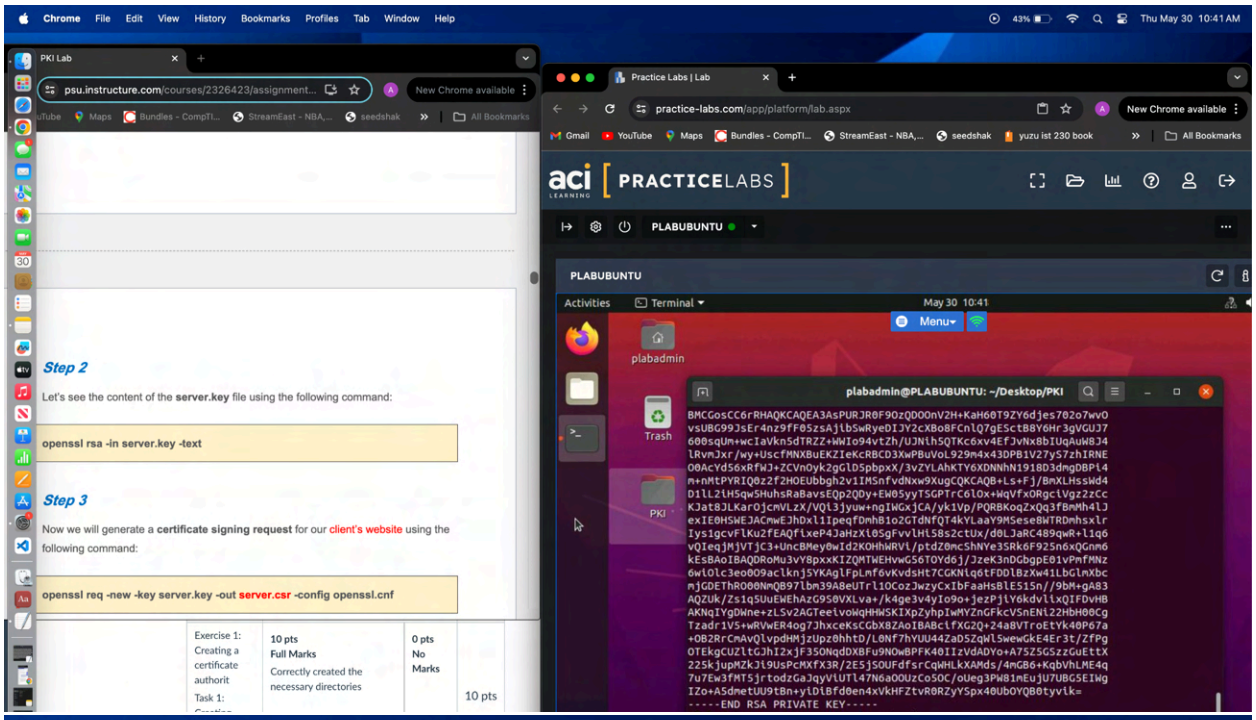


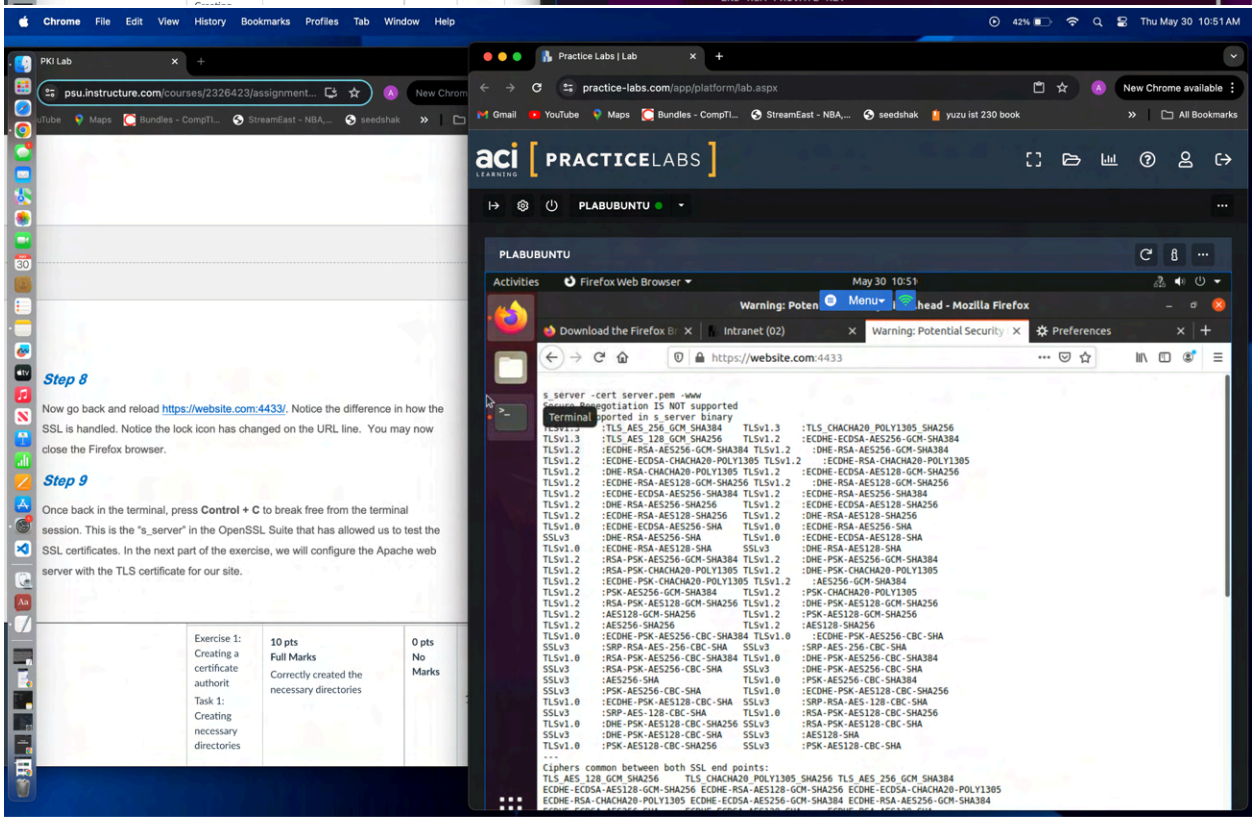
PKI Lab report by Anthony Coppolecchia



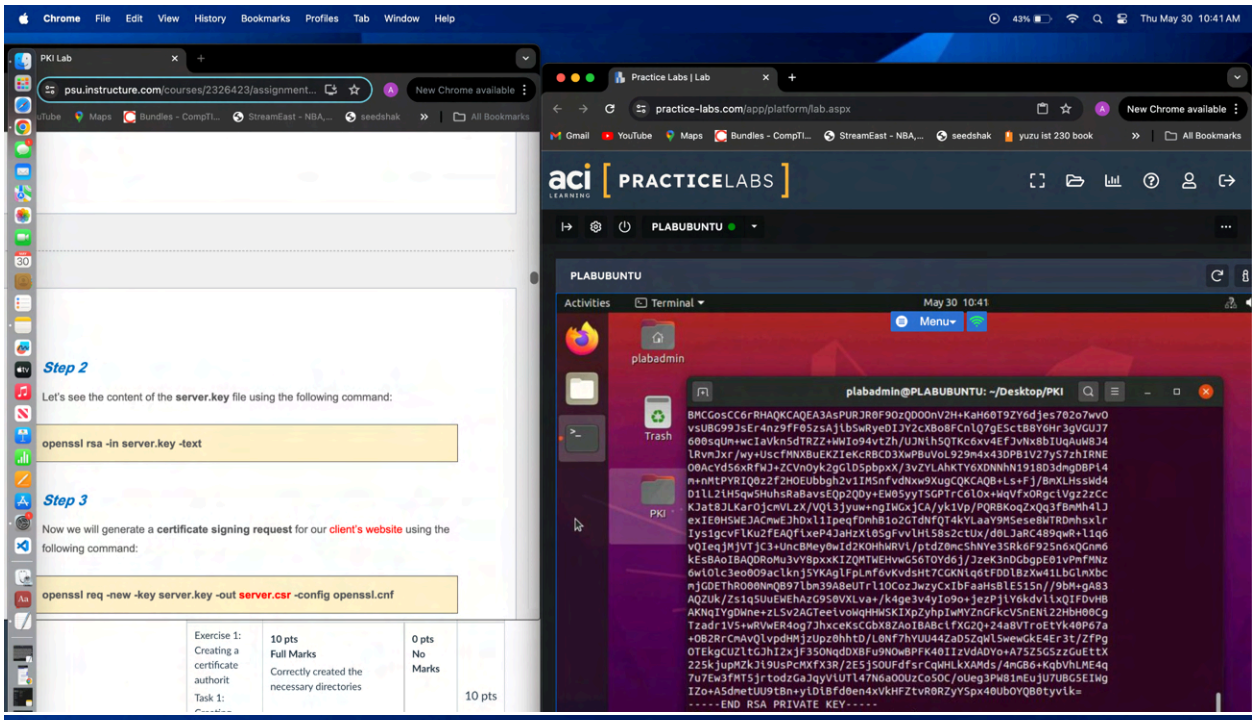


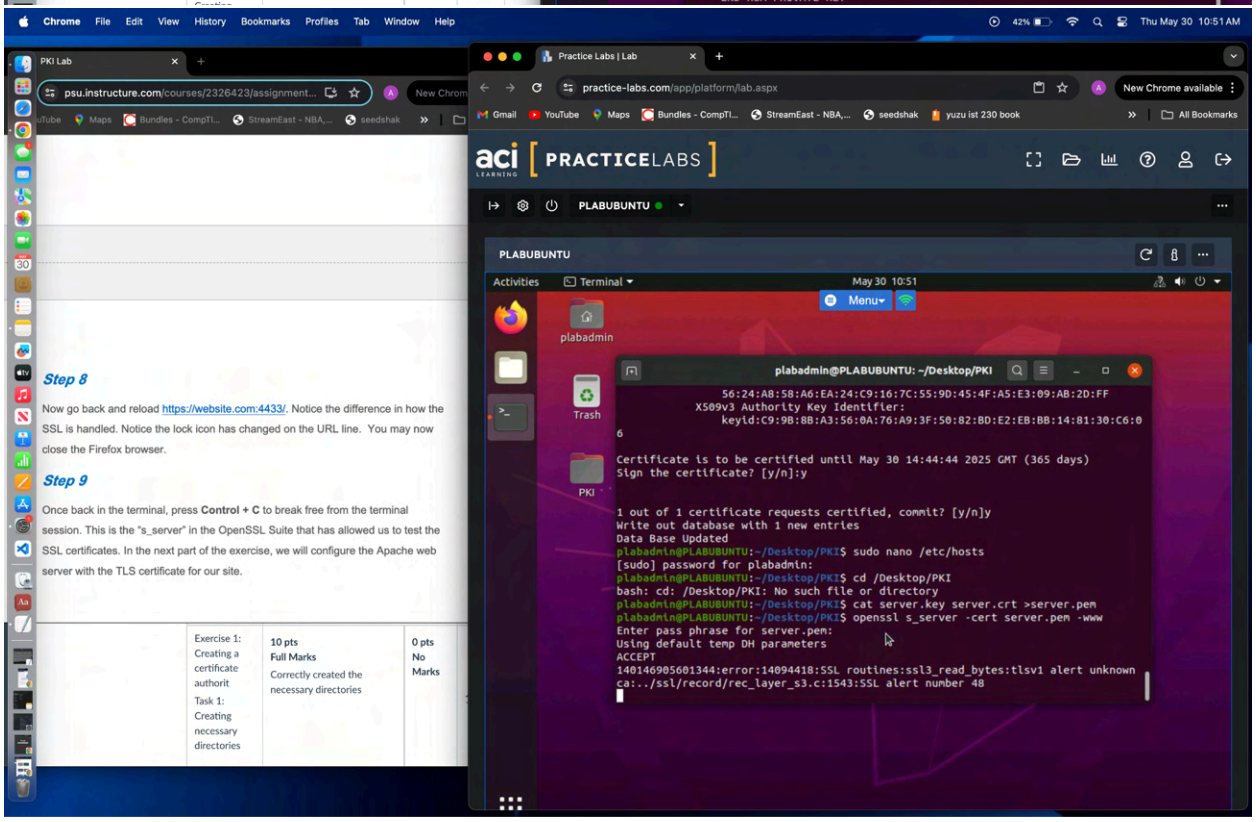
PKI Lab report by Anthony Coppolecchia



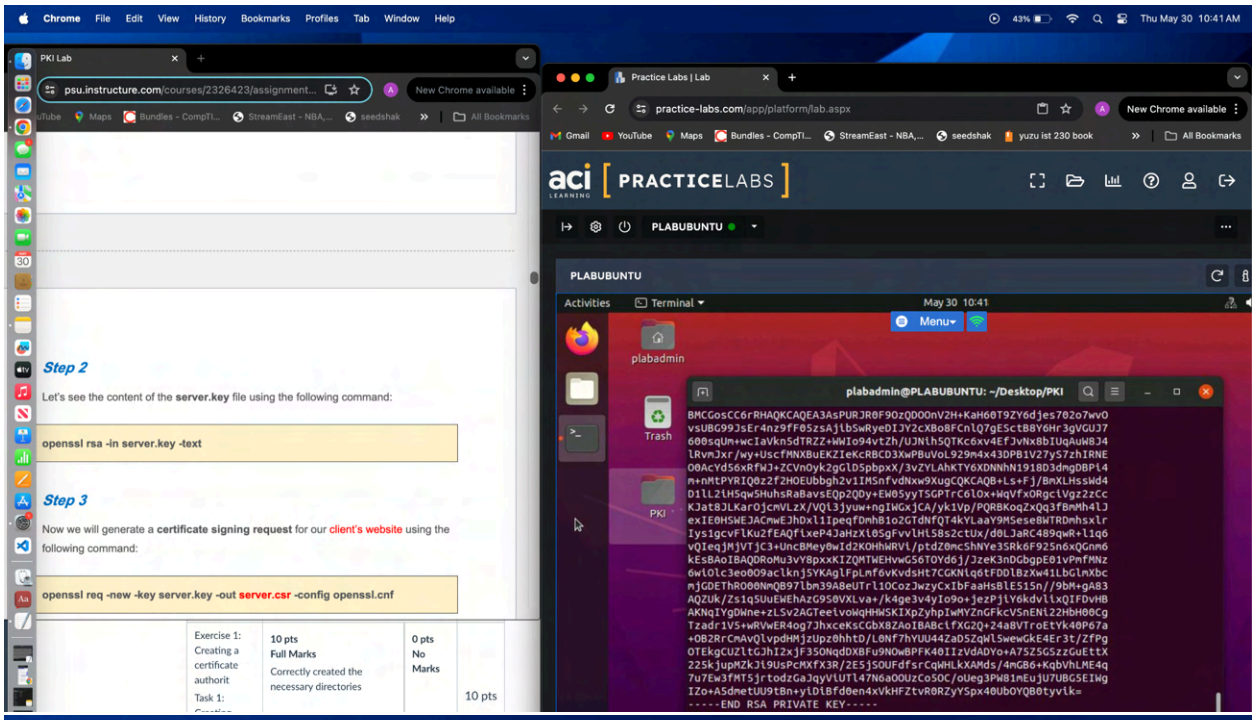


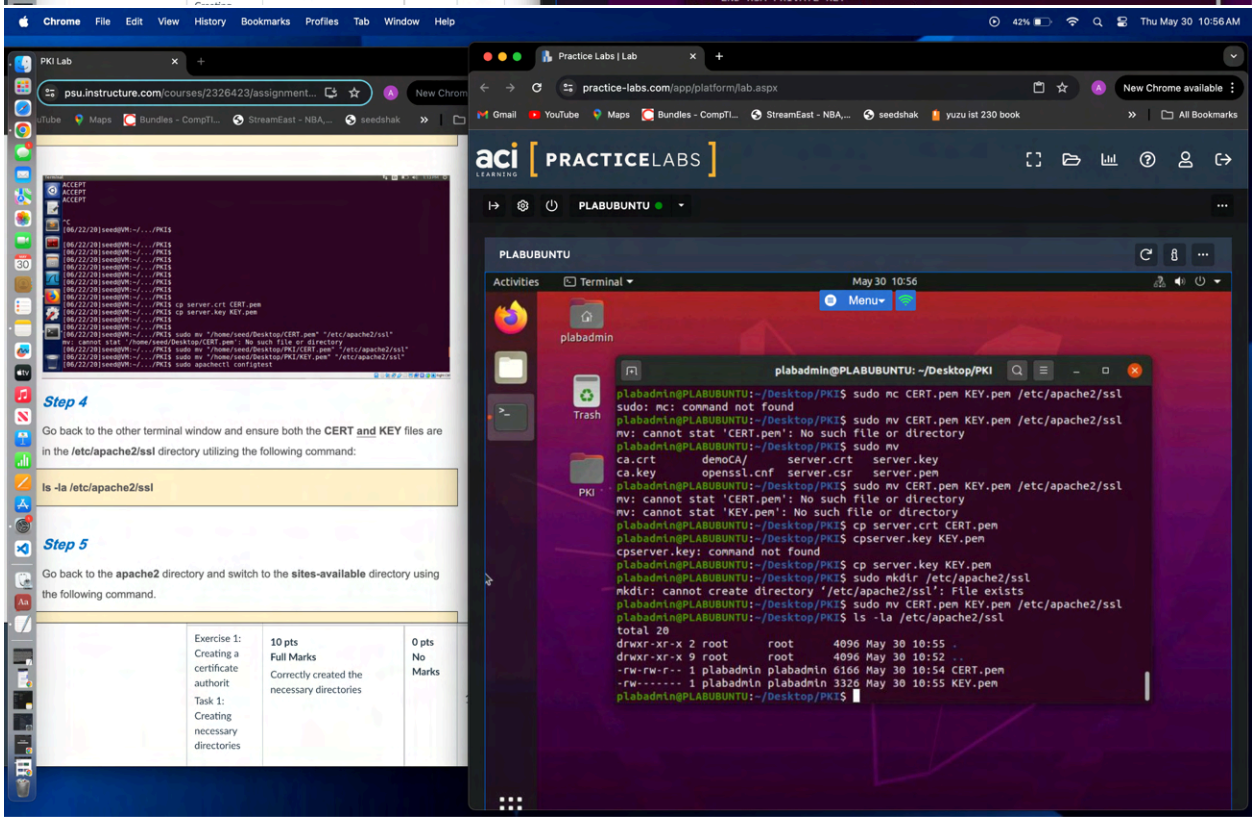
PKI Lab report by Anthony Coppolecchia



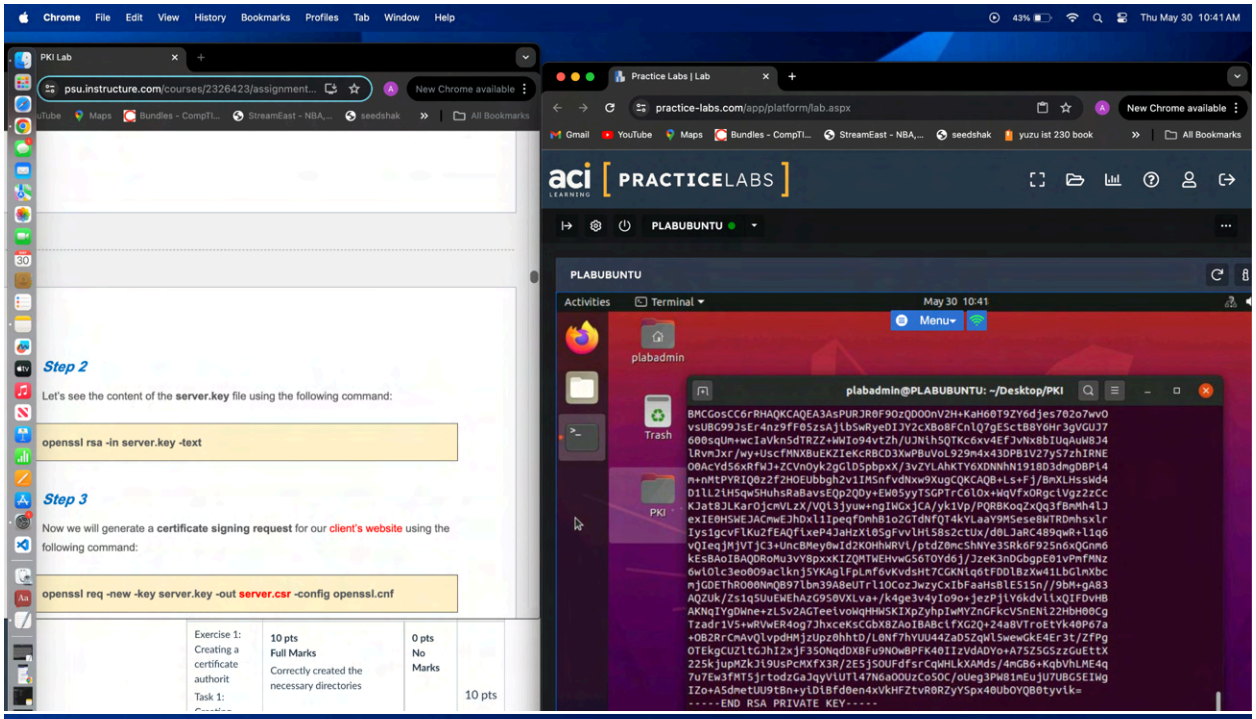


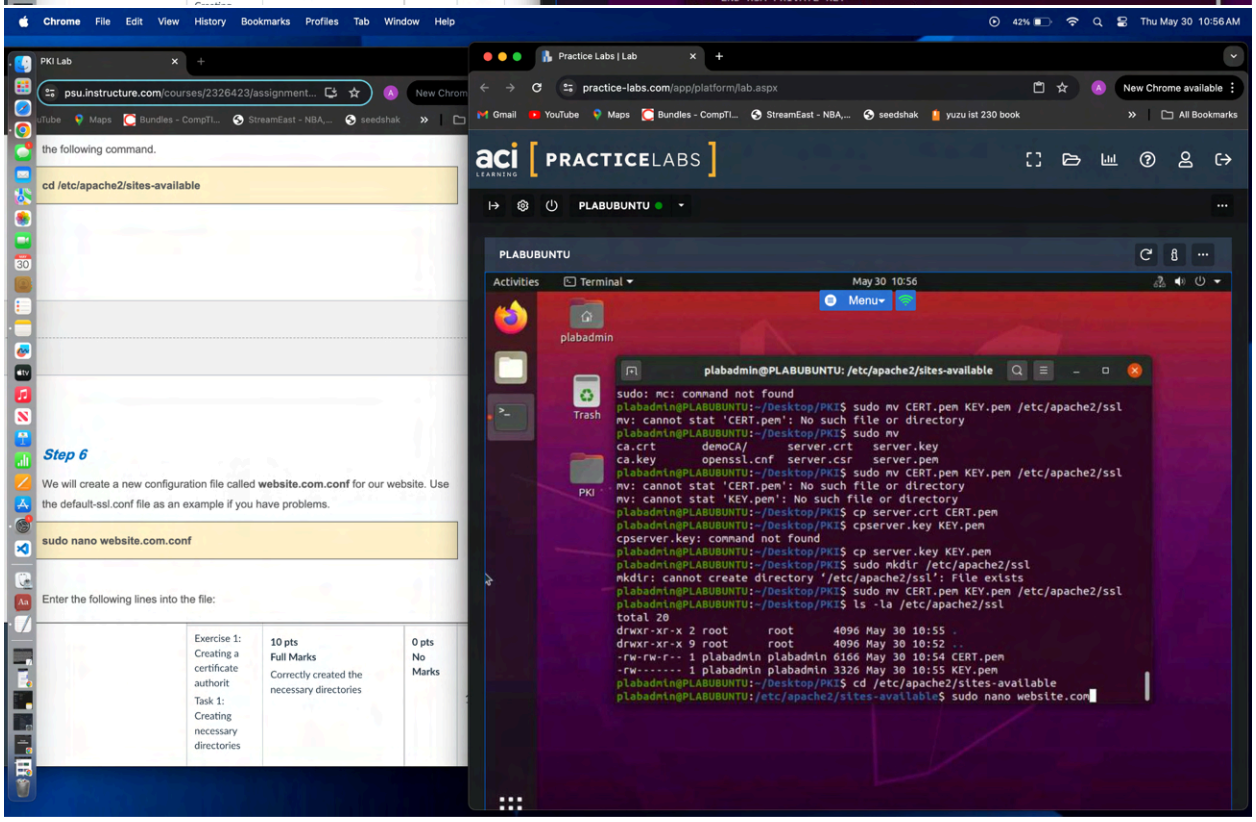
PKI Lab report by Anthony Coppolecchia



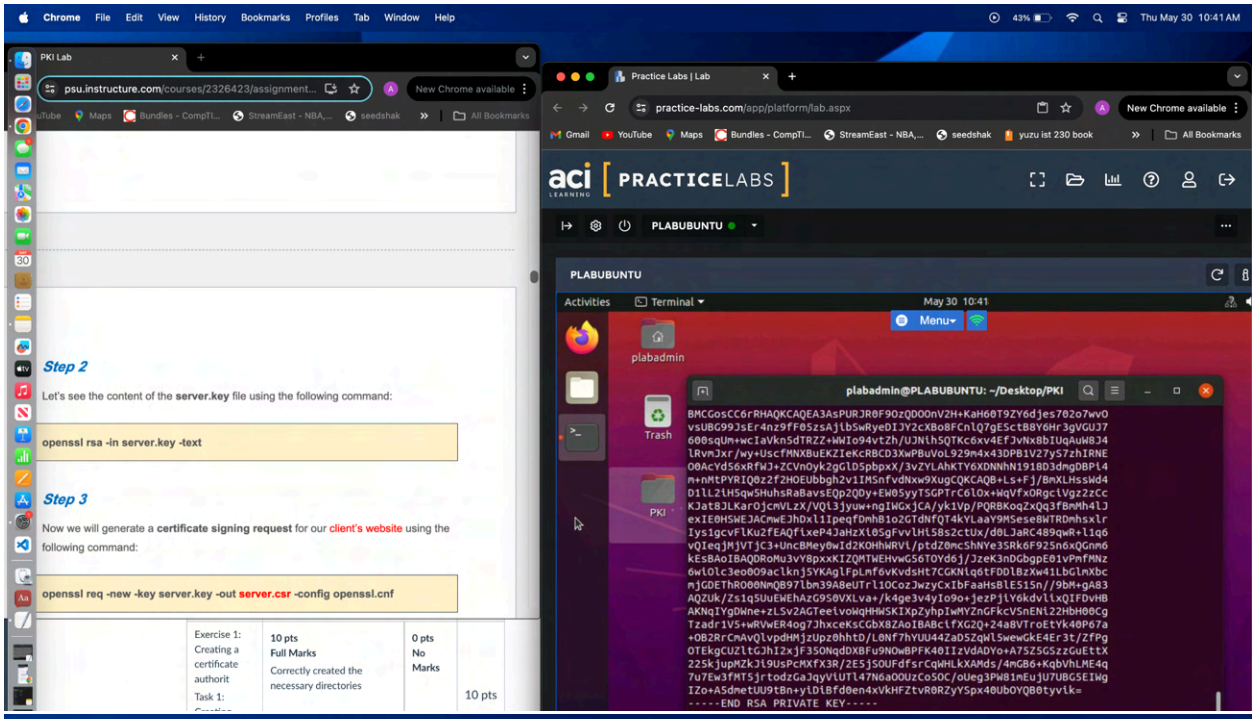


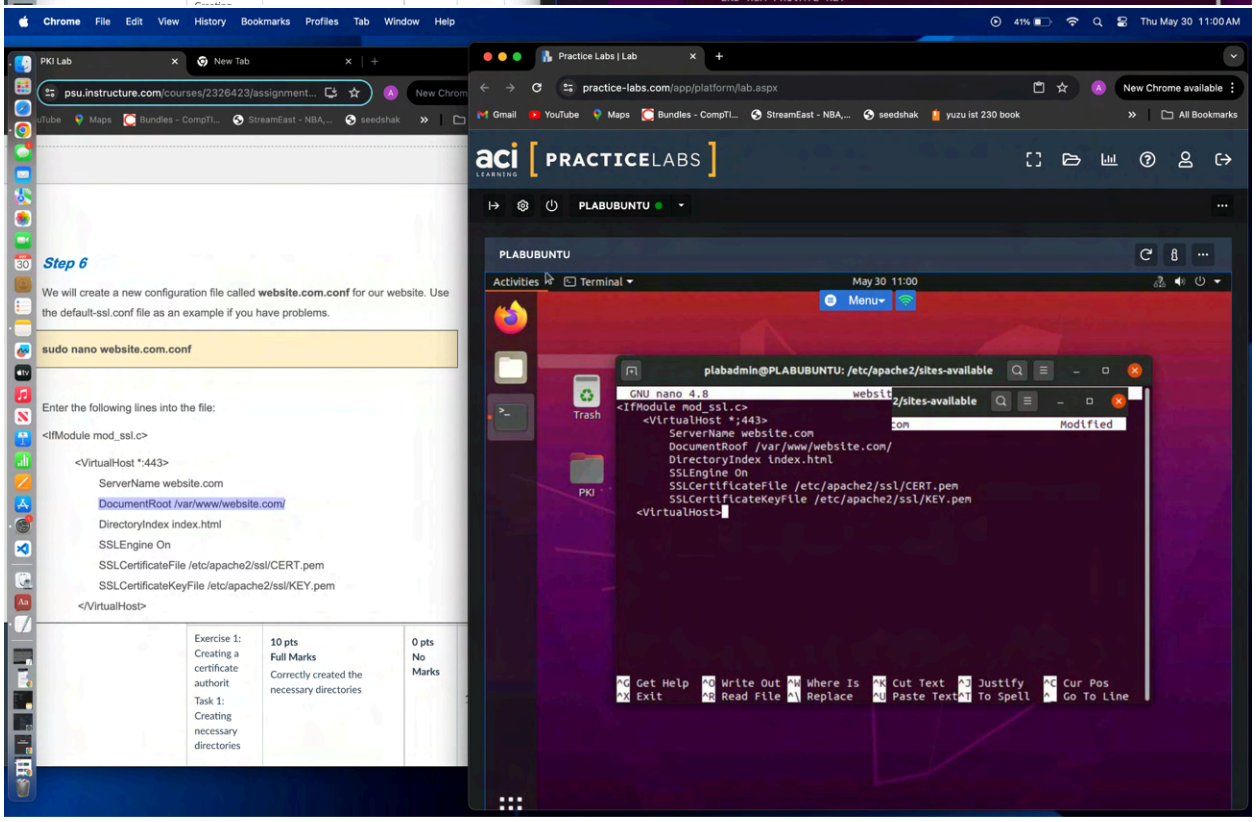
PKI Lab report by Anthony Coppolecchia



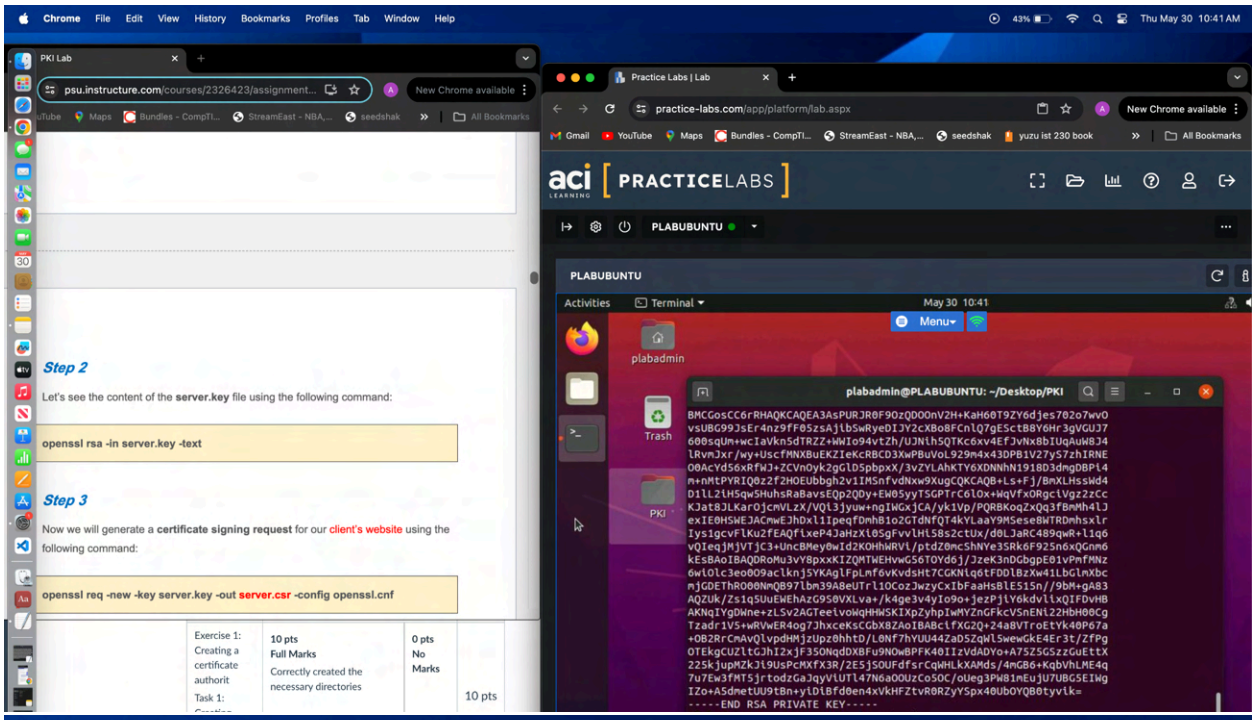


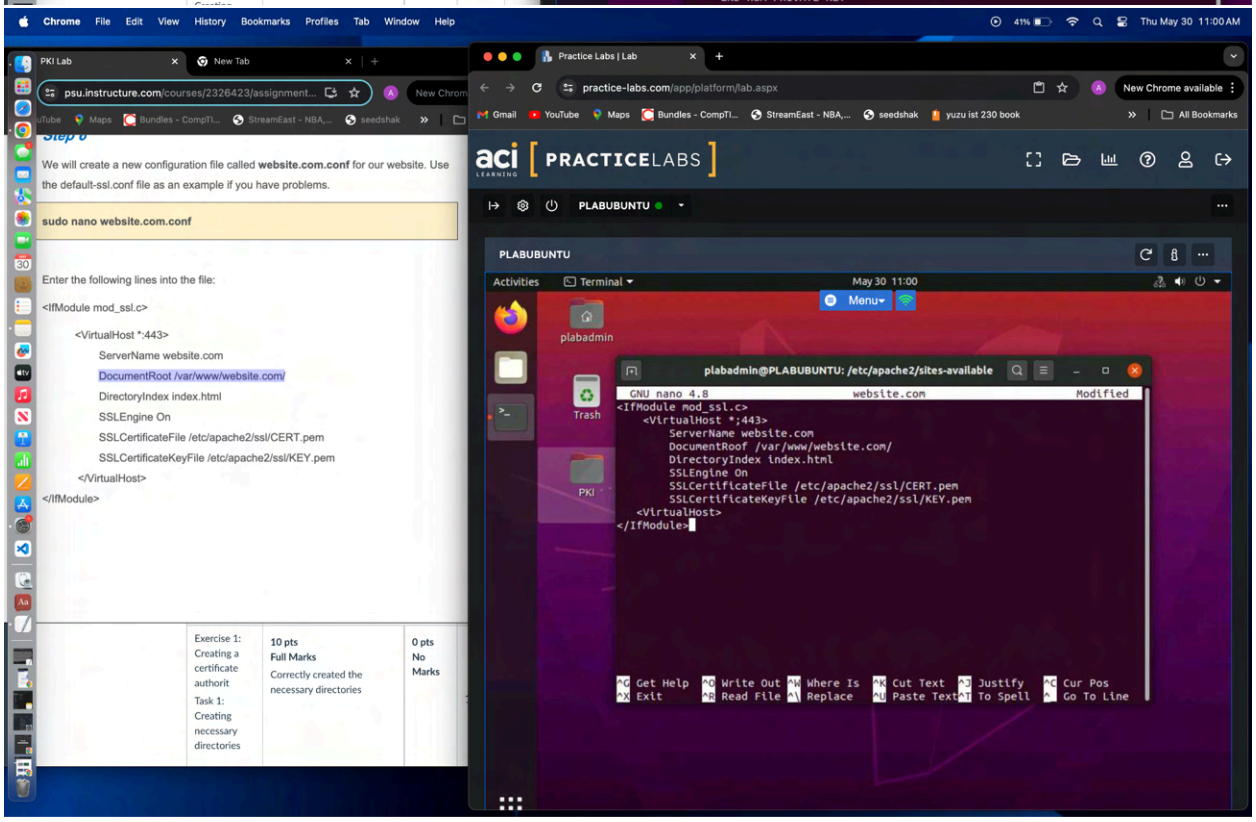
PKI Lab report by Anthony Coppolecchia



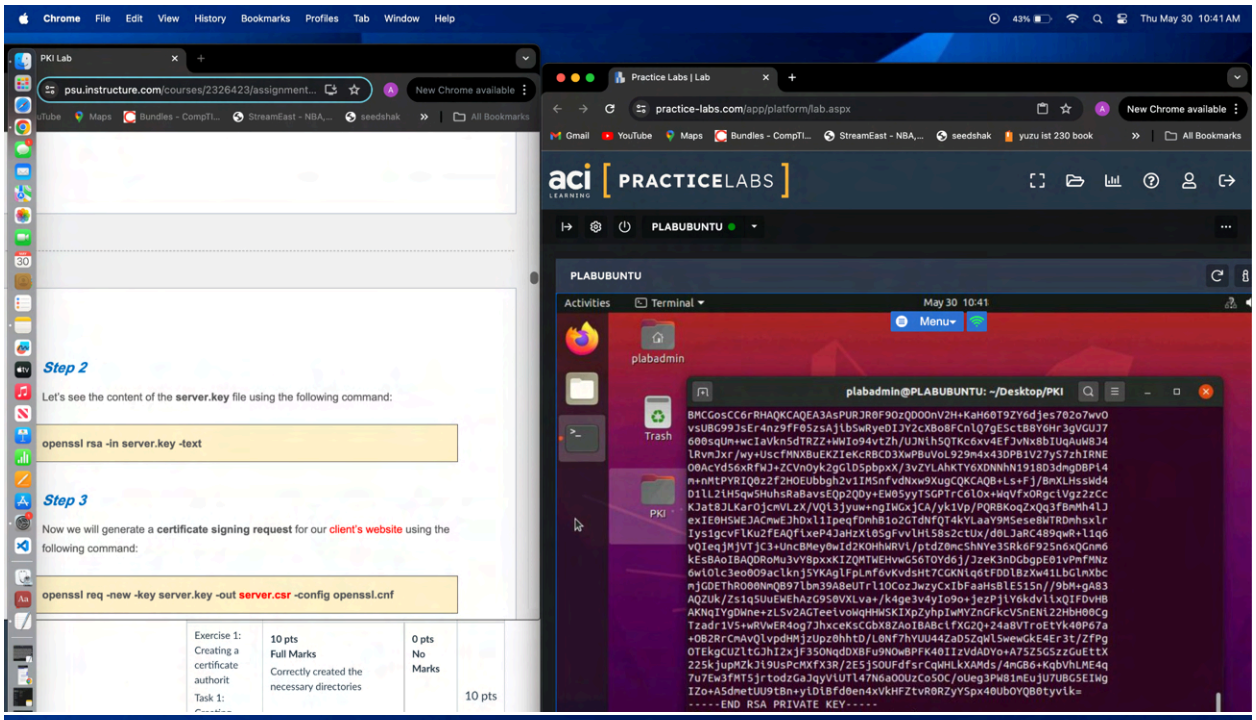


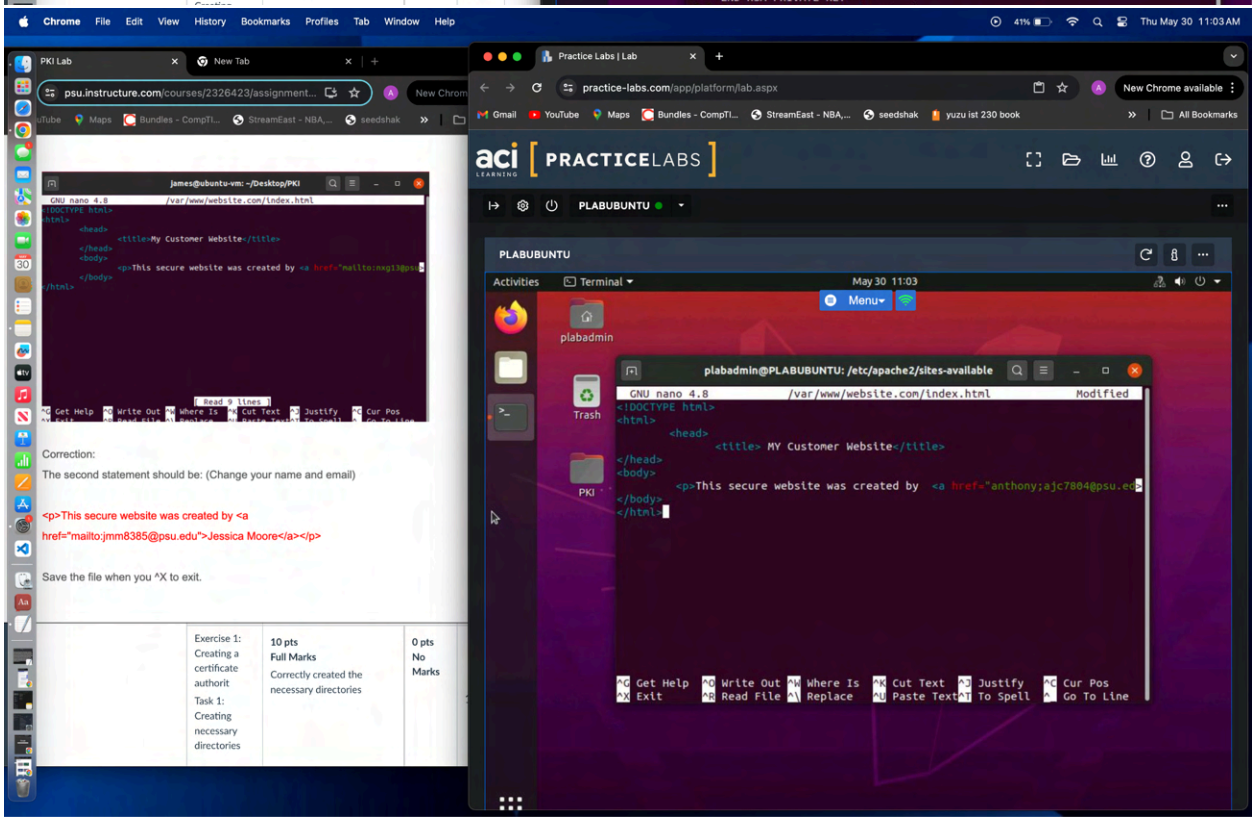
PKI Lab report by Anthony Coppolecchia



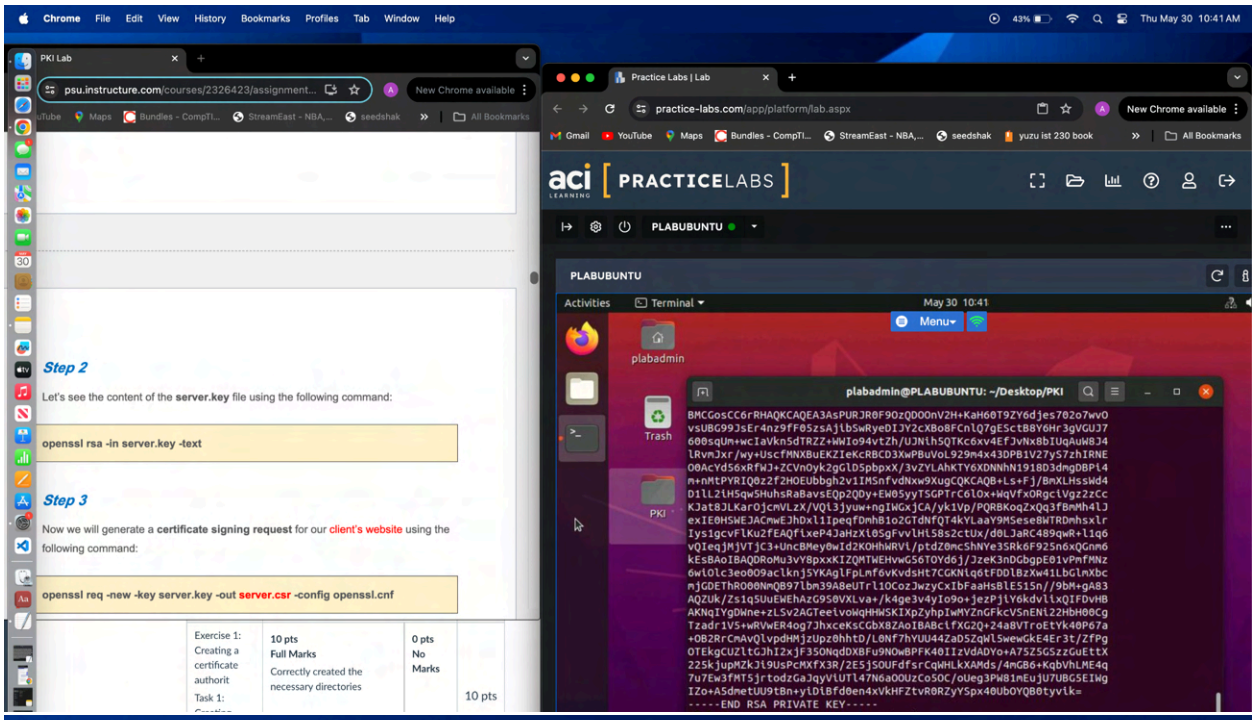


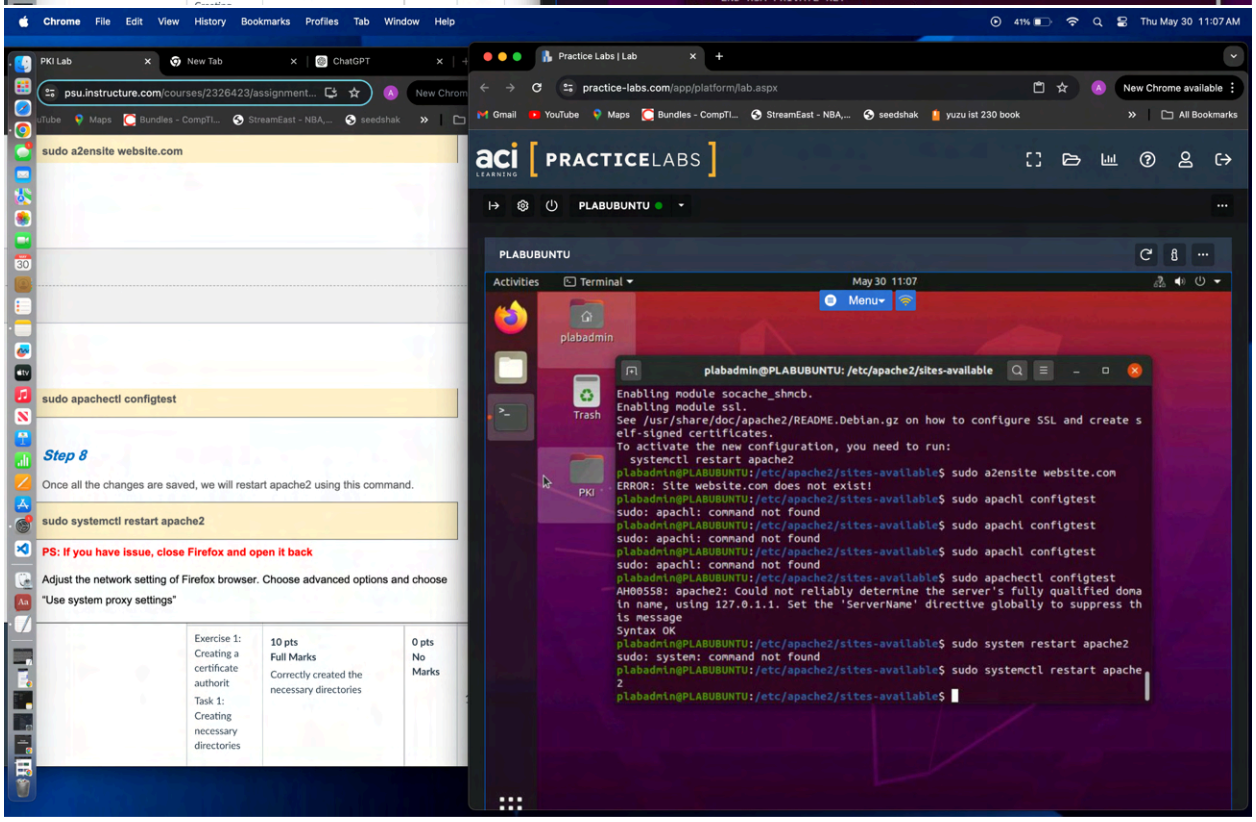
PKI Lab report by Anthony Coppolecchia





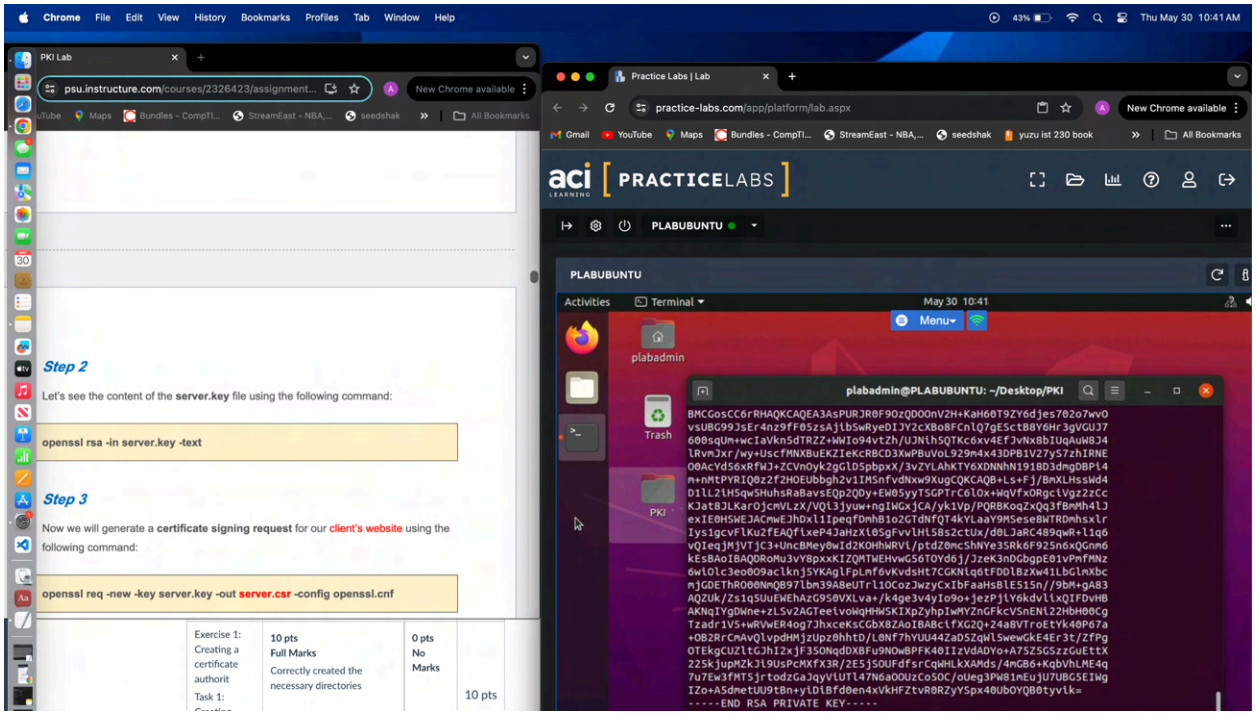
PKI Lab report by Anthony Coppolecchia





It was too hard to get my comments and text in between each screenshot so i will type my walkthrough here, next i checkek nontents of pki directory using ls -la. Next we generated a 4096 bit rsa public and private key pair for website.com and encrypted it to -aes256.
Next i viewed and showed the content of server.key file. Then i generated a certificate request signing for the website.com. Next we had the CA issue a certificate for the website using the

PKI Lab report by Anthony Coppolecchia



CSR we created. Next we added website.com to our hosts file to view it in web. Next we had to override network preferences and proxy settings. Next we added the certificate to the webserver with the commands `cd ~/Desktop/PKI`

`cat server.key server.crt > server.pem`

Next we tested the cert in server.pem launching a ssl tls server then we went into firefox and manually added the certificate and bypassed the warning message net we imported our certificate into firefox next we deployed the certificate to a more permanent web server. We created a directory to store certificates in apache 2 then we created and moved the cert.pem and key.pem to the ssl apache 2 directory then we switched to the sites-available directory then we created a new config file called website.com.conf then we created a simple wepface face using html code in the terminal.then we enabled the ssl module and our site config test and tested the files to make sure we get a syntax ok message. Then we restarted apache 2 and adjusted firefox network settings and reoopened https://website.com/ to make sure it is still working and active.