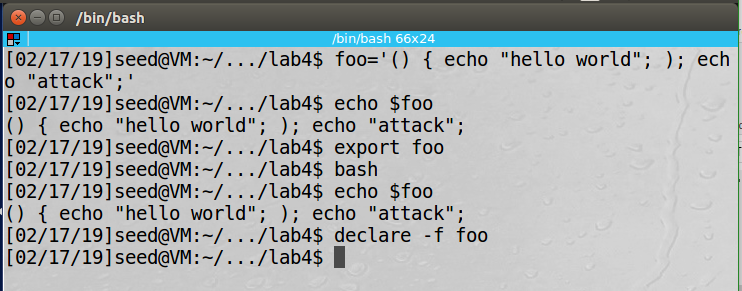
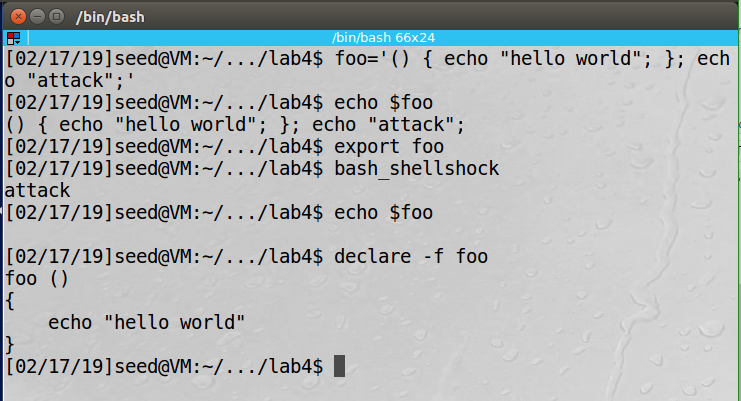
Task 1: with bash



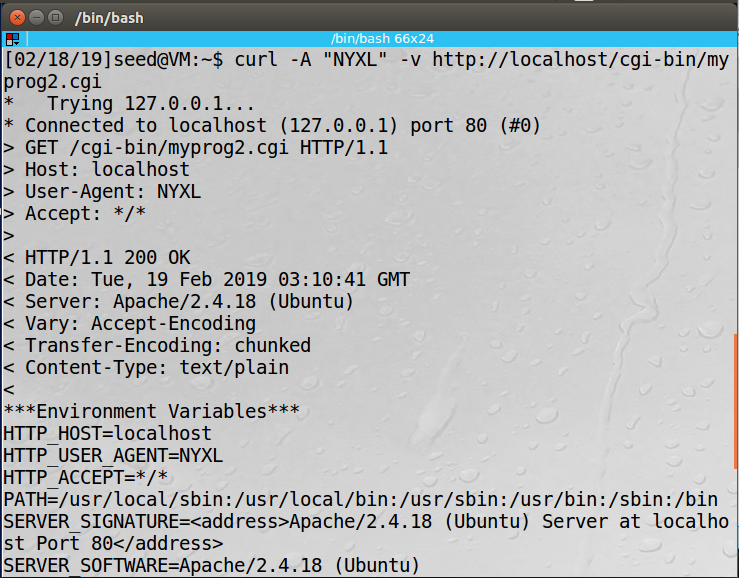
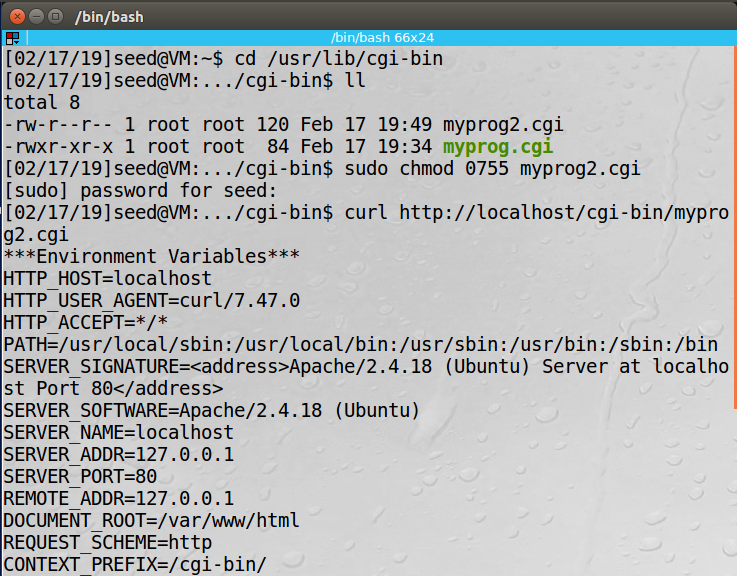
Task 1: with bash\_shellshock



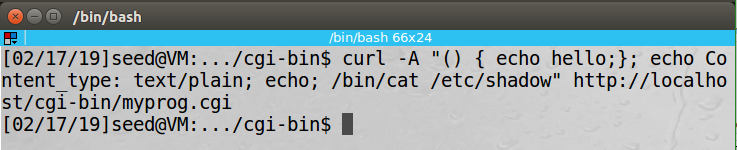
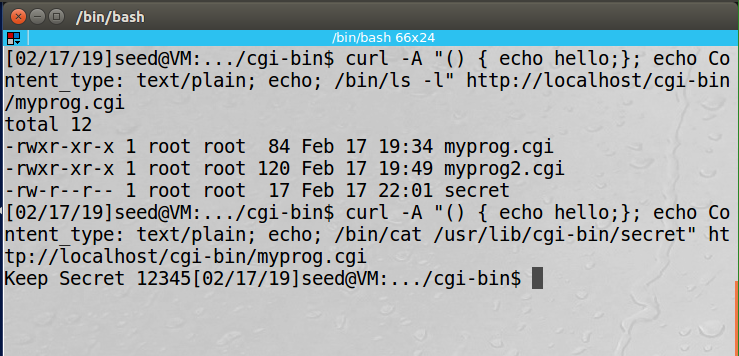
Task 2:



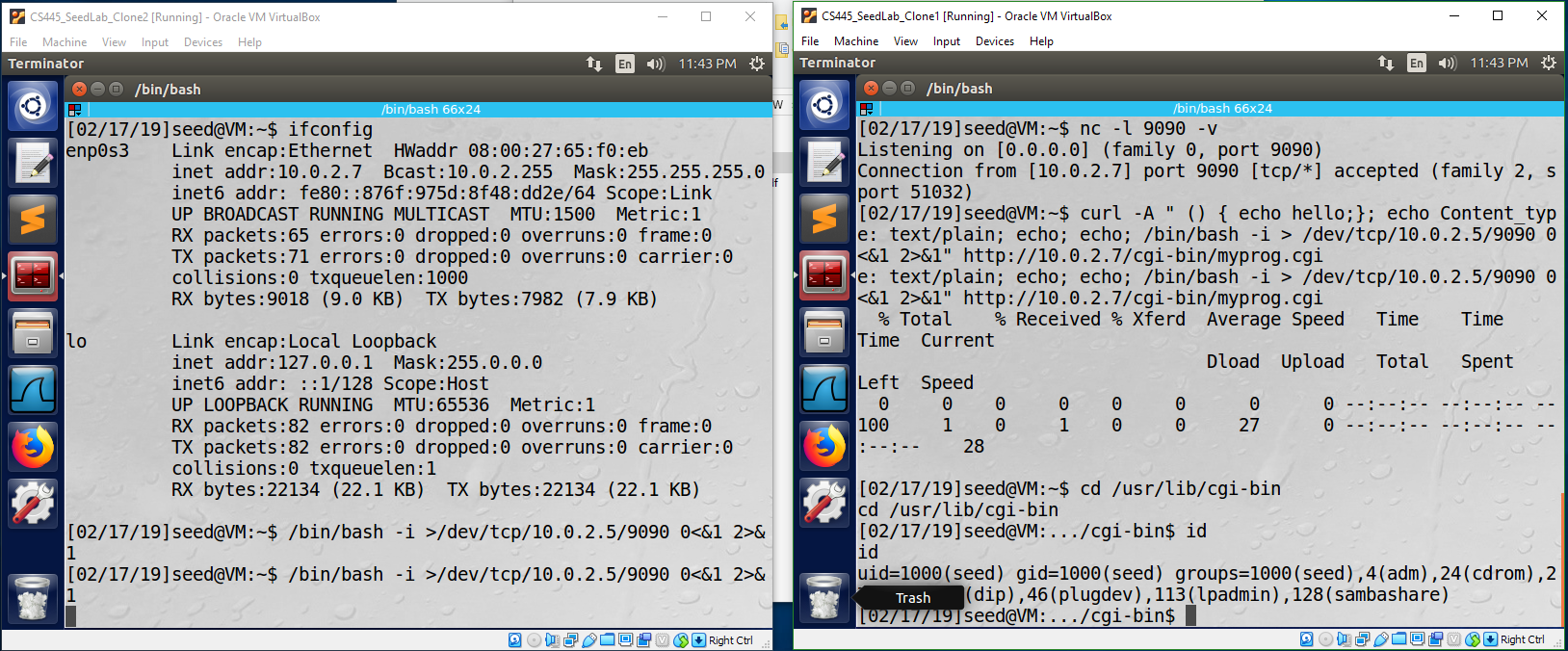
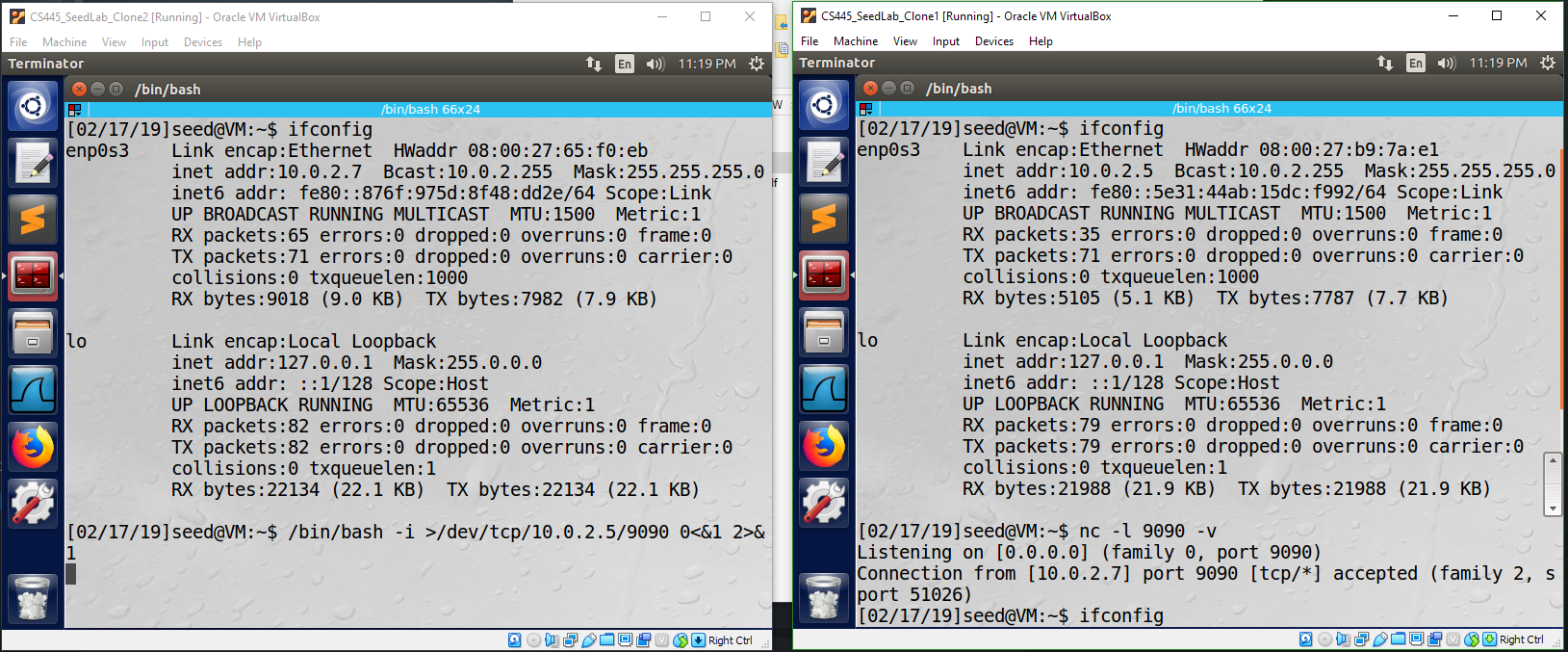
Task 3: The CGI process gets it values from the remote user so with the shellshock vulnerability an attack could feed the process malicious code.



Task 4: Using the shellshock attack I was able to look at the files and print out the contents of the secret file. However I was not able to access the shadow file since this program is not a Set-UID program.



Task 5: The attack sends out a netcat to listen for a connection to the server. Then when the server runs a bash shell for the attacker to use they route the standard output and standard error to their machine giving them full control of the bash shell.



Task 3 and Task 5 using the patched bash: Without the shellshock vulnerability task 3 still pass the variable to the user-agent but for task 5 the reverse shell did not work.

