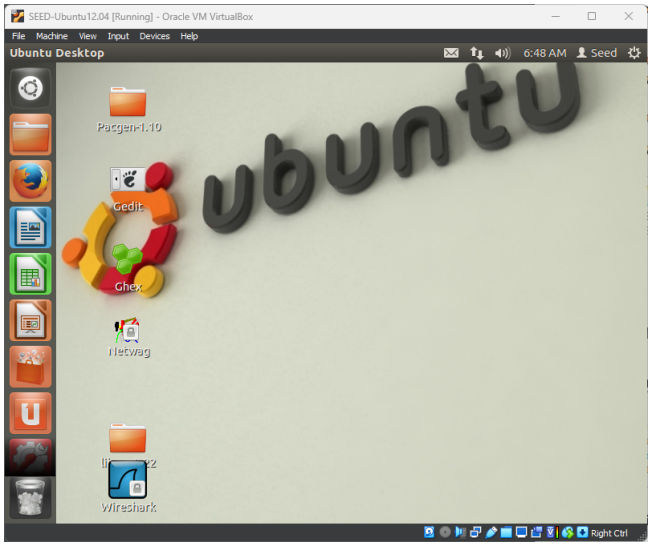
Computer Security

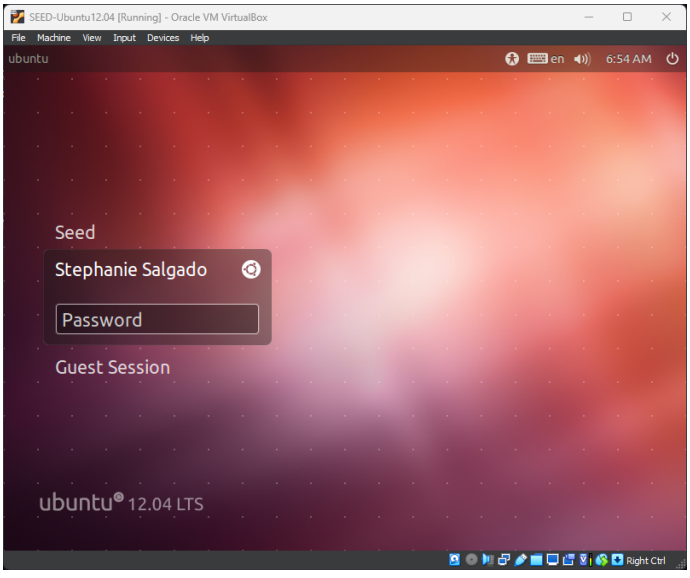
Lab 3 Demo: Dirty-COW Attack

Stephanie Salgado

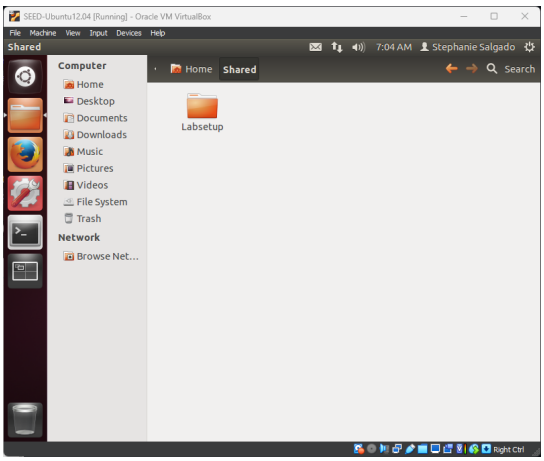
Configured and Launched SEED VM:



Created Username:

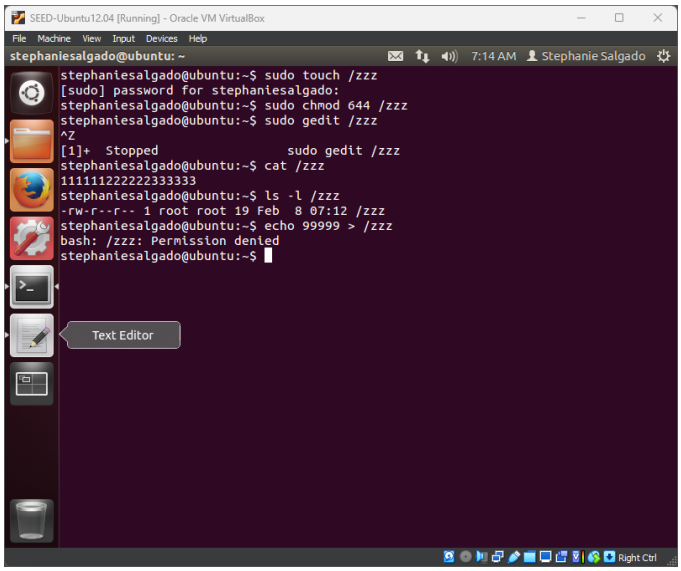


Demo:

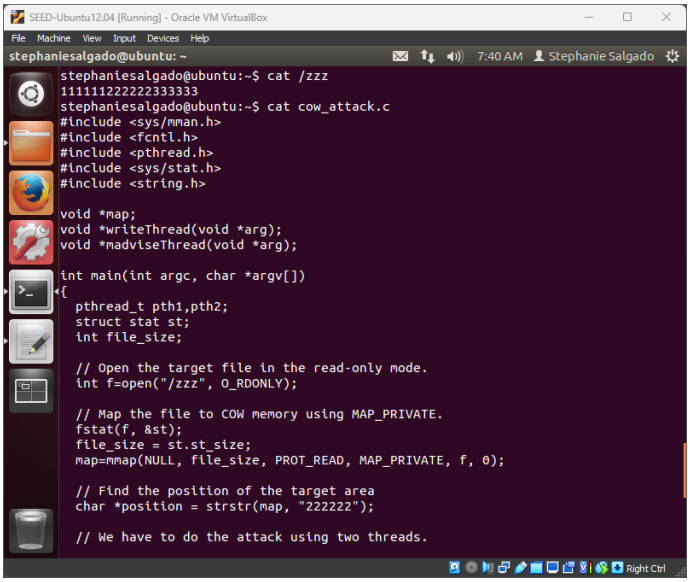


Prepared for the lab by adding the lab set up file to the shared folder.

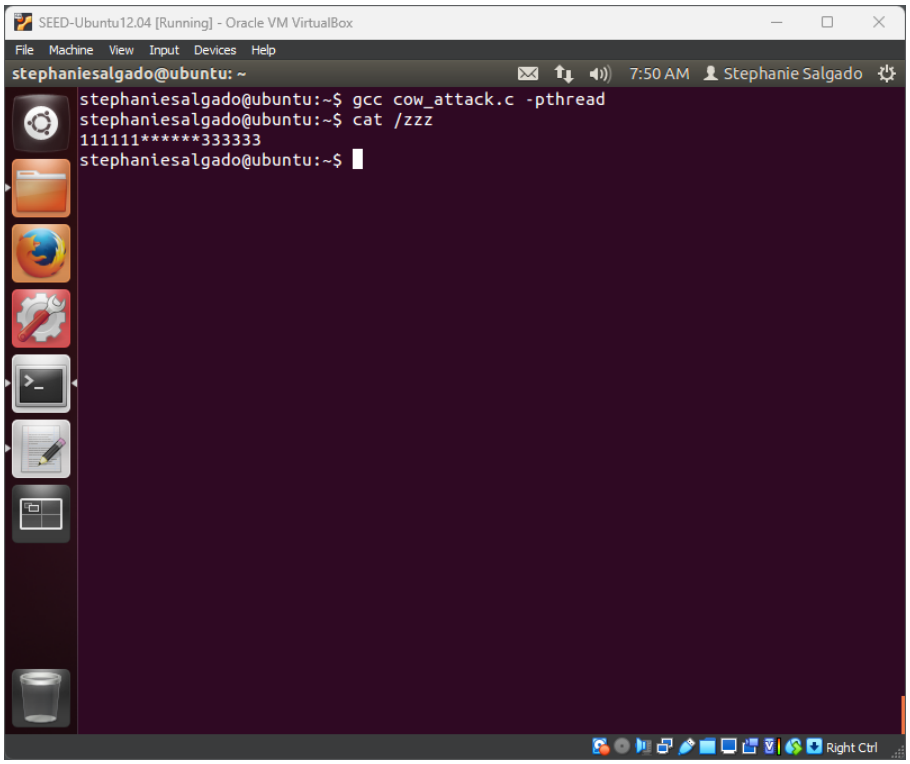
Task 1: Modify a Dummy Read-Only File



Created a file called zzz in the root directory, changed its permission to read-only for normal users. Put some random content (111111222222333333) into the file using “gedit”. Then “cat” the file to reveal its content. Checked the file’s permissions to confirm that it is read-only for normal users. If I try to write to it, I get “Permission denied”. Since our objective is to replace "222222" with "******", we can exploit the Dirty COW vulnerability.

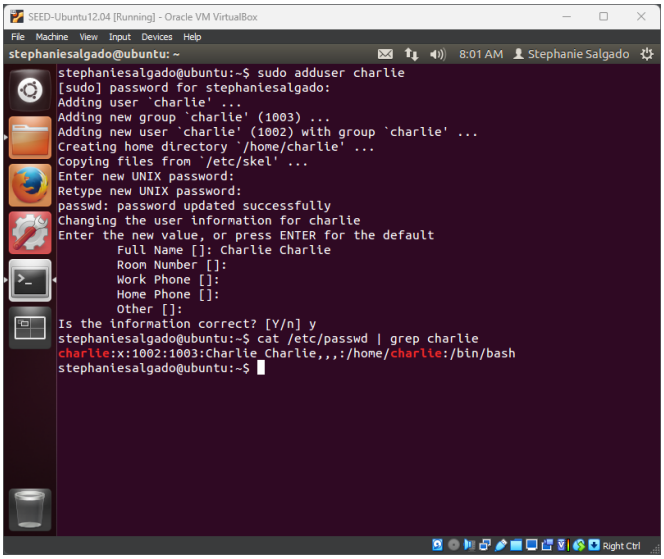


Before compiling and running the attack, I verified the contents of “zzz” were the same as when I created the file. Then I used “cat” to review the “cow_attack.c” file.

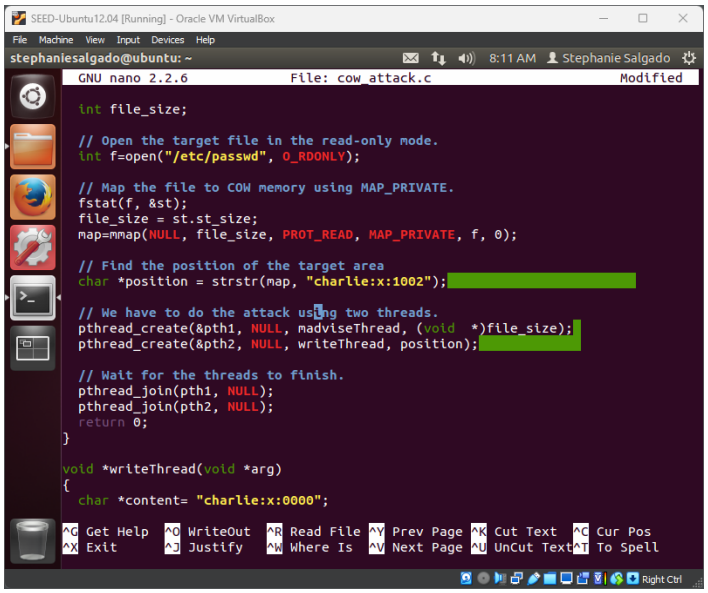


After compiling the code using “gcc” I used “cat” on the “zzz” file once again and the “222222” in the file was replaced with “******”.

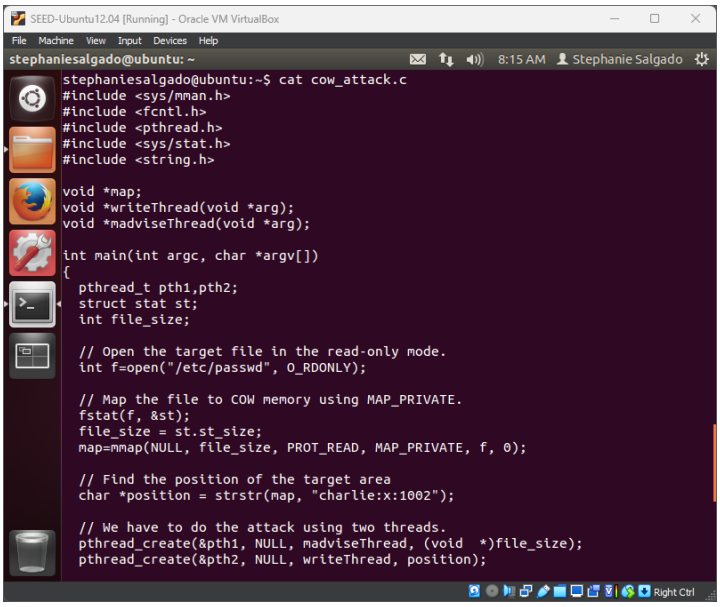
Task 2: Modify the Password File to Gain the Root Privilege



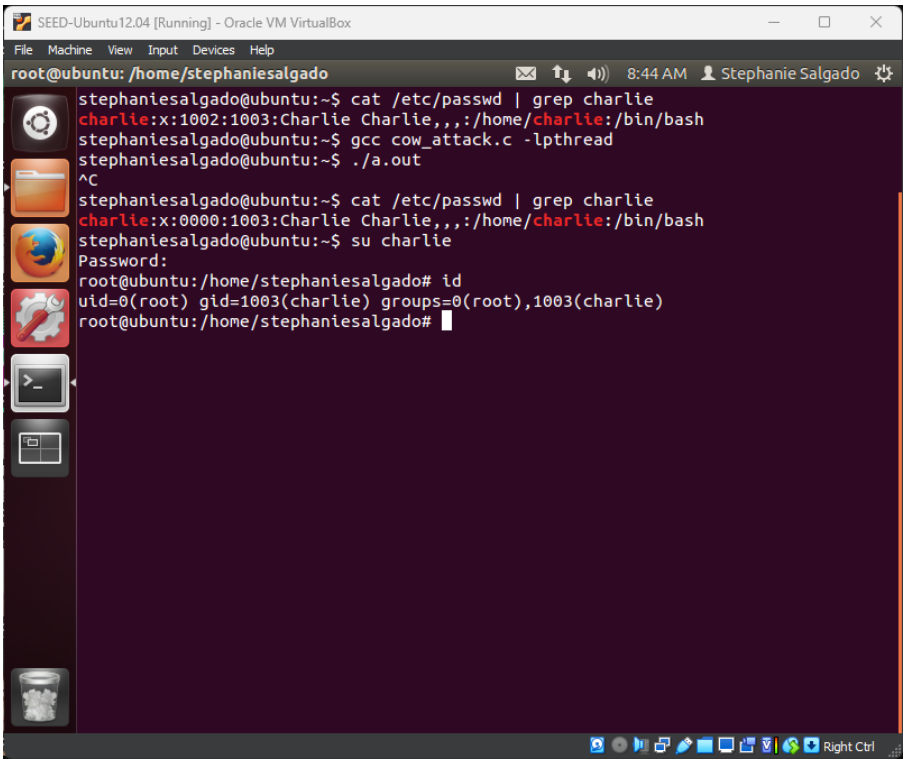
Added new user “charlie” and checked the “passwd” file for the new user. Also saved a copy of the passwd file as a precaution. The object then, is to modify the entry for “charlie” in the “/etc/passwd” file. The third field should go from “1002” to “0000”, which would turn “charlie” into a root account.



Since the “passwd” file is not writable to charlie, I used nano to modify the provided “cow_attack.c” program to use Dirty Cow and write to the file.



I “cat” the file to make sure the changes I made were saved.



After the changes, the attack was successful. I switched to the user “charlie” and noticed I was in the root shell because of the “#”. I then checked id and confirmed “charlie” got root privileges.

Summary:

Through this lab, I was able to learn that while a normal user might have read-only access to a file, it doesn't necessarily mean they would be unable to write to it. The Dirty COW race condition vulnerability is one of the methods that can be used to accomplish this. It was honestly alarming how easily the vulnerability can be exploited, especially because it can be used to change the permission on any user to grant root access.