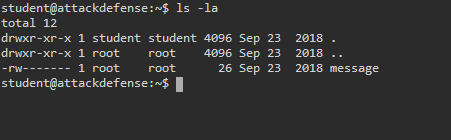
Scenario:

We’re starting off with a system that’s compromised and we got an account called “student”. We need to escalate privileges on the target machine.

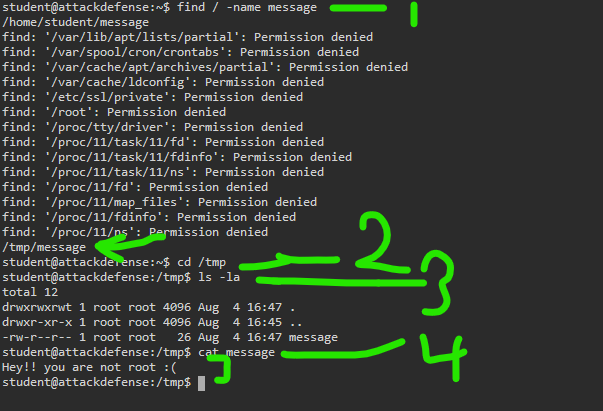
Start by viewing what’s in the student’s directory. This is simplified for the purposes of this lab. We see there’s something called “message” which was made by root? Seems we can’t read or write this message file, since the permissions only are for the creator’s slot.



Let’s find any files called message with

Command: find / -name message

Something shows up in the /tmp folder…



Above, we cat out the message, but it just tells us we aren’t root. This is the actual contents of the text file, and is poorly chosen, since this will confuse some learners. For clarity, this is NOT a system message, but the contents of this file in the temp folder.

Note that we have read access to the tmp message.

So, looking below now, 1) let’s grep to see if there are contents in any file matching “/tmp/message” since this has to be called somewhere, right?

2) We have full permissions on this file “copy.sh”

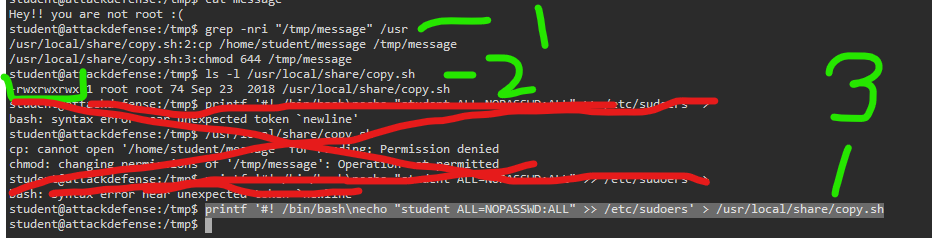
3) use printf to add the shell script permission to add student to the sudoers list, requiring no password

Command: printf ‘#! /bin/bash\necho “student ALL=NOPASSWD:ALL” >> /etc/sudoers’ > /urs/local/share/copy.sh

English: we’re appending a newline and the permission to the student user.

When copy.sh gets run, this new permission will be run too.

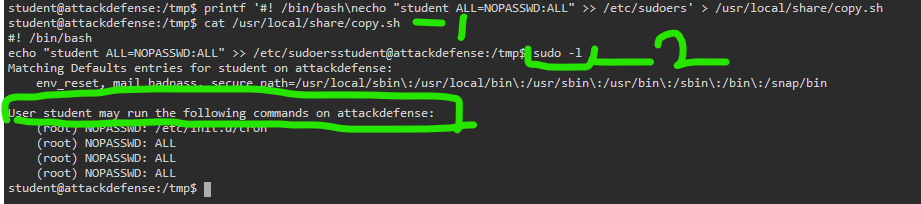
Command: grep -nri “target text” /usr



1) Check the contents of copy.sh to make sure it’s altered

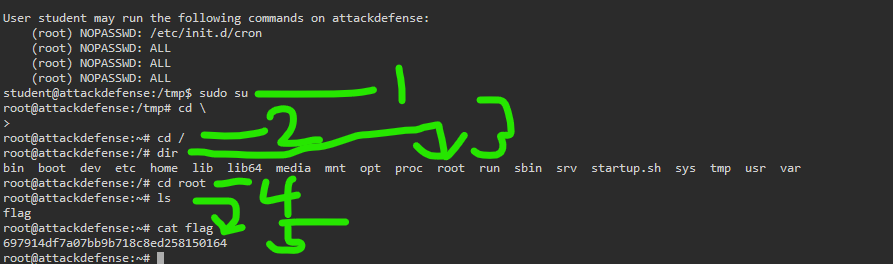
2) List out the sudoers with sudo -l

Student now has root privs with no password needed



That being the case 1) student can just choose to become a superuser now.

2-5) change to the root directory, and look for a flag there



That’s it.