**Homework 2**

**Question 1 (10 points):** Which access control mechanism, ACL or Capability, is easier to implement privilege enabling/disabling? Why?

**Answer:**

ACL is based on users, and their UID. In ACL, we can use chmod to enable/disable privilege of the user. In capability, we can enable or disable privilege by enabling or disabling the file descriptor.

When changes have to be made to user, ACL is a better option. chmod is used to change the permission of an object and thus the modification affects users of the groups that have access to the object as well.  
Chmod can only be done if you are the owner of a given object or file. Chmod cannot enable or diable the privileges if it is not the owner of a file.  
Sometimes, in groups users have different privilege levels, if we use ACL, then we will impose this rule on all the users of the group. If for a user a particular process a privilege in disabled, then it will affect all other processes that the user uses.

When privileges need to be restricted to a particular user, ACL should be used as we can simply enforce these rules by accessing the user by the use of userid.

Capabilities are used when we talk about processes, any user using a process will be granted the same privileges as the process.  
One way to implement enabling and disabling privileges is to create a user for each privilege. Multiple users can be created for the same functionality but having different levels of protection. For example, changing password functionality with respect to self, group and others. When normal user wants a privilege, the user has to assume the identity of that user which has the functionality that he wants.

ACL or capability approach may be used to enable or disable privilege depending on the situation. If all privilege associated with a particular user is to be disabled, we can use ACL. If only privilege of a particular process is to be disabled, we can use capability.

**Question 3 (10 points):** After a root process disables its capability, it is compromised by one of the following attacks. Can the attacker use the disabled capability (assuming that the root process will not enable the capability)?

o Race condition attack

o Buffer-overflow attack

**Answer:**

To use the disable capability is **not possible for race-condition attack**. Race-condition attack needs for both the malicious code as well as the root program to be run in the same window of operation, this will allow for the malicious code to interfere with the execution of the Set UID program. So in race-condition we work with 2 programs, and even if we try to re-enable the capability for the user level program it will not succeed. Root program will not modify its behavior on the basis of the attempted modification by the user level program. Once the capability has been dropped there is no way for the user level malicious program to re-enable it.

In **buffer-overflow attack** the buffer is over-written and we are able to access the privileged programs stack. The attacker can inject the malicious code here to enable the capability which had been disabled. The possibility of changing the behavior of a program using the injected code exists and so, the capability can be re-enabled.

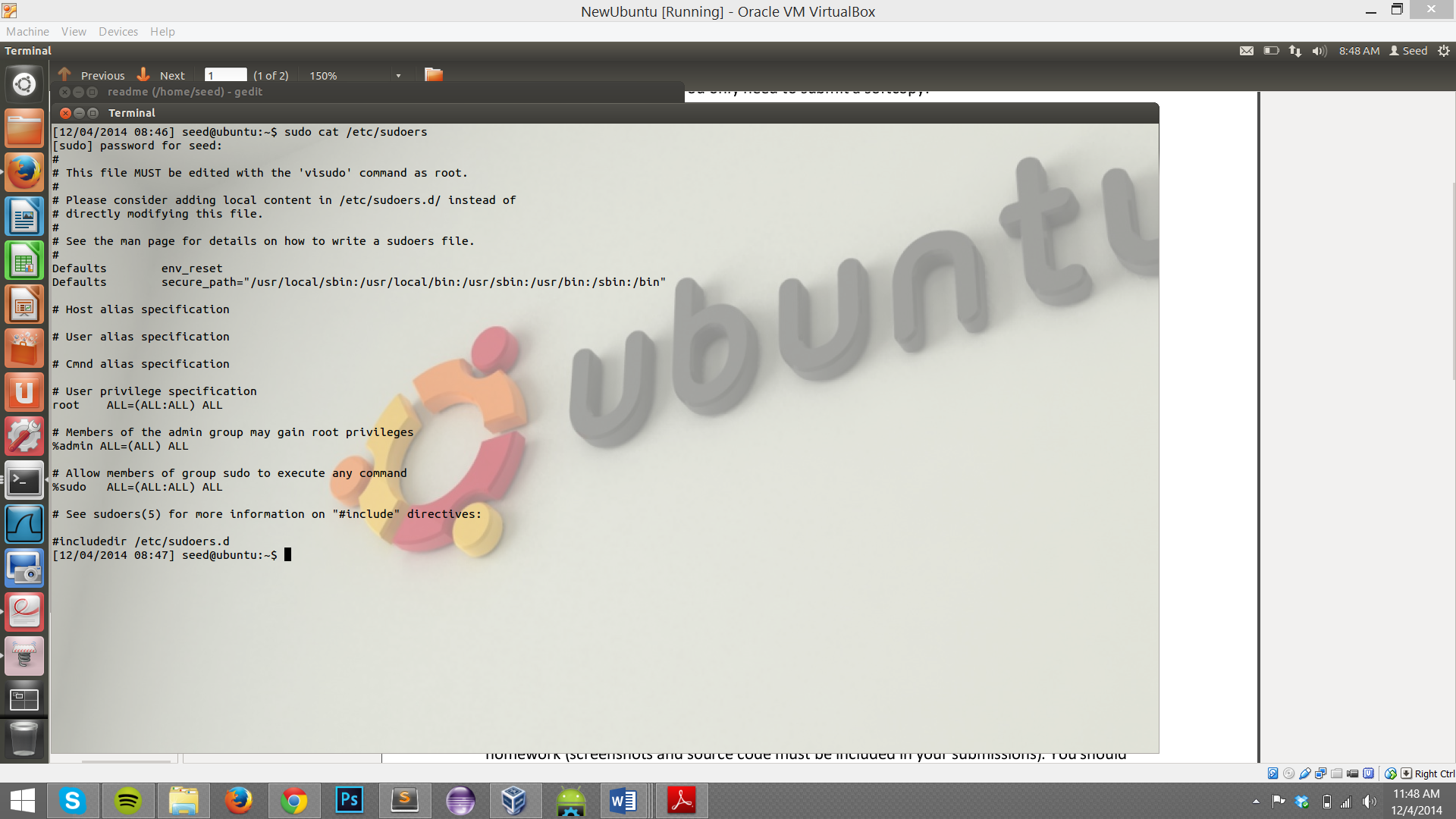
**Question 4 (15 points):** Please describe why the “seed” user in our VM can run any command as the root. You need to provide concrete evidence to support your explanation. You may want to pay attention to the following files:

* /etc/sudoers: this is the sudo configuration file.
* /etc/group: this file contains the information about groups.

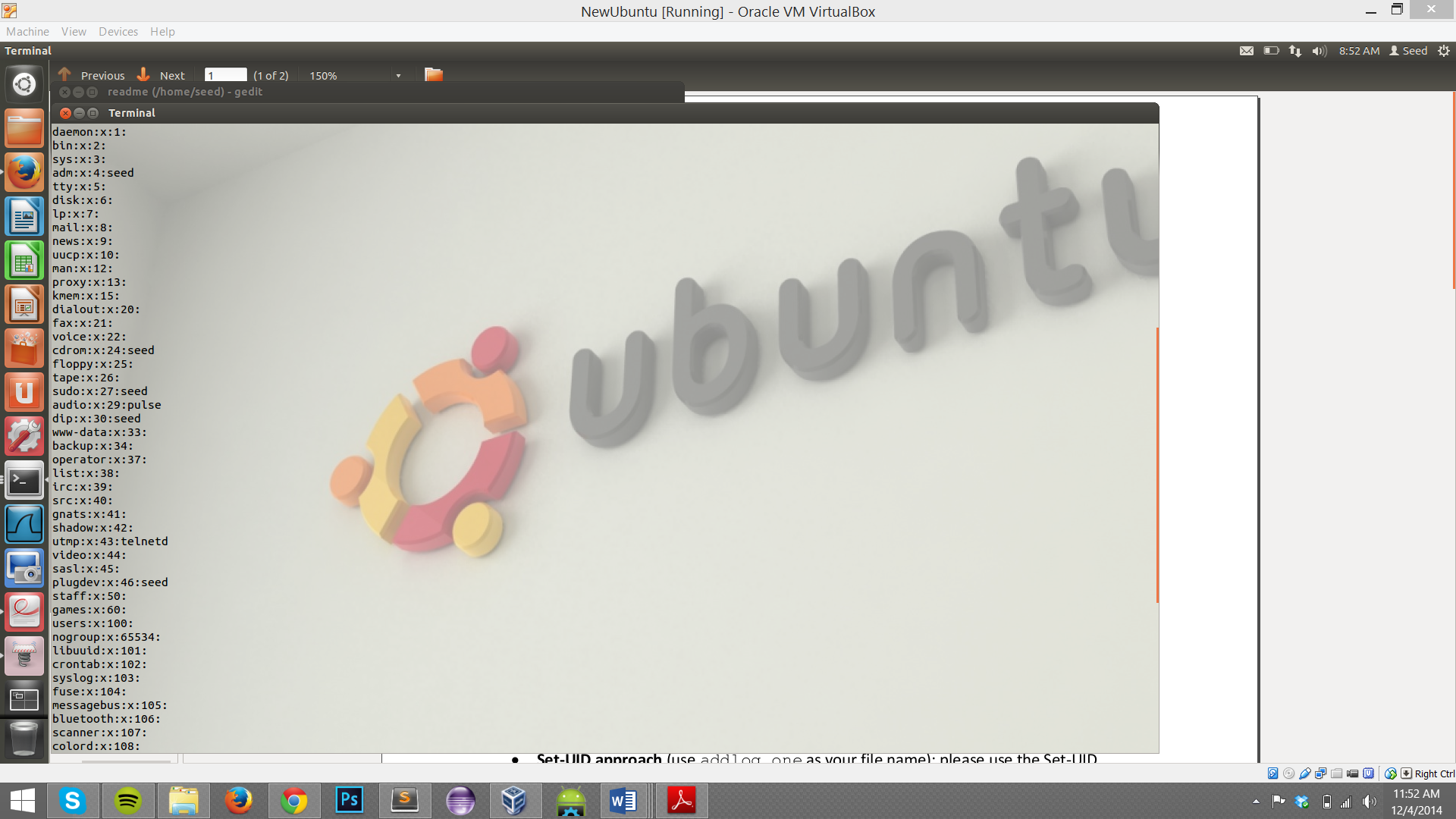
**Answer:**

Sudo is a set-UID program that allows normal users to perform operations on privileged levels. Access control is done inside the program. Sudo allows only one particular program to run with privileges of root.

From sudoers file we can see that all members of the group sudo are allowed to execute any command



From the /etc/group file it is evident that seed is in the sudo group, which as we have seen has a permission to run all commands.



Group sudo, gid is 27 and seed is in the group sudo