6G7Z1009 Introduction to Computer Forensics and Security week 12 – Lab

"Capability" is important for improving system security, especially in access control. A capability is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights (e.g., read/write, etc.).
This lab aims to explore Linux "Capability" and gain the first-hand experience on Capability, understand the advantage of capabilities in access control, and learn to use "Capability" in to achieve the principle of least privileges in Linux.

I. Reading the papers from the moodle

1.1 AccessContol.pdf
1.2 Capabilities.pdf

II. Preparation

2.1 Under Linux environment, open a terminal (use tab function for opening more terminals)

III. To explore Linux capability

In operating systems, there are many privileged operations that can only be conducted by privileged users. Examples of privileged operations include configuring network interface card, backing up all the user files, shutting down the computers, etc. Without capabilities, these operations can only be carried out by super-users. Therefore, letting super-users to conduct these privileged operations is a violation of the Least-Privilege Principle. Capabilities divide the powerful root privilege into a set of less powerful privileges. Each of these privileges is called a capability. With capabilities, we do not need to be a super-user to conduct privileged operations. All we need is to have the capabilities that are needed for the privileged operations. This lab task is to gain experience how capabilities can be used to remove unnecessary power assigned to certain privileged programs.

3.1 Taks1: to understand Linux capabilities by typing the command "man capabilities"

3.2 Task 2: to create a virtual machine using KVM

- **Open a terminal**
- **Type "man kvm" and understand the options of KVM**
- **Please answer what is "kvm"**

- **Type the command to create a virtual machine (to understand command options, please use "man kvm")**
  $kvm -cdrom /var/tmp/blossom-0.98.iso –m 512

3.3 Task 3 to understand Set-UID

- **Open a terminal in your host machine and type the command "man setuid"**
- **Please answer what is Set-UID**
- **Type the command "which ping" and find the directory of "ping" program and check who has a privilege to run this program and record your result.**
- **Now to find the virtual machine IP address, type the command**
  $ /sbin/ifconfig
- **After you get your host machine address (normally, it will be 10.0.2.2), type the command**

  $ ping -c 5 10.0.2.2
  $ ls –l /bin/ping

- **Please answer whether "ping" is a Set-UID program (please refer to linux manual page for "ls")?**
- **Think about and write down any possible vulnerability under the above situation?**

3.4 Task 4 to turn a Set-UID program into a non-Set-UID program to remove the privilege and reduce the risk

- **to remove the privilege (set-uid) and record your result.**
  $ sudo chmod u-s /bin/ping
  $ ls –l /bin/ping
  $ ping 10.0.2.2

3.5 Task 5, to use capability to give a program only the necessary privilege.

- **To install libcap2-bin package that provides the commands to set capabilities**
  $dpkg -s libcap2-bin
  (this is to show whether the package is installed you may see some error "package not installed". If not please install)
  $sudo aptitude install libcap2-bin

- **to check whether the capability is already set and record the result**
  $/sbin/getcap /bin/ping