**OPERATING SYSTEMS - Mini project1 I Intruder detection**

**NATIONAL INSTITUTE OF TECHNOLOGY**

**ANDHRA PRADESH**

By

K. Phani Rohitha (411634)

Introduction:

In information security, intruder detection is the art of detecting intruders behind attacks as unique persons. This technique tries to identify the person behind an attack by analysing their computational behaviour. This concept is sometimes confused with Intrusion Detection techniques which are the art of detecting intruder actions.

Abstract:

The idea behind this project is to identify the person, who performs an invalid login. On invalid login, kernel runs a script that captures the picture of the person and mail it (default - root) along with login details. This mechanism provides the information of the intruder to the root user of the system through mail services. Addition of this detection script helps in case of system thefts, privacy intrusion and in the times of threat.

Packages required

1. Mail Services
2. VMBox Extension Package
3. Webcam Services

Project Implementation:

Step1: Packages installation

1. Mail Services: Packages that provides mail services are ssmtp, mailutils, mailx etc.

Installed packages for this project are ssmtp and mailutils

Command*: sudo apt-get install <package\_name>*

1. VMBox Extension: Virtual Box Extension Pack provides support for USB 2.0 and 3.0 devices, Remote Desktop Protocol (RDP), disk encryption, NVMe and Preboot Execution Environment (PXE) etc., This also include webcam access by the guest OS of the virtual box.

Install extension pack **same** as that of the virtual box version being used.

c)Webcam Services: Packages like cheese, gstreamer, ffmpeg provides facility to capture picture or video by accessing the inbuilt webcam.

Command: *sudo apt-get install <package\_name>*

Step2:Bash script

The script that is to be implemented is under the name of ‘grab’ file. The bash script of the file is:

#!/bin/bash

streamer –o first.jpeg #*Captures the picture and saves it under the name first.jpeg in /home*

cp first.jpeg f.jpg  *#Copies the first.jpeg file to f.jpg*

[ “$PAM\_TYPE” = “open\_session” ] *#Describes the information of user account*

{printf “\nSorry! Someone tried to access your laptop\nUser is: $PAM\_USER\n^d”}*#Body of the mail*

| mail –s “Invalid Login” –A f.jpg <mail\_id>*# Sends the mail with provided attachment(Captured picture) for given mail\_id*

exit 0 *#Exit code*

Step 3:Granting Permissions

System user is not provided with all the facilities like accessing kernel files and utilities. So permissions are to be granted externally to the user by “sudo” command.

1. To place grab script in the ‘/usr/bin’ by system user.

Command:*sudo nano /usr/bin/grab*

the files in this location are executed when specified condition arises.

1. To make the saved grab file an executable program

Command: *sudo chmod –R 777 /usr/bin/grab*

1. To permit the changes to ‘common-auth’ file located at /etc/pam.d by system user

Command: *sudo chmod –R 777 /etc/pam.d/common-auth*

The files of pam.d directory list the PAMs that will do the authentication tasks required by this service, and the appropriate behaviour of the PAM-API in the event that individual PAMs fail.

Step4:Modifications of common-auth file

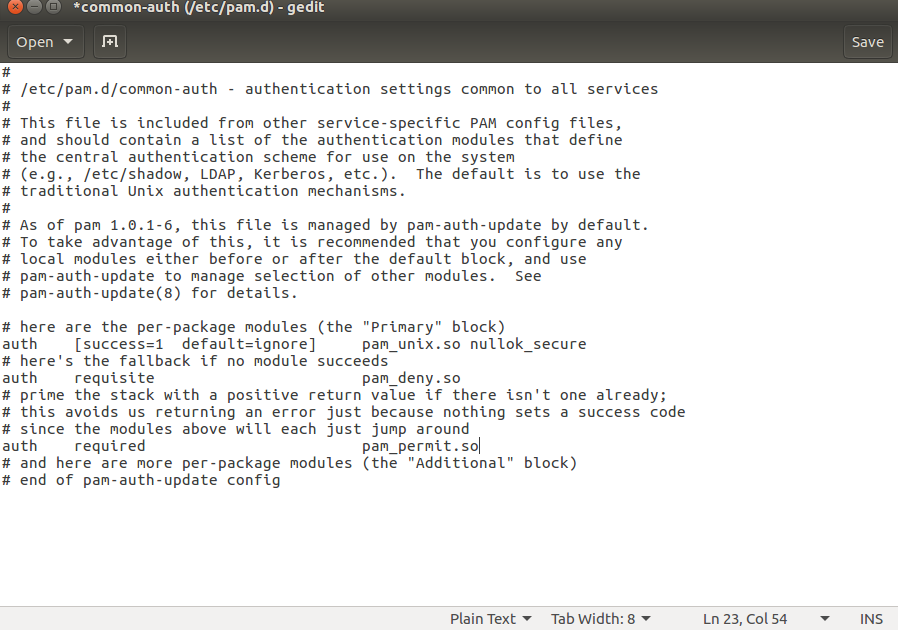
Edit the /etc/pam.d/common-auth file and insert this line immediately before the line with pm\_deny.so module,

*auth [default=ignore] pam\_exec.so seteuid /usr/bin/grab*

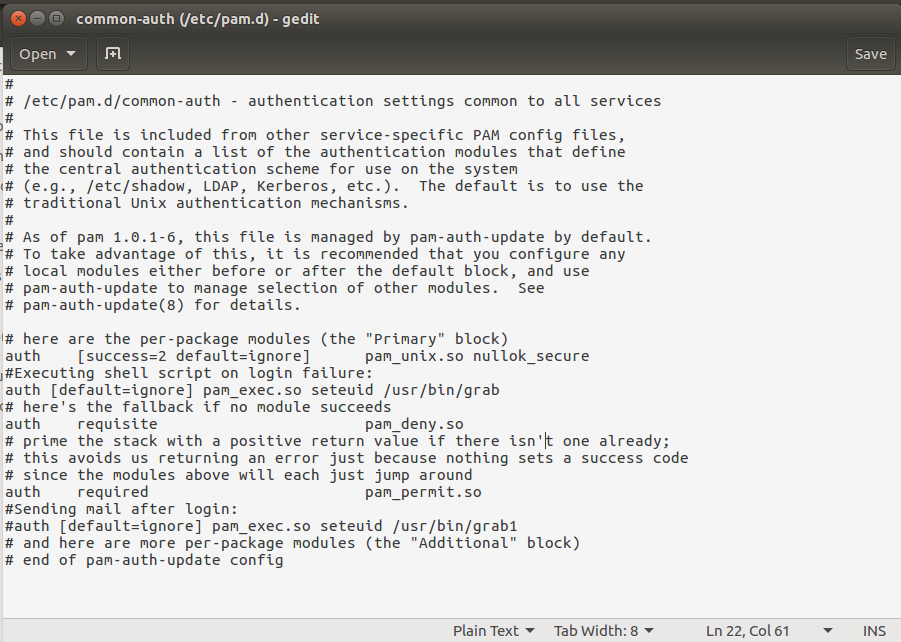
Now edit the two lines above (pam\_unix and pam\_winbind) and change the success=1 to success=2. This has it to skip an extra line when auth is successful. So it skips our script.

Make a script /usr/bin/grab to do what to do when login fails.

Original Common-auth File:

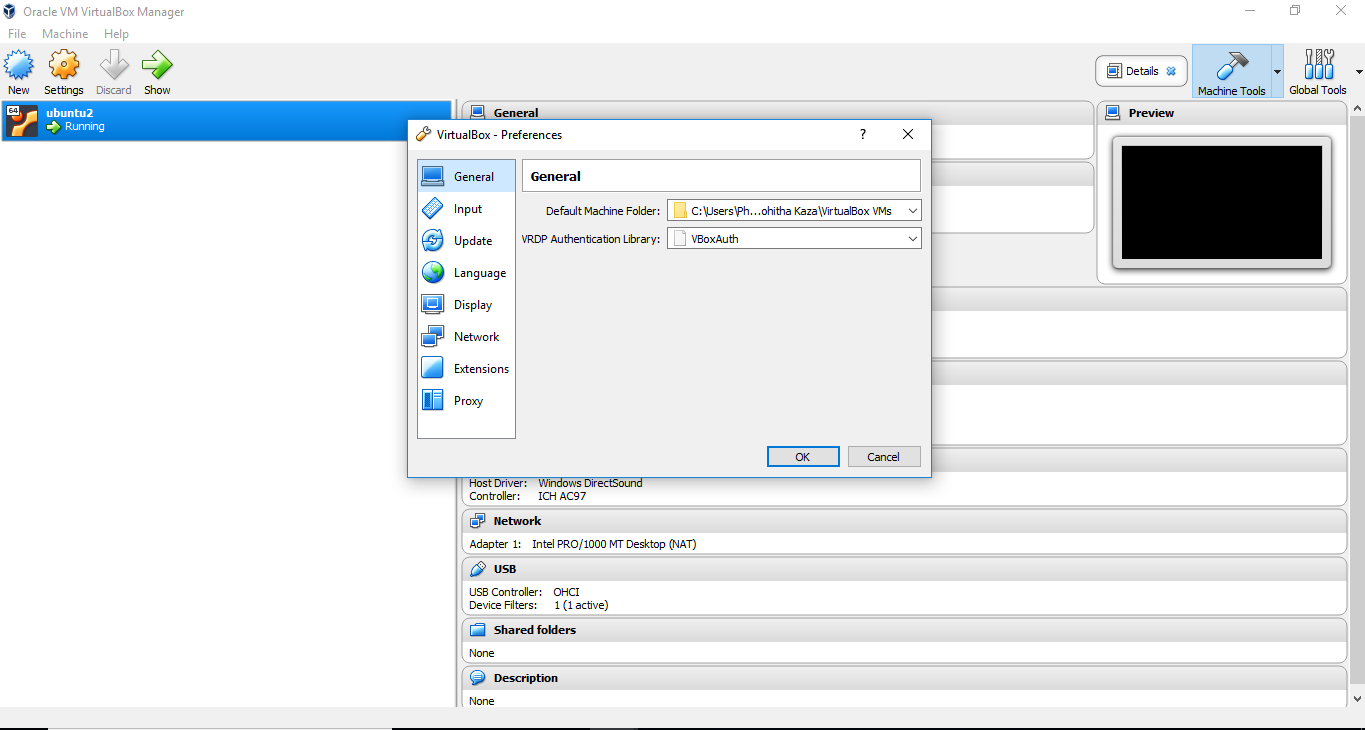


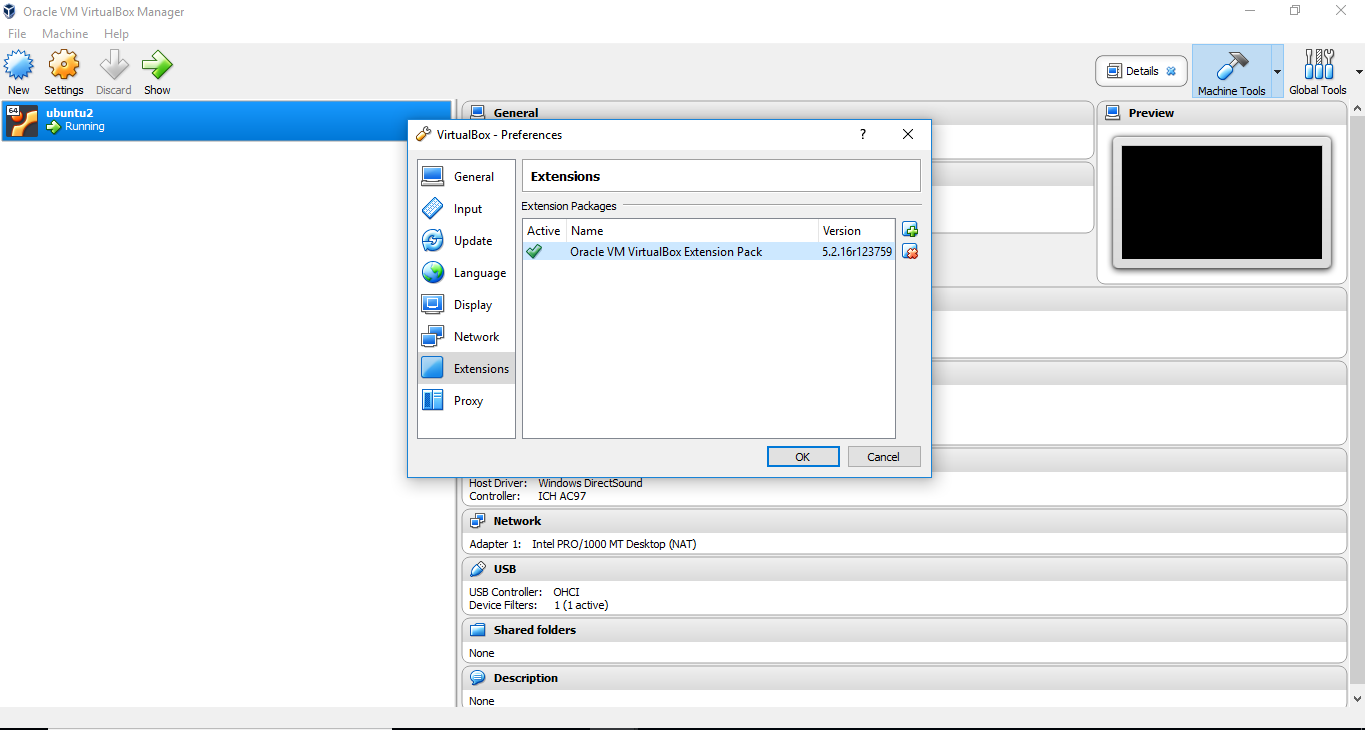
After Modification:



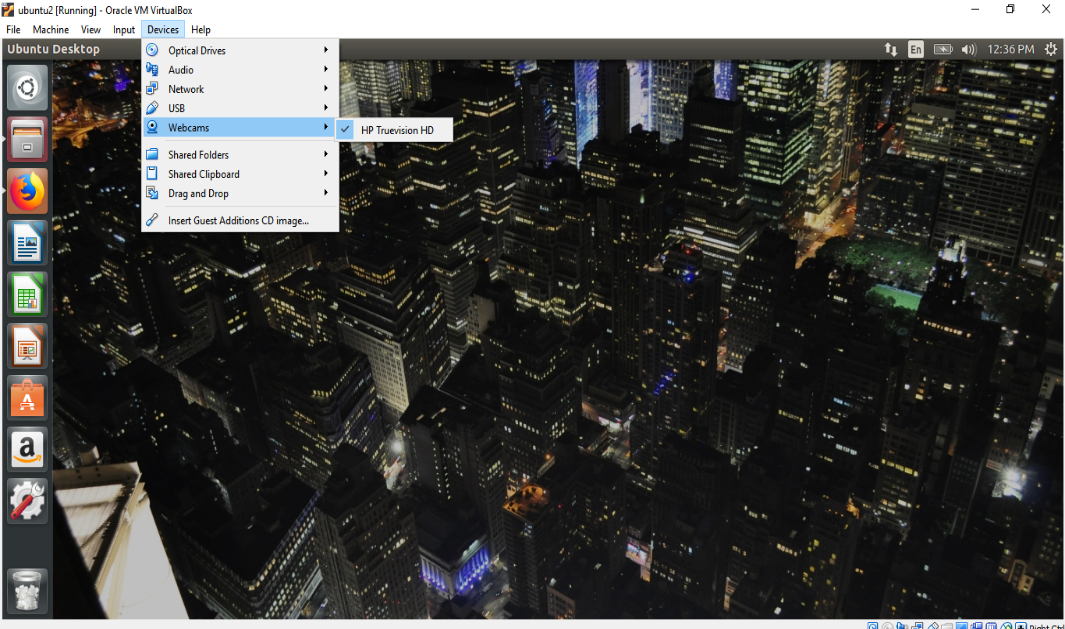
Step 5:VMExtension Pack

1.After installing extension pack same as that of virtual box version,add it to the extension tab in virtual box manager as shown in figure(s) below:





2.Activation of Webcam Device in Virtual Box:



Test Case:

On login session at the time of wrong password entry the User Interface is locked indicating that Invalid Password,please try again.

Result:

The mail received by the root user is:

