

Overview

Introduction

Use of the provided virtual machine

Work Submission

OPTION: Creating our own virtual machine

Introduction

Introduction to H.O.S. lab assignments

- ▶ To do the lab assignments we will be using a linux virtual machine with linux debian 12.9 installed
- ▶ This machine is the same as the one on which will be doing the examples in the theoretical lessons
- ▶ We need to download and install Virtualbox (<https://www.virtualbox.org/wiki/Downloads>) together with the Virtualbox Extension Pack
- ▶ a virtual machine (ova file). with debian 12.9 and all the software needed for the lab assignments is provided.
 - ▶ we just have to download it and import it in virtualbox

Use of the provided virtual machine

Use of the provided virtual machine

- ▶ The virtual machine is available at `moovi.uvigo.gal` under the *Hardening Operating Systems* course
- ▶ It has all the needed software for the Lab Assignments of the Linux part
- ▶ Password for user `root` is `t00r25`
- ▶ It has a user, *usuario*, with password *user25*
- ▶ It has 100 additional users: *user001*...*user100* with passwords *qwerty001*...*qwerty100*

Work Submission

Work submission

- ▶ After performing the corresponding tasks of any of the lab assignments, a pdf document, with the name of the student in the first page and describing what has been done (including screenshots showing the behaviour of the virtual machine, changes made to configuraton files, output from commands. . .) should be sent to
 - ▶ `antonio.yanez@udc.es`. (students at udc)
 - ▶ `yolanda@det.uvigo.es`. (students at uvigo)

Work submission

- ▶ The document has to cover only the tasks specific to the Lab Assignment (not the *preparation*)
- ▶ The subject of the mail should be *FSO: practica-N*, where *N* is the lab assignment number
- ▶ The attachment should be named with the lab assignment number and the surname and name of the student, in the form P1-Surname-Name.pdf, avoiding non-ascii caracteres (á, é, ñ ...)
 - ▶ For example, for the first lab assignment, the work submitted by student *Donald Trump Núñez* should come as an attached file named *P1-TrumpNunez-Donald.pdf* to a mail with the subject *FSO: practica-1*
- ▶ The work must be submitted within 15 minutes of the end of the lab assignment class
- ▶ Should some students decide to work in pairs, **ONLY ONE OF THEM** will submit the pdf document (as described before). The first pdf page should state both students names

OPTION: Creating our own virtual machine

Creating our own virtual machine

REMEMBER: this is optional. You can use the provided machine

- ▶ if, for whatever reason, we prefer to build our own virtual machine we can do so
- ▶ we can use whatever distribution we choose (ubuntu, debian ...). However we must follow these configuration options
 - ▶ NIC configured with dhcp
 - ▶ Shadow passwords must be enabled
 - ▶ root can login directly
 - ▶ We can choose either BIOS or UEFI tpe firmware, however *grub* must be used as the boot loader
 - ▶ We can partition in GPT or MBR partition schemes. However we must leave some free space to create at least one partition in the installation disk

Creating our own virtual machine

- ▶ If we want to take the full advantage of the Virtualbox Guest Additions we should install the following packages (names are given for debian distributions, names of packages might differ in other distributions)
 - ▶ *build-essential*
 - ▶ *dkms*
 - ▶ *module-assistant*
 - ▶ *linux-headers* (probably named `linux-headers-amd64`)
 - ▶ finally the VirtualBox Guest Additions ('Devices→ Insert Guest Additions CD image' in the Virtual Machine Menu and then run, as root, the program `VBoxLinuxAdditions.run` on the CD)

Creating our own virtual machine: Additional software

- ▶ The following software packages will be needed for different lab assignments. (Again the names of the packages are for the debian distro)
 - ▶ john, libpam-pwquality, alpine (for the hardening user accounts lab assignment)
 - ▶ acl, lvm2, cryptsetup, quota, encfs (for the hardening file system lab assignment)
 - ▶ lxc, cpulimit, ssh, apparmor-notify, apparmor-utils (for the hardening applications lab assignment)
 - ▶ nftables, inetutils-inetd, inetutils-ftpd, inetutils-telnetd, ftp, libpam-google-authenticator (for the hardening network lab assignment)
 - ▶ lynis (for the hardening maintenance lab assignment)

Creating our own virtual machine: Additional tasks

- ▶ In addition to the software we have installed in this machine, we'll perform the following modifications to its configuration, which will be used in several lab assignments
 - ▶ We must have at least 20 fully functioning (and with their home directories properly created and populated) user accounts available
 - ▶ We must add a second hard disk to the machine and partition it using the GPT scheme
 - ▶ In addition to the Network Interface Card configured during installation we'll add two more Network Interface Cards, connected to an internal network and with static addresses 192.168.10.101, 192.168.11.101, and 192.162.12.101 for one of the NICS and 192.168.20.101, 192.168.21.101, and 192.162.22.101 for the other.

Creating our own virtual machine: Additional tasks: network

- ▶ Be sure to either have ifupdown interfaces NOT MANAGED in Network Manager configuration or have Network Manager disabled
- ▶ This `/etc/network/interfaces` file will configure the interfaces in debian

```
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
    address 192.168.10.101/24
iface enp0s8 inet static
    address 192.168.11.101/24
iface enp0s8 inet static
    address 192.168.12.101/24

auto enp0s9
iface enp0s9 inet static
    address 192.168.20.101/24
iface enp0s9 inet static
    address 192.168.21.101/24
iface enp0s9 inet static
    address 192.168.22.101/24
```