Malware Analysis (CS6038)

Week 02.1 Virtualization & Labs

Scott Nusbaum
nusbausa@ucmail.uc.edu

January 22, 2019

University of CINCINNATI

Overview

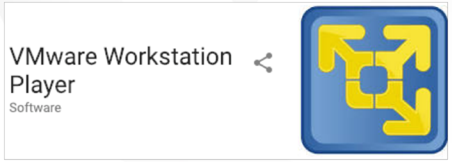
- Virtualization
  - Different options
  - Pros and Cons
- VirtualBox
  - Setup
  - Configuration
  - Demo installation of OVA

Lots of Virtualization

- OS Virtualization – Hypervisors - Virtual Machines
- Dockers – OS level virtualization (Shared Kernel)
- Application Virtualization – App runs locally but is stored on a server
- Application Server Virtualization – Helps with Load balancing
- Network Virtualization – Virtually emulating network gear
- Hardware Virtualization – (Emulates the hardware as well as software)
  - Android Emulator / Qemu
- Storage Virtualization – Virtual Filesystem (LVM)

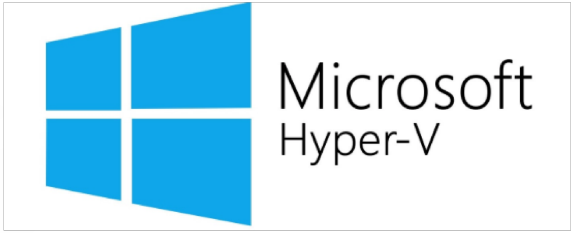
University of CINCINNATI

Virtualization Providers



VMware Workstation Player

Software



ORACLE
VirtualBox

VMWARE
11
FUSION

vmware
ESXi

vmware
vSphere 6.5

VirtualBox

Oracle VM VirtualBox is a free and open-source hosted hypervisor for x86 computers currently being developed by Oracle Corporation. Developed initially by Innotek GmbH, it was acquired by Sun Microsystems in 2008 which was in turn acquired by Oracle in 2010. Wikipedia

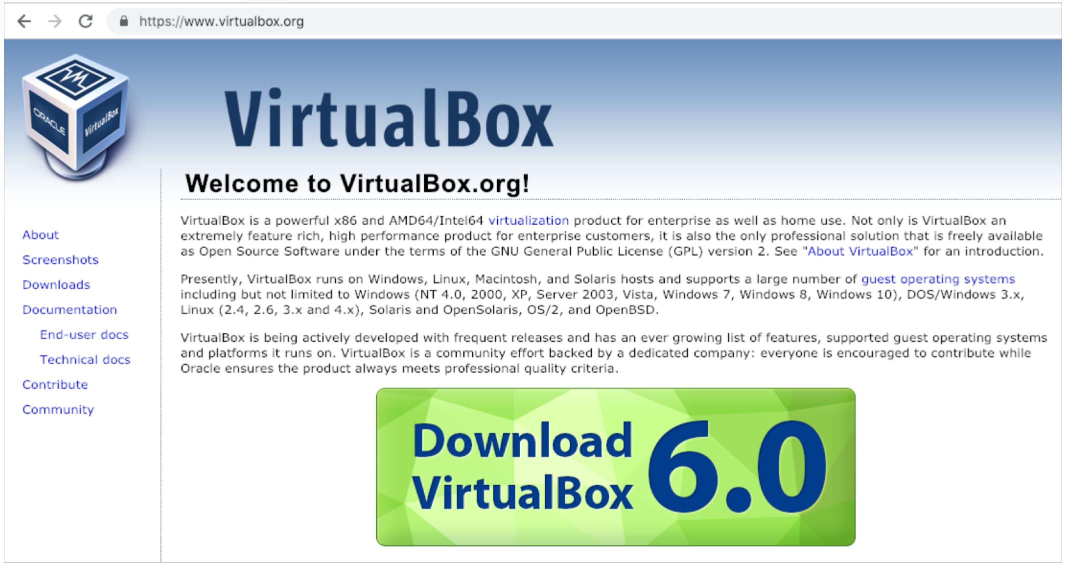
Pro’s for VirtualBox

- Open Source
- Multiple OS support
  - Same UI
- Virtual Networking
- Full Command-Line Interface

University of CINCINNATI

VirtualBox Installation

- Download newest version from https://www.virtualbox.org



Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "About VirtualBox" for an introduction.

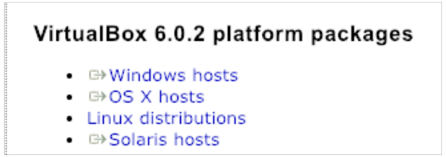
Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

University of CINCINNATI

VirtualBox Installation

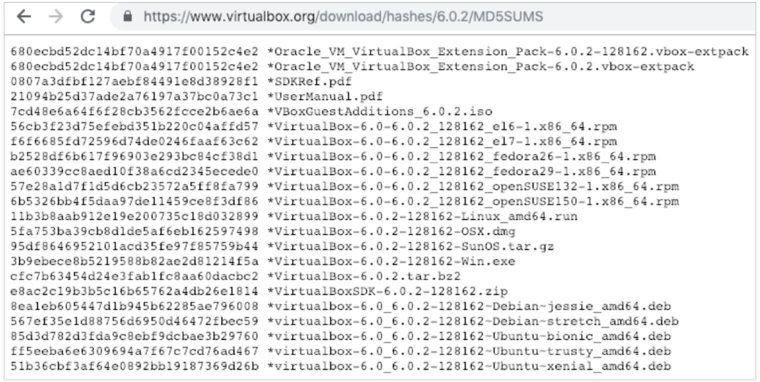
- Select the Host OS platform from the list



VirtualBox 6.0.2 platform packages

- Windows hosts
- OS X hosts
- Linux distributions
- Solaris hosts

- It is strongly encouraged to check the downloaded files hash against the provided Checksums



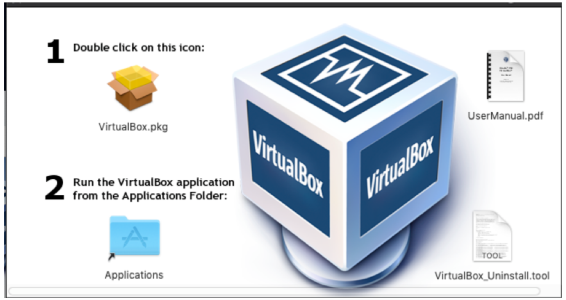
https://www.virtualbox.org/download/hashes/6.0.2/MD5SUMS

```
680ecbd52dc14bf70a4917f00152c4e2 *Oracle_VM_VirtualBox_Extension_Pack-6.0.2-128162.vbox-extpack
680ecbd52dc14bf70a4917f00152c4e2 *Oracle_VM_VirtualBox_Extension_Pack-6.0.2.vbox-extpack
0807a3dfbf127aebf84491e8d38928f1 *SDKRef.pdf
21094b25d37ade2a76197a37bc0a73c1 *UserManual.pdf
7cd48e6a64f6f28cb3562fcce2b6ae6a *VBoxGuestAdditions_6.0.2.iso
56cb3f23d75efebd351b220c04affd57 *VirtualBox-6.0-6.0.2_128162_el6-1.x86_64.rpm
f6f6685fd72596d74de0246faaf63c62 *VirtualBox-6.0-6.0.2_128162_el7-1.x86_64.rpm
b2528df6b617f96903e293bc84cf38d1 *VirtualBox-6.0-6.0.2_128162_fedora26-1.x86_64.rpm
ae60339cc8aed10f38a6cd2345ecede0 *VirtualBox-6.0-6.0.2_128162_fedora29-1.x86_64.rpm
57e28a1d7f1d5d6cb23572a5ff8fa799 *VirtualBox-6.0-6.0.2_128162_openSUSE132-1.x86_64.rpm
6b5326bb4f5daa97de11459ce8f3df86 *VirtualBox-6.0-6.0.2_128162_openSUSE150-1.x86_64.rpm
11b3b8aab912e19e200735c18d032899 *VirtualBox-6.0.2-128162-Linux_amd64.run
5fa753ba39cb8d1de5af6eb162597498 *VirtualBox-6.0.2-128162-OSX.dmg
95df8646952101acd35fe97f85759b44 *VirtualBox-6.0.2-128162-SunOS.tar.gz
3b9ebece8b5219588b82ae2d81214f5a *VirtualBox-6.0.2-128162-Win.exe
cfc7b63454d24e3fab1fc8aa60dacbc2 *VirtualBox-6.0.2.tar.bz2
e8ac2c19b3b5c16b65762a4db26e1814 *VirtualBoxSDK-6.0.2-128162.zip
8ea1eb605447d1b945b62285ae796008 *virtualbox-6.0_6.0.2-128162~Debian~jessie_amd64.deb
567ef35e1d88756d6950d46472fbec59 *virtualbox-6.0_6.0.2-128162~Debian~stretch_amd64.deb
85d3d782d3fda9c8ebf9dcbae3b29760 *virtualbox-6.0_6.0.2-128162~Ubuntu~bionic_amd64.deb
ff5eeba6e6309694a7f67c7cd76ad467 *virtualbox-6.0_6.0.2-128162~Ubuntu~trusty_amd64.deb
51b36cbf3af64e0892bb19187369d26b *virtualbox-6.0_6.0.2-128162~Ubuntu~xenial_amd64.deb
```

University of CINCINNATI

VirtualBox Installation

- Once the file is downloaded and the checksum is verified, install the application

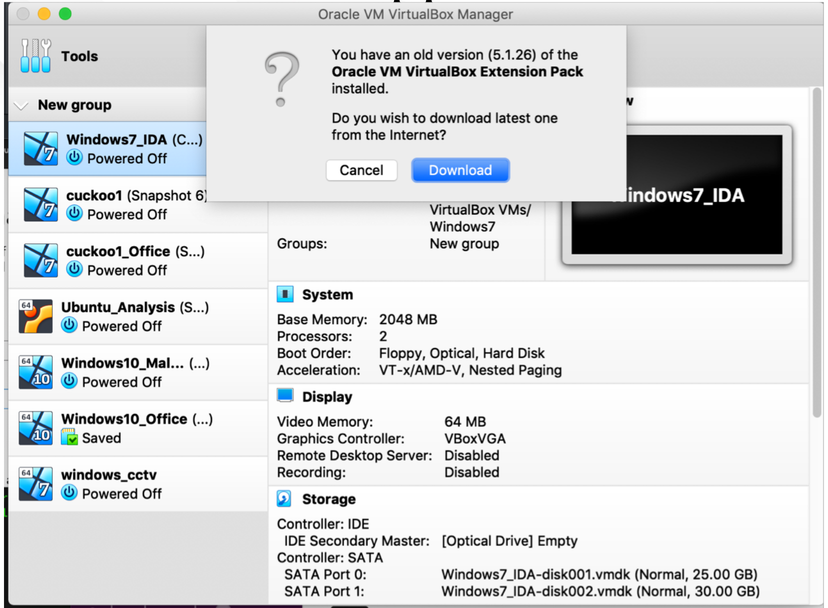


1 Double click on this icon:

VirtualBox.pkg

2 Run the VirtualBox application from the Applications Folder:

Applications



Oracle VM VirtualBox Manager

You have an old version (5.1.26) of the **Oracle VM VirtualBox Extension Pack** installed.

Do you wish to download latest one from the Internet?

Cancel | Download

Windows7_IDA (C...) Powered Off
cuckoo1 (Snapshot 6) Powered Off
cuckoo1_Office (S...) Powered Off
Ubuntu_Analysis (S...) Powered Off
Windows10_Mal... (...) Powered Off
Windows10_Office (...) Saved
windows_cctv Powered Off

VirtualBox VMs/
Windows7
Groups: New group

System
Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display
Video Memory: 64 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Windows7_IDA-disk001.vmdk (Normal, 25.00 GB)
SATA Port 1: Windows7_IDA-disk002.vmdk (Normal, 30.00 GB)

University of CINCINNATI

VirtualBox Demo

- Walk through the UI
  - – Provide an explanation and usage for the menu’s panes, buttons and tools
  - – Guest installs with Import or CD Installation
  - – Demonstrate Snapshots, and Cloning

University of CINCINNATI

VirtualBox Demo 2

- Walk through the CLI
  - Demonstrate how to start, stop and snapshot

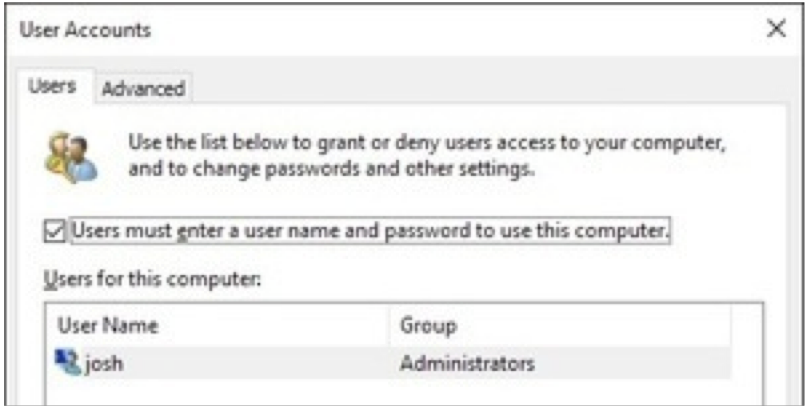
University of
CINCINNATI

VirtualBox Demo 3

- Demonstrate how to install an OVA
  - Show Configuration for Malware Lab
    - Configuring Internal or Host only Networking
    - Configure static IP addresses
    - Guest Additions – Might not want to install. Is checked by some malware!!!
    - Setting up Shared Drives
      - Optional and safer install CURL and python
    - Disabling Password
    - Disabling Firewall
    - Disabling Microsoft Defender
    - Disabling Windows Update
  - Install Monitoring software

Disable Password

- Open netplwiz
- Uncheck the “Users must enter a user name and password to use this computer”
- Apply - Reboot to confirm



User Accounts

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
josh	Administrators

Disable Firewall

- Open Control Panel
- System and Security
- Windows Defender Firewall
- Turn Windows Defender Firewall on or off
- Check “Turn off Windows Defender (Not Recommended)

  OR
- netsh advfirewall set allprofies state off

  OR
- Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False

Disable Defender

- gpedit.msc
- Computer configuration -> Administrative Templates -> Windows Components -> Windows Defender AntiVirtus
  - Turn off Windows Defender Antivirus
  - Select the ENABLED to disable windows defender
  - Verify Anti Malware service is disabled too

  OR
- regedit
- HKLM\SOFTWARE\Policies\Microsoft\Windows Defender
  - DisableAntiSpyware (Create is not there) -- DWORD (32-bit) Value
  - Set above key to 1

  OR
- Set-MpPreference -DisableRealtimeMonitoring $true

Disable Update

- Control Panel
- Administrative Tools
- Services -> scroll to “windows Update” Turn off
- Right click and select disable