VirtualBox Hardening

Holger Unterbrink
hunterbr@cisco.com

VirtualBox Hardening - Goals

- **Make VirtualBox hard to detect by malware (99%)**
- Don’t patch any binaries
- Make it as easy as possible to maintain the project
- Make it as easy as possible for other to use it

VirtualBox - VM Detection

- Mainly by “vbox” or other strings in different locations
  - Registry
  - BIOS
  - others
- Oracle VirtualBox PCI IDs
- Video Bios
- BIOS Boot Picture
- BIOS Date
- Typical Device
- Timing attacks
- others

“…0x30, 0x37, 0x2f, 0x32, 0x34, 0x2f, 0x31, 0x32..”
=> 07.24.13

Installation

VirtualBox Source Code Dependencies

Ubuntu 16.04.2 LTS server (ubuntu-16.04.2-server-amd64.iso)
xfce4, xfce4-goodies, vim, firefox packages installed

```
apt-get install subversion build-essential bcc iasl xsltproc uuid-dev zlib1g-dev libidl-dev \
        libsdl1.2-dev libxcursor-dev libasound2-dev libstdc++5 \
        libpulse-dev libxml2-dev libxslt1-dev \
        pyqt5-dev-tools libqt5opengl5-dev qtbase5-dev-tools libcap-dev \
        libxmu-dev mesa-common-dev libglu1-mesa-dev \
        linux-libc-dev libcurl4-openssl-dev libpam0g-dev \
        libxrandr-dev libxinerama-dev libqt5opengl5-dev makeself \
        libdevmapper-dev default-jdk texlive-latex-base \
        texlive-latex-extra texlive-latex-recommended \
        texlive-fonts-extra texlive-fonts-recommended \
        lib32ncurses5 lib32z1 libc6-dev-i386 lib32gcc1 gcc-multilib \
        lib32stdc++6 g++-multilib genisoimage libvpx-dev \
        qt5-default qttools5-dev-tools libqt5x11extras5-dev libssl-dev python-all-dev
```

Thank you Oracle for totally outdated build instructions !

VirtualBox – Get the source code

```
svn co http://www.virtualbox.org/svn/vbox/trunk vbox
```

A working source code can also be found at (in case the latest svn doesn’t work)
https://cisco.box.com/s/sy9yg8hae93b12jg1p2bmdauc9rfnk0i

Backup the org. source code (optional)*

```
cp -R vbox vbox-org
```

* just to avoid that you have to download it again, in case something goes wrong

Get Patch Script from Talos

Download project files:

```
git clone https://github.com/vrtadmin/vboxhardening.git
```

Disclaimer:
Alpha Status !

Script hu-patch-n-install-vbox.sh:

Edit Directories and filenames in script:

```
SOURCESDIR=/home/talos/Sources/vbox
KMKTOOLSSUBDIR=kBuild/bin/linux.amd64
MD5SUMOUT=$SOURCESDIR/kmk_md5.out
VBOXMANAGE=$SOURCESDIR/out/linux.amd64/release/bin/VXoxManage
…
```

Get Patch Script from Talos

Edit Strings and PCI IDs

VirtualBox=XirtualXox

virtualbox=xirtualxox

VIRTUALBOX=XIRTUALXOX

virtualBox=xirtualXox

vbox=vxox

Vbox=Vxox

VBox=VXox

VBOX=VXOX

Oracle=Xracle

oracle=xracle

innotek=xnnotek

InnoTek=XnnoTek

INNOTEK=XNNOTEK

PCI80EE=80EF

PCI80ee=80ef

Keep the same length !

Run Script

```
talos@ubuntu:~/sources/vbox$ ./hu-patch-n-install-vbox.sh

[*] !!! ---- READ THIS BEFORE PROCEEDING ---- !!!
[*]This scripts is patching the vbox souce code, compiles it and finally installs the VirtualBox application
[*]Run this script as the user who is supposed to use the VirtualBox app later
[*]Make sure you are in the vbox source code directory (same where the configure script is)
[*]This script was tested on Ubuntu 16.04.1 LTS - Jan 2017

[*] !!! MAKE SURE YOU HAVE FIXED THE VARIABLES in the header of this script before proceeding !!!

[*]Should we start renaming files (y/N)? y
[*]Logging to hu-patch-n-install-vbox.out
[*]Replacing string "VirtualBox" to "XirtualXox" in all filenames
[*]Replacing string "virtualbox" to "xirtualxox" in all filenames
[*]Replacing string "vbox" to "vxox" in all filenames
```

Copy the script to the vbox source directory

Only answer 'no' if you know what you do !

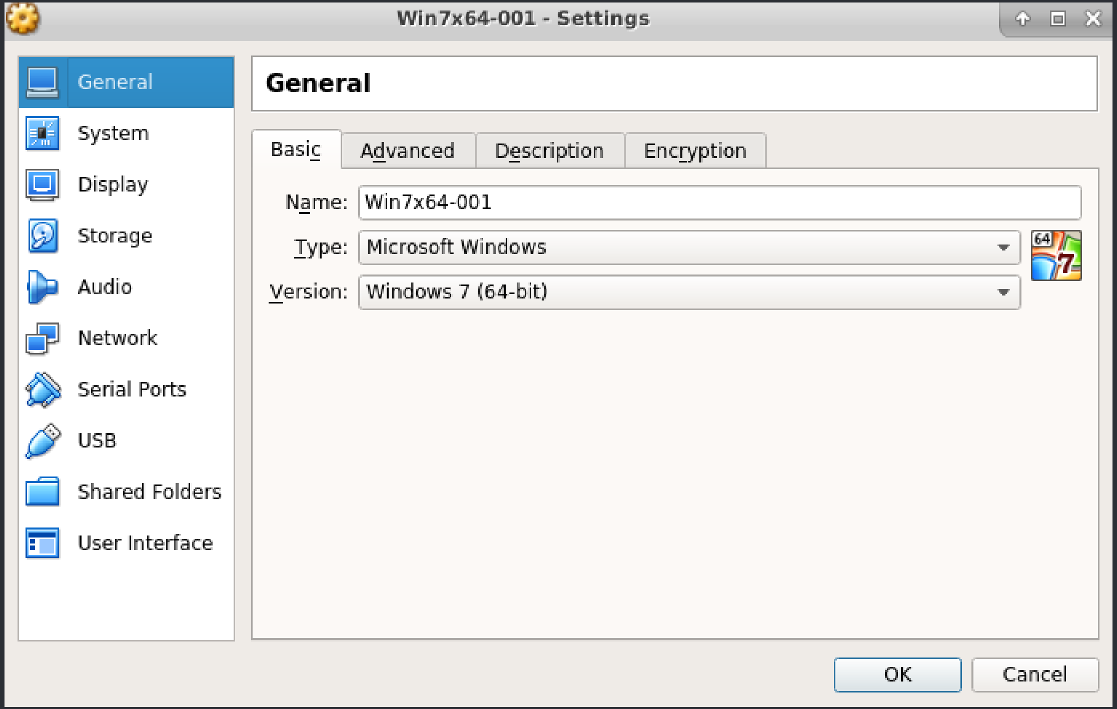
No, is only for cases when you run the script the 2nd time or similar.

Run Script

Reboot …

- If everything worked, you should see a vbox network interface e.g. *vxoxnet0*
- Start *ubuntu:~$* ***VirtualBox***

Setup your VirtualBox VM

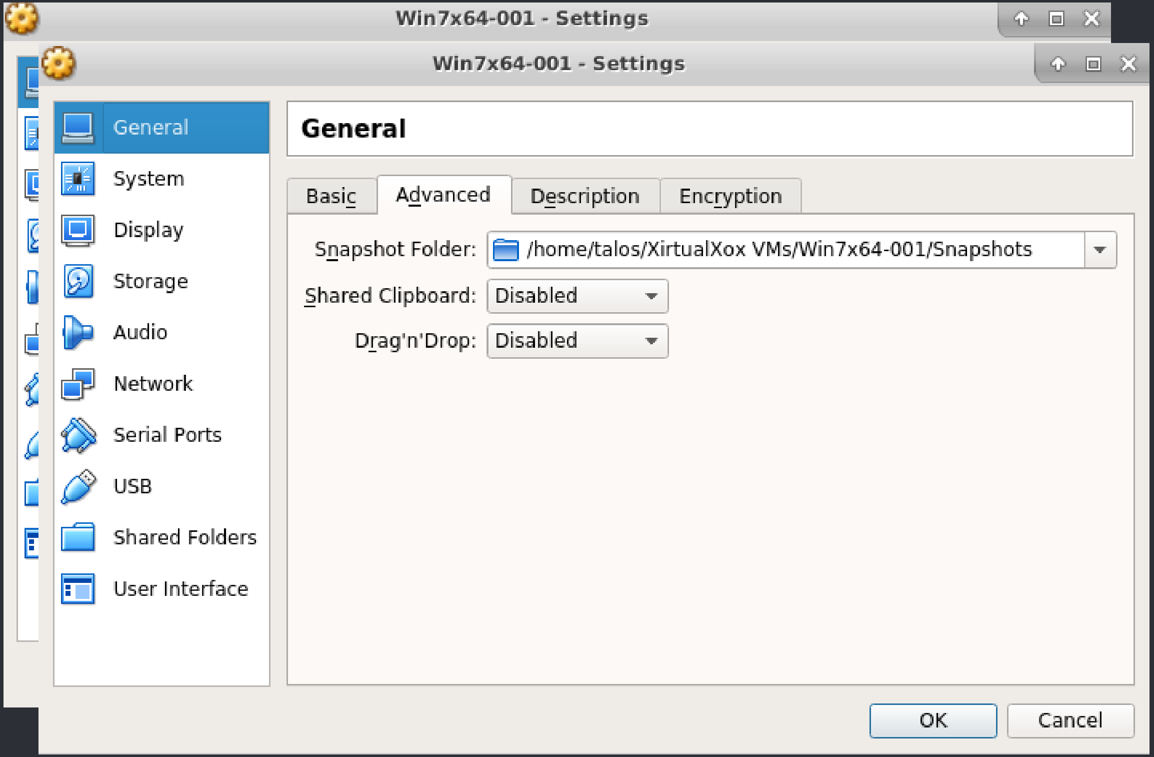


Name: Win7x64-001

Type: Microsoft Windows

Version: Windows 7 (64-bit)

Setup your VirtualBox VM



Win7x64-001 - Settings

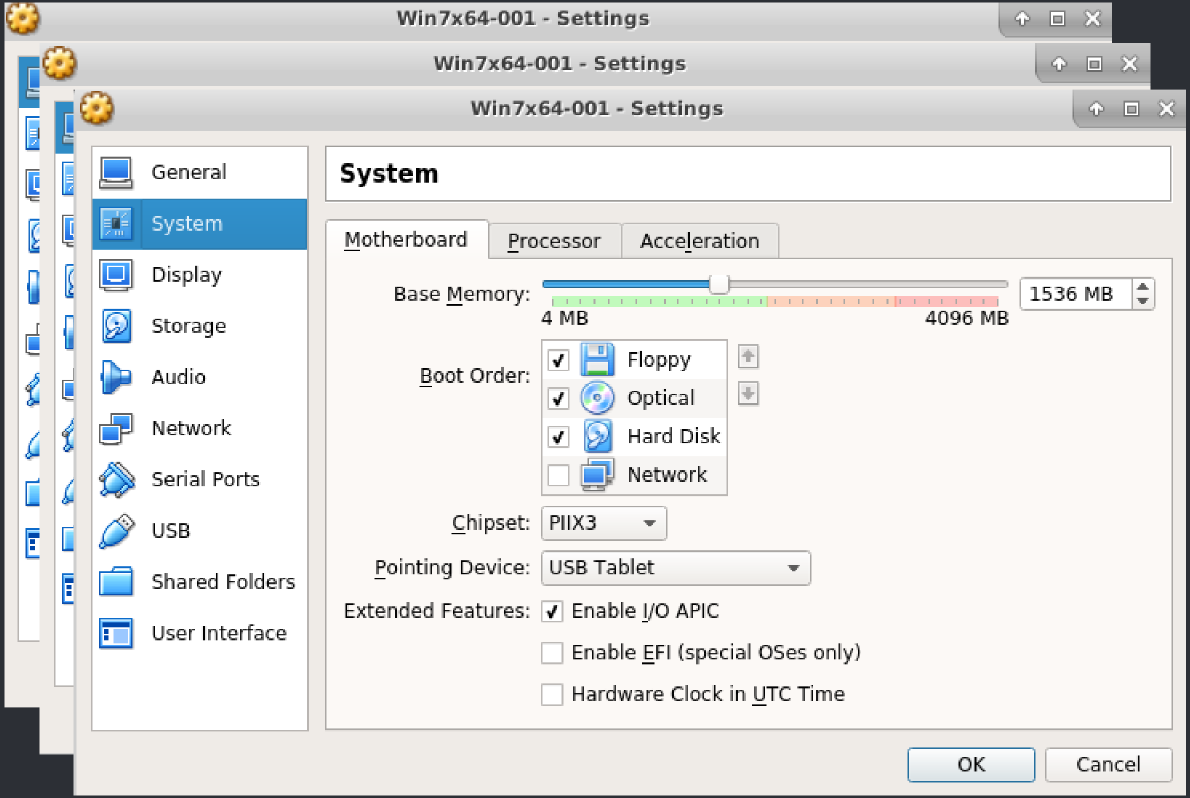
General

Snapshot Folder: /home/talos/XirtualXox VMs/Win7x64-001/Snapshots

Shared Clipboard: Disabled

Drag'n'Drop: Disabled

Setup your VirtualBox VM



System

Base Memory: 1536 MB (4 MB – 4096 MB)

Boot Order:

- ☑ Floppy
- ☑ Optical
- ☑ Hard Disk
- □ Network

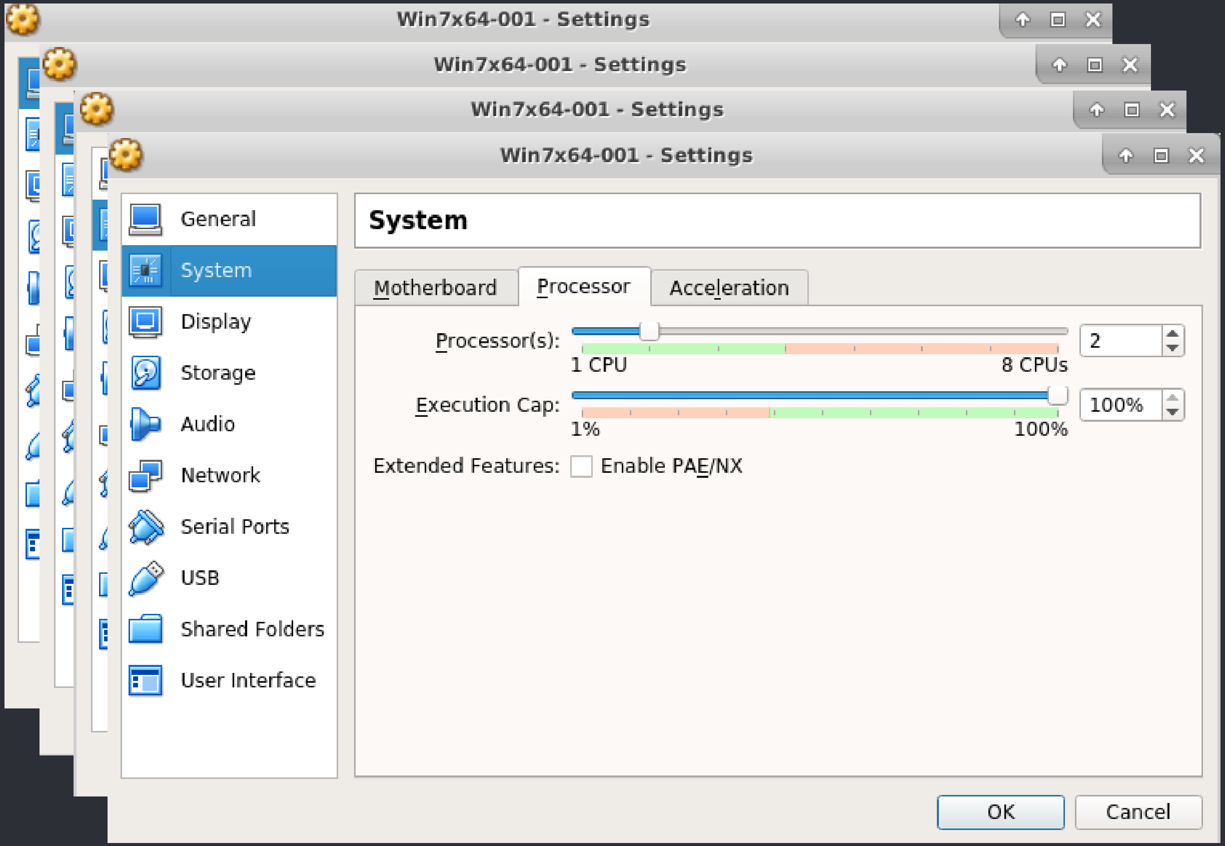
Chipset: PIIX3

Pointing Device: USB Tablet

Extended Features:

- ☑ Enable I/O APIC
- □ Enable EFI (special OSes only)
- □ Hardware Clock in UTC Time

Setup your VirtualBox VM



Win7x64-001 - Settings

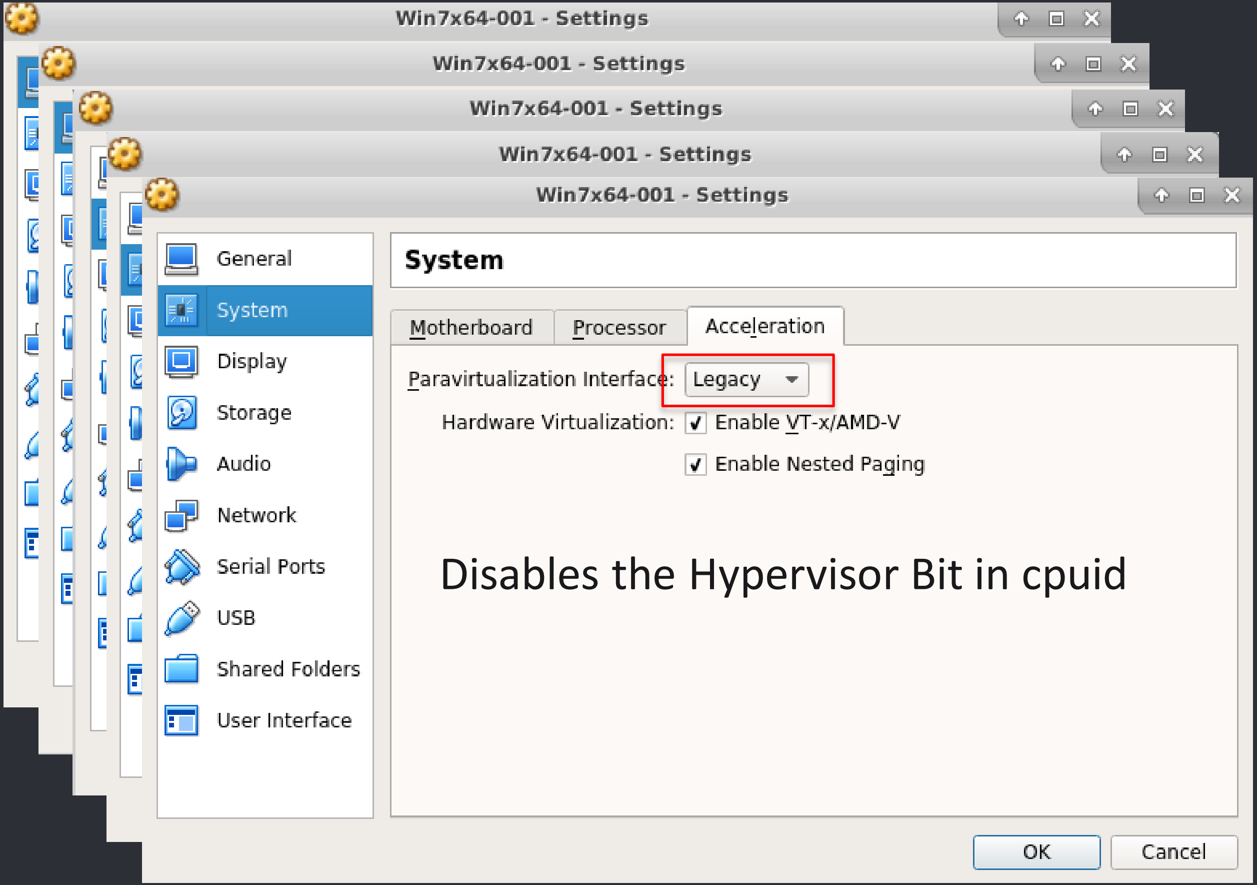
System

Processor(s): 2 (1 CPU – 8 CPUs)

Execution Cap: 100% (1% – 100%)

Extended Features: □ Enable PAE/NX

Setup your VirtualBox VM



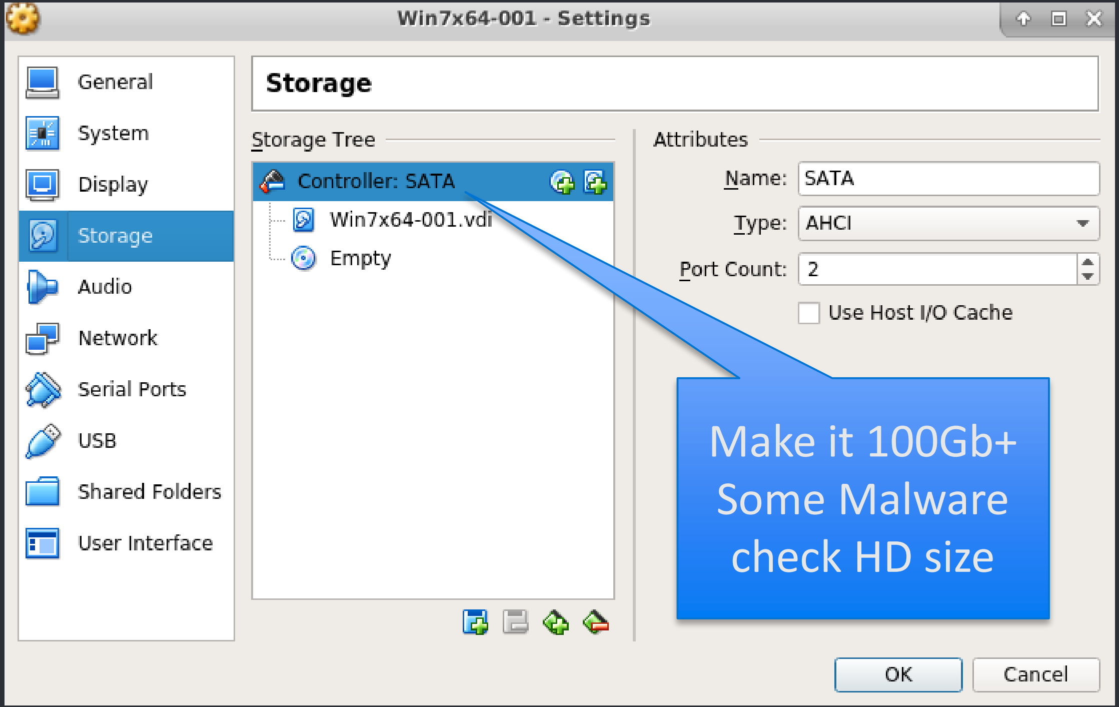
Paravirtualization Interface: Legacy

Hardware Virtualization: ☑ Enable VT-x/AMD-V

☑ Enable Nested Paging

Disables the Hypervisor Bit in cpuid

Setup your VirtualBox VM



Name: SATA

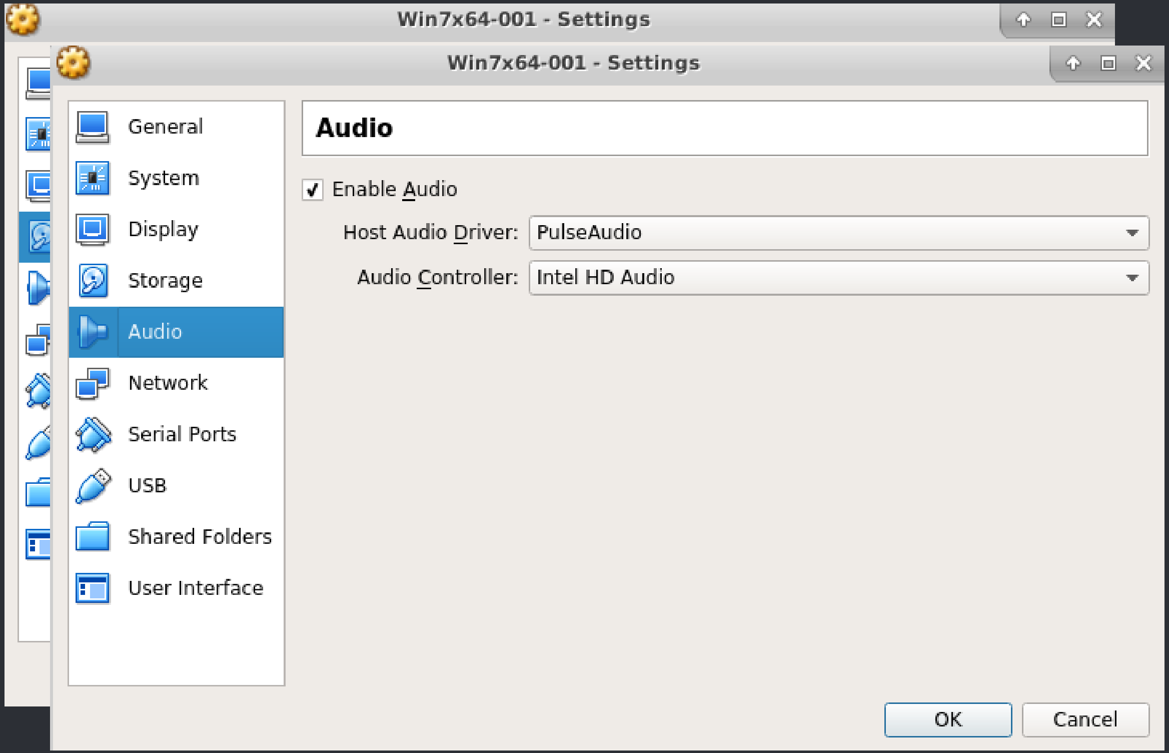
Type: AHCI

Port Count: 2

□ Use Host I/O Cache

Make it 100Gb+
Some Malware
check HD size

Setup your VirtualBox VM



Win7x64-001 - Settings

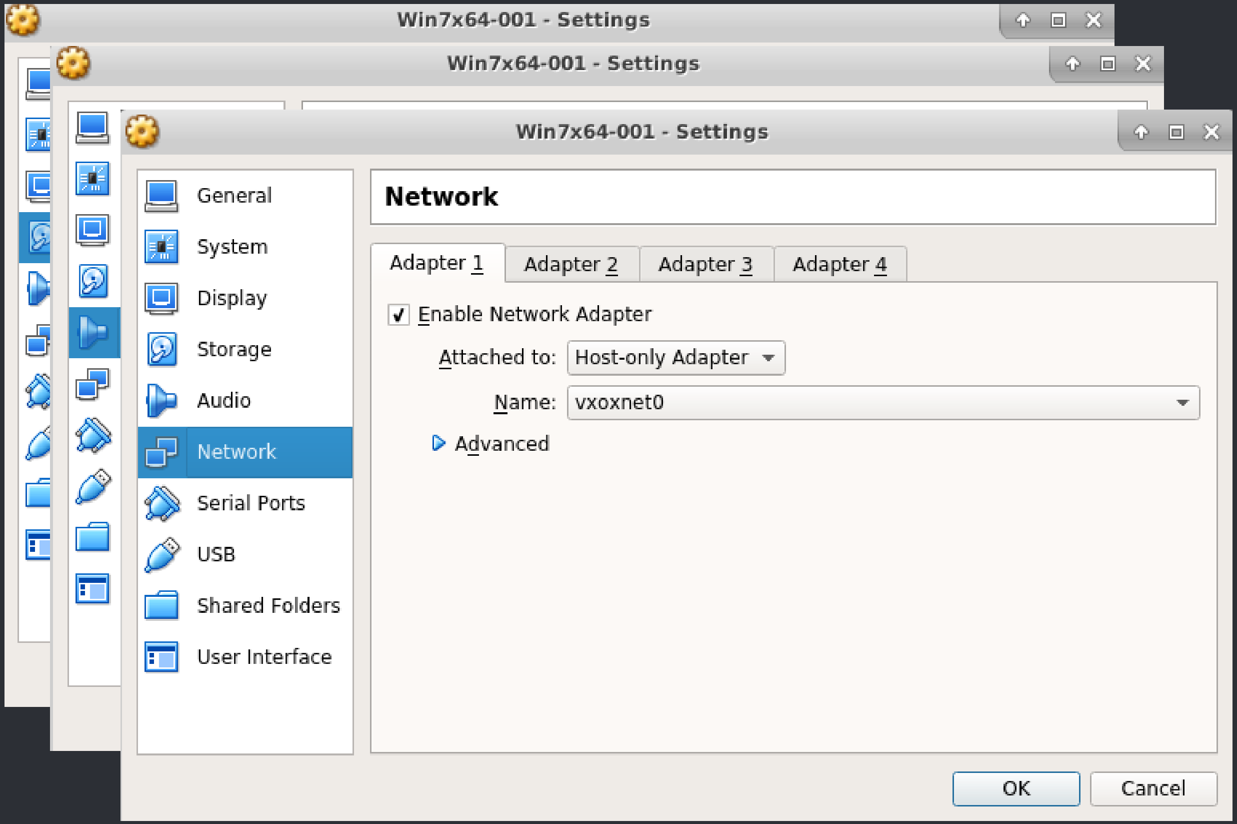
Audio

☑ Enable Audio

Host Audio Driver: PulseAudio

Audio Controller: Intel HD Audio

Setup your VirtualBox VM



Win7x64-001 - Settings

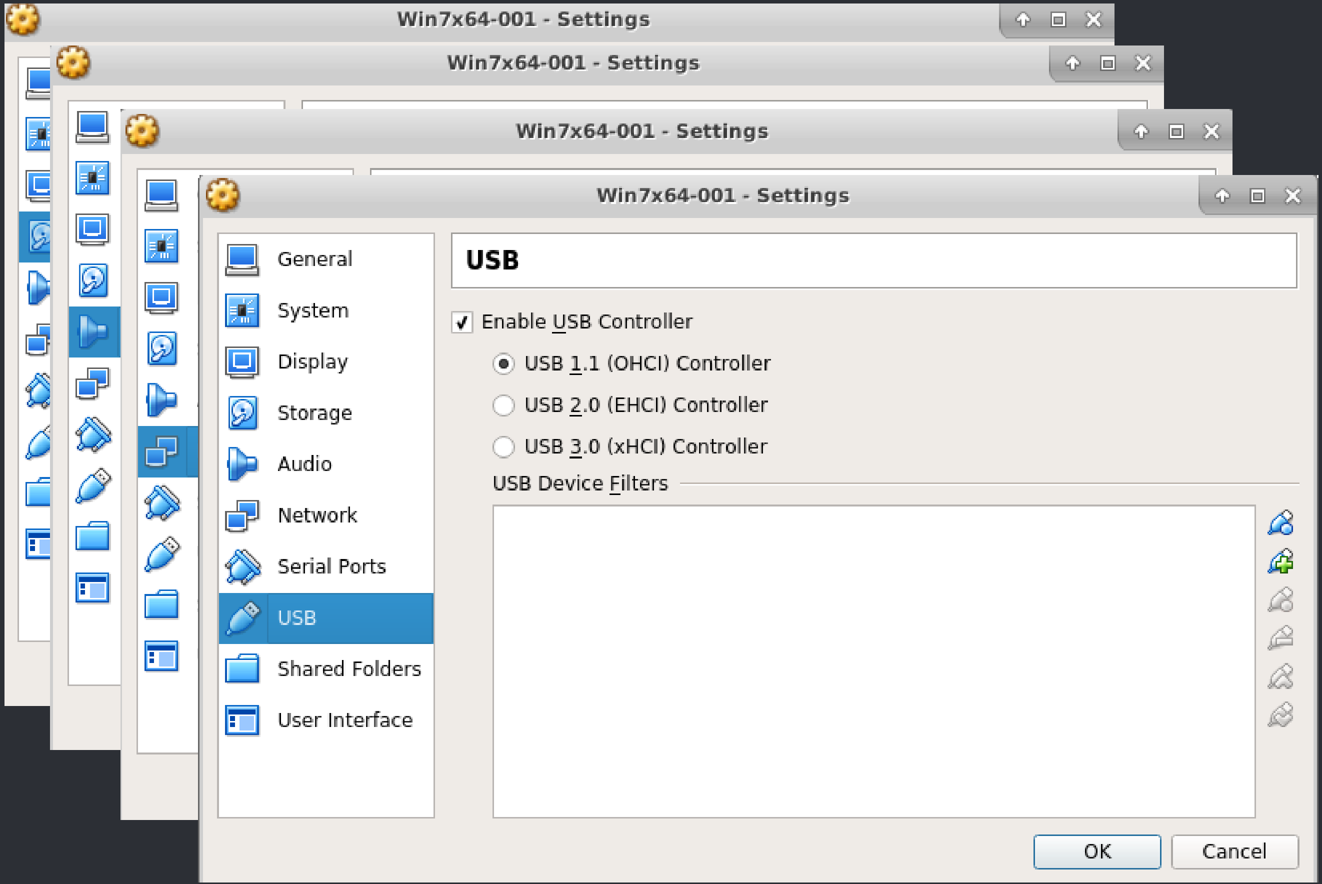
Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: vxoxnet0

Setup your VirtualBox VM



Win7x64-001 - Settings

USB

☑ Enable USB Controller

● USB 1.1 (OHCI) Controller

○ USB 2.0 (EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

TALOS

Setup your VirtualBox VM

Don’t start the VM yet!

Close VM and VirtualBox and
Proceed on next slide

Patch the Virtual Machine

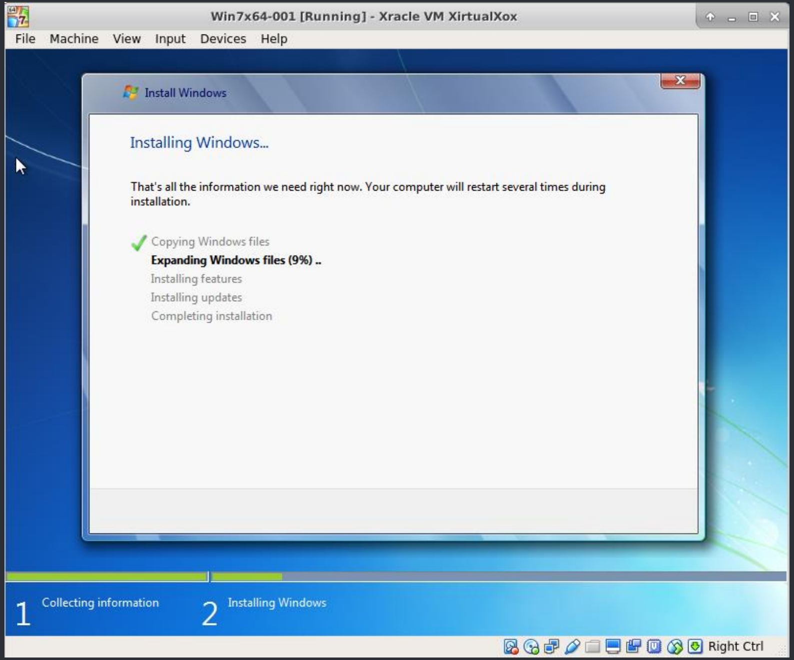
Fixing boot picture and stuff… (might integrate that in the patch script in the future)

Make sure you have edited the directories inside the script before executing !
e.g. VBODIR="/home/talos/sources/HU_VirtualBoxObfuscateHW2017“

```
talos@ubuntu:~$ ./hu-obfuscate-vm.sh

This script is patching an existing VirtualBox VM. It obfuscates a couple of HW strings
Make sure the VM and VirtualBox App is closed before you execute this script
Installed VMs:
[1] "Win7x64-001"
Which one do you want to patch (1-1): 1
…
```

Proceed installing OS in Vbox VM

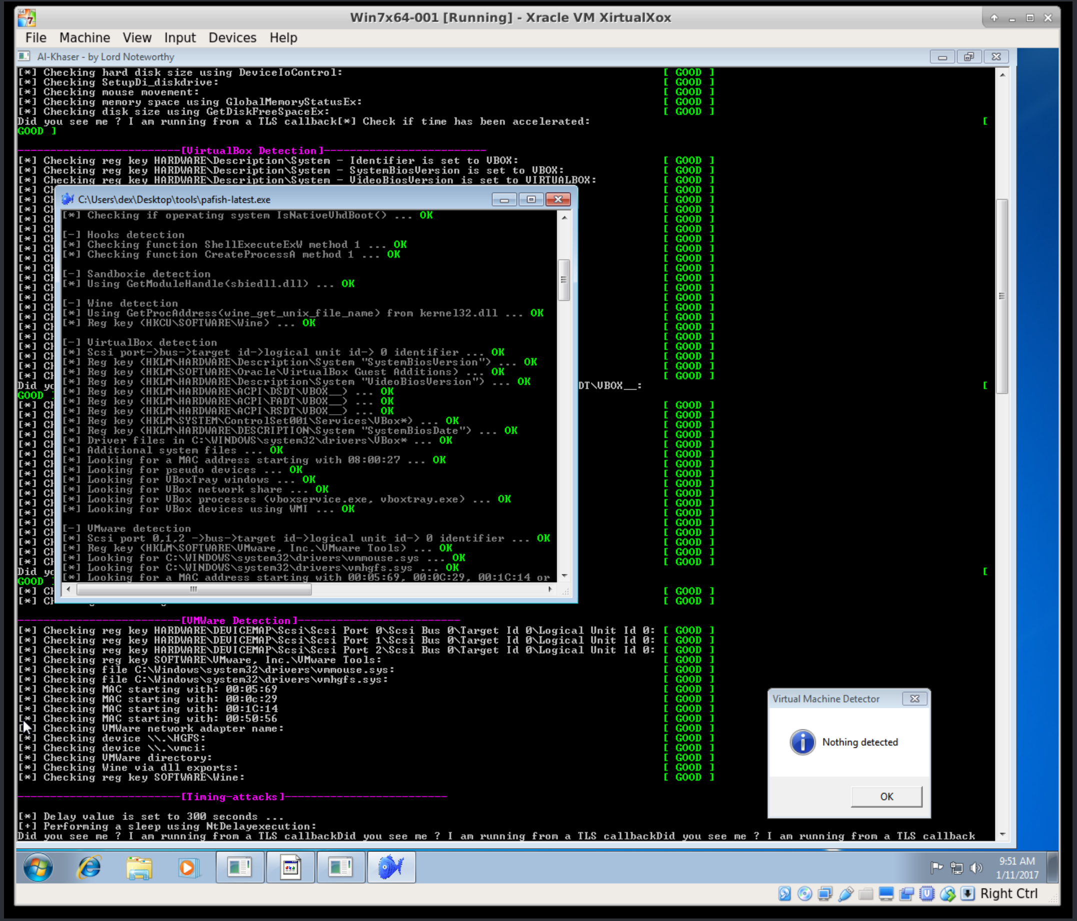


Installing Windows...

That's all the information we need right now. Your computer will restart several times during installation.

- ✓ Copying Windows files
- **Expanding Windows files (9%) ..**
- Installing features
- Installing updates
- Completing installation

Finally Run Vbox VM



Win7x64-001 [Running] - Xracle VM XirtualXox
File
Machine
View
Input
Devices
Help
Al-Khaser - by Lord Noteworthy
C:\Users\dex\Desktop\tools\pafish-latest.exe
9:51 AM
1/11/2017
Right Ctrl

```
[*] Checking hard disk size using DeviceIoControl:                                  [ GOOD ]
[*] Checking SetupDi_diskdrive:                                                     [ GOOD ]
[*] Checking mouse movement:                                                        [ GOOD ]
[*] Checking memory space using GlobalMemoryStatusEx:                               [ GOOD ]
[*] Checking disk size using GetDiskFreeSpaceEx:                                    [ GOOD ]
Did you see me ? I am running from a TLS callback[*] Check if time has been accelerated:                 [
GOOD ]

-------------------------[VirtualBox Detection]-------------------------
[*] Checking reg key HARDWARE\Description\System - Identifier is set to VBOX:       [ GOOD ]
[*] Checking reg key HARDWARE\Description\System - SystemBiosVersion is set to VBOX: [ GOOD ]
[*] Checking reg key HARDWARE\Description\System - VideoBiosVersion is set to VIRTUALBOX: [ GOOD ]
```

```
[*] Checking if operating system IsNativeVhdBoot() ... OK

[-] Hooks detection
[*] Checking function ShellExecuteExW method 1 ... OK
[*] Checking function CreateProcessA method 1 ... OK

[-] Sandboxie detection
[*] Using GetModuleHandle(sbiedll.dll) ... OK

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK
[*] Reg key (HKCU\SOFTWARE\Wine) ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\DSDT\VBOX__) ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\FADT\VBOX__) ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\RSDT\VBOX__) ... OK
[*] Reg key (HKLM\SYSTEM\ControlSet001\Services\VBox*) ... OK
[*] Reg key (HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate") ... OK
[*] Driver files in C:\WINDOWS\system32\drivers\VBox* ... OK
[*] Additional system files ... OK
[*] Looking for a MAC address starting with 08:00:27 ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VBoxTray windows ... OK
[*] Looking for VBox network share ... OK
[*] Looking for VBox processes (vboxservice.exe, vboxtray.exe) ... OK
[*] Looking for VBox devices using WMI ... OK

[-] VMware detection
[*] Scsi port 0,1,2 ->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK
[*] Looking for a MAC address starting with 00:05:69, 00:0C:29, 00:1C:14 or
```

```
-------------------------[VMWare Detection]-------------------------
[*] Checking reg key HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0: [ GOOD ]
[*] Checking reg key HARDWARE\DEVICEMAP\Scsi\Scsi Port 1\Scsi Bus 0\Target Id 0\Logical Unit Id 0: [ GOOD ]
[*] Checking reg key HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0\Target Id 0\Logical Unit Id 0: [ GOOD ]
[*] Checking reg key SOFTWARE\VMware, Inc.\VMware Tools:                            [ GOOD ]
[*] Checking file C:\Windows\system32\drivers\vmmouse.sys:                          [ GOOD ]
[*] Checking file C:\Windows\system32\drivers\vmhgfs.sys:                           [ GOOD ]
[*] Checking MAC starting with: 00:05:69                                            [ GOOD ]
[*] Checking MAC starting with: 00:0c:29                                            [ GOOD ]
[*] Checking MAC starting with: 00:1C:14                                            [ GOOD ]
[*] Checking MAC starting with: 00:50:56                                            [ GOOD ]
[*] Checking VMWare network adapter name:                                           [ GOOD ]
[*] Checking device \\.\HGFS:                                                       [ GOOD ]
[*] Checking device \\.\vmci:                                                       [ GOOD ]
[*] Checking VMWare directory:                                                      [ GOOD ]
[*] Checking Wine via dll exports:                                                  [ GOOD ]
[*] Checking reg key SOFTWARE\Wine:                                                 [ GOOD ]

-------------------------[Timing-attacks]-------------------------

[*] Delay value is set to 300 seconds ...
[+] Performing a sleep using NtDelayexecution:
Did you see me ? I am running from a TLS callbackDid you see me ? I am running from a TLS callbackDid you see me ? I am running from a TLS callback
```

Virtual Machine Detector

Nothing detected

OK

- Al-Khaser
- Pafish
- VMDE

99% undetected

Other Related Projects

Kernelmode.info: Windows – Patching binaries
http://www.kernelmode.info/forum/viewtopic.php?f=11&t=3478

Hardening Win7 x64 on VirtualBox for Malware Analysis
https://byte-atlas.blogspot.co.uk/2017/02/hardening-vbox-win7x64.html

Zer0m0n (Cuckoo 1.2)
https://github.com/motazreda/zer0m0n

Talos

http://www.talosintelligence.com/

@talossecurity

cisco™