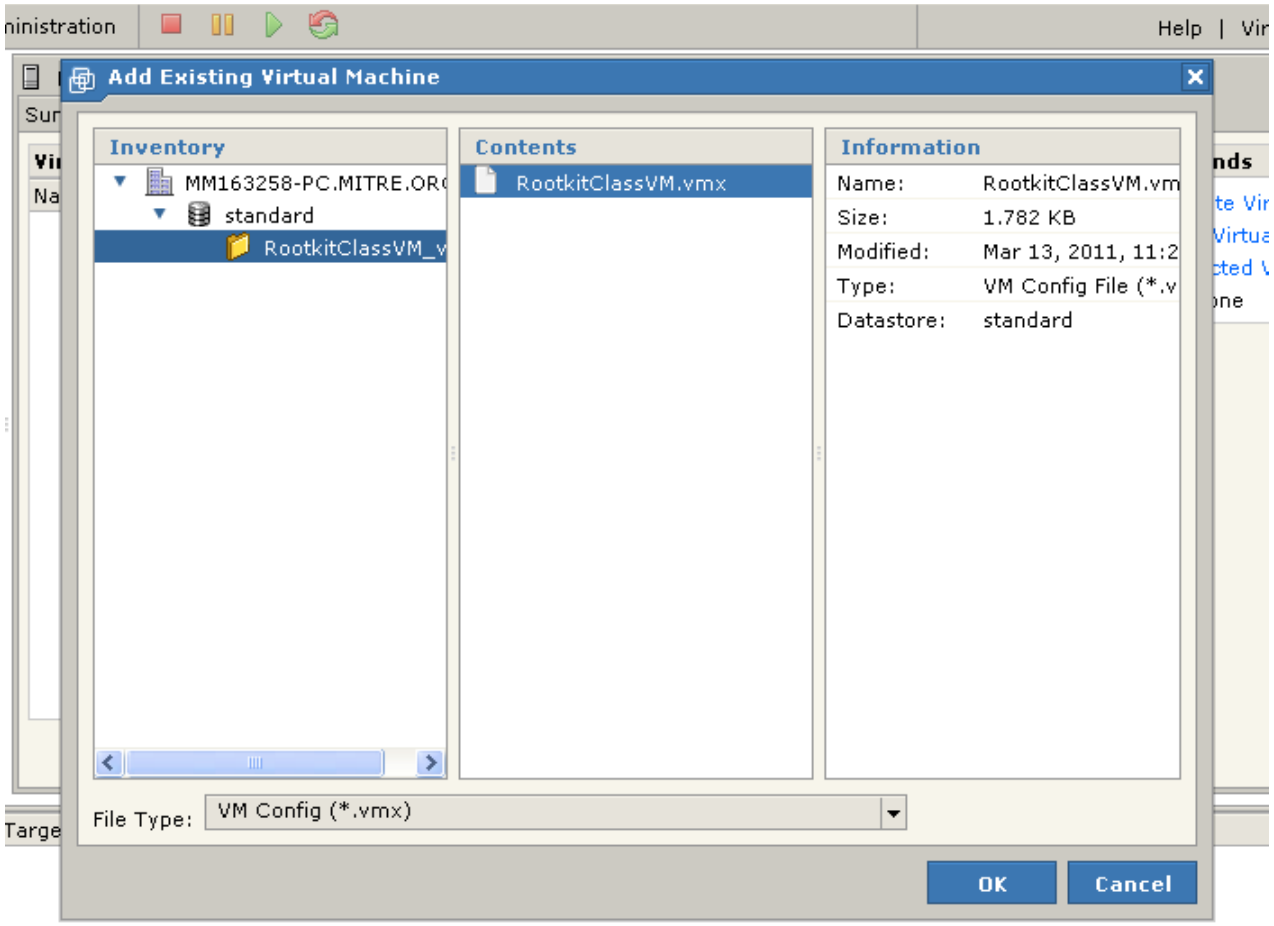
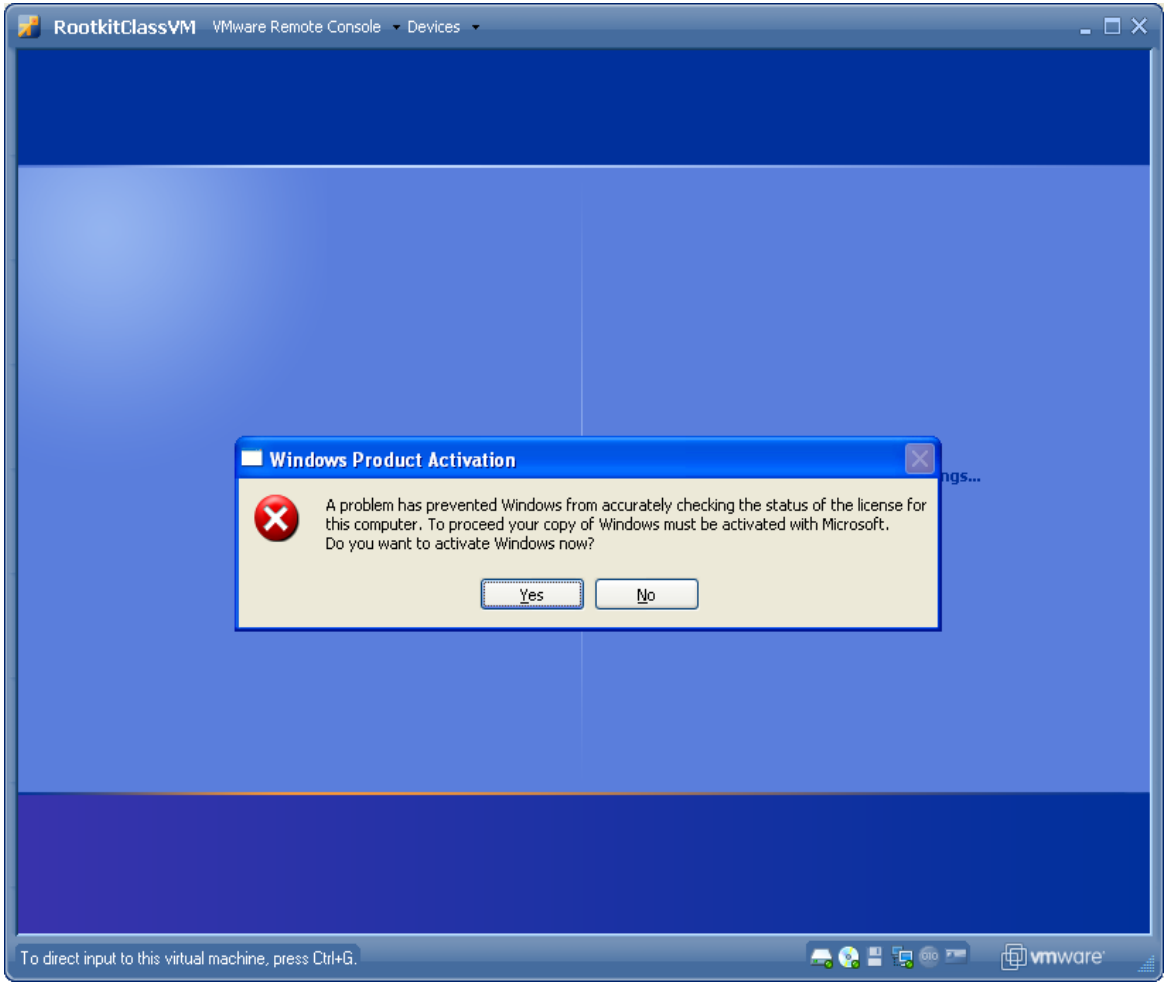
Adding Virtual Machine to Inventory



Turn off Networking then Start VM

- Infected with Vanquish. Deleting it failed.
- At nn:nn /interactive cmd.exe, the files were invisible.
- Hijackthis 2.0.5 beta
  - C:\windows\fat.bat
  - Http trusted zones
  - Checked everything!
  - Restart
  - Rescan
  - Restart

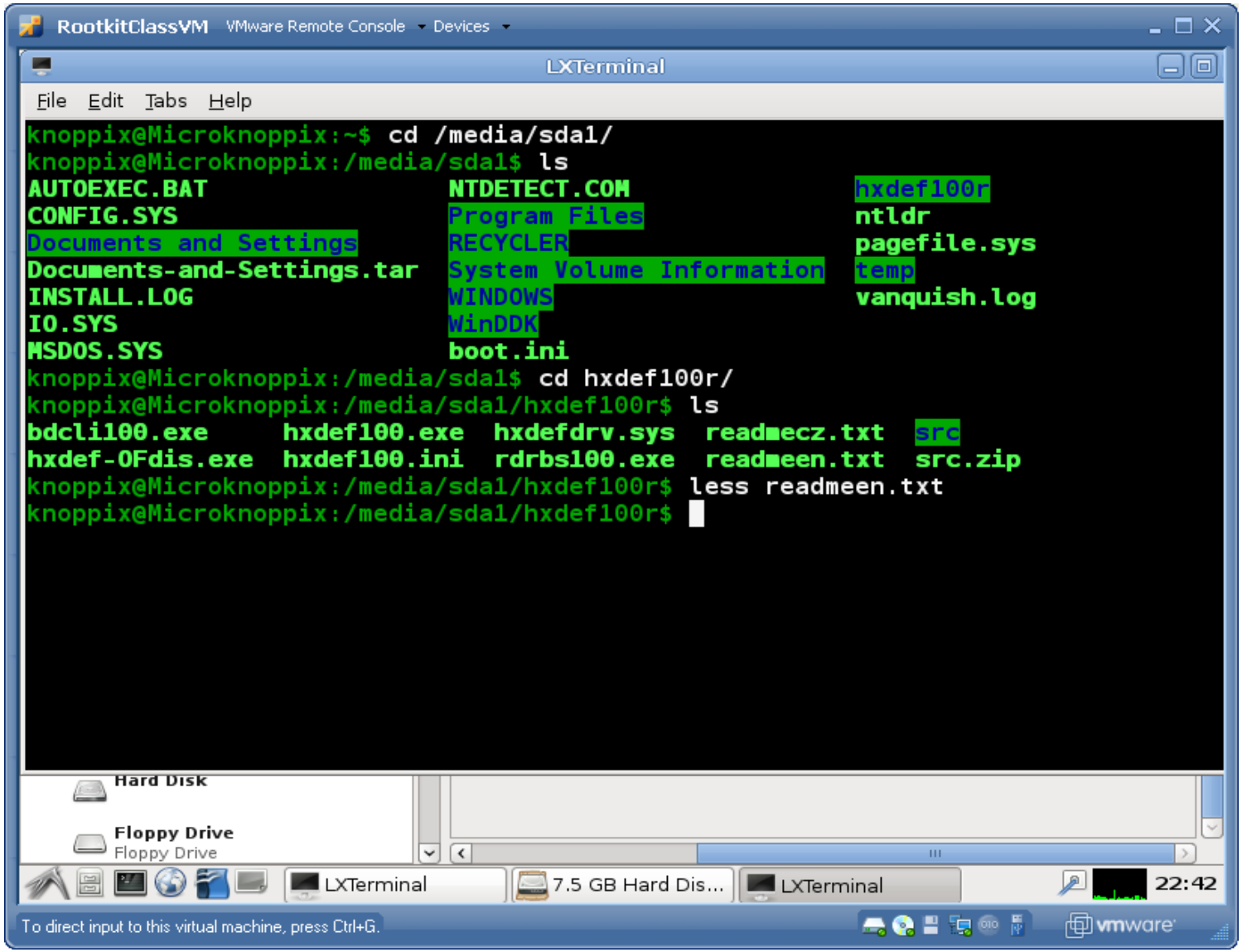
Windows Activation!



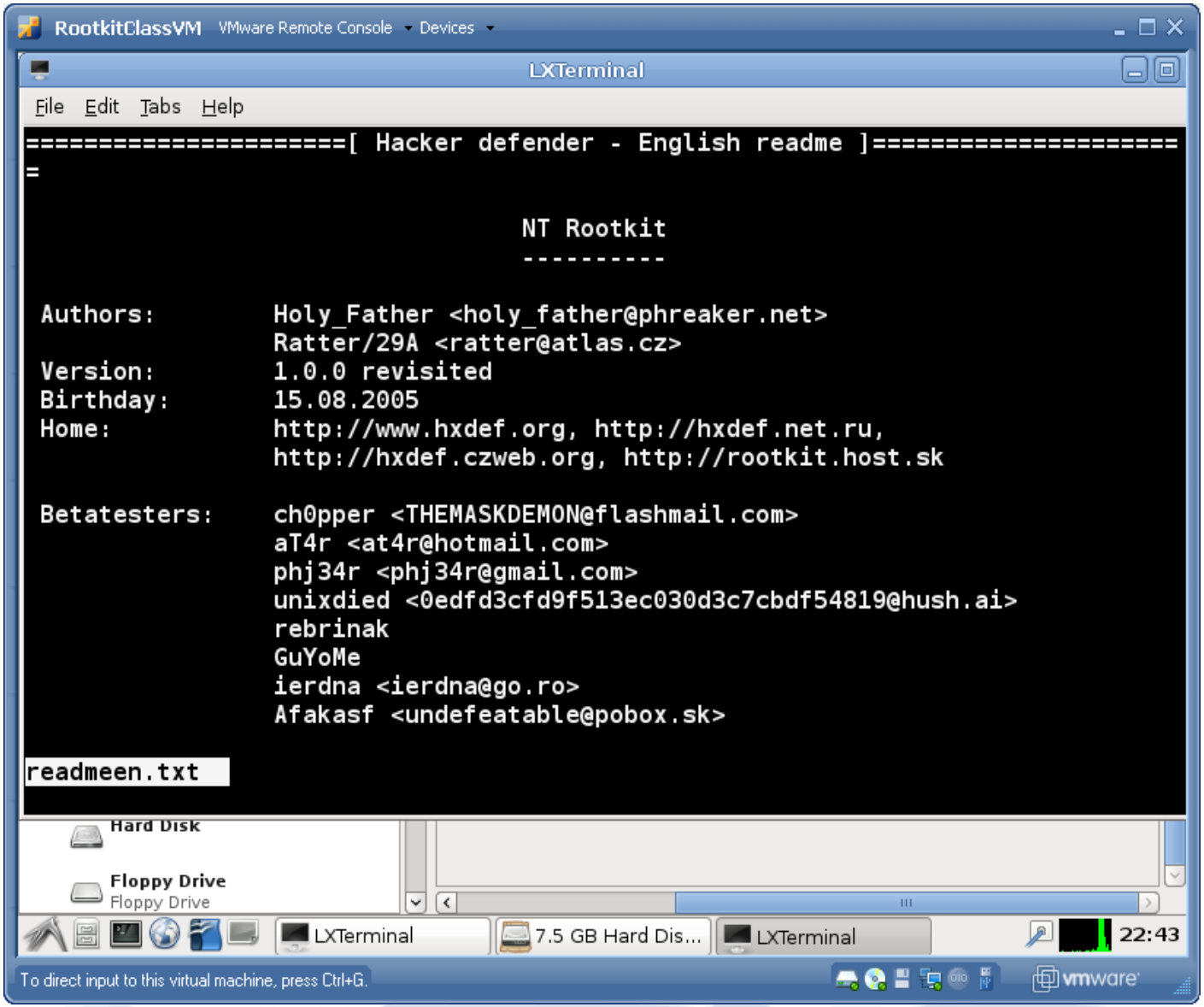
Knoppix 6.4.4 DVD

- Added following line to RootkitClassVM.vmx to gain access to BIOS settings
  - bios.bootDelay = "5000"
  - F2 at boot screen
  - Put CD-ROM at top
- Hard drive is /media/sda1
- Tarred Documents and Settings to /media/sda1 root

hxdef100r


RootkitClassVM
VMware Remote Console
Devices
LXTerminal
File Edit Tabs Help
knoppix@Microknoppix:~$ cd /media/sda1/
knoppix@Microknoppix:/media/sda1$ ls
AUTOEXEC.BAT
CONFIG.SYS
Documents and Settings
Documents-and-Settings.tar
INSTALL.LOG
IO.SYS
MSDOS.SYS
NTDETECT.COM
Program Files
RECYCLER
System Volume Information
WINDOWS
WinDDK
boot.ini
hxdef100r
ntldr
pagefile.sys
temp
vanquish.log
knoppix@Microknoppix:/media/sda1$ cd hxdef100r/
knoppix@Microknoppix:/media/sda1/hxdef100r$ ls
bdcli100.exe
hxdef-OFdis.exe
hxdef100.exe
hxdef100.ini
hxdefdrv.sys
rdrbs100.exe
readmecz.txt
readmeen.txt
src
src.zip
knoppix@Microknoppix:/media/sda1/hxdef100r$ less readmeen.txt
knoppix@Microknoppix:/media/sda1/hxdef100r$
Hard Disk
Floppy Drive
Floppy Drive
LXTerminal
7.5 GB Hard Dis...
LXTerminal
22:42
To direct input to this virtual machine, press Ctrl+G.
vmware

Hacker Defender



Findings

- Found 2 rootkits
  - Vanquish
  - Hacker Defender
  - Evidence of others – destructively deleted with hijack this
- Caused Microsoft to activate, had to boot from CD.
- BIOS seems to be clean, no time to verify

Sponsor Recommendation

- Drive is not safe!
- Pull network cable, continue offline analysis
- Bring in forensic analysis tools
- Carefully examine and restore user data not available elsewhere.
- Restore data to new machine.