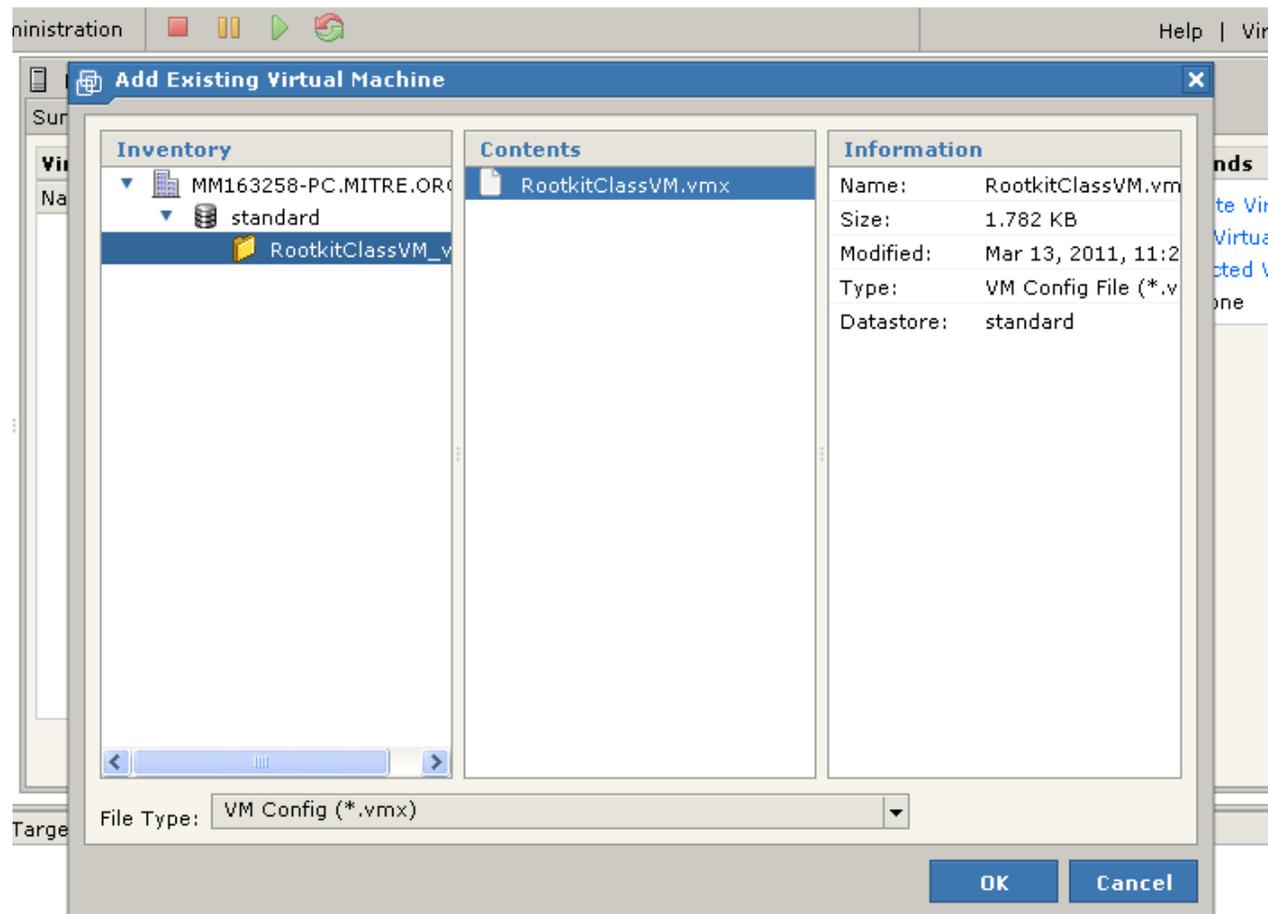


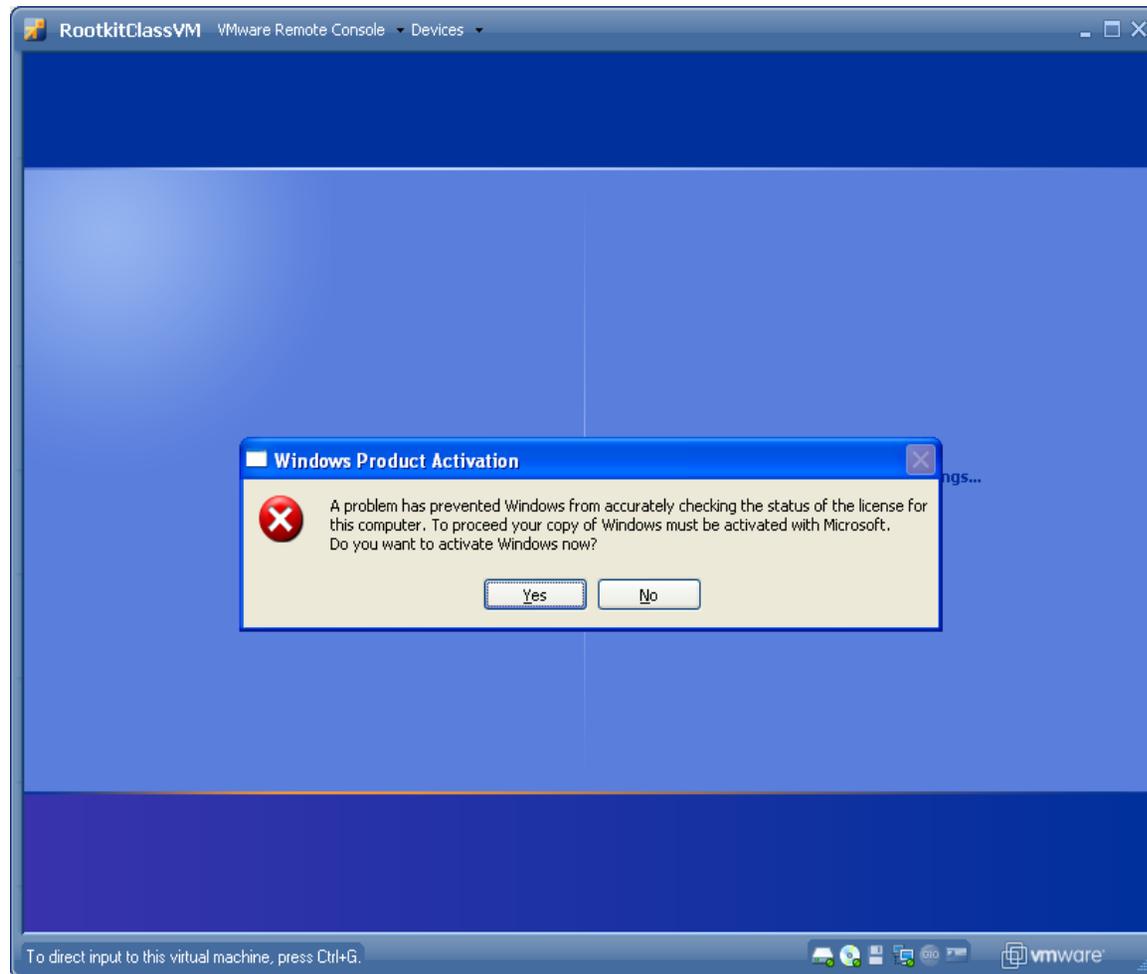
# Adding Virtual Machine to Inventory



# 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

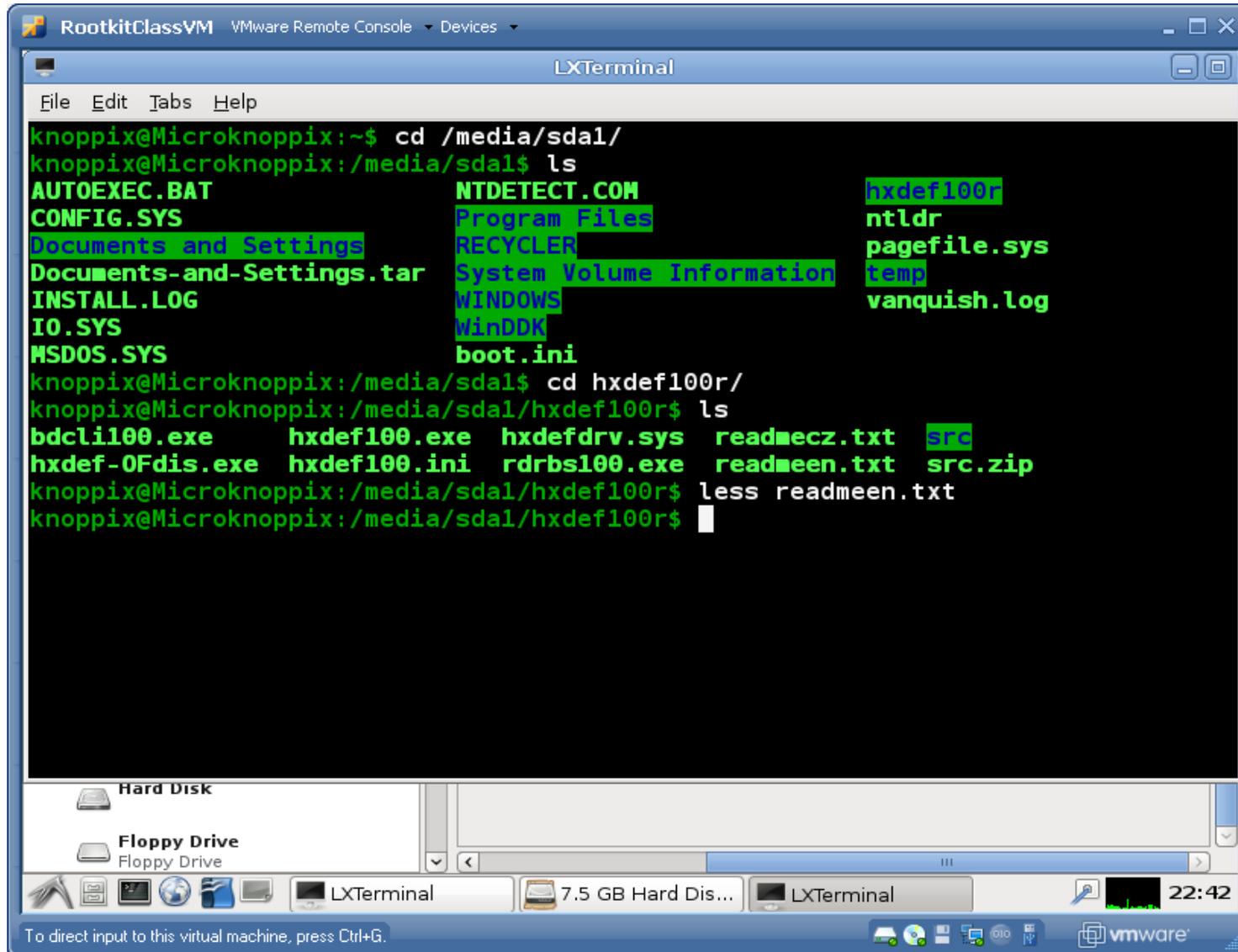
# Windows Activation!



# 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
- Tared Documents and Settings to /media/sda1 root

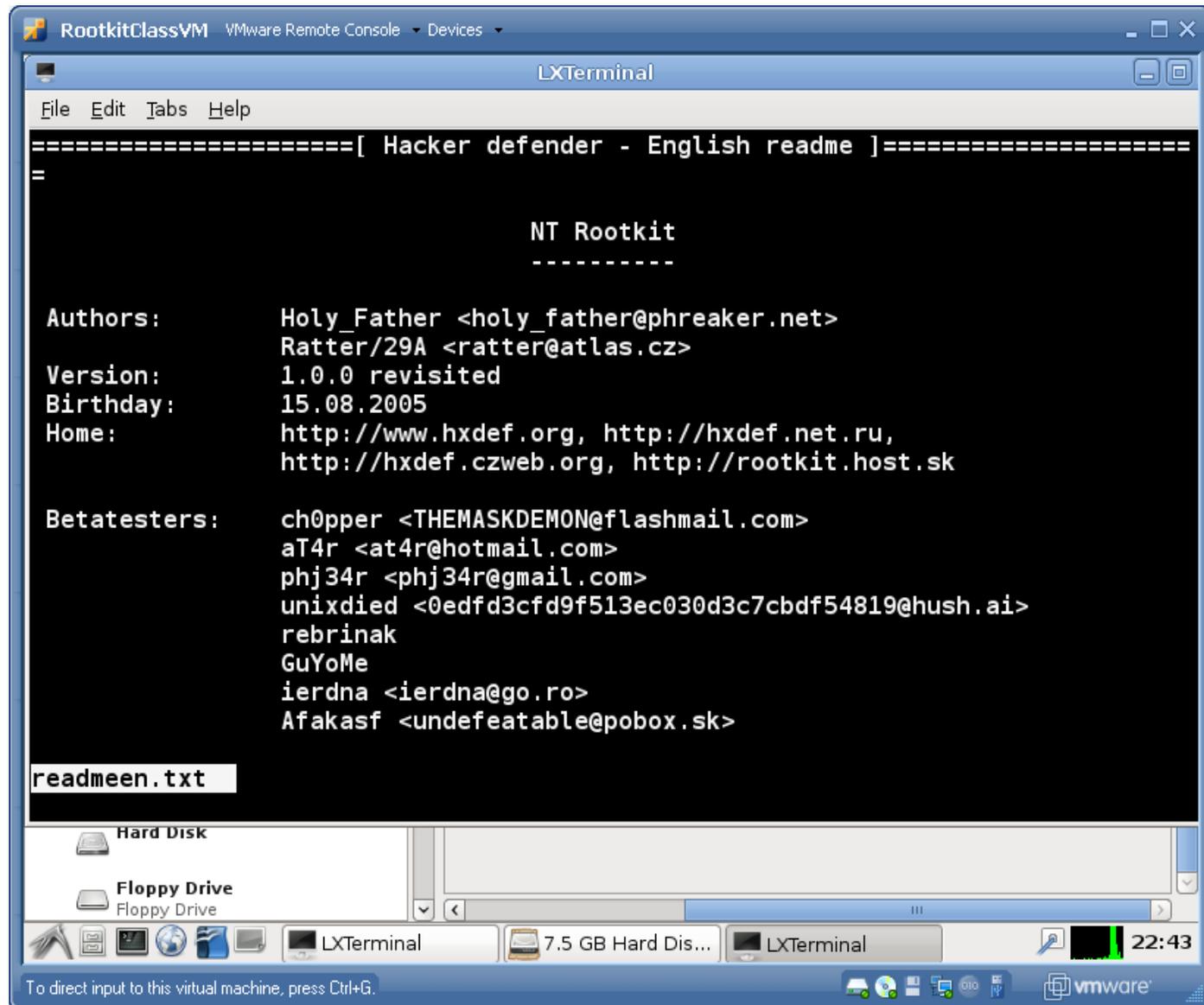
# hxdef100r



The screenshot shows a VMware Remote Console window titled "RootkitClassVM". Inside, an LXTerminal window is open, displaying a shell prompt "knoppix@Microknoppix:~\$". The user has navigated to the directory "/media/sda1/" and executed the "ls" command. The output shows a list of files and directories, including "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", and "vanquish.log". The user then navigates to the "hxdef100r" directory and runs "ls" again, showing files like "bdcli100.exe", "hxdef100.exe", "hxdefdrv.sys", "readmecz.txt", "src", "hxdef-0Fdis.exe", "hxdef100.ini", "rdrbs100.exe", "readmeen.txt", and "src.zip". Finally, the user runs "less readmeen.txt". The terminal window has a menu bar with "File", "Edit", "Tabs", and "Help". Below the terminal, there are icons for "Hard Disk" and "Floppy Drive". At the bottom, a taskbar shows "LXTerminal", "7.5 GB Hard Dis...", and another "LXTerminal" window. The system tray includes a search icon, a network icon, and the time "22:42". A VMware logo is visible in the bottom right corner. A footer note reads "To direct input to this virtual machine, press Ctrl+G."

```
knoppix@Microknoppix:~$ cd /media/sda1/
knoppix@Microknoppix:/media/sda1$ ls
AUTOEXEC.BAT          NTDETECT.COM        hxdef100r
CONFIG.SYS            Program Files       ntlldr
Documents and Settings  RECYCLER            pagefile.sys
Documents-and-Settings.tar  System Volume Information  temp
INSTALL.LOG          WINDOWS             vanquish.log
IO.SYS               WinDDK
MSDOS.SYS            boot.ini
knoppix@Microknoppix:/media/sda1$ cd hxdef100r/
knoppix@Microknoppix:/media/sda1/hxdef100r$ ls
bdcli100.exe      hxdef100.exe  hxdefdrv.sys  readmecz.txt  src
hxdef-0Fdis.exe  hxdef100.ini  rdrbs100.exe  readmeen.txt  src.zip
knoppix@Microknoppix:/media/sda1/hxdef100r$ less readmeen.txt
knoppix@Microknoppix:/media/sda1/hxdef100r$
```

# Hacker Defender



The screenshot shows a VMware Remote Console window titled "RootkitClassVM". Inside, an LXTerminal window displays the following text:

```
=====[ Hacker defender - English readme ]=====
=

                        NT Rootkit
                        -----

Authors:      Holy_Father <holy_father@phreaker.net>
              Ratter/29A <ratter@atlas.cz>
Version:      1.0.0 revisited
Birthday:     15.08.2005
Home:         http://www.hxdef.org, http://hxdef.net.ru,
              http://hxdef.czweb.org, http://rootkit.host.sk

Betatesters: ch0pper <THEMASKDEMON@flashmail.com>
              aT4r <at4r@hotmail.com>
              phj34r <phj34r@gmail.com>
              unixdied <0edfd3cfd9f513ec030d3c7cbdf54819@hush.ai>
              rebrinak
              GuYoMe
              ierdna <ierdna@go.ro>
              Afakasf <undefeatable@pobox.sk>

readmeen.txt
```

The terminal window also shows a file named "readmeen.txt" selected. The VMware interface includes a taskbar at the bottom with icons for "Hard Disk", "Floppy Drive", "LXTerminal", and "7.5 GB Hard Dis...". The system tray shows the time as 22:43 and the VMware logo.

# 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.