Setup your laptop for PDF workshop

- Copy directory “files” from DVD to your HD
- Unzip “VM\BT4-R1.zip” from DVD to your HD
- Return DVD to me
- Start VM (VirtualBox: create new VM, use .vmdk)
- Logon BackTrack4: user “root” password “toor”
- cat “readme.txt”
- Start analyzing exercise “ex001.pdf”, read “PDF Chapter.pdf” for help

PDF Analysis Workshop

- all exercise PDFs are bening, no exploit, except:
- zipped exercise PDFs contain bening exploits and might trigger AV
- password zip: infected
- First analyze PDF with pdfid.py
- Then analyze with pdf-parser.py