Scanners and rootkits

Part I

Your task is to run OpenVAS to analyze two of your computers (virtual machines). Analyze one windows machine and one linux. I have installed OpenVAS for you on a clonable image called 'bigparrot'. Begin by cloning that machine. After you have booted and changed your network settings, you should be able to run the following: `gsad --http-only --listen=127.0.0.1 -p 9392`, `openvasmd`, `openvassd`. Then visit the webpage. The username is `admin`, password is `foo`.

Essentially to start a scan you should add the host that you want to scan on the host screen and then add a task (a new scan) on the tasks screen. Then you hit the green start button to start the task.

Notes: On the machine that you are scanning you might want to install a few things to see if your vulnerability scanner can pick those up. Here are some recommentations (you can install whatever you want):

- Apache
- proftpd
- ssh
- telnet

To pass this off, prove to me that you were able to run a scan. Take a print screen and attach a copy of your report (put both at the end of your pdf document). At the beginning of your document, you MUST describe/summarize the results of your scan in paragraph form. What did you learn? What vulnerabilities does the machine you scanned have? You might also comment on how you could fix those vulnerabilities.

Here is an example of my report.

Part II

Follow the instructions here