The Windows XP VM was changed in the following ways:

- 2 hidden services were running (HackerDefender100 , HackerDefenderDrv100)
- UDP port 4500 was a “hidden” port
- 2 hidden drivers were loaded (msdirectx & mmpc)
- Process hxdef100.exe was a hidden process
- HackerDefenderDrv100 made a number of registry changes
- HackerDefender100 made a number of registry changes
- C:\hxdef100r was a hidden directory and all files and subdirectories were hidden
- C:\WINDOWS\system32\drivers\fu.exe was a hidden file
- C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\hxdef_private_version[1].png was a hidden file

The tool I used to garner these conclusion was Trend Micro’s RootkitBuster (http://esupport.trendmicro.com/3/Using-the-Trend-Micro-RootkitBuster.aspx). I first tried the tool on a machine which I assumed was not infected to establish a baseline and to familiarize myself with RootkitBuster. The areas of the host system that the tool could scan were the following:

Files and MBR
Registry entries
Processes
Drivers
File streams
Ports
Operating system service hooks
Kernel code patch
Services

I executed each of these scans sequentially and three of the scanning areas reported vulnerabilities on the clean machine: File Streams, Operating system service hooks and Kernel code patch. Although I would need to run the tool on more machines to be sure I imagine that the vulnerabilities that it detected were valid changes that security patching or other applications make to the OS. One example of a change that seemed legitimate was in the Operating system service hooks scan showing which reported discrepancies between the original and current IDT handlers. When ran on the clean machine the original and current handler were in a similar address space (ex. 0x80xxxxxx and 0x8axxxxxx) when the scan was ran later on the infected PC the address space for the original was the same 0x80xxxxxx but the current was 0xf4xxxxxx).

When I ran the tool in the infected VM it reported many more vulnerabilities that the scan on the clean system (see above) The tool provides an option to remove malicious files that it found but you need to reboot the system to see if it actually worked. Because you indicated in your instructions that the system can only be rebooted if absolutely necessary I assumed that rebooting the system would clear off the POC rootkits. When I did reboot to verify that the rootkits would not persist, I was somewhat surprised to see that the same vulnerabilities were detected by Rootkitdetector but it also detected an additional hidden files/services (vanquish.exe & vanquish.dll) which also made registry changes.

Although I am not certain I imagine that Rootkitdetector determines certain vulnerabilities by validating the IDT, GDT and system call table with a loadable module. Since there are many system calls that deal with running processes it could try each of the available calls to see if hidden processes are detected.