Rootkit Submission
Instructor: Xeno Kovah
Submission: April 3, 2011

The following is an assessment of what I found:

- I never had to enter a password in order to launch the VM fyi and I did not do anything special to circumvent the authentication
- I use a Microsoft Application called "*autoruns" to determine following:*
- Even though in MyComputer the filesystem reads NTFS during the logon there is a FAT initialization file that runs immediately during boot. If FAT is usurping NTFS by definition there is no file security and here is how:
- An executable fu.exe has the ability to inject .dll at runtime into current process stack among many other exploits. See http://www.prevx.com/filenames/X24965474357862442-X1/FU.EXE.html
- The next thing is that there is an executable named vanquish.exe http://wngz3r0.info/2006/09/vanquish/ that has ability to hide processes running from Task Manager as well as hide folders and files from being visible despite the settings in view under explorer for it to show all hidden files.
- Essentially these two tools will prevent utilities such as MRU, Zone Alarm, Task Manager, etc. from conventionally detecting processes rendering the tools useless.
- There are probably a myriad of other exploits running on this system but I did not want to clean the registry, reboot the system as you instructed to unveil what else might be running on the system

So my main question is how were you able to get the applications to infect the computer when you were not running as Administrator? I am assuming you did not install thee rootkits as an Admin. So here is what I surmised:

- You did not need to run these applications as admin because the injection takes place at boot time right into code running on the stack. The memory in stack and heap are not protected i.e. virtual memory included I assume so the stack pointer just executes the next instructions as it is suppose to. Windows operating system prevents files from being overwritten due to NTFS assuming NTFS is running and installed in the first place but it does not protect the instructions that are in memory being executed at runtime.
- To repair this I would both go through by hand and purge the registry of Vanquish and other utilities use to cloak or hide executables. If I could not do that I would just create another server profile, which generates a new registry by default but I would then need to reinstall all applications that modified the system registry. Once all files are visable I can then boot from a bootable CD and run an anti-malware and virus program to clean as much as possible off the disk. For files that persist such as an infected master boot

record or programs that run at boot time via startup folder, etc. you can use a program like autoruns or some industrial tool to clean those applications so that they do not persist upon power cycling and resets.

The bottom line is I do not see how you cannot resolve this problem without a soft reset of some kind to purge the current stack. The server in my opinion would have to go down at least once or more to execute this mitigation, UNLESS you can use the same applications like fu.exe to insert the “clean” .dll back onto the stack without power cycling. I guess that is an option as well but if I were the administrator I would do the former and not the latter for C.Y.A. alone.

Lastly the network did not run out of the box as well despite that DHCP server was running properly in VMWare and the ipconfig settings looked somewhat legit. I could have manually configured the network settings to test this again but I was afraid of this exercise getting out into the “wild” either by my own ignorance or someone else’s if I were to open Pandora’s Box so-to-speak.