RootKit Class Homework Write-Up

Below summarizes my activities for this exercise.

VMware Server Set-up

- Both my work (MITRE) and home notebook computers have Windows 7 Operating System. I tried installing the VMware Server 1.0.10 on both machines but ran into “unsigned driver” pop-up messages during installation and the VMware Server did not correctly run on Windows 7. Basically, I could not get it to connect to the host (local machine).

- Instead, I installed VMware Server 2.0 (Web browser) version on my home notebook and did the exercise on this setting (Windows 7 + VMware Server 2.0)

Observation of the VM Snapshot (After resuming the VM) + What I tried

- I managed to get to the VM (hostname: tehroot). I noticed an opened notepad file which contained the text of “red rum red rum”.

- I viewed Trusteer Rapport. It showed 90 trusted websites (mostly bank sites). It also blocked 18 instances of process alteration events.

- At my first run, Wireshark Netwok Analyzer did not seem to be running correctly as it opened "file open" pop-up window on every command/menu. It was not capturing any packets. The software itself seemed to stop working.

- I closed the Wireshark Network Analyzer and ran the Wireshark again and it ran. The system had IP address of 192.168.80.129 (I did IPCONFIG from command window) and it was getting packets for IP/UDP/IGMP/SSDP, from the address of 192.168.80.1.

- Recycle Bin had a folder called "temp" with a size of 9.8 mb. It did not contain any file (in the folder, "temp") - at least in the recycle bin. I restored it to its original C:\temp and it had an exe file (security update IE 8 - KB982381), timed at 03/13, 5:24:10 pm.

- I searched the MS Event Viewer (in application and system area) for errors. Application viewer showed some errors and System viewer listed a lot more errors on 03/13… the first two system error included: "Your computer has lost the lease to its IP address….” (DHCP error 1000), and "The system detected an address conflict for IP address…" (TCPIP error 4199).

- Above was followed with multiple instances of:
  "A device attached to the system is not functioning"
  "Cannot find path specified"
  "Media is write-protected".

- The DHCP error (1000) had happened many times before 03/13 but on 03/11 it had DHCP error (1002) - the DHCP lease has been denied (slightly different from DHCP error 1000) and on 03/13, the system had the first TCPIP error (4199).

- On 03/13/2011 (2:36:13 pm) - Following error (Event ID 1) happened: "The System Restore filter encountered unexpected error while processing the file '_filelst.cfg' on the volume HarddiskVolume 1. It has stopped monitoring the volume. This seems to tell that a system restore was attempted but did not succeed.

Second Observation/Run

- I removed the main VM files from the C:\Virtual Machines directory (from the first run) and copied the originally downloaded VM files again, to run the second observation.

- In the second run, when I tried running the Wireshark, it got a run time error.

Interim conclusion/Next Steps

- I sense that there has been an incident on this VM around 03/11 ~ 03/13 time period… I have not found what happened or what was altered on the system yet but I plan to give continuous try.