Exploratory testing

Once scripted tests were performed, it was time for exploratory testing. We used a method called Session-Based Test Management, which is exploratory testing executed in time-boxes or periods of roughly 90 minutes called “sessions” where each session is guided by a charter, or mission statement.

Test Lead John Bee suggested (and Rob Sabourin approved) 11 charters of exploration, which are as follows:

1) Take an XP and a Win2K config and run SecNet anti-virus and anti-spyware preference updates when using different user privileges. Pick one of each OS and log in to each as admin-level and user-level on each and see what you can find when updating preferences and logging into the other user. The intent here is to find a problem where SecNet tells the user they are protected with the latest definitions, but the definitions have not been implemented. For this test, you may have to email Frank to see if he has a virus for us to test with to ensure the definitions really are working to protect the PC when and if that virus is launched.

2) Take a config that has Norton AV installed and try a virus scan and definition update while SecNet runs. Also try some freeware anti-virus apps and see how SecNet reacts. Installation warns the user to uninstall their AV apps, but what if they don't?

3) Uploading / downloading / server -- In this session, you'll use two test machines, both running SecNet. Pick one config that is slated with the "server" category and another slated with the "download" category. Use the "download" machine to upload and download files from the server share. From the server machine, try to download a file from the other "download" machine. Take note of what SecNet reports (if anything).

4) Security: install a few free spyware apps from www.download.com and see if SecNet detects them.

5) Take a config that has ZoneAlarm installed (firewall software) and see how SecNet interacts. Which app will take control? Go to a port scanning site (like ShieldsUp! -- Steve Gibson's www.grc.com -- also http://grc.com/x/ne.dll?rh1dkyd2)

6) Take two machines, install SecNet on both, try to chat from one to the other using different chat apps

7) Install / Uninstall -- use Inctrl (located up on \\gasworks\share\utils) to take a snapshot of a typical SecNet install. Take a similar snapshot of an uninstall and see what's being left behind on the machine and in the registry.

8) Explore SecNet's interaction with Windows Updates on several of the 13 configs that call for it. How is it affected by new files being installed or the ensuing restart?

9) What are the risks of interacting with streaming multimedia from the web -- test configs that have RealOne, Winmedia, MM Jukebox, and Kazaa to see what problems SecNet might have.

10) On 4 or 5 of the top 10 configurations, take 20 minutes on each to Explore Form Filler, Parental Control, and Anti-Virus.

11) UI: pick config #1 or #2 and explore as much of the UI as possible that hasn't already been covered by the scripted tests.