Siddhant Shah
COMS 4187

Written Portion

1.
a. The abnormal addresses in the memory map indicate that the functions were changed and used a different amount of memory, forcing them to be allocated somewhere else in the executable when patched.

b. The Sony DRM was indeed using system resources while the player was not running, evidenced by the process continuing to use CPU even after the CD player was closed. The article notes that by using Filemon and Regmon, it could be determined that the DRM was inspecting all the CPU processes.

c. Doing so caused the CD drive to be unrecognized. The drivers no longer worked.

d. Hackers can utilize the functionality of the rootkit that is already installed on your computer, by adding files that fit the hidden specification. Having it such that it remains hidden to the user leaves them little recourse against such attacks.

2.

Morris's intent with the Morris worm was to have it span the internet and gauge its size.

3.
a. "Content Settings" → "Cookies" → "See all cookies and site data" → Select a cookie → Examine Content field

b. From the initial settings page, have Cookies directly listed under Privacy and Data. A new page, and a button for show all cookies. The data from the cookies is parsed into a table so that all cookie Content can be seen on a single page. Finally, on the same page, some interface tools to manage the cookies, and some button to delete all cookies.

c. The handlers option allows websites to send a pop-up that asks to become the default service when you invoke something. These invocations may happen when you agree to schedule something, or when you click a link to email someone.

An example would be having an email account on hotmail.com. Whenever you click an email link, if you have hotmail set as your protocol handler, it will open the draft for you on hotmail.com. However, if the option is disabled, then there may have been no pop-up from hotmail.com that asked to be your protocol handler. In that case, it'll open up your default email handler.

You should have this enabled because some websites may have custom protocols that enable their services. If you don't allow them to ask, then you can't use their services effectively.