CIS2376 PRACTICAL ANSWERS

Week 21

Answers

1.

i) We are told that *koobface* can survive reboots of an infected machine. Use Derrick Farmer's *A Windows Registry Quick Reference* and look at the auto-run registry keys with Volatility.

ii) Use Derrick Farmer's *A Windows Registry Quick Reference* and look at the MRU registry keys with Volatility. These keys will hold information about documents that have ben recently opened and executed.

2.

a. Use Derrick Farmer's *A Windows Registry Quick Reference* and look at the auto-run registry keys with Volatility.

b. Use Derrick Farmer's *A Windows Registry Quick Reference* and look at the auto-run registry keys with Volatility.

c. Infected software can arrive at a machine via:

- CD/DVDs
- USB flash pens
- the network

So, by examining registry keys associated with the above, we can determine when and if media was inserted into the machine (e.g. via CD/DVDs or USB pens).

Also, by examining MRUs, we might be able to locate network locations that have been recently visited and (potentially trojaned) documents that have been opened.

Again, look at Derrick Farmer's *A Windows Registry Quick Reference* in order to determine suitable registry keys for the above,