A number of recent (and some older) attacks have been described on the class blog. These include:

- The Java exploit CVE 2012-0507
- The new Metasploit module for CVE 2008-0610
- The use of ettercap for ARP poisoning
- The critical flaw MS12-020
- The use of Windows Credential Editor for pass-the-hash attacks
- The Adobe Flash Player flaw CVE 2012-0754
- The Firefox reduceRight flaw CVE 2011-2371
- The sudo format string vulnerability CVE 2012-0809
- The use of mimikatz to recover cleartext passwords from logged on Windows systems.

Select one of these topics. For your topic:

- Describe the flaw or tool.
- Provide a demonstration of how it can be exploited. Be sure to include screenshots or other evidence of success.
- Describe the traces left by the attack in the system logs.
- Describe how the attack might be detected by an intrusion detection system.
- If it is a flaw, describe how the flaw could be mitigated without patching and describe the patch (if any) that prevents the problem.
- If it is a tool, describe what settings should be modified or changed to mitigate or prevent the attack.

Successful use of the attack method in the exercise on April 9 & 11 counts as a successful demonstration and is encouraged (but not required).

Your write-up must do more than simply repeat the material contained in the sites listed on the class blog.