Draft final projects

Aase – Demonstrate steganography in the audible ranges by implementing it and then playing several audio files for the class with different amounts of information hidden in the audible ranges.

Abbina – Demonstrate a distributed port scan on many virtual machines on shasta. I'm particularly interested in how a typical distributed port scanning tool divides up the work and exchanges information among distributed nodes.

Alexander – Demonstrate the Lamer Exterminator virus on the Amiga 500 and give a security assessment of its cryptography (is it susceptible to linear cryptanalysis, for example?). You'll need to understand its code pretty well to describe the crypto, if it hasn't been published previously, which means disassembling the virus.

   Contingency: If, for some reason, Lamer Exterminator can't run on the hardware we have (the Amiga 500) it's okay to demonstrate it in an emulator.

Alvarez Bailleres – Demonstrate Bell-LaPadula with SE Linux in a Linux virtual machine. You should be able to show example access attempts being granted or denied based on the structure of a non-trivial lattice.

Cowdrey – Perform a basic forensic analysis of a hard drive image I have using BackTrack Linux. The Grayhat book has a bit of info on BackTrack Linux, and my grad student, Bilal, said he'd be happy to get you started and help you out. We'd like to know how it got infected in the first place and what kinds of hacking tools and Trojans the attacker placed there.

Danielson and Lott – Make an honest effort to use covert flow trees for finding new forms of idle scan and report on how well covert flow trees work for this purpose. Demonstrate some idle scans (either new ones or new ways of applying known ones) on a real network.

Jasthi – Demonstrate Bell-LaPadula with MACs in a FreeBSD virtual machine. You should be able to show example access attempts being granted or denied based on the structure of a non-trivial lattice.

Joginapally – Demonstrate a dictionary attack on a real /etc/passwd or /etc/shadow file. You should design an experiment where you put some number of passwords in and then see if each password gets cracked and how much time it takes.

Knockel – If TOMSkype looks fruitful in terms of getting the right version and finding something in the code, then do an analysis of TOMSkype to find out what the censored words were. If this is not feasible because you can't get the right version or the censorship seems to occur on the network, then
instead apply fuzz testing and/or static analysis tools to web-based software and see if you can find any vulnerabilities.

Levy – Demonstrate the Elk Cloner virus on real hardware, and then also demonstrate your own virus that has some kind of improvement over Elk Cloner:

   Contingency: If Elk Cloner cannot run on the hardware we have for some reason, it's okay to demonstrate it in a virtual machine.

Maine – Sign up for webmail accounts with Gmail, Hotmail, and Yahoo! Mail and then see if you can do a man-in-the-middle attack on any of them, e.g., by blocking HTTPS. Report on your findings, even if you find that man-in-the-middle attacks are difficult to do that will be interesting. Then give a live demonstration of a man-in-the-middle attack.

Xu – Demonstrate the SCA virus for the Amiga and explain how it does graphics (i.e., exactly what interface it uses). You'll need to disassemble the virus and get into its technical details by analyzing it.

   Contingency: If, for some reason, SCA can't run on the hardware we have (the Amiga 500) it's okay to demonstrate it in an emulator. Also, any virus that uses graphics will be interesting if SCA in particular doesn't work.