

**Graduate Project #1  
CS 436  
Spring 2007  
Gary Warner**

**For this project, the student will choose an operating system, either Unix/Linux (any flavor) or Windows (2000 or XP or Vista).**

**With regard to all the questions below, please assume that you have been asked to design the most secure configuration possible for a public work environment. (For instance, a computer lab in a public library.) Due to budgetary constraints, you may only use the security features built into the operating system itself. Although you are aware of many “free” programs which might be helpful, your administration does not allow you to install open source software. So, limit the scope of all of your answers to options that are available as part of the installation of your chosen Operating System.**

**Assume that each user will have a unique userid, and will “own” files in their own home directory on the system, which other users should not be able to access. Users will be able to surf the web, send and receive email, and use Word Processing software on this computer.**

**To simplify the scope, please assume that all userids are created locally on each machine. We will temporarily skip “Domains” and “rlogin” type system-sharing.**

**For the chosen operating system, please provide as much detail as possible about the security features present, or not present, in the operating system, in each of the following areas:**

**Explain how your OS differentiates between Principals, Subjects, and Objects**

**For Unix:**

**Explain UID and GID values and their meanings**

**For Windows:**

**Explain SIDs**

**Explain where passwords are stored (by default, and how to secure), and how users change their passwords. Are there any default passwords on your OS? How would you set password length and format rules on your OS?**

**Explain Access rules (file permissions) in your OS?**

**Explain the difference between system-privileged accounts and user-privilege accounts in your environment.**

**Explain how Controlled Invocation is handled on your system. (User processes calling System processes). (Hint: SUID on Unix – “Gateways” on Windows). How may hackers take advantage of this privilege change feature?**

**For Unix: explain “single-user mode” and kernel modification  
For Windows: explain the difference between “kernel mode” and “user mode”**

**How does your Operating System choose what system processes are invoked at boot-time? What changes would you make to the default start-up to better protect your system?**

**Explain how Process IDs function, and the use of “real” and “effective” UID and GID for processes.**

**Explain how permissions to objects are changed. What file permissions are available on your operating system? How might a user grant permission to an object for which he is the “owner” to another user? How are permissions for groups handled on your operating system?**

**Does the concept of “inheritance” apply to file permissions on your system? (Do files assume the permission of the directory in which they are located?)**

**Explain how files are deleted, and whether there are “residue” risks to this approach.**

**Explain what network or system services are enabled by default. How would you configure this Operating System to reduce risk. (Assume this machine will be a “general user” machine, shared by multiple users. Not a “server”.)**

**Explain what “Audit logging” is available on your system. Explain what audit settings you would recommend to protect your system, and why you would recommend them.**

**How are patches or updates made available to your system? Explain how you would ensure that appropriate patches are applied to this system.**

**Are there key commands or files which you would prevent general users from being able to use in a high-security environment?**

**Users will need to have the ability to write files to a floppy disk or USB drive. Does this present any security concerns on your system?**

**Your replies to these questions should be given in order, in the form of a paper.**

**(NOT Q1 – Answer 1**

**Q2 – Answer 2**

**So, an answer may be given in paragraph form, embedding the question into the answer. In some cases many paragraphs may be required for a single answer.**

**For instance:**

**On the Unix operating system, there are several network services which are enabled by default, including “telnetd”, “ftpd”, . . . . . It is recommended that the following services be removed from startup by using the following method . . . .**

**The paper may be any length which is sufficient to explain the answers requested thoroughly, but I would anticipate papers of 15-25 pages in length.**

**At least four reference documents, including your text book, should be listed in a bibliography at the end of your document. You should consider visiting a library as well as using documents on the Internet as part of your research.**