

# CS392/681 Lab 8

## Linux Security and Windows Security

### Due 12/10/2003

#### Introduction:

Setting up and maintaining the security system in a computer is as important as the security system itself. A system could be compromised if the security aspects of the system were configured correctly.

#### Requirements:

Read the following technical documents:

For Parts I and II

- <http://www.nsa.gov/snac/win2k/guides/w2k-7.pdf>
- <http://www.nsa.gov/snac/win2k/guides/w2k-8.pdf>
- <http://www.nsa.gov/snac/win2k/guides/w2k-2.pdf>
- <http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf>

For Part III

- <http://www.linuxsa.org.au/tips/file-permissions.html>
- <http://www.tldp.org/HOWTO/Security-HOWTO/>
- <http://dan.drydog.com/cops/documentation/farmer-spaff-cops.html>

#### Your Task:

##### **Part I: (Windows)**

Follow the guideline presented in the technical documents and find the security flaws and all possible entry points for hackers in the win2k server assigned to you. List these flaws you found and how to fix them.

Write a 3-page report on all bugs you found and how you fixed them.

##### **Part II: (Windows)**

Understand how win2k's security subsystems work from the below links and state what are difference between win2k and NT security architecture (2 page report)

- [http://www.chi-publishing.com/portal/backissues/pdfs/ISB\\_2000/ISB0506/ISB0506JJ.pdf](http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2000/ISB0506/ISB0506JJ.pdf)
- [http://www.chi-publishing.com/portal/backissues/pdfs/ISB\\_2000/ISB0507/ISB0507JJ.pdf](http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2000/ISB0507/ISB0507JJ.pdf)

##### **Part III: (Linux)**

###### **File Security**

Finding and fixing bad file permissions is one of the most important aspects of system security. Read about the following paper related to file permissions and local security

<http://www.linuxsa.org.au/tips/file-permissions.html>

<http://www.tldp.org/HOWTO/Security-HOWTO/> (Section 5).

Use the machine assigned to your group and try to find as many bugs related to file permissions and fix them.

###### **Password Security**

As a system administrator, it is your responsibility to make sure that other users on your machine have secure passwords. Try to crack the passwords of the users in your machine and make a report on your findings. Again read the document below for some hints on creating hard to crack passwords

<http://www.tldp.org/HOWTO/Security-HOWTO/> (Section 6)

As you can see in this part it is really easy to get the password file if you are logged on to the machine. Find a way to make this harder, that is the password file (/etc/passwd) or at least the passwords contained in it must not be readable by the users who login to the machine (shadow password file).

### **Internet security**

Even though you are only concerned with system security you still have to worry about connecting your Linux machine to the Internet. There are many ways one could gain access to your computer while connected to the Internet, you can protect your system by disabling vulnerable services. Read the section 8.2 on services and tcp\_wrappers and report on how secured your system is and solution for the problems you find.

### **Bug fixes and Patches**

Every day a new exploit is being discovered. As a system administrator it is your responsibility to check and patch any old software or service running in your machine. Check the following advisory

<http://www.linuxsecurity.com/advisories/redhat.html> and see if any patches available there could be used in your machine and add the patches you need to install. You must at least be able to find 5 patches appropriate for your system.

### **System Logs**

Even though one may think his/her system is completely secured, it is important to know who is doing what in your system. Read the section 9.4 and check your log files and report if you see something that is suspicious and not suppose to be that way.

### **COPS**

There are many tools available in the market to check your system and reports on the security bugs found in your system. One such software is called COPS (Computerized Oracle and Password System). Read this document describing COPS

<http://www.dan.drydog.com/cops/documentation/farmer-spaff-cops.html> and write a one-page report on how useful this tool can be for an administrator.

### **Tripwire**

Tripwire is another tool that comes handy for system administrators. A complete description of this tool is available at <http://www.tripwire.com/products/servers/>. Put your self in a position of and Administrator and study this tool and submit a one-page report on how useful this tool will be for you.

### **Hints:**

The most common services that need to be updated are ftp service (wu-ftpd), telnet, Kernel patches, and syslogd services.

### ***Post LAB report:***

Your report must include following:

#### **Part I**

3-page report on all bugs you found and how you fixed them.

#### **Part II**

2 page report.

#### **Part III**

One page summary for each section.

### ***Questions and Lab submission:***

Send to [lab8@cs392.biz](mailto:lab8@cs392.biz)