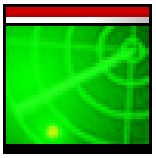
4.3.1

SECURITY VULNERABILITIES

(GFI LANGuard)



June 2008

Laboratory Overview

Objective

At the end of this lab students will be able to manage Windows updates, including service packs and hot fixes. Students will be able to scan network computers for vulnerabilities, and apply patches and fixes.

Information for Laboratory

A. Students will utilize Windows Update to check for up to date patches, hot fixes, and service packs
B. Students will utilize GFI Languard, a network security scanner to scan for vulnerabilities

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that each student computer have access to the Internet, Windows update, and GFI Languard should be installed and working on each student computer.

Estimated Completion Time

60 Minutes

Security Vulnerabilities

Security vulnerabilities have been found in major operating systems such as Windows 2003 Server, Windows XP, Vista, Unix, and Linux. For instance, a Windows computer on the Internet with certain vulnerabilities can be an open door to hackers and viruses. Depending on the vulnerabilities of the machine, a hacker or a virus could exploit those vulnerabilities, and thus, in certain cases, possibly execute code on the computer, or even lock or freeze up the targeted computer.

Basically, vulnerabilities are really nothing more than errors or "bad coding" in the software. When a vulnerability or error is found in software, fixes are made, and packaged as software updates.

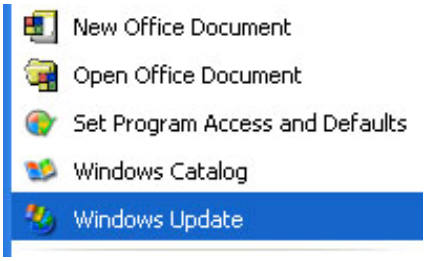
Microsoft has been known to have a lot of security related vulnerabilities in their Windows operating systems. Patches, or software updates are called Hot Fixes. Hot Fixes are packaged together every so often and called a Service Pack. All Windows computers should always have the latest up-to-date service packs and hot fixes installed. This helps prevent any security holes or vulnerabilities. Service packs and Hot fixes can be downloaded directly from Microsoft, and installed separately. Microsoft operating systems now come with what is called Windows Update Service. This service helps make sure that your computer has all the necessary fixes installed, and if not, it can download all of them together, and install them at the same time, making it easy to keep your computer up-to-date.

GFI Languard

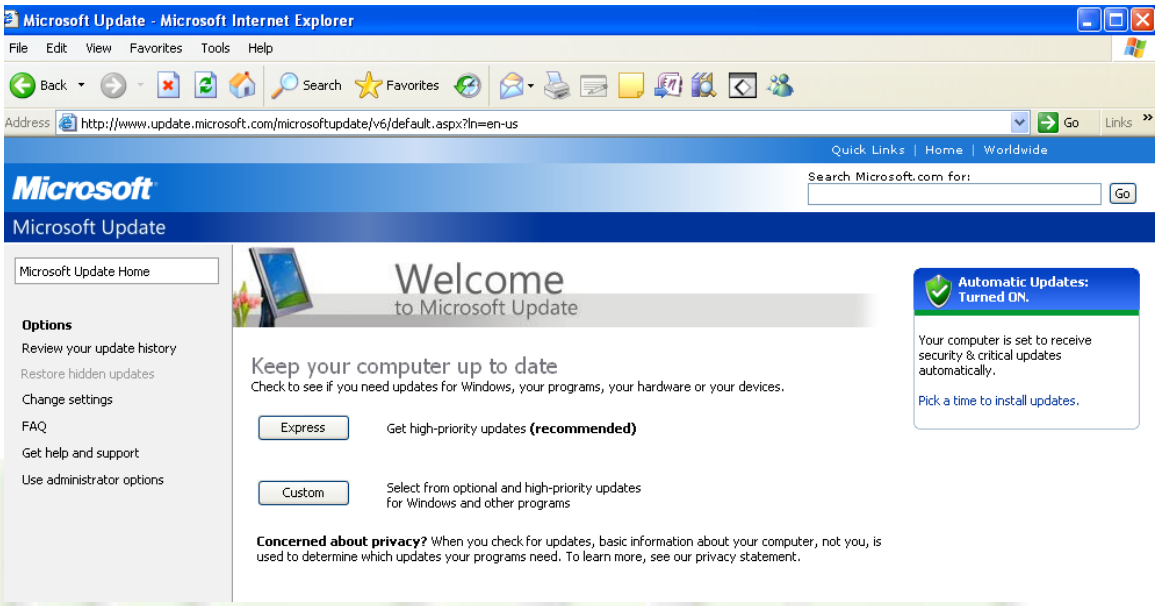
Languard is a network security/vulnerability scanner. From one computer, it can scan every computer on your network and check them for known vulnerabilities against a database that is always being updated. Since it is a commercially licensed product, we will be using the free 30-day demo available to download at www.gfi.com.

Step 1: Running Windows Update

Click Start, All Programs, and almost at the top of the program list, click Windows Update.

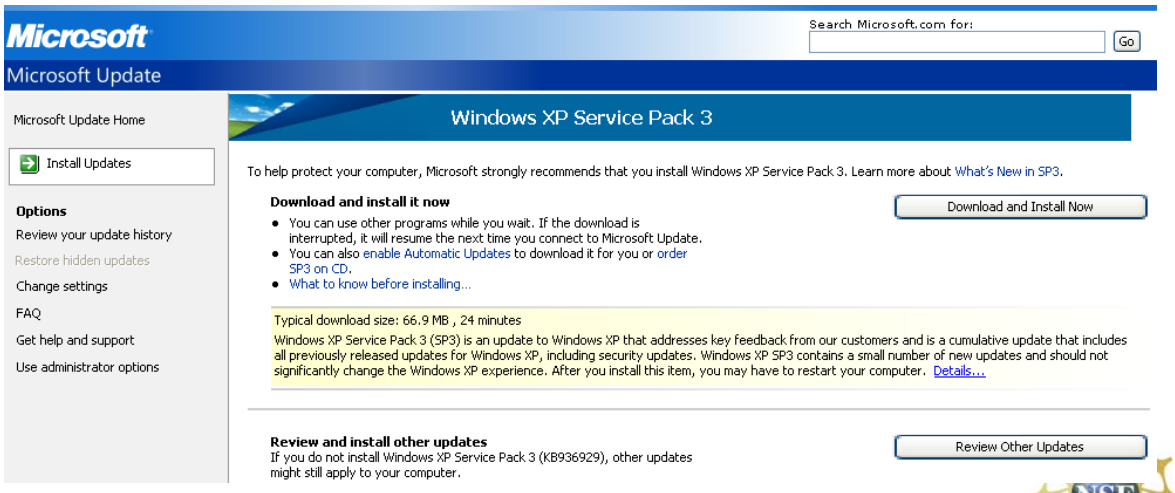


Windows Update will automatically launch Internet Explorer, and connect to the Microsoft update web page. You should see a screen similar to the one shown below

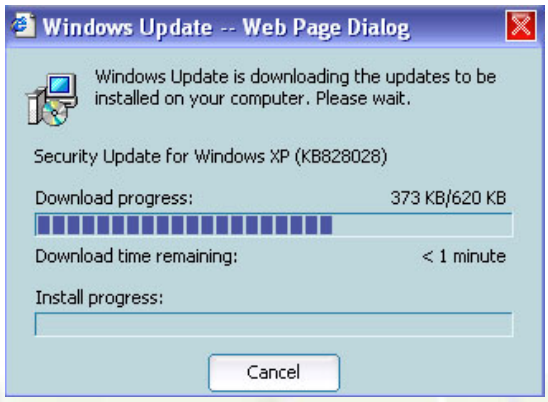


Step 2: Scanning for necessary updates

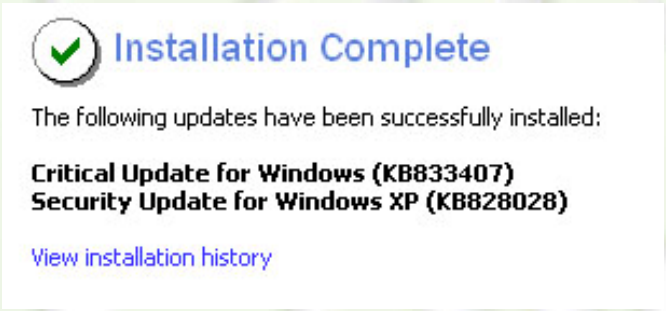
When Windows Update is open, click the Custom button for updates in the center.
Windows update will then scan the computer for installed updates, and prompt you to review and install updates, as below.



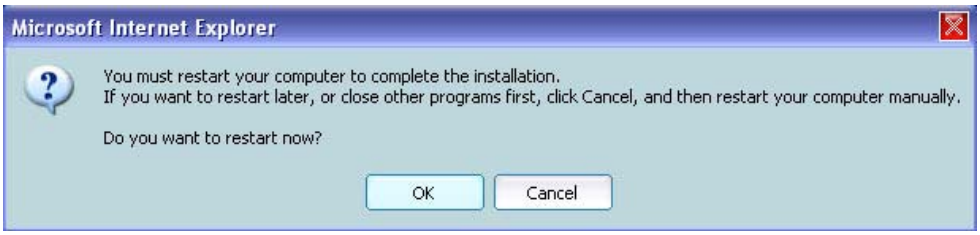
Depending upon your environment, results will vary so screen shot shown above may be different. Your instructor may or may not have you install updates. If you do install, Windows update will start the downloads, and install the updates



When done, Windows Update will show the installation history



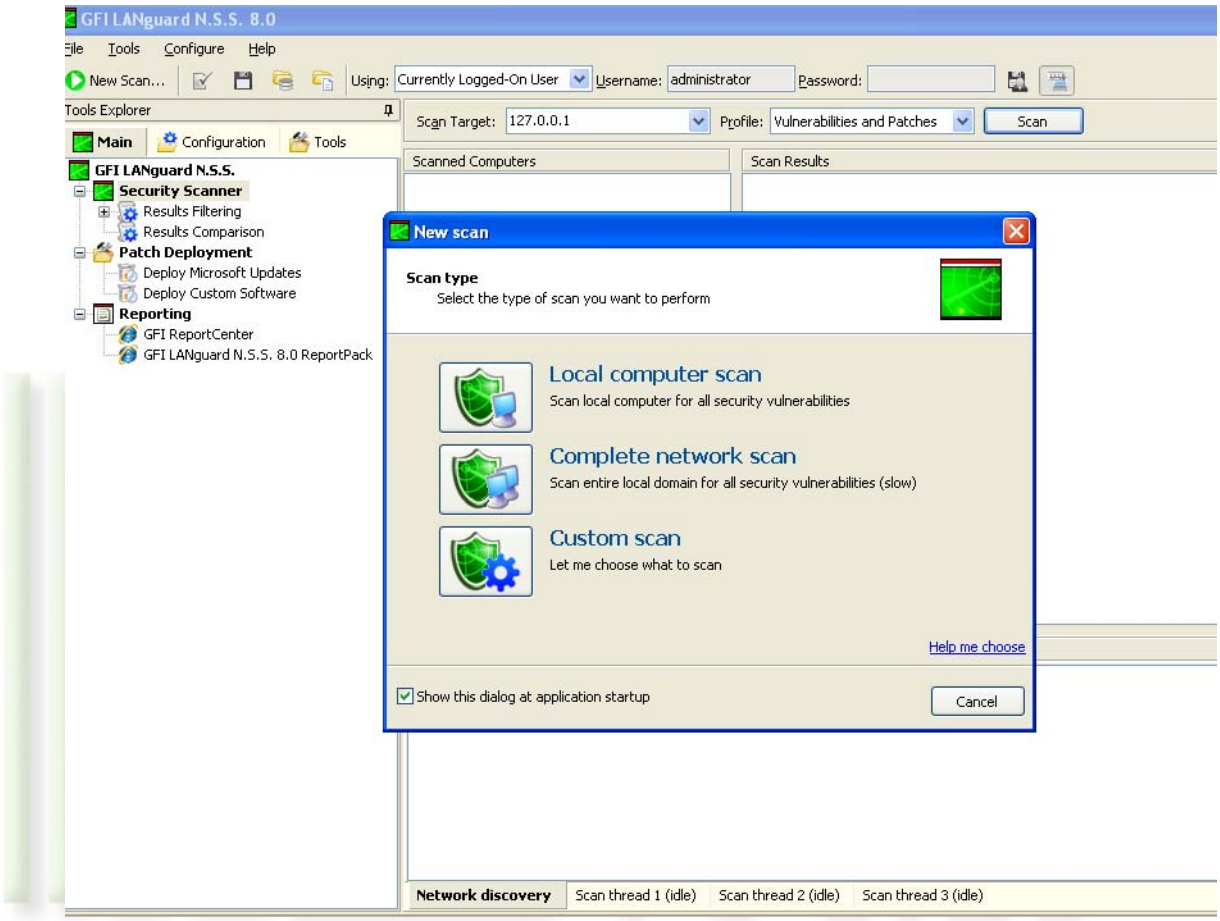
It may be necessary to restart the computer to complete the installation, if so, click OK.



When your computer comes back online, run windows update scan again, and make sure that there are no Critical Updates that need to be applied.

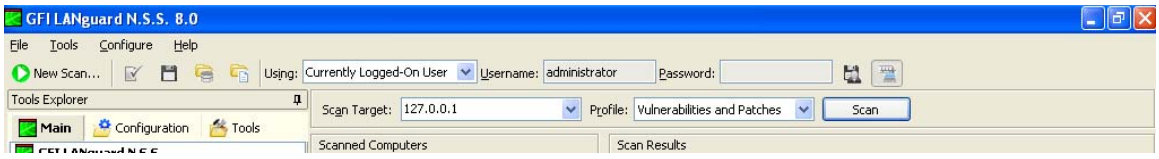
STEP 3: Running GFI Languard

From START, All Programs, GFI, Click Languard Network Security Scanner. You will see a screen similar to the one shown below:

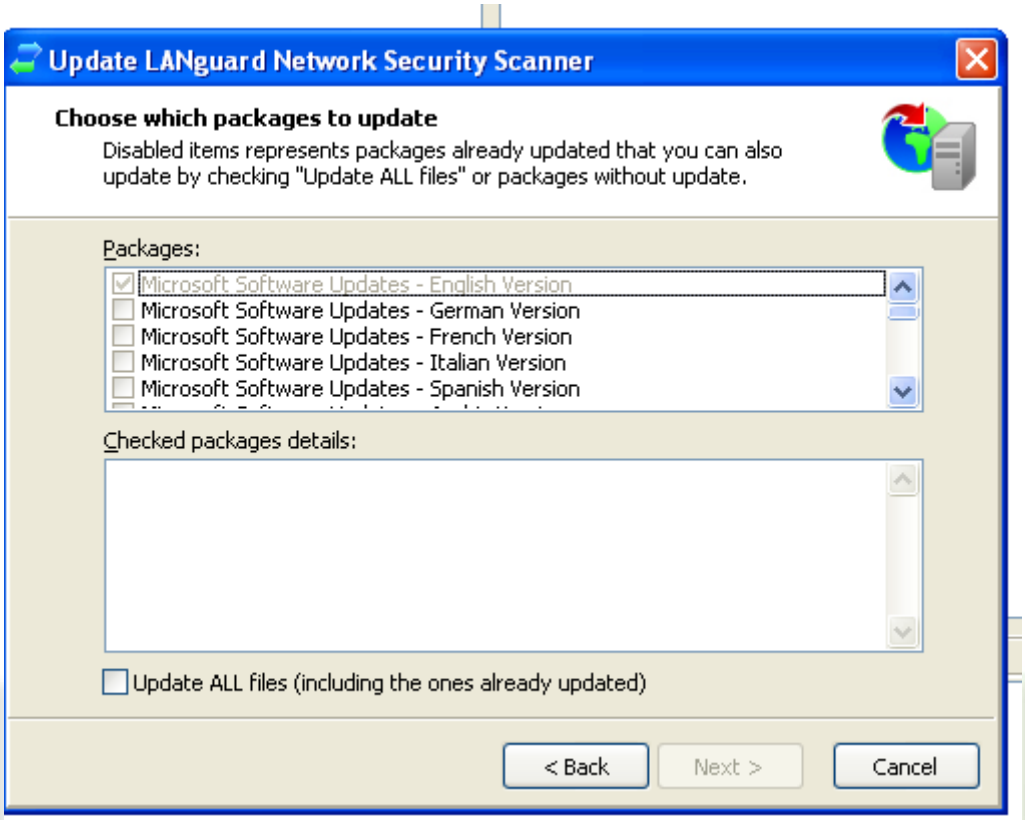


STEP 4: Update Languard database file. ONLY DO THIS WITH INSTRUCTOR APPROVAL.

Click on Help and Check for security updates



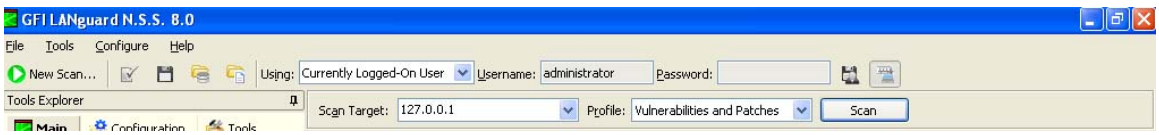
Click Next on the dialog box shown below and you will see the following screen



Languard will check the GFI website for any available updates Please NOTE! This may take quite a while to update. Be sure to check with instructor to see if you should do this.

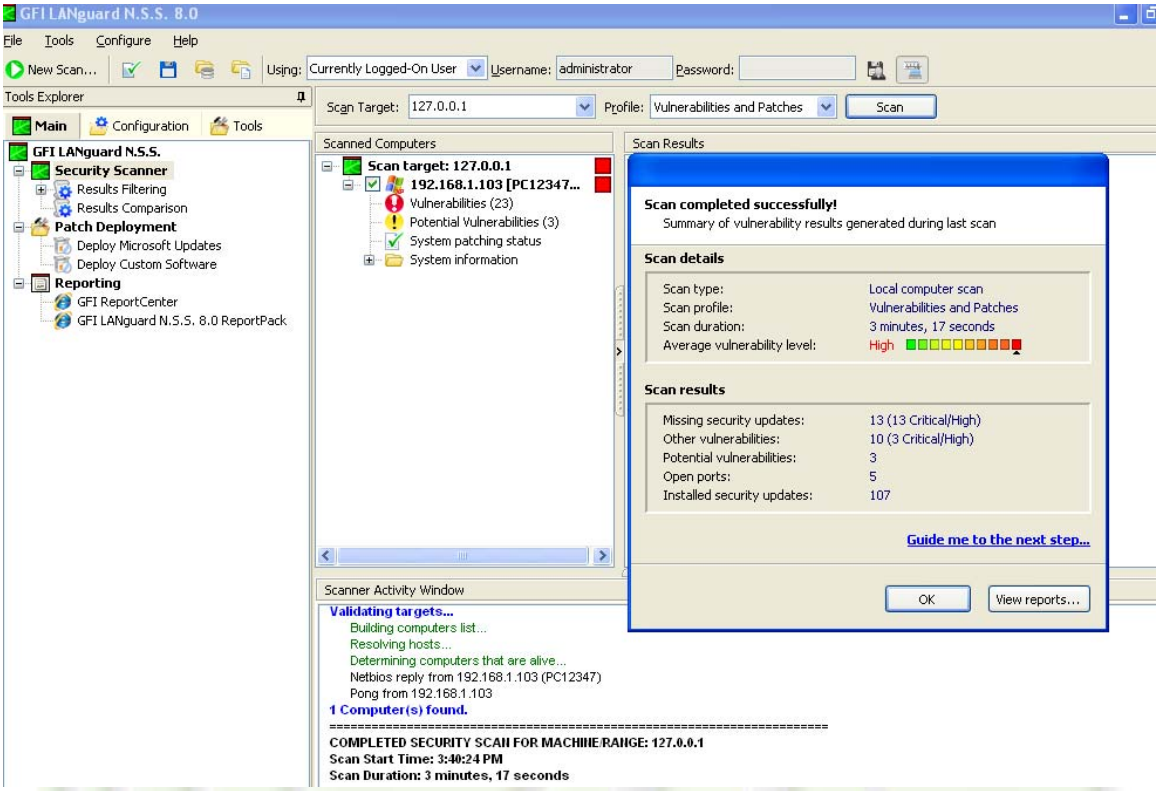
STEP 5: Scanning your local computer

We will use GFI Languard to scan your local computer. Click on the Scan button on top right-hand side of your screen .See screen shot below:



After clicking on Scan button, you will get a dialog box telling you about trial version. Click OK. It will then start to scan your computer. After completing the scan, it may look something like this. Note:

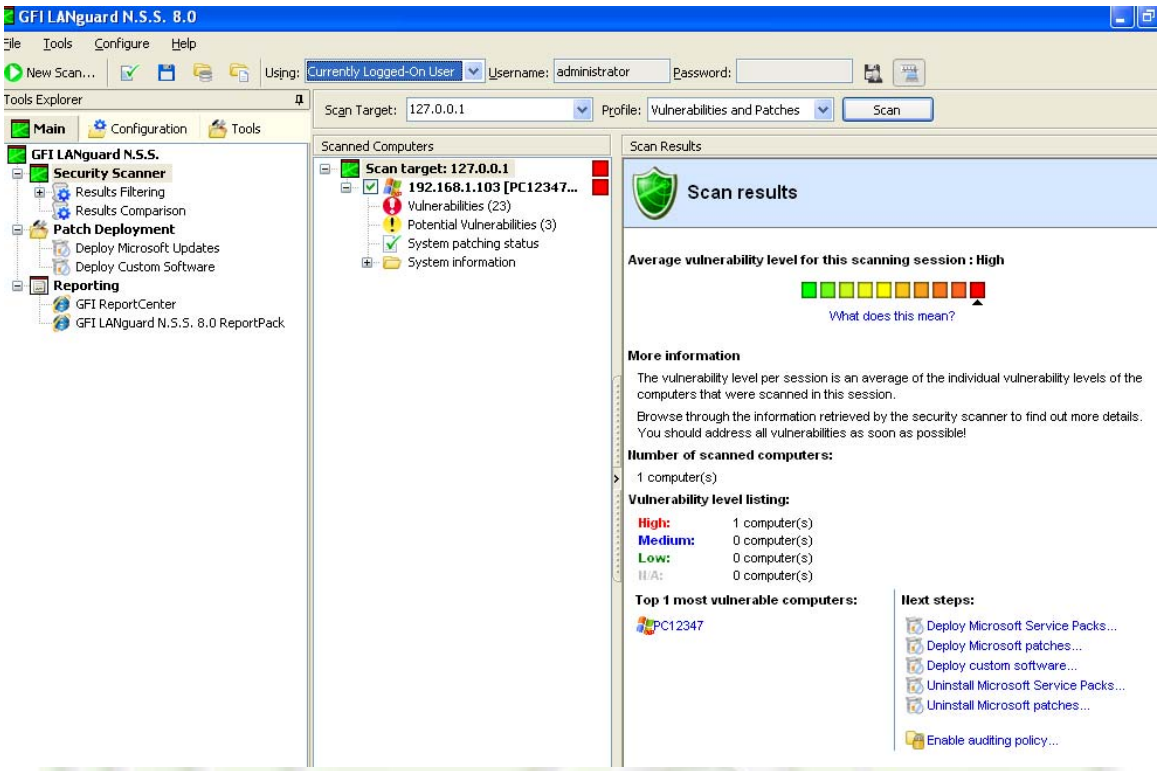
Results will vary greatly!



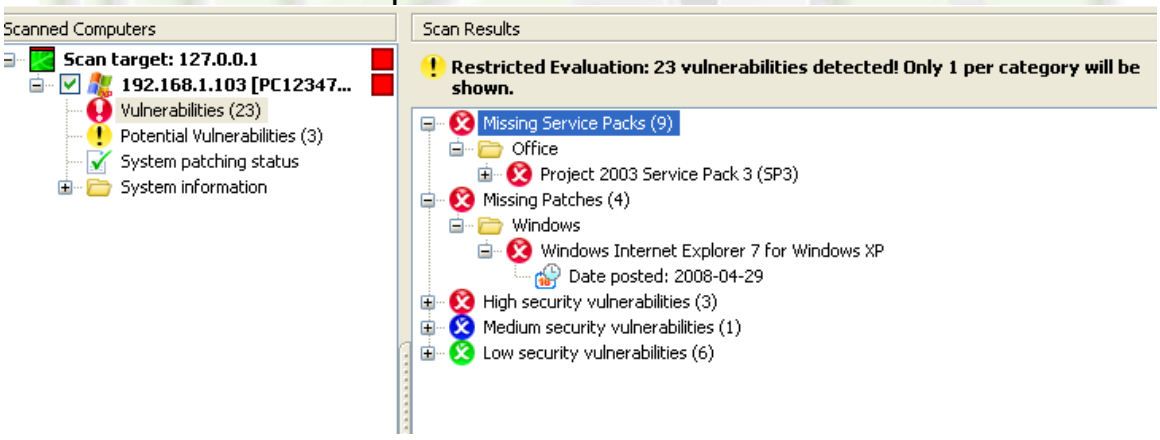
Languard will scan the local computer for any vulnerabilities that are in its database.

Step 6:
Click on the Guide me to the next step… link. It will bring you to the GFI Web site where it has instructions for the results shown on the Scan result screen.

Step 7
Click on the OK button and you will see a summary of the scan. A sample screen shot is shown below:



In the middle box, click on Vulnerabilities, or Potential Vulnerabilities and it will expand on right-hand side. For our example, I clicked on Vulnerabilities and sample screen shot is shown below

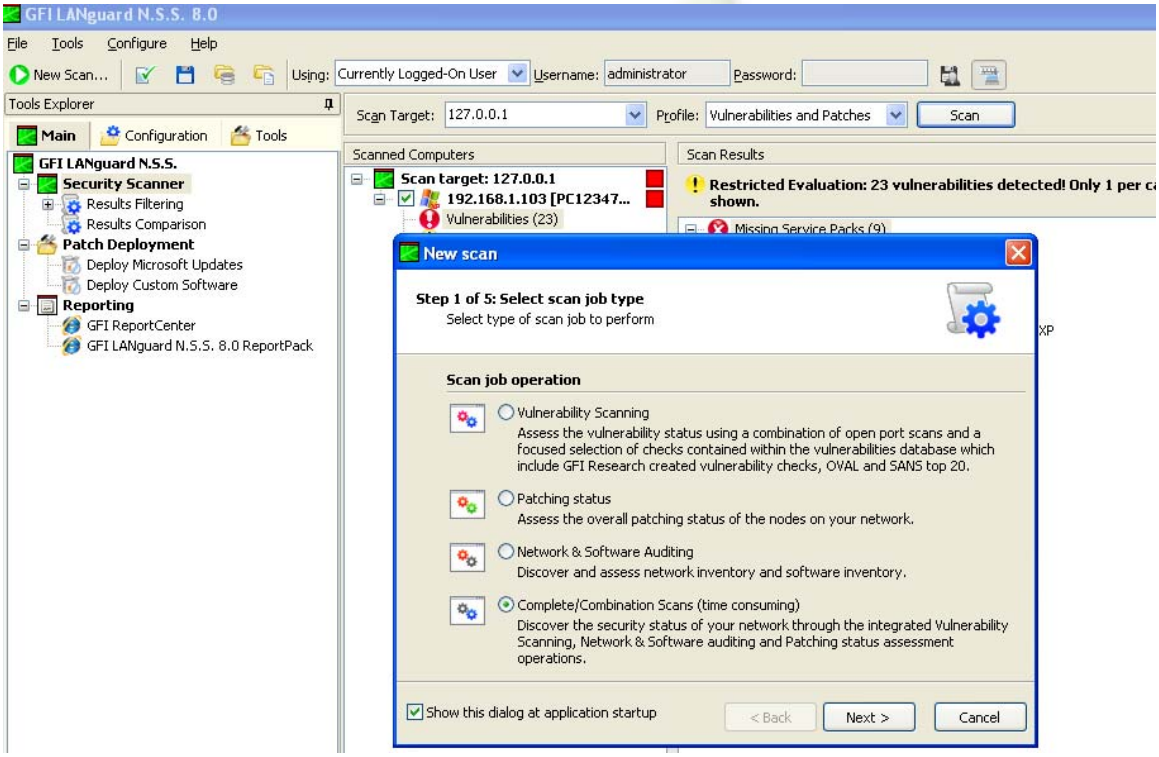


As you can see, it gives you great detail on what is missing and what to install. DO a printscreen of your computer and save to a MS Word file. Make sure you put your name within the document. Print off and give to instructor.

STEP 8: Network Scanning

LANguard has the ability to scan more than one IP address in a single scanning process. To scan your local network, Click on the New Scan… arrow New Scan…. You will see a new dialog box pop up . For Step 1, select Complete. For Step 2, Select Full, for Step 3, pick a range of computers within your network. For Step 4, select your IP Address Range and click the Add button. For Step 5, depending upon your environment, you can enter in Username/Password credentials for computers you wish to Scan.

Ex. 10.0.0.1-10.0.0.254 will scan the whole subnet
Ex. 10.0.0.1-10.0.0.10 will scan all computers .1 thru .10.



Step 9: Scanning a computer with a Firewall enabled

NOTE: You will need a partner to properly do step 9

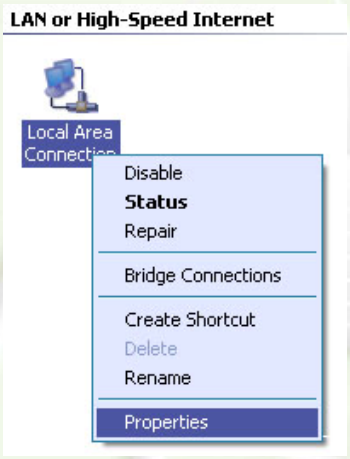
Partner A will enable the Firewall

Partner B will scan partner A's computer both with the firewall enabled and disabled.

Partner B: Just like step 5 from above, scan your partners computer. Instead of entering Localhost, you will enter the IP address of your partners computer. Note all the information that Languard is able to find.

Partner A: After your partner has first scanned your computer with no firewall, and noted the findings, now enable the firewall.

Close all open programs. From the desktop, Right click on My Network Places, and click properties. This will bring up the Network Connections box. From there, right click on Local Area Connection, and click properties as below.



From the Local Area Connection Properties box, Click the Advanced tab, located at the top right. Check the box to Protect my computer and network by limiting or preventing access to this computer from the Internet. By checking this box, you are enabling Windows XP Internet Connection Firewall.

Once checked, Click OK, and verify that the Firewall is enabled. The Local Area Connection icon should now have a gold icon of a lock in the top right corner, as below.

Partner B: Just as before, enter you partners IP address in the Target box, and attempt to scan the computer. If the Firewall is enabled and working properly, Languard should not return any information, and alert you The scanned computer is not responding. This is because the Firewall is blocking access to ICMP, SNMP, and all TCP/UDP ports. Click OK and Close Languard.

Partner A: From My Network Places, Local Area Connection, click on the advanced tab, and uncheck and disable the Internet Connection Firewall.

Analysis

1) Under what circumstances could you see using GFI Languard in a business setting? Explain your answer in detail

2) After working with these utilities, what about GFI Languard or

Windows Update do you feel you should study further? Why?

3) Why should you use Windows Update?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix:

This lab was developed using GFI LANGuard Version 8.0, which can be obtained from:

http://www.gfi.com

-or-

http://www.download.com

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).