UNIVERSITY OF BRIDGEPORT

Department Of Computer Science and Engineering

Final Project
MS Computer Engineering
(Cpe 597)

Issue's Related to Network Security

Submitted by
Tushar Gopani
St Id: - 565417

Submitted to
Prof Khaled Elleithy

TABLE OF CONTENT

ABSTRACT

As wireless technologies are becoming increasingly easier and cheaper to use, the frequency with which they are implemented in networks is also rising.

There are many issues related to wireless technology and its security that are affecting these networks. The security solutions available are not always implemented properly and/or users are simply unaware of the security risks involved.

In this project I will discuss about the wireless technologies available, equipments need to install, cost involved to create a small wireless network used in offices and home. Then I will be discussing various security issue related to the network, types of solutions available in market and cost effectiveness of the solution for our small network.

Then I will be using some tools available like GFI LANgaurd Network Security Scanner 6.0 to test our network and other network available on our campus. This tools are used to check whether wireless/LAN networks are vulnerable to attacks, are the network open to the public.

Finally a full report of the network will be generated and will be use to secure the network for the loop holes that can be easy attacked from the outside world, thus providing additional security to the network.

INTRODUCTION

Marketing trends estimate that by the end of 2006, 21 million homes will have implemented a Local Area Network (LAN), and of those 21 million homes 65% will use wireless solutions. The rapidly decreasing cost for wireless devices and the proliferation of wireless solutions provided by the major Internet Service Providers seem to clearly support these growth estimates.

Home wireless/LAN users and security professionals over the world are conceptually trying to solve similar problems. They both need to find a way to provide a secure working environment. There are two distinct approaches to this security dilemma, security prevention, and security detection. An example of security prevention would be a firewall device that restricts specific traffic or ports to or from specific hosts. Although this provides protection against unauthorized traffic, it has no means for determining if an attack is being attempted via an authorized port. An example of security detection would be an IDS (Intrusion Detection System) device that contains a signature to identify a specific attack via authorized or unauthorized ports. Security professionals often have the technology and resources to develop security solutions based on prevention, detection, or a combination of the two. However, home wireless/LAN users do not have the luxury of evaluating their security approach since the guidelines and wireless devices marketed to the home user demographic have an overwhelming dependency on preventative mechanisms.

Importance of Internal Network Security

Internal Network security is, more often than not, underestimated by its administrators. Very often, such security does not even exist, allowing one user to easily access another user's machine using well know exploits, trust relationships and default settings. Most of these attacks require little or no skill, putting the integrity of a network at stake.

Most employees do not need and should not have access to each other's machines, administrative functions, network devices and so on. However, because of the amount of flexibility needed for normal operation, internal networks cannot afford maximum security. On the other hand, with no security at all, internal users can be a major threat to many corporate internal networks.

A user within the company already has access to many internal resources and does not need to bypass firewalls or other security mechanisms which prevent non-trusted sources, such as Internet users, to access the internal network. Such internal users, equipped with hacking skills, can successfully penetrate and achieve remote administrative network rights while ensuring that their abuse is hard to identify or even detect.

Wireless Standards

This section will give a brief overview of some of the popular wireless standards being used. In this project we will be targeting 802.11 technology, but to get knowledge about different wireless standards I have included this topic.

802.11

802.11 is a standard from Institute of Electrical and Electronics Engineers that operates on radio frequency. The original standard specified bandwidth up to 2Mbps in 2.4 GHz spectrums. The spectrum is unlicensed and anyone can use it. The wireless technologies used in 802.11 are

- Frequency Hopping Spread Spectrum: Packets are sent across a range of frequencies.
- Direct Sequence Spread Spectrum: Signal is transmitted simultaneously over several frequencies.
- Infrared: Line of sight is required between transmitter and receiver.

802.11b

802.11b is an extension to the original 802.11 and it allows bandwidth up to 11Mbps in 2.4GHz spectrum. Unlike 802.11, 802.11b supports only Direct Sequence Spread Spectrum and is backwards compatible. Although the bandwidth is up to 11Mbps, the actual throughput is between 4 and 5Mbps. This too depends on environmental and operating conditions.

802.11b divides the RF spectrum into 14- 25MHz wide channels. However, in US 11- 83MHz wide channels are allowed. This means that only three channels can be used simultaneously (1, 6 and 11) without overlapping.

The standard defines Physical and Data Link layer corresponding to OSI reference model. At physical layer, 80211b extends 802.11 to support higher data rates by using Complimentary Code Keying (CCK) and Quadrature Phase Shift Keying (QPSK) modulation. The data link layer, which is called MAC layer,

specifies an interface between physical layer and the host device. It specifies Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as a mechanism to coordinate transmission. When a station is ready for transmission, it checks the media for signal. If no signal were detected, the station would wait for a random period of time and check the media again.

If there is still no transmission, station will start transmitting. Receiving stations send an acknowledgement upon receiving data. If collision is detected, all stations wait random amount of time before re-transmitting.

802.11b is by far the most common and that was the one we were interested in. Since 802.11g is backwards compatible with 802.11b it will more than likely become more commonly used but as of right now it's just starting to pick up.

802.11a

802.11a is another IEEE standard that supports up to 54Mbps of bandwidth in 5GHz spectrum. 802.11a uses a special type of frequency division multiplexing called orthogonal frequency division multiplexing. 802.11a is not backwards compatible with 802.11 or 802.11b. A significant difference between two standards is the coverage area.

802.11b compliant devices offer roughly double the range compared to the 802.11a compliant devices. This is because higher frequency signals have a lesser range than lower frequency signals (5Ghz vs. 2.4GHs)

Wi-Fi

Wi-Fi (Wireless Fidelity) is a not for profit group that certifies equipment from different manufacturers to be either 802.11a or 802.11b compliant.

802.11g

802.11g specify data rates as a high as 54Mbps using 2.4GHz frequency spectrum. Like 802.11a, it also used orthogonal frequency division multiplexing. Unlike 802.11b, this standard is backward compatible with 802.11b and 802.11 standards.

HiperLan/2

HiperLan/2 (High Performance Radio Local Area Network 2) is a standard from European Telecommunications Standardization Institute. It is similar to 802.11a in that it offers bandwidth up to 54 Mbps in 5GHz spectrum and use orthogonal frequency division multiplexing. The main difference between 802.11a and HiperLan/2 is the ability of HiperLan/2 to offer QoS because of its ability to establish connections between client and access point prior to transmission of data (and resulting in a connection-oriented transmission).

Bluetooth

Bluetooth is a personal area network standard for devices that exchange data in a short range (less than 10m). It operates in 2.4GHz spectrum and therefore may interfere with 802.11b devices. Bluetooth uses full duplex frequency hopping signal up to 1600hops/sec. This specification makes possible the connectivity between mobile phone, PDA, laptops and Internet.

IMPLEMENTATION

HARWARE TOOLS REQUIRED

Laptop (2)

P4 512 MB Ram 2.8Ghz

Belkin Wireless Internet Card

The Card works as an ideal standalone to give you instant networking capabilities. It features breakthrough 802.11g technology that makes wireless file transfers and downloads faster than ever before. 802.11g technology provides you with networking speeds nearly five times faster than the current Wi-Fi (802.11b) standard. The Card sets up with the ease and the simplicity of Plug-and-Play technology on any laptop equipped with a 32-bit CardBus slot. It slides into the 32-bit CardBus slot to enable a wireless connection to your network. 802.11g technology is the easiest wireless network to implement. The Card uses the wireless 802.11g 2.4GHz standard to offer you the widest working range - up to 1500 feet -and greater interoperability in mixed networking environments. 802.11g technology is backward-compatible with the 802.11b Wi-Fi networking

standard, so it allows you to implement faster wireless technologies in combination with existing 802.11b Wi-Fi networks.

- **Advantages:**

  1) Adds 802.11g wireless capabilities to laptop computers, for faster wireless networking available for home or office

  2) Fits any standard 32-bit CardBus slot

  3) Provides 3 times the wireless range of 802.11a clients

  4) Offers backward-compatibility with the 802.11b Wi-Fi networking standard

  5) Features wireless 64- and 128-bit WEP encryption

  6) Allows you to use Turbo Mode and network at 54Mbps, the highest data rate for all 802.11g clients

  7) Keeps notebook batteries running longer with advanced, low-power consumption chipset

Advantages:

1) Creates a network in your home or office without cables

2) Offers backward-compatibility with all 802.11b devices

3) Ensures data and network security with wireless 64- and 128-bit WEP encryption

CONFIGRATION AND IMPLEMENTATION

- **Architecture and implementation of wireless/LAN network for home or small office**

One of the key challenges with computer networks designed to communicate is that they communicate. When we simply "ping" another computer, it may create 6 messages: ARP (broadcast), DNS (unicast to DNS server), and (in Windows) 4 ICMP echo requests. It is important to know what our network is normally sending and when. This is the only way to properly manage systems traffic and to be able to detect abnormal traffic. A second fundamental group of ideas involves Threat, Vulnerability, and Countermeasure. The threat consists of all those nastiest that can attack the net - they belong to the enemy. We don't control the threats. We must know what they are, but we can't change them. Vulnerability is those conditions of our network and workstations that are susceptible to exploitation by the threats. We can manage vulnerabilities - eliminate by keeping software patches up-to-date, control both physical and network access to systems, train people to reduce "social engineering." Countermeasures are those systems - software, hardware, and policy - put in place to specifically address vulnerabilities to threats. This would include signed appropriate use statements and Intrusion Detection System.

A WLAN, or wireless local area network, is a group of computers, printers or other hardware that are all connected without wires in a reasonably small geographic location like a small office or home. A WLAN makes it possible for the connected users to share files and applications that usually reside on a server or some type of shared computer. WLAN were invented to let people and computers share information without physical connection. A server can have an application or database that is accessed by all the other computers on the WLAN. This allows users to share information quickly and easily without physically connection of wires

IEEE 802.11 is emerging as the primary standard for wireless network and Internet access. It supports 11 Mbit/s wireless access in the 2.4GHz radio band and works over longer distances than Bluetooth and Home RF.

Wireless LANs use electromagnetic airwaves, either infrared (IrDA) or radio frequency (RF), to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

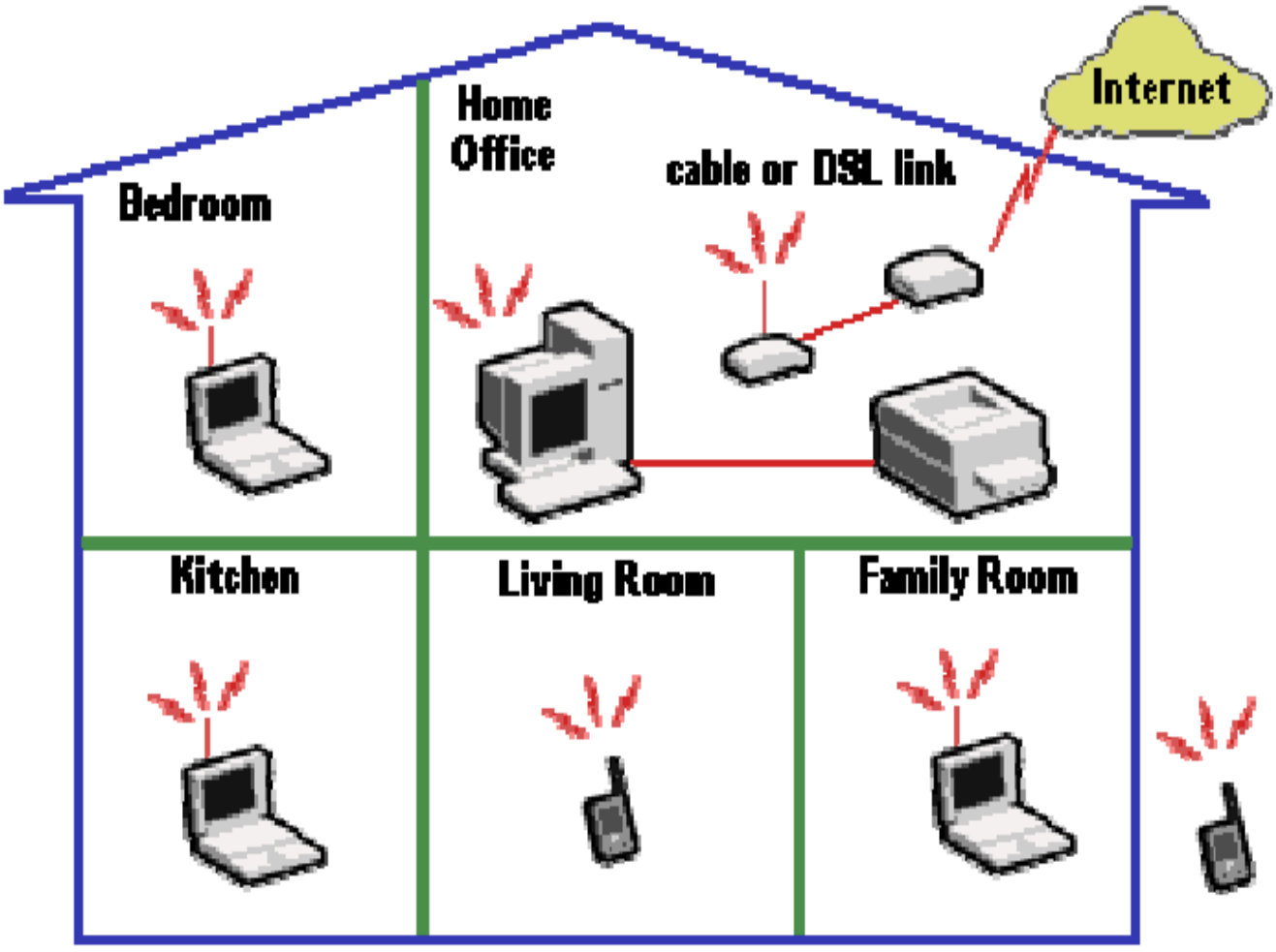
Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver or augment networks without installing or moving wires. Wireless LANs tunes in (or selects) one radio frequency while rejecting all other radio signals on different frequencies.

In a typical WLAN configuration, a transmitter/receiver (transceiver) device, called an Access point (AP), connects to the wired network from a fixed location using standard Ethernet cable. At a minimum, the Access Point receives, buffers, and transmits data between the WLAN and the wired network infrastructure. A single Access Point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The Access Point is usually mounted high but may be mounted essentially anywhere that is practical as long as the desired radio coverage is obtained.

End users access the WLAN through WLAN adapters, which are implemented as PCMCIA cards in notebook computer, ISA or PCI cards in desktop computers, or integrated within hand-held computers. WLAN adapters provide an interface

between the client Network Operating System (NOS) and the airwaves (via an antenna). The nature of the wireless connection is transparent to the NOS.

Following Diagram shows the structural overview of a wireless network at a small house. It shows Desktop placed in say computer room or study room and then laptop which can be carried in bedroom, kitchen or family room. Also PDA can be used in wireless network. You can carry your laptop or a PDA in your Lawn and Garden.



General Diagram For Home Network

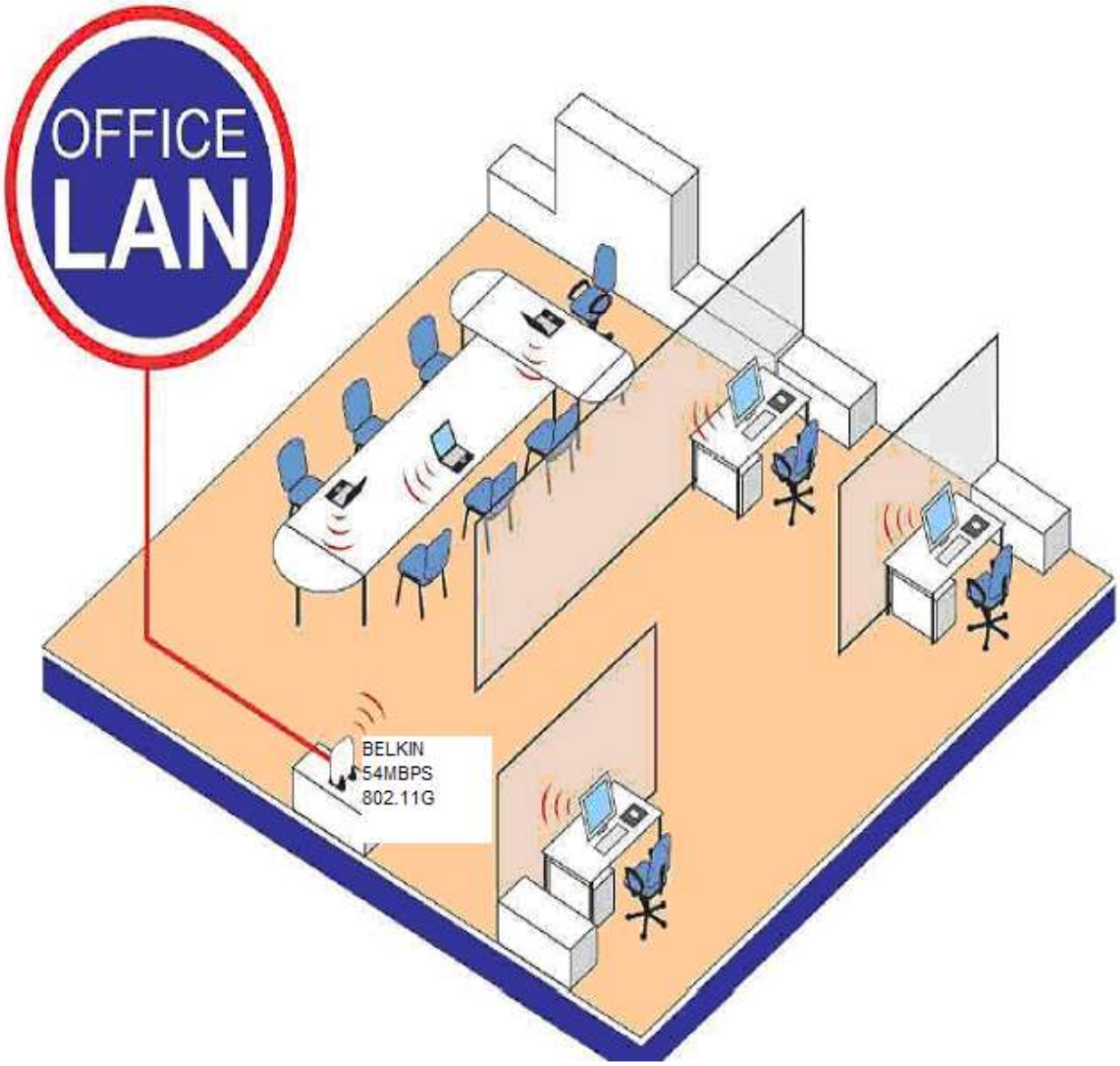


Diagram above shows you structural view of a small office where Wireless local area network can be used.

Implementation

To start with network first you should know the hardware part of the network, as I have already described what are the hardware components that will be needed for a soho. Again to describe briefly,

WLAN Adapters: -

Wireless adapters are made in the same basic form factors as their wired counterparts - PCMCIA, Card bus, PCI and USB. They also serve the same function, enabling end users to access the network. In a wired LAN, adapters provide the interface between the network operating system and the wire. In a WLAN, they provide the interface between the network operating system and an antenna, to create a transparent connection to the network.

Access Point or Wireless Router: -

Essentially, the Access Point is the wireless equivalent of a LAN hub. It receives, buffers and transmits data between the WLAN and the wired network, supporting a group of wireless user devices. An Access Point is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. The Access Point, or the antenna connected to it, is generally mounted high on a wall or on the ceiling. Like the cells in a cellular phone network, multiple Access Points can support hand-off from one Access Point to another as the user moves from area to area

Introduction to GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (GFI LANguard N.S.S.) is a tool that allows network administrators to quickly and easily perform a network security audit. GFI LANguard N.S.S. creates reports that can be used to fix security issues on a network. It can also perform patch management. Unlike other security scanners, GFI LANguard N.S.S. will not create a 'barrage' of information, which is virtually impossible to follow up on. On the contrary, it will help highlight the most important information. It also provides hyperlinks to security sites to find out more about these vulnerabilities. Using intelligent scanning, GFI LANguard N.S.S. gathers information on machines such as usernames, groups, network shares, USB devices, wireless devices and other information found on a Windows Domain. Apart from this, GFI LANguard N.S.S. also identifies specific vulnerabilities such as configuration problems in FTP servers, exploits in Microsoft IIS and Apache Web Servers or problems in Windows security policy configuration, plus many other potential security issues.

System Requirements

The installation of GFI LANguard Network Security Scanner requires the following:

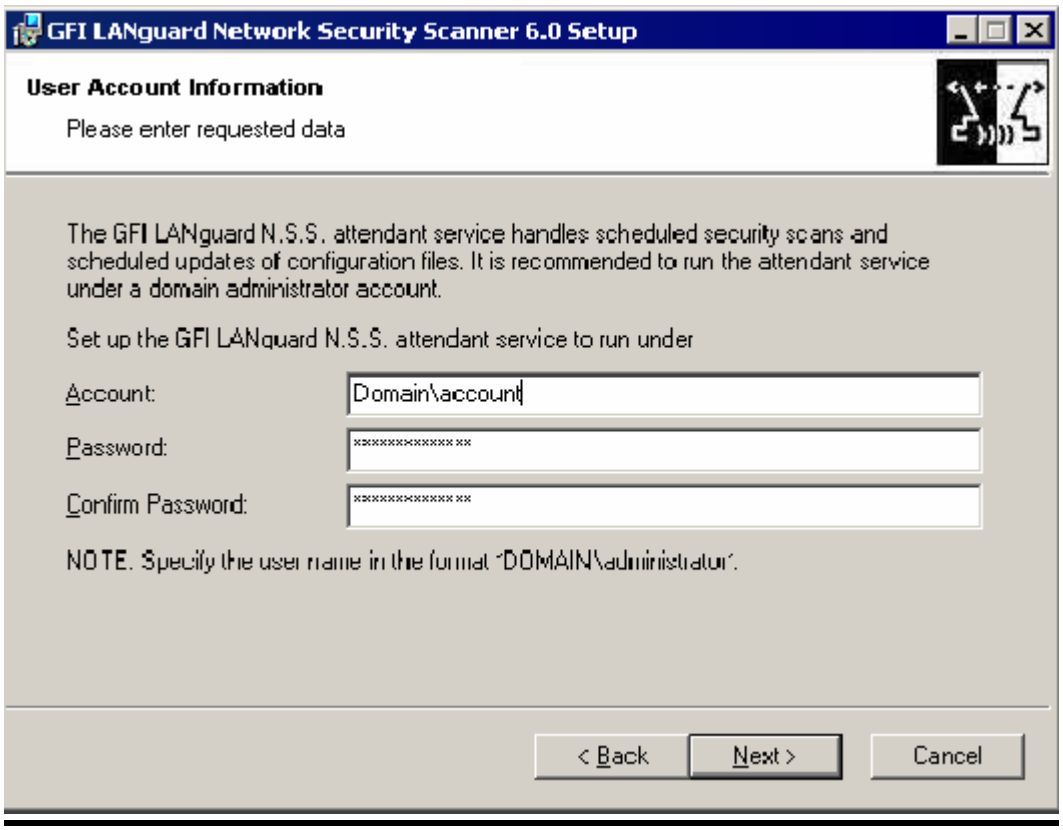
- Windows 2000/2003 or Windows XP
- Internet Explorer 5.1 or higher
- Client for Microsoft Networks must be installed.
- NO Personal Firewall software or the Windows XP Internet
- To deploy patches on remote machines you need to have administrator privileges

Installation Procedure:

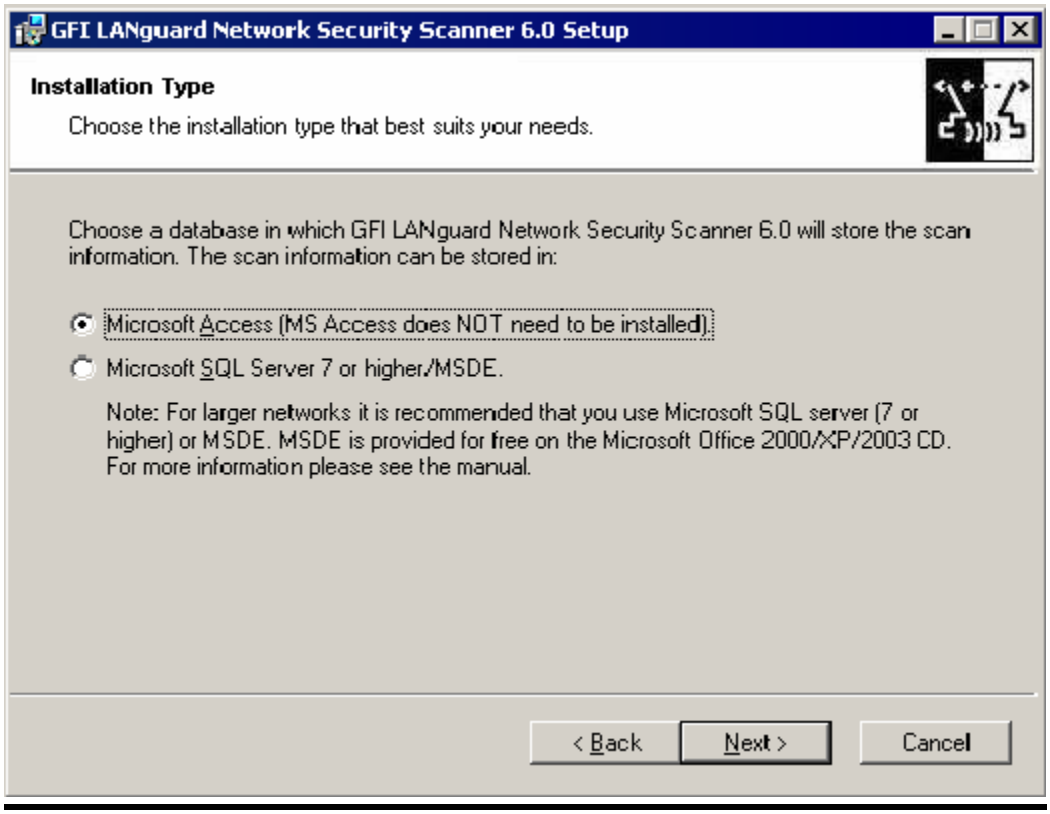
1. Run the LANguard Network Security Scanner setup program by double clicking on the languardnss6.exe file. Confirm that you wish to install GFI LANguard N.S.S. The setup wizard will start. Click Next.

2. After reading the License agreement dialog box, click Yes to accept the agreement and continue the installation.

3. Setup will ask you for user information and License key



4. Setup will ask you for domain administrator credentials which are used by the LANguard N.S.S Attendant service (which runs scheduled scans). Enter the necessary credentials and click Next.



5. Setup will ask you to choose the database backend for the GFI LANguard N.S.S database. Choose between Microsoft Access or Microsoft SQL Server\MSDE and click Next.

6. If you selected Microsoft SQL Server/MSDE as a database backend, you will be asked for the SQL credentials to use to log on to the database. Click Next to continue.

7. Setup will ask you for an administrator email address and your mail server name. These settings will be used for sending administrative alerts.

8. Choose the destination location for GFI LANguard N.S.S. and click Next. GFI LANguard N.S.S. will need approximately 40 MB of free hard disk space.

9. After GFI LANguard N.S.S. has been installed, you can run GFI LANguard Network Security Scanner from the start menu.

Introduction to Security Audits

An audit of network resources enables the administrator to identify possible risks within a network. Doing this manually requires a lot of time, because of the repetitive tasks and procedures, which have to be applied to each machine on the network. GFI LANguard N.S.S. automates the process of a security audit & easily identifies common vulnerabilities within your network in a short time.

Note: If your company runs any type of Intrusion Detection Software (IDS) then be aware that the use of LANguard Network Security Scanner will set off almost every bell and whistle in it. If you are not the one in charge of the IDS system, make sure that the administrator of that box or boxes is aware of the scan that is about to be run. Along with the warning of IDS software be aware that a lot of the scans will show up in log files across the board. Unix logs, web servers, etc. will all show the attempt from the machine running LANguard Network Security Scanner. If you are not the sole administrator at your site make sure that the other administrators are aware of the scans you are about to run.

Performing a Scan:

The first step in beginning an audit of a network is to perform a scan of current network machines and devices. To begin a new network scan:

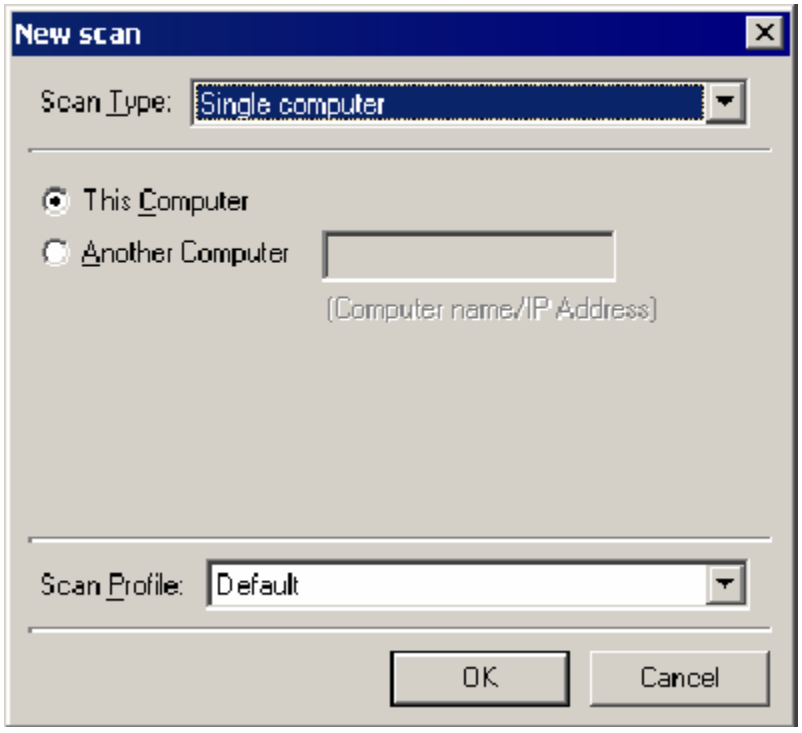
1. Click on (**File > New).**

2. Select what to scan. You can select the following:

- **a**. Scan one Computer - This will scan a single machine.
- **b**. Scan Range of Computers – This will scan a specific range of IP's
- **c**. Scan List of Computers – This scans a custom list of computers. Computers can be added to the list by selecting them from a list of enumerated computers, by entering them one by one, or by importing the list from a text file.
- **d**. Scan a Domain – This scans an entire windows domain.

3. Depending on what you want to scan input the starting and ending range of the network to be scanned.

4. Select (**Start Scan)**.



LANguard Network Security Scanner will now perform a scan. It will first detect which hosts/computers are on, and only scan those. This is done using NETBIOS probes, ICMP ping and SNMP queries. If a device does not answer to one of this GFI LANguard N.S.S. will assume, for now, that the device either does not exist at a specific IP address or that it is currently turned off.
Note: If you want to force a scan on IPs that do not respond, see the chapter 'Configuring scan options' for more information how to configure this.

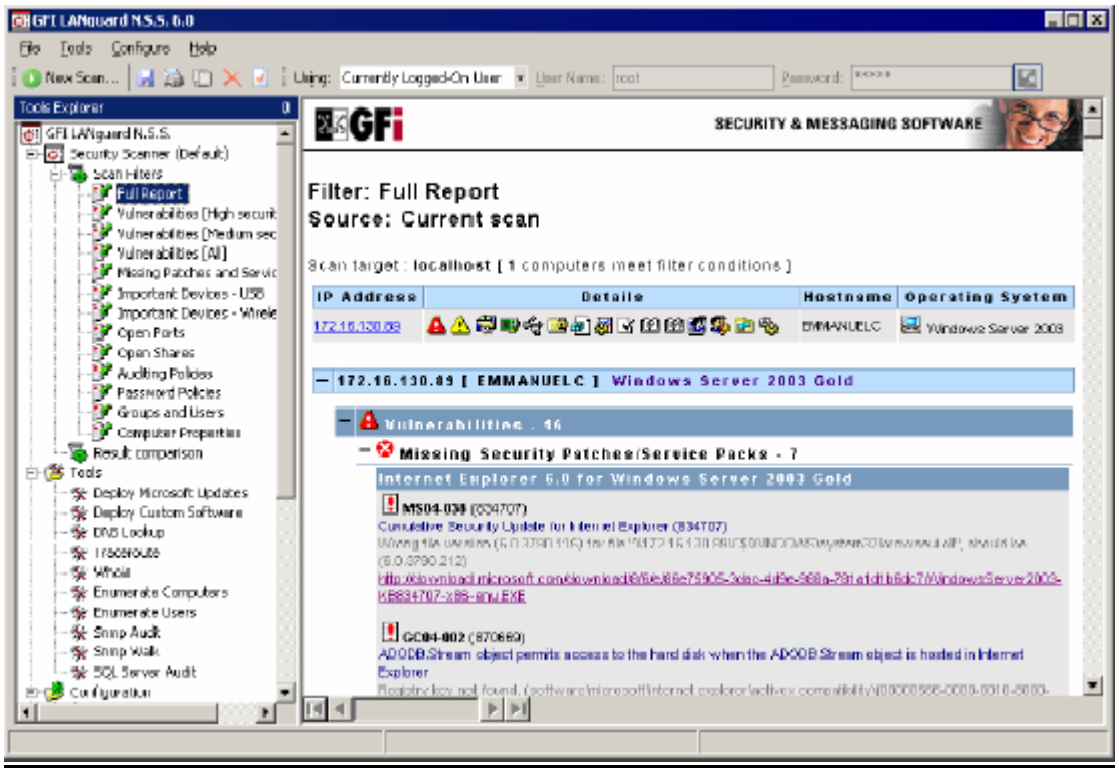
Saving and Loading scan results

Once GFI LANguard N.S.S. completes a security scan, it automatically saves the scan results to its database backend (MS Access / MS SQL Server). You can also save the scan results to an external XML file. Saved scan results can be re-loaded into the GFI LANguard N.S.S. user interface for further processing or result comparison. Loading saved scan results is very useful when one needs to run reports or deploy patches on an unchanged system, which does not require rescanning.

Filtering scan results

Introduction

After GFI LANguard N.S.S. has performed a scan, it will show the results in the 'Scan results' pane. If you have scanned a large number of machines, you might want to filter that data from the Scan filters node. Clicking on this node and selecting an existing filter will show the scan results based on what filter you selected. GFI LANguard N.S.S. ships with a number of default scan filters. In addition you can make your own custom scan filters.



The following scan filters are included by default:

Full report: Shows all security related data collected in a scan.

Vulnerabilities [High Security]: Shows issues, which require immediate attention – missing service packs, missing patches, high security vulnerabilities and open ports.

Vulnerabilities [Medium Security]: Shows issues, which may need to be addressed by the administrator – medium security vulnerabilities, patches which cannot be detected.

Vulnerabilities [All]: Shows all vulnerabilities detected – missing patches, missing service packs, potential information checks, patches which could not be detected, low & high security vulnerabilities.

Missing patches and service packs: lists all missing service packs and patch files on the machines scanned.

Important devices – USB: Lists all the USB devices attached to the scan targets.

Important devices – Wireless: Lists all the wireless network cards, (both PCI and USB) attached to the scan targets.

Open Ports: lists all open TCP and UDP ports.

Open Shares: lists all open shares and who has access to them.

Auditing Policies: lists the auditing policy settings on each of the scanned computers.

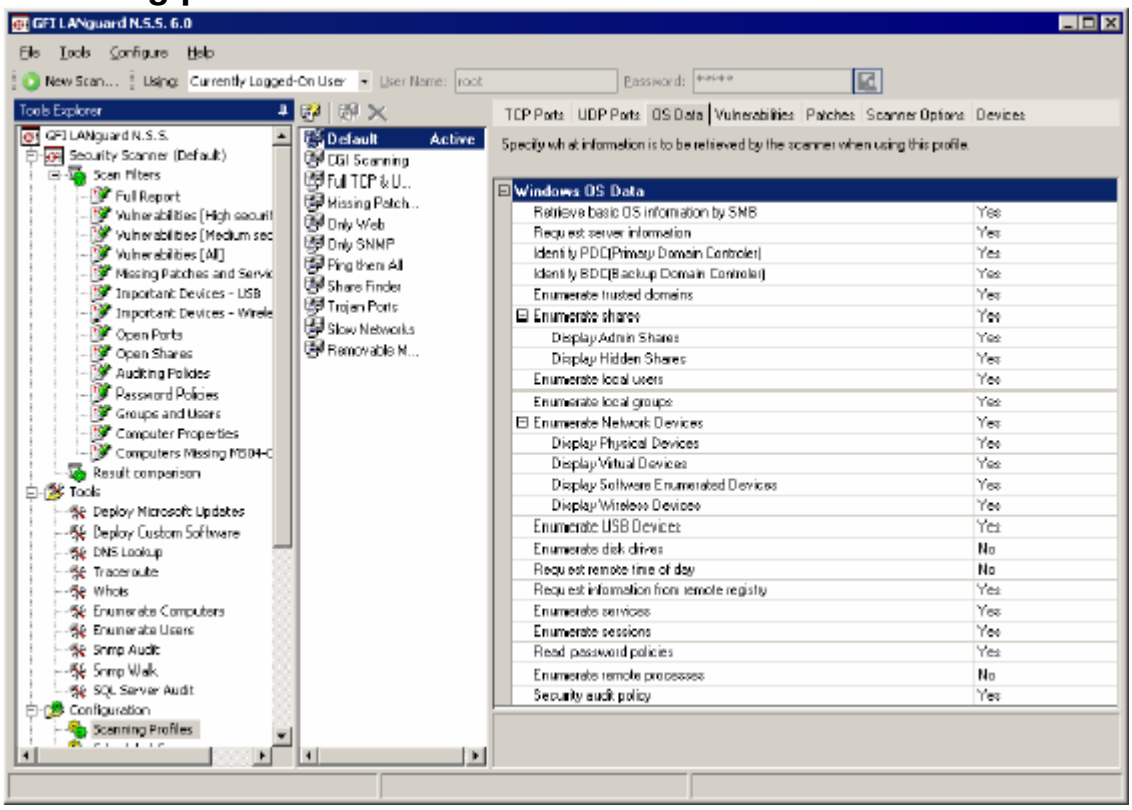
Password Policies: lists the active password policies on each of the scanned computers.

Groups and users: lists the users and groups detected on each of the scanned computers.

Computer properties: Shows the properties of each computer

Configuring GFI LANguard N.S.S.

Scanning profiles:



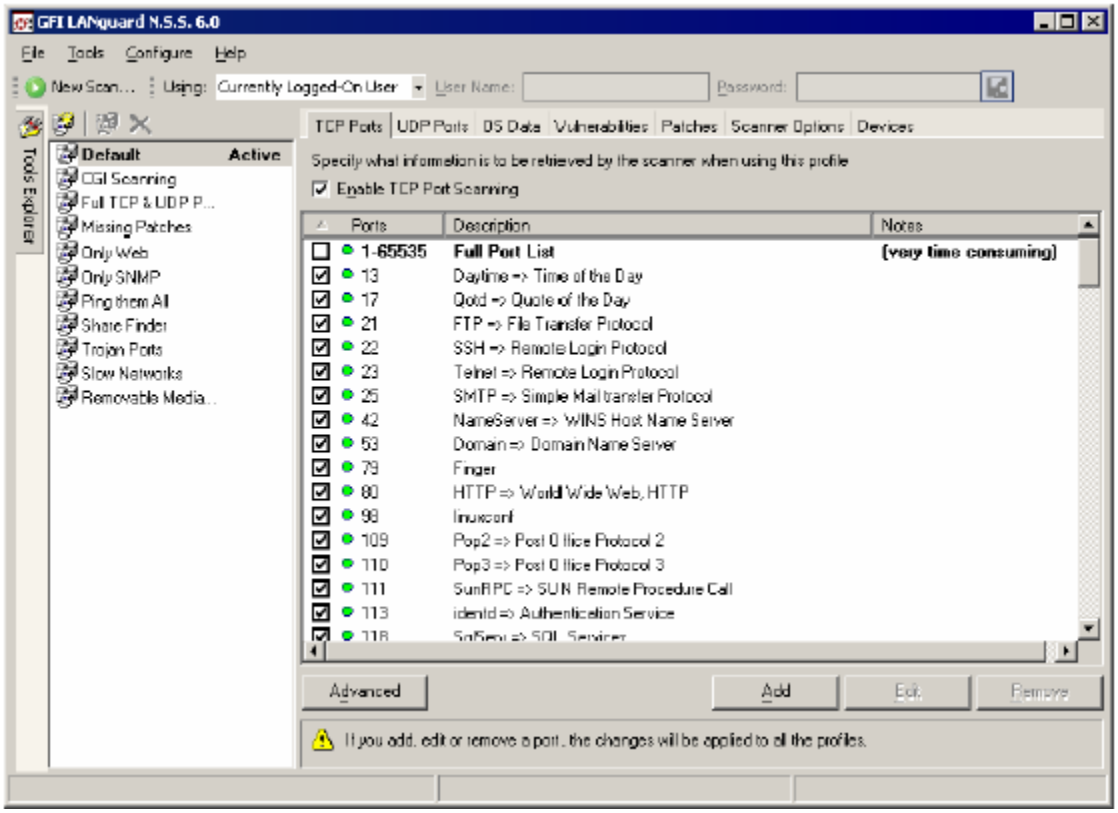
Using scanning profiles, you can configure different types of scans, and use these different scans to focus on particular types of information that you want to check for. A scan profile is created by going to the Configuration > Scanning profiles node right-clicking and selecting **New > Scan Profile…**

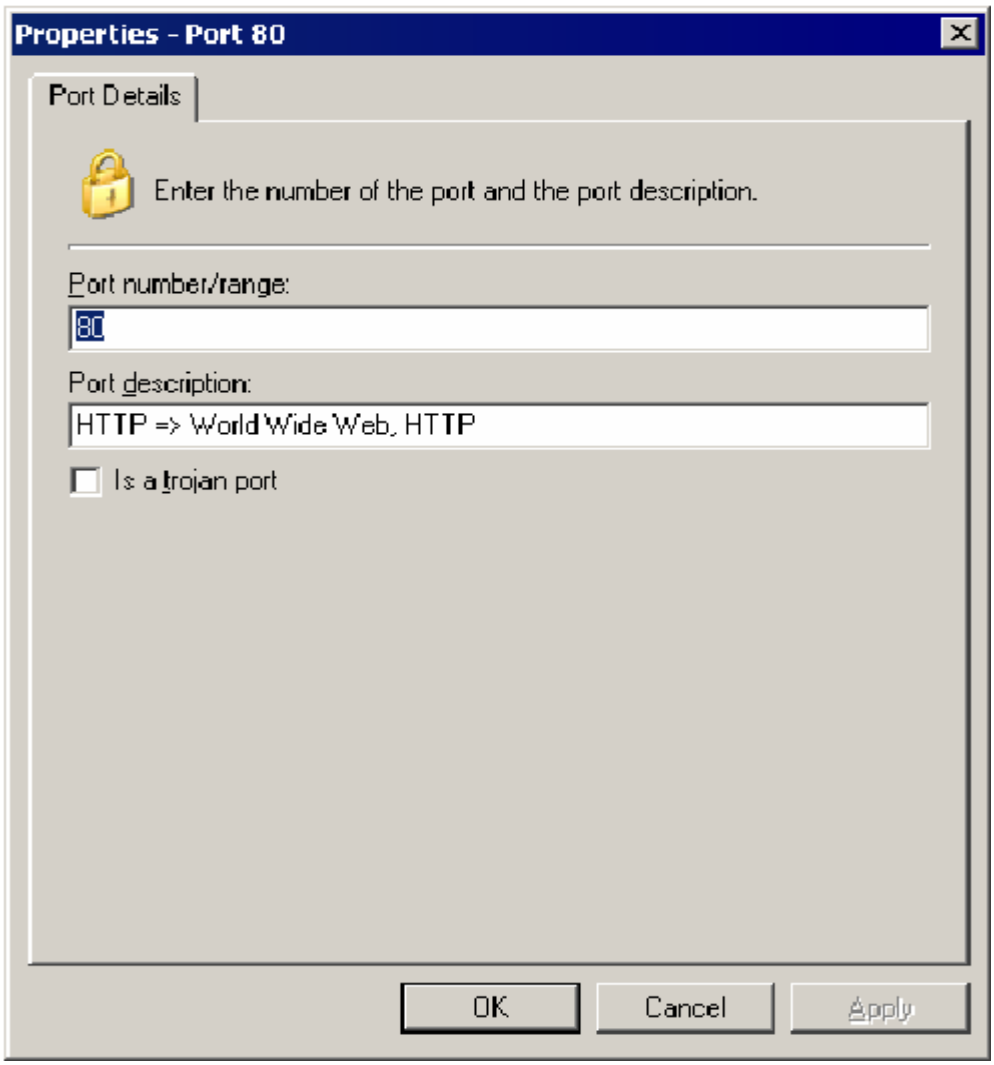
You can configure the following options for each profile:

1. Scanned TCP ports
2. Scanned UDP ports
3. Scanned OS data
4. Scanned Vulnerabilities
5. Scanned Patches
6. Scanner properties
7. Devices

Scanned TCP/UDP ports:

The scanned TCP/UDP ports tabs allow you to specify which TCP and UDP ports you wish to scan. To enable a port simply click on the tick box next to the port.



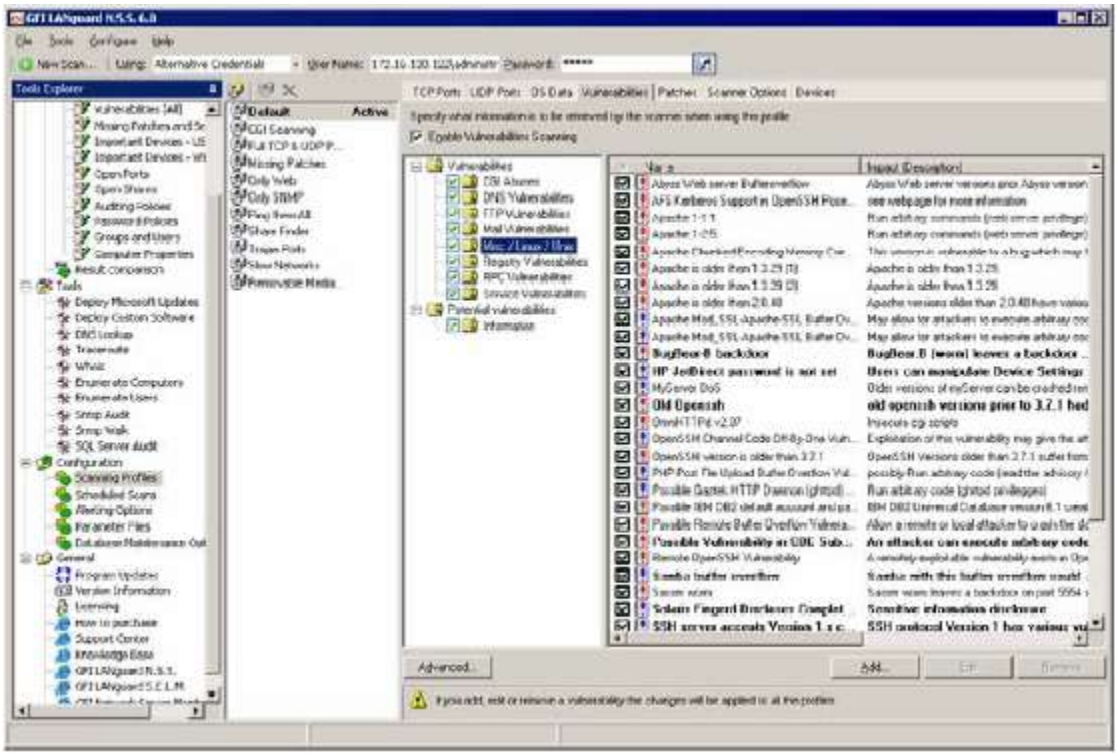


Simply enter a port number or a port range and enter a description of the program, which is supposed to run on that port. If the program associated with this port is a Trojan, click on the 'Is a Trojan port" check box. If you specify it is a Trojan port, the green / red circle next to the port will be red.

Scanned OS data:

The Scanned OS data tab specifies the kind of information you want GFI LANguard N.S.S. to collect from the operating system during the scan. Currently only Windows OS data is supported, however UNIX scan data is under development.

Scanned Vulnerabilities:



The scanned vulnerabilities tab lists all vulnerabilities that GFI LANguard N.S.S. can scan for. You can disable checking for all vulnerabilities by de-selecting the 'Check for vulnerabilities' check box. By default, GFI LANguard N.S.S. will scan for all vulnerabilities it knows. You can change this by removing the check box next to a particular vulnerability. From the right pane, you can change the options of a specific vulnerability by double clicking on it. You can change the security level of a particular vulnerability check from the "Security Level" option.

Types of Vulnerabilities

Vulnerabilities are broken down into the following sections: Missing Patches, Patches which cannot be detected, CGI Abuses, FTP Vulnerabilities, DNS Vulnerabilities, Mail Vulnerabilities, RPC Vulnerabilities, Service Vulnerabilities, Registry Vulnerabilities, and Miscellaneous Vulnerabilities.

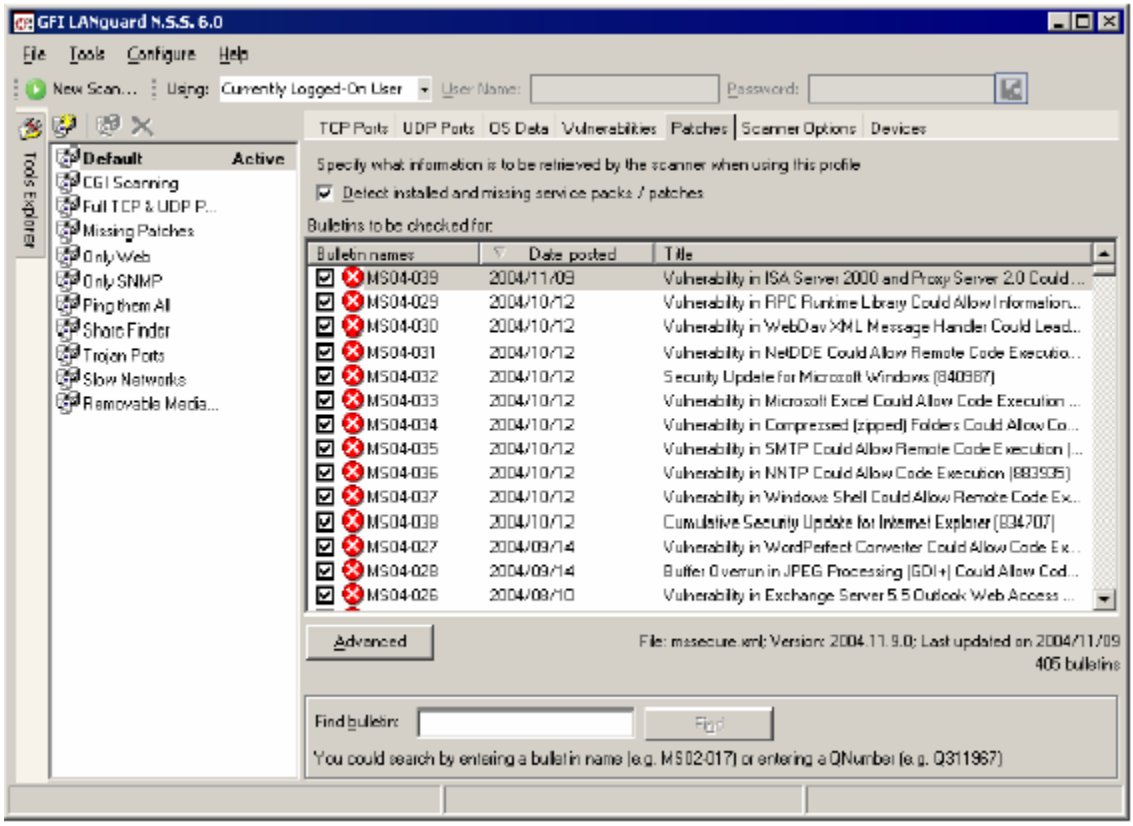
Vulnerability checks advanced options:

• **Internal Checks -** These include ftp anonymous password checks, weak password check etc.

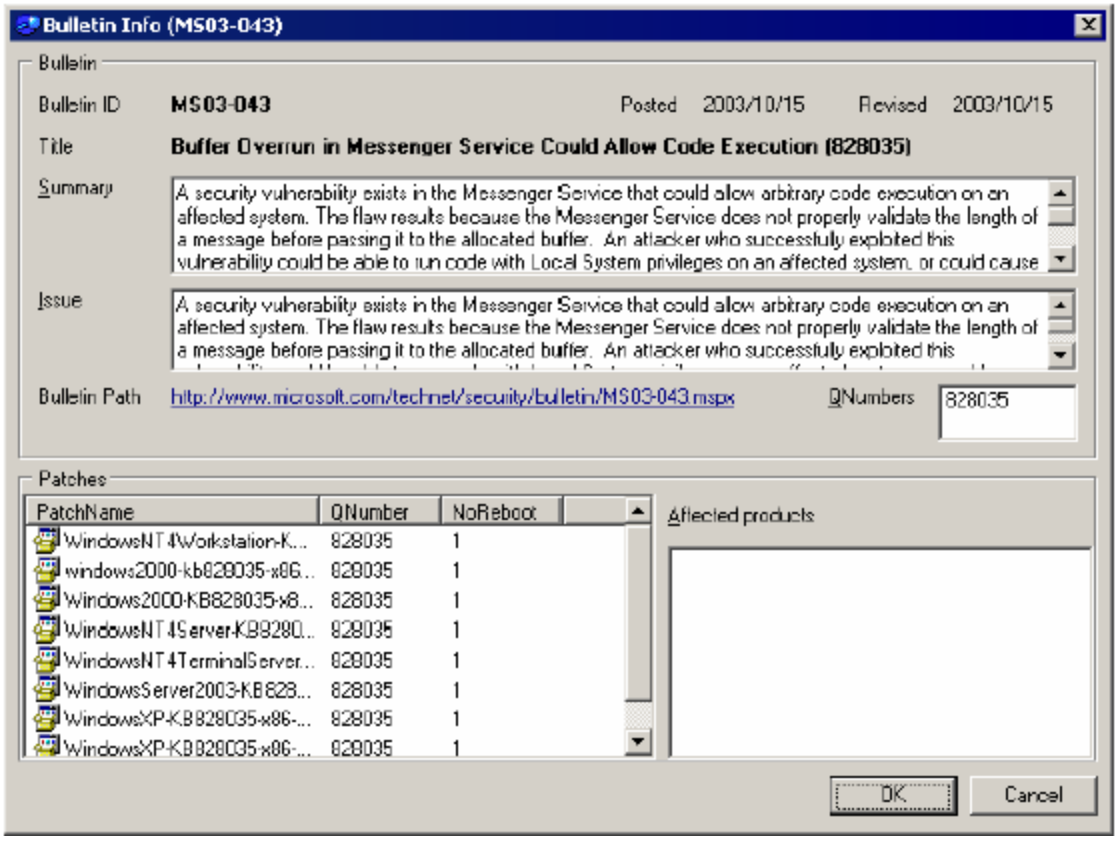
• **CGI Probing -** Switch on CGI probing if you are running web servers that use CGI. You can optionally specify a proxy server if you are located behind a proxy server.

• **New vulnerabilities are enabled by default** – Enables/Disables newly added vulnerabilities to be included in the scans of all.

Scanned Patches:



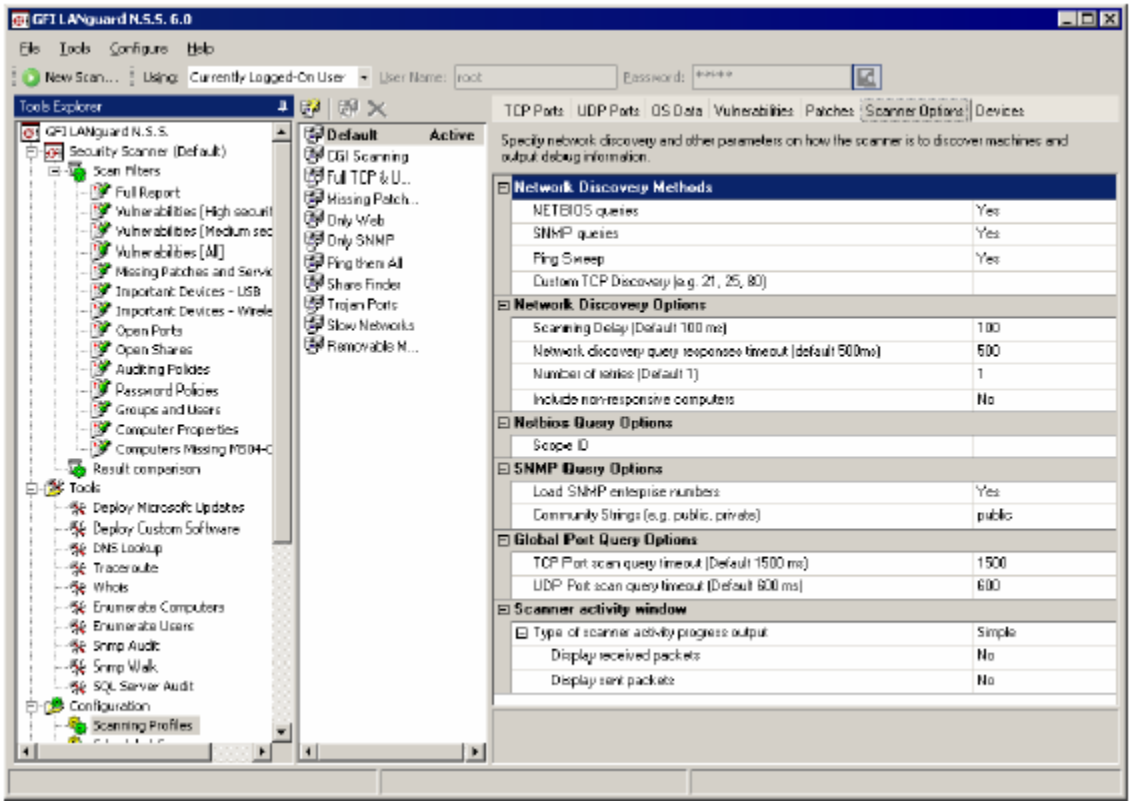
The scanned patches tab allows you to configure whether this particular scan profile should check for missing patches and/or service packs. The tab lists all the patches that GFI LANguard N.S.S. checks for. You can disable checking for particular patches for this profile by unchecking the tick box next to the patch bulletin. The list of patches is obtained by downloading the latest patch list from the GFI website, which in turn is obtained from Microsoft (mssecure.xml). GFI obtains the list of patches of Microsoft and checks it for correctness, since sometimes it contains errors.



For more information on a particular bulletin, double click on an the bulletin or right click on it and select Properties. You will be presented with more details on what the bulletin checks for and what it addresses.

Scanner options:

In this tab you can configure options relating to how GFI LANguard N.S.S. should perform a scan.



Network discovery methods

This section addresses which methods GFI LANguard N.S.S. is to use to discover machines over the network.

The **NETBIOS queries** option allows NetBIOS or SMB queries to be used. If the Client for Microsoft Networks is installed on the Windows Machine, or if Samba Services are installed on a Unix machine, then those machines will answer the NetBIOS type query. You can add a ScopeID to the NetBIOS Query. This is only required in some cases, in which systems have a ScopeID. If your organization has a ScopeID set on NetBIOS, input it here.

The **SNMP queries** option will allow SNMP packets to be sent out with the Community String that was set in the General tab. If the device responds to this query, GFI LANguard N.S.S. will request the Object Identifier from the device and compares that to a database to determine what that device is.

Ping Sweep does an ICMP ping of each network device.

Custom TCP Port Discovery checks for a particular open port on the target machines.

Network discovery options

The network discovery parameters allow you to tweak machine detection, to have the most reliable machine detection in the least time possible. Adjustable parameters include

• **Scanning Delay** is the time LANguard N.S.S. waits between TCP/UDP packets it sends out. The default is 100 ms. Depending on your network connection and the type of network you are on (LAN/WAN/MAN) you may need to adjust these settings. If it is set too low you may find your network congested with packets from GFI LANguard N.S.S. If you set it too high a lot of time will be wasted.

• **Wait for Responses** is the time GFI LANguard N.S.S. will actually wait for a response from the device. If you are running on a slow or busy network you may need to increase this timeout feature from 500 ms to something higher.

• **Number of retries** is the number of times that GFI LANguard N.S.S. will perform each type of scan. Under normal circumstances this setting should not be changed. Be aware, however, that if you do change this setting, it will run through each type of scan (NETBIOS, SNMP, and ICMP) that number of times.

• **Include non-responsive computers** is an option, which instructs the GFI LANguard N.S.S. security scanner to try to scan a machine which has not replied to any network discovery method.

NetBIOS Query Options

The scope of using a NetBIOS Scope ID is to isolate a group of computers on the network that can communicate only with other computers that are configured with the identical NetBIOS Scope ID. NetBIOS programs started on a computer using NetBIOS Scope ID cannot "see" (receive or send messages) to NetBIOS programs started by a process on a computer configured with a different NetBIOS Scope ID. GFI LANguard N.S.S. supports NETBIOS Scope ID in order to be able to scan these isolated computers that otherwise would be inaccessible.

SNMP Query Options

The option to Load **SNMP enterprise numbers** will allow GFI LANguard N.S.S. to extend support in SNMP scanning. If this is disabled, devices discovered by SNMP that are unknown to GFI LANguard N.S.S. will not report who the vendor is supposed to be. Unless you are running into problems, it is recommended to leave this option enabled. By default most SNMP enabled devices use the default community string ‘public’, but for security reasons most administrators will change this to something else. If you have changed the default SNMP community name on your network devices, you should add it to the list GFI LANguard N.S.S. uses.

Scanner activity windows options

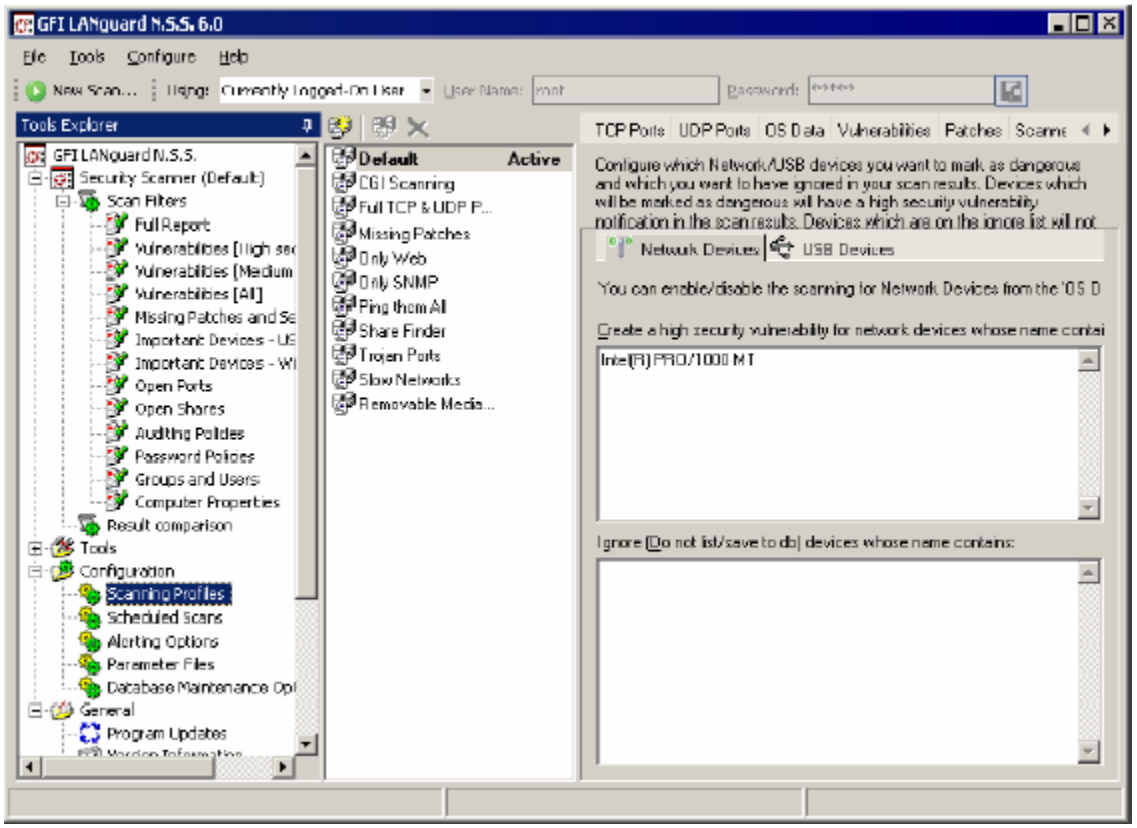
The output options allow you to configure what information to display on the scanner activity pane. It is useful to enable it, however only enable ‘Verbose’ or the ‘Display packets’ for exceptional debugging purposes.

Devices:

In this tab one can configure how LANguard N.S.S. will react when it detects a particular network or USB device. You can configure GFI LANguard N.S.S. to notify you via a critical vulnerability notification when a particular device is detected or configure GFI LANguard N.S.S. to ignore particular devices, such as USB keyboards or mice.

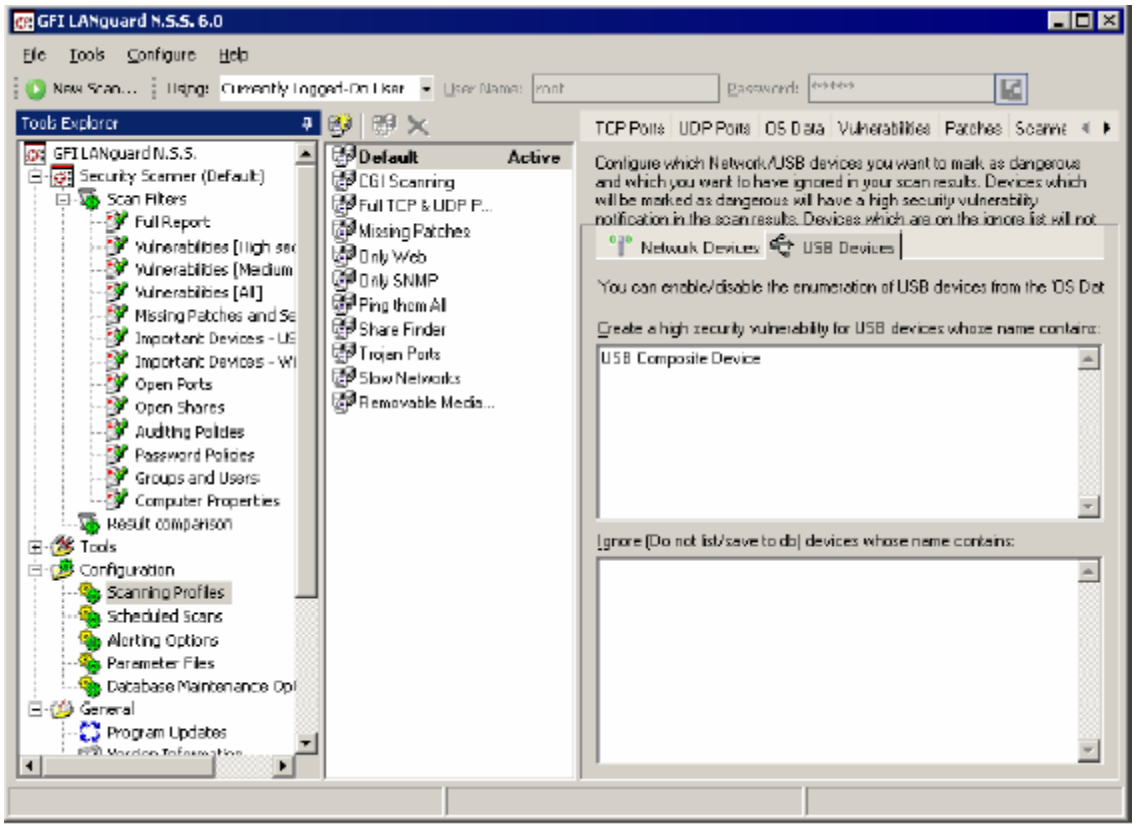
Network Devices

Every retrieved network device has a display name. If the detected device name contains any of the string entries in the “Create a high security vulnerability for network devices whose name contains:” list section (one per line), a high security vulnerability will be generated and reported for the computer on which the device was detected.



USB Devices

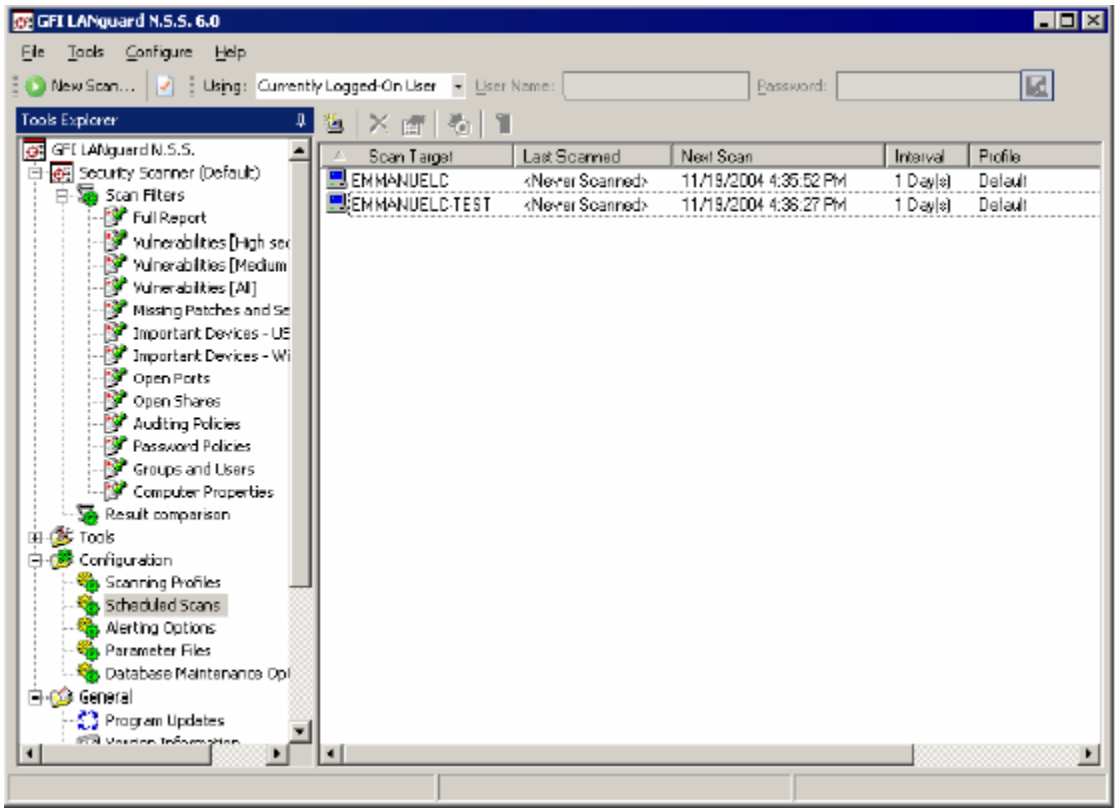
Every USB device retrieved has a display name. If the detected device name contains any of the string entries in the “Create a high security vulnerability for USB devices whose name contains:” list section (one per line), a high security vulnerability will be generated and reported for the computer on which the device was detected.



Scheduled Scans:

The scheduled scan feature allows you to configure scans which will be run automatically at a specific date / time. Scheduled scans can also be run periodically. This allows you to run a particular scan at night or early in the morning and can be used in conjunction with the results comparison feature, allowing you to receive a 'change report' automatically in your mailbox.

By default all scheduled scans are stored in the database. Optionally you can save all scheduled scan results to an XML file (one per scheduled scan). This can be done by right clicking on the Scheduled Scan node, selecting Properties, enabling the Save Scheduled Scan option and specifying a path for the XML files.

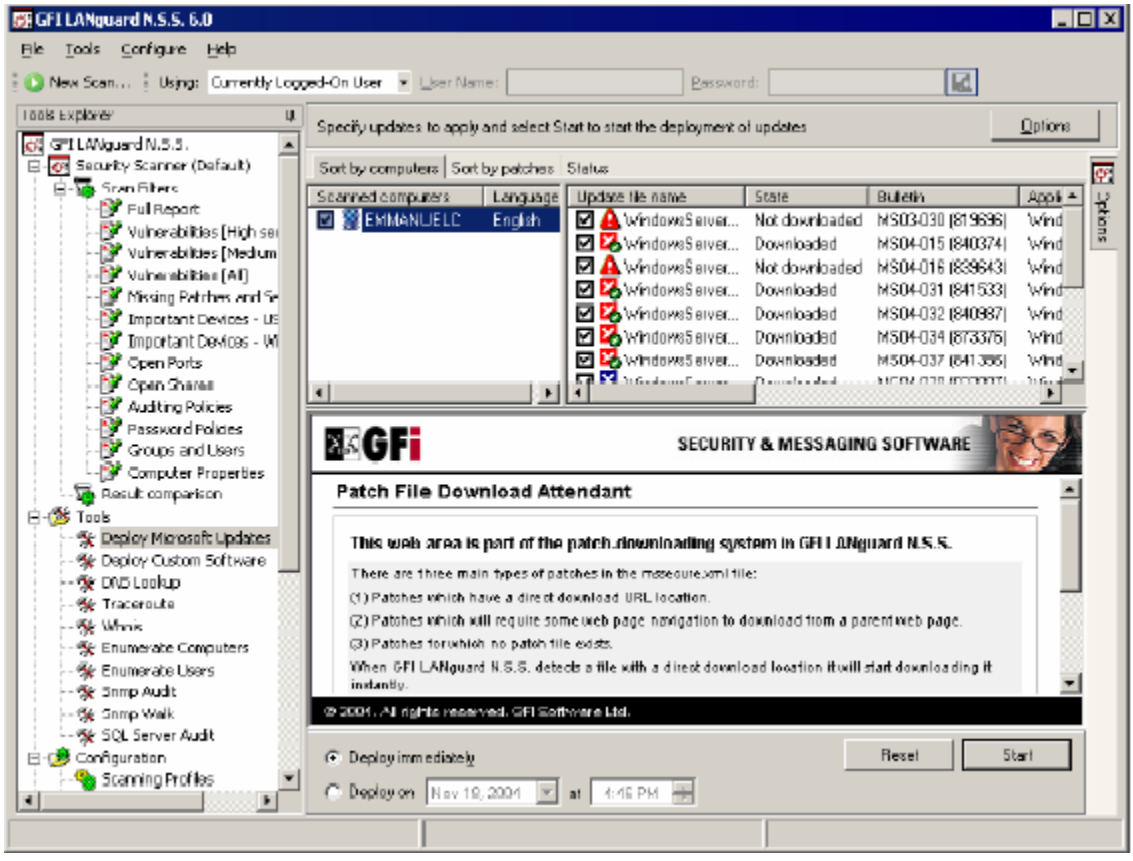


Patch Deployment:

Use the patch deployment tool to keep your Windows NT, 2000, XP and 2003 machines up to date with the latest security patches and service packs.

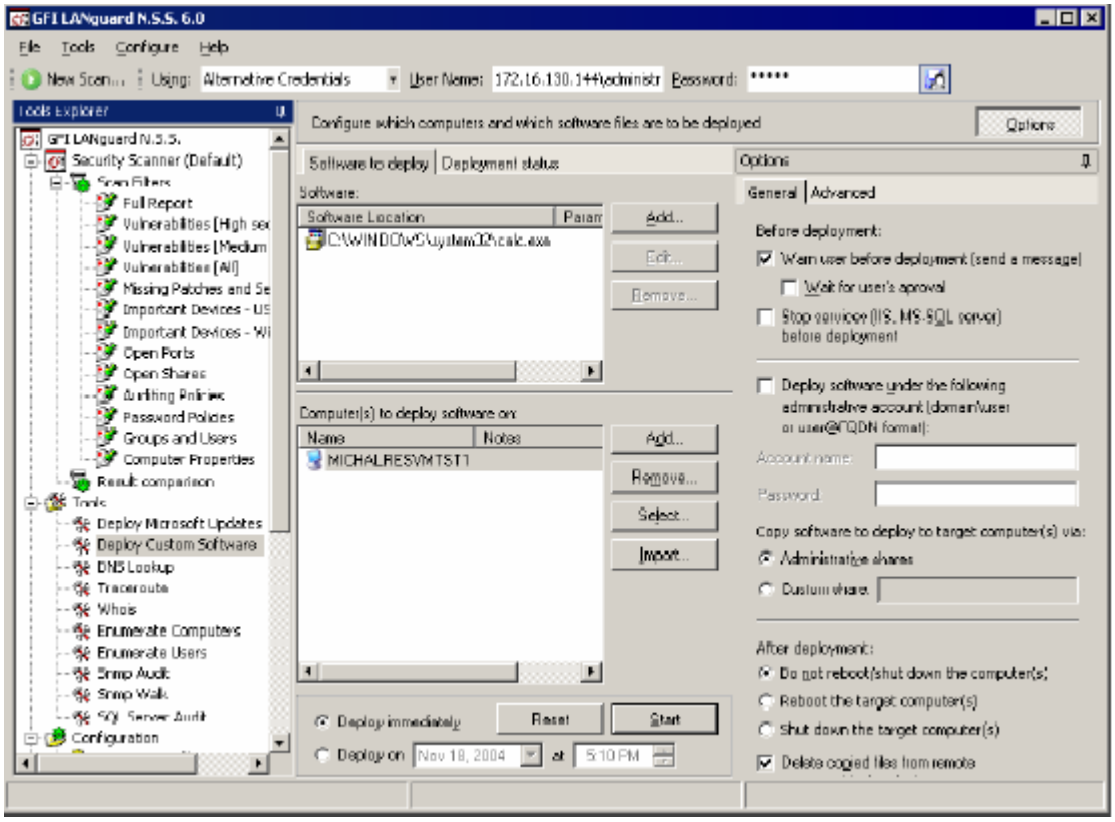
The patch deployment agent

GFI LANguard N.S.S. 6 uses a patch deployment agent, which is installed silently on the remote machine, to deploy patches, services packs and custom software. The patch deployment agent consists of a service which will run the installation at a scheduled time depending on the deployment parameters indicated. This architecture is much more reliable than without using a patch deployment agent. The patch deployment agent is installed automatically without administrator intervention.



Deploying custom software:

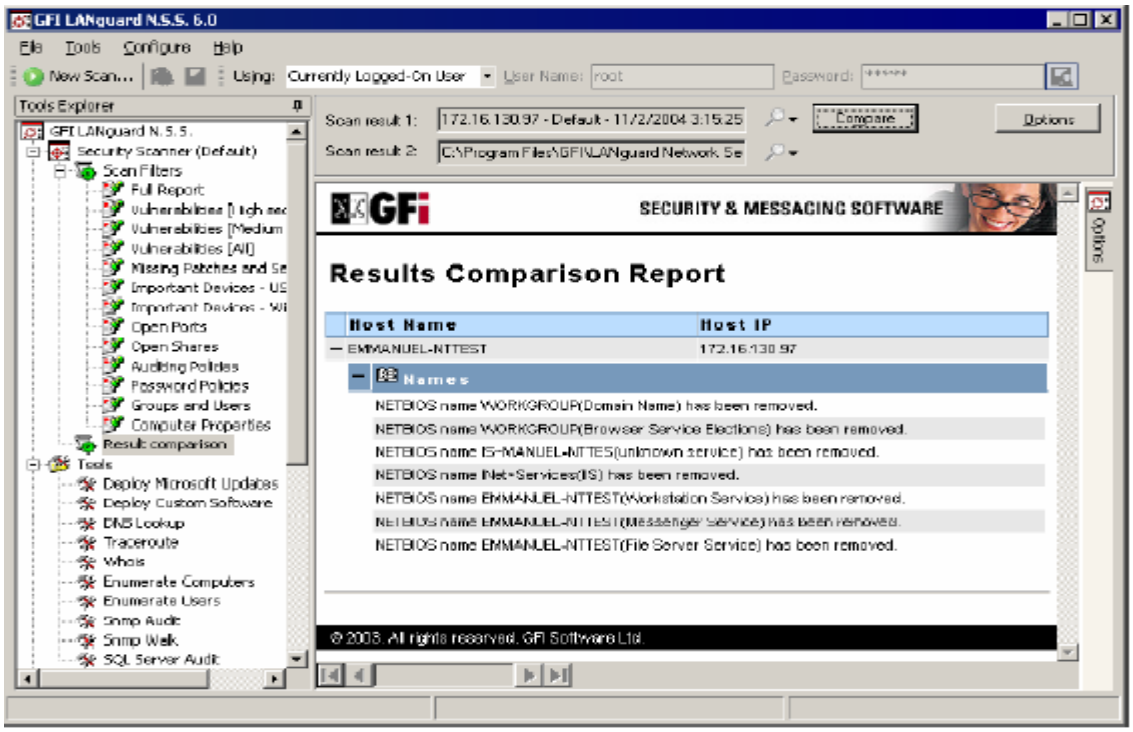
The custom software deployment tool is very handy to quickly deploy custom patches for software network wide, or even to install software network wide. The custom software deployment tool is also frequently used to deploy virus signature updates network wide. The process of deploying custom software is very similar to the process of patching a machine.



Results Comparison:

Why Compare Results?

By performing audits regularly and comparing results from previous scans you will get an idea of what security holes continually pop up or are reopened by users. This creates a more secure network. GFI LANguard Network Security Scanner helps you do this by allowing you to compare results between scans. GFI LANguard N.S.S. will report the differences and allow you to take action. You can compare results manually or through scheduled scans.



The result will be similar to the above screenshot. It tells you what has been enabled or disabled and any network changes since the last scan.

• New items will show anything new that occurred after the first scan.

• Removed items will show any devices/issues that were removed since the first scan.

• Changed items will display anything that has changed, such as a service being enabled or disabled between scans.

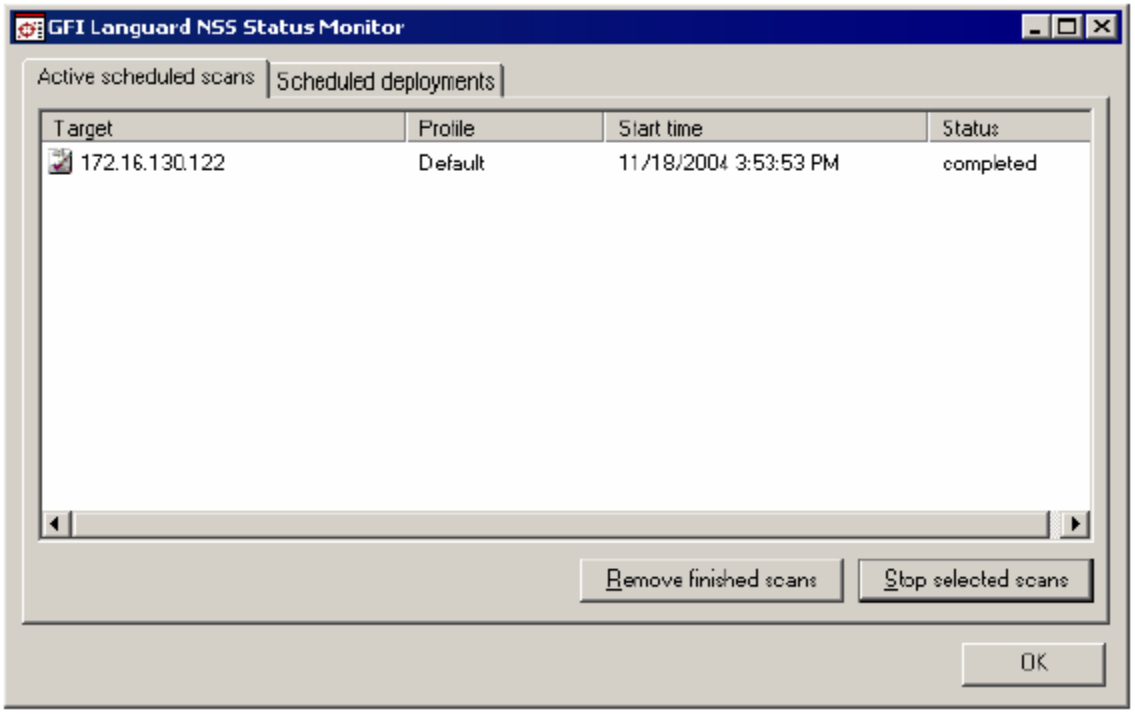
Performing a Comparison with the Scheduled Scans Option

Instead of manually scanning your network each day, week, or month, you can setup a scheduled scan. A Scheduled Scan will run automatically at a certain time and will email the differences between scheduled scans to the administrator. For example: the administrator can configure the Scheduled Scan feature to perform a scan every night at 23:00. The GFI LANguard N.S.S. attendant service will launch a security scan on the selected target computer(s) and save the results to the central database. Then, it will compare the current results with the results from the night before and report the differences, if any.

GFI LANguard N.S.S. Status Monitor:

Viewing scheduled operations

The GFI LANguard N.S.S. status monitor allows you to monitor the status of active scheduled scans and software update deployments. You can also cancel scheduled deployment operations.

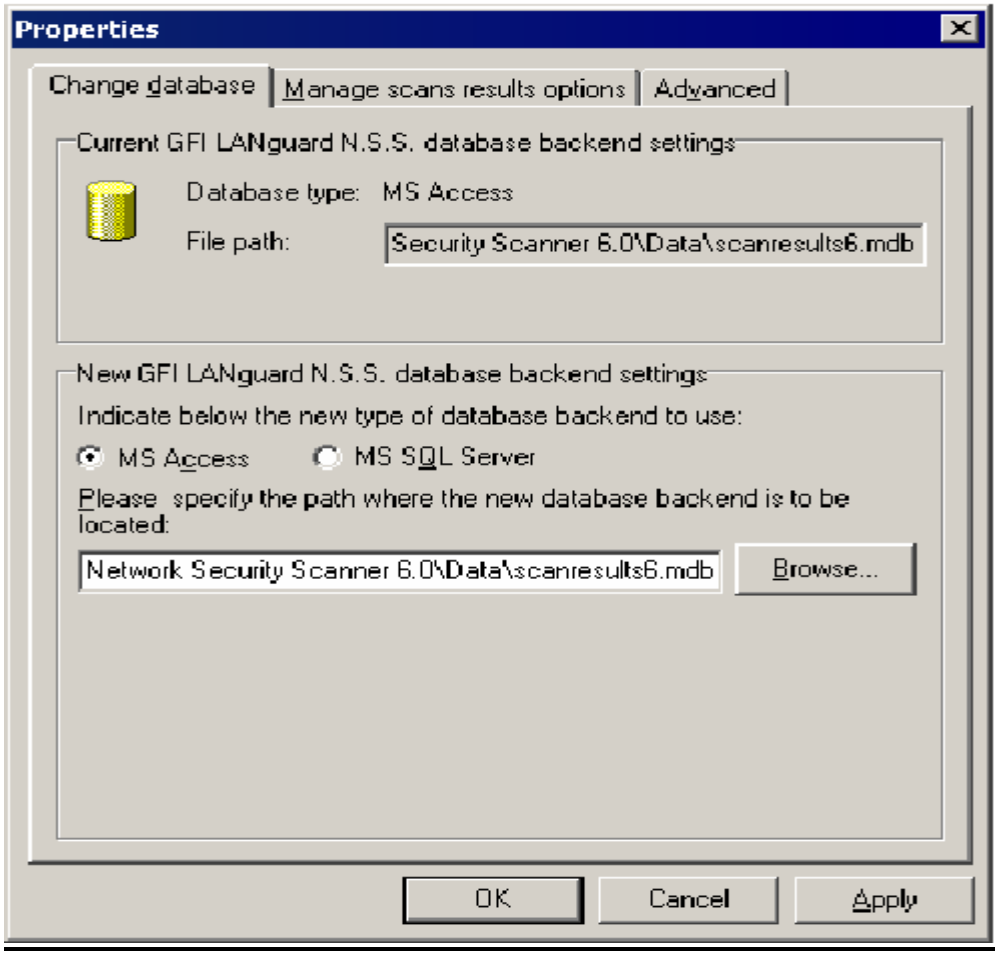


Database Maintenance Options:

Use the database maintenance options node to select which database backend to use to store your saved scan results. You can also configure database maintenance options, such as automatically deleting scan results older than a particular age.

Change Database

The **Change Database** tab contains the options for changing the database backend used by GFI LANguard N.S.S. to store the scan results in. Supported database back ends are MS Access or MS SQL Server.



Tools:

The following Tools can be found under the Tools Menu

• DNS Lookup

• Whois Client

• Trace Route

• SNMP Walk

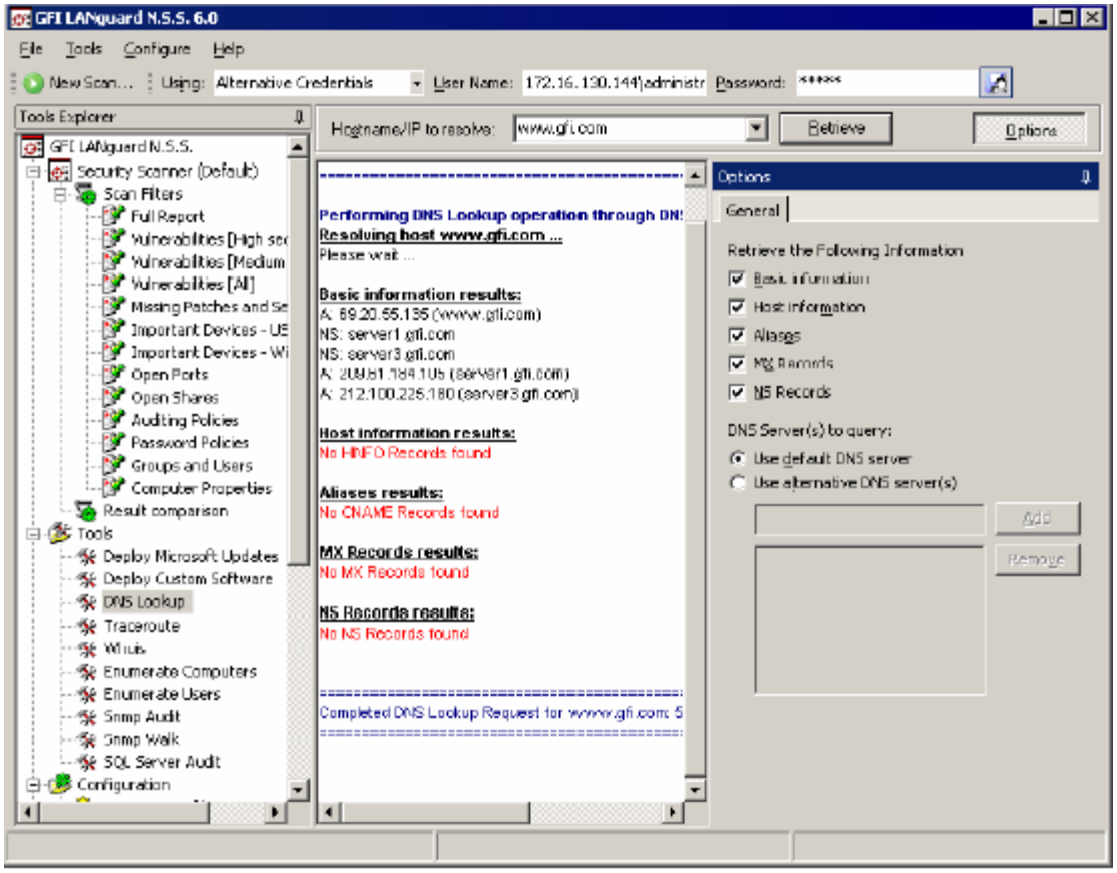
• SNMP Audit

• MS SQL Server Audit

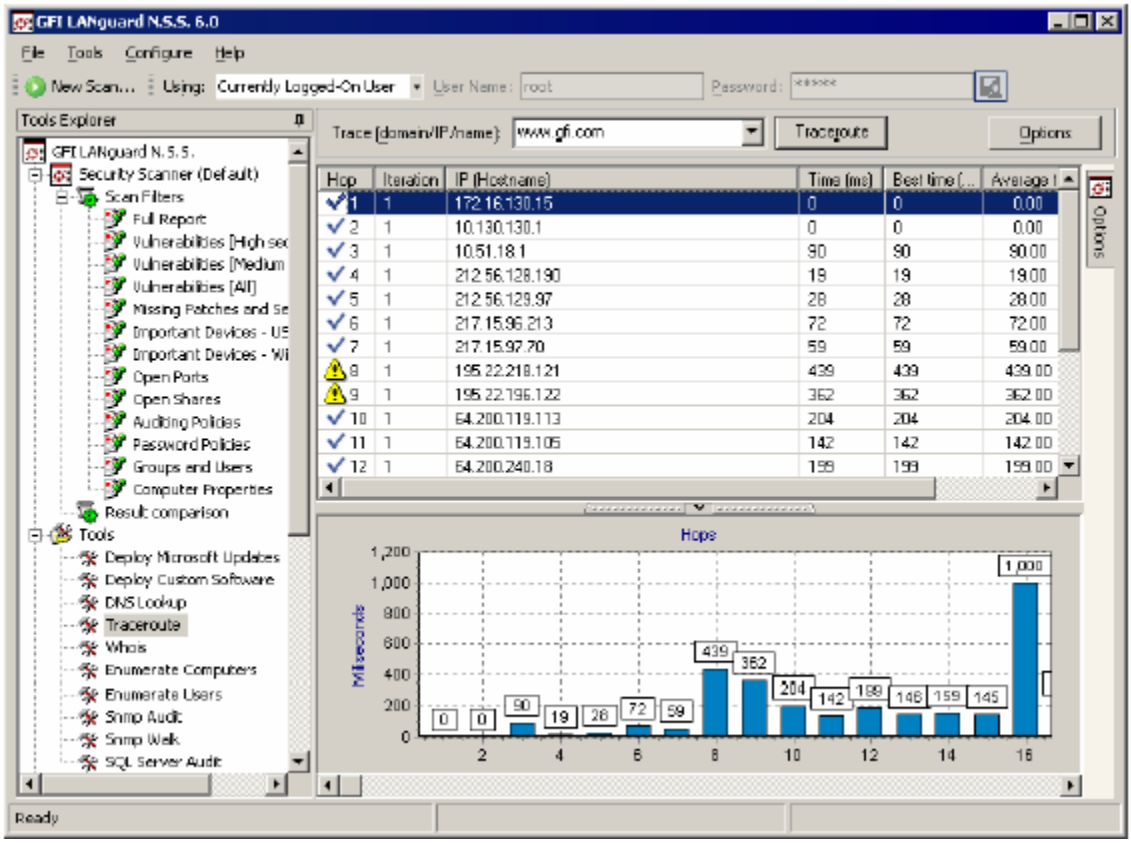
• Enumerate Computers

DNS lookup

This tool resolves the Domain Name to a corresponding IP address and in addition provides information about the domain name, such as whether it has an MX record etc.



Trace Route



This tool shows the network path that GFI LANguard N.S.S. followed to reach the target machine. When you perform a trace route, each hop has an icon next to it:

• Indicates a successful hop taken within normal parameters

• Indicates a successful hop, but time required was quite long.

• Indicates a successful hop, but the time required was too long

• Indicates that the hop timed out. (i.e. it took longer then 1000ms)

SNMP Walk

SNMP walk allows you to gather SNMP information. The right pane contains a list of names symbolizing specific Object ID's on the device. To find out more about the information provided by the SNMP walk, you will have to check with the vendor. Some vendors provide great details on what each piece of information means, others, though their devices support SNMP, provide no documentation on it at all.

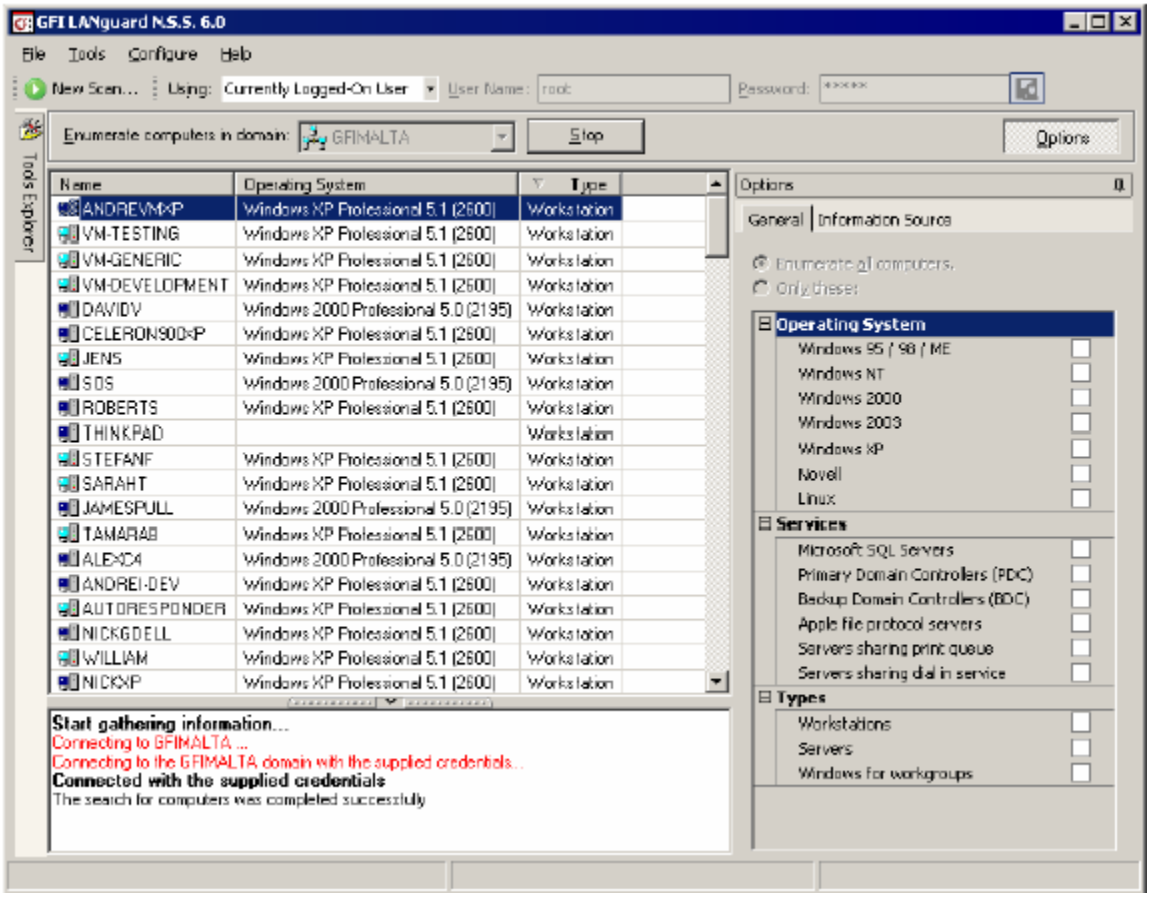
SNMP Audit

The SNMP Audit tool, allows you to perform an SNMP audit on a device and audit for weak community strings. Some network devices will have alternative or non-default community strings. The dictionary file contains a list of popular community strings to check for. The default file it uses for the dictionary attack is called snmp-pass.txt. You can either add new community names to this file, or direct the SNMP audit to use another file altogether. To use the utility, input the IP address of a machine running SNMP and click Retrieve.

MS SQL Server Audit

This tool allows you to perform an audit on a Microsoft SQL server installation. You can audit both the SA account, as well as all SQL accounts.

Enumerate Computers



This utility will search your network for Domains and/or Workgroups on it. Once it has found that, you will have the ability to scan those Domains for a list of computers in them. Once it has performed its scan it will list whatever OS is

installed on that machine, and any comments that might be listed through NETBIOS.

Computers can be enumerated using one of the following methods

• From Active Directory – This method is much faster and will also enumerate computers that are currently switched off

• Using the Windows Explorer interface – This method is slower and will not enumerate computers that are switched off.

You can specify which method to use from the Information Source tab. Note that you will need to perform the scan using an account that has access rights to Active Directory. Launching a security scan. Once the computers in the domain are enumerated you can launch a scan on selected machines by right-clicking on any of the enumerated computers and selecting Scan. If you want to launch the scan but continue to use the Enumerate computers tool, select Scan in background.

Enumerate Users

The Enumerate users function connects to Active Directory and retrieves all users and contacts in Active Directory

Security issue related to Network

Easy Access

LANs are easy to find. Strictly speaking, however, the information needed to join a network is also the information needed to launch an attack on a network. Beacon frames are not processed by any privacy functions, which means that your 802.11 network and its parameters are available for anybody with an 802.11 card. "War drivers" have used high-gain antennas and software to log the appearance of Beacon frames and associate them with a geographic location using GPS.

Short of moving into heavily-shielded office space that does not allow RF signals to escape, there is no solution for this problem. The best you can do is to mitigate the risk by using strong access control and encryption solutions to prevent a wireless network from being used as an easy entry point into the network. Deploy access points outside firewalls, and protect sensitive traffic with VPNs.

Check your network for all potential methods that a hacker might use to attack it. By analyzing the operating system and the applications running on your network, network scanner identifies possible security holes. In other words, it plays the devil's advocate and alerts you to weaknesses before a hacker can find them, enabling you to deal with these issues before a hacker can exploit them.

"Rogue" Access Points

Easy access to wireless LANs is coupled with easy deployment. When combined, these two characteristics can cause headaches for network administrators. Any user can run to a nearby computer store, purchase an access point, and connect it to the corporate network without authorization. Many access points are now priced well within the signing authority of even the most junior managers. Departments may also be able to roll out their own wireless LANs without authorization from the powers that be.

"Rogue" access points deployed by end users pose great security risks. End users are not security experts, and may not be aware of the risks posed by wireless LANs. Most existing small deployments mapped by war drivers do not enable the security features on products, and many access points have had only

minimal changes made to the default settings. It is hard to believe that end users within a large corporation will do much better.

Unauthorized Use of Service

Several war drivers have published results indicating that a clear majority of access points are put in service with only minimal modifications to their default configuration. Nearly all of the access points running with default configurations have not activated WEP (Wired Equivalent Privacy) or have a default key used by all the vendor's products out of the box. Without WEP, network access is usually there for the taking.

Two problems can result from such open access. In addition to bandwidth charges for unauthorized use, legal problems may result. Unauthorized users may not necessarily obey your service provider's terms of service, and it may take only one spammer to cause your ISP to revoke your connectivity.

MAC Spoofing and Session Hijacking

802.11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air." Just as on traditional Ethernet networks, there is no protection against forgery of frame source addresses. Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions.

Traffic Analysis and Eavesdropping

802.11 provide no protection against attacks that passively observe traffic. The main risk is that 802.11 do not provide a way to secure data in transit against eavesdropping. Frame headers are always "in the clear" and are visible to

anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned Wired Equivalent Privacy specification.

A great deal has been written about the flaws in WEP. It protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving attacker wide latitude to disrupt transmissions with spoofed frames.

Higher Level Attacks

Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell, though, is a soft, vulnerable (and tasty?) center.

Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack. Depending on the perimeter security in place, it may also expose other networks to attack, and you can bet that you will be quite unpopular if your network is used as a launch pad for attacks on the rest of the world.

Some more security issue related to WLAN.

- 802.11b has a couple problems with the protocol. First off the SSID (Service Set Identifier) which shows which logical network is on which

channel. The problem with the SSID is that it's in the header of the packet so it’s not encrypted and very easy to sniff. Of course, you don't really want anyone knowing the SSID of your WLAN unless you want them to have access.

- Secondly, WEP (Wired Equivalent Privacy), a RC4 symmetric stream cipher with 40 bit and 104 bit encryption keys is the encryption used with 802.11b. The problem with WEP is that it's easy to crack after collecting enough packets (5-10 million packets requires under a second to crack the encryption), there is a significant loss of bandwidth, and people from outside can’t eavesdrop but users can listen to each other inside the WLAN.
- Also, 802.11b does not have user authentication, unicast session management support, and no support for MAC filters. All of these have been implemented in other layers above the 802.11b protocol but it's still a weakness of 802.11b
- War-driving is a process in which an individual uses a wireless device such as a laptop or PDA to drive around looking for wireless networks. Some people do this as a hobby and map out different wireless networks, which they find. Other people, who can be considered hackers, will look for wireless networks and then break into the networks. If a wireless is not secure, it can be fairly easy to break into the network and obtain confidential information.
- War-chalking is a method of marking wireless networks by using chalk most commonly. War-driving is usually the method used to search for networks, and then the person will mark the network with chalk that gives information about the network. Some of the information would include, what the network name is, whether the network has security, and possibly the contact information of who owns the network. If your wireless network is War-chalked and you don't realize it, your network can be used and/or broken into faster, because of information shown about your network.

Software Tools Used In Project

Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g.

Wireless/Network Security Solutions

Wireless Security

Security for IEEE 802.11 consists of encryption and authentication. Encryption is used to encrypt, or scramble, the data in wireless frames before they are sent on

the wireless network. Authentication requires wireless clients to authenticate themselves before they are allowed to join the wireless network.

Properties of secure communications for wireless networks consist of the following:

Authentication Before being allowed to exchange data traffic with the wireless/network, the network node must be identified and (depending on the authentication method) must submit credentials that can be validated.

Encryption Before sending a wireless data packet, the network node must encrypt the data to ensure data confidentiality.

Data integrity Before sending a data packet, the wireless network node must include information in the packet so the receiver can determine that the contents of the packet were not modified in transit.

Encryption and Data Integrity: -

Due to the broadcast nature of wireless LAN networks, eavesdropping and remote sniffing of wireless LAN frames is very easy.

The following types of encryption are available for use with 802.11 networks:

- WEP
- WPA

Authentication

Open System

Open system authentication is not really authentication, because all it does is identify a wireless node using its wireless adapter hardware address. A hardware

address is an address assigned to the network adapter during its manufacture and is used to identify the source and destination address of wireless frames.

For infrastructure mode, although some wireless APs allow you to configure a list of allowed hardware addresses for open system authentication, it is a fairly simple matter for a malicious user to capture frames sent on your wireless network to determine the hardware address of allowed wireless nodes and then use that hardware address to perform open system authentication and join your wireless network.

For ad hoc mode, there is no equivalent to configuring the list of allowed hardware addresses in Windows XP. Therefore, any hardware address can be used to perform open system authentication and join your ad hoc mode-based wireless network.

SSID Broadcast

SSID or Service Set Identifier is a unique identifier specified in the header of wireless packets to act as a password for client connectivity to a wireless access point. This is commonly referred to as the wireless network name, and is broadcast on the wireless network by the access point. The following are guidelines for configuring SSID Broadcast on an AP.

1. Unlike WEP turn the SSID Broadcast off if possible
2. Change the default SSID name
3. Increase beacon interval to the maximum setting to make passive scanning more difficult.

The above guidelines only provide protection against the casual snooper. Increasing the beacon interval makes for a quieter access point, and increases the time between each SSID transmission, but as noted the access point still transmits the SSID. While changing the default SSID helps mitigate against accidental associations with your neighbors access point, which more often than not happens to be manufactured by the same vendor. It also prevents users from easily guessing the SSID when SSID broadcast is disabled. However malicious users passively watching communication on a wireless network can still

determine a changed SSID since it transmitted in every associate request and response frame. The features used to obfuscate a wireless network SSID does not provide much in the way of security however it is another key piece in a layered approach to wireless security.

MAC Filtering

A MAC (Media Access Control) is the unique hardware address assigned to every network adapter. The MAC address uniquely identifies each host on a wireless network. MAC Filtering is the process of creating an Access Control List (ACL) to specifically permit or deny certain MAC addresses from connecting to the AP. Listed below are a few important tips about MAC Filtering.

1. Enable MAC Filtering, it won't work otherwise.
2. Since home networks are generally limited to a handful of devices it is likely to be more efficient to create a permit ACL for the known devices on your network rather than a deny ACL for unknown devices.

MAC Filtering does not come without its issues. Address Resolution Protocol or ARP is the protocol used to determine the MAC to IP pairing for the hosts on the wireless network. ARP information is passed in the clear between the clients and the AP. It is only a matter time before a malicious user will discover a MAC address that is permitted to connect to the access point. Some of the most common ARP related attacks are sniffing, hijacking, broadcasting, DOS, and cloning. All is not lost, and although MAC Filtering appears to be no better at protecting wireless networks than WEP and SSID Broadcast, it is a key element in the layered approach to wireless security.

Intrusion detection

Intrusion detection systems (IDSs) attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDSs have traditionally been developed to detect intrusions and misuse for wired systems and networks. More recently, IDSs have been developed for use on wireless networks. These wireless IDSs can monitor and analyze user and system

activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic.

A Wireless IDS is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to WLAN intrusion and misuse detection.

Wireless IDSs can be purchased through a vendor or developed in-house. There are currently only a handful of vendors who offer a wireless IDS solution - but the products are effective and have an extensive feature set. Popular wireless IDS solutions include Airdefense RogueWatch and Airdefense Guard, and Internet Security Systems Real secure Server sensor and wireless scanner products. A homegrown wireless IDS can be developed with the use of the Linux operating system, for example, and some freely available software. Open source solutions include Snort-Wireless and WIDZ, among others.

VPN

Virtual private network defines a way for devices to communicate securely over a non-secure medium. VPN does this by encrypting data and providing appropriate integrity and authentication checks. A common application of VPN is its use by telecommuters to establish secure connection to the corporate network using Internet. The connection between two systems communicating via VPN is called a tunnel.

Brief Basic Precaution that should be taken to secure WLAN are as follows: -

The first step to improving your wireless security is to change away from the default settings. This includes your administrator password and SSID (Service Set Identifier). For your SSID, make it long and hard to guess.

The second step is to ensure that your access point (AP) comes with 128 bit encryption, also known as Wired Equivalent Privacy (WEP). Another way to increase your security is to purchase and access point with firmware that allows for security enhancement.

Once you know that your access point comes with WEP, make sure it is turned on. Although this increases your security, it does not prevent someone from using your system. There are programs available for download that allow a person to crack WEP within a matter of seconds. Some experts suggest that WEP be considered as insecure. So, if you have WEP enabled, and it is your primary security, make sure you change the keys often.

If you want to reduce the strength of the signal from your AP (Access Point) to areas outside your room or building, ensure that the AP is in the centre of the room and away from windows.

If you would rather block usage of unauthorized users, there are ways to accomplish this as well. IPsec (IP Security) and SSL (Secure Socket Layer) are protocols that employ public key encryption. Or, if your OS is Unix or Linux, you could use SSH (Secure Shell) which is a connection that encrypts everything including the password and thus is very difficult for another user to crack. All of these methods use encryption of information so that if someone is trying to access your system by watching packets, they will not see anything useful.

Another way to block some unauthorized users is to limit MAC (Media Access Control) addresses. These are the unique addesses that identify each node in a network. MAC addresses can be limited by MAC filters. Limiting them requires that they be on your list of acceptable addresses, but does not take into account the possibility of faking a MAC address.

Disabling DHCP (Dynamic Host Configuration Protocol) also increases the security of your system. DHCP is a protocol that dynamically assigns IP addresses and keeps track of them within the software. This makes it very easy to add another computer to the network without a system administrator's knowledge. So disabling DHCP makes it so you control which computers are added to your system.

Remote Authentication Dial-In User Service (RADIUS) is a protocol and software for client/server applications that allow remote servers to authenticate users and authorize their access to the system or service via a central server. As of November 2002 it was a proposed Internet Engineering Task Force (IETF) standard.

Extensible Authentication Protocol (EAP) can be used in conjunction with RADIUS. EAP is a protocol that has a user request a connection through an AP, that gets the id of the user and sends it to an authentication server (may be RADIUS). The server asks the AP for proof of id, which the AP gets from the user and sends back to the server before allowing access.

We can use other technologies as Installing and configure Radius Server and use more secured technologies provided by the 802.1ix but all are high-end technologies and need more tools and software and professional to do so which will be expensive and not required for a Small Home Network and Small Office Environment. Instead of that you can use software as Wi-Fi defense, which come cheap.

Conclusion

When it comes to wireless and Network, there is no one standard that guarantees security.. Organizations like IEEE and IETF are working on different standards to provide privacy, integrity and confidentiality comparable to wired

networks. Until these standards are ratified, tested and user confidence is restored in wireless/LAN networks, administrators will have loom for alternative ways and incorporate multiple technologies to secure wireless communication.

In this Project I have discussed about available wireless/network standards, implementation and configration of a secured Small office or Home Wireless Network, Discussed about various security Problem in LAN, WLAN. Used software tool available to prove how secure is the network, giving some example using graphics and data graph and the discussed various security measures that should be scanned to secure your Network.

Lastly I would like to emphasize that even though traditional method of securing networks (i.e. firewalls) cannot completely serve the network to be secure, they do provide additional layer of security. Strategic use to scanning software can reduce the risk of open loops for the outside world for a possible intrusion and thereby increasing an extra layer of security and relief for the network and its users.

References

lhttp://www.cisco.com/en/US/netsol/

lwww.microsoft.com

lhttp://www.wi-fiplanet.com/tutorials/article.php/953651

lwww.ieee.org

http://www.gfi.com/lannetscan/

lhttp://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214249,00.html