



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

## **Basic Lindows Security**

### **GIAC Security Essentials Certification Practical Assignment Version 1.4b Option 1**

**Andrew J Bernoth (27 January 2004)**

## Introduction

Lindows is a commercial operating system (OS), based on Linux. The Lindows Company positions their product as Linux for the Windows or MacOS user. With that in mind, the default Lindows installation configures for ease of use and interoperability so that the average user can install a new Lindows system in a short time, and, with minimum configuration, connect to their existing network.

This paper will explore the standard configuration and show how to make changes to increase the security of a Lindows system by disabling unneeded services, reconfiguring the firewall, installing system updates and running a virus scan.

## Objective

The target audience for this document is a new Lindows user, especially those new to the world of Linux. This document is not a complete Linux hardening guide. Steps in this document are an introduction to security in a Lindows environment. For more detailed Linux security guides see the reference section at the end of this document. If the Lindows system is within a business environment, compare the suggestions in this document with company policies.

Screen captures are from Lindows OS 4.0; however, similar configuration steps should be available in any Lindows version.

This guide assumes the use of a fresh Lindows installation with default settings, and that the Lindows system will connect directly to the Internet, or other untrusted network, with minimal secondary controls. This connection may be a direct dial-up, or a high-speed network without a firewall between the Internet connection and the local network.

This document leaves the more general settings to the user to complete, such as time zone and preferred language.

For a new system installation or a system recovery, the two primary goals are to obtain any system updates and run a virus scan. For either a fresh installation or system recovery, these goals will ensure the final system is not vulnerable to any issues discovered since creation of the OS media. For a system recovery, the virus scan will ensure the system backup did not contain any virus. However, the system could still be vulnerable to exploitation while obtaining the latest OS or virus definition updates. To protect the system while working toward the primary goals, it is important to disable any unneeded services and to reconfigure the firewall to restrict any unwanted access.

Throughout this document, examples from common audit tools (nmap and Nessus) are included to show how the system would appear to a network scan at that step. These examples are included to provide more information to the advanced user.

## Contents

First Time Setup.....	4
Administrator Password .....	5
Add Users .....	6
User Information .....	8
User Password.....	9
Password Properties.....	9
Rename This Computer .....	10
Network Audit Check 1 .....	11
Disabling Non-Essential Services .....	13
Displaying the Services.....	13
Determining the Run Level .....	14
Re-enabling the Services.....	16
Network Audit Check 2 .....	16
Reconfiguring the Firewall .....	17
Network Audit Check 3 .....	21
Running as a Normal User.....	21
System Updates.....	21
Virus Protection.....	24
Conclusion .....	28
Epilogue.....	29
Bibliography .....	30

## First Time Setup

As with any new system or clean OS installation, it is not advisable to connect the computer to any untrusted network (LAN, dial-up or other) before checking the default system settings. By default, Lindows will request IP configuration from any available DHCP server, becoming part of the connected network. If that network is untrusted, the new system could be vulnerable to both viruses and unauthorized access to the system. Often a hacker only requires a short window of opportunity where he or she has access to a system. During this short time, hidden programs can be installed providing access later through methods that may not appear in any log file.

After installing the OS and booting from the hard drive, or, for preinstalled systems, after answering the standard questions and rebooting, the user is presented with the “First Time Setup” window, see Figure 1. This window contains recommendations as well as the license agreement. Be sure to read the license agreement before checking the box indicating your acceptance of the license. As noted earlier, this is a good time to check the local time zone and local time settings.

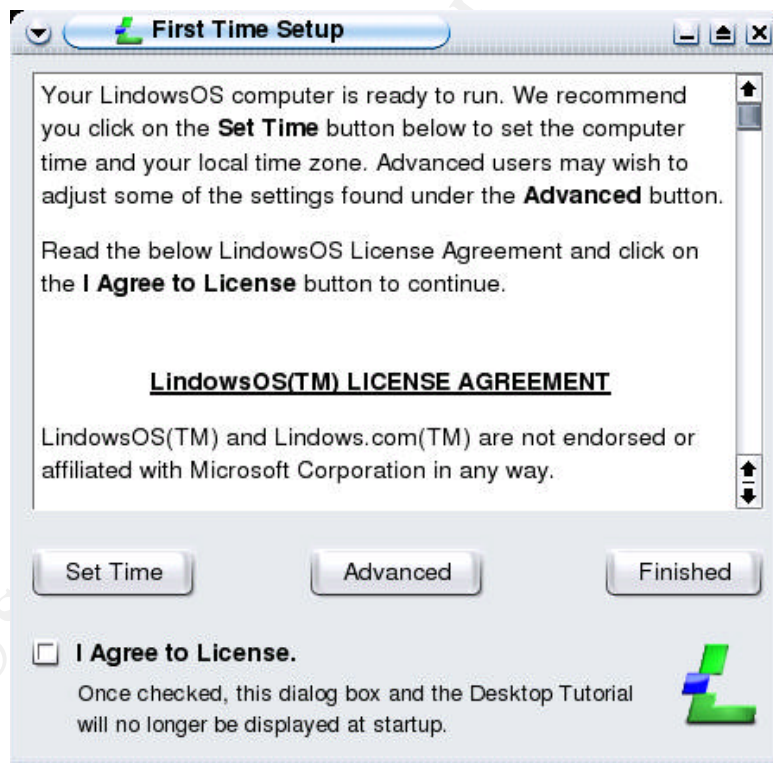
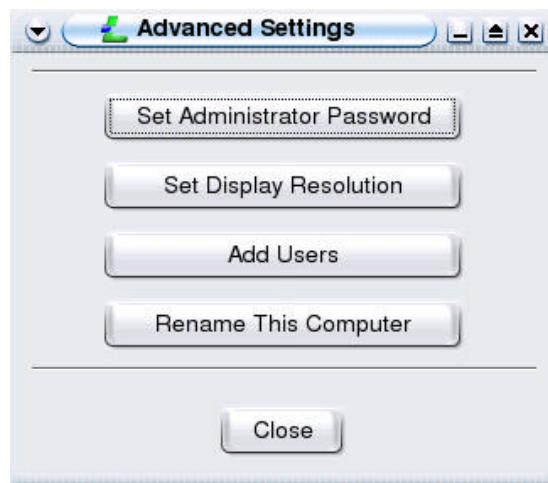


Figure 1 First Time Setup

## Administrator Password

At this point, it is tempting to ignore the “Advanced” button and start using Lindows. However, the system has booted and the current user is *administrator* (Lindows renames the Linux “root” user to “administrator”) without a password. This is the best time to change the administrator password and add other non-administrator users. Selecting the “Advanced” button brings up the “Advanced Settings” window as shown in Figure 2.



**Figure 2 Advanced Settings**

Click on the “Set Administrator Password” button to open the “Change Password” dialog, see Figure 3.

Always establish a strong password for the administrator account. Characteristics of a strong password include<sup>1</sup>:

- At least 8 characters long,
- Contains a combination of alphabetic and non-alphabetic characters,
- Not a single dictionary word,
- Not easily guessed (for example do not use names of family, birthday and favorite resort).

Consider the data stored on the system, what protection it has from untrusted environments, and the strength of the password. For example using a password

---

<sup>1</sup> Ullirch, J., “Windows XP: Surviving the First Day”, (23 November 2003)  
<http://www.sans.org/rr/papers/index.php?id=1298> (18 January 2004)

guessing system that has a decent speed, a password with 8 case-insensitive alphabetic characters could take 24 days to guess, however, a case sensitive password chosen from all printable characters could take 2287 years to guess<sup>2</sup>.



**Figure 3 Change Password**

Enter a strong password for the administrator – the password is not displayed in clear text so it must be verified in both entry fields. Click on “OK” when you have entered the password. If the two entries do not match, an error will advise you and then return you to the password entry dialog to try again. If the passwords do match, you will return to the “Advanced Settings” window, Figure 2.

### **Add Users**

Within most operating systems, the use of the “administrator” as the default user is not recommended. Within the Linux environment, there are tools to allow a user to switch to *root* (administrator) without the need to logout and login as the root user. Mourani states it clearly:

The *root* account has no security restrictions imposed upon it. This means the system assumes you know what you are doing, and will do exactly what you request – *no questions asked*. Therefore, it is easy, with a mistyped command, to wipe out crucial system files. When using this account it is important to be as careful as possible. For security reasons, never log in on your server as *root* unless it is absolutely an instance that necessitates root access.<sup>3</sup>

By logging in as another user, that does not have administrator privileges, any attempts to change the system will cause an error. If a change is required, the user can then use tools such as “sudo” or “su” to increase their authority to change the system. If these do not provide the necessary access permission, as

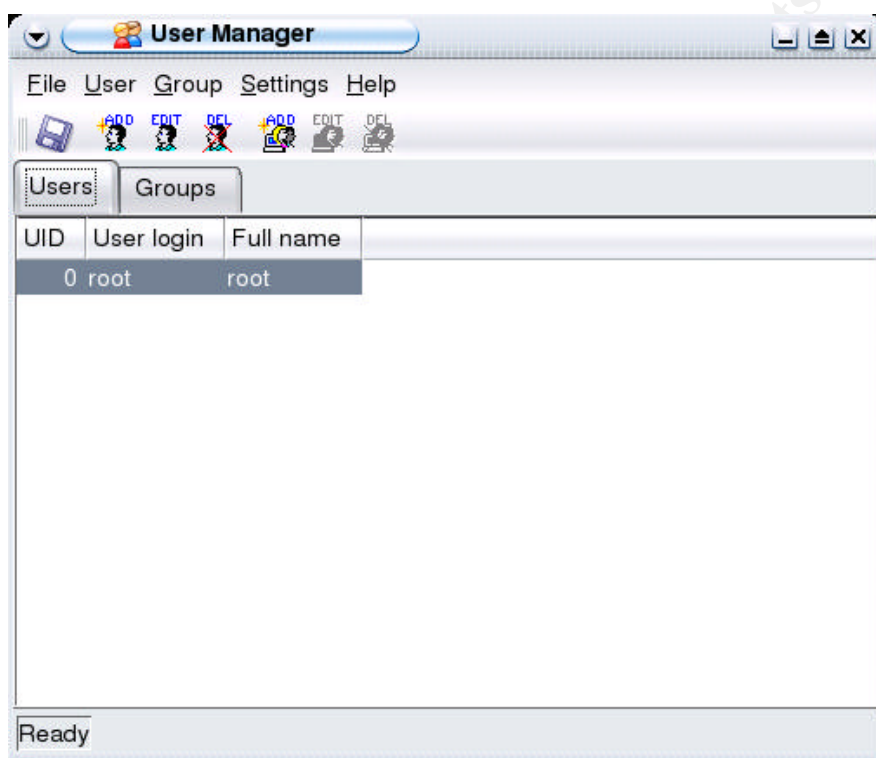
---

<sup>2</sup> LastBit Software. All About Passwords. LastBit Software, (2004).  
<http://lastbit.com/psw.asp>, (18 January 2004)

<sup>3</sup> Mourani, G., “Securing and Optimizing Linux”, (2000).  
<http://www.linuxsecurity.com/docs/Securing-Optimizing-v1.3>

a last resort, login as *root* to make the change. Once the required change is completed, return to the standard user mode. If using *sudo* or *su*, the command “exit” will exit out of the administrator privilege state. If you were required to login as root, then logout, and login as the standard user again.

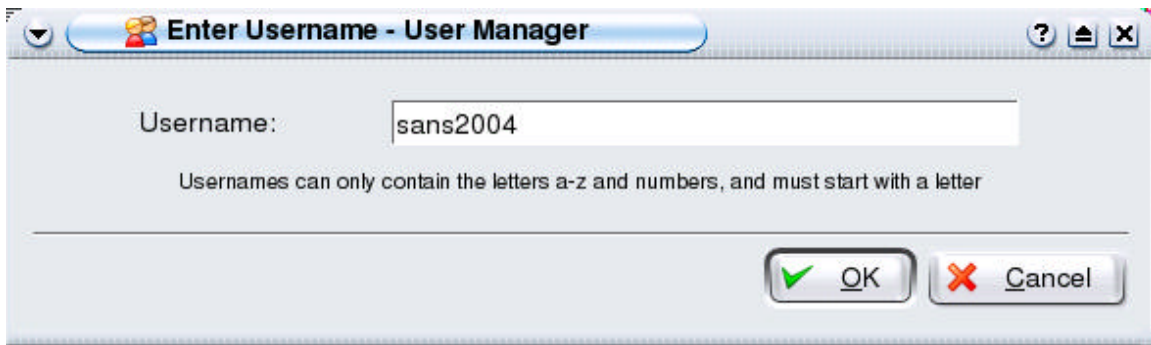
To add a user without administrator privileges, click on the “Add Users” button to open the “User Manager” window shown in Figure 4. The first time this opens, there will only be the “root” user in the list under the “Users” tab.



**Figure 4 User Manager**

The “add” button with only one person depicted in the icon will add a single user. Click on the add user button to display the “Enter Username” dialog shown in Figure 5.

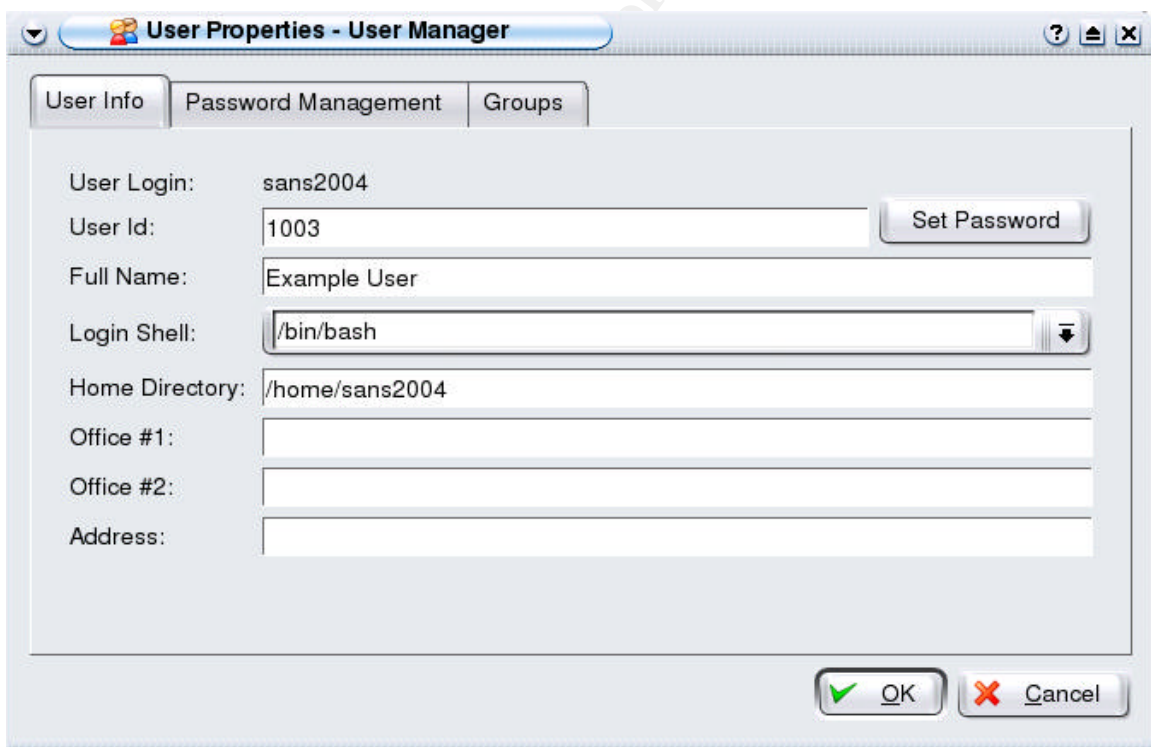




**Figure 5 Enter Username**

### ***User Information***

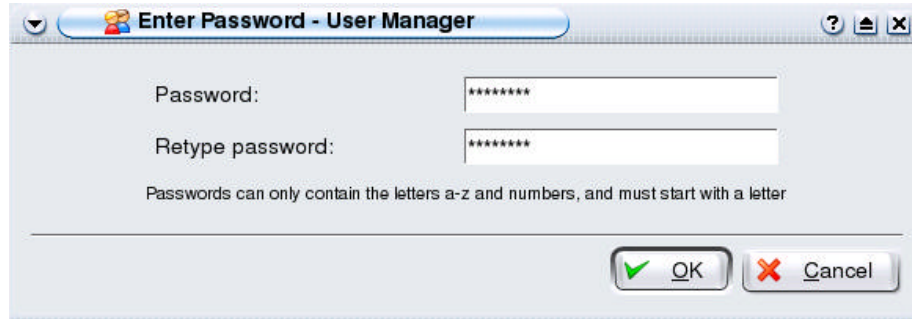
When you click “OK” the “User Properties” dialog is displayed, see Figure 6. Enter the full name of the user and any other data relevant to your environment. The User Id number and Home Directory take default values that are unique for each user, while the Login Shell takes the system default value.



**Figure 6 User Properties**

## ***User Password***

Click on the “Set Password” button to show the “Enter Password” dialog shown in Figure 7. Remember to use a strong password as described earlier. Click on “OK” to set the password, this will return you to the “User Properties” dialog.



**Figure 7 Enter Password**

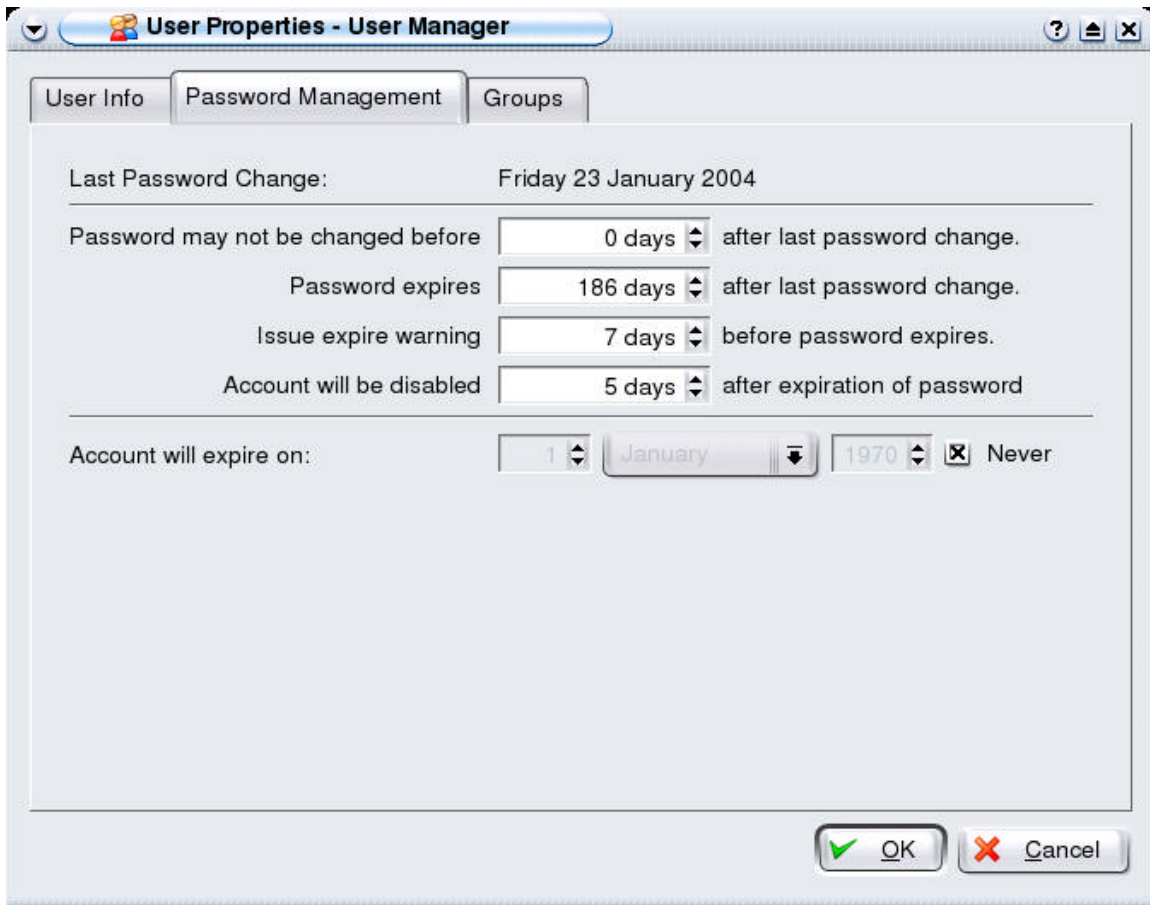
## ***Password Properties***

Before selecting “OK” in the “User Properties” dialog, make sure to confirm the settings on the “Password Management” tab, see Figure 8. The default for the “Password expires” field is almost 90 years, or in other words “never expires”. Adjust the expiration time to a value that matches your needs or corporate security policy.

If you have not considered password expiration before, some suggestions including common considerations would be:

- 30 days – for systems containing sensitive data always connected to the Internet.
- 90 days – for systems containing sensitive data not generally connected to the Internet.
- 186 days – for systems not containing sensitive data and not generally connected to the Internet (or all other systems).

Of course, these may not suit your environment, so consider all threats to your environment and the sensitivity of the data stored on the system when configuring the password expiration. These values can be changed later under the User Manager application.



**Figure 8 Password Management**

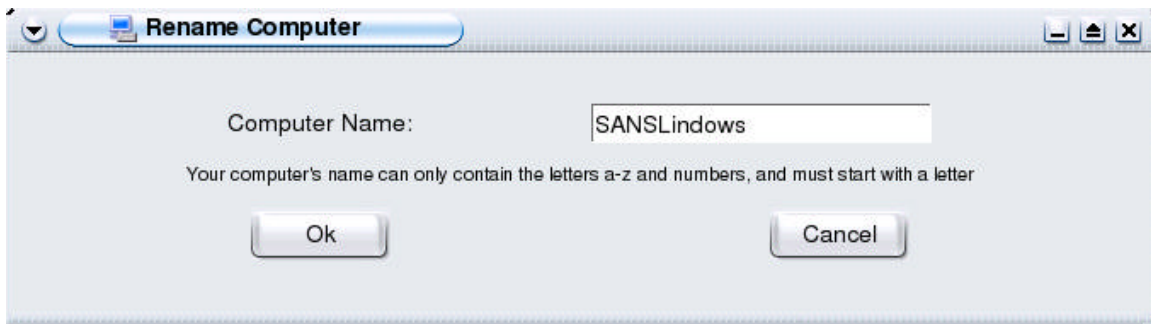
Select the "Groups" tab to ensure the new user is a member of only the groups needed. Keep in mind the system can be configured to allow users to act as administrator with either "sudo" or "su", so the user you intend to use on a daily basis can have a "primary group" of "users".

Click "OK" in the "User Properties" dialog to complete the user configuration. This returns to the "User Manager" screen (Figure 4) where the new user will be displayed in the updated user list.

When all users have been added and secured as required, close the "User Manager" application, this will return you to the "Advanced Settings" window (Figure 2).

### ***Rename This Computer***

Selecting the "Rename This Computer" button from the "Advanced Settings" window opens the "Rename Computer" dialog shown in Figure 9. Enter a name for this computer reflecting your naming scheme. The computer name may be visible to others, so do not use your password, social security number or other personal or sensitive information.



**Figure 9 Rename Computer**

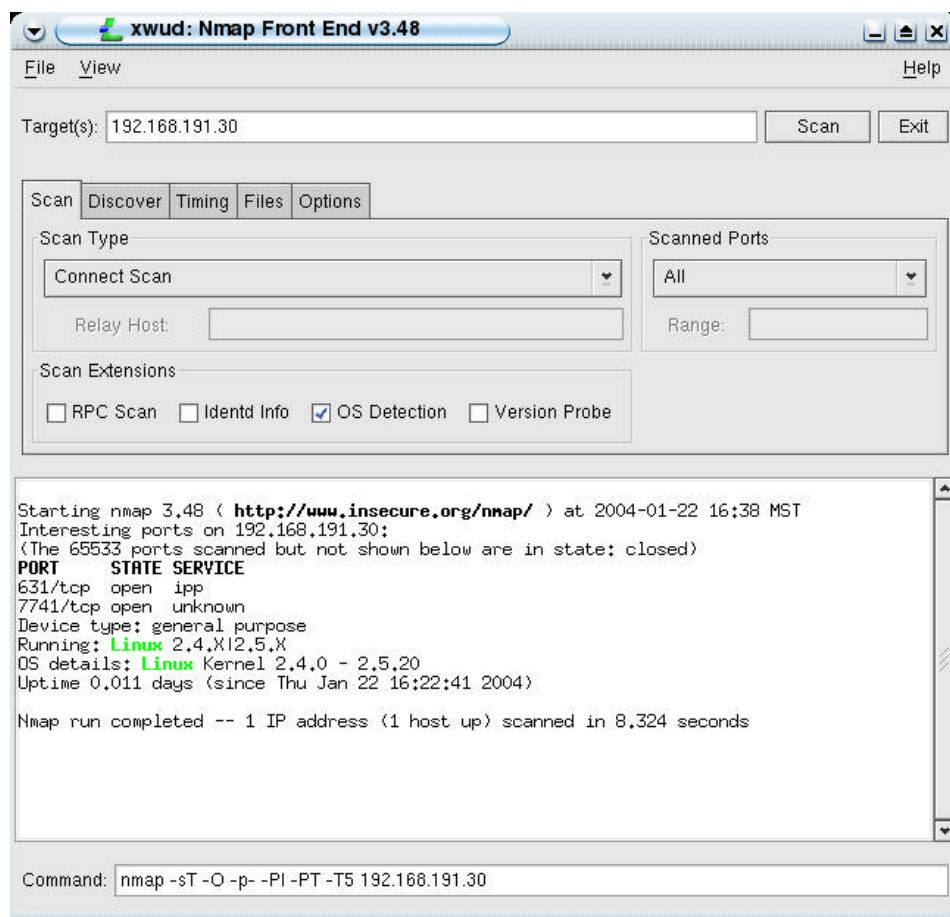
Close the “Advanced Settings” window (Figure 2) and click on “Finished” in the “First Time Setup” window (Figure 1). In Windows 4.0, this opens a desktop tutorial. If you do not need to view this tutorial, pressing <ALT-F4> will close it down, or you can use the tutorial control buttons to close the tutorial.

At this stage, Windows is ready for use and additional configuration changes. As noted earlier, our primary goal is to install any available system updates. So far, we have only made it more difficult for someone to guess administrator passwords or user name and password pairs. To increase system security while obtaining and installing any updates, we still need to disable non-essential services as well as harden the firewall.

## **Network Audit Check 1**

For the purposes of this document, a test system was connected to an isolated network, where all attached devices were trusted. This enabled network-scanning tools to identify how the system would look in a hostile environment. The tools used are *nmap* to scan for services that may be vulnerable, and *nessus* that can also identify known vulnerabilities in open services. Both of these tools are available for Linux and have a GUI front-end available. More information on *nmap* and *nessus* is available in the references at the end of this document.

The first tool, *nmap*, was configured to scan all ports, and the scan was run for all available options (primarily TCP, UDP, and Protocol scans). The *nmap* TCP scan discovered the open TCP ports as well as successfully identified the OS, see Figure 10. The *nmap* UDP scan returned similar results, showing the UDP ports open to the network. Using the information gained from these scans, a person can research potential vulnerabilities for both the OS version, and any services that are open. Such research could assist a malicious user to compromise your system.



**Figure 10 nmap Scan Results with Default Lindows Configuration**

The other tool, nessus, used the default configuration for scanning. The results from the nessus scan showed both the TCP and UDP ports that were active (see Figure 11). Nessus would have discovered all open ports if the configuration was modified to scan all ports rather than the default of well-known ports. Nessus also identified other potential vulnerabilities, such as the one shown below. In most cases, nessus also provided a reference for more information on the vulnerability, as well as suggesting a course of action; in this case “Contact your vendor for a patch”.

Nessus is a very good tool for auditing your environment, which naturally means it is also a great tool for malicious use. For more information on Nessus, see the references at the end of this document.

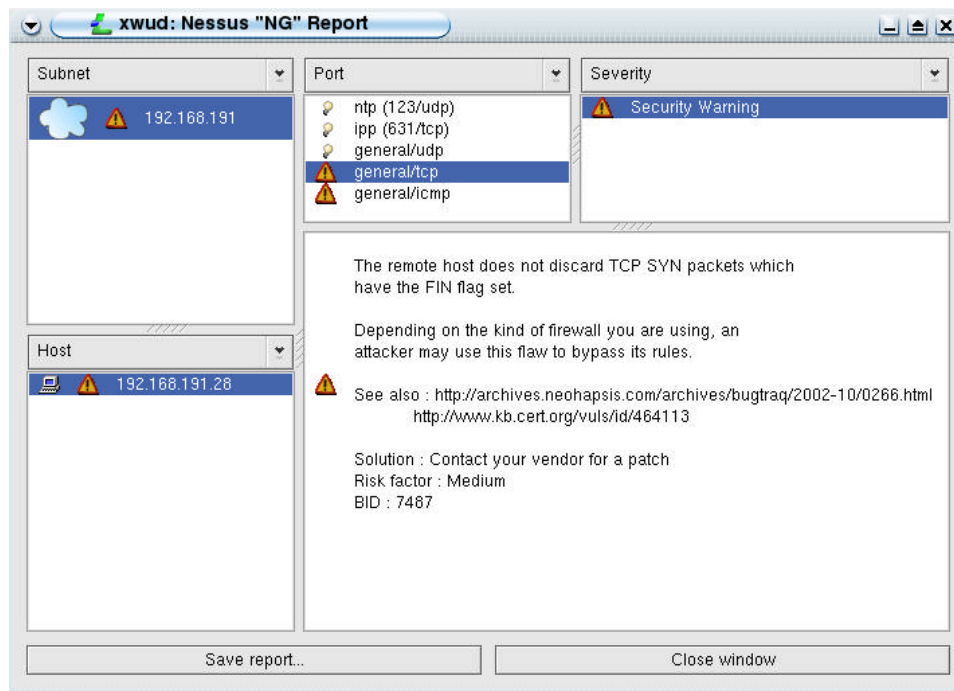


Figure 11 Nessus Default Scan Results

## Disabling Non-Essential Services

Every new system or OS installation will require patches; the problem is, since many of the patches are going to fix security vulnerabilities, the user needs to take care not to put their system at risk while obtaining updates. For this reason, the user should disable all but essential services before connecting to another network to obtain updates.

Open a console window by going to the start "L" in the lower left-hand corner of the screen, select "programs", then "utilities" and then "console". This provides command line access to the system.

### Displaying the Services

At the command prompt, enter "netstat -l | more". This will show the IP services that are actively listening for connections. In the Linux command line, the output of one program can be processed by another program using the "|" key (on most computers hold down the "shift key" while pressing the back-slash "\" key) – this is commonly referred to as "piping".

In this case, the text output of the "netstat" application would scroll over the length of the screen. To display only one screen of data, the "more" command will pause the display at each full screen until the user presses the *space-bar*, then the next screen of data will be displayed, repeating until all the data has been displayed or the user presses "q" to quit the display.

The example test system has 10 listening services, as shown in Figure 12; some applications open more than one service. A quick search of the Internet will show that most of these services have some risk involved, especially if the services are not updated or correctly configured.

The list of listening services includes:

- “ipp” (TCP 631 and UDP 631) is an IP print server,
- TCP 7741 and UDP 7741 which is running LISa or LAN Information Server (see the references for more information on LISa).
- UDP 1024 another port for LISa
- “bootpc” (UDP 68) this is required for obtaining an IP address through DHCP,
- ntp (UDP 123) is a Network Time Protocol server.
- ICMP, also required for LISa

For the primary goal, to install the latest system updates, we are going to disable any unneeded service. Since these services are currently running, they will start again if the system needs to reboot for any reason.

### ***Determining the Run Level***

Linux runs in a number of different possible configurations or levels. To determine the default level, type the command “*runlevel*”. This should provide an output similar to “N 2”, where “N” is the previous run level (“N” indicating there was no previous run level) and the “2” indicating the current run level.



```

Linux Console
Session Edit View Settings Help

SANSWindows:~# netstat -l | more
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 *:ssh                   *:*                     LISTEN
tcp      0      0 *:ipp                   *:*                     LISTEN
tcp      0      0 *:7741                  *:*                     LISTEN
udp      0      0 *:7741                  *:*
udp      0      0 *:bootpc                *:*
udp      0      0 *:ipp                   *:*
udp      0      0 SANSWindows:ntp        *:*
udp      0      0 localhost:ntp           *:*
udp      0      0 *:ntp                   *:*
raw      0      0 *:icmp                  *:*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State       I-Node Path
unix  2      [ ACC ] STREAM    LISTENING   3351  /tmp/.X11-unix/X0
unix  2      [ ACC ] STREAM    LISTENING   4501  /tmp/.ICE-unix/1304
unix  2      [ ACC ] STREAM    LISTENING   4364  /tmp/.ICE-unix/dcop1281
-1074872821
unix  2      [ ACC ] STREAM    LISTENING   4358  /tmp/ksocket-root/kdein
it-:0
unix  2      [ ACC ] STREAM    LISTENING   5203  /tmp/.esd/socket
unix  2      [ ACC ] STREAM    LISTENING   1903  /tmp/.font-unix/fs7100
--More--

```

Figure 12 netstat -l | more

Lindows does not include a GUI application, or even a command line application, to simplify service startup configuration. Therefore, the required configuration changes need to be made in the directory structure. This is done from the console. Only the “administrator” can disable services so they do not automatically start at boot. Since we are currently logged in *root* simply use the console from above.

If you have already logged out of the *root* user, open a console and enter the command:

```
su -
```

This will prompt for the administrator password. Given the correct password for the root user, the command line will now have root privileges until you exit from this instance of root using the “exit” command.

Run level configurations are soft links in a subdirectory specific to the run level; the format is “/etc/rcn.d” where “n” is the numeric value of the run level. From the “runlevel” command earlier, we need to make changes in the “/etc/rc2.d” directory. To do this, first change directory to the relevant run level:

```
cd /etc/rc2.d
```



The command “ls” lists the contents of the directory, and when used with the option “-l” for long description, more details about each file is available.

```
ls -l
```

In the current directory “/etc/init.d”, most of the files will have an “l” in the left most column of the directory listing. This “l” indicated a “soft link” which is the way Linux references a file from another directory without making a copy. The file name will then also display a pointer, “ -> ”, which points to the original file. For example:

```
lrwxrwxrwx 1 root root 13 Jan 22 16:20 S23ntp -> ../init.d/ntp
```

The file name “S23ntp” is a soft link to the original file “../init.d/ntp”, or “/etc/init.d/ntp”. For more on Linux file name conventions see the references at the end of this document.

To disable the services from automatic startup we delete the link. If your system requires the service later, recreating the link will enable the service to run on startup once again.

Since we determined the only service required for our system at this stage is the *bootp* service (to obtain an IP address) we can safely disable the other services.

Enter the following commands to delete the unneeded service links; keep in mind Linux is case sensitive.

```
rm S20cupsys
rm S20lisa
rm S23ntp
```

## ***Re-enabling the Services***

If needed later, the following commands will enable the services.

**Note: DO NOT ENTER THESE COMMANDS NOW.**

```
ln -s ../init.d/cupsys S20cupsys
ln -s ../init.d/lisa S20lisa
ln -s ../init.d/ntp S23ntp
```

## **Network Audit Check 2**

For the purposes of completing this audit checkpoint, we rebooted the test system before executing both nmap and nessus again.

The nmap scan shows all scanned ports are closed on the system see Figure 13. While this means the system does not have any services open, it is still responding to attempts to access any port in the TCP range. Therefore, enabling a service while in this state will allow that service to be accessible from the network. Remember, an authorized user could start a service by either

specifically starting the service or by starting another application that requires the service.

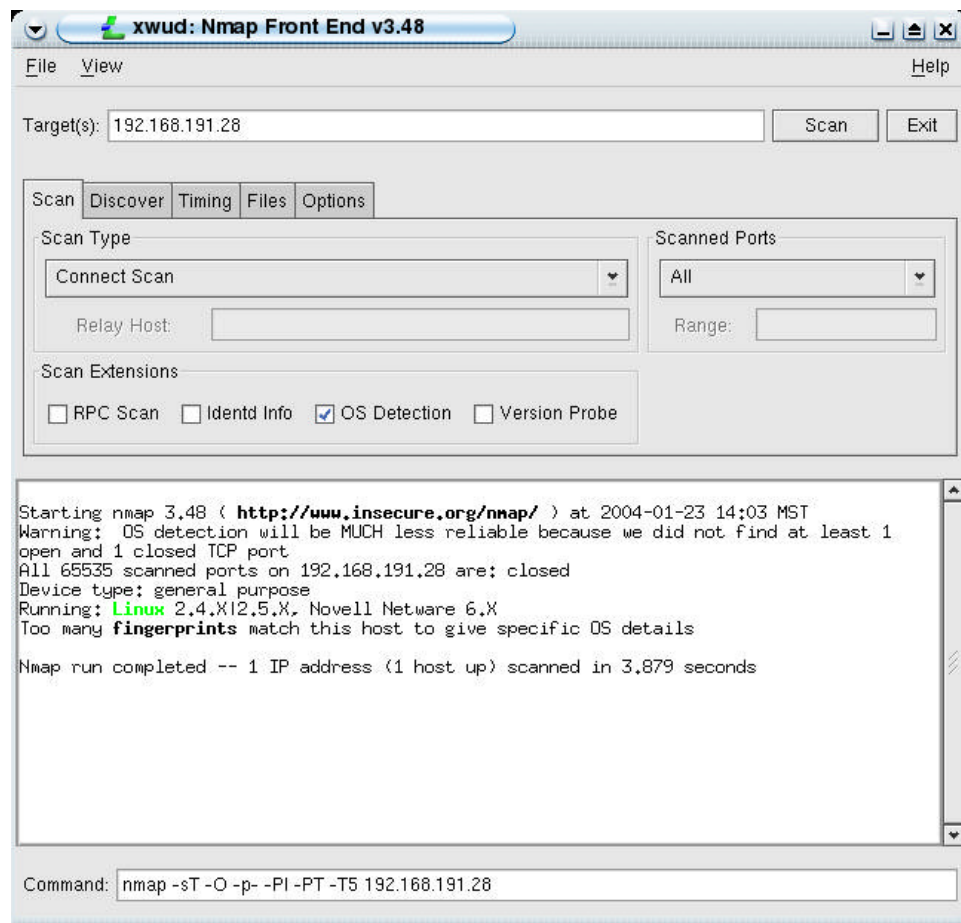


Figure 13 nmap Scan After Disabling Unneeded Services

Nessus showed the ports were closed; otherwise, the results were similar to the original Nessus scan shown in Figure 11.

## Reconfiguring the Firewall

Linux comes preloaded with the Linux IPtables firewall, which is also configured for use in a trusted environment. As mentioned earlier, many default configuration settings are for ease-of-use rather than optimum security. This is common to most operating systems.

Linux does not include a GUI firewall configuration tool, so these commands must be entered on the command line either while the user has root privileges, or logged in as root, as described previously.

While in the console as “administrator”, we need to change the firewall configuration to permit only required connections. Since we want to obtain any

available system updates, the firewall only needs to permit connections initiated from this system.

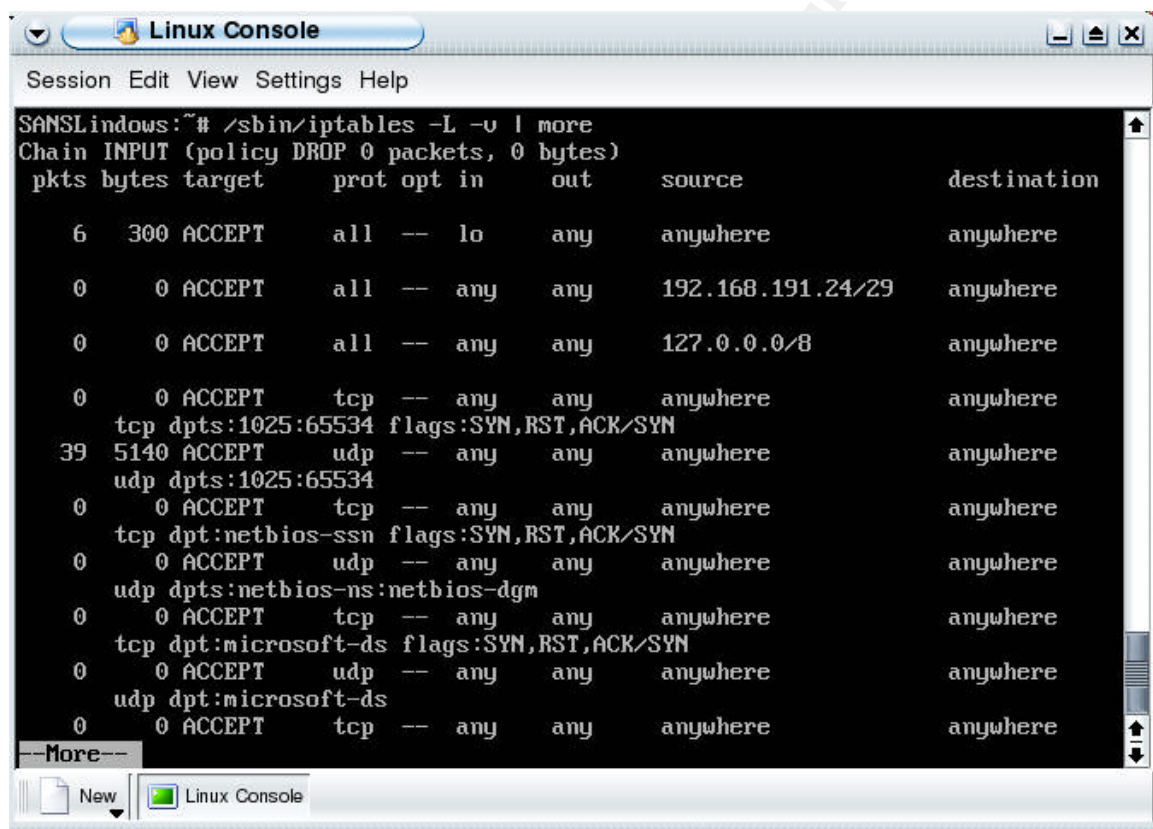
First, change directory to the same directory as the firewall configuration and then backup the configuration with the following commands.

```
cd /etc/init.d
cp lindows_fw lindows_fw.backup
```

To view the current (default) firewall status enter the command,

```
/usr/sbin/iptables -L -v
```

This provides the output as shown in Figure 14.



```
SANS Lindows:~# /sbin/iptables -L -v | more
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source            destination
  6   300 ACCEPT      all  --  lo      any     anywhere          anywhere
  0     0 ACCEPT      all  --  any     any     192.168.191.24/29  anywhere
  0     0 ACCEPT      all  --  any     any     127.0.0.0/8        anywhere
  0     0 ACCEPT      tcp  --  any     any     anywhere          anywhere
tcp dpts:1025:65534 flags:SYN,RST,ACK/SYN
 39  5140 ACCEPT      udp  --  any     any     anywhere          anywhere
udp dpts:1025:65534
  0     0 ACCEPT      tcp  --  any     any     anywhere          anywhere
tcp dpt:netbios-ssn flags:SYN,RST,ACK/SYN
  0     0 ACCEPT      udp  --  any     any     anywhere          anywhere
udp dpts:netbios-ns:netbios-dgm
  0     0 ACCEPT      tcp  --  any     any     anywhere          anywhere
tcp dpt:microsoft-ds flags:SYN,RST,ACK/SYN
  0     0 ACCEPT      udp  --  any     any     anywhere          anywhere
udp dpt:microsoft-ds
  0     0 ACCEPT      tcp  --  any     any     anywhere          anywhere
```

Figure 14 iptables -L -v

For more information on IPTables, and explanation of the output, see the references at the end of this document.

The default firewall configuration trusts all locally connected networks and also trusts any services running on unprivileged ports. Deleting these permissions will hide your system from any port scanners, as well as denying any incoming connections that were not initiated by your system.

Edit the file to look like the listing in Figure 15. If you are familiar with a console editor, edit the `lindows_fw` file with your favorite editor, otherwise now is a good time to logout and then login as “administrator”. To edit the `Lindows_fw` file in a GUI select the start “L” in the lower left-hand corner of the screen, select “programs”, then “Software Development”, and “Advanced Text Editor” for GUI. Then open the file “`/etc/init.d/lindows_fw`” to begin editing.

Save and close the file.

Click on the red button icon on the bottom right of the task bar to open a dialog with four options. Click on the “shutdown” option.

Connect the system to the network connection, or phone line for a dial-up connection.

Power the system up.

© SANS Institute 2004, Author retains full rights

```
#!/bin/sh

function start()
{
    prog=$1
    shift
    args=$*
    start-stop-daemon --start --exec $prog -- $args
}

case "$1" in
start|force-reload|restart)
    echo "Securing Network Connection..."

    # Define network interfaces
    outer_nic="eth1"
    echo "1" > /proc/sys/net/ipv4/ip_dynaddr
    echo "0" > /proc/sys/net/ipv4/ip_forward

    # Flush iptables
    start /sbin/iptables -F

    # Grant access to localhost
    start /sbin/iptables -A INPUT -i lo -p all -j ACCEPT
    start /sbin/iptables -A OUTPUT -o lo -p all -j ACCEPT

    # FORWARD rules
    start /sbin/iptables -P FORWARD DROP

    # Allow passive ftp
    start /sbin/modprobe ip_conntrack_ftp

    start /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

    # Deny everything else
    start /sbin/iptables -P INPUT DROP

    # DoS, syn, etc. protection
    start /sbin/iptables -A FORWARD -p tcp --syn -m --limit 1/s -j ACCEPT
    start /sbin/iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit \
--limit 1/s -j ACCEPT
    start /sbin/iptables -A FORWARD -p icmp --icmp-type echo-request -m limit \
--limit 1/s -j ACCEPT

    #limit logging levels
    start /sbin/iptables -A FORWARD -m limit -j LOG

    echo "Network Connection Secure"
    ;;

stop)
    echo "De-securing Network Connection..."
    echo "1" > /proc/sys/net/ipv4/ip_dynaddr
    echo "0" > /proc/sys/net/ipv4/ip_forward

    # Flush iptables
    start /sbin/iptables -F

    # Grant access to everyone
    start /sbin/iptables -A INPUT -p all -j ACCEPT
    start /sbin/iptables -A OUTPUT -p all -j ACCEPT
    ;;

```

**Figure 15 Listing of lindows\_fw**

## Network Audit Check 3

After the system reboot, we executed the audit tools, nmap and nessus, again. This time, the nmap scans showed all ports as *filtered*, which is how nmap reports that the system was not visible via TCP/IP on the Network. Nessus returned an empty report, indicating the same conclusion – that the system was not visible on the network. This is how we want the system to respond. The only systems outside our control that will know about our system are ones to which we initiate a connection. For all other systems, we will be effectively invisible.

## Running as a Normal User

After rebooting, you are required to select a user (or enter a username) and enter the password for that user. Login as the new user just created that does not have “administrator” privileges.

To perform our updates, we will utilize the program ‘CNR’. CNR is the Lindows “Click-n-Run” application that simplifies system updates as well as the loading of many applications.

Depending on the version of CNR installed, the “Run as root” dialog may be presented requesting you to enter the “administrator” password for the “CNR” application, see Figure 16. The “Run as root” dialog is displayed whenever an application is started that requires more privileges than the current user has.

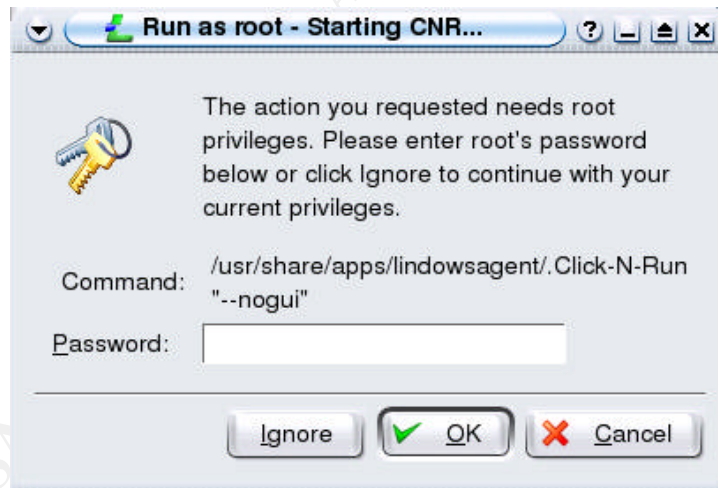


Figure 16 Run as root

## System Updates

As with any OS, occasionally, bugs are found in either the OS or applications. Some bugs may be performance related, others could be security related. One way to maintain a fully patched system is to subscribe to the relevant mailing lists and obtain updates from the sources. Since Lindows is a Linux system, there

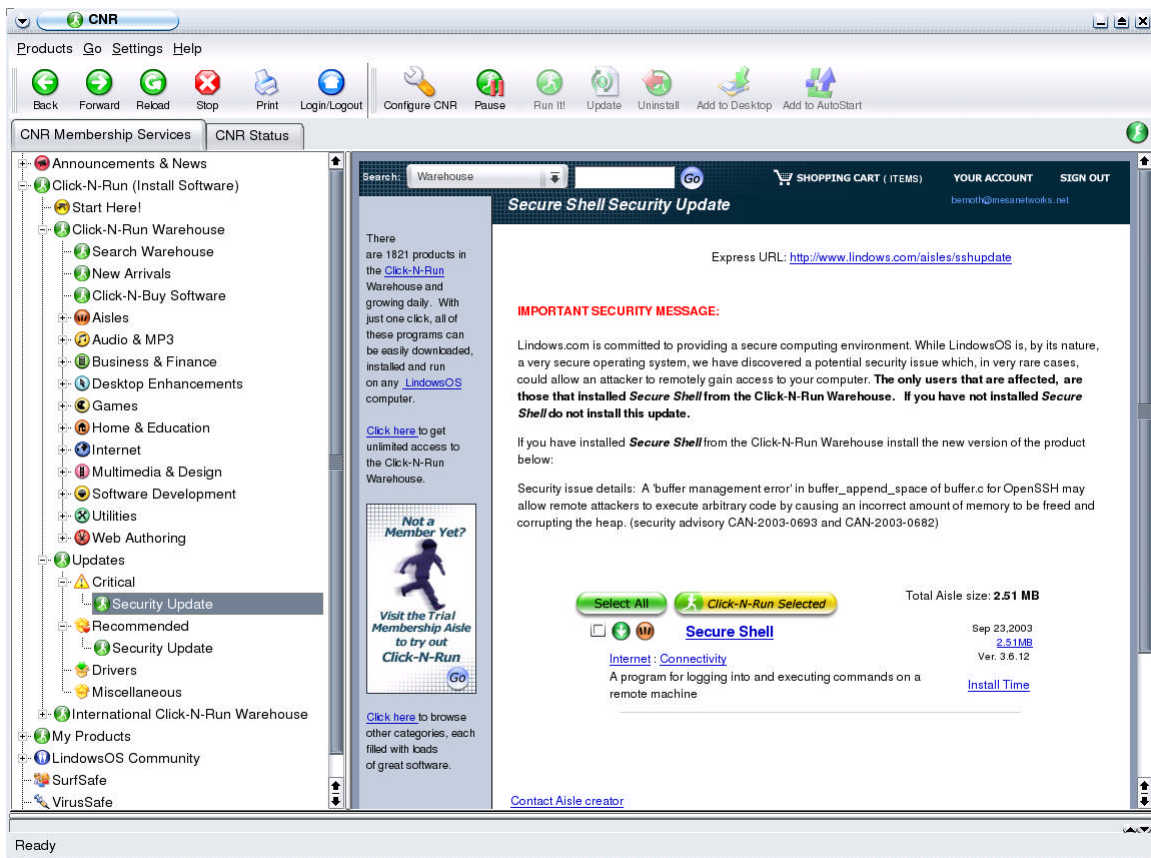
are numerous mailing lists available. However, Lindows is aimed at the Windows user, so the Lindows team created the Click-n-run (CNR) application.

The Click-n-run application checks the system's CNR database against the Lindows click-n-run database for available updates. When an update is required to the CNR application itself, it installs the update and prompts the user to restart CNR. Once CNR connects with the Lindows CNR system, the CNR icon turns green on the task bar. Clicking on this icon restores the CNR application in to view.

To view other application updates, scroll down in the left-hand frame of the "CNR Membership Services" tab to the "Updates" branch of available services. Expanding the "Updates" section shows the different branches of updates available, see Figure 17. Expanding each branch shows the types of updates available for that classification. While all updates are important, the "security updates" section is the first branch to view and identify items to update. In the system evaluated, both the "Critical" and "Recommended Updates" each contained a "security updates" branch.

**Proceed with caution:** the CNR application does not appear to verify that the system it is running on actually requires the updates. For example, the standard installation did not have Secure Shell installed, however as can be seen in Figure 17, CNR is advising that an update is available. Installing any service can introduce vulnerabilities if they are not configured correctly.

Similarly, expanding the "Recommended Updates" branch displays another "security updates" branch. This "security update" section contained updates to the SAMBA application that is included in the default installation. Failing to maintain services to a secure patch level can leave vulnerabilities available to malicious use.



**Figure 17 CNR Updates**

**CAUTION:** Be sure to read the information for each suggested update before installing. In all cases inspected, CNR did include a comment similar to the one shown in this diagram; “The only users that are affected, are those that installed Secure Shell from the Click-N-Run Warehouse. If you have not installed Secure Shell do not install this update.” This warning should not be ignored, as installing unneeded software may decrease the security of your system.

Another consideration with the list of suggested updates is the question “Is this application installed, but I do not use it?” If the application is installed, and you do not plan to uninstall it, the best action is to upgrade the package. While this may appear to be a time consuming decision, it is safer to have all installed applications up-to-date should you decide to either use it, or have another application in use with a dependency on that application.

During the installation process, the status information is updated in the frame below the “CNR Member Services” frame, including both successes and failures. All data displayed here is stored in a log that can be viewed by choosing the “CNR Status” tab, see Figure 18. Green check marks indicate successful processing – whether checking for CNR updates or installing an application. A red “x” indicates a failed process.

Expanding the messages displays summary information as to the actions taken. Part of the summary information includes the “Details” section that expands to



show complete details of the processes. The details of each update or installation are important to view, not only to understand failed installations or updates, but also to confirm that the expected systems were updated.

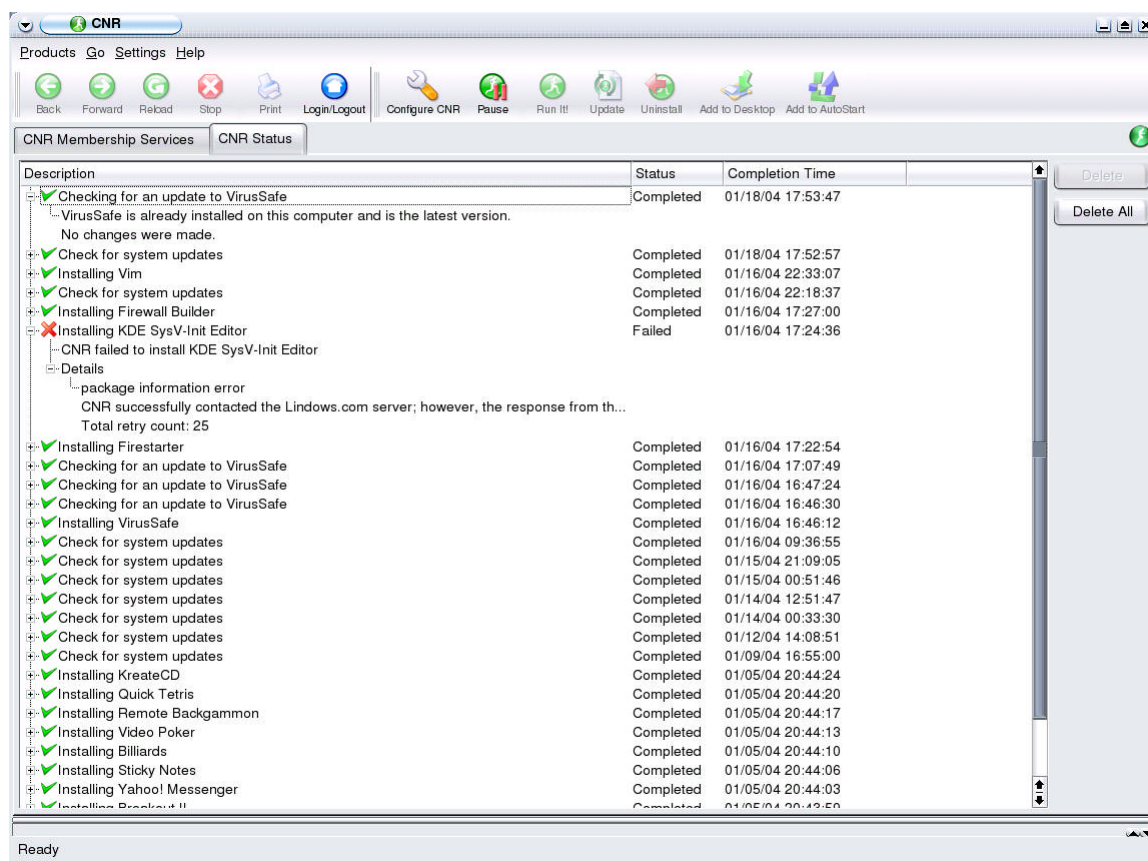


Figure 18 CNR Status

Before exiting CNR, consider activating virus protection.

## Virus Protection

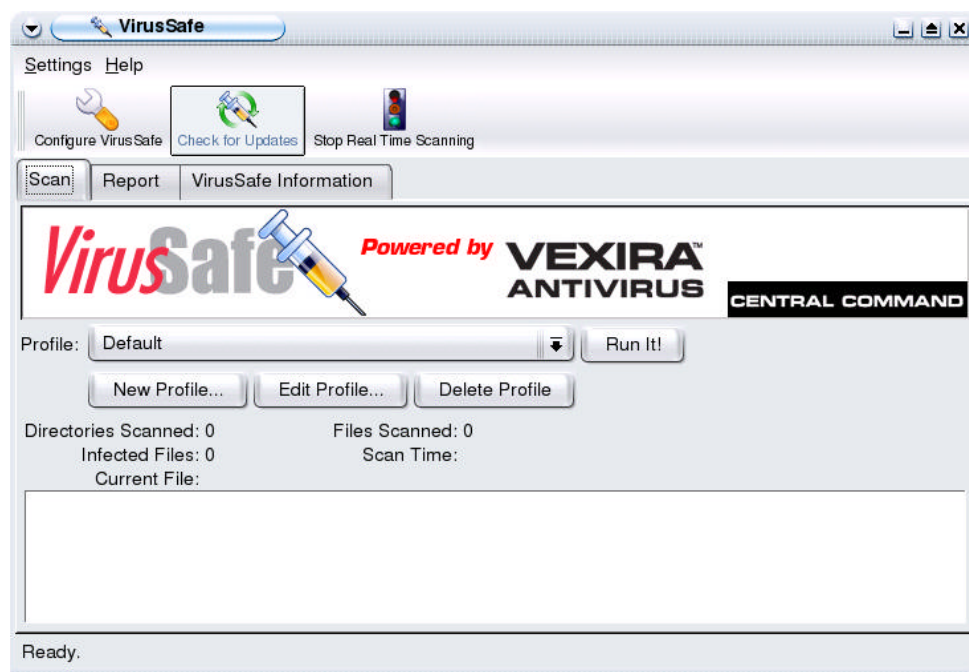
The debate is still raging as to what OS has more viruses, whether the quantity of viruses per OS is proportional to the install base, and many other considerations. The fact is, there are viruses for Linux (see the references for more information). While many steps in this document for Lindows and in other documents on securing Linux provide direction to secure the system, there is always a risk of obtaining a virus that could adversely affect your system. Virus protection is an integral part of system security.

In this document, the more common term “virus” is used for all instances of malicious code, whether a virus, worm, or Trojan.

Lindows comes preloaded with a virus protection application; however, it is not active. The user can search the Internet for a virus protection system that suits their needs, or activate the one that is preloaded and certified to work with

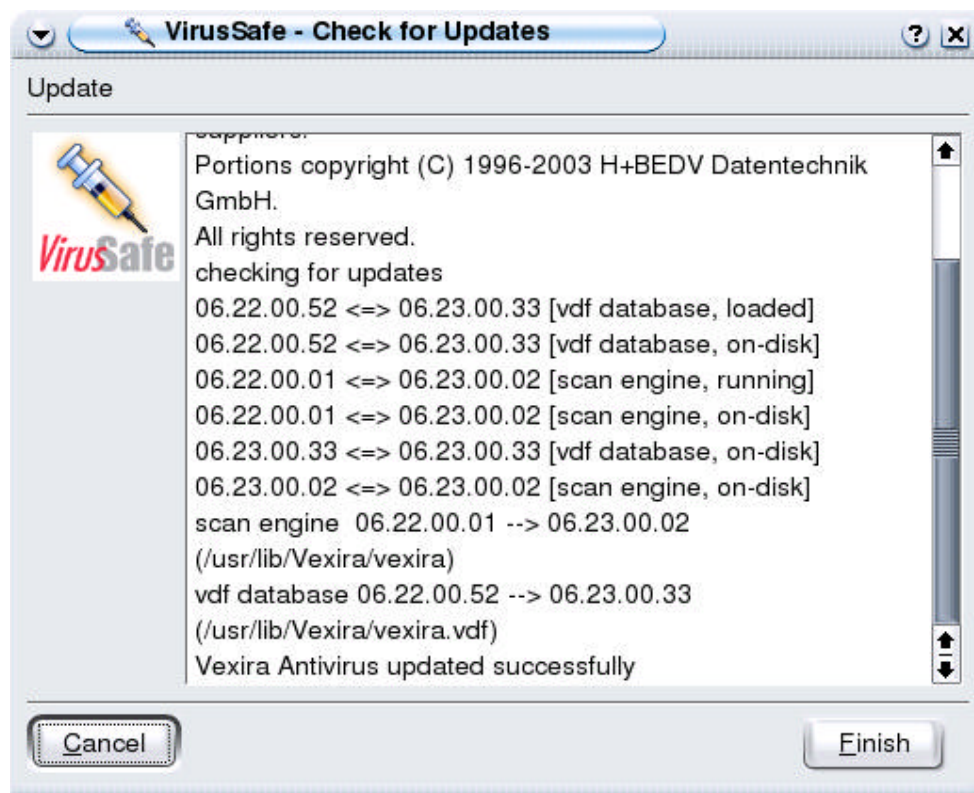
Windows. The only question you should ask yourself is whether to activate the preloaded anti-virus application or find another anti-virus application.

CNR provides an easy activation service for the VirusSafe preloaded application. Once activated, you are presented with the control panel for VirusSafe, see Figure 19. As virus-scanning companies discover new viruses, they update the virus definition databases, so start by checking for any available updates.



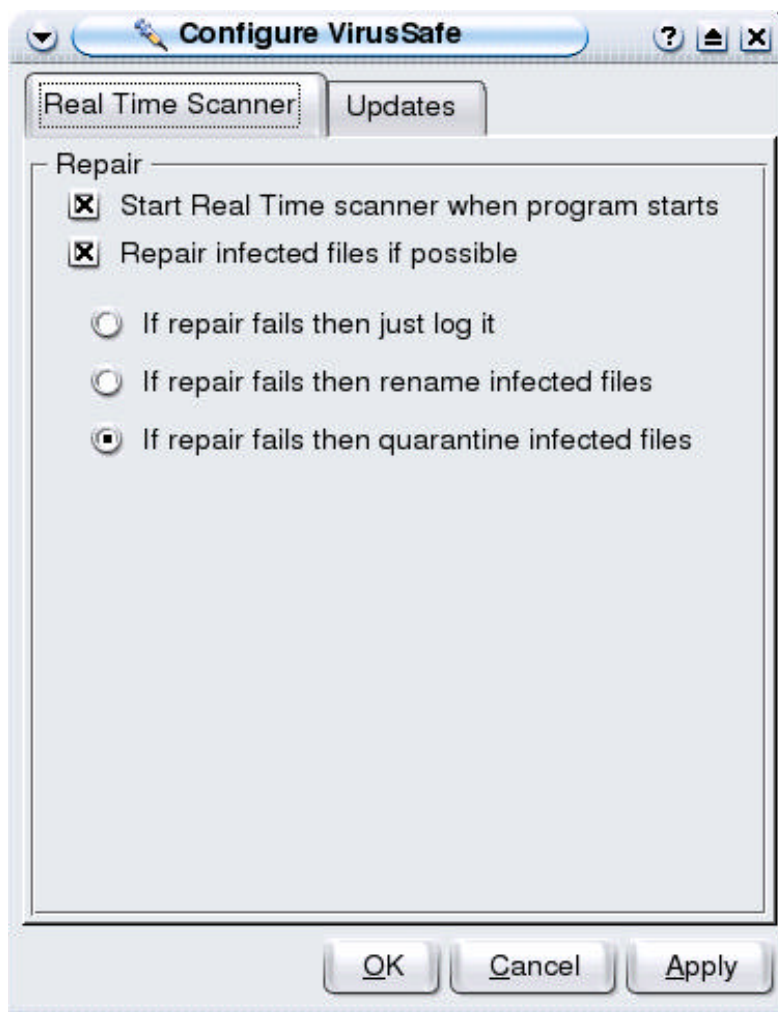
**Figure 19 Virus Safe**

Click on the "Check for Updates" button. This will open another dialog displaying both your current version and any available updated version. Click on "Next" on this dialog to install the update. The dialog will display each step as it executes. When the update is completed ensure the dialog is reporting all updates were successful, see Figure 20.



**Figure 20 Updated Successfully**

When the update has successfully completed, click on the “Finish” button to return to the main VirusSafe screen, Figure 19. Then select the “Configure VirusSafe” button to display the dialog shown in Figure 21. The default configuration uses the “If repair fails then just log it” option. Since the virus scanner will run at a scheduled time, without user interaction, it is better to change the default to one of the other options. If the virus scanner only logs when a file contains a virus that it cannot repair, it could be possible to unknowingly spread a virus. The user would need to check the scan logs for such messages before running any application to avoid spreading a virus. If an infected file is renamed or quarantined, a user cannot execute it accidentally; instead, any attempt to run the original name of the infected file will return an error, which may be just enough to remind you to check the virus scanning logs.



**Figure 21 Configure VirusSafe**

Also, check the configuration in the “Updates” tab to ensure the system will be active when scheduled to check for VirusSafe updates.

Scan your computer by clicking on “Run It!”. When the scan has completed, the results are displayed on the screen, see Figure 22, as well as in the “Reports” tab.

If your virus scanner has found a virus, the value in “Infected Files” as well as the “alerts” statistic will display the number of infected files. Check the report to ensure the virus was either successfully repaired or the infected file was quarantined or renamed. If a repair was not successful, check with the company that wrote the virus scanner, as to their suggested action with the particular virus found. Then decide whether the infected file is required. If the file is not required, the simple answer is to delete the infected file, then reboot and run another scan to ensure no trace of the virus remains.

If the file is required, determine how best to deal with the infection. Options would include:

- Wait for an update to the virus scanning application that can repair the infection, however, this may take some time.
- Delete the file or application and reinstall from a trusted, non-infected source.
- Restore the file, or system, from a non-infected backup. If this is your choice, remember to run the scan again to ensure the file is clean. Remember the virus signature may have been part of the recent update to the known virus database.

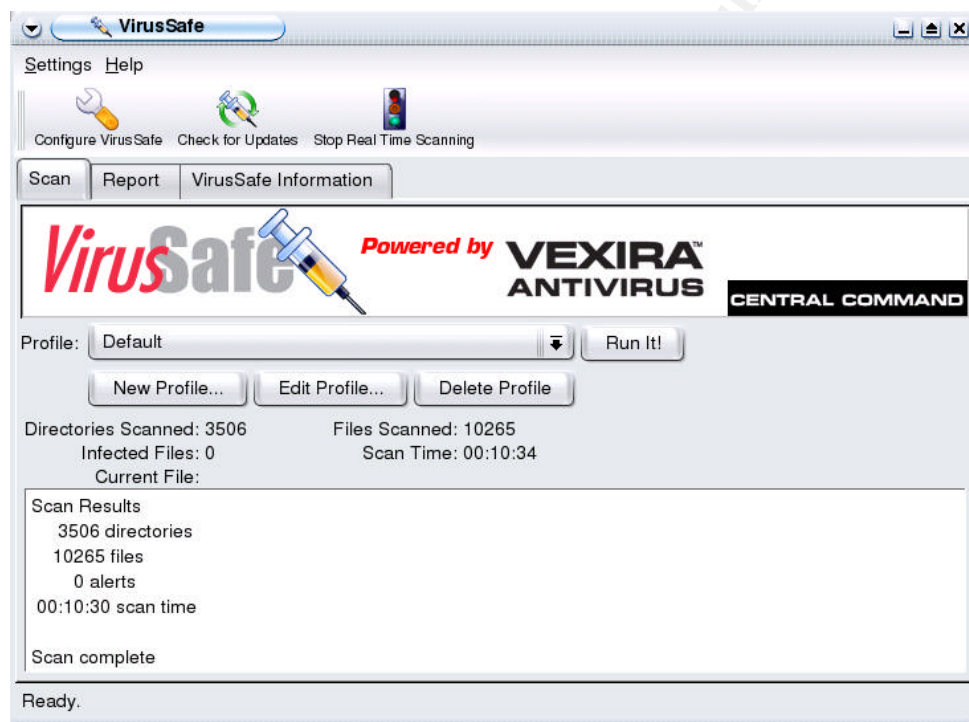


Figure 22 Clean Scan

## Conclusion

At this point, we have successfully hardened your system by:

- Disabling unneeded applications or services.
- Reconfiguring the firewall to deny any inbound initiations.
- Installation of system updates, especially those related to security.
- Installation and execution of virus protection software.

While this makes your system more secure, it is important not to become complacent as new vulnerabilities are identified on a regular basis. You will probably also be installing software, and you should be aware of the possibility of Trojan software that could be included with the package, especially if the package is acquired from an untrusted source.

Finally, to maintain a secure environment, the user should stay informed about vulnerability issues by subscribing to vulnerability publication services such as the SANS newsletter.

## Epilogue

In preparing this document, the author tested both Firestarter and Firewall Builder to simplify firewall configuration. However, neither application simplified the processes to the level required for the intended audience. Firestarter is a Windows tested application; however it required running as root to configure, and was not able to prompt for the root password. Firewall Builder required more configuration and other applications to operate correctly – it is designed for a more experienced firewall administrator.



## Bibliography

Lindows, "What is LindowsOS", (2004)

[http://www.lindows.com/lindows\\_sales\\_intro.php](http://www.lindows.com/lindows_sales_intro.php) (18 January 2004)

Lindows, "What is CNR?", (2004)

[http://www.lindows.com/products\\_clicknrun\\_whatism.php](http://www.lindows.com/products_clicknrun_whatism.php) (18 January 2004)

Andreasson, O., "Iptables Tutorial 1.1.19", (24 April 2003)

<http://iptables-tutorial.frozentux.net/chunkyhtml/index.html> (18 January 2004)

YoLinux, "Using Linux and iptables / ipchains to set up an internet gateway / firewall / router for home or office", (2003)

<http://www.yolinux.com/TUTORIALS/LinuxTutorialIptablesNetworkGateway.html>  
(18 January 2004)

Lindows, "What is VirusSafe", 2004

[http://www.lindows.com/products\\_virusafe\\_whatism.php](http://www.lindows.com/products_virusafe_whatism.php) (18 January 2004)

Central Command, "Vexira Antivirus for Linux Workstation",

[http://www.centralcommand.com/linux\\_workstationcomplete.html](http://www.centralcommand.com/linux_workstationcomplete.html) (18 January 2004)

Luz-Romero, P., "Secure OS Environments for Linux", (14 April 2003)

<http://www.sans.org/rr/papers/32/1083.pdf> (18 January 2004)

Junnonen, T., "Firestarter: Firewalls made easy", (17 August 2003)

<http://firestarter.sourceforge.net/manual/introduction.php> (18 January 2004)

Lindows, "Firestarter Details", (2004)

<http://www.lindows.com/firestarter> (18 January 2004)

NetCitadel, "Firewall Builder: About", (1 October 2003)

[http://www.fwbuilder.org/archives/cat\\_about.html](http://www.fwbuilder.org/archives/cat_about.html) (18 January 2004)

NetCitadel, "Firewall Builder: man\_fwbuilder", (1 September 2003)

[http://www.fwbuilder.org/archives/cat\\_man\\_fwbuilder.html](http://www.fwbuilder.org/archives/cat_man_fwbuilder.html) (18 January 2004)

Lindows, "Firewall Builder Details", (2004)

<http://www.lindows.com/fwbuilder> (18 January 2004)

Garrels, M., "General overview of the Linux file system", (1 January 2004)

[http://www.tldp.org/LDP/intro-linux/html/sect\\_03\\_01.html](http://www.tldp.org/LDP/intro-linux/html/sect_03_01.html) (23 January 2004)

Fyodor, "Nmap Network Security Scanner Man Page", (2004)

[http://www.insecure.org/nmap/data/nmap\\_manpage.html](http://www.insecure.org/nmap/data/nmap_manpage.html) (27 January 2004)

Nessus Project, “nessusd man page”, (February 2003)  
<http://www.nessus.org/doc/nessusd.html> (27 January 2004)

Nessus Project, “nessus man page”, (February 2003)  
<http://www.nessus.org/doc/nessus.html> (27 January 2004)

SANS, “Computer Security Newsletters”, (2002 – 2004)  
<http://www.sans.org/newsletters/> (27 January 2004)

Ullirch, J., “Windows XP: Surviving the First Day”, (23 November 2003)  
<http://www.sans.org/rr/papers/index.php?id=1298> (18 January 2004)

LastBit Software. All About Passwords. LastBit Software, (2004).  
<http://lastbit.com/psw.asp>, (18 January 2004)

Mourani, G., “Securing and Optimizing Linux”, (2000).  
<http://www.linuxsecurity.com/docs/Securing-Optimizing-v1.3>

© SANS Institute 2004, Author retains full rights.