



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>

Just give them Administrator rights that will allow them to run our software!

Bill Shaffer
May 18, 2002
Version 1.3

Introduction:

Like most IT Departments today, my IT Department gets nervous when a software manufacturer states you need to be an administrator of the local machine in order to run their program on Windows 2000 Professional. You see, my IT Department supports a K-12 Public School District. You can only imagine what would happen if we had to make a user a local administrator of Windows workstations just so students could successfully execute the software package just to learn to type.

With this paper I will explain to you how a program from Winternals called Monitoring Tools [2] can assist you in trying to eliminate the requirement of making a user a local administrator, while still allowing the user to run the program. First, this paper will explain some basic steps in using the Monitoring Tools and secondly, the paper will explain how I use the Monitoring Tools to get around the software manufactures statement of "The user has to be an Administrator to run this program on Windows 2000". These tools will not work for all programs but has worked for a majority of the software programs in our District that have stated "The user has to have Administrative rights to run this program on Windows 2000".

Software Security:

Some software manufacturers have taken the time to look into the security side of running their software on Windows 2000, while others have just stated that their software is compatible with Windows 2000 when the user is granted local administrative right. This can cause a real security issue within an organization if an employee or student has to be granted an elevation in user rights and access to a workstation just so their program will run.

[4] "At Microsoft, they always go for functionality over security," said Gary McGraw, vice president of corporate technology at Reliable Software Technologies. "That's what the marketplace wants, because the marketplace isn't very educated about security. It's easy to sell products to people who are ignorant. The customers' No.1 job isn't security, it's getting the job done."

[4] According to Scott Culp, a program manager with Microsoft's security response center "As a general rule, if you want higher security, you're going to take a bit of the cost in not being quite as easy to use. We provide features in all our products to let you decide where that balance is for you."

[3] Since September 11th there have been many concerns about creating laws that would deal with the question of, should software manufacturers who build their programs for functionality instead of security be held liable for damages caused by the use of their products? There is a report that was released by the US National Academy of Sciences (NAS) that will probably be passed to the US Congress for debate that recommends that the US Government should consider amend laws so that software makers can be held liable if their products put the public and businesses at risk. "Possible options include steps that would increase the exposure of software and system vendors and system operators to liability for system breaches," wrote the authors of the report."

A typical Insider Attack Scenario:

Shortly after school starts on Tuesday, a student walks out of the Principal's office, down the hall back to his typing class. After being seated in his chair in total disgust, thinking about the detention he just received for cheating on a programming test he took on Monday. This student decides to try and payback the student that turned him in. Being a computer geek he decides to see if he can use his Local Administrator rights (granted to him because of the typing program) to get back at the student.

This type of scenario is just one example of what could happen in my organization. Other scenarios could be an employee getting mad at another employee for getting the job he/she applied for. Or what if an employee wanted to find out personal information on another employee or worse yet a student! Since most employees/students already have legitimate accounts on the network this gives the attacker an easy and sometimes hidden way to attack. Also with high bandwidth being available to home users these attackers can attack from their homes and also from their workstations. Although the user was attacking the network from home I would consider this attack to be from the inside because the user has the right to use the network. While most network administrators and organizations are so increasingly worried about being attacked from the Internet, there are less security measures in place to help with these insider attacks.

Insider Attacks:

An insider attack usually refers to an attack that comes from inside your network or from its private side. Remember, these attacks are from someone who has an account and is authorized to use your network. Insider attacks are becoming more common and more damaging because employees are becoming more familiar with their computers and network resources in general. Some insider attacks are not committed on purpose they are done because an employee or student is just wondering through your network to see what is out there and are getting into areas that are not locked down by the administrators in charge of the network and often this is due to an oversight. On the other hand, there are the insider attacks that happen because an employee or student wants to test his/her hacking skills on a restricted network. Sometimes these types of insider attacks are done to cause havoc on your networks, or are done to just see what they can find out and other times for personal gain and/or publicity. The following are some of the documented high-profile internal IT security breaches [5]:

- **1985** A brokerage firm clerk alters computer records and changes the ownership and the price of 1,700 shares of Loren Industries stock

- **1989** A former employee of Southeastern Color Lithographs Inc. destroys billing and account information worth \$400,000.
- **1997** A temporary employee working as a computer technician at Forbes magazine is charged with crashing the company's network and causing more than \$100,000 in damage.

If we take a look at these insider attacks, we can ask ourselves could these have been prevented. If we take a look at the 1985 incident did the clerk really need to have access to this vital information dealing with the company's stocks? In the 1989 incident if the former employee's account would have been deleted or at least disabled could he have destroyed the account information? And finally in the 1997 incident the temporary computer technician was fired and then three day later the attack happened. It was believed the technician used someone else's password to attack the network. Could this have been prevented with a strong password policy for all users to follow or even an email sent to all the employees advising them to change their password if they had given them out to this technician?

The following is a chart dealing with some of the ways an administrator could help prevent insider attacks like the ones just mentioned:

[6] **Preventing Cybersabotage**

1. Act, don't react. Establish a reliable system for assigning access rights for critical company data resources. **1985 Incident?**
2. Identify dormant user IDs and orphaned accounts. **1989 Incident?**
3. Automate communications among IT, human resources and other departments. Link all who are responsible for granting access rights within departments. **1997 Incident?**
4. Define "need to know." You can't assume that everybody should have access to everything. **1985 Incident?**
5. Don't forget the sharing factor. Passwords get passed around. **1997 Incident?**
6. Reset passwords regularly.
7. Make nondisclosure policies routine. This contract should be brought to the attention of employees and business partners once a year.
8. Suspend terminated IDs. **1989 Incident?**
9. Reconcile active IDs with reality.
10. Operate out of opportunity rather than fear.

According to the annual 2001 CPI/FBI survey, 59% of companies surveyed said they have had one or more attacks reported internally. Almost 8% of these companies reported 60 or more internal incidents. While the most frequent attacks are coming from the Internet most of the damaging attacks come from deliberate internal attacks. Respondents detected a wide range of attacks and abuses. Here are some examples of attacks and abuses [7]:

- Forty percent detected system penetration from the outside.

- Forty percent detected denial of service attacks.
- Seventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).
- Eighty-five percent detected computer viruses.
- For the fourth year, we asked some questions about electronic commerce over the Internet. Here are some of the results:
- Ninety-eight percent of respondents have WWW sites.
- Fifty-two percent conduct electronic commerce on their sites.
- Thirty-eight percent suffered unauthorized access or misuse on their Web sites within the last twelve months. Twenty-one percent said that they didn't know if there had been unauthorized access or misuse.
- Twenty-five percent of those acknowledging attacks reported from two to five incidents. Thirty-nine percent reported ten or more incidents.
- Seventy percent of those attacked reported vandalism (only 64% in 2000).
- Fifty-five percent reported denial of service (only 60% in 2000).
- Twelve percent reported theft of transaction information.
- Six percent reported financial fraud (only 3% in 2000).

Winternals Monitoring Tools:

The Monitoring Tools include two different pieces of software, one component for monitoring the registry and one for monitoring file access. Although these tools are often used by programmers, I use them to see what files the user is trying to access that they do not have local rights to. Filemon and Regmon allow you to monitor all file system and registry activity on the local workstation as well as a remote workstation that is accessible via TCP/IP. I run this diagnostic software remotely as an administrator and run the student/user problem program as a normal user. Then when I have to change the access rights to a file or the registry I authenticate to the workstation/domain as an administrator of the local workstation. I do not recommend installing these tools on the user's workstation you want to monitor since you can monitor stations over your network. Also, if you load this on the station you want to monitor you will not be able to see what files the program (running under a normal user) will have access denied to since the monitoring tools have to be run with administrative rights. An easy way to run the Monitoring Tools is to load them on a laptop so you can run the tools from anywhere you can connect to the network.

[1] If Filemon or Regmon are run on a Windows NT/2000 station, Filemon.exe or Regmon.exe must be located on a non-network drive that you have administrative rights to. The administrative rights must be granted for the local station as well as the remote station. On windows NT/2000 the client portion of Filemon and Regmon will be installed automatically. The client portion will also be uninstalled from the remote station when you exit the monitoring program.



Steps I use to run the Monitoring Tools:

Here are the steps that I follow to see if the software program will not run because of file or registry access problems. An easy way to tell if there are access problems is to logon

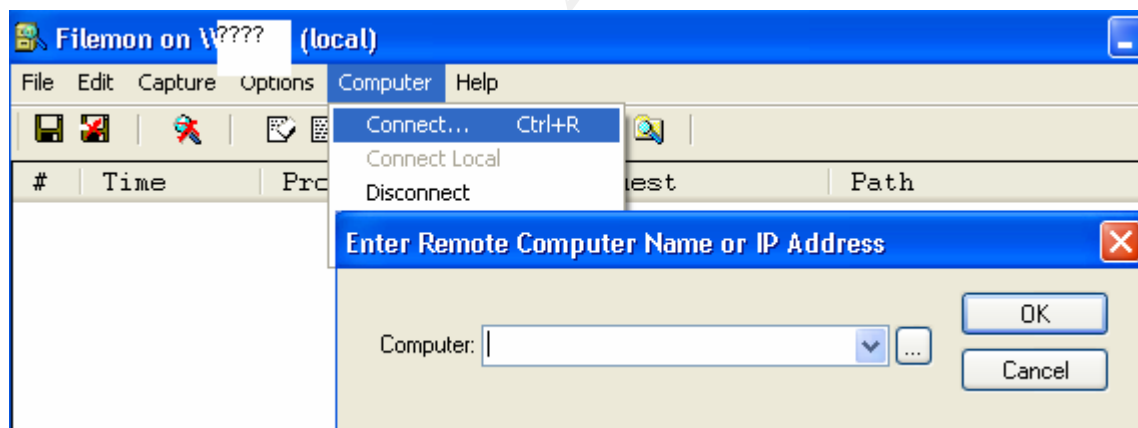
as an Administrator and see if the program will run ok. Now remember just because it runs ok for the Administrator does not always mean you can open files or the registry on that station to make it work for a normal user. I have ran into problems with some programs that would not run even after opening all the files that generated access denied errors and all the registry keys that generated access denied error as well.

The following scenario I will be using is where I am sitting next to the problem station and have with my laptop running the Monitoring Tools. The ideal situation would be to install this software on a test station in case this process does not work, that way you won't have to go back and lock the files or registry keys you just opened. There is another scenario where I have been called by a support technician in which he will logon the problem station as a normal user and I will run the monitoring tools from my desktop.

Step 1:

When Filemon or Regmon is first started it will start monitoring the local system. To stop the monitoring of the local station simply click on the Magnify Glass  on the toolbar. This will change to a Magnify Glass with a red X through it . I stop the monitoring of my station since I want to monitor a remote station.

To remotely monitor a station on my network I simply click on the Computer menu and then press the Connect button. Here I can browse to the computer I want to monitor or if I already know the name of the station I can just simply type in the name and click on OK.



After the connection is made I will receive a message stating "Filemon made a successful connection with computer name"



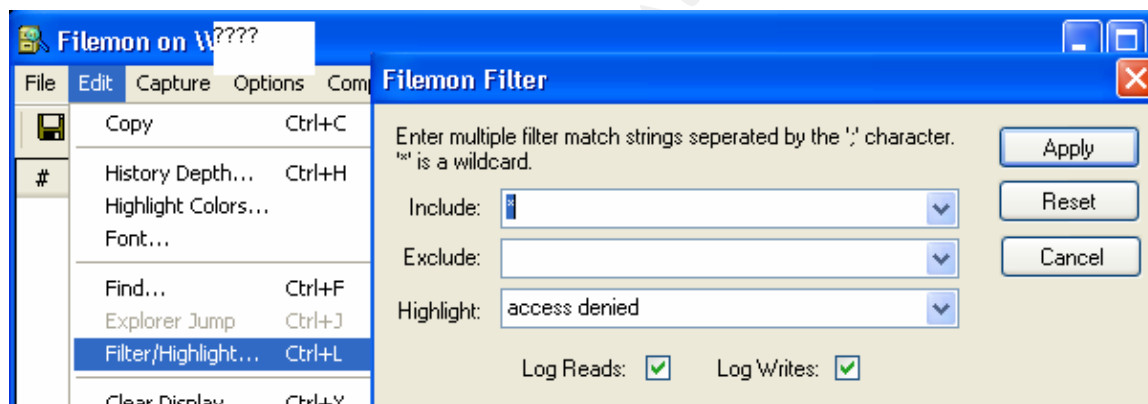
When a connection is made to the remote station a new capture screen is created. This can be seen by looking at the window title bar of the new capture screen; here I will see the name of the computer I just attached to.

Step 2


Once I have made a connection with the remote station I logon that station as a normal user and get to the point where all I have to do is click on the program.exe to start it. By this I mean if the only way to start the program is by going to Start > programs > program.exe then I do all of that before I start monitoring the station. I do this because as you will see there is a lot of information that these Monitoring Tools will capture.

Step 3

On my laptop I will make sure that under the Edit > Filter/Highlight > and in the include box there is an * and in the Highlight box there is access denied. What this will do is highlight all the access denied portions on the output log. These are the only entries I am interested in. All the other entries are what a programmer would need to see. This makes it very nice since some programs I have monitored produced anywhere from 1000 to 4000 lines of entries.




Step 4

On my laptop I will then start monitoring the remote station. This is done by simply clicking on the Magnify Glass with the red X through it .

Step 5

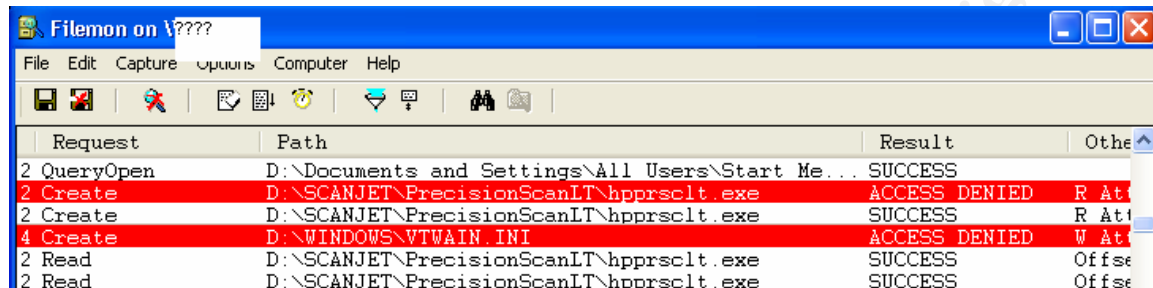
I will then start the program on the remote station and wait for the error message to show up. I will not do anything else on the remote station like close out the error message because this will cause unwanted data being captured by the monitoring station.

Step 6

I will then go back to my laptop and wait for the monitoring data to slow down to the point I believe it is basically done. You will be able to notice when that main part of the capture is done. I will then click on the Magnify Glass  to stop monitoring the remote station.

Step 7

I will then look through the data for the highlighted line that will show me the files or folders that the user needs access to but received access denied. Not only will these highlighted entries show you the file names but you will also see the complete path to the file. Here we can see that two of the files this user was not able to access were hpprsclt.exe and vtwain.ini.



The screenshot shows a window titled "Filemon on V????". It has a menu bar with "File", "Edit", "Capture", "Options", "Computer", and "Help". Below the menu bar is a toolbar with various icons. The main area contains a table with four columns: "Request", "Path", "Result", and "Other". The table lists several file requests, with two highlighted in red: "2 Create" for "D:\SCANJET\PrecisionScanLT\hpprsclt.exe" and "4 Create" for "D:\WINDOWS\VTWAIN.INI", both resulting in "ACCESS DENIED".

Request	Path	Result	Other
2 QueryOpen	D:\Documents and Settings\All Users\Start Me...	SUCCESS	
2 Create	D:\SCANJET\PrecisionScanLT\hpprsclt.exe	ACCESS DENIED	R Att
2 Create	D:\SCANJET\PrecisionScanLT\hpprsclt.exe	SUCCESS	R Att
4 Create	D:\WINDOWS\VTWAIN.INI	ACCESS DENIED	W Att
2 Read	D:\SCANJET\PrecisionScanLT\hpprsclt.exe	SUCCESS	Offse
2 Read	D:\SCANJET\PrecisionScanLT\hpprsclt.exe	SUCCESS	Offse

Step 8


I will then go back to the problem station and logon as an Administrator so I can give access rights to the files the user needs access to. I will normally give the user Write access and if that doesn't work I will then give Modify access to the specific files. I have never had to give a user Full access to the specific files to get a program to work. Now remember if this program is used by several users then you will want to give the access rights to a group instead of the user. So if the user is a student I would give the access rights to the student group for the domain.

Note: sometimes you might have to give Write access at the folder level because the program is trying to create a file inside a folder the user does not have Write access to. Later in this paper I will explain a way I got around this problem when I explain the needed Admin rights for a typing program we use in our district.

Step 9

I will then log back on as the same normal user and try to run the program again to see if I get any error message again. Sometimes you will get the same error message or a new error message; this is sometimes not related to the files you just granted access to. If the same files show up again then you will need to grant the user more access rights to the file. A lot of times when you open one file this will lead to another file that needs to be accessed later in the startup process. If the program starts and runs just fine then you have just fixed the problem without making the user an Administrator of the local station.

Step 10

If the program still produces error messages then I will clear out all the data on my laptop by clicking on the eraser button on the tool bar . I will get to the point again on the problem station to where all I have to do is click on the program.exe to start the program.

I will then click on the Magnify Glass with a red X through it to start monitoring the remote station again.

Step 11

I will repeat the monitoring process until all the Access Denied entries stop showing up in the data. If I clear all the Access Denied entries and I still get an error message, I will then turn to Regmon to see if any Access Denied entries are showing up in there.

All the steps you have used to run Filemon will be used to run Regmon. The only difference you will see is that you are monitoring the registry keys instead of the file system.

Step 12

If all the Access Denied entries are cleared up for the files and the registry and you are still getting an error message then there is something else that can't be seen that is causing you to be an Administrator before the program will run. You will have two options now; you can make the users Administrators or you can just not install the program. This will need to be determined on a per program basis. This should be determined by the network Administrator.

How some simple changes made Program X work without Admin rights!

A tech support person stated that after she installed this program X she was able to run it with no problems. When a normal user logged on and tried to run this program they received an error message "Please close other Program X applications" Since the Tech was able to run this program when logged on (with administrative rights) I figured it was a rights issue. So I went to Program X's website and found the following information under their support section:

Q. I get a message, "Please close other Program X applications" when trying to run the program on Windows 2000.

A. This will occur if you are attempting to run the program on a Windows 2000 system and you are not logged in as an administrator or a user with administrator access. You must be logged in with administrator level access in order to run the program.

After following the steps I described above I found two Access Denied entries. The first was the user did not have access to the file c:\winnt\apppatch\layerstorage.dat. I had the Tech give Write access to this file. The second entry was the program was not able to create a file called programx.mtx in the c:\winnt folder. Since we did not want to give Write access to the c:\winnt folder I wanted to try and trick the program into thinking the file was already there. Here is what I had the Tech do:

- Since this file was one that windows didn't know how to open I had the Tech go to another folder and look for a file that Windows didn't know how to open. I then had the Tech copy that file to the desktop. After copying the file to the desktop I then had the Tech open the file in Notepad making sure the Always Open With checkbox was unchecked.
- When the file opened the Tech then did a ctrl + a to select all the text. Then she deleted all the information and saved the file as programx.mtx
- The Tech then copied the file to c:\winnt and gave the user Modify access to file. The Tech then logged off as herself and logged on as the user and the program ran just fine. In case you're wondering this program has been running for a couple of months now with no problems.

This type of fix is not typical; usually it just takes modifying the access rights to certain files or registry keys to make the program run correctly. This is just one of many programs I have been able to run on Windows 2000 without granting the user Administrative privileges.

Conclusion

According to Tim Atkin [8] a member of the private-sector group Partnership for Critical Infrastructure Security and director of critical infrastructure protection at consulting firm SRA International Inc. in Fairfax, Va. "Right now, the view is [that] nothing should be considered sacred," Since the attacks against the US on Sept 11th and with security incidents increasing every year, we need to protect our customer's information and ourselves more diligently. One of the ways to help protect our organization is by limiting the rights our users have when they access our computers or our network. This document will hopefully help other IT Professionals from having to make users Administrators of their local workstations just to run programs made by companies that don't adhere to security when designing and compiling their programs. So the next time a program manufacturer states that the user must be an Administrator to run their program just remember where there's Winternals there's probably a way around it.

References

[1] Winternals User's Guide

URL:

<http://www.winternals.com/documentation/docs/monitoringtools/MonitoringTools.pdf>

[2] Winternals Regmon and Filemon Tools "Monitoring Tools" 2002

URL: <http://www.winternals.com/products/monitoringtools/monitoringtools.asp>

[3] US National Academy of Sciences "Software security law call" 16 January 2002

URL: http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_1762000/1762261.stm

[4] Paul Festa and Joe Wilcox. "Microsoft criticized for lack of software security" 5 May 2000

URL: <http://news.com.com/2102-1001-240184.html>

[5] DAN VERTON. "ANALYSTS: INSIDERS MAY POSE SECURITY THREAT" 15 OCTOBER 2001

URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO64774,00.html

[6] DAN VERTON. "Security: IT Locks Down" 1 January 2002

URL: http://www.computerworld.com/p100_2002/0,4639,NAV47_STO66813,00.html

[7] Richard Power "Computer Security Issues and Trends" Spring 2001

URL: <http://www.gocsi.com/prelea/000321.html>

[8] Patrick Thibodeau "War against terrorism raises IT security stakes" 24 September 2001

URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO64147,00.html

© SANS Institute 2000 - 2002, Author retains full rights.