Global Information Assurance Certification Paper

Free NT Security Tools
Douglas T. Orey
GSEC Practical Assignment
Version 1.2e
August 6, 2001

Introduction

One important security issue is not having the tools to secure your network. Those individuals who use Linux are lucky enough to have good security tools developed that they can use for free. Unfortunately that hasn't always been the case for NT. Not only do we not have the tools to use but security isn't even a real part of our training. Things of course are changing now….and for the better. NT Administrators now can start taking control of the security of their systems. We can now enjoy a lot of the free tools that Linux Administrators enjoy.

How many times have you typed in **netstat –a** and viewed the results wondering…"why are so many ports open and listening on my computer and what services is listening on those ports"? Now if your new to this like me your next question is. How do you find out what has these ports open?

I remember a call I received from a guy while I was working on the Netscape helpdesk. This guy was very angry. He said that Netscape was watching him on the internet. I assured him we wasn't but he didn't believe me. He said we have his port open and we are listening on it. If we don't stop monitoring him he is going to sue us. He said he knew what he was talking about because he did it to other people.

Now this might seem funny to you but at the time I didn't know about ports or that they might be listening. So it is not only vital to have these tools but also to know how to use them and interpret what you see. It is beyond the scope of this paper however to instruct in the uses of these tools. So it is important that you read the instructions and practice and learn how to use them efficiently.

Checking to see what services are running is a simple matter. In NT 4.0 you access the services through the control panel and then click on services. In Windows 2000 services are apart of the Administrative tools. This will tell you what services are running on your computer. At a command line you can type in *net start* and view the running services. Neither way however tells you what ports they are using.

You can also open up task manager and find out what process are running. Again this doesn't tell you what port is being used or for that matter what program is running that process. There are other viewers that you can use to view your processes and several comes with the NT Resource Kit. Still you are left with the same questions. What ports are they using and what programs started theses processes.

Have you ever wondered what kind of traffic is on your network but just can't work a

good sniffer into the budget? I know I tried for three months to get the okay to purchase one and then the answer was no!

Fortunately there are a few third party utilities that we can use with NT to make our life easier and help answer some of the questions. I believe that it is very important for us NT Administrators to be aware of these programs. They can certainly make securing our networks easier and they have the added benefit of being free. That is right they are free. Now there is no excuse for any of us not to download these programs and learn how to use them.

The point to this paper is that NT also has good free security tools just like Linux. This is not a tutorial on these products however. What I'm going to do is run through an incident I had a few weeks ago. I'll being using these free tools I have been talking about. I will do this step by step to show you how they can be used to resolve some of the basic security issues you might run into.

Free NT Tools

The best place to start is the beginning. I was playing with a free sniffer I had downloaded called **Ethereal** (http://www.ethereal.com/distribution/win32). This is actually a Linux program that was ported over to NT. You can download both the Linux and NT version from this website. For NT you also have to download **WinPcap.exe** (http://netgroup-serv.polito.it/winpcap/) and install it before Ethereal will work. Ethereal is a very nice utility to have. It is easy to use and read what it captures. You can use it in promiscuous mode with just a couple of clicks of the mouse.

I was trying to learning how to use Ethereal and interpret the packets floating out on my network. I started to notice a few strange things I didn't understand. 5 workstations were all using the same multicast address and the same port number 402. I work for a hospital and am fairly new here. They have a lot of little programs they have been using long before I got here and I'm constantly finding them. At first I just assumed it was a program that they were using because it seemed to come only from the nurses stations. As I kept looking at the packets that I had captured. I noticed a workstation that I had just recently put out on the floor using the same multicast address. Now I was really interested! The workstation is a Windows 2000 Professional so I knew no one could have installed a program with only domain user access.

At this point I decided to scan the workstation to see what ports were open. I used Super Scanner 3.0 (http://www.foundstone.com/rdlabs/tools.php?category=Scanner). I really like this scanner it is very easy to use and for me it does a good job. The only problem with it is that it is kind of slow. For this reason you might want to use a faster scanner.

I do have **Nmap** www.insecure.org/nmap/ (which is a Linux program) but haven't had the time really to get to know it very well. I do use **Nmapfe** which is a gui version of Nmap on Linux. Nmap has been ported to NT **NMAPNT** (www.eeye.com/html/Research/Tools/nmapnt.html). This like its counterpart Nmap is

also command line based. It works very well on NT but I haven't had the time to really sit down and play with it and see what it can do. I used it after Super Scan got finished to double check the results. NmapNT is much faster to use. This is another great tool for the NT side of the street.

I scanned all the ports on this workstation to see what was open. The results weren't too bad. There were only seven open ports on this particular workstation. I also downloaded a list of ports that was mentioned in the course material for Security Essentials. Actually they gave and ftp site but it has been moved to www.iana.org/assignments/port-numbers. So I looked up the open ports against this list. The ports that were open were:

- 135 -- epmap
- 139 -- ntbios-ssn
- 445 -- Microsoft-ds
- 1044 -- unassigned
- 1055 -- ansyslmd
- 2301 -- cpq-wbem (Compaq http)
- 49400 -- no reference

Okay ports 139 and 445 I recognize. Port 139 is a netbios port and 445 is used by Windows 2000 if you turn off netbios over tcp/ip. I have found a good paper on port 445 at http://ntsecurity.nu/papers/port445/ . It is only a page long but very informative.

I'm not sure what exactly epmap is but its description is DCE Endpoints. The 1044 is unassigned but that doesn't worry me too much but it still needs to be checked out. Up til now I've never had to worry about what ports were open on a computer. You always hear that you need to shut down unneeded services an close all unnecessary ports. Of course this is easier said then done if you don't know what port is opened by what service or program.

Also lets say you have all the services that don't need to be running turned off but you still notice a few high open ports. How do you find out what has this port open? There has to be a simpe way. Fortunately there is.

I found a program a month or two back that is called **The Cleaner** (http://www.moosoft.com/download.php). This program is not free however. You can download a trial version and if you like it then you must pay for it. This program is designed to clean Trojans off of your computer. I thought at the time I had a Trojan so I downloaded it to see if it worked. Well it turned out I didn't have a Trojan but I did find a useful utility that came with **The Cleaner**. It is called **TCActive!**. This is a neat little utility that checks the processes running on your computer and tells you what program started the process. For example I have process id '*628 stisvc.exe*' running right now. I have no idea what that is or what program initiated the process.

I run TCActive! and in the description column it describes this as a '*Still Image Device Monitor'*. Now if we want to track this down further we know more of what we are

looking at. Okay that is nice but what does that really mean for me?

It makes it easier to track down what programs started a process on your computer. If you know what program started it it is easier to tell if it is a legitimate process or not. No it doesn't tell you what ports it has open but it is still good information to know. I didn't actually use this program in tracking down the open ports on this workstation but I run it from time to time on my own and make a mapping of the processes that are normally running on my computer.

Now lets look at the rest of the open ports. Port 1055 ansyslmd has a description of ANSYS – License Manager and 2301 cpq-wbem's descriptions is Compaq http. Which I intend to uninstall when I get to the workstation. Now the port that really has me worried is the last one. Port 49400. I know that these high ports are used a lot for nefarious activities and to tell you the truth this is pretty much what I expected to find.

Now we are ready to move to the workstation and do a little detective work on it as well.

The first thing I do is go to a command prompt and do a "netstat –a" to get a list of open ports. I copy this to notepad and print it off. Now it is time for me to try a few utilities that I learned about in my Security Essentials course. I've been wanting a utility that would match open ports to the programs or processes that actually open them. I have searched several times on the internet with no success at finding such a free utility for NT. I was amazed when in Security Essential they mentioned not only one but two. Of course I had to try them out and I was glad I did.

The first utility I used is called **Inzider** by Arne Vidstrom and you can download it at http://ntsecurity.nu/toolbox/. Now to quote the authors description of his program. He says that Inzider *"Shows which processes listen at which ports, and can be useful for finding Back Orifice 2000 when it's hidden in another process. Let's find out which programs are responsible for all those open ports!"* . Sounds good to me I can't wait to try it out.

Installing it and using the program was very easy. It did map a few things like Outlook, Internet Explorer, Word, Winamp. It told you the process ID number and path of the program that started the process. It also told you what port it had open and even what interface it was bound to. It is a good program unfortunately this utility didn't map everything I was looking for. It is still a nice program and it is free!

The next program I'm going to use is called **fport.** This is a good program and can be downloaded from (http://www.foundstone.com/rdlabs/tools.php?category=Intrusion+Detection). Their description of fport is *"Reports all open TCP/IP and UDP ports and maps them to the owning application."*

Now that sounds real good too. I just hope it will also map the ports that I'm really wondering about…like port 49400. FPort does and excellent job. I copied its out put to notepad and printed it off as well. I then looked at the results closer. FPort actually broke

down its information into 5 easy to read columns: *Pid, Process, Port, Proto (Protocol),Path*. The path will give you the drive, directory and executable of the programming running this service. In one word COOL! The one thing FPort didn't tell me however is to what interface it was bound to.

I was wondering about port 1044 that my list says was unassigned. So I look at the results of my FPort program for port 1044:

- *pid 664*
- *process MSTASK*
- *port 1044*
- *proto TCP*
- *path c:\winnt\system32\svchost.exe*

Good. Port 1044 is being open by a legitimate program. Now lets check out the port 49400. I'm really curious to see what has opened such a high port number. Here are the results from Fport:

- *pid 600*
- *process LCRMS*
- *port 49400*
- *proto TCP*
- *path c:\program files\Compaq\lcrms\lcrms.exe*

Ha! Compaq is the Trojan I was expecting to see. I was happy to see it wasn't something bad at all! Well the fix for this was easy. I went into the Control panel and into Add/Remove Programs and removed the Compaq programs listed in there. They were mainly utility programs and we weren't using them. Well I ran netstat –a again and sure enough port 49400 wasn't listed so it had been closed when I removed those programs. I ran Fport one more time and double checked and no 49400 was not listed.

You might have noticed that I forgot about port 402 that they were using on the multicast address.

So I'm walking back to my desk happy that it wasn't a trojan and patting myself on the back for being able to track it down. That lasted til I got back to my desk and ran Ethereal again and noticed that that workstation was still using the multicast address as it was before on port 402. So I looked at the print out of the FPort that I had from the workstation. There was port 402 being initiated from a program called "aclient.exe" in a folder called Compaq. So I had to go back to the workstation and remove that folder as well. Rechecked everything and finally my problem is solved. Well, it will be after I visit four more workstations!

This process actually took me about 15 to 20 minutes from start to finish. Not long at all. To top it off all the tools I used was free. The TCActive! is the only utility that to my

knowledge isn't free. It came with The Cleaner which I downloaded as a trial version.

Conclusion

There are more free tools out there but if you only have those listed in this paper you will already have a well stocked toolbox. Security on NT doesn't have to be daunting or frustrating. It is actually fun and exciting. So take the time and download these programs and learn how to use them. Thanks to a few people who has made free easy to use programs for the common good of us all we are able to better track and control what is running on our network.

References:

www.ethereal.com

http://netgroup-serv.polito.it/winpcap/

http://www.foundstone.com/rdlabs/tools.php?category=Scanner

http://www.insecure.org/nmap/

http://www.eeye.com/html/Research/Tools/nmapnt.html

www.iana.org/assignments/port-numbers

http://ntsecurity.nu/papers/port445/

http://www.moosoft.com/download.php

http://ntsecurity.nu/toolbox/

http://www.foundstone.com/rdlabs/tools.php?category=Intrusion+Detection

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor