Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2f (amended August 13, 2001)

NT/2000 Security Tool Kit on A Budget
Albert Rice
October 9, 2001

Introduction:
"If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu On The Art of War, Translated by Lionel Giles, M.A.

In this time of shrinking IT budgets and doing more with less the cost of purchasing a commercial vulnerability scanning tool can cost several thousands of dollars. With Internet facing servers it is imperative to know if there are any vulnerabilities that can be exploited. To the rescue of under budgeted and over worked systems administrators comes freeware based security tools that are as good or even better than the equivalent commercial Internet security tools.

This paper will focus on the shareware, freeware and low cost commercial security tools that I have found useful and have used to solve security issues in the organization I presently work in. The following brief list is by no means all-inclusive as the environment I presently work in is almost exclusively Microsoft based with NT 4.0 as the primary operating system. Many of these security tools are direct ports from the Unix/Linux world.

CAUTION 1: As with any network scanner product make sure you have written and signed permission from Management **before** using it. This can literally be your get out of jail free card.

Disclaimer: These tools can get you in serious trouble with your employer and law enforcement. Use them with caution and at your own risk.

Question 1: Is your system as secure as you think? You've followed the hardening documents such as "Microsoft Windows NT 4.0 C2 Configuration Checklist", and the United States Navy's "Secure Windows NT Installation and Configuration Guide", you've downloaded the latest Service Pack and pertinent hot-fixes, you've worked out the permissions issues and registry settings for the applications your user's want and now do you know if there are any unknown vulnerabilities?

NOTE: Many of these descriptions were taken from the application or tools description located with the package, or from the tools home page.

Highly useful security utilities that have a relatively low cost:

First, purchase the Microsoft NT 4.0 Server Resource Kit (NTRK) and Supplement 4, which is

the all-inclusive upgrade of the prior three supplements for approximately $200, unless you can find it at a lower price on E-bay. Get the Server version of the Resource Kit as it contains the Workstation version tools and you will get the Server tools as well. The NTRK contains many useful utilities to help with the administration of your NT network and checking the security of your NT systems. As the NTRK is known in some circles as the NT Hacking Kit or NT Cracking Kit it is very useful for a System Administrator to know how to use. There are sample NTRK utilities that can be downloaded from Microsoft for free. The first URL is ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/ for the individual update NTRK files. The second Microsoft URL is http://www.microsoft.com/ntworkstation/downloads/Recommended/Featured/NTKit.asp choose "Resource Kit for Intel" and click on the "Download Now" button. The files size is about 7.2 MBs. NTRK tools such as rasusers, RMTshare, are very useful in determining who is or has been logged into your NT systems. An example of an important tool included in NTRK is passprop.exe, which sets two important features:

One: Password-complexity will be set forcing the use of mixed case or numbers or symbols.

Two: The ability to apply the system lockout policy to lock out the Administrator account from the network. Install the NTRK or copy the passprop.exe file to the c:\%systemroot%\system32, then run "passprop /complex /adminlockout" from the command prompt without the quotes.

For those of you using Windows 2000 the URL is http://www.Microsoft.com/windows2000/techinfo/reskit/tools/default.asp

Rasuers An NT Resource Nit (NTRK) command that shows which users have remote-access privileges on the system.

Kill An NTRK command that terminates a process.

And many more tools that are beyond the time and space constraints of this document.

NeoTrace v 3.25 by Neoworx is an excellent graphical based trace route program. The cost is $29.95 and they have a functional version available for evaluation. http://www.neoworx.com/

General Purpose Shareware/Freeware Vulnerability Scanning Tools

Get to know the tools included with NT 4.0 such as net, netstat, Arp, NBTStat, tracert, built-in NT networking utilities.

Brief listing of useful command line switches:

Net [option] session, share, file, use, user, view, start, stop, continue, pause, and etc.

Netstat –an, will show the status of TCP/IP network connections to and from the local computer. It can be used to show all active TCP and UDP ports on your workstation or server.

netstat –a

Show all active TCP connections and their connection status.

netstat –n
Do not try to resolve IP addresses into hostnames or convert port numbers to symbolic names. If there is a problem with DNS, this will prevent long delays waiting for DNS timeouts.
Netstat –p protocol
Limit display to specified protocol. Possible protocol types for the statistics display (-s) are icmp, ip, tcp, and udp. The display of connections are listening ports is limited to tcp and udp.
interval
Continuously redisplay netstat output every interval seconds. Type CONTROL-C to quit. This is handy if you want to observe changes in (almost) real time while something is happening on the network.

Arp A built-in system tool that shows the MAC addresses of systems that the target system has been communicating with, within the last minute. Here's two useful ARP commands:

Arp [options]
arp –a [IP-address]
Display contents of entire ARP cache or just the entry for IP-address. If there are multiple network interfaces, the –N option can limit the display to the ARP entries for a specific interface.
arp – N [Interface-address]
Prints the ARP entries for the interface Interface-address. If an interface is not specified, uses the first one found.

NBTStat A built-in system tool that lists the recent NetBIOS connections for approximately the last 10 minutes. Can be useful if you use NetBIOS.
Nbtstat –S
Display current NetBIOS sessions. Remote computers are listed by their IP addresses.

There are of course the standard tools such ping, route, and tracert all owing their existence to UNIX. For an excellent reference on Windows NT command line tools I recommend "Windows NT In A Nutshell" by Eric Pearce of O'Reilly, 1997.

This list of utilities is not all-inclusive. There are many more free ware and share ware tools such as Fpipe, pslist, listdlls and md5sum to just mention a few.

Whisker **http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2**
Description: Rain.Forest.Puppy's excellent CGI scanner that checks for known Web vulnerabilities. If you are running an Internet accessible web server this tool is a must. An excellent tutorial and description of this program is listed in the book, "Incident Response: Investigating Computer Crime," in Chapter 14: Investigating Web Attacks page 374 and 375.

Abacus Port Sentry http://www.psionic.com/abacus/portsentry/
Description: Portscan detection daemon PortSentry has the ability to detect portscans(including stealth scans) on the network interfaces of your machine. Upon alarm

it can block the attacker via hosts.deny, dropped route or firewall rule. It is part of the Abacus program suite. Note: If you have no idea what a port/stealth scan is; I'd recommend taking a look at http://www.psionic.com/abacus/portsentry/ before installing this package. Otherwise you might easily block hosts you will need (e.g. your NFS-server, DNS, etc.). This program is similar to TCP Wrappers by Wietse Venema.

Ethereal for windows http://www.ethereal.com
Description: Network traffic analyzer Ethereal, or "sniffer", for Unix and Unix-like operating systems. It uses GTK+, a graphical user interface library, and libpcap, a packet capture and filtering library.
Download the Windows version from http://www.ethereal.com/distribution/win32/
Please take a look at the paper "Free Tools For Network Security" by Jeffrey Shuron, May 16, 2001, for further additional information and usage instructions:
http://www.sans.org/inFosecFAQ/tools/free_tools.htm

NMAP or NMAPNT http://www.eeye.com/html/Research/Tools/nmapNT.html
One of the best general-purpose security tools is Nmap from Fyodor at http://www.insecure.org. This Unix/Linux based port-scanning tool has been ported to the NT environment and can be found at http://www.eeye.com/html/Research/Tools/nmapNT.html. Note: The known bugs list on their site. You will need a separate NT based machine to scan your network. Excellent tool to test which ports are open and listening on your servers and workstations. Did you forget to unbind NetBIOS from the Internet facing NIC?

Please take a look at the paper "Free Tools For Network Security" by Jeffrey Shuron, May 16, 2001, for further additional information and usage instructions:
http://www.sans.org/inFosecFAQ/tools/free_tools.htm

Perl www.perl.org
Description: A very powerful scripting language, which is often used to create "exploits" for the purpose of verifying security vulnerabilities. Of course, it is also used for all sorts of other things such as user administration in small to large networks. Even can be used for web page scripts. The present Active State Perl version for Windows NT is 5.6.1. If you don't speak Perl there are excellent books such as "Learning Perl on Win32 Systems" by Scwartz, Olson, and Christiansen, "Windows NT User Administration" by Meggitt and Ritchey or the many on line tutorials available at your favorite search engine.
The version of Perl included with the NTRK is extremely out of date. Download the latest Windows version from http://aspn.activestate.com/ASPN/Downloads/ActivePerl/

Nessus http://www.nessus.com
Description: Remote network security auditor, the client the Nessus Security Scanner is a security-auditing tool. It makes it possible to test security modules in an attempt to find vulnerabilities that should be fixed. . It is made up of two parts: a server, and a client. The server/daemon, nessusd, is in charge of the attacks, whereas the client, Nessus, interfaces with the user through a nice X11/GTK+ interface. There are three Windows version of the Nessus client.

The Windows version can be downloaded from http://www.nessus.org/win32.html. **Note: You will need a nessusd server to connect to make this scanner work. In other words a Linux based system.**

SARA http://www-arc.com/sara
Description: The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool. I know this paper is supposed to be about Windows NT based security utilities but I made an exception here as this Freeware tool is kept relatively current and strives for compliance with standards such as "SANS/ISTS" certification and Common Vulnerabilites and Exposure (CVE) list. SARA does keep track of many NT/2000 based vulnerabilities. Also, gives me the excuse to setup a Linux system. SARA can be compiled from hpux9, hpux, linux, linux-nansi, sunos4, sunos5, trusted-sunos5, aix, osf, bsd, bsdi, irix4, irix, dgux, freebsd essentially UNIX or variant. This info is taken from the SARA makefile version 3.4.9a. Sorry, you may have to subscribe to the SARA List Server at http://www.www-arc.com/sara/subscribe.html.

Snort **http://www.snort.org**
Description: Snort is an excellent no cost intrusion detection system (IDS), which is used to detect all of those pesky scans on your network. A highly flexible packet sniffer/logger that detects attacks by using a database. Snort is a libpcap-based packet sniffer/logger, which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has a real-time alerting capability, with alerts being sent to syslog, a separate "alert" file, or even to a Windows computer via Samba. Snort can be readily updated with latest intrusion signatures from the Snort web site.
Snort for win32 homepage http://www.silicondefense.com/techsupport/windows.htm
Download the Windows version from http://www.snort.org/downloads/Snort-1.8.1-win32-static.zip

Windump http://netgroup-serv.polito.it/windump/
WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX. Porting is currently based on version 3.5.2. WinDump is fully compatible with tcpdump and can be used to watch and diagnose network traffic according to various complex rules. It can run under Windows 95/98/ME, Windows NT and Windows 2000.

WinDump uses a libpcap-compatible library for Windows, WinPcap, which is freely downloadable from the WinPcap site.

http://netgroup-serv.polito.it/winpcap/install/default.htm#Developer

WinDump is free and the source code of the entire project is available under a Berkeley-style license.

Download the Windows version from http://netgroup-serv.polito.it/windump/

Microsoft Based Tools:
As this document deals with Microsoft Windows NT and a glance at Windows 2000, I offer up

information on Microsoft's efforts at securing their products from various Internet based threats:

IIS Lockdown, Microsoft Personal Security Advisory, Cleaner for Code Red II, Improved Cipher Security Tool, Qchain, Security Screen Savers, Windows 2000 Internet Server Security Tool, Security Planning Tool for IIS, and HFNetChk. Be sure to take a look at these resources.
http://www.microsoft.com/technet/security/tools/tools.asp

Microsoft Personal Security Advisor
A new tool is available that let's you ensure that your workstation is up to date on all security patches and configured for secure operation.
http://www.microsoft.com/technet/security/tools/mpsa.asp
Your mileage may vary, as with any automatic security configuration tool test it out on a non-production system before deployment in the real world.

HFNetChk
HFNetChk lets administrators scan their servers -- including remote ones -- to ensure that that they are up to date on all security patches for Windows NT 4.0, Windows 2000, IIS 4.0, IIS 5.0, IE and SQL Server. http://www.microsoft.com/technet/security/tools/hfnetchk.asp
Take Note of the Caution at the beginning of this document. Make sure you are scanning your network Servers and have written permissions.

Security Configuration Editor
The Microsoft Security Configuration Editor (SCE), which has been available, since SP4, is a useful tool for configuring ACLs and Registry settings with a script. The Technet article describing its use is located at:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winntas/maintain/security/scmnt4.asp
These Microsoft knowledge Base Articles relating to the SCE should be read and understand before using the SCE: Q195227, Q195509, Q214752.
Your mileage may vary, as with any automatic security configuration tool test it out on a non-production system before deployment in the real world. Debug those scripts and necessary permissions and dependencies for applications such as Microsoft Office, Corel Office, or Adobe Page Maker. Test, test and no matter how tempted to let your user test your configuration choices out test some more. You will spend a lot less time on the phone going over the finer points of the Registry Editor with your end users.

The Microsoft Security Tool Kit

New as of October 3, 2001 is the Microsoft Security Tool Kit. This comes in two flavors a FREE CD or download. According to Russ the NTBugtraq Editor, "There's a difference between the download and the CD. Quoted from the announcement page, "It (CD) includes automation scripts to quickly install all the security hot-fixes recommended in the kit.", but the CD may take from 3 to 6 weeks to arrive." The URL is http://www.microsoft.com/security/default.asp and best of all the CD is FREE. As this is really new I have not had time to test out the download version but from the description of the contents I have most of the files spread across two CD's. It will

be handy to have them on one CD.

Questions 2: What happens when you find an unknown IP address on your network? Answer: You investigate that address. Get your evidence documented under the directions of your security plan and then call your local Law Enforcement. You do have a well written and management approved security plan?

Sam Spade http://www.samspade.org/

Sam Spade is the all-in-one network investigation utility. The site contains very useful tools for researching Internet addresses. Can be used to research abusive sites (SPAM) and find out who owns the subnet or web site. The description of the individual tools are taken from the Sam Spade web site

The present version of the Windows based Sam Spade application is 1.14 and can be downloaded from http://www.samspade.org/ssw/download.html. Excellent all around IP address investigative utility that will run on Windows 9x, NT, 2000, and ME. The Sam Spade for Windows application has most of the following tools from the Sam Spade web site in one place.

This site includes numerous tools to investigate Internet addresses. You will have to register to use some of the more advanced tools. Registration is free. The useful tools I've used include:

> **The Address Digger:** It takes a hostname or an IP address, guesses at the domain name, and then runs some whois queries to find out who owns the domain and the block of IP addresses it lives in, and traces the route packets take to the host.
>
> **Obfuscated URLs**: A lot of SPAM includes pointers to websites. Often the URL is obfuscated in a variety of ways - by using %-encoded characters, bogus authentication information, and IP addresses written in strange ways. This tool will decode any legal URL, showing you how it was obfuscated, what the real URL looks like and who hosts the website.
>
> **Reverse DNS:** This tool checks the reverse DNS for the 256 addresses surrounding the one you're looking at. It shows the hostname claimed for each address (if any) and checks for forged and bogus reverse DNS.
> (If reverse DNS gives a hostname, which doesn't exist, it's described as bogus. If the hostname does exist, but doesn't resolve to the original IP address it's described as forged.)
>
> **traceroute:** Traceroute shows the route packets take from this host (samspade.org) to the host you're looking at. Each hop shows the hostname (or the IP address if there's no reverse DNS), the IP address of the system, the AS number of the system, and the round-trip time from samspade.org to the system.
> The AS number identifies the owner of the network neighbourhood the system is in. Following the AS number link will give contact information for the owner of that block of addresses - the system itself may be a customer of the block owner

Whois: The whois tool asks a question of a whois server. Typically the question is a domain name or an IP address.
You usually need to pick the right whois server to ask your question (whois.nic.fr only knows about French domains, for instance).

Rwhois: This is a very simple rwhois tool. It asks a single question of an rwhois server. Typically the question is an IP address.
You usually need to pick the right rwhois server to ask your question (rwhois.exodus.net only handles Exodus sub allocation, for instance).

Black hole list check: This queries several black hole lists to see if the server is listed for abusive e-mail better known as SPAM.
MAPS Realtime Blackhole List
This is a conservative list, containing sites that are actively supporting UBE senders or are aggressively indifferent to doing so.
MAPS Dialup Users List
This is a list of addresses belonging to dynamically allocated dialup modem pools. Blocking email sent directly from these users blocks a lot of senders of UBE, and affects almost no legitimate users.
MAPS Relayed SPAM Source
A list of servers which appear to have relayed SPAM and which appear to allow third-party relay.

DNS Query (disabled): This tool lets you ask the domain name system about a domain name or IP address.
Some useful queries are:
MX
The servers that handle email for the domain
NS
The authorative nameservers for the domain
SOA
Who is responsible for the zones DNS configuration, or in the case of an IP address who's responsible for reverse DNS
ANY
All information known about a domain by the Sam Spade name server. This **isn't** all information about the domain. If you're looking for a specific record type, query that type specifically

DNS: The dns tool asks basic questions of the domain name system. Typically the question is a domain name or an IP address.
It will provide the address and mailserver for a hostname, and the reverse DNS for an IP address

RFC: A complete searchable cross-indexed list of RFC's.

There are more tools on the Sam Spade web site than listed.

Conclusion:
As system's administrator trying to secure your network, it is important that you check your individual workstations and server's configurations. By using automatic scanning tools you can establish a base line security configuration. Then regularly using these tools (remember to get the updates) you can detect when the base line system configuration has changed or needs to be updated. Review your security policy which should be continually updated to address the latest responses to insider and out side security threats. Subscribe to Microsoft Security Update Service at http://www.microsoft.com/technet/security/notify.asp. To stay current with the latest NT/2000 security issues subscribe to NTBugtraq at http://www.ntbugraq.ntadvice.com/. And for the most current security consensus subscribe to http://www.sans.org/. Good luck and be ever vigilant.

References:

1. Sun Tzu On The Art of War, Translated by Lionel Giles, M.A. 1910
http://www.clas.ufl.edu/user/gthursby/taoism/suntext.htm

2. Microsoft Corp. "Sample Windows NT/2000 Resource Kit Utilities"
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/.
http://www.microsoft.com/ntworkstation/downloads/Recommended/Featured/NTKit.asp
http://www.Microsoft.com/windows2000/techinfo/reskit/tools/default.asp

3. NMAP users Top 50 Security Tools, May/June 2000.
http://www.insecure.org/tools.html

4. "Internet Security with Windows NT" by Mark Joseph Edwards, December 1997, Online and 29th Street Press.
http://www.windowsitlibrary.com/Documents/Book.cfm?DocumentID=121

5. Whisker by Rain.Forest.Puppy http://www.wiretrip.net/rfp/p/doc.ask?id=21&iface=2

6. Abacus Port Sentry http://www.psionic.com/abacus/portsentry/

7. Ethereal http://www.ethereal.com

8. NMAP http://www.insecure.org

9. NMAPNT http://www.eeye.com/html/Research/Tools/nmapNT.html

10. "Free Tools for Network Security" by Jeffrey Shuron, May 16, 2001.
http://www.sans.org/inFosecFAQ/tools/free_tools.htm

11. Perl http://www.perl.org

12. Perl for NT/2000 http://www.aspn.activestate.com/ASPN/Downloads/ActivePerl/

13. Nessus http://www.nessus.com

14. SARA http://www-arc.com/sara

15. Snort http://www.snort.org

16. Windump http://netgroup-serv.polito.it/windump/

17. Microsoft Corp. "Microsoft Product Security tools and checklist web page." http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp

18. Microsoft Support Knowledge Base is available on the Internet at http://support.microsot.com/support/search/.

19. Stefen Norberg, "**WinPcap Brings Unix Network Tools to Windows".** http://security.oreilly.com/news/securingnt2_1200.html

20. Scambray, McClure, Kurtz, "Hacking Exposed, 2nd Edition", 2001 Osborne McGraw-Hill Companies.

21. Mandia and Prosise, "Incident Response, Investigating Computer Crime". 2001 Osborne McGraw-Hill Companies.

22. Eric Pearce, "Windows NT In A Nutshell" 1997, O'Reilly.

23. Microsoft Corp. "Microsoft Security Configuration Editor" http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winntas/maintain/security/scmnt4.asp

24. Microsoft Corp. "The Microsoft Security Tool Kit" http://www.microsoft.com/security/default.asp

25. The authors of Hacking Exposed 2nd Edition have made available on their web sites http://www.hackingexposed.com/tools/tools.htm, and http://www.foundstone.com/rdlabs./tools/htm several NT security related tools.

26. Sam Spade http://www.samspade.org/