Global Information Assurance Certification Paper

Securing the NetOp Host Step-By Step

GSEC Practical Assignment (v1.4b)

Robert Rounsavall

June 09, 2003

Abstract

This paper details how to secure the NetOp Remote Control Host. The first part of the paper explains some of the different types of remote control and the risks associated with each type. The Second part of the paper introduces NetOp Remote control and its major components. The third and final part of the paper explains in detail how to lock down the NetOp Remote Control Host in checklist format.

Types of remote control

For the purpose of this paper we will break down remote control into 3 categories. The first category can be called trojan horses or back doors because these programs are often used by attackers to compromise machines. They include programs like NetBus[1] or Back Orifice[2]. These programs are sometimes sent via email, and are either self-executing or the victim is tricked into clicking on an executable file that installs a small program, makes a registry entry or two, and listens on a specific port. They are limited in functionality, but they can allow the attacker to have keyboard and mouse control, as well as perform annoying functions like open the CDROM tray, or wreak havoc on your system by modifying registry entries and deleting files or directories. Believe it or not, some people use these tools for system administration purposes as well. Any antivirus software should detect and remove these programs, as well as protect systems from installing them in the first place.

The second category of remote control programs are what I will call entry level remote control programs. They allow keyboard, video, and mouse control in a limited setting, usually on a limited number of machines. They are used for system administration and telecommuting. Usually there are not many built in security features. These would include programs like VNC[3] from AT&T Laboratories, and Microsoft's Remote Desktop[4] or Remote Assistance[5]. These programs are many times free, or part of a suite of management tools. With the exception of VNC, many of them only work on one operating system. They usually do not have many security or encryption features and are in many cases painfully slow, but are suitable for home use or use in a limited environment.

The third and final group of remote control products will fall into a category that can best be described as enterprise level remote control products. These are

[1] NWInternet.com. "NetBus, BO's Older Cousin." 25 November 1998. URL: http://www.nwinternet.com/~pchelp/nb/netbus.htm
[2] Cult of The Dead Cow. "Back Orifice Remote Administration Tool." URL: http://www.cultdeadcow.com/tools/bo.html
[3] Virtual Network Computing. URL: http://www.uk.research.att.com/vnc/
[4] Microsoft Remote Desktop. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/pree_rem_fhca.asp
[5] Microsoft Remote Assistance. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/rmassist.asp

commercial products that can be used across large networks with a number of operating systems. They typically can communicate over LANs, WANs, and the Internet. They can operate as fast as if you were sitting in front of the remote desktop. They also have a high level of functionality that includes tools such as scripting capabilities, inventory collection and management, and session recording. They also have a higher level of encryption that often meets or exceeds current government standards. Many times they are used by help desk personnel and are deployed on hundreds and even thousands of PC's in an organization. Products in this category include NetOp Remote Control[6], PCAnywhere[7], RemotelyAnywhere[8], and a small handful of others. Just because these tools are wonderfully fast, and have security features does not make them secure. They often have fully functional trial versions that can be downloaded for free, and have been used by attackers to compromise government systems. One example is when a hacker named Gary Mckinnon[9] managed to install RemotelyAnywhere on some US Military systems. He was caught when they realized that the software was installed, and then traced Mr. Mckinnon back to the download site of the software company. The risks associated with these products are basically the same as the risks associated with a Microsoft Operating System. Like most Microsoft operating systems, the default configuration of the remote control programs is not the locked down, disallow everything that we as security professionals would like to see, but usually relatively wide open, and can be operated without any login or password requirements whatsoever.

Now that we have discussed the different types of remote control programs, NetOp Remote Control, and get right into how to completely lock it down.
Now that we have discussed three types or classes of remote control, lets talk about
Like many of the other Remote Control Products, there are some wonderful benefits to NetOp Remote Control. There is just something nice about being able to fix a silly end user problem or run an update from the comfort of your own office, or not having to drive an hour to a remote site at 3 in the morning to perform some silly account reset. The things that set NetOp Remote Control apart from many other remote control products are its scalability to a large enterprise, and its security features. NetOp Remote Control has been implemented in some cases on over 100,000 machines in an organization. NetOp Remote Control has the ability to encrypt everything with 256 bit AES[10] encryption, and also integrate with Windows Security Management or an LDAP Server to name a few of the security features.

---

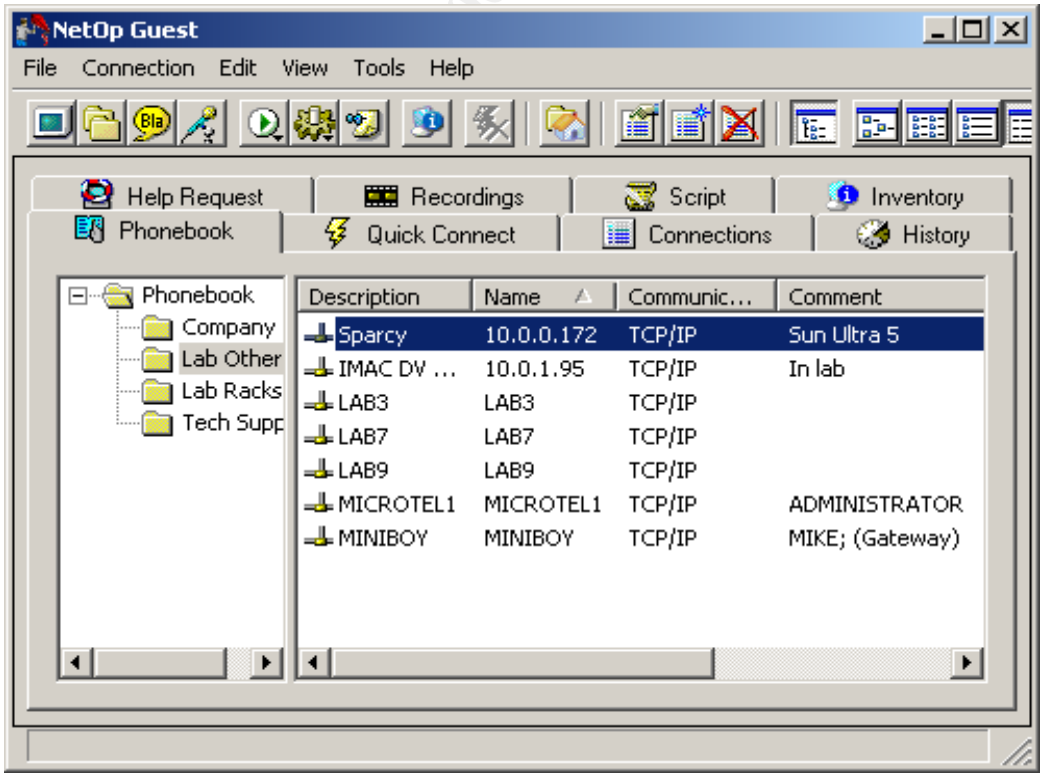
[6] NetOp Remote Control. URL: www.netop.com
[7] PCAnywhere. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=2
[8] Remotely Anywhere. URL: www.remotelyanywhere.com
[9] Williams, Brian. "Dot-Mil Hackers Download Mistake." Wired.com, 15 November 2002, URL: http://www.wired.com/news/technology/0,1282,56392,00.html.
[10] Advanced Encryption Standard. URL: http://csrc.nist.gov/CryptoToolkit/aes/

There are two main parts to a remote control session. One piece is the Guest, which is what the systems Administrator uses to control another machine, and the other is a Host, which resides on the machine being controlled, or the distant machine.

The way most people connect to the Host is with a standard NetOp Guest program, however there are some other ways to connect. Each involves a NetOp Guest, but in some cases, users might be connecting over the Internet with a NetOp Gateway, or using the ActiveX version of the Guest which can be integrated into a website. No matter how the connection is set up, there always has to be a Guest and a Host. Since the Host is at the remote location, and we want to keep the bad guys from having full keyboard and mouse control, we are going to focus on securing the Host, while at the same time maintaining functionality.

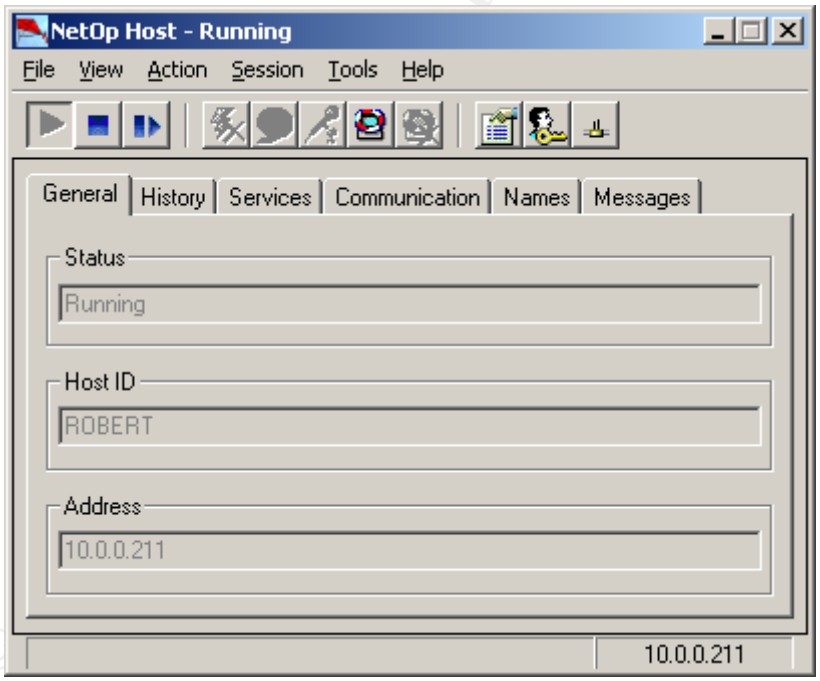
A full evaluation version of NetOp Remote Control can be obtained from the following URL for testing: www.crossteccorp.com/tryit. Note: It is required to fill out a short registration to obtain the free evaluation version.

We are now going to look at the major components of NetOp Remote Control: The Guest is the piece of software that resides on the computer where the user or administrator who is doing the controlling is physically sitting. It is the controlling piece. There are many tools and options available to the administrator from this interface. The Guest interface with the Phonebook tab is shown below.



An administrator can organize computers into groups by the folders on the left side of the screen, and then can connect to individual Hosts by double-clicking on the highlighted phonebook entry on the right hand side, or by right clicking on the entry and clicking remote control. It is an easy way to manage a large enterprise from one location.

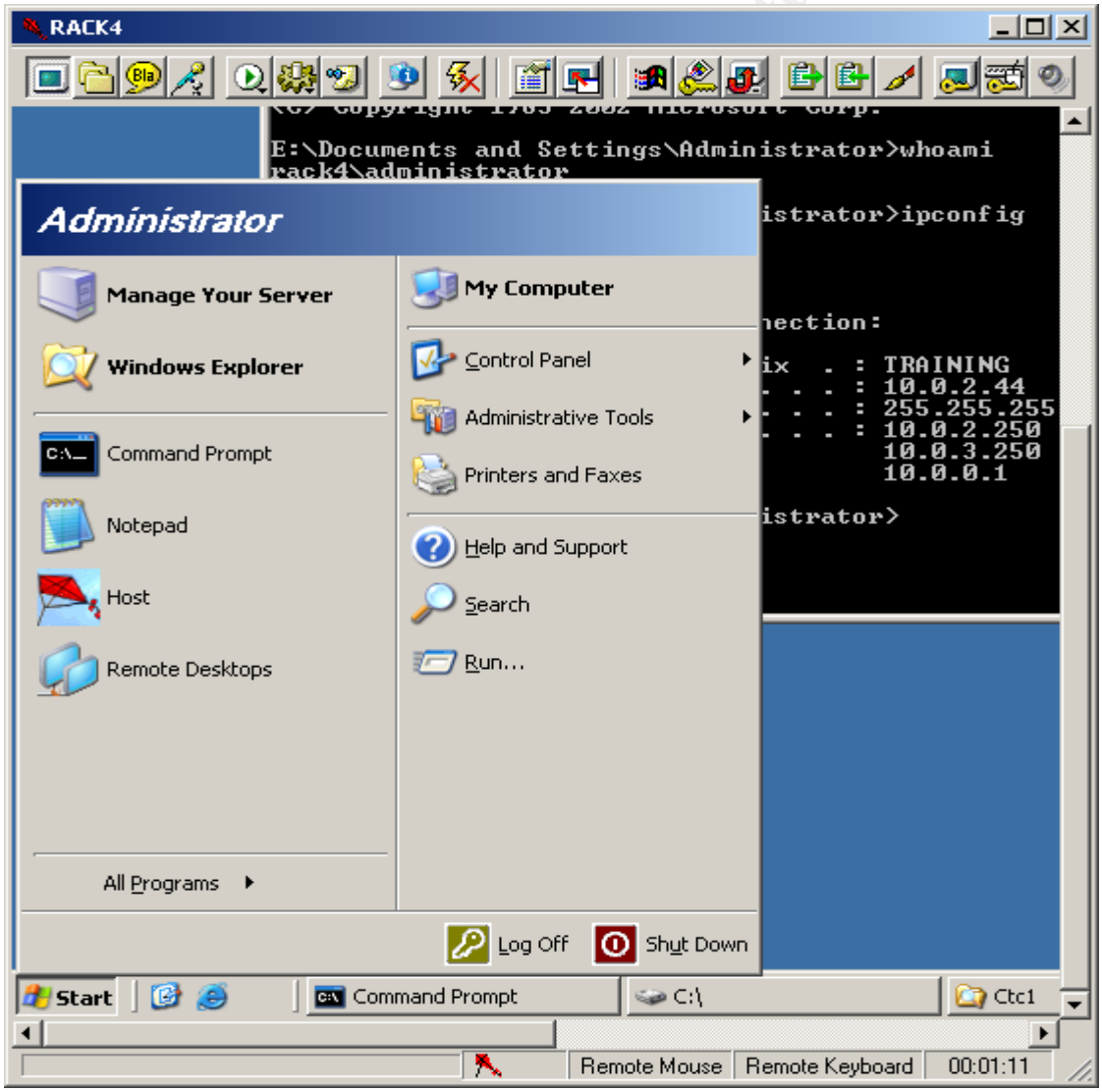
The Host interface resides on the computer that is being controlled. This interface can be hidden from the user of the remote machine if desired. The focus of this paper is locking down this piece of software since it is what sits on the machine that is being remotely controlled. With the default configuration, an attacker could possibly plug in a laptop to a port in a lobby or conference room, fire up a NetOp Guest (the free trial version that he just downloaded of course), browse the network, and connect to any server on the network. Most of the security configuration will be performed from the Tools menu on this interface. After the Host is configured to the desired security level in lab testing, the settings can be saved and deployed in the enterprise using whatever type of imaging or deployment tools that are used in the enterprise. The Host interface is shown below.



A Guest can call a Host in several ways, including IP address, Computer Name, and NetOp Host ID. NetOp can also run other operating systems such as Sun Solaris, Linux, OS2, and Mac OS X, but this paper will only focus on the Windows version.

Other NetOp modules, such as the Gateway, NameServer, and Security Server are described in detail in the NetOp Administrators Manual[11]. They are also modified Host Modules and many of the same security configuration that is described in this paper can be applied to any of them as well as the standard Host.

The window below shows a remote control session with a Windows 2003 Server. Even though only part of the screen is shown, you can easily view the entire desktop, or go to a full screen mode, where the desktop of the remote control session would cover everything on your desktop and it would appear as if you were sitting in front of the remote machine. The buttons across the top of the remote control window are the tools that can be used during a remote control session.



[11] NetOp Administrators Manual. URL: http://www.netop.com/tech/support/documentation/manuals.htm.

Now that we have seen the major parts of NetOp Remote Control, lets move on to the installation and securing of the NetOp Host. Now that you have purchased NetOp, or downloaded your evaluation version, I will explain quickly how to install the product. If installing from the CDROM, it should launch automatically, but since you are a security administrator, you probably have disabled that feature. Find the setup.exe file for your language on the CD and give it a double click. The setup program will run and take you through a series of windows, where you will have to click "Next" and "Yes" a few times to get through the setup. There are a couple of important windows to note during the setup, the first one is the second or third window allows you to select both the Guest and the Host. By default both are selected. If you are installing in your test environment, leaving them both selected is fine because you will be testing both parts, however in a production environment, you would only install the Host on the machines that you will be connecting to. The second window of note is the window that says "Type of host". You will always select the normal Host on your end user machines. There are three other Host modules available in this window. The first one is the Gateway, which lets you communicate from one protocol to another such as TCP/IP to IPX or NetBIOS, and have multiple NetOp sessions through the same port. The Gateway is usually used when an administrator is connecting to an internal network from the Internet. The gateway would reside on a machine with a static public IP address, and let authorized Guests get to normal Hosts inside the network. The second type of Host is the NetOp NameServer. These are normally used in extremely large WAN environments with many subnets to allow NetOp Guests to communicate with many machines with dynamic IP addresses. It resolves the Hosts IP address with the local computer name. The final Host module available is the NetOp Security Server. This Host module handles all the security configurations for multiple Hosts. It is also used in very large environments where users are coming in over the Internet, typically 1000 or more computers. Ok, now that we have got that out of the way, it is time to click finish, and NetOp is now installed. There is no rebooting required. There will be a folder opened on the desktop with a Guest and Host icon, or just a Host icon on your end user machines. Double-click the Host icon to start the Host. The first time the Host starts, a short wizard will guide you through getting started. It is pretty safe to select the defaults at this point, since we are going to go back and make a custom security configuration. By default, the NetOp Host forces you to put in a password before a Guest can connect to it. Hint: test, test123, abc, netop, administrator, and password are not good words to use here! According to the SANS/FBI Top 20 Most Critical Internet Security Vulnerabilities[12], accounts with no password or weak passwords is number seven on the Windows vulnerability list. Lets go ahead and make sure that we put a strong password here to help reduce the risks associated with poor passwords. Great job! Installation is done and now we are going to get to the fun stuff!

[12] SANS.org "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus." Version 3.23 May 29, 2003. URL: www.sans.org/top20

I am positive that as a security professional you installed in a test environment, not on a production server, or even on your workstation at work. I am also positive that you got written management approval before testing this software. Note: If you did not do either of the above things, stop right now! Move slowly away from the workstation or server! Go to the lab that is secure from the rest of the corporate network. Also check with management and get permission in writing to try this software. Some corporations have security policies forbidding the use of any type of remote control software. Ok, now that that is taken care of, let's look at what happened to your system during installation in the way of creating directories.

A default NetOp install creates the following directories:

C:\Program Files\Danware Data\NetOp Remote Control\Guest (if installed)
C:\Program Files\Danware Data\NetOp Remote Control\Host

C:\Documents and Settings\All Users\Application Data\Danware Data\NetOp Remote Control\Host
(This is where the Host configuration files are stored)

C:\Documents and Settings\%USERPROFILE%\Application Data\Danware Data\NetOp Remote Control\Guest (if installed)
(This is where the Guest configuration files are stored for each user)

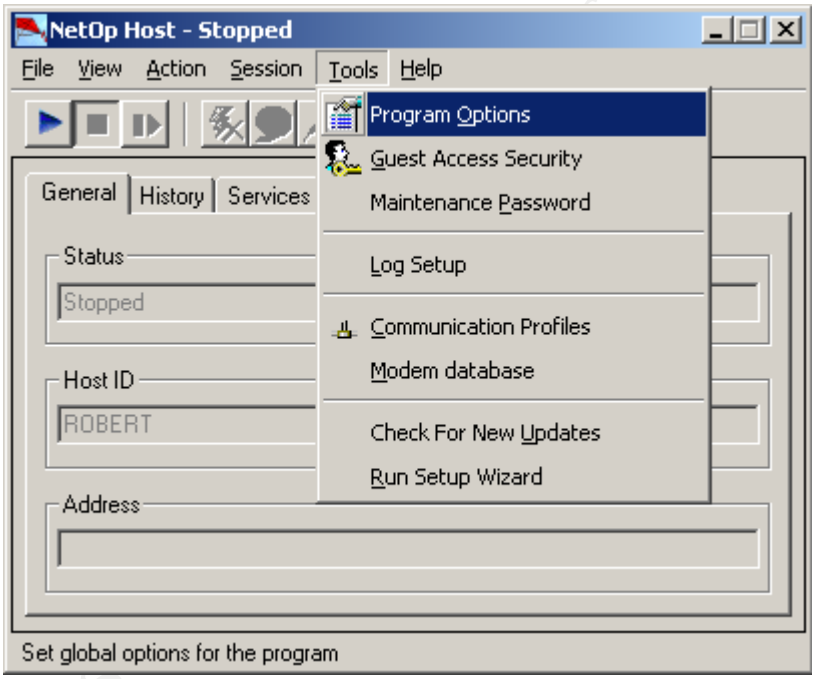
The only other major item of note is the NetOp.ini file, which is installed in the **C:\WINNT** directory or **C:\Windows** directory depending on the operating system.

Now that we have seen what happens more or less during the install, lets begin with the checklist for securing the Host.

This checklist is intended for use as a general guide to assist in having the most secure remote control session possible. Most of these settings will work on Windows 98 or above, however, they were tested on Windows 2000, Windows XP, and Windows 2003 Server. Some settings might not apply or be necessary for each environment. Some settings can also affect speed and functionality. If you have two computers in your home office connected with a crossover cable, and not connected to the internet, you wouldn't need the high encryption, etc, however if you are a systems administrator doing remote maintenance over the Internet on a machine in a medical office that holds patient data, or a company that has confidential data, such as news that a new patent will be approved in a week, then you would want the most secure session possible.

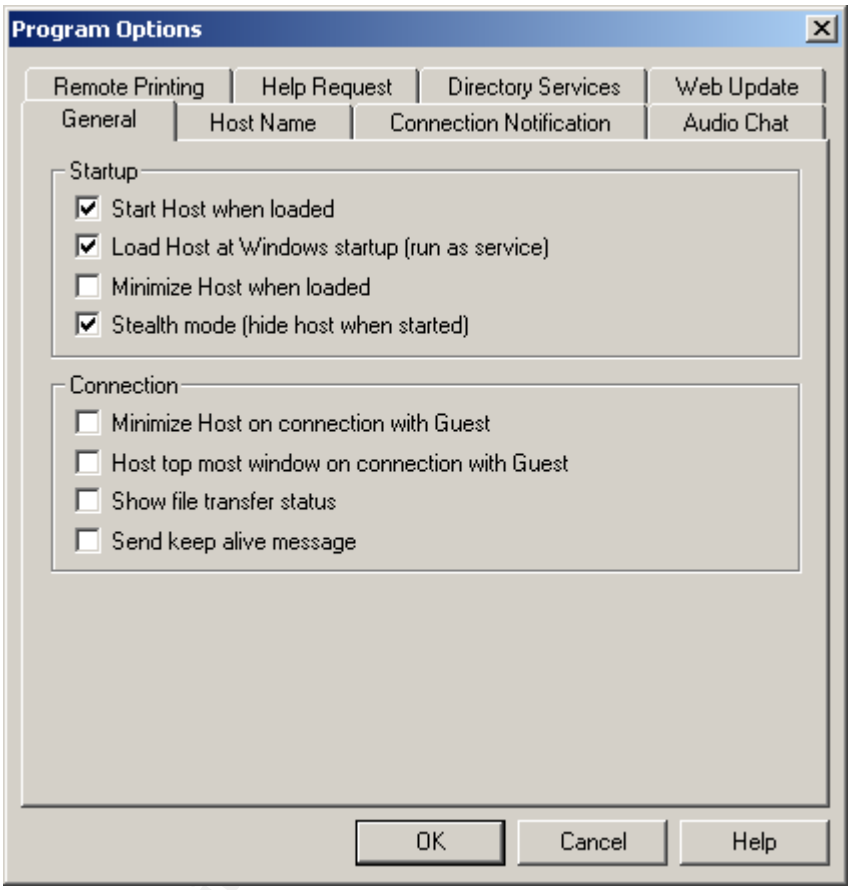
Disclaimer: Always test any configuration changes or build level updates in a non-production environment before implementing in a production environment. Also consult your company's security policy and obtain written approval from management before installing any type of software, especially any type of software that allows remote access or remote desktop capabilities.

Most of the security configuration will take place from the Tools Menu shown below, and we will work our way down each relevant option starting with program options. This menu is accessed by first clicking on the Tools menu item as shown.



Section 1: Program Options

In the program options menu, there are several tabs available. We will only cover the ones relevant to securing the Host. The program options menu with the General tab is shown below.



General Tab:

___ Check the Stealth Mode option: Stealth mode gives the user on the Host machine no indication that NetOp is installed or even running on the machine. To view the NetOp Host, the user must run the SHOWHOST.EXE program found in the Host folder in the Danware Data directory.

Host Name Tab:

___ Uncheck Public Host Name in Name Options: This prevents the host from responding to broadcasts from other guests. If an unauthorized user on the network downloaded an evaluation version of the NetOp Guest, and installed it, they would not see any NetOp Hosts on the network. This would force the attacker to not only know the computer name and/or IP address, but also to know that a NetOp Host is running as well.

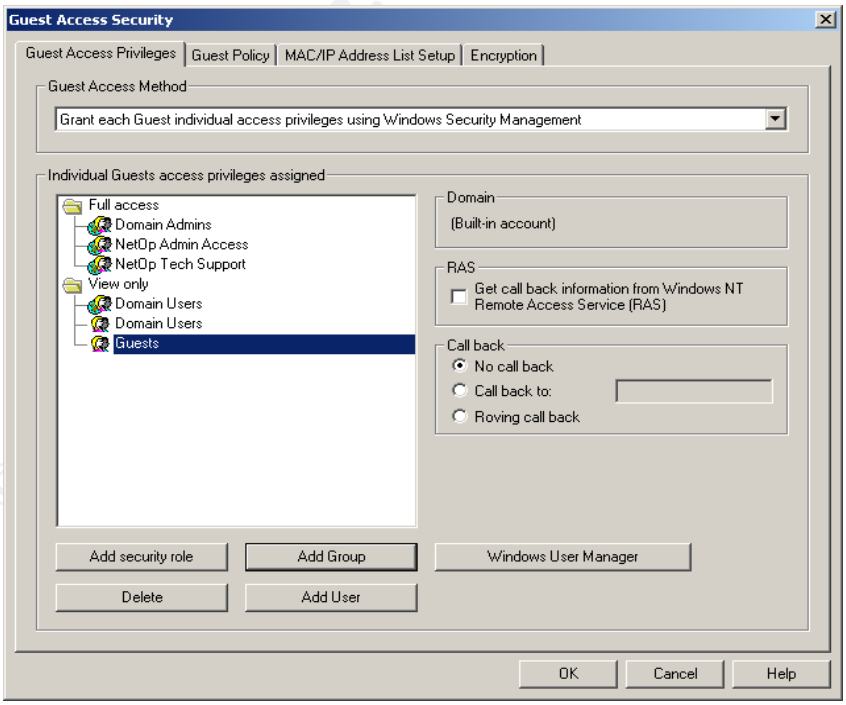
___ Change the default name of the NetOp NameServer: By default, the name in this field is “PUBLIC”. This name serves dual purpose. If using the NetOp NameServer (see users or administrators manual for detailed configuration information) the PUBLIC namespace will allow any other NetOp Guest to see this Host on the Internet. Many times a Guest user can simply enable the option to use the NetOp NameServer and browse the Internet and see a Host that some unsuspecting user did not put a password on their Host. By default the NameServer is not used with the host, but it is just a matter of putting a check mark in a box to enable it. The other purpose of the Name Space ID is during authentication[13].

Web Update Tab:

___ Update to be running the current build level. It is always important to be running the latest build of the software, however it is also important to test before applying any software updates. The current build can be determined by clicking Help, then About on the Host. That is where the version will be shown along with the date of the build. As of this document, the version is 7.60 and the build is shown in parenthesis as 2003146. 2003 is the year, and 146 will indicate the day of the year that the build was released.

Section 2. Guest Access Security

The Guest Access Security window is shown below.



[13] NetOp.com. “How NetOp modules employ encryption in version 7.x.” 05 March 2003. URL: http://www.netop.com/tech/support/documentation/encryption.htm

Guest Access Privileges Tab

___ Use Grant each Guest individual access privileges using Windows Security Management or Grant each Guest individual access privileges using Directory services. This allows customization of what a Guest user can do to a host. If the host is on a server, there are things that you can specify that a Guest cannot do such as restart the server, or run a program on the server. The Guest user would have to be able to log on to the server and perform functions while logged into the server rather than just being able to remotely restart the server. Also, do not add individual users, add groups to keep all users standardized, and reduce administrative overhead.

___ Use NetOp Security Server (where applicable): This option is mainly implemented in larger networks where more than 250 Hosts are used. It would be used in place of the above option. The NetOp Security Server is a special Host module that is a central management point for security configuration of all the Host modules on the network. It has a tool to let you manage security in one place for each Host in an organization without having to go from machine to machine to change the security configuration. It is best to install 2 NetOp Security Servers on 2 different machines in an organization for redundancy. Any time a Guest tries to connect to a Host that is using the NetOp Security Server, the Host checks with the NetOp Security Server to see if the Guest has the proper credentials to connect to the Host.

Guest Policy Tab

___ Password: This specifies the amount of times a Guest can attempt to connect to a Host before being disconnected. By default, after 3 failed attempts to connect, the Guest is disconnected. This can help prevent brute force attacks.

___ Select Lock Computer after disconnect: This will force the Guest user to enter the local password to unlock the machine if they have been disconnected due to failed logon attempts.

___ Select Disable file transfer before local login: NetOp has a wonderful file transfer feature that allows drag and drop of files and folders between the controlling machine and the remote machine. The Guest only has to authenticate with the Host in order for this feature to work. Disabling file transfer forces the Guest user to log in to the local machine before being able to perform a file transfer. This prevents a user that does not have local login privileges from getting any from the remote machine or sending files to the remote machine.

___ Enable record sessions: This depends on how often the machine will be remote controlled. If this is enabled, each remote control session will be recorded and can be played back by a user with a guest. Best practice would be to record the sessions to protected network drive or protected folder for viewing at a later time. Attackers frequently try to cover their tracks by deleting anything

that can show that they have been there. As equally as important as enabling this feature is to establish some sort of schedule to review the recorded sessions to make sure that only authorized users are connecting to your machines. The files can be collected via NetOp Scripts and viewed from a machine that has a Guest interface on it.

___ Confirm Access Timeout: only enable if the user logged into the remote computer has to give the Guest permission to connect. 30 seconds to a minute is usually sufficient for a user to decide if they want to let someone connect to their computer.

___ Authentication timeout: 1 minute. The authentication process takes longer if using the highest levels of authentication.

___ Inactivity: 5-15 minutes depending on what company security policy states. If a Guest user is connected and remote controlling a Host, and walks away from his or her computer, this prevents an unauthorized user from remote controlling the Host machine.

Mac/IP Address List Setup Tab

___ Enable IP address or MAC address lookup of Guest users (if static IP Addresses). If using another protocol such as NetBIOS or IPX, enter the MAC Address of the Network Interface Card. This keeps ensures that only certain machines can connect to the host. Note: Both IP and MAC addresses can be spoofed. Also if the MAC/IP address check is used, the browse function is disabled. The Host will not show up to a Guest user who tries to browse the network for running hosts.

Encryption Tab

___ Uncheck all other encryption except for Very High. Clicking on the show details button will reveal the characteristics of Very High Encryption below:

Encryption:
- Keyboard and mouse: 256 bit AES
- Screen and other data: 256 bit AES
- Logon and password: 256 bit AES

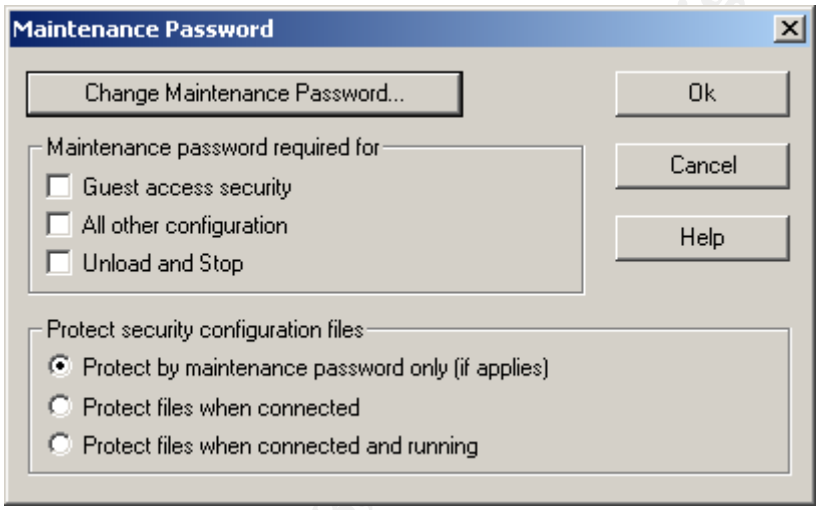
Integrity Check:
- Keyboard and mouse: 256 bit SHA HMACs
- Screen and other data: 256 bit SHA HMACs
- Logon and password: 256 bit SHA HMACs

Key Exchange: Combination of 2048 bits Diffie Helman, 256 bit AES and 512 bit SHA

This means that the Host is only able to communicate with the above encryption levels. These settings will also depend on your operating environment and speed requirements. If you are on an internal network behind a firewall or not connected to the network at all, it is possible to use no encryption for maximum speed.

Section 3: Maintenance Password Section

Below is the maintenance password window.



___ Choose a strong maintenance password: The maintenance password by default is not in use on the Guest or the Host. This password basically protects all the options on the tools menu, and keeps a Host user from shutting down the Host.

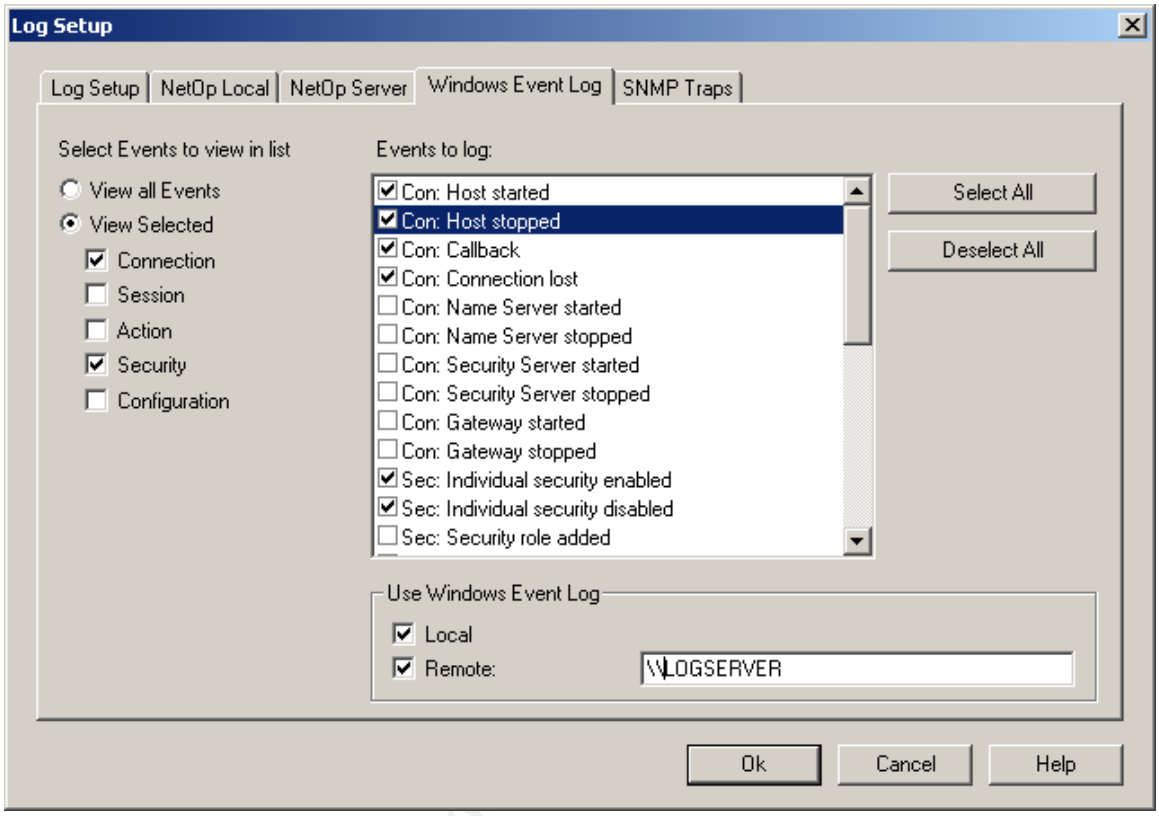
___ Check off all options in the section “Maintenance password required for”. This includes the following:

> **Guest Access Security:** Menu to change all security settings on the Host modules.
> **All other configuration:** Includes all of the options on the tools menu except for Guest Access Security.
> **Unload and stop:** Requires the password to stop the Host Module.

___ Select “Protect files when connected and running” in the Protect Security Configuration Files section. If this option is selected, none of the configuration files can be altered while the Host is running or connected. The Host must first be stopped, then changes can be made.

Section 4: Log Setup Section

The Logging window is shown below opened to the Windows Event Log tab.



___ Enable logging: There are several options in the logging section. For ease of management it is probably best to log to the Windows Event Log, to reduce the number of places that you have to go to look for errors. Also carefully plan what you want to log. At a minimum, select to log all the security events, so if any security changes are made, you will know about them. Also there is an option to log to a local or remote server. Attackers always like to cover their tracks, so if users log to a remote server, an attacker would have to delete the local event logs, and also compromise another machine, get into its event logs, and delete the events related to their attack. To log to a server on the LAN, enter the Windows Computer Name of the server that you want to log to.

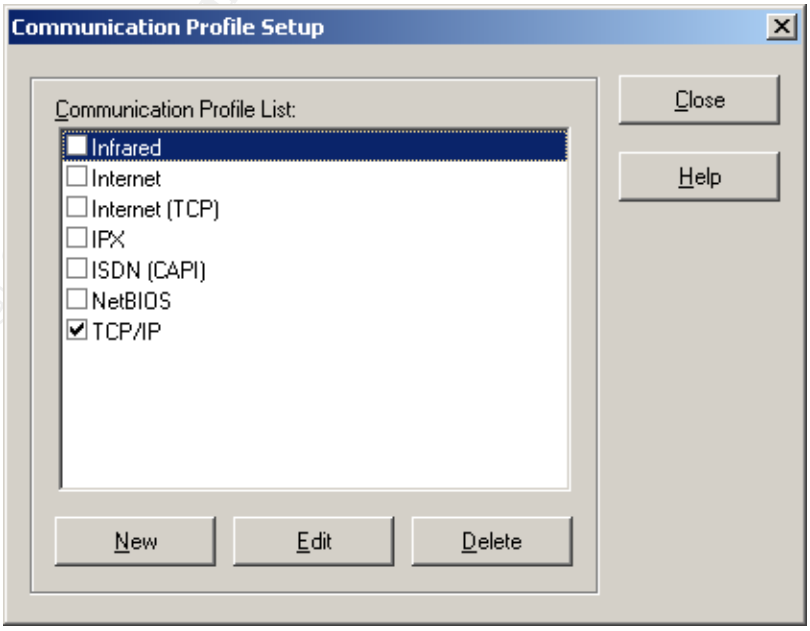
The security events that can be logged and their event codes are shown below.

Security

Event Name	Event Code	Arguments
Sec: Individual security enabled (and changed)	HSECINDIV+	Guest access method
Sec: Individual security disabled	HSECINDIV-	Guest access method
Sec: Security role added	HSECROLE +	Security role name
Sec: Security role deleted	HSECROLE -	Security role name
Sec: Security role changed	HSECROLE *	
Sec: Guest added to role	HSECGUEST+	Guest name
Sec: Guest deleted from role	HSECGUEST-	Guest name
Sec: Guest changed in role	HSECGUEST*	
Sec: Password enabled	HSECPW +	If *individual*: Guest name
Sec: Password disabled	HSECPW -	If *individual*: Guest name
Sec: Password changed	HSECPW *	If *individual*: Guest name
Sec: Callback enabled (*default* only)	HSECCALLB+	(none)
Sec: Callback disabled (*default* only)	HSECCALLB-	(none)
Sec: Callback changed (*default* only)	HSECCALLB*	(none)
Sec: Confirm access enabled	HSECCA +	If *individual*: security role name
Sec: Confirm access disabled	HSECCA -	If *individual*: security role name
Sec: Password rejected	*SECPW !	Guest name
Sec: Confirm access denied	*SECCA !	(none)
Sec: Illegal password limit reached	HSECPWLIM!	(none)
Sec: Timeout limit exceeded	HSECTMOUT	AC (inactivity), AU (authentication) or CA (confirm access).

Section 5: Communication Profiles

The Communication Profile Setup Window is shown below.



___ Remove all unused communication profiles: In NetOp terminology communication profiles determine how a Guest and Host talk to each other. NetOp is able to communicate over a variety of protocols including Modem or Point-to-Point, TCP/IP, IPX, NetBIOS, ISDN, or Infrared. Delete all unused communication profiles. In most LAN or WAN scenarios, you will want to use TCP/IP (UDP). If connecting from the Internet, use the Internet communication profile, which in NetOp's case is really TCP/IP (UDP) with a smaller packet size to be more efficient over the Internet. This will just reduce the ways someone can connect to the Host. This would usually only come into play if someone already has physical access to the machine, or the machine is already compromised by some other method.

___ Change default port numbers: Change port numbers by clicking on the TCP/IP communication profile, then clicking Edit, then Advanced. By default NetOp runs on UDP Port 6502. Anyone downloading a trial version is also by default running on Port 6502. This can pose a problem when an attacker from the outside does a port scan, and finds a listening port 6502. If they are on the network, and know a couple of common tools, they can find out enough information to try and exploit this. Change to a different port number that is not in use by another application, or better yet, use 2 port numbers, one to send and the other to receive. Just make sure that in the Guest, the Send port is the same as the Receive port on the host, and vice versa from Host to Guest.
Below we will show the results from 4 probes with 3 different scanning type tools. The first two probes are probes that would be done from a person on a machine inside the network. The second two are NMAP probes from a Linux box that could be done from outside the network.

Note: The output of these commands has been edited for ease of viewing for the paper as well as just to highlight the most important parts.

The first probe shows the results from the netstat command, which is a Microsoft Windows command that displays statistics for current TCP/IP connections. This tool or command is built into every current Windows operating system.

C:\>netstat -a

Active Connections

Proto	Local Address	Foreign Address	State
TCP	robert: 1719	SERVER:netbios-ssn	ESTABLISHED
TCP	robert: 1721	SERVER2:netbios-ssn	ESTABLISHED
TCP	robert: 5101	10.0.0.21:1442	ESTABLISHED
UDP	robert: epmap	*:*	
UDP	**robert: 6502**	***:***	

The bottom bold line shows port 6502 open. One interesting thing about this output is that it does not tell that it is NetOp; it just shows the open port, but if the

attacker knows that NetOp is being used, they know that it is on this machine, and can then try to exploit it.

The second probe or test if you will is done with Fport.exe[14] from Foundstone. This free tool takes the Netstat command one step further by matching open ports with services and even the directory where the services are running.

FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid	Process		Port	Proto	Path
444	svchost	->	135	TCP	C:\WINNT\system32\svchost.exe
748	MSTask	->	1026	TCP	C:\WINNT\system32\MSTask.exe
8	System	->	1027	TCP	
252	services	->	1025	UDP	C:\WINNT\system32\services.exe
1484	**Nhstw32**	**->**	**6502**	**UDP**	**E:\Program Files\NRC 7-6\HOST\Nhstw32.exe**

Notice that the tool reveals some interesting information such as the Pid, or process ID, the process associated with the service, and even better the folder where the program is located. The very bottom line, which is in bold shows the NetOp Host service (Nhstw32) running on port 6502 UDP, and it is in the E:\Program Files\NRC 7-6\HOST\ directory. This tool will show the service no matter which port it is on, but it is just something to look out for when deciding whether or not to let your end users install programs on their machines.

The final two scans are from a Linux box running NMAP[15]. This can be done from inside or outside the network, depending on how NetOp is being used. On the first scan we do a simple UDP scan, using the –sU switch on the nmap command. We are scanning a Windows 2003 server.

[root@Rack5 root]# nmap -sU 10.0.1.171
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on (10.0.1.171):
(The 1461 ports scanned but not shown below are in state: closed)

Port	State	Service
135/udp	open	loc-srv
137/udp	open	netbios-ns
138/udp	open	netbios-dgm
445/udp	open	microsoft-ds
500/udp	open	isakmp
4500/udp	open	sae-urn
6502/udp	**open**	**netop-rc**

Nmap run completed -- 1 IP address (1 host up) scanned in 9 seconds

[14] Foundstone.com URL: http://www.foundstone.com/resources/proddesc/fport.htm
[15] Insecure.org URL: www.insecure.org/nmap

Notice the line in bold that shows NetOp-RC running on port 6502. The service part that says netop-rc is something that nmap knows runs on that port. We then changed the default port to 10000, and scanned the machine with the same nmap command. The port didn't show up with just the –sU switch, so we added the –p switch and scanned a range of ports making sure we included port 10000 to see what we found.

[root@Rack5 root]# nmap –sU –p 1024-20000 10.0.1.171
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on (10.0.1.171):
(The 18973 ports scanned but not shown below are in state: closed)

Port	State	Service
1029/udp	open	unknown
1100/udp	open	unknown
10000/udp	**open**	**unknown ß (THIS IS NETOP)**

Nmap run completed -- 1 IP address (1 host up) scanned in 47 seconds

The bottom line in bold lettering shows our open port 10000. Notice that it says unknown, and doesn't advertise to the attacker that there is a NetOp Remote Control Host waiting to be exploited, therefore an external attacker would have no idea that this port is NetOp unless he was told that NetOp was on the machine, or had physical access to the machine.

___ Remove NetOp Name Server addresses if not in use: The NetOp Name Server (NNS) can be used to map IP addresses to NetOp Host names in large environments and over the Internet. There are 2 public NetOp Name Servers. The first one is nns1.netop.com and the second one is nns2.netop.dk. If someone accidentally or maliciously enables the nameserver, it could pose a potential problem. If the NNS is enabled each time the Host is started, or the machine is rebooted, it will register with the NNS. Anyone with a Guest module, who enables the NNS can browse, and see all the Hosts if they are using the PUBLIC (Default) Name Space ID.

___ Disable the local subnet broadcast: With this option checked, if someone installs a Guest either licensed or trial version and clicks the Browse button to see if there are any available hosts, none will show up. There could be 1, 5, or 50 hosts that are awaiting connection, but they just will not appear in the Browse list on the Guest. The attacker would have to know that there are Hosts installed on the machines they are trying to access.

Section 6: Other Miscellaneous configurations

___ Closed user group licensing option: If purchasing a large amount of Hosts for your enterprise, check and see if a closed user group is available. A closed user group is a special license that is unique to the organization, and only Guests and Hosts that have the special license can communicate with each other. Someone who downloads a trial version, or steals a serial number will not be able to connect to Hosts that have this license. There is no extra cost for a closed user group. It is best practice to request one if purchasing for a large implementation.

___ Protect the NETOP.INI file: This file is stored in the C:\WINNT directory. Make this file read only. There is no need to write to this file unless it is to be modified. The file tells NetOp where to look for its configuration files among other things. An attacker on the network can edit this file to point to different configuration files to override settings. We actually saw this at a school. The student thought that it would be enjoyable to modify the NETOP.INI file by adding the line that is highlighted in bold lettering below.

```
[INSTALL]
DIRECTORY=e:\program files\nrc 7_6
FOLDER=NRC
SCHOOL_DIRECTORY=E:\Program Files\NetOp School
SCHOOL_FOLDER=NS
[COEXISTENCE]
COEXIST=2
LOAD_WARNING=1
[GUEST]
LicenseWarning=0
[HOST]
LicenseWarning=0
ActualBufferReleaseBlock=300 4600
DataPath=X: \  (This makes NetOp look for its configuration files in the X:\ drive when the Host starts up)
```

That little entry effectively rendered the Host useless on next startup. The lesson to be learned here is do not give people more rights than they need. In this case the users were all in the Power Users Group. A person in the Users Group or Authenticated Users Group is unable to modify files in the C:\WINNT directory. Ordinarily, you would simply fire the person for violating the security policy, but it was a student. I personally know a few teachers who wish they could fire some of their more creative or technically savvy students! A list of all the NETOP.INI settings can be found on the NetOp Technical Support Website[16]. That's exactly where the mischievous student located the NETOP.INI setting he needed to cause the problem!

[16] NetOp.com, "Overview of available netop.ini settings." URL: http://www.netop.com/tech/support/other/netop_ini_pub_settings.htm

___ Remove SHOWHOST.EXE: This file resides in the C:\Program Files\Danware Data\NetOp Remote Control\Host folder. It is used to open the Host and view the Host interface. Even though you have configured your Hosts to run in Stealth Mode, this little program opens the GUI interface for the host. Remove it. You can put it on a floppy diskette, CDROM, or on some network drive that only system administrators have access to. This will prevent an attacker from opening the GUI and trying to modify the configuration.

This completes the checklist on securing the NetOp Remote Control Host. Following it step by step will help ensure that you are able to have the most secure remote control sessions possible. Below I have included a shortened format of the checklist that can be printed and used to check off items as you are securing your machines. Modify it to suit your organization, but try and come up with a standard format so you don't have 50 different security configurations. You will also sleep better at night, at least until you get that 3:00 am phone call requiring you to fix some problem. At least by implementing the checklist, you will have some comfort knowing that you can fix it from your desk in 5 minutes securely rather than driving all the way to the office to sit in front of a machine and restart some service!

The Checklist, Quick and Dirty:

Tools Menu

Program Options Section

General Tab

___ Check the Stealth Mode option

Host Name Tab

___ Uncheck Public Host Name in Name Options
___ Change the default name of the NetOp NameServer

Web Update Tab

___ Update to be running the current build level.

Guest Access Security section

Guest Access Privileges Tab

___ Use NetOp Authentication or Windows Security Management (anything but Grant All Guests Default access privileges)

___ Use NetOp Security Server (if applicable)

Guest Policy Tab

___ Password (3 password attempts to disconnect)
___ Select Disable file transfer before local login
___ Enable record sessions
___ Confirm Access Timeout
___ Authentication timeout: 1 minute
___ Inactivity: 5-15 minutes

MAC/IP Address List Setup Tab

___ Add IP if connecting from a static IP address or MAC address if using another communication protocol.

Encryption

___ Uncheck all other encryption except for Very High.

Maintenance Password Section

___ Choose a strong maintenance password.
___ Check off all options in the section “Maintenance password required for”.
___ Select “Protect files when connected and running” in the Protect Security Configuration Files section.

Log Setup Section

___ Enable logging.
___ Log all security events at minimum.
___ Log to a remote server.

Communication Profiles Section

___ Remove all unused communication profiles
___ Change default port numbers
___ Remove NetOp Name Server addresses if not in use
___ Disable the local subnet broadcast

Other Miscellaneous configurations
___ Closed user group (if applicable)
___ Protect NetOp.ini
___ Remove SHOWHOST.EXE

References:

NWInternet.com. "NetBus, BO's Older Cousin." 25 November 1998. URL: http://www.nwinternet.com/~pchelp/nb/netbus.htm

Cult of The Dead Cow. "Back Orifice Remote Administration Tool." URL: http://www.cultdeadcow.com/tools/bo.html

Virtual Network Computing. URL: http://www.uk.research.att.com/vnc/

Microsoft Remote Desktop. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/pree_rem_fhca.asp

Microsoft Remote Assistance. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/rmassist.asp

NetOp Remote Control. URL: www.netop.com

PCAnywhere. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=2

Remotely Anywhere. URL: www.remotelyanywhere.com

Williams, Brian. "Dot-Mil Hackers Download Mistake." Wired.com, 15 November 2002, URL: http://www.wired.com/news/technology/0,1282,56392,00.html.

Advanced Encryption Standard. URL: http://csrc.nist.gov/CryptoToolkit/aes/

NetOp Administrators Manual. URL: http://www.netop.com/tech/support/documentation/manuals.htm.

SANS.org "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus." Version 3.23 May 29, 2003. URL: www.sans.org/top20

NetOp.com. "How NetOp modules employ encryption in version 7.x." 05 March 2003. URL: http://www.netop.com/tech/support/documentation/encryption.htm

Foundstone.com URL: http://www.foundstone.com/resources/proddesc/fport.htm

Insecure.org URL: www.insecure.org/nmap

NetOp.com, “Overview of available netop.ini settings.” URL:
http://www.netop.com/tech/support/other/netop_ini_pub_settings.htm