*Preparing NT for a firewall*

# Armoring NT

**Lance Spitzner**
http://www.enteract.com/~lspitz/papers.html
Last Modified: 16 April, 2000

**Firewalls are one of the fastest growing tools in the field of information security. However, a firewall is only as secure as the operating system it resides upon. This article will take a step by step look at how you can best armor your NT box in preparation for a firewall. These steps can apply to any situation, however I will be using Checkpoint Firewall 1 on NT 4.0 as an example.**

## Installation

The best place to start in armoring your NT system is at the beginning, OS installation. Since this is your firewall, you cannot trust any previous installations. You want to start clean, where you can guarantee the system integrity. Also, NT is unique in that a great deal of the system armoring happens during the installation process. Even if you have just received the system from the manufacture, I recommend rebuilding the system so you know exactly what is running.

Place your system in an isolated network. At no time do you want to connect this box to an active network nor the Internet, exposing the system to a possible compromise. To get service packs and hot fixes later, you will need a second box that acts as a go between. This second box will download files from the Internet, then either burn them to a cdrom, or connect to your isolated, configuration "network" to transfer critical files. I have personally witnessed systems hacked within 15 minutes of connecting to the Internet. Morale of the story is keep your system isolated until it is fully armored.

Once you have placed your future firewall in an isolated network, you are ready to begin. For NT, a great deal of armoring happens during the installation process, so we will be covering it in detail. To begin with, we have two different options of which software to install, Workstation or Server. I recommend Server for several reasons. First, NT Server comes with the ability to mirror drives, whereas NT Workstation doesn't come standard with that ability. Second, NT server can handle far more connections then NT workstation (default is 5). This is critical if you intend on running any proxy applications on your firewall, such as the http or telnet security servers. Also, the registry permissions on NT Server are more restrictive.

NT installation begins with the command line interface. Here you select which partitions you install on and what file system you want, FAT or NTFS. I highly recommend NTFS, as it allows far great control and security of your file system. After this, you will begin the GUI part of the installation. From here you will select what kind of server to install, which services will run, and general system configuration. Remember, the whole idea during this process is to install and configure as few services as possible. The fewer services that are running, the fewer exploits or security issues you will have.

Following some initial licensing questions, you will be asked which OS package to load, There are three options, Primary Domain Controller, Backup Domain Controller, and Stand-Alone. I recommend Stand-Alone as this is our firewall and it should be doing only one thing, firewalling. After several more system options, you will be asked to select software components. By default, the system will install Accessories, Communications, Multimedia, and Accessibility. I highly recommend you eliminate at least Communications, Multimedia and Accessibility. Once again, the less software you install, the better. The system will then ask you if you want to install IIS web server (by default, it does). Do NOT install this, a web server is the last thing you want running on your firewall. After this, you will install and configure your NICs (Network Interface Cards). By default, the system installs both IPX and TCP/IP for the cards. Be sure you select only TCP/IP. Firewall 1 does not filter IPX. If your system is routing IPX, all IPX traffic will go right through the firewall (normally considered a bad thing).

Next, you will select what services you want to install. By default, the system will install RPC, Net BIOS, Workstation, and Server. We cannot de-select these services now, however we will be removing them later. The only service you may want to add here is SNMP. The firewall Management Module uses SNMP to monitor firewall modules (System Status Viewer). If you will not be using this feature, or do not have any distributed firewalls, you do not need SNMP.

After that, you configure your TCP/IP stack. Here you select the IP address, default router, and DNS server. Do NOT configure a WINS server or DHCP relay. We want to minimize what the firewall communicates with. Remember to enable IP Forwarding. If you do not enable this, your firewall will not route traffic (this however definitely makes for a more secure network :). The last thing the install process configures is what Domain or Workgroup you want to belong to. Well, you don't, you want to isolate the system as much as possible. I recommend creating a nonexistent Workgroup.

Following your installation (and reboot) we will want to install the latest Service Pack (current Service Pack 6a ) and the latest hotfixes. Staying current with the latest exploits is critical for a secure system.

# Eliminating Services & Tweaking

Once you have installed the latest Service Pack and hotfixes, there is allot of cleaning up to do. The first priority is turning off the services we had to install earlier. Go into Network Neighborhood properties and select Services. From here, remove RPC Configuration, Net BIOS Interface, Workstation, Server, and Computer Browser. None of these services are required to run a firewall, they only add possible security vulnerabilities. The only thing we should have left is SNMP Service (if you opted to install it). Several people have mentioned that they do not like to remove Workstation or Server because they lose some specific functionality. I leave the decision up to you, the reader :)

> " I like to keep workstation because it allows useful things like AT to run. I like to keep server because if you tweak the service for network applications, the firewall does run faster than not having the server service installed. Besides, if you unbind WINS and setup rules to block NBT to the firewall, you are killing access to these services at two levels already. If you really want to be secure, open user manager and remove everyone's right to logon from the network. (Chris Brenton)"

There are two other places we can eliminate services. The first is to disable WINS from our NICs (Network Interface Cards). This is done by going into Network Properties -> Bindings -> All Protocols -> WINS Client(TCP/IP). It should look something like this. The second place is the services menu itself, found in Settings -> Control Panel -> Services. Here you can disable several services that are manually or automatically started at bootup. I recommend disabling TCP/IP NetBIOS Helper. Anything else is done at your own risk :)

No additional services should be installed on the firewall, such as telnet, ftp, or PCanywhere. Limit access to console only. Most firewalls, including, Check Point Firewall-1, provide a client GUI that allows remote management of the firewall. All other system administration should be done physically on the system. The only software you may want to install is some form of anti-virus protection. Once again, the less that is running on our firewall, the better.

Next, we want to prevent the logon name of the last user from being displayed on the screen. To do this, set the Registry value of `DontDisplayLastUsername` to 1. You can find this at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
```

We also want to create a logon banner for all users. This banner will be a legal warning, forbidding any unauthorized access. To do this, set the Registry value `LegalNoticeCaption` with a short caption, and `LegalNoticeText` with the banner itself. You can find this at

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
```

To restrict anonymous connections to list account names, set `RestrictAnonymous` to 1
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

To restrict network access to the registry, create the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentcontrolSet\Control\SecurePipeServers\winreg`

# Accounts and Policies

There are a variety of modifications we can make to system accounts and permissions. The first is to change the name Administrator. By default, this is the logon account that has full privileges, so we want to protect this account. By changing the name, which everyone in the world already knows, we add one more layer of security. Also, have all admin users logon with their own respective accounts , without giving them the password for the "Admin" account. This allows you to track who is doing what. Another idea is to create a new dummy Administrator account that has no privileges, and track to see if anyone attempts to logon with the account.

Next, we want to control who has access to what on the system. I recommend having no more then two groups with access to the firewall, Administrators (for full access) and Power Users or Users (depending on what access they need). If you can limit access to only Administrators, that is even better. Regardless, the actual number of people who are authorized access should be no more then 2-4 people. The fewer hands that touch the keyboard, the better.

The next step is focusing on the system policies, specifically "Account", "User Rights" and "Audit", which you will find under User manager.

- **Account Policy** controls how user passwords and logon accounts are used. Several changes are recommended here.
    - Set "Minimum Password Length" to 8 characters
    - Set "Account lockout" to lockout after 3 bad logon attempts, reset counter after 30 minutes.

- **User Rights** controls who can access what, such as "Log on locally" and "Manage auditing and security log". I recommend limiting access to the two groups we discussed earlier. If nothing else, be sure to eliminate the group "Everyone" from all access.

- **Audit Policy** determines what events are logged. As this is our firewall, we want to log a variety of evens. I recommend you audit the following events.
    - Logon and Logoff (Both Success and Failure)
    - Security Policy Changes (Both Success and Failure)
    - Restart, Shutdown, and System (Both Success and Failure)

Whenever a user is done using the system for a particular session, they should ALWAYS logout with CTL-ALT-DEL. In case they forgot to do this, ensure you have a password protected screen saver that kicks in after no more then 5 minutes of inactivity.

# Staying Current

The problem with security is, by the time your system is secured, a new exploit has been released! So, to help you stay current, I recommend the following:

- First, subscribe to a listserv, so you will be updated via email with the latest security issues. Sometimes I forget to check out what the latest vulnerabilities are. The nice thing about a listserv is it comes to you. I recommend NTbugtraq or NTsecurity
- For websites, some of my favorite are www.ntsecurity.net, www.ntobjectives.com,and www.l0pht.com, ntsecurity focuses on securing you NT system, ntobjectives has several excellent security and admin NT utilities, and l0pht focus on hacking your NT system. Theses sites make an excellent combination.
- To audit your new installation, I highly recommend the tool WS_Ping ProPack. This Windows 95/NT tools has a variety of great utilities normally found on unix systems, to include a port scanner, snmpwalk, NetBios scanner, etc. Scan your system monthly to ensure nothing has been accidentally left open.
- Type the command "netstat -na", and make sure you do not have any connections open. The command shows what ports are listening, and if you have any established connections. The only connection you should see is UDP 161, which is SNMP (and that is only if you installed it). I highly recommend you check your system regularly with the "netstat -na" command. This ensures that no surprises "sneak up on you".

# Conclusion

We have covered some of the more basic steps involved in armoring a NT 4.0 box. The key to a secure system is having the minimal software installed, with security in layers. There are many additional steps that can be taken, such as file permissions, additional registry hacks, 3rd party software, etc. Remember, no system is truly 100% secure. However, with the steps outlined above, you greatly reduce the security risks.

***Author's bio***

*Lance Spitzner enjoys learning by blowing up his Unix systems at home. Before this, he was an Officer in the Rapid Deployment Force, where he blew up things of a different nature. You can reach him at lance@spitzner.net*