Protecting Your Networks With and Without Firewalls: Part VIII — NT Security

BY MARK BELL

IT departments are in the midst of a honeymoon period with NT. This operating system uses visually-based tools, has a short learning curve compared to UNIX, VMS, or MVS, and uses comparatively cheap hardware. NT has some superb applications available, including SQL server, that can match most of the characteristics of mainframe databases at a fraction of the cost. However, NT still has a serious rival; UNIX systems, including the under-rated LINUX, are capable of out-performing NT. UNIX is a multi-user operating system, whereas NT is still a single-user system. Hydra, the multi-user version of NT is still in beta, and comparisons with other operating systems have yet to be made.

NT is here to stay, and one of the reasons for its success has been the belief in its inherent security. While Microsoft's marketing department can take much of the credit for this, there has always been a perception that UNIX is insecure, and this has helped spur NT sales. However, all operating systems have security problems. Though none of the comments in this article should dissuade you from using or purchasing NT, you need to be aware of security concerns as they pertain to NT. You should be cautious about any new operating system or improved versions of old ones.

C2 SECURITY

One of the earliest arguments used in favor of NT (3.51) was C2 certification. C2 is part of the *Orange Book*, which is officially titled the "Department of Defense Trusted Computer Evaluation." The *Orange Book* was part of the "rainbow" series of specifications released by the DoD in 1982. Each specification in the series was released in a book with a colored cover.

Unfortunately, problems exist with the C2 classification: None of the *Orange Book* specifications, including C2, cover networks. At the time the *Orange Book* protocols were being specified, computer networks were still not common. However, when the specifications were published (December 1985) this situation had changed. Additional specifications concerning network security were published in 1987 in the *Red Book* titled "Trusted Network Interpretation of the Trusted Computer Systems Evaluation." NT has not been awarded *Red Book* certification.

C2 relies on limiting access to authorized personnel by using passwords and physical security; the computer should be in a locked room, guarded by a security guard or an appropriate electronic device such as a card entry system. Once the physical access has been restricted, then the computer itself must be configured to be C2-compliant. Microsoft has supplied the C2 audit program on the NT resource kit to assist this process. If you use this program, you will see that item 12 on the list of tasks is to remove all network connections. Clearly, C2 cannot apply to anything but a standalone workstation — servers are out and so is an NT workstation that is connected to a network!

If you've read the Microsoft literature carefully, you will see references to "C2 security-like features"; however, with C2 certification, a computer system is either compliant or it isn't. Whatever else you include in your assessment of NT, C2 classification should be avoided because for the vast majority of installations it won't apply. It is possible that the security improvements being made to NT 5.0 will

NT is becoming popular as both a file server and an application server. It installs TCP/IP as the default network protocol stack and contains many features that will encourage companies to use it in both intranet and Internet environments. While there has been a lot of marketing hype aimed toward reassuring network administrators that NT is completely safe, as with any operating system you need to be aware of the risks associated with using it.

© 1998 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

make the operating system *Red Book*-compliant — one of the enhancements will be hard disk encryption. Microsoft already has SSL available with NT 4.0 (IIS), and if the two features (SSL and hard disk encryption) are combined, data will be secure both in flight and in storage. An interesting note: Another system that has achieved the dubious distinction of being C2 compliant is SCO UNIX.

PASSWORD SECURITY

Password security is one of the major weaknesses of UNIX. The password file is stored in /etc, and is publicly readable. The file has a line for every user which contains details such as the user name, password, home directory, type of command shell, etc. The password field is encrypted, but the encryption method used is not strong enough to deter the "brute force" algorithms. Programs using these algorithms are known as crackers, and they all work in a similar fashion: The UNIX encryption algorithm is applied to every word in the online dictionary, and the results are stored in a "results" file. A copy of the password file is obtained, and the encrypted password field is compared with each word in the results file until there is a match or the program reaches the end of the dictionary. If the user has chosen an English word, the password will be guessed; this method may not be as elegant as decrypting the password directly, but it is effective.

In the UNIX world, two steps have been taken to combat password cracking:

1. The password fields have been removed from the password file and stored in a separate file. Access to this file is severely restricted.
2. The password encryption process uses extra values, known as a salt (an extra number placed at the start of the encryption password), which makes the encryption process far more complex.

NT, like UNIX, encrypts the password and keeps it in the registry. Both the registry editing tools and the registry itself are protected from the general user to some extent. Unlike UNIX, however, NT does not use a salt, and under some circumstances the password is vulnerable. A user who accesses the registry can use programs such as "pwdump" to dump usernames and passwords to a file and then use a cracker to break security.

Even without these problems, there are other vulnerabilities in NT security concerning passwords. When logging in, a Windows 95 user has his password stored locally; if he then logs into a server, the server password is stored on the server (i.e., the user has two passwords, one on the workstation and one on the server). Unfortunately, Windows 95 also offers the ability to synchronize local and server passwords so that both passwords are the same. This is a problem with the first release of 95, prior to service pack 1, because the encryption is weak and the password can be decrypted. If the user's local password is cracked, then the hacker will also have a copy of the user's password on the server.

NT is here to stay, and one of the reasons for its success has been the belief in its inherent security.

ENFORCING COMPLEX PASSWORDS

NT has "account policies" that control password length, age, and uniqueness. Password length can be used to require a minimum length (the longer the better), and password age controls how long a password will remain current. Password uniqueness keeps a record of up to 24 passwords. When a user changes his password, the list is checked to see if the password has been used before – if it has, the password change is rejected and the user is prompted to use another password. Account policies also control "account lockout." If the user repeatedly types the incorrect password, the account is locked, either for a fixed period of time or until the administrator releases the lock. However, there are two drawbacks to the lockout feature:

1. The administrator account cannot be locked out, regardless of the number of incorrect passwords.
2. It is only effective if the user doesn't have an easily guessed password.

The administrator account is present on every NT machine and is the obvious target for a hacker. The administrator cannot be locked out because he may be the only administrator on the machine (the default). If the lock can only be released by an administrator and he's locked out, who will release the lock? (NetWare does not have this problem — if the supervisor account is locked out, it can be released from the console.)

The way to ensure that the administrator is not easily attacked is to rename the administrator account and change its password regularly, enforcing the changes using account policies. Then copy a user account, and call the account "Administrator." This will act as a decoy; you can use audit policies on this account, setting the filter for both failed and successful logins. Repeated failed login attempts will demonstrate that someone is trying to break into the system. A successful attempt will mean that it's time to change both the password and the strategy.

Unlike NetWare, NT does not have a way of limiting the number of concurrent logons to an account. You cannot decide that the administrator can only log on to a server once; provided that another user possesses the correct password, he can connect to a domain controller, member server, or workstation as the administrator, even while the administrator is seated at the keyboard of the machine. The administrator will be unaware of the user unless he looks for the new connection using Server Manager or another NT utility. The reason for this weakness was that Microsoft wanted to be able to replicate files and databases across domains, without having to enforce a trust relationship. In retrospect, this was a mistake.

NT also lacks a method for limiting disk space on a per user basis – this requires a third-party add-on utility. This is scheduled to be fixed in NT 5.0.

LIMITING USERS TO DESIGNATED HOSTS

There is an option in NT that allows the administrator to limit each user to a particular workstation or group of workstations; the list of allowed workstations is then attached to the user's account details. By default, the user may log on to any workstation. Limiting this is accomplished by opening User Manager, selecting a user, choosing the "Logon to" button, and then entering a list of up to six workstations that the user can access. This is a "feel good" feature that is not secure at all. Workstation names are NetBios names. When a workstation powers up (assuming that the protocol in use is TCP/IP), its name is forwarded to WINS (Windows Internet Name Service) server; if the name is not contained in the WINS

© 1998 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

database, the name is registered and a message is sent back to the workstation confirming the workstation name. If the name is in the database, WINS then sends a message to the address associated with the name; if there is no reply, the query is repeated several times. If there is still no reply, the name is given to the requesting workstation and a message is sent confirming the name registration.

Unlike TCP/IP "domain" names, NetBios names are dynamic, which makes them easy to spoof. The system of using these names may work when NT Workstation is used to log on to an NT server, but it will fail with Windows 95 because unlike NT workstations Windows 95 workstations have no computer accounts. Therefore the server has no details about Windows 95 workstations. (See the next section for more details.) All the user has to do is to log on to Windows 95 locally, change the name of the workstation to one that is allowed access to the server, and power cycle the PC. Provided the "real" workstation is not powered on, he will get the NetBios name of an authorized workstation and evade security.

DOMAIN PECULIARITIES

Windows can organize users into groups and domains. NT domains are flat namespaces — all the users are kept in files on the PDC (Primary Domain Controller), and these files form part of the registry. This allows users on both NT servers and workstations to access resources on all servers in the domain with a single account and password. If the company has more than one NT domain, then a "trust" relationship, can be set up which allows users from one domain to access resources in another. The administrators in both domains wishing to set up a trust must take action to establish this relationship. Even after the trust is set up, the users do not have any access to resources in the other domain until they are granted the necessary permissions by the domain administrator. Administration of both the domains can be centralized, but this is not an automatic consequence of the trust relationship — this has to be set up by the administrators.

When either NT workstations or NT standalone servers join the domain, a computer account is set up with the PDC; the computer account is separate from the user account and is used every time the workstation is powered up. This computer account allows the domain controller and the NT workstation to set up an encrypted channel. When the user attempts to logon, this channel is used to protect the logon data from being sniffed by a network analyzer. A Windows 95 client, however, does not have the same relationship with the domain controller — it does not have a computer account. The controller is aware of the user but not the computer, which means that the same method of logon encryption cannot be used. Windows 95 uses an older method of access derived from the LAN Manager product that is weaker than NT encrypted tunnel. Programs have been written that will use a brute force algorithm against the passwords sent over the LAN by 95, allowing the use of a sniffer to break account security.

To deny hackers a way into your system you must ensure that the router used to connect NT hosts to the Internet is configured to discard any packets containing source routing options.

PENETRATING OTHER DOMAINS

There are some "accidental" vulnerabilities introduced by the domain login process as shown in Figure 1. If there are two domains, Domain A and Domain B, with no trust relationship between them, users in Domain A should not be able to access resources in Domain B under any circumstances. Unfortunately, this is not totally true; if a user in Domain A has the same account name and password as a user in Domain B, the user in domain A will be able to log on the account in domain B and use resources. Domain B sees the user as a local user in that domain, and will not even be aware that the user in Domain A exists. This occurs because domain controllers first compare the username and password to the list of users kept in the accounts database; even though the domain id is sent with every login request, it is not used unless the comparision fails.

The problem can also be propagated across a trust relationship with another domain. If Domain C trusts Domain B, then provided the users in Domain B have been granted the necessary permissions, they will be able to use resources in Domain C. If a user in Domain A is authenticated by Domain B, because he has the same password and username as a user in Domain B, the Domain A user will get access rights in Domain C.

TCP/IP UTILITIES

Microsoft refers to telnet, FTP, and other programs closely associated with TCP/IP as TCP/IP utilities. The Microsoft File and Print services are implemented using Server Message Block (SMB). All of the security features and devices mentioned here rely on the use of the SMB protocol and NBT (NetBios over TCP/IP). The NT resource kit contains a Telnet server and other Internet server programs, while IIS implements an FTP server. TCP utilities do not benefit from Microsoft Domain Security, and this implies that an NT Server or workstation using Internet server programs has no better protection against spoofing than UNIX or other operating systems.

NT also honors IP source routing (see the article "Protecting Networks With and Without Firewalls: Part II — IP Spoofing and Source Route Attacks," ***Technical Support,*** February 1997). To deny hackers a way into your system you must ensure that the router used to connect NT hosts to the Internet is configured to discard any packets containing source routing options. This is a wise precaution regardless of the operating system in use behind the firewall.

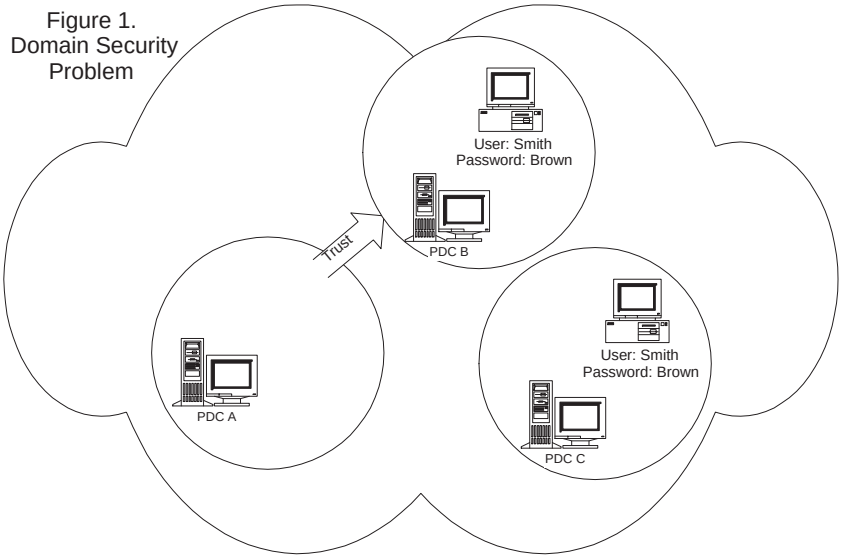
CONCLUSION

NT is becoming popular as both a file server and an application server. It installs TCP/IP as the default network protocol stack and contains many features (such as the free web server, IIS) that encourage companies to use it in both intranet and Internet environments. There has been a lot of marketing hype aimed toward reassuring the administrator that NT is completely safe. However, as with any operating system, you need to be aware of the risks associated with using it in order to provide a reasonable operating environment for users and the MIS department.

Editor's Note: *This series began in January 1997. Part I examined the sniffer attack. Part II (February) dealt with IP*

© 1998 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

Figure 1.
Domain Security
Problem



All of the domains are physically connected by a network. The arrow between Domains A and B represent a trust relationship, where the users in B may log on to the computers in A. (Note that the direction of the arrow is a Microsoft convention -- "Arrows point to people you can trust".) The user in Domain C has the same account name and password as a User in Domain B. He will get access to resources in both A and B.

spoofing and source route attacks. Part III (March) described TCP spoofing, the sequence number attack. Part IV (May) examined email forgery and other mail threats. Part V (July) dealt with DNS attacks. Part VI (August) discussed securing intranets and internal networks; and Part VII (October 1997) addressed using multiple firewalls in large networks.

For copies of previous articles in this series call (414) 768-8000, Ext. 115.

REFERENCES

Orange Book — "Department of Defense Trusted Computer System Evaluation Criteria" DOD 5200.28-STD. December 1985

Red Book — "Trusted Network Interpretation of the Trusted Computer System Evaluation" Criteria." NCSC-TG-005 1987 ts

NaSPA member Mark Bell founded Marol Consulting in 1993. He also teaches courses for Epcom Corporation, PPI and other training companies. He has been involved in the computer industry for 15 years, specializing in networking for the past eight. Mark can be reached at (313) 665-0601 or mbell@marol.com. Mark is currently under contract with MacMillan Publishing to write books on TCP/IP and networking. His first book is due to be published at the end of this year.

©1998 Technical Enterprises, Inc. For reprints of this document contact sales@naspa.net.