



The Insider Threat

By Peter Wood

peterw@fistbase.co.uk

Introduction

These days I spend my time breaking into networks and Web servers for a living. It's not that I'm of a criminal persuasion, but rather that many large organizations have decided that it's sensible to pay someone like me to break into their network before someone with malicious intent does. The impact of such a breach can be significant, yet most networks are woefully vulnerable. In fact, I sometimes despair at the common misconfigurations and ignorance I encounter day after day. Problems that have been well documented for months or even years raise their ugly heads at site after site. Simple mistakes are repeated again and again by otherwise perfectly good system administrators.

Breaking into Corporate Networks has Never Been Easier

When we all decided that Windows NT (and subsequently Windows 2000) was to be the corporate standard and that the Internet was to be the communications medium of choice, the network security model changed forever. Breaking into corporate networks, and thereby corporate information, has never been easier. Why? First, NT comes with many easily exploited security vulnerabilities by default. Second, most IT people either do not know about or do not have the incentive to fix these vulnerabilities. Third, information about how to exploit these vulnerabilities is freely available on the Internet for everyone to see. Fourth, access to systems at the desktop is universal. Lastly, most people, including the majority of techies, don't appear to know how to select reasonably secure passwords.

Of course, it's not that any given vulnerability grants you instant control of a company's systems, but rather that a combination of two or three such vulnerabilities do. My current favourite exploit has enabled me to gain control of most networks in less than 20 minutes. As usual, this exploit works thanks to a combination of ignorance and sloppiness (or lack of investment). It goes like this. Plug in a Windows laptop anywhere on the corporate network. This can be in the head office, at a branch office or store, anywhere in any trusted third-party premises or perhaps through a dial-up connection. Browse the network using Windows Explorer and you'll get to see all the Windows machines on the network. There's no need to log on or join a domain for this to happen. Select a server (they're usually named in an obvious fashion) and attempt a "null session" connection. Null sessions is a standard feature of NT and Windows 2000 and they enable you to list users, groups, group memberships, etc. without any form of authentication whatsoever. And, yes, there's plenty of software on the Internet that will help you to establish a null session and then interrogate this information. Now list the users in the Administrators and Domain Admins groups and look for patterns, or rather exceptions to a pattern. Typically, organizations use obvious

naming conventions for user accounts, but these are usually ignored where service accounts are concerned (Service accounts are administrator-level accounts used to enable applications to log on to servers and domains. Applications such as Backupexec, Arcserve, Tivoli are obvious examples). Select each of these service accounts in turn and try to guess its password. It's not as hard as you might think. Frequently, network administrators will select something obvious, such as a password the same as the account name! Beware that you don't exceed the account lockout threshold, otherwise even the most harassed admin will guess something is up. If these fail, try those accounts that look like shared administrator accounts or scripted accounts, such as Administrator, Install, AutoInstall or similar. At least fifty percent of the time you'll gain Domain Admin access, allowing you to create your own administrator account, join the domain legitimately, and help yourself to any information on any server.

Now this is not rocket science. In fact, it's something any teenage student could accomplish with the minimum of research. So why is it still possible to conduct this exploit at the majority of sites I visit? The answer has to be a combination of ignorance and disinterest. When I studied the official Microsoft NT courses, security issues were barely mentioned, so many MCSEs will remain ignorant of things like null sessions. Few organizations have invested in a technical security role with a remit to monitor new exploits and produce security build standards, review existing installations and plug the holes. Then most managers continue to believe that a firewall is a panacea, either ignorant or disbelieving of the fact that the majority of hacks come from within the organization. Senior management still fail to realize that anyone with Domain Admins privilege can read, alter and delete any document anywhere on their network, be it on a server, a workstation or even a laptop, and that there are often dozens of accounts with that privilege.


The apathy towards security is frightening. The push from the top for more results using the same or fewer people and resources makes it unrealistic for security to feature in any meaningful way. We seem to be becoming more aware of security in general terms but unwilling to make the investment in personnel, training and good solid procedures.

Resolving These Problems

So what can network admins do to resolve these problems? The steps to take are relatively straightforward. Firstly, patch the registry on each server so that null sessions don't permit you to list user names and groups. This won't affect Windows functionality, but it will stop unauthenticated intruders from viewing this important information. Next, rename all service accounts so that they look exactly like regular user account names (and don't use "stupid" names like AHitler or FBloggs). Now even authenticated users won't be able to tell which are people and which processes. Next set

a complex password on each service account, using punctuation characters as well as alphanumerics. This makes it a significantly more difficult process to crack, even if the perpetrator has got hold of your SAM file. And be sure to test your service accounts thoroughly with the new names and passwords before putting them into production.

For added security, turn off LAN Manager compatibility on all your machines. By default this is turned on, resulting in all passwords being converted to upper case and undermining your careful choice of mixed-case password. Finally, be sure to patch everything up to date. My second favorite way of getting admin on your servers is by exploiting vulnerabilities like the RPC DCOM problem. Most firms patch their Internet-facing hosts but aren't so careful with their internal systems.

If you apply all these solutions, your network will be significantly more secure than most and you will be able to sleep more soundly at night. 

Peter Wood is employed with First Base Technologies, where his work includes network security reviews, firewall penetration testing, and policy and procedures. He is a Fellow of the British Computer Society and a member of ISSA, IEEE, ISACA and ACM. He is also a BCS Registered Security Consultant, a Microsoft Certified Product Specialist and a member of Mensa.

