



Pivot Point Security

957 Route 33

Suite 111

Hamilton Square, NJ 08690

(609) 890-1131

www.pivotpointsecurity.com



Network security: Doing too much with too little will cost you

by [John Verry](#) | [More from John Verry](#) | Published: 11/13/02

Category: Technology | **Audience:** IT Consultant

Rating: 4.3 (out of 5) [Rate it](#) **Comments:** 9 | **0 NEW** | [View all](#)

Takeaway:

Organizations with strapped IT budgets sometimes cut corners when it comes to security. If that's the case for you, you may find some of the same vulnerabilities that one consultant identified in two clients' networks.

Small companies and small divisions of larger organizations often try to provide complete business functionality—e-mail, Web presence, domain-based network—with limited resources. As two recent engagements illustrate, attempting to do too much without sufficient resources and an awareness of some basic security practices can put an organization's security in jeopardy. When you come across client setups like the two I'll describe here, encourage the client to get back to basics and eliminate vulnerabilities created when networks aren't segmented correctly.

Different organizations, same problem

A division of state government and a regional office of an internationally recognized philanthropic organization wouldn't seem to have much in common. However, both organizations used a single internal Windows server—one NT, the other Windows 2000—to act as a domain controller and Internet mail server, due to limited budgets. One of the organizations also used the server to host its public Web site.

This configuration violates a basic tenet of network security: appropriately segmented assets and services. Since their servers were domain controllers, the organizations placed them on their internal network and provided the servers with external IP addresses to allow mail and Internet access. Both organizations also had nonfirewalled connections to their respective parent organizations' networks.

The state government hired our company, [COUR IT](#), after the Web site was defaced several times. They had also detected inappropriate access and nonauthorized security changes on the domain controller, including deletion of security logs.

The philanthropic organization engaged us for the IT security elements of a financial audit, during which we learned that they suspected that their network-attached PBX had been hacked. Two other "unexplainable" incidents had necessitated two complete rebuilds of the domain controller in the previous three months, causing the irreparable loss

of critical organizational data.

Know who is at the door before you answer

Whenever we find an organization with a domain controller assigned external IP addresses, usually for Web or e-mail access, it raises a red flag. This configuration is often a sign that the organization doesn't have an overall awareness of security best practices and usually indicates more significant security concerns.

Our initial step for both organizations was to scan the mail servers using [Nmap](#) and [SuperScan](#). We were extremely concerned by the high number of open ports, including TCP port 139 (see [Figure A](#)).

Figure A

```
* xxx.xxx.xxx.xxx server1.city.div.state.us
|_ 25 Simple Mail Transfer
|_ 27 NSW User System FE
|_ 42 WINS Host Name Server
|_ 80 World Wide Web HTTP
|_ 81 HOSTS2 Name Server
|_ 82 XFER Utility
|_ 83 MIT ML Device
|_ 110 Post Office Protocol - version 3
|_ 119 Network News Transfer Protocol
|_ 135 DCE endpoint resolution
|_ 139 NETBIOS Session Service
|_ 143 Internet Message Access Protocol
|_ 389 Lightweight Directory Access Protocol
|_ 443 https MCOM
|_ 593 ncacn_http/1.0
|_ 636 ssl-ldap
|_ 1061
|_ 1067 Installation Bootstrap Proto. Serv.
|_ 1069
|_ 1071
|_ 1074 ncacn_http/1.0
|_ 1080 socks
|_ 1077 ncacn_http/1.0
|_ 1083 Anasoft License Manager
|_ 1086 ncacn_http/1.0
|_ 1090
|_ 1093 ncacn_http/1.0
|_ 1132 ncacn_http/1.0
|_ 1135 ncacn_http/1.0
|_ 1745 remote-winsock
|_ 1863
|_ 3190 America-online
|_ 5590
|_ 6667
|_ 6668
|_ 7429
|_ 8054
|_ 8080 Standard HTTP Proxy
|_ 8088
```

A scan of the client's mail server

The NETBIOS standard allows a significant amount of information to be gathered via port 139, even if the domain controller doesn't authenticate the user. (This vulnerability is well documented; a good discussion is included in the well-regarded text [Hacking Exposed](#).)

One way the vulnerability can be easily exploited is with a tool used by security professionals and hackers alike: [NBTEnum](#) (Net Bios Enumeration). The scrubbed example of the output we gathered from one of the organizations illustrates the rich amount of information about a system, including all local groups/users, global groups/users, shares, and password policy information (including account lockout thresholds) that can be gathered.

Once a malicious external user has access to this information, it makes it significantly easier to gain inappropriate access to the network.

The password is "password"

The philanthropic organization had all its volunteers log on via two user accounts that were aptly named volunteer1 and volunteer2. We assumed, based on the organization's lax security posture, that these accounts were probably protected by simple, easily remembered passwords.

We attempted to connect to a network share remotely using the Windows run command: `\\xxx.xx.xxx\sharedfoldername` and were prompted for a username and password. Our first three attempts, using "password," "organization acronym1," and "organization acronym2" failed. On our fourth try, using "organization acronym3," we gained access. At this point, we were browsing shared network folders.

To make matters worse, the organization wasn't using an appropriate level of access control, and the volunteer accounts could browse the complete contents of the domain controller (the C: drive was inappropriately shared.)

Using our newfound access to the domain controller, we copied the registry to our machine and used LC3, better known as [L0phtCrack](#), a password-cracking tool, to attempt to determine user passwords. Using a dictionary attack—in which we tested each encoded password against the list of often used passwords—we returned 23 out of the 61 user account passwords.

Ironically, one of the first passwords cracked was an IT vendor's name used by the network administrator. This granted us complete administrative control of the domain controller.

Due to a series of poorly executed security measures (inviting untrusted traffic into the trusted network and onto the domain controller, null sessions enabled, poor password policy, poor access control), it took us less than an hour to take control of the client's network.

"Bubba" is in the house

The governmental division's assessment was strikingly similar. From previous conversations with the client, we knew their password policy specified passwords with a mix of at least six alpha and numeric characters. During a brief penetration testing session, we loaded LC3 with a list of common passwords and instructed it to append and preface all passwords with up to four random numbers.

We were quickly able to crack four of their 21 accounts; the most damaging was a test user account labeled "Bubba" that had been used to troubleshoot a problem several months before. (We have noticed that administrators for SMB networks often create temporary test accounts that share the same password as their own account.)

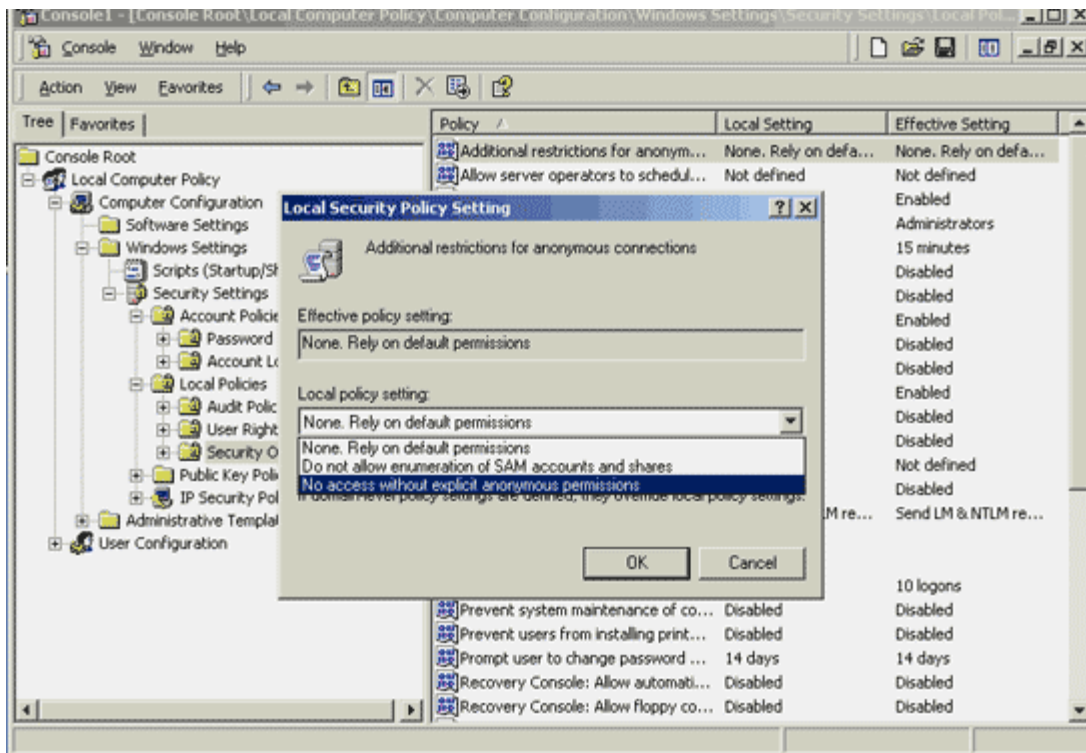
While the password didn't directly provide us with administrative-level access, its construction (football team name + calendar year) did allow us to rather quickly guess the actual password for the administrator's account (baseball team + year). The same series of poorly executed security measures used by the nonprofit organization had left their network vulnerable.

Preach fundamentals

Here is some general advice for clients who may be cutting corners the same way:

- Encourage the client to ensure that null sessions are disabled. If the configuration must stay in place for an extended period of time, enable Restrict Anonymous Browsing (Null Session). With Windows NT, the `HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous` Registry key should be set to 1. In Windows 2000, you can set the same key to 2 or, if you prefer, you can set it via the Microsoft Management Console (see **Figure B**).

Figure B



- Stress the importance of separating internal and external functionality.
- Stress the importance of establishing a good password policy that ensures passwords are difficult to guess. At a minimum, ensure that the policy disallows blank passwords, "password", and a password derived from the username.
- Stress the importance of good user account maintenance. At one of the organizations discussed above, there were three "garbage" accounts (including Bubba and Test) in the Administrator's group. User accounts should be reviewed on a regular basis, and inactive accounts should be removed. Temporary user accounts established for external consultants that remain after the engagement has ended are especially concerning.
- Stress the importance of learning the basics of network security.
- Ensure that the client has considered all options. The wide range of inexpensive Web and e-mail hosting plans often make pushing these functions to an external provider a solid choice for smaller organizations.