Global Information Assurance Certification Paper

Using Bindview's EMS and NOSAdmin to Tighten Security on our Mixed Network.

John Cunningham
Dec 18 2000

Wow. Our Novell Directory Service tree, which we only administer a portion of, in a large healthcare\university organization, has just been exploding over the past few years. We've had rapid growth, network administrators turning over like McDonalds, little policy and standards guidance and a user base that can diplomatically be described as "fluid". On top of this, we have HIPAA legislation bearing down and the simple knowledge that we have to get it in gear.

This is not to say we are hapless. We have many resources like firewalls, scanners, anti-virus software, proxy servers, security tokens, etc. Still there is something telling me that the largest gains in our overall system security is not to be made with high tech gizmos but with solid, consistent security administration on our servers.

Now it is possible that I am the last person on earth to realize this. I'm envisioning my wife giving me that "give me some credit" look when I state the obvious. Still I'm the one who is responsible for changing our direction and I need a tool that can help me achieve a level of control over several aspects of our systems. Here is what I would like to achieve.

I need a centralized method of monitoring and administering different facets of our network. I don't want a reporting tool that only points out our deficiencies but one that allows me to do the administration based on those reports in short order. We need to identify and remove stale accounts. Tap in to the native auditing capabilities of the operating system and one that has the flexibility to focus on only the branches of the tree we are responsible for. On top of these normal requirements is the need to do hard core security analysis like virus, hack - crack and network vulnerability assessment that is fed by information from IT security icons like the SANS Institute and CERT.ORG.

The System Administration, Networking, and Security Institute is a cooperative research and education organization made up of more than 96,000 system administrators, security professionals, and network administrators. The group, along with the FBI and the Justice Department, issued a list of top 10 Internet threats in June.

The tool that came out on top for us is Bindview's Enterprise Management Console. Soon to be Bindview's Risk Management System(32 bit). This latest release should be out in January 2001. Currently we are only using a few modules from the suite that they offer. Namely the EMS console and NOSAdmin for NetWare 4-5. Essentially this software can query the NDS database and make changes interactively to this database. Bindview really works as a shell on top of what the operating system already provides and accesses the auditing inherent to that system.

One caveat to this is NetWare's new NSS volume format that provides better performance and functionality but its auditing capability can not be used by the current version of Bindview 6.5.

Other tools like Crystal Reports and Microsoft Access can tap into these sources but Crystal Reports is read-only and Microsoft Access is not a recommended method to make adjustments. In addition, Bindview has done the legwork on identifying what each field in the database represents and then breaks down the different categories that compromise the NDS database. Almost no administrator has the time to do this level of detailed work and its value is quickly apparent.

One aspect favorable to Bindview is that it has an NT module that Chris Adams from Bindview has explained to me has equivalent reporting power and "active extensions" supplemental software to allow on the fly administration like it's brethren NetWare module. Us Midwesterners are slow to realize the waning market share of NetWare and we need to prepare for the eventuality of migrating completely to an NT/2000 network base. Pre-migration reports and this NT reporting\administration capability allow a flexibility that may be very useful in the not so distant future. Another module, bv-Admin, further eases administration on combined MS and NetWare directory services. “Put simply, bv-Admin is a management solution for multiple, heterogeneous directory services. It can show you NT and Win2K domains, organizational units (OUs), trees, forests, Novell NDS directories, and Microsoft Exchange directories in a single console. All of these directories are condensed to a single treeview, and commands are uniform across the full reach of directory services. For example, you can create or delete users across all directory services with a single operation.”

Bindview also offers a Web module, Hackershield, and Inventory management to boot. HackerShield comes with a large database that it uses to launch simulated attacks on your choice of network devices. HackerShield scans each computer’s OS and internal configuration. Scans include checking for incorrectly configured files, directories, users, and permissions. The scanner comes with a large dictionary and uses various techniques to identify passwords vulnerable to hacking. HackerShield’s database of MD5 checksums can also detect changes in key system files.

The ability to assess the strength of current system passwords is another advantage. When server based NLM's are loaded the brunt of processing is passed from the EMS console PC's processor to the servers with more capable processing power. Several files are provided for the dictionary based cracking routines and are editable.

One, if not the biggest determining need of having this type of software is that management needs trending and "quick answer" troubleshooting output to refer to when planning and presenting budget requests to our executives.

The graphing capability built in to Bindview 6.5 is not very sophisticated and their own staff has suggested that the data export features be used to populate Microsoft Excel spreadsheets to take advantage of its graphing ability. You are really on your own to form the output into a readable, sensible form.

How do we get the trending data organized and produced? There is nothing magical about it. Create and organize a directory structure that conforms to your needs. Then, from the multitudes of canned reports to select from, each should be copied (to preserve default syntax) to a user-defined tab\folder and further refined to meet exactly your needs. Then, because Bindview has no native scheduling capability a .arf file must be produced that contains the commands and parameters necessary to plug into any standard scheduling program like EZ Scheduler or AT\WinAT.

As far as performance goes, much depends on the efficiency of your NDS tree, the power and bandwidth available to the PC you have the EMS console loaded upon and the complexity of your query. Certain reports such as trustee and rights queries will search the length and breadth of your tree outside of your defined scope (i.e. containers) for obvious reasons. Be prepared for lengthy run-times. Because this tool rides on top of your NDS database, if you have a corrupt replica you can expect poor results. Also, if your rights within the tree are patchy and ill defined you can expect a slew of errors presenting themselves until this scenario is remedied.

The active administration fields are highlighted in blue and sweeping changes can be made at one time. Marking and selecting cells that are non-contiguous is a feature expected and delivered. When auditing is enabled the sub-field selections can be toggled on and off with a click and help reduce the apprehension of initiating those audits by being able to scale the items to monitor.

Though we have just begun to use Bindview, we are confident that with consistent use and analysis we will be able to close the fundamental gaps in system security administration that will let our perimeter and network defenses do the their best work.

Bibiliography:

1. Matthew G. Nelson - http://www.informationweek.com/story/IWK20000731S0009 July 31, 2000.htm
2. Mike Gunderloy - http://www.mcpmag.com/members/00dec/fea3main.asp#bvAdmin Dec 1. 2000
3. Chris Adams – Senior System Engineer Bindview. Dec 6 2000
4. Steve Manzuik http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9206&SearchString=hackershield May 16, 2000
5. Brittany Schaefer - Account Manager http://www.bindview.com Nov 2000