GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

NT Vulnerability Scanning Using Cerberus' Internet Scanner (CIS)
Rebecca Simon

Are you vulnerable?

The standard install of NT Server or Workstation leaves the operating environment open to access from all quarters. If this system is connected to the Internet, it gives a whole new meaning to allowing access by 'Everyone'. Hardening and securing the NT environment requires many levels of detail. The first step is to identify the known areas of vulnerability and to close those holes. If the domain under scrutiny is already in production, it is time consuming to examine the many levels of vulnerability throughout the domain. Thus enters vulnerability scanning tools and services.

A proactive approach to vulnerabilities

In a shared environment, particularly in the .edu world, a vulnerability in one area may impact users throughout the network. A responsible administrator will be alert to these vulnerabilities. But there may also be budgetary constraints that preclude top-drawer vulnerability scanning products and services. The Internet community has been blessed with many freely accessible tools that aid system security administrators in assessing their systems.

Tools of the trade

Microsoft, openly publishing the fact that NT out of the box is not a secure system, publishes its Windows NT 4.0 Domain Controller Configuration Checklist[i]. These are industry-accepted practices that aid in securing the NT operating environment. An optional tool for implementing these security tweaks, the Security Configuration Manager (SCM)[ii], was provided starting with service pack 4. Installing and configuring this tool is an involved process.

If your NT box is running Internet Information Server (IIS), this opens up an entirely different set of security concerns which are addressed by Microsoft in security patches and basic checklists downloadable from the Microsoft TechNet web site.[iii] Running IIS on a domain controller is not advisable, but for organizations with limited assets, this may be the only route.

A simple tool that provides an automated checklist was authored by David Litchfield and published as the Cerberus Internet Scanner under the auspices of Cerberus Information Securities Ltd. (http://www.cerberus-infosec.co.uk). This company was obtained by @stake in July, 2000, and touted as "U.K.'s Premier Internet Security Consultants".[iv] This, coupled with the fact that @stake was one of the participants in the Security

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Vulnerability Summit[v] (see www.vulnerabilitysummit.org) co-hosted by eWeek and the security company Guardent Inc., should give some indications as to the quality and reliability of this tool. @stake regularly publishes vulnerability advisories for all platforms.[vi]

Cerberus provides CIS version 5.0.02 as a free download and should be viewed as a 'lite' version of the 'commercial version of CIS, version 6, .. currently under development'. [vii] @stake also provides additional security tools at http://www.atstake.com/research/tools.html, but the Graphical User Interface (GUI) version of CIS has not been published there to date. The webscan module that is incorporated in CIS can be downloaded as a separate module. It is unclear whether CIS will continue to be updated, or whether version 5.0.02 is the end of the line. @stake provides heavy-duty international security services for profit and has a trademark on 'Securing the Internet Economy[SM]'. Organizations with tighter purse strings should be able to benefit from the expertise represented by these commercial ventures.

In a May/June 2000 survey conducted by Insecure.org, publishers of nmap port scanner, the CIS tool was listed as one of the Top 50 Security Tools.[viii]

Installing CIS

After obtaining the small zipped download from http://www.cerberus-infosec.co.uk/cis.shtml, merely extract all the included files to a directory on your hard drive. The install consists of the GUI executable, cis.exe, and a series of DLL's (12 in version 5.0.02) which drive the various modules. A ready-made directory structure is installed to house the reports generated from scans. Merely click on the executable to open the GUI.

Features of CIS

The modules included in version 5.0.02 and the number of checks made are:

Web - 126
FTP - 7
SMTP - 21
POP3 - 3
NT
    Registry - 40
    Service – 15
    Browser
NetBIOS
    Share Information - 3
    Group Information - 2
    Account Information - 8

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

MS SQL Server - 19
Other
- Finger
- DNS
- RPC

Specific check descriptions are documented at http://www.cerberus-infosec.co.uk/vulndb.txt.

Using CIS

To initiate a scan, open File... Select Host... and enter the target host name or IP address. Select the modules to be used by checking the boxes in File... Select Modules dialog. Then select File... Start scan... and sit back while the speedy little tool does its investigative reporting. The process is multi-threaded, so scan time is minimized. Even on mid-range processors and over the network, scan times are minimal.

To view the results of a scan, select File... View Report... The reports, which have been written in HTML format in the %install%\Reports directory. Each machine scanned has a primary page in the format *machinename*.html with additional files prefixed by the module used in the scan. If you are accessing the report directly from cis.exe, the main page automatically opens, with links to each module's results. If a subsequent reading of the report is desired, merely click on the desired report in the Reports directory. Individual reports are displayed in frames in a simple text format suitable for printing.

The NetBIOS report from a Domain Controller provides useful auditing information on the users and groups defined on the domain. For each user, the password age, the number of times the user-id has been used to log in and the account status (active or disabled) are reported. Group information is nicely displayed, showing all users assigned to the standard and domain specific groups. This report is easily generated at an auditor's request.

After the scan is complete, use the findings to modify registry entries (at your own risk, as Microsoft always says), apply permissions as stringently as possible, disable services if necessary, delete or move files as indicated. The output from the scan includes readable, specific instructions on how to make the alterations and the reasoning behind each fix. The web scan module contains links to Microsoft Advisories or other entities on the web that have published the vulnerability. The tool does not provide any automatic fixes, so the administrator is afforded an educational opportunity to repair their own system and gain an understanding of the registry entries. The administrator may also use knowledge of their own particular environment to weigh the effects of making any system change.

A direct link to any published update is found in the Tools menu of the tool itself. The most current update of any module is the webscan dated 5/27/00. Support is "coming soon", but the tool is so self-explanatory that none is needed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Summary

Free is good. Especially when value and quality are thrown in. The CIS tool provides ease-of-use at a cost that makes it possible for any NT system administrator to secure their system.

References

[i] Microsoft TechNet. *Windows NT 4.0 Domain Controller Configuration Checklist* March 29, 2000. URL: http://www.microsoft.com/technet/security/dccklst.asp (December 15, 2000)

ii Microsoft Product Support Services. *SP4 Security Configuration Manager Available for Download*. February 23, 1999. URL: http://support.microsoft.com/support/kb/articles/q195/2/27.asp

[iii] Microsoft TechNet. *Security Tools*. September 1, 2000. URL: http://www.microsoft.com/technet/security/tools.asp. (December 15, 2000)

[iv] Lois Paul and Partners. *@stake Acquires U.K.'s Premier Internet Security Consultants, Cerberus Information Security***.** July 26, 2000. URL: http://www.atstake.com/events_news/press_releases/cerberus.html (December 15, 2000)

[v] Rapoza, Jim. *Security Core: Best Practices*. eWeek, Vol. 17, Number 46. November 13, 2000. Also at URL: http://www.zdnet.com/eweek/stories/general/0,11011,2652346,00.html

[vi] @stake: Securing the Internet Economy[SM] . December 18, 2000. URL: http://www.atstake.com (December 18, 2000).

[vii] Cerberus Internet Scanner download site: http://www.cerberus-infosec.co.uk/cis.shtml (December 15, 2000)

[viii] Fyodor. *Top 50 Security Tools*. Insecure.org. Aug. 21, 2000. URL: http://www.insecure.org/tools.html (December 15, 2000).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Questions for **NT Vulnerability Scanning Using Cerberus' Internet Scanner (CIS)**
Rebecca Simon

1. Which of the following tools does NOT perform vulnerability scanning for Windows NT? (a) SCM (b) CIS (c) PGP (d) Hackershield (answer: c)

2. The Cerberus' Internet Scanner (CIS) is an example of a (a) port mapper (b) vulnerability scanner (c) firewall (d) intrusion detector. (answer: b)

3. The following function may be performed by running the Cerberus' Internet Scanner (CIS): (a) map ports to services (b) obtain internet browsing histories (c) check for system vulnerabilities (d) repair a corrupted registry. (answer: c)

4. To secure Windows NT 4.0, changes may have to be made in (a) the registry (b) file system permissions (c) services (d) all of these. (answer: d)

5. The Cerberus' Internet Scanner (CIS) may be used (a) only on the local system (b) only on one domain (c) over the Internet (d) on any system to which the logged in user has access. (answer: d)

6. Vulnerability scanning for Windows NT is an involved process best handled by an outside vendor. (False)

7. Microsoft provides a vulnerability scanner in the standard install of Windows NT 4.0. (False)

8. CIS will automatically make NT registry edits. (False)

9. One commercial enterprise which publishes vulnerability advisories is @stake. (True)

10. Microsoft Internet Information Server (IIS) version 4.0 must be installed on a Primary Domain Controller (PDC). (False)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.