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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

The Microsoft OOTBS Got You Down?
– Smile –
There is Treatment

By Becky Cosby

Microsoft Windows NT/2000 operating systems are secure to use as installed right out of the box. Right? WRONG!![1] For the purpose of this discussion, we will call this condition the "Out of the Box Syndrome", or the OOTBS (pronounced oot-bahs). There are three main areas of the OOTBS to be treated: 1) policies and rights, 2) registry key values and permissions, and 3) directory and file permissions.

Resources[2,3] are available from which to make checklists, to manually address vulnerabilities appropriate for each environment. This process, however, can be tedious, time consuming, and sometimes dangerous if care is not taken when editing the registry. This is also not a one-time task, but a continuous process that must be done to maintain system integrity and to address new vulnerabilities. But, don't despair and let the OOTBS get you down, there is hope available from a couple of tools. STAT from Harris[4] and Security Expressions from Pedestal Software[5] not only find the vulnerabilities, but also help you fix them, many times with just a click of the mouse.

These two tools have some differences in detection, reporting and deployment features that may appeal to professionals depending on need, environment, and level of expertise. An overview of the features of STAT and Security Expressions will be presented. Both tools evaluate Windows NT 3.51, 4.0, and Windows 2000, and both need to be run from an NT 4.0 operating system. More specific detail, pricing information and evaluation software is available from www.statonline.com and www.pedestalsoftware.com respectively.

Detection

Both STAT and Security Expressions claim to have a small footprint when scanning, and in the environments where tested, neither produced a performance problem. Scanning and probing tools should always be tested in a non-production time frame and on a limited number of machines to determine a safe threshold for that environment. Security Expressions has a nice feature that allows the user to specify the number of concurrent scans to be made from each batch of machines specified. STAT allows the user to select multiple machines to scan, but appears to scan only one machine at a time. Licensing also affects the number of machines that can be scanned as a batch for both products. Both products require administrative access to fully assess a machine. Security Expressions has a useful feature that allows the user to enter a login and password. This is very useful for scanning machines outside of the user's authentication domain. STAT requires the user to be signed on to each target machine with administrative rights before scanning. As is always the best practice, get permission in writing before scanning any machine for vulnerabilities.

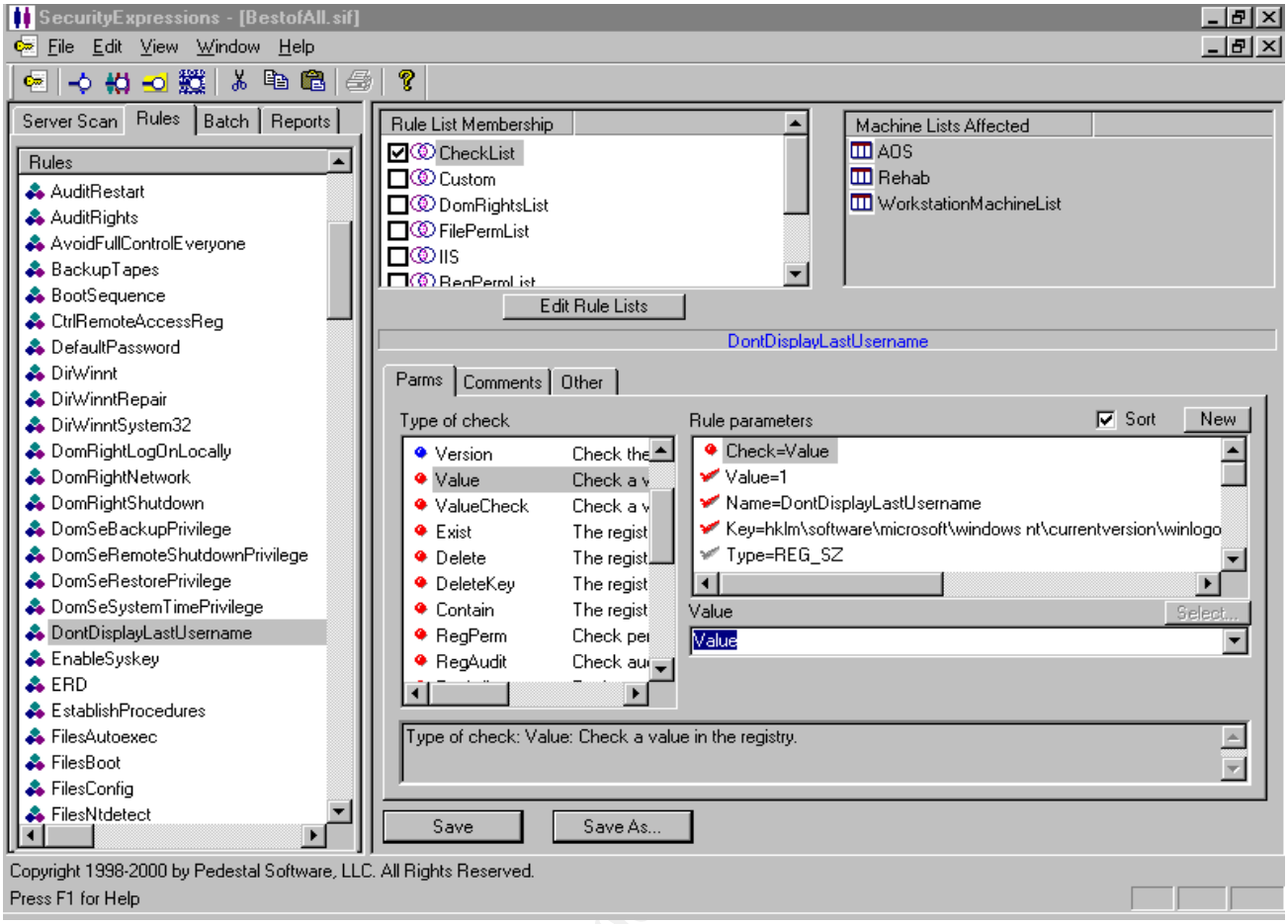
STAT and Security Expressions take slightly different approaches to detecting vulnerabilities. STAT boasts a vulnerability list of over 900 items as of this writing. An updated file containing new found bug checks is available from www.statonline.com for download by licensed users at least once a month. STAT's full vulnerability list is further

© SANS Institute 2000 - 2005 Author retains full rights.

subdivided into dat files such as W2K, 3_51, autofix, C2, CVE, IIS, Low, Medium, and others as indicated by the file name. A file containing the entire list, a specific or custom list can be loaded into the program for assessment. Any list can be edited for content, but specific items cannot be edited. Therefore, an item such as the minimum length of a password, which is presently specified by STAT as 8, would only check for numbers above 8. This value cannot be edited and any other desired value must be verified manually. Custom lists can be made by loading one of the provided files, such as the full list, and removing unnecessary items. It is not possible, however, to cut items from one list and paste them into another. Therefore, if a custom list is needed (for example, to reduce scan times), it must be created by adding or removing items from the new list after each update.

Security Expressions takes a different approach by offering templates (*.SIF) of rules recommended by SANS, Microsoft White Paper, and 3 levels of the Department of Navy recommendations. Windows 2000 Group Policy and Windows NT 4.0 Security Configuration Manager SCE, INF files can also be imported, modified as desired and saved as SIF files. Any of these template rule lists can be used as presented. The rules can also be customized by including or excluding items, pasting in rules from another list, or editing or creating individual rules in a template. This feature is very useful, but takes some time initially to configure. A new vulnerability update list is not posted on a scheduled basis. NTBugTraq[6] and Microsoft security bulletin[7] postings need to be monitored continuously so rules can be configured to check for and eliminate new bugs as they "hatch". This is much more time consuming than downloading a "canned list", but is also much more configurable. Below is a screen shot of Security Expressions' rules screen. The *Rule Parameters* in the lower right window are those configured for the highlighted rule from the *Rule* list on the left. A checked box in the upper, center *Rule List Membership* window indicates the rule list that this rule belongs to.

© SANS Institute 2000 - 2005 Author retains full rights.



While STAT scans for known Trojan file names, Security Expressions can be configured to search for any file name. This process does, however, require more expertise and time. As the name might suggest, Security Expressions uses scripts (or expressions) to search the registry, directories, and files, for ownership, dates, permissions, or just about any other attribute of interest. Various searches by group for members or policies can also be run. Although the expression search consoles are not for the faint of scripting, they are very powerful and do have wizards to assist with the script development. Technical support is also available from the Pedestal staff to assist with scripting.

Deployment

Detailed information describing each vulnerability discovered and how to correct it is available on both product report consoles by double clicking the item. The automated fix function button is also accessible for each machine if an automated fix is available for the specific vulnerability. Security Expressions has a “Fix Problems” checkbox that has the capability to try to automatically correct each problem found if the scan was run in batch mode. Both tools have the potential to detail the vulnerability and actions needed to correct them.

STAT vulnerability items include a description of how the vulnerability could be compromised, any advisories that may have been posted, Microsoft Knowledge Base references, as well as detailed instructions on correcting the situation. Security Expressions does not have as much detail as STAT. The custom rules have only the

© SANS Institute 2000 - 2005 Author retains full rights.

description that the rule creator put in the appropriate field. Security Expressions has a "Change History" option which logs each change made by date, time and action. From this screen the user can select an item, click the "Undo" button, and reverse any errant or unwanted changes. This is an excellent option that STAT does not have.

Reporting

The effectiveness of a given report depends upon the use for that report. A report could be needed for an Executive Summary, a detailed vulnerability listing, or for documentation of the exact action that is needed to fix a specific OOTBS symptom. STAT appears to have more variety in reports, although the latest release of Security Expressions (V1.2.2) does have improvements over previous releases. Both tools have graphs for Summary visualization as well as export facilities.

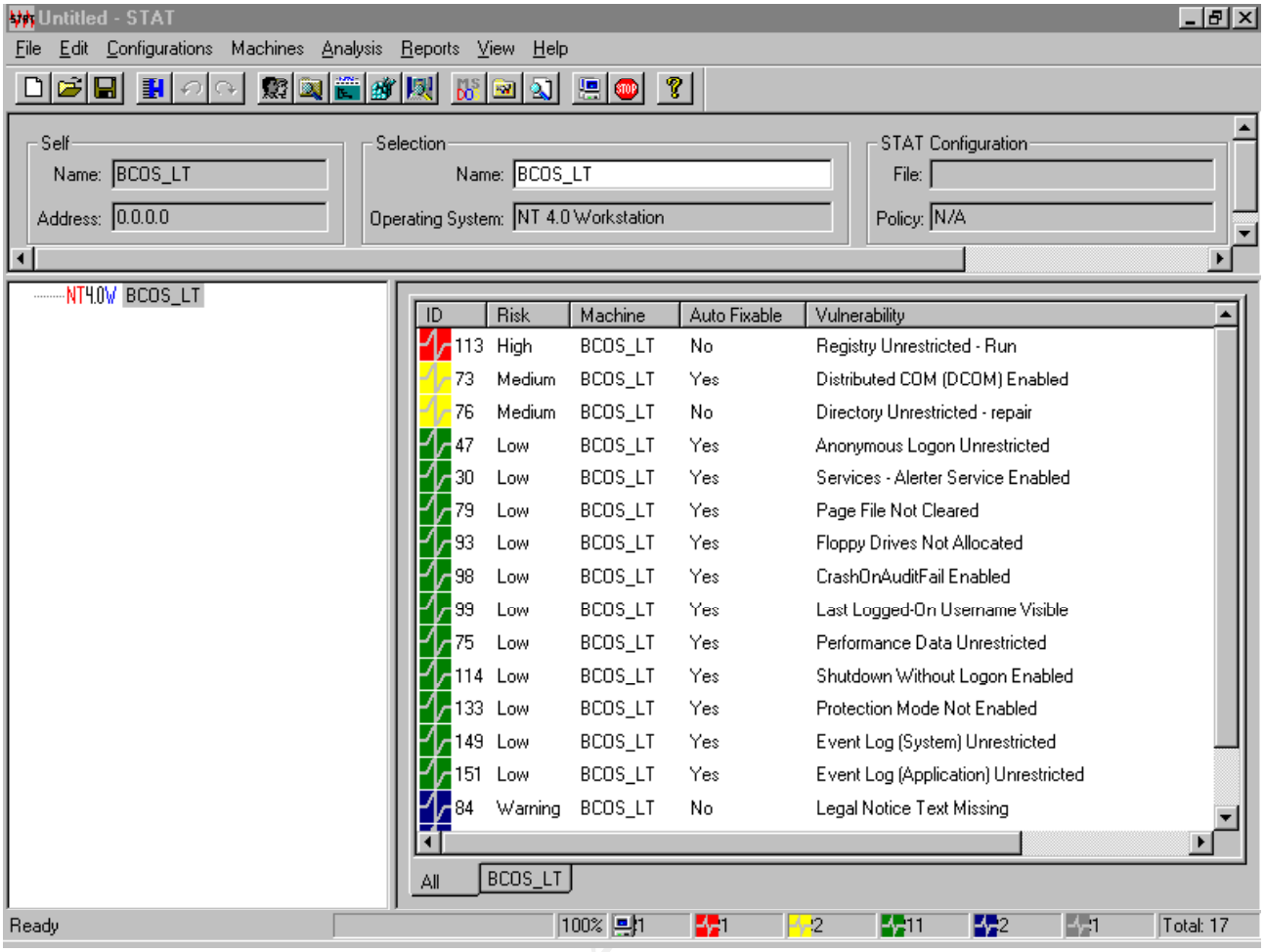
STAT reports has an *Executive Summary,* including a color pie graphing of the percentage of each level of vulnerability, and a summarized vulnerability risk depicted as high, medium, low, and warnings. A *Network Summary* 3D colored bar type graph is available which includes each scanned machine in a network graphed with the vulnerabilities, grouped by risk. *Vulnerability Summary* reports *by Count* and *by Category* as well as a "plain" *Vulnerability Summary*, which seems to be a detailed list to this observer. Other reports include *Detailed Vulnerabilities and Detailed Vulnerabilities By Risk*, as well as *Compact Detailed Vulnerabilities* or *Compact Detailed Vulnerabilities By Risk*. A *Simple Listing* report is also available. STAT also has a *Compare Scans* feature which is useful as a "before and after" type of report which lists the items remaining "after". It would seem more useful to be able to list the items that have been eliminated (or fixed). This report in a detailed form could then provide the needed documentation for exactly what registry keys, permissions, or policies were made.

Security Expressions reports are a bit less impressive and do not contain the detail that might be needed for documentation of changes made in many environments. Colored graph summaries are available, but previous scan reports are only available if the scan was run in batch mode. The reports tab offers reports on *Server Scan Tab*, *Batch Tab*, *Previous Scan*, and *SIF*. It is not obvious, even after reading the help file, how or when to use each option. The most detail is available on reports of previous scans, but this feature is not obvious and was discovered only by a technical support call.

User Friendliness

STAT's console and options are straightforward and easy to navigate. After a small amount of perusing the menus, a configuration file can be loaded, a machine or group of machines selected, and the scan run with no help from *Help*. The STAT console has icons for running *regedit, usrmgr, NT Diagnostics* and other system programs. While these icons are handy, the same result can be achieved just as easily by running the appropriate executables. Below is a screen shot of STAT's main console with the results of a scan of an OOTBS Windows NT 4.0 workstation install.

© SANS Institute 2000 - 2005 Author retains full rights.



Security Expressions' console and screens are not quite so intuitive. After loading both the SANS and the MS White Paper rule sets and running a quick scan, errors were found in the rules. Security Expressions has the potential to check for any registry key or value, registry permission, file or directory permission, policy parameter, and change them as needed. This process, however, does require quite a bit of time to configure and maintain. While STAT is much less time demanding and more intuitive to operate, it does not have the potential and flexibility of Security Expressions.

The "auto-fix" option in STAT works, but is not available for all vulnerabilities (although the console report does gives very detailed instructions for fixing all OOTBSs found). Security Expressions offers a "change" option for any registry key value, policy parameter, or permission change, but as noted earlier, care must be taken to ensure that the rules and changes that will be made are accurate.

Producing a report from STAT is just a matter of looking over the various reports on-screen and choosing an appropriate one to print or export. Securities Expressions' Reports tab screen is a little cryptic and the reports are difficult to read on screen (especially on a laptop).

Summary

While STAT seems the most user friendly to operate, Security Expressions has awesome

© SANS Institute 2000 - 2005 Author retains full rights.

potential. Each tool has its attributes and its deficiencies when used alone. After the initial OOTBS treatment, STAT could be used for a quick check to ensure that newly discovered vulnerabilities are addressed and documented. Security Expressions could then be used to make batch changes to policies, permissions and to search for inappropriate user/group rights or permissions. The best scenario, budget permitting, would be to use the tools in a complimentary fashion to beat the OOTBS and keep the continuous birth of baby NT bugs at bay.

---

[1] Bennett, Graeme. "Planning on improving your Windows NT/2000 Security? You should be.". July 6, 2000. URL: www.securepurchase.com/pcbuyersguide/solutions/security/NTSecurity.html
[2] Sans Institute Publications. "Windows NT Security – Step By Step". URL: www.sans.org/newlook/publications/ntstep.htm
[3] Microsoft Security Checklists. URL: www.microsoft.com/technet/security/tools.asp
[4] Harris Corporation • STAT • P.O. Box 8300 • Melbourne, FL 32902-8300, www.statonline.com
[5] Pedestal Software, LLC, www.pedestalsoftware.com
[6] ntbugtraq@listserv.ntsecurity.net or www.securityfocus.com
[7] Microsoft Security Bulletin e-mail. URL: www.microsoft.com/technet/security/notify.asp

© SANS Institute 2000 - 2005, Author retains full rights.