Global Information Assurance Certification Paper

WebTrends Security Analyzer
Patrick Wengert
March 16, 2001

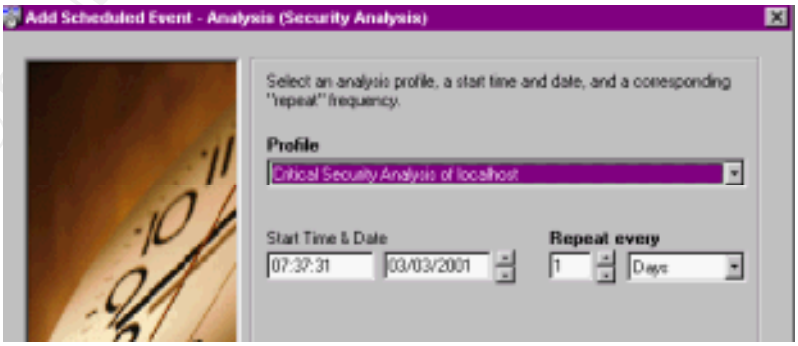
Introduction

Everyone focuses on securing their Internet servers, but what about the rest of your machines? The production department says their servers must be kept up and running, and no one has "hacked" them yet, and besides, who would want to?

According to most experts, the majority of network attacks will come from internal sources; they won't have to go through a firewall. The attackers are able to automate or script many of their attacks, why shouldn't you have some automated tools, also? While scanning software may not find all the holes, they can simplify the search on large networks. NetRecon, SARA, SAINT, and CyberCop are just a few of the scanners out today. I am going to look at WebTrends Security Analyzer – Enterprise Version.

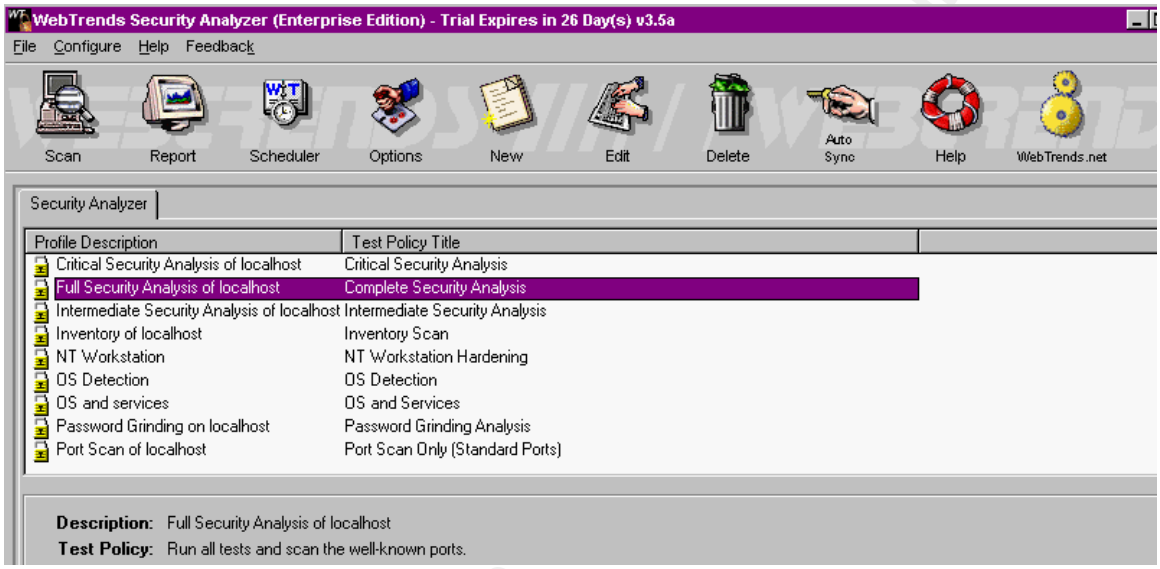
Security Analyzer

Using WebTrends Security Analyzer (WSA), there are three different methods of scanning your servers and workstations: local scans, network scans, and scans using agents. WSA can be installed and run locally on any Windows 9x, NT 4.x (x86) or 2000 machine. Once installed, it accesses the registry in order to perform its security checks. In order to run network scans, it must be installed on Windows NT or Windows 2000. It needs full access to the registry in order to do a security scan, if there is no registry or it does not have full access, it will do port scans. So to scan non-Microsoft operating systems, like Linux or Unix, the hosts need to have a standard TCP or UDP connection and WSA will do a port scan. There are, however, agents that can be loaded onto Microsoft, Linux, and Solaris machines. These agents will perform the scans locally, cutting down on the amount of network traffic generated by the software. To further alleviate network traffic, and to simplify the scanning process, WSA can schedule the scans to be performed. You select the date and time you wish the scan to start, and how often you want to repeat it.



Or, if you prefer, you can use the command line to schedule different scans or create batch jobs.

The minimum system requirements for running the program are 40 MB on the hard drive and 64 MB of memory, although the more memory you have, the better off you will be. I installed and ran the program on two IBM laptops, a P166 with 256 MB memory running nothing else, and on an 800 Mhz machine with 256 MB memory. You will definitely want to go with the faster computer. Installation of the software is very simple, just run the setup program; there are no settings to worry about. Once installed, it does not take long to get a feel for the software. The GUI interface is pretty straightforward. I was able to figure out most of the basics without resorting to the manual.



While previous versions of WSA seemed to focus only on NT-specific vulnerabilities, the current version has over 1100 different tests, with approximately 200 specifically for UNIX systems.

WSA uses "profiles" and "policies" to perform their scans. When you install the software, there are some default profiles and policies already configured, all you have to do is select one and click the scan button. Simply put, a profile determines what machines you are going to scan and what policy to use, while the policy is a collection of the different security tests.

POLICIES

Policies define the each vulnerability as a TEST, and then combine various TESTs into TEST GROUPs. There are 20 different test groups you can choose from. They cover things like: File Access Control; Registry Access Control; Application Vulnerabilities; Backdoor Vulnerabilities; Mail Server Vulnerabilities; Password Strength; Remote Admin Utilities; Unix Vulnerabilities; Web Servers; NT Privileges; and NT Workstation Hardening. Within each test group are the individual tests. The tests are prioritized in three categories – high, medium, and low risk. Some examples of these are: in the application vulnerability group, it classifies the L0phtCrack packet drivers as a high risk

vulnerability; it has various checks for the Office 2000 software at different levels of risk; in the Unix test group, it check for file ownerships and permissions, and depending on the file, determines its risk level.

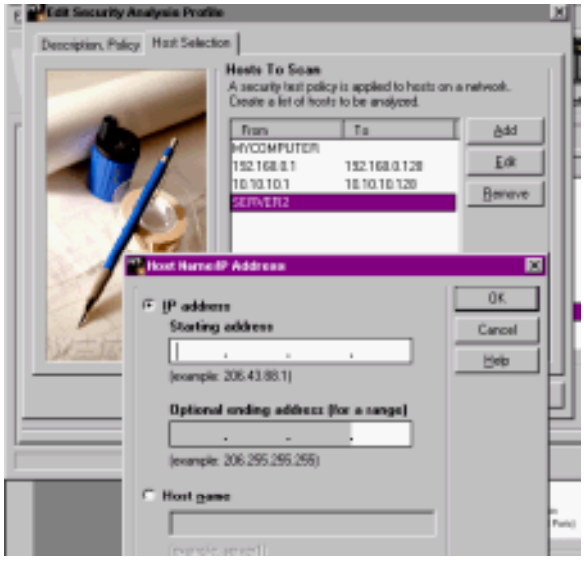
It will do a TCP/IP and/or UDP port scan of the common ports, or you can add/delete ports you wish scanned. There are specific tests for the BackOrifice and NetBus and NetBus Pro backdoors. You can see if the Chargen, Echo, Finger, FTP, Gopher, HTTP, NNTP, POP2, POP3, Rlogin, SMTP, and Telnet services are running. WSA is able to resolve Hostnames and it will try and detect the OS via NETBIOS and the Telnet Banner. It can differentiate between Solaris, Unix, Linux, Windows 95/98, NT 4 Workstation, NT 4 Server as a PDC, BDC or just server, and HP JetDirect Printers. Although not as thorough as NMAP at identifying the operating system, it is able to break out the Microsoft products. Security Analyzer also does a good job of breaking out the Microsoft share points and user names, again, if it can access the registry.

As we all know, new vulnerabilities are being discovered all the time, so how can you keep your tests up-to-date? WebTrends does have a Platform for Open Security Testing Security Developers' Kit (POST SDK) included, where you can write your own security tests. Or, you can use the AUTOSYNC feature, which will go to the WebTrends web site and download any new tests they have developed. There is also a place on their website for you to upload any tests you have created, and download any tests created and uploaded by others. These tests are broken into 2 sections, those certified by WebTrends, and those that are not certified. These new tests are given a risk factor and placed into a test group. When you create or modify a test policy, you have the option of selecting which of the new tests, by risk factor, you wish to have included in your scan. So each time you download new tests, they are automatically added to the scans, you do not have to go and edit the test policy.

Another vulnerability test WSA can perform is a Password Grinding Test. The software provides a master dictionary - *Install/Dictionary/full.dict*, which the program uses to try and "guess" account passwords. Any text editor can edit this dictionary, or you can create your own dictionary files and use them with or instead of the one provided. Finally, WSA will also let you know which passwords are under 8 characters.

PROFILES

When you create or edit a policy, you must define which machines the scan is going to look at. There are two ways to do this, by host name or by IP address. If there are just a few you wish to scan, you can enter their hostnames, if you want to do a range of IP addresses you can enter them – 192.168.0.1 through 192.168.2.254, or you can break it up into smaller ranges – 192.168.0.1 thru 192.168.0.128 and 10.10.10.1 thru 10.10.10.254 etc.



REPORTS

You have two options when running a report; it can be in HTML format or as a WORD document. Once the scan has completed, the data is broken down into a tables and graphs. You can get a graph of the number of host vulnerabilities, a table of the most vulnerable hosts, the most frequent high, medium and low risk vulnerabilities, all the detected vulnerabilities and their fixes, and a breakdown of fixes required by each host.

High - Unauthorized entry in NullSessionPipes key

An unauthorized entry was found in the NullSessionPipes key. These entriesallow null session access to the listed object.

Fix - Investigate NullSessionPipes entry and remove if unnecessary

If the entry is not necessary - remove it from the registry key. Before removing it, youshould make sure that it is not needed. If the entry is needed, you can add it to the list of authorized objectsby editing this test's properties.
The registry entry can be found at:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Name: NullSessionPipes

The software will generate different tables of service vulnerabilities, by host, platform, and total. You can select to print the test policies used in the scan; they will give the group and all tests used within the group. It will also list the ports you chose to scan. A service inventory can be generated, including a graph of the top services, all services detected, and a list of services detected by host.

mybadwebserver (123.456.789.10)

www-http[TCP:80] , Unknown (usually sunrpc)[TCP:111] , Unknown (usually loc-srv)[TCP:135] , Unknown (usually netbios-ssn)[TCP:139] , admin35-serv , Afd , Alerter , atapi , Beep , Cdfs , Cdrom ,

Disk , Diskperf , EventLog , Fastfat , Floppy , https-mybadwebserver, i8042prt , IBMFE , ipsraidn , Kbdclass , KSecDD , LanmanServer , LanmanWorkstation , LicenseService , LmHosts , Messenger , Mouclass , Msfs , Mup , Nbf , NDIS , NetBIOS , NetBT , NetfBase , NetFin , Norton Program Scheduler , Npfs , nsrexecd , Ntfs , Null , Parallel , Parport , ParVdm , PlugPlay , portmap , ProtectedStorage , Rdr , RpcSs , Scsiscan , Serial , SNMP , Spooler , Srv , Tcpip , TGrab , VgaSave , Unknown (usually sunrpc)[UDP:111] , Unknown (usually loc-srv)[UDP:135] , Unknown (usually netbios-ns)[UDP:137] , Unknown (usually netbios-dgm)[UDP:138] , Unknown (usually snmp)[UDP:161]

An inventory of the hosts detected and a total of the number of platforms detected can be had. You can also get a list of the shared resources by host, and the detected users and groups.

Previous scans are saved, and can be used to run comparison reports. You can get a list of vulnerabilities and services that no longer exist, a list of new ones, and/or a table with the results.

Vulnerability Differences			
Host	**Vulnerabilities**	**Current Scan Sat Mar 24 13:15:00 2001**	**Previous Scan Fri Mar 09 08:15:43 2001**
mybadwebserver	Unauthorized program in Run key / d:\PROGRA~1\nav\vptray.exe	Found	Not Found
	Schedule service	Not Found	Found
	Unauthorized program in Run key / C:\PROGRA~1\Navnt\npscheck.exe	Not Found	Found

Service Differences			
Host	**Services**	**Current Scan Sat Mar 24 13:15:00 2001**	**Previous Scan Fri Mar 09 08:15:43 2001**
mybadwebserver	DefWatch	Detected	Not Detected
	Intel Alert Handler	Detected	Not Detected
	Intel Alert Originator	Detected	Not Detected
	Intel File Transfer	Detected	Not Detected
	Intel PDS	Detected	Not Detected

All of this information can be customized into as many different report styles as you need. As with the scans, you can schedule the reports to also run after the scan, and then be emailed to the appropriate person.

Conclusion

While a security scanner will not solve all of your security problems on your servers and workstations, they can be used to speed up the process and verify some of the work was done. If you work in a large, diverse environment where security was never really an

issue, and no one person knows how all the servers are set up, and documentation doesn't exist, a scanner will at least provide a starting point. If you're not going to scan your network looking for vulnerabilities, someone else may.

Resources

Forristal, Jeff, and Greg Shipley. "Vulnerability Assessment Scanners." Network Computing. 8 Jan 2001. URL: http://www.networkcomputing.com/1201/1201f1b1.html (16 Mar. 2001).

Hammond, Eric. "WebTrends dispatches security agents." Federal Computing Week. 22 May 2000. URL: http://fcw.com/fcw/articles/2000/0522/tec-webtrend-05-22-00.asp (15 Mar 2001).

Korzeniowski, Paul. "Scanning for security holes." Federal Computing Week. 10 Apr 2000. URL: http://fcw.com/fcw/articles/2000/0410/sec-scan-04-10-00.asp (15 Mar 2001).

Mendelson, Edward. "The Danger Within." PC Magazine. 16 Nov 2000. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2651622,00.html (15 Mar 2001).

Mendelson, Edward. "WebTrends Security Analyzer 3.5." PC Magazine. 16 Nov 2000. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2651630,00.html (15 Mar 2001).

WebTrends Corporation.
http://www.webtrends.com.