Global Information Assurance Certification Paper

Securing an Existing IIS 5.0 DMZ Infrastructure

Julius Fitzgerald

GSEC Practical Version 1.4b

Option 2

March 24, 2004

Abstract

The task of designing a secure infrastructure for IIS 5.0 web servers within a DMZ is difficult enough. Securing an existing DMZ becomes exponentially more difficult due to the added requirement of retrofitting those currently working servers with more appropriate security settings, policies and operational procedures while not adversely affecting website or application availability and keep costs to a minimum throughout the process.

The purpose of this writing is to outline the steps I took to obtain management approval to review the existing security settings and procedures within the DMZ – Web Hosting Operations infrastructure, prepare a strategy for implementing additional security measures with minimal service impact, and outline additional security best practices our company implemented for maintaining the new security posture.

The environment referenced for this writing consists primarily of Windows 2000, SP4, IIS 5.0 web servers with the latest security rollup patches and hotfixes.

Assumptions

The author assumes the reader has a solid understanding of Windows 2000 Domain infrastructures, including Domain and Local User accounts and their differences, Organization Units, Group Policy Objects, application of Security Templates, IIS 5.0 architecture, Basic TCP/IP routing principals and firewall technologies.

For the purposes of this writing, user accounts, rights and permission references are limited to web service requirements only. There are many other permission requirements which need to be taken into account when hardening your Windows server systems.

Justifying the Review

Last fall I rejoined a company to supervise their Web Hosting Center operations. Having attended the SANS Security Essentials training course in early December, I found myself noticing a number of security best practices and protective measures, which had previously been in place, were no longer followed or being enforced.

I discovered the analysts within the Web Hosting Operations center were sharing user accounts with Enterprise Administrator privileges. The Local Administrator accounts on the web servers still had the same password that had originally been

created before I left almost three years before. Sure, company policies prohibited sharing accounts, and included instructions to change administrative account passwords at least every six months, but those policies had not been enforced due to a lack of user account auditing. Besides, the analysts who were aware of the policies had interpreted them as applying only to normal user accounts. After all, the systems administrators were the only ones who knew the shared account information, right? Most analysts did not even know there were company policies regarding administrative accounts. Analysts were given a copy of the company IT policies at the start of their employment, but were not required to sign a copy of the policy to show they had been reviewed.

I knew that in order to exact any changes to the current operational processes I would have to first gather some basic information to present to my manager. I would need to perform a systems audit and network vulnerability review to determine the extent of our exposure to malicious activity.
I approached my management with the idea of performing such an audit of our configuration and processes and received a cold shoulder. The overall general attitude toward security threats was "We haven't been compromised yet, so there must not be any real risk". It is a very difficult task to convince others that waiting for the day a serious compromise takes place, then scrambling to find and close the vulnerability, is not the proper security stance. My management assumed the cost of such an audit would be too much to justify.

Over the next two weeks, I took some time to interview each web analyst and review the existing company security policies in order to note the deficiencies and non-compliance within only the Web Hosting Operations area of responsibility to keep the scope of the review relatively small. I prepared a brief detailing the most evident deficiencies and presented this to my manager. Faced with a report detailing our current non-compliance, my manager conceded and agreed to allow me to perform a cursory system and network vulnerability scan. Following company procedures, I submitted a change request to perform the system and network vulnerability scan, and user account audit during a pre-defined maintenance window to limit potential service impact.

I ran the Microsoft Security Configuration and Analysis tool using a modified version of the HISECWEB.INF security template as my baseline configuration for analysis against one web server in each web farm. The HISECWEB template settings were modified to meet the recommended IIS 5.0 security settings from the National Security Agency's – "Guide to the Secure Configuration and Administration of Microsoft Internet Information Systems 5.0" written by Walker and Christman and Microsoft's - "Secure Internet Information Services 5 Checklist".

The analysis revealed unnecessary system services such as Alerter, Clipbook, DHCP Client, Internet Connection Sharing, Messenger, NetMeeting Remote Desktop Sharing, Utility Manager and others were running on most of the web

servers. User rights assignments had not been locked down. There were no user account policies, or auditing policies defined.

I also ran DumpSec, from SomarSoft, against one server in each web farm to gather more detailed information on current user rights, user account and group membership information, and file and directory ACLs (the use of DumpSec, and other tools mentioned will be discussed in more detail in the Tools section of this writing). The review of user account information, group membership and user rights assignments revealed numerous potential account vulnerabilities. Many administrator level user accounts had not had passwords changed for years, if ever. I discovered Domain Administrator accounts which had not been accessed for more than two years. Upon further investigation, I learned these accounts belonged to analysts that had moved on to other positions within the company, or had left the company altogether. The accounts had not been disabled, either. Service accounts with Domain Administrator privileges were being used for application services such as NetBackup, NetIQ, TrendMicro antivirus, and a myriad of web applications.

File and Directory ACLs revealed that the default Everyone group was still allowed full control access to a number of system files and executables, system administrative shares and the entire website directory structure.
The systems and network vulnerability scan, utilizing eEye's - Retina Network Security Scanner, revealed unnecessary TCP/IP port access allowed via both our edge router ACLs and firewall rules, leaving numerous attack vectors unchecked. RPC, ICMP, SMB and NetBIOS ports were accessible from any internal network computer if you knew the IP address of the system in the DMZ that you wanted to establish a connection to. SMTP port access was allowed to all web servers from the internet, even though the servers did not need SMTP services running. The web servers were allowed to initiate communication over any port to the internal database servers.

On the bright side, the DMZ servers had been kept up to date on critical security patches and Microsoft's IISLockdown tool and URLScan utility had been implemented on most of the web servers. Having run IISLockdown and installing URLScan on most of the web servers had at least mitigated some of the potential exposures. However, the server build procedures were out of date, and did not include running these utilities. This resulted in newly built servers not having even that level of protection.

There had previously been an Intrusion Detection System (IDS) in place. However, the IDS agents had been gradually removed from servers as Operating System upgrades were performed and the IDS agents were not upgraded. As far as management was concerned, there had been no known successful attacks since the inception of the Web Hosting Center. This false sense of security, and budget pressures, prompted management to decide there was no longer a need for an IDS system to warn of attempted probes and attacks. Fortunately,

Microsoft's IISLockdown tool and URLScan utility had been implemented prior to moving away from the IDS system. A review of URLScan and IIS web logs revealed numerous probes and attempts to hack our systems. Most of these were successfully blocked. However, the number of attack vectors being allowed via the router and firewall, and the servers lack of an audit policy and additional hardening, left me wondering how many times we may have already been compromised with no way to tell if the attacker gained system privileges and was able to cover his/her tracks.

I compiled the results of the system and network vulnerability reviews and consolidated them into a report of potential risks. The report, including a short list of recommendations to correct the most severe vulnerabilities first, was presented to management. The initial recommendations for adding Domain and Local security policies via Group Policy Objects for account privilege, password policy, and file and directory permission changes would take no more than a few Analyst cycles to test and implement since we had a lab to test the changes prior to placing into production. I was confident management would be willing to implement these recommendations since costs would be low.

The firewall rules and router ACL changes would take more time to implement as there would need to be considerably more network analysis performed before the full scope of needed changes could be determined, and a test environment was not readily available for these changes to be tested prior to placing into production. These changes would need to be gradually implemented to limit the potential to disrupt customer activities. This would be the most costly of the areas to implement.

Project Scope

My manager was amazed at the number of potential vulnerabilities discovered during such a minimal review. Since most of the vulnerabilities discovered during the initial review were already out of compliance with company security standards and policies, management approval to take the next step in further tightening security was not as difficult to obtain as I first imagined.

Upon receiving management approval to perform a more in-depth review, and implement the initial user account and password policy recommended changes, I was allocated a small number of analyst cycles to begin a project to further review and strengthen security within the DMZ. This afforded me the opportunity to assemble a project team consisting of analysts from the Web Hosting Operations, Systems Engineering, Network Engineering and GIS Security groups. The project scope was to audit our current security settings and make recommendations for bringing the DMZ services into line with Industry Best Practices and existing company policies. We were also tasked with defining new policies where applicable. The team's recommendations were to be summarized

and submitted to management for sign-off as each stage of the review was completed. The following project stages were defined to maintain group focus and allow for smooth implementation of changes.

- Define Domain and Local User Account Permissions, Rights.
- Removal of Unnecessary System Services.
- Service Account Permissions and Rights.
- File and Directory Permissions.
- Inbound and Outbound TCP/IP Traffic Analysis Review.
- Server Operating System - Service Pack and Security Rollup Patch Reviews.
- Security Policies Reviews

Tools

The team reviewed the tools currently available to us and decided on the below list to review the current vulnerability situation, prepare reports, and implement changes as we proceeded.

DumpSec from SomarSoft.
DumpSec is a free utility used to dump detailed security information for Windows users and groups, file and directory ACLs, registry ACLs, and audit settings. The results can be saved in a wide variety of file formats, including .txt or .csv for importing into Excel spreadsheets for sorting and ease of reading. It can also be saved in it's own native file format if you want to use the utility's built-in GUI for reviewing the reports. I consider DumpSec a must have for any system administrator's toolbox. DumpSec can be downloaded directly from SomarSoft at: http://www.somarsoft.com

Retina Network Security Scanner from eEye Digital Security.
The full featured version of Retina Network Security Scanner can be used to scan your entire network, or a subset of IP addresses, for vulnerabilities ranging from the SANS Top 20, to individually tailored application scans, or any combination of known exploit scans. Retina has one of the largest vulnerability databases on the market, and offers real time automatic updates as new exploits are discovered and added to their database. The HTML formatted reports are very intuitive, and simple to read. There are even different types of reports that can be generated. Report generation options range from Technical for administrators, to Executive overviews for your managers. The reports even offer suggestions for mitigating any exploits found during the scan. You can purchase Retina, or download an eval version at:
http://www.eeye.com/html/Products/Retina/Features.html

Sniffer Distributed Analysis Suite ver. 4.3.5 from Network Associates
The NA sniffer appliance has a web-based interface which allows for ease of management for network traffic monitoring, analysis and reporting. The sniffer

has very detailed filtering capabilities so your traces can be easily read to determine traffic patterns quickly and precisely. The product is pricey, but delivers unparalleled real-time network traffic monitoring. You can review the product at:
http://www.networkassociates.com/us/products/sniffer/mgmt_analysis/sniffer_distributed.htm

Microsoft Baseline Security Analyzer.
The MBSA is another free utility from Microsoft. It can be used to quickly scan your systems for security misconfigurations, security patch levels and vulnerabilities. It allows customization of the scan if you only want to scan for specific items such as patch levels, without having to review account settings, etc. It's HTML reports are easy to read, and it can determine if patches were successfully installed. I consider this tool another must for Microsoft systems administrators toolboxes. You can download the tool from Microsoft at:
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Microsoft Security Configuration and Analysis Tool.
The Security Configuration and Analysis Tool is a stand-alone MMC snap-in that can be used to analyze server security configurations, as well as for editing "canned" security templates. These templates can then be applied to your servers.
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/security_configuration_and_analysis.asp

Project Implementation

Defining Domain and Local User Account Permissions and Rights.
By applying the Principal of Least Privilege, domain and local user accounts were reviewed to determine which accounts required domain level administrative, or elevated privileges, and which accounts could be assigned lesser domain wide privileges while still maintaining sufficient local server privileges to perform daily administrative tasks.

- Web server analysts were assigned Domain User privileges and Local server Administrator privileges on web servers. This allowed the web analysts to perform all functions pertaining to web server administration, while reducing domain structure exposure if an account was compromised.
- The Default Domain Policy was configured to enforce password age, length, history and complexity.
- A Web Services Organizational Unit (OU) was created to allow application of GPOs and security templates specific to the web servers.
- A WebAnalysts domain group was created and delegated administrative access to the Web Services OU to provide the analysts with access to the servers. This allows the web analysts to control the web servers, while

preventing the web analysts from accessing other DMZ components such as DNS and Mail servers which were placed in other OUs to control access to those services.

- A Web Services security template was designed and applied to the newly created Web Services OU to enforce password history, complexity and minimum age requirements.
- Shared administrative accounts were removed and each web analyst was assigned an individual account with permissions restricted to that Analyst's administrative duty requirements. This allowed for effective account access auditing policies to be put into place for security reviews.
- Local Administrator accounts were renamed and a 16 character complex password was applied to each account. Each server had a different Local Administrator account name and password combination created to prevent an attacker from guessing another server's Administrator account in the event one of the web servers was compromised.
- A local WebUsers group was created on each server. The local IUSR_%machinename% and IWAM_%machinename% accounts were added to the new group. This group was assigned Log on Locally rights as required for access to IIS resources.
- The default Everyone group was removed from the Log on Locally, Access this Computer from the Network, and Logon as a Batch Job rights to prevent anonymous access to the servers. These rights were assigned to the Local Administrators group and the Local System accounts.

Removal of Unnecessary System Services.

A complete review of system services was performed and compared against Microsoft's Windows 2000 Security Configuration Guide and List of Services Needed to Run a Secure IIS Computer, Mark Burnett's Securing Microsoft Services, and the National Security Agency's Microsoft Windows 2000 Guides.

- Unnecessary services were disabled to limit potential buffer overrun exposures.
- Service startup parameters were added to our Web Services security template to enforce service restrictions.

Due the wide range of specific IIS5.0 server configuration requirements, these services will not be listed individually here. However, please review the above referenced guides to find what works within your specific IIS5.0 implementation.

Service Account Permissions and Rights.

Application services and the associated service accounts on each web server were reviewed for account permissions and rights assignment.

- Domain level service accounts were removed and each service was assigned a local server account based on the service's required privileges. For example, the NetIQ service account requires Local Administrator rights on a server to perform monitoring and management tasks. The NetBackup service account requires only Backup Operator privileges to perform required tasks.

Limiting services accounts to the local server, with unique account names for the services on each server, minimizes the possibility of the account being used to access domain resources in the event an account is compromised.

File and Directory Permissions.
File and directory ACLs from each of the web servers were reviewed. The permission dumps were compared against each server to determine what common access permissions could to be applied across all the web servers.

- A new folder structure was designed to separate static web content from scripts and executables.
- The WebUsers local group was given access to the web content folder structure based on access requirements. The group was given Read and Execute access to the script and executable directories, while being limited to Read only access for static content folders.
- The default Everyone group was removed from system administrative shares. The system administrative shares were limited to Administrators and Local Systems accounts having access.
- The local Users group was given Read access to necessary system folders to prevent web visitors from writing to protected system folders.
- The ACLs were applied to the Web Services security template to insure permissions remained enforced even if an analyst inadvertently changed permissions.

Inbound and Outbound TCP/IP Traffic Analysis.
The Network Associates – Sniffer Distributed appliance was used to analyze network traffic during normal web server operations. The results of the traces were examined to verify TCP/IP port requirements for web applications.

- Router ACLs and firewall configurations were reviewed. Current rules were re-evaluated to insure unnecessary and outdated rules were removed. Many firewall rules had been relaxed during the data center move two years ago to insure application communications were not interrupted. This relaxation of firewall rules was never reviewed following the data center move to once again restrict protocol access to a number of the web support services.
- Vendor documentation for the web applications was reviewed to insure only the appropriate protocol ports were being allowed, and more restrictive TCP/IP protocol rules could be implemented.
- Firewall rules were tightened for the internal network facing web server NICs to restrict traffic based on specific TCP/IP port requirements. This allowed us to maintain communication to backend services such as database, Network Management Systems, reverse proxy access to internal web servers, remote control access from internal management workstations, etc., while providing additional protection for our internal systems in the event of web server compromise.
- An outbound router ACL was implemented on the edge routers to restrict web server initiated traffic to the internet to only the IP addresses and

protocol ports required for communication with external party's servers. This reduces the possibility of a compromised server transmitting data outside the company's network unintentionally. This also reduces the likelihood of one of our servers infecting other internet web servers in the event of a system infection caused by such worms as CodeRed, Nimda, or Blaster.

- All TCP/IP port rules were fully documented on a per service basis to allow periodic reviews to be performed. This helps insure unnecessary ports are not left open as applications and services are retired.

Server Operating System - Service Pack and Security Rollup Patch Reviews.

The Microsoft Baseline Security Analyzer (MBSA) was used to poll each web server for patch level verification.

- A number of servers showed security rollup patches having not been successfully installed. These servers had the relevant patches reinstalled to bring servers current with security patch level requirements.
- Internet Explorer, MDAC and .NET versions were reviewed. Servers with older versions were updated to insure server build consistency. Applicable patches for these components were applied following component upgrades.
- IISLockdown and URLScan were applied to all existing web servers, and the Web Server build procedure has been updated to include instructions for applying both.

Security Policies Reviews

The existing company security policies were reviewed to insure they were both enforceable and easily understood. New policies were written to cover gaps in existing policies and to allow for enforcement of new security settings

- An Administrative Account Usage Policy was defined to reduce the use of privileged accounts. Use of administrative accounts must now be associated with an audit, a problem investigation, break/fix, or a project implementation.
- A new policy regarding aged accounts was written. The new policy requires administrative accounts for analysts who no longer work within a respective area, or leave the company, to be disabled for a minimum six month period after the analyst leaves. This allows account information to be available for future auditing of account usage, or other investigation requirements.
- The existing Local Administrator Account Password Policy was updated to include a schedule for changing passwords on a six month basis. Managers and supervisors are the only personnel allowed access to the passwords for the accounts.
- A new policy was written defining the appropriate use of service accounts. Service account creation requires management approval, and must be

limited to only the required permissions and access for the service to function.

- A new policy was written defining the introduction of new TCP/IP port requirements. New firewall port requirements must be reviewed by a committee consisting of representatives from Network Engineering, Systems Engineering and GIS Security before being added to the firewall rules. All port rules are now to be reviewed annually to insure security integrity is maintained.

Afterward

Although there is no sure fire way to completely protect web servers from malicious activities, the implementation of the new security procedures, combined with adherence to both the new and existing security procedures, has substantially reduced the possibility of compromised machines or accounts being used to launch attacks against additional targets both within our DMZ and outside our network.

The project has not only increased our security footing in the DMZ, but due to it's relatively inexpensive cost to implement (the entire project consumed a little over 100 analyst hours), has prompted corporate management to allocate additional funds to this year's IT budget for reviewing internal systems security settings and speed up domain migration efforts to allow the incorporation of Active Directory security implementation throughout the entire organization.

The project has also spawned a renewed interest in security among all members of the IT staff. We now hold monthly meetings between all IT groups to discuss current security trends and new vulnerabilities. All IT staff members are encouraged to attend these meetings and voice their opinions. This new "Open Policy" has generated a surge in staff participation throughout the organization.

Although we may not have all the necessary security measures in place today to profess we are fully safeguarding all our company assets, I do feel we are well on our way to getting there.

References

National Security Agency's - Microsoft Windows 2000 Guides
http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1

National Security Agency – Authors – William E. Walker IV and Sheila M. Christman – "Guide to the Secure Configuration and Administration of Microsoft Internet Information Systems 5.0" ver. 1.4 – 29 October 2003
http://www.nsa.gov/snac/os/win2k/iis_5_v1_4.pdf

Microsoft – Author – Michael Howard - “Secure Internet Information Services 5 Checklist” – 29 June 2000
http://www.microsoft.com/technet/Security/topics/issues/w2kccscg/default.mspx

Microsoft – “Windows 2000 Hardening Guide” ver. 1.0 – 24 January 2004
http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en

Burnett, Mark – “Securing Microsoft Services” – 22 May 2002
http://www.securityfocus.com/printable/infocus/1581
March 24, 2004

Microsoft – “How to Use and Apply the IIS Secure Internet Web Server and Secure Intranet Web Server Security Configuration Templates in Windows 2000”
http://support.microsoft.com/default.aspx?scid=kb;en-us;317376

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event