Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Introducing Defense-in-Depth to a Small ISP

With the recent spate of worms and vulnerabilities, and the increasing public awareness of same, a rural Internet Service Provider (ISP) requested some assistance in assessing the security of their production server and network environment. The ISP has limited in-house technical resources, and utilizes consultants on an as-needed basis. After a few service interruptions due to security-related issues (worms, web site defacement, Denial-of-Service attacks), I was asked to provide some specific recommendations on how to ...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Monitoring for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Introducing Defense-in-Depth to a Small ISP

A Case Study

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b Option 2

© SANS Institute 2003, Author retains full rights

Submitted by: Rodney R. Anderson
Date: November 12, 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

INTRODUCING DEFENSE-IN-DEPTH TO A SMALL ISP 1

Abstract 3

Assessment 3
Policies and Procedures 3
Network 4
Physical Security 4
Servers and Services 4

Recommendation and Implementation 5
Policies and Procedures 5
Network 6
Physical Security 7
Servers and Services 8
Newsgroup Server 8
Web/DNS Cluster 9
E-mail Cluster 11

Post-Implementation Assessment 12

References 14

© SANS Institute 2003, Author retains full rights

Abstract

With the recent spate of worms and vulnerabilities, and the increasing public awareness of same, a rural Internet Service Provider (ISP) requested some assistance in assessing the security of their production server and network environment. The ISP has limited in-house technical resources, and utilizes consultants on an as-needed basis. After a few service interruptions due to security-related issues (worms, web site defacement, Denial-of-Service attacks), I was asked to provide some specific recommendations on how to increase security and availability, without significantly increasing complexity or adversely affecting service usability.

Utilizing a "defense-in-depth" approach to security, I assessed their environment, made recommendations, and then re-assessed the environment to measure the impact of the changes. Because of the nature of an ISP's business, some recommended security "best-practices" are not practical, as they would adversely affect the services offered. In the highly competitive Internet access business, customers will not tolerate unreliable or hard-to-use services, so a balance must be struck between security and usability. So I was asked to limit the engagement to a few recommendations which could have the most impact, or best "bang for the buck". The layered nature of a "defense-in-depth" strategy, as outlined in the SANS Security Essentials track, seemed to make the most sense in this situation. Several areas were addressed which significantly increased security, yet did not take away from the usability of the services being offered.

Assessment

In order to assess the current state of the environment, I had to first define the environment and what was to be assessed. As the "customer" is an ISP, there are several services being provided to their customers. These are dial-up Internet access, broadband Internet access, web hosting, e-mail, and newsgroup access. The scope of my assessment was limited to the servers providing and supporting these services, the local network these servers reside on, and any policies and procedures relative to these servers and network. Exempted from the scope of my assessment were the modem banks and DHCP appliances used to support the dial-up and broadband Internet access. A firewall also exists between the servers and the open Internet, but it has also been exempted from the scope of this assessment, as its operation and management is currently outsourced.

Policies and Procedures

I initiated discussions with both management and staff to assess the existence and effectiveness of existing security policy and procedures. Immediately evident was a lack of any defined security policy. An operations manual existed, but covered only technical aspects of how to accomplish certain tasks, with no

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

particular regard to security. The staff involved in the day to day activities was somewhat security conscious, but there were no defined policies or procedures to assist them in keeping their environment secure.

Network

The network infrastructure was examined next. As the servers in question are providing services for customers of the ISP, they were separated on their own network, rather than being part of the parent company's corporate network. The only nodes on this network are the ISP servers, and there is no connectivity from them to any network or subnet other than the Internet. But, they were connected to the Internet via a very old router, which is no longer supported by the manufacturer. In addition to a lack of manufacturer support, we found that replacement parts are almost non-existent, which provided a definite risk to availability. The feature set of this router does not allow for any traffic filtering, address translation, etc., but only provides basic routing services.

Physical Security

The servers and network devices are all located within one computer room. The computer room also contains the helpdesk operator's desk, and is located adjacent to an office area and a customer-accessible demo room. There are four doors to the computer room, two to the outside, one to the office area, and one to the demo room. The outside doors are always locked, but the other two doors are never locked. Also, I found that several of the servers were logged in on their console, with no screen locks of any kind in force.

Servers and Services

There are four services being provided for the ISP customers. These are web hosting, Domain Name Service (DNS), newsgroup access, and e-mail. DNS and web services are provided by a two-node Microsoft cluster on Windows NT Server 4.0 Enterprise Edition. Newsgroup access is provided on a single standalone server running Windows NT Server 4.0. And e-mail is provided by another two-node Microsoft cluster, this one running Windows 2000 Advanced Server. The news server will be referred to as NT1, the web/DNS cluster servers as WD_A and WD_B, and the e-mail cluster servers as EM_A and EM_B. Each service required a slightly different approach to security, due to the presence or absence of a cluster, and the differing operating systems.

After proper permissions were obtained, industry-standard security tools were used to identify potential security problems with the servers used to provide these services. Although clearly written with their own tools and services in mind, Foundstone, Inc.'s whitepaper, "Scanning Safety", provided valuable reminders concerning vulnerability scanning on a live network. Nessus was used to scan for known vulnerabilities and nmap provided a listing of open ports. Microsoft's Baseline Security Analyzer was used to scan for missing service

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

packs, hotfixes, and known Microsoft vulnerabilities, and Foundstone's SuperScan, available from www.foundstone.com, was used to double check the nmap output. Output from each of these tools was then gathered and correlated to come up with recommendations to enhance the security of each server and service, without negatively affecting availability and usability.

Recommendation and Implementation

The results of interviews with staff and management, observances while onsite, and output from assessment tools were all combined to come up with several recommendations to enhance the overall security of this ISP environment. This section will detail those recommendations and the steps taken to implement them.

Policies and Procedures

The assessment highlighted a lack of defined security policy and a lack of security awareness in defined procedures. A security policy, no matter how rudimentary, is extremely important. The security policy answers a several key questions, such as *who* is responsible for *what*, and *why*. Policy gives direction and guidelines on what to do, when to do it, why to do it, and who should be doing it. Procedures take this one step further in defining how to do it, whatever it may be. Using the concepts outlined in SANS Security Essentials II: Defense in Depth, section 1.2.2, Basic Security Policy, I assisted the customer in outlining a basic security policy, to be evaluated and refined over time. An "acceptable use" policy did exist for their customers, but did not extend to their own employees. The security policy should define expected behaviors for users (customers, defined in the acceptable use policy and included in the security policy), administrators, and management. Without this policy, actions taken by administrators or security personnel could be misconstrued as malicious behavior. Or, malicious behavior (such as sabotage by a disgruntled employee) could occur and not be noticed until it's too late. Policies and procedures affect all aspects of IT security, and so additions are made to the policies as they are identified as necessary.

We began with an overall program policy, to define, at a high level, who is responsible for what aspects of information security. Management buy-in was obtained at the Vice President level, to provide credibility to the policies and their enforcement. Next, we created a few issue-specific policies, to provide guidelines on specific issues. As this will be evolving over time, we began with a few basics, namely passwords, physical security, and acceptable use. For example, some employees were using production servers to surf the Internet (they like the incredible speed), as there was no policy to prohibit it.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The existing operations manual, filled with procedures to accomplish day-to-day tasks, was also examined and augmented with security-specific procedures, including password administration and physical security procedures.

Network

Due to the outdated feature set and lack of manufacturer support, I strongly recommended that the existing router be replaced. A router was chosen from a reputable company, in a product family with a clear future direction. This will avoid winding up in the same situation as before, with an unsupported product in a business-critical position. And, by implementing an updated router, we were able to take advantage of security features that were previously unavailable to us. We began by implementing several of the general restrictions for Internet connectivity talked about in SANS Security Essentials I: Networking Concepts. The following steps were taken to decrease network exposure.

Internet Control Message Protocol (ICMP) is an extension to the Internet Protocol (IP) defined by RFC 792. ICMP provides a mechanism for control, error, and informational messages. For example, ping, a command commonly used to test network connectivity, uses ICMP packets to test connectivity between two IP addresses. While ICMP can be very useful in testing, it can also be used for malicious purposes. ICMP Unreachable packets could be used by an attacker to reconnaissance a network. ICMP Redirect packets could be used to send users to bogus servers on the Internet, rather than the servers they intended to reach. It is recommended to block both ICMP Unreachable and ICMP Redirect packets in the router. ICMP packets can also be used for Operating System fingerprinting, based on the responses received to certain ICMP packets. A very good discussion of ICMP and its potential misuses can be found in a whitepaper entitled “ICMP Usage in Scanning” by Ofir Arkin. There are differing opinions on whether to block all ICMP traffic, of just filter certain types. In order to minimize service disruptions, yet still take steps to increase network security, the customer and I elected to filter ICMP Unreachable and Redirect packets, while still allowing other types of ICMP packets through.

Network Time Protocol (ntp) is used to propagate and update the time on servers and networking equipment from designated time servers. Although there are time servers on the Internet that we could synchronize the time on our servers with, this gives an opening to a malicious user to change the time on our servers, thereby possibly hiding or changing evidence of an attack or compromise.

Simple Network Management Protocol (SNMP) is a protocol used to manage, monitor, and configure devices over a network. While SNMP can be a very useful protocol, it is not very secure in default configurations. And SNMP contains several known vulnerabilities. Since we do not use SNMP for management or monitoring, not allowing this traffic to come into our local network from the Internet reduces our exposure to well-publicized SNMP exploits.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IP source routing is a feature that allows a sender to specify the route a packet will take to a destination, as well as the route that any reply packets will take back to the sender. This is not a very well known IP capability, but is easily exploited by attackers, and should be blocked at the router.

An IP directed broadcast is a feature of IP where someone can send a packet to a network's broadcast address (a host address of all ones). Several network and reconnaissance attacks rely on the ability to send a broadcast and then analyze the return packets. This can be quite useful in trying to map a network for malicious purposes, but there is no legitimate need for a host on the Internet to be able to send broadcast traffic to the local network. These packets are also to be blocked in the router.

These few changes alone significantly reduced exposure to malicious intent. But there are more steps that can, and should, be taken to further minimize network exposure. Routers often include the ability to function as a minimal stateful firewall, with access control lists (ACL's) which can filter traffic based on source and destination ports, and connection state. The steps already taken and router based ACL's all address attacks from outside the local network. But we also need a way to determine if malicious activity is either originating on the local network, or has somehow been able to bypass or compromise the firewall or router protection. This is where a good Network Intrusion Detection System (NIDS) comes into the picture, and fits right in with a defense-in-depth layered strategy. There are several products available for network-based intrusion detection (NIDS), to assist in catching security breaches when they inevitably occur. A well-known (and free) NIDS is Snort, available from http://www.snort.org. Snort is an open source product with a large user community, so quite a bit of information is available to assist with implementation and use. A plan is in place to implement ACL's and Snort in the future, but these projects were beyond the scope of this initial engagement.

Physical Security

Physical security is quite often overlooked with regards to information security. It is also one of the most important aspects of information security, and ensures the safety of information technology workers as well as infrastructure and data. Once physical access has been gained, other security measures are much more subject to compromise. A good defense-in-depth strategy will help allow strengths in one area to augment deficiencies in others, but the overall strategy should involve all aspects of security. Physical security should address four objectives, confidentiality, integrity, availability, and safety. In my assessment I found that there were four entries into the computer room, two of which were not locked on a regular basis. Although a desk within the computer room is staffed during business hours, there will be times when no one is in the computer room, such as during breaks. I also found some of the servers were logged in with privileged access and no screen savers or screen locks in effect. Both of these

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

issues needed to be addressed, in order to satisfy our four objectives. In our environment, we have all of our servers located in one computer room, and also have the helpdesk located there. During business hours, the helpdesk is staffed by one employee at a time. If physical security is breached, then the safety of that employee is at risk, not to mention risks to data and infrastructure.

Using the security policy and procedures established as part of this engagement, physical security was augmented by implementing guidelines for access control through the four entryways into the computer room. Guidelines were also established for checks to be made at random intervals by key employees, to ensure that the policy was being followed. Procedures were also established to deal with emergencies and evacuation. Employees were briefed on procedures to follow, using checklists to aid compliance, to ensure that no servers were left unsecured. Security policy now mandates tight password control, so that privileged access is not granted without a specific business need.

Physical security encompasses several areas, many relative to safety. We found that many other corporate policies overlapped with our physical security requirements, so that we only needed to address a few key areas, such as password control, computer room access, and login discipline.

Servers and Services

As mentioned before, there are five servers used to provide Domain Name Service, e-mail, news, and web hosting services to the customers of the ISP. All of these are running some version of the Microsoft Windows operating system, which is a favorite target of hackers and virus writers. Although there are five servers, four are in two Microsoft Cluster Server clusters, and only one is a standalone server. The clustered servers were addressed as a cluster and the standalone server individually. Although steps were taken to decrease exposure and tighten security on the servers at this point in time, IT security is an evolutionary field, with new exploits, viruses, definitions, and patches released almost daily. Good procedures to keep servers up to date with the latest security patches and to check for known vulnerabilities are essential. The Microsoft Baseline Security Analyzer, available from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp, was implemented to be run on an ongoing basis to check for needed service packs or hotfixes. An addition to the security policy was also made to provide for periodic checks by a security consultant, to identify issues that may otherwise be overlooked.

Newsgroup Server

The newsgroup server, NT1, is the single standalone server. This server was found to be running Windows NT Server 4.0, Service Pack 5, with a few post-SP5 hotfixes. The security tools used to assess the server highlighted quite a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

few vulnerabilities that should be addressed immediately, as it's just a matter of time before the server would be compromised. The recommendation is to upgrade this server to Windows 2000 or Windows 2003 as soon as practicable, to take advantage of the increased security inherent in those releases. It is planned to upgrade in the near future, but I was asked to heighten security of this server in its current configuration for the interim. The first order of business was to upgrade to the latest Microsoft Service Pack, which is Service Pack 6a. Although it can be considered less secure than other means, Microsoft's Windows Update utility can be quite handy for a quick update. Since our aim was to get the most "bang for the buck", and increase security quickly, but without sacrificing functionality, I used Windows Update to quickly address the missing Service Packs and hotfixes. This server has no role other than to provide access to newsgroups for the ISP customers, so all non-essential services were stopped and disabled. With a little Internet research, Microsoft's "Microsoft Security Tool Kit: Securing and Existing NT 4.0 System" was located at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/nt4exist.asp. This document also contains a link to Microsoft's "Microsoft Windows NT Server 4.0 Security Checklist", available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/nt4svrcl.asp. These were utilized to further secure the operating system.

As Windows NT Server 4.0 does not contain a native newsgroup server software package, the customer was using a third party application. For performance and security reasons, we implemented access controls on the newsgroup server software, so that access is limited to customers of the ISP. This prevents access to the server from the open Internet, and limits the possibility that it could be compromised due to vulnerabilities in the application software. This also has the side benefit of keeping bandwidth usage to those people who are paying for the service, rather than allowing access by anyone.

Once these measures had been taken, a check was made using the Microsoft Baseline Security Analyzer and the Center for Internet Security's (CIS) benchmarking and scoring tools, available from www.cisecurity.org, were run as an additional check. Although these tools work great, one must still analyze their output to eliminate false positives and incorrect entries in the reports. One server and its applications can be quite different from another, so certain recommended security measures may not be applicable to a particular server. Careful examination of the recommendations from these tools is warranted, or else you could easily end up with service disruptions. As the role of this server was limited to one well-defined application, the reports were quite clean.

Web/DNS Cluster

The web hosting and DNS services are provided using a Microsoft Cluster, running on Windows NT Server 4.0, Enterprise Edition, Service Pack 6a. No

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Service Pack updates were available, but Windows Update was once again used to obtain any required hotfixes. The assessment tools used highlighted quite a few vulnerabilities, as the web server software in use was Microsoft's own Internet Information Server (IIS) 3.0. IIS is the single most targeted web server software on the Internet, as it is also the most widely available. The same Microsoft TechNet document used to begin securing the newsgroup server was as a starting point for the two cluster nodes, but additional information was needed, due to the presence of IIS. Once again, on both nodes, all non-essential services were stopped and disabled. This often results in a trial-and-error process to make sure all of your functionality works as needed. If something stops working, you can turn services back on until you figure out what service it is dependant on. It was immediately apparent that IIS needed to be upgraded to a later version. Once again, the final recommendation is to upgrade these servers to either Windows 2000 or Windows 2003, but once again that was not feasible at this time. The latest version of IIS available for Windows NT is IIS 4.0, provided in the Windows NT Option Pack. Installation of the Option Pack is a bit more involved now than when it was first released, as it was written to install with Service Pack 4. Additional research on the Internet was required to keep from breaking existing cluster functionality, and once again Microsoft TechNet came to the rescue. The Microsoft Knowledge Base Article 191138, "How to Install the Windows NT Option Pack on Microsoft Cluster Server", and article 241573, "How to Install IIS 4.0 onto a Single Node of MSCS 1.0" were invaluable in performing the IIS upgrade. This upgrade in itself solved a few IIS vulnerabilities, but still left a lot to be desired. I then followed recommendations in the SANS course book, "Securing Windows: Securing Internet Information Server" to further secure the IIS instance. As this cluster is used to host web pages for the ISP's customers, ftp is also enabled. Anonymous ftp was disabled, and permissions were set such that each user could only access their content. Another Microsoft document, Knowledge Base article 201771, "How to Set UP an FTP Site So That Users Log Onto Their Folders" was used to check the existing configuration for errors. The other IIS services, SMTP and NNTP, were disabled, as they were not utilized in this cluster. As Microsoft received quite a bit of negative press concerning the insecurity of its IIS product family, they have made a lot of information available to assist in securing these products. Microsoft now provides a couple of tools to assist in securing IIS, the IIS Lockdown Tool and URLScan. The IIS Lockdown Tool was recommended by the Microsoft Baseline Security Analyzer, as it had never been run on these servers. The IIS Lockdown Tool is designed to assist you in making changes to the IIS configuration to fix common security vulnerabilities. It was downloaded and executed, and tests were initiated to be sure that it had not broken any existing functionality. URLScan was also installed, as per Microsoft Knowledge Base article 307608, "INFO: Using URLScan on IIS". URLScan provides filtering to all URLs received by the IIS web server, and filters out any which fit certain signatures that indicate malicious intent. An example is the common directory traversal attacks, where a URL is formed to use relative pathing to gain access to files or directories not intended to be published. As with any security measure, care must be taken with URLScan,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

or you may break existing functionality. This is especially true if using any type of active content or CGI applications. One of the ISP customers was hosting a message board, which was initially broken by URLScan. Careful tweaking of the URLScan filters was necessary to ensure that functionality was balanced with security.

This cluster also provides DNS for the ISP customers. DNS servers are often targets of attacks, as a compromised DNS server can be used to redirect traffic to anywhere an attacker may wish. Another common tactic is to attempt a zone transfer from a DNS server, for reconnaissance purposes. This is where an attacker would pretend to be another DNS server, and request all of the DNS server's zone, or domain, information. This way they could find out what hosts are in use on a particular network, and what IP addresses are in use, even if you are using other means to try and block mapping and scanning. Once again, we see where a defense-in-depth strategy pays off, as limiting zone transfers to specified servers augments the security already implemented within the network. In this case, there were no authorized DNS servers outside the local network for the zones that this cluster handled, so zone transfers could be completely prohibited. Microsoft's implementation of DNS is also vulnerable to a DNS Spoofing attack. This vulnerability can be removed via a registry edit, found on the Internet at http://www.nthelp.com/50/dns_spoofing.htm. This web document provides detailed information on the indications of a DNS Spoofing attack on a Windows NT DNS server, as well as information on how to fix it. This procedure was also followed on both nodes of the cluster, to remove exposure to this vulnerability.

As with the newsgroup server, the Microsoft Baseline Security Analyzer was run after the above steps were taken, to highlight any hotfixes that may have been missed. A few things will almost always show up, as there will invariably be services or software that is not installed, and so there could be missing registry entries that the tools are looking for. The CIS tools for Windows NT 4.0 were also run, and once again, the reports were relatively clean. A plan was put in place to upgrade these servers to Windows 2000 as soon as practicable, as a further increase in security.

E-mail Cluster

The e-mail cluster was found to be running Windows 2000 Advance Server, Service Pack 1. This was an improvement over the newsgroup server and web/DNS cluster, as Windows 2000 has enhanced security features over Windows NT Server 4.0. But there are always improvements to be made. The first step was once again to make sure that any non-essential services were stopped and disabled. Once again, Windows Update was used to analyze and update both nodes to the latest Service Pack and hotfixes. The steps outlined in the SANS Step By Step guide, "Securing Windows 2000 Step By Step" were followed on both nodes, with testing done along the way to ensure that nothing

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

was broken by the steps taken. As these servers are providing e-mail services via a third party mail server application, quite a few Windows vulnerabilities were quickly avoided by disabling the default IIS instance installed with Windows 2000. And, since the role of these servers was limited to the mail server application, many of the sections of the Step By Step guide were not applicable to this cluster, making the job somewhat less tedious. Windows 2000 also includes a snap-in for the Microsoft Management Console (MMC) which reduces the need for registry editing that was prevalent in securing previous versions of Microsoft operating systems.

Unlike several well-known and popular mail transfer agents (MTAs), the mail server software being used had no reported vulnerabilities. It is very important, however, to avoid having a mail server act as an open relay. Not only do you waste bandwidth and possibly incur performance problems, you will most certainly be placed on relay blacklists, and other domains will begin to reject mail from your mail server. This could easily result in lost revenue for an ISP, as customers will not tolerate unreliable mail delivery. Using features present in the mail server software, I was able to limit relaying (delivery of mail to non-local domains) to those users who are authorized by the ISP to send mail through this mail server. And although Unsolicited Bulk E-mail (UBE), or SPAM, is not strictly a security issue, Relay Blacklists were implemented to limit the amount of SPAM received on the mail server. So the customer now has a mail server that will not allow open relaying, and will not accept mail from any mail server that does. These measures, along with the fortunate circumstance of using an MTA with no known vulnerabilities, reduced the workload of the server, saved bandwidth, increased user satisfaction, and reduced security exposure. Viruses are often spread through open relays and SPAM, and these measure reduced exposure significantly.

As previously outlined with the newsgroup server and web/DNS cluster, the Microsoft Baseline Security Analyzer was used after measures were taken to secure these servers, and the CIS scoring tool for Windows 2000 was run. Much less work was involved with this cluster than the other two environments, and there were less “false positives” to investigate from the output of the assessment tools.

Post-Implementation Assessment

Following the initial assessment, recommendations, and implementation of those recommendations, another assessment was in order. The same tools were used as in the initial assessment, and the scope remained the same. IT Security can be difficult to quantify, and therefore expenses in this realm can be difficult to justify. The reports generated by the tools exhibited significant decreases in exposure to known vulnerabilities. For example, nmap was easily able to fingerprint the operating systems of each server in the initial assessment, but

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

was unable to do so with any degree of certainty in the final checks. Although the tools may show a decrease in exposure and by extension an increase in security level, it can still be quite difficult to quantify the impact of the measures taken to someone not familiar with IT security. But, in this case, shortly after these measures were taken to increase the security level throughout this environment, the W32.Blaster, also called Lovsan, worm ran rampant through the Internet, followed closely by several variants. Although there were media reports of widespread effects on well known companies, none of these five servers were affected. The simple fact that no service disruptions were experienced, when there were widespread reports of the havoc being wreaked on the Internet by exploits to Microsoft's DCOM, gave credibility to all the efforts and expense required to attain the current level of security. And, this also emphasized the need to continue efforts to increase security awareness, and security levels, on an ongoing basis. Plans are already in place to address many items left undone by this "first pass". The need for security is evident, and the benefits of sound policies and procedures have been proven. IT security is evolutionary, and a sound defense-in-depth strategy will serve well as a basis for continued security efforts.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

"Scanning Safety", whitepaper available at http://www.foundstone.com/resources/whitepapers/wp_scanningsafety.pdf

"SANS Security Essentials with CISSP CBK, Volume One" by Eric Cole, Jason Fossen, Stephen Northcutt, and Hal Pomeranz

"SANS Security Essentials with CISSP CBK, Volume Two" by Eric Cole, Jason Fossen, Stephen Northcutt, and Hal Pomeranz

RFC 792 http://www.faqs.org/rfcs/rfc792.html

"ICMP Usage in Scanning, The Complete Know-How", whitepaper by Ofir Arkin http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

"Microsoft Security Tool Kit: Securing and Existing NT 4.0 System" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/nt4exist.asp.

"Microsoft Windows NT Server 4.0 Security Checklist" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/nt4svrcl.asp

Microsoft Knowledge Base Article 191138, "How to Install the Windows NT Option Pack on Microsoft Cluster Server"

Microsoft Knowledge Base Article 241573, "How to Install IIS 4.0 onto a Single Node of MSCS 1.0"

Microsoft Knowledge Base Article 201771, "How to Set UP an FTP Site So That Users Log Onto Their Folders"

"Securing Internet Information Server", SANS Institute

Microsoft Knowledge Base article 307608, "INFO: Using URLScan on IIS"

http://www.nthelp.com/50/dns_spoofing.htm

"Securing Windows 2000 Step By Step", SANS Institute

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 30th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Milan 2015	Milan, IT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
FOR578 Cyber Threat Intelligence	OnlineVAUS	Aug 31, 2015 - Sep 04, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced