Global Information Assurance Certification Paper

GIAC Security Audit Essentials
Security Essentials: Patch Management as a Necessary Part of Defense In Depth
A Case Study

GIAC IT Security Audit Essentials
GSAE – Practical Assignment
V1.1 (May 8, 2002)
Assignment 1 Option 2
Assignment 2

Kay A. Cornwell
SANS 1st Women's Only
New Orleans, LA
September 2002
Submitted Feb 20, 2003

Abstract
Assignment 1 Option 2

Security is becoming the watchword in Government agencies leaving many in catch up mode. For offices and divisions within agencies, policies and procedures may be handed down from above. Usually these policies are being implemented slowly, leaving holes that may need to be closed by the creation of local policies and procedures. In a research and university type of environment policy is often developed from community consensus which may or may not cover all local needs. The goals of the agency may lead to the implementation of technology that may not always fit perfectly with the Institutes, Divisions and Offices below. While it may seem to the security personnel of a small institute or office that there is not much to do except react, close examination reveals that implementing a local security plan strengthens the security posture of the Institute while also contributing to the Agency's overall security. SANS courses push the concept of attending to "low hanging fruit" first and concentrating on its Top 20 list of critical vulnerabilities. This case study will look at ways in which the Institute of Basic Cellular Research is applying patch management and vulnerability analysis tools to complete a defense in depth process as a part of a larger organization.

TABLE OF CONTENTS

Case Study Environment – Assignment 1, Option 2

The Institute for Basic Cellular Research (IBCR) is a component of the Federal Institutes of Health Services (FIHS) which is a branch of the Federal Government's Health Services Agency. The Institute for Basic Cellular Research (IBCR) supports basic biomedical research by funding work that focuses on learning more about the basic cellular functions that lead to advanced understanding of fundamental life processes and increases knowledge of the mechanisms involved in disease. The IBCR has used personal computing technology along with client server based networking for approximately 14 years. The Federal Institutes of Health Services (FIHS) prides itself on its university and research type atmosphere which has resulted in an open computing environment. Communications and collaboration were the guiding principles for connectivity. In the IBCR there has been little thought to security beyond passwords and basic access control lists. In 2003 security has become the watch word. The Federal Government is a favorite target for hacking and for many agencies a 180 degree shift in security posture has been mandatory. As a new security professional the challenge of learning and applying security procedures in an environment that has traditionally placed security concerns on the back burner can seem insurmountable. Armed with knowledge provided by SANS courses; creating checklists, how to write policy, auditing procedures, vulnerability scanning, risk assessments, firewalls, and more the question often becomes where to start. Add policy being pushed down from the parent agency and internet attacks that strike without warning, crippling resources and it becomes difficult to focus limited efforts effectively.

IT Infrastructure

Relationship with FIHS

While assessing the security needs of the institute one must first look at where the institute fits within the entire Federal Institutes of Health Services (FIHS) and its security program (see Figure 1). The IBCR's IT infrastructure is tied closely with the Federal Institutes of Health Services' (FIHS) IT infrastructure. The FIHS' Information Technology Center (ITC) provides the network cabling infrastructure for the institute, they also provide the border routers, switches, firewalls and intrusion detection systems along with the skill set needed to monitor and maintain them. The IBCR has found it beneficial to buy into many of the solutions the ITC has provided for the FIHS campus WAN which includes 300 LANs supporting more than 20,000 PCs, Macs, and UNIX workstations. The FIHS has traditionally operated as close to an academic and research atmosphere as possible. Access and security, while following government guidelines, have been as open as if FIHS were a major university campus.

New security mandates from FIHS' parent agency and the increase in attacks on the FIHS network has led the ITC, working in cooperation with all FIHS components, to provide overall security services rather than assisting each

component separately. Policy and procedures put in place over the last two years have followed federal law or are best practices recommended by NIST,

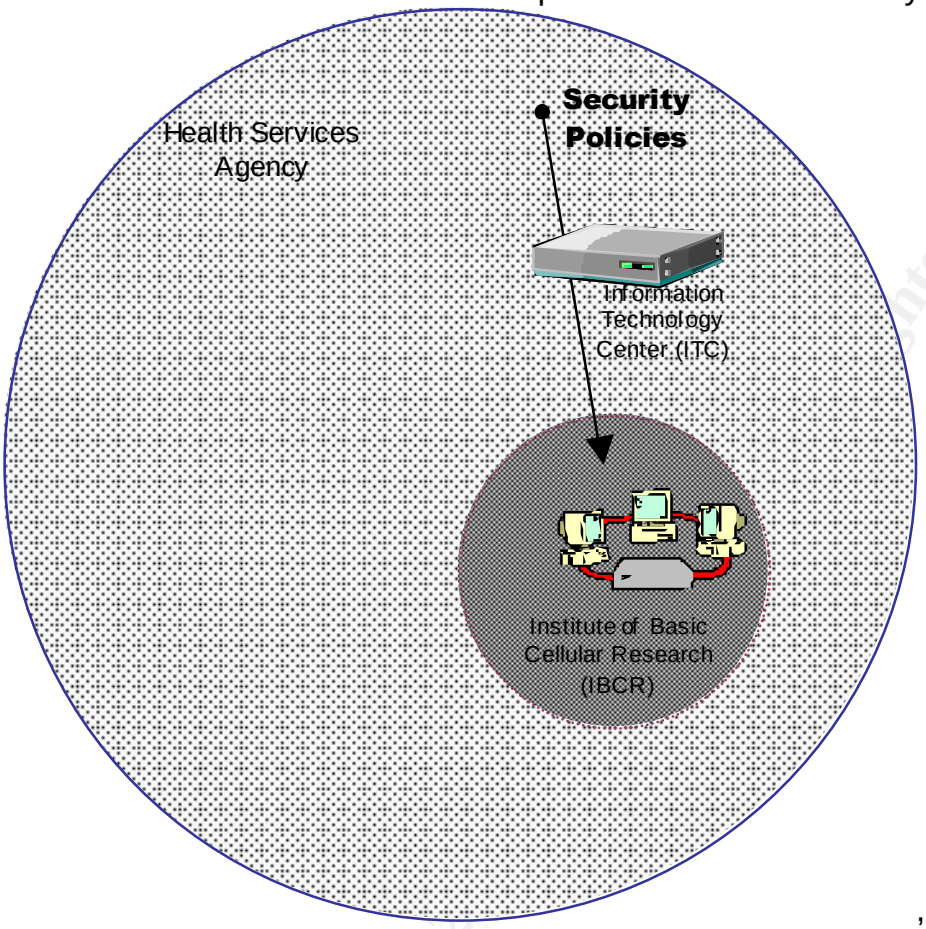


Figure 1. Security Program and IT Infrastructure Relationships

the National Institute of Standards and Technology and SANS. Due to the diverse FIHS community, policies are created via community consensus which has slowed the policy process and has not allowed all best practices to be implemented quickly. For example, FIHS was hit by the MS-SQL worm (SANS) released on January 25, 2003. If the deny all perimeter firewall policy had been implemented perhaps the amount of traffic generated by the worm might have been less. The best practice of a "deny all" firewall policy is scheduled to be implemented within the next two weeks. This policy by itself would not have prevented infection as will be discussed further on in this case study.

The institute's relationship with FIHS has lead to an economy of scale and savings. The IBCR pays a minimal service fee into a general fund to benefit from the perimeter firewall and IDS systems. The IBCR is free to install its own equipment to achieve an even greater defense in depth. The institute has joined the ITC's effort to place firewall and IDS products at all the FIHS component's perimeters. The ITC has provided the specifications for and will integrate the

equipment into a new gigabit router and switch upgrade which is currently ongoing. They will monitor the IDS and provide assistance with firewall rule sets and the creation of a DMZ for internet facing web services. It is necessary to discuss the IBCR's relationship with FIHS and its information technology infrastructure when considering a risk assessment as all packets that reach the IBCR network first travel through the FIHS network. The IBCR's risks and mitigation tactics depend largely on how good a job FIHS is doing on assessing and mitigating risk for the FIHS network as a whole. Due to FIHS' implementation of agency wide services the IBCR does not need to maintain or protect services such as DNS, WINS, and Email servers.

FIHS Infrastructure

A quick look at the FIHS infrastructure shows that the ITC has been working hard to protect the agency infrastructure by utilizing defense in depth. The FIHS' interface to the internet is redundant, as is the Gigabit Ethernet backbone allowing for automatic failover between border filtering routers and firewalls. The initial firewall policy had been to allow all as default. This has proved to be un-workable as the agency has been the target of numerous attacks. As consensus between FIHS components has been reached policy has been applied to close ports that are known as common vulnerabilities. For example, to help alleviate HTTP attacks and web defacements all components provided lists of IP addresses of web servers that needed to be open to the public. The firewall only passes port 80 traffic to these specified machines. Only the institute Information System Security Officer (ISSO) is allowed to modify their institute's list. This has lead to a marked decline in web compromises by simply limiting the number of web servers available from outside the firewall. Recent policy has been enacted to do the same for FTP servers and NetBIOS services. Policy to address Internet Relay Chat and SQL access is scheduled to be implemented soon. If the SQL port policy had been in place it might have limited the initial machines infected to only public facing machines with authorized SQL access. The chances are some of those machines were not patched and would have passed the infection to the internal FIHS network proving that firewall policy is only as good as the weakest link on the network.

During the last quarter of 2002 the FIHS has experienced heavy activity at the firewall. A change in security stance has been decided upon so that the policy of allowing all traffic will be changed to deny all except that which is expressly allowed. The need for this policy change was again made painfully aware on January 25 during the attack of the MS-SQL worm. This policy is currently in the final approval stage and should be implemented before this paper is completed. There is an IDS sensor behind the FIHS firewall. The sensor identifies attacks that may have circumvented the firewall. At this point an automatic block feature has been placed. In the event of an anomaly the IDS will automatically block traffic between the attacker and victim to prevent damage to FIHS resources or to prevent liability to FIHS in the event internal resources are compromised and used to stage attacks on other organizations. Unfortunately,

the IDS sensors did not recognize the MS-SQL worm as an attack. IDS' are good at recognizing known signature attacks but only some types are able to handle new, undefined attacks. In the case of the MS-SQL worm it managed to easily pass through defensive layers.

IBCR Infrastructure

The IBCR maintains its LAN in a single location spread over 2 floors. The IBCR LAN consists of a Cisco router and two gigabit Cisco switches. Two Lucent VPN Firewall Brick 1000s will be installed to create a DMZ for public services and a blade IDS will be implemented. The IBCR maintains 40+ Windows NT/2000 servers. Migration to the FIHS Active Directory service was completed in early January. Its full capabilities will not be available until the domain controllers are upgraded from NT 4.0. IBCR users were moved to its own Organizational Unit while a resource domain will be maintained by IBCR network staff. All servers are running McAfee anti-virus in the background and are monitored from McAfee's E-Policy Orchestrator[1] management console.

The Cisco gigabit switch upgrade and implementation of the Lucent firewalls will allow the IBCR to deploy a DMZ for publicly accessible services. The new IBCR firewalls will serve as components in a defense in depth strategy extending from the FIHS perimeter and will also serve to protect the institute from attack from within the FIHS network. The institute's perimeter has been a weak area and many institutes are starting to address the need for firewalls between FIHS components. While the ITC will maintain the new firewalls, there is a web-based interface available to the ISSO to audit logs and to change rule sets. If the ISSO does not feel comfortable with changing rule sets, the ITC will assist. An initial rule set will be discussed and implemented upon installation of the firewalls. The ISSO will be holding consulting meetings with the ITC to ensure the firewalls mirror FIHS firewall rules and to identify specific needs unique to the IBCR.

The ITC will maintain and monitor the IDS installed with the new switches. Anomalies will be handled by the same procedures as those used for the perimeter IDS. Anomalies, along with their log entries and a description of the suspected attack are emailed to the ISSO. The ISSO determines if a breach has been successful. The ISSO may call upon the ITC incident response team for assistance if needed or may investigate herself. The ISSO must respond within a reasonable amount of time to indicate the problem has been resolved. If the attack was successful details on how it occurred, what was done to clean up and what procedures where put in place to prevent a repeat are sent to the ITC incident response team.

The remainder of the IBCR network consists of approximately 170 Dell Optiplex Win2K desktop machines. Desktops are standardized and staff is not

[1] For more information on McAfee E-Policy Orchestrator see http://www.mcafeeb2b.com/products/epolicy/default.asp

permitted to download or install software, although there is no facility to prevent this. The standard desktop contains the Microsoft Office XP suite, a browser, FTP client, and custom applications written by the IBCR database group to access grant information and financial systems. The desktop also provides access to FIHS tools providing access to agency-wide grant processing software. All desktops have a centrally managed Antivirus program from McAfee that scans in the background during all web downloads, when opening email and attachments, inserting a floppy disk and on boot up. All machines are virus scanned weekly, upgrades and dat updates are managed from the central management console, E-Policy Orchestrator. Desktop machines are a concern as they are plentiful and need to be watched for vulnerabilities and be updated just as servers. Risk is mitigated by trying to ensure that only necessary user services are installed. Some type of automated vulnerability scanner is really necessary here as hand compliance testing is out of the question. The FIHS runs its vulnerability scanner, Sara[2] Scan on all institute machines monthly. Since these scans are covering the entire agency they usually are limited in scope. The ISSO feels these are too limited and do not occur often enough to adequately protect the institute but in defense, Sara Scan has found important vulnerabilities that did need to be addressed. The IBCR ISSO feels that it is necessary to run scans that are tailored to the IBCR environment as part of a comprehensive defense in depth strategy.

Windows 2000 laptops are available for permanent loan for upper management and a loaner laptop pool is available for staff use when they travel; need to temporarily work at home, or for training. The ITC maintains a remote dial-up service for all FIHS staff for travel and telework. The IBCR IT staff configures all laptops to use this service, requiring all those needing remote access to apply for a remote account. The business need for remote access is reviewed yearly. This service provides the teleworker with an FIHS IP address and places them behind the FIHS firewall granting access to the Institute's services. This service eliminates the need for the IBCR to support modems on site. The FIHS has been piloting a VPN solution to secure high speed access to the FIHS network. When accessing the FIHS VPN, staff connects to a remote access DMZ with a firewall, intrusion detection and email virus detection and removal. As with the remote dial-up service, management must approve staff's need for an account. Once the deny all policy at the firewall is put in place these services will be the only authorized way to remotely access the FIHS network. Remote access means that laptops need to be scanned for vulnerabilities and patched regularly to prevent them from becoming a source of attack.

The Patch Management Problem

After discussing the IT infrastructure what seems to be the problem? Defense in depth, firewalls, and intrusion detection services should provide fairly comprehensive protections for institute resources. The FIHS has been slowly

[2] For more information on Sara (Security Auditor's Research Assistant) see http://www-arc.com/sara/

implementing policy that will take it from an open environment to a more secure system based on best practices. Since the FIHS has responsibility for the network infrastructure and the individual institutes control their own computing environments, the FIHS strategy has been to secure the outside perimeter by closing the most abused ports and enforcing a policy of allowing only traffic to authorized servers. These servers are scanned weekly by a commercial vulnerability scanner that incorporates the SANS Top 20 Vulnerabilities (SANS). The FIHS will be implementing a closed firewall environment by the time this paper is complete. The FIHS has realized great success over the last year as HTTP, FTP, NetBIOS and other vulnerable ports have been closed and access limited to only authorized services. Moving to a "deny all except that which is explicitly allowed" security stance will certainly increase the FIHS' ability to fend off attacks. But as the MS-SQL Slammer Worm demonstrated, one incorrectly configured outside facing server could nullify all the work done at the perimeter firewall.

The IBCR, in collaboration with the ITC is installing firewalls at the IBCR perimeter, they will mirror the outer perimeter rules and an IBCR IDS will alert of any attacks from other institutes. In the event something like the MS-SQL worm did infect another institute's hosts the IBCR firewall would limit the risks of the IBCR becoming infected, right? Well, possibly. It depends on how the IBCR trusts the remainder of the FIHS, the IBCR business needs, what ports must be left open, the vulnerability of the IBCR's internet facing servers and of course the possibility of insider threats.

This is where this case study comes in or the answer to the question "What is the problem?" The FIHS firewall policies cannot entirely protect institute resources. A defense in depth process must be used with the IBCR being responsible for maintaining a portion of those defenses. Perimeter protection has been covered, along with intrusion detection but the hosts on the IBCR network need to be vulnerability free. The IBCR currently responds to the weekly vulnerability scan of its outside facing web servers, mitigating any problems identified by patching servers using Microsoft's Windows Update[3] and St. Bernard's Update Expert.[4] Due to the numbers of inside facing machines in the agency, the ITC scans of desktops and servers protected by the perimeter firewall only happen on a monthly basis and the scan is limited in what it identifies. The amount of time between scans and the resources needed to fix vulnerabilities leave the IBCR open to exploits if machines are not patched in a timely manner. This became evident when the IBCR was hit by the MS-SQL Server Worm in January. Many variables contributed to the state of institute vulnerabilities but weaknesses that need to be quickly repaired were clearly

[3] For more information on Microsoft's Window Update see http://v4.windowsupdate.microsoft.com/en/default.asp

[4] For information on St. Bernard's Update Expert see http://www.stbernard.com/products/updateexpert/products_updateexpert.asp.

evident. The weekly SARA scan did not scan for the missing patches which left SQL open to the Slammer exploit; therefore it could not have prevented such an attack. Since the scan is an FIHS level scan it is very difficult to cover the possible range of machinery and services used by the entire agency in a comprehensive manner.

The "deny all" firewall policy had not been implemented yet, leaving SQL ports open for servers that did not need to be open to the internet. As long as the firewall rules are open, all internal machines are vulnerable and need to be protected at the host level via vulnerability identification and mitigation. This specific problem will be repaired in short order but defense in depth forces one to look at the possibility of firewall failure. Redundant systems help limit this possibility but what if a new exploit could find its way around the firewall? Internally to the IBCR policy needs to be put in place to assist the ISSO with the responsibility for keeping up with patches. Currently patch management is more than a one person job with 40 plus servers in place and multiple staff installing servers and services. While the IBCR has purchased St. Bernard's Update Expert and it has proven itself useful, it alone cannot stand as the entire solution. Update Expert is limited to the maintenance of Microsoft products and it requires some quality time to learn how to use it effectively. For example, efforts should be pointed to spending some time learning how to identify and tag required updates to help in a global install. Operators will want to become familiar with the management and the conformance reporting functions to assist in easily pinpointing machines that need remediation. St. Bernard claims that it had everything in place to assist a system administrator in having machines patched to prevent the MS-SQL slammer worm and they are right. (St. Bernard) This demonstrates an important point of patch management. Having the tools themselves does not mean the network is protected. A process must be implemented guiding their timely and continuous use.

The IBCR ISSO subscribes to the many vulnerability notification lists and attempts to track important patches but obviously there is much room for improvement. The ISSO was not aware of all the servers that had the vulnerable software, new servers running SQL had gone up without the ISSO being notified making it difficult to know to even look for them. A reporting mechanism needs to be put in place to ensure that all machines are documented with running services. The ISSO has suggested that the reporting and documentation of all new servers be required in a Server Security policy written for SANS GISO Certification (Cornwell 42). This policy has been presented to IT Management for approval. Besides knowing what systems are on-line and knowing what to monitor for patches, one of the biggest obstacles to proper patch management in the institute has been the fact that it's very difficult to negotiate maintenance windows to allow for IT staff to test and deploy patches. IT management has surveyed staff on what weekends would be acceptable for a maintenance window and invariably staff insist they have to work every weekend. It always seems to be a critical time for at least one office and it has been extremely

difficult to get the time to take servers down for regular hardware maintenance much less patches. Downtime over the last year has been emergency down time as a result of imminent hardware failure. This is one reason that the SQL Service Pack 2 had not been deployed on one outside facing server that was hit by the Slammer worm. As a part of the ISSO's patch management process this machine had had all OS patches installed and evaluation revealed that the remaining work needed was the SQL service updated. This happened to be on January 22, 2003. Unfortunately at this particular time the machine could not suffer down time as it was the one specific week in the quarter that the machine was critical. It was decided that patching needed to wait until the critical process was over. Unfortunately, good intentions did not prevent the machine from becoming a victim of the MS-SQL worm. It is difficult to anticipate when an exploit might happen; therefore a conscious effort to patch as closely as possible to vulnerability notification must be made.

The ISSO realizes that a system needs to be put in place to assist in patch management, vulnerability scanning and mitigation. The IBCR environment has many of the same difficulties everyone suffers from. Competing needs for limited resources, functionality and business needs overshadowing security needs and it is difficult for IT management to convince business process owners that maintenance time is necessary. There is a lack of freely available tools to assist in making the job easier with helping the security professional maximize their limited time. While SANS attempts to point out the best in free tools to assist in automating the patch and vulnerability investigation process often commercial products are necessary. This case study was first going to attempt to create a patch process but upon research a GSEC practical paper that described an excellent system already existed. This case study instead will look into the application of the system proposed by Judy Klaren in her practical entitled "Managing Vulnerability Assessment and Patch Installations" (Klaren) and expand upon it by adding information about the implementation of vulnerability scanning and mitigation tools purchased by the IBCR to assist in automating the process. This case study will also briefly mention the new federal patch management system that many federal agencies are going to be required to use.

The Vulnerability Assessment and Patch Life Cycle

The Vulnerability Assessment and Patch Life Cycle is a five step process (Klaren 2).

1. Define your corporate policy on Vulnerability Assessment and Patch Management. This policy should include what the policy is, why you need it, the scope, and how and by whom it will be completed.
2. Inventory your systems. Know exactly what you're running so you know exactly what to worry about.
3. Manage the flow of information. Determine which information resources help you focus exclusively on the vulnerabilities that affect your systems.

4. Assess the information. Evaluate the actual risk to your organization's systems security.
5. Plan for response. Develop standard procedures to translate information into action.

Step 1 – Define a Policy

The first step in the Vulnerability Assessment and Patch Life Cycle is defining a corporate policy as it lays the ground rules for the process.

> "Information security policy establishes the charter for the security program and the rules that govern security within the organization. It takes on a very important role in the security program in general and network and Internet security in particular. It provides a key link back to the organization's goals. Information security policy is [t]he foundation of any security infrastructure. It can be tricky to develop and keep up to date. … A formal security policy clarifies higher-level organizational objectives. It thus serves as a guideline for employees' routine, day-to-day, security-related activities." (McBride, Patilla, Robinson and Thermos).

The important issue for a vulnerability and patch management policy is its ability to assist in creating procedures for the day to day security activities required. It should, because it "clarifies higher-level organizational objectives", i.e. to protect organizational resources via identifying any vulnerabilities and then mitigating them thus preventing exploits, provide the resources required for the security staff to fulfill the objectives. These resources would normally be the time required to acquire and test patch implementation, the maintenance time required to actually install the patch with some extra time for unforeseen problems, the time to update any configuration documentation to indicate the change in configuration and the time to run vulnerability scans to ensure compliance or to discover new vulnerabilities patches may introduce. It should also allow the organization the financial resources to purchase the tools that will help security staff do the job efficiently and in a timely manner.

Remembering from SANS courses the basic outline for policy development, the ISSO proposes a draft policy to present to IT management:

Vulnerability and Patch Management Policy

1.0 Purpose

The purpose of this policy is to establish standards for the timely and continuous vulnerability scanning and patch management of equipment that is owned and operated by the Institute of Basic Cellular Research (IBCR). Effective implementation of this policy will minimize unauthorized access to Institute of Basic Cellular Research (IBCR) proprietary information and technology.

2.0 Related Documents

Place links to *Server Security Policy*, *Server Configuration Guide*, *Exception Policy*, and *Desktop and Laptop Configuration Guide* here.

3.0 Background

The IBCR IT branch has seen the network grow from 5 servers to 40+ servers in use today. The network administration staff had responsibility for performing all help desk activities while maintaining the network until approximately three years ago. Over the last three years network administration staff have been training contractors in help desk procedure and installing new applications and servers. Network staff has not had adequate time to document installation procedures as new applications and services have been continuously added. As the need for services has grown other IT staff has often become involved in installing servers and adding services, complicating the network documentation process. With the federal government's attention turning to increased security procedures the IBCR has decided to officially institute an Information System Security Officer (ISSO) position. The ISSO is attempting to apply best practices to change the security stance of the IBCR to a more proactive position. One important security practice is the ongoing process of determining system vulnerabilities and keeping up with system and application patches. Only through the application of a formal process and management support for the needed resources can the ISSO ensure that the appropriate security is in place to protect the institute's information resources.

The IBCR is also responsible for responding to weekly, monthly and semi-annual vulnerability scans instituted by the ITC. Because these scans are limited to a small subset of institute equipment or occur at intervals that are not considered timely due to the current flood of vulnerabilities reported in the popular operating systems and applications used by the IBCR, the ISSO is instituting a more comprehensive vulnerability scanning process that will occur more often and scan all the institute's equipment on a more timely schedule as required to keep up with the internet community.

4.0 Scope

This policy applies to all servers, desktops and laptop equipment owned and operated by the Institute of Basic Cellular Research whether located on the Institute of Basic Cellular Research internal network domain or located at another facility or in IBCR staff's home.

5.0 Policy

5.1 Ownership and Responsibilities

All internal servers, desktops and laptops deployed at the Institute of Basic Cellular Research (IBCR) are owned by the IT Operations Section (ITOS) of the IBCR's Information Resource Management Branch. The network administration group is responsible for all server, desktop and laptop installation, administration and compliance. The ISSO is responsible for development of security guidelines,

auditing, scanning and patching of servers, desktops and laptops and compliance testing.

5.2 Action

A Chief of ITOS approved vulnerability scanning and patch management procedure must be established and maintained by the Information Systems Security Officer (ISSO). A mitigation procedure and timeline based on the IBCR business needs will be approved by the Chief of ITOS and the CIO. The network administration group will assist the ISSO in implementing patches and monitoring configuration compliance. There should be no exceptions to vulnerability scanning and patch management. Exceptions in mitigation procedures and timelines must be approved by the Chief of ITOS. The ISSO will establish a process for changing and updating the patch management and mitigation procedure. The process will include reviews and approval by the Chief of ITOS.

- All Servers must be registered in the IBCR asset management system along with informing the ISSO of deployment of new servers. See the Server Security Policy.
- All Desktops must be registered in the IBCR asset management system along with informing the ISSO of deployment of new desktops. See the Desktop Security Policy.
- All Laptops must be registered in the IBCR asset management system. Help desk staff are responsible for the loan paperwork for all permanent and temporary loans of institute laptops. Help Desk Staff will assist the ISSO in a quarterly vulnerability scanning process for all laptops. The help desk staff is also responsible for following the Laptop Checkout Guide (see Laptop Checkout Procedures) which requires the updating of patches before any laptop is let out on property pass.

5.2.1 Vulnerability Scanning Guidelines

- IBCR purchased vulnerability scanning software will be the main vulnerability scanning process for all Windows equipment owned and operated by the IBCR or hooked to the IBCR network.
- All Servers will be scanned weekly and vulnerabilities reported to the ISSO and Chief of ITOS.
- Laptops will be updated by hand during the laptop checkout procedure. Otherwise all laptops will be scanned quarterly with vulnerability scanning software.
- Desktops will be scanned weekly until the initial remediation is complete. Once all have been remediated an appropriate time period will be chosen that will be no more than once a week and no less than once a month.
- All scanning will occur from the vulnerability scanning software console. Access to the service will be protected through NT/Windows Domain Access control methods. Access will be limited to IT staff with direct responsibility for vulnerability discovery. Scanning results will be saved in

a secured network location with access limited to the ISSO, Chief of ITOS and network staff sharing vulnerability scanning responsibility.

- Vulnerabilities identified will be repaired via the process described in the mitigation guidelines. These guidelines will include means to document vulnerabilities and their mitigation. The ISSO and the Chief of ITOS will assign responsibility for mitigation of equipment to appropriate staff, either the ISSO or network staff responsible for the specific equipment needing remediation. (NOTE: The IBCR has purchased STAT Scanner[5] and STAT Analyzer[6] to scan for vulnerabilities and Hercules[7] from Citadel to assist in automatic remediation. Since policy is supposed to be flexible and not specific such that it doesn't have to be updated with every procedure change or different software choice, the exact mitigation process will be described in a procedures document rather than dictated by policy. Though this policy is definitely written with automatic procedures in mind.)
- Vulnerability scanning will be performed at a level that does not harm the IBCR network or its systems. Scanning will occur during business hours unless it is determined that scanning interferes with business processes. Scanning will be performed at the office location. Remote access scanning will only be allowed via FIHS provided VPN and terminal services and only if determined that scanning will not interfere with systems performance.
- The ISSO or appropriate network personnel must respond to all mitigation needs per the mitigation procedure and timeline. This document will likely change as IBCR gains experience with the vulnerability scanning and mitigation software. Experience will inform but mitigation should be performed before the next scan occurs so that scan can be used to judge compliance if possible. Staff performing mitigation must inform the Chief of ITOS if application of a patch would interfere with business requirements. Mitigation will also be constrained by maintenance windows and testing needs. Mitigation that will not affect business needs can be applied as soon as possible. Other patches and processes may be required to wait until the monthly maintenance window for server downtime or if critical a maintenance window will be negotiated.
- The ISSO and staff responsible for maintaining applications and equipment are responsible for monitoring the various patch mailing lists. Patch notices should be emailed to the ISSO so that vulnerability scanning software can be checked to ensure inclusion of vulnerability. If the vulnerability is not recognized the ISSO will check other patch sources for alternative means of deployment. (Note: The institute will probably be required by agency policy to monitor the new federal patch management service implemented by FedCirc, to be discussed later in this case study.)

[5] For information on Harris Corporation's STAT Scanner see http://www.statonline.com/solutions/vuln_assess/index.asp.
[6] For information on Harris Corporation's STAT Analyzer see http://www.statonline.com/solutions/sec_policy/index.asp.
[7] For information on Citadel Software's Hercules see http://www.citadel.com/Hercules.asp.

- The ISSO may not be intimately familiar with all applications and services on the network. An appropriately trained staff member will be responsible for maintaining those resources. If there is no vulnerability or patch management capability in the tools used by the IBCR those staff will be responsible for documenting the vulnerabilities discovered and mitigated for those services.
- Before being put into production or after a major configuration change servers will be scanned by the ISSO with the institute's vulnerability scanner and with FIHS' self Sara Scan.

5.2.2 Monitoring and Compliance

- As a form of monitoring and compliance vulnerabilities identified in a scan that are not mitigated by the next scan or the next maintenance window will be reported to the Chief of ITOS.
- The ISSO will use IBCR purchased patch management software to run as a compliance check for patches. It is expected that the vulnerability scanning software will identify and mitigate most patch needs. This will be done weekly for servers and at least monthly for desktops. Laptops will be checked on a quarterly basis.
- Microsoft Baseline Analyzer[8] will be run against all servers monthly. This will be used as a compliance check.
- The ISSO will respond to FIHS IRT notices and Sara Scan reports indicating attacks or vulnerabilities with a report on corrective measures or false positives within 1 week of notification. All responses will be carbon copied to the Chief of ITOS and the CIO. Machines identified with vulnerabilities will be scanned with the IBCR vulnerability scanner, the Microsoft Baseline Analyzer, the Patch management program and the FIHS self scan.
- Ecora Configuration Auditor[9] will be run against each server to baseline and then monitor for compliance.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Definitions

Term Definition

8.0 Revision History

This policy was revised on Feb 8, 2003 to fit the Institute of Basic Cellular Research.

[8] For information on Microsoft's Baseline Security Advisor see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp

[9] For information on Ecora's Configuration Auditor see http://www.ecora.com/ecora/

9.0 Signature
This policy is approved for use by: CIO's signature Date:

Note: This is a draft policy. It is expected to be a living document for a period of time until the ISSO and network staff has worked with the applications long enough to determine which process works best. Most of the changes will occur in procedural documents but after an efficient process has been designed the ISSO will want to revisit and tighten up the policy.

Besides needing to continuously scan for vulnerabilities it is important to ensure that newly placed servers and desktops have been patched before they come online. The vulnerability policy above refers to a Server Security policy that was discussed in the author's SANS GISO Practical (Cornwell 42). It is important to realize that the vulnerability policy goes hand in hand with a secure server, desktop and laptop configuration policy. The vulnerability and patch process will be more difficult if new machines being installed on the network are not being appropriately patched. In fact, the likelihood of new, unpatched machines being exploited is usually so high they will probably succumb to a common exploit before they would be picked up in a regular scan. This is self defeating; all new machines must be in a secure posture before going online. The author would add to step one that in addition to creating a vulnerability assessment and patch management policy a security policy covering the patch management for all new hardware additions to the network be in place to prevent running those responsible for patch management ragged while introducing risk into the network.

Step 2 – Inventory Systems

The second step in the Vulnerability Assessment and Patch Life Cycle is to inventory systems. There are three key steps necessary to correctly inventory the network. (Klaren 4)

1. Classify your network assets by platform. Conduct and maintain a complete inventory of the hardware and software, including the versions of software and firmware and any patches or upgrades that have been installed.
2. Determine risk potential. Identify the business exposure of each technology on your network. Which systems and software make up the critical core of your network?
3. Know what defensive tools you have in place. There are many kinds of defenses you can deploy, such as router filters, system logging and intrusion detection systems.

The author began this process in her GISO practical when discussing risk assessment (Cornwell 9). The author identified the critical servers, their main functions and discussed some risk of attack from the internet, other FIHS components, server vulnerabilities and the risk of internal threats to IBCR

resources. For each of these threats an essential component for mitigation was the use of commercial software to run vulnerability scans and to mitigate and patch discovered vulnerabilities. This case study has discussed the various layers of defense put in place by the FIHS and by the institute; filtering routers, firewalls, virus protection, intrusion detection and the fact that the institute is implementing a duplication of these levels with the addition of a firewall and IDS at its perimeter. These layers certainly reduce the risk to the hosts on the network but the premise for this case study is they do not reduce the risk to an acceptable level. Vulnerability scanning and patch management is a necessary process to reduce the risk to IBCR resources to an acceptable level.

The challenge of step two is simplified in some respects due to the fact that the institute only uses the Windows platform and has standardized all desktops. All servers are the same brand and some models are duplicated. The author's GISO practical discussed the implementation of a Server policy and procedure that would baseline servers. This policy is in the process of being reviewed for implementation. Currently the ISSO and network staff are installing new servers using the procedure discussed, refining it to the particular needs of the institute. This baseline procedure will assist the ISSO in the future to gather a comprehensive inventory of the network. The procedure discussed the use of some tools to assist in base lining. These tools gather inventory information and often allow snapshots to be taken and compared to a later picture making them also work for auditing, incident detection and configuration management. GFiLanGuard Network Security Scanner[10] is free for non-commercial use, providing a great opportunity to test the product in a live environment. LANGuard scans the network and gathers such information as "service pack level of the machine, missing security patches, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more." (GFi) The commercial version will install security patches, it also allows snapshots of each machine to be saved and compared later, thereby serving an auditing function.

> "A suggestion often made to make this process easier is to run only essential services, have only needed ports open, and all non-essential applications have been removed. Part of the inventory process is an understanding of what services and protocols are in use and/or installed." (Klaren 5)

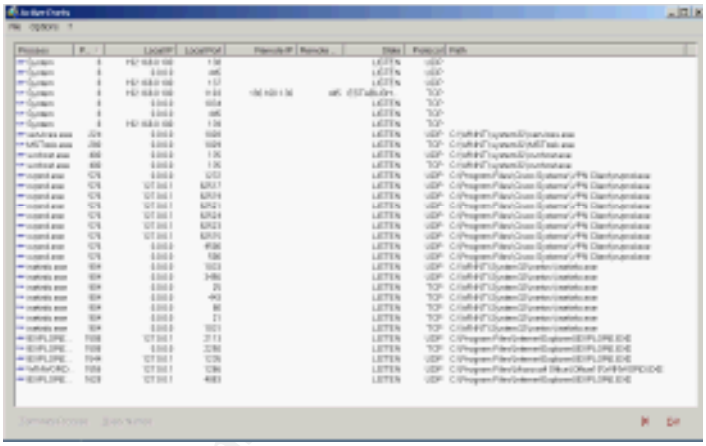
The main screen (see Figure 2) shows that LANGuard Network Scanner can assist in gathering this information. Once the open ports have been discovered Ms. Klaren suggests using Fport (Klaren 6), a free utility from Foundstone[11] to indicate the applications that are utilizing the open ports. The author prefers GUI

[10] For more information about GFiLANguard Network Security Scanner see http://www.gfi.com/lannetscan/index.htm.
[11] For more information about FPort see www.foundstone.com/knowledge/proddesc/fport.html.

applications and likes the freeware port analyzer program, Active Ports.[12] Information from Active Ports can be easily exported to a csv file making it easy to import into Excel (See Figure 3).

Figure 2 GFi LANGuard Network Scanner Main Screen. From GF Product Website
http://www.gfi.com/lannetscan/lanscanscreenshots.htm

Figure 3. Active Port Screen Shot



A comprehensive product that can greatly assist in a systems inventory, such as determining what applications are running on machines along with tons of other configuration information is Ecora's Configuration Auditor. This product can produce pages of documentation about a single server or for an array of common systems on a network. In fact, it may suffer from providing too much information.

Ecora considers itself a configuration auditing, change management and reporting program. Ecora Configuration Auditor[13] can provide baseline reports and change reports for all monitored systems. (See Figure 4) Reports can be set

[12] For more information about Active Ports see http://www.protect-me.com/freeware.html.
[13] For more information about Ecora Configuration Auditor see http://www.ecora.com/ecora/products/auditor.asp.

up to run automatically during off hours. The initial run can be used to inventory systems, after that use comparisons to monitor changes. Changes to a configuration will mean the system should be scanned for new vulnerabilities that new software may have introduced. Ecora Configuration Reporter[14] is a network assessment tool. It "automatically discovers and collects configuration data from virtually any device (servers, routers, switches, workstations, databases, operating systems) on a network and exports the data into HTML, DOC, or files for a relational database or spreadsheet." (Ecora)

Figure 4 Ecora Report Screen.
From http://www.ecora.com/ecora/products/windows/reporter.asp

Ecora can inventory items beyond Windows servers and desktops. It's a perfect product for the IBCR as it covers all the major server types we use.

- Cisco Routers/L3 Switches
- Lotus Domino Servers
- Microsoft SQL Servers
- Microsoft Exchange Servers
- Microsoft IIS Servers
- Windows Servers
- Windows Desktops
- Oracle Servers
- Novell Netware Servers
- Solaris Servers

The product can seem pricy for servers, it runs around $500. It's cheap for windows workstations at around $15 each. The reporting tool costs even less per system. When considering this tool can serve multiple functions such as assisting in auditing, vulnerability discovery, disaster recovery and configuration management and then figure how much it would cost in salary for the time to do this for a few servers on a regular basis, hhe math will indicate Ecora should pay for itself very quickly.

> "If you need to quickly know how your machines are configured, turn to Ecora's Configuration …. Ecora's goal is to do the dirty work you don't want to do: scrounge through the machines in the domain and figure out exactly how they've been put together. The Ecora applications come as

[14] For more information about Ecora Configuration Reporter see http://www.ecora.com/ecora/products/reporters.asp.

downloadable executables that are licensed for a particular number of servers and/or workstations.

Could you, theoretically, run to every server, gather the same information that Ecora can find and manually type it into a Word document? Sure. Could you do it in less than $500 worth of time? Probably not. Ecora's goal is not to ferret out problem spots in your environment, but, in a short amount of time, to simply "tell it like it is."

And Ecora tells it to you—in abundance." (Moskowitz)

Ecroa also sells a patch management program. At the time the ISSO investigated the product it wasn't ready for prime time. It may be worth taking a look at again. If the financial resources are available Ecora is worth a look as it is one of the only ways the IBCR ISSO can hope to keep up with a reasonably current network inventory. The Configuration Auditor will help to identify machines that are not in compliance with standards making it easier to narrow down the search for vulnerabilities and get them mitigated quickly. Ecora can also help with inventory of some Cisco switches and routers. Since routers and switches are part of a defense in depth strategy they should be inventoried and patched just as servers. The IBCR is not responsible for the switches, the IDS or the firewalls so the ISSO is dependent upon the ITC to ensure they are maintained and patched.

The final result of step two is (Klaren 7):

"you have reduced your level of vulnerability by getting rid of non-essential services. You have identified your areas of threat, by mapping out where the outsiders can access your system. You have identified your most critical systems. From here you should have a good idea where your highest areas of risk are, and what is at the top of your priority list. "

Ecora, LANGuard and Active Ports all provide the information needed to identify services that are running on systems. Determining what is non-essential and can be turned off is the second big challenge of step two. There are various places to research services. Security Focus Online hosts an article by Mark Burnett that explains the basics of services, how to shut them down, what to avoid and more. (Burnett) Included in the article is a link to Microsoft's Windows 2000 Services Definition[15] page and a script that can be used to determine what files services use. Also included is a service by category table that may assist in the search to determine what services are unnecessary. Knowing the systems on the network is an important step in being able to manage them. (See Table 1.)

[15] For more information about Microsoft's Windows 2000 Services Definition see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.asp

Table 1: Services by Category from http://online.securityfocus.com/infocus/1581

Clustering and Load Balancing	Remote Access
Distributed Transaction Coordinator Intersite Messaging	Internet Authentication Service Remote Access Auto Connection Manager Remote Access Connection Manager Routing and Remote Access
Collaboration	**Remote Administration**
ClipBook NetMeeting Remote Desktop Sharing	Remote Registry Service Telnet Terminal Services Terminal Services Licensing
Communications	**Remote Installation**
Fax Service Telephony	Boot Information Negotiation Layer Single Instance Storage Groveler Trivial FTP Daemon
Disk and File Management	**Removable and Remote Storage**
Distributed File System Distributed Link Tracking Client Distributed Link Tracking Server File Replication Indexing Service Logical Disk Manager Logical Disk Manager Administrative Service	Remote Storage Engine Remote Storage File Remote Storage Media Remote Storage Notification Removable Storage
Event Monitoring, Logging, and Alerting	**System Administration**
Alerter COM+ Event System Event Log Performance Logs and Alerts SNMP Trap Service System Event Notification	Application Management License Logging Service RunAs Service Task Scheduler Windows Installer Windows Management Instrumentation Windows Management Instrumentation Driver Extensions Windows Time
Hardware	**System Services**
Plug and Play Smart Card Smart Card Helper Uninterruptible Power Supply	Protected Storage Remote Procedure Call (RPC) Security Accounts Manager
Internet Clients	**TCP/IP Networking**
DHCP Client DNS Client	Internet Connection Sharing QoS Admission Control (RSVP) TCP/IP NetBIOS Helper Service
Internet Server Services	**Windows Networking**
DNS Server FTP Publishing Service IIS Admin Service Network News Transport Protocol (NNTP) Simple Mail Transport Protocol (SMTP) Simple TCP/IP Services Site Server ILS Service SNMP Service TCP/IP Print Server World Wide Web Publishing Service	Computer Browser IPSEC Policy Agent Kerberos Key Distribution Center Messenger Net Logon Network Connections Network DDE Network DDE DSDM NT LM Security Support Provider Remote Procedure Call (RPC) Locator Server Windows Internet Name Service (WINS) Workstation
Media Services	**Other**
On-line Presentation Broadcast Windows Media Monitor Service Windows Media Program Service Windows Media Station Service Windows Media Unicast Service	Print Spooler Utility Manager
Other OS Support	
File Server for Macintosh Print Server for Macintosh	

Step 3 – Manage Information

The third step is to mange information to assist in the identification of vulnerabilities. This means the management of vendor and security notices and to "scan your systems for existing vulnerabilities to verify" that they are patched. (Klaren 7). There are a plethora of mailing lists available that will send more information and alerts than one can handle. The best lists allow subscribers to zero in on the information needed by breaking the lists up by platform. Ms. Klaren recommends the Microsoft Security Notification Service[16], Cert Advisories,[17], and BugTraq.[18] SANS sponsors two mailing lists that are must haves; the Security Alert Consensus and the Critical Vulnerability Analysis list[19]. These various mailing lists are the most difficult part of the information flow to manage. Multiple emails a day indicating some new vulnerability begin to clog the inbox. Each needs to be addressed and checked against the systems and services on the network. Many of the tools mentioned in Step two track missing patches, allowing one to concentrate on the fixing of problems along with identifying them. This helps collapse the remainder of the steps in the life cycle.

The IBCR has been using St. Bernard's Update Expert for patch management. St. Bernard's Update Expert identifies Microsoft operating system and application vulnerabilities and allows patches to be managed from a central location. The program enumerates the network and indicates missing patches by machine, making it easy to combine the identification step with the mitigation step. While not yet in full deployment Update Expert has been used to update laptops and outside facing web servers when FIHS scans indicate problems. The ISSO has also used it to identify what versions of Internet Explorer are running on desktops and the absences of service packs for Office and the like. Update Expert has promise but there have been a few hiccups. One specific server will not respond to Update Expert, it is having problems with the Service Control Manager which prevents the patches from executing on the server. Also, the location from which Office was installed is necessary to install any office updates. Experimentation has shown that if Office was installed using the administrative network install Update Expert does not seem to be able to install needed patches. Update Expert does not always seem to be able to install service packs. These are all problems that will be discussed with the vendor. They have been responsive to questions in the past.

One advantage of Update Expert is that St. Bernard tests patches before they are released which may mean the need for less testing on standard systems. In the IBCR environment the ISSO has not experienced any crashes due to the installation of patches. In a few instances patches would not install but

[16] For more information about the Microsoft Security Notification Service see www.microsoft.com/technet/security/notify.asp.
[17] For more information about Cert Advisories see www.cert.org.
[18] For more information about BugTraq see www.securityfocus.com/cgi-bin/sfonline/subscribe.pl
[19] For more information about the Security Alert Consensus and the Critical Vulnerability Analysis list see http://www.sans.org/newsletters/.

it has never affected the target machine. The ISSO usually rolls out a small number of patches to a small number of machines. Update Expert chains patches and installs them in the correct order. It can also reboot the machine if needed. A test of a large rollout will be performed now that scheduled downtime for the network has been negotiated. Microsoft has just released 3 critical updates for Internet Explorer and the test will be to roll those out to the 170 desktops in the institute. This rollout will be tested on some desktops in the IT shop first to ensure no problems but also each update works differently and the ISSO has run across a few that require user attention to complete. For the first institute wide test a patch that requires end user attention is not the ideal. Update Expert does not require an agent on target machines and that was a main reason for its purchase. Update expert concentrates exclusively on Microsoft products. It manages updates for Windows OS, SQL, ISS, Office, Exchange, Outlook, Internet Explorer and MDAC but for the IBCR that covers a large part of the network.

Another aspect of step three is scanning systems for vulnerabilities. In her GSEC practical Ms. Klaren suggests scanning for the SANS/FBI Top 20 Most Unwanted Vulnerabilities.[20] (Klaren 8) These are the low hanging fruit or the easiest and most common compromises to fix. Since the IBCR only uses Windows systems the list is actually a top 10 list as the remainder cover the Unix platform. The good news is that many commercial vulnerability scanners have added the SANS Top 20 to their scanning patterns. Sara Scan, the scanner used by the FIHS, scans for the top 20 vulnerabilities listed by SANS. Ecora allows for security templates to be created. A template that covers the SANS Top 20 could be used to scan for these vulnerabilities.

So far the discussion has revolved around a rather manual way of identifying the need for patches via email or notification via vendor or research on the web and the use of patch management tools that combine identification with mitigation. It is still difficult to truly manage this information, there will be more email notices than one can process and there is always the possibility that the tools used may miss something. In response to the last few Internet crisis such as Code Red, Nimda and the MS-SQL Slammer high level Federal Government management have decided that patching is critical to protect the Government IT infrastructure and a contract was let to develop a government wide tool, FedCirc's Patch Authentication and Dissemination Capability (PADC)[21] web site. The feeling is that many agencies will be required to use this site. The word is that FIHS will require all components to register with this site.

The site has just begun operations and the IBCR has not registered so the author has not had time to look into the site in depth. The author has a few concerns for its effectiveness right off the bat. The purpose of the site is "To

[20] For more information on SANS/FBI Top 20 see http://www.sans.org/top20/

[21] For more information on FedCirc's Patch Authentication and Dissemination Capability (PADC) see https://padc.fedcirc.gov/.

assist agencies in mitigating vulnerabilities and keeping systems current with the latest Patches." (FedCirc) The site claims it will provide a "trusted source of validated patches and notifications of new threats and vulnerabilities." This is the current mission of many notification sites, CERT, SANS, Security Focus and more. Most commercial patch management products provide validated and tested patches. So how will this federal site help? An agency must register with the site and provide information on their specific infrastructure. This allows for customized notification profiles that target servers, OS, firewalls, routers, anti-virus and more. It claims to cover a much broader area then most current patch management programs, but the "supported technologies" currently listed on the site seem too limited. (PADC) The website will notify the agency when a new threat is discovered and when patches are released. Hopefully, due to the registration of equipment this might allow for a narrow target of information for the systems that are owned by an agency. This could save time and the ISSO from having to evaluate each notification from other services to find those relevant to the institute systems.

The PADC indicates that the patch download site will be secure and patches will be validated, most commercial products provide that. They also claim that a help desk will be available to assist agencies. If the help desk is properly staffed this might be worth it. The main problem the author sees is this is a static site; there is no connection between the servers and the patch management site. There will be a maintenance burden; if new systems and applications are not continuously updated then the site will quickly become inadequate. Also, one of the real reasons for using patch management programs is not necessarily the discovery of patches but for the dissemination of patches to multiple machines. The author fears that the PADC just makes the patch available for download and still leaves the problem of the rollout to 170 desktops and 40 servers to the network administrator. Commercial programs like Update Expert, Patchlink Plus and other vulnerability scanners assess each machine, indicate needed patches and then automate the dissemination of the patch. This is a more efficient way to handle patch management in the author's opinion. Of course, if PADC covers applications that are not currently managed by other software then it could very well be an improvement for those specific applications. The author wonders about the enormous size of the project, just thinking about the number of applications that must be used across the entire civilian government. One plus is that the PADC will be free to Federal Civilian government agencies. If an agency has no funds to purchase commercial programs the PADC will certainly be an important tool in their arsenal. If the PADC can help concentrate the notices that the ISSO needs to be aware of then it should be a worthwhile tool.

Step 4 – Assess the Information

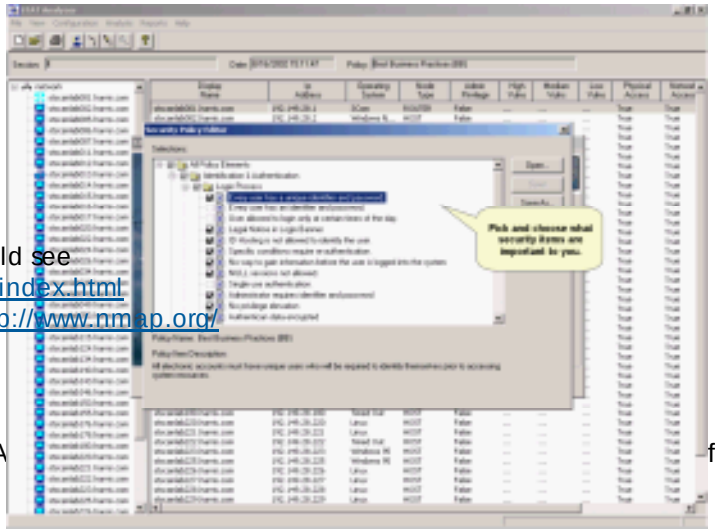
Step four is the point where the information gathered in previous steps is used to evaluate the risk to the Institute's systems. This is where risk, threats and vulnerabilities would be ranked to bring the most critical to the front. If scanning

for the SANS Top 20 it's a given that any positive signs of these vulnerabilities should be addressed immediately. In steps two and three a number of patch management tools were discussed along with information gathering tools that often identified missing patches as part of a configuration or auditing output. None of the tools discussed really ranked the vulnerabilities helping the ISSO prioritize remediation. The FIHS Sara Scan ranks vulnerabilities as Red; critical problems, Yellow indicates vulnerabilities that could lead to exploits and indicates Brown as a possible problem. The ITC asks that all reds and yellows be mitigated and results reported in a timely matter. The FIHS Scan, as discussed is limited and the ISSO feels that by itself it doesn't provide enough assistance in the reduction of risk.

Of concern to the ISSO is the initial scan and remediation for the institute will prove to be a large undertaking. While testing various products scans revealed over 4,000 vulnerabilities to be addressed. Another concern is the speed with which vulnerabilities are discovered and patches are released and the number of systems that are involved. A product that assists in the prioritization of remediation, something that basically tells the ISSO and network administrator what to fix first is necessary. The tools discussed so far can not help with prioritization.

The institute has picked a vulnerability scanning and mitigation solution from Harris Corporation. STAT Analyzer is designed to automate network security assessments. It goes beyond a patch assessment product like Update Expert as it checks for patches, compliance to a security policy, and for common vulnerabilities such as blank passwords and open shares. STAT Analyzer takes input from some of the best commercial scanners such as Harris' own STAT Scanner, Nessus, ISS Internet Scanner, and Network Associate's Cybercop and combines them to identify vulnerabilities. It uses IpSwitch's What's Up Gold[22] for network discovery and then Network Mapper (NMap)[23] a favorite freeware program of SANS to discover open ports and determine system OS.

IT management purchased STAT Scanner as it came bundled with Analyzer, saving the institute money. During testing it proved to be fast, generated a minimum number of false positives, and had good reporting capabilities. STAT Analyzer uses the input from STAT Scanner to compare results to the organization's security policy. Included are four security polices that offer basic to C2 security. Institute policy can be reflected in the scan by using the Security Policy Editor to pick from a tree structure of policy elements. (See Figure 5).



[22] For more information about What's Up Gold see http://www.ipswitch.com/Products/WhatsUp/index.html

[23] For more information about Nmap see http://www.nmap.org/

STAT Analyzer helps prioritize the institute's mitigation strategy by looking at multiple vulnerabilities that separately may only equal a low vulnerability but together indicates a highly possible exploit path. It also helps identify any low hanging fruit by including a scan for the SANS Top 20. Analyzer reduces false positives by checking to ensure that the conditions for the exploit exist. The results are ranked by severity and reports include detailed remediation information.

STAT Scanner includes an auto fix feature which remedies some of the identified vulnerabilities. STAT Scanner detects 1,250 vulnerabilities and according to SC Magazine "provides the most easily understood descriptions of vulnerabilities" (Marshall) which make it a useful training tool. If the auto fix feature fails, detailed manual fix information is included. The product's database of vulnerabilities is updated monthly, nicely integrating step three, managing information or the discovery of vulnerabilities, into an easy to use package which makes the job of vulnerability management much easier. STAT Analyzer also includes a report that allows the comparison of a base network snapshot to a current snapshot. Use this to graphically show that remediation and reduction of threats is on track or that perhaps there is a problem with policy that is somehow leaving systems open to attack.[24]

Figure 5 Stat Anaylzer Creating custom policy. From http://www.statonline.harris.com/solutions/sec_policy/reports/policy.pdf

The IBCR has not had time to fully deploy STAT Analyzer but due to the MS-SQL worm the ISSO is fast tracking its deployment. The ISSO anticipates that it will be easy to work into a process as testing proved it to be easy to use. The main problem will be first not to become overwhelmed at the initial count of vulnerabilities to be remediated. Second to ensure patches and fixes are tested and third getting the maintenance window to remediate identified problems. The author feels that once the tool has been fully deployed and the initial sets of vulnerabilities are remediated this tool will make keeping up with new vulnerabilities and exploits a manageable and hopefully even pleasant process. Trial versions are available for download on the STAT web site. For what it adds to the process the price is actually very reasonable. A 100 node license runs approximately $4,000.

Step 5 – Plan the Response

The last step is where the decision is made as to what to do with the identified vulnerabilities. There are multiple options such as installing a patch, implementing a suggested fix, performing a work around, adding another layer of defense as prevention, perhaps closing a port on the firewall, determining that the service is not needed and turning it off and the option to accept the risk and do nothing. A process that covers these various options should be created. The

[24] STAT Analyzer Session Compare Report see http://www.statonline.harris.com/solutions/sec_policy/reports/sesscompare.pdf

various tools discussed in this case study can definitely help by addressing the various steps from one interface. STAT Analyzer works across steps two through six; it helps determine what is running, it manages the flow of information in that vulnerabilities are updated monthly, it assesses the information, prioritizing vulnerabilities and it helps plan for response in its ability to roll out fixes.

One of the important components of step five is testing the proposed fixes or patches. The ideal environment would be to have a test network which duplicated the production network. Not everyone can afford that, while the IBCR could see its way to invest in these various tools, it could not afford to build a duplicate test network. One possibility is to install patches on non-critical machines first. Another possibility is to make sure the systems are backed up and can be easily restored in the event of a problem. Some of the tools help in that they test patches on standard setups before making them available. This might be adequate testing for standard Windows servers running common services such as IIS, or offering file or printing services.

The last tool to discuss for this case study is Citadel Software's Hercules product. Hercules takes input from STAT Analyzer and other popular commercial scanners and automates the remediation process. Hercules can identify unnecessary services and turn them off in the registry; it can disable insecure accounts and identify backdoors and misconfigurations. Hercules talks about the five steps for Vulnerability Assessment and Remediation. (Citadel)

1. **Identify Devices** - Identify the devices that could be at risk
2. **Assess Vulnerabilities** - Assess the vulnerabilities on systems that are at risk using a vulnerability scanner
3. **Review Vulnerabilities** - Review each vulnerability and determine which vulnerabilities should be resolved
4. **Remediate Vulnerabilities** - Fix each vulnerability that was selected in the review process
5. **Ongoing Management** - Set up a regular schedule for system scanning and remediation. This is essential to proactive security strategy that manages vulnerabilities.

The steps are almost identical to the process proposed by Ms. Klaren in her practical. Hercules understands and bases its product's operation on the life cycle of vulnerability assessment, making it an ideal tool to assist in this important security process. Hercules addresses steps three through five by identifying and remediating the five types of vulnerabilities: (Citadel)

1. Software Defects
2. Insecure Accounts
3. Backdoors
4. Unnecessary Services
5. Mis-configurations

Hercules allows remediation by vulnerability; many management software applications perform remediation by machine making it harder to address a specific vulnerability. Hercules lists the distinct vulnerabilities and allows one or more to be selected and remediated across all machines. The Hercules remediation database is updated when one of the supported scanners adds a new vulnerability signature to their scanner. One unique feature of Hercules is that certain fixes can be rolled back if a problem is discovered in the event the fix is not ready for primetime.

Hercules allows for logical grouping of machines, such as servers, web servers, database servers, desktops, laptops, etc. Device groups can be scheduled to be remediated at different times. Hercules allows automatic scheduling of remediation daily, weekly, or monthly. This could be a very useful facility once one becomes comfortable with allowing automatic remediation. The operator can select which vulnerabilities to remediate by approving the remediation profile so there is control of the process. The most difficult aspect of Hercules will be spending time getting comfortable with the automated remediation. Many administrators find handing over control a little difficult. But the various remediation activities Hercules can handle make it worth integrating into the vulnerability management process.

- Managing Accounts
  - Delete User
  - Disable User
  - Delete User from Group
  - Force Password Change
  - Manage Password Change Policy
  - Manage Password Expiration Policy
- Manage Account Privileges
  - Lock Memory Privilege
  - Increase Quota Privilege
  - Machine Account Privilege
  - Security Privilege
  - Take Ownership Privilege
  - Load Driver Privilege
  - Shutdown Privilege
  - Debug Privilege
  - Audit Privilege
  - System Environment Privilege
  - Enable Delegation Privilege
  - Manage Volume Privilege
  - Interaction Logon Right
  - Network Logon Right
  - Batch Logon Right
  - Service Logon Right
  - Remote Interactive Logon Right
- Execute system command and other applications as needed
- Manage files by using methods such as copy, move, delete or rename
- Install software patches including hotfixes and service packs
- Display informational messages regarding remediation process
- Adjust NTFS and other file system permissions for enhanced security
- Reboot the system as needed
- Perform registry operations such as add/move/delete/change and manage registry key security
- Disable, restart, remove and change startup parameters of Windows NT-based services
- Remove unnecessary disk shares or adjust access control permissions for shares
- Add or remove entries for configuration or INI files
- Terminate and remove running processes such as Trojan software or backdoor programs
- Manage system-wide audit settings to ensure auditing compliance
- Adjust domain policy settings such as:
  - Password lengths
  - Password history ages
  - Forced logoff
  - Account lockout parameters
- Adjust registry settings as necessary
  - Plus other activities.

Table 2. Hercules Remediation Activities from
http://www.citadel.com/Downloads/whitepaperherculesfinal.pdf

Putting It all Together

Before

The problems faced by the IBCR boiled down to slow implementation of policy at various points in the defense in depth strategy making it difficult to adequately protect the institute without putting in place a comprehensive vulnerability and patch management process. While the FIHS does run weehkly and monthly vulnerability scans they only identify a small subset of possible vulnerabilities and the ISSO does not feel that the institute can rely solely on these scans. The time interval was not often enough to keep up with the IT community's ability to identify new vulnerabilities and with vendor's release of patches. Many aspects of defense in depth for the FIHS are coming together, the firewall policy will be set to deny all by the time this paper is complete, agency scanning will increase but there is still the need for FIHS components to take patch and vulnerability management seriously. Even if the FIHS firewall perimeter and the IBCR firewall could entirely protect the institute there are still insider threats and outside facing machines on the IBCR network. Also, thought must be given to the possibly of a firewall failure or new exploits that can find their way through. The release of the MS-SQL worm indicated that the IBCR was not doing enough to protect its resources and the ISSO wanted to design a process to assist the institute in working toward a more proactive stance.

During

While doing research for this paper a well defined patch management process was found in Judy Klaren's GSEC Practical. Rather than re-inventing the wheel the author used the five step process described as the basis for a patch management process for the IBCR.

1. Define your corporate policy on Vulnerability Assessment and Patch Management. This policy should include what the policy is, why you need it, the scope, and how and by whom it will be completed.
2. Inventory your systems. Know exactly what you're running so you know exactly what to worry about.
3. Manage the flow of information. Determine which information resources help you focus exclusively on the vulnerabilities that affect your systems.
4. Assess the information. Evaluate the actual risk to your organization's systems security.
5. Plan for response. Develop standard procedures to translate information into action. (Klaren 2)

A vulnerability and patch management policy was created for management approval as the first step. The need for a standard baseline for servers and desktops was discussed as a way to ensure that new hardware is not going online without first being checked for vulnerabilities. Without such a baseline, vulnerability mitigation would always be playing catch up and new hardware may be placing the network at risk, possibly being exploited before it could be included in a scan.

The baseline policy works with and is aided by the systems inventory described in step two. The server security policy requires documentation of the business need and operation of each server along with the use of software to assist in documenting ports, applications and for ensuring the servers are patched. The IBCR has purchased some enterprise wide tools to assist in these steps and brief descriptions of how these tools could assist each step were covered. The ISSO is currently in the process of trying various tools to refine the process. One of the most comprehensive and promising is Ecora's Configuration Auditor. While preparing for this paper a server that would house the vulnerability tools discussed was set up using the process described in the author's GISO practical. Ecora was run to create a snapshot of the server resulting in a 58 page report detailing information on services running, groups and user accounts, domain user rights, audit policy, hotfixes installed and more. This software will be an immense help in the inventory process.

The remainder of the process can be handled by STAT Analyzer and Citadel's Hercules, vulnerability scanner and remediation products purchased by IBCR. STAT Analyzer scans the network devices and presents a listing of vulnerabilities ranked by severity. STAT Analyzer works with the top notification vendors to include all known vulnerabilities which are updated regularly helping to relieve some of the burden of information management in step three. Analyzer allows the ISSO to scan for compliance to security policy along with needed patches, misconfigurations and registry settings. It generates easy to read reports including executive reports and baseline reports to assist in prioritizing remediation needs. Analyzer also uses fuzzy logic to minimize false positives and allows for the input of multiple scanners. Analyzer produces a list of vulnerabilities, their severity and provides information on how to fix them basically performing step four for the operator. Step five defines the response to the information gathered in step four; basically it takes the list of vulnerabilities, their priority and creates a process for remediation. Analyzer can actually perform some remediation automatically, patch management tools like St. Bernard's Update Expert can apply patches across multiple machines but the IBCR purchased a product from Citadel that promises to automatically remediate the vulnerabilities identified by the top scanners. Hercules gives the operator complete control over the process and provides reporting. These tools promise to make what often is a tedious process that requires detail oriented reporting, time and resources into a manageable process. The ISSO plans to scan and

remediate on a weekly basis after using these tools to bring the institute up to a fully patched and protected state.

After

The author has used the St. Bernard's Update Expert patch management tool to some success. The test for this paper was going to be the implementation and use of STAT Analyzer and Hercules. A new server was installed using the Server Security procedure discussed in the author's GISO practical and the software was installed. A scan of the network servers was performed with STAT Scanner, which is a component of STAT Analyzer. The scanner took approximately 3 hours to scan 45 machines. The Executive Summary graph indicated the vulnerabilities broken down by Red for High, Yellow for Medium, Green for Low and Blue for information. (See Figure 6.) The totals are included below:

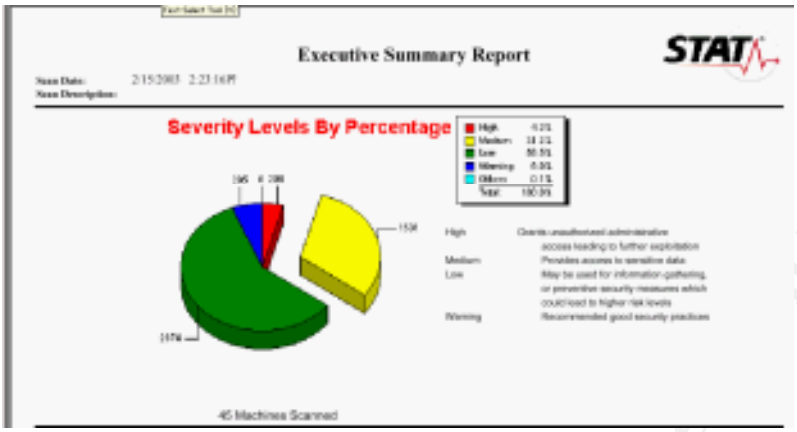


Figure 6. Executive Summary Report from STAT Scanner.

High	206
Medium	1531
Low	2874
Warning	295
Others	5
Totals	4911

The scanning did not negatively affect any of the servers. When attempting to run the scan using STAT Analyzer there was a software problem that prevented it from running. The STAT scanner results could not be analyzed to remove false positives or to chain vulnerabilities together to identify exploit paths that may need to be addressed. While testing the software Harris was very responsive and helpful. The author has already emailed the vendor and will be talking with them to address these issues. One of the things noticed by the author was that the average number of red vulnerabilities for each server ran around 6 to 10 but the three servers that had just been installed using the Server Security process discussed in the author's GISO practical had no red vulnerabilities. The author takes this as an indication that the process does make new servers safer, reducing risk to the network and that these tools can aid in the auditing and compliance process for servers.

Unfortunately, there was also a problem with Hercules, it remediated some chosen vulnerabilities but had problems with others. Therefore it could not be used extensively for this test. There were no problems importing the results of the STAT scan and a comprehensive list of vulnerabilities was produced. An agent has to be installed on each machine but not all responded to pushing remediation profiles down. The author has emailed the vendor and they are very eager to assist. While this is disappointing, the author feels that these are both very complex programs that are attempting to address complex issues and problems are bound to crop up. In the author's experience there is usually a learning curve and bumps in the road when installing such products. These products showed promise in testing and this is just a glitch. While researching this paper and looking at upgrades to STAT and Hercules, the author believes these products will become a large part of the IBCR's vulnerability mitigation plan.

While these programs did not function as desired it was still necessary to protect the IBCR servers. Management had provided a maintenance window and network staff wanted to make the best of it. After updating of hardware drivers the network staff updated Microsoft patches using Windows Update. After all servers had been updated the ISSO ran a second scan to compare a before and after. Unfortunately, due to the Snow Storm of '03 there will be no chance to discuss results in this paper.

In closing there is no magic bullet for the patch management and vulnerability discovery and mitigation process. But there is a better way to do it than by hand. The highlighted products will assist in the process of remediation but they will not make it as simple as pushing a button and forgetting about it. The software does not relieve staff from knowing about their systems. It does not relive staff from paying attention to the various notification sites. FedCIRC's PADC may assist federal agencies somewhat, but this service is barely off the ground at this time. These products do not relive staff from understanding how software interacts. Mitigation signatures will have to be studied closely to ensure they will do no harm, but the advantage is that as time is spent with this software administrators will learn more about their systems. For the security professional insight into exploits, software holes and configuration failures will be gained. Learning about the vulnerabilities should make it easier for the security professional to know where to concentrate on prevention and how to evaluate attacks. These software packages should make a daunting process manageable. The policy included in this paper and the process it requires will be a living document as the process is tested and refined. The author is counting on these software products to assist in making sure that the IBCR always comes up green on all FIHS scans and to ensure that all IBCR resources are protected.

References

Burnett, Mark. "Securing Microsoft Services." May 22, 2002. <http://online.securityfocus.com/infocus/1581>. (9 Feb 2003).

Citadel. "5 Steps for Vulnerability Assessment & Remediation." <http://www.citadel.com/5steps.asp>. (9 Feb 2003.)

Citadel. "Frequently Asked Questions about Hercules." <http://www.citadel.com/hercules.asp#Frequently%20Asked%20Questions%20about%20Hercules>. (9 Feb 2003).

Cornwell, Kay A. "GIAC Institute for Basic Cellular Research." Oct 16, 2002. <http://www.giac.org/practical/Kay_Cornwell_GISO.doc>. (9 Feb 2003).

Cornwell, Kay A. "GIAC Institute for Basic Cellular Research." Oct 16, 2002. 42. <http://www.giac.org/practical/Kay_Cornwell_GISO.doc>. (9 Feb 2003).

Cornwell, Kay A. "GIAC Institute for Basic Cellular Research." Oct 16, 2002. 9. <http://www.giac.org/practical/Kay_Cornwell_GISO.doc>. (9 Feb 2003).

Ecora. "Configuration Reporter" Product Site. <http://www.ecora.com/ecora/products/reporters.asp>. (9 Feb 2003).

FedCirc. "Federal Computer Incident Response Center PADC (Patch Authentication and Dissemination Capability." <https://padc.fedcirc.gov/images/PADC_slipsheet.pdf>. (9 Feb 2003).

GFi. "GFi LANGuard Network Security Scanner." Product Site. <http://www.gfi.com/lannetscan/>. (9 Feb 2003).

Klaren, Judy. "Managing Vulnerability Assessment and Patch Installations." January 24, 2003. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. "Managing Vulnerability Assessment and Patch Installations." January 24, 2003. 2. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. "Managing Vulnerability Assessment and Patch Installations." January 24, 2003. 4. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 5. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 6. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 7. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 8. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 2. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (9 Feb 2003).

Marshall, Geoff. “Stat Analyzer.” August 2002. <http://www.statonline.harris.com/news/media/analyzer_scmag.pdf>. (9 Feb 2003).

McBride, Patrick, Patilla, Jody, Robinson, Craig, Thermos, Peter. “Developing an Information Security Policy.” <http://www.scmagazine.com/scmagazine/2001_04/special.html>. (9 Feb 2003).

Microsoft. “Windows 2000 Server Baseline Security Checklist.” <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (14 Oct 2002).

Moskowitz, Jeremy. “How Fast Can You Document Your Network?” January 2002. <http://www.mcpmag.com/reviews/Products/article.asp?EditorialsID=206>. (9 Feb 2003).

PADC. "FedCIRC Patch Authentication and Dissemination Capability (PADC) Supported Technologies." <https://padc.fedcirc.gov/images/PADC_InitialTech.pdf>. (9 Feb 2003).

SANS "MS-SQL Server Worm (also called Sapphire, SQL Slammer, SQL Hell): A Special Report from the SANS Research Office." <http://www.sans.org/alerts/mssql.php>. (9 Feb 2003).

SANS "SANS/FBI Top 20 List." http://www.sans.org/top20/. (9 Feb 2003).

St. Bernard Software. "W32.Slammer and Service Pack 3 for SQL Server ™ 2000: Slam the Door on Patching." January 30, 2003. <http://www.stbernard.com/products/docs/DontGetSlammedByPatching.pdf>. (9 Feb 2003).

Footnote References (Product Websites)

[1] McAfee E-Policy Orchestrator Website
URL: http://www.mcafeeb2b.com/products/epolicy/default.asp (9 Feb 2003).

[2] Sara (Security Auditor's Research Assistant) Website
URL: http://www-arc.com/sara/ (9 Feb 2003).

[3] Microsoft's Window Update Website
URL: http://v4.windowsupdate.microsoft.com/en/default.asp (9 Feb 2003).

[4] St. Bernard's Update Expert Website
URL:http://www.stbernard.com/products/updateexpert/products_updateexpert.asp. (9 Feb 2003).

[5] Harris Corporation's STAT Scanner Website
URL: http://www.statonline.com/solutions/vuln_assess/index.asp. (9 Feb 2003).

[6] Harris Corporation's STAT Analyzer Website
URL: http://www.statonline.com/solutions/sec_policy/index.asp. (9 Feb 2003).

[7] Citadel Software's Hercules Website
URL: http://www.citadel.com/Hercules.asp. (9 Feb 2003).

[8] Microsoft Baseline Security Advisor
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp. (9 Feb 2003).

[9] Ecora's Configuration Auditor Website
URL: http://www.ecora.com/ecora/ (9 Feb 2003).

[10] GFiLANguard Network Security Scanner Website
URL: http://www.gfi.com/lannetscan/index.htm. (9 Feb 2003).

[11] Foundstone's FPort Website
URL: www.foundstone.com/knowledge/proddesc/fport.html. (9 Feb 2003).

[12] Smartline's Active Ports
URL: http://www.protect-me.com/freeware.html. (9 Feb 2003).

[13] Ecora Configuration Auditor
URL: http://www.ecora.com/ecora/products/auditor.asp. (9 Feb 2003).

[14] Ecora Configuration Reporter
URL: http://www.ecora.com/ecora/products/reporters.asp. (9 Feb 2003).

[15] Microsoft's Windows 2000 Services Definition
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.asp. (9 Feb 2003).

[16] Microsoft Security Notification Service
URL: www.microsoft.com/technet/security/notify.asp. (9 Feb 2003).

[17] Cert Advisories
URL: www.cert.org. (9 Feb 2003).

[18] BugTraq
URL: www.securityfocus.com/cgi-bin/sfonline/subscribe.pl. (9 Feb 2003).

[19] Security Alert Consensus and the Critical Vulnerability Analysis list
URL: http://www.sans.org/newsletters/. (9 Feb 2003).

[20] SANS/FBI Top 20
URL: http://www.sans.org/top20/. (9 Feb 2003).

[21] FedCirc Patch Authentication and Dissemination Capability (PADC)
URL: https://padc.fedcirc.gov/. (9 Feb 2003).

[22] What's Up Gold
URL: http://www.ipswitch.com/Products/WhatsUp/index.html (9 Feb 2003).

[23] Nmap
URL: http://www.nmap.org/ (9 Feb 2003).

[24] STAT Analyzer Session Compare Report
URL:
http://www.statonline.harris.com/solutions/sec_policy/reports/sesscompare.pdf (9 Feb 2003).

Assignment 2 – Abstract

Operating systems and applications often are vulnerable to exploits when installed out of the box. When installing new servers the Operating System settings should be examined and made more secure before a server is hooked to the network. Failure to do so can lead to a server compromise, sometimes in under 5 minutes. Best practice suggests that certain steps should be taken to protect a newly installed server. The author created a Server Security Policy and procedure in an effort to standardize and to harden the installation of Windows 2000 servers in the IBCR. The policy's aim is to create a standard baseline process to set up servers ensuring that best practices are followed to eliminate vulnerabilities before the servers are attached to the network and to ensure that all servers are set up in the same way when multiple staff have responsibility for installation.

The only way to ensure that policy and procedures are fulfilling their goals is to audit for compliance. Without auditing failure of policy or procedures will likely appear as exploits or intrusions. New server installations should be randomly audited to ensure procedures are followed. Auditing can help indicate if there are problems with the procedure, providing an opportunity to fix it. Auditing older servers can help identify configuration changes that are not being checked, as per policy and perhaps indicate that vulnerability and patch management procedures are not being followed. Auditing helps ensure that machines are running at a secure level and that staff is following policy as they install and make changes to servers. When preparing to audit the auditor must consider the scope or what is being audited, create a checklist that indicates what and how to audit and then prepare a report indicating the results. In this paper the author plans an audit of the Server Security Policy and procedure.

Assignment 2 – Server Audit Program

In order to earn the SANS GISO certification the author created a server security policy and procedure covering the installation of Windows 2000 servers in the IBCR. The policy's aim was to create a standard baseline process to set up servers ensuring that best practices were followed to eliminate vulnerabilities before the servers were attached to the network. The policy is still in review by management but the process has been used to set up the Vulnerability server discussed in Assignment 1 and other servers being upgraded. In Assignment 1 the author found that the machines set up by following the procedure had no red vulnerabilities while almost all other servers had from 3 to 10 apiece. The author believes this indicates that the standards are creating safer servers.

The only way to ensure that policy and procedures are fulfilling their goals is to audit servers for compliance to policy. Once a server is attached to the network it quickly becomes outdated as security and application patches are released and as software and hardware is installed by administrators. The vulnerability and patch management policy proposed in Assignment one dictates that servers are scanned and patched in a timely manner. Auditing will ensure that the machines are running at a secure level and that staff are following policy as they install and make changes to servers, it will also serve to indicate that vulnerability policy is being followed.

First let's outline the audit procedure as described by SANS.

1. Conduct research
2. Develop audit scope
3. Develop set of audit objectives
4. Develop checklist
5. Conduct the audit
6. Produce a report

Step 1 – Conduct Research

The need and type of research depends wholly on the type of auditing to be performed. This audit will be a conformance audit to ensure that policy is being followed. The research would consist of studying the Policy and the Procedures to be audited against so a checklist could be developed. The Server Security policy could also be audited against best practice, in that case the auditor would research what best practices are for Windows 2000 Server baselines. At the beginning of the checklist a list of resources used to help develop the checklist should be included.

Step 2 – Develop Audit Scope

Step two answers the question, what is the goal we are attempting to reach with the audit and what exactly is being audited.

The IBCR depends heavily on a network client/server environment composed of Windows 2000 servers which act as database servers, web servers, file servers and more. In order to protect IBCR resources and to ensure servers are hardened and protected from attack before they are attached to the network a Server Security policy and installation procedure was created. This audit will occur randomly after a new server is added to the network to ensure policy and procedure is being followed. This same audit checklist will be used to randomly audit older servers to ensure that compliance with vulnerability assessment and remediation is occurring on a timely basis and to ensure configuration changes are not weakening the initial security controls placed on the server.

Step 3 – Develop Set of Audit Objectives

This particular audit will be a conformance audit which measures an auditable entity against a policy or procedure. The overall objective is to ensure procedure and policy is being followed by staff as they install servers and to ensure that hardening procedures are applied after configuration changes. The audit will also help determine if all aspects of the policy is workable. Since this is a new policy and procedure the first audits may indicate areas where the policy and procedures are not working as planned due to unworkable or clumsy procedures. The Server Security Policy is included in Appendix A. The Server Security Procedure is included in Appendix B. A list of audit objectives was derived from the policy and procedure and audit controls were identified for each objective.

Objective: Ensure proper documentation is in place to support process
Control: Server configuration guides
Control: Exceptions are documented
Control: Server documentation available, server is registered
Control: Change management procedure is in place

Objective: Configure Server to prevent exploits
Control: Install and configure server offline
Control: Remove unnecessary services
Control: Scan for vulnerabilities and repair
Control: Configure terminal services for admin access only
Control: Before being put into production or after a major config change scan with vulnerability scan and FIHS Sara Scan
Control: Remove IIS if server is not an authorized web server
Control: Remove OS/2 and POSIX subsystems
Control: Apply custom Security Template to harden server
Control: Use CIS tools to audit Security Template over time
Control: Set up and Audit password policy to IBCR standard
Control: Set up and audit account lockout policy to IBCR standard
Control: Set up and audit audit policy to IBCR standard
Control: Set up and audit user rights policy to IBCR standard

Control: Set up and audit Security options policy to IBCR standard
Control: Winnt folder permissions should only allow Admin and system full control access
Control: Virus software is installed, runs continuously in background, monitored by E-Policy.

Objective: Only authorized users may have access to server
Control: Contractors must have permission from IT management for admin access or monitored during process that requires admin access
Control: set up NT access control to prevent unauthorized access
Control: network admin staff should use their admin accounts to access admin functions and not general admin accounts
Control: Servers must be physically located in the LAN room
Control: Rename administrator account and provide a strong password
Control: Guest account should have strong password and be disabled
Control: Display a logon warning banner
Control: Setup logon screen saver to kick in after 5 min
Control: Set file system to NTFS
Control: Replace EVERYONE on file system with Authenticated Users
Control: Audit Local Groups for authorized accounts
Control: Review trust relationships, IBCR only trusts FIHS domain
Control: Only authorized users are allowed to access network applications
Control: RAS services are not authorized for use in IBCR. Remove RAS services.
Control: Remote Access to the IBCR network is only allowed via FIHS VPN and Dial-in Service.

Objective: Keep server up to date by responding to notices of possible exploits
Control: respond to Fedcirc, cert and other notices of vulnerabilities that may apply
Control: Respond to FIHS Sara Scan identified vulnerabilities

Objective: Monitor Server for unauthorized use and protect audit trail, events should be reported immediately
Control: Monitor all security related events such as security logs
Control: Place security logs in a central console to help with monitoring
Control: Security logs must be set to at least 16mb in size and set to overwrite
Control: Backup security logs and keep for prescribed period of time
Control: Security related events must be reported to the ISSO immediately via alerts, ids, tripwire alert
Control: any identified breach should be reported to the FIHS IRT
Control: ISSO will keep a detail log of security events
Control: Create a dummy administrator account and place in guest group and log attempted access to monitor for possible attacks
Control: Only domain admins should have access to security logs

Control: Logs are collected and monitored via Net IQ Security Manager
Control: Tripwire is installed to protect OS files

Objective: Fix any identified vulnerabilities as soon as possible
Control: Process is in place to have corrective measures applied by Network admins within 1 week of identification.
Control: All mitigations will be reported to ISSO
Control: Process is in place for ISSO to respond to IRT and Sara Scan notices with corrective measure reports within 48 hours of notification. Copies will be sent to chief of ITOS and the CIO.

Objective: Ensure a standardized setup for each server
Control: Server name must reflect server function and follow IBCR Conventions
Control: Server is given static IP address within server range

Objective: Ensure server is set for high performance, availability, ease of troubleshooting
Control: NIC set to 100, full duplex
Control: Foreground applications performance boost should be set to NONE
Control: Recovery Options set for fast recovery, only write event to system log, reboot, use small memory dump
Control: Add /sos to end of boot string so boot process shows on screen
Control: Process to create ERD, update ERD and protect ERD.
Control: Registry should be backed up during normal backup routine
Control: Monitor registry for changes
Control: Servers are monitored and protected by UPS

Objective: Ensure IIS is installed in a secure manner
Control: Remove unnecessary protocols
Control: Disable NETBIOS over TCP/I
Control: Scan regularly with vulnerability scanners
Control: Audit and remove unnecessary ODBC connections
Control: Remove unnecessary services
Control: Web site contents are not stored on OS partition
Control: Specific executables should be limited to admin only
Control; Restrict Anonymous should be set to 1
Control: TCP/IP Syn Attack Protect should be set to 2 in registry
Control: Change default IIS user accounts, remove right to access machine from network, disable log on locally.
Control: Only the public web is authorized to use anonymous access all other web servers must use NT/Challenge authentication and is limited to IBCR staff.
Control: Secure the metabase using best practice
Control: Run the MS IIS Lockdown and URL Scan tool
Control: Only the Intranet web server is authorized to run SMTP, all other servers should have service removed.
Control: No NNTP services are needed in the IBCR, remove this service.

Control: IIS Admin Web Server (HTML interface) is not authorized for use, remove this service.
Control: Only the public web server is authorized for FTP use, there is no anonymous FTP authorized in IBCR
Control: Remove IIS documentation and samples
Control: Turn on file auditing for web site folders and files
Control: Turn off directory browsing

Objective: Ensure SNMP Security
Control: Private and public community strings must be changed from default
Control: Trap authentication failures
Control: Set permissions on SNMP registry keys for admins, system and creator to full
Control: Only authorized hosts are to be added to the community

Objective: Protect terminal service from allowing unauthorized access
Control: Terminal services are set for administrative access only
Control: Data encryption is set to 128bit
Control: Users accessing servers are always asked for authentication
Control: no guest access via terminal service

Objective: New Server installs are baselined for future reference
Control: New servers are scanned with St. Bernard's Update Expert and reports are saved.
Control: New servers are scanned with CIS scoring tool against IBCR custom template and reports are saved.
Control: New servers are scanned with Microsoft's Baseline Analyzer and reports are saved.
Control: New servers are scanned with Active Ports, non-standardized reports are documented and reports are saved.
Control: New servers have their registry snapshot taken and reports are saved.
Control: New servers are scanned with GFiLANguard and reports are saved.
Control: New servers are scanned by Ecora Configuration Auditor and reports are saved.
Control: New servers are scanned with STAT Analyzer and reports are saved.
Control: Control: New servers are scanned with Hercules and reports are saved.
Control: Any vulnerabilities found as a results of the above are mitigated and a report is saved.
Control: New servers are scanned with FIHS' Self Sara Scan and reports are saved.
Control: All reports are saved to a directory under the server's name. Access by security staff only.

Step 4 – Develop Checklist

When developing the checklist remember the scope. Use the audit objectives and audit controls developed in step four. Use best practice as the basis for creating the technical steps to fulfill the audit controls. For a conformance audit the policy and procedure should have been based on best practice, making the development of the checklist easy. When best practice is at odds with the policy or procedure, since this is a conformance audit the controls should reflect the procedure and policy being audited. The body of the checklist describes what to check and explains in detail how to check and measure compliance.

Checklist References

Checklist adapted from Auditing Windows 2000. Krishni Naidu, Score.
http://www.sans.org/score/checklists/AuditingWindows2000.doc
Windows 2000 Server Baseline Security Checklist. Microsoft
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp
Windows 2000 Server Configuration. Internal FIHS Document. Sept 9, 2002
Microsoft Windows 2000 and Windows XP Professional Desktop Security Checklist. Internal FIHS Document, Sept 19, 2002

Introduction

This checklist is to be used to audit Windows 2000 servers newly installed, after a major configuration change or for random checks to ensure vulnerability mitigation and patch management is being performed.
This checklist highlights technical security controls. However, it is also important to consider other security controls that are of a non-technical nature e.g. physical security for the server room.

Prior to using this checklist the following elements should be considered:

- Mitigating controls: Give consideration to the security elements of various other systems that may operate off the Windows 2000 box. These systems may include applications and databases. The security on the other elements may be so strong so as to mitigate a weakness in the Windows 2000 system. E.g. an application may encrypt its program and data files, thus it is not necessary to use EFS. However, this checklist does not provide all the security considerations if the Windows 2000 system interfaces with applications and databases. Standard setups will be considered for inclusion into this checklist else take each on a case by case basis.
- Practicality: This checklist provides security considerations for a secure Windows 2000 server in the IBCR environment. This check list reflects the accepted security stance of the institute considering the cost benefit factors of implementing security elements versus the business needs of the institute. This checklist is a growing document as new steps are

expected to be discovered which can be put into place to add more security for institute systems. Where possible the checklist provides security considerations if the Windows 2000 server where implemented in various instances e.g. as web server.

- Environmental considerations: Prior to using this checklist it is important to determine what clients and other hosts the Windows 2000 server interacts with. Windows 2000 server includes certain functionality that only works well with Windows 2000 clients or only in a fully Windows 2000 environment e.g. IPSEC requires the clients to be 2000 as well for full deployment.
- Updates: Since Windows 2000 is undergoing improvements due to vulnerability and operability requirements; this checklist is restricted to audit for functionality other than hotfixes and patches. Automated tools such as STAT Analyzer, Microsoft's Base Analyzer and St. Bernard's Update Expert will be used to identify missing patches and application vulnerabilities.

Prior to using this checklist it is important to determine the function of the Windows 2000 server in the environment and then tailor this checklist to suit the environment.

Checklist

No.	Control
1 ●	Server Configuration Guide Identify location of the approved server configuration guide and ensure there is an established process for updating the guide. Ensure the guide is periodically reviewed by the ISSO and Chief of ITOS.
2 ●	Exceptions to Baseline Ensure any exception policy is posted in the LAN Room and available in a central network location.
3 ●	Ensure Server is Approved Request for server and its business process submitted to Chief ITOS before installation began, request is on file. Information should be available in the server log book. • Need for the server and the original request • Hardware requirements • Software requirements including OS/Version • List of applications, main functions and any special needs/concerns • Who will need access, at what level and reasons • Any special considerations • Is service considered to be critical • Location of Backup service (Sans or Traditional) • Name of Installer and backup contact

	• Name of staff responsible for applications if not the same as above • Server name, URL/domain name, IP address & LAN tap no.
4 ●	Ensure Server is registered with IBCR asset management to include the following information: • Server name, URL and IP address, LAN Tap no. • Name of Installer, person with knowledge of apps, Name of backup staff • Location of Backup service (Sans or Traditional) • Hardware, Operating System/Version • Who requested, who approved • Main functions and applications, if applicable • Special considerations • Who needs administrative access
5 ●	Ensure change management procedures are in place
	General Configuration Guidelines
6 ●	Ensure Installation is performed while the server is OFFLINE.
7 ●	Services Removed Ensure that all services and applications that will not be used are removed or disabled. Check Services under Control Panel. (Note: after a period of experimentation a list of these services should be available. The IBCR custom list will be included into the checklist.)
8 ●	Access Control Ensure access to server is protected through NT/Windows Domain access-control methods. Ensure that Administrative access is limited to IT staff with direct responsibility for the server by checking admin group. Access should be logged in the Security logs.
9 ●	Vulnerability Scans Ensure the ISSO scans the server with a vulnerability tool weekly and reports vulnerabilities and applies patches and fixes to all high priority vulnerabilities unless application would interfere with business requirements. Monitor vulnerability logging and reports.
10 ●	Terminal Client access to server must be approved by ISSO or Chief of ITOS. Check to ensure only authorized users have terminal service turned on. Check user account properties.
11 ●	The ISSO must respond to notices of necessary security patches within 48 hours or must inform the Chief of ITOS if application would interfere with business requirements. Check date of last vulnerability scan and compare to audit date, exceptions should be addressed in email.
12	Contractors who need access must be cleared for administrative accounts or must be monitored by administrative staff while accessing the server.

●	
13 ●	Ensure Network administrative staff performs all admin functions with their private administrative account rather than the general administrative account.
14 ●	Before being put into production or after a major configuration change ensure servers are scanned by the ISSO with the institute's vulnerability scanner and with FIHS' self Sara Scan.
15 ●	Ensure server is physically located in the LAN room and the LAN room is closed and locked so that access is only via cipher lock.
	Monitoring
16 ●	Ensure that all security-related events are logged and audit trails saved as follows: • All security related logs are kept online for a minimum of 2 weeks, collected and maintained by a central logging program. • Daily incremental tape backups are retained for at least 6 months. • Weekly full tape backups of logs are retained for at least 6 months. • Monthly full backups are retained for a minimum of 6 months.
17 ●	Ensure a process is in place so that all security-related events are reported immediately to the ISSO or Chief of ITOS. Ensure the ISSO reviews logs and reports incidents to the Chief of ITOS. Corrective measures should be prescribed as needed; with any breaches reported to the FIHS IRT following FIHS incident reporting guidelines. Security-related events include, but are not limited to: • Port-scan attacks • Evidence of unauthorized access to privileged accounts • Anomalous occurrences that are not related to specific applications on the host. Ensure the ISSO keeps a detailed log of any security incidents in the incident log book.
18 ●	Ensure a process is in place so that corrective measures to be performed by network administrators are performed within 1 week. Process should indicate that problems will be brought to the attention of the ISSO immediately and that an electronic report of completion will be provided to the ISSO.
19 ●	Ensure a procedure is in place so that the ISSO will respond to FIHS IRT notices and Sara Scan reports with a report on corrective measures or false positives within 48 hours of notification. All responses will be carbon copied to the Chief of ITOS and the CIO.
	Operating System Install
20 ●	Ensure server name reflects its main function and follow the IBCR naming conventions of CRxxx or IBCRxxxx.
21	Ensure Server IP address is static and follows the IBCR address conventions.

●	
22 ●	Ensure the server NIC is set at 100 Full.
23 ●	Ensure IIS is not installed unless server is an approved web server.
24 ●	Ensure the administrator account is renamed. Following IBCR password conventions, use numbers and characters. Renaming the Administrator account will prevent hackers from breaking in.
25 ●	Ensure a dummy "Administrator" account has been created, disabled and made a member of the Guest group. Setting up a fake Administrator account, disabling it and placing it in the Guest group will prevent hackers from getting into the server and will also log the attempt.
26 ●	Ensure security Log files are set to no less than 16mb and enable over write. Log files are set to larger sizes to collect more information, overwrite ensures information is continually collected. Availability is the top priority so services can't stop. Other means will be used to attempt to determine attacks.
27 ●	Ensure that only domain admins have access permissions to the security event logs.
28 ●	Ensure Guest Account has a strong password and is disabled.
29 ●	Set Performance Options My Computer/Properties/Advanced Tab/Performance Options Set Foreground application performance boost to NONE
30 ●	Ensure Set Recovery Options is set to following options My Computer/Properties/Advanced Tab/Startup and Recovery Only write event to system log Automatically reboot Use Small Memory Dump Performance options are set so that servers evenly distribute resources to all services as high availability of critical services is a high priority.
31 ●	Check Boot.ini file for /sos at end of boot string so it displays process during boot-up. [boot loader] timeout=5 default=multi(0)disk(0)rdisk(0)partition(1)\WINNT [operating systems] multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft Windows 2000 Server" /fastdetect /sos

	The /sos tag in the BOOT.INI forces the boot-up process to display on the screen. This allows the administrator to view problems that occur doing boot-up. This may indicate impending problems or make troubleshooting easier.
32 ●	Ensure Logon Banner Displays – Check Local Security Policy ***** NOTICE ***** This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system. A logon banner provides warning that the user is entering a US Government system. Servers need to have logon banners in case of log on via Terminal Services or local access from staff.
33 ●	Ensure Logon Screen Saver is set with a 5-minute time out for all accounts. Logon Screen Saver ensures that the server will be locked after 5 minutes without input.
34 ●	Ensure that OS/2 and POSIX Subsystems have been removed. Ensure that the **\winnt\system32\os2** directory and all of its subdirectories have been deleted. Ensure the following registry entries have been removed via the Registry Editor: **Key:** HKEY_LOCAL_MACHINE\SOFTWARE **Subkey:** Microsoft\OS/2 Subsystem for NT **Entry:** delete all subkeys **Key:** HKEY_LOCAL_MACHINE\SYSTEM **Subkey:** CurrentControlSet\Control\Session Manager\Environment **Entry:** Os2LibPath **Value:** delete entry **Key:** HKEY_LOCAL_MACHINE\SYSTEM **Subkey:** CurrentControlSet\Control\Session Manager\SubSystems **Entry:** Optional **Values:** delete entry **Key:** HKEY_LOCAL_MACHINE\SYSTEM

	Key: HKEY_LOCAL_MACHINE\SYSTEM **Subkey:** CurrentControlSet\Control\Session Manager\SubSystems **Entry:** delete entries for OS2 and POSIX
35 ●	Ensure that all drives are NTFS. Settings/control panel/administrative tools/computer management/storage/disk management. Ensure that the built in EVERYONE group has been remove from the root of all drives and replaced with Authenticated Users or Domain Users as needed. Ensure that the correct permissions are allocated to sensitive data and application files and folders. Replacing EVERYONE with Authenticated Users in file and dir ACLs requires anyone trying to connect to the server to be an authenticated user.
	After OS Installation
36 ●	Update OS Ensure that the latest hotfixes and service packs are installed by running a Microsoft Base Analyzer scan and a STAT Analyzer scan. Ensure there is a process to scan and remediate server at least monthly. Also ensure there is a process to test hotfixes and service packs in a test environment before being rolled out to the production environment.
37 ●	Determine how often an ERD is made and ensure that it is stored in the fire proof safe, clearly labeled. Ensure that a backup of the registry is made along with weekly and incremental backups. Ensure that a base lining exercise is performed for the registry to identify unauthorized changes to the registry. Ensure that the reports generated by the baseline tools, such as Ecora are saved in a secure location with restricted access to the ISSO only.
38 ●	Ascertain if a security template is used. (NOTE: At this time a security template is not used – this has been included to remind the ISSO to keep working on using Templates to aid the server security process.) Ensure that the customized IBCR template is used. The templates and their system use are as follows: • basicwk.inf default workstation • basicsv.inf default server • basicdc.inf default domain controller • compatws.inf Compatible workstation or server • notssid.inf Terminal services backward compatibility • securews.inf Secure workstation or server • hisecws.inf Highly secure workstation or server • securedc.inf Secure domain controller • hisecdc.inf Highly secure domain controller If changes to the template have been made ascertain if the changes are plausible.

	Determine how often security analysis is performed and what steps are taken to correct the security weaknesses. Ensure that the template is stored on CD or floppy and an ISSO accessible only directory on the network. Ensure that a baseline analysis is maintained to ascertain the progress made in security configuration.
39 ●	Security Analysis (When Security Template is put in place) Run the security analysis. Start/Run/type mmc/OK. On the console menu choose Add/Remove Snap-in. In the Snap-in window choose add, choose Security Configuration and Analysis and click add. Right click on Security Configuration and Analysis, open database, type in name for database, click open. In the Import template window, select the IBCR custom template and click open. Right click Security Configuration and Analysis and select Perform analysis now and OK. You can then either review the results at the default location or alternatively export it in text format.

40
●
	Analyzing the results of the Security Analysis (When Security Template is put in place). The Hercules Mitigation tool and Microsoft Base Analyzer will both scan and indicate some of the settings discussed below.
	A tick appears next to the item that complies with the database and a red cross next to the one that does not.
	The results are split into the following areas:
	• Account Policies: Ensure that at a minimum the following settings are present:
	  • Password Policy
	  ❑ Password History = 10 previous passwords
	  ❑ Maximum password age = 180 days
	  ❑ Minimum password age = 1 day
	  ❑ Minimum password length = 8 characters
	  ❑ Password must meet complexity requirements = enabled
	  ❑ Store passwords using reversible encryption = disabled
	  • Account Lockout
	  ❑ Account is locked out for 30 minutes.
	  ❑ Account lockout threshold = 5 invalid passwords
	  ❑ Reset account lockout counter after 30 minutes
	• Local Policies
	  • Audit Policy
	  ❑ Audit account logon events – Success and Failure
	  ❑ Audit account management – Success and Failure
	  ❑ Audit directory service access – Success and Failure
	  ❑ Audit logon events – Success and Failure
	  ❑ Audit object access – Success and Failure
	  ❑ Audit policy changes – Success and Failure
	  ❑ Audit privilege use – Success and Failure
	  ❑ Audit Process tracking – Success and Failure
	  ❑ Audit System events – Success and Failure

- User Rights
  - ❑ Act as part of the operating system: Disable
  - ❑ Add workstations to the domain: System admin
  - ❑ Backup files and directories: backup operators & Admin.
  - ❑ Change the system time: Disable, system admin. only
  - ❑ Create a token object: system admin
  - ❑ Create permanent shared objects: system admin
  - ❑ Debug programs: Restrict to system admin
  - ❑ Deny logon as a batch job: Enable
  - ❑ Deny logon as a service: Enable
  - ❑ Force shutdown from a remote system: Enable
  - ❑ Generate security audits: Enable
  - ❑ Increase scheduling priority: Restricted to system admin
  - ❑ Load and unload device drivers: system admin
  - ❑ Lock pages in memory: Restricted to system admin
  - ❑ Logon as a batch job: Disable
  - ❑ Logon as a service: Disable
  - ❑ Manage auditing and security log : system admin
  - ❑ Restore files and directories : system admin & backup operators
  - ❑ Shutdown the system: Restrict to system admin
  - ❑ Synchronize directory service data: system admin
  - ❑ Take ownership of files or other objects : system admin
- Security Options
  - ❑ Allow system to be shutdown without having to logon: Disable
  - ❑ Amount of idle time allowed before disconnecting a session: Maximum 2 hours
  - ❑ Automatically Log Off Users When Logon Time Expires (Local): Enable
  - ❑ Digitally Sign Client Communication (When Possible): Enable
  - ❑ Digitally Sign Server Communication (When Possible): Enable
  - ❑ Audit the access of global system objects: Enable
  - ❑ Audit use of backup and restore privilege: Enable
  - ❑ Clear virtual memory pagefile when system shuts down: Enable
  - ❑ Disable CTRL+ALT+DEL requirement for logon: Disable if using smart cards
  - ❑ Don't display last username in logon screen : Enable
  - ❑ LAN Manager authentication level: Should be NTLMv2.
  - ❑ Message text for users attempting to log on: Enabled with the legal notice. See # 32.
  - ❑ Message title for users attempting to log on: Enabled with WARNING title. See # 32.
  - ❑ Number of previous logons to cache in case of domain controllers not available: one.
  - ❑ Prevent system maintenance of computer account password: Disable
  - ❑ Prevent users from installing print drivers : Enabled
  - ❑ Prompt user to change password before expiration : 14 days
  - ❑ Recovery console: Allow automatic administrative logon: Disable
  - ❑ Recovery console: Allow floppy copy and access to all drives and all folders: system administrator

- ❑ Rename administrator account : Enabled
- ❑ Rename guest account : Enabled
- ❑ Restrict CD ROM access to locally logged on user only : Enabled
- ❑ Restrict floppy access to locally logged on user only: Enabled
- ❑ Secure Netlogon channel: "Digitally Sign" & "Digitally Encrypt" when possible
- ❑ Shut down system immediately if unable to log security audits : Disable
- ❑ Send Unencrypted Credentials for Third Party SMB Servers: Disabled
- ❑ Configure Smart Card Removal Behavior: Lock Workstation
- ❑ Strengthen default permissions of global system objects e.g. symbolic links : Enabled
- ❑ Configure Unsigned Drive Installation: "Warn but allow installation."
- ❑ Configure Unsigned Non-Driver Installation: "Warn but allow installation."

- Event Log
  - Maximum log size for application, security and system log: minimum of 2MB, 16MB, 2MB respectively.
  - Restrict guest access to application, security and system log = enabled
  - Retain application, security and system log should be in terms of the security policy
  - Shutdown the computer when the audit log is full = disable.
- Restricted Groups
  - Administrators: Ensure only authorized users are members
  - Backup Operators: Ensure only authorized users are members
  - Guests: Ensure "fake" administrator is member.
  - Power Users: Ensure that no-one is a member of this group.
  - Replicator: Ensure that no-one is a member of this group.
  - Users: Ensure only the group domain users is a member of this group.
- System Services: Ensure that only those services, which are necessary for the server to perform its function, are enabled. All other services must be disabled. View the security relating to each enabled security element and ensure that only the administrator has full access to enable a service. The following services should be disabled:
  - ❑ Telnet
  - ❑ Others to be added as discovered
- Registry: Ensure that the following requirements are met
  - Legal notice enabled
  - Don't Display Last Username
  - Disable caching of logons
  - Disable floppy drives and hide drive letters
  - Print drivers are secured
  - Permissions on winreg key should be set to full access to system administrators and system account only.
  - Restrict anonymous access

	• Enable full privilege auditing • The permissions on the registry should be restricted to full access to the administrator and system accounts. • File System: Ensure that all partitions/drives are NTFS.
	IIS
41 ●	If Server is approved for IIS Ensure that unnecessary protocols especially NETBIOS is removed. Ensure that the TCP/IP configuration has the Disable NETBIOS over TCP/IP option enabled. Ensure that there are vulnerability scans with FIHS Sara Scan, STAT Analyzer and Microsoft's Base Analyzer to ensure that the most recent hot fixes are installed. Ensure that unnecessary ODBC connections are removed. Ensure that unnecessary services are removed. Services that should be set to automatic on IIS are as follows: • DNS client • Event log • Logical disk manager • Network connections • Protected storage • RPC • SAM • WMI • WMI Driver extensions Services that should be set to manual are as follows: • Logical disk manager administrative service • IIS Admin service • WWW publishing service Services that are not necessary on a web server are as follows: • Alerter • Clipbook server • Computer browser • DHCP client • Messenger • Netlogon • Network monitor agent • Simple TCP/IP services • Spooler • NetBIOS interface • TCP/IP NetBIOS helper • NWLink NetBIOS Ensure that each time a change in service configuration is made, it is tested. Ensure that the web site is stored on a different partition to the OS. Ensure that the following tools/utilities are renamed/deleted or have NTFS permissions set appropriately:

- Xcopy.exe
- At.exe
- Regeditr.exe
- Cacls.exe
- Regedt32.exe
- Cmd.exe
- Regini.exe
- Cscrpit.exe
- Regsrv32.exe
- Debug.exe
- Rexec.exe
- Edlin.exe
- Rsh.exe
- Finger.exe
- Runas.exe
- ftp.exe
- runonce.exe
- issync.exe
- telnet.exe
- nbtstat.exe
- tftp.exe
- net.exe
- tracert.exe
- netsh.exe
- tskill.exe
- poledit.exe
- wscript.exe
- rcp.exe

Ensure that the following registry key changes are made

- HKLM\System\currentcontrolset\control\lsa\restrict anonymous is set to a value of 1.
- Restnullsessaccess is set to a value of 1
- HKLM\System\currentcontrolset\services\tcpip\parameters\synattackprotect is set to a value of 2.

Ensure that TCP/IP or Routing and Remote Access Service filtering is enabled.
If anonymous authentication is used, ensure that the IUSR_Computername account is disabled and a new account created for anonymous access. Ensure that the account has the right to access this computer from the network disabled.
Ensure that the account is disabled from logging on locally.
Only a public web service is authorized to have anonymous authentication, all other web services must be using NT Challenge.
Securing the metabase:

- Ensure that all HTTP/FTP root folders are removed from %systemroot% volume
- Ensure that the registry key that determines the Metabase location is secured.
- Ensure that all failed access attempts to edit the metabase is logged.
- Ensure that the lissync.exe file is deleted from %systemroot%\system32\inetserv folder
- Ensure that the permissions for the metabase are set to administrators and system full control.
- Ensure that a backup of the metabase is made.
- Ensure that all failed attempts to the metabase backup folder are logged.
- Ensure that the permissions on the metabase backup folder are set to administrator and system full control.

Ensure the Microsoft IIS Lockdown and URL Scan tool has been installed.
Ensure that the SMTP, NNTP and IIS Admin Web Services are removed; these

	are not used in the IBCR environment (only the intranet server is authorized to run SMTP.) Ensure the FTP service is removed (only the public web server is authorized to run the FTP Service. Ensure documentation is not installed as it leaves dangerous script examples. Ensure that the permissions on the \adminscripts folder and %systemroot%\system32\cscript.exe are set to administrator full control. Ensure that all failed attempts to access the \adminscripts folder are logged. Ensure that the metaedit.exe and metautil.dll are moved from \program files folder to %systemroot%\system32\inetserv folder and that the start menu shortcut is adjusted. Ensure auditing is enabled on all scripts and bin folders as well as to directories containing files to be published as part of the web site. Ensure that the Internet guest account is disabled. Ensure that unnecessary file types are disabled. Ensure that the appropriate read/write/execute permissions are set on each folder. Ensure that directory browsing is disabled. Ensure that the connection time out for FTP is set to 300 seconds. Ensure that a welcome message stating limitations is added to the messages tab for ftp. Ensure that the appropriate permissions have been set for the ftp directories.
42 ●	Ensure that the Winnt folder has permissions set to allow only the administrator and system users full control.
43 ●	SNMP Security Ensure that Private and Public Community Strings are not defaults and are complex. Ensure that Send authentication trap is set whenever authentication fails. Ensure that only authorized hosts are added to the community. Ensure that appropriate permissions are allocated to the host to process SNMP packets. Path: Computer Managemernt/Serivces/SNMP AuthenticationTrap: SNMP/Action/Properties/Security Ensure that the permissions on the SNMP registry keys are as follows: • HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters • Permissions: Administrators, System, Creator Owner:Full
44 ●	Trust relationships Review the trust relationships, the only trust should be with the FIHS domain.
45 ●	Resource Kit Tools Appsec.exe Ensure that only authorized users are allowed to access the applications on the network to perform their job functions. Gpotool.exe

	Ensure that the Gpotool.exe is run to check consistency of policies across domain controllers and to provide information about corrupt policies. Tracelog.exe Ensure that tracelog.exe is run for event tracing.
46 ●	Ensure Remote Access Services are Removed. Access is only allowed via Administrative Terminal Services over FIHS sponsored VPN or dial-up.
47 ●	Terminal Services Ensure that Terminal Services is set for Administrative use only Ensure that data encryption level is set for data transmissions between clients and the terminal server at HIGH: 128bit • High: 128 bit. Encrypts data to and from server. Ensure that users are always prompted for a password before logging onto the server. Ensure that guest access is disabled. Ensure that the correct permissions have been allocated to the various users. The permissions are as follows: • Query information • Set information • Reset • Remote control • Logon • Logoff • Message • Connect • Disconnect • Virtual channels Ensure that auditing is enabled for permissions
	After Placing Server on Network
48 ●	Ensure Net IQ Security Manager Client is installed and set logs to be monitored from the Security Manager Console. (Not ready for implementation yet.) Net IQ Security Manager will provide the ISSO with a central security console to assist in auditing and monitoring all servers.
49 ●	Ensure that for critical servers Tripwire is installed. (Tripwire has not been implemented as of yet). Tripwire is a host-based intrusion detection that monitors files for alterations.
50 ●	Ensure Virus Software is installed, dat files are up to date and it is set to be monitored by E-Policy.
51 ●	Ensure Ups client (Network Version) is installed. Provides backup and clean power for servers.
	Auditing New Servers
52	If Server is a new addition ensure that auditing and baseline tools have been run

●	and recorded. • Ensure server is scanned with St. Bernard's Update Expert and patched as needed. • Ensure server is scanned with CIS scoring tool using custom template. • Ensure server is scanned with Microsoft Baseline Security Analyzer. • Ensure Active Ports results are captured; non-standard ports are documented and saved as baseline. • Ensure snapshot of registry is taken. • Ensure server is scanned with GFiLANguard and save report. • Ensure server is scanned with Ecora Configuration Auditor report • Ensure server is scanned with Stat Analyzer to determine any remaining vulnerabilities. • Ensure vulnerabilities are mitigated with Hercules – report results and save electronic version of report. • Ensure Self Sara Scan was run and report generate. All reports will be filed in an electronic directory under the servers name to be used as the basis for future auditing or incident handling. Access to this directory will be limited to security staff.
53 ●	This Auditing report will be filed in the electronic directory under the server's name. Access to this directory will be limited to security staff.

Note: The audit checklist contains some controls that are not reflected in the Server Security Procedure included in Appendix B. As the author was researching for this paper the sample audit checklists had controls the author felt should be added to the procedure. The procedure list is currently undergoing editing and was not completed for this paper to reflect these changes.

Step 5 – Conduct the Audit

The ideal format for the audit would be someone other than the ISSO or network staff would conduct the audit. This ensures that the person performing the audit does not have the temptation to "fix" or "fudge" the audit to ensure it shows complete or high compliance. The IBCR does not have an audit staff. For this exercise the author audited a new server placed on the network. This server was installed by a co-worker using the Server Security Procedures. The check list was printed out and the author went through each step taking notes and checking off controls for compliance.

Step 6 – Produce a Report

The Audit report consists of several sections. The report conveys the results of the audit and attempts to discover the cause for audit exceptions and makes recommendation on remediation or mitigation of audit exceptions.

Remediation and mitigation are always based on Best Practice, Policy and Procedure. An Executive Summary wraps up the report at a high level for Executive Management. The information needed to garner support for remediation and mitigation activities is placed in the Executive Summary. The goal is to ensure that exceptions are taken care of at the specific level management is comfortable with.

1. Executive Summary
    a. Statement of purpose
    b. Explanation of Scope
    c. Description of Methods
    d. High level over view of findings
2. Detailed Findings
    a. Audit Exceptions
        i. Root Cause – What Really went wrong
    b. Remediation: Recommendations on how to fix it
        i. Based on Best Practice
        ii. Based on Policy
        iii. Based on Procedure
    c. Mitigation – If cannot be fixed, recommend How to reduce Risk
        i. Based on Best Practice
        ii. Based on Policy
        iii. Based on Procedure
3. Summary

Executive Summary

Statement of purpose

On Feb 19, a newly installed server, IBCRfileserver, was audited for conformance to IBCR Server Security Policy and Procedures. The goal of the audit was to first, ensure the IBCRfileserver does not introduce any security risk to the IBCR network and secondly to evaluate the Server Security Policy and Procedure. The evaluation of Policy and procedure looks for compliance by network staff that have the responsibility for installing servers as it is necessary to ensure policy is being followed. If there are instances where policy is not followed it is important to discover the root cause. The policy may be weak; staff may not understand the need or the procedure may not include enough detail to complete the steps. The audit will result in a report of any audit exceptions and recommendations on remediation or mitigation based on policy, best practice or procedure. Application of the recommendations will result in better policy, more detailed, easier to follow procedures and ensuring that IBCRfileserver is secure and does not pose a risk to the IBCR network.

Explanation of Scope

The IBCR depends heavily on a network client/server environment composed of Windows 2000 servers which act as database servers, web servers, file servers and more. In order to protect IBCR resources and to ensure servers are hardened and protected from attack before they are attached to the network a Server Security policy and installation procedure was created. This audit will occur randomly after a new server is added to the network to ensure policy and procedure is being followed. This same audit checklist will be used to randomly audit older servers to ensure that compliance with vulnerability assessment and remediation is occurring on a timely basis and to ensure configuration changes are not weakening the initial security controls placed on the server.

Description of Methods

The auditor performed this audit at the console of the IBCRfileserver with the checklist and paper to take notes in hand. The auditor had administrative access to the machine to ensure that all settings are available to the auditor during the audit. A network administrator was not present for this audit, notes on questions the auditor wanted to ask the administrators were taken.

High Level Over View of Findings

The auditor found that many of the controls were not being followed. There were some unfavorable conditions that contributed to the high failure rate. The Server Policy and procedure being audited is new, the policy is in review and currently in flux as the IBCR works on its security stance and applying best practices that fit. The procedure has only been applied to three servers and staff has not had time to review the procedure and ensure that all steps fit the goal of reducing the risk of attaching vulnerable servers to the network. The policy has being approved which often leads to inadequate implementation. Staff may feel that some steps are not necessary and in the absence of policy to enforce their application, along with pressure to complete server installation will usually lead to skipped processes. The IBCR is currently moving from a lax security stance to a strong security stance and staff has to change their outlook on security.

The good news is that most of the audit exceptions can be easily remediated by revisiting the policy and procedure. Making sure all the steps fit the security stance required and then applying the policy to all further server installs. At that point staff will be required to "get with the program." The auditor and ISSO looks forward to this report opening up dialog between IT management to assist in drafting policy and procedure to ensure the perfect fit for the IBCR. IBCR IT management may wish to consider security training for network administration staff to assist the ISSO.

Detailed Findings

Audit Exceptions (reference checklist for # of steps)

1. Server Configuration Guide not available. The institute has only started considering IT security policy in the last year. Process and policy is new and just being implemented.
Remediation: As per policy create a Server Configuration Guide. Once complete, establish a process for updating and periodically ensure review by ISSO and Chief of ITOS.
2. Exceptions to Baseline not posted in LAN Room or available in central Network location.
No exceptions have been identified at this point.
3. Server has been approved but no request is on file and not all information is captured as required by policy.
Remediation: As per policy create a central location for collection of this information on the network and secure access to ISSO only. Ensure each server has a log book and this information is captured. Get policy approved and follow policy.
4. Server not registered with IBCR asset Management
Remediation: Asset Management controls should be set up as per policy
5. No change management procedures are in place.
Remediation: Design procedures as per policy

General Configuration Guidelines

7. Not all Unnecessary Services Removed
Mitigation: Best practice suggests removing Indexing Service. Sometimes it is not always adequate that services are not started. Network staff needs to research more into this area and try to product a list of services by server type. Add this list to the Server Security procedure.
8. Access Control
Local disk security set to EVERYONE full control.
Mitigation: As per policy and best practice set at least to Authenticated users. Network staff need to document network and attempt to apply least privilege access to the network. This will require a new way of looking at access and will take some time.
9. Weekly Vulnerability Scans.
Procedure not complete and in place.
Mitigation: As per policy set vulnerability scan process to ensure weekly scan and remediation time table.
10. Terminal Client Access
Windows default is to allow all accounts access. Guest account has access to terminal services and remote control and the fake Admin account has Terminal service access turned on.
Remediate: Turn off terminal service access. Network staff and ISSO need to research into best practice and find a way to remove default

access to terminal service or a way to use NT groups to control access to terminal service.
13. Ensure Net Admin staff performs admin functions with private administrative account rather than general admin account.
Remediation: No way to monitor this at this time. This will require a stance change. The ISSO has made some recommendations on changes in how administration accounts are handled. IT management needs to look into IT password policy and procedure,
14. Server not scanned with Sara Scan yet
Remediation: As per policy scan with Self Sara Scan and address any vulnerabilities.

Monitoring

16. Size of Security log only set to 2MB
Remediate: Size not large enough to keep 2 weeks worth of data. As per policy log should be increased to 16MB. Logs should be watched to ensure size is adequate to fulfill policy.
17. Log monitoring software not in place.
Remediate: Net IQ software should be implemented as soon as possible and all server logs monitored by its central console. Policy needs to be written to ensure that network admins are aware of the need to report incidents or questionable logs to the ISSO. A formal incident handling procedure should be put in place and communicated to all admins. The ISSO does keep a detailed log book of all incidents.
18. A process to allow for 1 week turn around on corrective measures by network admin if vulnerabilities are discovered by scanning or from email notices such as Cert, etc. are not in place.
Mitigation: Software to assist in scanning for vulnerabilities and mitigating problems has been installed and will be implemented shortly, once in place ensure policy addresses this need.

Operating System Install

23. IIS installs by default and was removed from this system but the Inetpub folder still remains.
Remediation: Remove Inetpub and its subfolders as per procedure.
25. Dummy admin account created and disabled but is currently a member of USERS and is set to user must change password on next logon.
Remediation: Set to user cannot change password, password never expires, ensure IBCR standard strong password is used. Remove from USERS group and place in GUEST as per procedure.
26. Security log file is only set to 2MB
Remediate: See step 16 above.
30. Set for Complete memory dump. This takes time before machine can reboot in the event of a crash. Availability is important and normally staff never analyzes memory dumps

Remediate: Set to small as per procedure.
32. Log on banner not displayed
Remediate: add log on banner as per policy.
34. OS/2 and Posix Subsystem not removed
Remediate: Remove OS/2 and Posix Subsystem as indicated in procedure.
35. Everyone has full control at root of local hard drives.
Mitigate: Replace Everyone with authenticated users as prescribed by best practice or domain users as needed.
36. Microsoft updates performed. Machine was scanned but there has not been time to remediate scan results. Process for monthly or weekly scans is in process of being created. No process to test hotfixes described.
Mitigation: Setup scanning process. As suggested by Best practices determine best way to test hotfixes.
37. No information on ERD available.
Remediate: Must discuss with Network admin and determine best practice. Possibly backups cover this?
38. Security templates not in use at this time.
Mitigate: The ISSO wants to apply templates to assist in the installation of new servers. Applying controls by hand is difficult. Time to research templates is necessary. Also the IBCR has just moved to Active directory. Servers are being migrated from NT to Windows 2000 to take advantage of new capabilities. Active Directory will make templates more important.
40. Template not in use so analysis was performed by hand as settings need to be set as prescribed in procedures.

No password polices set

Remediate: Set as per procedure

No account lockout policies set

Remediate: Set as per procedure

Local Audit Policies

- Audit directory service access not set
  Remediate: Set to success, failure as per procedure

Local Policies – User Rights

- Act as part of operating System – IBCRsystem account
  Mitigate: Research best practice. Perhaps procedure needs to include this rather than disable this account
- Change system time
  Remediate: Remove power users as per procedure
- Check for appropriateness (Best Practice) of IBCRService account having access to Increase scheduling priority, load & unload device drivers, lock pages in memory, log on as a service, restore files and directories.
- Shut down the system
  Remediate: Remove backup operators and power users as per procedure

Local policies – Security options

- Audit access of global system objects
  Remediate: Enable as per procedure
- Disable Ctrl+Alt+Del requirement for logon
  Remediate: Since not using smart cards – enable as per procedure
- Clear virtual memory pagefile when system shuts down
  Remediate: As per procedure enable
- Do not display last log on
  Remediate: As per procedure enable
- LAN Manager authentication level
  ICBR has not moved to a Windows 2000 only mode, as per procedure this should be set to use NTLMv2 session security if negotiated. Once all servers are Windows 2000, this should be revisited for best practice.
- Warning banner needs to be placed
  Remediate: Add banner as per procedure
- Number of previous logons to cache
  Remediate: Set to 1, procedure had set to 10, this should be changed.
- Restrict floppy access to locally logged on user only
  Remediate: As per procedure – enable

42. Winnt is insecure
Remediate: Remove access rights for everyone, power users, and users as per procedure.
43. SNMP
Mitigate: Research for best practices. Consult with Network admins to ensure policy for SNMP makes sense then apply agreed upon procedures
45. Resource Kit Tools
No steps here have been applied, need to study these and make sure they will aid in the goal of server security.
47. Terminal Service - Data encryption currently set to medium.
Mitigate: Set encryption to high. Terminal services needs to be addressed from an enterprise function to ensure security. Research best practices.

After Placing Server on Network

48. Net IQ is not yet implemented
Remediate: Implement Net IQ as per policy.
49. Tripwire is not yet implemented.
Remediate: Implement Tripwire as per policy.
50. Virus software not installed.
Remediate: Install Virus software immediately.

Auditing New Servers

Since this is a new server these services should been run as soon as possible after the server is placed on the network. Due to time limit for this paper and snow these have not been done yet

Scan with Update Expert
Scan with CIS Scoring tool. No template
Scan with MS Baseline Analyzer
Scan with Active Ports, explore non-standard ports
Take snapshot of registry
Scan with GFiLANguard
Scan with Ecora Configuration Auditor
Mitigate vulnerabilities in Hercules
Scan with Sara Self Scan
A secure location needs to be implemented for auditing files and reports.

Remediate: Run scans and generate reports and place in a secure location for future auditing.

Summary

The auditor found that many of the controls were not being followed. The ICBR is moving from a lax security state to a more controlled security environment. There will be growing pains with new procedures and policies to implement. The Server Security policy is still under review. The ISSO and network administrators are learning how to apply security principles in their environment. The auditor wants to point out that this exercise is designed to assist in filling in the holes and tightening procedures to ensure the network resources are adequately protected and not to point out staff work habits or lack of security knowledge. Auditing allows management to test for compliance and to discover were financial, human and knowledge resources need to be applied.

Appendix A – Server Security Policy
(Cornwell 42)

Server Security Policy
1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and operated by the GIAC Institute of Basic Cellular Research (IBCR). Effective implementation of this policy will minimize unauthorized access to the GIAC Institute of Basic Cellular Research (IBCR) proprietary information and technology.

2.0 Related Documents
Place links to Server Configuration Guide, Exception Policy, and Internet DMZ Equipment Policy here.

3.0 Background
The IBCR IT branch has seen the network grown from 5 servers to over 40 servers in use today. The network administration staff had responsibility for the help desk up until approximately three years ago. Over the last three years network administration staff have been training contractors in help desk procedure and installing new applications and servers. Network staff has not had time to document installation procedures. With the federal government's attention turning to increased security, it has become necessary to implement baselining procedures and to standardize server installation to ensure that the appropriate security is in place to protect the institute's information resources.

4.0 Scope
This policy applies to server equipment owned and operated by the GIAC Institute of Basic Cellular Research (IBCR), and to servers registered under any GIAC Institute of Basic Cellular Research (IBCR) -owned internal network domain.

This policy is specifically for server equipment on the internal Institute of Basic Cellular Research (IBCR) network. For secure configuration of server equipment external to the Institute of Basic Cellular Research (IBCR) on the DMZ, refer to the *Institute of Basic Cellular Research (IBCR) Internet DMZ Equipment Polic*y.

5.0 Policy

5.1 Ownership and Responsibilities
All internal servers deployed at the Institute of Basic Cellular Research (IBCR) are owned by the IT Operations Section (ITOS) of the IBCR's Information Resource Management Branch. The network administration group is responsible for all server installation, administration and compliance. The ISSO is responsible for development of security guidelines, auditing of servers and compliance testing.

5.2 Action

A Chief of ITOS approved server configuration guide must be established and maintained by the network administration group, based on IBCR business needs and approved by the Information Systems Security Officer (ISSO). The network administration group and ISSO will monitor configuration compliance. An exception policy will be written by the ISSO and approved by the Chief of ITOS. The exception policy will be posted in the LAN room and made available from a central network location. The network administration group will establish a process for changing and updating the configuration guides. The process will include reviews by the ISSO and approval by the Chief of ITOS.

- Servers must be registered in the IBCR asset management system along with informing the ISSO of deployment of new servers. The following information is required to positively identify the server:
    - Server name, URL and IP address, LAN Tap no.
    - Name of Installer, person with knowledge of apps, Name of backup staff
    - Location of Backup service (Sans or Traditional)
    - Hardware, Operating System/Version
    - Who requested, who approved
    - Main functions and applications, if applicable
    - Special considerations
    - Who needs administrative access
- Information in the IBCR asset management system must be kept up-to-date along with changes forwarded to ISSO.
- Configuration changes for production servers must follow the appropriate change management procedures.

5.2.1 General Configuration Guidelines

- Operating System configuration should be in accordance with approved ISSO and FIHS security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services will be protected through NT/Windows Domain access-control methods. Administrative access will be limited to IT staff with direct responsibility for the server. Access should be logged.
- Remote access will only be allowed via FIHS provided VPN or dial-in service. Contractors who need access must be cleared for administrative accounts or must be monitored by administrative staff while accessing the server.
- Terminal Client access must be approved by ISSO or Chief of ITOS.
- The ISSO must respond to notices of necessary security patches within 48 hours or must inform the Chief of ITOS if application would interfere with business requirements.
- The ISSO will scan all servers with a vulnerability tool weekly and inform the Chief of ITOS of reported vulnerabilities and apply patches and fixes to

all high priority vulnerabilities unless application would interfere with business requirements.

- Always use standard security principles of least required access to perform a function.
- Network administrative staff will perform all admin functions on servers with their private administrative account rather than the general administrative account.
- Before being put into production or after a major configuration change servers will be scanned by the ISSO with the institute's vulnerability scanner and with FIHS' self Sara Scan.
- Servers will be physically located in the LAN room and the LAN room will be closed and locked so that access is only via cipher lock.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- This policy applies to all installations of Windows/NT/XP servers, even those used for development and testing.

5.2.2 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 2 weeks and collected and maintained by a central logging program.
    - Daily incremental tape backups will be retained for at least 6 months.
    - Weekly full tape backups of logs will be retained for at least 6 months.
    - Monthly full backups will be retained for a minimum of 6 months.
- The ISSO and Network administrators will be trained in the use of tools installed to assist in monitoring the network for possible attack. It will be the responsibility of the ISSO and a backup to monitor logs of host-based intrusion systems or to respond to alerts.
- Security-related events will be reported immediately to the ISSO or Chief of ITOS. The ISSO will review logs and report incidents to the Chief of ITOS. Corrective measures will be prescribed as needed; breaches will be reported to the FIHS IRT following the FIHS incident reporting guidelines. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.
- The ISSO will keep a detailed log of any security incidents in the incident log book.
- Corrective measures to be performed by network administrators must be performed within 48 hours. Problems will be brought to the attention of the ISSO immediately. Report of completion will be provided electronically to the ISSO.

- The ISSO will respond to FIHS IRT notices and Sara Scan reports indicating attacks or vulnerabilities with a report on corrective measures or false positives within 48 hours of notification. All responses will be carbon copied to the Chief of ITOS and the CIO.

5.2.3 Compliance

- Audits will be performed on a regular basis by the ISSO.
- Audits will be performed on newly installed servers and upon major configuration changes.
- Audits will be managed by the ISSO in accordance with the *Audit Policy*. The ISSO will present the findings to Chief of ITOS for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal IBCR Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

8.0 Revision History

This policy was revised on Oct 13, 2002 to fit the GIAC Institute of Basic Cellular Research.

9.0 Signature

This policy is approved for use by: CIO's signature Date:

Appendix B – Server Security Procedure
(Cornwell 42)

Server Security Installation Procedure

Server Installation will be performed by IBCR network administration personal in the IBCR LAN room in response to an official request from the Chief of ITOS. Servers are not to be located in accessible office areas. The following information must be submitted in writing to the ITOS Chief with a copy provided to the ISSO before installation begins.

- Need for the server and the original request
- Hardware requirements
- Software requirements including OS/Version
- List of applications, main functions and any special needs/concerns
- Who will need access, at what level and reasons
- Any special considerations
- Is service considered to be critical
- Location of Backup service (Sans or Traditional)
- Name of Installer and backup contact
- Name of staff responsible for applications if not the same as above
- Server name, URL/domain name, IP address & LAN tap no.

Installation Check List (DRAFT)

Installation should occur off network if possible. If not, then immediately after OS installation install all patches from the Microsoft Update site. Do not leave the machine unattended until after all patches have been installed. If there is a time lag between the time the operating system is installed and the time patches can be installed, remove the machine from the network for that period. Immediately after patches are updated perform a Self Sara Scan. Work with the ISSO to fix any vulnerabilities before continuing the install process. Until this is done, do not leave the machine on the network unattended.

<u>Operating System Install</u>

1. Run Compaq Smart Start (for Compaq Servers)
2. Install Windows 2000 Server from CD
3. Server name should reflect its main function and be approved by the ITOS Chief and follow the IBCR naming conventions
4. Set static IP address
5. Configure NIC 100 Full.
6. Use only NTFS file system
7. Do not install IIS unless approved
8. Rename the administrator account. Follow IBCR password conventions, use numbers and characters.
9. Create a dummy “Administrator” account, disable it and make it a member of the Guest group.

10. Enable network lockout of the Administrator account. Use PASSPROP.EXE from the Resource Kit.
11. Set Log files to 80mb and enable over write.
12. Set domain admin permissions on the security event logs.
13. Disable Guest Account.
14. Set Performance Options
    My Computer/Properties/Advanced Tab/Performance Options
    Set Foreground application performance boost to NONE
15. Set Recovery Options
    My Computer/Properties/Advanced Tab/Startup and Recovery
    Only write event to system log
    Automatically reboot
    Use Small Memory Dump
        Edit Boot.ini file so it displays process during boot-up.
        Add /sos to end of boot string in BOOT.INI file
        Do not change the line marked "default="

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft Windows 2000 Server" /fastdetect /sos
```

16. Enable Auditing

Event	Level of Auditing
Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Failure
Policy change	Failure
Privilege use	Failure
System events	Success, failure

17. Replace the EVERYONE group on file ACL's with Authenticated Users.
18. Display log on banner

***** NOTICE *****

This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person,

whether authorized or unauthorized, constitutes consent to these terms.
There is no right of privacy in this system.

19. Set Logon Screen Saver with a 5-minute time out for all accounts
20. Apply Windows Server Gold template (when available)
21. Remove the OS/2 and POSIX Subsystems
    Delete the **\winnt\system32\os2** directory and all of its subdirectories.
    Use the Registry Editor to remove the following registry entries:

Key:	HKEY_LOCAL_MACHINE\SOFTWARE
Subkey:	Microsoft\OS/2 Subsystem for NT
Entry:	delete all subkeys
Key:	HKEY_LOCAL_MACHINE\SYSTEM
Subkey:	CurrentControlSet\Control\Session Manager\Environment
Entry:	Os2LibPath
Value:	delete entry
Key:	HKEY_LOCAL_MACHINE\SYSTEM
Subkey:	CurrentControlSet\Control\Session Manager\SubSystems
Entry:	Optional
Values:	delete entry
Key:	HKEY_LOCAL_MACHINE\SYSTEM
Subkey:	CurrentControlSet\Control\Session Manager\SubSystems
Entry:	delete entries for OS2 and POSIX

22. Table of settings – apply the following settings

Configuration Setting:	Recommended:
Configure the Account Policy In Local Security Policy under Administrative Tools.	8+ characters for passwords. Minimum password age: 1day Password history 24 Require complex password Enable account lockout to 4 hours after 5 failures and reset after 4 hours
Secure the Administrator and Guest Accounts	Rename accounts and assign 14 character complex passwords. Disable Guest.
Customize Security Options	
Additional Restrictions for Anonymous Connections	"No access without explicit anonymous permissions."
Allow System to be Shut Down Without Having to Log On	Disable
Audit Use of Backup and Restore Privilege.	Enable
Automatically Log Off Users When Logon Time Expires (Local)	Enable
Digitally Sign Client Communication (Always/When Possible)	Enable "When Possible."
Digitally Sign Server Communication	Enable "When Possible."

Configuration Setting:	Recommended:
(Always/When Possible)	
Do Not Display Last User Name in Logon Screen	Enable
LAN Manager Authentication Level	At least 2
Message Text/Title for users attempting to Logon	Use FIHS standard warning banner – see step 17 above
Number of Previous Logons to Cache (if Domain Controller is Not Available)	10
Prevent System Maintenance of Computer Account Password	Disable
Prevent Users From Installing Print Drivers	Enable
Prompt User to Change Password Before Expiration	14 Days
Recovery Console: Allow Automatic Administrative Logon	Disable
Recovery Console: Allow Floppy Copy and Access to All Drives and Folders	Disable
Restrict the CD-ROM and Floppy Drive access to locally logged on user only	Enable
Secure the Netlogon Channel	"Digitally Sign…" and "Digitally Encrypt" when possible.
Send Unencrypted Credentials for Third Party SMB Servers	Disable
Configure Smart Card Removal Behavior	Lock Workstation
Strengthen Default Permissions of Global System Objects	Enable
Configure Unsigned Driver Installation Behavior	"Warn but allow installation"
Configure Unsigned Non-Driver Installation Behavior	"Warn but allow installation"

23. Install all Service Packs and Updates from Microsoft.com
24. Scan with St. Bernard Update Expert
25. Run Microsoft Baseline Security Analyzer, save the report.

Installation of Support Software

1. If not already place server on network.
2. Configure Additional Drive Partitions.
3. Install Compaq Smart Start
4. Install SNMP for Compaq Insight Manager.
5. Set Community string name as xxxxxxxx and remove public community name.
6. Install Terminal Services. Set for domain admin access only, unless written requirements direct otherwise.
7. Install Net IQ Security Manager client and set logs to be monitored from the Security Manager Console.
8. For critical servers install Tripwire, generate report (currently on order).
9. Install Ups client (Network Version).
10. Configure IT located Network Printer.

11. Install Virus Software, set to be monitored by E-Policy.

Security Scan and Audit

1. The ISSO will scan server with St. Bernard's Update Expert and patch as needed.
2. The ISSO will run the CIS scoring tool – mitigating any problems and save reports
3. The ISSO will run Microsoft Baseline Security Analyzer and save the report.
4. The ISSO will scan with port scanner; investigate non-standard ports and save as baseline.
5. The ISSO will scan with GFiLANguard and save report.
6. The ISSO will scan with Active Network Monitor and save report.
7. The ISSO will scan with Stat Analyzer to determine any remaining vulnerabilities.
8. The ISSO will mitigate any vulnerabilities with Hercules – report results and save electronic version of report.
9. The ISSO will run a Self Sara Scan and save the report.
10. ISSO will release server for production when cleared.
11. All reports will be filed in an electronic directory under the servers name to be used as the basis for future auditing. Access to this directory will be limited to security staff.

References

Cornwell, Kay A. "GIAC Institute for Basic Cellular Research." Oct 16, 2002. 42. <http://www.giac.org/practical/Kay_Cornwell_GISO.doc>. (9 Feb 2003).

FIHS. "Windows 2000 Server Configuration." Sept 9, 2002

FIHS. "Microsoft Windows 2000 and Windows XP Professional Desktop Security Checklist." Sept 19, 2002

Naidu, Krishni. "Auditing Windows 2000." <http://www.sans.org/score/checklists/AuditingWindows2000.doc>. (9 Feb 2003).

Microsoft. "Windows 2000 Server Baseline Security Checklist." <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp>. (9 Feb 2003).