Global Information Assurance Certification Paper

Proactive Protection against Windows Vulnerabilities

GCWN Version 4.0
Option 1 – **Identify a Windows Security Challenge**

Suchun Wu
Sunday, August 15, 2004

Table of Contents

Executive Summary

This paper is to fulfill the practical requirements of GCWN version 4.0. It depicts a proactive patch management process in helping maintain operational efficiency and effectiveness, overcome security vulnerabilities, and preserve stability of the production environment for a fictional and relatively big information security consulting company – the GIAC Enterprises.

In face of increasing software and application vulnerabilities, the corporate direction decides to establish a process which allows the company to quickly assess the company's overall network security vulnerability, mitigate security risks, and reduce the company's overall IT operation and maintenance cost.

As one of the most important security measures in mitigating software vulnerabilities, the GIAC executives realize that the traditional and manual patch management practices are no longer effective. The efforts are towards setting up a managed and automatic/semi-automatic patch management process.

In order to better provide the evidence of the effectiveness of the process, we address the process within the GIAC Enterprises environments.

This paper is organized as follows.

- Section1 presents the GIAC operational environment by describing an overview of the company as well as an overview of the network infrastructure of the company. The challenges that the GIAC is facing are described in the second subsection.
- Section 2 addresses risk assessment in accordance with the challenges identified in the previous section.
- Section 3 describes in detail the patch management process itself and how it works within the GIAC.
- Section 4 presents a SUS patching system for the whole GIAC enterprises and its installation guidelines
- Section 5 addresses patch system validations and some other security enforcements in complementary to the patch management.
- Section 6 presents a concise summary of our work.

1. Security Challenge Identification and Description

1.1 Environments

The GIAC Enterprises is one of the leading information security services providers in North America. The GIAC Enterprises provides a broad range of security services, such as vulnerability assessment, intrusion detection and management, Anti-virus management, and secure network architecture and solutions.

The GIAC Enterprises established its headquarters in Toronto, Ontario, Canada in 1988. 15 years after, the GIAC has grown to a multinational corporation. It opens consulting offices in all major Canadian cities. And it will open new offices in other American cities where there is a potential consumer market for the GIAC to offer security services and/or to support security infrastructure for empowering customers' business.

Like any sizeable Corporate, the GIAC Enterprises comprises different departments such as Research and Development (R&D), Sales and Marketing, Accounting and Finance, and Human Resources. Except R&D department, most departments are located in Toronto headquarters. R&D is located in Ottawa. The number of staff in each city's office is variable. They are mostly local technical engineers along with one or two sales/accountant representatives. In terms of the general business flow and transactional volume, each city office reports either to a Toronto site or Ottawa site according to the nature of work the persons assume. Generally speaking, engineers report to Ottawa site and Sales persons and accountants report to Toronto site. Each city office is to maintain and store customers' data locally and transfer them periodically to the headquarters in a secure way. Any unresolved technical issues from each city office can be escalated to technical support personnel at Ottawa site.

Since the GIAC Enterprises has a lot of contractual projects with both Canadian and the US governments and militaries, the data they deal with should be generally considered very confidential (often these data are classified by the government).

By carefully examining the actual network infrastructure in the aim of increasing its professional competence, the GIAC Enterprises is aware of the necessity to renovate its existing network infrastructure with the latest proven windows technologies. Although the corporate direction is aware of some risks in using windows systems rather than other systems, it considers the strong and mature security features and new functionalities provided by Windows 2000 systems being much more overwhelming and advantageous for the company to meet its established business goals.

1.1.1 Communications Boundaries

All networks external to the GIAC Enterprises network infrastructure are considered 'hostile'. To address this presumption, firewall systems and routers' access control lists are established between the GIAC's network infrastructure and the Internet. These systems constitute the first line defense to the company.

1.1.2 VPN and Remote Access between Main Sites and City Offices

There are two methods of remote access for the GIAC employees who locate in different places, i.e. between head office and city offices, and between Ottawa R&D and city offices.

- Dialing directly to the company and through VPN over the Internet by using SecureID authentication from RSA Security Inc. (http://www.rsasecurity.com). and
- Using the IPSec tunnel between the employees' laptop and the enterprise's firewall.
-

The communications between Toronto Headquarter and Ottawa R&D take place within leased T3 line. The traffic is encrypted according to the sensitivity of the transferred data.

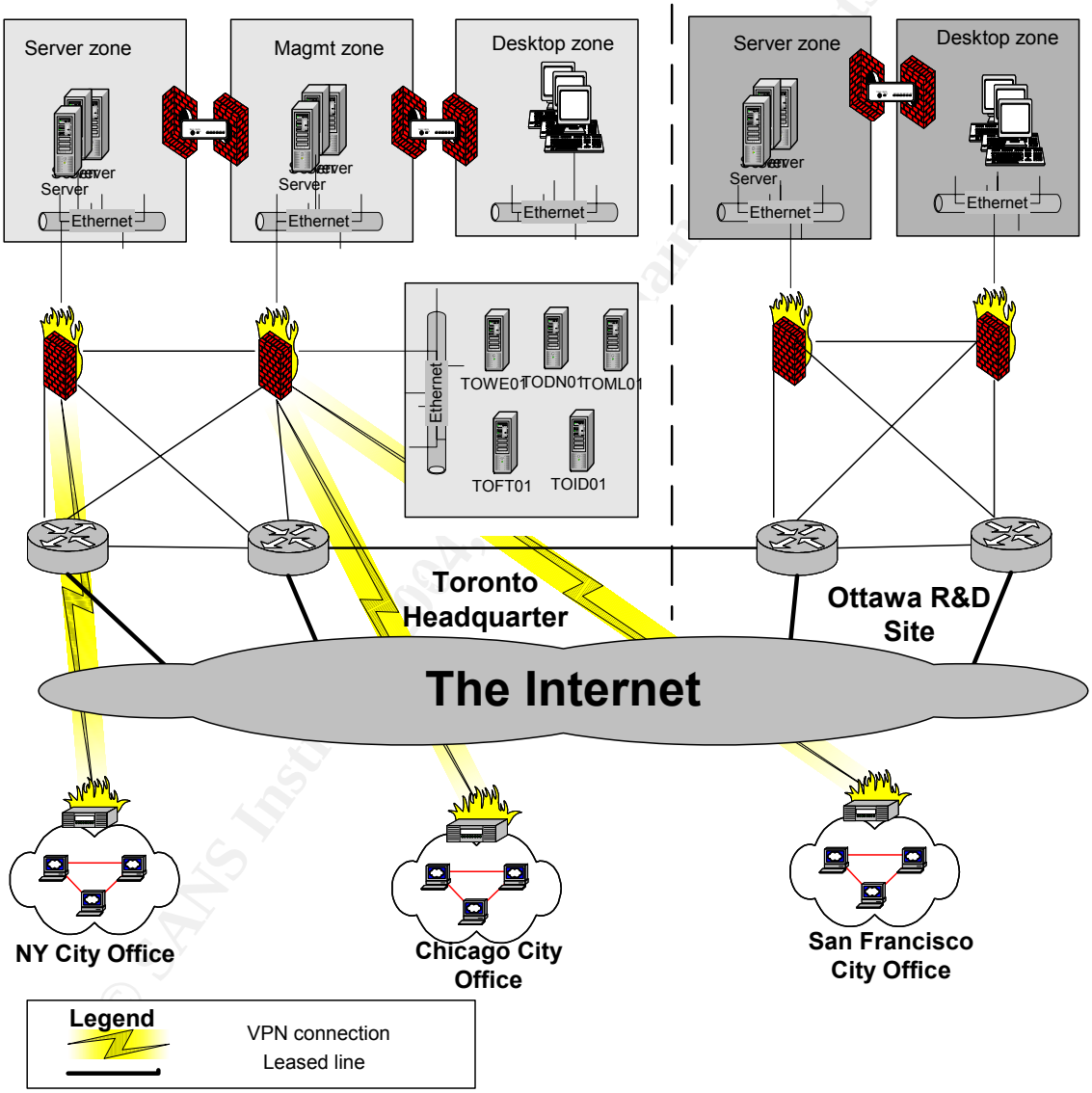

Figure 1 GIAC Enterprises networking architecture

1.1.3 Internal Network Zoning

In addition, because of the confidentiality of the security data collected and processed by the consultants from customers, a second line of defense is established by sub-zoning the whole internal network into several zones, e.g. between the general operation environment and data storage environment. As shown in Figure 1, for example, there are four zones at Toronto Headquarter: Server zone, Management Zone, Desktop zone, and Demilitarized Zone. Between these sub-zones, firewalls are used to make more granular and appropriate controls over the traffic flow (see Figure 1).

1.1.4 Logical Architecture Diagram

Figure 1 shows a high level logical architecture for the GIAC networks.

1.2 Challenges

Reports on information security vulnerabilities and their exploits have been greatly increasing, especially since 21 century (see Figure 2 from Cert survey at http://www.cert.org). These ever growing threats pose significant challenges to any company's IT production systems. The challenges are reflected in the following four aspects.

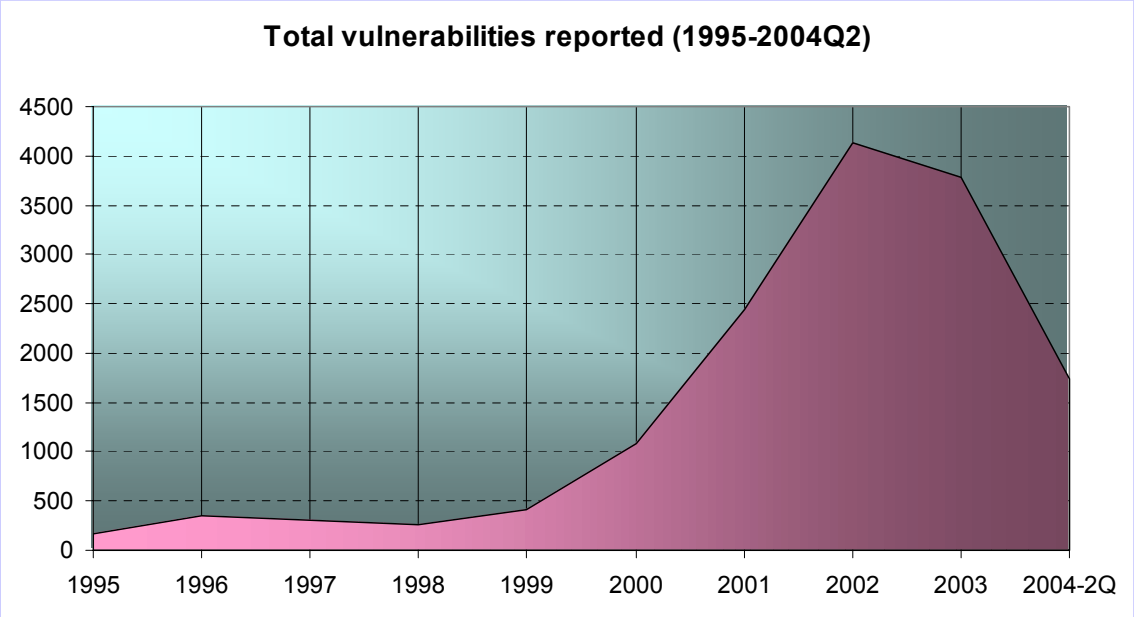

Figure 2 Security Vulnerabilities, 1995 – 2002

1.2.1 Software and application bugs are a fact of life

Vulnerabilities in software exist when defects or flaws in its code are not discovered during testing while the software is released for production. No software maker is immune vulnerabilities from its products. Because of the wide

use of its Windows products, Microsoft in particular has experienced a significant amount of public visibility due to defects discovered in its software.

According to NIST's report [10], most software statisticians estimate that for the number of bugs in published software, it can range from 5 to 20 bugs per 1,000 lines of code. With such an estimated proportion, Windows 3.1, released in 1992, had estimated 3 million lines of code; thus, it would contain an estimated 15,000 to 60,000 potential bugs. In 1999, Windows 2000 was released with a low estimate of 35 million lines of code. There would be, therefore, 175,000 to 700,000 potential bugs within Windows 2000.

As software goes to the market, the vulnerabilities can be discovered by its users who may be maliciously intentional or not all. Once these vulnerabilities are known publicly, attackers may attempt to exploit them. It is, therefore, understandable that as the growing number of known vulnerabilities increases the number of potential attacks generated by hackers increases too. As security professionals, we should react as quickly as possible so as to leave no room for hackers, i.e. make them "zero-day" to exploit the vulnerabilities.

The fact of existing vulnerabilities in software presents a challenge:

Challenge 1: How to discover vulnerabilities timely?

1.2.2 Networks are vulnerable

As shown in Figure 1, the GIAC Enterprises leverages TCP/IP networking and security technologies with the worldwide Internet in order to bring remote offices and business partners into its trusted network environments.

While this enables broader interaction with customers and streamlining of operations, reduced operating cost, it also comes with another problem: the openness and ubiquity make the GIAC's network at danger.

CERT/Coordination Center (http://www.cert.org) estimates that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches. Another Federal Computer Week even reports that 98 percent of successful hacker attacks are the result of known software bugs or other vulnerabilities that could have been fixed with available patches. These two reports tell us that in an increasingly interconnected world, it is critical that system administrators keep their systems patched to the most secure level.

A common misperception among some system administrators is that a firewall can reduce the need for timely patching. A typical example in correcting this misperception is SQL Slammer outbreak on the Internet. In January 2003, a so called SQL Slammer worm infected the Internet at such a high rate that it was classified as a "flash worm." It spread with incredibly high speed of 55 million scans per second: within 10 minutes of the start, the infection reached estimated 250,000-300,000 hosts all over the world. This worm targeted Microsoft Windows

servers running Microsoft SQL Server software. In fact, the vulnerability exploited by SQL Slammer had been published six months ago in July 2002, and a patch from Microsoft was available at that time as well.

Another devastating worm outbreak was Nimda a bit earlier than Slammer worm in September 2001. This worm attacked un-patched servers running Internet Information Server (IIS) and desktops using the IIS personal Web server. Both Slammer and Nimda worms had taken advantage of known vulnerabilities that had been exposed and widely publicized months earlier. In both situations, hot-fixes/patches were readily available that could have prevented worms from spreading.

Learned from these events, and others, many IT professionals have taken a more proactive stance by searching for the best ways to deploy patches and enforce effective security measurements before disaster strikes.

The vulnerable networks present a challenge:

Challenge 2: How to assess the vulnerability impacts to the networks and ensure correct patch implementation?

1.2.3 Number of Patches and Service Packs is growing

Some of vulnerabilities or bugs cause little or no concern. Some may cause catastrophic failures or give a malevolent person the ability to gain access to a system and even be granted administrative privileges. When discovered, the software makers try to repair the bugs by providing an immediate solution. It is called a ***patch***. It is logic that if the number of vulnerabilities grows, then the number of patches grows too.

What is the difference between a Service Pack (SP) and Patch? According to [11], a service pack is a strategic delivery, while a patch is tactical. The former is often well planned and includes improvements and enhancements to operation or performance of a software and application program, in addition to including most patches issued since the last service pack or product version.

A patch or service pack can often be downloaded from the software maker's Web site. It should be noted that a patch or a SP may modify or replace core system files, with possible interactions or conflicts with other files and applications. It may also alter the system's Registry, with other potential ramifications.

The number and complexity of patches present a challenge for administrators:

Challenge 3: How to deal with growing number of patches in a production environment?

1.2.4 Traditional patches management is problematic

There are five problems identified in traditional patch management.

Firstly, in traditional Windows Update scenarios, if a client Windows 2000 computer installed service pack 4, it runs the Automatic Update service to automatically pull a list of applicable updates directly from Microsoft Windows update servers (http://v4.windowsupdate.microsoft.com). With this solution, we see there are at least two problems existing in following situations:

1) If computers located behind a proxy, they have no way to directly connect to Microsoft servers. In this case, the updates just cannot happened at all. In reality, this is true for most enterprises in the world.

2) With the Automatic Update service running on client computers, the administrators have no way to customize the way it updates the computers. This means that it is too "automatic" to control what you want the patches installed, i.e. you have to "blindly" accept every patch matching to your computer, even there is a risk of denial of a particular application or service on the computer when a specific patch is installed.

Secondly, because of the above "too automatic" problem, in many cases, the administrators have to download individual patches from Microsoft sites and put them on a CD or other media. They then use this media to apply the patches on each computer. This process is too "manual" to be deployed for a large amount of computers in a big company like the GIAC Enterprises. This operation becomes daunting, given the big number of machines to patch, downtime considerations (most of patches for Microsoft Windows systems need a reboot after their installation), and available personnel to perform the updates. It is clear that automating this task is critical to keeping the environment protected, especially in a big enterprise.

Thirdly, a problem with patches is keeping abreast of what is out there, i.e. what patches are available. To keep current, every administrator must periodically check for updates at the Microsoft support Web site. This is a time and resource consuming activity.

Fourthly, in order to ensure a quality deployment, each administrator has to control the risks associated with updating systems by assessing the criticality of the patch to his/her own environment before a patch is deployed. This requires an administrator possessing of knowledge on both the patch/vulnerability itself and his/her environment. This means that this system administrator should be also a security expert. This seems unrealistic. The risk assessment of a patch installation should leave a security professional to do. More importantly, we should always keep in mind that testing is not always thorough enough before patches are released and that patches can wreak havoc with a system if it is not properly tested.

Finally time management becomes an obvious component of the patch management challenge. The process of testing and patching numerous systems over an entire enterprise is extremely time-consuming, especially if the administrator cannot automate the deployment process.

The traditional patch management practices present a challenge:

Challenge 4: How to make patch management effectively?

2. Risk Assessment and Mitigation Plan

While it is essential to protect company IT assets from attacks, patching vulnerabilities is only one part of the risk equation. Let us consider two situations: the one is that a patch to a vulnerability may cause little problem to the GIAC environments. The other is that several patches may come out at the same time. These situations imply that the importance of deploying the patches can vary from one to another and from one environment to another. This requires the professionals handling patches to prioritize the patches' deployment by effectively assessing their environments.

For these reasons, the direction of the GIAC decided to set up a set of criteria to look at the potential threat along with the vulnerability to determine the risk of having an un-patched system.

2.1 Risk Assessment

As mentioned in section 1, we address patch management issues only within Windows environment. As such, we need first to understand how Microsoft deals with the patches. When Microsoft prepares a patch for a vulnerability it is released by a Microsoft Security Bulletin. Security Bulletins generally contain an analysis of the vulnerability, a severity rating, Frequently Asked Questions and links to the patch and the accompanying Knowledge Base articles. The text version of the security bulletin that is distributed in email has links to the detailed bulletin and an end user version of the bulletin.

When a patch is released, Microsoft rates its severity with a rating system which consists of four severity levels: *critical*, *important, moderate*, and *low* (see [12] for more detail.).

In our case, in order to avoid ad hoc individual decisions on a patch deployment over company's production computers, we consider that it is necessary to create a vulnerability (associated with the release patch) analysis matrix in order for security analysts or system administrators to determine when to apply the announced patches on top of its severity defined in Microsoft security bulletin.

The matrix presented in Table 1 helps a security professional to rate the risk (very high, high, medium, and low) associated with the patch by comparing the result of successful exploitation of the vulnerability with the ease of its exploitation.

Result category / Ease	Auto-trigger	Easy	Moderate	Difficult
Admin, User, DoS, Run code	Very high	high	medium	Medium
Enumerate resource, other	High	medium	medium	Low

Table 1 Patch risk analysis matrix

There are two categories of exploitation results.

- The first is administrator level access, user level access or permissions of the currently logged on user, Denial of Service (DoS) of any kind or the ability of the attacker to run any code in any context. These results also include the ability to take any action based on the level of access or to view, copy, or modify any data or system files.
- The second category is enumeration of resources and others including obtaining the results of a successful null session, listing the shares on the target and determining any other facts about the target.

There are four levels of exploitation easiness:

- Auto-trigger: The exploitation of the vulnerability can be executed by anyone and anything like public script, even in an automatic way. The typical example is the vulnerabilities exploited by different kinds of Worm.
- Easy: The exploitation of the vulnerability can be easily made.
- Moderate: The exploitation of the vulnerability can be made with a certain amount of efforts.
- Difficult: It is difficult to make an effective exploitation unless the hacker posses some specific knowledge and experiences.

There are four risk levels for production systems:

- **Very-high risk**. A number of systems could stop functioning correctly within a shot period of time or indefinitely.
- **High risk**. One or more individual systems stop functioning correctly, or highly sensitive data (such as critical business and customer) loss.
- **Medium risk**. Sensitive data (such as system, business, or intellectual) loss.
- **Low risk**. Less sensitive data loss or malfunction of unimportant applications for which the associated risk is neither medium, nor high, nor very-high.

Based on the risk rating by using the above matrix, a timeline for application or deployment of the patch can be set in the following way:

- If Very high, the patch should applied within 24 hours;
- If High, the patch should applied within three days;
- If Medium, the patch should applied within 10 days;
- If Low, the patch is applied at administrator's discretion.

As we will see in next section, a security analyst who identifies a security risk, may decide, according to the matrix along with an enterprise-wide patch database, that a particular patch needs to be applied as soon as possible; or announce that the company is not vulnerable due to the absence of the software in the company; or acknowledge that the flaw has already been patched.

2.2 Mitigation Plan

To meet with the challenges identified in section 1, a mitigation plan is set up in order to formalize the deployment process of security-related patches. As a sub-process of the patch management process addressed in section 3, this mitigation strategy consists of the following four phases:

1) Discovery

This phase is designed for meeting challenge 1: *How to discover vulnerabilities timely?*

In order to discover vulnerabilities and available patches, one or more responsible personnel (see next section) should know where to find related information resources.

- The main source for information regarding operating system vulnerabilities is the operating system vendor. In our case, it is Microsoft. The GIAC CSO (Chief Security Office) suggests that every Windows system administers should subscribe to Microsoft Security Bulletins and read and analyze each bulletin released via http://www.microsoft.com/security.
- Other reliable information is the Computer Emergency Response Team Coordination Center (CERT-CC) at the Software Engineering Institute of Carnie-Mellon University (www.cert.org). CERT-CC publishes advisories that detail vulnerabilities and mitigating actions.
- The SANS (www.sans.org) Critical Vulnerability Analysis list should also be subscribed to along with SANS NewsBites. The Critical Vulnerability Analysis focuses on actions other organizations have taken to mitigate the risk associated with vulnerabilities.
- Common Vulnerabilities and Exposures (CVE) is "A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures" (http://www.cve.mitre.org/).

2) Assessment

This phase is designed for meeting challenge 2: How to assess the vulnerability impacts to the networks and ensure correct patch implementation? In section 2.1, we have defined a vulnerability assessment matrix to assist security responsible to make appropriate decisions in patch deployment.

It should be noted that in order to undertake this task effectively, this security responsible must posses of knowledge on both available patches and relevant asset. In common practice, this person or team need to inventory computers, application software, and patches installed over the time within the GIAC Enterprises (see next section).

3) Coordination

This phase is for challenge 3: How to deal with growing number of patches in a production environment? As pointed out in section 1, patch management is not trial work, especially in a large company and actual growing number of vulnerabilities. It is absolutely not one or two persons can ensure protecting the company from security attacks because of the growing number vulnerabilities.

In order to cope with this challenge, the GIAC considers that it is necessary to create a Patch Management Group (PMG). Its main duties are described in next section. Here, we keep in mind that this group plays a central role in facilitating and coordinating the patching activities within the GIAC Enterprises.

4) Streamlining

This phase is for Challenge 4: How to make patch management effectively? This phase is designed to ensure best practices in patch management with additional guidance for patch deployment. In this phase, the GIAC Enterprises uses again the PMG approach to undertake the following tasks in cope with the problems identified in section 1.2 correspondently:

- Creating an effective and automatic patching system.
- Distributing patch and vulnerability information to local administrators.
- Testing patches for functionality and security.
- Verifying patch installation through network and host vulnerability scanning.
- Training system administrators in the use of patch management infrastructure and tools.

A patch management process that includes mitigation strategy/plan will be address in detail in section 3.

3. Patch Management Process Establishment

In response to the challenges identified in section 1, the direction board of the GIAC realizes that to secure enterprise assets, an effective process for security patch management needs to be created. The aim is to minimize any impact on the company from malicious activity.

Because we are working on the scale of a big enterprise, ad hoc and individual efforts are not likely to be successful. Success will require that we coordinate the collective efforts throughout the company according to a rigorous patch management process. Such a process ensures that the security vulnerabilities affecting the company's information systems are addressed in an efficient, thoughtful, timely and effective manner. The intent of this section is to provide a framework around which to build an effective security patch management process, and to serve as a starting point for the GIAC Enterprises system administrators and security professionals to gain the best practice in the life cycle of the patch management.

The key idea underlying this process is a clear definition of the roles and responsibilities for people involved in the process. The approach adapted is to create a centralized group who will support vulnerability assessment, risk mitigation, coordinating patching activities of local administrators.

The following eight steps consist of an effective security patch management process in the GIAC Enterprises environment.

3.1 Step1. Policy and Responsibility

The company direction clearly understands the first paramount need is to establish a security policy along with a comprehensive process in order to lay the ground rules for the process.

Although the full description of the policy is out of scope of this paper, it is worthy to outline some important issues that the policy contains:

- Clarify higher-level organizational objectives and rules for the governance of the process.
- Determine the resources including personnel involved in the process; hardware, software, and technologies used for monitoring, assessing, and implementing new vulnerabilities and patches.
- Define resource ownership.
- Assign responsibilities to personnel.
- Draw the guidelines on how to deal with vulnerabilities and patch updates.
- Policy enforcement.

In accordance with the company's policy, the patch management process should define the roles and responsibilities of groups and individuals who will be involved in the process. So, the first concrete action or step for us is to define these groups and individuals, and their responsibilities.

There are three groups of people playing important roles in patch management process.

PMG (Patch Management Group)

This group facilitates the identification and distribution of patches within the whole GIAC Enterprises. It is constituted of a manager and a dozen of technical personnel with different security experience and expertise. The manager is accountable for the entire security patching process. Each staff will undertake one or more duties listed as follows:

1) Creating and consolidating a company's hardware and software inventory.
2) Monitoring security sources (mainly from the credible web sites on the Internet) for new security vulnerabilities and patches.
3) Assessing vulnerabilities and prioritizing patch application for different networking zones.
4) Creating an enterprise-wide patch database where patching activities histories are stored.
5) Compiling and publishing timely the security vulnerability advisory pertaining to the GIAC environment, distributing related patches and vulnerability information to local administrators.
6) Coordinating and guiding patch tests for different environments with local system administrators.
7) Verifying patch installation through network and host vulnerability scanning.
8) Assisting local system administrators in configuring SUS patching system and Automatic Update of Applications.
9) Assisting local system administrators in deploying patches as automatically as possible.

As we see from above, one of key activities for PMG is *coordination*.

LSO (Local Security Officers)

This group of staff takes care of the systems within their networking zones (see Figure 1). LSO are technical personnel who could be security officers or system administrators who know their networking environments and security needs within the environments. Their duties in this process include:

1) Creating each zone's hardware and software inventory and reporting to PMG
2) Applying patches identified by the PMG.
3) Testing patches on their specific target systems.

4) Identify patches and vulnerabilities associated with software in their own environment.

SM (Senior Managers)

The policy requires that each department must assign a SM being involved in the patch management process. SMs' responsibilities include:

1) Responding within 24 hours to requests from the PMG to assist in the analysis of security vulnerabilities and development of a suitable response.
2) Calling and attending relevant meetings, as required; leading LSOs to determine the impact of new vulnerabilities on the systems for which they are responsible.
3) Leading the development and testing of patch deployment through their departments.
4) Approving the final patch deployment plan after ensuring that an evaluation of the testing results is done prior to patch implementation.

3.2 Step 2. System inventory

By now, we have clearly pointed out that the patch management is a critical element in protecting the GIAC against emerging security threats. As mentioned in [13], patch management is a subset of the overall configuration management process. From ITIL point of view [14], this means that an organization should have in place a strategy for establishing, documenting, maintaining and changing the configuration of all servers and workstations according to their function.

Based on best ITIL practices and in order to monitor for information about vulnerabilities and patches that correspond to the company's network resources, one important step is to identify, classify and inventory the network resources. For this reason, with the inputs from the LSOs, PMG creates a database containing the hardware equipment and software packages and version numbers of those packages most used within the GIAC. Specific attention should be given to those software packages that are used on critical servers or that are used by a large number of systems.

When the inventory database is created, the PMG makes it available to LSOs. As other systems, it will be necessary to maintain this inventory after it goes to production. The maintenance of the inventory will require the PMG to work closely with LSOs so that the inventory is updated in a timely manner when a patch is installed or upgraded on the systems; and when a system asset is newly added or deleted.

3.3 Step 3. Monitoring and Evaluating

The PMG is responsible for daily monitoring of all appropriate security intelligence sources for exposures that may impact platforms or applications utilized by the company. Since new security advisories and patches for

vulnerabilities are released frequently, diligence on the part of PMG will be required at all times.

The PMG is also responsible for informing LSOs and SMs patches that correspond to software packages included in the GIAC software inventory. Email lists and the PMG's internal secure web site should provide effective methods for distributing patch information.

This information will normally consist of a detailed, formal announcement (often called advisory) of security vulnerabilities. The announcement within the whole GIAC enterprises is "synchronized" with Microsoft security bulletin announcement once a month. Just after Microsoft's bulletin is released, the PMG will digest the announcement and analyze intensively the related vulnerabilities. The PMG staff then announces their analysis to the whole GIAC within 24 hours.

The announcements made by the PMG usually provide a description of the vulnerability, criticality of the patch deployment, the platform or application affected, and the steps necessary (when available) to eliminate the risk.

Normally, the PMG will proactively monitor security sites to obtain the latest vulnerability information, examine the potential effects on the GIAC's infrastructure, and take appropriate action to mitigate any threat. However, the GIAC employees or contractors outside of the PMG may become aware of vulnerabilities through their personal sources, and hands-on experiences. They are encouraged to report these vulnerabilities to the PMG through security awareness propagation and any other regular communications occasions.

3.4 Step 4. Risk assessment

When a vulnerability is discovered and a related patch and/or alternative workaround is released, the PMG should consider the following important aspects:

- the importance of the system to operations,
- the criticality of the vulnerability, and
- the risk of applying the patch.

Since some patches could cause unexpected disruption to systems and business, the GIAC chooses not to apply every patch, at least not immediately, even though it may be deemed critical by the software vendor that created it.

Furthermore in view of the fact that each environment is different, the PMG should assess the risk of deploying the patches in working with local LSOs and SMs to determine and prioritize the patching plan for each environment. If necessary, the PMG may conduct a vulnerability assessment by using different scan tools (see section 5) prior to a patch deployment plan is drawn. Note that the PMG is responsible for assessing vulnerability for the whole GIAC. It scan quarterly all the networks. Here, the vulnerability assessment is more specific

with a relation to an actually published vulnerability. Such a vulnerability assess is only conducted if the published vulnerability is new and critical.

Once a vulnerability that affects a platform or application in use within the environment has been identified, the PMG should perform an initial review to establish the resources required to perform adequate analysis of the vulnerability and to establish an initial level of exposure. This should be completed within 24 hours of the vulnerability being identified. These resources will include not only other groups from within the company, but also product vendors.

PMG and the LSOs would then assess the impact of the vulnerability on the environments by using the matrix defined in section 2.1.

3.5 Step 5. Duty segregation along with network zones

Breaking the network into more manageable chunks is modern security practice in big companies like the GIAC enterprise. LSO's responsibility scope is segregated based on networking zones (see Figure 1). There are two obvious benefits by doing this:

- Software and Applications become manageable by LSOs because they are more similar in a specific zone.
- LSOs can quickly familiarize the environment and gain more time on managing their systems more appropriately and securely.

3.6 Step 6. Developing and testing

When a patch is released, a general testing plan is first proposed by the PMG. And the tests themselves are executed by LSOs under the PMG manager's coordination. The testing results are documented and feedback to the PMG.

According to previous experiences by LSOs in each environment, a back-out plan would also be developed and prepared by the PMG. This is to ensure that if the patch adversely affects a production system, it can be quickly reversed and the system restored to its original state. This plan could include:

- Vendor-specific procedures to remove the patch or fix
- Other backup and restore procedures to bring a disrupted system back to its original state

3.7 Step 7. Deployment

The senior managers of departments are responsible for approving the implementation plan for production use based on the test results and recommendations from the LSOs with concurrence from the PMG. The senior manager must also validate that the patch is protected from malicious activity before it is installed on the system.

Once approved, the deployment process is required as automatically as possible by using the patching infrastructure described in section 4. However, the PMG recommends LSOs not to switch on the automatic installation on Microsoft

Automatic Update Client for mission critical production systems and small working units, i.e. using the option “Auto Download and notify for install”.

3.8 Step 8. Documenting Tracking, and Reporting

The PMG will maintain consolidated reports on each security vulnerability and affected system. For each vulnerability, the following documentation will be maintained by the PMG:

- Vulnerability overview with appropriate references to supporting documentation.
- Test plan and results for relevant security-related patches or other remedial measures.
- Detailed implementation and back-out plans for all affected systems.
- Progress reports and scorecards tracking systems that have been patched.

All supporting documentation for a processed security vulnerability is stored in the PMG database (which is a restricted data storage area, available only to the PMG members and designated information security specialists). The PMG publishes a list of security-related patches that have been determined to be necessary to protect the GIAC. This list is reissued whenever a new security-related patch is sanctioned by the PMG.

An online system is used to report status. LSOs are required to report progress when deploying required remedial measures. When feasible, the PMG monitors vulnerable systems to ensure that all required remedial measures have been successfully implemented.

A scorecard is used in the reporting process to ensure that any vulnerable system is in fact fixed. For tracking this issue, a periodic network and host vulnerability scanning will be executed by the PMG in order to identify systems that have not been patched.

4. Using Microsoft SUS for Patching System

This section describes an automatic patching system for the GIAC Enterprise by using Microsoft SUS servers. It also delineates how to set up and configure it. It is written according to the author’s personal experience on setting up SUS patching system for the GIAC Enterprises and can be served as a script for system administrators to set up a patch system according to their own proper environments.

4.1 Software Update Service

Microsoft SUS (Software Update Service, see [17]) is a free and managed version of the Microsoft Windows Update website (http://windowsupdate.microsoft.com), which can be run on a local IIS server and

allows an administrator to approve patches before they are automatically deployed to Windows systems.

A SUS server runs on IIS 5.0 or above, and communicates with one or more clients running Windows 2000 (Professional, Server or Advanced Server) with Service Pack 2 or higher. A Windows automatic updating client software can automatically query the SUS server via HTTP to determine if there is any patch needed by the local computer. If the client finds there are new patches for the local computer, it download them from the SUS server it is configured to. Note the client can also download patches directly from one of Microsoft's Windows Update Servers and install them, if it has direct Internet access.

The downloading of the patch uses the Background Intelligent Transfer Service (BITS) which uses idle network bandwidth in order to prevent any network disruption. Once the patches have been downloaded, the installation can happen either automatically (immediately or at a scheduled time) or the next time an administrator logs into the local computer.

Key Features

SUS has several useful features, namely:

- First, clearly the most important feature is the ability to roll out tested patches automatically without having to visit every machine one to another.
- Second, SUS and its client components allow scheduled installation of patches to minimize disruption of production boxes.
- Third, a security feature is that all update packages can be digitally signed. By checking this digital signature the SUS server and Automatic Update clients are able to detect if the files have been tampered with or corrupted.
- Finally, another useful feature is that the Automatic Update client can send results back to the SUS IIS server that are logged in the IIS logs together with any other logging that IIS is currently configured to perform. This gives administrators the ability to keep track of a client computer/server's patch status and evaluate if systems are not being patched correctly. For reference purpose, the default location for the IIS logs is %WINDOWS%/system32/. The name is LogFiles/W3SVCx where x is an integer. The format of the file name for the log files is *exyymmddhh.log,* for example ex04080315.log

4.2 Windows Automatic Update Client

In order to function in a real environment, a whole patching system needs to have one or more SUS's client components: Windows Automatic Update Client.

Automatic Update Client is a proactive pull service that enables users with administrative privileges to automatically download and install Windows updates such as critical operating-system fixes and Windows security patches. This client uses the Windows Update service technologies to scan the system and determine which updates are applicable to the computer it resides on. It uses the

Windows Update technologies to install downloaded updates. If multiple updates are being installed and one of them requires a restart, Automatic Updates installs them all together and then requests a single restart. In an Active Directory environment, an administrator can configure the behavior of Automatic Updates using Group Policy (see section 4.5.2).

4.3 The GIAC Patching Architecture

In setting up a patching system for the whole company, the PMG has come up a scalable solution which is approved by the company's board of direction.

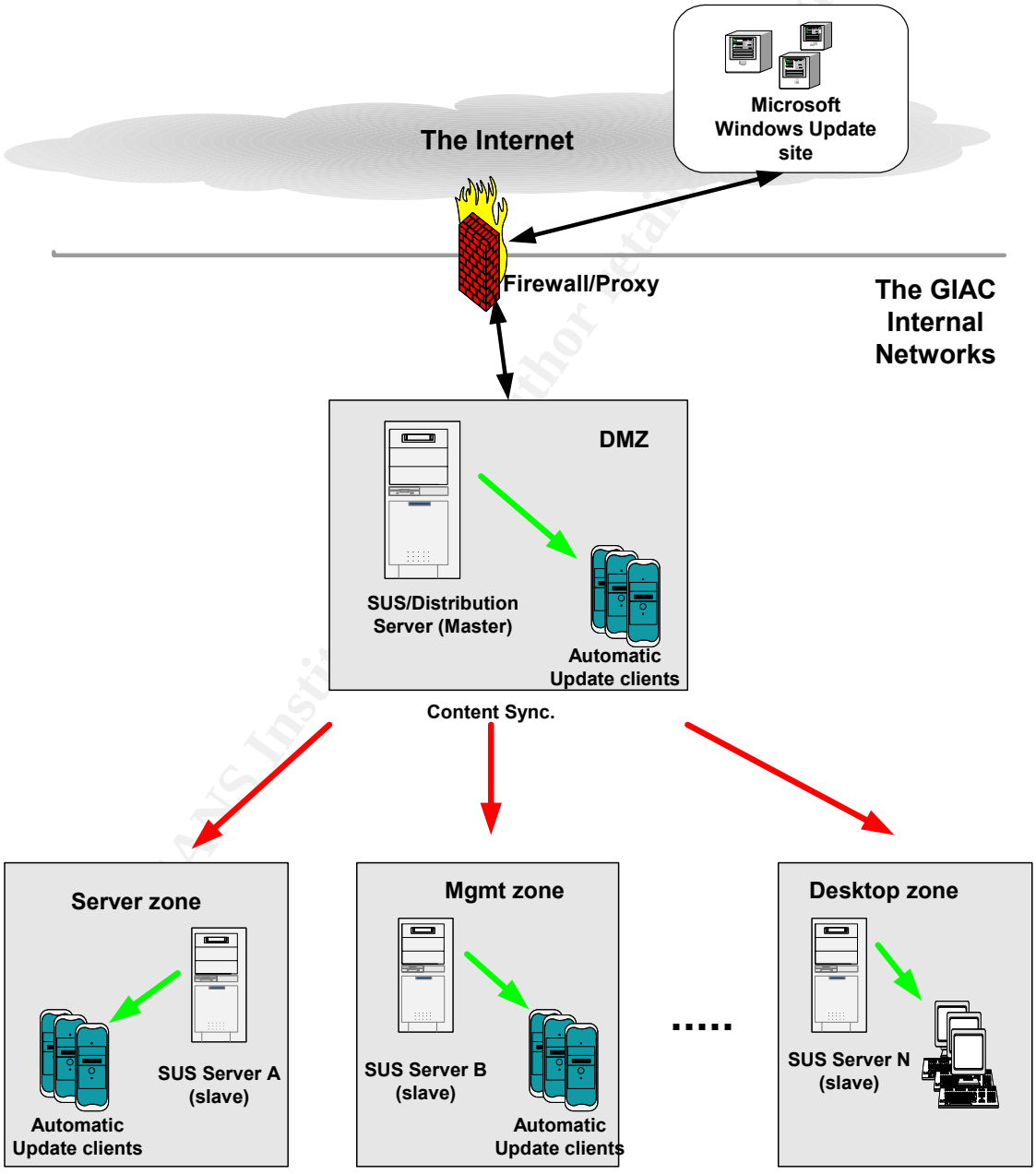

Figure 3 The GIAC SUS patching architecture

Without going into the detailed design process and documentations, I present, in this sub-section a general architectural view of the system. Some descriptions of important system components are given thereafter.

4.3.1 Master-Slave structure

One of features SUS has is that a server running SUS can be synchronized with Microsoft's public Windows Updates servers as content distribution point (master server). The other SUS servers (slave servers) can then synchronize with that master server.

This is an interesting feature to the GIAC because

- The GIAC is a big company which has multiple logical zones for its own internal networks. For a scalable solution, it is appropriate for the GIAC to have one or more servers running SUS for each networking zones (see Figure 1). With a master-slave structure, only one server needs to access the Internet to synchronize content with Microsoft's (see Figure 3).
- For security reasons, not all sites and servers are allowed to have Internet access and inter-zones access. It is justifiable again to have a SUS server within a zone.
- Each environment has its own particularity. Therefore, it is appropriate to test content in each particular test environment so as to push the content that you have tested to your production environment.

4.3.2 Content synchronization between SUS servers

As shown in Figure 3, the GIAC's master SUS server M synchronizes the contents over the Internet with Microsoft Windows Update site (http://windowsupdate.microsoft.com). This master server is maintained by the GMP. The internal SUS servers from A, B, to N (refer to slaves) will synchronize content from server M. These slave servers are maintained by LSOs.

4.3.3 How to configure

To make the communication between two SUS servers successful we need to maintain the following configuration.

The master SUS server must:

- Be configured to "Save updates to a local folder" on the **Set options** page.
- Be configured to support all the locales that child servers might request on the **Set options** page.

The slave SUS server must:

- Be configured to “Synchronize content from a local Software Updates Services server” and correctly provide the name of master SUS server on the **Set options** page.
- Be configured to “Save updates to a local folder” on the **Set options** page.
- Only select locales to support that are also supported on master SUS server. Otherwise the server will try to synchronize for locales that do not exist on master SUS server.

4.4 SUS Server and Automatic Update Client Installation

4.4.1 Server Requirements

SUS requires a Windows 2000 (with Service Pack 2) or higher server running IIS. The hardware required to run SUS is a 700MHz Pentium III with 512MB of RAM and 6 Gigabytes of available disk space. The client computer simply needs to be running Windows 2000 Professional, Server or Advanced Server with Service Pack two or higher or any version of Windows XP and Windows Server 2003.

4.4.2 Some installation concerns

- Since SUS is installed and incorporated into any existing IIS environment, the IIS Lockdown and Urlscan policies should be installed with SUS [1].

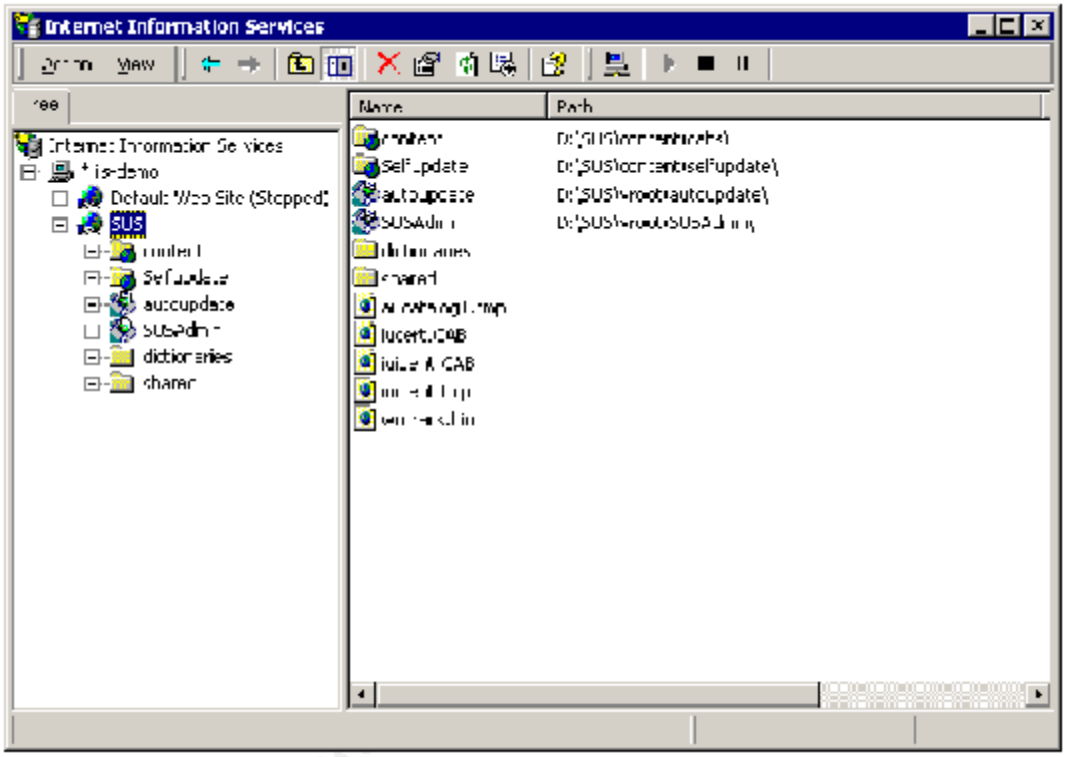

Figure 4 SUS installed as its own Site

- Following Microsoft recommends, install SUS on a dedicated server. For this, stop all websites in the Internet Information Services Snap-in and allow SUS to install itself to a new web site bound to port 80 (see Figure 4). In this way, the new website will not have any of the default files and folders associated with IIS, thus eliminating the possibility that some of the files are tampered by scripts and worms such as Nimda, which attempt to exploit vulnerabilities through the directories /scripts, /_vti_bin, /_mem_bin and /msadc.
- During a custom installation, it is desirable to use separated server's disk drivers for placing the website and SUS itself. The disk on which the SUS is installed requires a bigger space for downloaded patches.
- From an ongoing management stand point, one has to decide how to handle updated patches. From time to time, Microsoft updates releases patches. When this happens, SUS can be configured to either automatically approve the patches or require the administrator to approve it. Here, the GIAC PMG recommends the SUS administrators use latter method during the server installation. This is because some updates/patches may cause problems within particular application environments. Furthermore, according to the process requirement (see previous section), a test should be done before the patch is installed.

4.5 Configuration

It is important to configure both the server and the client properly. Otherwise, the patching system as whole simply does not work in a way you want.

4.5.1 Configure Server

Set Options

Configuring SUS server is reasonably straightforward. It is accomplished through the use of a web page on the SUS server. This interface (see Figure 5) looks a lot like the Microsoft Windows Update Server website and is the primary interface for all SUS configuration and management.

The configurable options include:

- the languages supported,
- the file storage location, and
- proxy settings.

Note that most of the configuration options can be defined with custom installation; however the options to set the computer's name and configure proxy settings for Internet access are only available from the "Set Options" screen.

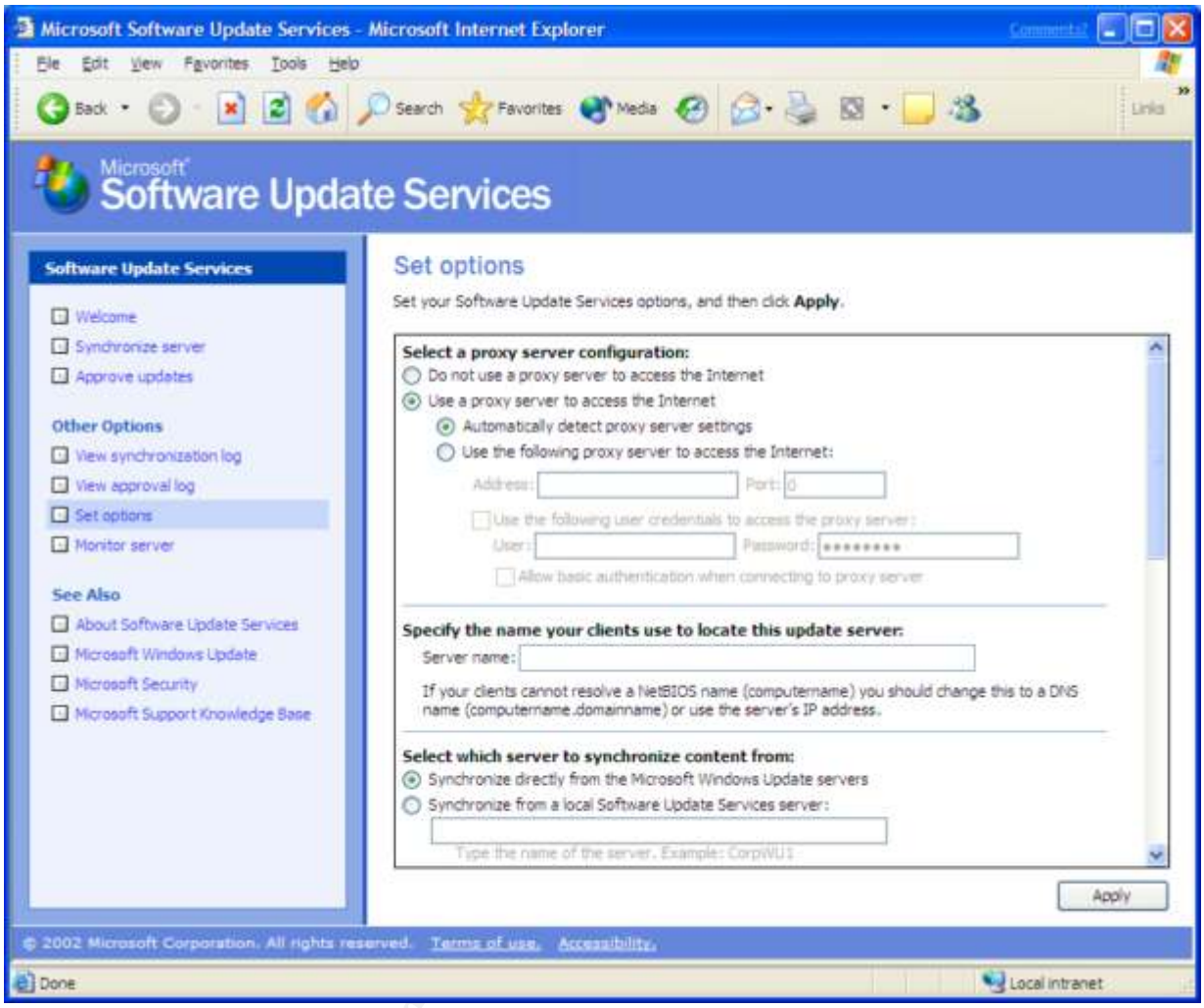

Figure 5 SUS Options Setup

One of the most important options that can be set for the server is the "Synchronize Server" screen found on the left hand side of the SUSAdmin page. From this page it is possible to either "Synchronize Now" or set a "Synchronization Schedule." As the name implies, "Synchronize Now" is a manual synchronization with the Windows Update servers which immediately downloads the current version of Aucatalog1.cab. In contrast to the manual synchronization, "Synchronization Schedule" opens a dialog box in a separate (see Figure 5) allowing the Administrator to schedule regular synchronizations based upon time and day of week (or everyday if so desired).

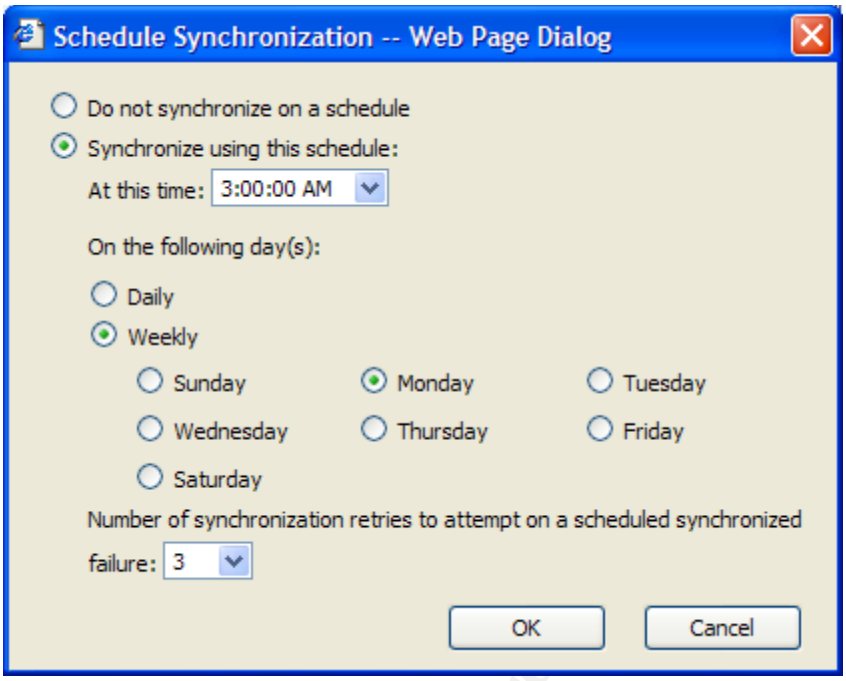

Figure 6 Configure SUS synchronization schedule

Synchronize the SUS server

Once the Internet connection is ready, it begins the process of synchronizing the server. For the GIAC's master server (see Figure 3), it contacts directly with the Microsoft Windows Update website and downloads the appropriate updates. This done by doing the following:

1) On the SUS Web site home page, click Synchronize server in the navigation bar.
2) Click Synchronize Now. When the synchronization is complete, the list of updates you can approve appears on the Approve updates page.
3) You will be notified whether the synchronization was successful. For more information about current or past synchronizations, and the specific update packages that were downloaded, click View synchronization log in the navigation bar.

Approve the updates

Once the synchronizing was complete, The GIAC PMG requires the SUS administrators to manually select each update in a control way:

- Click **Approve updates** in the navigation bar, select the updates that you want to distribute to client computers, and then click **Approve.**
- You will be notified that the approval was successful. For more information about which updates you have approved, click **View approval log** in the navigation bar.

4.5.2 Configure Client

Configuring SUS clients is a bit complex. Two environments need to be considered. The one is that the client servers or desktops are in an active directory environment. And the other is that the client servers or desktops are not attached to any domain.

In both environments, it is necessary to configure the update schedule, location and whether updates are automatically installed or just downloaded on the client computers. This configuration can be accomplished through edits to the registry and/or Group Policy (either domain level GPO's or local Group Policy).

1) In No-Active Directory Environment

When dealing with systems in a non-Active Directory environment, in order for the client to be able successfully to communicate the server and get new updates from there, we need to do the following steps:

a. Load WUAU.adm. This file describes the new policy settings for Automatic Updates. This file comes with service pack 2 or higher. So, following the procedures to load %windir%\inf\wuau.adm as an administrative template in the Local Group Policy Object Editor:

- Click **Start**, and then click **Run**.
- Type **GPEDIT.msc** to load the Group Policy snap-in.
- Under **Computer Configuration**, right-click **Administrative Templates**.
- Click **Add/Remove Templates**, and then click **Add**.
- Enter the name of the Automatic Updates ADM file: **%windir%\inf\WUAU.adm**
- Click **Open**, and then click **Close** to load the wuau.adm file.

b. Configuring Automatic Updates policy settings. After loading WUAU.adm, the folder "Windows Update" appears under Windows Components folder. There are four items in right side windows. To configure them, just double click on them.

Note that the detailed definition for these items can be fined in Microsoft knowledge base article 328010 (see table-2 below).

c. Edit Registry. For a stand alone client computer, it is necessary to edit related registry keys. In order to avoid unnecessary hazard by editing registry, the GIAC PMG experts have created a registry value template for the following key

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

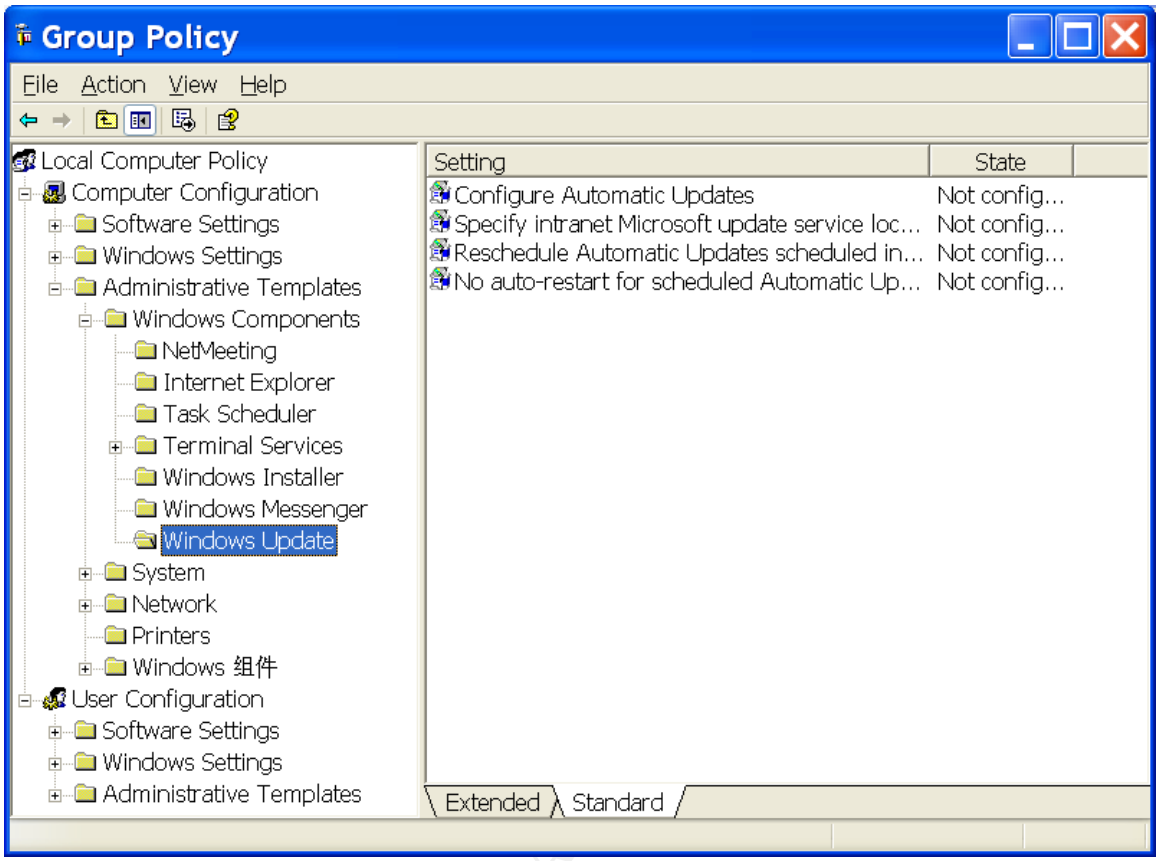

Figure 7 Configuring Automatic Updates policy settings

---------- Cut Here ----------

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\]
"WUServer"="http://sus-srv"
"WUStatusServer"="http://sus-srv"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\\AU]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000003
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"UseWUServer"=dword:00000001
"RescheduleWaitTime"=dword:00000005
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
```

---------- Cut Here ----------

Note: for the meanings of the above integer values, please refer to Appendix A.

An administrator who is configuring the client can copy and past the above lines into a file called “Winupdate.temp” in directory C:\reg-temp, for example. Then, he/she imports this file into the registry at command line as follows:

- regedit.exe /c /s C:\reg-temp\Winupdate.temp

Note that there is another way to obtain the "Windupdate.temp" file by exporting the registry value from client computer within a domain. Do the following at command line:

- regedit.exe /e C:\reg-temp\Winupdate.temp \
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate"

  Where: "\" is an escape symbol for new line

d. Edit hosts file if the SUS server is not DNS resolvable on the client computer. If a client computer is not attached to a domain and it cannot communicate with SUS server by its name. It is better to define an entry in the hosts file in directory %windir%\System32\drivers\etc. For example, if the server name is "SUS-SRV", the following entry is added to the file:

   172.17.17.12 SUS-SRV

e. Raise a firewall rule change request. If there is a firewall in between the client computer and SUS server, a rule that allows the client computers to communicate with SUS Server via port HTTP need to be added. If the firewall uses NAT, a NATed IP should be defined for the SUS server. The firewall administrator should inform the client computers' administrators so that they can configure the related settings according with the local group policy edit (see point 2 above.).

2) In an Active Directory environment

In order to change a large number of computers quickly the best method is using Active Directory Group Policy. Since the GIAC uses Active Directory for its networking infrastructure and environments, most local system administrators have to familiarize with this configuration task.

Although detailed steps have been described in Microsoft Knowledgebase article Q328010, "How to Configure Automatic Updates by Using Group Policy or Registry Settings", For a sake of clarity, we just go through what we should do exactly in our case.

a) Loading Policy Settings
As configuring a client computer in a no-active directory environment, one should first load policy settings by using Group Policy in Active Directory:

1. On an Active Directory domain controller, click **Start**, and then click **Run**.
2. Type **dsa.msc**.

3. Right-click the organizational unit or domain where you want to create the policy, and then click **Properties**.
4. Click the **Group Policy** tab, and then click **New**.
5. Type a name for the policy, and then click **Edit**.
6. Under **Computer Settings**, right-click **Administrative Templates**.
7. Click **Add/Remove Templates**, and then click **Add**.
8. Type the name of the Automatic Updates .adm file, for example, type ***windows_folder*\inf\wuau.adm**.
9. Click **Open**.

b) Configuring Automatic Updates Group Policy settings
In the Group Policy Object Editor

- Click Computer Configuration, and then expand Administrative Templates.
- Click Windows Components, and then click Windows Update. The four policies that you can set appear in the right pane.

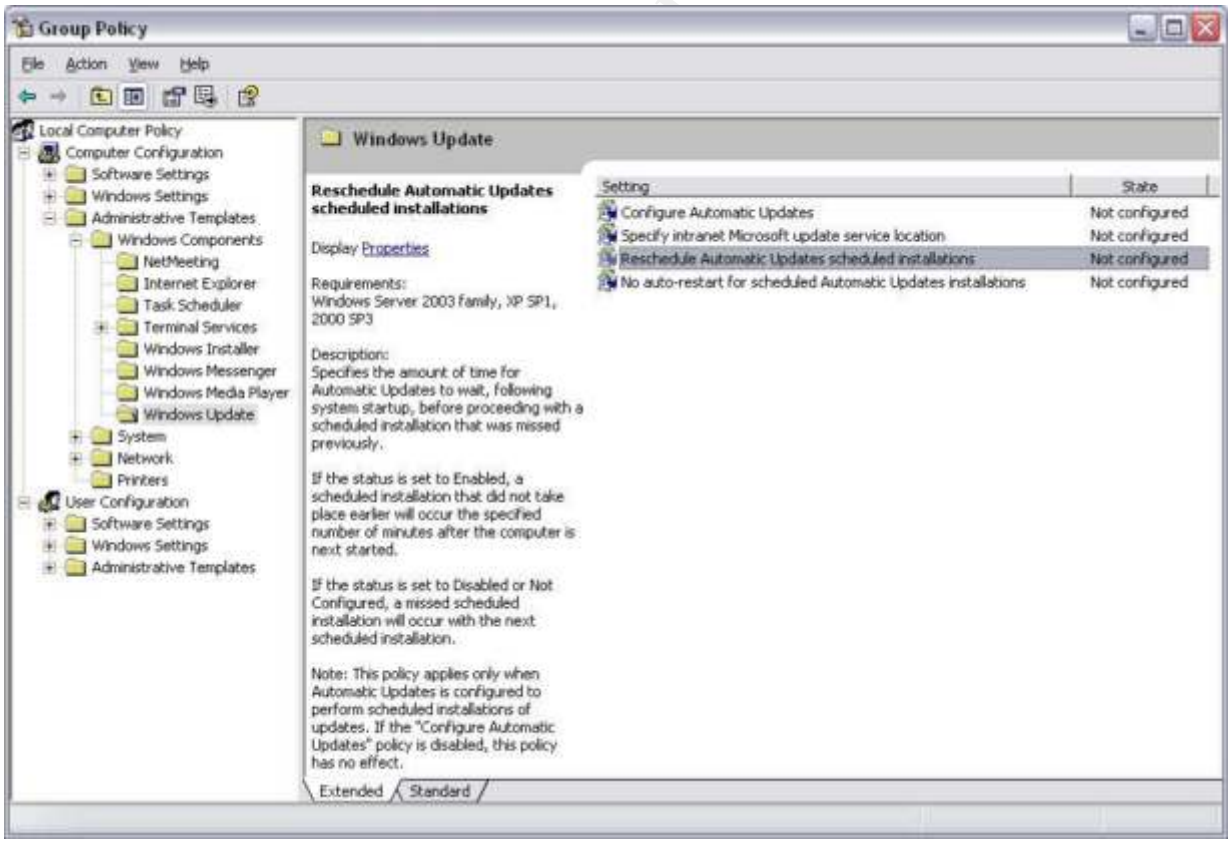

Figure 8 Group Policy setting to configure Automatic Updates service

c) Configure the behavior of Automatic Updates

In order to configure the behavior of Automatic Updates, double click on "**Configure Automatic Updates",** for example. A Windows menu appears. Check the choice which is appropriate to your own environment. Table 2 gives a mapping between the GPO settings and registry values. A recommended registry value for each setting is given by the GIAC PMG.

GPO setting in graphic menu	**Description**	**Registry name and value**	**Recommended value**
Configure Automatic Updates (menu)			
	Keep my computer up to date has been disabled in Automatic Updates	AUOptions 1	
Notify for download and notify for install	notifies a logged-on administrative user prior to the download and prior to the installation of the updates.	AUOptions 2	
Auto download and notify for install	automatically begins downloading updates and then notifies a logged-on administrative user prior to installing the updates.	AUOptions 3	This value for an environment with less then 50 computers
Auto download and schedule the install	If Automatic Updates is configured to perform a scheduled installation, the recurring scheduled installation day and time is also set.	AUOptions 4	This value for an environment with more than 50 computers
scheduled installation days and times			
Day: "Every day" and "Every Sunday" to "Every Saturday"		ScheduledInstallDay (0-7) 0: every day	Every day
Time: 12 AM to 11 PM in 24-hour format (00:00 to 23:00)		ScheduledInstallTime (0-23)	Time which is appropriate to the local environment. Night installation is recommended in most cases.
Specify intranet Microsoft update service location (menu)			
Set the intranet update service for detecting updates:	SUS server name	WUServer=http://sus-server	http://sus-srv

Set the intranet statistic server:	SUS Statistics server name	WUStatusServer=http://statistic-server	http://sus-srv
Reschedule Automatic Updates scheduled installations (menu)	To set the wait time between the time Automatic Updates starts and the time it begins installations whose scheduled time has passed		
Wait after system startup (minutes):		**RescheduleWaitTime (0-23)**	5
No automatic restart for scheduled Automatic Updates installed (menu)	To prevent Automatic Updates from restarting a computer while users are logged on		
Not configured			
Enabled		NoAutoRebootWithLoggedOnUsers 1	1
Disabled		NoAutoRebootWithLoggedOnUsers 0	

Table-2 Recommended values for the behavior of Automatic Updates

4.6 Limitations

Though very good as it meets most of our needs, Microsoft's SUS does have a few limitations:

- It does not push out service packs; the system administrators need to use a separate solution for new service pack.
- It requires Windows 2000 and up, so it cannot patch Windows NT 4 systems.
- It only handles patches at operating system level (including Internet Explorer and IIS), but not application patches such as Microsoft Office, Microsoft Exchange Server, Microsoft SQL Server, etc. This requires not only additional installation steps needing to be done, but also some efforts in keep track the patch history by a system administrator.
- It cannot deploy custom patches for third party software.
- It does not allow a system administrator to scan the network for missing patches. This also requires some additional efforts from the system administrator to use other tools to check out whether everything has been installed correctly.
- Another problem with SUS is that it lacks of granularity, i.e. it is not possible to distinguish who gets what patch without a complex infrastructure with multiple SUS servers. With this limitation, every automatic update client will download and install every approved

update on the SUS server it connects to. In case of different requirements for different groups, the best way is to establish one or more separate SUS servers for each sub-group (see installation section).

5. Patching System Validation and Security Enforcement

5.1 Patching system validations

In order to validate if the process does its job, it is helpful to determine whether the patches and service packs are successfully applied and installed on the system. In this section, we are concerned with three validations: Patch installation, Security, and Performance validations.

5.1.1 Patch installation validation

This validation is executed with the aid of tools by employing scan techniques.

There exist many tools either commercial or free software to check the patch status on computers. In this section, we present three free tools: one from SysInternals, and two from Microsoft.

PSInfo

PSInfo is an excellent diagnostic application. It provides patch stauts and other system information. The canning output of a workstation is shown in Figure 9.

The “-h” switch shows hotfixes by Microsoft knowledge base article, and the “-d” switch displays disk volumes.

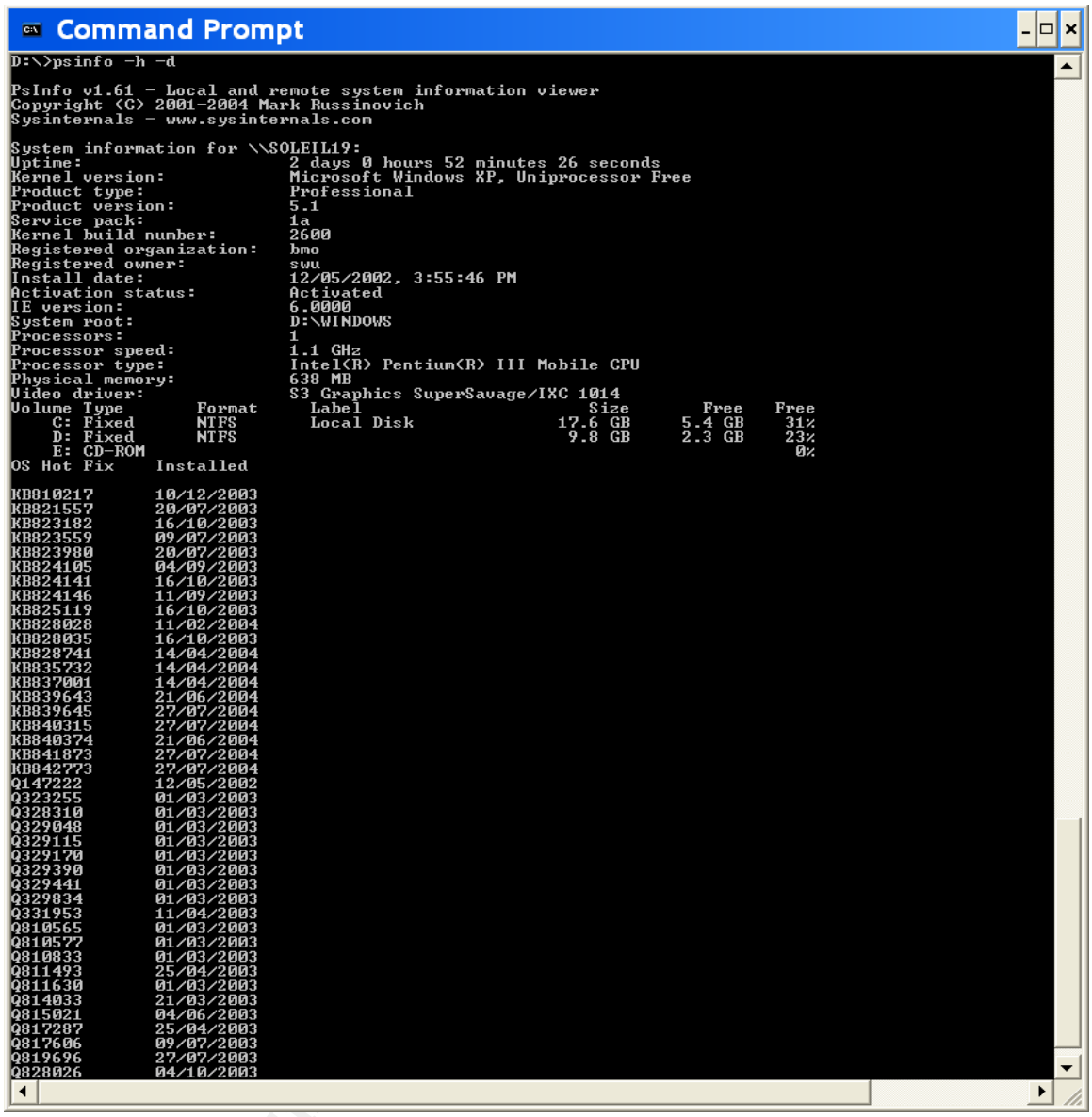

Figure 9 the sample output of running PSInfo

MSBA

For Microsoft operating systems, IIS Servers, and SQL Servers, there is a graphical tool called MS Baseline Analyzer (MSBA). This tool, provided freely by Microsoft, gets updated patch information from the web browser every time it is run. It quickly reports what security updates are missing and checks for basic security practices over the system. This tool can be used to scan single computer, or a range of computers. It stores past reports for late review. Each result has additional information about what was scanned, result details, and how to correct the problem.

Figure 10 an example output of running MSBA

Unfortunately, with actual version the scanned information about patch level on the scanned computers is often incorrect. But it's a good start for a preliminary estimation on the patch status over the computers.

Hotfix Checker

Another simple and powerful tool is the command line utility: HFNetChk.exe (Note: this executive program named ***mbsacli.exe*** is included in MSBA package of veriosn 1.2). This tool is developed for Microsoft by Shavlik Technologies. HFNetChk relies on an XML file that defines the current list of updates and service packs that Microsoft has released. If the machine running the tool is connected to the Internet, the tool will download and use the current version of the XML file on the fly. In order to scan machines not connected to the Internet, the XML file can be downloaded manually and identified using command line switches when HFNetChk is executed. HFNetChk can individually scan stand-alone machines or machine groups remotely. It can produce various formats of reports, and also scans for updates to a large number of Microsoft operating systems and applications, excluding Office.

Because HFNetChk is command-line based, it can easily be set up to run as a Windows scheduled task to scan a group of machines on a regular basis and generate reports to be reviewed by administrators to determine patch compliance.

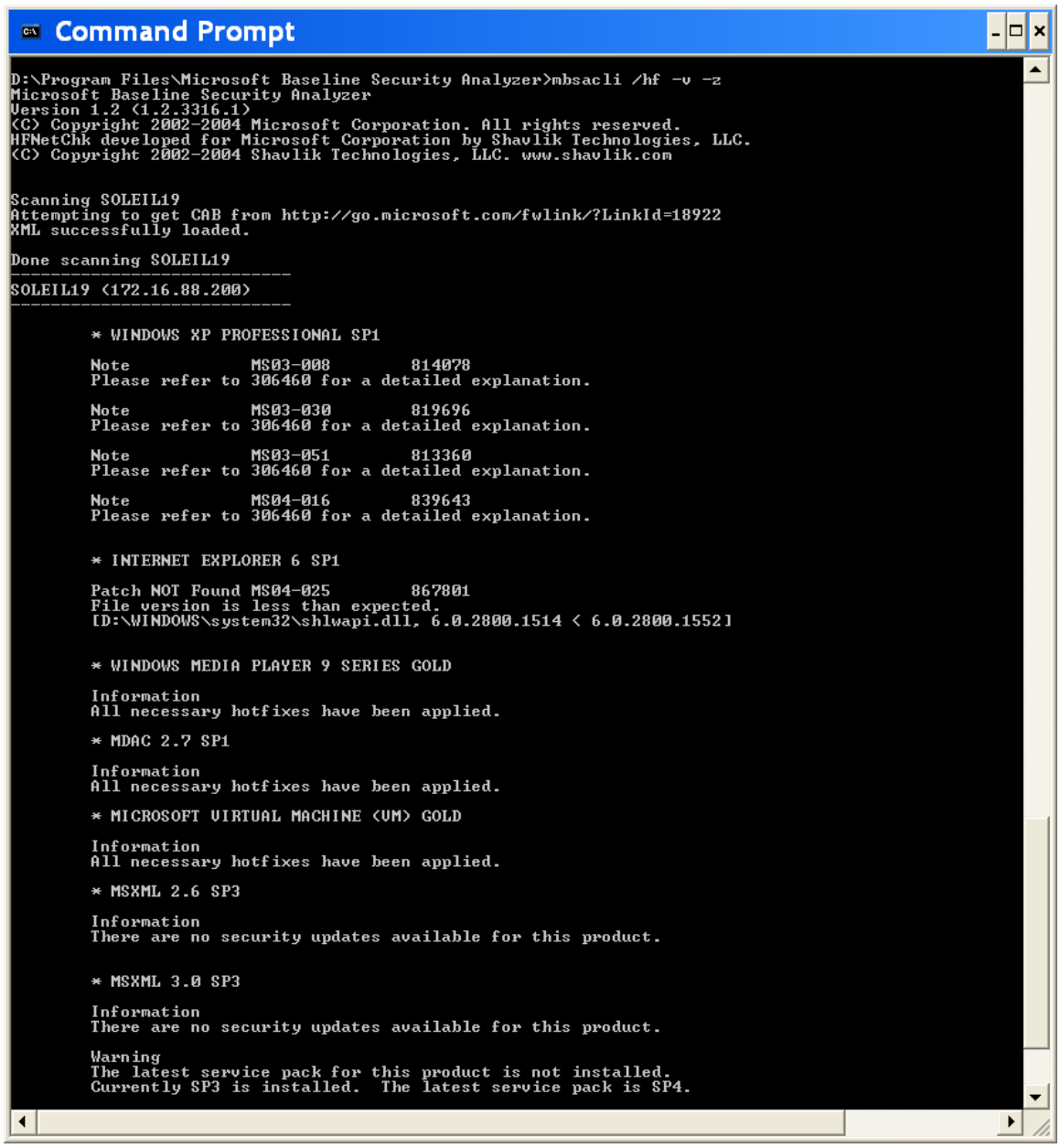

Figure 11 the sample output of mbsacli.exe

It is worthy noting that MSBA builds upon HFNetChK, and adds a graphical interface to it. MSBA also checks a number of windows security settings such as local account password policies, whether the file system is NTFS, and Internet Explorer security zones.

5.1.2 Security validation

Are the patch system and its data secure?

One area that is particularly lacking in the documentation that accompanies SUS is the lack of discussion dealing with the host computer's security. As with any web or application server, SUS can only be as secure as its underlying operating system. Though Microsoft has taken some necessary steps to ensure the integrity of the patches installed by clients, there are no absolutes. As mentioned earlier, there is still the danger that someone with access to the SUS server could potentially alter the patches or (a more likely scenario) damage them to prevent distribution. With this in mind it is vital that administrators use recognized best practices on their SUS servers. These best practices would include eliminating unnecessary services, disabling file and print services (though this may not be possible if the machine is not a dedicated SUS server), disabling NetBIOS over TCP/IP (again this may not be possible in some environments), using security templates to lock down the server, using IPSec to encrypt traffic to non- web related ports and potentially doing periodic.

Since a SUS server requires IIS server to function, recommended best practices (see [1]) on securing IIS are followed. Most of job can be done by using IIS lockdown tool for Windows 2000. (http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&displaylang=en).

5.1.3 System performance validation

As pointed out in one of SUS deployment white papers entitled "Deploying Microsoft Software Update Services" by Microsoft, a SUS can handle approximately 15,000 clients. In order to make enough room for systems' performance the GIAC uses the half of this number (i.e. 7,500) as a threshold to determine if it is necessary to set up an additional SUS server for a specific networking zone. In the GIAC case, most zones contain client computers of much less than 7,500. Only in the Desktop Zone (see Figure 1) at Toronto headquarter the number of client computers approaches this. In order to have an optimal performance and security, the GIAC decided to set up two SUS servers for this zone.

After setting up these servers, the local administrators led by their senior manager have conducted a web load stress and performance test. The detailed testing cases and results are reported to the PMG, and not presented here because it is out of this paper scope.

Another particularity of this Desktop zone is that most desktops will be shutdown during the night so that the normal scheduled update time during the night for servers is not appropriate for the most clients in this zone. With due diligence, the PMG along with LSOs has revised the automatic update schedule for this zone's

clients to make sure that the clients in different departments have different time slots for their patch updates during working hours.

5.2 Other Security Measurements

Is patch management enough?
The answer is negative. In addition to implementing effective patch management practices, several additional steps beyond patch management can be considered when addressing software vulnerabilities and malicious hackers exploiting these vulnerabilities. These are:

5.2.1 Windows System Hardening

Although it is very important for a computer system staying current with current security vulnerabilities and their patches/hot-fixes, it is more important to make an appropriate hardening on the computer itself before it goes to production. The GIAC management has a strong requirement to the system administrators to know how to hardening the Windows system in accordance with SANS Windows hardening guidelines [16]. Furthermore, the company has established a good training program for the administrators to keep their security knowledge and professional certification current.

5.2.2 Anti-Virus Management

It is well known that the windows platform is a major target for many viruses. The company has established a particular policy to cope with this risk. This policy dictates that every workstation and windows servers should use anti-virus software signatures updates and virus scan should be automatically executed at least once a day.

In order to enforce this policy, the company has carefully chosen an anti-virus software of enterprise version that allows the administrators at the headquarter to initiate remote scanning and signature status checking to every workstations throughout the whole company. In case of any problem found by the central servers, such as an obsolete dat file on a computer, the server can automatically push the new dat file onto the computer without knowing by its users.

5.2.3 Intrusion Detection and Management

In the protection of the organization from hazards, it is generally considered that firewall provides the first line of defense. However, for a completed protection, using only firewall is not sufficient. One needs to build the defense in depth and in hierarch. This means that one needs to build the second and even third line of defenses. In order to achieve this, people are increasingly using IDS (Intrusion Detection Systems) to make the defense more solid and complete than that with only firewall in place.

An IDS helps the system administrator to see how their systems and networks are scanned, probed and possibly exploited, not only from outside the

organization but also from inside. There are two kinds of IDS: network-based or host-based. For a comprehensive coverage for such a company like GIAC, using both systems could be quite cost. For this reason, the company has decided to deploy network-based IDS as the first step to some critical points of the network. The next step is to deploy host-based IDS onto the critical servers.

5.2.4. Disaster Recovery

Disaster Recovery is considered one of important security measures by the company's executives. It is planned carefully and extensively. The full description of this plan is out of scope of this paper. However, we outlines below some important points as concrete support to the company's business continuity plan.

All production servers in the whole company are backed up weekly with a full backup and nightly with a differential backup. The weekly full backup tapes are kept offsite in a secure location with two years retention before the tapes are recycled.

Once per quarter, the domain controllers are brought offline in turn to make Ghost image and burnt to CDs. These CDs are sent out to a secure location offsite with the backup tapes. This image will allow for a rapid recovery of our Active Directory domain in case of a disaster.

Disaster recovery plan is tested twice a year. This is done by completing practice scenarios at the contingency site. A rotation is established so that all administrators will have an opportunity to become familiar with the procedures and have hands-on experience recovering the network.

6. Conclusions

Effective and efficient patch management is more important than ever for a corporation to remain competitive. It helps maintain operational efficiency and effectiveness, overcome security vulnerabilities, and preserve stability of the production environment.

With a well established patch management, system administrators will know exactly what resides on each server and desktop, and will be able to quickly manage risky software and services before hacking or infringement becomes an issue.

With a vigorously defined process in place, the GIAC is able to respond more quickly to security vulnerability and ensure the appropriate patches installed onto the needed systems. Most importantly this process is scalable and can be automated in processing risk management and remediation to an acceptable level, so as to save the staff's time and company's money while closing the window of opportunity for possible vulnerability exploitation.

Bibliography

[1] Fossen, Jason “Securing Windows” SANS Course Material
[2] Cert Coordination Center, “CERT/CC Overview”, http://www.cert.org/present/cert-overview-trends/module-1.pdf
[3] Minasi, Mark, et al. “Mastering Windows 2000 Server Third Edition”, Sybex 2001
[4] Microsoft Corporation “Microsoft Solution for Securing Windows 2000 Server -- Chapter 3 - Understanding the Security Risk Management Discipline”, URL - http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/03secrsk.mspx
[5] Microsoft Corporation “Patch Management Using Microsoft Software Update -- Chapter 1 - Introduction”, URL- **http://www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsus/pmsus251.mspx**
[6] Microsoft Corporation “Microsoft Security Guidance Center: Patch Management Index”, http://www.microsoft.com/security/guidance/topics/PatchManagement.mspx
[7] Information Technology Security, Practices & Checklists/Implementation Guides. **http://www.csrc.nist.gov/pcig/cig.html**
[8] Nicolett, M., Colville R., “Robust Patch Management Requires Specific Capabilities”, Technology, T-19-4570, 18 March 2003, Gartner Group
[9] “Patch Management Using Microsoft Systems Management Server - Operations Guide” http://www.microsoft.com/technet/technet/itsolutions/msm/swdist/pmsms/pmsmsog.asp
[10] NIST Special Publication 800-40, “Procedures for Handling Security Patches”, August, 2002
[11] Microsoft Corporation “Why Service Packs are Better Than Patches”, http://www.microsoft.com/technet/archive/community/columns/security/essays/srvpatch.mspx
[12] Microsoft Corporation “Microsoft Security Response Center Security Bulletin Severity Rating System (Revised, November 2002)”, http://www.microsoft.com/technet/security/bulletin/rating.mspx
[13] Colville, R., Wagner, R., Nicolett, M., “Patch management Benefits, Challenges and Prerequisites”, DF-18-0680, 4 November 2002, Gartner Group.
[14] IT Infrastructure Library Service Support (CCTA), Jun 2000, ISBN: 0-11-330015-8
[15] MSCEworld, ” Microsoft Software Update Service (SUS)”, http://www.petri.co.il/sus.htm
[16] The SANS Institute “Securing windows 2000 – Step by Step”, Version 1.0 May, 2001
[17] Microsoft Corporation ” Deploying Microsoft Software Update Services”, Jan, 2003

Appendix A: Windows Auto-Update Registry Values

This appendix presents the value definitions for the key:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU

Value name: **NoAutoUpdate**
Value data: 0 or 1

- 0: Automatic Updates is enabled (default).
- 1: Automatic Updates is disabled.

Registry Value Type: Reg_DWORD

- Value name: **AUOptions**
  Value data: 1 to 4
  - 1: Keep my computer up to date has been disabled in Automatic Updates.
  - 2: Notify of download and installation.
  - 3: Automatically download and notify of installation.
  - 4: Automatically download and scheduled installation.

  Registry Value Type: Reg_DWORD

- Value name: **ScheduledInstallDay**
  Value data: 0 to 7
  - 0: Every day.
  - 1 through 7: The days of the week from Sunday (1) to Saturday (7).

  Registry Value Type: Reg_DWORD

- Value name: **ScheduledInstallTime**
  Value data: *n*, where *n* equals the time of day in a 24-hour format (0-23).
  Registry Value Type: Reg_DWORD
- Value name: **UseWUServer**
  Value data: Set this value to 1 to configure Automatic Updates to use a server that is running Software Update Services instead of Windows Update.
  Registry Value Type: Reg_DWORD
- Value name: **RescheduleWaitTime**
  Value data: *m*, where *m* equals the time to wait between the time Automatic Updates starts and the time it begins installations where the scheduled times have passed. The time is set in minutes from 1 to 60, representing 1 minute to 60 minutes)
  Registry Value Type: Reg_DWORD