Global Information Assurance Certification Paper

Implementing a Secure WebDAV System

Richard Ross
GIAC Security Essentials (GSEC)
Practical Assignment
Version 1.4b, Option 2
5 August 2004

Abstract

This paper describes the process of implementing a secure remote file sharing system using WebDAV. It tells why a remote file sharing system is needed, how a secure solution is implemented and assesses the security of the solution.

What is WebDAV

"Briefly: WebDAV stands for "Web-based Distributed Authoring and Versioning". It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers."[1]

Before

The Old Way of Doing Business

Employees in our company tend to work on short-term contracts or support multiple customers at multiple locations including the corporate office. Because of this, many of them use the corporate file servers to store and share their data. We issue them laptops and provide remote connectivity to the company intranet and file servers using VPN or dial-up. This allows them to not be constrained with coming to the office and they can have immediate access to the corporate resources. By using our laptops and corporate network for customer work, our employees experience the following benefits:

- They can work at home, while traveling, while at our office or while at their customer location
- They can backup or store data on our file servers
- The data they store is backed up nightly to tape
- The data on our file servers can be shared by several employees
- The data on our file servers can be accessed by the same employee working at different locations
- Employees can use our corporate e-mail as a single point of contact if they are working multiple contracts or change contracts frequently
- They have reach back to other employees across the company to help solve problems

What Changed

Upper management in the company decided that there were a number of significant risks in taking the company laptop to a customer location and having access to the corporate network/e-mail from the customer location. There were several reasons for this decision. Some of them were security related and some were problems with perception.

On the security side, one of the problems is that a customer or competitor may inadvertently or otherwise see company proprietary data. A malicious competitor

[1] http://www.webdav.org/

or customer could also attempt to break into the laptop while the employee takes a break, goes to lunch, or is otherwise distracted. Although we use mandatory screen saver timeouts that lock the laptop and require user ids and strong passwords to gain access to the laptop, this risk was seen as too great. Also, since some of our work involves government classified data, there is a risk that an employee could inadvertently put classified data on the laptop and transfer it to the company network.

On the perception side, company leaders were worried that our customers or competitors may perceive that we are doing work that is not contract related. Our employees are routinely working on proposals for new work or renewal of current work. This work is not chargeable to the customer. Although most of this work is done at the corporate office or at home, some employees will spend their lunch time or other non-chargeable time at the customer location doing this type of work. Depending on their work location, it may not be feasible to go to the office and the time constraints may require a quick turnaround.

Because of these risks, the employees were told that they could no longer take their laptops to customer locations or access the corporate network from customer locations. Laptops could only be used at the company offices, employee's homes, or at hotels while traveling.

What's the Solution

Because the laptops and the connectivity they provided back to the corporate network had become such an integral part of the tool set we bring the customer, simply removing them left several of the employees in a rather difficult situation. One of the biggest problems the employees now faced was the ability to access and store files on our corporate file servers. To solve this problem, we decided to implement a web-based solution on a separate network using WebDAV. The WebDAV server will provide a file storage area that is not on our corporate servers, yet is still available via an internet connection. Our office already has a second T-1 that is currently used by sub-contractors that work in our office and by customers when they are visiting our office. To implement the WebDAV solution, all we need to do is purchase a domain name, point it to our external IP address and build a WebDAV server. With a WebDAV server, any employee needing to share or store files only needs a connection to the internet. Most employees already have a LAN account on their customer network or a broadband connection at home. The rules of engagement will be:

- The server is only to be used for customer work
- No company data will be placed on the server
- Government For Official Use Only (FOUO) will be allowed on the server. Because of the location and physical security of the server, it meets our requirements to protect FOUO
- The server is not approved for classified storage

This solution will in some ways improve our employee's way of doing business. When using their laptops, our employees were mostly dialing into our corporate network because they were not allowed to connect their laptops to customer networks. This solution allows them to use a customer computer and access their files at LAN speeds rather than dial-up speeds.

During

Set up a test environment

Before I could get approval to proceed with this solution, I needed a "proof of concept" to verify that the solution would work and that it would be an acceptable solution for the effected users and managers. So, I put together a test system that employees could play with and management could see in action.

I built the system using an old Dell PowerEdge 1550 sitting on the shelf waiting to be returned from lease. The T-1 I am using comes in on a Prelude CSU/DSU, then to a Cisco 1705 router. The router connects to a 3COM switch. From there, the network is split into several sub-networks, each behind its own workgroup router/firewall. This particular network is sitting behind a Cisco PIX 501 (Figure 1).

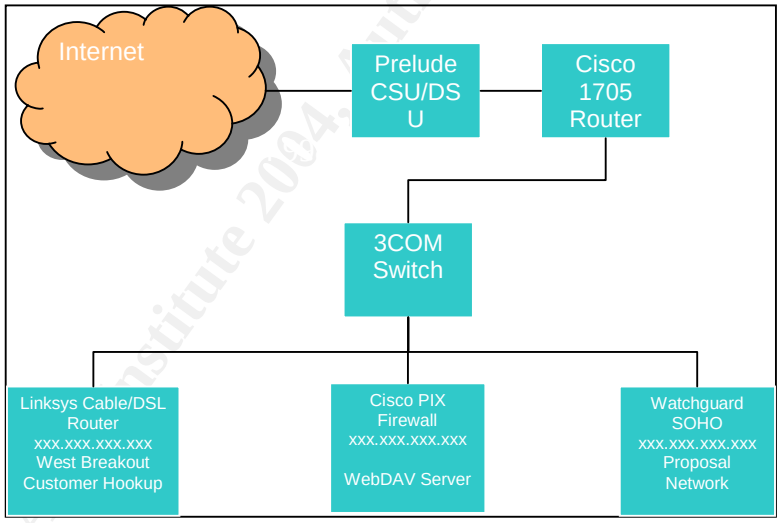

Figure 1 – Network Layout

Our corporate intranet developer secured the domain name from Register.com and directed it to our local IP address.

The first step to building the WebDAV server was to install Windows Server 2003 using the defaults on a 12 Gb partition. After the server was up and running, I downloaded all the current Critical Updates from the Windows Update service (http://v4.windowsupdate.microsoft.com/en/default.asp). Once all the latest patches were installed, I set up an Active Directory domain with the server as the only member. We have an existing license for Symantec AntiVirus Corporate

Edition 8.0 for our office PCs, laptops and servers, so I installed that to meet virus protection requirements. Next, I created an extended partition using the remaining disk space so that the data and web site can reside on a partition separate from the operating system.

Since Server 2003 doesn't install most services by default, IIS 6.0 needed to be installed.[2] I used the "Configure your server" wizard to install IIS 6.0. After installing IIS, it is configured and managed using the **Internet Information Services (IIS) Manager** (Figure 2). This can be found in Start | Programs | Administrative Tools. After launching the IIS Manager, the first thing I did was delete the default web site that was created when installing IIS. After that, I went to **Web Service Extensions** and set **WebDAV** to **Allowed**. Next, I created two folders on the d:\ drive. One is used to hold the web site front end and the other is used to hold the WebDAV folder. Going back to the IIS Manager, I created a new web site. This is done by right clinking **Web Sites** and selecting **New** -> **Web Site**. The path for this site is the folder I created on the d:\ drive for the web site front end. After the site was created, I created a Virtual Directory by right-clicking the site and selecting **New** -> **Virtual Directory...** The path for this is the folder created for WebDAV on the d:\ drive.

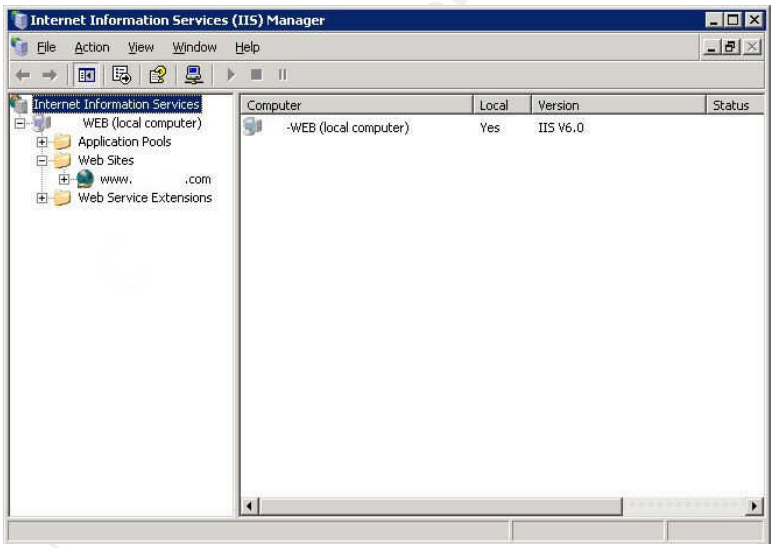

Figure 2 – IIS Manager

The following properties needed to be set for the web site in the IIS manager. These are accessed by right clicking the web site, and selecting **Properties**. On the **Directory Security** tab, I ensured **Authentication and access control** was set to anonymous. This is set by clicking **Edit** and checking **Enable anonymous access** (Figure 3). This allows any visitor to see the main page.

[2] http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/default.mspx

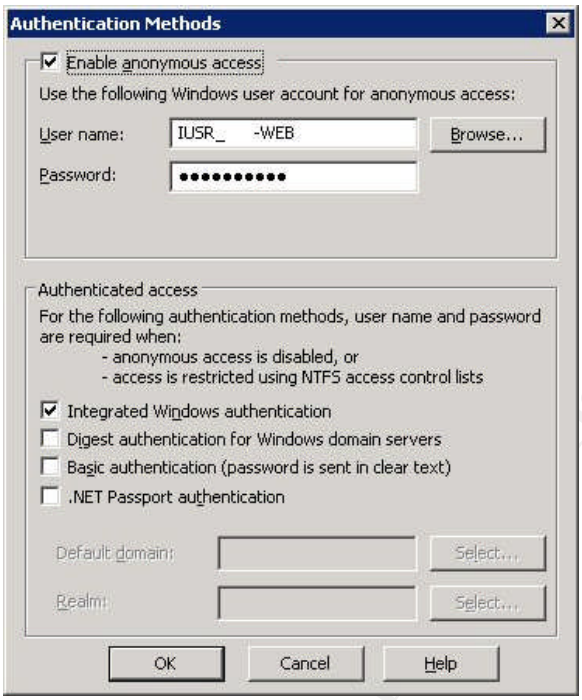

Figure 3 – Authentication Methods

To set up SSL, the following properties were set for the WebDAV folder. These are set by right- clicking the Virtual Directory that was created and selecting **Properties**. On the **Web Site** tab, I entered **443** in the **SSL Port** field. On the **Virtual Directory** tab, I checked the following:

- Script Source Access
- Read
- Write
- Directory Browsing
- Log Visits

I also set **Execute Permissions** to **Scripts and Executables** (Figure 4). These all needed to be set so that the user can store executable files in the WebDAV folder as well and non-executable files. On the **Directory Security** tab, after clicking the **Edit** button I made sure that the only thing checked was **Integrated Windows Authentication**. Under **Secure Communications**, click **Edit** and check **Require Secure Channel (SSL)** and **Require 128 bit Encryption** (Figure 5).

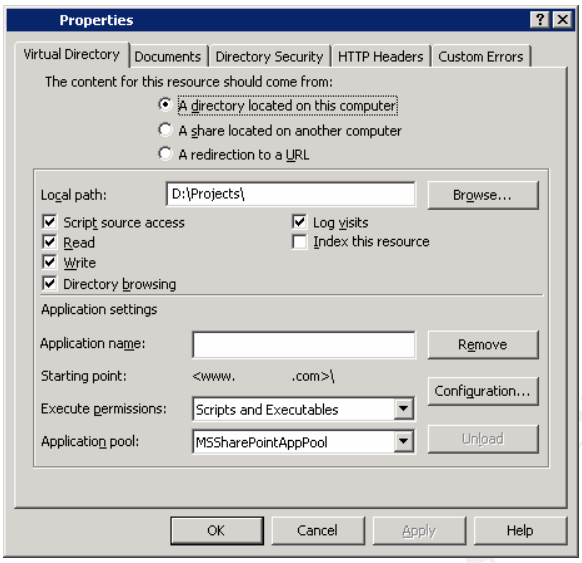

Figure 4 – Virtual Directory Properties

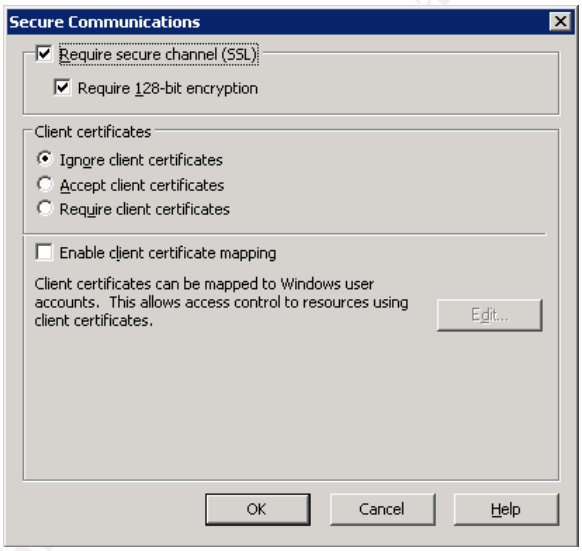

Figure 5 – Secure Communications

Finally, I needed an SSL certificate so that SSL and 128 bit encryption would actually work. Since the system doesn't need a verified certificate right now, I loaded an SSL certificate into the web site using the **IIS 6.0 Resource Kit**. I elected not to go with a certificate from a Trusted Authority such as VeriSign because I only needed to encrypt the connection. If it becomes necessary to assure the user that the site is authentic, I can purchase a certificate from a Trusted Authority and install it later. For the initial deployment, my goal was only to have an encrypted connection. The IIS Resource kit can be found at http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en. Once this is downloaded, just double-click the executable and install it on the server. The SelfSSL program is found in the **IIS Resources** program group accessed through the Start menu. The program will bring up a command prompt and display the available switches.

The command I ran is **selfssl /T /K:2048 /V:365 /S:1390543837.** /T puts the certificate in the list of trusted certificates on the server. 2048 is the key length. 365 is the number of days the key is valid. And 1390543837 is the web site identifier. Using this command, the command generated a 2048 bit key that is good for 365 days and installed it to the web site identified with the /S switch and also put the certificate in the trusted certificates list for the server. The web site id can be found in the **IIS Manager** and clicking on **Web Sites**. The right pane shows all the web sites on the server. The second column contains the web site identifier. After setting this up, when someone tries to access the WebDAV portion of the web site, they are forced to use a 128 bit SSL connection. They also have to accept the certificate each time because it does not come from a trusted authority that their system recognizes.

The final step I did was set up a single web page with a link that opens the WebDAV site as a web folder. The HTML to open the web folder is:

```
<a FOLDER="https://www.yoursite.com/WebDAVFolder/"
TARGET="_blank" href="https://www.yoursite.com/WebDAVFolder
"> </a>.
```

I named the file index.html and put it in the folder on the d:\ drive that was created to hold the web site front end.

To test the solution, I selected two technically competent users from the group that will ultimately use the solution. I created their user accounts using the Active Directory Users and Computers Snap-in. They accessed the site from within the corporate office, from their customer location and their homes. In all cases, they were able to add, delete and modify files. They found the solution to be easy to use, fast and met their needs.

My final hurdle was to convince management that this was a good solution. I put together a briefing describing my solution and forwarded it to my boss and the managers in charge of the end users. I also created accounts for them so that they could test drive the solution. The user's managers loved it because met their needs. So, we decided to implement it.

Set Up and Secure the Operational System

For the operational system, I purchased a Dell PowerEdge 2650 server and a Dell PowerVault 110T DLT tape drive. I followed the same installation as the test system. Windows Server 2003 is hardened pretty well by default. However, there are a few things to make it a little more secure. To secure the IIS server, I used some of the guidelines provided by Microsoft® in the "Windows Server 2003 Security Guide".[3] Some of the suggestions used were renaming the administrator account, putting the web site on a dedicated volume other than the operating system volume, enable logging, installing only the components necessary to do what we want, enabling only the necessary web service

[3] http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

extensions and installing an antivirus solution. The components I installed for the Application Server were:

- Enable network COM+ Access
- Internet Information Services (IIS)
    - Common Files
    - Internet Information Services Manager
    - World Wide Web Services
        - WebDAV Publishing
        - World Wide Web Service

The rest of the services were the default services

The antivirus solution is Symantec Antivirus Corporate Edition 8.0

The web site and WebDAV folders are on the d:\ drive, separate from the operating system.

Logging is turned on and will be discussed later.

The next thing that needed to be installed and configured is a backup solution. I purchased a Dell PowerVault 110T DLT drive for backups. It is a single DLT drive. There was no need for a drive that supports more than one tape at this time. I don't expect to have a huge amount of data to back up. The software I am using is Veritas NetBackup 5.0. This is the solution we are using on our corporate servers, so it made sense to use it here. With NetBackup, you basically create policies for how you want your data backed up. The policy I set up will do a full backup Friday night and an incremental backup daily Monday through Thursday.

One final change I made to the operational system was to give the users the ability to change their passwords via a web interface. Since the server is the only computer on the network and the users do not have physical access to it, they need another way to change their passwords. Windows Server 2003 comes with some web administration tools that allow you to build a web interface that will let users change their passwords.[4] To set this up, create a new Virtual Directory in the web site called IISADMPWD. The path for this virtual directory will be c:\windows\system32\netsrv\iisadmpwd. On the Virtual Directory tab, all that should be checked is **Read** and **Log Visits**. **Execute Permissions** should be Scripts Only. Under the Directory Security tab, turn off the setting to allow anonymous access and require it to use SSL and 128 bit encryption. The procedure is the same as for setting up the WebDAV virtual directory. The certificate loaded before will work to set up the SSL connection. Next, you need to allow Active Server Pages to run on the site. To do this, in the IIS Manager, Click on **Web Service Extensions** and set **Active Server Pages** to **Allow**. Finally, to give the users easy access to this feature, add a link to the main web page. The html to do this is:

[4] http://www.winnetmag.com/Article/ArticleID/42407/42407.html

```
Click<a title="https://yoursite.com/iisadmpwd/aexp2b.asp"
target="_blank"
href="https://yoursite.com/iisadmpwd/aexp2b.asp">here</a>
to change your password</p>
```

Lock Down the Firewall

One of the most important things to secure the system is to lock down the firewall so that the only communication allowed in is the communication I want. This is also important due to the fact that the only access to the server is through the web interface or by gaining access to the communication equipment room and logging on to the server itself. I used "Configuring and Troubleshooting the Cisco Secure PIX Firewall with a Single Internal Network"[5] as a guide on how to limit access through the firewall. I added the following static commands to the firewall:

```
access-list outside_access_in permit tcp any host xxx.xxx.xxx.xxx eq
https
access-list outside_access_in permit tcp any host xxx.xxx.xxx.xxx eq
www
static (inside,outside) tcp interface https 192.168.1.10 https netmask
255.255.255.255 0 0
static (inside,outside) tcp interface www 192.168.1.10 www netmask
255.255.255.255 0 0
access-group outside_access_in in interface outside
```

The end effect of these commands is that the only traffic allowed through the firewall and routed to our server is http or https. This will be verified later using nmap.

Physical Security

Physical security is extremely important because the server will potentially store government FOUO data. The T-1 terminates in our Communication Equipment Room. All equipment including the server, firewall, and router are located there as well. This room is accessible only by company IS and company Security personnel. Access is controlled with a proximity card reader. There are no other computers on the sub network with the WebDAV server. The server can only be accessed by someone connecting through the internet or logging onto it directly.

After

Does it Meet the Users' Needs

The system has been up and operational for approximately three months now. I am getting more requests for access to it. Our employees travel a great deal and they are finding it extremely useful as a place to store data they need while traveling, at their customer location, or at the office. Another sign of success is that one of our other locations is implementing a similar solution based on this design.

[5] http://www.cisco.com/warp/public/110/single-net.shtml

One request I have had and will add on later is an e-mail system. It will most likely be a web-based system and the users will be forced to use a 128 bit SSL connection like the WebDAV implementation. The only change I will need to make is to open the firewall for smtp, pop3 and a WebMail port.

Assess the Security of the System

Using the "SANS Security Essentials Cookbook"[6], I analyzed the server with the Secure Domain Controller template. The only discrepancies were the minimum and maximum password age and the setting for "Domain member: Digitally encrypt or sign secure channel data" settings. The server is set to 1 day, 180 days, and disabled for these settings. The security template recommends 2 days, 42 days and enabled. I believe these are reasonable settings for my implementation. Because he system remembers the last 24 passwords used and the minimum age is 1 day, the user would have to change his password 24 times in 24 days to cycle back to the password he just changed. Also by forcing a strong password, I think 180 days for maximum password age is a good compromise. The password is reasonably difficult to break and the user only has to memorize a new password every six months. Finally, there is no need to enable "Domain Member: Digitally encrypt or sign secure channel data" because the server is the only member of the domain. There are no domain members to communicate with it.

I also ran an nmap[7] session to verify that the only open ports going to the server were the ones I wanted to go to the server. I used Knoppix STD 0.1[8] to execute the nmap scan. Figure 6 shows the results of the nmap scan. The only open ports are 80 and 443 which are used for the http and https connections.

```
# nmap 3.48 scan initiated Fri Jul 23 18:33:57 2004 as: nmap -sS -O -p-
-PI -PT -oN nmap.txt xxx.xxx.xxx.xxx
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on xxx.xxx.xxx.xxx:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows Server 2003 Enterprise Edition, Microsoft
Windows 2000 SP3

# Nmap run completed at Fri Jul 23 19:20:47 2004 -- 1 IP address (1
host up) scanned in 2809.645 seconds
```

Figure 6 – NMAP Port Scan

[6] SANS Security Essentials Cookbook Version 1.0, p 22-1
[7] http://www.insecure.org/nmap
[8] http://www.knoppix-std.org/

What are the threats to the system?
Since the role of the system is data storage, the threat faced is compromise of the data. This can be in the form of gaining access to the system either physically or through the internet, or by capturing the data as it is transmitted.

How do we mitigate the threats?
These threats have been mitigated by the following methods:

- **Physical Security**. The server is in a controlled room with very limited access
- **Transmission Security/Confidentiality**. All communication with the server and transmission of data is 128 bit SSL encrypted. Also, by setting the firewall to only allow http or https traffic, the threat of network based attacks such as Blaster or Welchia are greatly diminished.
- **Operations Security**. Users are required to use a strong password that is at least 8 characters in length. They must change their passwords every 180 days or less.
- **Availability/Backup**. Regular full and incremental backups ensure the data will still be available if the server crashes.
- **Integrity**. The integrity of the data is maintained because access is restricted to the users of the data and all communications are encrypted. Of course, they can mess it up, but the protections in place can reasonably assure the user that the data they store has not been tampered with.

How to Maintain the System

Now that the system is set up and operational, what needs to be done to maintain the system and verify it is still secure? The first three items in the list will keep the system protected from attack.

- **Windows Updates**
  Windows Server 2003 has the same Automatic Update feature of the other Windows products. I set the Automatic Update service to keep the system up to date automatically by downloading and installing any critical updates everyday at 3:00 AM. Turning this feature on will ensure that the server has the latest security and critical updates in a timely manner without my intervention.
- **Virus Updates**
  Symantec Antivirus Corporate Edition gives the user the ability to schedule live updates. It is scheduled to automatically update virus definitions at 8:00 PM every evening. By keeping virus definitions up to date, the system is protected from virus attacks.
- **Backup**
  A full backup of the server is accomplished every Friday evening and incremental backups are accomplished Monday through Thursday

evening. Having frequent backups will ensure the data is not lost in the event of a server crash.

The next three items are critical to detect system attacks or compromise. Due to the size of the system and the simplicity of the system, I elected not to install any type of intrusion detection or monitoring tools. I am using various log files to keep track of system activity.

- **Web Logs**
  The IIS 6.0 Resource Kit contains Microsoft's LogParser tool which can be used to parse the IIS log files in several different ways. Security Focus has a very good article with different ways to apply this tool and more effectively analyze the complex log files generated by IIS.[9] The log files will be checked weekly using this tool.
- **Windows Event Viewer**
  The Windows Event Viewer will be checked weekly. Particular emphasis will be placed on the Security, Application, and System events.
- **Firewall Logs**
  Finally, the PIX has a web-based administrative interface called PDM (PIX Device Manager). The SYSLOG can be easily viewed through this interface. It will be checked weekly as well.

Conclusion

WebDAV is a great extension to http and has many benefits over other remote file sharing methods such as ftp. Because it uses http, we get the benefit of a highly secure connection using https. Also, the user gets the benefits of being able to use a web browser to access their remotely stored data. The interface presented looks just like any other Windows folder. By applying several layers of security such as physical access to the data server, limited access through the firewall, and strong encryption of the transmission, the user has a secure, yet easy to use remote file sharing system.

[9] http://www.securityfocus.com/infocus/1712

Bibliography

WebDAV Resources
http://www.webdav.org/

Internet Information Services 6.0 Technical Reference
http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/default.mspx

Windows Server 2003 Security Guide
http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

Q. Does Windows Server 2003 provide a way to let users change their passwords remotely on the Web?
http://www.winnetmag.com/Article/ArticleID/42407/42407.html

Configuring and Troubleshooting the Cisco Secure PIX Firewall with a Single Internal Network
http://www.cisco.com/warp/public/110/single-net.shtml

SANS Security Essentials Cookbook Version 1.0, p 22-1

Nmap
http://www.insecure.org/nmap

Knoppix STD
http://www.knoppix-std.org/

Forensic Log Parsing with Microsoft's LogParser
http://www.securityfocus.com/infocus/1712