Global Information Assurance Certification Paper

Creating a stable and secure connection from a remote website to the inside of a network

GSEC Practical (v.1.4) **RESUBMISSION** July 17, 2002
Tom Williams

Abstract

This paper will examine the best way to grant remote access to the network of a very small business for employees who are out of the office on the road. After examining the benefits and disadvantages of various commercial and homegrown options available, the paper will describe how to set up an FTP server with Microsoft's IIS (Internet Information Services), which is built in to Microsoft Windows 2000. The paper will then show how to harden IIS and then describe other measures to add defense in depth to the project.
The paper concludes that IIS is an acceptable way to share files for certain organizations, but only if extra steps are taken to harden the system, and only as long as the organization in question is extremely small with a trusted group of employees who have a modicum of technical ability.

Introduction

Humantail is a small consulting company with three employees who are often out on the road meeting with clients. There are four Windows 2000 Professional machines networked through a Gigafast EE 400-RP broadband router connected to the Internet through a cable modem. At present there is no web server running on any of the machines, but the company does have a website, which is hosted remotely by a hosting company.

The three employees of Humantail need read/write access to files on each of the networked machines, however, they do not need remote administration privileges, nor would they ever need to execute an application or service remotely. In addition, all the files they need access to are located in one folder per machine, and that folder has no other files in it- anything in the folder should be available, and nothing in the folder should not be available.

The Choices

There are several different ways to approach the objective of granting remote access to files on a host from a web browser. Which is the best choice depends heavily on factors such as the number of people needing remote access, the

technological sophistication of the users, and of course, budget.

Because the company isn't growing anytime soon, scalability is not a concern.

The administrator has several choices on how to connect remote users to their data. Due to budget limitations and the small scale of the project, several solutions can be discarded immediately. Several others should be discarded as insecure or too complex for end-users to manage, leaving us with two feasible options.[1]

VPN- Virtual Private Network. This is rapidly becoming one of the fixtures of corporate IT, providing fast and reliable remote access to a network as if they're right there in the office connected with an Ethernet cable straight to the network. VPNs are extremely secure now that IPsec (Internet Protocol Security) has been adopted as industry-standard. VPNs which use MPLS (Multiprotocol Label Switching) have the added advantage of reliable connection speeds, important for certain legacy applications and QOS (Quality of Service) agreements.

VPNs are not appropriate for this project because the remote user will not know which network they'll be using when accessing the host network, so authentication is impossible. They won't have a PC with a client already installed and a VPN would offer too much access to the host, such as the ability to launch applications.

RAS- Remote Access Services.
RAS is an excellent choice for a larger organization considering it is relatively inexpensive and easy to set up, but Humantail cannot afford to have its employees calling in via phone lines given the international reach of their business travels, nor is the host computer connected to the PSTN (Public Switched Telephone Network) as Humantail employees are 100% cellular-based. Another disadvantage is the slow speed that a dial up connection entails, especially considering that most public web access is now broadband.

Web-based remote access service providers.
There is a growing industry of web-based service providers who will provide a gateway between a private network and the Internet; examples include gotomypc.com (www.gotomypc.com) , pcAnywhere (www.symantec.com/pcanywhere), and LoudPC (www.loudpc.com). These services are certainly simple to operate, and vendors have taken many steps to earn the confidence of security managers. However, there are several inherent risks with these services that make them unsuitable for the project.[2]

---

[1] TechRepublic, Apr 6, 2000
http://www.techrepublic.com/article.jhtml?id=r00120000406bot01.htm&src=search&_requestid=77070

[2] Infosecurity, 1999 http://www.infosecuritymag.com/articles/1999/remote.shtml

First, the level of remote control is too high. Humantail only needs access to files. The employees will not need to access application files, change settings or any of the other remote capabilities pcAnywhere offers. Other inherent security concerns include the fact that pcAnywhere utilizes ports other than Port 80. Anytime a port is opened, an opportunity is given to hackers to launch a DoS (Denial of Service) or other attack, especially when they know which application is sitting and listening on the port, just waiting to respond to a command. Some experts are also concerned about the method that pcAnywhere uses when it initiates a client negotiation, fearing that its UDP (User Datagram Protocol) broadcast to the whole subnet could be logged and trigger a false alarm of "system wide attack".

The final nail in the coffin of web-based service providers is their very nature: Service Providers. As we have seen with the now-dead ASP (Application Service Provider) industry, Service Providers cannot be trusted to be in business next week. Furthermore, while they are more likely to have more resources dedicated to their internal security, they are also a monumentally larger target for hackers. Once their security is broken, say by a gang of professional Russian hackers, so is your security. And you'll never know because you don't have access to logs or other resources to conduct an audit.

Token or key-chain hard drive

Commercial token systems would not be appropriate for Humantail as the time and expense to set up and maintain is prohibitive.[3]

The Setup- Practicing Defense in Depth

After evaluating the other options, the most secure way to share files is by setting up a secure FTP (File Transfer Protocol) server on one of Humantail's production machines. There are several advantages to this method, for example, limiting the scope of damage that a successful attack (as remote control is not enabled) and reducing the reliance on any 3rd party service provider who could be compromised or unavailable (thus reducing availability, one of the three key missions of good security)

FTP also has some inherent weakness that require special attention to ensure the closure of security exploits, the traditional ones being allowing anonymous login and sending usernames and passwords in clear text.[4] These concerns will be addressed individually below.

---

[3] Infosecurity, 1999
http://www.infosecuritymag.com/articles/1999/token.shtml

[4] CERN Institute, June 2002
http://security.web.cern.ch/security/ftp/default.htm

Foundation- Harden the OS
The first and most important part of good security is a solid foundation. Unless your OS (Operating System) is secure, nothing is safe, all the more so when you start offering services into the machine.

Other papers and resources exist to secure a Windows 2000 machine. Microsoft and the Federal government offer excellent Best Practices papers at http://www.microsoft.com/technet/security/bestprac/default.asp and http://csrc.nist.gov/fasp/.

In short, to maintain a secure operating system, the administrator must keep up on Service Packs, practice a policy of least privilege, run regular virus checks, and establish then enforce the organization's Security Policy.

Microsoft also offers a template for basic Windows 2000 security available for download at http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q316347&.

Configuring IIS FTP server
Windows 2000 Professional comes with a built in FTP service as part of its *Internet Information Services* (IIS). Unfortunately, IIS is the battleground in a never ending battle between hackers discovering exploits and Microsoft releasing patches to fix the holes, so it is imperative that the service be hardened before exposing your IIS-enabled production servers to the Internet. It is equally important that Humantail's administrator keep up on the latest patches and hotfixes via Microsoft's Update service and stays aware of exploit warnings from organizations like CERT (Computer Emergency Response Team).

These warnings can be obtained at no cost through an email alert notice sent by Microsoft which can be subscribed to at http://www.microsoft.com/technet/security/bulletin/notify.asp .

As Microsoft itself says: "**Important:** You MUST stay on top of new security issues as they arise. This cannot be stressed enough." [5]

Hardening IIS
There are some smart precautions that would improve the security of the Humantail FTP site that cannot be implemented due to a lack of resources. For example, it is a best practice to host your FTP service on a stand alone server

[5] Microsoft, January 2001
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp

that doesn't host more confidential data[6]. This can't be implemented because Humantail requires access to live data on its production machines. It's not feasible to maintain a separate copy of files just for the FTP server.

Microsoft's Tech Support site details the procedures on how to harden the IIS service. Allaire-Macromedia rated this checklist in its white *paper "Security: Securing IIS How to Implement a Secure IIS Web Server"* as "the most thorough secure-implementation guideline available." [7]

- Set Appropriate ACLs on Virtual Directories
- Set Appropriate IIS Log File ACLs
- Enable Logging
- Set IP Address/DNS Address Restrictions
- Executable Content Validated for Trustworthiness
- Update Root CA Certificates at the IIS Server
- Disable or Remove All Sample Applications
- Disable or Remove Unneeded COM Components
- Remove the IISADMPWD Virtual Directory
- Remove Unused Script Mappings
- Check <FORM> and Querystring Input in Your ASP Code
- Disable Parent Paths
- Disable IP Address in Content-Location

Source: Microsoft,
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp

These steps drastically reduce the chance that an attacker can use a known weakness of an application, feature or service. Default settings are bad because the hacker knows what to expect. Removing unnecessary features reduces the opportunity for exploitation.

Encryption

Normal FTP is a non-encrypted protocol which means user names and passwords are sent across the Internet in clear-text.[8] This obviously poses an unnecessary security risk. However, by requiring an SLL (Secure Socket Layer) connection between the host computer and the FTP server, the risk can be reduced to almost zero: by encrypting the pipe, all the traffic inside it is invisible to snoopers.

---

[6] SearchSecurity.com, January 2002 (http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci790654,00.html)

[7] Macromedia, January 2001 http://www.bitpipe.com/data/detail?id=1020108274_293&type=RES&src=FEATURE_SPOTLIGHT&x=500080766

[8] SearchSecurity, January 2002 http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci790654,00.html

There are two options in setting up a secure server: Set up your own certificate and use IIS to manage a secure server, or use a third party application.

Setting up your own SSL connection

1. Set up a server side certificate using the Web Server Certificate Wizard (access via ISS/Default Web Properties/Directory Security/ Server Certificate).
2. Certify your Certificate with a third party CA such as Verasign or issue your own certificate. It's better to go with a third party as a self-signed certificate has no trust, but the fees involved range from $300 into the thousands.

Third Party Applications

There is a growing market for plug and play SSL solutions for Windows. All of the solutions below cost less than $600, just a little more than the cost of a certificate from a tier one CA (Certificate Authority).

WS_FTP, Ipswitch (www.ipswitch.com/Products/file-transfer.html)
Networkworld gave WS_FTP a very favorable review, and prefers this application to the Java ones described below. "WS_FTP Server has an extensive feature list, including many security attributes, and unlike the Microsoft IIS FTP service, the site command and stat command don't give anything away." [9]

SSH for Windows (www.ssh.com)
SSH for Windows was developed by SSH Communications Security, the same company that developed the original SSH standard, now the de facto standard for web security. Originally a Unix/ Linux based application, in June they released a Windows port of their technology. SSH is an industry standard, and the product enjoys a positive reputation in the security world, especially when implemented alongside IPSec.

A couple of companies have written Java applets that perform the same tasks, for example **GlubTech's FTP Wrapper** (www.glub.com/products/ftpswrap) and **SoftKnot's' iFS** (www.softknot.com/skc_products/ifs2.html). Secure FTP Wrapper 2.0 allows for an SSL, connection to be made to your FTP server and can encrypt both the command and data channels. Because FTP Wrapper was written in 100% Pure Java, it is supported on Windows, MacOS X, and any Unix platform where a Java 2 runtime environment (1.3+) is present.[10] There have not been any identified exploits for either of these Java based applications.

---

[9] Networkworld, September 2001
http://www.nwfusion.com/columnists/2001/0903gearhead.html

[10] Java Boutique, February 2002
http://javaboutique.internet.com/javabytes/200202.html

Port assignment
FTP is usually assigned to Port 21. However, because this is widely known, Port 21 is often targeted for attack. By assigning the IIS FTP service to a higher port, we can safely close Port 21, making it impervious to exploitation. By selecting a port number over 5000, we can reduce the chances of a port scanner finding the open port, simply because attackers tend to focus on the lower assigned ports, and scanning up into the thousands of ports takes too long to be effective.

In this case, we assigned port 5023 to be the FTP server and closed all other ports (including 21 and 80) to incoming traffic. This step alone will secure Humantail from 90% of random port scans as random scanners will have no idea there are any services available on the Humantail IP address.

The commercial applications discussed above have their own port assignments, and then route data to the FTP server. These port assignments have defaults, but all of the applications have the ability to change the port assignment. Because only internal users need to know the port, we have the luxury of being able to change the assignment to a non-standard port, thus reducing exposure to scanners.

Passwords
A strong password is crucial to protect against hackers. Using brute force attacks with applications such as L0pht Crack, John the Ripper and others, hackers can break text and number passwords in just days, or even hours.

To defend against this, Humantail has established a password policy that requires the use of strong passwords. This means the passwords should be at least 12 characters (Microsoft suggests 14 characters as that is the longest password a Windows 98 machine can handle should a Humantail employee be logging in from an old machine), should contain at least two special characters (such as !@#$% ~ etc.) and a mixture of upper and lower case.

Dictionary words with letters substituted are not sufficient. The best recommendation is to create an anagram and include a couple of special characters. [11]

We have also defined a requirement that the FTP password be changed at least every two months. If an audit of login attempts indicate there are a large number of unauthorized attempts to connect to the FTP site, we will re-evaluate the frequency of password rotation in favor of a more frequent change.

It should be noted that several security experts, for example Richard E. Smith,

[11] Center for Password Sanity, May 2002
http://www.visi.com/crypto/sanity/pwrecom.html

PhD, CISSP of the Center for Password Sanity, warn against too-frequent password changes as it leads to greater risk: employees are more likely to write down their passwords (exposing them to wandering eyes) and there are greater help desk costs associated with people not remembering their passwords. [12]

As Humantail is comprised of a very small staff with excellent memories, these issues are not of concern. However, they should be weighed when making policy for a larger organization.

Limiting Access Once Logged In

In keeping with defense in depth, it's important to limit the rights of users once they're logged onto the FTP server. This includes limiting users to their own directories and setting an automatic time-out for open but idle connections.

The best way to manage this is by taking advantage of the security capabilities of the NTFS (NT File System) file system, setting user permissions inside Windows 2000 to allow users access only to their directory. The commercial products mentioned above provide an interface for this procedure, or you can address it yourself inside the Local Security Settings Administrative Tool.[13] The Security Account setting inside the FTP site properties in IIS can control the amount of time a connection can remain open.

Anonymous login

Probably the most simple yet strongest protective step to take is to not allow anonymous login. This is a simple setting in IIS and in the commercial products described. Many attacks rely on anonymous login to get access to the targeted computer. Ending anonymous login stops attackers gaining an easy beach front on our servers. [14]

How to connect through Firewall

Humantail's internal network is protected by a Gigafast router/ firewall. By its nature, the firewall does not allow packets through to the machines on the network unless it's specifically told to. There's a simple setting in the firewall's Admin controls that allow for specific traffic to pass through. In this case, we just allowed Port 5023 traffic, and directed it to the IP address of the internal machine hosting the FTP site. At the same time, we specifically forbade FTP traffic on port 21 as a measure of extra security.

---

[12] Center for Password Sanity, May 2002
http://www.visi.com/crypto/sanity/pwrecom.html

[13] SearchSecurity.com, May 2001
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci554104,00.html

[14] CERN Institute, June 2002
http://security.web.cern.ch/security/ftp/default.htm

Humantail also runs a personal firewall on each production machine, Zone Alarm. To let FTP traffic through Zone Alarm, we had to allow IIS server to connect to the Internet and receive requests. Zone Alarm is an application-based firewall, and as such there was no need to deal with the port assignments for this application.

Logging

Logging is the most important tool in the security administrator's tool box. Without adequate logging and subsequent auditing of those logs, we will never know if attacks are being attempted or be able to react to potential threats before they are successful.

The current Humantail firewall (a Gigafast router/ firewall) does not support logging, and is clearly the weakest link in our security measures. In fact, Humantail must purchase a new firewall if any of the other measures are going to do any good at preventing infiltration.

Practicing defense in depth, once the new firewall is installed and the FTP server is started, we will also audit the IIS logs once a week to ensure only authorized users are accessing the FTP site. Being a small company, we have the advantage of being able to talk with employees should there be a large number of unusual connections or connection requests. Any unaccounted-for connections will quickly be noticed.

Because the priority of log audits are often sacrificed to more immediate "fires" to be put out, Humantail should consider employing log monitoring software such as ELM Log Monitor (www.tntsoftware.com/products/ELM3/ELM30/default.asp).

Establish a Beachhead

As a final defense in depth precaution, we recognize that the public terminals used by our employees when they're out on the road could well have been compromised, and could potentially have keystroke capture or other monitoring software that would allow hackers to pick up our password etc to the FTP server no matter how well encrypted.

To mitigate this risk, employees will be able to download the following tools to clean the computer they're using to connect to the FTP site before they type

sensitive information. Not all these tools are necessary for every situation, but having them readily at hand could proof useful should the need arise.

- AVG Anti-Virus system- a free virus checker (www.grisoft.com/html/us_downl.htm)
- WS_FTP95LE- a free and secure FTP client (http://download.com.com/3000-2160-1572132.html?tag=lst-0-1)
- SwatIt Trojan Scanner 1.0- a dedicated Trojan scanner (http://download.com.com/3000-2239-7720479.html?tag=lst-0-1)

Threat Vectors

In setting up any secure system, the threat vectors should be identified and accounted for.

Internal hacks

With only three employees, Humantail is fortunate not to have to worry about insider attacks, normally the most dangerous threat to the security of a network. As the company grows, internal sabotage will become more of an issue. When the company grows to 10 employees we will enact a formal internal user policy that defines acceptable behavior. As Humantail is not expected to grow, such a policy is not necessary at this time and would only reduce the efficiency of the three employees and add to the workload of the IT administration. If the staff does grow we will determine necessary steps to ensure safety. Steps will include monitoring user workstations for dangerous or suspicious applications (port scanners, password sniffers, etc.) using inventory tools such as Microsoft SMS (www.microsoft.com/smserver/default.asp , TechTracker ITX (www.techtracker.com/products/itx), or Blue Ocean (www.blueocean.com). We will also place more emphasis on studying the logs of internal machines to ensure no one is attempting to connect to unauthorized machines on the network.

Most importantly, we will update the employee manual to spell out the security policy of the company, our expectations of employees, and a clear definition of the consequences of violating policy.

Random Port Scans

In terms of raw numbers, the vast majority of attacks are not deliberately targeted. Hackers scan large blocks of IP addresses looking for open ports with known vulnerabilities. By moving the FTP port from 21 to 5023 and closing all the

ports of our FTP machine, including port 21, Humantail is significantly safer from random port scanning.

It does mean users have to know to request a different port when connecting to the FTP, but as internal staff will be the only authorized users of the service, it doesn't pose a problem for Humantail.

Industrial espionage
This is our most significant threat vector. With trusted employees and fairly strong protection from random attack (via closed ports, SSL connections and strong passwords), a targeted concerted effort to gain access to our data is the main threat. Our main protection against this threat is the audit. With only three employees, it will be simple to account for all authorized attempts to log in, and identify when there is a concerted external effort to break in.

Known Vulnerabilities
A determined hacker, be it a targeted attacker or a random scanner who found our FTP port, will proceed to attack our security in two ways: trying passwords and exploiting vulnerabilities in our setup. New vulnerabilities are discovered everyday and unfortunately, there's nothing Humantail can do to stop them. The site http://www.wwdsi.com/demo/saint_tutorials/FTP_vulnerabilities.html lists excellent examples of the options hackers have to attack our setup.

What we can do is pay attention to security bulletin and make sure we are always up to date on patches and hotfixes for every piece of our setup: the OS, the firewall, IIS, and any third party applications (for example FTP Wrapper, as mentioned above).

The best way to accomplish this is to use a vulnerability scan and notification service such as the one offered by Steve Gibson, Patchwork (www.grc.com/pw/patchwork.htm), or by TechTracker's ITX software update alert product (www.techtracker.com/products/itx).

Department of Homeland Security
Only time will tell what impact the Department of Homeland Security will have on the private affairs of United States citizens.

Conclusion

By implementing an IIS FTP server, we have successfully identified a way for Humantail employees to access the files they need securely and reliably. The most immediate concern is the need to purchase a firewall that is capable of

logging. Future improvements will need to be made to the system if Humantail starts to employ more than a handful of staff. Future revisions will also include the investigation of a dedicated Linux machine to act as a server, with internal requests to the production machines where needed files reside. However, given the current budget constraints, we are limited to the resources available.

Bibliography

TechRepublic, Apr 6, 2000
http://www.techrepublic.com/article.jhtml?id=r00120000406bot01.htm&src=search&_requestid=77070

Infosecurity, 1999
http://www.infosecuritymag.com/articles/1999/remote.shtml

Infosecurity, 1999
http://www.infosecuritymag.com/articles/1999/token.shtml

CERN Institute, June 2002
http://security.web.cern.ch/security/ftp/default.htm

SearchSecurity.com, January 2002
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci790654,00.html

Microsoft, January 2001
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp

Macromedia, January 2001
http://www.bitpipe.com/data/detail?id=1020108274_293&type=RES&src=FEATURE_SPOTLIGHT&x=500080766

Networkworld, September 2001
http://www.nwfusion.com/columnists/2001/0903gearhead.html

Java Boutique, February 2002
http://javaboutique.internet.com/javabytes/200202.html

Center for Password Sanity, May 2002
http://www.visi.com/crypto/sanity/pwrecom.html