How to Secure your SFTP Server

Tips and techniques on keeping corporate systems and data safe from attack

Bruce P Blackshaw
December 2014

EnterpriseDT
SECURE FILE TRANSFER & SHARING

Introduction

This white paper explains in detail the strategies you can implement to secure your corporate SFTP servers (and FTP servers) from attack.

If your server has a direct connection to the Internet, this is critically important – the Internet is flooded with bots that are port scanning every IP address available. Once a server is made available to the Internet, it is often only hours or minutes before hacking attempts begin.

Even if your server is not directly connected to the Internet, there are always people who are eager to break in and steal your data. They may even be your employees. So in almost all circumstances, it is wise to make your server as secure as possible. It just might save you a lot of grief.

This white paper will use our server, CompleteFTP, as the reference server to secure, but the suggestions made will be applicable to and useful for all SFTP and FTP servers.

Tip 1: keep software up-to-date

The first tip on how to secure your SFTP or FTP server is a basic one, but one that is very often neglected. And yet it is probably the most important thing you can do to keep intruders out of your systems.

It is this – *keep your operating system and your server software up-to-date with the latest security patches*. This means regularly applying Windows updates as soon as possible after they become available, and ensuring you do the same for your SFTP or FTP server. New vulnerabilities are regularly found in Windows and in protocols such as SSL/TLS.

Two recent important examples of this are the Heartbleed vulnerability in OpenSSL, and the POODLE SSL 3.0 exploit.

Heartbleed is an extremely serious vulnerability, possibly the worst ever in the Internet era, and it affected millions of servers, including some very high traffic websites. It is imperative that all servers affected are patched as soon as possible. At the time of writing there are still thousands of unpatched servers. Fortunately our server, CompleteFTP, does not use OpenSSL and so was not affected by Heartbleed.

POODLE is far less severe, and not nearly as likely to be exploited, but it is still important to obtain the latest server patch that disables the vulnerable SSL 3.0 protocol for FTPS and HTTPS. CompleteFTP 8.1.3 was released specifically in response to POODLE.

So, if your server software is not up-to-date and you haven't applied the latest Windows updates, do so as soon as possible.

Tip 2: use your corporate firewall effectively

Next, make sure you make full use of your corporate firewall. The best way to ensure that your server is never hacked is to make sure hackers never get near it, and that is best accomplished by keeping intruders out of your corporate network. This means keeping your firewall's software current, and keeping vigilant by proactively monitoring your firewall logs. It may also mean conducting regular penetration testing to ensure your firewall is doing its job.

On a related note, if your SFTP server is not required to be accessible from the Internet, ensure that it cannot be accessed from the Internet. Note that this does not mean intruders cannot indirectly access your server from another compromised corporate server, but it will help.

On the internal corporate network, it is likely that not all users will require access to your server, so wherever possible ensure that only authorized corporate users do have access. And of course, all the usual caveats about disabling access when employees move on apply.

Applying the above security measures is not difficult, but ensuring that they are regularly enforced certainly is. When security measures are not enforced, or are applied haphazardly, no-one notices – until finally there is a serious attack and valuable corporate data is stolen. Clear policies and competent, diligent network administrators are required. If the value of corporate data is very high, it may well be worthwhile conducting regular security audits by a trusted third party.

Tip 3: use IP filtering and autobans

Now we've done our best to keep intruders away from our server machine by effective use of our firewalls, now it's time to ensure that those who attempt to log onto the SFTP server are only those permitted to do so.

How do SFTP servers like CompleteFTP typically prevent unauthorized users from gaining access? Via three security mechanisms – IP filtering, auto-banning, and strong password policies.

IP filtering means setting up the server's IP filter rules so that only users from permitted IP addresses are able to access the server. IP addresses that do not pass the rule set have their connection terminated immediately. It is best to use a whitelist rather than a blacklist. A whitelist bars all IP addresses except for those listed. This means external IPs must be explicitly added. This is tedious, but safer - although it may not be possible if all the permitted IP addresses are not known. A blacklist is a list of banned IP addresses or address ranges. Given the vast range of IP addresses that an attacker may use, blacklists are not usually practical.

Auto-banning is the second useful security mechanism. It works by automatically banning IP addresses from connecting (for a period of time) if they have failed to authenticate a certain number of times within a time period. For example, an attacker from a given IP address might fail to guess a password correctly 10 times within a 60 second period. With auto-banning, their IP address would be banned from connecting for the next hour. After an hour has elapsed, the ban would be automatically lifted.

Why is auto-banning helpful? It helps to prevent dictionary attacks – cycling through an entire dictionary of passwords and trying them out one by one. Because the IP address is banned after only a few attempts, dictionary attacks are discouraged, as they are made extremely time consuming. And of course auto-banned IP addresses can be permanently banned by adding a new IP filter rule.

It is important that strong password policies are enforced in conjunction with auto-banning. If an attacker can guess a user's password after a few tries by using common default passwords, auto-banning will be ineffective. Most servers allow password policies to be enforced so that a minimum password length and a mix of characters, case and digits must be used.

If IP filtering, auto-banning and strong password policies are suitably configured and their performance is regularly reviewed, the chances of an attacker successfully logging in (and subsequently stealing corporate data) will be minimized.

Tip 4: disable unused protocols

The most important group of changes is at the protocol level. Quite simply, if a protocol that your server supports is not required, disable it.

For example, CompleteFTP server supports FTP, FTPS, SSH, SFTP, SFTP, HTTP and HTTPS. If you only require, for example, FTP, FTPS and SFTP, then disable HTTP and HTTPS, as well as SCP and SSH logons.

Ideally, FTP and HTTP should always be disabled as they are insecure protocols that can be easily hacked. FTP is the worst offender in this regard, as it sends usernames and passwords unencrypted. Always use FTPS rather than FTP (if this is possible). Of course, you may have to support certain protocols depending on what clients are accessing your server.

Also, it might be that particular users require certain protocols, but most do not. In that case, ensure that only users who require those protocols are able to access them – disable protocols at the user level for all other users.

There are also some protocol-specific settings that should be considered.

If plain FTP must be supported, consider whether anonymous users are required. Traditionally, FTP servers have supported anonymous logins with read-only access to certain public directories. If you don't need anonymous logins, disable them.

If FTPS or HTTPS is required, make sure SSL 3.0 is disabled so that the POODLE vulnerability cannot be exploited. If your server version doesn't support this, upgrade to a version that does or change servers - if your server vendor has not issued a patch for this by now your data is not safe on their server.

Finally, enforce strong permissions on your directory structure. Make sure that shared directories only permit the right users access to them, and that users are locked into their home directories by default. Test and review permissions regularly, and remove or disable old logins that are no longer in use.

Tip 5: secure the SFTP and SSH protocols

Secure file servers such as CompleteFTP support many protocols, including FTP, FTPS, HTTP, HTTPS, SCP and SFTP. The suggestions above have explained various techniques that help protect your server against attackers. These techniques have been largely generic, and apply across all protocols. This post will focus on the SFTP and SSH protocols, and examine protocol-specific settings that should be enabled to make your SFTP server as secure as possible.

The first tip has already been mentioned, but it is worth repeating – disable SSH terminal access unless it is absolutely required. SSH terminal access is dangerous – it gives far greater access to the operating system than SFTP does, often including commands like 'exec' which allow the execution of any binary on the server that is accessible. SFTP also runs over an SSH connection, but it does not give terminal access. If a certain user must have SSH terminal access, disable it for all other users.

Secondly, restrict authentication methods. SFTP (as well as SSH and SCP, which also runs over SSH) supports a number of methods – password authentication, public key authentication, and keyboard-interactive authentication. It is best to disable password and keyboard-interactive authentication if this is possible – it means that users must have the appropriate private key to be able to authenticate. This eliminates the possibility of an attacker trying to guess passwords. It is important to encrypt the private key with a passphrase.

Sometimes, a password must be supplied – for example Windows users in CompleteFTP need a password to log in to Windows. In that situation, you can require public key authentication as well as password authentication – both must succeed for the user to log in. This combines two authentication methods, making them both compulsory.

Thirdly, restrict the server's algorithms to the strongest that are available. SSH supports both RSA and DSA host key algorithms. Disable DSA, and ensure the server's RSA key is 2048 bits. Use the more secure ciphers, such as the 128, 192 or 256 bit AES ciphers. For MAC algorithms, disable MD5 and prefer SHA1 if possible. Even better, use SHA2 algorithms for MACs, if the server and your clients support them (not all SFTP clients do).

Next, ensure the SSH banner message that is sent to clients contains the appropriate legal warnings about unauthorized access. This won't stop intruders, of course, but it is necessary for legal reasons, and your legal department or legal counsel should be consulted.

Finally, you should be able to hide the server's product name and version string that is sent to clients when they connect using an SSH client. For example, by default the current version of CompleteFTP will send "SSH-2.0-CompleteFTP-8.1.4", but when the "Hide server product details" option is selected, the string returned is "SSH-2.0-Unknown". This gives away no information about the server, which helps if it happens to be an older version with known exploits. Of course hiding the product details won't stop a determined attacker, but it means they won't begin with a vulnerability that is likely to succeed.

Tip 6: prevent social engineering

The previous tips focused on using various technologies appropriately to secure your corporate network and servers.

It is important to be aware that many successful attacks stem from social engineering, or from disgruntled employees or ex-employees. Social engineering is when people are manipulated into providing confidential information – by calling help desks, for example, and claiming to have lost their password. Former employees may still have access to company systems, and current employees may have access to systems they should not be using. In all these cases, attackers are in possession of valid usernames and passwords, and so they are not easily detected. Many of the techniques presented earlier are of limited value when valid credentials are being used, particularly if attackers are your employees.

To prevent these kinds of attacks, certain business processes must be put in place. For example, when a person leaves the company, any credentials and access they may have should be immediately disabled. This requires the human resources department to coordinate with IT prior to the person's departure.

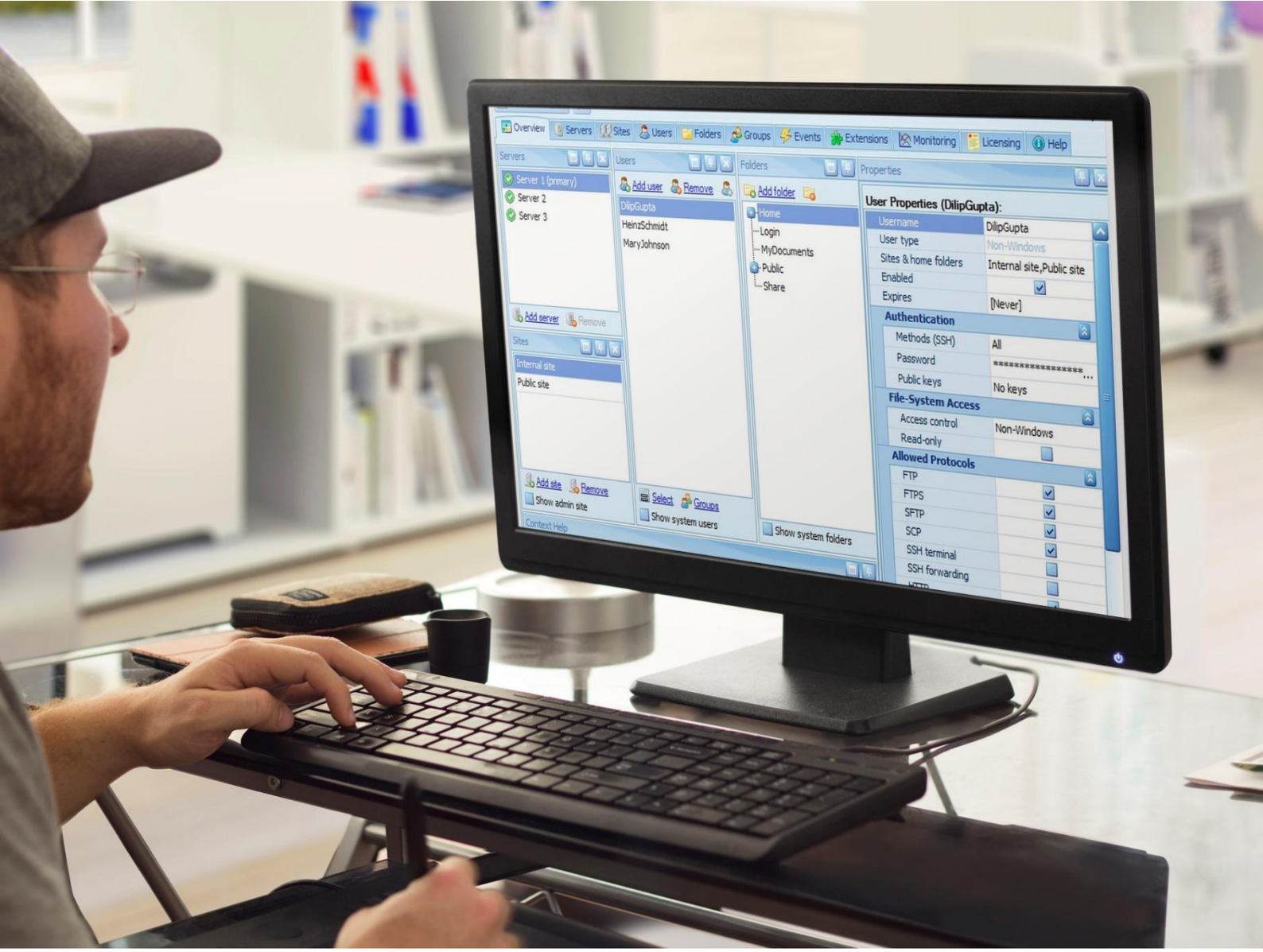
For social engineering attacks, help desk staff must be trained to properly identify callers, and not to give out sensitive company details. Passwords should never be disclosed. Guests should be escorted at all times while they are on the company premises. Document management is important, particularly document destruction. Sensitive documents that are being disposed of should be dealt with securely.

Phishing is a form of social engineering, and can be used to obtain credentials and other sensitive information. Phishing is usually done by encouraging people to click on email links that lead to disguised sites infected with malware. Good anti-virus software and user training will reduce the risk of employees succumbing to phishing attacks.

Summary

Unfortunately, securing your servers, your network and your confidential data means eternal vigilance. Administrators must regularly check logs, test security measures, and ensure security patches are applied as they become available. Suspicious activity needs to be acted on immediately.

It can be an intimidating task when you are aware of the possible ways that your systems can be compromised. But thorough, on-going preparation based on the advice presented in this white paper will significantly minimize the risks.



Complete FTP

Secure & reliable file transfer server for Windows

Thousands of companies worldwide rely on CompleteFTP to securely transfer their confidential files. It is packed with features that help you easily integrate secure file transfer into your business processes:

- easy to install and administer
- extensive range of features to suit small and big business alike
- highly customisable

We compared more than 10 products. CompleteFTP was by-far the winner on a cost/feature comparison.

MSM Group – Ohio, USA

Try it FREE for 30 days

completeftp.com

Bruce Blackshaw has been writing software professionally for almost 25 years. He has wide experience in encryption, security, and network protocols such as SSL/TLS, SSH, SFTP and FTPS across a variety of industries. Bruce is a founding partner of Enterprise DT and is currently one of the principal developers of their flagship product for secure and reliable file transfer, CompleteFTP.

www.enterprisedt.com | sales@enterprisedt.com
PO Box 3027, Yeronga QLD 4104, AUSTRALIA | +61-7-3053 8544