

Assessing Your FTP Exposure

As a result of the new reporting requirements and compliance rules, auditors have begun taking a close look at the usage and management of FTP in the enterprise. New regulations have been imposed by Federal and State governments (PCI, SOX, HIPAA, FISMA, etc.) over the past few years to protect individuals from inadvertent disclosure of their sensitive financial and health information.

This, combined with the alarming number of recent data breaches has created a pressing need for I.T. organizations to take a closer look at their data security procedures and identify and **address the exposure that FTP usage creates.**

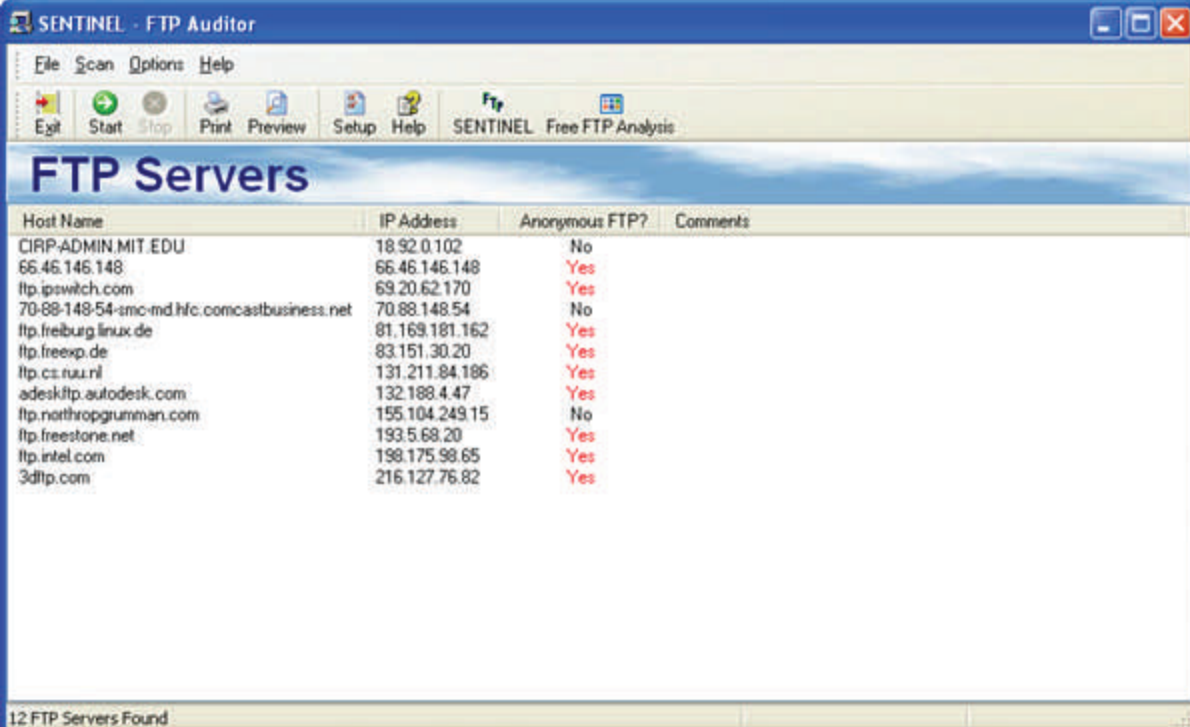
FTP Exposure

FTP is a very convenient method for transmitting data from system to system. It is integral to the business operation of most large corporations. The problem FTP poses, however, is that most FTP activity is unsecured. As a result, the exposure to any organization, especially with the new regulatory requirements, is too great to ignore. The overwhelming majority of FTP activity today is unsecured which results in exposing logon information

and data which travels in “clear text” format. In addition, FTP makes it very easy to send data outside of the enterprise. All that is required is read-level access to data and an Internet connection for someone to be able to send the data virtually anywhere in the world. It is the responsibility of the data center to monitor FTP activity to ensure that the security of sensitive data is not being breached through the FTP process.

How FTP Auditor Can Help

The first step in gaining control over your FTP exposure is to identify and assess all of the FTP servers in your organization. Until you know where they are, you can't start the process of auditing their usage. FTP/WatchDog's FTP Auditor is a Windows application that enables you to identify and evaluate the FTP servers that are running on a network. It reports on where the FTP servers are and whether they accept anonymous logon. Run it regularly to find out if new FTP servers have been added to the network.



The screenshot shows the 'SENTINEL - FTP Auditor' application window. The title bar includes the application name and standard window controls. The menu bar contains 'File', 'Scan', 'Options', and 'Help'. The toolbar includes icons for 'Exit', 'Start', 'Stop', 'Print', 'Preview', 'Setup', 'Help', and 'SENTINEL Free FTP Analysis'. The main content area is titled 'FTP Servers' and displays a table with the following data:

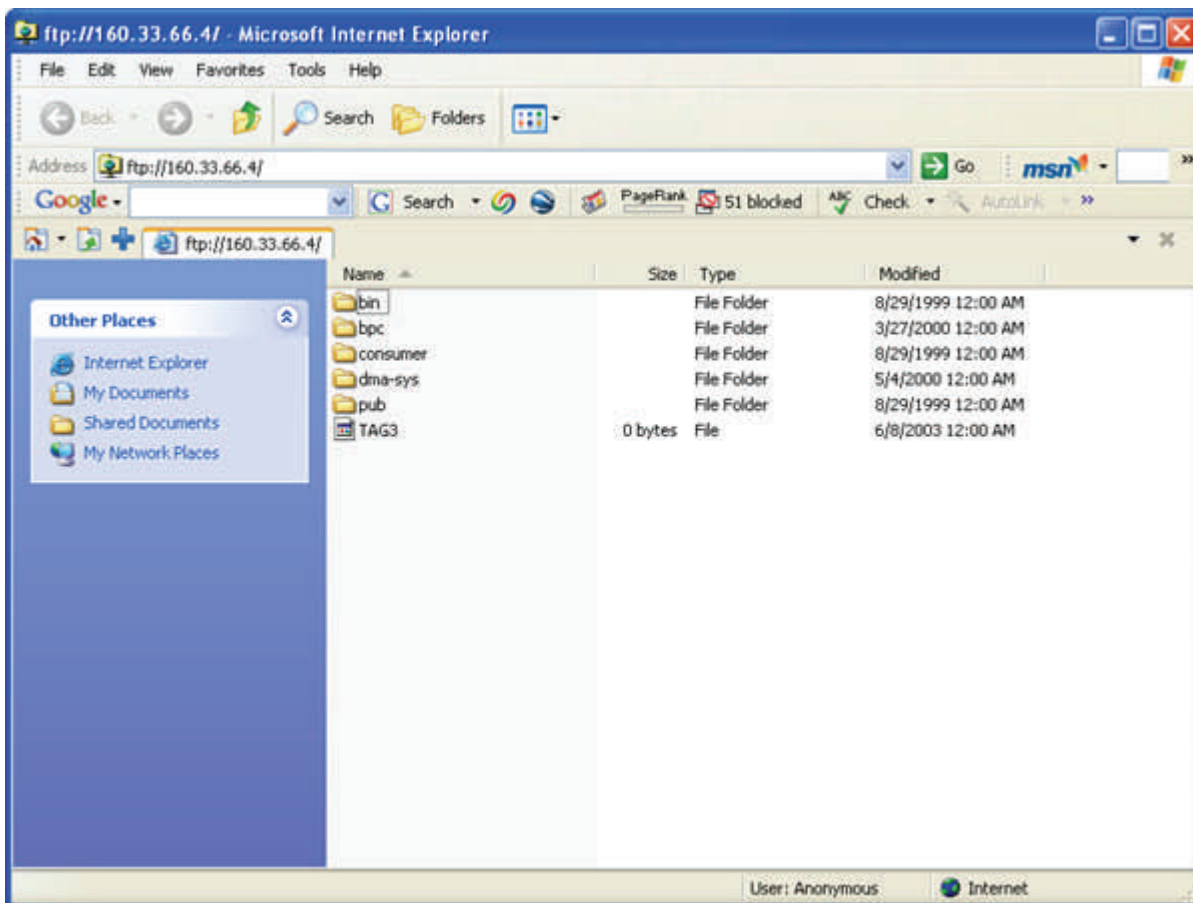
Host Name	IP Address	Anonymous FTP?	Comments
CIRP-ADMIN.MIT.EDU	18.92.0.102	No	
66.46.146.148	66.46.146.148	Yes	
ftp.ipswitch.com	69.20.62.170	Yes	
70-88-148-54-smo-md.hfc.comcastbusiness.net	70.88.148.54	No	
ftp.freiburg.linux.de	81.169.181.162	Yes	
ftp.freexp.de	83.151.30.20	Yes	
ftp.cs.ruu.nl	131.211.84.186	Yes	
adeskftp.autodesk.com	132.188.4.47	Yes	
ftp.northropgrumman.com	155.104.249.15	No	
ftp.freestone.net	193.5.68.20	Yes	
ftp.intel.com	198.175.98.65	Yes	
3dftp.com	216.127.76.82	Yes	

At the bottom of the window, a status bar indicates '12 FTP Servers Found'.

See What Data is Exposed?

Double-click on any of the servers that the FTP Auditor finds to display the files and folders available on the server. If the server allows anonymous logon, the

files and folders in its root folder will be displayed. If it does not support anonymous logon, you will be prompted to enter a valid user ID and password to use to log on.



Anonymous Logon

Anonymous FTP is a very convenient way to make data available without having to maintain a burdensome list of user IDs and passwords. The trade-off, however, is that you need to keep a close eye on how it is being used and what data is available for anonymous download. Anyone with network access can log onto an FTP server that supports anonymous logon and download any of the files that are available on the server. In some cases, these same people can upload data to the server and that uploaded data will be universally available.

An FTP server that supports anonymous FTP requires a higher level of care and monitoring to ensure that no sensitive or protected data resides in the fold-



ers that are accessible by the server. If uploading is allowed, further monitoring must be performed to ensure that no sensitive or protected data is uploaded to the server folders.

Wherever anonymous FTP is not critical to the business operation, you might consider shutting it down. Only leave it in-place where the business benefit outweighs the exposure it creates for your company.

Try It Today

You can download and try the FTP Auditor on your network today. Call or email us today to receive a link for downloading the software. You'll be glad you did.

Phone: (408) 973-8374
Email: sales@softwareassist.net
Web: <http://www.softwareassist.net>