GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, Exploits, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GCIH Practical Assignment, Version 1.5c

Charles W. Kelly

March 1, 2005

FTP Site Compromise: Detection, Neutralization, Resolution

Executive Summary

On &date, we were informed by a third party that our FTP site was being used as a launch point for malicious actions in their domain. This document describes the incident, and the steps that were taken to resolve both the immediate threat to the third party, and to prevent future similar exploits from being initiated from our domain.

Preparation

File transfer is a common method of exchanging large documents and binaries among our customers, business partners, and employees located around the world. To facilitate that exchange of information, we permitted anonymous access to our FTP site, as shown in Figure 1.

With this configuration, anonymous users are permitted to access the site for both reading and writing files. Simple listing of files is not permitted, however, so if someone left a file at the site, anyone that wanted to pick it up had to know the path and filename. That worked as intended when the person leaving the file was one of our customers, and the person picking up the file was one of our tech support reps. It worked equally well, as demonstrated by this incident, when the two people who wanted to exchange files were cooperative with one another, and completely disassociated from our company.

As a result of this configuration, we had no control over what was being dropped or picked up at our own site. The goals for administering the site were to optimize the storage requirements by expiring and removing files that were not in use. Within those bounds, the entire Internet was able to use, or abuse, our FTP site with little or no intervention from us. This type of configuration is typical for FTP sites at universities, and software clearinghouses whose primary mission is open access to the public. It was chosen as our configuration several years ago when the security concerns of our company did not include threats from the public via the Internet.

To complete the description of our preparations for this incident, I'll describe the way we are organized to respond to threats and disasters.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We use a severity scale ranging from one to four for identifying the resources and time and time frame for resolution of issues:

```
1 = System/Component down or unusable; critical impact; no
circumvention available; affects 10 or more people.
```
Resolution: ASAP

```
2 = Component down or degraded; critical impact; circumvention
available. (Note that single machines down are sev. 2.)
```
Resolution: Close of business, same or next business day

```
3 = Component down or degraded; not critical but some operational
impact; circumvention available.
```
Resolution: 3 business days

```
4 = Component/Procedure usable or circumvention possible with no
operational impact; not critical; deferred maintenance acceptable.
```
Resolution: 10 business days

Our data center is run on a lights-on basis twenty-four hours a day, and is the default owner of all severity 1 issues. The data center staff relies on several teams of personnel that are "on-call" for the resolution of severity 1 issues. The on-call teams provide coverage for network communications, email communications, mainframe systems, telecommunications, UNIX systems, desktop systems, business-critical applications, and Internet/Intranet systems.

The help desk has been established as our frontline for responding to IT issues and threats, including our initial response to incidents prior to escalation. It is a centralized resource predominantly used to handle issues and threats that either originate or have ramifications for our North American operations. During North American business hours the help desk is also responsive to issues and threats that occur in our global points of presence, typically as an escalation point for marshalling additional resources or expertise to resolve a problem that is occurring elsewhere in the world.

The help desk is self reliant for 95% of incoming calls for assistance. When a call requires expertise that is out of scope for the help desk staff they rely on the same on-call teams described above.

When the help desk and on-call support feel that an incident needs escalation, the information security manager notifies the response team and convenes a meeting within 4 hours of the initial escalation of the incident. The information security manager is responsible for maintaining a current list of response team contacts.
Our response team is a loosely organized collection of representatives from legal, web server administration, email administration, Unix and Windows server administration, Windows desktop management, LAN and WAN administration, systems and information

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

security, and the help desk. The "team" does not meet on a regular basis, but is committed to being responsive within four hours of initial notice.

Identification

First notice of this incident was received via email addressed to our webmaster describing the exploitation, and the evidence that had been collected that allowed the administrator to surmise that our site was an origination point for the delivery of undesirable content to his site. The text of the message:

```
Hi,

Your anonymous ftp site is being used as a base for cybercrime.

Recently, a system I maintain was breached.

Part of the script that was used in the attack downloaded tools from
your anonymous ftp directory.

Specifically:
ftp://ftp.mycompany.com/incoming/gaa/t0rntd

I see that it is still there.

A simple 'ls' on the incoming directory does not reveal its presence,
but you can 'cd incoming/gaa'.

I would appreciate it if you removed these files and took steps to
prevent further abuses of your system.
```

Because the email was addressed to our webmaster, all standard response measures were bypassed, and the incident was immediately escalated to the response team. The webmaster forwarded the message to the information security manager, Unix administration, and legal. Unix administration verified the existence of the directories and files noted in the email. The Information Security Manager convened a meeting of the full response team, which generated four action items:

1. Respond to the external party that brought the problem to our attention
2. Change the FTP site in three stages.
   - Stage 1
     - Make files in incoming directories unavailable for download from ftp server
     - Mirror ftp directories/files to internal file system
     - Document supported outgoing ftp processes
   - Stage 2
     - Scan the files for viruses prior to mirroring to the internal file system
   - Stage 3

© SANS Institute 2000 - 2002, Author retains full rights.

- Create a 'generic' userid/password for placing files on the ftp server, the userid/password would be able to be shared with customers and employees and the password would be changed periodically

3. Send email to department heads that may be affected to gather information on feasibility of proposed solution. Post an article to the internal web site describing the change
4. Implement virus scanning for all files placed on the ftp site.

In addition to the action items, the response team recommended taking no action to pursue the individuals that were responsible for the abuse of our resources. Instead of initiating a resource intensive forensic and legal process, the response team decided to minimize the impact of the incident on our company, assist the third party that we attacked if asked, and eliminate the opportunity for future similar incidents originating on our site.

Since the proposed changes to the FTP site would have consequences in many areas of the company, it was decided to notify broadly prior to initiating the change in the hopes of quickly bringing unanticipated issues to the surface. The text of the email that was sent out:

```
One day this year we were notified by a site administrator that he has
evidence that lead him to conclude that our FTP site was being used as
a storage and staging site for an ongoing attack on his site. While we
have taken measures to minimize any consequences that may have arisen
from this incident, we also feel strongly that additional measures are
needed to prevent future incidents of this type from occurring.

Effective three weeks from now, the properties of the INCOMING
directory will be changed from "world read/write" to "world read". This
will prevent anonymous agents from being able to deposit files for use
by other agents external to us. We will also mirror the contents of the
INCOMING directory to an internally accessible directory so that our
employees have ready access to the files that are deposited for their
use.

This change should not have any adverse impact on the intended usage
patterns of the FTP site.  I am soliciting your feedback at this time
if you have business processes that will be negatively impacted by this
change. Please send your comments to me as soon as possible so I have
an opportunity to accommodate your needs.

Thank you for your assistance with this issue.
```

The changes were not scheduled to take place immediately, to make sure no one was unnecessarily deprived of the use of our FTP service. The factors engaged in making that decision are discussed later in this paper.

© SANS Institute 2000 - 2002, Author retains full rights.

The message sent to the admin that notified us of the compromise was necessarily brief:

```
Mr. Admin,

Thank you for contacting us directly. Earlier today, we removed the
directory in question.

As you probably realize, we do not, in any way, condone this use of our
anonymous FTP area and we are investigating the matter further.

Regards,
```

Containment

According to the US Department of Transportation online document, *Departmental Guide to Incident Handling Planning*, containment is a series of short-term solutions design to minimize the detrimental effects of the incident, while providing maximum communication of the situation to all impacted parties. To that end, the directory and files that were placed on our FTP site were moved to a safe location inside our firewall, scanned for viruses, then inspected by the Network Security Team. The team ascertained, from file naming conventions and their organization into groups, that the primary purpose of the files was, for all intents and purposes, malicious. The directory and files were then manually deleted. The files were located in a directory space that was not automatically backed up, so the chance of the files inadvertently becoming available in the future was minimized. Once they were deleted, they were eradicated from our internal and external systems. To prevent reoccurrence of the exploit a script was put in place that would scan the /INCOMING directory structure of the FTP site every ten minutes, searching for the directories and files of the same names as the ones that caused the incident. If the files were found, the script would act to delete them as soon as they were detected.

We were not concerned about the effects of our containment measures on our ability to diagnose the incident, or to collect forensic evidence for the purpose of prosecuting the perpetrators. The diagnosis was straightforward, and did not require special consideration with respect to the preservation of material evidence. As far as the forensic evidence, as a company, we do not rule out the possibility of prosecuting miscreants that perpetrate future incidents against us. But in this case, we were satisfied that stopping the current exploit from re-occurring would be sufficient to protect us from further damages, and elected to minimize the resources required to put this incident to rest as soon as possible.

This was in large part a decision championed by the representatives from our Legal staff. While those of us in IT were considering the possibility of a forensic collection of data, and a wild ride through the scripts of movies and dime store novel plots, our lawyers were skillful in reining those thoughts back to reality. It was simply not feasible from a business perspective to put any effort into capturing the perpetrators of this violation of our resources. There was no harm done to any individual in our company, no harm to any

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

aspect of our business processes, no harm done to our reputation or the perception of our company in the eyes of our customers or shareholders. There was no reason to pursue this event any further than to make sure no harm was done to the single affected site, and make sure that there was no continuing threat of the event repeating itself.

Eradication

This incident prompted a close look at our vulnerability to this type of abusive behavior, and resulted in an overhaul of our FTP site to eliminate the probability of a re-occurrence. Due to our business model, it was not possible to completely do away with anonymous access to the site. Our customers, partners, and consultants are constantly exchanging information and data with our developers, technical support representatives, and sales and marketing representatives. It was a business priority that we find a way to preserve the ease of use that all parties had become accustomed to over the years, while at the same time eliminating the opportunity for malicious content to be stored and forwarded from our FTP site.

One option that was discussed briefly was issuing logon credentials to each person at each customer site that wanted to exchange files with us. The logistics associated with that option were frightening, and resulted in a historically brief discussion of this option.

The alternative that we chose was to change the access permission on the /INCOMING directory to be world-writeable, but not world-readable.

Changing the permissions on the /INCOMING directory accomplished our goal of keeping ANONYMOUS access to the site. It also prevented ANONYMOUS from dropping files onto the site for later retrieval, or retrieval by another party. To make business transactions available to our internal user community, we mirror the contents of /INCOMING to an internal directory. To prevent malicious code from becoming resident in that internal directory, we scan it for viruses as soon as it is refreshed, and quarantine any matches to the current signature file in a holding directory that is inaccessible by all but a few administrators.

As an extra precaution, we also changed the procedure for sending files out from inside our company. We created an /OUTBOUND directory with permissions set to world readable. We created an internal directory in which files that are destined to be picked up by customers, partners, vendors, etc., can be placed. That directory is scanned for viruses, and mirrored to the /OUTBOUND directory, where the files can then be retrieved.

This new configuration for the FTP site is diagrammed in Figure 2.

The eradication of the vulnerability that permitted the abuse of our FTP site was delayed in order to assess the impact that this change in process would have on our customers. It was unclear, for instance, whether we were introducing too much complexity to s system that had been running smoothly for many years. The only way to determine that was to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

poll the responsible parts of the company that would take the brunt of dissatisfied customers if that were the case.

In our company, the FTP site is used by many parts of the organization, but only two use it extensively as part of their communications with customers – Technical Support, and Consulting. Technical Support routinely accepts core dumps, customer code, logs, etc., from customers, via email. But if the size of the files that need to be examined or exchanged exceeds a threshold determined by our Email Administration group, FTP is the logical alternative for those types of transactions. Our consultants have a different usage pattern for the exchange of large files with customers, typically hinged on the delivery or receipt of solutions, compiled or in source form, to on site locations. Many testing cycles can be expedited by the delivery of large files containing entire applications that can be installed to replace the version that is currently in place at a customer location.

For both of these parts of the company, timely delivery or receipt of large files was considered critical to the effective maintenance of good customer relationships. When asked to consider the new procedures for moving files in and out of the FTP site, the only question asked was how frequently will the files be moved into and out of the internal network. Once we settled on a 15-minute latency period for either direction, there were no more issues to resolve, and implementation moved forward.

Recovery

The recovery aspect of this incident can be divided into two parts:

1. Verification of the hardware and operating system for the server that supports the FTP site.
2. Verification that all files and directories on the FTP site were free from contamination, and could be made available to both internal and external customers.

From all outward appearances, the server was fine. But how can we be sure there was not a subtle difference in its operation that allowed it to harbor a backdoor, or a dormant Trojan that would allow our resources to participate in the next coordinated distributed denial of service attack? We could not be sure without the use of a file integrity check program, which we used to verify that the files that are currently in use for the operating system are the same as the ones that were last in place when the integrity database was updated. Since we do not use a commercial, off-the-shelf, file integrity product, I will provide some details on the methods we used.

All of the servers and resources that we put in "harm's way" are candidates for file integrity checking. Most of our production servers are Unix servers, so we have adopted the use of the public version of Tripwire. To assure that we are not using a hacked up version of the tool, we obtained the source, free from the Internet (see references for URL), and compiled our own executables. Tripwire uses a combination of hashes, an

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MD5 checksum, and other algorithms to create a unique identifier for a file. We added additional elements to ensure uniqueness, like timestamps from file attributes, to make it difficult to recreate or spoof a file identifier. All the unique identifiers for all the files that are tagged as critical are combined into single file, known as the integrity file.

For our use, the integrity files for all servers that use Tripwire are remotely located from the servers themselves. That prevents a penetration attempt from gaining access to the integrity files themselves as a way of covering their tracks. Once we have added a server's integrity file to the collection, we add a nightly batch job to re-create the integrity file on the server, and pass it back to another server for comparison with the master integrity file. Any mismatched identifiers causes an exception flag to be raised, issuing email notification to the Information Security Team that a critical file has been modified on a server. For the server that supported the FTP process, there was no indication of loss of critical file integrity.

The next step could have been very tedious, since the files that customers place on the site are not considered critical to the operation of the server, and hence are not candidates for integrity assurances. We decided to make an assumption: files that were not located in the offending directory structure were probably not part of the attack scenario that was reported to us by the affected administrator. So we were not necessarily looking for tools, which may or may not trigger a virus alarm. We were looking for malicious code that hopefully would trigger a virus alarm, but most of the scanning packages are designed for protecting Windows desktop machines, not Unix servers. We resolved this by taking advantage of a storage device known as a network appliance.

A network appliance allows storage of files that can be shared between Windows and Unix servers and desktop machines. To effect the scanning of the all the files, they were transferred to a network appliance. The location of the directories was mapped as a local drive on a desktop machine, and the virus scanning software on the desktop was used to scan the files.

Once the hardware, operating system, critical services, and the FTP site files were verified as safe for continued use, the site was put back into operation under the new configuration and operating procedures.

Follow-Up

We have had no further contact with the site that was attacked. Our response to this incident was not confined to the aforementioned re-structuring of our FTP site. We have taken a closer look at how we exchange data and information with our customers and business partners, and developed new guidelines and procedures for managing it. We now have a corporate data usage policy, enforced globally, that specifically outlines the appropriate use of data contained within company-owned databases about individuals and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

companies with whom we conduct business. This includes the FTP site that is used to exchange information with our customers and partners. We are also moving quickly to implement a data classification scheme to be used to determine the measures and controls that are appropriate for different types of data. The data that is moved in and out of the FTP site will likely be classified for high levels of security, since it is customer-centric, and many times customer-owned. Any time we accept responsibility for managing data on behalf of our customers, we accept stewardship of its confidentiality and privacy. Many of our large customers are beginning to require audits of our security and privacy policies and procedures as a pre-requisite to doing business that requires the exchange of confidential information.

These types of policy initiations have also spawned discussions of the international implications of expectations of privacy. The United States is moving aggressively to protect the privacy of individuals when their data is collected and subsequently used by corporate entities, government agencies, and other organizations. As a U.S.-based company we are well aware of statutes and regulations already put in place, and poised to take effect, at the state and federal levels. We have recently added an organization at the executive level of the company to monitor legislative actions and decisions that may impact our business operations. But the complexity of compliance for a global organization is the search for the most conservative set of statutes among the countries represented by international offices and subsidiaries. Compliance with US federal statutes is proving to be too liberal for some European country offices, and requires enforcing stricter policies and procedures than would be satisfactory for U.S.-only operations. Conversely, holding all parties to the highest of all standards can have an adverse impact on some operations by requiring potentially costly measures to be put into place as pre-requisite for conducting business as an equal partner with the rest of the world. We are discovering that compromise is the best recourse, where it is at all possible.

Another consequence of this incident is the institution of a second, secure FTP site that employs SSH (secure shell). SSH is used in many ways at our company, on both Windows and Unix clients and servers. It is an excellent way to introduce strong authentication and encryption technology to both user-based and process-based sessions.

For users, SSH appears to be a simple challenge for authentication credentials. But the usefulness of the protocol comes from the exchange of digital keys between the machines on either end of the connection. The keys are used to positively identify the user to the server, and to provide a shared basis for encrypting the session.

For process-based sessions, SSH provides one of the better ways of allowing strong authentication to replace the use of hard-coded passwords embedded in source code. This is such a leap forward in utility that it has accelerated the use of SSH in many of our production environments.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For the FTP site, we are taking advantage of the usefulness of SSH for users. Use of this site is limited to data and information transactions that require positive identification of users, and high confidentiality. SSH, when coupled with the FTP protocol, provides additional layers of authentication and encryption for file transfers. As described by Kaeo in Designing Network Security, "the SSH protocol consists of three major components:

- The Transport layer protocol, which provides server authentication, confidentiality, and integrity with perfect forward secrecy. Optionally, it may provide compression.
- The user authentication protocol, which authenticates the client to the server.
- The connection protocol, which multiplexes the encrypted tunnel into several logical channels".

The use of this new, secure FTP site requires more coordination between participants, but has already proved extremely useful in transactions with our most security conscious customers and partners.

Summary

This practical assignment provided an opportunity to closely examine an unfortunate incident, and document the actions and lessons learned. In hindsight, the incident was entirely preventable, but that is true for most events that are examined after the fact. And while this incident was relatively benign, it is representative of many more malicious exploits because of the changes in policy and practice that resulted from the experience. Our corporate view of file exchange between the company and customers has been forever changed as a direct consequence of these events. That is perhaps the most important outcome of events like this – the reshaping of perceptions among the community of people that are affected by the changed environment. We now view the external world with infinite caution, and full expectations of experiencing the "worst case scenario". That posture is expressed in our policies, our internal working procedures, and our efforts to use best practices in information security to unite our global corporate community under a single safe umbrella.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Departmental Guide to Incident Handling Planning, U.S. Department of Transportation, Office of the Secretary, DOT H 1350.255, http://cio.ost.dot.gov/InfoAssurance/HTML/DOT_H1350.255.HTML

Designing Network Security, Merike Kaeo, Macmillan Technical Publishing, 1999, p 67.

http://www.tripwire.org

http://www.netapp.com

Figures

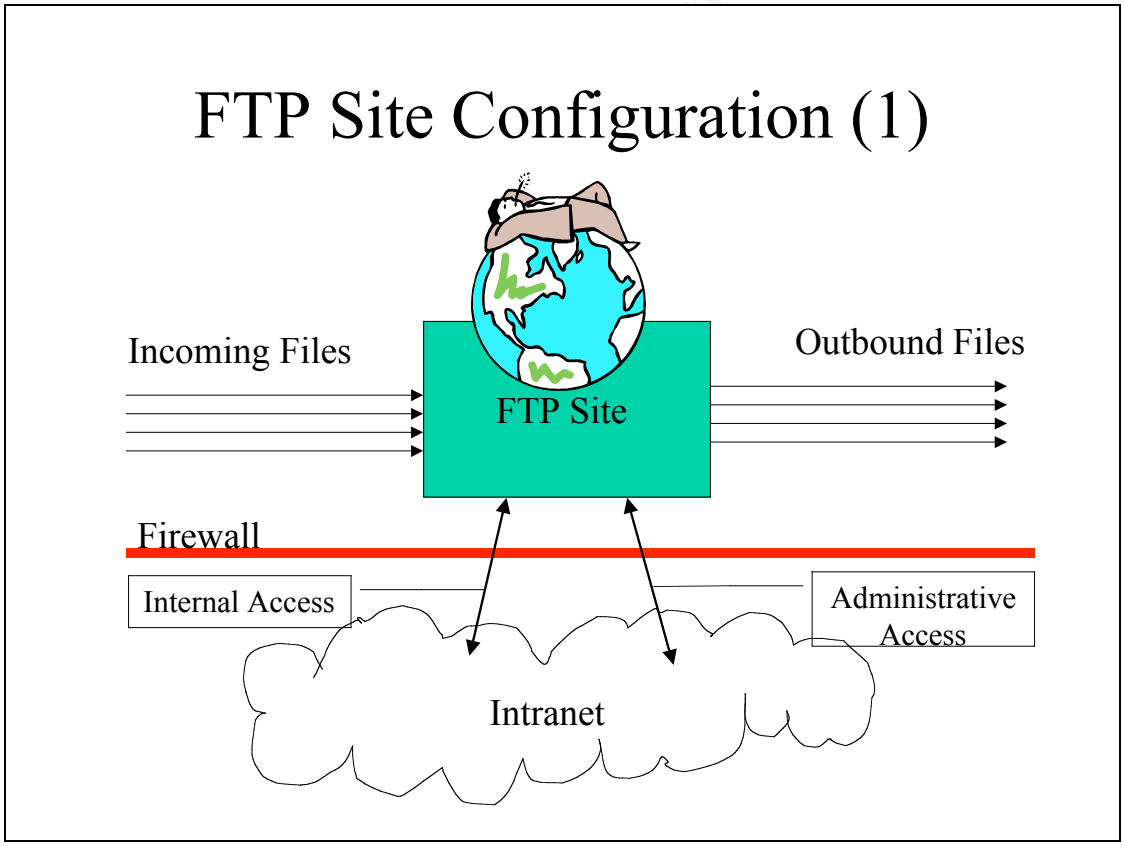

Figure 1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

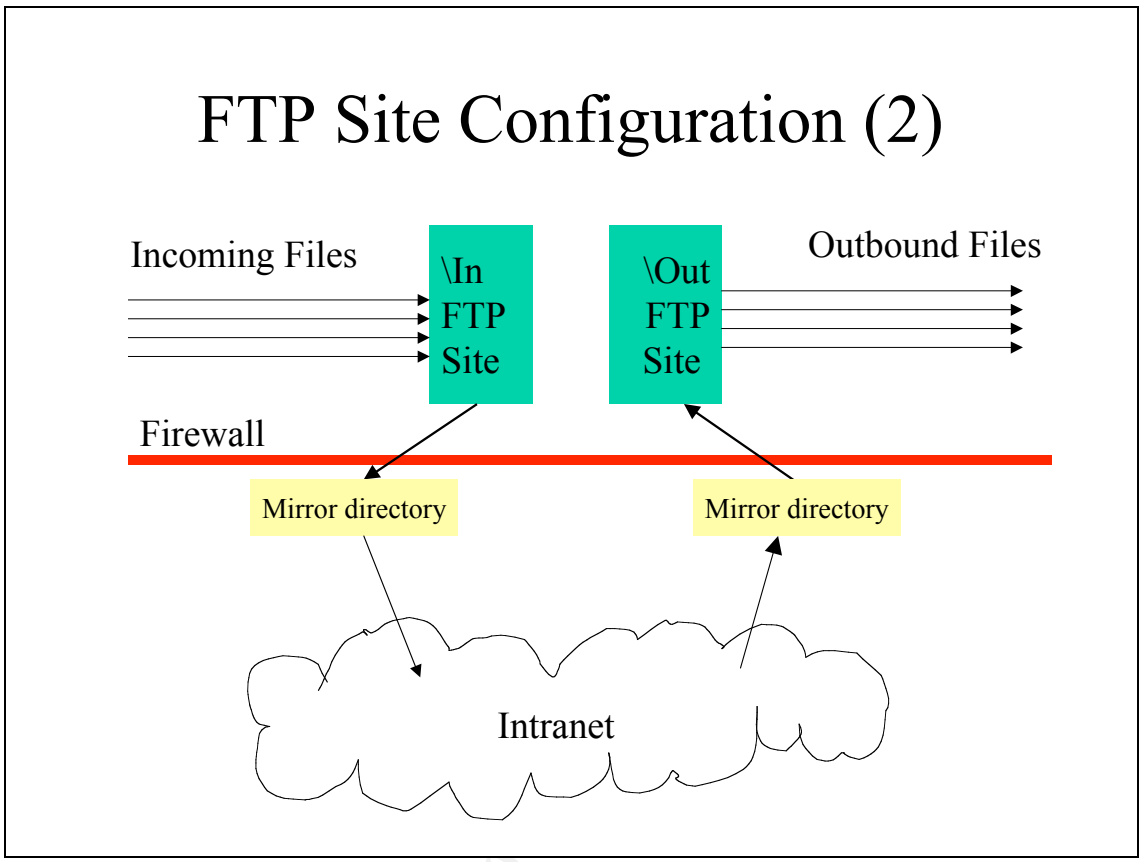

Figure 2

© SANS Institute 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: July 24th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event