

FTP

1. История и идеи на протокола

- Започнат през 1971, официалният стандарт е от 1985
- Прехвърляне на файлове м/у различни машини
Варианти за конвертиране м/у различни типове данни
- Опростен протокол

2. Принцип на работа

- login
- retr/stor
трансферът става в отделна връзка(pasv,active)
- quit

3. Самият протокол

- дефиниция на връщаните кодове (RFC959)
 - 1yz Positive Preliminary reply
 - 2yz Positive Completion reply
 - 3yz Positive Intermediate reply
 - 4yz Transient Negative Completion reply
 - 5yz Permanent Negative Completion reply
 - 6yz RFC2228 protected replies

 - x0z Syntax -
 - x1z Information
 - x2z Connections
 - x3z Authentication and accounting
 - x4z Unspecified as yet.
 - x5z File system
- Вид на continuous messages
XXX-something
whatever();
another whatever();
XXX end
- Доста по-точно дефиниран от други протоколи, с крайни автомати и описание на командите

4. Команди

- auth
USER <SP> <username> <CRLF>
PASS <SP> <password> <CRLF>
ACCT <SP> <account-information> <CRLF>
- dir. navigation
CWD <SP> <pathname> <CRLF>
PWD <CRLF>
CDUP <CRLF>
SMNT <SP> <pathname> <CRLF>
- misc
QUIT <CRLF>
REIN <CRLF>
- data connection type
PORT <SP> <host-port> <CRLF>
PASV <CRLF>
- data transfer type
TYPE <SP> <type-code> <CRLF>
ASCII
EBCDIC
IMAGE
LOCAL
STRU <SP> <structure-code> <CRLF>

- FILE
- RECORD
- PAGE
- MODE <SP> <mode-code> <CRLF>
 - Stream
 - Block
 - Compressed
- file management
 - RETR <SP> <pathname> <CRLF>
 - STOR <SP> <pathname> <CRLF>
 - STOU <CRLF>
 - APPE <SP> <pathname> <CRLF>
 - ALLO <SP> <decimal-integer> [<SP> R <SP> <decimal-integer>] <CRLF>

 - REST <SP> <marker> <CRLF>

 - RNFR <SP> <pathname> <CRLF>
 - RNTO <SP> <pathname> <CRLF>

 - ABOR <CRLF>

 - DELE <SP> <pathname> <CRLF>
- dir. management
 - RMD <SP> <pathname> <CRLF>
 - MKD <SP> <pathname> <CRLF>
- list
 - LIST [<SP> <pathname>] <CRLF>
 - NLST [<SP> <pathname>] <CRLF>
- site specific
 - SITE <SP> <string> <CRLF>
 - SYST <CRLF>
 - STAT [<SP> <pathname>] <CRLF>
- additional
 - HELP [<SP> <string>] <CRLF>
 - NOOP <CRLF>
- protected (RFC2228)
 - AUTH (Authentication/Security Mechanism),
 - ADAT (Authentication/Security Data),
 - PROT (Data Channel Protection Level),
 - C – Clear
 - S – Safe (integrity check)
 - E – Confidential (encryption)
 - P – Private (Safe+Confidential)
 - PBSZ (Protection Buffer Size),
 - CCC (Clear Command Channel),
 - MIC (Integrity Protected Command),
 - CONF (Confidentiality Protected Command), and
 - ENC (Privacy Protected Command).

5. Сървъри

- wu-ftp
- sendmail при ftp сървърите
- proftpd
- BSD ftpd
- lukemftpd
- vsftpd
- IIS

6. Атаки/security проблеми

- Некриптиран протокол
 - SSL/TLS, S/Key, OPIE, Kerberos - нестандартни добавки
 - RFC2228, RFC2773

- ftp bounce
сканиране чрез тази атака
- GET dirname.tar и т.н.
- SITE exec, SITE...
- Прескачане на firewalls
- Възможност за крадене на файлове, поради поредността на портовете при PASV
- directory traversal проблеми
- globbing DoS (ls */*/*/*/* ...), con, prn, aux при windows
- Сериозно количество exploits за различните сървъри
- exploit-и за различни кофти написани клиенти