

```

# Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
# This file may contain proprietary rules that were created,
# tested and
# certified by Sourcefire, Inc. (the "VRT Certified Rules") as
# well as
# rules that were created by Sourcefire and other third parties
# and
# distributed under the GNU General Public License (the "GPL
# Rules"). The
# VRT Certified Rules contained in this file are the property of
# Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights
# Reserved.
# The GPL Rules created by Sourcefire, Inc. are the property of
# Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All
# Rights
# Reserved. All other GPL Rules are owned and copyrighted by
# their
# respective owners (please see www.snort.org/contributors for a
# list of
# owners and their respective copyrights). In order to determine
# what
# rules are VRT Certified Rules or GPL Rules, please refer to the
# VRT
# Certified Rules License Agreement.
#
#
# $Id: ftp.rules,v 1.57.2.7.2.6 2005/07/22 19:19:54 mwatchinski
# Exp $
#-----
# FTP RULES
#-----

# protocol verification
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MDTM
overflow attempt"; flow:to_server,established; content:"MDTM";
nocase; isdataat:100,relative; pcre:"/^MDTM\s[^\n]{100}/smi";
reference:bugtraq,9751; reference:cve,2001-1021;
reference:cve,2004-0330; reference:nessus,12080;
classtype:attempted-admin; sid:2546; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XMKD
overflow attempt"; flow:to_server,established; content:"XMKD";
nocase; isdataat:100,relative; pcre:"/^XMKD\s[^\n]{100}/smi";
reference:bugtraq,7909; reference:cve,2000-0133;
reference:cve,2001-1021; classtype:attempted-admin; sid:2373;
rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP NLST
overflow attempt"; flow:to_server,established; content:"NLST";
nocase; isdataat:100,relative; pcre:"/^NLST\s[^\n]{100}/smi";
reference:bugtraq,10184; reference:bugtraq,7909;
reference:bugtraq,9675; reference:cve,1999-1544;

```

```

classtype:attempted-admin; sid:2374; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP ALLO
overflow attempt"; flow:to_server,established; content:"ALLO";
nocase; isdataat:100,relative; pcre:"/^ALLO\s[^\n]{100}/smi";
reference:bugtraq,9953; classtype:attempted-admin; sid:2449;
rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNT0
overflow attempt"; flow:to_server,established; content:"RNT0";
nocase; isdataat:100,relative; pcre:"/^RNT0\s[^\n]{100}/smi";
reference:bugtraq,8315; reference:cve,2000-0133;
reference:cve,2001-1021; reference:cve,2003-0466;
classtype:attempted-admin; sid:2389; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOU
overflow attempt"; flow:to_server,established; content:"STOU";
nocase; isdataat:100,relative; pcre:"/^STOU\s[^\n]{100}/smi";
reference:bugtraq,8315; reference:cve,2003-0466;
classtype:attempted-admin; sid:2390; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP APPE
overflow attempt"; flow:to_server,established; content:"APPE";
nocase; isdataat:100,relative; pcre:"/^APPE\s[^\n]{100}/smi";
reference:bugtraq,8315; reference:bugtraq,8542;
reference:cve,2000-0133; reference:cve,2003-0466;
classtype:attempted-admin; sid:2391; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RETR
overflow attempt"; flow:to_server,established; content:"RETR";
nocase; isdataat:100,relative; pcre:"/^RETR\s[^\n]{100}/smi";
reference:bugtraq,8315; reference:cve,2003-0466;
reference:cve,2004-0287; reference:cve,2004-0298;
classtype:attempted-admin; sid:2392; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOR
overflow attempt"; flow:to_server,established; content:"STOR";
nocase; isdataat:100,relative; pcre:"/^STOR\s[^\n]{100}/smi";
reference:bugtraq,8668; reference:cve,2000-0133;
classtype:attempted-admin; sid:2343; rev:3;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CEL
overflow attempt"; flow:to_server,established; content:"CEL";
nocase; isdataat:100,relative; pcre:"/^CEL\s[^\n]{100}/smi";
reference:arachnids,257; reference:bugtraq,679;
reference:cve,1999-0789; reference:nessus,10009;
classtype:attempted-admin; sid:337; rev:12;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XCWD
overflow attempt"; flow:to_server,established; content:"XCWD";
nocase; isdataat:100,relative; pcre:"/^XCWD\s[^\n]{100}/smi";
reference:bugtraq,11542; reference:bugtraq,8704;
classtype:attempted-admin; sid:2344; rev:3;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD
overflow attempt"; flow:to_server,established; content:"CWD";
nocase; isdataat:100,relative; pcre:"/^CWD\s[^\n]{100}/smi";
reference:bugtraq,11069; reference:bugtraq,1227;
reference:bugtraq,1690; reference:bugtraq,6869;
reference:bugtraq,7251; reference:bugtraq,7950;
reference:cve,1999-0219; reference:cve,1999-1058;

```

```

reference:cve,1999-1510; reference:cve,2000-1035;
reference:cve,2000-1194; reference:cve,2001-0781;
reference:cve,2002-0126; reference:cve,2002-0405;
classtype:attempted-admin; sid:1919; rev:22;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CMD
overflow attempt"; flow:to_server,established; content:"CMD";
nocase; isdataat:100,relative; pcre:"/^CMD\s[^\n]{100}/smi";
classtype:attempted-admin; sid:1621; rev:10;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STAT
overflow attempt"; flow:to_server,established; content:"STAT";
nocase; isdataat:100,relative; pcre:"/^STAT\s[^\n]{100}/smi";
reference:bugtraq,3507; reference:bugtraq,8542;
reference:cve,2001-0325; reference:cve,2001-1021;
reference:url,labs.defcom.com/adv/2001/def-2001-31.txt;
classtype:attempted-admin; sid:1379; rev:12;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHMOD
overflow attempt"; flow:to_server,established; content:"SITE";
nocase; content:"CHMOD"; distance:0; nocase;
isdataat:100,relative; pcre:"/^SITE\s+CHMOD\s[^\n]{100}/smi";
reference:bugtraq,10181; reference:bugtraq,9483;
reference:bugtraq,9675; reference:cve,1999-0838;
reference:nessus,12037; classtype:attempted-admin; sid:2340;
rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHOWN
overflow attempt"; flow:to_server,established; content:"SITE";
nocase; content:"CHOWN"; distance:0; nocase;
isdataat:100,relative; pcre:"/^SITE\s+CHOWN\s[^\n]{100}/smi";
reference:bugtraq,2120; reference:cve,2001-0065;
classtype:attempted-admin; sid:1562; rev:11;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE NEWER
overflow attempt"; flow:to_server,established; content:"SITE";
nocase; content:"NEWER"; distance:0; nocase;
isdataat:100,relative; pcre:"/^SITE\s+NEWER\s[^\n]{100}/smi";
reference:bugtraq,229; reference:cve,1999-0800;
classtype:attempted-admin; sid:1920; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CPWD
overflow attempt"; flow:established,to_server; content:"SITE";
nocase; content:"CPWD"; distance:0; nocase;
isdataat:100,relative; pcre:"/^SITE\s+CPWD\s[^\n]{100}/smi";
reference:bugtraq,5427; reference:cve,2002-0826; classtype:misc-
attack; sid:1888; rev:8;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE EXEC
format string attempt"; flow:to_server,established;
content:"SITE"; nocase; content:"EXEC"; distance:0; nocase;
pcre:"/^SITE\s+EXEC\s[^\n]*?%[^\n]*?%/smi"; classtype:bad-
unknown; sid:1971; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE
overflow attempt"; flow:to_server,established; content:"SITE";
nocase; isdataat:100,relative; pcre:"/^SITE\s[^\n]{100}/smi";
reference:cve,1999-0838; reference:cve,2001-0755;
reference:cve,2001-0770; classtype:attempted-admin; sid:1529;
rev:10;)

```

```

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP USER
overflow attempt"; flow:to_server,established,no_stream;
content:"USER"; nocase; isdataat:100,relative; pcre:"/^USER\s[^\n]{100}/smi"; reference:bugtraq,10078; reference:bugtraq,1227;
reference:bugtraq,1504; reference:bugtraq,1690;
reference:bugtraq,4638; reference:bugtraq,7307;
reference:bugtraq,8376; reference:cve,1999-1510;
reference:cve,1999-1514; reference:cve,1999-1519;
reference:cve,1999-1539; reference:cve,2000-0479;
reference:cve,2000-0656; reference:cve,2000-0761;
reference:cve,2000-0943; reference:cve,2000-1035;
reference:cve,2000-1194; reference:cve,2001-0256;
reference:cve,2001-0794; reference:cve,2001-0826;
reference:cve,2002-0126; reference:cve,2002-1522;
reference:cve,2003-0271; reference:cve,2004-0286;
classtype:attempted-admin; sid:1734; rev:30;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP PASS
overflow attempt"; flow:to_server,established,no_stream;
content:"PASS"; nocase; isdataat:100,relative; pcre:"/^PASS\s[^\n]{100}/smi"; reference:bugtraq,10078; reference:bugtraq,10720;
reference:bugtraq,1690; reference:bugtraq,3884;
reference:bugtraq,8601; reference:bugtraq,9285;
reference:cve,1999-1519; reference:cve,1999-1539;
reference:cve,2000-1035; reference:cve,2002-0126;
reference:cve,2002-0895; classtype:attempted-admin; sid:1972;
rev:16;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RMDIR
overflow attempt"; flow:to_server,established; content:"RMDIR";
nocase; isdataat:100,relative; pcre:"/^RMDIR\s[^\n]{100}/smi";
reference:bugtraq,819; classtype:attempted-admin; sid:1942;
rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MKD
overflow attempt"; flow:to_server,established; content:"MKD";
nocase; isdataat:100,relative; pcre:"/^MKD\s[^\n]{100}/smi";
reference:bugtraq,612; reference:bugtraq,7278;
reference:bugtraq,9872; reference:cve,1999-0911;
reference:nessus,12108; classtype:attempted-admin; sid:1973;
rev:9;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP REST
overflow attempt"; flow:to_server,established; content:"REST";
nocase; isdataat:100,relative; pcre:"/^REST\s[^\n]{100}/smi";
reference:bugtraq,2972; reference:cve,2001-0826;
classtype:attempted-admin; sid:1974; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP DELE
overflow attempt"; flow:to_server,established; content:"DELE";
nocase; isdataat:100,relative; pcre:"/^DELE\s[^\n]{100}/smi";
reference:bugtraq,2972; reference:cve,2001-0826;
reference:cve,2001-1021; classtype:attempted-admin; sid:1975;
rev:8;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RMD
overflow attempt"; flow:to_server,established; content:"RMD";
nocase; isdataat:100,relative; pcre:"/^RMD\s[^\n]{100}/smi";

```

```

reference:bugtraq,2972; reference:cve,2000-0133;
reference:cve,2001-0826; reference:cve,2001-1021;
classtype:attempted-admin; sid:1976; rev:9;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP invalid
MODE"; flow:to_server,established; content:"MODE"; nocase;
pcpre:"/^MODE\s+[\^ABSC]{1}/msi"; classtype:protocol-command-
decode; sid:1623; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP large PWD
command"; flow:to_server,established; dsize:10; content:"PWD";
nocase; classtype:protocol-command-decode; sid:1624; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP large SYST
command"; flow:to_server,established; dsize:10; content:"SYST";
nocase; classtype:protocol-command-decode; sid:1625; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD Root
directory transversal attempt"; flow:to_server,established;
content:"CWD"; nocase; content:"C|3A 5C|"; distance:1;
reference:bugtraq,7674; reference:cve,2003-0392;
reference:nessus,11677; classtype:protocol-command-decode;
sid:2125; rev:8;)

# bad ftp commands
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE ZIPCHK
overflow attempt"; flow:to_server,established; content:"SITE";
nocase; content:"ZIPCHK"; distance:1; nocase;
isdataat:100,relative; pcpre:"/^SITE\s+ZIPCHK\s[\^\\n]{100}/smi";
reference:cve,2000-0040; classtype:attempted-admin; sid:1921;
rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE NEWER
attempt"; flow:to_server,established; content:"SITE"; nocase;
content:"NEWER"; distance:1; nocase; pcpre:"/^SITE\s+NEWER/smi";
reference:cve,1999-0880; reference:nessus,10319;
classtype:attempted-dos; sid:1864; rev:7;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE EXEC
attempt"; flow:to_server,established; content:"SITE"; nocase;
content:"EXEC"; distance:0; nocase; pcpre:"/^SITE\s+EXEC/smi";
reference:arachnids,317; reference:bugtraq,2241;
reference:cve,1999-0080; reference:cve,1999-0955; classtype:bad-
unknown; sid:361; rev:15;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP EXPLOIT
STAT * dos attempt"; flow:to_server,established; content:"STAT";
nocase; pcpre:"/^STAT\s+[\^\\n]*\x2a/smi"; reference:bugtraq,4482;
reference:cve,2002-0073; reference:nessus,10934;
reference:url,www.microsoft.com/technet/security/bulletin/MS02-01
8.msp; classtype:attempted-dos; sid:1777; rev:8;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP EXPLOIT
STAT ? dos attempt"; flow:to_server,established; content:"STAT";
nocase; pcpre:"/^STAT\s+[\^\\n]*\x3f/smi"; reference:bugtraq,4482;

```

```

reference:cve,2002-0073; reference:nessus,10934;
reference:url,www.microsoft.com/technet/security/bulletin/MS02-01
8.msp; classtype:attempted-dos; sid:1778; rev:8;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP tar
parameters"; flow:to_server,established; content:" --use-
compress-program "; nocase; reference:arachnids,134;
reference:bugtraq,2240; reference:cve,1999-0202;
reference:cve,1999-0997; classtype:bad-unknown; sid:362; rev:12;)

# bad directories
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD ~root
attempt"; flow:to_server,established; content:"CWD"; nocase;
content:"~root"; distance:1; nocase; pcre:"/^CWD\s+~root/smi";
reference:arachnids,318; reference:cve,1999-0082; classtype:bad-
unknown; sid:336; rev:10;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD ...";
flow:to_server,established; content:"CWD"; nocase; content:"...";
distance:0; pcre:"/^CWD\s[^\n]*?\.\.\./smi";
reference:bugtraq,9237; classtype:bad-unknown; sid:1229; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD ~
attempt"; flow:to_server,established; content:"CWD"; nocase;
pcre:"/^CWD\s+~/smi"; reference:bugtraq,2601;
reference:bugtraq,9215; reference:cve,2001-0421;
classtype:denial-of-service; sid:1672; rev:11;)

# vulnerabilities against specific implementations of ftp
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP serv-u
directory transversal"; flow:to_server,established; content:">%
20."; nocase; reference:bugtraq,2052; reference:cve,2001-0054;
classtype:bad-unknown; sid:360; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP wu-ftp bad
file completion attempt ["; flow:to_server,established;
content:"~"; content:"["; distance:0; reference:bugtraq,3581;
reference:bugtraq,3707; reference:cve,2001-0550;
reference:cve,2001-0886; classtype:misc-attack; sid:1377;
rev:15;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP wu-ftp bad
file completion attempt {"; flow:to_server,established;
content:"~"; content:"{"; distance:0; reference:bugtraq,3581;
reference:bugtraq,3707; reference:cve,2001-0550;
reference:cve,2001-0886; classtype:misc-attack; sid:1378;
rev:15;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNFR ../
attempt"; flow:to_server,established; content:"RNFR "; nocase;
content:" ../"; nocase; classtype:misc-attack; sid:1622; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP command
overflow attempt"; flow:to_server,established,no_stream;
dsize:>100; reference:bugtraq,4638; reference:cve,2002-0606;
classtype:protocol-command-decode; sid:1748; rev:8;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP LIST
directory traversal attempt"; flow:to_server,established;
content:"LIST"; nocase; content:".."; distance:1; content:"..";

```

```

distance:1; reference:bugtraq,2618; reference:cve,2001-0680;
reference:cve,2002-1054; reference:nessus,11112;
classtype:protocol-command-decode; sid:1992; rev:8;)

# BAD FILES
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP .forward";
flow:to_server,established; content:".forward";
reference:arachnids,319; classtype:suspicious-filename-detect;
sid:334; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP .rhosts";
flow:to_server,established; content:".rhosts";
reference:arachnids,328; classtype:suspicious-filename-detect;
sid:335; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP
authorized_keys"; flow:to_server,established;
content:"authorized_keys"; classtype:suspicious-filename-detect;
sid:1927; rev:2;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP passwd
retrieval attempt"; flow:to_server,established; content:"RETR";
nocase; content:"passwd"; reference:arachnids,213;
classtype:suspicious-filename-detect; sid:356; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP shadow
retrieval attempt"; flow:to_server,established; content:"RETR";
nocase; content:"shadow"; classtype:suspicious-filename-detect;
sid:1928; rev:3;)

# suspicious login attempts
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP ADMw0rm ftp
login attempt"; flow:to_server,established; content:"USER";
nocase; content:"w0rm"; distance:1; nocase; pcre:"/^USER
\s+w0rm/smi"; reference:arachnids,01; classtype:suspicious-login;
sid:144; rev:9;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP adm scan";
flow:to_server,established; content:"PASS ddd@|0A|";
reference:arachnids,332; classtype:suspicious-login; sid:353;
rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP iss scan";
flow:to_server,established; content:"pass -iss@iss";
reference:arachnids,331; classtype:suspicious-login; sid:354;
rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP pass
wh00t"; flow:to_server,established; content:"pass wh00t"; nocase;
reference:arachnids,324; classtype:suspicious-login; sid:355;
rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP piss scan";
flow:to_server,established; content:"pass -cklaus";
classtype:suspicious-login; sid:357; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP saint
scan"; flow:to_server,established; content:"pass -saint";
reference:arachnids,330; classtype:suspicious-login; sid:358;
rev:5;)

```

```

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP satan
scan"; flow:to_server,established; content:"pass -satan";
reference:arachnids,329; classtype:suspicious-login; sid:359;
rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP USER format
string attempt"; flow:to_server,established; content:"USER";
nocase; pcre:"/^USER\s[^\n]*%[^\n]*%/smi";
reference:bugtraq,7474; reference:bugtraq,7776;
reference:bugtraq,9262; reference:bugtraq,9402;
reference:bugtraq,9600; reference:bugtraq,9800;
reference:cve,2004-0277; reference:nessus,10041;
reference:nessus,11687; classtype:misc-attack; sid:2178; rev:16;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP PASS format
string attempt"; flow:to_server,established; content:"PASS";
nocase; pcre:"/^PASS\s[^\n]*%[^\n]*%/smi";
reference:bugtraq,7474; reference:bugtraq,9262;
reference:bugtraq,9800; reference:cve,2000-0699; classtype:misc-
attack; sid:2179; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MKDIR
format string attempt"; flow:to_server,established;
content:"MKDIR"; nocase; pcre:"/^MKDIR\s[^\n]*%[^\n]*%/smi";
reference:bugtraq,9262; classtype:misc-attack; sid:2332; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RENAME
format string attempt"; flow:to_server,established;
content:"RENAME"; nocase; pcre:"/^RENAME\s[^\n]*%[^\n]*%/smi";
reference:bugtraq,9262; classtype:misc-attack; sid:2333; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP LIST buffer
overflow attempt"; flow:to_server,established; content:"LIST";
nocase; pcre:"/^LIST\s[^\n]{100,}/smi"; reference:bugtraq,10181;
reference:bugtraq,6869; reference:bugtraq,7251;
reference:bugtraq,7861; reference:bugtraq,8486;
reference:bugtraq,9675; reference:cve,1999-0349;
reference:cve,1999-1510; reference:cve,2000-0129;
reference:url,www.microsoft.com/technet/security/bulletin/MS99-00
3.msp; classtype:misc-attack; sid:2338; rev:13;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP LIST
integer overflow attempt"; flow:to_server,established;
content:"LIST"; nocase; pcre:"/^LIST\s+\x22-W\s+\d+/smi";
reference:bugtraq,8875; reference:cve,2003-0853;
reference:cve,2003-0854; classtype:misc-attack; sid:2272; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 3535 (msg:"FTP Yak! FTP
server default account login attempt";
flow:to_server,established; content:"USER"; nocase;
content:"y049575046"; nocase; pcre:"/^USER\s+y049575046/smi";
reference:bugtraq,9072; classtype:suspicious-login; sid:2334;
rev:2;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 3535 (msg:"FTP RMD /
attempt"; flow:to_server,established; content:"RMD"; nocase;
pcre:"/^RMD\s+\x2f$/smi"; reference:bugtraq,9159;
classtype:attempted-dos; sid:2335; rev:2;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP invalid
MDTM command attempt"; flow:to_server,established;

```

```

content:"MDTM"; nocase; pcre:"/^MDTM \d+[-+]\D/smi";
reference:bugtraq,9751; reference:cve,2001-1021;
reference:cve,2004-0330; classtype:attempted-admin; sid:2416;
rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP format
string attempt"; flow:to_server,established; content:"%"; pcre:"/
\s+.*?%.*/smi"; classtype:string-detect; sid:2417; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RETR format
string attempt"; flow:to_server,established; content:"RETR";
nocase; pcre:"/^RETR\s[^\n]*%[^\n]*%/smi";
reference:bugtraq,9800; classtype:attempted-admin; sid:2574;
rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNFR
overflow attempt"; flow:to_server,established; content:"RNFR";
nocase; isdataat:100,relative; pcre:"/^RNFR\s[^\n]{100}/smi";
classtype:attempted-admin; sid:3077; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP REST with
numeric argument"; flow:to_server,established; content:"REST";
nocase; pcre:"/REST\s+[0-9]+\n/i"; reference:bugtraq,7825;
classtype:attempted-recon; sid:3460; rev:2;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP PORT bounce
attempt"; flow:to_server,established; content:"PORT"; nocase;
ftpbounce; pcre:"/^PORT/smi"; classtype:misc-attack; sid:3441;
rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 2100 (msg:"FTP ORACLE
password buffer overflow attempt"; flow:to_server,established;
content:"pass"; nocase; pcre:"/^PASS\s+[^\n]{100}/smi";
reference:bugtraq,8375; classtype:attempted-user; sid:3532;
rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE INDEX
format string attempt"; flow:to_server,established;
content:"SITE"; nocase; content:"INDEX"; distance:0; nocase;
pcre:"/^SITE\s+INDEX\s[^\n]*%[^\n]*%/smi"; classtype:bad-
unknown; sid:3523; rev:2;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 2100 (msg:"FTP ORACLE
TEST command buffer overflow attempt";
flow:to_server,established; content:"TEST"; nocase; pcre:"/^TEST
\s+[^\n]{100,}/smi"; reference:bugtraq,8375; classtype:misc-
attack; sid:3630; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 2100 (msg:"FTP ORACLE
user name buffer overflow attempt"; flow:to_server,established;
content:"user"; nocase; pcre:"/^USER\s+[^\n]{100,}/smi";
reference:bugtraq,8375; classtype:attempted-user; sid:3631;
rev:1;)

```