Information on Hydra
hydra - a very fast network logon cracker which supports many different services
SYNOPSIS

hydra
[[[-l LOGIN|-L FILE] [-p PASS|-P FILE|-x OPT -y]] | [-C FILE]]
[-e nsr] [-u] [-f|-F] [-M FILE] [-o FILE] [-b FORMAT]
[-t TASKS] [-T TASKS] [-w TIME] [-W TIME] [-m OPTIONS] [-s PORT]
[-c TIME] [-S] [-O] [-4|6] [-I] [-vV] [-d] server service [OPTIONS]
DESCRIPTION

Hydra is a parallelized login cracker which supports numerous protocols to attack. New modules are easy to add, beside that, it is flexible and very fast.

This tool gives researchers and security consultants the possibility to show how easy it would be to gain unauthorized access from remote to a system.

Currently this tool supports:
adam6500 afp asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql(v4) mysql5 ncp nntp oracle oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres rdp radmin2 redis rexec rlogin rpcap rsh rtsp s7-300 sapr3 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

For most protocols SSL is supported (e.g. https-get, ftp-ssl, etc.). If not all necessary libraries are found during compile time, your available services will be less. Type "hydra" to see what is available.
Options

target
a target to attack, can be an IPv4 address, IPv6 address or DNS name.
service
a service to attack, see the list of protocols available
OPTIONAL SERVICE PARAMETER
Some modules have optional or mandatory options. type "hydra -U <servicename>" to get help on on the options of a service.
-R
restore a previously aborted session. Requires a hydra.restore file was written. Options are restored, but can be changed by setting them after -R on the command line
-S
connect via SSL
-O
use old SSL v2 and v3

-s PORT
   if the service is on a different default port, define it here
-l LOGIN
   or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS
   or -P FILE try password PASS, or load several passwords from FILE
-x min:max:charset
   generate passwords from min to max length. charset can contain 1 for numbers, a for lowcase and A for upcase characters.
   Any other character is added is put to the list.
   Example: 1:2:a1%.
   The generated passwords will be of length 1 to 2 and contain lowcase letters, numbers and/or percent signs and dots.
-y
   disable use of symbols in -x bruteforce, see above
-e nsr
   additional checks, "n" for null password, "s" try login as pass, "r" try the reverse login as pass
-C FILE
   colon separated "login:pass" format, instead of -L/-P options
-u
   by default Hydra checks all passwords for one login and then tries the next login. This option loops around the passwords, so the first password is tried on all logins, then the next password.
-f
   exit after the first found login/password pair (per host if -M)
-F
   exit after the first found login/password pair for any host (for usage with -M)
-M FILE
   server list for parallel attacks, one entry per line
-o FILE
   write found login/password pairs to FILE instead of stdout
-b FORMAT
   specify the format for the -o FILE: text(default), json, jsonv1
-t TASKS
   run TASKS number of connects in parallel (default: 16)
-m OPTIONS
   module specific options. See hydra -U <module> what options are available.
-w TIME
   defines the max wait time in seconds for responses (default: 32)
-W TIME
   defines a wait time between each connection a task performs. This usually only makes sense if a low task number is used, .e.g -t 1
-c TIME
   the wait time in seconds per login attempt over all threads (-t 1 is recommended) This usually only makes sense if a low task number is used, .e.g -t 1

-4 / -6
   prefer IPv4 (default) or IPv6 addresses
-v / -V
   verbose mode / show login+pass combination for each attempt
-d
   debug mode
-I
   ignore an existing restore file (don't wait 10 seconds)
-h, --help
   Show summary of options.

Common usernames and passwords
Usernames:
msfadmin
admin
user
kali
tester

Passwords:
admin
default
password
msfadmin
volleyball
tester