Password Brute Forcing

Password brute forcing is a method used to gain unauthorized access to accounts or systems by systematically attempting all possible combinations of passwords until the correct one is found. This approach relies on the principle that, given enough time and computational resources, any password can eventually be cracked.

Mechanism: A brute-force attack involves an automated tool that tries various password combinations, starting from the simplest to the most complex.

Types of Brute Force Attacks:

- **Simple Brute Force**: Attempts every combination without any constraints.
- **Hybrid Attacks**: Combines dictionary words with variations (e.g., adding numbers or symbols).
- **Credential Stuffing**: Uses leaked username-password pairs from other breaches.

Tool: Hydra

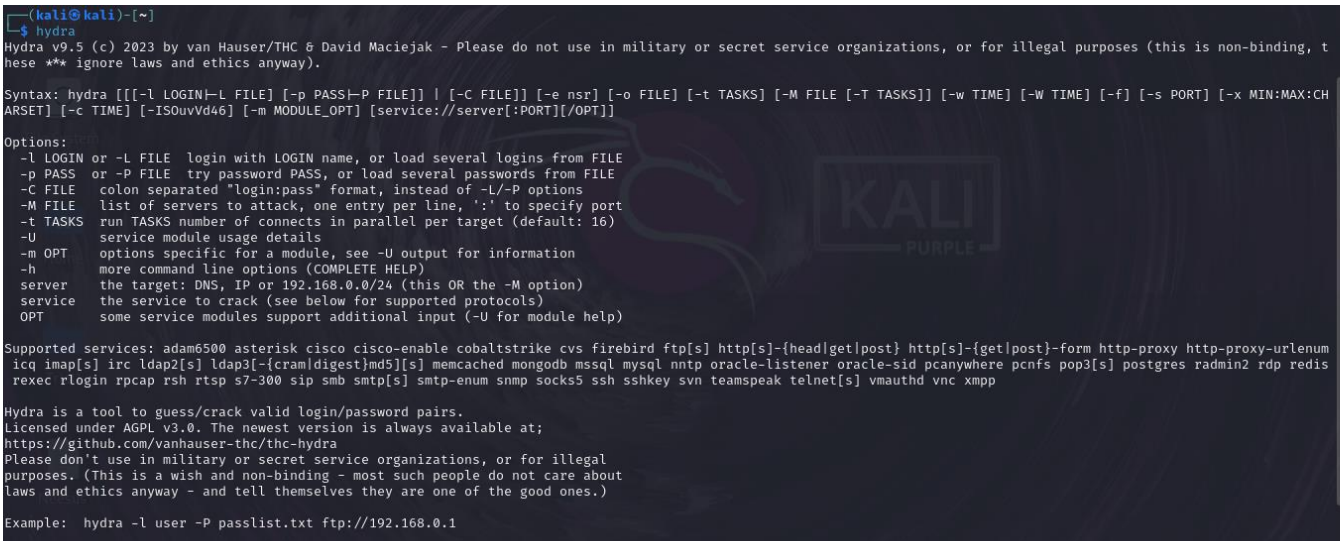
Hydra, also known as THC-Hydra, is a widely used network logon password cracking tool that specializes in brute forcing passwords across various protocols.

Hydra supports a multitude of protocols, including but not limited to FTP, HTTP, HTTPS, SMB, and SSH. Its strength lies in its ability to conduct rapid dictionary attacks, which can test thousands of passwords per minute against a target service. One of Hydra's notable features is its parallel processing capability, allowing multiple connections to be attempted simultaneously. This significantly reduces the time required to crack passwords, which is critical in penetration testing environments where speed is often essential.

Usage and Configuration

Using Hydra involves specifying the target service, the username, and the password list, along with any additional options that might refine the attack.

>>hydra -l username -P /path/to/passwords.txt ftp://target_ip



```
┌──(kali㉿kali)-[~]
└─$ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, t
hese *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CH
ARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
  -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
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] 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] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis
 rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Password Spraying

Password spraying is a type of cyberattack where an attacker attempts to gain unauthorized access to a large number of accounts by systematically trying a small number of common passwords rather than targeting a single account with numerous password attempts. This approach aims to evade detection and account lockout mechanisms that are often triggered by multiple failed login attempts.

Mechanism: Password spraying involves attackers targeting a list of usernames, often sourced from data breaches, to exploit weak passwords commonly used by many individuals. Instead of attempting numerous passwords on a single account, they test a small set of popular passwords across multiple accounts.

Tools: Kerbrute

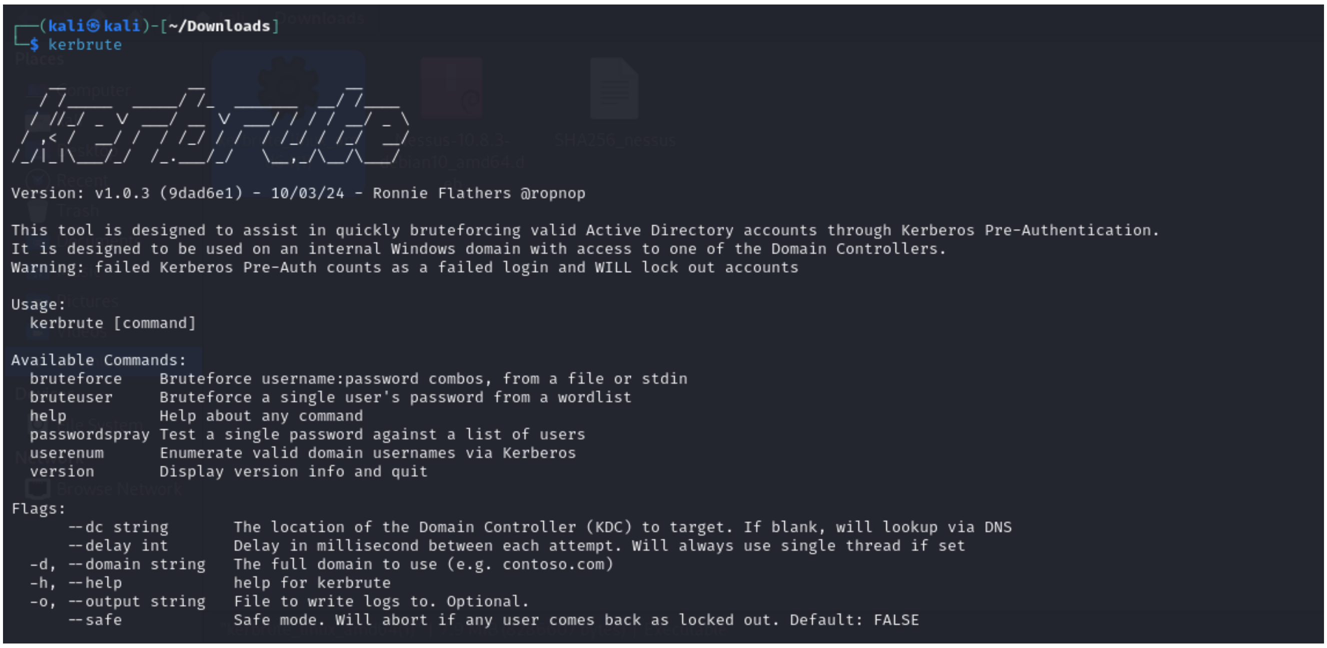
Kerbrute is a powerful tool specifically designed for conducting brute-force attacks against Kerberos authentication systems, often found in Microsoft Active Directory environments. It focuses on brute-forcing passwords and password spraying attacks.

Kerbrute targets usernames sourced from data breaches or reconnaissance and tests a limited set of common passwords across these accounts, which is a hallmark of password spraying. It operates efficiently, minimizing the likelihood of triggering account lockout mechanisms. By distributing login attempts across multiple accounts and restricting attempts per account, Kerbrute reduces the risk of detection by security systems, allowing for stealthier attacks

Usage and Configuration

With passwordspray, Kerbrute will perform a horizontal brute force attack against a list of domain users. This is useful for testing one or two common passwords when you have a large list of users. This will increment the failed login count and lock out accounts.

root@kali:~# ./kerbrute_linux_amd64 passwordspray -d lab.ropnop.com domain_users.txt Password123



```
┌──(kali㉿kali)-[~/Downloads]
└─$ kerbrute

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/03/24 - Ronnie Flathers @ropnop

This tool is designed to assist in quickly bruteforcing valid Active Directory accounts through Kerberos Pre-Authentication.
It is designed to be used on an internal Windows domain with access to one of the Domain Controllers.
Warning: failed Kerberos Pre-Auth counts as a failed login and WILL lock out accounts

Usage:
  kerbrute [command]

Available Commands:
  bruteforce    Bruteforce username:password combos, from a file or stdin
  bruteuser     Bruteforce a single user's password from a wordlist
  help          Help about any command
  passwordspray Test a single password against a list of users
  userenum      Enumerate valid domain usernames via Kerberos
  version       Display version info and quit

Flags:
      --dc string       The location of the Domain Controller (KDC) to target. If blank, will lookup via DNS
      --delay int       Delay in millisecond between each attempt. Will always use single thread if set
  -d, --domain string   The full domain to use (e.g. contoso.com)
  -h, --help            help for kerbrute
  -o, --output string   File to write logs to. Optional.
      --safe            Safe mode. Will abort if any user comes back as locked out. Default: FALSE
```