Attacker Viewpoint

a. **Who** is likely to attack the system?

Attackers who collect user information and messages between the server and multiple clients.

b. What are they likely to attack to accomplish their goal?

Transfer spam files
Disclose private messages
Spoofing both client side or server side
Tampering messages and files
Attack the database
Sending numerous packets to the server through messages and DoS the server

Asset Viewpoint

a. What is the asset?

b. What value does the asset have to the application?

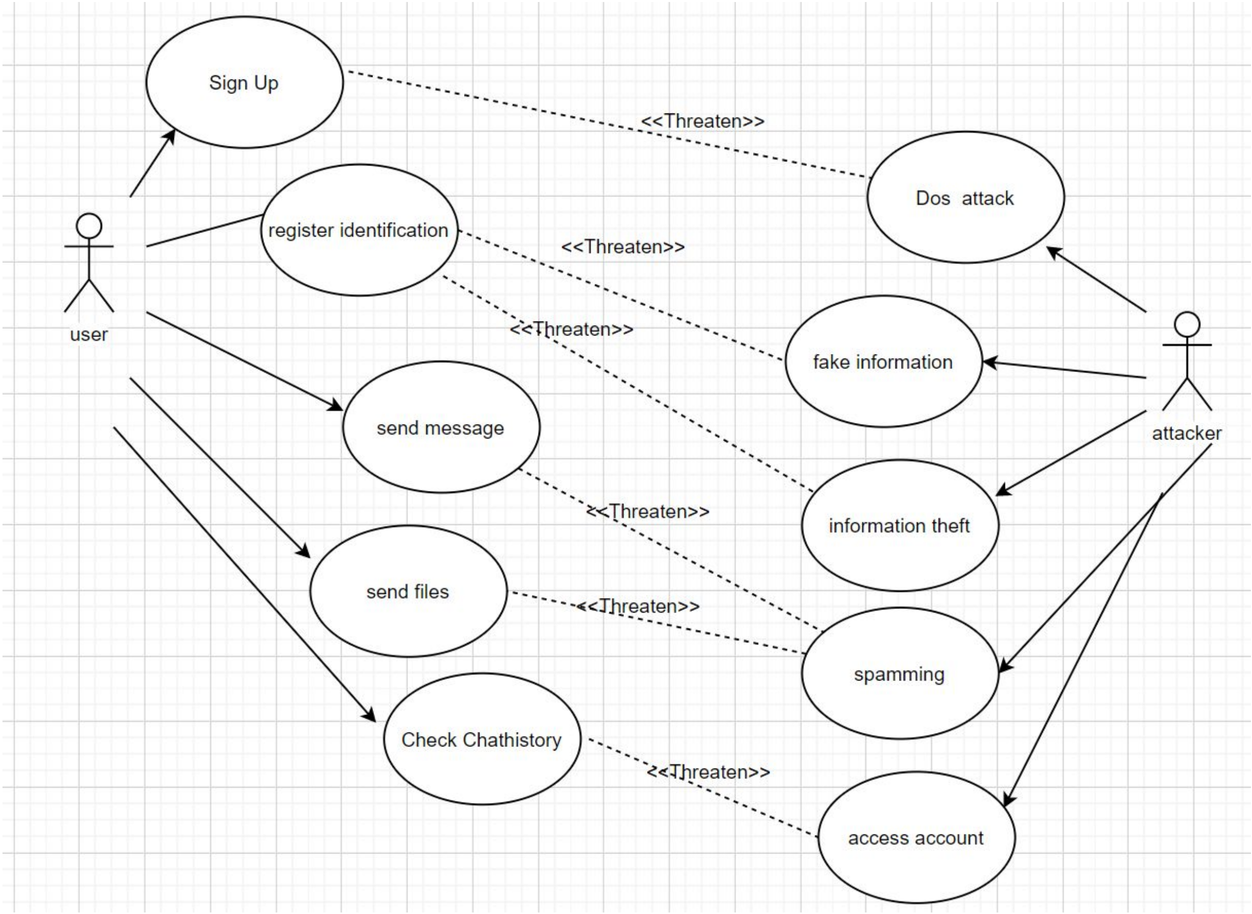
c. How might that asset be exploited by an attacker?

Asset	Value	Exploited path
User Credential	User authentication	Tampering through message or file transfer
User Personal Information	Username, password, host port, host address, message history	Information disclosure attack, attack on database for the user information or scanning through activities
Data File	Server IP, port, client socket IP address and port, server thread	Attackers may spoof the data file, tampering the data collection or exploit the data file by sending malicious files or massage code.
Availability of Server	The server be able to provide complete service to client	Attack can sending numerous packets asking for service to make the server denial of service
Availability of data file	Data file give the access for the server to receive the socket and authenticate the user with user information stored	Attackers can tampering the process of sending malicious file or massage code to the server to attack the data file

Chat History readable	Be able to view the chat history of clients	Sending the malicious code to mop up or destroy the chat history
Ability to sign up	Client can sign up an user account by signing up	Attackers can send numerous packets to the server and DoS the service. Or attackers can use user's information to sign up one already.

STRIDE

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
The attacker may access user account and send messages in name of the user	Shared files between users may be altered.	The chat history fails to write data received from users	Private message may be captured by the attacker	DDoS attack on the chat server	The attacker may gain administrator's privilege to manage user accounts
Data may be stored to attacker's target, instead of the data file	Chat history may be altered	One user fails to receive files from other users	The attacker may unauthorized access to user's message history	An external agent prevents access to a data store on the other side of the trust boundary.	An attacker may gain remote access
	User information such as names may be altered	The server claims it didn't receive data from user side			


Sign Up
<<Threaten>>
Dos attack
register identification
<<Threaten>>
user
<<Threaten>>
fake information
attacker
send message
information theft
<<Threaten>>
send files
<<Threaten>>
spamming
Check Chathistory
<<Threaten>>
access account