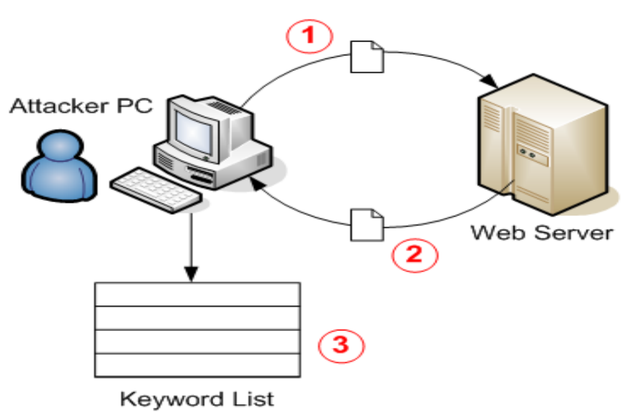
THREAT MODELING IN SOCIAL NETWORKS

1. Problem Statement:

- Social networks are ubiquitous and prone to security attacks.



2. Aim:

Comparing threat modeling tools in relation to identifying security vulnerabilities in social networks.

Vulnerability Categorization:

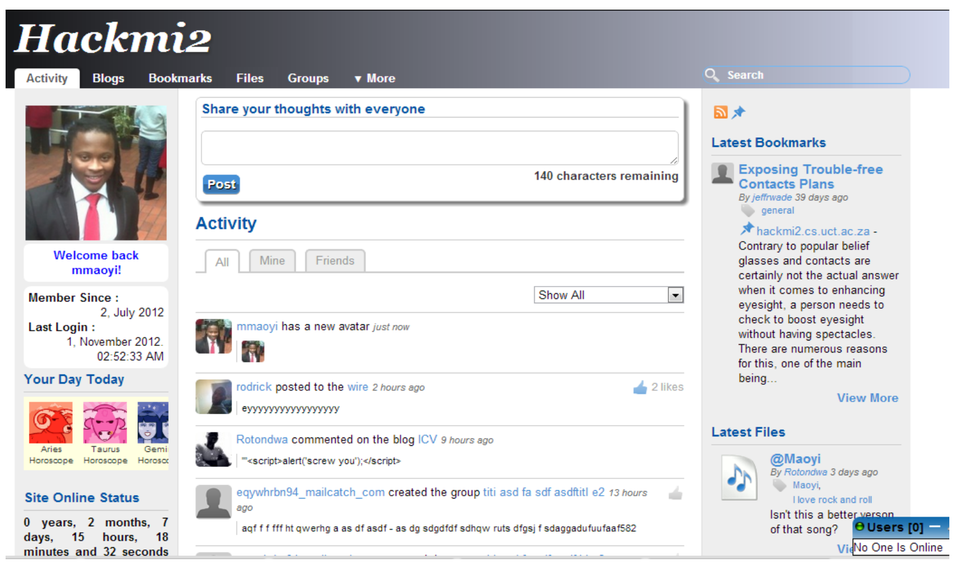
STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service.

Threat Prioritization:

DREAD – Damage potential, Reproducibility, Exploitability, Affected users, Discoverability.

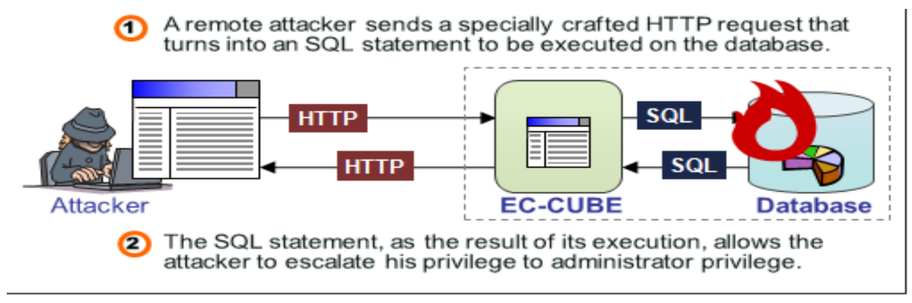
3. Solution:

- Build the Hackmi2 Social Network as a test bed for evaluating the three threat modeling tools.



4. Threat Modeling Approach:

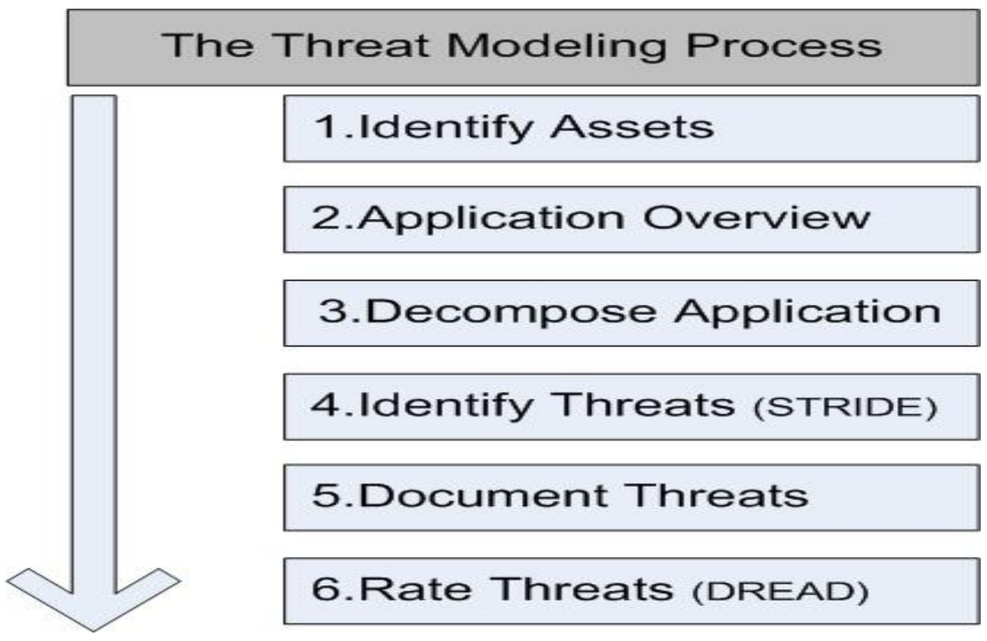
Attack Centric:



Defence centric:

5. Threat Modeling Process:

- Apply the threat modeling process to the social network using each of the three threat modeling tools.



6. Comparison:

	SensePost CTM tool	Microsoft SDL Tool	Microsoft TAM tool
Can be used by non-security experts	✗	✓	✓
Built-in Dataflow Diagrams	✗	✓	✗
STRIDE Classification of Threats	✗	✓	✓
DREAD rating to rank impact and prioritization	✓	✓	✓
Generate Attacks Trees	✗	✗	✓
Generate Threat Reports	✓	✓	✓

Department of Computer Science
University of Cape Town
Private Bag X3
Rondebosch 7701
Email : dept@cs.uct.ac.za
Tel : 021 650-2663

Supervisor

Dr Anne Kayem

Dominic White (SensePost)

Team Members

Molulaqhooa Maoyi
Rotondwa Ratshidaho
Sanele Macanda