Date:..........................

Sun Mon Tue Wed Thu Fri Sat

Activity #5.

Information Security

212-5614

Type: The type of malware involved in it is the backdoor. In backdoor the malware is able to bypass the traditional security system and can access the system.

Evade:

High privileges: Operate with elevated access to bypass security.

Concealment: Hide unauthorized access points and actions

Exploitation: Use system vulnerabilities to avoid detection.

Modification: Alter system files to prevent being spotted by security tools.

Recommended Security Measures:

-> Conduct regular security assessments to identify vulnerabilities and suspicious activities.

→ Implement kernel protection

→ Aware staff about phishing attacks.

(2) In heapoverflow attacks thed data is written beyond buffer limits, corrupting the adjacent memory. Attackers can alter pointers/ control overflow to run malicious code.

Consequences:

Heap overflow attacks can lead to unauthorized access, allowing attackers to gain control of the system and execute arbitrary code. This can result in data corruption, causing system crashes or unpredictable behaviour. Additionally, attackers may exploit this vulnerability for privilege escalation, gaining higher levels of access within the system.

Prevention:

→ Input Validation

→ Use functions like strncpy to limit copying.

→ Detect heap overflow

→ Identify issues early in development.

3 Common Techniques for SQL injection Attacks:

→ Tautology - Based Attacks: Injecting a tautology into a query to by-pass authentications checks.

→ Union-Based: Using UnionSELECT to combine results from multiple queries and extract data from tables.

→ Blind SQL Injection: Where attackers deduce information based on the application's responses to crafted queries, even without seeing direct output.

Security Measures:

→ Deploy Webapplication Firewalls.

→ Limit Database permissions

→ Employ stored procedures that encapsulate SQL statements

→ Use prepared statements with bound parameters to seperate SQL code from data

4 Data Inference and Encryption:

"These attacks occur when attackers analyze multiple publicly available datasets to deduce sensitive information, such as identifying individuals

This can result in risks like identity disclosure, reputational damage, and legal repercussions. To prevent such breaches, data encryption techniques like data-at-rest and ~~dat~~ data-in-transit encryption. are essential, while homomorphic encryption enables computation on encrypted data. However, querying encrypted data presents challenges, including performance overhead, complexity in queries, and limitations in analytic capabilities, potentially hindering data usability.