Malware Analysis and Prevention

Case Study: A healthcare provider experienced a data breach where patient records were stolen. Upon investigation, it was discovered that the systems were infected with a sophisticated rootkit that had been silently operating for months, capturing sensitive information and transmitting it to a remote server. The rootkit exploited vulnerabilities in the network infrastructure and bypassed traditional security measures.

Question: Analyze the type of malware involved in this case and explain how rootkits evade detection. What security measures should the healthcare provider implement to prevent similar attacks in the future?

Memory Corruption and Exploitation

Case Study: A social media platform was found to be vulnerable to a heap overflow attack. Attackers exploited a memory allocation error to overwrite critical data structures and gain control of the execution flow. This allowed them to execute arbitrary code, potentially leading to unauthorized access or system compromise.

Question: Explain the mechanisms of heap overflow attacks and the potential consequences. Discuss the techniques that could have been used to prevent or mitigate this vulnerability.

SQL Injection and Countermeasures

Case Study: An online banking platform experienced a data breach where customer financial information was compromised. The attacker injected malicious SQL code into a search form, bypassing input validation and executing unauthorized queries. This allowed the attacker to extract sensitive data, including account balances and transaction history.

Question: Describe the common techniques used to launch SQL injection attacks. What security measures can be implemented to prevent SQL injection vulnerabilities in web applications?

Data Inference and Encryption

Case Study: A government agency faced a privacy breach where sensitive personal information was inferred from publicly available data. By combining and analyzing various datasets, attackers were able to reconstruct individuals' identities and reveal confidential details. The agency needed to protect its data while still enabling legitimate data analysis.

Question: Explain how data inference attacks can be carried out and the potential risks involved. What encryption techniques can the agency employ to safeguard its data, and what are the challenges in querying encrypted data?