MOVEit hack (10 points)

On June 15, 2023, Reuters reported that several US federal agencies have had their data compromised by a global hacking campaign. Attackers used a zero-day attack against MOVEit, which was used by these agencies. MOVEit manages encryption and decryption for secure file transfer over the Internet, using SSH to secure communications. Data successfully stolen by the attackers includes that of millions of American citizens' personal information.

MOVEit allows authentication by SSH or a web portal (HTTPS). The web portal has a vulnerability that parses specially crafted packets incorrectly, allowing the attacker to execute any command on the SQL database. Attackers did not have arbitrary code execution capabilities on the attacked machine itself.

Remember to explain your answers.

(1) [2 points] Based on the information in the question, what type of vulnerability did the attackers use?

(2) [2 points] The attacker created a new user with the login name 'Health Check Service'. Then, attackers can remotely login at any time as this user and download data from the database. Which malware exploit technique does this describe?

(3) [2 points] Suppose there is no patch yet. How can you block this attack without disabling MOVEit?

(4) [2 points] It is possible that details of SSH, including the public verification key, hash algorithms and encryption algorithms used, and key length of AES may be stolen by such an attack. How would this affect the security of MOVEit?

(5) [2 points] MOVEit encrypts files using PGP — the receiver's public key is delivered out of band (assume it is securely delivered). **Assume the MOVEit attack does not exist** and compare the security of MOVEit to sending files by Gmail (which uses TLS).