Component	Description
Asset	System itself
Threat Category	A. Protection Mechanism: Technology B. State: Transit C. Asset: Elevation of Privilege
Risk	A. Damage Potential: 10, whole file structure could be destroyed. B. Reproducibility: 10, could be successful every time C. Exploitability: 6, skilled cracker could succeed. D. Affected Users: 1 E. Discoverability: 6, can be found with thought or reason.
Mitigation	Don't allow the student commands to run as an admin. Make them run as the service user.
Comments	This is a very dangerous problem. It is important that the student cannot run commands that would be ran as a system account.

Strategy Type: Prevention

The best strategy for this threat is prevention.

Prevention-This is the chosen strategy.

Preemption- It is nearly impossible to know which student would launch an attack, because of this a preemptive strategy type would be ineffective and most likely cause large amounts of collateral damage.

Deterrence- This strategy type would work for any students that wanted to stay at the school, unfortunately this strategy still leaves a large attack surface.

Deflection- This strategy is not applicable in this situation.

Detection- This strategy is similar to deterrence, in that it would work for a set of students but would still leave an attack surface.

Countermeasure- This strategy would work but would be more complex than prevention.

Implementation

This bug will be fixed by creating a separate account that has limited permissions. When the testbed command is called, the program will run as that account.

Verification

The testing of this will require a test program that has several functions that try to copy, delete or otherwise preform elevated actions. The tester will load the program and run it against the testbed. The tester will then confirm that the targeted files and actions were not moved, deleted or completed.