



Root Cause Analysis

Event: Reset of Student Lab Domain Account Passwords

Summary:

- A. Synopsis: Reported by OIT Service Support Center that multiple student Lab domain accounts appeared to have their passwords reset between 4:45PM and 5:05PM, Thursday 7 Sep 2006
- B. Cause: Account creation script malfunctioned
- C. Action Items: Determined the cause of the issue and modified the account creation script.
- D. Future Prevention: Q&A all scripts by a second technician and test in non-production environment prior to deployment.

Detail:

Synopsis: OIT Service Support Center from lower campus called to report that they were receiving multiple reports of student accounts in the Labs domain appearing to have had their passwords reset. It was determined that this happened between 4:45PM and 5:05PM on Thursday 7 Sep 2006.

Cause: Check of server event logs did not show any unusual activity relating to password resets being accomplished by individuals or by a service running in the background. Continued trouble shooting of issue revealed that a technician was working on issues relating to account creations in the labs domain that had been reported earlier in the day. As part of the trouble shooting process, the technician ran the account creation script to test that accounts were being created. A portion of the script, that had been remarked out so as not to run, accidentally ran modifying accounts. The result of the modification portion was to reset account passwords back to default. Check of modification logs revealed that 225 accounts were affected.

Action Items: Upon discovery of issue, immediately notified OIT Service Support Center of the result and what action to take to aid affected students to be able to login and reset their passwords. Additionally, notified OIT CAT that

they should post notices in the various Labs describing the issue and the action that a student would need to take to insure they could login and change their passwords. OIT-ITS Windows Servers removed the portion of the script that performed the account modifications from the creation script.

Future Prevention: Procedures were immediately put in place requiring a Q&A of any modifications to currently running scripts by a second technician and to test any changes to scripts in a non-production environment. Trouble shooting procedures will be updated to include the above actions to prevent future possibilities of re-occurrence.