# Global Information Assurance Certification Paper

# SANS GIAC ADVANCED INCIDENT HANDLING PRACTICUM

## OPTION 1: INCIDENT ANALYSIS

**BY: ROBIN ANDERSON**

**Date: February 20, 2001**

# TABLE OF CONTENTS

# EXECUTIVE ABSTRACT & SUMMARY

*Please note: The identities of the parties involved (especially students protected under FERPA) have been sanitized for the purposes of this report.*

The series of related incidents detailed in this report involved an insider abusing a position of trust within our organization. The insider was a student who worked for the Help Desk, and as such, had privileges to change other users' passwords. The insider obtained the username/password pair of another trusted student who also worked for Help Desk and subverted that student's account as a blind for future illicit activity. Since the compromise of the coworker's account was done in a non-obvious way, it went undetected for nearly three months.

The insider, using the coworker's account, changed the passwords on several other students' accounts without their permission or consent. The insider then accessed, and in one case tampered with, these accounts and copied out course-related project files and tried to cover his tracks.

The insider's particular motives (plagiarism) are more-or-less unique to the academic/university environment, though his methods (abuse of privilege) are not. Universities that receive federal funds are also subject to a number of guidelines that do not obtain in the commercial world – for instance, FERPA (the Family Educational Rights and Privacy Act, *see References*) mandates that educational documents and records pertaining to identified students be kept confidential. This, combined with the gravity of an accusation of academic plagiarism and the fact that our investigation pointed to an insider, meant that we had to act both quickly and circumspectly.

This report will first present some terminology, and a description of the in-house tools that were abused by the insider.

Next, our organization's preparations for and responses to this incident will be examined in terms of the SANS Institute's six-phase model. The lessons we learned from these incidents are also considered, along with some improvements we plan to make to our organization's internal procedures.

We conclude with a detailed analysis of critical steps in the process and the evidence gathered to support our interpretation of events.

# BACKGROUND

## Terms Used and Parties Involved in the Incidents

| | |
|---|---|
| Campus Department responsible for Computer Security: | Campus Computing Services (CCS) |
| CCS Security Officer and NIDS Handler: | Andy |
| CCS Junior Security Officer: | Robin *(the author of this report)* |
| | |
| The Insider: | Evan (username evan) |
| The Blind used by the Insider: | Irwin (username irwin) |
| Primary Victims: | Arnold (username Arnold), Beatrice (username beatrice) |
| Ancillary victims: | AV1, AV2, AV3, AV4, AV5, AV6, AV7, AV8 |
| | |
| Course Involved: | CIS Programming I |

## Background – CCS In-House Tools

WebAdmin is an online, web-based tool written and used by CCS to allow designated professional and student employees to perform account maintenance for other users. The most common maintenance activity is password changing; users who have forgotten their account passwords must physically present themselves at the CCS Help Desk and show valid student, state, or military ID to get a new password. Help Desk management staff must approve any other user verification mechanism.

Employees must authenticate themselves prior to any WebAdmin activity by entering their username and password. Once employees are password verified and checked against an LDAP access list, they receive transient authorization "cookies" that allow them to perform a series of tasks without having to re-authenticate for each individual command. The system requires an explicit "logout" operation from the user in order to delete the authorization cookie. In the evidence logs *(see Evidence and Chain of Custody)*, this action is referred to as "WebAdmin service ticket issued."

*(Please see Appendix A: Screenshots, Figures 1 & 2 for WebAdmin screen shots)*

# THE INCIDENTS

## Phase 1: Preparation

CCS employs a Security Officer who is responsible for the organization's preparedness across a broad range of security issues. As a result of long-term efforts, the following relevant measures were already in place before the incidents under consideration occurred:

- Well-established channels of communication with key campus offices and departmental personnel

  Possibly the most important thing a University security officer can do is to establish good working relationships with critical folks. These include the various legal offices on campus (University Counsel and Student Judicial Affairs), centralized and departmental sysadmins, and application developers.

  CCS Security has an excellent relationship with the Director for Student Judicial Affairs. This facilitates the efficient exchange of information, whether about University policy, case specifics, or progress updates. After the conclusion of our investigation, we were able to coordinate the insider's dismissal from CCS and the lodging of formal University charges.

  Sysadmins had two tasks in resolving this incident, one direct and one indirect. Their direct involvement was limited to the partial restoration of Beatrice's damaged files by the central Unix sysadmin in December. Their indirect involvement – the logging mechanisms they had set up on their various systems – was more significant to the investigation. Without logs to provide correlation, we would have been at a loss to determine what really happened. Discussions between the Security Officer and site Sysadmins yielded a strong and cohesive policy on centralized logging (see below).

  Having good communications with application developers means that security measures can be built into the actual design of new programs from the start. CCS Security can also get advance notice of new applications released into production. In this incident, the Security Officer had to confer with the WebAdmin developer to find out where certain information was being logged, in what format it was being logged, and how it corresponded to other logs. Deciphering and correlating the log information would have been quite tedious and difficult without the designer's help.

- Centralized, dedicated log host

  Another important thing a large-site Security Officer should do – whether the site is academic or commercial – is set up a centralized, dedicated log host and convince site sysadmins to direct logging to it. Correlation without supporting data streams is impossible. The incidents presented here could not have been successfully resolved without extensive log analysis. Having reliable logs in a central location meant that we could be sure of having all the data possible at our disposal. It turned out to be particularly important in this case since our theory of events changed drastically as we did more research (*see Phase*

*Two: Identification)*.

- Log analysis scripts with designated maintainer who was very familiar with site logging setup and code

  The CCS Security Officer is the developer and maintainer of a number of log analysis and information retrieval scripts. Again, this turned out to be crucial in this incident, since we had a large volume of data to parse and the WebAdmin log format and content were still quite new to us. The Security Officer's familiarity with the system and how to manipulate it saved us all a great deal of time and headache. *(See Appendix B: Scripts for key scripts)*

- Authentication procedures for WebAdmin password changing facility

  UMBC began using a Kerberos authentication scheme for all centralized accounts and services long before CCS developed the WebAdmin suite. Because of the limited logging capabilities and enormous power of the standard Kerberos `kadmin` tool, only full-time sysadmins and a very small number of highly trusted student employees were given access to change other users' passwords. As the user base at UMBC grew, CCS realized that a larger number of student employees would need to be able to assist users with password changes.

  This meant that CCS needed to develop tools that were both easier to use and better at logging. WebAdmin was designed as an authenticated, controlled web portal to handle password manipulation and other privileged tasks. Once WebAdmin was in production, `kadmin` privileges were revoked for all student employees. Now they had to hold not only the appropriate username/password pair for their own authentication, but their user instance had to be in a specific access group defined in the central LDAP directory. This gave CCS a fairly high degree of certainty as to who (or at least, whose account) was performing privileged activities on behalf of other users.

- Logging of WebAdmin Privileged Activities

  Because of the sensitive nature of the privileged activities available through WebAdmin, every transaction is logged to the central logging server. This way, CCS knew that a clean copy of the logs could be accessed if necessary and analyzed at will. While this incident showed that we needed to make some modifications to WebAdmin's log messages, it also proved once again that logs are the Security Officer's best friends.

  In fact, CCS Security has been helped so much by these kinds of logs that it is now standard practice in the department to have *all* newly developed applications log to the central logging server, even if only for their shakedown period.

- Limits on WebAdmin authority

  There are self-regulating constraints built into the design of WebAdmin. For example, no one can change the password of another user with the same or greater WebAdmin privileges. This prevents an insider from simply changing the password of a higher-level administrator and wreaking havoc with it. While this cannot protect users with lesser privileges, it is a sanity check. It also means that student employees cannot simply change coworkers' passwords for illicit activities. The subverted account username/password pair in this incident were obtained in an old-fashioned way – the insider saw them written down! *(See Phase Four: Eradication, February 14).* Any attempts to make same-level or higher-level password changes are logged with a specific tagline.

- Internal Trouble Ticket Assignment Procedures

  When users report suspected security problems, including hacked accounts and other related misuses, the report is entered into the CCS trouble ticketing system and by established procedure, is then assigned to the Security group. From there, they are assigned to a specific incident handler on the team for investigation.

## Phase 2: Identification

*The development of this investigation is rather interesting; the progression of our theories, the uncovering of new evidence, and the forensics all proved quite challenging.*

What appeared at first to be a simple incident became more involved every time we tried to close the case. With each expansion came a new theory of what kinds of misconduct had taken place. Soon we found that we were unsure even of the nature and number of the infringements, much less who might be responsible for them.

The timeline that follows in Phases 2-6 represents our progressive understanding of the incident and how it developed into a full-fledged insider-run-amok story. For specific log entries, please see the "Evidence" section of this report.

**December 13**

This was the first indication that there was a problem.

Beatrice's complaint about repeated, unauthorized password changes was entered into the Remedy trouble ticket system and was assigned to the Security workgroup at a normal priority level.

An hour later, Beatrice physically went to the Help Desk to get her password changed and to elaborate on the related problems she was experiencing. The Help Desk student on duty

entered the following case notes:

> Each time user has a project due for CIS Programming I her password does not work. This is the second time her password has become unusable. She believes someone gets into her account to try to get her work. It happens every time a project is due. I did change her password, but she would like to have her account investigated. She was able to log in the am on Monday, but not since.
>
> The code within her project files is missing. There is now just a line with dummy letters. Even the project she had submitted and was working properly is now like that. The professor brought this to her attention after she submitted the project. Customer is wondering if we can have her backup files from Saturday or Sunday. The project was completed on Saturday with code intact. She did the comments on Sunday and the file was intact, but when she submitted it, the code somehow got changed. This is a potential security violation issue.
>
> Also, is there any way of telling when her password has been changed, besides today? The customer has NOT been changing her password. The last time she changed her password herself was over two weeks ago, and she didn't think anything was wrong, just that the password had gone bad for some reason. But since this happened again, she suspects a security violation, especially since her code disappeared.

*Status Summary and Working Hypothesis*

> *Investigation opened.*
> *No tentative hypothesis yet.*

**December 14**

Andy's notes from his conversation with Beatrice:

> Beatrice said that her project files had been corrupted and her password changed. She also said that her password had been changed before without her knowledge. Thus far, the complaint seemed to fit the usual profile for stalking, but Beatrice insisted that she did not have current or former boyfriends nor had anyone been behaving as if they wished to be future boyfriends. She also believed that her project files had been copied to be turned in as someone else's work, though I thought it odd that someone would call attention to themselves by corrupting the originals. She said that she had last worked on her project on Sunday, 10-dec-2000. When I told her that there had been activity in her account on Monday afternoon from the library, she assured me that it hadn't been her.

```
Dec-11 17:43:55     webadmin[11846]:password change successful for Beatrice by guid=irwin
-----------------------------------------------
Dec-11 18:06:47     sgi2 /login[3336619]:?@library-authenticated-pc27 as Beatrice
-----------------------------------------------
Dec-11 18:11:22     sgi2 /ftpd[3371275]:login from library-authenticated-pc27 as Beatrice
```

> She said that she had no friends or acquaintances in CIS Programming I. At this point I was considering a stalker or hostile prankster as a strong possibility. Beatrice said that she had never shared her password, but shoulder-surfing is not unusual in a crowded lab.

A long listing of the user's damaged directory indicates that the project files were modified between 18:14 and 18:16 on 11-dec-2000:

```
[admin@restore]$ ls -l
total 20
-rw-------    1 beatrice  general       30 Dec 11 18:14 BTNode.cc
-rw-------    1 beatrice  general       21 Dec 11 18:14 BTNode.h
-rw-------    1 beatrice  general       38 Dec 11 18:14 BinTree.cc
-rw-------    1 beatrice  general       23 Dec 11 18:14 BinTree.h
-rw-------    1 beatrice  general       22 Dec 11 18:15 Knowledge.cc
-rw-------    1 beatrice  general       29 Dec 11 18:15 Knowledge.h
drwx------    2 beatrice  general     2048 Dec  9 19:37 ii_files
-rw-------    1 beatrice  general       10 Dec 11 18:15 makefile
-rwx------    1 beatrice  general        0 Dec 11 18:16 proj4
-rw-------    1 beatrice  general       10 Dec 11 18:16 proj4.cc
drwx------    3 beatrice  general     2048 Dec 13 11:27 temp
drwx------    3 beatrice  general     2048 Dec  8 19:32 temp2
```

*Status Summary and Working Hypothesis*

*After talking with Beatrice, Andy began to suspect that this incident might be a prank pulled by someone she knew. Since she said that her password had been changed without her knowledge or consent, Andy checked the WebAdmin logs to find out who had done it, thinking that it would be the prankster. It turned out to be Irwin's account and he was known to be a student employee of the Help Desk.*

*Pranksters and stalkers are often our initial guess, especially when a female student finds that her account has been tampered with. An unfortunately high percentage of university computer security incidents are stalking-related (see Assessment Tools, question list, 4f).*

*So, our first guess at identification was "Stalker."*

**December 15**

Andy assigned the Remedy trouble ticket for this incident to me for further investigation. Jointly working on case, we used log analysis tools *(see Appendix B: Scripts, "snarf-string")* to begin checking Beatrice's recent activity. We also wrote up a set of CCS-standard questions to ask her *(see Assessment Tools)*.

That afternoon, Beatrice called the Help Desk to check on the progress of the investigation. The call was transferred to me and I asked her the standard questions mentioned above and followed up with a few specifics that had raised some mental flags as we reviewed the data.

Robin's notes from 1st phone interview:

> Between 7-8pm Monday, she couldn't log in. "Same thing" happened when proj3 due 2-3 weeks ago. (Her password changed - she turned in code successfully.) She did not change her password on 11th or have anyone else do it. Help Desk changed it for her on the 13th. She logged in after Help Desk changed to check everything and found her code was garbage.
>
> Checked with professor - he got copies from 11th and they were garbage. She submitted 9th or 10th.
>
> On 13th, she requested restore of files from Sat. or Sun. to verify that they weren't garbage.
>
> Never told anyone her password, never shared it, not even with family. Not a real word.

Logs in from labs, 104 or 005, occasionally from library. Thinks she logged in from library to see if files were restored. Logs in from home with dial-up.

Doesn't know of people who might be problem. Not allowed to date.

Classmate? CIS Programming I

*Status Summary and Working Hypothesis*

*I talked with Beatrice and confirmed that she had not requested or authorized any password changed (other than on the 13th) and that she was generally quite careful with her password. Since she emphasized the course angle so much, we started looking for some kind of connection between the illicit activity and CIS Programming I.*

**December 18**

Checking the logs for Irwin's activity yielded no correlations.

Checking the logs for the workstation from which Beatrice's account was accessed yielded activity from the AV7 account:

```
Dec-11 17:58:07       library-authenticated-pc27/login[GINA]: AV7
-----------------------------------------------
Dec-11 17:59:45       sgi2 /telnetd[2977104]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 17:59:57       sgi2 /login[3222534]:?@library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:03:20       sgi2/ftpd[3059295]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:03:24       sgi2/ftpd[3059295]:login from library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:06:33       sgi2/telnetd[3392025]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:06:47       sgi2/login[3336619]:?@library-authenticated-pc27 as beatrice
-----------------------------------------------
Dec-11 18:11:21       sgi2/ftpd[3371275]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:11:22       sgi2/ftpd[3371275]:login from library-authenticated-pc27 as beatrice
-----------------------------------------------
Dec-11 18:19:58       sgi2/telnetd[1999271]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:20:12       sgi2/login[3262427]:?@library-authenticated-pc27 as AV7
```

From the Security Officer's logs:

This seemed to bring back the harassment theory. We looked for further correlation.

Activity logs for AV7 showed that password being changed at about the same time as Beatrice's. This took place while AV7 was logged in through an ISP and were followed by several failed login attempts.

Finally, the activity logs for the Web Admin system showed three passwords, all being changed at about the same time, all using the Irwin's account:

```
Dec 11 17:42:49 webadmin[11942]: password change successful for AV7 by guid=irwin
-----------------------------------------------
Dec 11 17:43:55 webadmin[11846]: password change successful for beatrice by guid=irwin
```

```
------------------------------------------------
Dec 11 17:46:21 webadmin[11846]: password change successful for AV6 by guid=irwin
```

*Status Summary and Working Hypothesis*

*We began analyzing stored system logs from the 11th. The most significant item we found was that two other users (AV6 and AV7) had activity patterns – and password change times – that paralleled Beatrice's. It now appeared that she was not the only victim in this incident.*

*The same Help Desk employee had changed all three passwords within the span of four minutes. If it turned out that the three victims and Irwin were all in the CIS Programming I class, then the case promised to tie up very neatly.*

*The requested files were restored, but there was no backup of Beatrice's most recent work. She had done a significant amount of work after the files had been committed to tape, but the files were corrupted before the next backup occurred.*

*Our next guess at identification was "Course-mate," so the next question was whether Help Desk student employee Irwin was also taking CIS Programming I.*

**December 19**

Robin's notes from 2nd phone interview:

> Beatrice does use CCS lab in Library basement consistently, she did use it on the 11th. She did use computer in lab 216 before going to Help Desk, but couldn't log in. Uses telnet from home. Often logs into "Net Zero" ISP before connecting here.

Andy wanted to investigate the other accounts found in the password-change cluster, so he began by retrieving activity logs for AV7 on December 11th. What follows is the pertinent excerpt. The first entry shows AV7 being able to login normally. The second entry shows the illicit password change for AV7, while AV7 was still remotely logged in. The third entry shows the insider logging into AV7's compromised account. After this, we see a long series of remote login failures for AV7. The last entry shows AV7's password being reset by the Help Desk.

```
Dec-11 17:31:05       sgi1/login[409569]:?@psi.net as AV7
------------------------------------------------
Dec-11 17:42:49       webadmin[11942]:password change successful for AV7 by guid=irwin---
------------------------------------------------
Dec-11 17:58:07       login[GINA]:library-authenticated-27  as AV7
------------------------------------------------
Dec-11 17:59:57       sgi2/login[3222534]:?@library-authenticated-pc27 as AV7
------------------------------------------------
Dec-11 18:03:24       sgi2/ftpd[3059295]:login from library-authenticated-pc27 as AV7
------------------------------------------------
Dec-11 18:04:44       sgi1/login[409569]:Logout: AV7
------------------------------------------------
Dec-11 18:20:12       sgi2/login[3262427]:?@library-authenticated-pc27 as AV7
------------------------------------------------
Dec-11 18:53:49       sgi1/login[425702]:failed: ?@psi.net as AV7
------------------------------------------------
Dec-11 18:54:00       sgi1/login[425702]:failed: ?@psi.net as AV7
------------------------------------------------
Dec-11 18:54:25       sgi2/sshd[3117538]:log: Password authentication of user AV7 using
Kerberos failed: Decrypt integrity check failed
------------------------------------------------
```

```
Dec-11 18:54:32       sgi2/sshd[3117538]:log: Password authentication of user AV7 using
Kerberos failed: Decrypt integrity check failed
-----------------------------------------------
Dec-11 18:54:39       sgi2/sshd[3117538]:log: Password authentication of user AV7 using
Kerberos failed: Decrypt integrity check failed
-----------------------------------------------
Dec-11 19:01:48       sgi1/login[335811]:failed: ?@psi.net as AV7
-----------------------------------------------
Dec-11 23:55:43       sgi1/login[507201]:failed: ?@aol.com as AV7
-----------------------------------------------
Dec-12 02:44:20       sgi2/login[3175768]:failed: ?@aol.com as AV7
-----------------------------------------------
Dec-12 11:11:28       sgi1/login[574377]:failed: ?@aol.com as AV7
-----------------------------------------------
Dec-12 16:15:46       sgi2/login[3466982]:failed: ?@lab-06 as AV7
-----------------------------------------------
Dec-12 16:15:59       sgi2/login[3466982]:failed: ?@lab-06 as AV7
-----------------------------------------------
Dec-12 16:17:31       webadmin[20415]:password change successful for AV7 by guid=Help
Desk
```

Andy also checked for activity by AV6 on December 11th. What follows is the pertinent excerpt. The first two entries show AV6 being able to login normally. The third entry shows the illicit password change for AV6, after which we see a long series of remote login failures for AV6. The last entry shows AV6's password being reset by the Help Desk.

```
Dec-11 09:17:39       sgi2/login[3014359]:?@aol.com as AV6
-----------------------------------------------
Dec-11 09:18:01       sgi2/login[3014359]:Logout: AV6
-----------------------------------------------
Dec-11 17:46:21       webadmin[11846]:password change successful for AV6 by guid=irwin
-----------------------------------------------
Dec-11 17:51:56       sgi2/login[3215708]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:52:06       sgi2/login[3215708]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:52:22       sgi2/login[3215708]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:52:59       sgi2/login[3215082]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:53:23       sgi2/login[3215082]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:57:43       sgi1/login[351676]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:58:00       sgi1/login[351676]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:58:09       sgi1/login[351676]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:59:07       sgi1/login[376546]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:00:56       sgi1/login[289132]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:01:05       sgi1/login[289132]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:01:17       sgi1/login[289132]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:02:58       sgi1/login[306220]:failed: ?@linux2 as AV6
-----------------------------------------------
Dec-11 18:04:26       sgi1/login[363013]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:30:00       sgi1/login[273697]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:30:15       sgi1/login[273697]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:30:42       sgi1/login[422624]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:35:27       sgi2/login[3340290]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:41:56       sgi1/login[283278]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:42:06       sgi1/login[283278]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:42:14       sgi1/login[283278]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:48:24       sgi2/login[3252506]:failed: ?@aol.com as AV6
-----------------------------------------------
```

```
Dec-11 18:48:32       sgi2/login[3252506]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:49:10       sgi2/login[3252506]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:55:02       sgi1/login[425388]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:55:09       sgi1/login[425388]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:55:15       sgi1/login[425388]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 19:22:10       sgi2/login[3124786]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 20:15:16       webadmin[11456]:password change successful for AV6 by Help Desk
```

*Status Summary and Working Hypothesis*

*We found further log evidence that suggested AV6 and AV7 were also unaware of the password changes made to their respective accounts. Once each of them visited the Help Desk and had their passwords reset, the login failures stopped.*

*Since password changes were involved, we checked the WebAdmin logs; the clustering of password changes made us somewhat suspicious. When we correlated and found out that the WebAdmin access was coming from a machine outside the Help Desk (and even more to the point, from an unauthenticated machine) we were able to narrow our field of inquiry. We now suspected the Help Desk student Irwin, since it was his username that made the password changes.*

*So now we had a new identification to consider for the incident – "Insider."*

**January 2 (2001)**

Andy sent an email message to the CIS Programming I professor asking him whether Irwin, AV6, and/or AV7 were students in the same class/section.

Later the same afternoon, the professor responded, saying:

```
> I'm looking into a problem reported by one of your former students, Beatrice.
> If you don't mind, could you please let me know if any of the following students
> was in that class/section?
>
> Irwin
> AV6
> AV7

Hi Andy,

        The second two were in the 020x sections (my lecture), but I don't
recognize the first name.  If the student was enrolled in 202 at all this semester
(I just checked the class lists for both sections on myUMBC), s/he dropped before
the last drop date.

        If there's anything else I can help with, please let me know.
```

So Beatrice, AV6, and AV7 were all in CIS Programming I and all three had their passwords changed by Irwin in the space of a few minutes right around the time when they had projects due.

*Status Summary and Working Hypothesis*

*The CIS Programming I professor told Andy that while AV6 and AV7 were in the class, Irwin was not. This threw up a stumbling block for us. Where was our insider's motivation if he was not enrolled in the same class? Our puzzlement grew when the Help Desk manager told us that Irwin was a long-time employee who was well trusted. But no matter how we looked at it, it still seemed that Irwin had abused his privileges, whatever his reasons.*

*Our identification of the problem as coming from an Insider still looked valid, though the degree to which Irwin had earned trust from the Help Desk over a number of years was troubling. We obviously needed more correlations*

**January 9**

Excerpt from www/webauth/logs/error_log:

```
[Mon Dec 11 17:33:24 2000] [error] [client library-public-access-08] tgt cookie:
UMBCAuthTicketTGS=key&xKpjDLj18f6OxU4Zqd5XUQ6bMFC7soUANm6Cj8EWlgoIfXd96qwQuE%7E44rEm11M2mA8UH7VCR
gDGVOwuLloXCfXaMLrMy%2FGoIIb3mo7rY4O4vx65pOG7DiettnGFatjnLDY5BNLXnOYJKDTK%7ExfRlw%3D%3D&version&1
; domain=webauth; path=/

[Mon Dec 11 17:33:24 2000] [notice] [client library-public-access-08] service ticket issued for
webadmin, evan

[Mon Dec 11 17:33:24 2000] [notice] [client library-public-access-08] returning to:
https://webadmin.umbc.edu/admin/acct/?

[Mon Dec 11 17:33:58 2000] [notice] [client library-public-access-08] Invalidating ticket for TGS

[Mon Dec 11 17:33:58 2000] [notice] [client library-public-access-08] Invalidating ticket for
webadmin

[Mon Dec 11 17:40:51 2000] [error] [client library-public-access-08] tgt cookie:
UMBCAuthTicketTGS=key&GmS8rHeP5I1xZdDExoj5nWjIGuLhojPOm2GdwYrw84YIfXd96qwQuE%7E44rEm11M2mA8UH7VCR
gBSYVOJG36bwUinBllK1M15DOY%2F%7EHze4uC4vx65pOG7DiettnGFatjnLDY5BNLXnOYJKDTK%7ExfRlw%3D%3D&version
&1; domain=webauth; path=/

[Mon Dec 11 17:40:51 2000] [notice] [client library-public-access-08] service ticket issued for
webadmin, irwin

[Mon Dec 11 17:40:51 2000] [notice] [client library-public-access-08] returning to:
https://webadmin.umbc.edu/admin/acct/?

[Mon Dec 11 17:44:23 2000] [notice] [client library-public-access-08] authenticate_from_tgt user:
irwin

[Mon Dec 11 17:44:23 2000] [notice] [client library-public-access-08] service ticket issued for
webadmin, irwin

[Mon Dec 11 17:44:23 2000] [notice] [client library-public-access-08] returning to:
https://webadmin.umbc.edu/admin/acct/?
```

At this point, Andy retrieved activity logs for Evan on December 11th:

```
Dec-11 16:50:15       sgi2/login[3151436]:?@library-public-access-08 as evan
-----------------------------------------------
Dec-11 17:14:54       sgi2/login[2950281]:?@library-public-access-08 as evan
-----------------------------------------------
Dec-11 17:35:14       sgi2/login[3310376]:?@library-public-access-08 as evan
-----------------------------------------------
-----------------------------------------------
Dec-11 17:55:57       library-authenticated-pc27/login[GINA]: as evan
-----------------------------------------------
```

```
Dec-11 17:56:55       library-authenticated-pc27/logout[GINA]: as evan
-----------------------------------------------
-----------------------------------------------
Dec-11 21:23:52       sgi2/login[2912049]:?@ dialup-150 as evan
-----------------------------------------------
Dec-11 21:54:58       sgi2/login[3432278]:failed: ?@dialup-150 as evan
-----------------------------------------------
Dec-11 21:55:06       sgi2/login[3432278]:?@dialup-150 as evan
-----------------------------------------------
```

*Status Summary and Working Hypothesis*

*We tried a different angle. Suppose that Irwin was acting with or on behalf of someone else. Then that other party might be present when Irwin was changing passwords or using the compromised accounts.*

*Of course, it was also possible that someone else was using Irwin's account (with or without his knowledge) though that seemed less likely. In any case, experience said that those who use other people's accounts often use their own immediately before or after. It's generally worth looking at activity on a workstation both before and after an incident involving the workstation takes place.*

*With this in mind, Andy checked the WebAdmin logs again and found that Evan's account showed authentications just minutes before Irwin's account did (all just before the illicit password changes). Andy then correlated this with Evan's activity records in the December 11th logs and found that he logged into the same Library machines used for the illicit password changes and account accesses, again, just minutes before the events in question.*

*So now we seriously suspected that Irwin was not the actual (or at least not the only) perpetrator; Evan's consistent appearance just before the various misuses tipped us off. But we were still missing any connection between Irwin or Evan and CIS Programming I.*

*The identification became "Possible Outsider, Subverting Trusted/Privileged User Account."*

**January 10**

Email message from WebAdmin developer to Andy:

> The first time Irwin got a ticket (where it wasn't preceded by an authenticate_from_tgt line), we *know* he entered his username & password. The second time could have been "someone else", if he didn't either a) close his browser, or b) "delete" his cookies by hitting the convenient logout button.

At the least it appears that Irwin was extraordinarily sloppy in his use of webadmin privileges.

From the Security Officer's log:

> Around 10th or 11th of January, having prepared Irwin's execution, I noticed activity from

Evan immediately before the passwords were changed on library-authenticated-27:

```
Dec-11 17:55:57       library-authenticated-pc27/login[GINA]: as evan
-----------------------------------------------
Dec-11 17:56:55       library-authenticated-pc27/logout[GINA]: as evan
```

On the assumption that he might be involved with Irwin's activities, I checked the log for Evan's records.

*Status Summary and Working Hypothesis*

*The WebAdmin developer explained the authentication and cookie-generating procedures associated with the password-changing interface. Only the initial WebAdmin access requires the user to authenticate; subsequent accesses simply use the cookie the initial process created. Had Irwin authenticated and then for some reason left his session open, anyone walking up to the terminal could use his privileges. This seemed a reasonable enough theory, since we get reports of this sort of behavior on the part of non-privileged users quite frequently.*

*So now even if Irwin hadn't been in collusion, he was still very careless with privileged access.*

*We were considering modifying our identification to include "Collusion."*

**January 11**

From the Security Officer's notes:

After a meeting with the CCS Director, we decided that:

- Andy would double-check the activity of another student – possibly another Help Desk consultant – whose account activity appears in proximity to the activity being investigated. The username is evan.
- Andy will schedule a meeting with the Help Desk manager, the CCS Director and himself. The Help Desk manager will arrange to have Irwin attend.

*Status Summary and Working Hypothesis*

*The CCS Director met with the Security Officer about this incident. The determination of this meeting was that Andy should further investigate Evan's potential role in this incident. They also decided that they and the Help Desk manager needed to meet with Irwin to hear his story.*

**January 12**

From the Security Officer's notes:

Examination of activity logs shows that Evan authenticated to library-public-access-08 at 16:50 and seems to have been active at least until 17:35. He also authenticated to

library-authenticated-pc27 at 17:55 and logged out at 17:56. This places him in the library immediately before the questionable activity on both library systems… I have asked the professor if Evan was in CIS Programming I. I will ask the Student Judicial Affairs director if he knows the name (Evan).

Andy ran an activity check for Beatrice on December 11th. What follows is the pertinent excerpt. The first entry shows the illicit password change for Beatrice's account, after which we see a series of local and remote login failures over the next two days for beatrice. The last entry shows her password being reset by the Help Desk.

```
Dec-11 17:43:55         webadmin[11846]:password change successful for beatrice by guid=irwin
-------------------------------------------------
Dec-11 18:06:47         sgi2/login[3336619]:?@library-authenticated-pc27 as beatrice
-------------------------------------------------
Dec-11 18:11:22         sgi2/ftpd[3371275]:login from library-authenticated-pc27 as beatrice
-------------------------------------------------
Dec-11 20:13:16         sgi2/login[3260851]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:13:24         sgi2/login[3260851]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:13:32         sgi2/login[3260851]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:13:51         sgi1/login[355999]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:13:59         sgi1/login[355999]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:14:08         sgi1/login[355999]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:14:36         sgi2/login[3308630]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:14:54         sgi2/login[3308630]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:15:00         sgi2/login[3308630]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:15:58         sgi1/login[370345]:failed: ?@library-public-access-16 as beatrice
-------------------------------------------------
Dec-11 20:16:10         sgi1/login[370345]:failed: ?@library-public-access-16 as beatrice
-------------------------------------------------
Dec-11 20:16:41         sgi2/login[3275520]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-11 20:16:49         sgi2/login[3275520]:failed: ?@library-public-access-15 as beatrice
-------------------------------------------------
Dec-12 15:50:15         sgi1/login[683983]:failed: ?@level3.net as beatrice
-------------------------------------------------
Dec-13 11:06:58         sgi2/login[3418814]:failed: ?@CS machine as beatrice
-------------------------------------------------
Dec-13 11:07:47         sgi2/sshd[3277731]:log: Rsa authentication refused for beatrice
-------------------------------------------------
Dec-13 11:07:51         sgi2/sshd[3277731]:log: Password authentication of user beatrice using
Kerberos failed: Decrypt integrity check failed
-------------------------------------------------
Dec-13 11:12:46         sgi1/login[820487]:failed: ?@Help Desk as beatrice
-------------------------------------------------
Dec-13 11:19:01         webadmin[28300]:password change successful for beatrice by guid=Help Desk
```

When we once again saw that Evan had consistently logged into the relevant Library machines just prior to the illicit password modifications and subsequent account accesses, we shifted most of our attention to him. This was reinforced when the CIS Programming I professor told us that Evan was suspected of plagiarism in the course.

We came full circle when the Help Desk manager informed us that Evan was one of their student employees and had WebAdmin privileges.

*Status Summary and Working Hypothesis*

*The CIS Programming I professor confirmed that Evan was in that class and gave us even more information – there had been ongoing suspicions of plagiarism, and Evan was the alleged plagiarist.*

*We now felt entirely confident in saying that the perpetrator was definitely an insider to our organization and that the motive was coursework cheating. Our hunch was that Irwin was just a blind and that Evan was the real black hat. We still needed to verify this as much as possible before making our move, though.*

*The identification began to settle down to "Insider" again, but this time with Evan as the black perpetrator. We no longer really suspected collusion, but rather, subversion.*

**January 18**

Andy also checked for activity on the machine "library-authenticated-pc27" (the machine used to access the accounts whose passwords had just been illicitly changed) on December 11th. Notice that evan logged in and out immediately before one of the purloined accounts did. What follows is the pertinent excerpt.

```
Dec-11 17:55:57              login[GINA]:library-authenticated-27  as evan
-----------------------------------------------
Dec-11 17:56:55              logout[GINA]:library-authenticated-27  as evan
-----------------------------------------------
Dec-11 17:58:07              login[GINA]:library-authenticated-27  as AV7
-----------------------------------------------
Dec-11 17:59:45              sgi2/telnetd[2977104]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 17:59:57              sgi2/login[3222534]:?@library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:03:20              sgi2/ftpd[3059295]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:03:24              sgi2/ftpd[3059295]:login from library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:06:33              sgi2/telnetd[3392025]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:06:47              sgi2/login[3336619]:?@library-authenticated-pc27 as beatrice
-----------------------------------------------
Dec-11 18:11:21              sgi2/ftpd[3371275]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:11:22              sgi2/ftpd[3371275]:login from library-authenticated-pc27 as
beatrice
-----------------------------------------------
Dec-11 18:19:58              sgi2/telnetd[1999271]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:20:12              sgi2/login[3262427]:?@library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:30:41              reboot[GINA]:library-authenticated-27
```

*Status Summary and Working Hypothesis*

*Andy checked the December 11 activity logs for the machine "library-authenticated-pc27" (the one used to access the accounts whose passwords had just been illicitly changed). As we had come to expect, Evan logged in and out less than two minutes before one of the purloined accounts did. There were also a series of ftp connections to the compromised accounts, probably so that Evan could retrieve the project code he was after.*

**January 25**

More email communication between Andy and the CIS professor about plagiarized projects:

> May I ask who the other students were and approximately when the projects were due?

It was AV1 (proj1 - around 25 Sept) in one of the 010x sections and "someone else" (proj3 - around 25 Oct) in one of the 020x sections. I hope that helps.

The "someone else" in this email was a username that did not appear in our investigation logs.

WebAdmin log extracts generated by "sed-replace-guid" *(see Appendix B: Scripts)*:

```
Sep-25 14:23:53               webadmin[197]:
***irwin***
Attempt to change password for webadmin admin user evan by guid=irwin
-----------------------------------------------
-----------------------------------------------
Sep-25 18:20:45               webadmin[373]:
***irwin***
password change successful for cmadhu1 by guid=irwin
-----------------------------------------------
Sep-25 18:23:56               webadmin[1288]:
***irwin***
password change successful for AV1 by guid=irwin
-----------------------------------------------
Sep-25 18:29:39               webadmin[373]:
***irwin***
password change successful for AV2 by guid=irwin
-----------------------------------------------
Sep-25 18:32:45               webadmin[1288]:
***irwin***
password change successful for AV3 by guid=irwin
-----------------------------------------------
Sep-25 18:34:38               webadmin[373]:
***irwin***
password change successful for AV4 by guid=irwin
-----------------------------------------------
Sep-25 18:36:49               webadmin[197]:
***irwin***
password change successful for Arnold by guid=irwin
-----------------------------------------------


[Mon Sep 25 14:23:43 2000] [notice] [client lab-mac20] service ticket issued for webadmin, irwin
-----------------------------------------------
[Mon Sep 25 14:23:43 2000] [notice] [client lab-mac20] returning to:
https://webadmin.umbc.edu/admin/acct/?
-----------------------------------------------
[Mon Sep 25 14:24:12 2000] [notice] [client lab-mac20] Invalidating ticket for TGS
-----------------------------------------------
[Mon Sep 25 14:24:12 2000] [notice] [client lab-mac20] Invalidating ticket for webadmin
-----------------------------------------------
[Mon Sep 25 18:19:58 2000] [notice] [client lab-pc08] service ticket issued for webadmin, irwin
-----------------------------------------------
[Mon Sep 25 18:19:58 2000] [notice] [client lab-pc08] returning to:
https://webadmin.umbc.edu/admin/acct/?
```

This activity seems to support our identification of Evan as the Insider.

*Status Summary and Working Hypothesis*

*The CIS professor gave Andy some more details about the suspected plagiarized projects. He suspected that Evan took Arnold's project 1, which was due on September 25. Project 2 was due on October 25 and Evan's work looked remarkably like another student's (whose username was not in our logs as being tampered with).*

*So we reviewed our WebAdmin logs from September 25 and found that irwin authenticated, then attempted to change evan's password. We thought this a bit odd, especially since all Help Desk workers know that they cannot change the password of anyone with the same privilege level or higher. We began to suspect that Evan simply forgot whom he had authenticated as when he tried this.*

*We were now ready to move into action and contain the incident. I set up a meeting with the Help Desk manager, the Security Officer, and Irwin to review the circumstances of the case and see what he had to say. I also drafted a report that Student Judicial Affairs could use to work up a charge letter against Evan and that CCS could use internally while meeting with the suspects.*

*A subsequent conference was scheduled in coordination with Student Judicial Affairs to present charges to Evan (and hopefully get an allocution from him). We planned to notify him of the charges (by official letter) and to dismiss him from CCS immediately after our meeting with Irwin.*

*If the first meeting were to have revealed a situation substantially different than the one we had reconstructed, we could amend or drop the university charges against Evan before he or others were made aware of them. If we had learned anything from this case, it was that we couldn't be too hasty to assume that we had all the necessary facts.*

***After this point, we have left the identification stage and entered the Containment phase.***

## Phase 3: Containment

In order to effectively contain the problem, CCS had to nullify the effects of a malicious insider. This included making sure that any other privileged accounts that Evan may have subverted were also rendered inaccessible to him at least by the time he was made aware of the outcome of our investigation. Containment amounted to three separate steps:

- Daily monitoring of the suspect's and subverted user's accounts

  Since we needed to collect evidence without the insider's knowledge, we could not immediately suspend privileges. Instead, we closely monitored Evan and Irwin's activities, especially when they involved privileges. The only reason we felt at all sanguine about doing this was that the semester had ended and so, presumably, Evan's motive for cracking other users' accounts was gone.

- Suspension of privileges for both potential suspects (up to hearing)

  All Help Desk privileges were revoked for both Irwin and Evan on February 8th. This was

done for the protection of both CCS and the campus users.

- Finally, all student staff were required to change their passwords. While we have no indication that Evan subverted any accounts other than Irwin's, we felt it was too much of a risk to simply assume. This also gave us an opportunity to review good password hygiene with the student employees.

## Phase 4: Eradication

Eradication in this case consisted of firing Evan and barring him from taking a position with CCS in the future. Getting rid of the malicious insider was the only way to effectively get rid of the problem. We also had to be satisfied that Irwin's account was truly subverted and not used with his knowledge or consent.

So on February 6, we closed in. An official University Student Judicial Affairs charge letter was drafted regarding Evan. The charges were based on violations of the campus Code of Student Conduct *(see excerpts in References, Code of Student Conduct).*

On February 8, CCS Security and the Help Desk manager met with Irwin to hear his story. All Irwin's Help Desk privileges were suspended just beforehand. This was mainly for CCS's protection, since if it turned out that either Irwin *had* been involved or that Evan caught wind of the investigation, more illicit activities might be performed under either authentication.

The interview confirmed our belief that Irwin knew nothing about the subversion of his account. Irwin also independently suggested that Evan might be the insider we were looking for. Irwin stated that he had no idea how Evan had come into possession of his username/password pair, though he said that he had trained Evan in late August of that year. We formulated a working hypothesis that Evan had "shoulder-surfed" Irwin's password at that time.

Irwin's privileges remained suspended until after all investigations and student judicial proceedings were complete.

Evan's privileges were revoked immediately after the meeting with Irwin was concluded. After verifying the revocation, the Help Desk manager and Director of Student Judicial Affairs hand-delivered the charge letter and fired Evan.

Finally, on February 14, the Student Judicial Affairs Conference convened to hear Evan's case. When we arrived, the director showed us a letter that Evan had written admitting to all charges and basically throwing himself on the mercy of the Office.

We proceeded to hear a full allocution and asked a number of questions regarding the case. Evan's story closely conformed to our reconstruction of events. Perhaps the most disturbing thing, other than Evan's apparent lack of real remorse or even awareness of fault, was the way he obtained Irwin's account information. Even though Irwin was a senior Help Desk student, both trusted and trained to caution, he wrote down his username/password pair on a pad of paper at his workstation. Since Evan was training with Irwin, he was able to get access to the paper and subvert Irwin's account without leaving any real telltales.

Student Judicial Affairs imposed additional penalties and sanctions on Evan, including suspension, but these fell outside the realm of CCS Security's responsibility.

And we clearly had some internal housekeeping to do.

## Phase 5: Recovery

There was very little that CCS actually needed to do in terms of recovering from these particular incidents. Basically, there were only two items:

- Restoring Beatrice's damaged files – As noted above, the requested files were restored, but they were not up to date with her most recent work *(see Backup Process).*
- Reviewing password hygiene with all student employees, especially those with access to privileged commands or information *(see Lessons Learned)*

## Phase 6: Follow Up / Lessons Learned

- The most important lesson for incident handling that was reinforced by this case is, "Don't shoot from the hip." As we investigated more, always looking for more corroboration for a working hypothesis, we were faced with an ever-changing theory of the incident. Had we acted on our first (or even second) evidence, we would have both gone after the wrong person and tipped our hand to the real perpetrator.

- We were also painfully reminded that any new tool *will* be abused just as soon as someone can figure out how. Cynical, but all too true. Especially for sensitive applications, the logging functions should be well understood and tested before production deployment.

- The CCS WebAdmin developer is planning to improve logging for the password changing facilities, including correlating the different types of logs the application keeps. At the time of the incident, WebAdmin maintained two sets of logs. One was for initial authorization requests that showed the request vector (machine name, ISP, etc). The other log showed cookie use, but did not record the activity vector.

- The Security Officer has already begun writing new and improved scripts to produce daily reports for WebAdmin password changing activity. These reports show time-stamped password changes grouped by the changer's username. This allows us to easily scan for the kind of clustered activity that alerted us in this case.

- CCS is also considering imposing location/machine-based restrictions on WebAdmin password changing facilities. Since WebAdmin is a true web-based portal, it can be accessed from anywhere on the Internet. We are now considering restricting privileged access (i.e. access to accounts other than the authenticating user's) to machines in the

Help Desk, especially for student staff.

- This case also served as another reminder that we should decrease the number, or at least the utility, of unauthenticated terminals. It does make sense to have a small number of unauthenticated machines available in public areas for visitor use, but if a machine allows open access, it should be limited to *only* running a web browser. This precaution would not have necessarily helped in this instance (since the insider already had someone else's username and password), but the question "who was using the terminal where the misuse occurred?" came up more than once during the investigation.

- CCS was already planning this, but this incident has stepped up our timeline to improve user education on several issues:
    - General password hygiene - this includes tips for choosing good passwords, changing and storing passwords safely. It turns out that the insider was able to subvert the other Help Desk student's account because Irwin had written down his username/password pair! All users need to be educated about the dangers of carelessness.
    - The importance of reporting oddities - as always, security cannot operate in a vacuum. The reason we became aware of the insider at all was that Beatrice reported more than just a password problem; she told us that there was a pattern of problems at project submission times. If more users knew how to detect anomalies and to whom they should be reported, we'd probably catch more crackers.
    - The importance of faculty reporting suspected computer security-related incidents to the CCS Help Desk - this would provide us with another correlation data point as well as early warning of incidents like the ones detailed in this report.

- CCS is also planning to hold regular, specific student employee presentations to review standard password hygiene and reinforce the gravity of the trust inherent in their positions (especially those with access to privileged commands or information). Help Desk students are also going to be made more aware of security concerns and how to detect and report them. The first two of these presentations are going to be held this week (February 19-23, 2001).

- This case also served to help us develop a better checklist for this kind of investigation in the future. We are refining our list of questions *(see Assessment Tools)*, log analysis scripts *(see Appendix B: Scripts)*, and overall process.

## THE ASSESSMENT TOOLS AND CONTAINMENT PROCESS

One of the most difficult things about this case was the fact that it was done by an insider, though apparently not while he was on the clock. This meant that CCS needed to distinguish legitimate password changes from those done illicitly. Some logged behavior that seemed at first to be suspicious turned out simply to be business as usual in the Help Desk.

There were four major tools in our jump kit:

- Andy's log parsing scripts - These scripts allowed us to pull formatted strings out of the logs. We were able to trace usernames and machine names and to correlate the activity with the output of these scripts. *(See Appendix B: Scripts)*
- Andy's sed replacement script - This script allowed us to replace the cumbersome guids listed in the logs with more readable usernames. *(See Appendix B: Scripts)*

- Highlighters - while this is admittedly a low-tech solution, it was nevertheless the key to our assessment of the situation. The log parsing scripts listed above formatted the system log data which we then printed out. I sat with a bevy of different-colored highlighters and began to trace suspicious activity. It was quite interesting to note how many of the oddities matched up with the incidents we were intending to investigate.
- These are the (evolving) CCS-standard questions to ask a user who suspects account/password compromise (mostly involving password hygiene):

    a. Have you shared your password?
    b. If not, have you told anyone what your password is? This includes parents, roommates, brother/sister, and boyfriend/girlfriend.
        i. *Note: The repetition of the same question is purposely done because many users don't seem to believe that telling their close relatives "really counts" as sharing their password.*
    c. Was your password (prior to the Help Desk's changing of it) a real word or words (in any language)?
    d. Was anyone ever in a position to see you type in your password?
    e. Have you ever written down your password? If so, what did you do with the paper / where is it kept?
    f. Is there anyone who might want to cause you problems or "play tricks" on you?
        i. *Note: This question is raised early in the investigation because of the high incidence of stalking and related cases that are handled by our office. In a very informal poll taken in the University workshop at the SANS San Francisco 1999 conference, most University sysadmins agreed that about 80% of their computer security incidents are related to stalking-type cases.*
    g. When, to your knowledge, has your password been changed?
        i. *Note: This allows us extra correlation and independent confirmation vectors.*
    h. From where do you normally do computer work on UMBC systems (from home, from work, on campus)?
    i. If from off-campus, how do you normally connect to UMBC (dial-in, through another ISP, other)? What program do you use (telnet, ssh, other)?
        i. *Note: This question often takes a little explaining to non-technical users.*

j. When do you normally log into UMBC systems?

## THE BACKUP PROCESS

No systems actually required backing up as a result of this incident. We did, however utilize backups to restore Beatrice's damaged work and to keep a copy of Evan's account.

- AFS nightly account backups to <top-level>/backup

  The backup directory (found under a user's top-level directory) contains a "snapshot" of the associated home volume from the previous day, providing an easy means of recovering any accidentally deleted files. Had Beatrice realized that her files had been corrupted on the same day, she could have simply retrieved the original versions (as they appeared in the snapshot, of course, not as she had last modified them).

  The backup directory doesn't take up any of the user's quota space since it is a separate image of the user's volume. The mechanism for this snapshot-backup system is an "auto-magical" part of the AFS and is necessary to the way that AFS's backups work. Mounting the volume for the convenience of users and sysadmins is a specific implementation detail at our campus.

- Tape-based restore system of Beatrice's project files

  I asked the central Unix sysadmin what he needed to do in order to restore Beatrice's damaged files. He said that he followed the steps outlined in the standard restore procedures document *(see References, Restore Procedures)*. The following is a reconstruction of those steps:

```
[admin@restore]$ fs lq ~beatrice
Volume Name           Quota      Used     %Used   Partition
user.beatrice         15000      6880     46%     82%
```

```
[admin@restore]$ ps -ef | grep backup
root     504970    1  0   Dec 15 ?      0:45 /usr/local/bin/perl /usr/afs/backup/bin/scheduler
```

```
[admin@restore]$ /usr/afsws/etc/backup
backup> volrestore -server restore -partition /vicepm -volume user.beatrice -extension .2001210 -
        portoffset 2 -date 12/10/2000
```

< *Email sent by system requesting tape holding this particular backup* >
< *Once requested tape is available, procedure continues…* >

< Admin types *Control-Z* to momentarily return to the command line >

```
[admin@restore]$ /usr/afs/backup/bin/rescan

[admin@restore]$ fg

< Time passes … >

backup> quit

[admin@restore]$ cd ~beatrice/..

[admin@restore]$ fs mkmount -dir home.20001210 -vol user.beatrice.2001210

[admin@restore]$ find home.20001210 -type d -exec fs setacl \{\} system:anyuser none \;

[admin@restore]$ find home.20001210 -type d -exec fs setacl \{\} beatrice rl \;
```

< Admin emails Beatrice to let her know that the volume is now available and to give her directions on copying the files she needs from the old volume to her current one >

The only problem encountered was not a technical one, but still serious from Beatrice's point of view. As mentioned earlier, the backups on tape did not have the most recent versions of her project files. She completed her work after the previous night's backups ran, but lost the files to sabotage before the next night's backups took place. Thus, she had to reconstruct much of her work. The Security Officer confirmed Beatrice's account of these activities to her professor to ensure that she would not be held accountable for missing project deadlines. Students in such situations are encouraged to ask their instructor to contact CCS, though our policy is that we do not give out any information beyond a confirmation that the victim's work was interfered with.

- Backing up and storing the insider's account

The Security Officer backed up and stored the insider's account before the insider was notified of the charges brought against him, just in case we might need to access it later for evidence. This is part of our standard incident handling procedures. The following command created a "tarball" of Evan's account from the top-level. This is important, because the top-level includes the user's Mail, public, and backup directories as well as his main home directory.

We do not currently perform any kind of checksum or other cryptographic hash on the stored files for long-term integrity-checking purposes. Such files are stored in AFS space owned by the Security Officer.

```
[admin@backup]$ tar cvf /security/storage/naughtyusers/evan.0012215-1.tar ~evan/..
```

```
[admin@backup]$  gzip -9 /security/storage/naughtyusers/evan.0012215-1.tar
```

## THE EVIDENCE AND CHAIN OF CUSTODY

We currently do not have any method of proving that the logs are pristine and stored in the same state as when they were gathered. This level of reliability has not been considered worth the cost it would incur, since we do not have any great expectations of having to go to court with our logs, as a general rule. Most matters investigated by CCS are (thankfully) handled within the University's disciplinary system rather than civil or criminal court.

Log excerpts, analyses, and related electronic documents are kept in a secured AFS director owned by the Security Officer. All documents that were printed out were either kept with the CCS Security Officers, Student Judicial Affairs, or shredded. All of the log excerpts shown below are entirely reproducible from the stored logs.

"Log Analysis and Comments" shows the summary report that was given to Student Judicial Affairs. It walks through the incidents as they occurred and contains explanatory comments.

### Log Analysis and Comments

September 25

| Time | Vector | Username | Action |
|---|---|---|---|
| 14:23:43 | lab-mac20 | lrwin | WebAdmin service ticket issued |
| 14:23 | WebAdmin | lrwin | Attempt to change password: Evan |
| 18:19 | lab-pc08 | lrwin | WebAdmin service ticket issued |
| 18:20 | WebAdmin | lrwin | Password changed: AV1 |
| 18:23 | WebAdmin | lrwin | Password changed: AV2 |
| 18:29 | WebAdmin | lrwin | Password changed: AV3 |
| 18:32 | WebAdmin | lrwin | Password changed: AV4 |
| 18:34 | WebAdmin | lrwin | Password change: AV5 |
| 18:36 | WebAdmin | lrwin | Password change: Arnold |
| 19:02 | WebAdmin | Help Desk | Password change requested in person: AV4 |
| 21:03 | WebAdmin | Help Desk | Password change requested in person: AV5 |
| 21:13 | WebAdmin | Help Desk | Password change requested in person: AV3 |
| 22:42 | WebAdmin | Help Desk | Password change requested in person: AV2 |

Notes: This is the first incident under consideration. Six distinct user passwords were changed in the space of 16 minutes, *five* of which were changed again in less than 24 hours.

Usernames AV1-AV5 and Arnold are verified as belonging to students who were enrolled in CIS Programming I on Sep-25-2000. Note that CIS Programming I project1 was due on this date, by midnight.
Except where specifically indicated, we must presume that the password changes made by Help Desk were requested in person there.

September 26

| Time | Vector | Username | Action |
|---|---|---|---|
| 13:34 | WebAdmin | Help Desk | Password changed: AV1 |

Note: We must presume that this password change was requested in person at the Help Desk.

October 23

| | | | |
|---|---|---|---|
| 18:22 | WebAdmin | Irwin | Password changed: AV7 |
| 18:30 | WebAdmin | Irwin | Password changed: AV8 |
| 19:42 | WebAdmin | Help Desk | Password change requested in person: AV8 |
| 20:55 | WebAdmin | Help Desk | Password change requested in person: AV7 |

Notes: This is shortly before CIS Programming I project3 due date.

December 11

| | | | |
|---|---|---|---|
| 09:17 | AOL | Arnold | Login to sgi2 |
| 09:18 | AOL | Arnold | Logout of sgi2 |
| 16:50 | library-public-access-08 | Evan | Login to sgi2 |
| 17:14 | library-public-access-08 | Evan | Login to sgi1 |
| 17:31 | Laurel ISP | AV7 | Login to sgi1 (session id 409569) |

Notes: This is the beginning of the second incident under consideration.
Here we see “Arnold” and “AV7” able to access their accounts normally.

| | | | |
|---|---|---|---|
| 17:33 | library-public-access-08 | Evan | WebAdmin service ticket issued |
| 17:35 | library-public-access-08 | Evan | Login to sgi2 |
| 17:40 | library-public-access-08 | Irwin | WebAdmin service ticket issued |
| 17:42 | WebAdmin | Irwin | Password changed: AV7 |
| 17:43 | WebAdmin | Irwin | Password changed: Beatrice |
| 17:46 | WebAdmin | Irwin | Password changed: AV6 |
| 17:44 | library-public-access-08 | Irwin | WebAdmin service ticket issued |

Notes: Library-public-access-08 is a public access machine. This means that users do not have to authenticate in order to use the machine (for example, to launch a web browser). We believe that Evan knew this and used this machine to help further disguise/hide illicit activity.

All three of the accounts whose passwords were changed were verified as registered for CIS Programming I. The fourth project for that class was due the next day (December 12).

Beatrice attests that she did not request or authorize a password change on this date.

| Time | | Vector | Username | Action |
|---|---|---|---|---|
| 17:51 | 18:30:00 | | | |
| 17:52:06 | 18:30:15 | | | |
| 17:52:22 | 18:30:42 | | | |
| 17:52:59 | 18:35 | | | |
| 17:53 | 18:41 | | | |
| 17:57 | 18:42:06 | | | |
| 17:58:00 | 18:42:14 | AOL | AV6 | Failed login attempts to sgi1 and sgi2 |
| 17:58:09 | 18:48:24 | | | |
| 17:59 | 18:48:32 | | | |
| 18:00 | 18:49 | | | |
| 18:01:05 | 18:55:02 | | | |
| 18:01:17 | 18:55:09 | | | |
| 18:02 | 18:55:15 | | | |
| 18:04 | 19:22 | | | |

Notes: All attempted logins for “AV6” both locally and from AOL fail until password reset at 20:15. This shows that the legitimate user did not know about the password change.

| | | | |
|---|---|---|---|
| 17:55 | library-authenticated-27 | Evan | Login to library-authenticated-27 |
| 17:56 | library-authenticated-27 | Evan | Logout of library-authenticated-27 |
| 17:58 | library-authenticated-27 | AV7 | Login to library-authenticated-27 |
| 17:59 | library-authenticated-27 | AV7 | Login to sgi2 |
| 18:03 | library-authenticated-27 | AV7 | ftp to sgi2 |
| 18:04 | Laurel ISP | AV7 | Logout of sgi1 (session id 409569) |

Notes: "AV7" last authenticated from a Laurel ISP, most likely from his home in Laurel, at 17:31. We believe that it is not possible for him to have done so then also legitimately logged in from a Library computer at 17:58 (or have requested a legitimate password change at 17:42). Also note that "AV7" logged out of the Laurel ISP-based session at 18:04.

Library-authenticated-27 supports authenticated user logins. We believe that Evan began accessing the accounts he just tampered with (probably for their CIS Programming I project files), especially given his login just prior to that of "AV7".

| Time | Vector | Username | Action |
|---|---|---|---|
| 18:06 | library-authenticated-27 | Beatrice | Login to sgi2 |
| 18:11 | library-authenticated-27 | Beatrice | ftp to sgi2 |
| 18:14 | | | Project files belonging to Beatrice corrupted |

Notes: Library-authenticated-27 supports authenticated user logins. We believe that Evan was accessing the accounts he just tampered with for their CIS Programming I project files. The `ftp` protocol is used to transfer files from one machine to another. Timestamps indicate that Beatrice's CIS Programming I project files were corrupted just after this `ftp` session.

| | | | |
|---|---|---|---|
| 18:20 | library-authenticated-27 | AV7 | Login to sgi2 |
| 18:30 | library-authenticated-27 | | Machine reboot, all users logged off |

Note: We believe that Evan rebooted library-authenticated-27 once he was done with accessing other users' files to try to cover his tracks.

| | | | |
|---|---|---|---|
| 18:53<br>18:54:00<br>18:54:25<br>18:54:32<br>18:54:39<br>19:01<br>23:55 | Laurel ISP, AOL | AV7 | Failed login attempts to sgi1, sgi2 |

Notes: All attempted logins for AV7 from the Laurel ISP fail until password reset on December 12. This shows that the legitimate user did not know about the password change.

| Time | Vector | Username | Action |
|---|---|---|---|
| 20:13:16<br>20:13:24<br>20:13:32<br>20:13:51<br>20:13:59<br>20:14:08<br>20:14:36<br>20:14:54<br>20:15:00<br>20:15:58<br>20:16:10<br>20:16:41<br>20:16:49 | lib156pub-15<br>and<br>lib156pub-16 | Beatrice | Failed login attempts to sgi1 and sgi2 |

Notes: We believe that this series of failed login attempts is genuine – that Beatrice was trying (and failing) to legitimately access the account. Again, this shows that the legitimate user did not know about the password change.

| | | | |
|---|---|---|---|
| 20:15 | WebAdmin | Help Desk | Password change requested in person: AV6 |

Note: We must presume that the password change was requested in person at the Help Desk.

December 12

| | | | |
|---|---|---|---|
| 02:44<br>11:11<br>16:15:46<br>16:15:59 | AOL<br>On-campus | AV7 | Failed login attempts to sgi1 and sgi2 |
| 15:50 | DC ISP | Beatrice | Failed login attempts to sgi1 |

Notes: Again, we believe that this failed login attempt is genuine – that the actual owner of the "Beatrice" account is trying (and failing) to legitimately access the account.

| | | | |
|---|---|---|---|
| 16:17 | WebAdmin | Help Desk | Password changed: AV7 |

Note: We must presume that the password change was requested in person at the Help Desk.

December 13

| Time | Vector | Username | Action |
|---|---|---|---|
| 11:06<br>11:07:47<br>11:07:51<br>11:12 | On-campus machines | Beatrice | Failed login attempts to sgi2 |

Notes: Again, we believe that this series of failed login attempts is genuine – that the actual owner of the "Beatrice" account is trying (and failing) to legitimately access the account.

| | | | |
|---|---|---|---|
| 11:12 | Help Desk machine | Beatrice | Failed login attempt to sgi1 |
| 11:19 | WebAdmin | Help Desk | Password change requested in person: Beatrice |

Notes: The incidents were first brought to CCS's attention on this date. Beatrice went to the Help Desk and requested that her password be changed and also reported the following: her password always seemed to "break" around the same time that CIS Programming I projects were due; each of her most recent project files had been deleted and replaced with a few lines of garbage.

"Sequential Relevant Log Entry Extracts" shows the actual log entries that pertain to these incidents. These entries are the foundation upon which all the rest of the case was built. Their spare wording and cryptic content show why so much effort went into correlation and presentation. Logs may be a Security Officer's best friends, but they aren't always terribly friendly.

## Sequential Relevant Log Entry Extracts

```
[Mon Sep 25 14:23:43 2000] [notice] [client lab-mac20] service ticket issued for webadmin, irwin
-----------------------------------------------
[Mon Sep 25 14:23:43 2000] [notice] [client lab-mac20] returning to: https://webadmin.umbc.edu/admin/acct/?
-----------------------------------------------
Sep-25 14:23:53       webadmin[197]:Attempt to change password for webadmin admin user evan by guid=irwin
-----------------------------------------------
[Mon Sep 25 14:24:12 2000] [notice] [client lab-mac20] Invalidating ticket for TGS
-----------------------------------------------
[Mon Sep 25 14:24:12 2000] [notice] [client lab-mac20] Invalidating ticket for webadmin
-----------------------------------------------
[Mon Sep 25 18:19:58 2000] [notice] [client lab-pc08] service ticket issued for webadmin, irwin
-----------------------------------------------
[Mon Sep 25 18:19:58 2000] [notice] [client lab-pc08] returning to: https://webadmin.umbc.edu/admin/acct/?
-----------------------------------------------
Sep-25 18:20:45       webadmin[373]:password change successful for AV1 by guid=irwin
-----------------------------------------------
Sep-25 18:23:56       webadmin[1288]:password change successful for Av2 by guid=irwin
-----------------------------------------------
Sep-25 18:29:39       webadmin[373]:password change successful for AV3 by guid=irwin
-----------------------------------------------
Sep-25 18:32:45       webadmin[1288]:password change successful for AV4 by guid=irwin
-----------------------------------------------
Sep-25 18:34:38       webadmin[373]:password change successful for AV5 by guid=irwin
-----------------------------------------------
Sep-25 18:36:49       webadmin[197]:password change successful for Arnold by guid=irwin
-----------------------------------------------

-----------------------------------------------
-----------------------------------------------

-----------------------------------------------
Dec-11 09:17:39       sgi2/login[3014359]:?@aol.com as AV6
-----------------------------------------------
Dec-11 09:18:01       sgi2/login[3014359]:Logout: AV6
-----------------------------------------------
Dec-11 16:50:15       sgi2/login[3151436]:?@library-public-access-08 as evan
-----------------------------------------------
Dec-11 17:14:54       sgi2/login[2950281]:?@library-public-access-08 as evan
-----------------------------------------------
Dec-11 17:31:05       sgi1/login[409569]:?@psi.net as AV6
-----------------------------------------------
[Mon Dec 11 17:33:24 2000] [error] [client library-public-access-08] tgt cookie:
UMBCAuthTicketTGS=key&xKpjDLj18f6OxU4Zqd5XUQ6bMFC7soUANm6Cj8EWlgoIfXd96qwQuE%7E44rEm11M2mA8UH7VCRgDGV0wuLloXCfXa
MLrMy%2FGoIIb3mo7rY4O4vx65p0G7DiettnGFatjnLDY5BNLXn0YJKDTK%7ExfRlw%3D%3D&version&1; domain=webauth; path=/
-----------------------------------------------
[Mon Dec 11 17:33:24 2000] [notice] [client library-public-access-08] service ticket issued for webadmin, evan
-----------------------------------------------
[Mon Dec 11 17:33:24 2000] [notice] [client library-public-access-08] returning to:
https://webadmin.umbc.edu/admin/acct/?
-----------------------------------------------
[Mon Dec 11 17:33:58 2000] [notice] [client library-public-access-08] Invalidating ticket for TGS
-----------------------------------------------
[Mon Dec 11 17:33:58 2000] [notice] [client library-public-access-08] Invalidating ticket for webadmin
-----------------------------------------------
Dec-11 17:35:14       sgi2/login[3310376]:?@library-public-access-08 as evan
-----------------------------------------------
[Mon Dec 11 17:40:51 2000] [error] [client library-public-access-08] tgt cookie:
UMBCAuthTicketTGS=key&GmS8rHeP5I1xZdDExoj5nWjIGuLhojPOm2GdwYrw84YIfXd96qwQuE%7E44rEm11M2mA8UH7VCRgBSYVOJG36bwUin
BllK1M15DOY%2F%7EHze4uC4vx65p0G7DiettnGFatjnLDY5BNLXn0YJKDTK%7ExfRlw%3D%3D&version&1; domain=webauth; path=/
-----------------------------------------------
[Mon Dec 11 17:40:51 2000] [notice] [client library-public-access-08] service ticket issued for webadmin, irwin
-----------------------------------------------
[Mon Dec 11 17:40:51 2000] [notice] [client library-public-access-08] returning to:
https://webadmin.umbc.edu/admin/acct/?
-----------------------------------------------
Dec 11 17:43:55       webadmin[11846]: password change successful for beatrice by guid=irwin
-----------------------------------------------
[Mon Dec 11 17:44:23 2000] [notice] [client library-public-access-08] authenticate_from_tgt user: irwin
-----------------------------------------------
[Mon Dec 11 17:44:23 2000] [notice] [client library-public-access-08] service ticket issued for webadmin, irwin
-----------------------------------------------
```

```
[Mon Dec 11 17:44:23 2000] [notice] [client library-public-access-08] returning to:
https://webadmin.umbc.edu/admin/acct/?Dec 11 17:42:49       webadmin[11942]: password change successful for AV7
by guid=irwin
-----------------------------------------------
Dec 11 17:46:21       webadmin[11846]: password change successful for AV6 by guid=irwin
-----------------------------------------------
Dec-11 17:51:56       sgi2/login[3215708]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:52:06       sgi2/login[3215708]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:52:22       sgi2/login[3215708]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:52:59       sgi2/login[3215082]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:53:23       sgi2/login[3215082]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:55:57       library-authenticated-pc27/login[GINA]: as evan
-----------------------------------------------
Dec-11 17:56:55       library-authenticated-pc27/logout[GINA]: as evan
-----------------------------------------------
Dec-11 17:57:43       sgi1/login[351676]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:58:00       sgi1/login[351676]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:58:07       login[GINA]:library-authenticated-27  as AV7
-----------------------------------------------
Dec-11 17:58:09       sgi1/login[351676]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:59:07       sgi1/login[376546]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 17:59:45       sgi2 /telnetd[2977104]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 17:59:57       sgi2 /login[3222534]:?@library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:00:56       sgi1/login[289132]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:01:05       sgi1/login[289132]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:01:17       sgi1/login[289132]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:02:58       sgi1/login[306220]:failed: ?@linux2 as AV6
-----------------------------------------------
Dec-11 18:03:20       sgi2/ftpd[3059295]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:03:24       sgi2/ftpd[3059295]:login from library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:04:26       sgi1/login[363013]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:04:44       sgi1/login[409569]:Logout: AV7
-----------------------------------------------
Dec-11 18:06:33       sgi2/telnetd[3392025]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:06:47       sgi2/login[3336619]:?@library-authenticated-pc27 as beatrice
-----------------------------------------------
Dec-11 18:11:21       sgi2/ftpd[3371275]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:11:22       sgi2/ftpd[3371275]:login from library-authenticated-pc27 as beatrice
-----------------------------------------------
Dec-11 18:19:58       sgi2/telnetd[1999271]:connect from library-authenticated-pc27
-----------------------------------------------
Dec-11 18:20:12       sgi2/login[3262427]:?@library-authenticated-pc27 as AV7
-----------------------------------------------
Dec-11 18:30:00       sgi1/login[273697]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:30:15       sgi1/login[273697]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:30:41       reboot[GINA]:library-authenticated-27
-----------------------------------------------
Dec-11 18:30:42       sgi1/login[422624]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:35:27       sgi2/login[3340290]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:41:56       sgi1/login[283278]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:42:06       sgi1/login[283278]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:42:14       sgi1/login[283278]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:48:24       sgi2/login[3252506]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:48:32       sgi2/login[3252506]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:49:10       sgi2/login[3252506]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:53:49       sgi1/login[425702]:failed: ?@psi.net as AV7
```

```
-----------------------------------------------
Dec-11 18:54:00       sgi1/login[425702]:failed: ?@psi.net as AV7
-----------------------------------------------
Dec-11 18:54:25       sgi2/sshd[3117538]:log: Password authentication of user AV7 using Kerberos failed:
Decrypt integrity check failed
-----------------------------------------------
Dec-11 18:54:32       sgi2/sshd[3117538]:log: Password authentication of user AV7 using Kerberos failed:
Decrypt integrity check failed
-----------------------------------------------
Dec-11 18:54:39       sgi2/sshd[3117538]:log: Password authentication of user AV7 using Kerberos failed:
Decrypt integrity check failed
-----------------------------------------------
Dec-11 18:55:02       sgi1/login[425388]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:55:09       sgi1/login[425388]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 18:55:15       sgi1/login[425388]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 19:01:48       sgi1/login[335811]:failed: ?@psi.net as AV7
-----------------------------------------------
Dec-11 19:22:10       sgi2/login[3124786]:failed: ?@aol.com as AV6
-----------------------------------------------
Dec-11 20:13:16       sgi2/login[3260851]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:13:24       sgi2/login[3260851]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:13:32       sgi2/login[3260851]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:13:51       sgi1/login[355999]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:13:59       sgi1/login[355999]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:14:08       sgi1/login[355999]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:14:36       sgi2/login[3308630]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:14:54       sgi2/login[3308630]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:15:00       sgi2/login[3308630]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:15:16       webadmin[11456]:password change successful for AV6 by Help Desk
-----------------------------------------------
Dec-11 20:15:58       sgi1/login[370345]:failed: ?@library-public-access-16 as beatrice
-----------------------------------------------
Dec-11 20:16:10       sgi1/login[370345]:failed: ?@library-public-access-16 as beatrice
-----------------------------------------------
Dec-11 20:16:41       sgi2/login[3275520]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 20:16:49       sgi2/login[3275520]:failed: ?@library-public-access-15 as beatrice
-----------------------------------------------
Dec-11 21:23:52       sgi2/login[2912049]:?@ dialup-150 as evan
-----------------------------------------------
Dec-11 21:54:58       sgi2/login[3432278]:failed: ?@dialup-150 as evan
-----------------------------------------------
Dec-11 21:55:06       sgi2/login[3432278]:?@dialup-150 as evan
-----------------------------------------------
Dec-11 23:55:43       sgi1/login[507201]:failed: ?@aol.com as AV7
-----------------------------------------------

-----------------------------------------------
-----------------------------------------------

-----------------------------------------------
Dec-12 02:44:20       sgi2/login[3175768]:failed: ?@aol.com as AV7
-----------------------------------------------
Dec-12 11:11:28       sgi1/login[574377]:failed: ?@aol.com as AV7
-----------------------------------------------
Dec-12 15:50:15       sgi1/login[683983]:failed: ?@level3.net as beatrice
-----------------------------------------------
Dec-12 16:15:46       sgi2/login[3466982]:failed: ?@lab-06 as AV7
-----------------------------------------------
Dec-12 16:15:59       sgi2/login[3466982]:failed: ?@lab-06 as AV7
-----------------------------------------------
Dec-12 16:17:31       webadmin[20415]:password change successful for AV7 by guid=Help Desk
-----------------------------------------------

-----------------------------------------------
-----------------------------------------------

-----------------------------------------------
Dec-13 11:06:58       sgi2/login[3418814]:failed: ?@CS machine as beatrice
-----------------------------------------------
Dec-13 11:07:47       sgi2/sshd[3277731]:log: Rsa authentication refused for beatrice
-----------------------------------------------
```

```
Dec-13 11:07:51       sgi2/sshd[3277731]:log: Password authentication of user beatrice using Kerberos failed:
Decrypt integrity check failed
-----------------------------------------------
Dec-13 11:12:46       sgi1/login[820487]:failed: ?@Help Desk as beatrice
-----------------------------------------------
Dec-13 11:19:01       webadmin[28300]:password change successful for beatrice by guid=Help Desk
```

# REFERENCES

*Please include at least **three** references to outside sources, not including the course material*

Policy for Responsible Computing at UMBC
(http://Help Desk.umbc.edu/umbc-aup.html)

### *POLICY FOR RESPONSIBLE COMPUTING AT UMBC*

PREAMBLE

This Policy sets forth the principles that govern appropriate use of computing and digital information resources. Such resources are the property of the State of Maryland, and users are bound by all pertinent University, State, and Federal policies and statutes. Access to UMBC computing resources is a privilege granted by the University. Computing policies, like other university policies, where ever possible are governed by the principle of academic freedom.

POLICY STATEMENT

UMBC provides access to computing and information resources for students, staff, faculty, and certain other users in support of UMBC's mission of teaching, research, public service, and in support of the official duties of the University. When activating an account, a user implicitly affirms that: they will abide by the broadest interpretation of the following policies; failure to follow policies may result in loss of computing privileges; UMBC may monitor computer use to protect the system; and the university may terminate the account of anyone who has been determined to use his or her access for unlawful purposes or in contravention of this policy. Computer users shall:

Act responsibly so as to ensure the integrity and ethical use of computing and information resources. Respect the rights of others, and not threaten, harass, intimidate, or commit theft or fraud. Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information. Use University computing resources and user accounts only for appropriate University activities. Acknowledge that system administrators may examine files, mail, and printer listings for the purpose of diagnosing and correcting problems with the system. Acknowledge the right of the University to restrict or rescind computing privileges for cause.

EXAMPLES OF ACTIVITIES SPECIFICALLY PROHIBITED

The following are some of the things that are prohibited activities; this list in not inclusive. No person may:

- Intentionally corrupt, misuse, or steal software or any other computing resource.
- Access information resources, data, equipment, or facilities in violation of any restriction on use.
- Use University computing resources for personal or private financial gain without written authorization. Excepted from this provision is remuneration to faculty and staff for customary university related activities from: approved consulting; copy rights; patents; royalties; honoraria; reviews; etc.
- Use another person's computer account.
- Establish an independent computer system, except those specifically authorized for departmental use.
- Knowingly, without written authorization, execute a program which may hamper normal computing activities at UMBC
  or elsewhere.

ACTION TO PRESERVE PUBLIC SAFETY OR INTEGRITY OF COMPUTING RESOURCES

If a *Campus Computing Services (CCS)* official reasonably believes that a user is engaged in activities which may pose an imminent threat to: 1) the health or safety of others; 2) the integrity of data; or 3) computing resources which may adversely affect system operations, the official may temporarily suspend user privileges for no more than two working days (excluding weekends and university holidays) before consulting an Administration official.

In all other cases, the *CCS* official shall consult the Associate Vice President for Academic Affairs and follow existing University procedures, where applicable, prior to:

- Investigating alleged improper or illegal use of data, programs, or UCS equipment or resources;
- Accessing data and files pertinent to the investigation; or
- Limiting user privileges until the matter is resolved.

If appropriate, or required, findings from investigations may be reported to other University officials for review and action, or to State or Federal authorities.

INFORMING USER OF ACTIONS TAKEN

Unless such notification may impede an investigation, within one week University officials shall disclose in writing to an affected user that:

- The user's account has been suspended, or that
- The user is under investigation, and that
- The user may submit evidence to those conducting the investigation, and the procedures that are applicable to the investigation.

ACKNOWLEDGEMENT OF POLICY

By activating a computing account, a user implicitly agrees to abide by the above policy in its entirety.

Approved for distribution:

_____
Freeman A. Hrabowski, President
26 September 1996

Code of Student Conduct, UMBC *(excerpts)*

(http://www.umbc.edu/NewsEvents/Student/stconduct.html)

Relevant sections:

**Article V. Proscribed Conduct**

**B.**

5. Thefts or Property Damage. This rule prohibits, but is not limited to, the following, whether by intentional or negligent acts and whether attempted or completed acts:

   a. destruction, damage, abuse, theft, or fraudulent use of University or private property, including credit cards; or

   b. destruction, damage, abuse, theft, or fraudulent use of University services such as computer systems, telephones, and mail services

7. Acts of Dishonesty or Falsifying University Records. This rule prohibits, but is not limited to, the following:

   b. falsifying, forging, altering, causing the alteration of, or furnishing false information regarding identification cards, absence excuses, parking stickers, transcripts, grade reports, test papers, answer sheets, examinations, admissions or financial aid applications, registration materials, and computer records;

9. Disruption of Any University Activity. This rule prohibits, but is not limited to, the following:

   a. acts inhibiting, interfering with, obstructing, or damaging either (i) an academic activity (e.g., teaching, research, or University Administration) or organized student activity; or (ii) a campus resource relating to academic materials (e.g., library books, audiovisual materials and tapes);

13. Violation of Published University Rules, Regulations or Policies. Students are responsible for knowing and observing all UMBC rules, regulations and policies regarding the use of University equipment, grounds and facilities, the time, place, and manner of expression or expression-related conduct, and, campus demonstrations, among other University policies.

14. Improper Uses of Computers and Technology. This rule prohibits the breach of computer security, harmful access, unauthorized copying of programs and/or data, unauthorized transfer of programs and/or data access denial, or the attempt to commit such acts. See the UMBC Policy for Responsible Computing

Restore Procedures *(excerpts)*
(http://www.gl.umbc.edu/root/backup.shtml)

Relevant section:

**AFS (gl) Restore Procedure**

The first thing, as always, is to know what you're restoring and when you're restoring it from. In the following example, we're assuming that we need to restore lostit1's afs home directory from the first of October, 2000.

The very first step is to find the name of the volume to restore. To do this, you run **fs lq *directory***, where directory is the name of the directory being restored:

```
[jon@smirnoff home]$ fs lq ~lostit1
Volume Name                 Quota      Used %Used   Partition
user.lostit1                15000      6880   46%         82%
```

The volume, in this case, is user.lostit1. (All user volumes should be in the form of user.username, such as user.jon, user.banz, or user.jack.)

All restores must be done on Smirnoff. Log onto smirnoff. Make sure that no backups are in progress: run **ps -ef|grep backup** and verify that only the scheduler is running. If a backup is running, wait until it is complete before continuing. (You may want to ask around, find out how long it has been running, etc. to get an idea of when.) Now run the backup software: **/usr/afsws/etc/backup**. This will bring up the **backup>** prompt.

Now the volume may be restored. Typically, the volume should be restored on the last /vice?? partition on quigon, which at present is /vicepm. If this changes in the future, any such change should be documented here.

The general format for the restore command is **volrestore -server *server-to-restore-to* -partition *partition-to-restore-to* -volume *volume-to-be-restored* -extension *extension-to-volume-name* -portoffset *port-number* -date *date-to-be-restored-from***

The extension should be the date the backup is being restored from, and the portoffset should be a random number between two and five. The date format is MM/DD/YYYY, so in the above case, the restore command given was **volrestore -server quigon.umbc.edu -partition /vicepm -volume user.lostit1 -extension .20001001 -portoffset 2 -date 10/01/2000**

The system responds with several messages, indicating that a restore has been started. At some point, it should ask for a tape. This tape request will appear via e-mail. Operations should put the requested tape in one of smirnoff's tape drive. You should probably call down to operations and request this. Once the correct tape is in the drive, you can suspend the backup software by typing *Control-Z*, and then run the command **sudo /usr/afs/backup/bin/rescan** which will respond with a message indicating that it's retrying the tape drive. Re-enter the backup program by typing **fg** and hitting enter.

After several tapes have been restored from, the backup software should tell you that the full restore has been finished, and you can quit by typing **quit** at the prompt. Now the newly restored volume has to be mounted and the ACLs have to be set correctly.

The restored volume should be placed above the user's home directory, inside their home volume. You should cd into this directory with a command such as **cd ~lostit1/..** and then make the mount point.The command is **fs mkmount -dir *new-directory-name* -vol *volume-to-be-mounted*** This command needs two parameters: the name of the directory you would like the volume mounted as, and the name of the volume to be mounted.

In this case, the volume name is user.lostit1.20001001; a good directory name is generally the word 'home' followed by the date of the restore, which in this case is home.20001001. This gives us the command **fs mkmount -dir home.20001001 -vol user.lostit1.20001001**

Finally, we have to restore the ACLs for that directory so that not everyone can read it, and so that the user can. ACLs apply on a per-directory basis. To remove permissions for any user to read that directory, the general command is **find *top-level-directory* -type d -exec fs setacl \{\} system:anyuser none \;** which, with a top level directory of home.20001001, ends up being **find home.20001001 -type d -exec fs setacl \{\} system:anyuser none \;**

This will spew a number of error messages about not being able to change a backup or readonly volume. Don't w0orry about these messages. Finally, you wish to give the user read and list access to the volume, which you can do with the command **find *top-level-directory* -type d -exec fs setacl \{\} *user-name* rl \;** which ends up being **find home.20001001 -type d -exec fs setacl \{\} lostit1 rl \;**

This will also spew many error messages, as above. The procedure is now finished; mail the user that the volume is now available, giving directions on copying stuff from the old volume to the new. When the user indicates that she or he is finished, you should remove the mount point and the volume.

## Family Educational and Privacy Rights (FERPA) *(excerpts)*

(http://campussafety.org/publicpolicy/laws/ferpa.html)

The website cited above has extensive documentation on FERPA and corollary amendments to the original 1994 statute. The segments of FERPA that probably have the most impact on federally funded university Campus Security Officers follow:

**(3)** For the purposes of this section the term "educational agency or institution" means any public or private agency or institution which is the recipient of funds under any applicable program.

**(4)(A)** For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which--

**(i)** contain information directly related to a student; and

**(ii)** are maintained by an educational agency or institution or by a person acting for such agency or institution.

**(B)** The term "education records" does not include--

**(i)** records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

**(ii)** records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;

**(iii)** in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or

**(iv)** records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.

# APPENDIX

## A: Screen shots

Figure 1: The following screenshot of the UMBC WebAdmin interface shows the login screen; this is where authorization tokens are generated and stored as browser cookies.

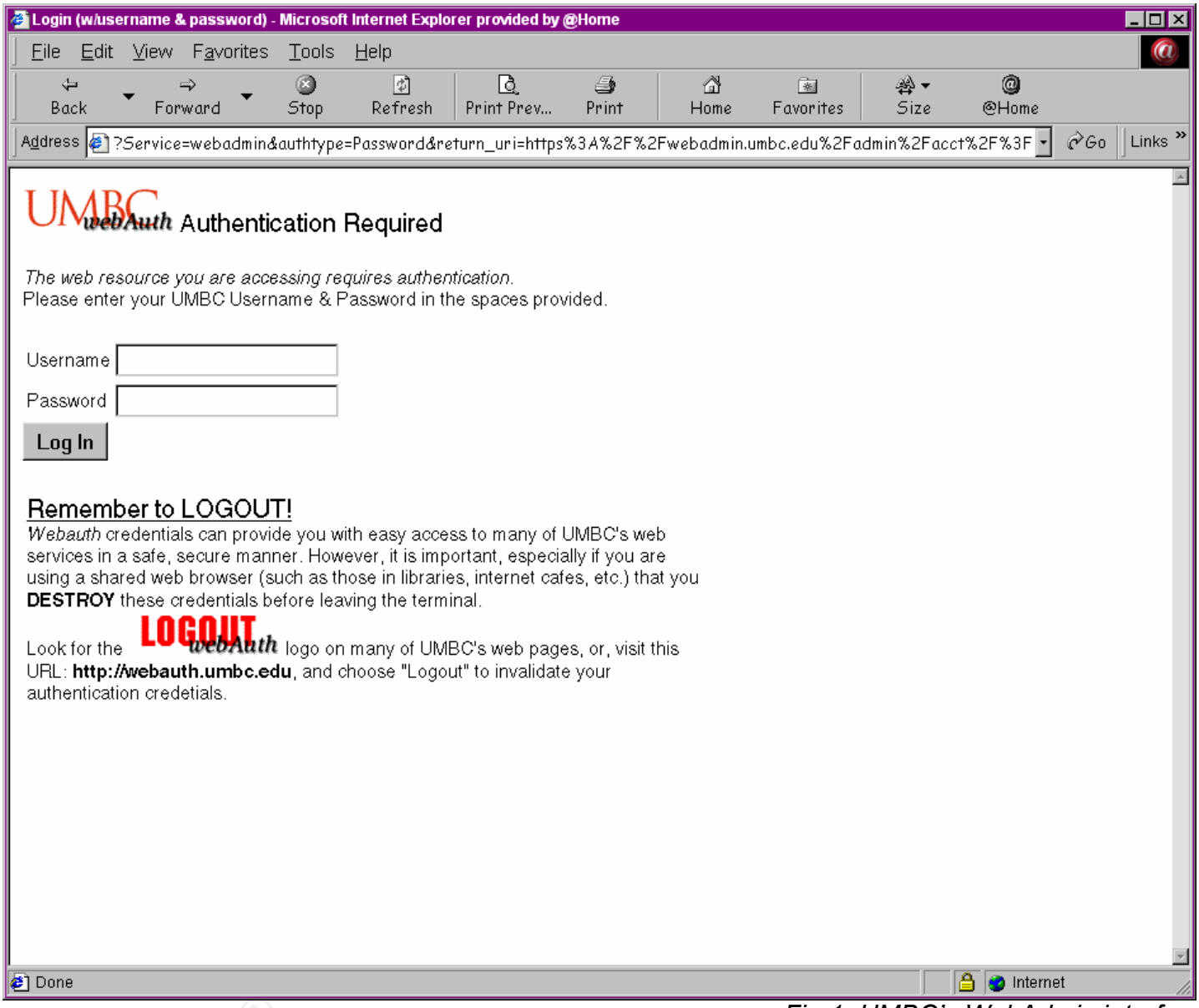


*Fig 1: UMBC's WebAdmin interface*

Figure 2: The following screenshot of the WebAdmin password-changing interface shows the screen that authenticated and privileged users get after clicking on “Change a Password.”

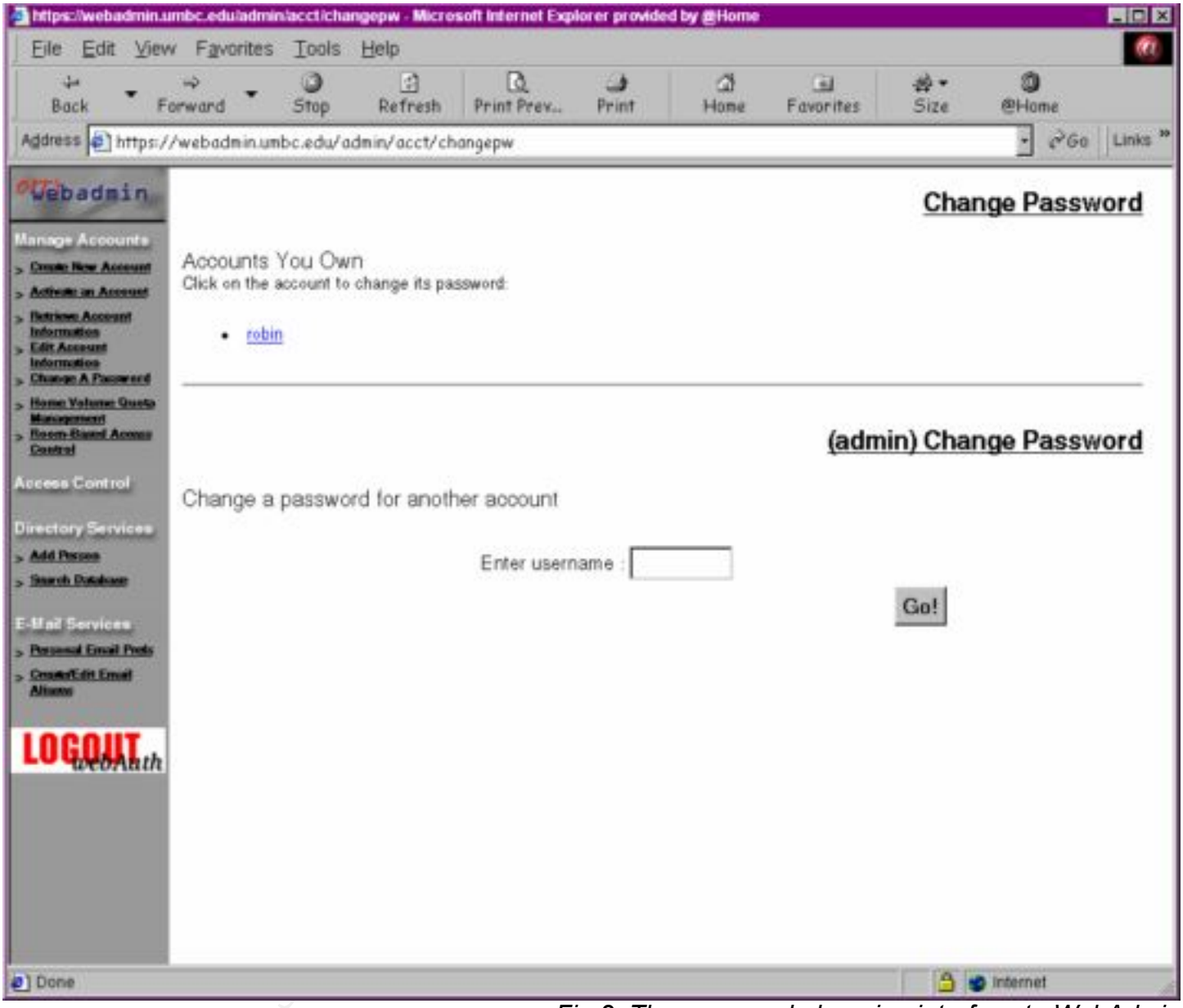


*Fig 2: The password-changing interface to WebAdmin*

## B: Scripts

"snarf-string"

*This Perl program will search through a specified log file for the string indicated and format the output string before printing it to* `stdout`*. Can be used to grab usernames, machine names, etc, from syslog-style files. Written and maintained by Andy.*

```
#!/usr/local/bin/perl

# Quick-and-Dirty - needs tightening up - AFJ

if ($#ARGV >= 0)
{
       $log = shift @ARGV;
       open (LOG,$log) || die "Cannot open $log";
}
else
{
       $log = "-";
}


print "Extract from log $log";

if ($#ARGV == 0)
{
       $searchstring = shift @ARGV;
       print "\tSearch string: $searchstring";
}

print "\n\n";

if ($log eq "-")
{
       while (<STDIN>)
       {
              if ($searchstring)
              {
                     /$searchstring/i || next;
              }

              ($mon, $day, $time, $host, $process, @therest) = split (/\s+/);

              if ($process !~ /sendmail/)
              {
                     print ("$mon-$day $time          $host/$process\n",
                            join (" ", @therest),"\n",
                     "-----------------------------------------------\n");
              }
       }
}
else
{
       while (<LOG>)
       {
              if ($searchstring)
              {
                     /$searchstring/i || next;
              }

              ($mon, $day, $time, $host, $process, @therest) = split (/\s+/);

              if ($process !~ /sendmail/)
              {
                     print ("$mon-$day $time          $host/$process\n",
                            join (" ", @therest),"\n",
                     "-----------------------------------------------\n");
              }
       }
}
```

“sed-replace-guid”

This sed script file replaces the “unfriendly” guid string with a more human-readable username or description (highlighted with asterisks). When it is invoked on a copy of a log file, it makes the analyst’s job easier. Again, please note that the guids as well as the description have been sanitized. Written by Andy.

```
/guid=111111-111111-111111-111111/ i\
***evan***

/guid=222222-222222-222222-222222/ i\
***irwin***

/guid=333333-333333-333333-333333/ i\
***Help Desk supervisor 1***

/guid=444444-444444-444444-444444/ i\
***Help Desk supervisor 2***

/guid=555555-555555-555555-555555/ i\
***Help Desk student 1***

/guid=666666-666666-666666-666666/ i\
***Help Desk student 2***
```

Last Updated: July 21st, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Security Awareness Summit & Training 2017 | Nashville, TN | Jul 31, 2017 - Aug 09, 2017 | Live Event |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| Community SANS Memphis SEC504 | Memphis, TN | Aug 21, 2017 - Aug 26, 2017 | Community SANS |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Mentor Session AW - SEC504 | Milwaukee, WI | Aug 23, 2017 - Sep 29, 2017 | Mentor |
| Mentor Session AW - SEC504 | New York, NY | Aug 24, 2017 - Sep 08, 2017 | Mentor |
| Mentor Session - SEC504 | Denver, CO | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling | SEC504 - 201709, | Sep 05, 2017 - Oct 12, 2017 | vLive |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| Mentor AW - SEC504 | Santa Clara, CA | Sep 11, 2017 - Sep 22, 2017 | Mentor |
| SANS Dublin 2017 | Dublin, Ireland | Sep 11, 2017 - Sep 16, 2017 | Live Event |
| Mentor Session - SEC504 | Arlington, VA | Sep 20, 2017 - Nov 01, 2017 | Mentor |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS SEC504 at Cyber Security Week 2017 | The Hague, Netherlands | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Columbia SEC504 | Columbia, MD | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Mentor Session - SEC504 | Boston, MA | Sep 26, 2017 - Nov 07, 2017 | Mentor |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Mentor Session AW - SEC504 | Houston, TX | Oct 02, 2017 - Dec 11, 2017 | Mentor |
| Mentor Session - SEC504 | Columbia, SC | Oct 03, 2017 - Nov 14, 2017 | Mentor |
| Community SANS Chicago SEC504 | Chicago, IL | Oct 09, 2017 - Oct 14, 2017 | Community SANS |
| SANS Phoenix-Mesa 2017 | Mesa, AZ | Oct 09, 2017 - Oct 14, 2017 | Live Event |