Global Information Assurance Certification Paper

MBUS 543 Practical Assignment

Anatomy of an Insider Incident

By Walter P. Opaska

Table of Contents

Preface – The Insider Threat

Much of the emphasis of computer security incident handling focuses on the threat from outsiders. Outsiders use sophisticated methods to compromise systems. Because of the high tech nature of systems and the technological expertise required to develop and maintain them, it is not surprising that experts have devoted the overwhelming attention to technological vulnerabilities and solutions[1].

However, those responsible for computer security must also prepare for another type of threat, the threat by an insider. An insider is a person with some level of authorized access to a computer system or network. Many insiders have the access and knowledge to compromise entire systems or networks[2]. Insiders are the source of many computer incidents. For example, a 1999 survey by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) found that 80% of the information security professionals who responded to the survey cited disgruntled and dishonest employees (insiders) as the most likely source of attack on their computer systems[3]. Also 55% of the respondents to the same CSI/FBI survey reported incidents of unauthorized access by insiders[4].

The focus of this paper will be an actual incident caused by an insider at a large agency. After summarizing the incident, I will use the Sans Institute's Handbook, Computer Security Incident Handling Step by Step, and the materials from the course, MBUS 543, Incident Handling and Malicious Code, to compare and critique how this incident was handled with those recommended by these guidelines. Finally, in the 'Lessons Learned' section, I will summarize what steps could be implemented to prevent this type of insider incident in the future.

Executive Summary

---

[1] E. Shaw, K. Ruby, and E. Post, The Insider Threat to Information Systems. Department of Energy, Nonproliferation and National Security Institute, URL: www.nnsi.doe.gov/c/Security_Guide/Treason/Infosys.htm. (February 16, 2001).

[2] Threats to Computer Systems, Department of Energy, Nonproliferation and National Security Institute, URL: www.nnsi.doe.gov/c/Security_Guide/V1comput/threats.htm. (February 16, 2001).

[3] Richard Power, "1999 CSI/FBI Computer Crime Survey," Computer Security Issues and Trends, Winter, 1999.

[4] Cyber Attacks Arise from Outside and Inside Corporations, Computer Security Institute, March 5, 1999. URL: www.gocsi.com/prelea990301.htm, (February 16, 2001).

At approximately 7:30 AM one weekday morning, the chief systems administrator of a large national agency was sitting at his desk attempting to log into one of the agency's VAX/VMS computer systems. He was unable to log into the system from his account despite using his correct passwords. Nor was he able to log in with any of the system accounts. Subsequent investigation revealed that all user IDs were disabled. Also, the intruder "turned off" auditing and deleted the audit log. The system hosted a highly sensitive labor and employee relations database. The investigation revealed that a former contract employee, an insider who quit the day before, caused the incident. He dialed into the system the night before using an user ID with system (root) level privileges. He suspended all user IDs, stopped the audit mechanism, and deleted the audit log. Appendix I provides a graphical representation of the incident.

Phase 1: Preparation

The preparation phase is defined as the steps that had been taken to prevent, minimize, and/or respond to a computer security incident before it has occurred. Some of the steps in the Preparation Phase include: 1) Establish policy and post warning banners, 2) Develop management support for an incident handling capability, 3) Select, organize and train an incident handling team, 4) Develop easy reporting facilities and an emergency communications plan, 5) Establish guidelines for inter-departmental cooperation, 6) Pay particular attention to system and network administrators, and 7) Develop interfaces to law enforcement and computer security response teams[5].

The agency followed some of the steps in the Preparation Phase. It had a detailed written policy for handling and reporting computer security incidents. An agency information security handbook enunciated this policy. This policy detailed such essentials as:

- What is an incident.
- Who should be notified.
- The types of incidents that will be investigated.
- The groups who will investigate incidents
- How incidents are reported

The handbook defined incident reporting facilities and established guidelines for inter-departmental cooperation. In particular it detailed the roles information systems, system owners, and headquarters would play during an incident.

The agency used warning banners extensively. The criteria for banners was stated in the agency information security handbook. The facility's computers all had warning banners.

[5] Incident Handling Step By Step, SANS Institute, 1998, p. 1.

Another preparation step the agency made was to establish an interface with law enforcement. The organization is an independent agency within the United States federal government. It also has an internal investigative department with federal law enforcement authority. This department has an important role in investigating computer security incidents. For example, it investigates all serious computer security breeches and presents them for possible prosecution. Its role is well defined in the agency's information system security handbook.

Despite these strengths, the agency was not adequately prepared for manage this computer security incident. Two areas stand out:

- Lack of management support
- Poor relationship with system administrators

While management developed a computer incident management program at this facility, the program did not cover the host that was attacked. The facility computer security officer (CSO) publicly stated that this host was not his responsibility. Nor was it covered by his plan. The manager of this facility supported him. Both opposed the relocation of the computer to the facility.

This computer ran an operating system, VMS, and a database system, Basis, which were not used elsewhere at the facility at the time of the incident. The CSO was not familiar with either and felt his major responsibilities were in other areas. He stayed uninvolved and left security administration to the system managers and administrators.

However, system administration was in disarray. The assigned administrators also took little interest in system management, leaving it to a recently hired contract employee. When hiring this associate system administrator, a critical personnel security control was bypassed. He did not have to complete the screening process required for all personnel holding a critical position, such as associate system administrator. The screening process may have identified the incident where, as a high school student, he hacked into a college's computer system. Instead of pressing charges, the college hired him to identify computer security weaknesses.

The associate system administrator was very knowledgeable and intelligent. However, he was given little supervision or direction from management or the CSO. He quickly became distrustful and contemptuous of both.

Jump Kit or Tools Used

Because of the above defects, the investigators did not have an established set of procedures and tools, i.e. a jump kit available to investigators of this type of incidents.

Nor did they have an established checklist to follow in case of an incident. The investigators improvised a jump kit. They used standard Digital Command Language (DCL) commands such MODIFY, LIST, and SHOW to research the problem. They also ran the Authorize (SYS$SYSTEM:AUTHORIZE) and Accounting (SYS$SYSTEM:ACCOUNTING) utilities. AUTHORIZE allows a user with system privileges access to the User Authorization File (UAF). The UAF file contains information on all accounts and contains their encrypted passwords. ACCOUNTING controls the system audit trail. They used the hardcopy produced by the operator console to document the commands they issued and their results.

Phase 2: Identification

The Identification phase involves determining whether or not an incident has occurred, and one has occurred, the nature of the incident and, if possible, the impact to the business. Identification normally begins after someone has noticed an anomaly in a system. This phase also includes informing and soliciting help from people who can help you understand and solve the problem[6].

This phase has these steps: 1) Determine whether or not an event is actually an incident; 2) Assign a person to be responsible for the incident; 3) maintain a chain of custody; 4) Coordinate with network services, and 5) Notify appropriate officials[7].

Did an Incident Occur

It was simple to determine that an incident occurred. No users could log in. At 7:30 AM, the section head could not log in under his own user ID. Nor was he able to log in under any of the available system IDs. Users were calling the customer support line asking why they could not log into the system. As the system worked fine the day before, it appeared to the system manager that something was wrong, possibly a security incident.

Responsibility, Coordination and Notification

After determining that the event was an incident, the section manager contacted the CSO. After finding out that the event occurred on the VAX, the CSO stated that it was not his responsibility. However, the section manager was persistent in asking for the CSO to help manage this incident. The CSO reluctantly agreed. He called the vendor's support line. They said that a service engineer would be dispatched. He then notified the appropriate officials: the agency's law enforcement group, the

[6] Ibid., p. 15.
[7] Ibid.

headquarters security staff, the help desk, and the customer. The latter two were important. The help desk handled all inquiries as to the login problems. The customer was periodically briefed about the problem. Keeping him informed minimized pressure from that area.

Chain of Custody

The agency's law enforcement group stated the rules for the chain of custody. All items available, such as the system's hardcopy log, would be preserved. Since this was not a networked system, this limited the scope of the investigation.

Phase 3: Containment

The goal of the containment phase is to limit the scope and magnitude of an incident, to keep the incident from getting worse[8]. The containment phase has a number of steps, some of which the agency performed very well. These include: 1) Avoid compromised code, if possible; 2) Backup the system; 3) Deploy a on-site survey team; 4) Keep a low profile; 5) Determine the risk of continuing operations; 6) Continue to consult with system owners; and 7) Change passwords.

Avoid Compromised Code

Because the machine was connected only by a modem bank to the operations center, it was easy to avoid any compromised code by isolating the machine. This was relatively easy. The compromised machine was disconnected from the outside by busying its modems. This isolated the machine and allowed it to be examined. For operational reasons, the machine was not connected to any type of network, either TCP/IP or DECnet. All users were required to dial into the system.

Backup the System

A machine backup was not immediately performed, mainly for two reasons. First, there was much confusion as to what steps to take in. More importantly, there was much pressure to continue operations. Later, when the cause of the incident was identified, a backup was made of the data using the standard VMS Backup utility. No other backup utility was available for use by the investigators. No problems occurred while making the backup.

Deploy a System Team

[8] Ibid., p.17.

An on site team was surveying the situation, with the section manager as the de facto head. The teams ultimately consisted of the section manager, section staff members, the CSO, a service engineer, agency law enforcement personnel, and other employees with VAX/VMS experience. The system owner was available for consultation.

Keep a Low Profile

Keeping a low profile was impossible. Rumors spread quickly through the facility about a possible hacker. However, the help desk was enlisted in minimizing the effects of rumors and distributing what information that was available to the users and workers at the facility.

Consult with the System Owner and Assess Risk

The team had extensive consultations with the system owner to determine the risk of continuing operations. The sole application on the machine consisted of a database containing records of agency labor and employee actions in internal grievance and arbitration cases. Employee and labor relations personnel consulted the database to obtain a history of labor actions. They used this history to determine if any precedents existed that affected the case(s) on which they were responsible. The systems owner argued forcefully for the resumption of service, based on the cost of downtime, which he calculated as running into the thousands of dollars a day.

Both the team and the system owner agreed to wait until the arrival of the agency law enforcement personnel later that morning. All wanted agency law enforcement personnel to become a part of the investigation. No additional steps, such as changing passwords, were taken until law enforcement was on site.

Phase 4: Eradication

The goal of the eradication phase is to make sure the problem is eliminated and the avenue of entry is closed off[9]. Steps that are part of the eradication phase include: 1) Determine cause and symptoms of the incident; 2) Improve defenses; 3) Perform a vulnerability analysis; 4) Remove the cause of the incident; 5) Backup, restore, and validate the system; 6) Restore operations and monitor the system. This paper will focus on steps one, four, five, and six. These are the steps most relevant to this incident.

[9] Ibid., p.21.

Determine Cause and Symptoms of the Incident

The major symptom was that no one could log into the system, i.e. all logon IDs were suspended. Nobody could access the system to find out what exactly occurred. However, a hardcopy log was available at an operator's console in the secured computer room. The information contained on this log was very limited, consisting of system status messages. Nothing of importance was on this log.

However, the console was logged in as a system user and was still a "live," active account. In VMS, if an account is logged on, as long as it is still active, it keeps the attributes it had at login time. Therefore, this active account still was usable and had system privileges. Therefore, this account was useable as an investigative tool at the console. Under the supervision of the agency's law enforcement investigators, an experienced VAX/VMS system user entered a number of commands from the hardcopy console. As this was making a printout of each command and its result, the law enforcement personnel deemed this to be sufficient as forensic evidence for a possible criminal investigation.

After determining that this account was available, the next step was to use the account to attempt to determine the cause of the event. Among the first commands entered were "SHOW PROCESSES" and "SHOW SYSTEM." These commands were issued to determine if any abnormal processes or operating programs were running. An experienced VAX/VMS system administrator noticed one anomaly; the ACCOUNTING utility was not running. ACCOUNTING is a utility that produces a file of system events including logins. On this system, ACCOUNTING was the sole system audit trail. Exhibit 1 provides an example of the audit information the ACCOUNTING utility provides[10].

Exhibit 1 – Sample ACCCOUNTING Utility Data

[10] OpenVMS System Manager's Manual, January 9, 2001, chapter 19.6. URL: http://www.openvms.compaq.com:8000/72final/6017/6017pro_085.html#index_x_4883. (February 16, 2001). Please note that this chart represents the type of data that would be retrieved from an investigation and is not an actual incident-related screen shot.

As Exhibit 1 shows, the ACCOUNTING utility can be used as an audit trail for VMS logins. It can also track login failures. It is logically equivalent to a combination of the Unix log files /log/var/wtmp and log/var/btmp.

The next step was to run the command 'SHOW ACCOUNTING.' The purpose of this command is to determine if auditing is currently operating. The results of this command returned a message stating that ACCOUNTING is currently disabled (not operating).

The final accounting related step was to run the command 'DIRECTORY SYS$MANAGER: ACCOUNTING.DAT.' The purpose of this command was to determine if the ACCOUNTING file, the audit trail, existed. The command returned a file not found message. This meant that the audit trail file did not exist. As ACCOUNTING was enabled the day before, this was evidence that someone possibly tampered with the system.

Then the investigator ran the AUTHORIZE utility using the command 'RUN SYS$SYSTEM: AUTHORIZE.' The AUTHORIZE utility gives a user with system privileges access to the UAF file. The UAF file contains information on all accounts and contains their encrypted passwords. For investigative purposes, UAF is logically equivalent to a combination of the Unix passwd and shadow files.

The next step was to run the SHOW command for selected users to display the contents of the UAF. The most important result was that all users displayed had the flag 'DISUSER' set on their accounts. DISUSER means that the account is suspended and cannot be used to log into the machine. As Exhibit 2 shows[11], all logins fail with DISUSER set.

---

[11] OpenVMS System Manager's Manual, January 9, 2001, chapter 6.3. URL: http://www.openvms.compaq.com:8000/72final/6017/6017pro_019.html#index_x_1070. (February 16, 2001).

Exhibit 2 – System Login Flow

Step	Action	Result
1.	System examines the login flags.	The system begins with DISUSER. If the DISUSER flag is set, the login attempt fails. Note that setting this flag for powerful, infrequently used accounts (such as Field Service accounts) eliminates the risk of guessed passwords for those accounts.

Exhibit 3 illustrates the commands a user would use to suspend an account[12]. The login flag DISUSER disables the user and prevents anyone from logging in to that account.

Exhibit 3 – Commands Used to DISUSER an Account

[redacted]

For example:

[redacted]

The investigation disclosed that no other system, production or user files or processes were found to be altered. The conclusion, therefore, was that some user with system privileges deliberately altered the system to prevent its operation.

One suspect already existed. An associate system administrator resigned the day before. He was very hostile to management and demonstrated it by telling his manager "I quit," just before the end of his shift. He was interviewed by the criminal investigators. At the interview, he admitted locking out all the users and deleting both the ACCOUNTING file and process. He used an obscure system account that only he knew the password. Although his account was suspended and the passwords on most of the system level accounts were changed, this one was missed. This case was presented to the local prosecutor who declined to press charges. No other action was taken against the former employee.

Remove the Cause of the Incident

When the former associate system manager admitted causing the incident, the immediate cause of the incident was removed. To prevent a reoccurrence, all passwords were changed on the restored system for all users and all accounts.

[12] Ibid. Please note that this exhibit represents the type of data that could be retrieved from an investigation and is not an actual incident-related screen shot.

Backup, Restore, and Validate the System

The final investigative act was to backup the system to tape. Although this was described briefly in a prior section, this section will describe the backup procedures taken. An image backup of all files was made. An image operation processes all files on the input disk. An image backup (also called a full backup) saves a copy of all the files on a disk (or volume) to a special file called a save set[13].

An image backup is logically equivalent the Unix command 'dump 0.' It copies all files on the system. However, unlike the Unix backup command 'dd,' it does not read input files block by block. For forensic purposes, an image backup is not the optimal solution, because it does not capture deleted files, as does dd. It was the best solution available. The image backup was kept as evidence.

Because a complete set of full and incremental backups were available, the decision was made to restore the data from the day before and use that. All system level accounts had their passwords changed. Non privileged accounts had their passwords were set to expire to force a change at login. The system owner agreed with this decision and put out a system message to covey this to all users. The help desk was also notified of this and handled many of the questions arising from these decisions.

No problems occurred while making the backup.

The former associate system manager admitted that he accessed the system very late at night. He stated that he did nothing to yesterday's data. Therefore, a decision was made that yesterday's day was adequate to use. The goal was to have the system operational the next day. The investigators and the system owner randomly validated selected system and data files to determine if any files were altered. They emphasized files changed that day. No additional evidence of tampering could be found. Therefore, rather than spend additional days performing a full validation, all decided that the risk of tampering was less than the cost of performing a full validation. Therefore, the system was operational the next day with the latest backup.

Restore Operations and Monitor the System

As stated above, the system was operational the next day using the latest backup. The staff continued monitoring the system for any additional evidence of tampering.

---

[13] OpenVMS System Manager's Manual, October 2, 1997, URL: http://www.openvms.compaq.com:8000/ssb71/6017/6017p029.htm#6017backup (February 24, 2001).

Chain of Custody Procedures

The agency's criminal investigators gathered and kept all evidence. The investigators were on site on the first day of the incident. The chain of custody began when the evidence was turned over to the investigators. The investigators used a standard form developed by their group for criminal investigations. They initialed, dated, and numbered all notes and printouts. They labeled all items they took as evidence. The investigators gave the section manager receipts for the items they kept as evidence.

The following is a list of all known evidence taken by the agency's criminal investigators for this incident.

- Hardcopy system log from the console.
- System backup tape that included the time the incident occurred.
- Notes from interviews with the system personnel, the section manager, and other facility personnel.
- Notes from the interview with the perpetrator of the incident.

Phase 5: Recovery

The recovery phase the task is to restore the system to a fully operational status. As stated in Phase 4, the system was operational the next day using the latest backup. This backup came from the day before. Because the incident happened late at night, no data was lost. Nor was any tampering of data.

In addition, the staff continued monitoring the system for any additional evidence of tampering. None was found. An active 'home grown' intrusion detection system was developed for this host. The system administrators managed the intrusion system under the close supervision of the associate CSO. This system analyzed audit data to look for such discrepancies as system default accounts used from unlikely sources and late night activity.

Phase 6: Follow-up/Lessons Learned

Follow-up

The purpose of the follow-up phase is to critique the situation to identify areas where improvements can be made. The accepted method of compiling the data so it can be used in the future is the follow-up report. At the request of the headquarters security staff, an assistant CSO wrote a follow-up report. This follow-up report followed the guidelines stated in the agency's information system security manual. This follow-up

report not only critiqued the incident but also provided guidance for responding to future events. In addition, it recommended a comprehensive set of additional security controls be put in place.

Lessons Learned

Lessons learned are a list of those follow-up activities that, if changed, will enhance computer response techniques. Also, included in lessons learned are those actions that can prevent future computer security incidents from occurring.

A number of lessons learned came from this incident. Those that affect computer security response and prevention include:

1) Facility management must be held responsible for all computers at his/her facility. Ignoring a platform is a recipe for disaster.

2) The CSO is must be responsible for security on all computers at his/her facility. If the CSO does not have expertise in a particular area, then he must either be trained or provide staff with the requisite skills

3) All personnel procedures must be followed. These include pre-employment screening and resignation for employees and contractors with high-level system authorities.

4) An incident response toolkit must be developed. This toolkit must be general enough to respond to incidents on all platforms, yet specialized enough to handle all agency platforms. Headquarters security staff was tasked with developing this toolkit.

5) All systems must be monitored. Audit techniques must be developed to monitors all computer systems at a facility. Monitoring should be done either by the CSO or by systems administrators under the direction of the CSO.

References

1) Computer Security Evaluation FAQ, Version 2.1, URL: http://www.bookcase.com/library/faq/archive/computer-security/evaluations.html, (February 16, 2001).

2) Computer Security Institute, Cyber Attacks Arise from Outside and Inside Corporations, , March 5, 1999. URL: www.gocsi.com/prelea990301.htm, (February

16, 2001).

3) OpenVMS System Guide to System Security, January 9, 2001, URL: http://www.openvms.compaq.com:8000/72final/6346/6346pro_021.html - index_x_4883. (February 16, 2001).

4) OpenVMS System Manager's Manual, January 9, 2001, URL: http://www.openvms.compaq.com:8000/72final/6017/6017pro_085.html#index_x_4883. (February 16, 2001).

5) OpenVMS System Manager's Manual, October 2, 1997, URL: http://www.openvms.compaq.com:8000/ssb71/6017/6017p029.htm#6017backup (February 24, 2001).

6) Power, Richard, "1999 CSI/FBI Computer Crime Survey," Computer Security Issues and Trends, Winter, 1999.

7) Shaw, E., Ruby, K., and Post, E., The Insider Threat to Information Systems, Department of Energy, Nonproliferation and National Security Institute, URL: www.nnsi.doe.gov/c/Security_Guide/Treason/Infosys.htm. (February 16, 2001).

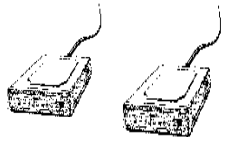
8) Threats to Computer Systems, Department of Energy, Nonproliferation and National Security Institute, URL: www.nnsi.doe.gov/c/Security_Guide/V1comput/threats.htm. (February 16, 2001).

9) SANS Institute, Incident Handling Step By Step, 1998.

10) SANS Institute, The Network Security Roadmap Poster, http://www.sans.org/newlook/publications/roadmap.htm. (February 16, 2001).

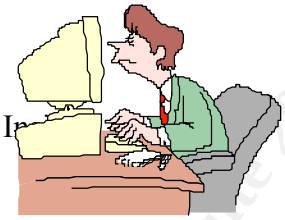
11) Segan, Sascha, Airports in Danger, ABCNEWS.com, October 16, 2000, URL: http://www.abcnews.go.com/sections/us/DailyNews/faa_computers001016.html. (February 16, 2001).

Appendix I – Graphical Representation of the Incident

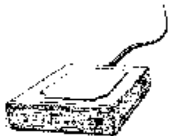


Agency' VMS Computer

Agency Modem Bank



I ns



ider's Modem