

Incident Handling Procedure

1. Introduction

This document provides some general guidelines and procedures for dealing with computer security incidents. The document is meant to provide Montana Tech support personnel with some guidelines on what to do if they discover a security incident. The term incident in this document is defined as any irregular or adverse event that occurs on any part of the Montana Tech computing systems and facilities. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are:

- You see a strange process running and accumulating a lot of CPU time.
- You have discovered an intruder logged into your system.
- You have discovered a virus has infected your system.
- You have determined that someone from a remote site is trying to penetrate the system.

The steps involved in handling a security incident are categorized into five stages: protection of the system; identification of the problem; containment of the problem; eradication of the problem; recovering from the incident and the follow-up analysis. The actions taken in some of these stages are common to all types of security incidents and are discussed in section 2. Section 3 discusses specific procedures for dealing with worm/virus incidents and hacker/cracker incidents.

1.1. Terms

- Some terms used in this document are:
- ISO - Installation Security Officer
- CSO - Computer Security Officer
- CSA - Computer Security Analyst
- LSA - Lead System Analyst
- CERT - Computer Emergency Response Team
- CIAC - Computer Incident Advisory Capability
- Coordinator – College Computer Specialist

1.2. Areas of Responsibility

In many cases, the actions outlined in this guideline will not be performed by a single person on a single system. Many people may be involved during the course of an active security incident which affects several of Montana Tech's systems at one time (i.e., a worm attack). The Montana

Tech CSA should always be involved in the investigation of any security incident.

The Montana Tech ISO, CSO, CSA and campus Computer Coordinators will act as the incident coordination team for all security-related incidents. In minor incidents, only the CSA or Coordinators will be involved. However, in more severe incidents all may be involved in the coordination effort. The incident coordination team will be responsible for assigning people to work on specific tasks of the incident handling process and will coordinate the overall incident response process. All people involved in the incident response and clean-up are responsible for providing any needed information to members of the incident coordination team.

Any directives given by a member of the incident coordination team will supersede this document.

1.3. Important Considerations

A computer security incident can occur at anytime of the day or night, although most hacker/cracker incidents occur during the off hours when hackers do not expect system managers to be watching their flocks. However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important. If the first person on the call list to be notified can not respond within a reasonable time frame, then the second person must be called in addition to the first. It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

The media is also an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge from a site currently responding to the incident. Providing information to the wrong people could have undesirable side effects. Section 2.4 discusses the policy on release of information.

2. General Procedures

This section discusses procedures that are common for all types of security incidents.

2.1. Keep a Log Book

Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that can not be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- People you have contacted or have contacted you.
- Names of systems, programs or networks that have been affected.

2.2. Inform the Appropriate People

Informing the appropriate people is of extreme importance. There are some actions that can only be authorized by CSO or CSA. Montana Tech also has the responsibility to inform other sites about an incident which may effect them. A list of contacts is provided below. Section 3 discusses who should be called and when for each type of security incident.

Phone numbers for the people below can be obtained from the Montana Tech Phone Book. Also, the campus telephone operator can be of help when trying to contact the appropriate people.

2.3. List of Contacts

- Montana Tech CSO
- Montana Tech CSA
- Montana Tech Coordinators

2.4. Release of Information

Control of information during the course of a security incident or investigation of a possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved. All release of information must be authorized by the Montana Tech administration (Chancellor or Vice Chancellors) as appropriate. Also, incident specific information, such as accounts involved, programs or system names, are not to be provided to any callers claiming to be a security officer from another site. All suspicious requests for information (i.e., requests made by callers claiming to be a CSA for another site), should be forwarded to the Montana Tech CSO. If there is any doubt about whether you can release a specific piece of information contact the Montana Tech CSO or appropriate administrative head.

2.5. Follow-Up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from

each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). If applicable, a set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the Montana Tech CSO and distributed to all appropriate personnel.

3. Incident Specific Procedures

This section discusses the procedure for handling virus, worm and hacker/cracker incidents.

3.1. Virus and Worm Incidents

Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via IRC (Internet Relay Chat). Viruses are not self-replicating and, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes; thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of the attack, then proceed as if the attack was worm related.

3.1.1. Isolate the System

Isolate infected system(s) from the remaining Montana Tech network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the LAN from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since the campus network will be disconnected from sites which may have patches. The Montana Tech CSO must authorize the isolation of the Montana Tech network from the outside world.

Log all actions.

Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.

Notify Appropriate People

Notify the Montana Tech CSA or Coordinator as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person.

The Montana Tech CSA will then be responsible for notifying other appropriate personnel.

***** NOTE** - Below, different times are given for suspected worm attack and for a suspected virus attack.

The Montana Tech CSA will notify the CSO as soon as possible. If unable to reach him within one hour (10 minutes for a worm attack), his backup person will be contacted.

The CSA or CSO will escalate to higher level management if necessary. The control room or CSA should notify all involved Coordinators within four hours (two hours for a worm attack).

3.1.2. Identify the Problem

Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system should be taken and saved. Review the process prior to an actual event. Save a copy of all system log files.

- Save a copy of all system log history, active user files
- Capture all process status information in a file.

If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files. Also, get a listing of all active network connections. The CSA can provide assistance in obtaining snap-shot information on the system.

Run an intrusion detection scanner against the infect system(s) or security monitor to identify other possible problems such as altered system files, new programs or hidden special files. It may be necessary to install a clean version from tape.

If other sites have been involved at this point, they may have helpful information on the problem and possible short term solutions. Also, any helpful information gained about the virus or worm should be passed along to Internet CERT sites, after approval by the Montana Tech CSO. Log all actions.

3.1.3. Contain the virus or worm

All suspicious processes should now be halted and removed from the system. Make a full dump/backup of the system and store in a safe place. The tapes should be carefully labeled so unsuspecting people will not use them in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all Montana Tech systems have been inoculated and/or the other internet sites have been cleaned up and inoculated. **Log all actions.**

3.1.4. Inoculate the System(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the tasks of assessing the damage is not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested. If possible, the virus or worm should be let loose on an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. **Log all actions.**

3.1.5. Return to a Normal Operating Mode

Prior to bringing the systems back into full operation mode, you should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to request all users to change their passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. **Log all actions.**

3.1.6. Follow-up Analysis

Perform follow-up analysis as described section 2.4.

3.2. Hacker/Cracker Incidents

Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naive young students looking for a thrill. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to the Montana Tech computing system.

Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events which have been discovered after the fact. Of the three, an active hacker/cracker session is the most severe and must be dealt with as soon as possible.

There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state (see section 3.2.2). The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to a identification and possible criminal conviction (see section 3.2.3). The method used to

handle a cracker/hacker incident will be determined by the level of understanding of the risks involved.

3.2.1. Attempted Probes into a Montana Tech System

Incidents of this type would include: repeated login attempts, repeated ftp, telnet or rsh commands, and repeated dial-back attempts (this is not inclusive).

Identify Problem

Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such as system logs files, the root history file, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. **Log all actions.**

Notify Montana Tech CSO and CSA

Notify the Montana Tech CSA within 30 minutes. If the CSA can not be reached then notify the CSO or the CSA backup person. The CSA or their backup person will be responsible for notifying other levels of management.

Identify Hacker/Cracker

If the source of the attacks can be identified, then the Montana Tech CSA (or a designated person) will contact the system administrator or security analyst for that site and attempt to obtain the identity of the hacker/cracker. The NIC may be one source for obtaining the name and phone number of the site administrator of the remote site. If the hacker/cracker can be identified, the information should be provided to the CSO or CSA. They will provide directions on how to proceed, if necessary. **Log all actions.**

Notify CERT

If the source of the attacks can not be identified, then the Montana Tech CSA will contact the Internet CERT and CIAC teams and provide them with information concerning the attack. ***NOTE - Release of information must be approved by the Montana Tech CSO or someone he designates. **Log all actions.**

Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the Montana Tech CSA or CSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.

3.2.2. Active Hacker/Cracker Activity

Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active rlogin or telnet session, an active ftp session, or a successful dial-back

attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker/cracker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. This decision must be made by the Montana Tech CSO or someone he designates (i.e., the CSA). The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

Notify Appropriate People

Notify the Montana Tech CSA as soon as possible. If unable to reach him/her within 5 minutes, contact the backup person. The CSA will then be responsible for notifying other appropriate personnel. The CSA, with possible help from the involved LSA or Coordinator, will be responsible for trying to assess what the hacker/cracker is after and the risks involved in letting the hacker/cracker continue his/her activity.

The CSA will notify the CSO as soon as possible. If unable to reach him within ten minutes, his backup person should be contacted. The CSO can make the decision to allow the hacker to continue or to lock him out of the system. Based on the decision, follow the procedures in 3.1 or 3.2 below.

The Montana Tech CSA or CSO will escalate notification to higher level management if necessary.

3.2.3. Removal of Hacker/Cracker From the System

Snap-shot the System

Make copies of all audit trail information and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections. The CSA may provide assistance in obtaining snapshot information on the system. **Log all actions.**

Lock Out the Hacker

Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. **Log all actions.**

Restore the System

Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close

any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the log book for this incident. **Log all actions.**

Notify Other Agencies

Report the incident to the Ames CNSRT, the Internet CERT and to CIAC. ***NOTE- Release of information must be approved by the Montana Tech CSO or someone he designates, see section 2.3. **Log all actions.**

Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the Montana Tech CSA or CSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.

3.2.4. Monitoring of Hacker/Cracker Activity

There are no set procedures for monitoring the activity of a hacker. Each incident will be dealt with on a case by case basis. The Montana Tech CSO or the person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system(s), the steps outlined in section 3.2.3 above should be followed.

3.2.5. Evidence of Past Incidents

In the case of where an incident is discovered after the fact, there is not always a lot of evidence available to identify who the person was or how they gained access to the system. If you should discover that someone had successfully broke into a Montana Tech system, notify the CSA within one working day. The CSA will be responsible for notifying the appropriate people and investigating the incident.

