

This guideline provides the major steps involved in the initial handling of an *incident*. Portions of this guideline were adapted from *Computer Security Incident Handling Guide* (NIST Special Pub. 800-61), <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>, and references are made to relevant *Guide* pages and other useful materials.

Note that the actual steps performed may vary based on the type of *incident* being handled, the nature of individual *incidents* and the strategies chosen for containment, eradication and recovery. For example, if the handler knows exactly what has happened based on analysis of indications (Detection and Analysis, Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. This guideline provides guidance to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Actions should be coordinated as described in the Incident Response Standard. More than one person may be responsible for the steps described in this guideline.

Detection and Analysis

1. Determine whether an *incident* has occurred
 - 1.1. Analyze the precursors and indications
 - 1.2. Look for correlating information
 - 1.3. Perform research, using –
 - 1.3.1. *Guide* references in Step 2
 - 1.3.2. SANS' *Intrusion Detection Cheat Sheets for Linux*,
http://www.sans.org/score/checklists/ID_Linux.pdf
 - 1.3.3. SANS' *Intrusion Detection Cheat Sheets for Windows*,
http://www.sans.org/score/checklists/ID_Windows.pdf
 - 1.3.4. search engines
 - 1.3.5. knowledge base
 - 1.3.6. SANS *Incident Identification Form* for recording basic info,
http://www.sans.org/score/incidentforms/IH_Identification.pdf
 - 1.3.7. *Security Incident Survey Cheat Sheet for Server Administrators*,
<http://security.arizona.edu/files/admin-incident.pdf>
 - 1.3.8. *Initial Security Incident Questionnaire for Responders*,
<http://security.arizona.edu/files/responder-incident.pdf>
 - 1.4. As soon as the handler believes an *incident* has occurred, begin documenting the investigation and gathering evidence, being careful to ensure that evidence can be preserved, if necessary (see 1.1 of "Containment, Eradication and Recovery")
2. Classify the *incident* as:
 - 2.1. Denial of service (*Guide* at 4-7)
 - 2.2. Malicious code (*Guide* at 5-5)
 - 2.3. Unauthorized access (*Guide* at 6-3)
 - 2.4. Inappropriate usage (*Guide* at 7-3)
 - 2.5. Multiple components (*Guide* at 8-1)
 - 2.6. Generic, if none of the above (*Guide* at 3-5)
3. Identify which resources have been affected and forecast which resources will be affected

4. Estimate the current and potential technical effect of the *incident*
5. Prioritize handling the *incident* based on the operational impact

Reporting

1. Report the *incident* to the appropriate internal personnel and external organizations, as provided in the Incident Response Standard
2. If reporting to the *UIISO*, University Information Technology Services, the HIPAA Privacy Officer, FSO – Bursar’s Department Services and/or law enforcement is required, coordinate remaining steps with personnel from such organizations

Resource:

Incident Response Standard, <http://security.arizona.edu/files/ISS1100.pdf>

Containment, Eradication and Recovery

1. Generic Incidents

- 1.1. Acquire, preserve, secure and document evidence
- 1.2. Contain the evidence
- 1.3. Eradicate the *incident*
- 1.4. Identify and mitigate all vulnerabilities that were exploited
- 1.5. Remove malicious code, inappropriate materials, and other components
- 1.6. Recover from the *incident*
- 1.7. Return affected systems to an operationally ready state
- 1.8. Confirm that the affected systems are functioning normally
- 1.9. If necessary, implement additional monitoring to look for future related activity

Resources:

Guide at 3-17 (see link in first paragraph)

CIS Benchmarks and Scoring Tools, <http://security.arizona.edu/auth/CIS>

2. Denial of Service Incidents

- 2.1. Acquire, preserve, secure, and document evidence
- 2.2. Contain the *incident*—halt the denial of service if it has not already stopped
 - 2.2.1. Identify and mitigate all vulnerabilities that were used
 - 2.2.2. If not yet contained, implement filtering based on the characteristics of the attack, if feasible
 - 2.2.3. If not yet contained, contact the Internet service provider (UIITS for most *units*) for assistance in filtering the attack
 - 2.2.4. If not yet contained, relocate the target
- 2.3. Eradicate the *incident*; if Step 2.2.1 was not performed, identify and mitigate all vulnerabilities that were used
- 2.4. Recover from the *incident*
 - 2.4.1. Return affected systems to an operationally ready state
 - 2.4.2. Confirm that the affected systems are functioning normally
 - 2.4.3. If necessary and feasible, implement additional monitoring to look for future related activity

Resources:

Guide at 4-9 (see link in first paragraph)

CIS Benchmarks and Scoring Tools, <http://security.arizona.edu/auth/CIS>

Network DDOS Incident Response Cheat Sheet,
<http://security.arizona.edu/files/ddos-incident.pdf>

3. Malicious Code Incidents

- 3.1. Contain the *incident*
 - 3.1.1. Identify infected systems
 - 3.1.2. Disconnect infected systems from the network
 - 3.1.3. Mitigate vulnerabilities that were exploited by the malicious code
 - 3.1.4. If necessary, block the transmission mechanisms for the malicious code
- 3.2. Eradicate the *incident*
- 3.3. Disinfect, quarantine, delete, and replace infected files
- 3.4. Mitigate the exploited vulnerabilities for other hosts within the *unit* and/or the university
- 3.5. Recover from the *incident*
 - 3.5.1. Confirm that the affected systems are functioning normally

Resources:

UITS Security Operations web site,

<http://ccit.web.arizona.edu/index.php?id=guidelines#c6987>

<http://ccit.web.arizona.edu/index.php?id=2076#c6972>

Guide at 5-7 (see link in first paragraph)

CIS Benchmarks and Scoring Tools, <http://security.arizona.edu/auth/CIS>

4. Unauthorized Access Incidents

- 4.1. Perform an initial containment of the *incident*
- 4.2. Acquire, preserve, secure, and document evidence
- 4.3. Confirm the containment of the *incident*
 - 4.3.1. Further analyze the *incident* and determine if containment was sufficient (including checking other systems for signs of intrusion)
 - 4.3.2. Implement additional containment measures if necessary
- 4.4. Eradicate the *incident*
 - 4.4.1. Identify and mitigate all vulnerabilities that were exploited
 - 4.4.2. Remove components of the *incident* from systems
- 4.5. Recover from the *incident*
 - 4.5.1. Return affected systems to an operationally ready state
 - 4.5.2. Confirm that the affected systems are functioning normally
 - 4.5.3. If necessary, implement additional monitoring to look for future related activity

Resources:

Guide at 6-5 (see link in first paragraph)

SANS, *Intrusion Detection Cheat Sheets for Linux*,

http://www.sans.org/score/checklists/ID_Linux.pdf

SANS, *Intrusion Detection Cheat Sheets for Windows*,

http://www.sans.org/score/checklists/ID_Windows.pdf

CERT, *Steps for Recovering from a UNIX or NT System Compromise*,

http://www.cert.org/tech_tips/root_compromise.html

CIS Benchmarks and Scoring Tools, <http://security.arizona.edu/auth/CIS>

5. Inappropriate Usage Incidents

- 5.1. Acquire, preserve, secure, and document evidence
- 5.2. If necessary, contain and eradicate the *incident* (e.g., remove inappropriate materials)

Resource:
Guide at 7-5 (see link in first paragraph)

6. Multiple Component Incidents

6.1. Follow the Containment, Eradication, and Recovery steps for each component, based on the results of Detection and Analysis

Resource:
Guide at 8-2 (see link in first paragraph)

Post Incident Activity

1. Create a follow-up report
2. Hold a lessons-learned meeting (*Guide* at 3-22)

All italicized terms used in this guideline are defined in the Information Security Terms Guideline (IS-G100).

Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Incident Response Standard (IS-S1100)
Incident Response Plan (IS-P1100)
Computer Security Incident Handling Guide (NIST Special Pub. 800-61)
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>
SANS, *Intrusion Detection Cheat Sheets for Linux*,
http://www.sans.org/score/checklists/ID_Linux.pdf
SANS, *Intrusion Detection Cheat Sheets for Windows*,
http://www.sans.org/score/checklists/ID_Windows.pdf
SANS, Incident Identification Form,
http://www.sans.org/score/incidentforms/IH_Identification.pdf
CERT, *Steps for Recovering from a UNIX or NT System Compromise*,
http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
Security Incident Survey Cheat Sheet for Server Administrators,
<http://security.arizona.edu/files/admin-incident.pdf>
Initial Security Incident Questionnaire for Responders,
<http://security.arizona.edu/files/responder-incident.pdf>
Network DDOS Incident Response Cheat Sheet, <http://security.arizona.edu/files/ddos-incident.pdf>

Revision History

| | |
|----------------|---------|
| Initial Draft | 11/8/08 |
| UA-ISAC Review | 4/2/09 |
| Effective Date | 7/1/09 |