

## Incident Response Part# 2: Identification

By Gregory S. Miles, Ph.D.

Last issue we looked at the critical step of being prepared for a computer security incident. This article is the second of a six part series in Incident Response (IR). IR professionals have adopted a basic core set of activities that encompass the IR discipline that includes IR preparation, identification, containment, eradication, recovery, and follow-up.

Professional organizations that provide advice in the IR arena include but are not limited to the Carnegie Mellon Software Engineering Institute CERT<sup>®</sup> Coordination Center ([www.cert.org](http://www.cert.org)), the SANS Institute ([www.sans.org](http://www.sans.org)), CanCERT<sup>™</sup> in Canada ([www.cancert.ca](http://www.cancert.ca)), and the Forum for Incident Response Security Teams (FIRST) ([www.first.org](http://www.first.org)). This article focuses on IR Containment.

Identification of a computer security incident is one of the most critical and difficult elements of the CIRT activity. This is due to the fact that without the proper detection tools, logging, and security awareness, most incidents will go unnoticed for a long period of time. By the time it is discovered a great deal

of damage can be done to the system or network.

The primary function of identification is to determine if a problem really exists. And it may be difficult to determine because there are not always clear signs of an incident. You may experience a slow system, missing data, or other problems. In order to identify whether something is an incident, it is useful to have intrusion detection tools, virus scanning tools, audit logs, etc.

**“The primary function of identification is to determine if a problem really exists.”**

Without investigation by a subject matter expert many incidents can be incorrectly labeled as user error, equipment failure, etc... Technicians and SA's need to investigate problems fully and pass to the appropriate security personnel.

**There are certain indications or "symptoms" of an incident that deserve special attention:**

- System crashes
- New user accounts or high activity on a previously low usage account.
- New files (possibly with strange file names, such as data.xx or k or .xx )
- Accounting discrepancies (in a UNIX system you might notice the shrinking of an accounting file called /usr/admin/lastlog, something that

should make you very suspicious that there may be an intruder).

- Changes in file lengths or dates
- Unexplained web page changes (defacement)
- Attempts to write to system
- Data modification or deletion
- Denial of service
- Unexplained, poor system performance
- Anomalies (strange unexplained/abnormal events)
- Suspicious probes (there are numerous unsuccessful login attempts from another node).
- Suspicious browsing
- Inability of a user to log in due to unexplained account modifications

Incident identification involves more than just identifying the type of incident. It also involves identifying the scope of the incident. The scope of the incident will identify how far reaching the incident may be. Does the incident affect one system or all? Is it applicable to one operating system or all? A serious investigation of how far reaching the incident is going to be critical in the containment and recovery process.

Classifying an incident is one of the last critical steps of the identification process. The following is a list of possible classifications of incidents. This list is by no means comprehensive,

but provides solid examples from which to build your tailored set of classifications to meet your IT process needs.

## **Incident Type Classifications:**

1. Unauthorized Privileged (root) Access -- Access gained to a system and the use of root privileges without authorization.
2. Unauthorized Limited (user) Access - - Access gained to a system and the use of user privileges without authorization.
3. Unauthorized Unsuccessful Attempted Access -- Repeated attempts to gain access as root or user on the same host, service, or system with a certain number of connections from the same source.
4. Unauthorized Probe -- Any attempt to gather information about an Automated Information System (AIS) or its users on-line by scanning a site and accessing ports through operating system vulnerabilities.)
5. Poor Security Practices -- Bad passwords, direct privileged logins, etc., which are collected from network monitor systems.
6. Denial Of Service (DOS) information attacks -- Any action that preempts or degrades performance of a system or network affecting the mission, business, or function of an organization.

7. Malicious Logic -- Self-replicating software that is viral in nature; is disseminated by attaching to or mimicking authorized computer system files; or acts as a trojan horse, worm, malicious scripting, or a logic bomb. Usually hidden and some have the potential to Replicate. Effects can range from simple monitoring of system/network traffic to complicated automated backdoor with full system rights.
8. Hardware/Software Failure -- Non-malicious failure of HW or SW assets
9. Infrastructure Failure -- Non-malicious failure of supporting infrastructure to include power failure, natural disasters, forced evacuation, service provider failure to deliver services, etc.

Other classifications that should be considered based on your organization's security and system use policy include:

- Unauthorized Utilization of Services – This can include game play, relaying mail without approval, creating dial-up access, use organizational equipment for personal gain, and personal servers on the network.
- Espionage – This includes information stealing or manipulation, email monitoring, computer theft, data copying, and trojan/tunneling.

Along with the incident identification and classification process, the incident needs to be labeled with an incident

severity level that will help to identify the suspected impact of the incident on the business operation and help to establish the priority that will be associated with its resolution.

## Incident Severity Levels:

1. Severity Level 1: Incident could have long-term effects on business or incident affects critical systems.
2. Severity Level 2: Incursion on non-critical system; detection of precursor to a focused attack; believed threat of an imminent attack.
3. Severity Level 3: Threat of a future attack; detection of reconnaissance.
4. Severity Level 4: Unsubstantiated rumor of security incident

You must realize that this process may take as short as a few minutes to as long as weeks to complete the identification process. Ideally, the identification process is completed quickly, and the CIRT can then work out a plan for the containment of the incident, and begin the recovery process.

**Next IR article, we will be discussing Incident Response Part 3: Containment.**

© Security Horizon Inc. 2001

*Dr. Miles is the COO/CFO for Security Horizon Inc and the Director of CyberCrime Response for JAWZ Inc. You can contact him at [gmiles@securityhorizon.com](mailto:gmiles@securityhorizon.com).*