



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

From Events to Incidents

As more data on computer forensics becomes available, many have come to realize that the resource cost involved in incident handling situations is fairly significant. In addition, staffing an incident handling team with the proper skills required to effectively carry out incident handling is quite a challenge. This is even more of a challenge for many large organizations with sizeable networks. As such, it is in their best interest to optimally deploy such scarce resources. As in the case of a less ...

Copyright SANS Institute
Author Retains Full Rights

AD

An advertisement banner for Watchfire. On the left, there is a graphic of a globe and a login form with fields for "login" and "password". The text "Testing Web applications for vulnerabilities?" is written in white on a dark blue background. To the right is the Watchfire logo, which consists of a red flame icon and the word "watchfire" in a lowercase, sans-serif font.

Testing Web applications for vulnerabilities?

From Events to Incidents
Charles Pham
November 29, 2001
SANS GSEC Practical Assignment version 1.2f

Introduction

In all computer incident handling situation, some form of computer forensic is required in order to support the eradication, recovery and applying the lesson learned. As more data on computer forensic becomes available, many have come to realize that the resource cost involved in incident handling situation is fairly significant. In addition, staffing an incident handling team with the proper skills required to effectively carry out incident handling is quite challenge. This is even more of a challenge for many large organizations with sizeable network. As such, it is in their best interest to optimally deploy such scarce resource.

As in the case of a less than optimized intrusion detection system, incident handlers are often sent on a wild goose chase when the “incident” turned out to be an “event”. This type of activity in itself is a risk as it consumes cycles away from the real incidents. As in the case of an intrusion detection system, it would make sense to apply some form of filter to eliminate most of the false positives. For incident handling, filtering for ”events” can be provided through the use of a security helpdesk or junior security staffs. However, guidelines and training must be provided in order for these junior staffs to carry out the intended function. This paper is an attempt at clarifying “events” and “incidents” for training purposes so that effective filtering can be apply when it come to reporting an incident.

Definition:

Events:

An event is an observable occurrence in an information system that actually happened at some point in time. For example:

- An email
- A phone call
- A system crash
- A request for virus scans to be performed on a file or attachment

Incidents:

There are many definition of an incident available, however this depends on many factors within an organization. In most organization, combining the following generic definitions with the organization’s security policies can create a fairly comprehensive definition.

Summary of SANS guidelines indicates that an incident is an adverse event in an information system – includes the significant threat of an adverse event. In another word, it implies harm or the attempt to harm.

Summary of CERT guidelines [Reference 4] indicates an incident can be:

- 1) violation of an explicit or implied security policy
- 2) the attempts to gain unauthorized access
- 3) unwanted denial of resources
- 4) unauthorized use
- 5) changes without the owner's knowledge, instruction, or consent.

Incidents versus Events Types

What should be noted there is that an event can feed into an incident but the opposite is not true. However, when it comes to reporting an incident, one simple rule must be followed:

When in doubt, go ahead and report it.

The following are some sample scenarios to demonstrate the logic behind the distinction made between “Incidents” and “Events” under the computing scope.

1) Malicious code attacks

Event – User reporting that they might have been hit with a particular virus.

Potential incident – Their system exhibits behaviors typical for that particular virus.

2) Denial of resources

Event – User reporting that they can't access a service.

Potential incident – Many users reporting that they can't access a service.

3) Intrusions

Event – A system admin think a system was broken into.

Potential incident – A system admin provided the log indicating suspicious activities took place.

4) Misuse

Event – Web proxy log indicates an user has one hit to a porn site and company policies dictate that such activities are not allowed.

Potential incident – Web proxy log indicates an user has multiple hits to porn sites and company policies dictate that such activities is not allowed.

5) Unauthorized use

Event – User tumbled onto an undocumented game within a commercial program by accident.

Possible incident – User play the undocumented game within the commercial program and there exist a policy stating that game playing is not allowed.

6) Hoaxes

Event – User send an email containing false information usually associated with chain emails to the masses.

Possible incident – User send an email containing false information usually associated with chain emails to the masses asking them to do the same.

7) Information gathering

In organization where security is of utmost priority, these types of activities (port scan, war dialing and etc.) can be classified under incident types. However, in organization where security is of lower importance, such activities are usually tolerated and thus can be classified under event types. This sort of definition should be clearly defined in the company's security policy.

As illustrated above, the line between event and incident is a thin one and most often, asking further questions is the only way one can determine which side of line the issue should belong to. Typical questions that can be applied in these situations are listed under the Process and Procedures section below.

Incidents and Intrusion Detection

In a corporation where the Incident Handling function and Intrusion Detection function are distinct and are organized by team, alerts from intrusion detection system can be considered as events until some forms of verification has been performed by the intrusion detection team. Fortunately, logging is one of the core functions that an IDS can provide in such a way that verification of events can be easily obtained. In addition, IDS are often used to detect security violation and as a result, are more focus in incident determination scope.

There are five basic questions that should be answered when verifying event types reported by an IDS. Those are: Who, What, Where, When and most importantly, is the behavior contrary to the company security policies ?

Incidents and Virus/Trojan/Malicious Code Detection

Computer virus/trojan detection is one of the most well covered subjects in the field of information security. In addition, since virus/trojan infection is state-based, response to such an incident is often automated. However, it should be noted that virus/trojan detection software are not 100% foolproof in that most successful commercial products are not very successful at detecting unknown viruses/trojans. In situations where the virus scanner failed, the incident would usually be reported as an event falling under the malicious code classification.

It should be duly noted that recent attack trends point to the emergence of a new threat, that of malware, which combines techniques usually associated with viruses, trojans, worms, and other network-based attacks. As a result, the distinction between viruses, trojans, worms, and other attack techniques will soon disappear as detection products evolve to keep up with the new threat.

Process and procedures

Event documentation is extremely important when such an event becomes an incident. It is vital that the following information is recorded on such an event:

- Date
- Time
- Source of event report (Who or what?)
- Description of event

If the event itself was reported by an IDS, additional information should be obtained to assist in the incident determination process:

- The apparent source address(es) of the event
- The apparent target address(es) of the event
- The specific of the alarm(s)/alert(s) that were raised by the IDS
- The sensor(s) where the activities took place
- Time when the first alarm/alert was triggered
- Time when the last alarm/alert was triggered if applicable.
- Reverse DNS lookup using tool such as nslookup.
- Resolve the addresses using services such as whois from ARIN, APNIC, and RIPE
- “Compare activity against previous activity logs to see if the same source has been involved in other activities.” [Reference 7]
- “Assess whether the activity could have compromised your systems or was contained by the existing security controls in place.” [Reference 7]

The above information should be recorded in the event documentation and submitted as part of the incident documentation if this event turned out to be an incident. Note that in

the event of an incident that might lead to legal prosecution, it is not wise to perform direct reverse network activities such as ping or traceroute as it might alert the intruder.

The next step would be to determine if the event should be classified as an incident. Obtaining answers to these questions might provide a clearer picture of how to classify the issue:

- Is it a risk to data integrity ?
- Is it a risk to the availability of the resource ?
- Is it a risk to the confidentiality of the data ?
- Is the activity abnormal ? Is it a violation against company security policies ?

If the answer to one of the above questions is yes, it is probable to say the event is an incident and escalation to an Incident Response Team is required. However, in order to ensure a timely response, communication of such an incident would need to be as informative as possible. Listed below are some of the common terminologies that can be used to communicate the nature of the incident:

- Intrusion
- Unauthorized access
- Compromise of system integrity
- Theft
- Web site defacement
- Email Hoax
- Denial of resources
- Virus
- Trojan
- IP spoofing
- Email SPAM
- Unauthorized use
- Port scan
- War dialing
- Email bomb
- Buffer overflow exploit
- Repeated failed login attempts
- Unexpected network bandwidth consumption
- Unexplained system behavior
- Session hijacking

Lastly, it is very important to keep in mind that information regarding a security incident is highly sensitive and should be kept to a need-to-know basis.

Summary

Due to resource constraint, it is essential that the incident handling team is not caught up with chasing events while real incidents takes place. Junior security personnel can be adapted to filter out most of the false positives when it comes to incident handling. The above materials provide a starting point to train and educate new staffs on what constitute an incident.

References

1. Understanding Incident Response
URL: <http://www.fedcirc.gov/docs/understanding.html> (Sept 14, 2001)
2. Eric Cole, Incident Handling: Step-by-Step and Computer Crime Investigation
SANS manual for Advanced Incident Handling and Hacker Exploits Track
(August 2000)
3. Eugene Schultz, Effective Incident Response
Published by SANS (August 2000)
4. CERT/CC Incident Reporting Guidelines, Revision Jul 30, 2001
URL: http://www.cert.org/tech_tips/incident_reporting.html (Sept 14, 2001)
5. Jed Pickel & Roman Danyliw, Enabling Automated Detection of Security
Events that affect Multiple Administrative Domains, November 2000
<http://www.incident.org/thesis/book1.html> (Sept 14, 2001)
6. Taxonomy of the Computer Security Incident related terminology
URL: http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/i-taxonomy_terms.html (Nov 29, 2001)
7. OPERATIONS MANUAL Information Protection Centre
URL: <http://www.security-focus.com/cgi-bin/infocus.pl?head=Incidents:IPC&id=1454> (Sept 14, 2001)



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS SOS London 2009	London, United Kingdom	Jul 13, 2009 - Jul 18, 2009	Live Event
SANS Future Visions 2009 Tokyo	Tokyo, Japan	Jul 15, 2009 - Jul 17, 2009	Live Event
SANS IMPACT 2009	Kuala Lumpur, Malaysia	Jul 27, 2009 - Aug 01, 2009	Live Event
SANS SEC563: Mobile Device Forensics Debut	Baltimore, MD	Jul 27, 2009 - Jul 31, 2009	Live Event
SANS Boston 2009	Boston, MA	Aug 02, 2009 - Aug 09, 2009	Live Event
SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009	Washington, DC	Aug 17, 2009 - Aug 21, 2009	Live Event
SANS Atlanta 2009	Atlanta, GA	Aug 17, 2009 - Aug 28, 2009	Live Event
SANS Virginia Beach 2009	Virginia Beach, VA	Aug 28, 2009 - Sep 04, 2009	Live Event
SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009	Ottawa, ON	Sep 09, 2009 - Sep 10, 2009	Live Event
SANS Critical Infrastructure Protection at Oceania CACS2009	Canberra, Australia	Sep 10, 2009 - Sep 11, 2009	Live Event
SANS Network Security 2009	San Diego, CA	Sep 14, 2009 - Sep 22, 2009	Live Event
SANS SCDP Cutting Edge Hacking Techniques - June 2009	Ottawa, ON	Sep 15, 2009 - Sep 15, 2009	Live Event
SANS Rocky Mountain 2009	OnlineCO	Jul 07, 2009 - Jul 13, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced