

**A Summary of “Incident Response- A Strategic Guide to
Handling System and Network Security Breaches”
by Dr. Eugene Schultz**

**WRITTEN BY:
JOHN THOMPSON
5/16/2003**

Abstract

Over the past 5 years, I have been learning how to be an effective systems administrator and have learned many great lessons that I will take with me into future careers. One of the areas of knowledge I have gained is in the area of security, primarily around incident response. This knowledge has been useful in many ways, and is even more useful now that companies have decided to focus more on protection of their assets and information systems business processes for they now understand the value of down time and are taking a more aggressive approach to minimize it.

I have read the book “Incident Response- A Strategic Guide to Handling System and Network Security Breaches” by Dr. Eugene Schultz and I found it to be very insightful into the intricacies of how businesses need to handle security breaches and the methods and processes that go into preventing, protecting and restoring the confidentiality of their assets.

The following is a summary of the book, written for my fellow MIS students. I would like them to be able to get an overview of Incident Response and know the basic principles and processes without having to spend a semester reading and studying the text as I did.

An Introduction to Incident Response

What is Incident Response?

Incident: adverse events that threaten security in computing systems and networks

Main types of incidents:

- CIA: threaten the confidentiality of information, integrity or availability
- Reconnaissance: discovery of information used during attack. This would include port scanning, vulnerability scans, social engineering and an analysis of the physical location of the system.
- Repudiation: someone acting on behalf of someone else who takes an action and then denies doing so later.
- Harassment: bothering, embarrassing, threatening or intimidating someone.
- Extortion: attempting to receive benefits from the result of a threat.
- Pornography Trafficking
- Organized Crime Activity
- Subversion: where the intended system appears to function, but indeed does not. An example of which would be a trojaned logon screen.
- Hoaxes: incidents caused by dissemination of false information.

In short, incident response is the actions taken to deal with a computer security incident.

Risk Analysis

In the most fundamental sense, risk analysis is the means used to determine the quantitative value of the expected loss due to an incident.

The method used to find the quantitative value for the loss is usually done through the Annual Loss Expectancy (ALE). In short, the probability of an incident x expected loss due to incident = annual risk where (risk = probability x loss).

Qualitative risk analysis is done by determining a list of potential incidents and then assigning a categorical high, medium, or low value for the probability that the incident will occur.

Types of incidents (risk categories):

Break-ins: Unauthorized access to one or more systems in which the attacker masquerades as a legitimate user.

Unauthorized execution of programs or commands: The ability of an attacker to exploit a system and then run the programs of their choosing on the victim's machine.

Privilege escalation: Gaining privileges or increasing your current privileges without permission to do so.

Exploitation of CGI or ASP programs: The ability of an attacker to exploit design flaws in the programs that are being run through the web interface, CGI or ASP, whereby they are able to run rogue code, deface web sites, or access private files.

Denial of Service (DoS) Attacks: A remote attack on a host that causes the machine to stop functioning the way it was intended to function.

Virus and Worm Attacks: Self-reproducing programs that spread through user applications such as through infected macros, disk sharing, and email clients.

Malicious Active Content: Active web content such as ActiveX can be used to run without the user's knowledge to cause system crashes and capture sensitive data and return it to the web site without the user's knowledge.

Back Doors or Remote Control Programs: Methods (usually programs) set up on victim's systems to readily regain access when the attacker desires to.

Spoofing Attacks: Establishing a connection with a client to an unknown server by making the client appear to be a legitimate client.

Session Tampering Attacks: The attacker does something that allows the attacker to modify the packets in an existing connection.

Session Hijacking Attacks: An attacker takes over an already existing session, posing as the legitimate client.

Session Replay Attacks: The attacker rebroadcasts packets that were already transmitted (such as authentication sequences and credentials).

Methodology for incident response

The author recommends the six stage methodology for incident handling- which is the steps and actions taken after detecting a potential security breach.

1. Preparation

Be ready to respond to an incident before it occurs.

- Set up a reasonable set of defenses / controls based on the threat that presents itself
- Create asset of procedures to deal with incidents as efficiently as possible
- Obtain the resources and personnel necessary to deal with the problem
- Establish an infrastructure to support incident response activity

2. Detection

Without detecting an incident, there is nothing you can do to respond to it, making the rest of the incident response methodology worthless. There are two main things you need to do to detect an incident:

- Properly configure your security policies, audit logs, third party intrusion detection systems (IDS) and other system security so that there is data you can look at to determine if someone is trying to get in or has already compromised your system.
- Regularly monitor your logs and explore any anomalies you may come across.

Once you have determined that an incident has or most probably has occurred, you then should do the following:

- Take the time to analyze all anomalies
- Enable enhanced auditing to capture even more information
- Obtain a full backup of the system to use as evidence
- Document everything that happens and maintain a chain of evidence log where you list everything that is done to the system and who did it
- Report the incident to your boss

3. Containment

The purpose of containment is simply to limit the extent of the attack in an attempt to minimize damage or loss while balancing this desire with the understanding of the business processes and the associated costs. This is the hardest part for you need to determine the damage that is occurring, identify what the attacker could do in the immediate future, identify countermeasures, and then you need to balance the effects of the countermeasures on your existing operations with the damage that could be done by the attacker and then make a containment decision. It is generally safe to follow these principles:

- Gather as much information as you can about the incident
- Report it to your boss and find out where your boss thinks the cutoff should be for both business process interruption as well as maximum acceptable damage by the attacker
- Adhere to previously defined containment procedures
- Do not speak to press or people outside of the immediate “need to know” group
- Advise end users of the temporary disruption – if one exists- using a generic system down message approved by your boss

4. Eradication

Now that the incident has been contained, it is now time to eradicate the cause of the incident. The goal is to determine the cause of the incident. There are some good cause finding procedures for Unix and Windows starting on page 63 of the book. Once you have determined how the attacker compromised the system, blocked their access, and removed any backdoors, you are ready to move to recovery.

5. Recovery

The goal of recovery is to return any compromised system and or network device back to its normal mission status.

The basic principle is that you need to spend only as much “expense” discovering the cause as you can without exceeding the “cost” of simply re-installing a clean system and restoring the uncompromised and verified backup tapes.

6. Follow-Up

The goal is to review and integrate information related to an incident that has occurred. This stage is the most likely to be overlooked, however it is one of the most important steps because it is where you tie it all that happened and all that you learned together, better preparing you for the next incident.

- Review performance during the incident
- Discuss problems and ways they can be avoided in the future
- Create a final report of the incident that can be used for future reference

How to form and manage an incident response team

It is important to have a semblance of an incident response team in any organization. This team will vary in large organizations and smaller institutions. In a large organization it will be larger, more formal, and well structured; whereas in a small organization it may be a group of contract consultants who's expertise will be utilized in the case that an incident occurs.

Basically, you need to find out what your role is in any security incident and find out what your basic duties are. Then you need to identify your constituency- your team- and determine how you will communicate with them. You need to ensure that your team understands their role and how the team's objectives fit with the overall business needs.

Tracing Network Intrusions

Tracing network intrusions is the process by which you try to identify the IP Address, MAC address or hostname of the attacking system. This information is used to block future attacks, speak with the management group of the attacking system, or to pursue legal action.

Intrusion tracing techniques

Search engines may be used to find perpetrators who brag about their exploits. If your group has had their web site defaced, check alldas.org or www.antionline.org. You may also search for their IP address to identify who they are and who owns their web address. This may be done at www.arin.net. To find the IP address of all systems currently connected or communicating with your Windows system, type:

```
netstat -a -n
```

If you would like to use scheduler and dump the netstat text to a text file, this can be done by appending ">> textfile.txt" to the end of the netstat command.

Log Data can be used to identify the following:

- The start and end time of access
- The port number used to access the system
- The name of the task executed or command entered
- Attempts to change permissions
- Files accessed

Intrusion detection systems are very useful in identifying and blocking attacks. Additionally, they provide logging features which will give you more information about the actual attacks that were used against your system. For more information about the actual data the attacker was sending to your system you could use tools such as TCP Dump, Ettercap or Snort that records the apparent source of the IP Address and all packets that come from that host.

Constructing an “Attack Path”

During or after an attack, it is useful to determine the path an attacker took to your system. This is done through combining what you currently know with tools that will give you more information and finally through interpersonal communication with people up the river on the network. This is extremely difficult and usually fails because it is so difficult to get outside parties to assist because they either aren't interested or are afraid of legal ramifications.

The objective is to map out a physical path the attacker took to get to you. This can be done by using the previously described netstat command or log files to find the attacker's IP address. You then can use traceroute to backtrack to the attacker's IP address, identifying intermediate hops along the way. You can then look up the hops at www.arin.net and contact the administrators of those systems to request assistance and hope that they will look at their logs, block the attacker, or possibly trace from their location to the next hop. You can then contact that administrator and so on until you have a path to the actual attacker.

At this time, you would then want to contact their boss or their organization and share enough of what you know to give them enough information to determine if they want to do something about it. Don't give out too much information, for you may be speaking directly to the attacker. Additionally, don't be too rushed to charge in with guns blazing because more than 75% of the time, the incident will be caused by viruses, or their system is actually compromised and they, too, are a victim. This step is very complicated and hard to do, which is why most people don't trace the attacks unless mass damage or theft was conducted.

Closing Remarks

I hope that you have found this paper useful and that you, my fellow students, were able to learn a lot about Incident Response. This book has been very helpful to me in my job, and in understanding how businesses look at qualitative numbers when making tough decisions about what to secure, how to secure it, and on the spot decision such as when to allow an attacker to continue compromising the system or when to pull the plug and disrupt the business process. I hope you found this to be as helpful as I did, and that you will now have knowledge of Incident Response in a way that other MIS students will lack and that this will help you in your future career in MIS.