Global Information Assurance Certification Paper

Incident Handling Policies and Procedures: Prepare Now!
Aaron Fitton
GSEC v1.4b – Option 1

Abstract

Often the focus of security discussions revolve around issues like the buying, installing or setting up of firewalls, intrusion detection systems or other security technologies. Of lesser importance seems to be the planning, drafting and testing of detailed policies and procedures for incident handling. Yet, without these policies and procedures the large expenditures of time and money spent on establishing these defences are wasted.

At first glance some may see this as another expense consuming more valuable time and resources or as something that would never even be used. It is only after an incident has occurred that the value of advance planning and training is truly highlighted. Just like insurance no one likes to pay for it, but really appreciates it when it is needed. By examining the likelihood of an incident occurring and examining the steps of incident handling, I intend to establish the benefits of advance preparation but without having to experience the pain of a compromise.

Why do you need to prepare to be compromised? Quite simply because you will be compromised. It is only a matter of time. Why? Unless you are operating on an isolated computer network you are likely connected in some way to the Internet and thus are going to be probed and attacked. There are three factors to consider: Volume, Speed and Zero Day (0 Day).

1. Volume

The CERT Coordination Center is a major reporting centre for Internet security problems. The increase of reported vulnerabilities is obvious in their annual statistics(1). In 1999, there were 417 reported vulnerabilities. In 2000, that increased to 1090. In 2001, it again increased to 2437. The first two quarters of 2002 indicate 2148 reported vulnerabilities already.

The main goal of the Honeynet project (http://www.honeynet.org) is to try to demonstrate the activity of possible intruders. Let's look at an example. The honeypot used in this example was configured on a home network. As a result, this honeypot was on an effectively unused network with negligible traffic. There was not any significant traffic or any other behaviour to draw attention to itself such as many commercial or corporate sites would in their normal day-to-day operations.

The project showed an increase in unique scans going from 103 in May 2000 to 206 in February 2001 (2). The first is thing to note is the 100% increase in

activity. This helps us to see an increase in the number of vulnerabilities and a parallel in the attempts to find these vulnerabilities. Also demonstrated is that even a system that is effectively invisible on the Internet will be found and scanned.

We can see from these sources an increasing number of vulnerabilities and attempts to locate and exploit these vulnerabilities.

2. Speed

The speed with which a machine can be scanned and compromised can be quite shocking, not just in terms of the actual speed of the act, but also how quickly it can happen from the time when the system goes live.

Consider more interesting statistics from the Honeynet Project. The first involved default installations of Red Hat 6.2 server. These were attacked within three days of being connected to the Internet. The paper states:

"The fastest time ever... was 15 minutes. This means the system was scanned, probed, and exploited within 15 minutes of connecting to the Internet."(2)

Another machine was hooked up to the Internet, this was a Windows 98 machine. In this case, not only was it compromised within twenty four hours, but over the next three days, it was compromised an additional four times. Remember as well from the previous example that a low profile system will eventually be found and scanned.

These examples help to highlight the speed with which machines connected to the Internet are targeted and potentially compromised. There is no grace period. It is not safe to think that your system will not be found and scanned because it is has only recently been activated.

3. Zero Day (0 Day)

Robert Graham's Hacking Lexicon defines Zero Day as "…an exploit that is not publicly known. It describe [sic] tools by elite hackers who have discovered a new bug and shared it only with close friends."(3)

There are always new exploits. It takes time to identify them and to build a defence against them. Until an exploit has been identified and a defence is devised, you are vulnerable. An example of this is anti-virus tools. Most rely on definitions to identify malicious code. When a new virus is released, the anti-virus companies will obtain a copy of it. They then analyse it, develop a way for their scanners to identify it and hopefully, a way to block or remove it. All of this takes time. In the meantime you are potentially vulnerable.

Combining all three factors, volume, speed and Zero Day, an inevitable conclusion is reached. You will experience a compromise. Clearly a plan to deal with this should be in place.

You can manage the risk associated with a compromise by creating incident handling policies and procedures. These can help in reducing any potential damage you face as a result of the compromise or the resulting investigation. It gives you a chance to eliminate potential errors in the investigation process before they become critical. This means that you do not to have to simply accept the damage caused by an incident, you can actively work to manage it ahead of time.

To start with, let's establish the basic steps to incident handling. There are six basic phases of incident handling(4). They are:

Preparation
Identification (some call it detection)
Containment
Eradication
Recovery
Follow-up

It is beyond the scope of this paper to give a complete and total breakdown of each of these phases. Rather, the focus is to help the reader to see the positive impact of advance preparation in each of these potential areas. Each organization can then generate its own recommendations based on its own situation.

Preparation

This is the key point. As such, I will continue with a simple listing of what activities are included in the basic steps of incident response and then return to this step.

Identification/Detection

Key elements of identification/detection include:

- The definition of an incident.
- The layout and effectiveness of your defences. This would include how you have deployed your NIDS or HIDS. What is your rule set for your firewall? What will trigger alerts?
- Steps of the chain of custody.
- Who is responsible for leading the investigation?

It is important that you have defined ahead of time what constitutes an incident and the procedures for identifying it. You do not want analysts to be issuing

unnecessary alerts over every event that happens, but you do want them to have guidance as to what events should always generate an alert. This will help to avoid the "boy who cried wolf" syndrome. Now as with most security related issues there are few hard and fast rules. Guidance for this definition is essential. As well, you want to provide procedures on how to issue alerts and to whom. For example: If you want to ensure that certain areas of your organization receive a more detailed warning, then be sure to document what additional information needs to be provided, who needs to receive it and how quickly they need it.

It is very important to identify who is responsible for an investigation. There can only be one captain of a boat. The same is true of an investigation. Time could be wasted and key procedures missed while people try to decide who is in charge. Avoid this by having it clearly documented ahead of time.

Containment

Key elements of containment include:

- Secure the area immediately.
- Collect any volatile information.
- Make backups of affected systems and work from these.
- Prevent any continued intruder access.
- Determine if the system needs to come off the network or be shutdown.
- Regain control of the system.
- Determine the scope and impact of the incident.
- Obtain help if needed.

Improvement in the area of containment can be derived from pre-determined and documented procedures. By providing a checklist you can ensure that the incident responder does not miss a crucial step. This document can include basic steps such as ensuring that backups are made, that compromised passwords are changed, how to bring down the system and how to document these actions, who can be contacted if assistance or guidance are needed and how it is decided if the systems should be pulled from the network.

Tools for these processes can be assembled in advance. This takes time and research. A good suggestion is to look on the Web and see what tools others have used. An excellent example is W2K First Responders Kit by H. Carvey(5). After determining what tools are appropriate for your environment, you then need to ensure that staff knows how to use them properly. Training on how to use these tools and the proper procedures to follow is an essential and ongoing need.

A final and seemingly obvious step is to ensure that the tools and the procedures for using them are readily available. Well thought out toolkits and procedures will be of no benefit if the only copies you have are on the server that has just gone down. Assembling a jump bag with all the necessary equipment, tools and

documentation ahead of time, can help to ensure that things go smoothly when an incident occurs. Having the steps for these types of things worked out in advance will help an investigation run smoothly.

Eradication

Key elements of eradication include:

- Ascertain the cause. This will mean looking through all sources of information available (firewalls, routers, IDS, compromised systems, etc.).
- Determine what the intruder did (read email, installed a network sniffer, etc.).
- Identify how to correct the problems (install patches, change permissions, etc.).
- Check system to ensure there are no other problems (another vulnerability that was not used, but is present).
- Double check that all methods used to gain access are identified and corrected.
- Check connected systems to make sure they have not been affected too.
- Do not put a system back online until the problem has been fixed.
- Preserve all relevant information.

During an investigation, valuable time will be consumed and mistakes will be likely if the following questions are not addresses ahead of time: Where would the handler find the appropriate contact information if he suspects that another system has been compromised but is in a different department then he is investigating now? Is an up-to-date vulnerability scanner available? Is there a clear explanation of what information needs to be recorded and how it is to be preserved?

Recovery

Key elements of recovery include:

- Determine when the system needs to go back online. The importance of the affected system will have a bearing on this.
- Restore from a trusted backup. Additional verification may be necessary to ensure backups were not compromised.
- Monitor closely for reoccurrence.

When drafting incident handling policies and procedures consider, is it clearly identified where and how to get the backups? Is there a protocol for how to continue to monitor a restored system? What tools should be used to verify the backup's integrity? Reducing the amount of extra work that occurs during an investigation will be beneficial.

Follow-up

Key elements of follow-up include:

- Complete all documentation required.

- Identify areas of improvement in processes, tools, policies, documentation etc.
- Have a wrap up meeting to review.
- Enact needed changes.
- Submit report and recommendations to management.

Instead of thinking of this as the end of an incident, it is better to view it as the restarting of your preparation phase. Having identified where things worked well and where they need improvement, you can continue to develop your documentation and procedures. Without regular review and updating, documentation and procedures quickly become outdated and ineffective.

Preparation

This is one of the most important areas. Pay now and save later. Pay now by planning, drafting and testing detailed polices and procedures for incident handling. Do your work now, when you have the time as opposed to when an incident occurs and you are under pressure and time constraints. You could view it this way: If you have a bill that you have to pay. Would you rather pay it now when you have the money or would you rather put it off until later and then borrow the money to pay it? No matter which way you choose you still have to pay the bill. Yet, by waiting until you no longer have the money to pay it, you now incur the additional expense of having to borrow the money, providing funds are even available. The same is true with incident handling, you will have to pay at some point. Why not do it now, when you are more likely to be able to afford it?

Each organization will have its own priorities. Some will want to recover and move on from the incident. Others may want to follow up the investigation with possible legal action. This means that documentation and evidence preservation is critical.

Consider the differences between these two scenarios. The following are not an exhaustive list of steps, rather they are sets of simplified steps for dealing with an incident. The first is the “protect and forget” method. The second is the “apprehend and prosecute" method(6).

“Protect and Forget”(6)
- Decide if the incident is real.
- Stop the current intrusion.
- Determine when and how access was gained.
- Were any other systems compromised?
- Restore from an uncompromised backup.
- Secure systems from the method of attack and any other vulnerabilities discovered.

- Document the steps taken.
- Review processes and learn.
- Submit report to management.

"Apprehend and Prosecute"(6)

- Decide if the incident is real.
- Inform appropriate authorities.
- Document all actions taken. Specifically this would have to include the precise date, time and who was present.
- Isolate compromised systems from the rest of the network.
- Discover the identity of the intruder while documenting his or her activity.
- Determine the method of attack, when it was initiated and secure all uncompromised systems.
- Stop the current intrusion once enough evidence has been gathered or if key systems are endangered.
- Document the current state of compromised systems.
- Restore from an uncompromised backup.
- Secure systems from the method of attack and any other vulnerabilities discovered.
- Document the steps taken. Include cost estimates and man-hours involved.
- Secure all evidence, from the obvious (logs, network traces etc.) to the less obvious (your notes, emails reporting the initial problem, etc.).
- Review processes and learn.
- Submit report to management.

These simple lists clearly demonstrate how different the processes are. A handler should not have to guess at which method to follow while investigating.

Documentation is essential and the timing of certain events, such as when to disconnect an intruder and how logs, et cetera, are stored, need to be handled in a specific manner. These are all decisions and processes you want to make and document ahead of time. Determining policies in advance will guide the incident investigation in the method desired by management.

Let's look at a scenario of what could happen if incident handling polices and procedures are not defined.

You receive a call from a local university. They are calling to tell you that they detected an attempted compromise on one of their web servers by a machine from your organization. They had just recently set-up their intrusion detection system and it had almost immediately caught this compromise. They want to make you aware of the situation and as well to see if your investigations can turn up any evidence of intrusions prior to the set-up of their IDS. Already you are faced with a decision. What information can you share with them? Would you be placing the company at legal risk?

You start your investigation. It appears that at least one of your machines has been compromised. You ask yourself, "Should I inform law enforcement? What type of documentation will I need? Is it good enough if I just keep track of what I do?"

The attacker appears to still be connected. Do you want to disconnect them immediately? If you disconnect them immediately will you have enough evidence to establish who they are and what they are doing? Will you have sufficient and legitimate evidence for legal action? Is this system important enough to require immediate action or can some time be spent learning what the intruder is doing after having isolated this system from the rest of the network?

As you start your analysis you take some brief notes on how you have found the system.

- The ps command does not seem to work correctly.
- There appears to be extra user accounts.
- The reported amount of disk usage does not seem to be correct.
- It appears that the intruder used a BIND vulnerability to gain access and then ran a rootkit.

Will these notes be detailed enough? As you work at restoring the system you continue to take notes.

- Analysed logs from firewall and compromised system.
- Intrusion appears to have occurred two weeks ago.
- Restored system from backups made two weeks ago.
- Verified restored system was not already compromised.
- Upgraded to latest version of BIND.
- Sent an email outlining the problem, when and how it occurred and how it was fixed.

Should you save those firewall logs you used? Should you make mention of the three hours you had to spend looking for an administrator to get the backup tape you needed?

By following this you start to see what kind of problems you can run into by not having clearly defined policies and procedures in advance. If certain actions are not taken at the time of the incident, it could be too late afterwards. Some of the questions that you could have faced are:

- What information can you share with outside organizations?
- Would you be placing the company at legal risk?
- Should you involve law enforcement?
- What type of documentation is needed?

- Should you disconnect an intruder immediately?
- Can you identify the intruder? Do you need to?
- Do you need to preserve the logs and files you used to investigate the incident? How do you do this? Does it matter where and how these are kept?
- Do you need to account for all time spent?

Time is essential during an incident investigation. If you prepare now you can save later. At what point, do you think time is more valuable, before an incident when it can be scheduled or during an incident when it moves relentlessly forward and all you can do is respond? When do you want to spend your valuable time making decisions? Do you want to have to second guess your decisions as you go? What if the "protect and forget" method is followed and then management comes to you looking for evidence as it believes that a competitor may have been behind the attack and they want to try to take legal action against them? How do you think that management is going to react when they find out that you did not preserve enough evidence? If the company policy was to always have enough evidence gathered in case the need for legal action ever arose, then the damage may have been minimalized.

Or what if you decide to follow the "apprehend and prosecute" method and involve law enforcement? The next day after the story is broadcast on national news and the company stock dives 25% you are called into a meeting with management to explain why you decided to make this information public. If the steps to be taken had been clearly laid out in advance the organization would have had the opportunity to decide that it is preferable to avoid adverse publicity than to catch who was responsible for the intrusion.

Advance planning cannot solve all problems. There are always downsides no matter what advance work is done. It can though, allow an organization to at least work toward the methods and solutions previously approved for responding to incidents. This can help to minimize the damage done by a compromise.

Conclusion

It cannot be denied that you will be faced with a compromise at some point when you consider the following factors:

1) **Volume** - An increasing number of vulnerabilities and attempts to locate and exploit these vulnerabilities.
2) **Speed** - The speed with which machines connected to the Internet are targeted and potentially compromised.
3) **Zero Day** - New exploits that need to be identified and a defence against devised.

From this conclusion you can work to build on the value of your security investments by designing clear incident handling polices and procedures in advance. This advance planning will help you to minimize damage from a compromise by enabling incident handlers to react quickly in an approved method.

Written policies and detailed procedures will go a long way in helping to prevent mistakes and wrong decisions during incident handling. Some of the potential benefits are:

- Quick and sure actions to contain the spread of damage to valuable data by ensuring that additional systems are not compromised.
- Legal liabilities are reduced by ensuring that all steps of the process have been assessed and approved by your legal advisors.
- Knowing what information will be made public and what will not, will prepare you to manage any damage to your organization's reputation.

It is evident that there are substantial rewards for creating and implementing detailed incident handling policies and procedures in advance of a compromise. If organizations expend the time and resources to create, test and regularly update these policies and procedures now, they will maximize their expenditures in security.

1 CERT/CC. "CERT/CC Statistics 1988-2002" URL: http://www.cert.org/stats/ (26 Sept 2002).2 The Honeynet Project, "Know Your Enemy: Statistics" 22 July 2001. URL: http://project.honeynet.org/papers/stats/ (26 Sept 2002).

3 Graham, Robert. "Hacking Lexicon" version 0.7.0, 11 Nov 2001. URL: http://www.robertgraham.com/pubs/hacking-dict.html#0-day-exploit. (26 Sept 2002)

4 E. Cole, K. Kolde, C. Wendt. "SANS Security Essentials II: Network Security." Information Assurance Foundations. Version 1.3. The SANS Institute, 2001. P. 4-1 – 4-23.
5 Carvey, H. "Win2K First Responder's Guide". 05 September 2002. URL: http://online.securityfocus.com/infocus/1624. (20 Sept 2002)
6 Adler, David and Grossman, Kenneth L. "Establishing A Computer Incident Response Plan." Data Security Management. December 2001. URL: http://www.fedcirc.gov/docs/82-02-70.pdf (23 Sept 2002)
Kossakowski, Klaus-Peter et al. "Responding to Intrusions" Security Improvement Module CMU/SEI-SIM-006. February 1999. URL: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim006.pdf. (23 Sept 2002)CIT. "Incident Handling Guidelines." 06 June 2002. URL: http://irm.cit.nih.gov/security/ih_guidelines.html. (22 Sept 2002)
Lee, Rob. "Incident and Wiretap of a Real Case." 14 June 2000. URL: http://www.incident-response.org/incident.doc. (26 Sept 2002)
Lee, Rob. "Unix Forensics Techniques for Incident Response." 12 Dec 2000. URL: http://www.incident-response.org/incidentresponse.ppt. (26 Sept 2002)
CERT/CC. "Establish Procedures and Policies for Responding to Intrusions." URL: http://www.cert.org/security-improvement/practices/p044.html. (Sept 26 2002)