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.

# Mining gold... A primer on incident handling and response

Copyright SANS Institute
Author Retains Full Rights

AD

© SANS Institute 2003, Author retains full rights.

# Mining gold... A primer on incident handling and response

*GCIH Gold Certification*

Author: Stacy Jordan, stacyjordan@juno.com

Adviser: Jim Purcell

Accepted: September 13, 2007



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Table of Content

1. Abstract ..... 1
2. Introduction ..... 1
3. Key Definitions
   3.1 Security breach ..... 7
   3.2 Event ..... 7
   3.3 Incident ..... 7
   3.4 Attack ..... 8
   3.5 Target ..... 8
   3.6 Security incident .....8
   3.7 Difference between an event and incident ..... 9
   3.8 When does an event become an incident? ..... 10
4. What is incident handling? ..... 13
   4.1 Why is it important? ..... 14
   4.2 How are incidents detected? ..... 15
   4.3 Whose responsible for handling incidents? ..... 20
5. Incident handling process ..... 21



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

5.1 Preparation phrase ..... 23

5.1.1 Management support of incident handling capability ..... 24

5.1.2 Incident response (handling) team ..... 25

5.1.3 Types of computer incident response teams . 26

5.1.4 How does an incident handler interact with law enforcement? ..... 29

5.2 Identification ..... 30

5.3 Containment ..... 30

5.4 Eradication ..... 31

5.5 Recovery ..... 32

5.6 Lesson learned (follow-up) .....33

6. How to build a successful incident response team

6.1 Staff skill set .....34

6.2 IRT cost considerations .....39

7. Tools and resources for supporting the work of incident handlers .....42

7A. Forensic analysis tools .....43



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

7A.1 Unix disk imaging tools .....44

7A.1.1 Windows disk imaging .....46

7A.1.2 Linux and Windows Live cds .....48

7A.1.3 Snort used for forensic .....53

7A.2 Examining systems and process .....54

7A.3 Port scanning .....55

7A.4 IPv6 network incident handling .....57

7B. Incident handling resources .....-
58

8. Summary .....60

9. Appendix section

Appendix A: Online tools and resources .....62

Appendix B: Frequently asked questions .....66

Appendix C: Instruction on creating a live multi-session
DVD .....71

10. References .....78



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## 1. Abstract

Incident handling and response is a key area in the IT security arena. As a part of the GIAC GOLD program, several outstanding papers on the subject have been generated. This paper has collected information from those papers to serve as basic for future research. Topical areas in the paper include: defining what a incident is, incident handling process, how to create a computer incident response team and tools/resources for supporting incident handlers.

## 2. Introduction

When you look in the Javvin.com dictionary of information, computer and network security terms it defines incident handling as an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods and other security-related events (2007). Besides those events, educational institutions and government have to deal with non-traditional events as well i.e. cyber stalking, child pornography and copyright violation. Unfortunately, all types of organizations have experienced a variety of negative security activities i.e. breaches, malware, virus outbreaks, stolen data from hard drives and laptops over the past couple of years. At my agency, we've experienced two security breaches and notified the public about



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

1 more in another government agency in the past two years as well. It doesn't matter the size of the business, having a plan and personnel to resolve an incident is key. Even with the right plan and an incident response team, the proper tools and resources to perform the task is vital as well.

One of the best places to find information on incident handling and response is CERT located at Carnegie Mellon University in Pittsburgh, PA. CERT contains guides on creating a computer incident response team, research security vulnerabilities and offer security policy advice. Another excellent resource is National Institute of Standards in Technology's (NIST) and their computer security incident handling guide. This guide talks about how to create an incident response capability, 6 steps for handling an incident and offer specific guidelines for handling denial of service, malicious code, inappropriate usage and unauthorized access security incidents. A great resource for higher education institution is EDUCAUSE. According to their website, EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology (EDUCAUSE, 2007). Even with these other places for security research, SANS through its various research projects and GIAC gold program has some of the best information on



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

incident handling. Now, let's begin to define key terms in the incident handling arena.

## 3. Key definitions

### 3.1 Security breach

- Businessdictionary.com defines a security breach as an external act that bypasses or contravenes security policies, practices, or procedures (2007).

### 3.2 Event

- An event is an observable occurrence in an information system that actively happened at some point in time (Pham, 2001). Type of items that are considered events include: phone call, system crash or request for virus scan to be performed on a file or attachment (ditto).

### 3.3 Incident

- An incident is defined by the particular organization in question. But, combining the following generic definition with the organization's security policies can create a fairly comprehensive



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

definition (Pham, 2001). 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 applies harm or the attempt to harm (ditto).

### 3.4 Attack

- An assault on system security that derives from an intelligent threat, i.e. an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. Attack can be active or passive, by insider or by outsider or via attack mediator (Arvidsson, 1998).

### 3.5 Target

- A computer or network logical entity (account, process or data) or physical entity component, computer, network or internetwork (ditto).

### 3.6 Security incident

- A *computer security incident* is a violation or imminent



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

threat of violation of computer security policies, acceptable use policies, or standard security practices. (Scarfone & Grance & Masone, 2007)

### 3.7 Difference between an event and an incident

Before I define what the difference is between an event and incident in words, take a look at the following figure.

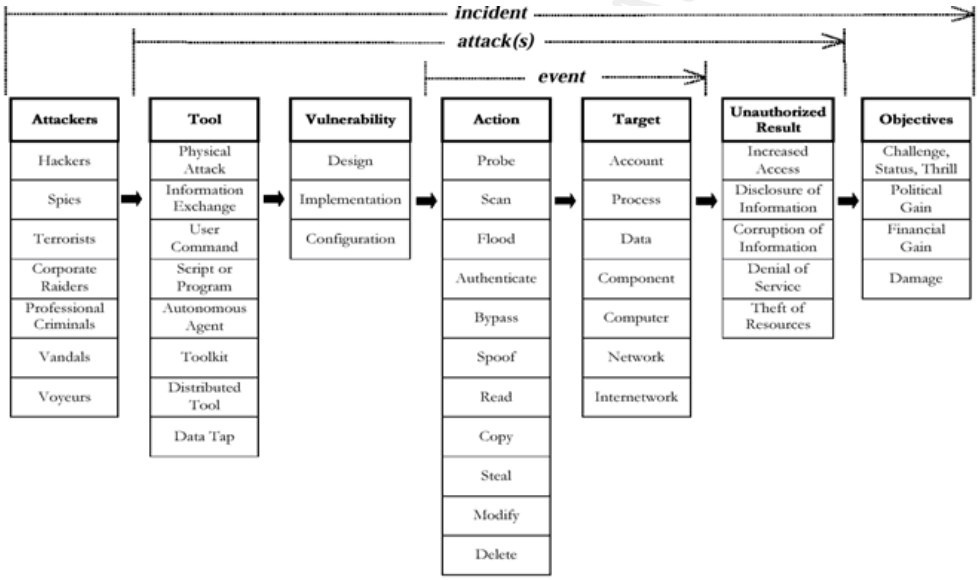


Figure 1-Computer and Network Incident Taxonomy



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Figure 1 presents a matrix of possible attacks. Attacks have five parts which depict the logical steps an attacker must take. An attacker uses a *tool* to exploit a *vulnerability* to perform an *action* on a *target* in order to achieve an *unauthorized result*. To be successful, an attacker must find paths that can be connected (attacks), perhaps simultaneously or repeatedly (Howard & Longstaff, 1998). Therefore, an event is an action on a particular target (i.e. stealing domain administrative account password). On the other hand, an incident is classified as a hacker using stolen account password from an e-commerce web server to get credit card numbers. What should be noted is that an event can feed into an incident but the opposition is not true (Pham, 2001).

### 3.8 When does an event become an incident?

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.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**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. (ditto).

Depending on how important information security is to an organization, will determine how an event becomes a security incident. For the State of Georgia, an incident can be classified as either computer security or criminal in nature. Computer security incident is defined as an incident that's a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. While criminal incident is when an employee or contractor downloads or access child pornography or any other criminal activity (GTA, 2005).

The following is how GTA defines an event and incident for all state agencies:

1) Event of Interest



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- In-bound traffic blocked at firewall that appears to be a directed attack
- Cluster of several PC's infected with the same virus/worm, but still requiring minimal cleanup
- Excessive or targeted spam leaking past existing filters
- Ad-Ware that affects normal machine operation or contains spy ware
- Novel or directed Phishing attack to agency employees
- Inadvertent unintentional infraction of accepted policy

2) Event of Concern

- Direct attack on firewall itself, but without success
- Large virus/worm infection or propagation by new vector
- Internally propagating virus/worm
- Repeated or serious infractions of accepted use policy
- Downloading or accessing adult pornography

3) Security Incident

- Penetration of firewall
- Compromise of any server, including Web server defacement



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Compromise on loss of data on server
- Infractions of accepted use policy that [is] flagrant or extreme
- External propagation of virus/worm (ditto).

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 the line an issue should belong to (Pham, 2001).

## 4. Incident handling

Incident handling is a generalized term that refers to the response by a person or organization to an attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster (Cook, 2000). It typically involves incident analysis, evidence collection, tracking the origins of the intruder, response support for the victim(s) of the attack and coordination among other [incident response team] (IRT), administrators and service providers (Proffitt, 2007). Another term that used in concert with incident handling is incident response. According to whatis.com, incident response is an organized approach to addressing and managing the aftermath of a



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs (2007). Furthermore, incident response normally represents some form of intervention to negate or minimize the impact of the incident. Actions can be initiated by either humans or computer systems (Shultz and Shumway, 2001). For the purpose of this paper, will be using incident handling and incident response interchangeably.

### 4.1 Why is incident handling (response) important?

No matter how well your network is protected, eventually there will be an incident that you are not prepared to handle by yourself (Borodkin, 2001). Incident response has become necessary because attacks frequently cause the compromise of personal and business data (Scarfone & Grance & Masone, 2007). Due to the nature and amount of business being done through the Internet, minimizing security vulnerabilities and responding to security incidents in an efficient and thorough manner can become critical to business continuity (Osborne, 2001). Another way to look at the need for incident handling is unless you know your organization from top to bottom, making a list of all possible services needed after an attacker



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

compromise your environment can be an insurmountable task (Hall, 2003).

To address these threats, the concept of computer security incident response has become widely accepted and implemented in the Federal government, private sector, and academia (Scarfone & Grance & Masone, 2007). Effective incident response is in tune with an organization's security objectives so that the infrastructure established for incident response and the particular procedures put in place reflect the relative importance of each of the security goals for that organization (Schultz and Shumway, 2001). Later in this paper, will discuss in detail the methodology used to handle a computer security incident.

**4.2 How are incidents detected?**

It should be noted, that incidents are captured in a variety of different ways (ie. hardware, software, system logs, etc.) On the hardware side, an intrusion detection system (IDS) is one of the most popular methods. An IDS can be categorized into two types: host and network based. A host-based IDS (HIDS) involves loading a piece or pieces of software on the system to be monitored. The loaded software uses log file and/or the system’s auditing agents as sources



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

of data (Zirkle, 2007). Best known HIDS include commercial products from Cybersafe, ISS and TripWire. To give you an overview of what a commercial HIDS can provide, will discuss the general features of Tripwire version 7.

The makers of Tripwire have two versions of their product: enterprise and server. Like the name suggests, enterprise version enables configuration auditing and control by detecting all change across the IT infrastructure, automatically correlating change with multiple acceptance criteria and generating actionable change reports. Tripwire Enterprise detects and analyzes changes to millions of elements (e.g. files, directories, registry settings, directory server objects, and configuration files) on servers, databases, network devices, desktops and directory servers. It improves configuration control by alerting you of any change and enabling quick remediation (TripWire, 2007). Server edition of the product is suitable for server / desktop configuration monitoring; has the ability to roll back the desktop or server to a known and trusted state if necessary (ditto).

In addition, they're several open source HIDS which include Aide, Samhain and Osiris. But, the most popular open-source HIDS is OSSEC. From its web-site, OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

powerful correlation and analysis engine, integrating log analysis; file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows (2007). Recently, OSSEC was updated to version 1.4 and has about 5,000 downloads/month.

Network based IDS can gather data from its sensors/systems and process this data on a central host (Shultz and Shumway, 2001). One of the most used network-based IDS is SNORT. This product is open-sourced and has a large user based as a result. Sourcefire recently updated the version to 2.8 and it's capable of performing real-time traffic analysis and packet logging on IP networks. In addition, can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts and much more (Sourcefire, 2007).

Also, Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Windows clients using Samba's smbclient (ditto). Snort has a variety of plug-ins that further assists incident handlers in doing the job effectively. I will talk about a couple of Snort plug-ins (barnyard, SQUID) in the tools/resources section of the paper.

Another way to detect incidents is through software. One of the most common software is virus detection. Major vendors in this space include Mcafee, Norton, Grisoft and F-prot to name a few. These same companies also produce personal firewall software. This allows home users to block or allow access to the Internet or specific ports from their workstations in order to prevent intrusion for outsiders. Microsoft has been installing firewall software in their operating system since Windows XP and their latest version is called Windows Defender for Vista operating system. I personally use Zone Alarm from CheckPoint and it allows me to restrict which programs have access to the Internet. Further, provides notification when a program tries to access the Internet for the first time or use a strange port it does not recognize.

These personal (desktop) firewalls may be used in combination with hardware units on a corporate network. Examples of hardware firewalls include Cisco Pix, CheckPoint NG-1, Netscreen 5-G and Nokia IP560. GTA have a variety of hardware devices on the local and enterprise (state) backbone. These devices range from Cisco Pix 500



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

series (515 and 535) to Nokia IP560. In addition, we have implemented Netscreen 5-GTs to several law enforcement agencies so that they're in compliance with FBI (NCIS) encryption standards (SSL-IPSEC). Enterprise class hardware firewall devices don't just have a single purpose but added functionality like unified threat management (UTM), virtual private networking (VPN) and securing voice over IP (VoIP). An alternative to detection software and hardware is setting up a honeypot.

According to Wikipedia, honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated, (un)protected and monitored, and which seems to contain information or a resource that would be of value to attackers (2007). They're several different types of honeypots including honeyd, spam honeypots, email trap and honeynet.

From "honey pot systems explained" by Loras Even, honeypots can be setup inside, outside or in the DMZ of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes. In a sense, they are variants of standard Intruder Detection Systems (IDS) but with more of a focus on information gathering and deception (2007). The figure below



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

illustrates a honey pot system installed in a traditional Internet security design:

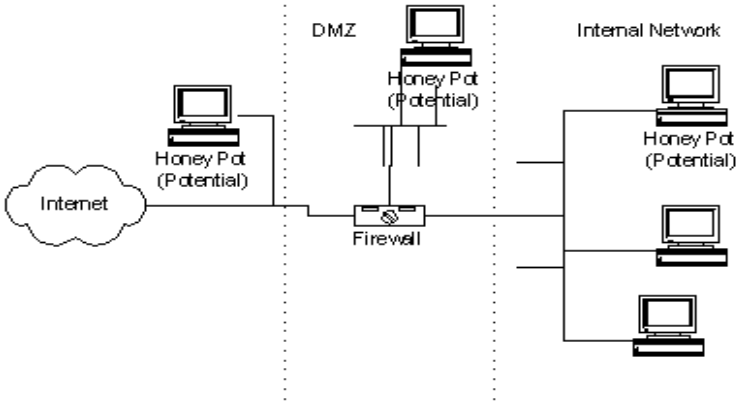


*Figure 2: Honeypot design for internet (Even, 2007)*

Even with all the detection methods, the system is only as good as the current revision or software patch. The only exception is a honeypot were ensuring it is away from the production network is key.

**4.3 Whose responsible for handling an incident?**

Most people would assume that only the organization's IT staff is responsible for handling an incident. Successful incident response efforts are usually multidisciplinary efforts that involve a range of participants with a variety of skills (Schultz and Shumway,



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2001). A list of individuals who would handle an incident may include but not limited to:

- Human resources
- Management
- Legal
- Team lead
- Auditor
- Security staff
- Risk manager

These same individuals can be members of your incident response team and before I talk about incident response team, will discuss the six-step process (methodology) to handling an incident.

## 5. Incident handling process

So far, I've defined several terms used to describe a security event and incident. In addition, I've provided examples of hardware and software components that could be used to detect incidents on a network. Now, I'll go into detail on the methodology used by incident handlers to handle an incident. The incident handling process has 6 phases: preparation, identification, eradication, recovery and lesson learned (follow-up). These phases provide the "gameplan" for any size incident response team (IRT) to properly



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

mitigate an incident in a timely fashion. The SANS Institute created a step-by-step guide entitled *Computer Security Incident Handling* that detailed each phrase of the incident handling process. Understanding these stages and what can go wrong in each, facilities a more methodical response. Also, it helps in avoiding duplication of effort and assist with dealing with unexpected aspects of incidents (Northcutt, 2003). In a presentation given by Shinil Hong of the University of Buffalo-State University of New York, he illustrated the six phrases of the SANS model in the following way:

*Figure 3--SANS 6-step incident handling methodology*

As you can see, preparation phrase is the catalyst for the other phrases in the incident handling methodology.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**5.1 Preparation phrase**

This phrase allows the incident handler to verify and ensure that the proper tools and personnel are in place when the call is made to declare a network security incident. In addition, it is an excellent opportunity to train less experienced members of the incident response team and practice your incident handling response. When discussing the skill sets required to be successful, incident handling has often been compared to emergency medicine. Both are usually performed in a highly stressful environment and require quick thinking and a calm presence. The amount of preparation you do before an event occurs is the most important factor in determining how successful you can handle an incident (Murray, 2007). SANS has broken down this phrase into 9 steps and besides the ones mentioned above, other steps in the preparation phrase are as follows:

- Select incident handling team members and organize the team
- Develop management support for the incident handling capability
- Develop an emergency communication plan
- Provide easy reporting facilities
- Establish guidelines for inter-departmental cooperation



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Pay particular attention to relationships with system administrators
- Develop interfaces to law enforcement and other computer incident response teams (CIRTs)

At this time, I will go into detail on a few steps in this phrase. In particular, I will discuss the following 3 steps: management support for incident handling, types of incident handling team and interacting with law enforcement.

### 5.1.1 Management support for incident handling

It goes without saying that management support of incident handling and CSIRT is a must. Management provides the funding, approval of staffing and the necessary authority to make high-level decisions (i.e. network shutdown, consulting law enforcement, etc.). These types of decisions often require consultation and senior management agreement, so the team will need these people on your side early in this process (Theunissen, 2001). An example of the need for management support is when the IRT may need external support. External support costs money and takes time and effort to select partners (ditto). Management can allocate the necessary resources up front so that if the CIRT needs to engage others, the process is already there. The incident handling process will end up being a



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

very 'woolly' procedure if you can't get management to agree formally to a robust structure and to make some important decisions up front (ditto).

### 5.1.2 Incident response (handling) team

Most individuals first thought would be that having a dedicated team to handle incidents isn't necessary. Even some management personnel in many organizations feel that such a team is an unnecessary corporate expense. Without such a team in place, [when and not] if an incident where to occur, how would it be handled within the organization, who would coordinate these efforts and ultimately be responsible for following through with incident resolution and return to business (Hall, 2003). According to CERT, there are a wide variety of acronyms for incident response teams that exist around the world. Some of the more common include:



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

| | |
|---|---|
| CSIRT | Computer Security Incident Response Team |
| CIRC | Computer Incident Response Capability |
| CIRT | Computer Incident Response Team |
| IRC | Incident Response Center or Incident Response Capability |
| IRT | Incident Response Team |
| SERT | Security Emergency Response Team |
| SIRT | Security Incident Response Team |

For the purpose of this paper, the following acronyms will be used: CSIRT, CIRT and IRT. A CIRT is a carefully selected and well-trained group of people whose purpose is to promptly and correctly handle an incident so that it can be quickly contained, investigated and recovered from (Borodkin, 2001). The primary function of a CSIRT is to react in a timely fashion, to intrusions, types of theft, denial of service attacks and many other security events (CERT, 2007).

### 5.1.3 Types of incident response teams

IRTs can be divided into a variety of different categories which may include but not limited to the following:



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Coordination centers
- Internal
- Analysis centers
- Incident response providers
- National

Organizations may interact with a number of different IRTs because of their line of business. For example, GTA network operation and security center (NOSC) interact with several IRTs each day via our abuse.state.ga.us list serve. NOSC receives reports of security events and incidents from incident response provider (vendor) IBM ISS, internal (specific agency IRT, analysis center (REN-ISAC), national (CERT-BR: Brazilian CERT) on a daily basis. At this time, will discuss two of the most common CIRTs: public and internal.

A public IRT can be defined as providing localized assistance for their own constituencies and typically draw on funding provided by some form of fee upon their entire constituency (Forno, Van Wyk, 2001). Each IRT service offerings vary, but the core services include the following:

- Technical and procedural guidance to sites affected by an incident
- Vulnerability reporting, analysis, tracking and advisory distribution



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Statistic gathering, analysis and report
- Training programs (Forno & van Wyk, 2001)

Public IRTs may interact with coordinating centers (CCs) in handling security incidents as well. The purpose of a CC is to coordinate and facilitate the handling of incidents across various CSIRTs (CERT, 2007). The best examples of CCs include CERT based in Pittsburgh, PA and US-CERT (United States Computer Emergency Readiness Team) based in Washington, DC.

The next type of IRT is internal and this is limited to a particular organization and its funding is based on where the team is housed within in the organization. Some IRTs are funded through either the chief executive officer (CEO) or chief information security officer (CISO) budget but it may not always be the case. Regardless of its funding, internal IRT should be placed where it can best support the business units without facing conflicts of interests or significant interference by the corporate environment (Forno, van Wyk, 2001). For the state of Georgia, no specific IRT has been formed but the levels of responsibility for handling an incident has been defined based on who the customer reports the incident to.

On an operational level within GTA, our Network Security group is the primary party that modifies enterprise firewalls, interact



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

with our managed security service provider (ISS) and receive escalation when a customer reports an incident through the GTA Command Center. Our command center houses the NOSC which conducts the initial triage (investigation) of possible security events / incidents and document all reports via our ticket management system (Peregrine ServiceCenter). On a policy level, the Office of Information Security is responsible for policy, enforcement and escalating incidents to law enforcement (Georgia Bureau of Investigation).

#### 5.1.4 How do incident handlers interact with law enforcement?

Some incidents because of their scope require the incident handler to inform law enforcement and collect evidence that could be used in a trial. At GTA, interaction with law enforcement is through the Office of Information Security. But, other organizations may require the handler to communication directly with law enforcement and key to this interaction is ensuring everything is documented and evidence is handled properly. More discussion on evidence handling will be done in the "tools" section of the paper. When dealing with law enforcement agencies, here are some key points to keep in mind:

- Familiarize yourself with applicable laws
- Know the types of cases law enforcement will be interested in



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Contact local law enforcement before there is an incident
- Have someone on the CSIRT become a member of InfraGuard (SANS, 2003).

**5.2 Identification phrase**

This phrase is important because this is where the handler decides whether or not an event seen is critical enough to be classified as an incident. In section 3 of this paper, it defined the difference between an event and incident. Understanding this key difference will allow the incident handler to focus his or her energies in the appropriate direction. In this phase, it's extremely important that the handler don't allow outside influences to cloud their judgment. Gather all of the facts and make your judgment based on those facts (Murray, 2007).

**5.3 Containment**

As the name implies, this phase is to limit the damage of the security incident on the computing environment. The IRT is hard at work during this phase by doing a variety of tasks: patching systems, password changes, firewall rule changes, account management, stopping of services and rootkit / antivirus system scans. On the employee side the CSIRT may place phone calls to halt a business process, obtain paper materials or printouts that contain false information or



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

send a corporate wide communication to alert the workforce (Profitt, 2007).

Another key task in this phase is gathering and preserving evidence of the security incident that will be admissible in legal proceedings. To do this, you might image the entire system or part of the system or capture volatile data, such as running process, RAM, network connections and so on. Whatever method you use for preserving evidence, make sure that you are using clean binaries and document everything that you do. In some cases, it is inevitable that a task you perform will change something on the system. Be prepared to explain what changed and why you performed that action (Murray, 2007). In the tools section of this paper, will provide ways that evidence can be obtained by incident handlers from a computer's running process, RAM, etc.

### 5.4 Eradication

The eradication phase involves the removal of any malicious activity or artifacts left by the intrusion. Typically eradication engages in removing virus infections, backdoor software, data left by the intruder and uninstalling attack tools (Proffitt, 2007). In some cases, you might be able to eradicate the attack without having to rebuild the system (Murray, 2007). In the event that the system was



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

compromised by a rootkit, the only way to properly recover is through a complete rebuild (ditto). Other activities in this phase from the SANS step by step guide include the following:

- Improve defenses
- Conduct a vulnerability analysis
- Find the last clean backup of the affected system (2003)

These three steps are important because correcting the way an attacker entered the network will decrease the likelihood of success in the future. In addition, checking for known operating system or web application vulnerabilities allow incident handlers to be more proactive instead of reactive. Using the information found in the vulnerability analysis, incident handlers can develop a relationship with system administrators to check their devices for current patches and software revisions. Finally, ensuring that a clean back-up exist for the affected system (s) will ensure that the same problem that affected the system in the first place doesn't come back into the computing environment again (ditto).

**5.5 Recovery**

The main focus of this particular phrase is the return of the system to normal operation. Full system functionality testing by the system owner should be conducted before placing the system back into



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

production (Smith, 2007). In addition, validating that the source of the incident has been resolved is important as well. A CIRT doesn't want to put the system back on-line just to appease the business owner knowing that it could be compromised again. To avoid any further problems, some level of system monitoring is appropriate. This will ensure that another attack on the system hasn't occurred and further remediation isn't required.

### 5.6 Lesson learned (follow-up)

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Many organizations have found that holding a "lessons learned" meeting with all involved parties after a major incident, and periodically after lesser incidents, is extremely helpful in improving security measures and the incident handling process itself (Northcutt, 2003). This phrase is when a formal report of findings and lesson learned is generated and submitted to all interested parties. The parties include business owners of the affected systems and management. At GTA, after major incidents a root cause analysis (RCA) meeting is held to go over what could have been done better and lesson learned activities for further reference. Our Quality management group is responsible for generating a "to-do"



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

list of action items and submission of the final report to management and other parties (ie.IRT, outside agency contact, GTA account management, etc).

## 6. How to build a successful incident response team?

Earlier in the paper, I defined an incident response team and the types of incident response teams. Right now, I will discuss how to build a successful incident response team. They're several factors involved with building a successful IRT team: IRT skill levels and adequate resources (e.g. money, tools, etc). Regardless of how large an organization, providing CSIRT with the necessary skills and resources can make a difference.

### 6.1 IRT staff skill set

According to CERT, skills are separated into two broad groups: personal skills and technical skills.

**Personal skills**

CSIRT members should be able to communicate well either through written or oral communication. Incident handlers are responsible for documentation of the incident, evidence handling and management briefings. Without good written skills, the final report of the incident will not make sense and isn't useful if the incident goes to court. Oral communication is accomplished either through face-to-



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

face or telephone interaction (CERT, 2007). Both written and oral communications allow IRT members to interact with a variety of people including:

- System and network administrators (or other IT staff)
- Application owners/developers
- Subject matter or technical experts
- Members of other IRTs
- Law enforcement
- Management
- Vendors (CERT, 2007)

Having several CSIRT members with good communication skills is useful when the team have to explain its mission and goals, services, strategic direction and activities undertaken by the team (ditto). Other required personal skills include:

- Diplomacy
- Ability to follow policies and procedures
- Able to work as a good team member
- Knowing one's limit
- Integrity
- Coping with stress
- Time management (ditto)



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**Technical skills**

The basic technical skills that CSIRT staff need have been separated into two categories: technical foundation and incident handling skills (CERT, 2007). Technical foundation can be defined as having the basic understanding of the underlying technologies used by the IRT and its constituency. Incident handlers also need to have an understanding of the issues that affect the team or constituency (ditto). An example of issues may include the following:

- Type of incident activity that is being reported or seen by the community
- The way in which CSIRT services are being provided (the level and depth of technical assistance provided to the constituency)
- The responses that are appropriate for the team (e.g. what policies and procedures or other regulations must be considered or followed while undertaking the response)
- The level of authority the CSIRT has in taking any specific actions when applying technical solutions to an incident reported to the CSIRT (2007).



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

According to CERT, basic technical skills for any IRT member should include the following:

- Having a basic understanding of security principles (e.g. confidentiality, integrity and availability)
- Knowing about security vulnerabilities/weaknesses and how it is used to cause an attack
- Historical background of the Internet
- Computer security risk analysis and how attacks effect the overall network availability
- Understanding core network protocols and how they work/common types of threats
- Knowledge of network application and services (e.g. DNS, SSH, Telnet, etc.) and how it's used for an attack / mitigation strategies
- Network security issues
- Understanding host/system security issues: incident handlers should have experience with operating systems (OS) used by the team (UNIX or Windows) and how to maintain said OS.
- Malicious code programs (e.g. Trojans, viruses, worms and malware)



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Some level of programming skills and concept of secure programming (coding).

**Incident handling skills**

CSIRT members need to posses the necessary skills to work an incident in any environment that the team has been deployed into action. Having a complete understanding of the following is critical:

- Local team policies and procedures
- Understanding and identifying intruder techniques
- Proper communication with sites
- Incident analysis
- Maintenance of incident records

All of the above skills are vital to the success of the CSIRT. If an incident isn't handled properly or the evidence is damaged in any way, the creditability of the group as a whole is jeopardized. Sometimes CIRT members have to be "jack-of-all trades" and learn on the fly to build on their skills. It's not possible for every member to have all skills but the majority should have the personal / technical skills to get the job done in the most effective and professional matter.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## 6.2 IRT cost consideration

The majority of the businesses today do not have an endless amount of money or resources that CSIRTs can have at their disposal. Earlier I mentioned that depending on where the IRT is housed in an organization, determines how much money or resources the team has to operate effectively. Even with the increased use of the web by businesses, some have failed to include incident response-specific costs in their overall budget. It is hard to calculate the cost of an IRT or program and even harder to quantify the money saved by having one as opposed to not having a team or program. A report commissioned by PGP Corporation and released by Ponemon Institute has created a benchmark to calculate the cost of a data breach in the United States.

Their report released in November 2007 shows that the total average costs of a data breach grew to $197 per record compromised, an increase of 8 percent since 2006 and 43 percent compared to 2005. The average total cost per reporting company was more than $6.3 million per breach and ranged from $225,000 to almost $35 million (Ponemon Institute, 2007). The report surveyed 35 companies for the report and were a cross representation of industries who had



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

experienced a data breach within the past year. Some of the companies had IRTs and others were mom/pop shops who just had a couple of IT staffers charged with responding to computer security incidents.

Another area that is affected by the lack of funding is training. Most organizations do not allocate sufficient funding for training and maintaining skills (Scarfone & Grance & Masone, 2007). To counteract the lack of funding for training, IRT management can send part of the staff to training and make them responsible for coming back and providing internal training to other staff members. Another way to train CSIRT members is through lunch & learns sessions conducted by subject matter experts (SME). For those handlers who learn best by reading, an organization can offer to pay for relevant learning materials (Pokladnik, 2007). An example of learning material is getting an extra set of courseware (e.g. SANS' institute SEC 504 class) when a staffer is sent to training. I find a good source of training material is by ordering IT security books from bookpool.com. Bookpool.com has access to most of the major publishers and sells their books at a discount off the suggested retail price.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Even with a limited budget, any organization can have an incident handling capability. Those with limited resources can have a type of incident response team called central incident response team. It is a single incident response team [that] handles incidents throughout the organization (Scarfone & Grance & Masone, 2007). This model is effective for small organizations and for large organizations with minimal geographic diversity in terms of computing resources (ditto). This smaller, faster, cheaper team is not necessarily the most resilient group. Those positions where one person wears several hats will make your response much less effective if they are unavailable. So you should return to your networking roots and apply defense in depth. Make sure there is a backup for as many of the personnel on your team as possible (Pokladnik, 2007).

One of the best resources when the company doesn't have enough staff or the money to hire security consultants is policy. A successful CSIRT is one that has documented standards and procedures. Standards should be written from how the CSIRT will begin its investigations and report the findings to standards written for how the CSIRT will be trained and what authority the members will be granted (Profitt, 2007). They're several resources out on the Internet that have policy templates to assist companies in writing



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

their own security policies. SANS through its security policy project has a repository of different resources: from templates to whitepapers. You can go to http://www.sans.org/resources/policies/ and check it policies for HIPAA, acceptable use and even 3rd party interconnectivity.

Another place for excellent computer security policy is from the National Institute of Standards and Technology (NIST). NIST offers policy guides and standards that have been adopted not only by government but private sector as well. By having written policy documents detailing what a handler should do when an incident has been identified, this allow IRT members the framework to conduct their work and serve as a reference document in the event of a problem. Policy documents are the most inexpensive item that a CSIRT can have and should be updated on a regular basis to reflect new threats, etc.

## 7. Tools and resources for supporting the work of incident handlers

The "best friend" for any incident handler is having a good set of tools to identify, mitigate and eradicate the aftermath of an incident. When I did my initial search for tools, most were focused on conducting forensic analysis of an affected workstation. After



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

consulting my SANS 401 coursework (Security Essentials), I did find one web-site that contained a variety of tools that are beneficial for incident handling. The web-site is http://sectools.org/ and has a listing of the Top 100 security tools as determined by over 3000 individuals in the IT security field (hackers and incident handlers). This page is maintained by Fyodor and many of the tools listed have been used by SANS instructors (e.g. nmap, nessus, Wireshark) so it is a good starting point for any novice. Besides forensic tools, other types of tools include the following:

- Examine systems and processes
- Port scanning
- IPv6 network incident handling tools
- Analysis software
- Hardware

For the purpose of this paper, I'll provide information on 3 products within each subcategory. Please note that additional tools will be listed in the appendix section of the paper.

**7.A Forensic analysis tools**

Forensic analysis tools can be divided into two areas: disk imaging and live CDs. In addition, I will discuss how Snort which main purpose is for intrusion detection can be used as a forensic



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

tool as well. Disk imaging tools are mainly found for the UNIX operating systems. Disk imaging can be defined as to make a secure forensically sound copy to media that can retain the data for extended period of time (Saudi, 2001). Most of UNIX tools selected for further discussion were ones that have been tested by NIST through its computer forensic tool testing program.

**7.A.1 UNIX disk imaging tools**

The first UNIX disk imaging tool that I will talk about is the oldest: dd. The **dd** command has been around since the 1970s, ported to many systems, rewritten many times, and proved to be an indispensable UNIX tool (softpanomar, 2001). A clone of dd is a part of the GNU coreutils tool set that's maintained by GNU.org. The **dd** command in UNIX … can be used to do direct dumps from one device to file or vise versa. It is a useful tool to create a disk image or to make a disk from an image (ditto). Another good Unix/Linux disk imaging tool is Encase. This software is created by Guidance software and the current version is 6.0. The following illustrates how Encase works:



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

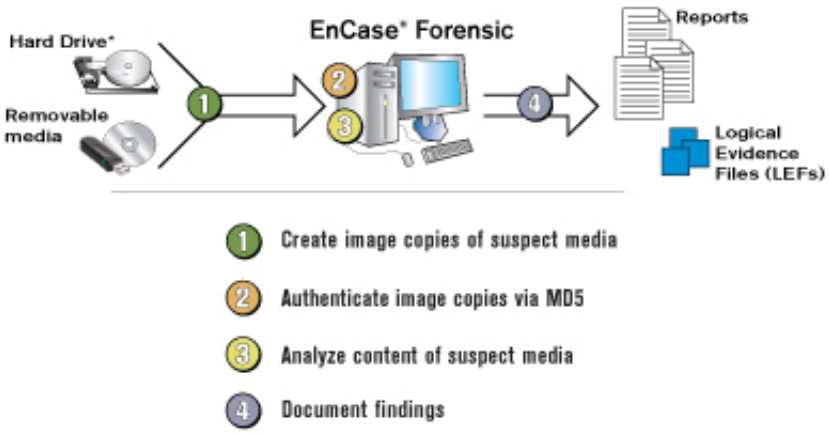


*Figure 4: How EnCase® Forensic Works (2008)*

Besides Unix, Encase supports the following file systems: FAT12/16/32, NTFS, EXT2/3 (Linux), Reiser (Linux), UFS (Sun Solaris), AIX Journaling File System (JFS and jfs) LVM8, FFS (OpenBSD, NetBSD and FreeBSD), Palm, HFS, HFS+ (Macintosh), CDFS, ISO 9660, UDF, DVD, and TiVo® 1 and TiVo 2 file systems (ditto).

The last UNIX disk imaging tool is Safeback. This software is from New Technologies, Inc which is a part of Armour Forensics. SafeBack is used to create mirror-image (bit-stream) backup files of hard disks or to make a mirror-image copy of an entire hard disk drive or partition. The process is analogous to photography and the



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

creation of a photo negative. Once the photo negative has been made several exact reproductions can be made of the original. Unlike the taking of a photo, SafeBack image files can detect attempts to alter the reproduction (2008).

### 7A.1.1. Windows disk imaging tools

Besides Encase, they're three other software products that are useful to create disk images for Windows. The first product that I will discuss is ILook version 8.0. The program was created by the Internal Revenue Service Criminal Investigation Division (IRS-CID) and Eliot Spencer, Perlustro LP. ILook is a multi threaded, Unicode compliant, fast forensic analysis tool designed to analyze an image taken from a seized computer system or other digital media. ILook will run on the following 32 bit platforms: - Win2K or WinXP and the following 64 bit platforms: Windows XP / Server 2003. ILook can be used to examine images obtained from other forensic imaging tools that produce a raw bit stream image. It may also be used to examine some commercial imager formats. ILook product suite is available for free to law enforcement agencies around the world (2008).

Next software suite that does computer forensic for Windows



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

operating system is X-ways Forensics. This software is produced by X-ways software technology AG and is tightly integrated with WinHex. X-Ways Forensics is an advanced work environment for computer forensic examiners and runs under Windows 98/Me/2000/XP/2003/and Vista. It is closely integrated with the **WinHex** hex and disk editor and can be purchased as a forensic license for WinHex. Part of an efficient workflow model where computer forensic examiners share data and collaborate with other specialized investigators that use X-Ways Investigator [software program]. X-Ways Forensics comprises all the general and specialist features known from WinHex (x-ways, 2008). The cost of the software is about $902 plus $59 for a personal license of WinHex; can even read image files created by Encase as well.

The most well-known and used software is GHOST by Symantec. Originally was created as a software package created to duplicate liked hardware for system recovery, it is now being used for forensic purposes as well. Features most useful for disk imaging are as follows:

- Full system backup of everything on a hard drive or partition
- File and folder backup of only the files you choose



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

- Backs up files by the type you choose (such as photos or financial documents)
- Makes incremental backups to save storage space and save time
- Backs up on key events, such as new application installation or sudden increases in data storage
- Advanced compression and encryption minimize storage space and keep data safe
- Recovers system and data even when operating system won't restart (Symantec, 2008).

GHOST can even create images for Linux EXT2/3 and Linux swap partition as well. The cost of the software is about $70 and includes one year of free updates.

### 7A.1.2 Linux and Windows live cds

My first experience with using a Live CD of Linux came when I took SANS' SEC 401 (Security Essentials with bootcamp). Because my background was Windows, it took a couple of hours for me to obtain a basic understanding on Linux. A good resource that provides incident handlers with the pros and cons of using Linux/Windows Live CDs for incident handling and forensic is the paper written by Ricky Smith and located in the SANS Reading Room. This section provides a high-level overview and not instructions on how to run or test Live



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

CDs. Live CDs are bootable CDs that have an operating system installed that can be run directly from the CD (Smith, 2007). Most Live CDs are for the Unix/Linux operating system. However, Windows does have a couple of Live CDs but a lot of prep work has to be done before creating the CDs for usage.

**Unix/Linux Live CDs**

They are a few Linux live-cds available depending on what favor of Linux/Unix the incident handler is familiar. Some of the newer Linux operating environments (Gentoo and Ubuntu) have a separate live CD or DVD distribution as well. Most incident handlers use one of the following Linux distributions: Knoppix, Helix, Backtrack and F.I.R.E. (Forensic and Incident Response Environment) as they have been available for a long time and their ease of use.

**Knoppix:**

Knoppix is what most Linux Live CDs based their particular version upon and is widely used by incident handlers. Knoppix is a bootable Live system on CD or DVD, consisting of a representative collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals. Knoppix can be used as a productive Linux



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

system for the desktop, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk (Knoppix, 2008). Current version of Knoppix is 5.1.1 and available in six different languages as well.

**Helix:**

This is a live CD distro based on Knoppix and used by incident handlers and forensic analysts. Tools found on the CD can be run using both Windows and Linux based operating systems. Unlike the other Live CDs, Helix can be used for Windows based live response as well (Bandukwala, 2007). Helix is can be downloaded from http://www.e-fense.com/helix/ and current version is 1.9a (July 2007).

**Backtrack:**

Backtrack was created out of a merger between Auditor and Whax. Auditor was a GPL-licensed live CD based on Knoppix, with more than 300 security software tools. Auditor was maintained by a team of 7 and the same team also maintained another Live CD distro called Whax. Whax started as Whoppix and was a stand-alone penetration-testing live CD based on KNOPPIX. When the kernel was upgraded to better support WiFi, the name changed to WHAX and its base changed from



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

KNOPPIX to the more modular SLAX live CD (distrowatch, 2008). The software can be downloaded from http://www.remote-exploit.org/backtrack_download.html and first version of Backtrack was released in May 2006. After a few months of testing, version 2.0 came out in March 2007. This version is different from 1.0 because Nessus is no longer built-in (licensing issue). A beta release (version 3.0) just came out in December 2007 and allows for usage as a CD-rom, DVD-rom or USB flash drive.

***F.I.R.E: Forensic and Incident Response Environment Bootable environment***

F.I.R.E. is a portable bootable cd-rom based distribution with the goal of providing an immediate environment to perform forensic analysis, incident response, data recovery, virus scanning and vulnerability assessment. It also provides necessary tools for live forensics/analysis on win32, sparc solaris and x86 linux hosts just by mounting the cdrom and using trusted static binaries available in /statbins (2008). Unfortunately, the last real update was in 2004 but could still be a viable Live CD (in a punch). Software can be obtained from http://sourceforge.net/projects/biatchux/.

**Windows Live CDs**



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Live CD for the Windows operating systems is limited due to the licensing restrictions of Windows itself. The two most known options are Windows PE from Microsoft and BartPE (Smith, 2007). The Microsoft Windows Live CD (Windows PE) is only available to software assurance customers and BartPE can be built using the installation media for a licensed copy of Windows XP or Windows Server 2003 (ditto). From the BartPE website, it provides a listing of the differences between BartPE and Windows PE:

**BartPE vs.Windows PE?**

- BartPE is not supported by Microsoft. Windows PE is an official Microsoft product.
- BartPE has a graphical user interface. Windows PE has a command line interface.
- The tools needed to make a BartPE installation are free software. Windows PE is available only to Microsoft OEM users.
- BartPE allows unlimited custom plugins. Windows PE has a limited range of plugins options (Lagerweij, 2008).

Finally, another player in the Windows Live CD market space is Active@ Boot Disk from NTFS.com. Not only does it have a boot disk product that works for Windows XP/2000/Vista but a DOS version as



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

well. The software is offered as a 10-day demo and can be purchased for $69.95 (personal) and $89.95 (corporate) license that includes free updates. The product is based on lightweight Windows VISTA (WinPE 2.0) operation environment and contains disk image, data recovery, password resetting, data erasure, network access tools and system utilities. The installation package contains all necessary tools to create bootable USB/CD/DVD media (NTFS.com, 2008). Within their Live CD, an option is available to perform a disk image. The disk image program is called Active Disk Image and it has the ability to create a raw image that can be used for forensic analysis.

### 7A.1.3 Snort used for forensic analysis

In an earlier section of this paper, I talked about Snort being used to detect incidents. Another way to use snort is for network forensics. By using Snort along with a few plugins (Sancp + barnyard + squil) and packet logging, Snort can be an interesting way to perform network forensics. By setting up Snort at important network chokepoints, this will allow incident handles to see whether attacks succeeded without even having to check the systems under attack (Pokladnik, 2007). Of course, verifying an attack on the system will provide further confirmation in the event of a false positive by Snort.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## 7A.2 Examining systems and processes

Tools in this section came as a result of the work by the clearinghouse for incident handling tools (CHIHT). Purpose of the CHIHT is to collect tools and information from European CSIRTS as a result of a project in the framework of the *Trans-European Research and Education Networking Association* (TERENA) task force: TF-CSIRT (2008). Most of the tools can be used for the Windows operating system but a few are used under Unix as well.

**Name:** Netcat
**Source:** http://netcat.sourceforge.net/
**Platform:** Unix, Windows

Netcat is a program to create network connections, TCP or UDP, to or from any port number. It is most commonly used with other commands as part of a script. In the security field it can be used to capture or originate flows of packets for network or traffic debugging. It can also be used for scanning networks for vulnerable servers, testing firewalls, building proxies, etc.

**Name:** sockstat
**Source:** Built-in command
**Platform:** FreeBSD

The sockstat command lists open sockets on a system so can be used to identify any unexpected connections, for example from packet sniffers.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**Name:** Fstat
**Source:** Built-in command
**Platform:** FreeBSD

The fstat command lists open files on a system so can be used to identify any unexpected logfiles, for example from packet sniffers.

**Name:** Foundstone Forensic tools
**Source:** http://www.foundstone.com/knowledge/forensics.html
**Platform:** Windows

The Foundstone Forensics toolkit includes programs to list open ports and the processes controlling them; to track logins and activity on Windows systems; to examine file access times and permissions.

**Name:** Sysinternals tools
**Source:** http://technet.microsoft.com/en-us/sysinternals/default.aspx
**Platform:** Windows

SysInternals tools for Windows includes utilities to examine Windows processes, files and ports. The site also includes a great deal of information on undocumented features of Windows operating systems.

## 7A.3 Port scanners

According to tech-faq.com, a port scanner is a program which attempts to connect to a list or range of TCP (Transmission Control



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Protocol) or UDP (User Datagram Protocol) ports on a list or range of IP addresses. Port scanners are used for network mapping and for network security assessments (2008). Two of the most used port scanners are Nessus and Nmap. Both Nessus and Nmap can be run under Unix (Linux) and Windows operating systems.

**Nessus**

Initially, this was an open source product but is now being maintained by Tenable software. To obtain program updates, it requires registration and free uses get plugins a few days after paid customers. The latest version is 3.0.6 and can be downloaded from http://www.nessus.org/nessus/. Primary usage of Nessus is as a port scanner to check for any type of system vulnerability.

**Nmap**

Nmap ("Network Mapper") is a free and open source (license) utility for network exploration or security auditing (Fyodor, 2008). Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical versions are available (ditto).

## 7A.4 IPv6 network incident handling tools

As more people gain access to the Internet, the current number of internet protocol (IP) addresses is running out. The current version of IP is version 4 and was adequate until the raise of DSL and cable internet access in the past five years. IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as routing and network auto configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period (IPv6, 2008). At this time, they are not many tools that have been upgraded or created for handling security incidents on an IPv6 based network. But, I did find several different resources if your network has been converted to IPv6.

DNSstuff is a web-based tool used to find out who owns a particular IP address. On their website, it has several forms that will find who owns a particular IPv6 IP address. URL is http://member.dnsstuff.com/pages/ipv6tools.php. Another good website



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

for troubleshooting is from the European IPv6 Internet Exchange. Their website (http://lg.consulintel.euro6ix.org/) provides a means to run ping, traceroute, dig and mtr for an IPv6 address. I found a port scanner for IPv6 called HalfScan6 and it can be downloaded from ftp://ftp.habets.pp.se/pub/synscan/halfscan6-0.2.tar.gz. This program will only work under Linux. Several network tools have been upgraded to run on IPv6. These include Netcat, Nmap, Wireshark and The Hacker's Choice.

## 7.B. Incident handling resources

Besides software and Internet tools, incident handlers need specific hardware and analysis resources to get their job done. The following information is taken from the NIST Computer Security Incident Handling guidelines (table 3.1) which list some of the tools and resources available for incident handlers.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**Table 7-1. Tools and Resources for Incident Handlers**

| Incident Analysis Hardware and Software |
|---|
| **Computer forensic workstations and/or backup devices** to create disk images, preserve log files, and save other relevant incident data |
| **Laptops,** which provide easily portable workstations for activities such as analyzing data, sniffing packets, and writing reports |
| **Spare workstations, servers, and networking equipment**, which may be used for many purposes, such as restoring backups and trying out malicious code; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using operating system (OS) emulation software |
| **Blank media,** such as floppy disks, CD-Rs, and DVD-Rs |
| **Easily portable printer** to print copies of log files and other evidence from non-networked systems |
| **Packet sniffers and protocol analyzers** to capture and analyze network traffic that may contain evidence of an incident |
| **Computer forensic software** to analyze disk images for evidence of an incident |
| **Removable media** with trusted versions of programs to be used to gather evidence from systems |
| **Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions |

| Incident Analysis Resources |
|---|
| **Port lists,** including commonly used ports and Trojan horse ports |
| **Documentation** for OSs, applications, protocols, and intrusion detection and antivirus signatures |
| **Network diagrams and lists of critical assets,** such as Web, email, and database servers |
| **Baselines** of expected network, system and application activity |
| **Cryptographic hashes** of critical files34 to speed the analysis, verification, and eradication of incidents |



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## 8. Summary

One of the main objectives of this paper is to define key terms of incident handling and give readers some options on how to develop an incident handling capability in their place of business. Incident handling is not an activity that organizations should take for granted. Because so much of economic commerce is done via the Internet, having a group of individuals dedicated to resolve a computer security incident should be standard operating procedure. IT professionals who have incident handling responsibility need to understand the difference between an event and a security incident. Once an incident has been declared, cooperation between all parties involved is a major key to success. Without management support and appropriate resources for incident handling, recovering from an incident may take longer and cost the organization not only money but customer goodwill as well.

Fortunately, incident handlers have many different resources to help discover when a system has been comprised and mitigate the damage. Firewalls, intrusion detection systems and anti-virus software are just a few example of items used for incident detection. Other resources come from the federal government (US-CERT and NIST), educational IT (EDUCAUSE) and internet (insecure.org). Even with the



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

right amount of resources, an incident handler is only as good their training and knowledge of malicious activity and system vulnerabilities. The SANS institute through their training and security policy project, provides resources to assist novice and experienced handlers. Incident handling is an evolving field as the Internet change from using IPv4 to IPv6 addressing.

Regardless of what local operating system is being used, tools to boot, examine system processes and perform forensic investigates are available. For the adventurous, information has been provided to make your own multi-session handling tool DVD. So if you are an IT professional that has been given incident handling duties, use this paper as a resource to get you up to speed. Being ready to handle an incident in a professional matter will provide big dividends to your organization and emphasis the importance of “always being prepared.”



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## Appendix A---Online Tools and Resources:

The following information is taken from the Computer Security Incident Handling guide maintained by NIST.

## Incident Response Organizations

| Organization | URL |
|---|---|
| Australian Computer Emergency Response Team (AusCERT) | http://www.auscert.org.au |
| Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice | http://www.cybercrime.gov |
| CERT® Coordination Center, Carnegie Mellon University (CERT®/CC) | http://www.cert.org |
| CERT®/CC Incident Reporting System | https://irf.cc.cert.org |
| Computer Incident Advisory Capability (CIAC), U.S. Department of Energy | http://www.ciac.org/ciac |
| Forum of Incident Response and Security Teams (FIRST) | http://www.first.org |
| Government Forum of Incident Response and Security Teams (GFIRST) | http://www.us-cert.gov/federal/gfirst.html |
| High Technology Crime Investigation Association (HTCIA) | http://www.htcia.org |
| IETF Extended Incident Handling (inch) Working Group | http://www.ietf.org/html.charters/inch-charter.html |
| InfraGard | http://www.infragard.net |
| Internet Storm Center (ISC) | http://isc.incidents.org |
| United States Computer Emergency Response Team (US-CERT) | http://www.us-cert.gov |



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## Incident Response-Related Mailing Lists

| Mailing List Name | Archive Location |
|---|---|
| Bugtraq | http://www.securityfocus.com/archive/1 |
| DShield | http://www.dshield.org/pipermail/list |
| Focus on IDS | http://www.securityfocus.com/archive/96 |
| Forensics | http://www.securityfocus.com/archive/104 |
| Incidents | http://www.securityfocus.com/archive/75 |
| Intrusions | http://cert.uni-stuttgart.de/archive/intrusions |
| LogAnalysis | http://airsnarf.shmoo.com/pipermail/loganalysis |
| National Cyber Alert System | http://www.us-cert.gov/cas/ |
| Technical Cyber Security Alerts | http://www.us-cert.gov/cas/techalerts/ |
| Cyber Security Alerts | http://www.us-cert.gov/cas/alerts/ |
| Cyber Security Bulletins | http://www.us-cert.gov/cas/bulletins/ |
| Cyber Security Tips | http://www.us-cert.gov/cas/tips/ |
| Current Activity | http://www.us-cert.gov/current/ |



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## Technical Resource Sites

| Resource Name | URL |
|---|---|
| Center for Education and Research in Information Assurance and Security (CERIAS) Intrusion Detection Pages | http://www.cerias.purdue.edu/about/history/coast/archive/data/category_index.php |
| Clearing House for Incident Handling Tools (CHIHT) | http://chiht.dfn-cert.de |
| CSIRT Development, CERT®/CC | http://www.cert.org/csirts |
| Computer Security Resource Center (CSRC), NIST | http://csrc.nist.gov |
| Distributed Intrusion Detection System (DShield) | http://www.dshield.org |
| Incident Handling Links and Documents | http://www.honeypots.net/incidents/links |
| Intrusion Detection FAQ, SANS Institute | http://www.sans.org/resources/idfaq |
| Intrusion Detection Links and Documents | http://www.honeypots.net/ids/links |
| Loganalysis.org | http://www.loganalysis.org |
| National Institute of Justice (NIJ) Electronic Crime Program | http://www.ojp.usdoj.gov/nij/topics/ecrime/welcome.html |
| NIST Internet Time Service | http://www.boulder.nist.gov/timefreq/service/its.htm |
| SANS Institute Reading Room | http://www.sans.org/rr |
| SecurityFocus | http://www.securityfocus.com |
| The Electronic Evidence Information Center | http://www.e-evidence.info |



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## Vulnerability and Exploit Information Resources

| Resource Name | URL |
|---|---|
| CERT®/CC Advisories | http://www.cert.org/advisories |
| CERT®/CC Incident Notes | http://www.cert.org/incident_notes |
| CERT®/CC Vulnerability Notes Database | http://www.kb.cert.org/vuls |
| CIAC Bulletins and Advisories | http://www.ciac.org/cgi-bin/index/bulletins |
| Common Vulnerabilities and Exposures (CVE) | http://www.cve.mitre.org |
| National Vulnerability Database (NVD) | http://nvd.nist.gov/ |
| Open Vulnerability Assessment Language (OVAL) | http://oval.mitre.org/ |
| Packet Storm | http://www.packetstormsecurity.com |
| SANS/FBI Top 20 List | http://www.sans.org/top20 |
| SecurityFocus Vulnerabilities Database | http://www.securityfocus.com/bid |



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## Appendix B-Frequently asked questions

NIST in their computer security handling guide has created this document for organization to provide their users, system administrators, information security staff members, and others within the organization that may have questions about incident response. The following are frequently asked questions (FAQ) regarding incident response.

**1. What is an incident?**

In general, an incident is a violation of computer security policies, acceptable use policies, or standard computer security practices. Examples of incidents are—

- A distributed denial of service attack against a public Web server
- A worm that infects hundreds of workstations on a network and effectively shuts down the network
- An attacker who gains remote administrator-level access to an email server
- A user who downloads password cracking tools
- A user who defaces another organization's public Web site.

**2. What is incident handling?**

Incident handling is the process of detecting and analyzing incidents and limiting the incident's effect. For example, if an attacker breaks into a system through the Internet, the incident handling process should detect the security breach. Incident handlers will then analyze the data and determine how serious the attack is. The incident will be prioritized, and the incident handlers will take action to ensure that the progress of the



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

incident is halted and that the affected systems return to normal operation as soon as possible.

**3. What is incident response?**
The terms "incident handling" and "incident response" are synonymous in this document.

**4. What is an incident response team?**
An incident response team (also known as a Computer Security Incident Response Team [CSIRT]) is responsible for providing incident response services to part or all of an organization. The team receives information on possible incidents, investigates them, and takes action to ensure that the damage caused by the incidents is minimized. In some organizations, the incident response team is a formalized, full-time group; in others, incident response team members are pulled from other job functions as needed. Some organizations have no incident response team because they outsource incident response duties.

**5. What services does the incident response team provide?**
The particular services that incident response teams offer vary widely among organizations. Besides performing incident handling, a team typically distributes advisories regarding new threats, and educates and raises the awareness of users and technical staff on their roles in incident prevention and handling. Many teams also assume responsibility for intrusion detection system monitoring and management. Some teams perform additional services, such as auditing and penetration testing.

**6. To whom should incidents be reported?**
Organizations should establish clear points of contact (POC) for reporting incidents internally. Some organizations will structure their incident response capability so that all incidents are reported directly to the incident response team, whereas others will use existing support structures, such as the information technology (IT) help desk, for an initial POC. The organization should recognize that external parties, such as other incident response teams, would report some incidents. Federal



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

agencies are required under the law to report all incidents to the United States Computer Emergency Readiness Team (US-CERT).

**7. How are incidents reported?**
Most organizations have multiple methods for reporting an incident. Different reporting methods may be preferable as a result of variations in the skills of the person reporting the activity, the urgency of the incident, and the sensitivity of the incident. A phone number or pager number should be established to report emergencies. An email address may be provided for informal incident reporting, whereas a Web-based form may be useful in formal incident reporting. Sensitive information can be provided to the team by sending a fax to a machine in a secured area or by using a public key published by the team to encrypt the material.

**8. What information should be provided when reporting an incident?**
The more precise the information is the better. For example, if a workstation appears to have been infected by malicious code, the incident report should include the following data:

- The user's name, user ID, and contact information (e.g., phone number, email address)
- The workstation's location, model number, serial number, hostname, and IP address
- The date and time that the incident occurred
- A step-by-step explanation of what happened; including what was done to the workstation after the infection was discovered. This explanation should be detailed, including the exact wording of messages, such as those displayed by the malicious code or by antivirus software alerts.

**9. How quickly does the incident response team respond to an incident report?**



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The response time depends on several factors, such as the type of incident, the criticality of the resources and data that are affected, the severity of the incident, existing Service Level Agreements (SLA) for affected resources, the time and day of the week, and other incidents that the team is handling. Generally, the highest priority is handling incidents that are likely to cause the most damage to the organization or to other organizations.

**10. When should a person involved with an incident contact law enforcement?**
Communications with law enforcement agencies should be initiated by the incident response team members, the chief information officer (CIO) or other designated official—users, system administrators, system owners, and other involved parties should not initiate contact. The incident response team should contact law enforcement at the appropriate time according to established policies and procedures.

**11. What should someone do who discovers that a system has been attacked?**
The person should immediately stop using the system and contact the incident response team. The person may need to assist in the initial handling of the incident—for instance, disconnecting the network cable from the attacked system or physically monitoring the system until incident handlers arrive to protect evidence on the system.

**12. What should someone do who receives spam?**
The person should forward the spam to the email address that the organization has designated for reporting spam. Statistics compiled on spam may be used to justify additional antispam measures. The statistics will also be provided to incident reporting organizations that study trends in computer security incidents. The person usually should not reply to the spam message in any way, including asking to be removed from a mailing list, because this would validate to the sender that the email address is valid and actively used.

**13. What should someone do who receives a warning from a friend about a new virus?**



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

The person should check a virus hoax Web site to see if the new virus is legitimate or a hoax. Many virus warnings distributed through email are hoaxes, and some of the instructions provided in the hoaxes may cause damage to systems if they are followed. Antivirus vendor Web sites often contain virus hoax information; the NIST Computer Incident Advisory Capability (CIAC) Hoaxbusters web site (http://hoaxbusters.ciac.org/) is another good source. A person who is still in doubt about the authenticity of a virus warning should contact the help desk for further assistance.

**14. What should someone do who is contacted by the media regarding an incident?**

A person who has been part of the incident response may answer the media's questions in accordance with the organization's policy regarding incidents and outside parties. If the person is not qualified to represent the organization in terms of discussing the incident, the person should make no comment regarding the incident, other than to refer the caller to the organization's public affairs office. This will allow the public affairs office to provide accurate and consistent information to the media and the public.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## Appendix C- Information for creating a live multi-session DVD

The following information is from a GIAC GCIH Gold paper by Jamal Bandukwala. Mr. Bandukwala established instructions on creating a multi-session live DVD.

**Customizing and building your own Multi-session DVD Set: A Walkthrough**

**Brief: How the Walkthrough will be organized**
The walkthrough will start by going through the steps needed prior to actually updating and customizing the live CD's such as verifying the integrity of your tools and setting up the environment. Once the CD customization walk through has been completed the guide will move to taking the reader through the steps necessary to put all the newly created ISO's together into a multi session DVD.

**Step 1: Choose your Live CD's**
There are a large number of live CD distributions currently available, some are better known and are actively maintained while others have been abandoned but have a good setup and collection of tools and happen to also be the reader's favorites. I would strongly recommend the analyst examine the various live CD's available, look at what each one has to offer, examine their own needs and decide on which distributions, they want to include as part of their toolkit. I would also strongly recommend the analyst or tester get completely familiar with the tools and how they affect a system prior to using them in any investigation, or production/ real environment.

**Step 2: Download your ISO's and other tools**



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Once the reader decides which live distributions to include in their toolkit it is time to download them; it is best to obtain the distributions from the original sources and then verify that these are indeed the legitimate downloads by verifying these against the original's md5 check if available.

**Step 3: Setting up your workspace**

Making sure one's workspace is setup correctly will increase the likelihood of success, and reduce the number of failed attempts when trying to re-master a live CD, or multi-os DVD. In order to successfully customize your live CD, you first need to install a Linux operating system. While almost any of the major Linux distributions would do, one may want to consider installing a Debian based system, whether Debian itself, Ubuntu or a Knoppix build (especially if one plans to work with largely debian or knoppix based distributions). This is well documented and may make it easier to re-master a live CD as necessary, additionally as the CD's being remastered have a Debian base, most of the commands will also be fairly similar. It is important to point out, that I choose to use VMware, as it makes it easier for me to test out and experiment with different settings as needed, this is certainly not a requirement and you may wish to use real hardware, if you have this at your disposal. The First thing one must do is create a new VMware machine and configure it to load from an ISO. Once this is complete, start the machine, and install a Linux distribution as your base image, make sure to give it plenty of RAM and swap space. The following website provides an excellent walkthrough on using cfdisk, setting up your machine and installing Linux in VMware (http://www.securityexplained.net/topics/virtEnv/index2.html). One must keep in mind that while most of the commands here will be identical, the partitions may differ based on your machines setup. While some may argue that this is unnecessary and most people installing or setting up Linux should already know how to do this,



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

there may be some readers, or members of the incident handling team who may not have installed Linux before or simply do not install Linux that often. This process will allow anyone whether it is a new member to the incident handling team or an experienced member who simply needs a refresher to quickly follow the guide and begin preparing their workstation for base operating system installation. In this case I chose to install Ubuntu 6.06 LTS as my base operating system. I chose this distribution/operating system over others for several reasons. One feature I really liked about this distribution was its ease of use and hardware detection, it was fairly easy to install this version of Ubuntu and my hardware was detected without a problem. In addition to this, I also liked the'clean' interface, as this made it more enjoyable to use and as it is based on Debian I knew that most of the commands would work effectively for the distributions I was re-mastering. It is important to point out that simply installing Linux on your workstation is not enough, while some distributions may install all the tools one needs' to start re-mastering and developing the distributions, the Ubuntu distribution I chose did not have all the utilities I needed installed by default. One can add the necessary tools by executing the following command using the bash

***'sudo apt-get install cloop-utils mkisofs squashfs-tools qemu'***

If one is unable to find the packages they need using this method, they may also wish to use the GUI based synaptic package manger which lists most of the packages available. In my case in addition to the packages mentioned above I also needed to install the pbuilder and debpkg packages. Once the user has downloaded the packages they require, some of the packages will need to be setup. A guide to installing and setting up the chroot environment for Ubuntu 6.06 can be found at the following site https://help.ubuntu.com/6.06/ubuntu/packagingguide/C/append



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

ix-chroot.html. If the user needs to find a package and has been unable to find it this way, they may wish to search ubuntu's package repositories for the utility they are looking for. These packages include utilities to setup the chroot environment and build and edit packages and also include file systems one might need. It is important to point out that different live CD's (even if based on debian) can use different file systems. If one is remastering an ubuntu live CD they would need the squashfstools file system, while knoppix based live CD's generally use the cloop-utils package.

**Step 4: Copy the cd content over into your virtual workstation**
This step depends on the distributions one is working with, different Linux and UNIX distributions may require slightly different steps to execute this. It is strongly recommended that the analyst search for documentation relating to the distribution they wish to work with, as commands between distributions may differ and furthermore some distributions and versions may have steps or commands unique to them. In this case I had burnt the ISO's of the live CD's I was planning to work with to DVD, prior to entering my Ubuntu workstation. I started by copying the ISO I planned to work with to my desktop and then moved the ISO to a working directory by using the following commands at the bash prompt:
***'mkdir ~/live'***
***'cd /home/user/Desktop/helix'***
***'mv Helix_v1.9-07-13-2007.iso ~/live'***
Once the ISO has been copied, it is time to extract the CD contents; in this case I did this using the following commands at the bash prompt (Ubuntu, 2007):
***'mkdir mnt'***
***'sudo mount-o loop Helix_v1.9-07-13-2007.iso mnt'***
***'mkdir extract-cd'***
***'rsync –exclude=/usr/local/sbin/extract_compressed_fs –a mnt/ extract-cd'***



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**Step 5: Update the content for your live CD**
In order to update the CD without negatively affecting the host system it is best to work in the chroot environment (Granneman, 2006). Once the user has entered the chroot environment, they can use the apt-get (Debian) system to modify the components they wish to update. The user can enter the chroot system using the following command sequence: ***'sudo chroot extract-cd'***
At this point one can start using the apt-get command sequence to update the files they wish to. I would not recommend updating all the files available, and would only update the applications you need to. When remastering a specific distribution it is best to check for any notes or comments made by the author of that distribution. This is because some live CD's may have customized kernels', modules or special libraries setup to work with the different tools on the CD. If one just attempts to update everything on a live CD, there is a risk that the customized CD may not work as intended. In order to update the CD using the apt-get system, one can use the following sequence of commands:
***'sudo apt-get remove Mozilla-firefox'*** (note: this removes the current version of firefox)
***'sudo apt-get install Mozilla-firefox'*** (note: this will download and install the latest version of firefox)
When this is complete, it is time for the analyst to clean up and exit the chroot environment. The cleanup routine can be done by executing the first of the following commands, when this is complete it is time to compress the file system, this can be executed using the second command sequence listed below (Granneman, 2006).

***'sudo apt-get clean'***
***'sudo mkisofs -iso-level 4 -R -U -V "Helix Custom" -hiderr-moved -cache-inodes -no-bak -pad /usr/local/sbin/extract-cd | nice -5 create_compressed_fs -***



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

***65536 > /usr/local/sbin/extract-cd'***

**Step 6: Create your new ISO and burn it to CD**

**Step 7: Calculate the new md5 hash value and record it**
After you have burnt the ISO, calculate the new md5 hash value and record it. This helps you make sure that the next time you burn a copy of your customized distribution; it has not been compromised or gone corrupt.

**Step 8: Test your new customized live CD**
Having burnt the ISO and calculated the new md5 hash value, it is time to test out your new live CD on both virtual and real hardware if possible. This is to ensure that it works as designed and verify you can see or access the tools you have added, removed or customized.

**Step 9: Record the md5 values for the CD's you will be packaging.**
Once you have completed step 8, burn all the distributions you will be packaging on separate CD's and record the md5 sum values and Release/ Distribution version information for all of these. In case something fails or a distribution on your DVD is called into question or challenged, this demonstrates that you have a list of known good checksums and can test or prove that the version on your multi-os DVD matches this.

**Step 10: Burn the distributions on to a DVD**
When you have completed step 9, start your remastering Linux station and follow the steps outlined in Anindya Roy's creating a multi-boot DVD document, found at the following site: http://pcquest.ciol.com/content/enterprise/2005/105070101.asp.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

**Step 11: TEST**
After you have completed step 10, and the DVD has been successfully burnt, test in on multiple configurations (this depends on one's specific environment and needs; verify that everything is working as designed on both virtual and real hardware. If this is successful and you are satisfied with your new tool, calculate the new md5 value for the Multi-OS DVD and record this along with your other Md5 sums.

**Congratulations!** You now have a powerful tool, with plenty of documentation and a strong process which can be analyzed, criticized and adapted as needed by your organization. In addition to this, the commands used to build the CD can be modified and possibly scripted to suit one's environment, resulting in the automation of a part of the build process.



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

## 10. References

"2007 Annual Study: US cost of a data breach." Retrieved January 2008 from http://www.pgp.com/downloads/research_reports/ponemon_reg_direct.html (registration required)

Arvidsson, Jimmy (1998). Taxonomy of the Computer Security incident related terminology. Retrieved October 2007 from http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html

Bandukwala, Jamal (2007). Multi-tool DVD sets: an important addition to the incident handler and pen tester's toolkit. SANS Reading Room, Retrieved January 2008 from http://www.sans.org/reading_room/whitepapers/incident/2001.php

Bezroukov, Nikolai (2007). Unix DD Command and Image Creation. Softpanorama, Retrieved January 2008 from http://softpanorama.org/Tools/dd.shtml

Bodhnar, Ladistav (2007). Distrowatch.com: Whax. Retrieved January 2008 from http://distrowatch.com/table.php?distribution=whoppix



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Borodkin, Michelle (2001). Computer incident response team. SANS Reading Room, Retrieved September 2007 from http://www.sans.org/reading_room/whitepapers/incident/641.php

Businessdirectionary.com. "security breach." Retrieved September 2007 from http://www.businessdictionary.com/definition/security-breach.html

Cid, Daniel B. (2007). About OSSEC. OSSEC, Retrieved November 2007 from http://www.ossec.net/main/about/

Cook, Chad (2000). An introduction to incident handling. SecurityFocus, Retrieved October 2007 from http://www.securityfocus.com/infocus/1184

Carnegie Mellon University/Software Engineering Institute (2007). CERT/CC: staffing your Computer Security Incident Response Team-what basic skills are needed. Retrieved September 2007 from http://www.cert.org/csirts/csirt_faq.html

Carnegie Mellon University/Software Engineering Institute (2007). CERT/CC: Computer Security Incident Response Team FAQ. Retrieved



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

2007 from http://www.cert.org/csirts/csirt-staffing.html

Dmzs-biatchux. F.I.R.E. Forensic and incident response environment bootable CD, Retrieved January 2008 from http://fire.dmzs.com/?section=features

e-fense (2005). Helix-incident response and computer forensics Live CD by e-fense™. Retrieved January 2008 from http://www.e-fense.com/helix/index.php

Even, Loras R. Honey Pot Systems Explained. SANS Intrusion Detection FAQ, Retrieved October 2007 from http://www.sans.org/resources/idfaq/honeypot3.php?portal=e7c9bbd6185d97b426483fd82795a9bc

Forno, Richard & van Wyk, Kenneth (2001). Incident Response. O'Reilly. Retrieved October 2007 via Safari Books Online, LLC.

Fydor. Free security scanner for network exploration &security audits, Retrieved January 2008 from http://nmap.org/ ,

Georgia Technology Authority (2005). Responding to security incidents, Retrieved Sept 2007 from



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

http://gta.georgia.gov/internal/downloads/?url=/vgn/images/portal/cit_1210/61/37/102088875IncidentResponseStandard (ISOconsensus).pdf

Guidance Software (2008). How Encase® Forensics Works. Retrieved January 2008 from http://www.guidancesoftware.com/products/ef_works.aspx

Hall, Missy (2003). Implementing a computer incident response team on a smaller, limited resource organizational setting. SANS Reading Room, Retrieved from http://www.sans.org/reading_room/whitepapers/incident/1065.php

Hong, Shinil (2007). Security Incident handling. University of Buffalo-State University of New York. Retrieved October 2007 from http://computersecurity.buffalo.edu/presentations-07/shinil-UB_InfoSec_Workshop_Incident_Handling_part2.pdf

Howard, John D. & Longstaff, Thomas (1998). A common language for computer security incidents. Retrieved October 2007 from http:// www.cert.org/research/taxonomy_988667.pdf



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Ilook (2007). ILookv8. Retrieved January 2008 from http://www.ilook-forensics.org/iLookv8.html

IPv6 (2008). Retrieved January 2008 from http://www.ipv6.org/

Javvin.com "incident handling." Retrieved September 2007 from http://www.javvin.com/networksecurity/IncidentHandling.html

Knoppix (2008). What is knoppix? Retrieved January 2008 from http://www.knoppix.org/

Lagerweij, Bart (2008). Bart's pre-installed environment (BartPE) bootable live windows CD/DVD. Nu Productions, Retrieved January 2008 from http://www.nu2.nu/pebuilder/

Murray, Jim (2007). Analysis of the incident handling Six step process. GIAC Research in the Common Body of Knowledge (CISSP) Retrieved September 2007 from http://www.giac.org/resources/whitepaper/network/17.php

New Technologies, Inc. (2008). Safeback 3.0. Retrieved January 2008 from http://www.forensics-intl.com/safeback.html



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Northcutt, Stephen (2003): Incident Handling Step by Step guide. SANS Institute.

NTFS.com (2007). Active @ Boot disk. NTFS.com by Active Data Recovery Software, Retrieved January 2008 from http://www.ntfs.com/boot-disk-win.htm

Osborne, Tia R. (2001). Building an incident response program to suit your business. SANS Reading Room, Retrieved Sept 2007 from http://www.sans.org/reading_room/whitepapers/incident/627.php

Petersen, Rodney (2006). Incident handling and forensics. EDUCASE, Retrieved September 19, 2007 from https://wiki.internet2.edu/confluence/pages/viewpage.action?pageId=2862

Pham, Charles (2001). From events to incidents. SANS Reading Room, Retrieved September 2007 from http://www.sans.org/reading_room/whitepapers/incident/646.php

Pokladnik, Mason (2007). An incident handling process for small and



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

medium business. SANS Reading Room, Retrieved November 2007 from http://www.sans.org/reading_room/whitepapers/incident/1791.php

Profitt, Tim (2007). Creating and managing an incident response team for a large company. SANS Reading Room, Retrieved November 2007 from http://www.sans.org/reading_room/whitepapers/incident/1821.php

Remote-exploit.org (2007). Backtrack. Retrieved January 2008 from http://www.remote-exploit.org/backtrack.html

Saudi, Madihah M. (2001). An overview of disk imaging tools in computer forensics. SANS Reading Room, Retrieved November 2007 from http://www.sans.org/reading_room/papers/download.php?id=643

Scarfone, Karen & Grance, Tim & Masone, Kelly (2007). Computer Security Incident Handling Guide (draft-SP800-61rev1). Retrieved October 2007 from http://csrc.nist.gov/publications/PubsSPs.html

Schultz, Eugene & Shumway, Russell (2001). Incident Response: A strategic guide to handling system and network security



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

breaches. SAMS. Retrieved October 2007 via Safari Books Online, LLC.

Searchsecurity.com definitions (powered by whatis.com) "incident response (2007)." Retrieved September 2007 from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1121085,00.html

Smith, Ricky D. (2007). Pros and cons of using Linux and Windows Live CDs in incident handling and forensics. SANS Reading Room, Retrieved September 2007 from http://www.sans.org/reading_room/whitepapers/incident/1706.php

Sourcefire (2007). Sourcefire Network security-SNORT. Retrieved December 2007 from http://www.sourcefire.com/products/snort/

Symantec (2008). Norton Ghost 12.0: System restore-PC backup software. Retrieved January 2008 from http://www.symantec.com/norton/products/overview.jsp?pcid=br&pvid=ghost12

Tech-faq.com (2008). "port scanner." Retrieved January 2008 from



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

http://www.tech-faq.com/port-scanner.shtml

Theunissen, David (2001). Corporate Incident handling guidelines. SANS Reading Room, Retrieved September 2007 from http://www.sans.org/reading_room/whitepapers/incident/645.php

Tripwire (2007). Tripwire: Configuration audit and control. Received October 2007 from http://www.tripwire.com/products/enterprise/servers_desktops.cfm

Wikipedia (2007). "honeypot." Retrieved October 2007 from http://en.wikipedia.org/wiki/Honeypot_%28computing%29

X-Ways Software Technology AG. X-Way Forensics: Integrated computer forensic software, Retrieved January 2008 from http://www.winhex.com/forensics/index-m.html

Zirkle, Laurie. Intrusion detection FAQ: What is host-based intrusion detection? SANS Intrusion Detection FAQ, Retrieved October 2007 from http://www.sans.org/resources/idfaq/host_based.php



© SANS Institute 2008, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |