INTRUSION INVESTIGATION AND POST-INTRUSION COMPUTER FORENSIC ANALYSIS

Federal Agent Byron S. Collie (Australian Federal Police)
Directorate of Information Warfare
Headquarters Air Command, Royal Australian Air Force

Abstract

Computer intrusions are becoming ever more prevalent in today's interconnected society. Given this fact, with more and more companies and organisations connecting to the Internet, the ability to effectively handle computer security incidents is becoming crucial for organisational survival.

This paper seeks to provide an overview of the handling and investigation of computer security incidents, from the perspective of a law enforcement computer crime investigator. Topics covered include incident response, intrusion investigation, real-time intrusion investigation, post-intrusion computer forensics, and legal considerations. Legal considerations are highlighted throughout the paper as are mechanisms through which organisations can greatly assist the incident handling and investigative processes.

This paper does not seek to replace the extensive references available on the subject of incident handling. It seeks to provide the reader with a basic knowledge of what a computer crime investigator should be able to expect from a victim organisation when responding to a complaint about a computer security incident.

1. Introduction

This document provides an introduction to the investigation of computer intrusions and further describes a number of post-intrusion computer forensic procedures and tools[1] for both the UNIX and Windows NT operating systems. Most organisations are not adequately prepared to deal with intrusions. They are likely to address the need to prepare and respond only after a network security breach occurs. The result is that when an intrusion is detected, often inadvertently, there is no appropriate decision chain in place and many decisions are made in haste. These problems can significantly reduce an organisation's ability to:

a. determine the source and extent of an intrusion,
b. protect sensitive data contained on systems,
c. protect the systems, the networks, and their ability to continue operating,
d. recover systems,
e. collect information about what has occurred in a manner consistent with legal evidentiary requirements, and

[1] Software described are indicative of the capabilities required to conduct an intrusion investigation. Description of these tools, their utilisation and functionality does not constitute endorsement by the author, the Australian Federal Police or the Royal Australian Air Force. Other similar tools are available and choice of software utilised is up to the individual administrator or organisation. Use of these tools is on an "At your own risk" basis and no liability is accepted by the author or the Commonwealth of Australia.

f. provide support to law enforcement (LE) investigations.

Organisations need to develop formal policies and procedures for handling intrusions that include preparation, detection, and response and cover those subjects listed above. The absence of systematic and well-defined policies and procedures can lead to:

a. extensive damage to data, systems, and networks due to not taking timely action to contain an intrusion,
b. the possibility of an intrusion affecting multiple systems both inside and outside an organisation because staff did not know who to notify and what actions to take,
c. negative exposure in the news media that can damage an organisation's public image and reputation, and
d. possible legal liability and prosecution for failure to exercise due care when systems are inadvertently or intentionally used to attack others.

The paper will not seek to comprehensively address the subjects of intrusion investigation or post-intrusion forensics but attempt to impart to the reader with a basic understanding of the topics and legal considerations affecting them.

1.1 Aim

The aim of the paper is to provide System Administrators (sysadms) and Information System Security Officers (ISSOs) with a general knowledge of the procedures for conducting a computer intrusion investigation. It will also describe generic computer forensic procedures, tools and techniques related to investigative process to ensure that ISSOs and sysadms are aware of the evidentiary requirements for preserving and analysing computer evidence to support investigation and prosecution.

The paper will briefly cover:

1. Definitions,
2. Incident Response,
3. Intrusion Investigation,
4. Real-Time Intrusion Investigation,
5. Post Intrusion Computer Forensics, and
5. Legal Considerations

2. Definitions

In discussing the subject of computer intrusions, we must first come to a common understanding of the key terms. In this paper the following definitions are used:

Computer Security Incident "A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism, or an attempted or threatened breach of those mechanisms.[2]"

[2] *Responding to Computer Security Incidents: Guidelines for Incident Handling*, Eugene Schultz, David Brown, Tom Longstaff, July 23, 1990, UCRL-ID-104689.

Computer Forensics A new and emerging discipline that involves the collection of audit and intrusion detection data, assesses damage to a computer resulting from an information attack or malicious destruction of data, permits data recovery, and produces evidence for prosecution purposes.[3]

Continuity of Evidence Verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. For a proven chain of custody to occur, the evidence must be accounted for at all times.

Incident Response Actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event occurs; involves contingency planning and contingency response.[4]

Intrusion An event of unauthorised entry, or attempted entry, to an Information System.[5]

Intrusion Detection Detecting, tracking and logging unauthorised activity on a computer system or computer network," and "Detecting and investigating anomalous activities that might be the result of an attempted intrusion or virus infection.[6]

Intrusion Detection System (IDS) Automated security tool that monitors computer network traffic and information systems for suspicious activity, collects information on targeted unit networks and systems by detecting unauthorised activity, and provides an Indications and Warning capability for networked information systems.[7]

Post-Intrusion The period immediately following the suspicion, and/or verification, by a sysadm or ISSO that an intrusion has occurred.

3. Incident Response

Successful network security requires not only successfully detecting intruders, but also responding appropriately to allow the intruder/s to be effectively contained and dealt with.

Incident response actions may include:

a. denying access to an intruder, possibly by disconnecting the affected system from the network and shutting down the system,
b. reporting the incident to an Incident Response Team (IRT) and/or LE,
c. containing an intrusion and limiting the actions of an intruder,
d. continuing operation to gather additional information, and
e. restoring the affected system.

---

[3] Australian Defence Headquarters Draft Definition.
[4] *Effective Incident Response*. Eugene Schultz. The Fourth Annual UNIX and NT Network Security Conference. Orlando, FL: The SANS Institute, October 24-31, 1998.
[5] ibid.
[6] *Practical Intrusion Detection - Introduction*, Sandy Sparks, FedCIRC-W and Rich Pethia, FedCIRC-E, UCRL-MI-127241, CSTC 97-063.
[7] Australian Defence Headquarters Draft Definition.

In conjunction with the proper authorities, sites can potentially track the intruder back to their system of origin. During this process, evidence may be collected that will not only indicate the damage that has resulted to the site's system but that could prove to be invaluable should prosecution of the attacker be undertaken. Intruder tracking is discussed later in the paper.

3.1 Incident Response Plan

Incident response protocols will vary from organisation to organisation and from site to site, and it is therefore imperative that organisations have a Security Policy or Plan that includes an comprehensive Incident Response Plan (IRP). This IRP should indicate what types of intrusion response actions require management approval and which are pre-approved. The IRP should document the circumstances under which the site intends to:

a. stay connected to pursue an intruder by gathering additional information,
b. protect systems by disconnecting and shutting down, and
c. conduct covert monitoring of network traffic and file access.

The IRP should document that the individuals or team responsible for intrusion response have pre-authorisation from management to disconnect from the network and shut down the affected system/s, if appropriate. This will cause a denial of service condition on the affected system until it is returned to operation.

The IRP should detail procedures for:

a. analysing all available information to characterise an intrusion, including assessing the damage and extent of an intrusion and an intruder's activities,
b. communicating with all parties that need to be aware of an intrusion and participate in handling it, taking into account that an intruder may be able to access and monitor communications,
c. collecting and protecting information associated with an intrusion,
d. containing an intrusion and determining what actions to take,
e. eliminating an intruder's means of access and any related vulnerabilities,
f. returning the systems to normal operation,
g. following up including performing a post mortem review of events as they occurred, and
h. conducting post-incident reviews of policies and procedures.

An example of a simple IRP is shown in Annex D of the Defence Signals Directorate (DSD) *Gateway Accreditation Guide*[8].

3.2 Incident Reporting

Incident reporting is a critical element of incident response. Many sites do not report incidents due to fears of ridicule, public opinion (particularly commercial sites), lack of knowledge or through sheer complacency.

For Australian Commonwealth Government organisations, an incident reporting mechanism known as the Information Security Incident Detection, Reporting and Analysis Scheme

[8] http://www.dsd.gov.au/infosec/gateway/

(ISIDRAS), has been developed by the DSD in consultation with the Australian Federal Police (AFP) and other agencies. For wider ranging incidents with respect to Australian organisations, the Australian Computer Emergency Response Team (AusCERT) provides an incident response point of contact.

AusCERT has assisted the AFP in a number of successful computer intrusion investigations by acting as the coordination point for contacting other sites that may have similarly been affected by intrusions originating from the same source. It should be recognised however that CERT teams have no obligation to provide information to LE and will normally operate under the provisions of a confidentiality agreement with their constituents. In most cases unless the victim site expressly agrees to it, the CERT will not normally provide detailed information about intrusions to any LE agency.

3.3 Response Options

There are a number of possible actions that can be taken once an intrusion into a network or system is suspected or has been confirmed. These options should be discussed in the organisation's IRP.

If an intrusion is only suspected, not confirmed, then it may be desirable to use real-time network monitoring, in conjunction with File Integrity Assessment (FIA) and other forensic techniques, to confirm whether or not an intrusion has in fact taken place. If an intrusion is confirmed however, then the protocols detailed in the IRP should provide the blueprint for what occurs next.

There are really only two options available with respect to responding to an intrusion:

a. disconnecting the intruder, system or network and recovering the system, or
b. leaving the system open and attempting to monitor and trace the intruder.

The first step in intrusion response is to stop the intruder's flow of traffic limiting the amount of compromised data in order to determine what has occurred. If possible this should be done in such a way as to make it appear that there has been some sort of fault that has disconnected the intruder. This can be accomplished using filters at the router to deny incoming access to the network from the intruder's host. If, however, they have compromised other systems they may then attempt to determine if access is being selectively blocked by probing from another site.

The best solution may in fact be to fully disconnect from the external network simulating a line dropout, however this is site dependent and the circumstances in which this may be done should be articulated in the IRP. In any case the result is a temporary respite to hold the hacker off and determine what other action should be taken. Dependent on circumstances and the directions given in the IRP, if an intruder has compromised an entire machine or the machine contains no critical data, the best way to analyse the situation may be to monitor the intruder in real time.

No matter what action is taken as an immediate response, some form of intrusion investigation should be conducted.

4. Intrusion Investigation

Sources of evidence with respect to intrusion investigation fall into 3 broad categories: host based evidence, network based evidence and the first person (direct) evidence of witnesses. Appropriate collection of data generated by system, network, application and user activities is essential to detecting signs of intrusion, conducting real-time investigations and preserving evidence so that it is admissible in court.

Of critical importance is maintaining appropriate records of what has been observed or discovered. A written chronological event log of the intruders suspected activities and site responses should be maintained. The log should detail what is suspected, what actions were taken, who was contacted as a result and what evidence of the intruders activities was located.

Resource utilisation including man-hours and equipment used to re-establish the system and locate the perpetrator should also be detailed to assist in later developing a victim impact statement.

4.1 Intrusion Detection Methods

Intrusion detection falls into two categories, manual intrusion detection, such as log analysis and manual correlation, and the use of automated Intrusion Detection Systems (IDS). The optimal solution is normally a combination of both mechanisms as IDS do not and will not detect all possible attacks.

4.2 Manual Intrusion Detection Methods

Knowledge of, and the ability to competently apply, manual intrusion detection techniques is essential to comprehensive network security. IDS, which rely on various techniques including attack signature recognition and system/network anomaly detection, can lull management and administrators into a false sense of security. Firewalls may engender a similar false sense of security, particularly if they are not managed properly.

Manual intrusion detection relies on the extensive knowledge an administrator has about his or her network. Applying manual intrusion detection methods in a time critical environment such as a post-intrusion scenario requires the sysadm/ISSO to be familiar and competent with the tools they will utilise to conduct their examinations and have a consistent set of procedures for conducting their analyses.

Manual intrusion detection is conducted by:

a. identification of anomalous entries in system logs,
b. verification of the integrity of critical system files,
c. identification (and preservation) of suspicious users, processes, files and other intruder remnants,
d. analysis of network transaction records, and
e. correlation of all relevant data to develop a picture of what has occurred.

Not all attacks or suspicious activities need to be investigated in the same way, so tools utilised to assist in an investigation must allow the user to access various levels of detail according to their needs. This requires the sysadm/ISSO to maintain a comprehensive suite of

audit, data recovery and analysis tools to provide the flexibility necessary to deal with the activities of an unknown intruder.

4.2.1 System Log Analysis

Log files contain information about what activities have occurred over time. They are often the only record of suspicious behaviour making them probably the most crucial form of evidence in an intrusion investigation. There must be recognition at a high level within an organisation that system log files are in fact crucial records for an organisation and they must be treated as such.

Different systems provide different types of logging information and some systems do not provide adequate logging in their default configuration. Some “trusted” operating systems however, such as those accredited by national security agencies for classified use, produce a much larger quantity of logs with a consequently higher degree of detail.

Sysadms/ISSOs should identify, prior to any intrusion, the types of logs and logging mechanisms available to each system (file access logs, process logs, network logs, application specific logs, etc.) and identify the data recorded within each log. These logging mechanisms should then be enabled to the maximum extant possible. Failure to enable these mechanisms may seriously impact on a site's ability to determine whether or not an intrusion has been attempted or in fact succeeded.

Simply enabling logging is not enough however. A site must have the necessary procedures and tools available to process and analyse the products of logging. There are many tools that can assist in this process.

4.2.2 File Integrity Assessment (FIA)

Intruders, as part of their normal *Modus Operandi*, will alter the configuration of a system to allowed continued access, conceal their presence and carry out their goals on the system. If no record of the system's baseline configuration is maintained determination of what modifications have been made by an intruder to the system will be difficult. File Integrity Assessment (FIA), through the use of cryptographic checksums, creates a baseline database of a system, and then allows the administrator to monitor files for unauthorised changes. System files should not change, except when updated or patched, and log files should only grow in size.

Forensic application of FIA allows administrators to build a complete list of what has been altered on a system. The FIA of the altered system will form an essential part of the evidence supporting prosecution, particularly where legislation imposes greater penalties for the insertion, alteration or deletion of data in a system as is the case with Australian Commonwealth law.

After a compromised system is backed up using binary imaging as described later, a FIA should be run to provide a baseline for the evidence to be handed to LE. This guarantees that no matter how many tests or analyses are done on restored image of the system subsequently, the integrity of the altered system is maintained. This way it can be demonstrated that the file system or backup tape is unaltered at the point in time in the future when the case is ultimately prosecuted.

The most well known automated tool for carrying out FIA is Tripwire[9], which is available for both UNIX and NT systems. Many anti-virus programs also use cryptographic checksums for file validation. A good anti-virus program may also, therefore, assist in intrusion investigation. Manual cryptographic checksums may also be developed using freely available software implementing Message Digest 5 (MD5) and the Secure Hash Algorithm – 1 (SHA-1).

4.2.3 Intruder Artifacts

Intruders often leave all sorts of files on the systems that they compromise. These can range from sniffer log files, stolen password files, exploit scripts, and source code to various programs. Smarter and more experienced intruders will often only leave processes running in memory.

Generically, programs that have been left behind by intruders are called *remnant files*. Potentially malicious scripts, source code and programs are referred to as *artifacts*. Some of these files may not, in fact, be malicious however they must always be treated as such until they have been comprehensively analysed.

Intruders normally replace system files with other files that differ in operation from the original program, but have the same name. These trojan programs are popular among intruders as they offer a method of concealment for their activities. The trojan programs themselves may also provide valuable information or functionality to support further intrusions.

Many trojan programs are identical to their original namesake with respect to all file system attributes except content, meaning that only a proper cryptographic checksum analysis can detect a difference between files. Keeping off-line, read-only lists of checksums of system files and important programs is therefore essential. Cryptographic checksums of the artifact/s on the original system are also essential when giving copies to LE in order to validate the integrity of the copy of the artifact provided.

If artifacts have been recovered from a compromised system, LE may sometimes request a site assist them by analysing the artifact to determine its function. This may prove particularly important if a search warrant is later executed on a suspect and uncompiled trojan code recovered from their computer system. In some cases the LE agency may in fact provide the victim site with copies of the seized code and request they compare it with the artifacts recovered from the site.

Artifacts should not be analysed on compromised system/s. Care should be taken to make a copy of the artifact/s plus surroundings that, where possible, exactly mirror the original environment. Ideally artifacts should be analysed on an isolated system.

4.2.4 Network Transaction Auditing

Network transaction auditing is a useful tool in determining what is happening on your network both in real-time, and from a historical perspective. Like intrusion detection (which

[9] http://www.tripwiresecurity.com

transaction auditing supports), network transaction auditing can be separated into methods and tools that support historical and/or real-time analysis.

4.2.4.1 Historical Analysis

There are a number of benefits to maintaining historical network logs including:

a. verifying network security policies are effective,
b. detecting attempts to break through firewalls and host-based security mechanisms,
c. analysing network service utilisation,
d. developing models of network behaviour so that deviations can be detected, and
e. troubleshooting transient network problems including Denial of Service attacks.

Logs from network infrastructure devices such as routers and switches may also provide an appropriate source of data for network transaction analysis. The issue with these types of logs however comes down to the quantity. If an appropriate parsing mechanism is in place to reduce the quantity to a manageable level then these logs may provide a valuable source of evidence.

Tools like Argus and Tcptrace support analysis of network traffic in both textual and graphical formats. Graphical analysis particularly can make identification of anomalous network conditions, such as those that may be encountered during intrusion incidents, easily discernible.

Argus[10] is a publicly available, generic UNIX IP transaction auditing tool that was developed by the Carnegie Mellon University's Software Engineering Institute. Argus generates network traffic status records for the network activity it sees flow past the systems network interface.

Tcptrace[11] is a publicly available UNIX utility, written by Dr. Shawn Ostermann of Ohio University, to allow analysis of network connections captured by a number of popular network packet capture programs including tcpdump, snoop, etherpeek and netm. Tcptrace will extract data from the dump files produced by these programs in a user definable format for both TCP and UDP network connections.

At LE request Dr. Ostermann has modified tcptrace to allow data extracted to be easily fed into a relatively simple network connectivity database that can then be easily analysed using graphical link analysis tools such as Analyst Notebook[12] and Netmap[13].

4.2.4.2 Graphical Link Analysis Tools

Graphical link (entity relationship) analysis tools can provide significant assistance in analysing traffic monitored using appropriate monitoring software. These tools treat data as a network of nodes and links. Nodes can be any entity, in the case of network traffic; normally the system IP address and originating/destination port. Links are relationships between nodes, in the case of Internet traffic, TCP/IP packets. Nodes can have attributes that further define

[10] ftp://ftp.sei.cmu.edu/pub/argus-1.5
[11] http://jarok.cs.ohiou.edu/software/tcptrace/tcptrace.html
[12] http://www.i2.com.uk
[13] http://www.netmap.com.au

the node and links can have qualifiers that detail the link. Analysis is carried out through filtering, sorting, grouping and colouring nodes based on their various attributes. Links are analysed by filtering and colouring based on their relative qualifiers. Various network layouts can then be utilised to then display the relationships within the network to reveal patterns that may be indicative of intrusive behaviour.

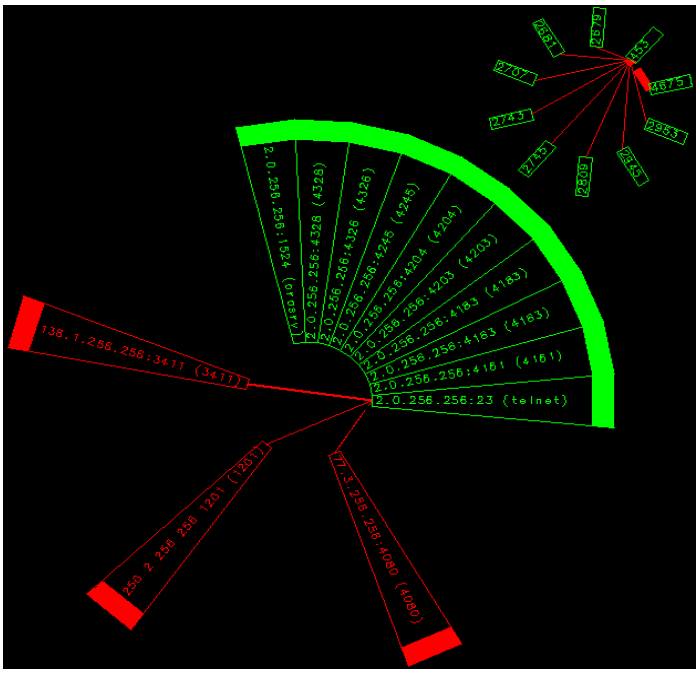

Figure 1 - Netmap Link Analysis

4.2.4.3 Real-Time Network Transaction Auditing

If an intrusion has been detected in real-time, the ability to determine what systems are being accessed and the types of network connections that are being made across the network is crucial. There are a number of commercial and freely available network analysis utilities that can provide real-time visibility of transactions on a network for both network management and network security purposes. One such tool is Etherboy[14] shown in Figure 2.

Network management systems such as HP Openview[15] may also provide significant assistance providing visibility of what is occurring on the network in real-time.

[14] http://www.ndg.com.au
[15] http://www.hewlettpackard.com

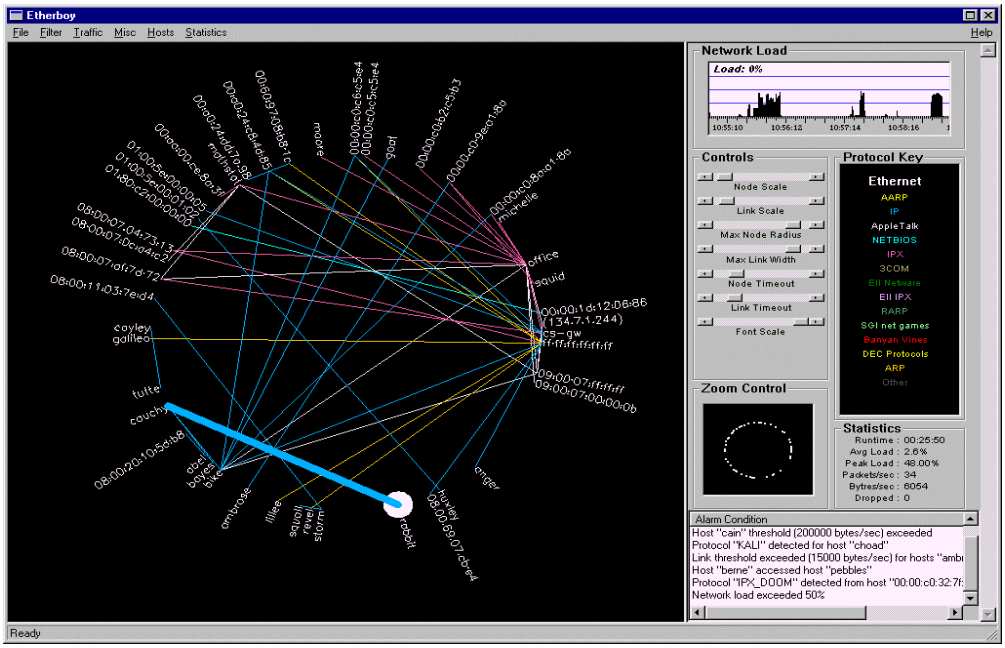

Figure 2 - Etherboy display

4.3 Intrusion Detection Systems (IDS)

The IDS market place is very volatile given the movement of commerce to the Internet and the race to market network security products to protect and support Internet connectivity and commerce. Some of the better known commercial IDS include RealSecure[16] from Internet Security Systems, Sessionwall-3[17] from Platinum Systems, Netranger[18] from Cisco Systems and Cybercop Monitor[19] from Network Associates.

There are also a number of free IDS available on the Internet for non-commercial use. These systems include SHADOW[20] and Network Flight Recorder[21] (NFR). These freely available systems are not as user friendly as the commercial systems but they are much more customizable.

Automated IDS are useful for perimeter defence, however they cannot keep up with the fact that security threats are constantly changing and may differ from enterprise to enterprise. Network based IDS do not address the issue of internal threats to the network and, like firewalls, automated IDS need to be properly monitored and maintained.

5. Real-Time Intrusion Investigation

The process of conducting a "real-time" investigation of an attack begins with the IRT determining the bounds of investigation, in accordance with the organisation's IRP. This should also be done in consultation with appropriate legal and LE authorities to ensure that

[16] http://www.iss.net/press_rel/rs_new.php3
[17] http://www.abirnet.com/sw3intro.html
[18] http://www.cisco.com
[19] http://www.nai.com/products/security/cybercop_scanner/monitor.asp
[20] http://www.nswc.navy.mil/ISSEC/CID/
[21] http://www.nfr.com

evidentiary requirements and legal obligations are addressed and the LE agency's own investigative actions are not going to be compromised by site activities.

The victim site may also need to consider a number of factors (if they haven't been considered in the IRP) before deciding to undertake a real-time investigation including:

a. whether the system is being used to compromise other sites,
b. legal issues with respect to monitoring of network traffic,
c. whether continued monitoring will yield more information about the intruder, and
d. which systems are mission critical and need to be secured immediately.

A real-time investigation, by revealing the intruder's intent, may assist with evaluating and limiting the dispersal of the compromised data. It will also reveal the types of vulnerabilities being exploited, which can help to further secure the network. It may be possible to set up a "sandbox" or "honeypot" system to allow the intruder to access dummy files in order to determine their intentions.

5.1 "Sandboxing"

"Sandboxing" is a method of containing an intruder by directing them into a "honeypot" subnet or system. This system, which appears similar to an organisation's legitimate network or system is in fact specifically set up to engage and contain the intruder so that they may be monitored and traced. If an appropriately configured system is available with false and misleading files containing information relevant to the organisation, then it may also be possible to determine the intruder's particular interest and possibly, their motive. Clifford Stoll used the technique effectively when tracking his intruder in *The Cuckoo's Egg*.

"Sandboxing" is relatively resource intensive activity requiring access to appropriate "deception" systems and monitoring capabilities. High level authorisation may also be required for the activity, particularly if the intruder is utilising the compromised system for further attacks on external organisations. Legal issues related to entrapment must be considered when conducting this activity to ensure that evidence obtained is admissible in court.

5.2 System Logging

One of the first actions taken, after a system has been backed up in a manner appropriate to secure evidence, is to enable all available audit logging. This particularly includes **process accounting** that should show the commands and programs an intruder has used. Intruders routinely delete entries from audit log files so it is suggested, if possible, to save and store the logs in an encrypted form.

Log files that show suspicious activities should be printed out and signed once it has been confirmed the site has been compromised. Logs should always be saved to back up media after first running a message digest or checksum to validate them. The copies should then also be checked to validate the copy process.

5.3 Intruder Tracking Procedures

Attempts should be made to track the intruder back to the originating site in order to both help determine the nature of the break-in and to gather evidence for prosecution. Great care should be taken in attempting to track an intruder as alerting the intruder that they have been discovered and are actively being pursued may cause them to completely disconnect and lie low, ruining the chances of location.

Historical tracing of an intruder is problematic and may in fact prove impossible unless victim sites provide detailed logs and evidence is recovered from the suspect's computer. In fact, it may only be possible to carry out prosecution for offences carried out after the identification of the suspect and when appropriate monitoring and tracing mechanisms have been in place for some time to gather sufficient evidence of the hackers activities.

Monitoring and tracing of victim's may, however, support prosecution of historical activities if historical monitoring can be correlated with real-time monitoring to show the intruder's activities are of sufficient technical uniqueness that another intruder could not have been responsible for the activities. Other historical evidence including remnants recovered from victim sites and material retrieved from the suspect's hard drive may then be sufficient to support prosecution.

If sites have implemented appropriate intrusion detection and monitoring mechanisms prior to an intrusion actually occurring then the chances of both real-time and historical tracking and prosecution are greatly increased. The other lesson is that LE agencies **must** be advised early enough in the site's intrusion investigation process to allow them to be able to assist in tracking of the intruder over the Internet and through other telecommunications networks.

5.3.1 Internet

Due to the extent and availability of the Internet, most intrusions will of course have some Internet based element. If an Internet based intrusion is detected then there are a number of mechanisms to identify the source of the attack. As previously mentioned, router logs may provide extensive visibility of the intruders activities particularly identifying the originating IP address. Execution of a **traceroute** command may also show the path to the attacking system. The originating system should **NOT** however be "pinged" or "fingered" as this may alert the intruder.

IP and DNS spoofing on the part of the intruder, may however render these tracing activities ineffectual.

5.3.2 X.25 Data Networks

Tracking of intruders over commercial X.25 networks is easier than tracking over the Internet. All data transactions on X.25 are logged and it is possible to obtain the Network User Identifier (NUI) and Network User Address (NUA) of a suspected attacker from your own transaction logs or from those of the X.25 provider.

5.3.3 Dialup Intrusions

Intrusions into systems and networks via dialup modem connections over Public Switched Telephone Networks (PSTN) still occur. Tracing intruders carrying out these types of intrusions is however becoming easier due to the introduction and proliferation of publicly available caller identification (CallerID) systems. Telephone technologies and legislative requirements for conducting telecommunications tracing do vary from country to country, so there is, however, no one solution to carrying tracing intrusions over the PSTN particularly if the connection crosses international boundaries.

If a dialup attack is discovered in progress then, in most countries, the victim may be able to contact the harassing telephone call area of the Telephone Company to request a trace be conducted. Alternatively, the local LE computer crime unit may be able to arrange a trace. The appropriate LE agency should in any case be contacted as the results of any successful trace are normally only provided to the investigating officer of a LE agency.

5.3.4 Intruder Evasion Techniques

Intruders have developed a number of techniques they may use to make tracking by victims, CERTs, national security and LE agencies more difficult. The most common of these techniques is known as ***connection laundering***.

Connection laundering involves the use of a number of different sites and telecommunications services in order to defeat tracking and tracing activities. A well-known Australian hacker, Timothy John COOPER, aka "The Crawler", used sophisticated connection laundering techniques during extensive intrusion activities in 1992 and 1993.

One of the intrusions with which he was charged serves as an excellent example of connection laundering:

a. COOPER used his computer and modem from home to dial into a Commonwealth government agency over the PSTN (the first telecommunications network),

b. the Commonwealth agency's modem is connected via a network to an X.25 data communications terminal. He used the international X.25 data communications network (the second telecommunications network) to gain unauthorised access to a computer system operated by a US Government agency,

c. the compromised US Government computer system is also connected to the Internet (the third telecommunications network). This system is then used to gain unauthorised access over the Internet to another system operated by another Commonwealth government agency in Canberra, and

d. this system is then used to gain access to other computer systems operated by that agency using Telstra’s domestic X.25 network (the fourth telecommunications network).

As can be seen from this example, real time tracing of an intruder may prove extremely difficult given the possible requirement for international coordination of the tracking and tracing activities. An example of an intrusion trail is illustrated in Figure 3. As mentioned

previously, differing legal requirements for conducting tracing in each jurisdiction may also make this coordination even more difficult. As can also be seen however, it can be done.

Figure 3 – A notional intrusion trail

Another mechanism that intruders have been observed using is termed a "telnet bouncer". This "bouncer" is a small program that this intruder installs on a compromised system to allow them to use the system as a "conduit" to their real destination, without having to actually log in to the system. The program completely bypasses the normal login process, and it's logging mechanism. Normally the program is installed to reside on a high numbered port masquerading as a legitimate program. The three intruders charged over the US "Solar Sunrise" operation in 1998 extensively used telnet bouncers.

5.4 Network Monitoring

Network monitoring is in many circumstances conducted as a day to day activity by network engineers for network administration and troubleshooting. It can also be used as an extremely effective investigative tool to assist in determining:

a. if the intrusions are ongoing,
b. what systems in your network have been compromised,
c. how the system was originally broken into,
d. where the intruder has installed their files,
e. what their motivation is, and
f. what external systems has the intruder compromised.

There are however, very strict legal factors that must be considered before network monitoring is employed. These considerations will be discussed in some detail later.

Network monitoring systems can vary greatly in capability. In some instances, the tool will be a network management tool that is being adapted to meet a security requirement. Examples of this are the Windows NT Network Monitor (NetMon) and tcpdump.

In other cases, the system may be a purposefully designed piece of software or hardware that has been specifically designed for capturing, displaying and analysing the contents of network communications. Examples of these systems in commercial form include Sessionwall-3 and

T-Sight.[22] The freeware UNIX software Review provides a similar style of graphical interface as these systems for tcpdump.

Windows NT Network monitor (Netmon) is a standalone NT program provided as part of Microsoft's System Management Server (SMS) that allows authorised users to monitor traffic specific to the system where it is installed. It does not capture all network traffic on a given network segment and does not provide an interpretation of the data streams, only provide access to the raw packet data itself.

The user portion of the program calls upon the services of the Network Monitor Agent, which is a kernel driver that ships with NT. The Network Monitor Agent also provides an interface for a remote machine to connect and capture local data, provided it passes authentication.[23] Netmon can also be configured to utilise a trigger feature that will start capturing data based on the appearance of specific data in a packet. This feature can be utilised as a simple IDS that can start capturing data on suspicious activities and provide an alert to the sysadm/ISSO.

Tcpdump[24] is a freely available UNIX program that is primarily utilised by network administrators for protocol analysis. Tcpdump will capture all data passing over a network segment and provides a rich language to allow user specification of what data to capture. Tcpdump has also been ported to Windows NT[25]. The native output of tcpdump is not very useful and individual network connections need to be extracted and translated into meaningful information. Review, described below, and tcptrace, described previously, are systems for extracting and analysing tcpdump data.

Sessionwall-3, shown in Figure 4 and mentioned previously, is a commercial program that functions as both a network monitor and an IDS. It also provides the capability to disconnect certain types of network sessions at the operator's discretion.

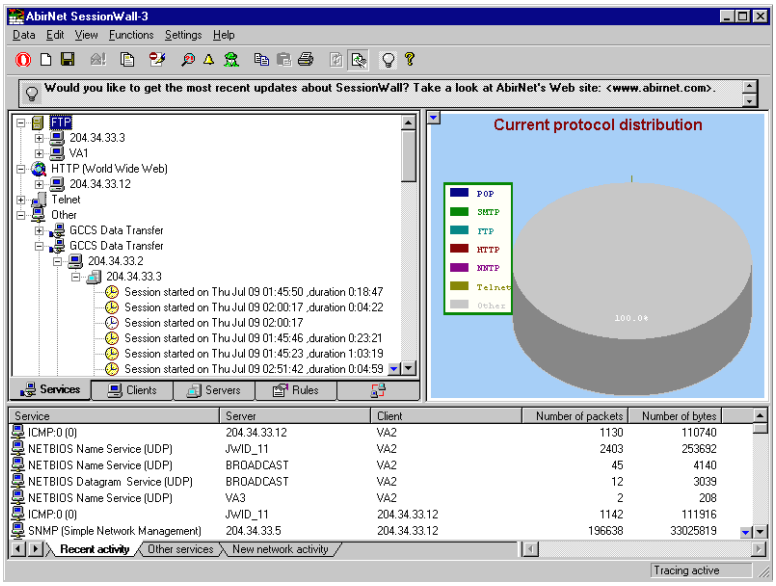

Figure 4 – Sessionwall-3

[22] http://www.engarde.com/software/t-sight
[23] *Practical Intrusion Detection - Non-UNIX Based Systems*, Marcey Kelley, FedCIRC, UCRL-MI-127226, CSTC 97-062.
[24] ftp://ftp.ee.lbl.gov/tcpdump.tar.gz
[25] http://netgroup-serv.polito.it/analyzer

Review[26], shown in Figure 5, is a freeware UNIX X-Windows Tk/Tcl interface for tcpdump, was developed by Mr. Steve Romig from Ohio State University as a tool for analysing intrusions. The tcpdump, tcptrace and Review combination provides a fully functional network monitoring package for the UNIX environment that is readily distributable to victim sites. Tcpdump is native to many operating system distributions these days meaning many sysadms/ISSOs are familiar with the program. This, together with the platform portability of Review and tcptrace allow a fully functional network monitoring system to be set up with relatively little trouble.

One particularly useful feature of Review is it's ability to be able to extract files from network file transfers. This can include images on web pages or files transferred using ftp.

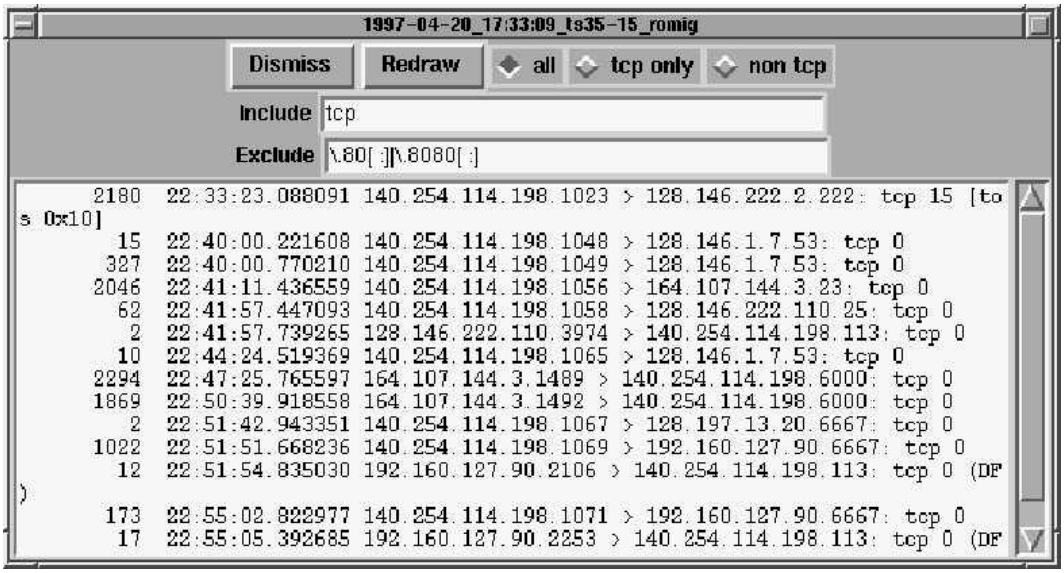

Figure 5 – A typical Review network session summary window, filtering out web traffic

6. Post-Intrusion Computer Forensics

As previously stated, every public network connected organisation should have an IRP that includes a detailed Post-Intrusion Forensic Plan[27]. The challenge for the organisation, in concert with appropriate LE agencies, is to be able to obtain computer evidence relating to a computer security incident in a manner that ensures its authenticity and veracity. Due to the transitory nature of information stored on computer systems, there are a number of legal obstacles that have to be addressed, namely:

a. computer evidence can be readily altered or deleted,
b. computer evidence can be invisibly and undetectably altered,
c. computer evidence can appear to be copied while in fact it is undergoing alteration,
d. while in transit, computer evidence can share the same transport pipeline as other data,
e. computer evidence is stored in a different format to that when it is printed or displayed, and
f. computer evidence is generally difficult for the layman to understand.

[26] http://ftp.net.ohio-state.edu/users/romig/review
[27] This material is based heavily on material provided in the Defence Signals Directorate *Gateway Accreditation Guide Sample Forensic Plan*.

In conducting computer forensic procedures to support an intrusion investigation, the person responsible for conducting the investigation at the site (referred to as the Incident Investigation Officer, IIO) should be appointed from within the site IRT. This person then becomes responsible for the management of the incident until the incident closure or until they are formally relieved by someone in higher authority.

6.1 Chronological Event and Evidence Registers

As previously stated, one of the most crucial activities conducted during an incident is keeping a written chronological event register. This log should document the intruders suspected activities and the site's responses detailing what is suspected, what the site did and who was contacted as a result. Who, what, why, where, when and how should be covered. Detail should cover resources used including man-hours and equipment used to re-establish the system and locate the perpetrator. A separate evidence register listing full details of what evidence has been located, by who, how and when, and the chain of custody should also be kept.

Access to labeled evidence shall be restricted to members of the IRT and LE only, and such access shall be for activities directly related to aspects of the ongoing investigation or prosecution. Any officer given access to labeled evidence shall record details of the access in writing in the evidence register. Such details should include:

a. who is accessing the evidence and for what purpose,
b. the date and time of such access,
c. details of the forensic procedures that were carried out; and
d. the name of the host on which the forensic procedures were carried out.

Ideally only one person should be responsible for securing potential evidence. This makes continuity of evidence proceeds much easier and statements for court much simpler.

6.2 'Freezing the Scene'

Many administrators respond to an attack by turning off a compromised system and re-starting their system from backups and/or vendor disks. During this process, they neglect to collect information about the attack's chronology of events. While restoration can be a long process in itself, it does not provide information on the extent of the damage to the network, the information compromised, or the identity of the intruder.

This information can be critical whether you are restoring an entire network or recovering from data theft. It is also essential if prosecution of the intruder is to be sought. Both attempted and successful prosecutions, of course, will help to prevent future security breaches by illuminating the consequences of network break-ins or data theft.

One of the duties of the IIO is therefore to ensure that any forensic procedures carried out on the system do not alter the material. Immediately after the intruder has been cut off from the system or it has been identified that an intrusion into a system has occurred, a backup of the entire machine needs to be made. This needs to carried out before **anything** else is done as even a simple directory scan can destroy important data on the system and render any further evidence obtained inadmissible. Even people with extensive computing experience, but no legal knowledge, can carry out activities that make critical evidence inadmissible.

The best form of immediate backup to make is a binary disk image. This ensures that data that has been deleted by the intruder, but may be recoverable is preserved on the backup. This type of backup also preserves the integrity of all the time stamps on the system. There are a number of freeware and commercial utilities available for carrying out image backups including the UNIX operating systems native **dd** command, the commercial program Ghost[28] and the LE program Safeback.[29]

Once completed, the backup should be write protected and labelled. This label should include the time and date, system name/IP, backup software used and the name and signature of the person making the backup. A witness should countersign this signature. This backup should then be secured in a lockable container with very restricted access.

6.3 Previous Backups

Previous system backups, not necessarily image backups, should be isolated and secured. A copy of the software utilised to make the backups should also be isolated and secured. These previous system backups, possibly made prior to the intruder's access, are required to show the original status of the system and may be useful in determining when the first intrusion occurred and what the intruder has done over time to the system. This is particularly important in developing a chronology of events surrounding the intrusion.

6.4 "Capturing the Moment"

One of the best methods of conducting an examination of an original compromised system is to use a terminal logging program, like UNIX's **script** command, to retain a permanent record of the examination. Similar utilities are available for Windows systems.

Some specific forensic analysis systems have been prepared with video cards with output to a video recorder. This captures everything seen on the computer monitor to a videotape which then becomes the best evidence of the examination. Actually using a standard video camera to tape the examination is another possibility.

6.5 Examining the Original System

Exact techniques employed in examining the compromised system will vary, however, at a minimum the following actions should be taken:

a. any clock drift in the system should be noted identifying the variance and the correct time,
b. a FIA should be done, generating cryptographic checksums of all the files on the system and saving these to removable media,
c. any suspicious processes running in memory should be dumped to disk using an appropriate tool. For UNIX this may be the **gcore** or **kcore** commands. For an NT system it may mean running the program **Handleex**[30] and a debugger,
d. any log files should be copied to removable media using appropriate commands to preserve file attributes,

---

[28] http://www.symantec.com/product/ghost
[29] http://www.sydex.com/sbqa.html
[30] Handleex, Regmon, NTPmon, Portman, Tcpview and Filemon, all useful programs for analysing NT systems are available from http://www,sysinternals.com.

e. make backups of damaged files, altered files or any other suspicious files found on the system,
f. a copy of the program or utility which was used to make the file copies should be placed onto the same physical media as the file copies, and
g. a cryptographic checksum should be made for each file prior to and after copying to validate the copy process. The resultant signatures should be documented and securely stored.

6.6 Online Evidence

If approval is given to keep the compromised system open to monitor and trace the intruder any important data on the system relating to intruder's discovery should be removed or encrypted using DES. This particularly should include audit log files particularly if no network monitoring system is available. This makes it difficult for intruders to employ their usual technique of editing entries from the system audit logs.

6.7 Time Stamping

System time stamping is a ***critical*** factor in being able to correlate the disparate events at different locations that may surround a computer security incident, particularly where there are multiple sites involved. Records where date stamping is critical include all forms of computer evidence but particularly:

a. telephone connection records,
b. modem bank logs,
c. router logs,
d. system access and related logs, and
e. system files.

To show the direct linkage between the suspect and the victim system, the investigator must correlate these records relying on time stamping. Clock drift and different time zones further complicate this process. In one particular case, for one agency, the clock drift (from UTC/GMT) varied for six compromised machines from 20 minutes to 6 days.

Sysadms and ISSO's can easily make this correlation process easier for the investigator (as well as themselves) by ensuring their systems and networks utilise a common, validated time source. A secure network time server is the best to ensure time and date stamping is consistent across the network. This consistency should include network infrastructure such as switches and routers.

One of the first things a sysadmn/ISSO should do when examining a system is look at the system's time and date. This will quickly identify any clock drift in the system and may also identify if the intruder has been tampering with the system clock itself.

Very importantly, if there is clock drift or is evidence that the clock has been tampered with, ***DO NOT ALTER OR RESET THE SYSTEM CLOCK!!!!*** Doing so makes examination of the system files and processes that much more complicated. The system should be backed up completely prior to making any alteration. Comprehensive notes about any alteration made should include what the clock's drift was, the time zone utilised, and whether daylight saving time was in use on the system.

In referring to activities on the system/network with both LE agencies and CERT agencies, use of UTC/GMT is preferred to allow correlation with other, possibly interstate or international incidents.

6.8 Forensic Analysis of the Backup

The easiest way to do this is to have a specific secure host established for the purpose. As with artifact analysis, this system should be isolated. The image backup can then be restored to this system without destroying the "fingerprints" on the data. Data recovered can then be used to determine the method of compromise and what actions the intruder has carried out on the system. The IIO is to ensure that any forensic procedures carried out are repeatable by others, particularly by members of the defence team, and achieve the same results.

6.9 Intrusion Reconstruction

Intrusion reconstruction involves correlating and analysing all data recovered with respect to the intrusion. Documentation supporting reconstruction can include spreadsheet correlating log time, network diagrams and related methods for correlating and visualising data. The graphical link analysis tools described previously may also prove useful.

In analysing the intrusion any information gaps should be hightlighted.

7. Legal Considerations

In order to meet legal requirements for the production of computer evidence in court, the evidence handling protocols mentioned throughout this paper have been developed. These protocols determine that computer evidence needs to be:

1. **Admissible**. It must conform to certain legal rules before it can be put before a jury;
2. **Authentic**. It must be possible to positively tie evidentiary material to the incident;
3. **Complete**. It must tell the whole story and not just a particular perspective;
4. **Reliable**. There must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity; and
5. **Believable**. It must be readily believable and understandable to members of a jury.

The procedures highlighted throughout this paper should be applied to any form of computer evidence to ensure that it may presented before a court. Where there is any doubt with respect to the admissibility of a piece of computer evidence, seek legal advice or talk to a LE agency.

7.1 Network Monitoring Legal Considerations

Specific conditions must exist to allow the use of content monitoring of network traffic and keystroke monitoring of users on systems. Those conditions are:

a. where it is suspected systems have been compromised and the monitoring is being carried out to locate and determine the activities of the intruder/s,

b. where content and keystroke monitoring of user activities has been explicitly acknowledged (by the user) in the system/network acceptable usage policy, or

c. where systems and gateways on the network have banners indicating access to the system is an acknowledgment of agreement to allow monitoring of the user's activities.

A suggested monitoring banner is as follows:

> **"This system is for the use of authorised users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this network/system monitored and recorded by system personnel.**
>
> **In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorised users may also be monitored.**
>
> **Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."**

This section was modified from CERT Advisory CA-2:19.Keystroke.Logging.Banner.Notice

Privacy must also be considered. In Australia, unlawful interception of telecommunications is a federal offence. Where there is any doubt about the legality of conducting network monitoring to support an intrusion investigation, legal advice should be sought from a solicitor or through a LE computer crime agency.

8. Conclusion

This paper has sought to provide an overview of the processes used to investigate computer security incidents. It has also sought to provide an overview of the computer forensic processes required to preserve evidence related to an intrusion. Mechanisms, tools and techniques required for effectively handling an intrusion, from a victim site perspective, have also been broadly mentioned.

There is a large amount of material freely available on the Internet dealing with the handling of incidents. Some of it has been prepared in consultation with law enforcement but a significant amount has not. This paper has hopefully provided some idea of the perspective a computer crime investigator brings to an intrusion, both from an investigative perspective and from a forensic perspective.

References:

K. Pichnarczyk, S. Weeber, R. Feingold, *"UNIX Incident Guide: How to Detect an Intrusion"*, CIAC-2305 R.1, December 1994.

The SANS Institute. *"Computer Security Incident Handling: Step by Step"*, November 1998.

Defence Signals Directorate, “ACSI-33 - Security Guidelines for Australian Government IT Systems,” April 1998.

J. Kochmar, J. Allen, C. Alberts, C. Cohen, G. Ford, B. Fraser, S. Konda, K. Kossakowski D. Simmel,*“Prepating to Detect Signs of Intrusion”*, CMU/SEI-SIM-005, June 1998.

R. Firth, G. Ford, B. Fraser, J. Kochmar, S. Konda, J. Richael, D. Simmel, Lisa Cunningham,*“Detecting Signs of Intrusion”*, CMU/SEI-SIM-001, February 1999.

K. Kossakowski, J. Allen, C. Alberts, C. Cohen, G. Ford, B. Fraser, E. Hayes, J. Kochmar, S. Konda, W. Wilson,*“Responding to Intrusions”*, CMU/SEI-SIM-006, February 1999.

M.J. West-Brown, D. Stikvoort, K. Kossakowski, *“Handbook for Computer Security Incident Response Teams (CSIRTs)”*, CMU/SEI-98-HB-001, December 1998.