Internet Engineering Task Force   Nevil Brownlee
INTERNET-DRAFT   The University of Auckland
                                                        April 1996

Expectations for Security Incident Response

Status of this Memo

Abstract

This document is intended to facilitate the setting of expectations regarding the operation of Security Incicident Response Teams (SIRTs). It describes the various important topics in the form of a 'template,' through which every SIRT should describe itself and its functions.

SIRT clients have a legitimate need and right to fully understand the policies and procedures of their Security Incident Response Team. A SIRT's template supplies details for the various important topics which clients must consider when selecting a SIRT.

Contents

1 Introduction 2
1.1 Definitions 3
1.2 Publishing SIRT Templates 5
1.3 Establishing Peering Between SIRTs 6

2 Description Template: Security Incident Response Team 6

3 Purpose of the Template 8
3.1 Other Related Material 8

4 The Security Incident Response Team Template 9
4.1 Contact Information 9
4.2 Template Updates 10
4.2.1Date of last update 10
4.2.2Distribution list for Template Updates 10
4.3 Charter 10
4.3.1Mission Statement 10
4.3.2Constituency 11
4.3.3Sponsoring organisation / affiliation 11
4.3.4Authority 11
4.4 Policies 12
4.4.1Types of incidents and level of support 12
4.4.2Co-operation and interaction with other organizations . . . 12
4.4.3Reporting and Disclosure 13
4.4.4Communication and authentication 14
4.5 Services 14
4.6 Incident reporting Forms 15
4.7 Disclaimers 15

5 Secondary Purposes of this Document 16

6 Appendix A: Note on procedure definitions 16

7 Appendix B: Known Incident Response Teams 17

8 Appendix C: Sample Incident Reporting Form 17

9 Security Considerations 25

10 Editor's Address 25

1 Introduction

The GRIP Working Group was formed to produce guidelines and recommendations to facilitate the consistent handling of security incidents in the Internet community. Although it is focused on the Internet, many of the concepts discussed will also be useful for other forms of local- and wide-area networks and internets.

Many computer security incidents either originate outside local community boundaries and affect other 'outside' sites, or originate outside the local community and affect hosts or users within it. The handling of security incidents will therefore often involve multiple Security Incident Response Teams. Because of this characteristic it is important for every community to have a good security policy, and to have a Security Incident Response Team (SIRT) in place to manage communications across community boundaries in a consistent way.

In the past there have been misunderstandings regarding expectations of response teams. The goal of this document is to provide a framework in which to set expectations. By defining such a framework the community can express areas and topics that need to addressed by any SIRT.

'Consistent handling' implies that any group calling itself a SIRT must react to security incidents or to threats of them in ways which the Internet community agrees to be in its general interest. Every SIRT needs to define clearly the services they offer and the level at which they are offered to the client. Such definitions will be particularly important in contracts and/or agreements which SIRTs make with their clients.

The "Expectations for Security Incident Response" document is seen as resting on the work of individual SIRTs and the cooperation between them. It recommends a 'template' through which every SIRT should describe itself and its functions. It further recommends that templates should be accessible among teams, to make possible a fully effective cooperative response framework for incidents or threats across the entire domain affected by them.

1.1 Definitions

This section defines terms used in describing security incidents and response teams. For the purpose of the GRIP documents only a limited list is really needed. This should help maintain focus on the purpose of the documents, and prevent a duplication of other definitions or - even worse - a proliferation of competing definitions.

Constituency

Implicit in the purpose of a Security Incident Response Team is the existence of a constituency. This is the group of clients, sites, networks or organizations served by the team.

Security Incident

For the purpose of this document:

> 'A computer security incident is any event which compromises some aspect of computer or network security.'

The definition of an incident may vary between organizations, but at least the following categories are generally applicable:

- loss of confidentiality,
- compromise of integrity,
- denial of service,
- misuse,
- damage.

These are very general categories. For instance the forging of an electronic mail message and a successful password attack are two examples of 'compromise of integrity.'

Within the definition of an incident the word 'compromised' is used. Sometimes an administrator may only 'suspect' an incident. During the handling of a call it must be established whether or not an incident really occurred.

Security Incident Response Team

Based on two of the definitions given above:

> 'A Security Incident Response Team is a group authorized to manage response to security incidents that involve sites within its defined constituency.'

In order to be considered a SIRT, a group must:

- provide a channel for receiving reports about suspected incidents,
- provide assistance to members of its constituency in handling these

incidents,

- disseminate incident-related information to its constituency and to other related parties.

Vendor

A 'vendor' is any entity that produces networking or computing technology, and is responsible for the technical content of that technology. Examples of 'technology' include hardware (desktop computers, routers, switches, etc.), and software (operating systems, mail forwarding systems, etc.).

Note that the supplier of a technology is not necessarily the 'vendor' of that technology. As an example, an Internet Services Provider (ISP) might supply routers to each of its customers, but the 'vendor' is the manufacturer, being the entity responsible for the technical content of the router, rather than the ISP.

Vulnerability

A 'vulnerability' is a characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program allowed ordinary userss to execute operating system commands in privileged mode, this "feature" would be a vulnerability.

1.2 Publishing SIRT Templates

Every SIRT should publish information about its policies and services in the form of a completed template. The simplest way for a SIRT to make its template widely available is to publish it on its own information server so that clients in its constituency can easily find it. Templates published as pages in the World Wide Web should include the phrase 'SIRT Template' in their title - this will allow Web search engines to find them easily.

Whether or not templates are published in a repository, clients - and potential clients - of a SIRT will need to be able to authenticate a template (verify that it was indeed published by the SIRT) and check that it has not been modified (for example by verifying a digital signature for it).

To facilitate interaction between SIRTs, it would be useful to have a central repository for them. The GRIP Working Group believe that some of the existing Internet archive areas could be used for this purpose. The keeper of each template repository will be responsibly for verifying the identity of each SIRT lodging a template in the repository.

1.3 Establishing Peering Between SIRTs

When a SIRT (SIRT A) wishes to establish a working relationship with another SIRT (SIRT B), a responsible person from SIRT A will need to contact a similarly responsible person at SIRT B. The SIRT B person then has the problem: "how do I know who I'm talking to?"

It is very easy to send forged e-mail, and not hard to establish a (false) identity by telephone. PGP provides an effective way of securing e-mail, but securing voice communications is much harder. At present call-back is probably the only simple authentication method. This may change as technologies such as scrambled telephones, or PGP-phone on the Internet become available.

PGP relies on a 'web of trust,' built up by having known (and trusted) people sign PGP keys. This model could also be used for SIRTs. To achieve this each SIRT should publish a list of the SIRTs they have peering arrangements (i.e. working relationships) with, including PGP public keys for them.

Note that there is a difference between a peering agreement, where the SIRTs involved agree to work together and share information, and simple co-operation, where SIRT B (or any other client) simply contacts SIRT A and asks for help or advice. Note also that any client wanting direct help in tracking an incident must be prepared to provide sufficient information about the incident to make tracking possible.

2 Description Template: Security Incident Response Team

The Template is summarized in the section immediately below, and the remainder of the document describes its components.

```
Contact Information
-------------------
 * name of the team
 * address
 * time zone
 * telephone number
```

* facsimile number

* other telecommunication like STU-III, secure facsimile
* electronic mail address
* encryption methods for communication: PGP, PEM, MOSS, ..
* PGP public key (if PGP used)

Template Updates
----

* date of last update
* locations where this template may be found

Charter
----

* mission statement
* constituency
* sponsor / affiliation
* authority

Policies
----

* types of incidents
* level of support
* disclosure
    - of compromised site's information
    - the compromise of SIRT site to constituency
    - incident reporting requirements
* cooperation & interaction with
    - incident response teams
    - vendors
    - investigative agencies
    - involved sites
    - press
* communication & authentication
* point of customer contacts

Services
----

* incident response
    - verification
    - understanding
    - coping
    - notification
* proactive activities

Incident Reporting Forms

Disclaimers
----

3 Purpose of the Template

The Template which this document proposes is expected to be used by a response team to describe what it does, and in the process create criteria against which its performance can be measured. The Template does not attempt to specify a "correct" way for the team to operate, but does recommend on specific policies and functions seen as necessary for such a team to play a consistent role with other SIRTs throughout the networking community. It also comments on additional roles a team might include in the ambit of its operations.

The primary purposes of the Template are:

- to help SIRTs improve the way they operate;
- to improve interactions between different SIRTs, and between SIRTs and other organizations such as vendors and law-enforcement agencies;
- to note necessary interactions with their constituencies in setting expectations and defining policies;
- to help new groups understand what it takes to "be" a SIRT.

A Template might appear to provide a marketing tool for comparing different teams, but this kind of marketing use (or abuse) is strongly discouraged by the GRIP Working Group.

3.1 Other Related Material

This 'Framework for Response Teams' document is the first produced by the GRIP Working Group. A second document will set out guide-lines for technology vendors to help them handle security incidents. The definition of terms given in the next section applies to both documents.

Another relevant IETF document is RFC 1244, the Site Security Handbook, produced by (and being updated by) the Site Security Handbook Working

Group (SSH). Site requirements and recommendations are covered by the Handbook, while response team expectations and procedures are addressed by the GRIP documents.

Other documents of interest for the discussion of incident response teams and their tasks are available by anonymous FTP. A collection can be found on:

- ftp://ftp.nic.surfnet.nl/surfnet/net-security/
  cert-nl/docs/reports/R-92-01

Some especially interesting documents are:

- CERT-NL Framework
  ftp://ftp.cert.dfn.de/pub/csir/docs/cert-nl.opframe.txt

- FIRST potential members
  ftp://ftp.first.org/pub/first/newmemlt.txt
  ftp://ftp.first.org/pub/first/profile.txt
  ftp://ftp.first.org/pub/first/op`frame.txt
  http://www.first.org/first

- NRL Incident Response Manual
  http://hightop.nrl.navy.mil/news/incident.html

- Bibliography
  http://www.cert.dfn.de/eng/team/kpk/certbib.html

4 The Security Incident Response Team Template

This material which follows is addressed to those responsible for Security Incident Response Teams.

4.1 Contact Information

Full details of how to contact the SIRT should be listed here.

4.2 Template Updates

Details of a Security IRT change with time, so the template must indicate when it was last changed, who will be informed of future changes, and (by implication) who will not. Without this, it is inevitable that misunderstandings and misconceptions will arise over time.

4.2.1 Date of last update

This should be sufficient to allow anyone interested to evaluate the currency of the template.

4.2.2 Distribution list for Template Updates

Persons on this list are notified automatically whenever the template is changed. The list might normally cover the constituency and any other groups the SIRT has frequent interactions with. Readers not on the list can then recognise that they should check the central repository (above) for possible updates.

Digital signatures should be used for update messages sent by a SIRT to those on its distribution list.

4.3 Charter

Every SIRT must have a charter which specifying what it is to do, and the authority under which it will do it. The charter should include at least the following:

* mission statement
* constituency
* sponsor / affiliation
* authority

4.3.1 Mission Statement

The mission statement should focus on the team's core activities, already stated in the definition of a SIRT. In order to be considered a Security Incident Response Team, the team MUST provide incident response, as defined in section 1.1.

The goals and purposes of a team are especially important, and require clear, succinct definition.

4.3.2 Constituency

A SIRT's constituency (as defined above) can be determined in many ways. For example it could be a company's employees or its paid subscribers, or it could be defined in terms of a technological focus, such as the users of a particular operating system.

The definition of constituency should create a perimeter around the group to whom the team will provide service. The policy section (below) should explain how requests from outside the perimeter will be handled.

Constituencies might overlap, as when an ISP supports a SIRT, but delivers services to customer sites which also have SIRTs. The Authority section (below) should make such relationships clear.

People within the constituency have to learn that there is a Security IRT for their purposes; the building of a trusted relationship with the constituency is an on-going process which never ends.

4.3.3 Sponsoring organisation / affiliation

Any sponsoring organisations or affiliations, if they exist, must be disclosed to constituents. For example, the CERT Coordination Centre's sponsoring organisation is the Software Engineering Institute, Carnegie Mellon University; the sponsoring organisation for a SIRT within a large coprporation would be the corporation itself. SIRTs within smaller organisations may have no sponsoring organisation, in which case they should specify 'none.'

4.3.4 Authority

SIRTs may not have authority to intervene in the operation of all the systems within their perimeters. Each should identify the scope of its control as distinct from the perimeter of its constituency; if other SIRTs operate hierachically within this perimeter, they should be identified.

For example, a corporate SIRT may have authority to force the installation of software patches as the result of an incident. Other SIRTs, such as a national SIRT, may only be able to advise that such patches should be installed.

4.4 Policies

4.4.1 Types of incidents and level of support

The types of incident which the team is authorised to address and the level of support the team will contribute in assisting with each type of incident should be summarized here in list form. The Services section (later) provides opportunity for more detailed definition.

The team should state whether it will act on information it receives about vulnerabilities which create opportunities for future incidents. A commitment to act on such information on behalf of its constituency is regarded as an optional pro-active service policy rather than a core service requirement for a SIRT.

4.4.2 Co-operation and interaction with other organizations

This section should make explicit the related groups with which the SIRT routinely interacts. Examples of these are listed below.

Incident Response Teams: A SIRT will often need to interact with other SIRTs. For example a SIRT within a large company may need to report incidents to a national SIRT, and a national SIRT may need to report incidents to national SIRTs in other countries.

Vendors: The interaction here is in reporting vulnerabilities discovered during an incident. If your SIRT has relationships with product vendors, these should be described here. Larger vendors have their own SIRTs, but smaller vendors may not. In such cases a SIRT will need to work directly with a vendor.

Law-enforcement agencies: These include the police and other investigative agencies. SIRTs and users of the template should be sensitive to local laws and regulations, which may vary considerably in different countries.

Press: A SIRT may be approached by the Press for information and comment from time to time. This is discussed in more detail below (Reporting and Disclosure).

4.4.3 Reporting and Disclosure

The default status of any and all security-related information which a team receives can only be 'confidential,' but rigid adherence to this makes the team a 'black hole.' Its template should define what information it will report or disclose, to whom, and under what circumstances.

Different teams are likely to be subject to different legal restraints requiring or limiting disclosure, especially if they work in different jurisdictions. In addition, they mave have reporting requirements imposed by their sponsoring organisation, or they may be required by law to report certain kinds of security incident. Each team's template should specify any such restraints and requirements, both to clarify clients' expectations and to inform other teams. As an example of such restraints, the Dutch equivalent of the U.S. Federal Bureau of Investigation (FBI) has some kinds of documents which may NOT be recorded electronically.

Conflicts of interest, particularly in commercial matters, may also restrain disclosure by a team; this document does not recommend on how such conflicts should be addressed.

An explicit policy concerning disclosure to the Press can be helpful, particularly in clarifying the expectations of a SIRT's constituency.

'Disclosure' includes:

- reporting incidents within the constituency to other teams;

- handling incidents occurring within the constituency, but reported from outside it.

- reporting observations from within the constituency indicating suspected or confirmed incidents outside it;

- acting on reports of incidents occurring outside the constituency;

- passing information about vulnerabilities to vendors, to Partner SIRTs or directly to affected sites lying within or outside the constituency;

- feed-back to parties reporting incidents or vulnerabilities;

- the provision of contact information relating to members of the constituency, members of other constituencies, other SIRTs or law-enforcement agencies.

The reporting and disclosure policy should make clear who will be the recipients of a SIRT's reports in each circumstance. It should also note whether the team will expect to deal through another Security IRT or directly with a member of another constituency over matters directly involving that member.

A team will normally collect statistics. If they are distributed, the template's reporting and disclosure policy should say so, and should list the recipients.

4.4.4 Communication and authentication

Methods of secure and verifiable communication should be established. This is necessary for communication between SIRTs and between a SIRT and its constituents. The template should include public keys or pointers to them, including key fingerprints, together with guidelines on how to use this information to check authenticity.

At the moment it is recommended that every SIRT have, as a minimum, a PGP key available, since PGP is available world-wide. Teams may also make other mechanisms available, for example PEM.

For communication via telephone or facsimile a SIRT may keep secret authentication data for parties with whom they may deal, such as an agreed password or phrase.

4.5 Services

Services should be defined in two sections, as listed below.

```
  * direct incident response
     + verification of the incident, i.e. help in determining whether
         the problem really is caused by a security compromise
     + technical analysis assistance to understand the nature of the
         compromise
     + notification of other involved parties
     + guidance with eradication of the incident, i.e. steps
         to eliminate the compromise and prevent it recurring
     + guidance in recovery from the incident

  * optional
     + vulnerability analysis outside of direct incident activity
     + information provision
        - maintaining a vulnerability archive
```

- developing and supplying patches and resolutions

+ tool development and distribution
+ education
+ audit and consulting
+ product evaluation

Security Incident response Teams may provide different kinds of services to different sub-constituencies; this needs to be spelled out. For example, 'we are willing to provide direct incident response to other communities as follows ..'

4.6 Incident reporting Forms

Samples of reporting forms used by the SIRT (or pointers to them) should be included at this point in a template. As an example, the CERT Coordination Centre's incident reporting form is attached as Appendix C.

4.7 Disclaimers

Although the template does not constitute a contract, liability might conceivably result from its descriptions of services and purposes. The inclusion of a disclaimer at the end of the template is recommended.

It should be noted that some forms of reporting or disclosure relating to specific incidents or vulnerabilities can imply liability, and SIRTs should consider the inclusion of disclaimers in such material.

In situations where the original version of a template must be translated into another language, the translation should carry a disclaimer and a pointer to the original. For example:

> Although we tried to carefully translate our German template into English, we can not be certain that both documents express the same thoughts in the same level of detail and correctness. In all cases, where there is a difference between both versions, the German version is the binding version for our operation.

5 Secondary Purposes of this Document

The primary audience of this document are the administrators responsible for communities of users, i.e. 'constituencies.' This section provides some brief notes on what SIRT clients should expect of their teams.

An incident response team exists primarily to support the clients in its constituency. It is vital that those clients understand what they should expect of their team. Provided that a SIRT has published its template, a constituent/client should be able to read the template and discover what to expect, for example in such areas as privacy and confidentiality of information, and whether the response team will be contacting downstream sites. Clients should certainly expect a SIRT to provide the services they detail in their template.

An important aspect of incident response is the 'follow through' - every incident should be investigated and appropriate actions taken. Clients should be encouraged by their SIRT to report incidents so they can be acted upon. It must be emphasised that without active participation (especially reporting) from clients the effectiveness of the services they depend on can be greatly diminished. As a minimum, clients need to know that they should report security incidents, and know how and where they should report them.

Individual users (i.e. those who are not part of an organisation which provides a SIRT for its members) who observe a security incident should ask their Internet Service Provider for details of the most suitable SIRT to report it to.

Appendix B (below) provides some pointers to SIRTs which were known when this document was published.

6 Appendix A: Note on procedure definitions

Policies and statements of services in the template have to be implemented as procedures, but descriptions of those procedures should not be included in the template.

The following notes are intended to assist those seeking to form or to improve their SIRTs.

- External
  - identify other response teams
  - define supported clients:
    - by domain, through registration system, other means

```
    + establish secure communication practices
        - use of network, cell-phones, etc
    + define information that a client site must/should provide
        - use of reporting forms
```

```
* Internal
  + secure the team's infrastructure
  + protect information servers
  + protect sensitive data
  + define expiry of sensitive data
  + define disposal practice for sensitive data
  + establish methods for gathering and keeping statistics
  + establish 'knowledge base' of lessons learned from past incidents
  + create practical implementations of disclosure policies
  + document explicit practices for disclosure to the Press
```

The Site Security Handbook is a first resource to consult in securing a team's infrastructure. SIRT-specific security measures may evolve later.

7 Appendix B: Known Incident Response Teams

FIRST is the Forum of Incident Response and Security Teams. Information about FIRST can be found via their World Wide Web home page:

   http://www.first.org/first

This page contains pointers to 'Team Contact Information' for SIRTs who are FIRST members, and to 'Teams with WWW Servers.'

8 Appendix C: Sample Incident Reporting Form

The following is the form which clients should use to report incidents to the CERT Co-ordination Centre:

```
version 3.0
February 28, 1996

                   CERT(sm) Coordination Center
```

Incident Reporting Form

The CERT Coordination Center (CERT/CC) has developed the following form in an effort to gather incident information. We would appreciate your completing the form below in as much detail as possible. The information is optional, but from our experience we have found that having the answers to all the questions enables us to provide the best assistance. Completing the form also helps avoid delays while we get back to you requesting the information we need in order to help you. Sites have told us, as well, that filling out the form has helped them work through the incident.

Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Please feel free to duplicate any section as required. Please return this form to cert@cert.org. If you are unable to email this form, please send it by FAX. The CERT/CC FAX number is

+1 412 268 6989

Thank you for your cooperation and help.
....

1.0. General Information

1.1. Incident number (to be assigned by the CERT/CC): CERT#

1.2. Reporting site information

1.2.1. Name (e.g., CERT Coordination Center):
1.2.2. Domain Name (e.g., cert.org):
1.2.3. Brief description of the organization:
1.2.4. Is your site an Internet Service Provider (Yes/No):

2.0. Contact Information

2.1. Your contact information

2.1.1. Name:
2.1.2. Email address:
2.1.3. Telephone number:
2.1.4. FAX number:
2.1.5. Pager number:
2.1.6. Home telephone number (for CERT/CC internal use only):
2.1.7. Secure communication channel (e.g., PGP, PEM, DES, secure telephone/FAX) [NOTE -- we will call to

obtain the secure communication channel
information] (Yes/No):

2.2. Additional contact information (if available)

2.2.1. Name:
2.2.2. Email address:
2.2.3. Telephone number:
2.2.4. FAX number:
2.2.5. Pager number:
2.2.6. Home telephone number (for CERT/CC internal use only):
2.2.7. Secure communication channel (Yes/No):

2.3. Site security contact information (if applicable)

2.3.1. Name:
2.3.2. Email address:
2.3.3. Telephone number:
2.3.4. FAX number:
2.3.5. Pager number:
2.3.6. Home telephone number (for our internal use only):
2.3.7. Secure communication channel (Yes/No):

2.4. Contact information for other site(s) involved in this incident (if available)

2.4.1. Site name:
2.4.2. Contact person name:
2.4.3. Email address:
2.4.4. Telephone number:
2.4.5. FAX number:
2.4.6. Pager number:
2.4.7. Home telephone number (for CERT/CC internal use only):
2.4.8. Secure communication channel (Yes/No):

2.5. Contact information for any other incident response team(s) (IRTs) that has/have been notified (if available)

2.5.1. IRT name:
2.5.2. Constituency domain:
2.5.3. Contact person name:
2.5.4. Email address:
2.5.5. Telephone number:
2.5.6. FAX number:
2.5.7. Pager number:
2.5.8. Home telephone number (for CERT/CC internal use only):
2.5.9. Secure communication channel (Yes/No):
2.5.10. IRT reference number:

2.6. Contact information for any law enforcement agency(ies) that has/have been notified (if available)

2.6.1. Law enforcement agency name:
2.6.2. Contact person name:
2.6.3. Email address:
2.6.4. Telephone number:
2.6.5. FAX number:
2.6.6. Pager number:
2.6.7. Home telephone number (for CERT/CC internal use only):
2.6.8. Secure communication channel (Yes/No):
2.6.9. Law enforcement agency reference number:

3.0. Contacting Sites Involved

3.1. We ask that reporting sites contact other sites involved in incident activity. Please let us know if you need assistance in obtaining contact information for the site(s) involved.

When contacting the other sites, we would very much appreciate a cc to the "cert@cert.org" alias. This helps us identify connections between incidents and understand the scope of intruder activity. We would also appreciate your including our incident number in the subject line of any correspondence relating to this incident if one has been assigned (see item 1.1.).

If you are unable to contact the involved sites, please get in touch with us to discuss how we can assist you.

3.2. Disclosure information -- may we give the following types of information to

3.2.1. the sites involved in this incident

3.2.1.1. your domain (Yes/No):
3.2.1.2. your host(s) involved (Yes/No):
3.2.1.3. your contact information (Yes/No):

3.2.2. incident response teams, for sites from their constituencies involved in this incident

3.2.2.1. your domain (Yes/No):
3.2.2.2. your host(s) involved (Yes/No):
3.2.2.3. your contact information (Yes/No):

3.2.3. law enforcement agency(ies) if there is a legal investigation

3.2.3.1. your domain (Yes/No):
3.2.3.2. your host(s) involved (Yes/No):
3.2.3.3. your contact information (Yes/No):

4.0. Host Information

4.1. Host(s) involved at your site. Please provide information on all host(s) involved in this incident at the time of the incident (one entry per host please)

4.1.1. Hostname:
4.1.2. IP address(es):
4.1.3. Vendor hardware, OS, and version:
4.1.4. Security patches applied/installed as currently recommended by the vendor and the CERT/CC (Yes/No/Unknown):
4.1.5. Function(s) of the involved host

4.1.5.1. Router (Yes/No):
4.1.5.2. Terminal server (Yes/No):
4.1.5.3. Other (e.g. mail hub, information server, DNS [external or internal], etc.):

4.1.6. Where on the network is the involved host (e.g. backbone, subnet):
4.1.7. Nature of the information at risk on the involved host (e.g. router configuration, proprietary, personnel, financial, etc.):
4.1.8. Timezone of the involved host (relative to GMT):
4.1.9. In the attack, was the host the source, the victim, or both:
4.1.10. Was this host compromised as a result of this attack (Yes/No):

4.2. Host(s) involved at other other sites (one entry per host please)

4.2.1. Hostname:
4.2.2. IP address(es):
4.2.3. Vendor hardware, OS, and version:
4.2.4. Has the site been notified (Yes/No):
4.2.5. In the attack, was the host the source, the victim, or both:
4.2.6. Was this host compromised as a result of this attack (Yes/No):

5.0. Incident Categories

5.1. Please mark as many categories as are appropriate to this incident

5.1.1. Probe(s):
5.1.2. Scan(s):
5.1.3. Prank:
5.1.4. Scam:
5.1.5. Email Spoofing:
5.1.6. Email bombardment:

5.1.6.1. was this denial-of-service attack successful (Yes/No):

5.1.7. Sendmail attack:

5.1.7.1. did this attack result in a compromise (Yes/No):

5.1.8. Break-in

5.1.8.1. Intruder gained root access (Yes/No):
5.1.8.2. Intruder installed Trojan horse program(s) (Yes/No):
5.1.8.3. Intruder installed packet sniffer (Yes/No):

5.1.8.3.1. What was the full pathname(s) of the sniffer output file(s):
5.1.8.3.2. How many sessions did the sniffer log (use "grep -c 'DATA' <filename>" to obtain this information):

5.1.8.4. NIS (yellow pages) attack (Yes/No):
5.1.8.5. NFS attack (Yes/No):
5.1.8.6. TFTP attack (Yes/No):
5.1.8.7. FTP attack (Yes/No):
5.1.8.8. Telnet attack (Yes/No):
5.1.8.9. Rlogin or rsh attack (Yes/No):
5.1.8.10. Cracked password (Yes/No):
5.1.8.11. Easily-guessable password (Yes/No):

5.1.9. Anonymous FTP abuse (Yes/No):
5.1.10. IP spoofing (Yes/No):
5.1.11. Product vulnerability (Yes/No):

5.1.11.1. Vulnerability exploited:

5.1.12. Configuration error (Yes/No):

5.1.12.1. Type of configuration error:

5.1.13. Misuse of host(s) resources (Yes/No):

```
          5.1.14. Worm (Yes/No):
          5.1.15. Virus (Yes/No):
          5.1.16. Other (please specify):
```

6.0. Security Tools

```
     6.1. At the time of the incident, were you any using the following
          security tools (Yes/No; How often)

          Network Monitoring tools
             6.1.1.  Argus:
             6.1.2.  netlog (part of the TAMU Security Package):

          Authentication/Password tools
             6.1.3.  Crack:
             6.1.4.  One-time passwords:
             6.1.5.  Proactive password checkers:
             6.1.6.  Shadow passwords:
             6.1.7.  Kerberos:

          Service filtering tools
             6.1.8.  Host access control via modified daemons or
                     wrappers:
             6.1.9.  Drawbridge (part of the TAMU Security Package):
             6.1.10. Firewall (what product):
             6.1.11. TCP access control using packet filtering:

          Tools to scan hosts for known vulnerabilities
             6.1.12. ISS:
             6.1.13. SATAN:

          Multi-purpose tools
             6.1.14. C2 security:
             6.1.15. COPS:
             6.1.16. Tiger (part of the TAMU Security Package):

          File Integrity Checking tools
             6.1.17. MD5:
             6.1.18. Tripwire:

          Other tools
             6.1.19. lsof:
             6.1.20. cpm:
             6.1.21. smrsh:
             6.1.22. append-only file systems:

          Additional tools (please specify):

     6.2. At the time of the incident, which of the following logs were
```

you using, if any (Yes/No)

6.2.1. syslog:
6.2.2. utmp:
6.2.3. wtmp:
6.2.4. TCP wrapper:
6.2.5. process accounting:

6.3. What do you believe to be the reliability and integrity of these logs (e.g., are the logs stored offline or on a different host):

7.0. Detailed description of the incident

7.1. Please complete in as much detail as possible

7.1.1. Date and duration of incident:
7.1.2. How you discovered the incident:
7.1.3. Method used to gain access to the affected host(s):
7.1.4. Details of vulnerabilities exploited that are not addressed in previous sections:
7.1.5. Other aspects of the "attack":
7.1.6. Hidden files/directories:
7.1.7. The source of the attack (if known):
7.1.8. Steps taken to address the incident (e.g., binaries reinstalled, patches applied):
7.1.9. Planned steps to address the incident (if any):
7.1.10. Do you plan to start using any of the tools listed above in question 6.0 (please list tools expected to use):
7.1.11. Other:

7.2. Please append any log information or directory listings and timezone information (relative to GMT).

7.3. Please indicate if any of the following were left on your system by the intruder (Yes/No):

7.3.1. intruder tool output (such as packet sniffer output logs):
7.3.2. tools/scripts to exploit vulnerabilities:
7.3.3. source code programs (such as Trojan horse programs, sniffer programs):
7.3.4. binary code programs (such as Trojan horse programs, sniffer programs):
7.3.5. other files:

If you answered yes to any of the last 5 questions, please call the CERT/CC hotline (+1 412 268 7090) for instructions on uploading files to us by FTP. Thanks.

     7.4. What assistance would you like from the CERT/CC?

9 Security Considerations

This document discusses the operation of Security Incident Response Teams, and is therefore not directly concerned with the security of protocols or network systems themselves.

Nonetheless, it is vital that SIRTs establish secure communication channels with other teams, and with members of their constituency. They must also secure their own systems and infrastructure.

10 Editor's Address

Nevil Brownlee
ITSS Technology Developmenta
The University of Auckland

Phone: +64 9 373 7599 x8941
E-mail: n.brownlee@auckland.ac.nz