Network Working Group
Request for Comments: 3227
BCP: 55
Category: Best Current Practice

D. Brezinski
In-Q-Tel
T. Killalea
neart.org

February 2002

Guidelines for Evidence Collection and Archiving

Status of this Memo

Copyright Notice

Abstract

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

Table of Contents

1 Introduction..... 2
1.1 Conventions Used in this Document..... 2
2 Guiding Principles during Evidence Collection..... 3
2.1 Order of Volatility..... 4
2.2 Things to avoid..... 4
2.3 Privacy Considerations..... 5
2.4 Legal Considerations..... 5
3 The Collection Procedure..... 6
3.1 Transparency..... 6
3.2 Collection Steps..... 6
4 The Archiving Procedure..... 7
4.1 Chain of Custody..... 7
4.2 The Archive..... 7
5 Tools you'll need..... 7

6 References..... 8
7 Acknowledgements..... 8
8 Security Considerations..... 8
9 Authors' Addresses..... 9
10 Full Copyright Statement.....10

1 Introduction

A "security incident" as defined in [RFC2828] is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident. It's not our intention to insist that all System Administrators rigidly follow these guidelines every time they have a security incident. Rather, we want to provide guidance on what they should do if they elect to collect and protect information relating to an intrusion.

Such collection represents a considerable effort on the part of the System Administrator. Great progress has been made in recent years to speed up the re-installation of the Operating System and to facilitate the reversion of a system to a 'known' state, thus making the 'easy option' even more attractive. Meanwhile little has been done to provide easy ways of archiving evidence (the difficult option). Further, increasing disk and memory capacities and the more widespread use of stealth and cover-your-tracks tactics by attackers have exacerbated the problem.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

You should use these guidelines as a basis for formulating your site's evidence collection procedures, and should incorporate your site's procedures into your Incident Handling documentation. The guidelines in this document may not be appropriate under all jurisdictions. Once you've formulated your site's evidence collection procedures, you should have law enforcement for your jurisdiction confirm that they're adequate.

1.1 Conventions Used in this Document

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

2 Guiding Principles during Evidence Collection

- Adhere to your site's Security Policy and engage the appropriate Incident Handling and Law Enforcement personnel.

- Capture as accurate a picture of the system as possible.

- Keep detailed notes. These should include dates and times. If possible generate an automatic transcript. (e.g., On Unix systems the 'script' program can be used, however the output file it generates should not be to media that is part of the evidence). Notes and print-outs should be signed and dated.

- Note the difference between the system clock and UTC. For each timestamp provided, indicate whether UTC or local time is used.

- Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.

- Minimise changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times.

- Remove external avenues for change.

- When confronted with a choice between collection and analysis you should do collection first and analysis later.

- Though it hardly needs stating, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly in a crisis. If possible procedures should be automated for reasons of speed and accuracy. Be methodical.

- For each device, a methodical approach should be adopted which follows the guidelines laid down in your collection procedure. Speed will often be critical so where there are a number of devices requiring examination it may be appropriate to spread the work among your team to collect the evidence in parallel. However on a single given system collection should be done step by step.

- Proceed from the volatile to the less volatile (see the Order of Volatility below).

- You should make a bit-level copy of the system's media. If you wish to do forensics analysis you should make a bit-level copy of your evidence copy for that purpose, as your analysis will almost certainly alter file access times. Avoid doing forensics on the evidence copy.

2.1 Order of Volatility

When collecting evidence you should proceed from the volatile to the less volatile. Here is an example order of volatility for a typical system.

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

2.2 Things to avoid

It's all too easy to destroy evidence, however inadvertently.

- Don't shutdown until you've completed evidence collection. Much evidence may be lost and the attacker may have altered the startup/shutdown scripts/services to destroy evidence.
- Don't trust the programs on the system. Run your evidence gathering programs from appropriately protected media (see below).
- Don't run programs that modify the access time of all files on the system (e.g., 'tar' or 'xcopy').

- When removing external avenues for change note that simply disconnecting or filtering from the network may trigger "deadman switches" that detect when they're off the net and wipe evidence.

2.3 Privacy Considerations

- Respect the privacy rules and guidelines of your company and your legal jurisdiction. In particular, make sure no information collected along with the evidence you are searching for is available to anyone who would not normally have access to this information. This includes access to log files (which may reveal patterns of user behaviour) as well as personal data files.

- Do not intrude on people's privacy without strong justification. In particular, do not collect information from areas you do not normally have reason to access (such as personal file stores) unless you have sufficient indication that there is a real incident.

- Make sure you have the backing of your company's established procedures in taking the steps you do to collect evidence of an incident.

2.4 Legal Considerations

Computer evidence needs to be

- Admissible: It must conform to certain legal rules before it can be put before a court.

- Authentic: It must be possible to positively tie evidentiary material to the incident.

- Complete: It must tell the whole story and not just a particular perspective.

- Reliable: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.

- Believable: It must be readily believable and understandable by a court.

3 The Collection Procedure

Your collection procedures should be as detailed as possible. As is the case with your overall Incident Handling procedures, they should be unambiguous, and should minimise the amount of decision-making needed during the collection process.

3.1 Transparency

The methods used to collect evidence should be transparent and reproducible. You should be prepared to reproduce precisely the methods you used, and have those methods tested by independent experts.

3.2 Collection Steps

- Where is the evidence? List what systems were involved in the incident and from which evidence will be collected.
- Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.
- For each system, obtain the relevant order of volatility.
- Remove external avenues for change.
- Following the order of volatility, collect the evidence with tools as discussed in Section 5.
- Record the extent of the system’s clock drift.
- Question what else may be evidence as you work through the collection steps.
- Document each step.
- Don’t forget the people involved. Make notes of who was there and what were they doing, what they observed and how they reacted.

Where feasible you should consider generating checksums and cryptographically signing the collected evidence, as this may make it easier to preserve a strong chain of evidence. In doing so you must not alter the evidence.

4 The Archiving Procedure

Evidence must be strictly secured. In addition, the Chain of Custody needs to be clearly documented.

4.1 Chain of Custody

You should be able to clearly describe how the evidence was found, how it was handled and everything that happened to it.

The following need to be documented

- Where, when, and by whom was the evidence discovered and collected.
- Where, when and by whom was the evidence handled or examined.
- Who had custody of the evidence, during what period. How was it stored.
- When the evidence changed custody, when and how did the transfer occur (include shipping numbers, etc.).

4.2 Where and how to Archive

If possible commonly used media (rather than some obscure storage media) should be used for archiving.

Access to evidence should be extremely restricted, and should be clearly documented. It should be possible to detect unauthorised access.

5 Tools you'll need

You should have the programs you need to do evidence collection and forensics on read-only media (e.g., a CD). You should have prepared such a set of tools for each of the Operating Systems that you manage in advance of having to use it.

Your set of tools should include the following:

- a program for examining processes (e.g., 'ps').
- programs for examining system state (e.g., 'showrev', 'ifconfig', 'netstat', 'arp').
- a program for doing bit-to-bit copies (e.g., 'dd', 'SafeBack').

- programs for generating checksums and signatures (e.g., 'sha1sum', a checksum-enabled 'dd', 'SafeBack', 'pgp').

- programs for generating core images and for examining them (e.g., 'gcore', 'gdb').

- scripts to automate evidence collection (e.g., The Coroner's Toolkit [FAR1999]).

The programs in your set of tools should be statically linked, and should not require the use of any libraries other than those on the read-only media. Even then, since modern rootkits may be installed through loadable kernel modules, you should consider that your tools might not be giving you a full picture of the system.

You should be prepared to testify to the authenticity and reliability of the tools that you use.

6 References

[FAR1999] Farmer, D., and W Venema, "Computer Forensics Analysis Class Handouts", http://www.fish.com/forensics/

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", FYI 8, RFC 2350, June 1998.

[RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

7 Acknowledgements

We gratefully acknowledge the constructive comments received from Harald Alvestrand, Byron Collie, Barbara Y. Fraser, Gordon Lennox, Andrew Rees, Steve Romig and Floyd Short.

8 Security Considerations

This entire document discuses security issues.

9 Authors' Addresses

Dominique Brezinski
In-Q-Tel
1000 Wilson Blvd., Ste. 2900
Arlington, VA 22209
USA

EMail: dbrezinski@In-Q-Tel.org

Tom Killalea
Lisi/n na Bro/n
Be/al A/tha na Muice
Co. Mhaigh Eo
IRELAND

Phone: +1 206 266-2196
EMail: tomk@neart.org

10. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.