Global Information Assurance Certification Paper

Reporting Unauthorized Intrusions: A "How To" Guide

Melton J. Roland
UserID: chuck.g001
GIAC Security Essentials Certification (GSEC)
Assignment Version 1.2e
Original Submission
Enrolled through Federal Emergency Management Agency (FEMA)

Thursday, July 26, 2001

Reporting Unauthorized Intrusions:
"A How to Guide"

Introduction

You have spent many hours implementing security on your network. Your firewall is running smoothly, you have installed every service pack and patch available. You could wall paper your office with the audits you have been logging. Yet, despite your best efforts criminal hackers somehow compromise your network. What do you do?

When an incident happens you may not have the time or focus to search for the proper way of reporting it or the authorities to which it should be reported. This document will provide such information in a few simple steps.

The scope of this document is limited to the actions that should be taken after an illegal infiltration into a private or corporate network. It is assumed that the reader already has a good working knowledge of technology security.

Step 1: Gather The Evidence

Using your experience and knowledge and any available tools you must gather evidence that a crime is or has been committed. Although there are many resources and techniques that will assist you in this effort, these will not be covered in this document. However, a few examples from the National Infrastructure Protection Center are listed below:

> *To protect evidence and help federal, state, or local law enforcement agencies investigate the incident, take the following actions:*
>
> - *make backup copies of damaged or altered files, and keep these backups in a secure location;*
> - *activate all auditing software;*
> - *consider implementing a keystroke monitoring program, provided an adequate warning banner is displayed on your system; and*
> - *DO NOT contact the suspected perpetrator.*
>
> From NIPC Web site: http://www.nipc.gov/incident/incident.htm

If there is significant damage being done or sensitive material is being compromised, shut down and stop the intrusion. If necessary, disconnect the affected device from the network. Sometimes the risk of compromising sensitive material is not worth the risk of trying to catch the perpetrator.

That said if there is not significant damage being done or if you can afford the risk of the intrusion, continue on to Step 2 of this document.

The main goal of this initial step is to gather as much detail about the intrusion as possible. This means finding answers to the following questions:

- How was the attack initiated?
- When did the attack occur? (Date and time)
- Where did the attack occur?
- What tools did the intruder use?
- What was compromised?

These are only a few questions that need to be answered. More specific questions may be developed on a case-by-case basis. Ensure that you fully document every detail of the incident.

Step 2: Confirm your suspicions.

Although this step may sound foolish it really may be worth the effort. For example you need to make sure that the intruder is for real. What could be more embarrassing than reporting a hacker to the authorities when all along it was just your boss who forgot his password?

Double-check the elements of the incident. If these elements are outside the scope of your knowledge or experience, seek advice from more experienced staff members or from an outside source or organization.

Step 3: Report The Violation

This is of course the most important step and the main purpose of this document. Do you know who the authorities are? Do you report the incident to an internal or external source? What steps need to be taken to report the incident internally and externally?

The first person notified when you discover that an attack has occurred should be your first line supervisor. This individual will assist you in the notification process. The Chief Security Officer and Chief Information Officer (CIO) of your organization should be notified immediately and presented with as many facts and reports of the incident as are available. The bottom line is that management should know about this AS SOON AS POSSIBLE.

The next level of incident notification should be to your local Federal Bureau of Investigation (FBI) office, the local U.S. Secret Service office or the National Infrastructure Protection Center (NIPC).

The National Infrastructure Protection Center (NIPC) is a government agency whose "mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based." (http://www.nipc.gov/about/about.htm)

The NIPC has guidelines for reporting the need for immediate assistance found in the table below:

Immediate Assistance

If you need immediate assistance contact your local FBI field office or other appropriate law enforcement agency immediately and report the following:

- *names, location, and purpose of operating systems involved;*
- *names and location of programs accessed;*
- *how intrusion access was obtained;*
- *highest classification of information stored in the systems; and*
- *impact (compromise of information of dollar loss).*

From NIPC web site: http://www.nipc.gov/incident/incident.htm

The U.S Secret Service Electronic Crimes Branch also investigates "criminal misuses of electronic crimes". Some of their duties include:

What does the ECB do?

- *We provide administrative control of all computer-related and telecommunications investigations.*
- *We provide technical assistance to our special agents in the development of their cases, including the preparation and service of search warrants on electronic storage devices.*
- *We provide laboratory analysis and courtroom testimony concerning the evidentiary contents of electronic storage devices seized during criminal investigations.*
- *We provide educational presentations to classes and seminars for law enforcement officers, other government agencies, and private industry.*
- *We meet regularly with other government agencies, hardware manufacturers, and software publishers to stay at the leading edge of this quickly changing technology.*
- *We conduct research and development projects in order to address new problem areas, linked to new technology.*
  http://www.treas.gov/usss/

The Department of Justice Computer Crime and Intellectual Property Section has a Website with guidelines and Points of Contact for reporting attacks. This Web site is located at: http://www.usdoj.gov/criminal/cybercrime/reporting.htm. The CCIPS main Web site is at http://www.cybercrime.gov/. Here is a description of the main duties of the CCIPS:

"The Computer Crime and Intellectual Property Section ("CCIPS") attorney staff consists of about two dozen lawyers who focus exclusively on the issues raised by computer and intellectual property crime. Section attorneys advise federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups. Other areas of expertise possessed by CCIPS attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations, and intellectual property crimes."(http://www.cybercrime.gov/ccips.html)

Visit the links above for each agency and become familiar with their reporting procedures. Better yet, copy the contact information found on the various Web

sites and ensure all technical personnel have a copy and know the reporting procedures. Include this information in your operating procedures document.

It is important to report security attacks to as many authority groups as possible. This will ensure that your incident will be noticed and action will be taken. When reporting incidents to these groups ensure you have readily available the evidence you compiled in step 1.

Step 4: Plug The Hole

After sufficient evidence has been gathered or another agency (FBI, Secret Service) has completed their investigation, you must return to the task of information security.

Ensure that another party could not use the means by which the original intruder has gained access again. Essentially… plug the hole. This will prevent further damage or compromise to your network.

Document the procedures taken and publish them for use by others. Ensure that all your documented information is available to those individuals within your organization who may also be vulnerable to the same or similar attacks.

Step 5: Seek Legal Advice

Although complex legal details are beyond the scope of this document, it is an area that may require your attention. Your organization probably already has in place the procedures for criminal prosecution of hackers. Ensure you consult with your legal department so that you are not subject to prosecution.

Cooperate with any outside agency involved with your incident and with the security teams within your organization. Ensure that all parties involved have full access to the well-documented evidence you gathered in step 1.

For a list of Federal Laws and Regulations for computer security visit: http://fedlaw.gsa.gov/legal8.htm.

The United States Department of Justice has specific guidelines for the search and seizure of electronic equipment that has been used in a crime. These guidelines are found at: http://www.usdoj.gov/criminal/cybercrime/searching.html.

Step 6: Learn From The Experience

After all the chaos is over you will have gained the knowledge of experience and a new found respect for the issue of security. Share your knowledge you have gained. The most important element of network security is that of sharing knowledge. It is important to report security compromises so that they will happen less frequently. Others can learn from your experience and can prevent this from happening to them.

One suggestion that you may pursue is an after action review. Go over the incident again in an open meeting and find out where the discrepancies were, what did you do right? What did you do wrong? What should have been done differently? Ask yourself if this attack could happen again somewhere else within your organization. Another question you should ask is, have we already begun to implement the procedures that we have learned from this incident?

Equally important is the task of documentation. This documentation should be precise in the explanation of the attack, and should answer certain questions. Questions such as: What was the nature of the attack? How did the perpetrator gain access? What could have prevented this attack? Documentation will allow you to handle another incident in a much more efficient manner.

Conclusion

Because no network is completely 100% safe from intruders it is important that each incident is documented and reported. These actions will help achieve the following goals:

- One more hacker could be prosecuted and taken out of “circulation”
- The attack will be documented and shared with the global security community
- You will gain experience and knowledge from your experience
- Others can learn from your experience prevent the same type of attack
- In the event of another security compromise, you will know who the authorities are that should be informed

The steps listed in this document are only guidelines that should be taken when an electronic attack has occurred on your network. Specific actions should be followed in accordance with the Standard Operating Procedures set forth by your organization.

Sources Cited

Dick, Ron. National Infrastructure Protection Center “Welcome” 27 July07
URL: http://www.nipc.gov/about/about.htm (7/27/01)

National Infrastructure Protection Center “Incident Report” 27 July07
URL: http://www.nipc.gov/incident/incident.htm (7/27/01)

United States Secret Service “What does the ECB do?” 27 July 01
URL: http://www.treas.gov/usss/financial_crimes.htm#ecb (7/27/01)

usdoj-crm/mis/jam. “How to Report Internet Related Crime.” Computer Crime and Intellectual Property Section (CCIPS) 09 July 2001
URL: http://www.usdoj.gov/criminal/cybercrime/reporting.html (7/26/01)

usdoj-crm/mis/jam. “Computer Crime and Intellectual Property Section (CCIPS) 24 February 2000 URL: http://www.cybercrime.gov/(7/20/01)

usdoj-crm/mis/jam. “What does CCIPS do?” Computer Crime and Intellectual Property Section

(CCIPS) 24 February 2000 URL: http://www.cybercrime.gov/ccips.html(7/26/01)

FedLaw Web site"Computers and Information Technology"
URL: http://fedlaw.gsa.gov/legal8.htm. (7/26/01)

usdoj-crm/mis/jam. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." Computer Crime and Intellectual Property Section (CCIPS) 09 July 2001 URL: http://www.usdoj.gov/criminal/cybercrime/searching.html (7/26/01)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event