Global Information Assurance Certification Paper

Incident Report for GCIH
Capitol SANS 2000, Washington DC December 2000
Carl Burgess
February 20, 2000

Option 1 – Illustrate an Incident

1. Executive Summary

The information in this report describes an incident involving the breach of an external web server during December 2000. Because of the lack of security expertise available within the business units there was no one available to perform a thorough detailed investigation. Investigations prior to this incident had centered on users abusing their access not on how to respond and prepare for and respond to an incident involving an external hacker.

Prior to the event Management focus was primarily on granting user access to resources as expeditiously as possible. Controlling access to system resources for only authorized users was not paramount in the business model. The company considered their information sensitive but did not believe that any hacker one would be interested in them as a target. The safeguards in place in the business unit were focused on authentication, but once an unauthorized user had breached these controls access to sensitive internal information was readily available. There were no intruder detection systems within the network and no demilitarized zones established to safeguard the internal systems. I will detail the incident and highlight the shortcomings of the investigation, and the errors in the initial set up that caused the security breach. I will also incorporate changes that could have assisted the investigation as stated in the SANS Computer Security Incident Handling Step by Step Guide.

During the first week of December a law enforcement agency discovered information from our business unit in the possession of a known hacker. The information was not considered public knowledge and the perpetrator was not an employee and had no direct relationship with any employee or contractor of the business unit. Research by the business unit revealed that the information in the possession of law enforcement was very sensitive company information. The information contained new product designs that were not available to normal system users.

In retracing the steps of the incident and after interviewing the system administrators it was apparent that several users noticed unusual system activity. Help desk tickets and call logs were consistent in the temporary loss of data files and the movement of data to other storage area. The movement of data was by a system administrator that was non-existent prior to October 2000. Log records on the firewall showed data files leaving the network via FTP. Coordination with

law enforcement verified that the files in possession of the hacker were identical to the data files sent from our site via FTP to an unidentified server.

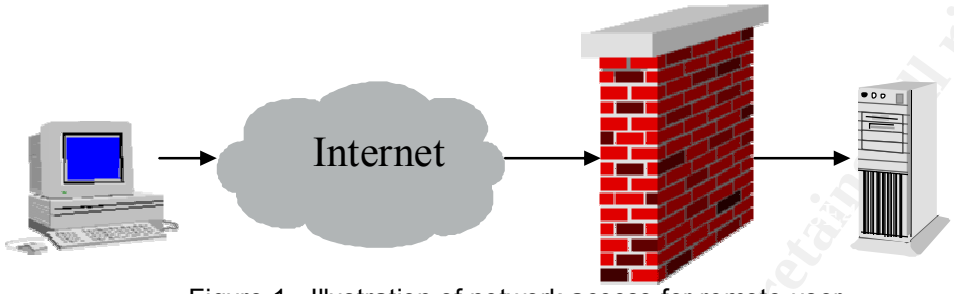

Figure 1. Illustration of network access for remote user

1. Preparation

Preparation is prior planning and training to respond to an incident. The lack of preparation was critical in the inability of the business to respond to the attack. The list includes policies, warning banners, guidelines for cooperation, etc. I will explain the use of each step within the business.

1.1 Policy

An outside consulting company who was the developers of the web site dictated preparation for the external web area. The business requirement for the web site was ease of access by the user. The business did not want to appear overbearing and intrusive to external users so a warning banner was not placed on the web site prior to deployment as required by company policy. The web site was protected by a firewall as required by company policy; however, there was nothing in the policy dictating the rules required for the firewall.

Without the use of a warning banner the intruder could view the information contained within the web environment as open data and could use this point in litigation because he was unaware of any company constraints on data access. However, other areas breached did contain company-warning banners and warned that data was the property of the corporation and was for use by only authorized employees or contractors engaged in the support of the company.

1.2 Management Support

The management of the I business unit did not value security as a necessary investment for the business. Incidents documented at other companies and business units were viewed as isolated occurrences and dismissed. This lack of management oversight fostered a false sense of security and an adherence to basic security practices.

1.3 Incident Handling Team

With no management support the business unit never developed and incident handling team as required by policy. System administrators of the system focused on operational readiness not operational security. To respond to the incident the business unit's departmental security organization required assistance from within other business units to scope the extent of the attack.

1.4 Emergency Communications Plan

The communications plan was non-existent so no call list was available. The CIO, Director of Infrastructure and the system administrators would be key players needed to set up a cohesive communication structure. set up outside of the breached environment.

1.5 Reporting System

There was not an established criteria established to monitor the computer network or the individual servers. Without a monitoring system the business unit was unaware that an incident was occurring until notification from an external law enforcement agency. When the system administrator did notice irregularities he was unsure where to report the incident. Help desk trouble tickets were not reviewed so no one was aware that the network was under attack.

1.6 Training

Security training for the incident response team was not conducted because of the lack of an established team. The key members for the training will be the system administrators and the help desk.

1.7 Inter-departmental Cooperation

Business units did not share security information resources and notification channels were not coordinated. An action plan was established to allow notification of any incident to be coordinated with the Help desks. The Help desk will notify the business unit security department of any unusual incident such as:

- Servers Crashing
- Multiple user accounts locked out
- Systems not responding to network request

1.8 System Administration Relationships

System Administrators were isolated and unaware of their impact on the business. Consultation with the system administrator revealed that the system had been performing erratically for a few months. The system administrator unaware of the breach of the system destroyed evidence in attempting to keep the system operational. System logging was not used on the NT System and the only detailed logs of the attack were the Router logs.

1.9 Law Enforcement

The incident was first noticed by the law enforcement agency for the area. Notification was provided to the business unit of the possibility of a data compromise. Law enforcement involvement required the handling of known evidence by police criteria. This involved escorting law enforcement personnel to the data center and handing over data pertinent to their investigation. Later our legal department determined that this was not necessary but with no experience in dealing with law enforcement agencies we were a little to willing to offer assistance.

2. Identification

2.1 Responsibilities

With no experienced investigators available inside of the business the research of the system anomaly took on an ad hoc approach. The lead of the investigation assigned users according to their areas of expertise with no real indication of what they were searching for and what would be the end result. The investigator was primarily concerned with getting the system back into operation as soon as possible. This meant that we were to provide the law enforcement agency as much information as required so that they would let us return to running the business.

2.2 Incident Determination

The report from the law enforcement agency detailed times and dates of an alleged intruder. The review of the Router logs showed nothing unusual for system operations. However, detailed inspections between the Windows NT Log and the CheckPoint firewall log revealed abnormalities and deletions of various time periods. The time periods deleted did not follow normal system Change control procedure. Review of the NT System showed account access by an unknown system administrator before the change in the log pattern. This was indicative of an event occurring but the extent was unknown. The review was coordinated with lead investigator and a member of the law enforcement agency. A two-person chain of custody was required for review and acknowledgment of all events in question.

2.3 Chain of Custody

During consultation with the legal department it was recommended that the web server machines in question should be pulled of the network and locked into a secure room for evaluation. This would mean a disruption of business but with law enforcement involvement the machine was removed. The firewall logs were copied to an Oracle database and archived on CD-ROM with the time and date and the initials of the reviewer and his assistant. All information including notes taken by the investigators were kept within the secure facility for safekeeping.

2.4 Coordination

ISP service was provided through an outside vendor who was willing to cooperate with the inquiry into the alleged breach of the system. A request was initiated for the ISP to review all known incidents within the time frame indicated by the network logs. Action at the ISP uncovered the attack was widespread and effected multiple users. Multiple systems were being probed or exploited by the same signature discovered during the investigation on the target system.

2.5 Notification

Notification of the widespread nature of the attack was relayed to the by the law enforcement agency to the corporate office of targeted companies. Internal management was kept abreast on the on-going investigation and the need to work as expeditiously and as silently as possible. No notification was given to the public until the extent of the attack was known.

3. Containment

3.1 On Site-Survey

The on-site survey concluded that data was lost due to either system administration error or the intruder. An interview with the system administrator provided knowledge that led to the conclusion that evidence may have been inadvertently destroyed by the administrator. The server and the remaining system logs were secured and placed into a locked room until a backup of the system in question could be conducted and a full review concluded.

3.2 Low Profile

With the widespread attack no one was sure whether the intruder was still actively engaged within the network. With the need to isolate and contain and get the system back on-line there was no time to create internal "Honey pots" or "treasures". Logging was turned on for the NT system to monitor user activity.

3.3 Code Tampering

There was concern with the code of the compromised server and without knowledge of the true start date of the attack none of the software currently installed on the server was viewed as being "trusted." A detailed investigation of the server logs revealed multiple changes to the NT Registry that invalidated everything on the server so the server was considered untrusted.

3.4 System Backup

Backup copies were made on CD ROM write once media and stored in a safe in the data center for review. Access to the data center was

controlled through a key card reader. The safe combination was changed so that only the Lead investigator and the security chief had the combination.

3.5 Risk of Continuing Operation

The start date of the attack could not be determined quickly and there was no way of determining whether the system could be safely put back into operation without compromise. Consultation with the law enforcement agency allowed us to conclude that the attack had been going on for quite some time before they were alerted. The business was not necessarily a specific target as other users of the ISP were also probed and exploited. Recommendation relayed to management was to rebuild the external system architecture before contemplating placing the server back on-line. Also we recommend that the server be re-built with the original shrink-wrapped software for a check of all systems before resuming operations. This recommendation was acceptable to the business.

3.6 Consultation with System owners

There was a daily briefing of the findings and the recommendations with the business unit. The briefings outlined the impact of ignoring the recommendations and allowing the known vulnerability to continue.

3.7 Password Change

A review of the target system indicated that the perpetrator had gained access to a system administrator password. A review of the system administrator accounts resulted in multiple discrepancies and the creation of several new administrator accounts. All system administration accounts were reviewed and new accounts deleted and all passwords changed.

4. Eradication

4.1 Cause of Breach

There were multiple causes of the breach and all played a key role in allowing the perpetrator access to information. The firewall was not properly secured and known vulnerable Windows NT NetBIOS ports were not blocked at the firewall. The firewall administrators did not understand the policy rules that were required for protection of the infrastructure in relation to the new application. The rule set in place on the CheckPoint Firewall-1 at the time of the incident were a contributing factor to the security incident because there were no changes made to the firewall to restrict access and protocols to the web server. However, the blame for this incident does not reside solely on the firewall administrator.

The Microsoft Windows NT IIS web server was easily exploited after getting by firewall. The reason for this easy exploit was because the IIS web server was set up in a default configuration recommended by the web

application developer. In addition the web server was built as a domain controller with no restrictions during the default IIS web server install. The Windows NT "Everyone" group was used with no restrictions granting broad user rights to all system users including anonymous users.

The intruder had a wide choice of attacks and possibly gained entry by probing the targeted system and gaining access through open NetBIOS ports in the firewall. The attacker probably used the anonymous user account to gain access with elevated rights associated with the "Everyone" group that had log on locally rights. After gaining access to the NTFS as a privileged user on the internal NT system the intruder made modifications to the registry and proceeded to monitor and search for sensitive information.

4.2 Improve Defense

To protect the external web server the packet filter firewall was upgraded to a proxy firewall with a hardened Router to filter IP addresses in front. To improve the defense of the firewall only business required functionality would be open on the firewall. Ports and protocols that were not a legitimate business requirement were disabled and filtered. All new applications would be reviewed to ensure that there functionality would not have an adverse effect on firewall perimeter security

The web servers placed into the DMZ would follow similar criteria allowing only necessary functionality that is requirement for the application to function. Server and application ease of administration would not take precedence over the security of the content of the web environment. The IIS web server would be rebuilt to the criteria in the SANS checklist for Windows NT.

- No batch programs on the web server
- Modify the directory structure
- Remove CGI scripts with "server-side includes
- Use IP address filtering
- Disable NetBIOS

Access rights controls will be as follows:

C:\InetPub\wwwroot;
C:\InetPub\Scripts

Owner	Administrators
Administrators	Full Control
CREATOR OWNER	Full Control
SYSTEM	Full Control
Web Masters	Full Control
Web Authors	Full Control
Users	Read
Guests	Read

C:\Winnt\System32\LogFiles

Owner	Administrators
Administrators	Full Control
SYSTEM	Full Control
Web Masters	Read

C:\Winnt\System32\inetsrvr

Owner	Administrators
Administrators	Full Control
SYSTEM	Full Control
Web Masters	Read

The IIS web server was placed into a DMZ with a SQL proxy to control access to internal systems. The web server was installed with Axent Enterprise Security Manager (ESM) software installed to monitor changes in system level access. Axent Intruder Alert (ITA) was installed on the server to detect known vulnerabilities or system abnormalities. We will also install a Netegrity SiteMinder agent on the web server to controls user access to web system content.

4.3 Vulnerability Analysis

System vulnerability analysis was conducted using Axent ESM to ensure we were limiting access to system resources on a need basis. Network vulnerability analysis was conducted using Northwest Performance NetScan Tools Pro2000, and Network Associates CyberCop. The purchase and the deployment of these tools is only a temporary fix until we develop the expertise and the knowledge to use these tools.

Other vulnerabilities will come from reviewing the latest incidents from CIAC and CERT and other vendor specific web sites. The system review has shown that the entire network system was vulnerable to attack.

There was no protection initiated to reduce the possibility of a DDO S attack from launching from the network. The business unit did not have any filtering of users or content to control access to internal resources. The review of the mail server resulted in a warning notice from ORB (Open Relay Behavior Modification System) that we could be used a launching point for SPAM.

4.4 Remove the Cause

Because of the unknown length of the attack it was decided to eliminate the possibility of a reoccurrence by loading only the original application software and the operating system. The data updated and stored in the back end databases was a difficult issue to manage. The information was very important to the business but no one could be sure that data was correct. The recommendation was to manually re-enter this information from a clean copy was accepted but not without reservation.

4.5 Re-Load Backup

Reviewing the logs and still unable to pinpointing the start of the attack to it was decided to reload the server and to re-do all changes and updates in a controlled environment. This involved re-engaging the software developer to provide copies and the code to all of their updates to the application software.

5. Recovery

5.1 Restore from Backup

The process to restore the system to operation required a review of the data and the system logs as the system functioned in a test environment. Data that was questionable from the logs was verified with the application developer. This process let us understand the function of the code in relation to the operating system and reduced the possibility that a Trojan was stored within the code. Any discrepancies in the test area will be removed before the system is placed into production.

5.2 System Validation

After reloading the system with shrink-wrapped software and application updates it is time to test the system. Testing is required before certification is granted and the system is placed back into operation. After loading the original application software and updates we discovered that modifications to software code would be necessary to achieve system functionality. Testing and validation of the system changes in a real-world environment helps eliminate the need to re-visit the application after it is placed into production.

5.3 Restore Operation

After the changes to the operating system and the blocking of ports in the firewall functionality was lost in the application. The application was built to function in an open NT environment with full use of NetBIOS. A modification in the code to correct the vulnerability was not under consideration by the software vendor. To accommodate the software functionality required changes in the internal firewall to allow NetBIOS function as request from internal systems only. The web server would serve as a front end to the application server. Users who required access to the application would be put into a controlled group inside of SiteMinder and only those users could use the URL to run the application. Additional security was enabled by the purchase of an additional server to separate the Shopping cart function from access to the internal database system.

5.4 Monitor

The code changes made by the programmers may contain hidden code that may allow backdoors into the system. With the use of modules and other rapid software development tools programmers borrow code from each other and from unknown third parties. The unknown software can lead to further exposure of even hardened systems and if you rely solely on Intrusion Detection Systems (IDS) you may never detect unusual authorized system functions. To alleviate concerns the logs on the IIS web server were activated and reviewed daily by the system administrator. The administrator will be checking for unusual activity with the IUSR_<hs001> attempting to gain or change user level. The logs will be written to an Oracle database and archived monthly.

6 Lessons Learned

6.1 Follow-up Report

The investigation into the intruder gaining access to resources on the internal system revealed that there was little oversight in regards to security at the business unit. Preparation for an incident was non-existent and coordination with other business units was never considered. There was no investment in any intruder detection tools including freeware. System administrators were unsure of how to respond to changes within their environment when they detected the abnormalities. Without management involvement and no guidance on how to respond to an attack their was no containment of the intruder. The lack of management oversight resulted in the posting of company sensitive information on an external bulletin board.

The information now in the hands of a hacker may have been divulged to competitors. This information if used by others may result in lawsuits and court cost that could prove very costly. This does not address the dollars spent on research and development that may now prove useless if the legal proceedings are unfavorable. The cost of the investigation was in excess of 600 man-hours and an additional cost in 300 hours in consultant fees to rebuild the application software. The lost in revenue while the system was out of operation was minimal but the black eye given by the FBI being aware of an incident with your data before you are aware will not be positively received by shareholders.

Refernces:

ORB
http://www.orbs.org

CheckPoint:
http://www.checkpoint.com/products/downloads/fw1-4_1tech.pdf

MIS Training Institute "Web and Intranet Security"
SANS GIAC "Incident Handling 4.1"

Last Updated: July 24th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
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
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS