Global Information Assurance Certification Paper

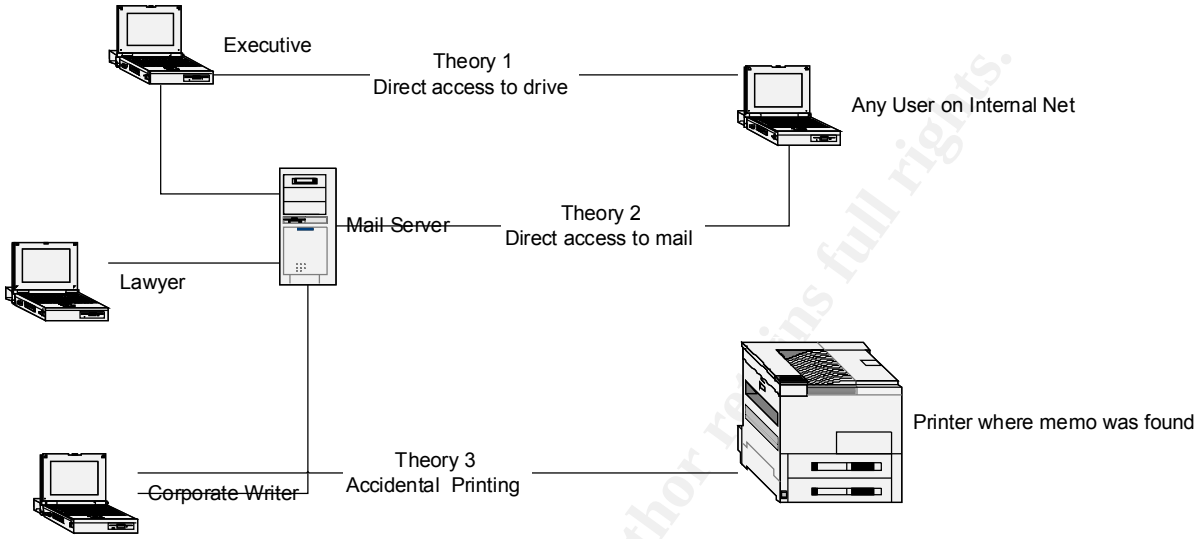
Nick Sherwood
Practical Assignment for SANS
Advanced Incident Handling and Hacker Exploits
Option 1 – Illustrate an Incident

The case of the printed memo

Executive Summary

An email of a highly sensitive nature containing potentially liable information was printed on a common printer and the information contained within was shared and spread throughout the company. While several security flaws and possible explanations exist for the cause of the incident, it was determined that human error was the true cause. An incident is an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. While it was determined that this incident did not begin with malicious intent, however the vulnerabilities that were discovered during the investigation were significant enough to be considered a threat. Some of the threats found have already been fixed, and others are in the planning stage. Several theories were documented during the investigation, however they could not be proved and have been eliminated. They did bring to light some issues for follow-up. The cause was determined to be theory 3 – accidental printing. While this sounds like an unavoidable accident, the cause of the accidental printing in the case was absolutely avoidable and has been remedied.

Nick Sherwood
Practical Assignment for SANS
Advanced Incident Handling and Hacker Exploits
Option 1 – Illustrate an Incident



Preparation

An extensive security policy does exist at this site. A general security standard as well as more specific standards for various operating systems also exist. Not all of these standards were implemented at the time of the incident. Warning banners are on all server systems. Pre-approval exists for the containment of unauthorized access. A well defined security/incident handling team is also in place. Policies are in place for internet and email usage, and monitoring tools for these systems are in place as well. A user education program is integrated into new employee orientation.

Identification

Nick Sherwood
Practical Assignment for SANS
Advanced Incident Handling and Hacker Exploits
Option 1 – Illustrate an Incident

A memo regarding the cancellation of a multi-million dollar project was printed on a printer located in the corporate help center. The memo was from the executive lawyer and addressed to all employees. It was assumed by members of the help desk that the memo was common knowledge and began discussing the memo and its ramifications with other employees. Given the nature of the information contained in the memo, the information was soon being spread via word of mouth all over the company. News eventually reached the corporate lawyer, who initially created the memo, and a phone call was immediately made to the CIO who in turn contacted the VP of security. By the time the VP of security was informed, approximately 3 hours had gone by. He then had the incident handling team begin an investigation. The incident handling team had actually heard the news contained within the memo before it was known to be an incident. It turns out that the memo was only one of three possible scenarios and that the only people who had seen it were the corporate lawyer, a technical writer, and an executive. These three had been e-mailing the document back and forth during the previous week revising it.

Within hours of the document being printed the incident handling team was pulled together to investigate. The manager and security officer were also involved. Given the accidental release of this important information it was immediately investigated by the incident handling team.

Containment

This was approached from several different angles. Several methods were used to track the true source of the document. Information was gathered on the machines involved, and potentially involved. This included the IP addresses, net bios names, user id's, user names, position and departments. The most obvious way to find out who printed the document was not possible. A review of the print log was not an option because logging had been disabled on the print server. The initial list of users to investigate included those who normally printed to the help desk printer. A search was then performed on users mailboxes, and system hard drives. In order to keep a low profile, all of these searches were performed remotely without the users knowledge. A list of command used during the search are detailed later in this document. The hard drives and network home directories were searched for all users that normally print to the help desk printer. The mail boxes for the three users involved where checked to see if proxy access (a method of allowing others into you mailbox) was given to any of the mail boxes involved. One had an administrative assistant with proxy access. That machine was also added to the search. It was determined that 2 of the 3 users did not have a password set on their e-mail client. This meant that anyone (internal) could have connected to and viewed their inbox and any messages it contained. This put the number of potential suspects to all users. The statistical properties of the document were reviewed and it was determined that the memo had an editing time of over 300 minutes. This is an excessive amount of time

given the length of the memo was less then a page in length. This led to another potential method of release. Merely someone walking up to an unattended machine and reviewing the material, copying it etc. No screen saver on local workstation was set on 1 of the 3 users. Another possible method of the documents pre release was improper local machine security which allowed "everyone" full access to all drives on all PC's. 2 of the 3 machines had the user everyone in the local administrators group. This was another very bad finding which opened up the potential suspects to all users. During the containment phase reports were being made to the proper chain of command both horizontally and vertically. The system owners (mail server and print server) were also kept informed and actually helped in some of the searching that took place. It was determined that one the of the 3 users had a new "image" place on there machine and that the image had a default printer of the help desk printer defined on it. The proper print mapping had not been pushed out yet via SMS and therefore the PC was not printing to the proper location. This was determined as the actual release of the information.

Eradication

Passwords were set up on the email system for the 2 users that did not have them set. Proper domain security was set up on the machines to make sure that other users were not mapping drives. Auditing was turned on the workstations so that mapping attempts could be recorded. Printer mappings

were verified for accurate connections. The document it self was password protected. Procedures for document handling were explained to those involved. The process of machine image creation was examined for further review during the follow-up of this incident.

Recovery

A follow-up memo correcting the information was out of the question for several days. The information that was verbally shared to the incident handling team the those initially involved was the memo was one of several possible memos and that it was not to be release until the following week pending outcome of various discussions. Since no machines were backed up or taken off-line, the recovery phase did not require these steps.

Follow Up

The critical review of this incident brought to light several severe security flaws. No mandatory password on email accounts. This issue was one that the security team had been pushing for some time. Unfortunately it took an issue this large to make it happen. No protection from drive mappings/unwanted connections. This was a major architectural change and required the cooperation of several different groups. Agreement was reached and changes are being implemented. No logging on the print server. Logging levels had been defined in the security standards, but were not being followed. This incident

prompted the review of sever other servers as well. Default images containing defaults for printing. The process for image creation was reviewed and has been changed so that default images do not come with a printer defined. This is a post installation requirement. Some of these changes required significant architecture changes to the environment that required time, effort and coordination in order to change. It did result in a more secure environment however.

Tools/Command Used

nlist user /A /S > thelist.txt

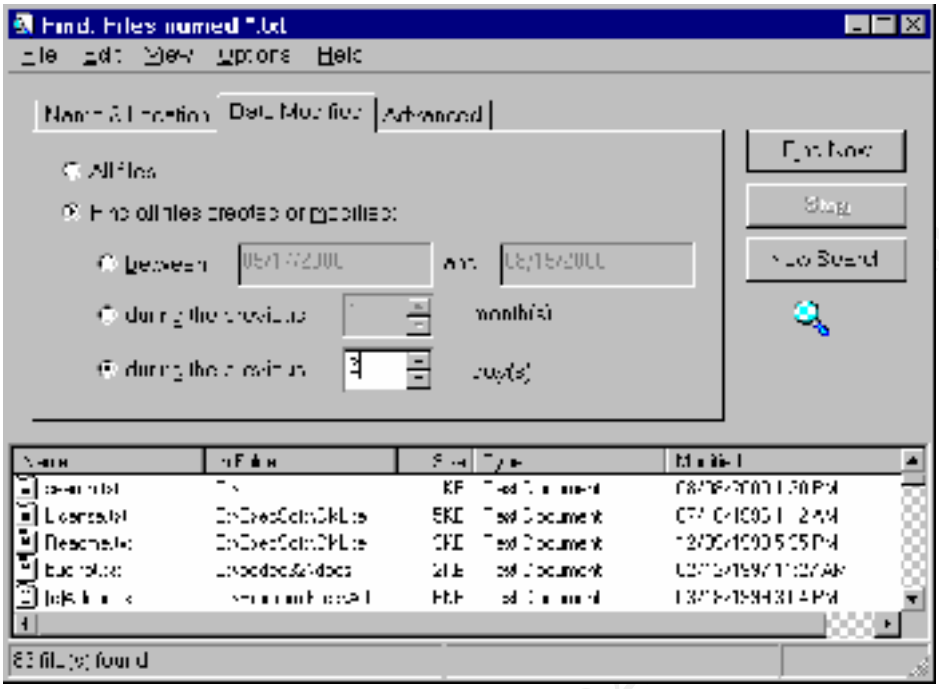
When used in a NetWare environment creates a file with all currently logged in users to the NDS tree. Provides user id, and MAC address.

net use (drive:) \ \ ipaddress\c$ /user : administrator

Used for mapping drives. The command line version is helpful for scripting mappings.

nbtstat – A ipaddress

This will list a machines name table given an IP address. This is also useful for determining the userid logged into a given machine.



This search engine which comes with Microsoft operating systems is helpful for searching for files.

Backup of any systems was not required in this incident.

Last Updated: July 25th, 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 Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
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 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
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event