Global Information Assurance Certification Paper

SANS Practical
Advanced Incident Handling and Hacking Exploits

Executive Summary: The incident described in this practical is unique and shows the varied incidents we must support. I found it difficult to describe this incident in the Incident Handling steps.

- June 12, 2000, my supervisor called me at home to tell me to be prepared to perform forensics on a laptop our legal department had just received from one of our salesmen.
- June 13, 2000, my supervisor and I meet with a lawyer in the legal department. The lawyer described the incident and what he wanted from us.

-- One our salesmen was defrauding my company and one of our customers and using his company computer to email his co-conspirators and track the amount of money defrauded. Our job was, if possible, to break into the salesmen's laptop to see if I could find any evidence of the fraud.

- June 13, 2000, my supervisor and I were able to access the files on the laptop and found evidence of the fraud. We informed the legal department who then took control of the laptop.
- June 14, 2000 the legal depart called and told us to be prepared to talk to both the local police and the FBI

Preparation: My company and especially my department, the Information Security Department, were not prepared for an incident involving use of company equipment for fraud. (I was hired to start our Monitoring and Reporting program and a subset of that program is the Incident Handling and Response program.) We had just begun discussions on policies for handling outside attacks but had not gotten into discussions

about insider incidents—it had taken me three months just to get the rest of the team to believe the majority of incidents involve insiders.

I began my preparation for this incident the night my supervisor called. I brainstormed about what I might to do and came up with the following list: access the laptop, backup the hard drive, review files, make hardcopy and softcopy files, and begin a chain of evidence. I was also concerned about the possible ramifications of our accessing the system without prior approval from law enforcement, so I came up with two questions to ask the lawyers when we met the next morning: First, is our accessing the system authorized by law enforcement? Second, what kind of records do I need to keep?

After my brainstorming session, I began to look further into each area. I was very concerned about accessing the laptop; I knew how difficult it would be to "break" into the laptop—an IBM Think Pad 600X with NT4.0 SP 6.0 loaded (all our sales force computers have the same image.) My first hope was the salesman would either have the password somewhere on the laptop or would have sent the password with laptop. Thinking the worst case, I researched several NT 4.0 books I had at home, but did not find any material to help me. I then remembered reading a string on one of the security reading lists I belong to about "breaking" into a NT 4.0 system. I researched the archives and made notes on the areas I thought would help. Finally, I thought I could change the salesperson password in the domain, connect his laptop to the domain, and sign on using the new password.

In addition, to thinking about "breaking" into the system, I also thought about the possible ways I could backup the hard drive onto the network. I knew we would not want to have the company we outsource LAN support to to do the backup; I would have to do

the backup. I also knew if the company was not going to the backup we would not be able to use their equipment and we did not own any backup equipment. Based on those constraints, I would either have to use the backup command that comes with NT or map a network drive on the laptop. I was not familiar with the backup process on NT to chance deleting the files on the hard drive, so I chose to map a network drive to the laptop and copy the files from the hard drive to the mapped network drive and limiting access to the directory to myself and my supervisor.

My next step was to come up with a plan for looking at the files on the backup. I prepared a check list: 1) call up the hard drive directory using the MS-DOS dir command to look for any last access, 2) using Explorer, change the attributes for reading files to all files to see if the salesman had any hidden files, 3) again using Explorer, review files in the folders, 4) replicate his Lotus Notes email to the network hard drive as a working copy, 5) have a trusted agent in the Lotus Notes group review his email activity for the past two years.get a hardcopy on the working network drive.

My biggest concern, however, was keeping a proper chain of evidence for law enforcement. I had purchased and read a copy of the SANS publication. *Computer Incident Handling: Step-by-Step* for the incident handling policies we were instituting and remembered reading a section on proper evidence handling. I reviewed the methodology presented in the publication.

After I reviewed my checklists and re-read the section on evidence handling, I thought I was prepared to begin the review of the files.

Identification: My company did not identify the incident; the company (we will call it Company A) we were doing business with identified the incident. Our headquarters sales

force director received a call on June 7 from a vice-president Company A. The vice-president of Company wanted to know when my company was going to pay Company A the incentive money my company owed Company A. The director said he would check into the problem. The director then called the salesman to review the incident. The next day, the salesman called the director and told the director what he had done; he also turned himself into the police and mailed the laptop to headquarters. In addition, Company A called the FBI.

Containment: Containment as defined in the incident handling steps does not pertain to this incident.

Eradication: No eradication was necessary.

Recovery: In the definition of incident handling, recovery of our systems was necessary.

Follow-up: Lessons Learned

- Company lessons learned
  -- Computer Security Incident Handling policies are a must—directed the Information Security Group to expedite the process
  -- Computer incidents do not just happen from outsiders trying to get in
  -- We must be more concerned with the proper handling of computer-derived evidence

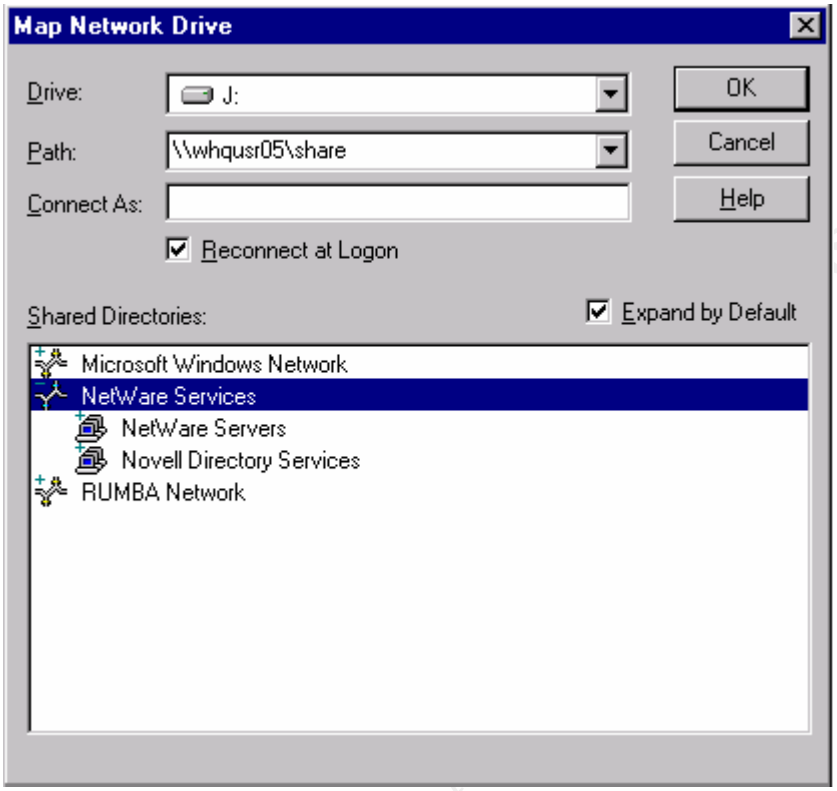
- Information Security Group lessons learned
  -- Must have a team of security incident handlers identified, including players from legal and human resources
  -- incident handlers must be prepared with both training and tools
  -- the group must have the capability to perform backups
  -- the group must have senior executive level authority to perform investigations
  -- the group must have a computer that is off the network—although I limited access on the directory, I was still very concerned of others trying to gain access to this directory
  -- Our executive directors, directors, immediate supervisors, and the general population of the company need education on computer security

- My lessons learned
  -- I was woefully unprepared to handle this incident, or any other incident for that matter
  -- I need to be more familiar with various backup methodologies
  -- I must have a toolkit ready to go at all times
  -- I must continually pressure my supervisor for training
  -- I must continually train the members of the Information Security Group on incident handling, especially now that we moving toward having the capability to monitor our networks
  -- I should have also followed the checklists provided in the *Computer Incident Handling: Step-by-Step*
  -- I need to make contact with my local law enforcement agency providing computer crime investigations as well as the local FBI office for computer crimes
  -- I must know hands down the proper methods for controlling evidence
  -- When trying to determine last accessed date, use the dir command before you access any files via Explorer
  -- I must document everything
  -- In addition to setting the permissions on the directory, I should have started auditing
  -- I have a lot to learn about proper incident handling and response

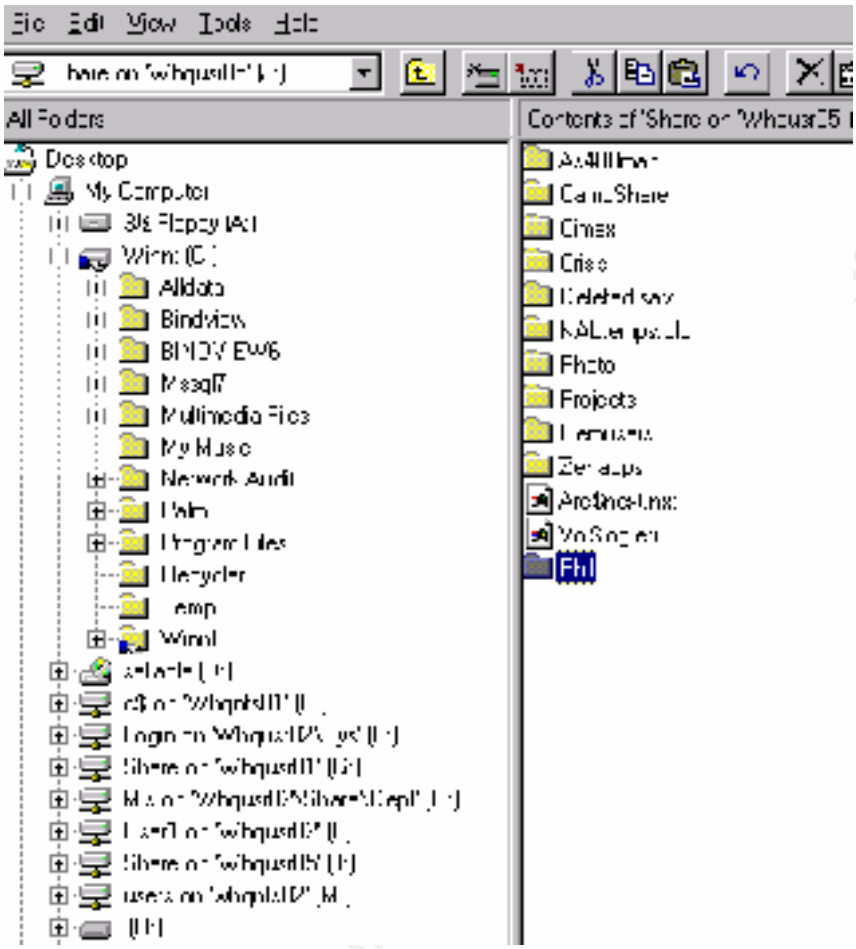
Tools: I used no special tools in this incident. I was very fortunate that the salesman left his userid and password written on a piece of paper on the laptop.

Backup: My steps to backup the laptops hard drive were as follows:

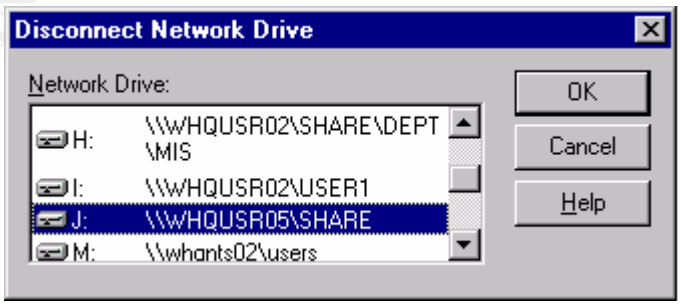
1. I put in a 10/100 PCMCIA ethernet card into the PCMCIA slot.
2. I hooked my extra network cable into the card.
3. I accessed the laptop using the userid and password
4. I mapped one of the network servers onto the laptop: LC on the Explorer icon the Office toolbar→LC on the map network drive icon→in the path section entered name of the server→LC OK



5. I created a directory called Phil on the network server: LC drive name in Explorer→LC File→LC New→LC Folder→Entered folder name, hit Enter

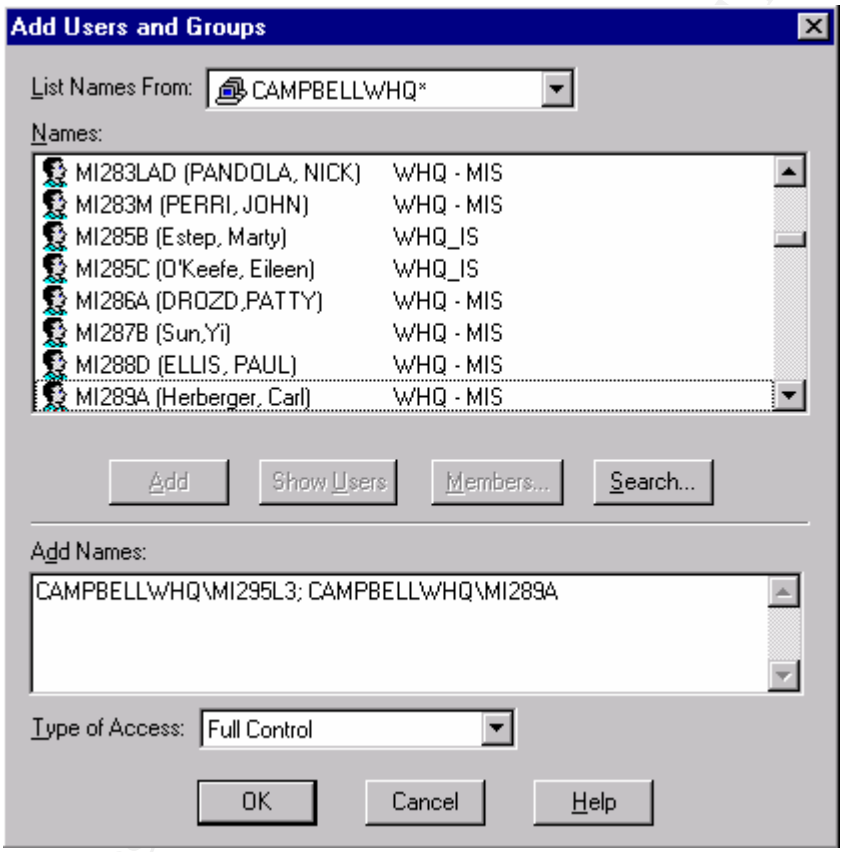


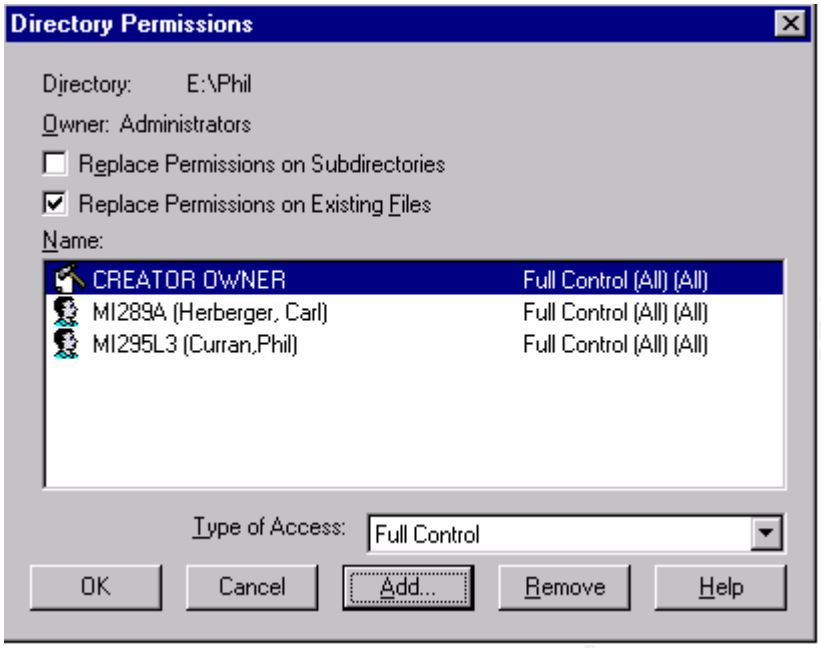
6. I copied the hard drive from the laptop to Phil. LC on Windows Explorer Icon on tool bar→LC on Winnt (C:)→LC Edit→LC Select All→Drag and drop in Phil
7. I disconnected the laptop from the LAN and removed the mapped drive: LC Disconnect mapped drive icon→LC on correct drive→LC OK



8. I powered up my PC and accessed Phil through the WHQUSR05\Share I already had mapped on my PC. I then accessed the security permissions of

Phil, removed the everyone group and added myself and my supervisor with full control: RC on Phil→LC on Properties→LC on Security Tab→LC Everyone→LC Remove→LC OK→LC my userid→change access to full control→LC OK→LC Add→LC Show Users→DC my supervisors id→change access to full controll→LC OK→LC OK





After I had copied the hard drive from the laptop to the server, I knew this was not the best method, but I was unprepared to use other backup methodologies.

I backed up approximately 1 GB of data from the hard drive of a IBM 600X Think Pad to a Compaq 2500 series server with a 200MHz processor, 512MB of Ram, three 9 GB hard drives.

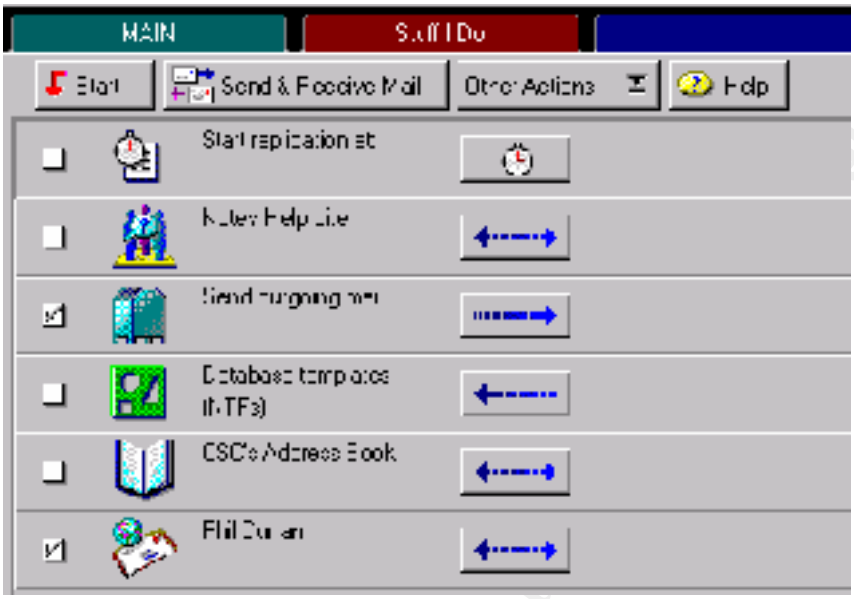
Chain of Evidence: My first concern was whether we should be trying the review the files in the computer or leaving the investigation to law enforcement. I voiced this concern to the lawyer and his reply was he too was concerned and had hired a consultant to advise him during the course of this incident. The consultant—a former Department of Justice lawyer with 10-years of computer crime experience—said the laptop was company property and we had every right to review the files and folders that were on the laptop. I then asked what kind of records I needed to keep as I reviewed the files on the laptop. The lawyer said nothing very detailed, just a brief description of what I had done will be enough. I also stated it would probably be a good idea if my

supervisor and I signed for the computer when we took it over to the computer lab. He stated this was not necessary, but we could if we wanted to. My supervisor and I wrote the following and signed the bottom:

We the undersigned signed out this computer from "my company" legal department on June 13, 2000 and 0800 hours.

As my supervisor and I were walking from the legal department to my desk, I told him I was uncomfortable with tampering with what might be evidence in a criminal case. I told him I thought we should keep a checklist of what we had done. We decided on the following format: time (in 24 hour time) and actions. My log is paraphrased as follows:

0810 – inserted 10BT PCMCIA card into PCMCIA slot
0810 – connected ethernet cable to PCMCIA card
0815 – Powered up laptop
0815 – Signed on using userid and password found on piece of paper on lower right corner of laptop
0816 – Entered two icons on main screen that made me think there might be evidence in the folders the icon is pointing to. Both icons led to empty folders
0817 – Entered Explorer to map network drive so I can copy hard drive to server
0817 – Decided to replicate Lotus Email before copying hard drive: LC Lotus Notes Icon→LC replicate



0820 – Re-entered Explored to map network drive: LC map network drive icon→in the path box, entered "server name"—LC OK
0821 – created directoy "Phil" on server
0821 – deleted mapped network server LC unmap network drive icon→LC on drive→ LC OK
0822 – Shut down laptop
0822 – accessed directory "Phil" from my desktop computer via Explorer
0822 – set permissions on "Phil" so only myself and supervisor have access to directory
0823 – accessed folder "y" to review for information
0823 – went to DOS prompt and typed in dir /p to determine file structure and to review last access dates. Saw evidence of recent access to directories that had same names as icons I looked at previously.
0824 – used print screen to make copies of directory structure to show supervisor and legal department
0825 – realized all sales images automatically create archive of mail older than 60 days on laptop hard drive
0825 – accessed archived mail file through Lotus Notes and began reviewing mail
0845 – finished reviewing archived mail and began to review current mail
0905 – finished reviewing current mail and began reviewing directories
…
…
1015 – returned laptop to legal department, lawyer refused to sign for laptop

I made some mistakes in the chain of custody for the potential evidence. First, I should have reviewed the directory structure with DOS dir /p command before I accessed any files—the last access dates of the folders I entered changed to the date I accessed them and overwrote the last date the salesman entered the folders. Second, I just handed the paper copies of the directory structure and my log over to my supervisor my supervisor who handed them over to the legal department. I made no attempt to properly mark them with date, time, and person who created them let alone put them in separate them. Further, I should have made the legal department sign for the laptop and the paper copies when we returned the laptop. Finally, I made a half-hearted attempt to correct my mistakes once I realized I made them. My mistakes had the potential to get the case thrown out of court for improper handling of evidence.

After I returned from SANS training, my supervisor and I reviewed my mistakes on evidence handling during this incident. We devised a methodology for proper evidence handling and documentation of an incident based on the *Incident Handling: Step by Step* guide and what I learned while attending this class. In the future, all potential evidence will be signed for when it passes from person to person—we have submitted a form to our legal department for their approval. In addition, we will have at least two people as part of the investigation team: one person will document everything the team does including time and actions. Further, we are in the process of revising the checklist in *Step by Step* to suit our companies needs. We believe these steps are just the beginning for us. As we grow in incident handling we will continue to mature our processes.

I realize this practical is out of the ordinary. I used this example for two reasons: First, I thought it showed a new theme on the computer incidents we must deal with. Second, it shows just how inadequately prepared my company is for handling computer security incidents.

Based on the information we provided, eg. Hidden excel spreadsheets with two years of fraud information, the possibility of deleted files based on last access date and empty folders, and the email trail to co-conspirators, our legal was able to present evidence to the salesman who then provided paper copies of the files he deleted and identified three co-conspirators: the first was an insider in Company A, the second was a bank teller friend of his, and the third was his wife.

My supervisor and I are still waiting to hear from any law enforcement agency.

Philip J. Curran