Global Information Assurance Certification Paper

GIAC Level Two Advanced Incident Handling and Hacker Exploits

Option 1 – Illustrate an Incident

Peter Szczepankiewicz
Candidate for GIAC Certified Incident Handler (GCIH)
Attended 8-12 Jan 2001

Table Of Contents

1. EXECUTIVE SUMMARY

In February 2000, our Computer Emergency Response Team (CERT) received a phone call requesting an on-site visit. The victim site was called Naskapi. There were many problems going on with their LAN, and they had reason to believe that there was an unauthorized access by an insider.

There were several reports of suspicious activity on their Windows NT LAN. Some of the events are shown below:

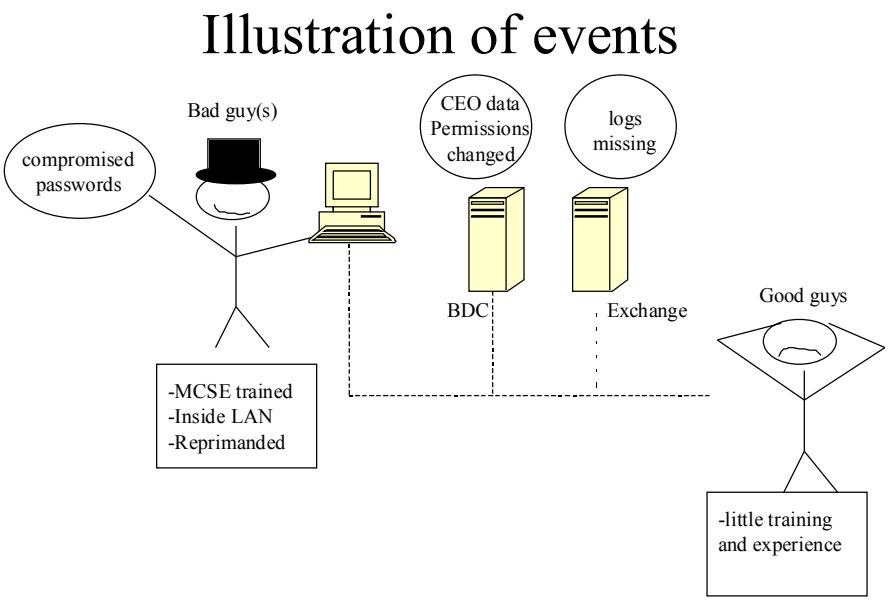


Figure 1. Illustration of strange events on LAN.

Figure 1 shows three strange occurrences on the LAN, including permission changes on CEO directory, a CD was missing with the passwords on it, and a Exchange logs were reported as missing. There were suspicious people working at Naskapi, who had recently been reprimanded and were prior systems administrators. Some of them had MCSE training. On the other hand, the good systems administrators were chasing their tails on this legacy LAN, with little to no experience or training.

The CEO of Naskapi had three basic questions. Who was in? What did they see? What did they leave behind?

Our CERT assembled a team that flew out on site. The evidence was kept as pristine as possible and was given to law enforcement. Security policies were given a face-lift. The system administrators were given lots of OJT, about 500 man-hours worth.

Poor systems administration influenced every reported event. For example, there was a practice of many people sharing one Administrator account. The Administrator account password had not been changed for a long time. Some local Administrator account passwords were blank. Important logs were never enabled. The CERT analyzed the data and found no evidence to validate that an unauthorized access did occur.

The topology of the LAN is shown below.

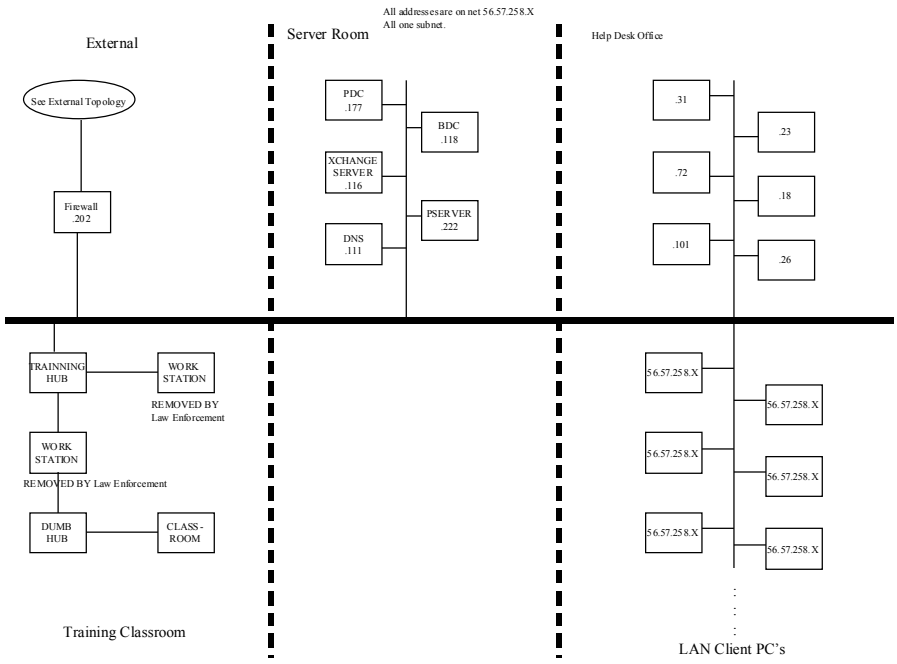


Figure 2. LAN Topology.

This LAN is all one subnet. The dotted lines are shown here to divide this topology into digestible parts.

2. SIX STAGES OF INCIDENT HANDLING

A. Preparation

About 10 months prior, Naskapi's web site was hacked, which prompted an emergency on-site visit from another agency. The visitors set up the servers during that visit.

Several good things had already been done. Naskapi's NT LAN did have a warning banner that gave consent to monitoring. We had management support. The visit occurred during a long weekend, so we did not have many users at work. The server room itself had a lock on it. No signs were posted because we were trying to keep a low profile so as not to tip our hat to an inside attacker.

Our jump bag included a laptop, ISS Scanner, l0phtcrack, NTCrack, NT Server 4 Resource Kit, and a few other books. Small incident handling notebooks were also brought to record all evidence. All people were instructed to take notes for everything they do.

We put together a small visiting team of four people. Two of us were from the CERT. One was from a software engineering company that had worked with Naskapi before. One person was a law enforcement officer, specializing in cyber-crime. We knew that we could be potential witnesses should this incident go to court.

The visiting team meshed with the Naskapi systems administrators. There were approximately ten systems administrators from Naskapi who were there to help. Three core Naskapi people were identified that would work on this incident until it was finished. We now had a core team of 7, plus lots of hands for follow-up labor.

We all sat in a circle in the help desk office and gathered intelligence. We had no pre-designed forms, but for each event we tried to answer the six W's: Who, What, When, Where, How, and Why. Phone numbers were collected from key witnesses. From this raw intelligence, I tried to separate out the important events as shown in appendix A. This was one tool to help triage, or prioritize which incident to attend to first. We agreed that nothing would be touched without the security manager's permission. This was important to keep people from being "in the way" and destroying evidence.

During the intelligence-gathering meeting, the security manager first spoke about multi-user Administrator account. This was an indication of poor security. Further, one of the people who used to work on the help desk was administratively removed and placed in another department. That individual was considered a disgruntled employee, and he knew the administrator account password. This individual was a student in the MCSE course. The inside attacker could have been that individual or the MCSE instructor.

After the group meeting, the security manager and I set up a small headquarters in the help desk office. This provided an easy reporting facility for the systems administrators. We had phone contact with the server room, and could centrally monitor all operations. Plus, our policies and other paperwork were all located in the help desk office.

Out of band communications were used to communicate with our 24x7 CERT headquarters. We used the telephone to keep in contact. I have a small contact list with me at all times as a regular part of my job. Towards the end of our time on station, I had to send a report back to headquarters. Instead of using the MS Exchange server on-site, I used an out of band e-mail provider. I chose yahoo mail because it was easy to set up a one-time account. I zipped the files with WinZip, using a password. Then I called headquarters, gave the password over the phone, and sent the attachment. I remained on the phone until the attachment was successfully unzipped and routed to the incident handlers in headquarters.

B. Identification

The first suspected misfeasance had occurred about three months prior. There was unexplained modification of permissions and deletion of data in the folder with the CEO's files in it. See event number 1 in appendix A. CEO Data was stored in this folder. The specific folder was \\NaskapiBDC\data\home\executiveitems\. This folder contained sensitive information on all legal proceedings, power of attorney, etc. Smith checked the permissions on this folder and assigned modify permissions to the Administrative Assistants Group. The next day full control was encountered again, and Smith never granted full control. Permission changes flow downward to all data in subfolders. This unexplained permission change was a recurring event since the MCSE class started about one month prior to our visit.

At the same time the MCSE class was ongoing there was an NT5.0 modified event ongoing. Before resetting the perms, Smith reported that there was no owner. The folder ownership was apparently blank. Smith, who was logged in as Administrator, took ownership and then re-assigned perms. The warning was in a

pop up window that only appeared for the Administrator account. A screen snapshot is shown below.

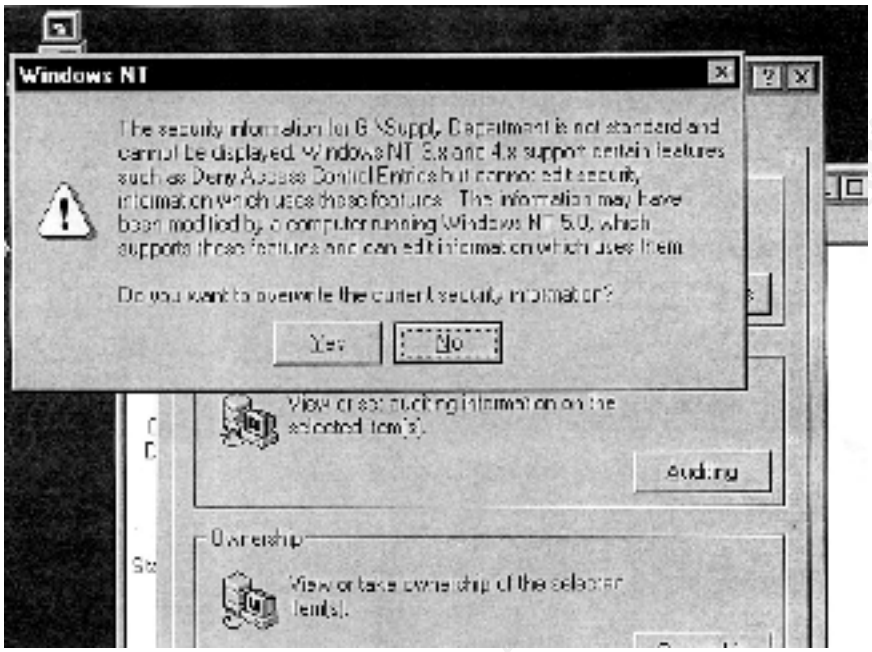


Figure 3. Windows NT5 Error.

I personally saw this warning only once. I printed a screen capture of the warning. One of the technicians told me that they had just been clicking OK every time they saw that warning. There are many errors that users see in windows and just click yes to get past the window. Unfortunately, this behavior may have contributed to the permission changes on the CEO's data.

One of the administrators told me that he suspected that this error was due to an attempted install of the Security Configuration Manager (SCM). I took down his information and recorded it in my notebook. Some MS technical articles were researched and they do suggest that there is some interaction between SCM and NT5.0 permissions on NT4, but this specific error is not defined. The specific MS technical articles are Q195509, Q195227, Q221074, and Q221472.

There was also error 1016. The following is a snippet from the Exchange Application Log that seems to suggest that some automated process is trying to insert the entire command into an SvcAdmin account.

2/6/00,7:12:22 PM, MSExchangeIS Private, Success Audit,(16),1016,N/A, NASKAPI , The description for Event ID (1016) in Source (MSExchangeIS Private) could not be found. It contains the following insertion string(s): NASKAPIDOM\SvcAdmin; Neal.
2/6/00,7:12:21 PM, MSExchangeIS Private, Success Audit,(16),1016,N/A, NASKAPI, The description for Event ID (1016) in Source (MSExchangeIS Private) could not be found. It contains the following insertion string(s): NASKAPIDOM \ SvcAdmin; Robert.

The above log entry is illogical because SvcAdmin is an account, not a group. User accounts cannot be added to other user accounts. The NT5 error coupled with the log error loosely suggested that there was software misconfigured in this system that was making permission changes. Perhaps this misconfiguration was also affecting permission changes on the CEO's folder. These pieces of evidence do not necessarily rule out the

theory of an internal hacker, but they don't necessarily rule out the theory of poor security.

There were other events, but the data in these folders was of such a sensitive nature that this event was our first priority. For detail on the other three events, please see appendix A.

There was a report that a user accounts from the classroom domain appeared in the Naskapi domain. One person witnessed a specific account called something like "instructor". The account was present during the MCSE class for about 2 days. This sounded very suspicious.

Before we arrived, the Win2K PC's were physically removed and were already in law enforcement custody. That portion of the investigation was already contained. The attacker may have used those PC's to exploit the administrator account in the WinNT domain.

These reported events were not yet corroborated by any facts in the logs or tape backups. The reports were not yet validated, and therefore not yet considered computer events. Unfortunately, there was no tape backup of the BDC from the time of the MCSE class. There were also no NT logs enabled for the folders in question. It was apparent that this incident would be very difficult to validate.

Being careful to not drop any evidence, I hoped that our CERT headquarters and forensic analysis of law enforcement would gather evidence on the insider. My task was to preserve as much evidence as possible. Still there was a nagging feeling that the cause and symptoms of these four incidents was basically poor security. I wanted to thoroughly scrub all the evidence we had available to us, patchy as it was. That included listening up for the "oh by the way" items that people would verbalize from time to time. Alas, no diamond in the rough appeared.

C. Containment

We kept a critical mindset and considered the conclusions that others had reached, trying to go strictly by facts from the logs. However, the systems had been rebooted and touched by several different technicians before we arrived. It was impossible to keep the events pristinely preserved because the activity began one month prior to calling us.

We did contact Naskapi's distant end network provider when we unplugged our point-to-point connection. Since the intruder was thought to be an insider, we did not spread news of the investigation upstream.

We were careful to keep a low profile. Technically, we knew that the insider might still be logged on. There was the possibility that the inside attacker could be monitoring our work at this point. In order to gather evidence, it was worth the risk to down the servers. First, the technicians checked the server manager tool to see if any users were still logged in. There were no NT logons when we began to shut down systems.

Physically, even the CEO mentioned that he would like to keep our presence unknown for as long as possible. For instance, one user walked into the office asking when the exchange server would be back up and running. The security manager told him to wait until Tuesday, and that Naskapi had some consultants doing technical work. We were able to maintain anonymity throughout the long weekend. Even on Tuesday morning, I was surprised to find how well we were hidden in this small company.

Zero level backups with verify onto a new tape was the first order of business. We gathered tape backups before doing anything to each server. Once the BDC and Exchange servers were backed up and the original hard drives were removed, we were able to modify the system.

We decided to not pull out the cat5 cable from the back of the BDC and Exchange servers at this point. Even though our incident handling from this point forward did not require the network, denial of service for an extended period might indicate our presence to the hacker.

Logs were collected. The matrix below shows which logs were available. An X indicates that log was present, and DNE means Does Not Exist.

SERVER	SYSTEM	SECURITY	APPLICA-TION
BDC	X	X	X
EXCHANGE	X	DNE	X
PDC	X	X	X
PRINT SVR	X	DNE	X
DNS	X	DNE	X
FIREWALL	?	?	?

Figure 4. Logs collected.

Please note that the security logs were never enabled on the Exchange server. This made it difficult to validate the verbal intelligence reports. Also, the firewall was an Intel PC running freebsd unix, not Windows NT. Nobody on-site had the password to the firewall and so we could not collect those logs. The firewall was constructed by a different agency some months ago.

To eliminate the possible introduction of malicious code, such as Trojan horses, back doors, or viruses, we intended to rebuild all the server operating systems. We specifically did not restore the operating system files from the tape backup. We avoided suspicious code. For example, we found automachron on one computer. Automachron is an ntp client for windows, but the fact that this software was not authorized made it look suspicious.

The system administrators at Naskapi were the system owners. A sense of trust was maintained with them. In addition to setting the stage of teamwork at the initial meeting, we specifically kept our fingers away from the keyboards and had them do almost all of the typing. There were hours when we would stand behind a system administrator and talk them through what to type next. We spoke out the commands, giving the system administrator time to understand what to do next. This was on the job training. As the lead incident handler, I was always mindful that the trust between our two teams was crucial. I think we were successful in establishing and maintaining trust. As a manager, one supporting piece of evidence was the fact that the local systems administrators willingly worked 7am to 1am with us for 5 days straight.

The Naskapi administrators decided to combine DNS and print services onto one box. Their thinking, innovation, and reinvention of that inherited legacy system gave them more a sense of ownership than they had ever had.

The decision to discontinue operations for the weekend came straight from the top. The CEO had given us clearance to shut down all services for the weekend if needed. He wanted a thorough collection of detailed forensic evidence, and basically LAN operations had taken a back seat to our visit. We tried to balance this liberty with keeping a low profile so that the insider would hopefully not detect our presence. LAN operations were fully up and running by the following Tuesday.

D. Eradication

We performed some general systems administrator scrubs. Good security is based on good systems administration. In hindsight, this seems to be the most relevant eradication to the problem at hand of poor security.

The following systems administrator tasks were performed while we were on site. We removed the practice of Administrator multi user account. Only two people knew the new Administrator password. Those two people were the security manager and the work-center supervisor. The new password was written to a form, sealed in an envelope, signed along the seal and locked up in a safe. The valid systems administrator's personal accounts were added to the Domain Administrators group. We secured the registry from remote administration.

We changed all account passwords. Whoever did not have a signed user agreement form on file was considered an unknown account. Unknown accounts were locked out. Many accounts were locked out, but only a few people walked into the IT shop on Tuesday morning to unlock their accounts. When they came in, the administrators collected a user agreement form before unlocking the account. For future user accounts, we made one hardened account. For example, logon hours and logon workstations were restricted. That template would be used for new accounts.

We began to write down the business plan for group access to needed objects. Once this plan was finished, Naskapi could review all domain groups, members, ACLs, and permissions. DumpACL could be used to aid this process. We began to re-write computer security policies with principle of least privilege (POLP), and defense in depth (DID) philosophies.

There was an MCSE instructor contracted at Naskapi. He used to be physically connected to the operational LAN. There was no policy to state that contractors should not be allowed to plug their equipment right into the LAN. We included this idea in the new security policy. It was possible that the visiting MCSE instructor, or one of his students, had actually hacked into the domain controllers.

We checked for malicious code on all NT Servers. Anything that runs upon startup should be documented, and you should know why it runs. There are 4 places that can run a program when you turn on a windows NT machine. They are:

1. C:\WINNT\Profiles\All Users\Start Menu\Programs\Startup
2. C:\WINNT\Profiles\????????\Start Menu\Programs\Startup – where the question marks represent any specific user account.
3. HKLM\Software\Microsoft\Current Version\Run
4. HKLM\Software\Microsoft\Current Version\Run Once

Even after manually checking these places, a Trojan horse may have still been present in the domain controllers.

We scanned the internal network to look for vulnerabilities and malicious software. We knew that we could not target individual users, so we scanned the entire NT hard drives for malicious tools. We scanned the help desk office first. This was done for training purposes. The administrators on site were able to patch the vulnerabilities found with basic downloads from the vendor web site. They gained confidence in their skills, and were prepared to help secure the servers if need be.

With confidence growing in the administrators, we asked about scanning the training classroom where Win2K was installed. We saw for our own eyes that both Win2K PC's were removed and all that remained was an empty hub. We moved on to scan other parts of the LAN.

On the weekend, we scanned all of the PC's that were powered on. This scan covered 72 out of approximately 300 hosts on the LAN.

We then scanned the server room. There were no high-risk vulnerabilities found in the server room. This seemed to be supporting evidence that the attacker was not covert at all. He was probably walking in the front door with the administrator password.

One big question remained in my mind. Are there any attacks from outside the firewall? We had no log files, but we could try to find active vulnerabilities in the firewall. We spent hours of preparation work to scan the external interface of the firewall. We collected topology documents, discussed them, and called the distant end. The actual scan took only about 20 minutes. The results were no high vulnerabilities in the firewall.

On Monday night, the Exchange services would not start until we used the old name and password. An insider may have known this password. Logon and logoff audit for SvcAdmin was turned on the night before LAN Operations began. In the out briefing with the CEO, I requested permission to try to change that password and reboot the Exchange server at lunchtime. The password change took effect at about noon. The exchange service account was vulnerable on our LAN for one morning, but was fixed. No unexplained SvcAdmin account logons were found in the log.

To eradicate an inside attacker, we tried to imagine what the inside attacker would do next. He would probably go after the CEO's administrative data directory. So we turned on auditing for every type of access on that folder and all subfolders. He would probably also try to get the new Administrator passwords. We had run syskey on all servers. Since pwdump2 functions with syskey, we turned on auditing for all the places in windows NT that contain passwords. They are:

C:\winnt\system32\config\

C:\winnt\repair\

The registry key, HKLM\Security, was also audited.

Emergency Repair Disks (ERD's) were protected. The rdisk /s command stores the passwords to the disk. On this LAN, the registry was small enough to compress onto a floppy. Eventually, the registry will outgrow a floppy disk, so some other removable media will be required soon, such as a CD-ROM or zip disk. The security manager was told to be sure to secure these in the safe.

The attacker might try to walk into the server room and run getadmin, so we verified that SP6a stops getadmin. In case a new variation of getadmin that thwarts SP 6a came

out, we made sure someone was always present in the server room. BeAdmin might have been used, as I learned in the GIAC class.

The screen capture below is an example.

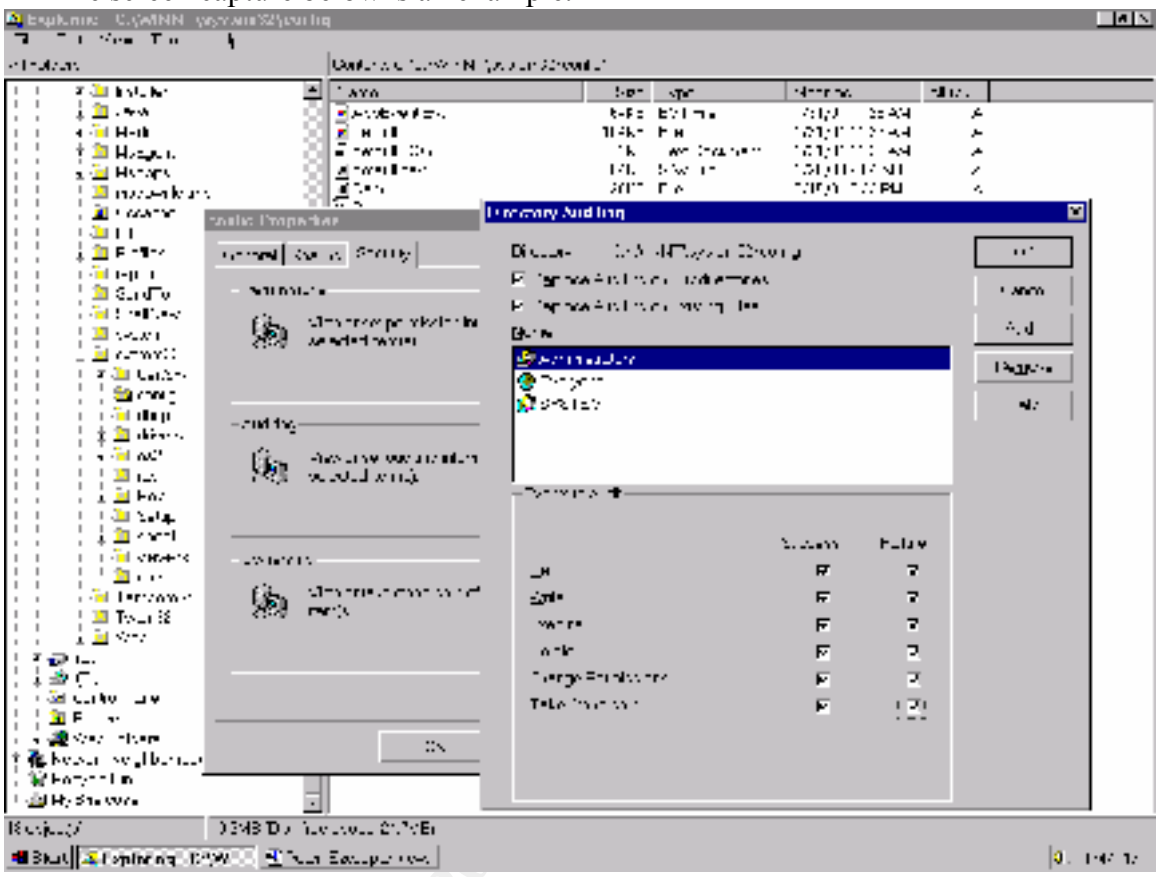


Figure 5. Screen capture of audit policy on the config directory.

If the attacker were to try to run pwdump2 to dump the passwords from the SAM, how could we see that in an audit? We were looking for the footprint of pwdump2 in the NT audit logs. We ran pwdump2 and found that a write_dac event is generated.

Now we should at least be able to tell if our passwords file was dumped from the active registry. The attacker would successfully collect the hashed administrator password and would begin to try to crack the Administrator password. A pass phrase was used for the Administrator password, with 14 characters, using letters, both capital and small, numbers, and special characters. At this point there would be a race in time. We would have to notice the pwdump footprint before the attacker could crack the password. The requirement for real time alerts led to the recommendation to install an IDS.

We cracked passwords. Reports were taken of passwords cracked within 1 minute, 10 minutes, and one hour. A new password policy was drafted. Naskapi used passfilt.dll and SYSKEY to help implement their password policy.

Basic training in Windows NT was covered, such as local logon versus domain logon. One of the common vulnerabilities found was a blank password for the local administrator account. We kept a checklist of all PC's with a blank password for local admin and performed the following checks. We checked for backdoors by opening user manager and looking for unauthorized accounts, probably with admin rights for local machine. We showed Naskapi how to identify the Administrator account in the registry.

The Administrator account SID ends with 500. Guest ends with 501. The account name does not necessarily need to be "Administrator."

We checked for accounts that were assigned the advanced permission "debug programs." This can be seen by clicking on Start – Programs –Administrative tools - User Manager – Policies menu – User rights – check Show advanced user rights – check Debug Programs. This right is not granted by default in NT. Granting yourself the debug programs right used to be an effective back door with SP3. That account would be prepared to successfully getadmin.

The security manager learned how leaving the door open just a little is like an invitation to a hacker to push the door all the way open and walk right into the domain. I spent time with the security manager reviewing policies, and how to implement those policies.

We also recommended that the Security Manager write and maintain the disaster recover plan. What's it worth to loose data? How high is the risk? We also noted that the data backup schedule needed to be reworked. Check the backups with regularly check restores. We recommended that management fund the IT shop for one spare server to drill these critical data restores. The security manager had been asking for a spare server for some time, and now he had the data to justify his request. The spare server was funded during the out briefing.

E. Recovery

Because we did not have replacement hard drives on station, a team of people searched for new hard drives. This finally paid off on Saturday afternoon when several 40 GB IDE hard drives arrived. The original servers had ultra-wide SCSI RAID 5 arrays. The best we could find were 40 GB IDE hard drives and IDE controller cards. This was a compromise that led to many technical problems.

All the NT servers in the server room were restored. This includes the Print Server and DNS server, which were fully rebuilt from original media. The BDC, PDC, and Exchange server were restored from data backups.

With a clean system install, we searched for the most recent backup before the intrusion had taken place. This was a problem. The suspect intrusion first occurred about one month prior to our visit and the tape backup rotation did not reach that far back. Some improvisation was used to avoid any malicious code.

BDC Restore.

We configured two 40 GB drives as a mirror set, providing 40 GB of space. We also put in a smaller hard drive of 4 to 6 GB for the OS. This hard drive was a spare that we had in the IT Office.

We ran into some problems with restoring data. The BDC tape backup had data only and no operating system, so we had to find an operating system from elsewhere. We made a mirror of the system disk on the PDC and put this copy into the BDC. We took the system disk back into the BDC and booted up. Upon boot up, the system thought it should be the PDC but it offered us the option to demote to BDC. We chose to demote to BDC and were moving forward. We now had a valid system disk working in the BDC.

In retrospect, we would have been wiser to rebuild the system disk from the original media. Such an approach would have further limited our exposure to malicious code.

We partitioned the mirror set as the BDC was configured previously. We then restored all BDC data onto the mirror set.

Because the registry was not available for restore, the user data shares were not in place on the restored BDC. We had to manually create home shares for each user. One had to create the share and set permissions for every user.

PDC Restore.

The new PDC hardware was different from the old PDC, so a new system had to be installed. We restored only the SAM from the tape backup onto the new PDC. We then built the BDC and synchronized the SAM. This method limited our risk exposure to any malicious code on the tape backup.

We swapped out the hard drive in the PDC in the following manner. We took the original PDC off line. Then, we promoted the BDC to a PDC. We removed the hard drive from the original PDC and handed it to the security manager. We placed a new 40 GB hard drive in the original PDC. We built the original PDC from the original media. During the system load, we joined the domain as a BDC. After the system was installed, we promoted back to become the PDC.

In retrospect, this technique gave us somewhat of a clean install. We did limit our exposure to malicious code in the system by rebuilding from the original media. The action of joining a domain causes the SAM to be copied from the existing Domain Controller. The registry itself is not likely to contain malicious code. However, the registry could contain pointers to malicious code. The malicious files might even be stored on a mapped drive, not on the local drive.

By 5pm on Saturday, the BDC had been restored, and was configured and working. So we tried to do the same with the Exchange server.

Exchange Server restore.

Saturday afternoon, we had a successful backup of Exchange. We had a small OS drive, and two 40 GB hard drives for a mirror set. We were able to restore the data onto the mirror set.

The system drive was rebuilt, using the original NT server disk. We nuked the Exchange server from high orbit.

The Exchange system drive was complex to restore. We built it first with a standard NT load. We loaded the NT server and prepared the data drives. The data was copied down to the 40 GB mirror set, restoring all data. Then we reloaded Exchange from a BackOffice CD. We tried to create a new service account with a new name and password. Whenever we started to bring up the Exchange server services, we got a communication error. The services would not start with a new password. The IS was looking for the old familiar name and password. We re-installed the Exchange software system. This time, with a fresh install, we used the old Exchange service account. The Exchange services started right up this time. The data imported fine. We were also very tired at this point.

Validating that systems were up and operational was easy for us because of our hand-off practice. Difficult as it was at first to not touch the keyboard, it proved to pay off in the end. Not only did the Naskapi administrators validate all operations on the LAN, but

they had rebuilt every NT server in the server room. Their re-invention gave them a huge confidence boost and detailed interest in computer security.

On the first day, IT Office personnel were present in the server room the whole day. It was reported that no one outside of the IT Office tried to walk in. After one day back in operation, there was no new evidence of an inside attacker.

F. Follow up / Lessons Learned

Naskapi decided to purchase a scanning program and routinely run scans on their network. This became a standard procedure assigned to the work center supervisor.

A follow up report was written. The outline is in an Appendix to this paper. True consensus was not reached for the follow up report. I had a feeling that most people would agree with the report, but I never ran the report by the key players.

The only affirmations gained from forensic analysis was poor security. No inside attacker was ever pin-pointed, either from the law enforcement forensics, nor from my on site incident handling.

Replacement hard drives should have been on site before our arrival. Also, a drive duplicator would have helped immensely with our Exchange backup problems.

Our jump kit was incomplete and should be fixed. Incident handlers must be familiar with these tools before going on site. The jump kit should contain the following:

- PGP and key exchange with headquarters
- Small tape recorder
- Binary backup – Safeback or ghost
- Disk duplicator with ultra wide SCSI and IDE interfaces
- Undelete for NTFS
- 10 New 40GB backup tapes
- Backup hardware, such as the Quantum DLT4000.
- CD's with system binaries for Linux, NT, and win2K
- Windows NT4 Server and Win2K Resource Kits
    - Security Configuration Manager
    - C2 config tools
    - Syskey
    - Poledit
    - Dumpel
    - Dumpevt
    - Dumpacl
    - Dumpreg
- SANS NT Security Checklist
- 4 port 10MB hub
- 4 10BT cables
- Laptop with NT and Linux
    - For NT and Linux, scan self and patch all vulnerabilities possible
    - For NT, shut off the browser service
- ISS Scanner
- Tcpdump or snort
- Call list to reach CERT headquarters

- Cell phone
- L0phtcrack with pwdump1 and 2
- Inctrl
- Tripwire
- 10 Small Notebooks

Checklists were not used until the follow up phase. A checklist on backup exec would have been good to have. I was inventing on the fly. Without a checklist, I forgot to double check one important thing. The security log eventually reached its default maximum capacity and began to overwrite events during the day. Although I trust that the systems administrators were checking the logs frequently, I did not have the ability to query through all the data at the end of the day. I had hoped to do some queries of the full logs. The log size was increased to prevent this from occurring again. Naskapi was encouraged to get the Windows NT security checklist from SANS.

PGP keys should have been exchanged with our CERT prior to the visit. Sending mail by yahoo was still on the network, and the insider would still see the e-mail header going to the CERT if the insider was using a sniffer.

There was one domain trust that was present with a domain called Purple. This was a two-way trust. The Purple domain was a well-known domain and the trust had been in place for a long time. This domain was not investigated. In retrospect, I should have investigated more about the Purple domain. I know there was only one PDC, with about 4 users in the domain. This was really more like a workgroup. Perhaps somebody decided to set up a domain rather than a workgroup to protect some sensitive data. If so, the Purple domain was probably also compromised by the insider. Furthermore, there may have been better security log files in the purple domain. This potential source of evidence was never checked.

In class, we learned that if we have to get on a plane to handle and incident, then you're probably not organized right. My company would fit this mold. I understand that ideally we should be able to contact an office in the local area of the incident and send a representative out from the local office. Our company can barely retain systems administrators due in part to the opportunity cost. With limited resources, we have one central CERT with a team of computer security experts. We train centrally, handle incident remotely whenever possible, and fly away when an on site visit is needed. I believe that a centralized incident handling team is probably the most realistic type of organization for us today.

The risk that the inside attacker was monitoring our work could have been better addressed with a little more detailed checking. In addition to checking server manager for active logons, netstat would show what tcp connections were currently open. Even better would be a hardware sniffer or tcpdump on a laptop plugged into the local server hub would help us determine if any covert sessions were ongoing with the servers.

Our laptop was not hardened before going into the wild. The browser service was left on and there were common vulnerabilities present. This needs to be corrected for next time.

An empty hub was present in the training classroom. In hindsight, there were a few opportunities there that we did not have the time to pursue. The hacker was likely plugged into this physical hub with a Win2K PC. It would have been worthwhile to plug a PC into that hub and build a Win2K Server from scratch, just to see what becomes

available to this Win2K machine. Does the Win2K PC produce that NT5 error on the NT4 boxes? Does that Win2K change permissions on any directories, especially the CEO's Administration directory? Why was that directory so easy to delete? What are the interactions between WinNT and Win2K, in this unique LAN situation?

This LAN was all one big collision domain, which is a poor design. There is a security benefit to subnetting. With subnets, I could have looked through the router logs to locate the hacker's PC. The first router was the firewall. The firewall logs would have at least helped me to determine if an attack was coming from the outside.

We trusted that the logic within ISS Scanner properly identified that high-risk vulnerabilities are truly the most imperative to fix. I later learned from Eric Cole that you should not blindly trust any one scanner to find high-risk vulnerabilities. Using the defense in depth framework, it would have been logical to use nmap to scan for interesting ports, especially on the firewall. Any two scanners should give me more data for a better vulnerability analysis than one scanner can provide.

What rules were in place on that firewall? One enormous problem we discovered was that nobody had the password to log into the firewall to see the rules that were in place. The firewall was installed about 10 months prior to my visit and the person with the password had since left the contracted company.

The history of such a messy situation deserves explanation. In the world of network administration, there are a whole lot of temporary fixes. This freeBSD firewall was only supposed to be in place for a few weeks, until a hardware-based firewall could be installed. Besides, this LAN was firewalled from the Internet at some point upstream. So, while this LAN was exposed to neighboring LAN's, we were not wide open to the chaos of the Internet. To make a long story short, the true firewall was not installed some 10 months later, and brought to the attention of management by an on-site intrusion response team. I left this problem with the site security manager.

I wanted to be able to say with absolute technical confidence that there were no firewall rule violations occurring. It would be good to know that no strange tcp and udp ports were open, and verified by the logs. Also, I would check for fragmented packets, footprints of firewalker, and icmp packets communicating with anything internal through the firewall. Needless the say, our analysis of the firewall was cut extremely short.

Tripwire could have been used to check for malicious code in the restored Exchange server. As described on slide 83 of the SANS guide, we could build a fresh Exchange server on the side and compare it with the Exchange system files on the restored system.

Concerning physical security, a new lock should be placed on the gate and there should be tight controls over the key. For example, there could be one key available from the IT Office, locked in a desk drawer out of plain sight. Then a backup key should be locked away in the safe with the administrator password in the security manager's office.

Naskapi could try to corner the insider in action. Give a walkie-talkie to each of the ten IT Administrators throughout this first workday. The technician in the server room monitors all failed logons. Then the server room radios all personnel when there is a failed logon, with finger on the map of the physical layout of all workstations. Even a real administrator should not be trying to log into the administrator account. Just use a camera for impartial evidence. If not, then the closest person to that workstation should walk over and check out who is sitting at that workstation. Suppose that an attacker was casually sitting at that workstation. In order to secure legal prosecution, the IT person

should then note the time on the office clock, write it down in pen in a marble notebook, and get a second credible witness to notice that this casual user is sitting at that workstation at this time. It would be best to win such a battle in court rather than confront the attacker moments after he attempted intrusion. Collect the facts, get witnesses, and turn it all over to law enforcement.

We should have documented the specific security policies we left in place. On a domain controller, open user manager for domains. From the policy menu, select Audit. Capture that screen using alt-print screen and then paste it into this word document here. This is an example.

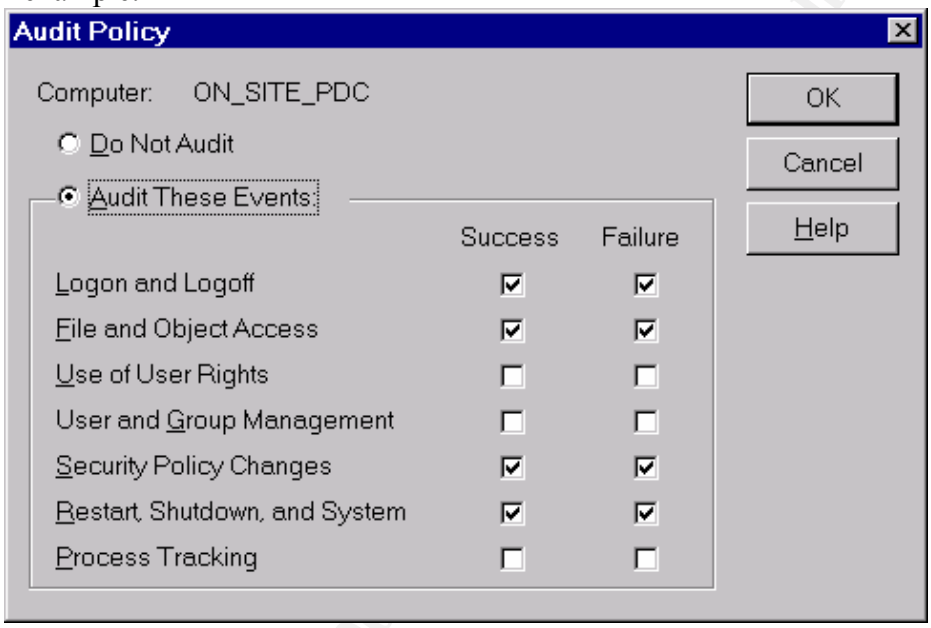


Figure 6. Audit policy from User Manager for Domains.

On each NT server, what is the audit policy on the c:\winnt\system32\config folder? From windows explorer, drill down into c:\winnt\system32\config. Right click on config and select properties. From the security tab, click Auditing. What does that window say? Use alt-print to capture the window and paste it here. This is only an example.

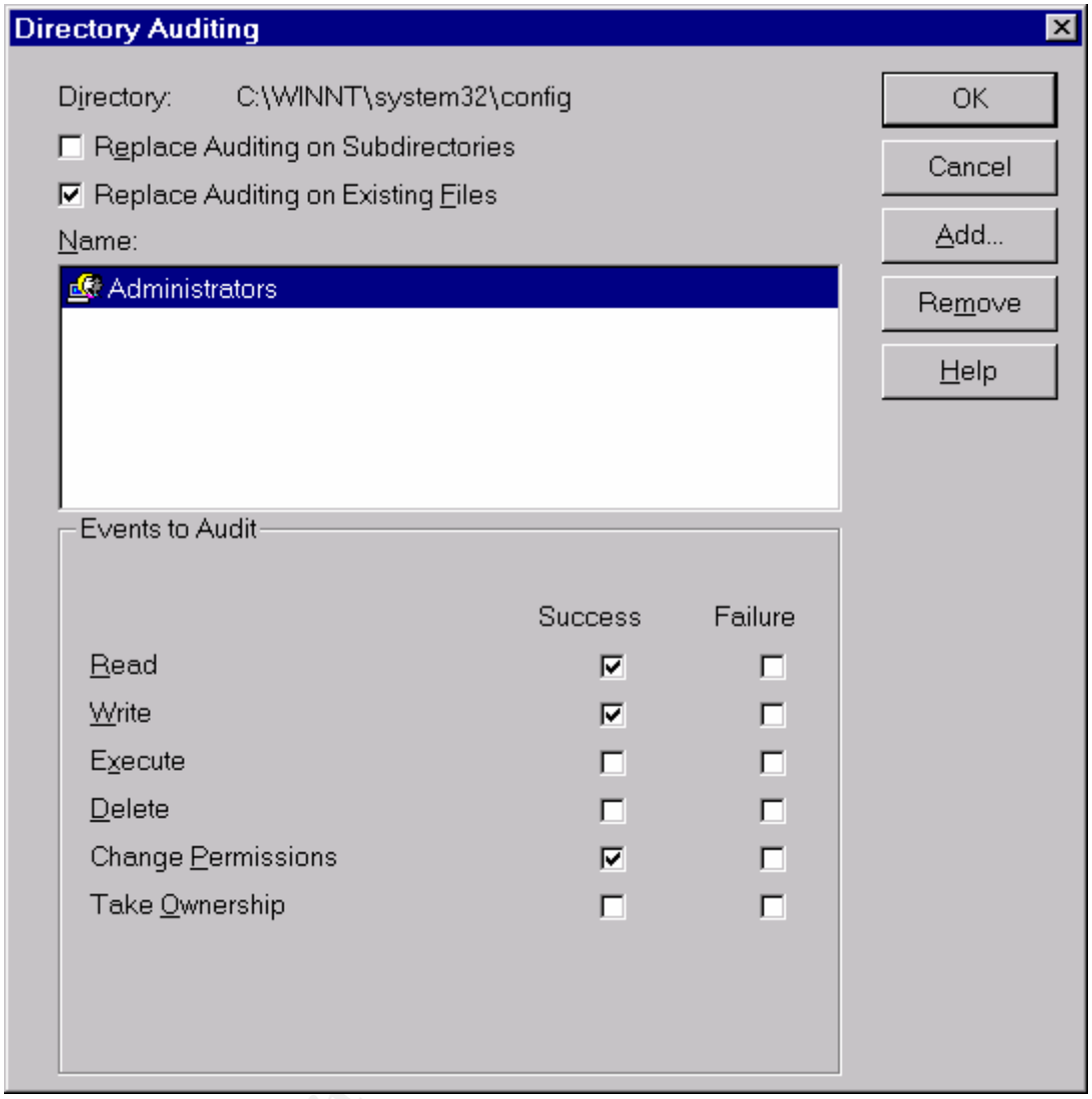


Figure 7. Audit policy on the config folder.

Inside the config folder, what is the audit policy on the file called sam? Right click on sam, select properties, security tab, and audit. Alt-print screen. Click over to word. Hit ctrl-v to paste that screen here.

Inside the config folder, what is the audit policy on the file called Sam. log? Right click on sam.log, select properties, security tab, and audit. Hit Alt-print to screen capture. Click over to word. Hit ctrl-v to paste that screen.

We wrote down a procedure on how to check when a person last logged onto a computer. One idea was to open windows explorer, click on the user profile, search all files, and sort by date modified. A similar idea is shown in the Appendix with In Control.

3. CONTAINMENT PROCESS

We set a small trap with the C:\winnt\repair\ directory after the system was rebuilt. On the PDC and BDC, we opened user manager, changed the administrator password back to the old one. We ran rdisk /s from the command prompt. This made a copy of the SAM into the repair directory, but the administrator password was stored as the old one.

Then we opened back into user manager for domains, and changed the administrator password into the new one for regular operations.

We turned on all auditing for the repair directory. There would be no performance hit, since the NT system does not normally access this directory. The repair directory is used by the system only when rdisk is run. With auditing in place, even if the attacker managed to grab the SAM file from the repair directory, he would get the old password, which he probably had in the first place. This just might produce enough confusion for the attacker and he might try to logon with that old password. This human behavior would produce a computer event, a failed logon attempt.

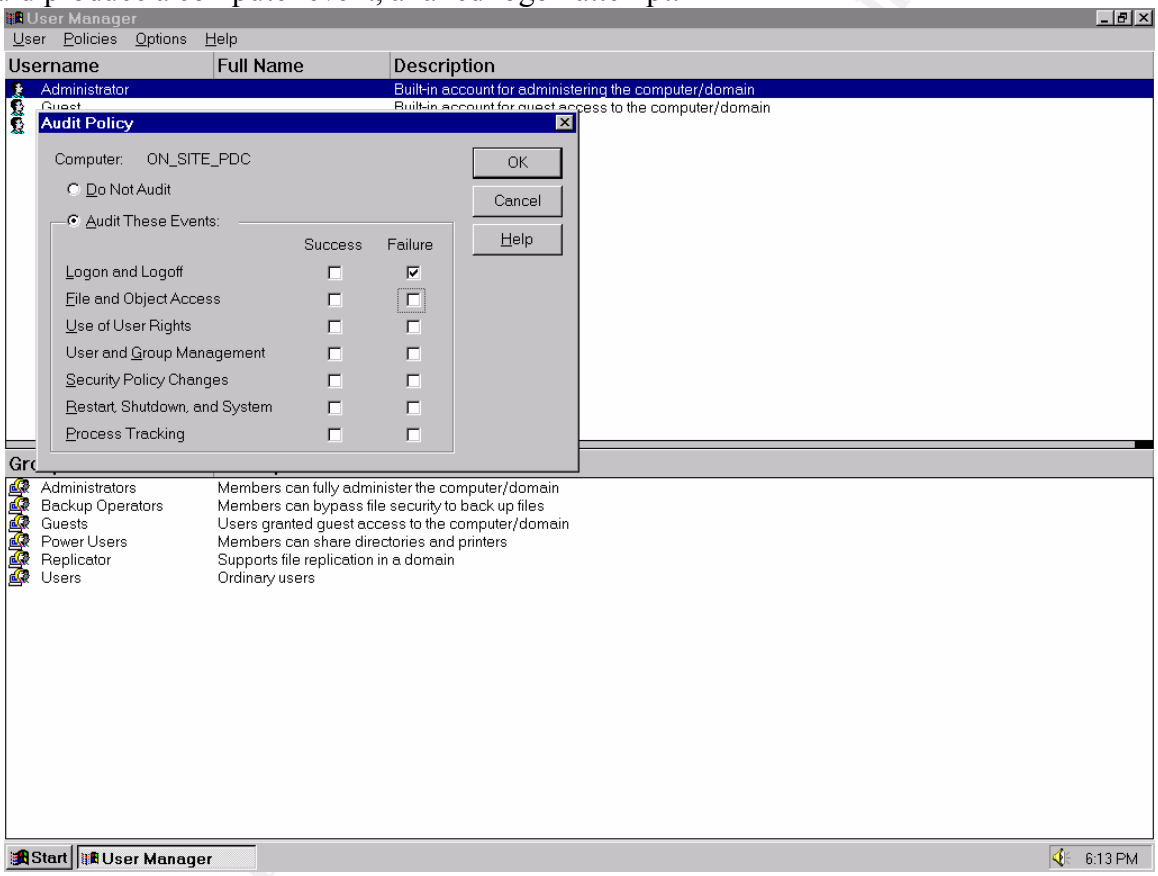


Figure 8. Audit the Administrator account for failed logon attempts.

In user manager for domains, we set up auditing for all failed logon attempts for the Administrator account. A failed logon entry in the NT logs would allow us to pinpoint what computer on the LAN was used, as shown in the example screen capture below.

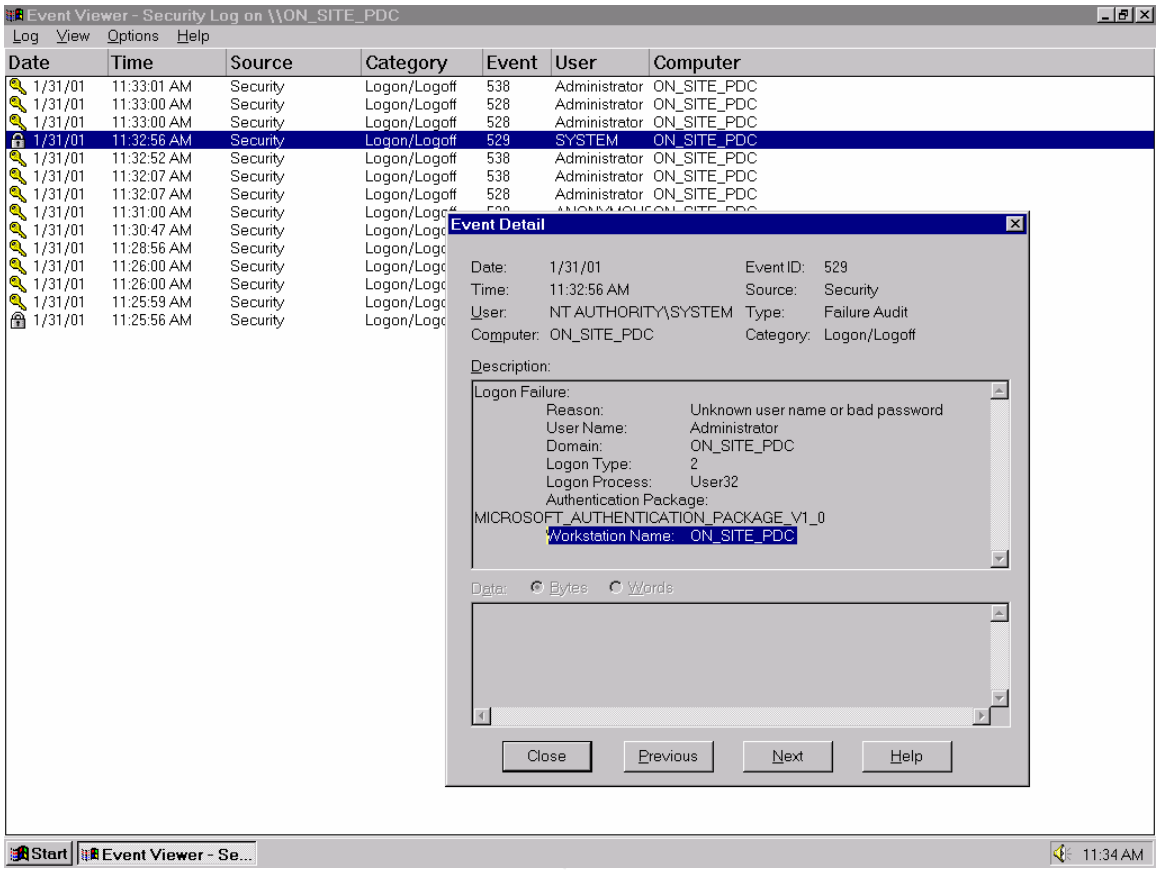


Figure 9. Workstation names are identified in failed logon attempts.

This screen capture shows WinNT event viewer. Notice the background window and see the lock icon by the failed logon attempt. This lock icon is visually easy to recognize when scanning the logs. Double clicking on this failed logon verifies that someone was trying to logon to the Administrator account from a specific workstation on my LAN. In this example, the workstation name is ON_SITE_PDC. Therefore, if the inside attacker were to try to logon with the Administrator account, we would know what workstation was used for the attempt.

Concerning honey pots, we discussed changing the IP addresses of the servers. However, the insider was hacking from above the NetBIOS layer. Changing the IP address would not draw the attention of this hack. The NetBIOS name was the target. Changing the NetBIOS name would impact operations in a Windows NT LAN. There was no easy way to set up a decoy PDC or Exchange server for the insider to attack, while carrying on operations.

The Administrator password was changed, and stored in a signed, sealed envelope with the security manager. The Exchange service account password was changed. Any user account with no user agreement form was disabled. Those old accounts might be backdoors for the insider. We subscribe to the theory of deny all and permit only what is known. We verified that no users were granted Administrator rights. No user accounts were found in the Administrators group that should not have been there. We ran a password crack on the SAM, using l0phtcrack to enforce the password policy. Finally, ISS Scanner was used to find vulnerabilities, which were manually patched.

4. SYSTEM BACKUPS

The tape backup system was the DLT4000, from quantum, distributed by Dell. Specifications for this tape backup system are available at the following url: http://www.quantum.com/products/dlt/dlt4000/dlt_4000_overview.htm.

This backup system plugs into the SCSI port on the back of the server. Backups occur out of band from the network. The tapes were 40 GB each. We were able to do a zero level backup to a new tape with verify turned on for all the backups run. The backup software was Backup Exec from Veritas. The BDC, PDC and the Exchange server were backed up to tape.

BDC Stats:
Server Hardware Manufacturer and Model: Dell 6300
Corporate Property Number: 000906
Operating System: Windows NT 4 Server
Disk Capacity: Six of the 9.2 GB Hard Drives in a RAID 5 Array
Bus: ultra wide SCSI

The BDC backup had completed the night before our arrival on site. This backup was part of the rotation that the lead system administrator was trying to get started as a regular practice. However, this backed up only the data and not the operating system. Thinking that we had a good tape backup, we pulled the drives out and turned them over to the security manager. The BDC data contained the CEO folder that was experiencing permission changes.

PDC Stats:
Server Hardware Manufacturer and Model: P-II 400 MHz, Dell Optiplex GX1
RAM: 128 MB
Corporate Property Number: 000905
Operating System: Windows NT 4 Server
Disk Capacity: 6.4 GB
Disk Manufacturer: and Model: Maxtor 90463E6
Bus: IDE

The PDC backup ran without problems. It took less than 1 hour to complete. The PDC contained mainly system data.

Exchange Server Stats:
Server Hardware Manufacturer and Model: Dell 6300
Corporate Property Number: 000908
Operating System: Windows NT 4 Server
Server Software: MS Exchange Server 5.5
Disk Capacity: Six of the 9.2 GB Hard Drives in a RAID 5 Array
Bus: ultra wide SCSI

The data on the Exchange server was about 20 GB. The restore was failing at about 10 GB, which took about 4 hours, each time. The specific error of that first hang was a backup exec software error, a dependency error. The log had about a hundred of these entries just when the backup aborted. One entry is shown below:

Fri 7:07pm event log entry

"NT user NASKAPI\svcadmin logged onto Tommy mailbox, and it is not the primary winnt account on this mailbox."

Naskapi had two versions of backup exec. On Saturday morning we did re-install the other Backup Exec. Even with the different version of Backup Exec, we still had the same problem with the Exchange backup.

The second attempt ran for about 4 more hours and then hung again at 10:20 pm. We stopped all MS Exchange services in the services applet of the control panel. Then we started backup for a third time.

The third attempt was set in motion and we went home for some sleep. When we returned at 7 am, we found that the backup had run for about 4 hours and then it hung again. The same error occurred. We looked over the standard backup exec job settings in the GUI. We stepped through the menus and looked for anything abnormal. Everything looked like it was in good working order. We tried to run the backup again, but we got the same error again at 11am and the backup failed.

At this point we looked outward for assistance. A friend of one of the administrators volunteered expert help, using Ghost. We tried to copy the Exchange data from RAID drives to a 40 GB IDE hard drive. This became a game of mental gymnastics to copy data from a RAID array through the SCSI interface onto the IDE interface to an IDE hard drive. We checked our terminators and jumpers several times to ensure that the SCSI chain was properly terminated, and that the IDE jumpers were properly configured. Vendor diagnostic disks showed that the SCSI side was working and the IDE side was working. For some reason, the Ghost backup could not work with the two together.

We returned to Backup Exec. We knew that the failure happened at about 10 GB, so we broke the backup job into two jobs of less than 10GB each. The C drive with the system files was one job. The D drive with the Exchange Information Store (IS) was another job. Using the backup exec software, we created new jobs, putting the appropriate drives into the particular job. The jobs ran until mid afternoon and it completed successfully. In the end, the MS Exchange drives were secured as forensic evidence for law enforcement.

5. EVIDENCE HANDLING

The list of all evidence is as follows:

1. Win2K PC's.
2. Hard Drives from servers.
3. Interviews.

The visiting MCSE instructor used the Windows 2000 training PCs. Both of those computers were removed and entirely turned over to law enforcement prior to our arrival.

The hard drives from the servers were treated as possible evidence. If there was a misfeasor, then there might be some clues remaining on the server drives. We were meticulous about which drives might contain evidence. We considered the BDC, Exchange Server, the PDC, Print Server and DNS server drives as possible evidence. We considered the old DNS server because IIS was installed. The host may have had many vulnerabilities that could have been exploited. Without rebooting, we downed the DNS and print servers, removed the hard drives and handed them over to the security manager. For the remaining servers, after a good backup, the drives were pulled out and handed to the security manager.

The chain of custody procedures were very simple. Any hard drive that law enforcement might use in a court of law was treated as evidence. The security manager locked them in a safe in his office. He was the only one who knew the combination to that safe. No one else was able to tamper with the evidence. The drives were removed from the safe and handed over directly to law enforcement when they arrived.

Not rebooting hard drives is ideal because there may be deleted files left behind by a hacker. Recall how files are still on a hard drive when deleted. Only a pointer to those files is actually deleted. The data files are now considered white space and can be written over as the computer needs. During a boot-up, temporary files are written to the disk. That is why simply rebooting can destroy evidence. For the Exchange server, BDC, and PDC, we had to reboot a few times due to problems encountered with the backup and restore.

Law enforcement conducted forensic analysis of the hard drives. A good discussion of computer forensics can be found in Cybershock, by Schwartau. The law enforcement officers mentioned that they would be looking for deleted files on these drives. The interviews that we conducted upon our arrival that first night were analyzed and broken down into four distinct incidents. All of this information was made available to law enforcement, from our original notes, to the analysis reports.

6. REFERENCES

1. Brown et al. Competing on the Edge, Strategy as Structured Chaos. 1998. Harvard Business School Press.
2. Carnegie Mellon University. Software Engineering Institute. NT Security Brief.
3. Electronic Communications Privacy Act.
4. http://www.quantum.com/products/dlt/dlt4000/dlt_4000_overview.htm
5. Hutt et al. 1995. Computer Security Handbook Third Ed. John Wiley and Sons, Inc. ISBN 0-471-11854-0
6. ISS Scanner User's Guide
7. James et al. Microsoft Windows NT 4.0. Security, Audit, and Control. MS Press. ISBN 1-57231-818-X.
8. Lammle et al. CCNA Study Guide. Sybex
9. Northcutt. Network Intrusion Detection, An Analysts Handbook. 1999. New Riders Publishing
10. SANS Institute GIAC Certified Incident Handler. Book I Incident Handling. January 8-12, 2001.
11. SANS NT Security Checklist.
12. Schwartau. Cybershock.
13. Windows NT 4 Resource Kits, both Server and Workstation
14. www.microsoft.com

APPENDIX A. INTELLIGENCE GATHERED

Chronology of significant events:

Apr 1999	Alsoft gives 2 CDs with NTCrack to Naskapi. Alsoft installs firewall and Exchange server at Naskapi.
June or July	Administrative memo for Roberts
July	Administrative memo for Norman
11-29Jan. 2000	MCSE class ongoing
Approx. 13 Jan.	Full control perms noticed on Administrative Assistants group for CEO Data.
18-22Jan.	Instructor account seen in Naskapi domain.
19-23Jan.	Instructor account gone from Naskapi domain.
18-22Jan.Thru Feb	Pop up Warning, Perms changed by nt5 error.
27Jan.	Administrative memo for Earnie
Approx. 25Jan.	First time that failed map attempt to \\NASKAPIBDC\earnie$ was noticed.
Approx. 25Jan.	Automachron appears on Mr. Smith's PC.
Jan.2000	CD with NTCrack is noticed missing.
3Feb.	Exchange services would not start.
3Feb. Approx. 2030	Noticed missing Exchange logs.
4Feb.	Fred profile noticed on BDC.
7Feb.	No password for firewall.

Event Report
Unique ID Number _1___

I. What:

A. Event: Administrative Assistants permissions had changed to full control for CEO Data.

B. Purpose of System: BDC. Data storage including CEO data.

C. **OS and Software:** NT4 Svr. Software was user data for group called Administrative Assistants. The specific folder had modified perms:

1. \\NaskapiBDC\data\home\executiveitems\

This folder contains sensitive information on all legal proceedings, power of attorney, etc.

D. **Vulnerability exploited:** Unk. Could be compromised/well known Administrator password.

II. Who reported:

A. POC, position: Ms. Yau. Mr. Smith Mrs. Anzio.

B. Company: Naskapi

C. Phone #: 619.504.8320

D. E-mail: yau @Naskapi.net

III. When:

A. Date noticed: 3April Approx. 0750 by Mr. Smith.

B. Date of event: Sometime between 13 and 14Jan. Smith checked Perms Monday. Perms changed overnight. Recurring event. Smith would assign less than full control and the next day full control was encountered again. Ongoing since MCSE class.

IV. Where:

A. Physical location of target system: Server Room.

B. Target IP: BDC 56.57.258.118

C. Source IP: Unk.

V. Why:

A. How discovered: Smith noticed that ADMIN was given full control during routine checks of the BDC permissions.

B. After exploit was done, what did intruder do:
Exploit is change perms to full control.
Unk what was done next.

VI. Comments: Full control rights are never given out by Smith. About 3 weeks ago, at the same time the MCSE class was ongoing and NT5.0 modified event was ongoing, Smith changed perms on these folders back to something less

than full control, modify I think. The following day, the folders had been assigned full control to Administrative Assistants. This was also the same day he saw the Fred profile on the BDC. While changing the perms, he could not see who the owner was. Smith took ownership and then assigned perms.
By the way, there was a lot of noise from the MCSE class. For example, two domains appeared in browser traffic. Approx. names were My Group and Classroom. Not necessarily significant.. Regular browser function of WinNT.
Another example is the users from the classroom domains appeared in the NASKAPI domain, One specific account was called something like instructor. The account was present after the class had been going on for about 1 ½ weeks. The account then vanished a day or 2 later.
It is unknown if there were any domain trusts established.
Permission changes flow downward to all data in subfolders.

A warning was popping up throughout this time that said approximately the following: 'Permissions have been changed by a machine running NT5 or higher.' This warning occurred since about the 2nd or 3rd week of class the first time. The warning popped up whenever a Help Desk person would log onto the domain. This warning has been ongoing and tapered off when the NT5 boxes were removed.

VII. Timeline:

11-29Jan.	MCSE class ongoing
Approx. 13 Jan..	Full control perms noticed.
04April	Fred profile noticed on BDC.
18-22Jan.	instructor account seen in NASKAPI domain.
19-23Jan.	instructor account gone from NASKAPI domain.
18-22Jan. Thru Feb	Warning, Perms changed by nt5.

VIII. Unanswered questions:

1. Verify all facts. Logs, deleted files, etc.
2. What was done in those folders once full control was gained? Did intruder read, copy, change any files?

Event Report
Unique ID Number _2___

IX. What:

E. Event: NTCrack is missing.
F. Purpose of System: NT Password crack utility.
OS and Software: Windows NT 4.0.

G. Vulnerability exploited: CD physically removed from spaces.

X. Who:

E. POC, position: MR. Yau, Help Desk tech.
F. Company: Naskapi
G. Phone #: 619.504.8320
H. E-mail: yau
@Naskapi.net

XI. When:

C. Date noticed: ~18Jan.
D. Date of event: Sometime between Feb. 1999 and Jan.2000.

XII. Where:

D. Physical location of target system: NTCrack CD stored in Help Desk office, in an unlocked desk drawer.
E. Target IP: N/A
F. Source IP: N/A

XIII. Why:

C. How discovered: Unk
D. After exploit was done, what did intruder do:
Exploit is change perms to full control.
Unk what was done next.

XIV. **Comments:** Other POC's:
Mr. McKitrick
Mrs. Manuel, former Security Manager.

Alsoft came here in February to rebuild Exchange server and provided Naskapi with two CD copies of NTCrack. The CD that the Help Desk currently has does have the domain SAM on it. SAM is dated Jan 2000. The same software is likely on the missing CD.

CD contents: NTCrack
Pwdump 1 and 2
SAM database from Feb. 1999

XV. Timeline:

Feb.1999	Alsoft gives 2 CDs to Naskapi.
Jan. 2000	One CD is noticed missing.

XVI. Unanswered questions:

3. Verify all facts. Logs, deleted files, etc.
4. Ask Ms. Manuel how he first noticed missing CD.
5. Address this event in physical security policy.

Event Report
Unique ID Number _3___

XVII. What:

H. Event: Exchange public folder with Audit logs erased. Exchange was down, therefore this is also a possible Denial of Service (DOS).

I. Purpose of System: Exchange. E-mail.
OS and Software: Windows NT 4.0. Server. Exchange.

J. Vulnerability exploited: UNK. Possible administrator password disclosure.

K.

XVIII. Who:

I. POC, position: MR. Yau, Help Desk tech.
J. Company: Naskapi
K. Phone #: 619.504.8320
L. E-mail: yau
@Naskapi.net

XIX. When:

E. Date noticed: Tues. 3Feb. after 2030.
F. Date of event: Sometime the week prior.

XX. Where:

G. Physical location of target system: Server room.
H. Target IP: 56.57.258.116
I. Source IP: UNK

XXI. Why:

E. How discovered: Mr. Yau was troubleshooting Exchange problems. He was trying to get Exchange services to start. He called a friend who is an MCSE for help .

F. After exploit was done, what did intruder do:
Normally, Exchange has a folder structure as follows:
\public folder\Event Config\
Public folder was deleted. Event Config is reported to contain Exchange logging information, showing what mailbox the user has logged into. Service activity is also logged there.

XXII. **Comments:**

XXIII. Timeline:

3Feb. Exchange services would not start.
Approx. 2030 Noticed missing logs.

XXIV. Unanswered questions:

6. Verify all facts. Logs, deleted files, etc.
7. Get MS tech net articles about Exchange logs
   Article ID
   Q187523
   Q190993
   Q270855
8. Is there any other place that could indicate the time of deletion?
9. What handle deleted it? What account is responsible for that handle?
10. When is the last good backup of Exchange and can Law Enforcement have that backup?

Event Report
Unique ID Number 4

XXV. What:

L. Event: Hidden share behavior when domain administrator logs in.
M. Purpose of System: Mr. Smith's PC.
N. **OS and Software:** Windows NT 4.0 Wksta.
O. Vulnerability exploited: UNK.
P.

XXVI. Who:

M. POC, position: Mr. Smith, Help Desk Tech
N. Company: Naskapi
O. **Phone #:** 5491-2534
P. E-mail: smith @Naskapi.net

XXVII. When:

G. Date noticed: Approx. 25Jan.
H. Date of event: Unk

XXVIII. Where:

J. Physical location of target system: Server room. BDC
K. Target IP: 56.57.258.118
L. Source IP: UNK. Maybe done on BDC, maybe done on Smith' PC which is host id .239.

XXIX. Why:

G. How discovered: Logged on to rsmith domain account. Event had a definitive start date.
H. After exploit was done, what did intruder do:
UNK. Misconfiguration on mapping in profiles. Don't know if intentional or not. May have mapped to entire Server drive.

XXX. **Comments:**

User's drive pops up when anybody logs onto BDC.
NT automatically tries to reconnect drives after a user maps it once and leaves default checked to try to connect drive again.
This event was first noticed a couple of days before Earnie received an Administrative memo.
Similar but not exact example:
When logged on as local administrator, in an account called svcAdmin, a window pops up with the following info:
Enter Network Password
Incorrect password or unknown username for \\NASKAPIBDC\earnie$

Note that this is a hidden share.
Shares are messed up on BDC.
Normally, the domain users are constructed as follows:

Folder	Contents
W:\public	all users can see data in here.
W:\private	for each individual user, blocks all others.
W:\exchange	All outlook stuff. Ntuser.dat. Personal Address Book. Mailbox.

The data that is normally in the W drive was showing up in a new drive, the D drive, for the earnie account.

Also, there is a strange application on Mr. Smith's local PC that he did not install. This application appeared around the same timeframe. Viewed from the start menu, we see the application as follows, including a screen capture:
Start – Programs – One Guy Coding – Automachron

This shortcut points to D:\private\achron.exe. Again, the D drive is not mapped right now. Achron.exe is not present on Smith's local drive.

XXXI. Timeline:

Approx. 25Jan.	First time that failed map attempt was noticed.
Approx. 25Jan.	Automachron appears on Mr. Smith' PC.

XXXII. Unanswered questions:

11. Verify all facts. Logs, deleted files, etc.
12. Is this hidden share mapping stored in the SvcAdmin domain account? Where is it stored exactly?
13. Why is \\NASKAPIBDC\earnie$ a hidden share?
14. What does \\NASKAPIBDC\earnie$ point to on the server? The entire hard drive?
15. When did Earnie get an Administrative memo?
16. Is Automachron a trojan horse, or a valid time protocol application?
17. Is achron.exe present anywhere on the servers?

APPENDIX B. SPECIFIC ANSWERS TO QUESTIONS

The following questions are listed at the end of each distinct incident in Appendix A. These are the answers to those questions.

Event 1 – CEO Data permissions were changing.

18. Verify all facts. Logs, deleted files, etc.

After intensive log review, none of these claims were validated by facts in the logs.

We tried to pursue the news that there was an account created in the NT4 domain called Instructor. This name never appeared in any of the logs.

It is quite possible that a software conflict, specifically the NT5 error, was causing permissions to be changed. The fact that the folder's owner was listed as null is supporting evidence. The system may often leave behind no trace of itself in NT. Normally, the owner is listed.

19. What was done in those folders once full control was gained? Did intruder read, copy, change any files?

It could not be shown that any one individual gained full control. We could not eliminate the possibility that there was a glitch in the system. To really get to the bottom of this, the ACL's would have to be re-invented from the ground up. Only then would we be able to pick out the snag in this rats nest. This would be labor intensive, and requires the management on site to make business decisions of who gets access to what. As the consultant, I specified that this task had to be done.

Event 2 – NTCrack is missing.

1. Verify all facts. Logs, deleted files, etc.

This was a physical security issue and the larceny would not be in the electronic logs. Use of NTCrack could leave an auditable footprint. We turned on auditing. Keep in mind that the domain SAM was also on the CD with NTCrack. We cannot audit for local cracking. Just in case the passwords were cracked, we changed every password in the domain before the LAN opened back up again. We also removed any unknown accounts, in case there was a back door account.

2. Ask Ms. Manuel how she first noticed missing CD.

She said that she noticed it a month after it was missing. She was trying to do the right things, but was overwhelmed with daily LAN Administration.

3. Address this event in physical security policy.

When I spoke with the security manager, it was pointed out that a separate documented physical security policy was needed. Little details can easily fall through the cracks that undermine the entire system.

Event 3- Exchange public folder with audit logs erased.

1. Verify all facts. Logs, deleted files, etc.

This report cannot be accurate. Exchange does not store security data within it's own logs. The only logs that the exchange application has are transaction logs. Events produced by the exchange application are stored in the application logs of Windows NT. Exchange does, however, allow you to turn on diagnostic logging, which produces more entries into the application log. What may have happened here is that diagnostic logging

was turned on by one person. Then that person returned to the exchange server and found that diagnostic logging had been turned off. Only an insider could have turned off diagnostic logging, but this alone would not cover a hacker's tracks.

Note that security information from Exchange is stored in the NT Application log. The Application Log was not turned on before we came on site and we still had no solid data to validate this reported event.

2. Get MS tech net articles about Exchange logs

Q187523
Q190993
Q270855

I have gathered all of these technotes. They basically discuss how to restart exchange services. There is nothing about audit logs in the Event Config folder. It seems like MS tech support gave us these tech notes during the data restore when the Exchange services were not restarting. We found out that the problem was with the name and password of the service account.

3. Is there any other place that could indicate the time of deletion?

Unknown.

4. What handle deleted it? What account is responsible for that handle?

Unknown.

5. When is the last good backup of Exchange and can Law Enforcement have that backup?

A backup just prior to the suspected deletion could be used to clarify what exactly was deleted. Alas, the last tape backup was from after the event. There was essentially no value in that.

Event 4 – Hidden share behavior when domain administrator logs in.

1. Verify all facts. Logs, deleted files, etc.

Several logons of this user were found, but nothing that would indicate subversive activity.

2. Is this hidden share mapping stored in the SvcAdmin domain account? Where is it stored exactly?

This hidden share was a twisted home profile. It is not clear exactly what was wrong with the profile, but it does not look malicious.

3. Why is \\NASKAPIBDC\earnie$ a hidden share?

This is the natural state of the home profile share.

4. What does \\NASKAPIBDC\earnie$ point to on the server? The entire hard drive?

This could not be verified after the server rebuild. The profile looks like it was just pointed to a home directory, nothing as malicious as exposing the entire c: drive of the domain controller.

5. When did Earnie receive an administrative memo on his work performance?

Some time before this event.

6. Is Automachron a trojan horse, or a valid time protocol application?

Automachron is freely available for download from the Internet.

7. Is achron.exe present anywhere on the servers?

The version on this LAN was not found and could not be tested for malicious code.

APPENDIX C. VULNERABILITY ANALYSIS REPORT

Report Description

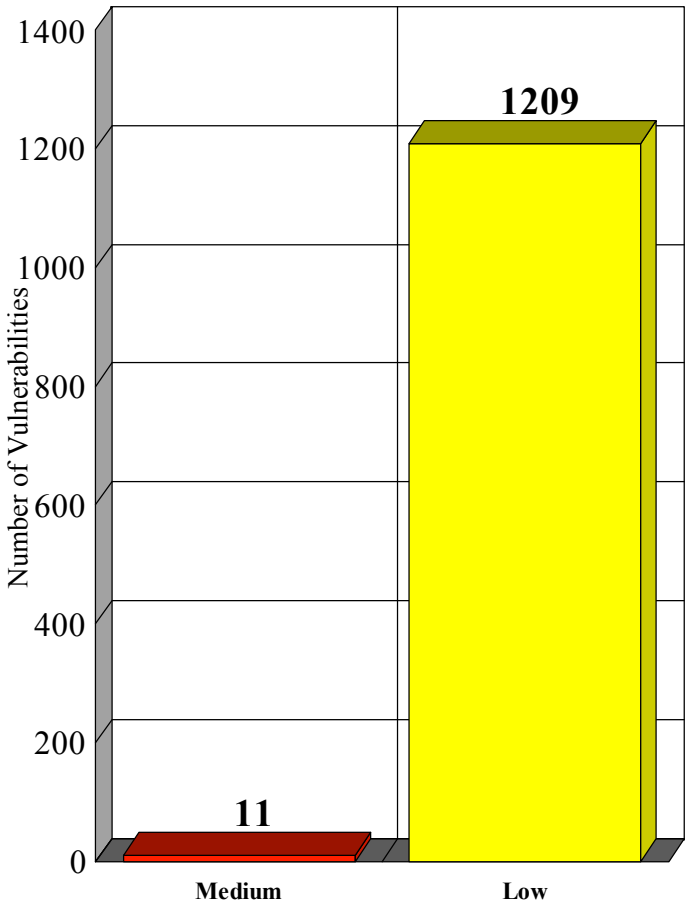
This report summarizes the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, the summary graphics describe percent of vulnerabilities by severity and number of vulnerabilities by severity. Vulnerabilities are classified as high, medium or low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploration of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

Session Name:	srvrroom.session	**Session ID:**	23
Template:	no_slam	**Termination Status:**	Finished
File Name:	srvrroom.session_00~		

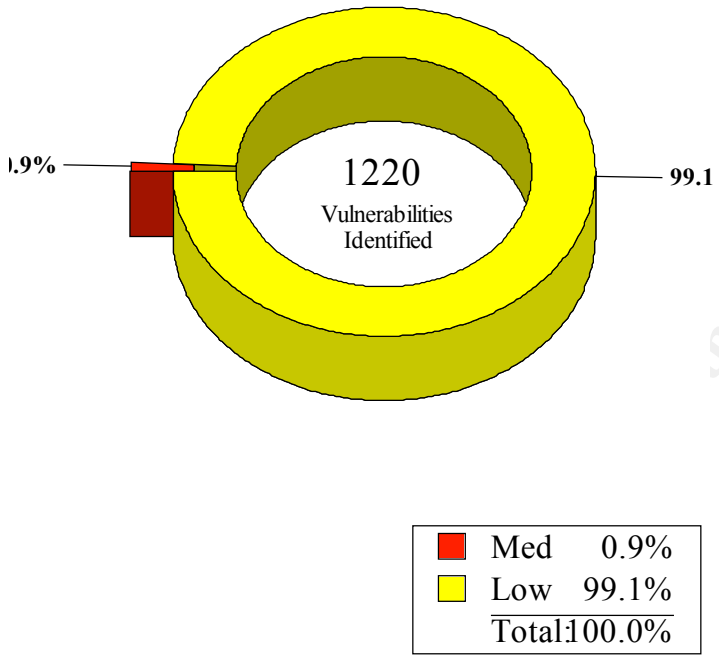
Scan Summary Information

Hosts Scanned:	4	**Scan Start:**	2000/02/09 20:59:56
Hosts Active:	3	**Scan End:**	2000/02/09 21:23:11
Hosts InActive:	1	**Elapsed:**	00:23:15

Number of Vulnerabilities by Severity



Percent of Vulnerabilities by Severity



APPENDIX D. TOC OF REPORT LEFT ON SITE

Please note that this is the TOC of the first report written. Compare this TOC here with the TOC at the start of this GIAC paper.

Table of Contents

5. Follow-up Notes
5.1. How to prevent this in the future:
5.1.1. Training specifics
5.1.1.1. Library, Training program.
5.1.1.2. Check out the Corporate pipelines.
5.1.1.3. Industry Certifications
5.1.1.3.1. Cisco Certified Designer Associate, CCDA – to address collision domain.
5.1.1.3.2. MCSE
5.1.2. Have solid well thought out policies in place.
5.2. Estimated completion time for CERT and Law Enforcement.
5.2.1. Check for backdoors. In places where blank admin existed, check local SAM for unauthorized accounts with admin rights for local machine. Check all IT shop, server room, checklist of who had blank passwords.
5.2.2. Backdoors – Are there any services that have launched Trojan horses?
5.3. Naskapi to call CERT for follow-up vulnerability scan.

APPENDIX E. FOLLOW-UP REPORTS

18 Feb 00

Peter Szczepankiewicz
Lead Incident Handler
CERT

Mr. Smith
Security Manager
Naskapi Systems Inc.

Dear Mr. Smith,

This letter is the final report for the on site visit

1. The CERT has concluded our review of all data gathered from the on site visit. There are suspicious entries in the logs that may be caused by either malicious activity or poor systems administration. Poor systems administration cannot be isolated. The conclusion is overall poor computer security practices.

2. The problems from this on site visit are systemic in nature. To effectively prevent computer security events in the future, Naskapi would benefit from education and training for the IT shop. There are formal pipelines for IT training that you can take advantage of. For example, you might want to have the following requirements in your billets:

Billet	certification	Experience	Number of personnel
IT Manager	IT Manager	5 yrs	1
Security Manager	CISSP	12 yrs	1
Vulnerability Tech	SSCP	5 yrs	1
Network Engineer	CCNP	3 yrs	1
System Admin	Network+, MCSE	1 yr	2-3

Encl (1) is a comparison of these formal schools with civilian certifications. If it is not possible to use the Corporate pipeline now, then the industry certifications could help in the short term. Continual IT training is also needed.

3. Ref (a) is a binder of organized information from the on site visit. The binder is currently with Mr. Smith. There were four distinct events under analysis, which are listed as follows:

Event 1 Permission changes.
Event 2 Ntcrack/pwdump CD with SAM from February is missing.
Event 3 Exchange public folder missing.
Event 4 Hidden share drive-mapping fails.

Each of these four events has a detailed description in the binder, in the Groundwork tab. Encl (2) contains detailed findings of evidence that may be related to each event as well as recommended specific practices to eliminate or mitigate the event.

4. Concerning event 1, the logs show that something is trying to add users into an administrator account. Error 1016 is discussed in Encl (2) and in the Exchange Application Logs. Recommend that the following items be thoroughly researched, starting from the Microsoft web site:
Error 1016
Service pack 4 related to NT5.0
security configuration manager (SCM)
access control list (ACL) editor
Windows 2000 interactions with Windows NT4.0.

5. Concerning event 2, recommend installing an Intrusion Detection System (IDS) internally because the missing CD with NTCrack could be in the wrong hands. A real time monitoring system is the best technology available today to catch internal attacks.

6. To assist you in writing your computer security policies, Encl (3) is an example Security Manager policy.

7. To assist you in implementing your security policy and procedures, ref (b) is a short 36-page guide with a checklist. This guide is a compilation of best practices on Windows NT security. I recommend you use this checklist before, during, and after rebuilding any more servers. Ref (c) is a book devoted exclusively to Windows NT auditing. I recommend that your command buy this book to assist the Security Manager in implementing an audit review program, aimed at eliminating network problems.
Summary of expenses:

Item	Cost
Pdf file. SANS Windows NT Security Best Practices Guide	$79
Book. Microsoft Windows NT 4.0 Security, Audit and Control	$40

8. I would like to invite you to call us back in a few months for a follow up Video Teleconference (VTC) to discuss any questions you might have. Perhaps we could set up another vulnerabilities scan at that time.

Sincerely,

Peter Szczepankiewicz

Enclosures:

(1) Training Matrix
(2) Analysis Notes concerning the four events
(3) Example Policy

References:

(a) CERT On Site Binder dated 10 Feb. 00.
(b) SANS Windows NT Security Best Practices Guide
http://www.sans.org/newlook/publications/ntstep.htm
(c) Microsoft Windows NT 4.0 Security, Audit and Control.
ISBN 1-57231-818-X

APPENDIX F. UNDERNEATH NT ACCOUNT CREATION

One idea to try to find some evidence of the instructor account was to look in the registry. Alas, the key that is created with a new user is also deleted automatically when that user name is deleted from User Manager. This behavior is shown in the screen captures below.

I opened up regedt32. I adjusted permissions on the SAM key and all subkeys and drilled down to SAM/SAM/Domains/Account/Users/Names. I observed only the Administrator key and Guest key. Then I opened User Manager and created a new user called George. Immediately, the George key appears in the registry. See the screen capture below.

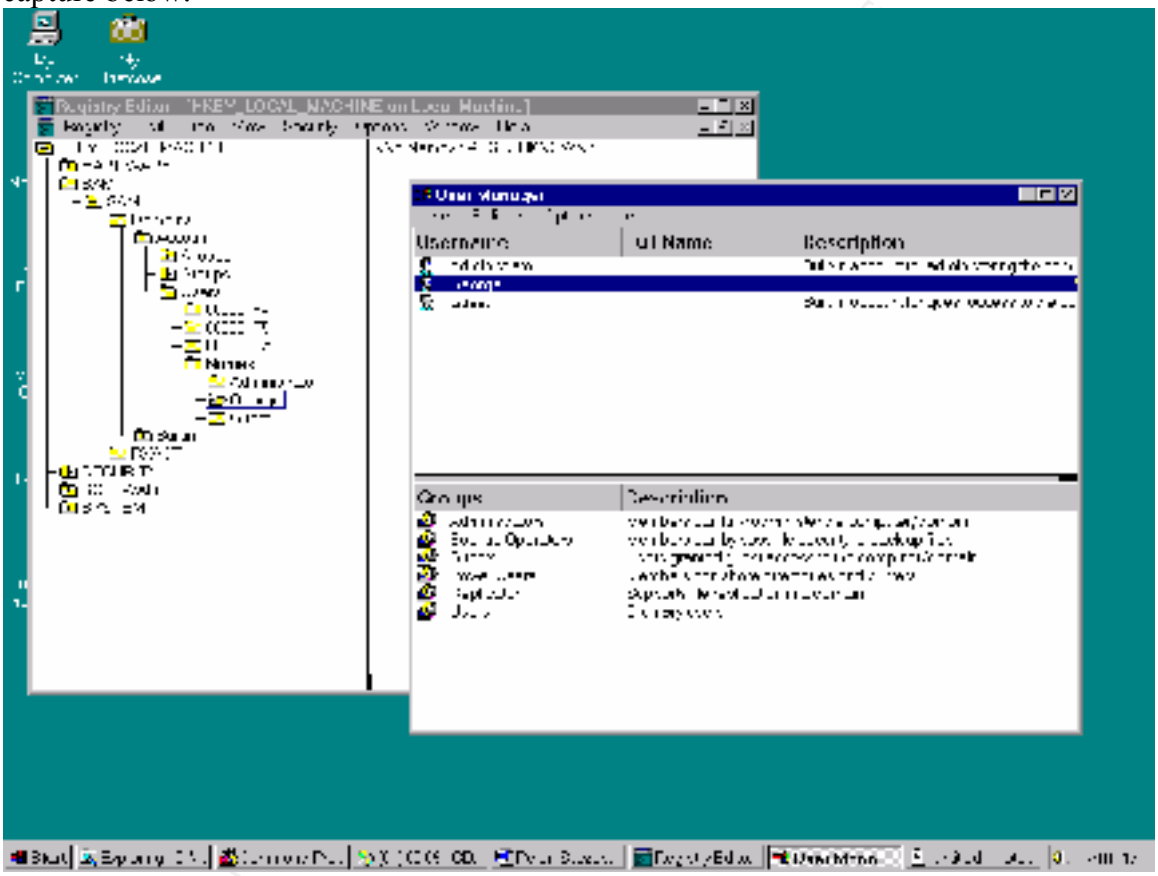


Figure 10. Before. Registry key is formed when NT user account is created in the User Manager GUI.

When I delete the George account in User Manager, his keys are automatically deleted from the registry.

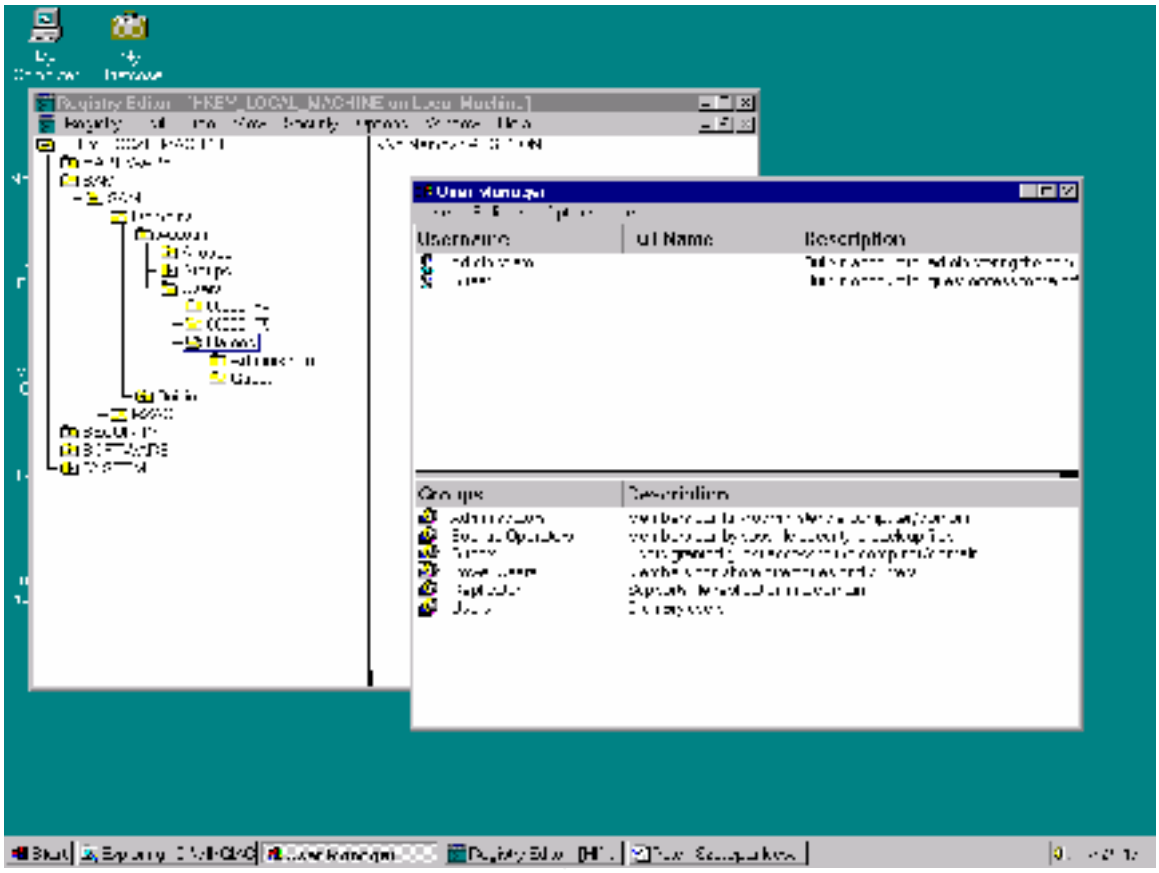


Figure 11. After. Registry keys disappear when user is deleted.

Run InCtrl. Does not check

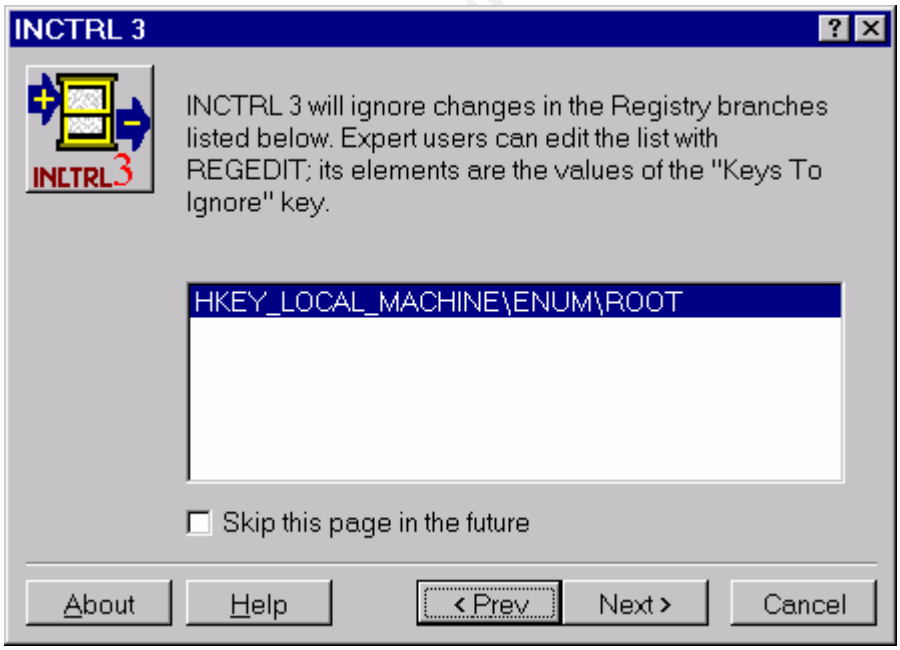


Figure 12. InControl tool does not check one registry key by default.

Are there any telltale signs of a user remaining in the registry when a user account is deleted?

1.

Snapshot.
Create Instructor account.
Snapshot.
Results?
Installation report: Create a User
(generated by INCTRL 3, version 3.01)
Thursday, February 15, 2001 08:06 PM
Windows NT, version 4.00
Notification by Disk contents comparison
Tracking:
c:\
d:\
FILES CHANGED: (6)
c:\WINNT\Profiles\Administrator\ntuser.dat.LOG
c:\WINNT\Profiles\Administrator\Recent
c:\WINNT\system32\config\SAM.LOG
c:\WINNT\system32\config\SAM
c:\WINNT\system32\config\software.LOG

NO CHANGES IN Registry
This report shown above was taken while InCtrl did not look inside the SAM key. InCtrl errors out when I allow permission to look into the SAM key.

2.
Snapshot
Delete Instructor account
Snapshot
Results?
Nothing new. Just sam files.

2.
Grant Administrator full ctrl to SAM and Security keys.
Snapshot
Make Instructor
Delete Instructor
Snapshot
Results?

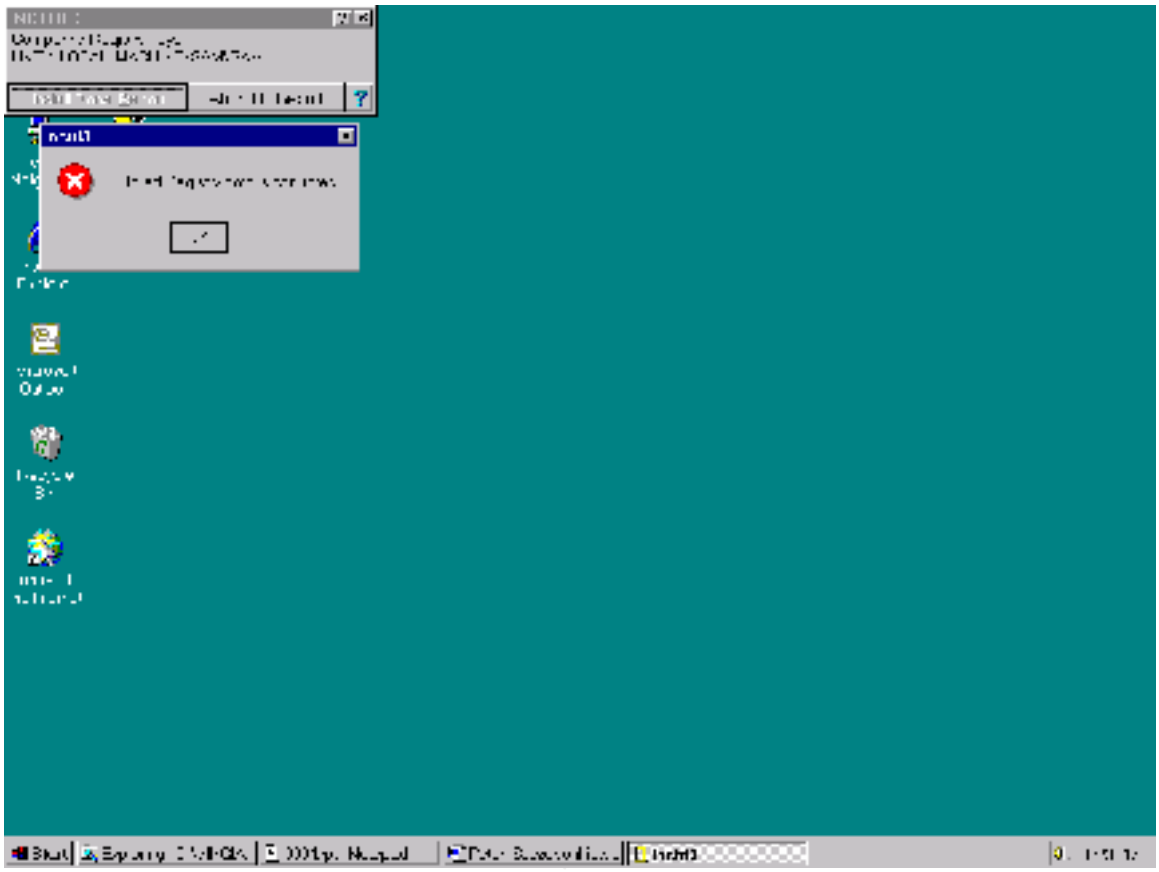


Figure 13. In control cannot check the SAM key in the registry.

Installation report: FC Access Granted into SAM and Security Keys. Create and del user.
(generated by INCTRL 3, version 3.01)
Thursday, February 15, 2001 08:22 PM
Windows NT, version 4.00
Notification by Disk contents comparison
Tracking:
c:\
d:\
FILES CHANGED: (7)
c:\TEMP
c:\WINNT\Profiles\Administrator\Application Data\Microsoft\Templates
c:\WINNT\Profiles\Administrator\ntuser.dat.LOG
c:\WINNT\system32\config\SAM.LOG
c:\WINNT\system32\config\SAM
c:\WINNT\system32\config\software.LOG

Last Updated: July 27th, 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 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
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
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
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
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
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
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