Summer 2005

Establishing Regis Network Security Policy

Michael T. Ortwein
Regis University

Regis University
School for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Establishing Regis Network Security Policy

by

Michael T. Ortwein

A Project/Practicum Report submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Information Technology

School for Professional Studies
Regis University
Denver, Colorado

June 1st, 2005

School for Professional Studies
Regis University

An Abstract of a Project/Practicum Report Submitted to Regis University School for Professional Studies in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Technology

ABSTRACT: ESTABLISHING REGIS NETWORK SECURITY POLICY

by

Michael T. Ortwein

June 1st, 2005

This project proposes to establish a security policy for the computer lab Local Area Network (LAN) at the Colorado Springs Campus (CSC) for the Network Lab Practicum (NLP) by completing a network analysis to determine requirements. Utilizing the current network configuration, a risk assessment will be performed to identify vulnerabilities and threats to the information system. Once the risk analysis is completed, a network security plan will be developed to protect system resources. The security policy will include, at a minimum, access policies, password management, firewall policy, policy on use of active code and the Internet, standards and interoperability policies, a VPN policy, and enforcement standards. The System Development Life Cycle (SDLC) approach will be used as the project methodology. Key deliverables will include a configuration management baseline, security policy and procedures, wiring diagram, firewall, anti virus protection and lessons learned. The project will culminate with a presentation to the academic board. Class utilization of the LAN will determine the success of the project. In the final phase of the project, the LAN will be turned over to the CSC NLP for administration, classroom support and future project opportunities.

Keywords: security policy, risk assessment, lessons learned, local area network, system development life cycle, password, firewall, antivirus, configuration management.

ACKNOWLEDGMENTS

I would like to extend my thanks to Mr. Bob Bowles, my Faculty Advisor, and Sonny Cordova, Colorado Springs Tier III/Team Lead. Your mentorship has been enlightening.

I owe a deep debt of gratitude to my girls Kelsey and Emily for their understanding when daddy had to “go to school.”

Karen – this is for you. I could not have done this without your love and support.

TABLE OF CONTENTS

CERTIFICATION OF AUTHORSHIP OF PROFESSIONAL PROJECT/PRACTICUM WORK ..... **II**

ADVISOR/MSC 696 FACULTY APPROVAL FORM ..... **III**

ABSTRACT: ESTABLISHING REGIS NETWORK SECURITY POLICY ..... **IV**

ACKNOWLEDGMENTS ..... **V**

TABLE OF CONTENTS ..... **VI**

EXECUTIVE SUMMARY **1**

CHAPTER 1 INTRODUCTION **2**

CHAPTER 2 REVIEW OF LITERATURE AND RESEARCH **5**

CHAPTER 3 METHODOLOGY **7**

CHAPTER 4 PROJECT HISTORY **9**

CHAPTER 5 LESSONS LEARNED AND PROJECT EVOLUTION **29**

WORKS CITED **32**

APPENDIX A **34**

DOMAIN SECURITY POLICY - DEFAULT 34

APPENDIX B **44**

DOMAIN SECURITY POLICY - IMPLEMENTED 44

APPENDIX C **50**

ANTIVIRUS SOFTWARE – AUTO UPDATE 50

APPENDIX D **54**

ANTIVIRUS SOFTWARE – AUTOSCAN 54

APPENDIX E **66**

SECURITY POLICY – RECOMMENDED GUIDELINES 66

APPENDIX F **80**

JOURNAL LOG 80

EXECUTIVE SUMMARY

Regis University's Networking Lab Practicum (NLP) offers graduate students enrolled in the MSCIT program the opportunity to complete their professional projects by working to create functional LAN segments across the various Regis campus locations. In lieu of working individual, stand-alone professional projects, the NLP affords the chance to work as a team unit combining aspects of system design and systems implementation/engineering to move the LAN segment toward fully functional status. This has the benefit of providing the student with a "hands-on" practical experience to further the more "theoretical" learning acquired in the classroom.

The NLP team I worked with at the Colorado Springs campus focused on second-generation improvements to the LAN. The previous team had done the very basic legwork required to establish a functional LAN: cabling and connections; servers and client workstations; and OS installation. Our job, then, was to move the LAN forward by implementing follow-on necessities: configuring MS Exchange; a backup and recovery system; a firewall; security policy; and configuration management policy. Despite the fact that each of us worked full-time jobs of widely varying schedules, we worked well as a cohesive team in the lab atmosphere and were able to tackle a number of basic lab enhancements as a group before moving on to focus on the specific areas mentioned above. Given my interest in computer network security, I gravitated toward the security policy development aspect of the LAN, and delved into what basic security elements would be required to bootstrap LAN security. Chapter Four is a detailed description of that implementation; while security "ABCs" are covered herein, a security manager's job is never complete, and I close with suggestions for future NLP security focus.

CHAPTER 1 INTRODUCTION

Development of the Regis University Academic Research Network (ARN) requires the implementation of a Wide Area Network (WAN) linking Local Area Networks (LANs) at the various campus locations. Previous Networking Lab Practicum (NLP) students had established a baseline configuration at the Colorado Springs campus (fig x) for further enhancement/development. NLP leadership established specific goals for the 2003 NLP group: Microsoft Exchange Server, to implement an e-mail program; continued configuration management, to track the numerous changes to LAN software and hardware setup; firewall implementation, to help protect the network; establishment of a backup and recovery program, to ensure continued LAN operation during a contingency; and establishment of a baseline security policy for the lab. Coming from the field of military intelligence and having particular interest in computer security, I gravitated toward the security policy topic. As a Tier I student, my goal for the NLP was to not merely study and understand the LAN itself, but to develop, document, and implement a sound security policy, which future NLP students could refine as required. While the LAN at Colorado Springs exists only in lab form and is not yet utilized by students, staff and/or faculty as a "live" segment of the Regis WAN, making security a relatively low priority, its eventual transition to a fully employed WAN segment will make the security aspect a critical component of its overall competency/utility/capacity? Clearly, a thoroughly-developed security policy is a critical component of any organization's networking hierarchy.

In order to proceed, I had to first understand the operating system's built-in security mechanisms, and subsequently identify the baseline security configuration. The Primary Domain Controller (PDC) for the Colorado Springs campus lab runs Microsoft

Windows 2000 for the nine client computers in the lab. Based on Windows NT technology, Win2000 supports a solid network security program via the Active Directory (AD). The first task, then, was to develop an understanding of how AD provides for domain security, and, secondly, how the AD domain profiles were currently configured. Not having seen any security-related topics developed by the previous Colorado Springs NLP students, I assumed very little, if any, work on AD security services had been accomplished.

In terms of project scope, my goal was to baseline the security program, implement a basic security policy for the current state of the LAN (per a risk assessment to identify threats and vulnerabilities), and document my work in order to provide future students the ability to enhance the security of the LAN as required. One major barrier to project completion was a thorough lack of personal knowledge regarding the system administration side of security implementation for a specific Operating System environment (in this case, Windows 2000). A second barrier proved to be the number of temporary duties involving travel I faced at work due to the concurrent stand-up of a new Combatant Command (United States Northern Command) in Colorado Springs. Finally, a significant limitation for the project was the lack of an articulated vision for the future of the LAN in terms of programs, applications, data storage parameters – simply put, LAN utilization – that made a more thorough and forward-looking risk assessment impossible. Instead of attempting to forecast such requirements, I utilized the information and LAN status available for the purposes of creating, or "bootstrapping," a security policy from the ground level. Clearly, "security" is an almost boundless topic where new threats emerge on a frequent basis. This project is an attempt to take the

current configuration of the Colorado Springs lab and develop a baseline security strategy which future NLP students will be able to enhance as required. The security policy will cover several areas: access policies; password and account management; firewall policy; policy on use of active code and the Internet; VPN policy; and enforcement standards.

Definition of terms:

AD: Active Directory. Microsoft's component for integrating directory services in a distributed computing architecture. AD allows for central management and information sharing in a Windows environment.

ARN: Regis University's Academic Research Network. A graduate student managed internetwork of campus computer information technology labs.

Domain: a collection of computers and other devices on a network that are administered as a cohesive unit using common procedures. Windows 2000 Server supports domain architecture through the use of Active Directory. The computer configured as a server and administering the domain is known as the primary domain controller (PDC).

LAN: Local Area Network. A network of computing devices spanning a relatively small physical area, such as a building or group of collocated buildings (campus).

NLP: Network Lab Practicum. A continuum of graduate-level work designed for students to enhance their CIT understanding while gaining hands-on experience through the development of the Regis University Academic Research Network (ARN).

OS: Operating System. The baseline software program running on a PC and/or server permitting the device to communicate with peripheral devices, organizing system data resources, and allowing other programs/applications to be run. For purposes of this project, the OS is Windows 2000 (unless stated otherwise).

Risk Assessment: a study of network configuration vulnerabilities and threats to the information system. By combining this with an understanding of the enterprise data to be protected, network security personnel can formulate plans to mitigate the dangers.

SDLC: Systems Development Life Cycle. SDLC is a framework for developing information systems via phases: analysis of requirements; design; implementation and testing; and administration/maintenance.

VPN: Virtual Private Network. A network established through the use of "tunneling" protocol(s) to securely link one's enterprise system with that of a mobile user or business partner via public wiring.

WAN: Wide Area Network. A network made up of multiple connected LANs spanning a geographically larger area.

In summary, NLP leadership established the requirement for development of a security policy to enhance the lab's progress toward a fully functional state. The goal was to study the LAN's current configuration and, utilizing the SDLC framework, produce a compatible security policy that could be further refined based on future additions/alterations to the LAN.

CHAPTER 2 REVIEW OF LITERATURE AND RESEARCH

There is no shortage of literature and research source material available for the Microsoft Windows 2000 operating system. Searches of bookstores and the Internet revealed dozens of titles and hundreds of hits, respectively. Texts and documents discussing Win2000 security are only slightly less plentiful. The major task proved to be culling the vast amount of information down to a useable level.

No particular scientific research method was utilized. Rather, my approach was to identify the problem (lack of an instituted security policy), gain an understanding of the present baseline network configuration, and simultaneously gather information on the network components that would impact resolution of the project (i.e., Active Directory and domain security tools). Once this was accomplished, I reviewed available literature in an attempt to assist in development of a plan to baseline a security policy for an enterprise that, for all intents and purposes, had none in place.

As previously stated, tomes of text have been written discussing networking security. Refining the material to that dealing specifically with the Windows 2000 OS was not especially difficult. Finding research material suitable to the topic at hand was simpler at the beginning of the project, while I was focused on broad security overviews, but grew more challenging once I began to delve into specific sectors of the OS or security policy (i.e., mitigating the effects of active code by utilizing Internet Explorer's security zone management tools).

Given that Windows 2000 has been fielded for years at this point, security policy surrounding the OS is well developed and security issues have been well documented. That said, there are always new developments in the field of network security; while security can never be "perfect," it can almost always be better. The sheer number of questions and answers in Microsoft's online "knowledge base" dealing with security issues is testament to the battle being waged on a daily basis between malicious insiders and hackers on the one hand, and network security personnel on the other.

This project will make no groundbreaking contribution to the field of network security. It is not intended to delve deeply into any one specific area of network security;

the intent is rather to apply acquired knowledge to the Colorado Springs lab in an effort to enhance the baseline security of that portion of the Regis University's Academic Research Network. If successful, the work incorporated herein could be applied to other segments of the Regis WAN running Windows 2000. At the very least, I will highlight areas where one of the subsequent NLP teams may wish to refine or advance security should future network configuration make it prudent to do so.

CHAPTER 3 METHODOLOGY

In order to develop a product or refine a process in a non-haphazard fashion, some form of developmental framework is a necessity. By utilizing a life cycle model, we can accomplish specific sets of tasks in an orderly and cohesive manner. Information technology projects lend themselves well to a variety of models: more "linear" processes such as the System Development Life Cycle (SDLC), or similar "waterfall" which proscribe a set of phases designed to import analytical rigor to the process; or more non-traditional design frameworks like RAD – rapid application development – or the iterative "spiral" methodology wherein the designers cycle through requirements, design, testing and application on a continual basis until the process is complete. Given the task of developing a security policy, a more linear development process was clearly the answer. The RAD framework is best suited to an organization requiring imminent application development, and lends itself to increased risk of error (especially with a less qualified (Tier I) project leader). The iterative-type of systems design/implementation (spiral) is also less applicable to a step-by-step process, with clearly defined objectives, characterized by systems security design/implementation. I therefore opted to utilize the SDLC framework. SDLC describes the life cycle as beginning with a requirement of

some kind. This is followed by a period of research and analysis intended to pinpoint the problem and develop possible theoretical solutions, which in turn leads naturally into the design phase, where a possible solution is crafted. This solution is subsequently implemented and tested for applicability and results, and is maintained post-implementation. Documentation of all aspects of the project, from inception to post-implementation, is a critical component of a thorough life cycle methodology, allowing for future systems designers to clearly understand each aspect of the process.

Development of a sound security policy is well-suited to the SDLC framework. The underlying requirement is simple enough: develop a policy to provide for a secure computing environment at the Colorado Springs ARN lab, while maintaining a balance between system protection and user connectivity and productivity. Research and analysis will support and result in a risk assessment describing how and where the network is most vulnerable, which will provide the impetus for the design of an overall baseline security policy. This policy will be implemented and subsequently tested, and following any alterations to the policy resulting from the testing, maintained (and possibly refined) by future NLP students.

Project deliverables will include this paper and its appendices describing an implemented security policy and a security policy drafted to support the Colorado Springs campus (and others as applicable) at Appendix E. The Information Systems Security Policy (ISSP) is designed to support a "prevent, detect, respond" security policy and consists of a Security Policy (borrowed heavily from a University of North Texas policy) and an Acceptable Use policy (borrowed heavily from a University of Arizona policy). These two policies make up the cornerstone of any educational institution's

overarching security policy and have been adapted to fit the Regis University information technology environment. Further adaptations may be required and the policies should certainly be vetted by the University's legal and administrative staff prior to any implementation. Chapter Four will spell out specific security-related details (accounts and auditing as well as Internet Explorer and port management) that underpin the more general security policy found at Appendix E.

CHAPTER 4 PROJECT HISTORY

Bob Bowles piqued my initial interest in the overall Networking Lab Practicum when he raised the possibility during a class at Colorado Springs in 2002. It seemed an ideal solution for an individual student in my situation, having received over two years of graduate CIT instruction but having little to no real "hands-on" time in a Lab. I had learned much of the theory, but little of the practical application for the degree program I was pursuing. Because of my particular employment situation, working with classified government systems as a user, developing a sound "real-world" project to use as my seminal project proved infeasible. I therefore jumped at the opportunity to join in a team project that would both provide an enhanced level of expertise and yet require me to stretch my knowledge – and apply that knowledge – in a specific area of the Lab.

Management of the NLP was clearly established at the outset, and my understanding of the structure was enhanced by the first few monthly business meetings held at the Lowell campus. Essentially, the Project Manager, Dan Likarish, established a set of priorities for implementation of the various phases of a Regis University WAN. Project Advisors (in our case Bob Bowles) then adapted these priorities for the specific

campus projects. For Colorado Springs, those goals were articulated as second stage requirements following the standup of the initial LAN as completed by the previous CS NLP group. Handed a working LAN, it would be our responsibility to develop basic administrative-type operational functionality as a logical "next step" in the NLP process. These particular requirements included establishment of a backup and recovery system, installation of Microsoft Exchange, implementation of a functional firewall, establishment of a sound methodology for configuration management, and development of a baseline security policy. With a Tier II/III student to provide project guidance, individuals in the group selected a specific project and commenced their research and implementation. The group concurred that weekly meetings at the Lab would prove beneficial to all members, both to work on issues affecting the group as a whole and to update each other as to individual project status. Once these issues were completed at each weekly gathering, the Tier II/III student circulated among the Tier I students to check on their progress and assist them as required.

There were few significant milestones for this project. Selection of the particular project subject and implementation of a baseline security policy are the major events that marked progression toward project completion. As a Tier I student, the vast majority of project work involved researching sound security policy guidelines and attempting to ensure that all implementation was properly documented and thoroughly completed.

The following paragraphs summarize how group policy was implemented for security at the Colorado Springs Lab and the reasoning behind the decisions at which we arrived. As previously stated, Windows 2000 employs Group Policy Objects (GPOs) to establish domain-wide configuration. In establishing the domain security policy, security

is effectively implemented down to the PC level across the domain. After researching the implications of the various issues surrounding policy implementation, I utilized domain policy settings to establish account policies for passwords, account lockouts, and Kerberos; a single policy for each is required at the domain level in Windows 2000.

Passwords are clearly critical to the authentication process in any given network. A user's password allows the system to identify and authenticate the individual, permitting him or her to access system resources and carry out authorized tasks using those resources. As such, the password represents a powerful, but dangerous, tool. In many environments, such as the Colorado Springs campus, a password is the only thing other than user name required to access the system. Weak password policy could permit unauthorized users to either guess or use widely available software tools to discover the password and thus gain access to the network. Not only must the password be somewhat complex, but it should be changed periodically to enhance its safety from compromise. The enterprise security manager must consider several facets of password security policy.

The first of these is password history. "Enforce Password History" establishes the number of unique new passwords a user must cycle through prior to reusing an old password. The significance here is that frequent reuse of passwords opens up the possibility that users will adopt the same passwords repeatedly, opening them up to increased chances of compromise. As with any policy, however, there are drawbacks to making things too difficult for the system user. Setting the password history value (ranging from 0 to 24, where lower values allow users to reuse former passwords more frequently) at too high a number would force users to have to invent new passwords more frequently, thereby increasing the risk that they would simply write down their "secret"

password so as not to forget it (Microsoft Solutions 11). For Regis, I determined that a reasonable password history should be set to a value of six: that is, a user could return to an old password after having established six new passwords in the intervening timeframe. Setting the value higher would only penalize the teaching staff and administrative personnel, while students would cycle through six passwords over a two-year period, approximately the lifetime of his or her enrollment at Regis.

The next password-associated policy, "Maximum Password Age," establishes the duration (in days) that a single password can be utilized before being required to change it. System settings range from a minimum of one to a maximum of 999 days; a zero day setting indicates the password will never expire. This setting, like password history, is a crucial aspect of protecting user's passwords: the more frequent the passwords change, the less risk that an adversary will be able to crack the password over time. Again, the drawback is that a significant decrease in the amount of time that a user can employ a password correspondingly increases the chance that users will write their passwords down so as not to forget them – a major security lapse (Microsoft Solutions 12). While most security-minded sources recommend a 30-60 day value be set, I believe that to be too restrictive in the current Regis environment and opted to implement a 120-day value. I would recommend, however, that future security managers revisit this setting; should more important data begin to be stored on lab system resources, it might be prudent to decrease this particular value. At present, however, risk management and the lack of such vital data argue for a more relaxed setting.

The "Minimum Password Age" setting identifies, in a specified number of days, how long a password must be utilized before it can be changed by the user. This function

is designed to thwart those users who would simply cycle through their required six passwords sequentially at a single sitting in order to reestablish their original or favorite password. As already pointed out above, use of a single password is a breach of sound security practice and should be avoided. Minimum Password Age can be set to values of zero (allowing immediate password reset) up to 998 days (Microsoft Solutions 12). (Note: a setting of zero would render the above "Enforce Password History" policy ineffective, as it would allow immediate reset.) After researching the impacts of setting this value, I opted to establish the Regis NLP setting for this policy at 2 days. While a low setting, this value should serve to discourage users from moving rapidly through passwords in order to return to a previously used password.

Another password-associated policy is "Minimum Password Length." This policy and the next (password complexity) are designed to enable security managers to require the enterprise's user base to employ passwords of enough strength to avoid simple attacks designed to illegally break and obtain a password. Minimum Password Length can set to values, of least characters required, between zero (where no password at all is required) to 14 characters. The larger the number of characters required, the more difficult a password will be for brute force and dictionary-based attacks to obtain. As is normally the case, however, there are negative impacts to establishing too high a value to this setting. By requiring users to employ a password of lengthy characters, the chances are increased that they will need to write the password down, in turn, as above, equating to increased risk of individuals being able to gain access to unauthorized system resources. Another possible implication is simply that lengthy passwords are more easily mistyped, leading subsequently to more account lockouts (and therefore to increased help desk

workload!) (Microsoft Solutions 13). Most security organizations recommend setting a value of eight characters for password length; again, this appeared to be perhaps slightly excessive for the current state of the LAN and I therefore established a setting of six characters. When combined with the account policy immediately following this one, a minimum length of six characters should prove adequate to protect system resources.

"Passwords Must Meet Complexity Requirements" is the next password-associated account policy to be considered. As mentioned in passing in the above paragraph, many hackers employ dictionary- and/or brute force-type attack programs to attempt to break both user and system passwords. Passwords made up of only alpha or alphanumeric characters are therefore more susceptible to these types of widely available attack methods. By avoiding obvious words and simultaneously employing special characters, users can make their passwords exponentially more difficult to obtain. In Windows 2000, this policy setting is either enabled or disabled. If enabled, passwords are required to meet the following criteria: a password cannot contain any portion of the user account name; the password must be at least six characters in length; and the password must use characters from at least three categories (upper case; lower case; the digits 0 to 9; nonalphanumeric special character - %, $, etc.). If enabled, these rules apply every time a user creates or changes a password (Microsoft Solutions 13). While enabling this policy setting may have a slight impact to the user base, especially to those who are not familiar with typing special characters as a part of their passwords, the effect is minimal, especially in light of the significantly enhanced security posture. Requiring password complexity is simply a wise addition to a sound security practice, and I therefore set this policy to "enabled."

The final password-associated policy setting involves encryption. "Store Password Using Reversible Encryption" determines whether or not user passwords will be stored in the system in a form equivalent to plaintext. If enabled, it effectively stores these passwords in a weaker format. This policy is normally only enabled when using a particular portion of the Point-to-Point Protocol (PPP) (specifically, the Challenge Handshake Authentication Protocol, or CHAP) via remote access. Unless applications require this specific protocol use, enabling this policy is not normally accomplished (Microsoft Solutions 14). Windows 2000 domain security defaults to disabled; I opted to leave this setting at its default in order to maintain improved security for password storage.

The next set of security policies to be implemented in the Windows 2000 environment at the domain level deal with account lockout. Account lockout policies assist security managers by configuring the system to track and respond to possible attempts by unauthorized individuals to acquire a password through a trial and error process. Depending upon how security managers set account policy values, Windows 2000 Server will keep track of logon attempts and lock the account in question for a specified time frame before resetting the particular account.

"Account Lockout Threshold" is the first of these domain policies. To avoid allowing unauthorized personnel an unlimited number of attempts to "guess" a user's password, or, currently more dangerously, to break one using the heretofore mentioned automated programs, Windows 2000 Server can be programmed to lock a user's account after a specified number of attempts has been reached. Values for this policy, defined in number of logons attempted, run from zero (ensuring that no accounts are ever locked out

based solely on logon attempts) to 999 attempts. As always, there are negative impacts to employing a lockout policy. Should a hacker, for example, launch a simultaneous password attack against numerous enterprise users, he could quickly exceed the identified threshold of logon attempts, essentially creating a massive denial of service for those users as their accounts are locked. An attack of this type will obviously impact any organization's help desk. On the other hand, setting the threshold for account lockout to zero would permit such a hacker to make an unlimited number of password attack attempts, which could go unnoticed by security managers until it is too late and the system is compromised (Microsoft Solutions 16). Most organizations would not set this value to zero unless they also enforce extremely complex passwords and have a solid auditing policy in place. Given the current state of the network at Regis University, establishing and enforcing such complexity is not desirable. Setting the Account Lockout Threshold to a relatively low number in order to both prevent brute force attacks against user passwords and yet allow users to make a few mistakes when typing in their passwords thus seems prudent. I implemented a value of five logon attempts before the system will lock the account.

The second account lockout policy describes the length of time that a locked account will remain unavailable to the user. "Account Lockout Duration" can be set from zero (no account lockout will occur) to 99,999 minutes. Setting the value for this domain policy too high will make the account more unavailable to potential hackers, but will likewise restrict the account's use by authorized users, and may result in more calls from frustrated users to the help desk . Setting the value very low could increase its availability to hackers, but has less impact on authorized users who have been locked out

by mistake (Microsoft Solutions 15). For the Regis environment, a 30-minute lockout should prove sufficient to both deter hacking attempts to access an account while also limiting the impact to those users who have locked their accounts by accident.

The last of the three account lockout policies, "Reset Account Lockout Counter," specifies what time must elapse after a failed attempt to log in before the counter is reset to zero. The value range for this policy setting runs between 1 to 99,999 minutes; it is important to note that, if the security manager designates an Account Lockout Threshold, the Reset Account Lockout Counter must be equivalent to or less than the Account Lockout Duration. Thus, having set the threshold at 5 attempts, the reset time would need to be set at 30 minutes or less (Microsoft Solutions 17). In fact, I established the Reset Account Lockout Counter to 30 minutes in order to afford an acceptable modicum of security against brute force attacks against Regis user passwords. For Regis, therefore, a user who makes five failed logon attempts within 30 minutes would be locked out of his or her account; the account would automatically be reset once 30 minutes had elapsed. An account administrator could, of course, reset the account manually before that time passed if necessary.

The last of the domain security policies involves the Kerberos authentication protocol. Windows 2000 Server employs Kerberos (which is based upon both a password and private key encryption) as the tool for both authentication services and as authentication for a user to access and employ system resources. In essence, Kerberos acts as a go-between for the user (logging on at a client PC) and the program managing the security for that resource (in our case, the Primary Domain Controller, PDC). Because it is not acceptable practice to transmit user names and passwords in clear text

across the network, Kerberos provides encryption for that communication (Bott 34). For most organizations, the default settings for Kerberos are sufficient; I chose to leave the default values in place. These values include a 10-hour maximum lifetime service ticket; a 10-hour maximum lifetime user ticket; a seven-day maximum lifetime for user ticket renewal; and a five-minute maximum tolerance for computer clock synchronization.

Strengthening the logon and authentication process by utilizing the previous account group policy objects is a good start, but other significant security-related items remain to be dealt with. "Prevent, detect, respond" are the watchwords for every enterprise security manager. The policy implementations described above fall into the "prevent" category; a good security team will also strive to ensure that mechanisms are in place to notice any breach, should one occur, and alert security personnel so that a timely response is possible. Fortunately, the Windows 2000 OS comes equipped with the means to audit certain system events, allowing security management to perform the required consequence management. The subsequent paragraphs detail how this auditing has been implemented at the Colorado Springs campus lab.

Windows 2000 has the ability to monitor and track a wide range of security-related events. The challenge for the security manager is deciding, based upon risk management, exactly which types of events to audit. A large organization with an array of irreplaceable data thought to be at some degree of risk is likely to employ many or even all of the operating system's auditing capabilities. Windows 2000 can audit account logon events; account management (when an account or security group is created or changed); directory service access (when a user attempts to access an AD object); object access (when a user attempts to access a file or folder set for auditing); policy changes;

privilege use (when a user exercises a set right); process tracking (program activation, indirect object access); and system events (Bott 681-682). By default, all security auditing is disabled. Clearly, indiscriminately attempting to track every instance within each of these categories is self-defeating. Not only would the sheer volume of auditing activity hinder overall system performance, it would have the effect of having a probably already understaffed security management team looking for the proverbial needle in the haystack.

Given the current state of the Colorado Springs LAN, many of these auditing categories are simply not required. I opted to implement a minimum level of auditing, enabling monitoring for failed logon attempts, successful write access to program files, and successful instances of privileged use, policy changes, account management, and system events. By tracking failed logon attempts, the log may empower security personnel to discover attempts by unauthorized personnel to access the network and system resources. Auditing successful write access to program files (i.e., those with .exe, .com, and .dll extensions) may be indicative of virus activity within the network. Finally, by monitoring successful privilege use, policy changes, account management, and system events, the security log may flag instances of misuse of administrative privileges.

The remaining audit log question lies in how to configure the specific security log to compile and maintain the above data. The OS provides for three solutions: (1) simply overwrite the older events once the log is full; (2) overwrite the log after a specified timeframe has elapsed (the default, set to seven days); or (3) not to overwrite any logged events. The first and second options are the least manpower intensive, but could result in significant data being overwritten and lost. The third option keeps all information in the

log, but requires some level of monitoring to ensure the log does not fill up (and subsequently effect system performance), at which point it must be manually cleared. This drawback can, however, be mitigated to some degree by simply limiting the overall size of the audit log itself (Windows NT Configuration Guidelines 11). Again, in applying log maintenance to the current Regis system and corresponding low risk environment, I opted to employ the first option, whereby the log simply continues to compile information until full, at which point it overwrites older data. I allowed the log name and file size to remain at their default settings (C:\\WINDOWS\System32\config\SecEvent.Evt and 512KB, respectively). Only members of the Administrators group can view (and clear) the log, by utilizing Event Viewer, a Microsoft Management Console snap-in located in *Computer Management* under *System Tools*.

As with many of the security settings outlined above, revisiting the array of auditing capabilities should be accomplished by future NLP security managers to ensure that LAN/WAN architectural and software alterations have not effected this initial approach to audit policy.

Another major security-related arena in any network associated with the Internet or even accessible media is ensuring an effective antivirus program is installed and in place. Early in the Practicum, our Tier III student emphasized the importance of ensuring the applicable antivirus software (in our case, Network Associates, Incorporated's McAfee Virus Shield) was (first) running on our clients and (second) updated with the latest antivirus files. Given its significance as a security-related item, I offered my services to ensure the program was available and current on our client base. As a group

project during a weekly meeting at the Colorado Springs campus, we walked through the steps to locate the software and program the application to automatically retrieve the latest engine and associated antivirus (DAT) files. Initially, we attempted to force the clients to point back to the Domain Controller server to find its most current antivirus files, but this effort failed when the clients did not seem to recognize the appropriate PDC files.

We then attempted to point the client-side program, via dial-up, to go directly to the NAI Internet site to retrieve updated files. This appeared to work, and we programmed the update to occur on a weekly basis (every Sunday night at midnight) when it would not interfere with ongoing student or other Lab work. In the following weeks, I checked each PC to ensure that the updates were occurring as scheduled (which in fact they did) and subsequently documented (utilizing step-by-step screen captures and accompanying text) how we programmed McAfee to acquire the updated information.

Some weeks later, I realized that we had failed to take the next step in ensuring a successful antivirus application, because we had not set up the McAfee program to scan the clients' hard drives for virus-associated data. Having become more familiar with the NAI software, I was able to step through the process required to establish an automatic weekly hard drive scan as well as put in place an autoscan of introduced media (floppy disks or CD-ROMs) and incoming e-mail and attachments. Again, I documented the steps to accomplish this with screen captures of the appropriate windows accompanied by textual instructions.

Another area directly influencing the security status of any Internet-connected LAN is how securely the installed browser is configured. A browser is, simply put, a tool

to display HTML-formatted information. All too frequently, however, malicious code is resident on HTML web pages. This presents the standard quandary for systems security personnel, pitting the functionality of Internet display and content against increasing risk. Internet Explorer (IE) is no exception to this rule, and risk management is a key concept in deciding just how to implement the security options resident in the program. Microsoft has included built-in security levels with IE that permit security managers to adopt, on a sliding scale, a level of acceptable risk. By employing this functionality at the domain level, and then ensuring that users are unable to alter those settings, security personnel can mitigate much of the risk inherent in accessing and viewing web pages. Nevertheless, securing IE is an imperfect science at best, and opting for drastic security levels will almost certainly create significant consternation among the user community.

Active content includes ActiveX controls and plug-ins, Java applets, and scripts. While each of these is designed to improve the overall web application environment in terms of activity automation and ease of use, they may also contain either unintentional defects (that in some cases can lead to exploitation) or intentionally malicious code designed to allow unauthorized actions to occur on our system. Security managers must therefore review how their network's browser will access information on the Internet and how it can provide some mitigation for these dangers. Internet Explorer deals with security concerns by establishing five different security zones and allows security managers and users to subsequently adopt a level of trust (essentially, acceptable risk) for each of those zones. The zones are defined as Internet, Local Intranet, Trusted Sites, Restricted Sites, and My Computer. (The My Computer zone, consisting of only those programs installed by the OS itself, is configured only through the IE Administration Kit,

and will not be covered further here.) A sliding scale from low, medium-low, medium, high, and custom is available for each zone; these settings correspond to whether or not IE will enable, disable, or prompt the user for response whenever it comes across potentially dangerous material in that specific zone (Bott 267-269).

The Local Intranet zone consists of those connections identified through a Universal Naming Convention path along with sites designed to bypass the LAN's proxy server (assuming they are not listed in either the Trusted Sits or Restricted Sites zones). These are sites lying behind the network firewall, topographically speaking. IE security for this zone defaults to medium-low, which generally enables running and downloading most active content (How to Use Security Zones in Internet Explorer 1). This makes sense, for the Intranet zone should reflect sites that are implicitly trusted more than those lying outside the enterprise's intranet. For the Colorado Springs LAN, I kept the default value in place.

The Trusted Sites zone can be considered even safer than the Local Intranet zone. Trusted Sites are those web sites, outside the firewall, in which the organization has established a high level of trust based upon mutual business dealings resulting in a high degree of confidence, or those Web sites on the organization's intranet itself. IE defaults to a low setting, enabling almost all active content except for unsigned ActiveX downloads (which prompts the user for a response) (Bott 267-269). Again, this setting is presently satisfactory and I made no adjustments.

The Restricted Sites zone lists those Web sites that the enterprise does not trust to be safe. By adding a site to this zone, the organization has decided that material on the site is likely to be harmful to the network. For obvious reasons, IE defaults to a security

setting of high for this zone, disabling the downloading or running of almost all files containing active content, to include even Java permissions run on the virtual machine (How to Use Security Zones in Internet Explorer 1; Bott 267-269). This setting also appears to be the prudent option for this category of potentially damaging content.

The Internet zone can be considered a default zone, as it contains whatever web sites are not included among the other zones. By definition, then, this setting will probably impact the user on a prevalent basis, as the vast majority of sites will fall within this category. IE defaults to a medium setting, disabling the downloading and running of unsigned ActiveX controls, prompting the user for potentially unsafe displays, downloads and program execution while still enabling safe browsing using some ActiveX and Java applets (How to Use Security Zones in Internet Explorer 1; Bott 267-269). The medium setting is currently acceptable and was left in place, but may require further study by future security managers as the LAN becomes more widely used.

In order to prevent local users from making changes to the implemented security policy settings above at the client level, I opted to change the Group Policy Object for IE at the domain level. By enabling *Disable the security page*, I ensured that users would not see IE's security tab on their local machine.

Tightening security on a network connected to the Internet invariably must also include a plan to disable any unnecessary protocols and services. Leaving any unneeded ports open is tantamount to leaving the windows in a house open when the occupant knows there are burglars prowling in the neighborhood. The following ports represent those with the potential for a hacker to gain possibly harmful data such as usernames,

computer names, and services used by those computers (Windows NT Configuration Guidelines 3-4).

Function	Static ports
Browsing	UDP:137,138
DHCP Lease	UDP:67,68
DHCP Manager	TCP:135
Directory Replication	UDP:138 TCP:139
DNS Administration	TCP:135
DNS Resolution	UDP:53
Event Viewer	TCP:139
File Sharing	TCP:139
Logon Sequence	UDP:137,138 TCP:139
NetLogon	UDP:138
Pass Through Validation	UDP:137,138 TCP:139
Performance Monitor	TCP:139
PPTP	TCP:1723 IP Protocol:47 (GRE)
Printing	UDP:137,138 TCP:139
Registry Editor	TCP:139
Server Manager	TCP:139
Trusts	UDP:137,138 TCP:139
User Manager	TCP:139
WinNT Diagnostics	TCP:139
WinNT Secure Channel	UDP:137,138 TCP:139
WINS Replication	TCP:42
WINS Manager	TCP:135
WINS Registration	TCP:137

Obviously, blocking external connections to, specifically, TCP and UDP ports 135, 137, 139 and UDP port 138 could prevent the hacker from acquiring potentially devastating information.

There are several methods available to security managers for restricting access to ports. These include using TCP/IP filtering, a limited option that applies to incoming packets only (and not by IP address); using a software firewall (inherently weak, as a virus making its way to the computer itself could disable the firewall); using a hardware firewall; or utilizing IPSec filtering (much like TCP/IP filtering, but with the additional security of encryption and authentication). IPSec filtering uses a model to note specific IP data, which is subsequently either blocked, allowed, or allowed after encrypting and/or

authenticating it. IPSec filtering is a relatively sophisticated means of filtering access to ports, requiring development of an IPSec policy with filter rules and lists, enabling the policy, and then monitoring it and modifying it as needed (Bott 570-572). For these reasons, the current Colorado Springs NLP policy will be to manage port access via the hardware firewall (Smoothwall). For the immediate future, all ports will be blocked with the exception of those needed by the NLP to support FTP, HTTP, HTTPS, and possibly SMTP. Other ports will be opened as justified to support additional protocols and IP services when needed.

Services are another potential security nightmare. Services are those programs, not requested by the user, that run in the background and work on requests from other active programs or the network. Services are configured through the Services console. Windows offers numerous services; while many effect overall system performance, I will elaborate only upon those services most critical from a systems security standpoint. *Cryptographic Services* provide digital signature verification for signed files (device drivers and ActiveX controls, for example); this service should be left at the default setting of Automatic. *Event Log* keeps the system's Event Log operational and should never be disabled as the Log can be a critical tool for monitoring system security. *FTP Publishing* is a part of Internet Information Services and represents a security risk. Disabling this service prevents any FTP server from starting in IIS (generating an error message about the service). *Remote Registry* can permit remote workstations to alter the local Windows registry, and should therefore be disabled. Remote management work can be valuable, but the potential vulnerability for remote abuse is significant. *Simple Mail Transfer Protocol (SMTP)* is another IIS service (for e-mail transport) representing a

system vulnerability and ought to be disabled in the Services Console. (In addition to being a security risk, SMTP can be hijacked by spammers when misconfigured.) Finally, *Telnet* represents another command-line access threat to the system and should be disabled.

Like services and ports, disabling unnecessary accounts is a critical step in enhancing any organization's security stance. Every account represents a potential attack point for an attacker. In addition to performing simple account management to ensure that accounts of former students, faculty and staff are deleted when no longer required, Windows 2000 security managers must be concerned with two specific accounts: Administrator and Guest. Both accounts are inherent to Windows 2000 and both represent a danger simply due to the fact that hackers know that those specific accounts exist. The good news is that there are simple ways to make these accounts less susceptible to attack. The Guest account is a non-password required, limited access account designed to allow the occasional organizational guest or visitor to check e-mail or use a word processor, for example (Bott 85-86). The best option available for the Guest account is simple: disable it. This is the default account status, and I left it disabled.

The Administrator account is the more dangerous of the two, since administrators have root privileges and hence a significant level of control over domain resources. Microsoft (and other security proponents) therefore encourages security managers to take the following actions: first, rename the account to a "non-obvious" name (not, for example, "root" or "admin"); second, assign the account a very strong password (and change it frequently); third, establish a decoy Administrator account (without privileges)

and check the event log to see if there have been attempts to access the account; fourth, enable lockout of the actual account using the passprop utility; finally, disable the client PCs' Administrator accounts. By completing these actions, the security manager can not only decrease the Administrator account's potential risk, but also increase the ability to take note of possible hacking attempts and take further action to defeat these efforts (Bott 83-85). Given the minimal risk to "crown jewel" type data presently located on the Colorado Springs LAN, I opted to take only the first step above and rename the Administrator account in an effort to shield it from prying eyes. Future security personnel may wish to establish the decoy account, or "honey pot," in an effort to provide advanced warning of possibly impending network reconnaissance and attack.

Finally, one frequently overlooked security aspect is that of physical security. Preoccupation with script kiddies and the myriad of technical issues often obfuscates the simple need to physically secure the network's most precious resources. This very basic threat requires absolutely no technical aptitude but can be as or more devastating than any Internet-borne code. An open door to the server room can invite a malicious or disgruntled individual to physically damage the organization's servers, carry one off, or allow him the access required to install network surveillance software, a Trojan horse program like Back Orifice, or one of any number of malicious programs. In this case, all of the above technically-related solutions to lock down the system will have been for naught. The Colorado Springs server closet is relatively secure: it remains locked when not in use and has no other means of physical access. Keys are kept at the front desk and are only given out to personnel on the specified access roster provided to the staff by the NLP advisor. A security guard makes the occasional rounds of the building, to include

the classroom area where the server closet is located. Weaknesses include a relatively flimsy door with a single lock and the fact that the closet is located at a distance from the front desk where the guard spends most of his shift. The closet is also located at the outer perimeter of the building, not an optimal location for the critical network resources in the event of more drastic natural disasters or very determined attackers, but suitable for the school's present LAN equipment.

CHAPTER 5 LESSONS LEARNED AND PROJECT EVOLUTION

The experience gained from working this project has proven invaluable. While a student with more experience in the system administration realm might have accomplished this particular project in much less time, it has proven extremely beneficial for me to gain a thorough understanding of the major issues involved in securing a network. The "hands-on" training, including everything from cable management to domain security policy application, has been a significant boost to my confidence level when dealing with IT issues.

In hindsight, there are some things that I might have approached differently. For instance, I would have purchased the enormous tome (Bott) I utilized on securing the Windows 2000 environment earlier in the process and read it thoroughly prior to conducting the Internet searches I ran for basic security-related documentation. The book's well-organized information on a wealth of security issues would certainly have helped baseline my knowledge level and refine the searches I eventually used. In actuality, by the time I found and purchased the book, I used it more as a reference guide in support of the material I had gleaned from the Internet.

The project met most of my initial expectations. I desired to supplement the classroom-based "theory" provided by the Regis MSCIT with the hands-on "practice" afforded by the NLP. While I had additionally hoped to spend more of my NLP allotted time working even more technical issues (i.e., the firewall implementation or the MS Exchange load), a three-month business trip kept me from being able to spend the required time working with a major second area of the Colorado Springs LAN.

There is most definitely room for evolution of this particular project as the NLP process moves forward. As I have repeatedly stated, the policy delineated above in this paper is a "mile long but an inch thick;" that is to say, it covers a very wide range of security topics but probably not to the kind of depth required for a fully functional, on-line internetwork. My recommendation would be for a future NLP student to take this security policy to the next level, especially as new applications and programs are added to the ARN that might require policy refinement or students find that some aspect of the security policy is too restrictive and inhibits productivity to an unacceptable level.

Specific areas of future concern may well have to do with some of the following issues. As the LAN goes "live," Microsoft IIS implementation and its corresponding security baggage will represent a major concern. IIS, while offering potent services, is also notoriously full of potential security holes and must be very carefully administered. IIS is notorious for allowing semi-savvy hackers access to network resources. Just as important will be eliminating any security seams between the LAN and the firewall. Continual review of what services are really required by instructors, students and administrators will be a challenge to the firewall administrator. Clear communication between the network administrator(s) and security administrator(s) will prove critical and

will doubtless effect port management. As mentioned in the previous chapter, I also believe that future security managers ought to review Internet Explorer security zone settings, review which events are audited and logged, and perhaps establish "honey pot" simulated Administrator or other accounts to draw in possible hackers as well as warn security personnel of potential attacks. As discussed above, I recommend that one student in the following NLP groups register for Microsoft's automatic e-mail distribution list in order to receive notification of updated security patches. Unfortunately, viruses, like bad news, travel fast in today's computing environment, making rapid deployment of security-related patches critical to system reliability. Finally, to enhance the "detect" portion of the information systems security mantra "prevent, detect, respond," implementation of some form of network intrusion detection system would be a prudent next step. Given the resource-limited environment in which we are working, a public domain (free!) IDS along the lines of Shadow or Snort would be suitable applications to employ on the LAN.

At a more strategic level, I would recommend that Regis University faculty leadership strive to overcome the current extremely limited budget and resource backing for the NLP program. It will be even more important for future NLP students implementing advanced LAN/WAN applications and programs to be able to rely on the latest technology – and most current hardware to run it – to move the network forward. Regis University should be a recognized leader in this field; a specific recommendation would be to dedicate an NLP student to the work of seeking out business partnerships up and down Colorado's technology corridor that would fund and sustain modernization efforts for the NLP program. It is unpleasant to be loading an application critical to the

success of one's NLP work, and simultaneously be wondering whether or not the system's limited disk space or memory will be able to handle the load or successfully run the program once installed. NLP students ought to find themselves working "hands-on" with the technology they are likely to find as they begin to utilize their Regis degree in the workplace.

WORKS CITED

"Acceptable Use of Computers and Networks at the University of Arizona." University of Arizona Center for Computing and Information Technology. <http://www.arizona.edu/~compute/accounts/policyua.htm>

"Active Directory Overview." Microsoft Windows 2000. 30 June 1999. <http://microsoft.com/windows2000/server/evaluation/features/dirlist.asp>

Blarcharski, Dan. "Emerging Technology: Create Order with a Strong Security Policy." Network Magazine. 10 July 2000. <http://www.networkmagazine.com/article/NMG20000710S0015>

Bott, Ed, and Carl Siechert. Microsoft Windows Security for Windows XP and Windows 2000. Redmond: Microsoft Press, 2003.

Gibaldi, Joseph. MLA Handbook for Writers of Research Papers. New York: The Modern Language Association of America, 2003.

Gryparis, Mark. “How to Bootstrap Information Security in your Organization.” SANS Info Sec Reading Room. 30 May 2001. <http://www.sans.org/rr/bootstrap.php>

“How to Use Security Zones in Internet Explorer.” Microsoft Knowledge Base Article – 174360. 12 May 2003. <http://support.microsoft.com/default.asp>

“Internet Explorer Safety.” James Madison University. <http:www.jmu.edu/computing/info-security/engineering/issues/ie.shtml>

“Microsoft Baseline Security Analyzer V1.1.1.” Microsoft TechNet. White Paper. June 2003. <http://www.microsoft.com/technet/security/tools/tools/mbsawp.asp>

“Microsoft Solution for Securing Windows 2000 Server. Chapter 5 – Securing the Domain Infrastructure.” Microsoft TechNet. 2003. <http://www.microsoft.com/ technet/security/prodtech/windows/secwin2k/ 05secdom.asp>

Smith, Randy Franklin. “Internet Explorer Security Options, Part 6.” Windows & .NET Magazine. 7 June 2001. <http://www.winnetmag.com/Article/ArticleID/21282/ 21282.html>

“UNT Information Resources Security Policy.” Policy Manual – University of North Texas. October 2002. >http://www.unt.edu/planning/UNT_Policy/ volume2/3_6.html>

“Windows 2000 Security Services Features.” Microsoft Windows 2000. 19 April 1999. <http://microsoft.com/windows2000/server/evaluation/features/security.asp>

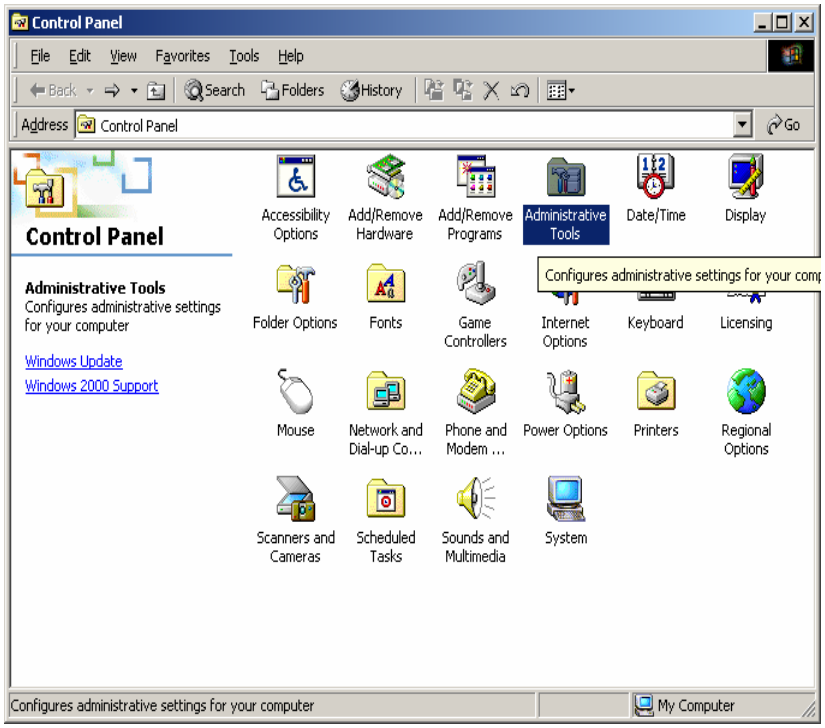
“Windows 2000 Server Baseline Security Checklist.” Microsoft TechNet. 2001. <http://microsoft.com/technet/security/tools/chklist/w2ksvrcl.asp>

“Windows NT Configuration Guidelines.” CERT Coordination Center. 2000. <http://www.cert.org/tech_tips/win_configuration_guidelines.html>

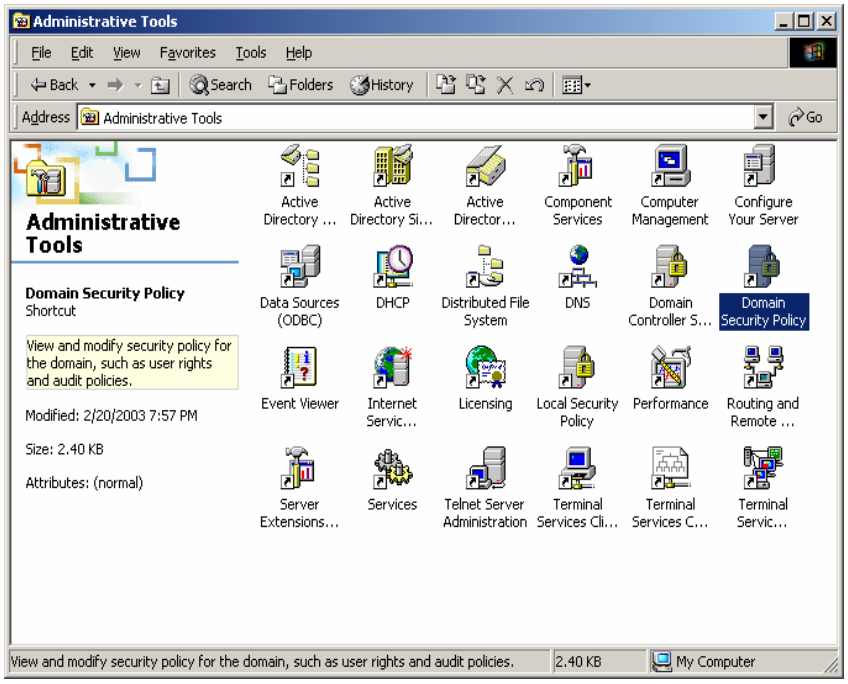
APPENDIX A

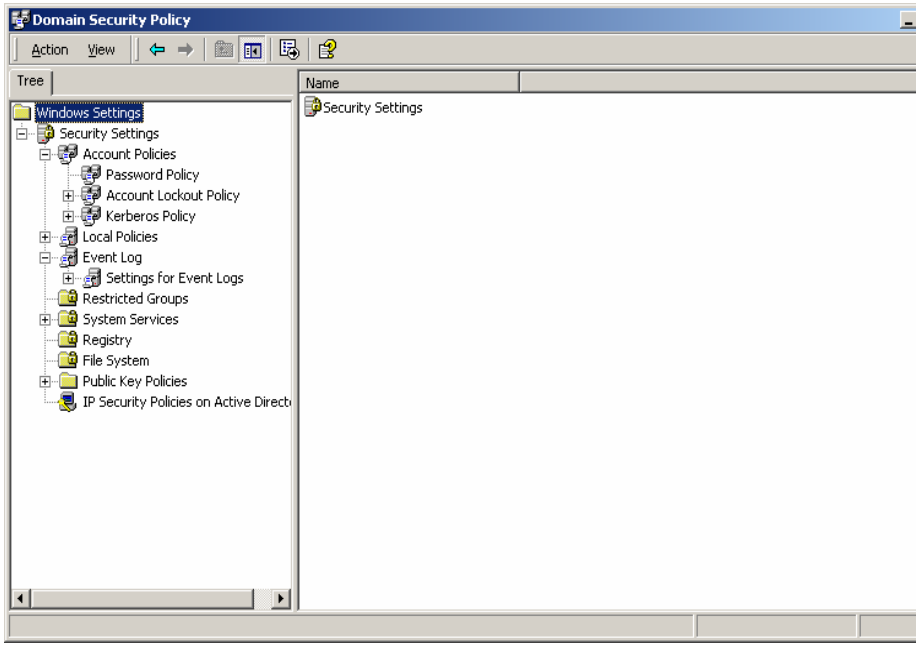
DOMAIN SECURITY POLICY - DEFAULT

START, settings, control panel, administrative tools

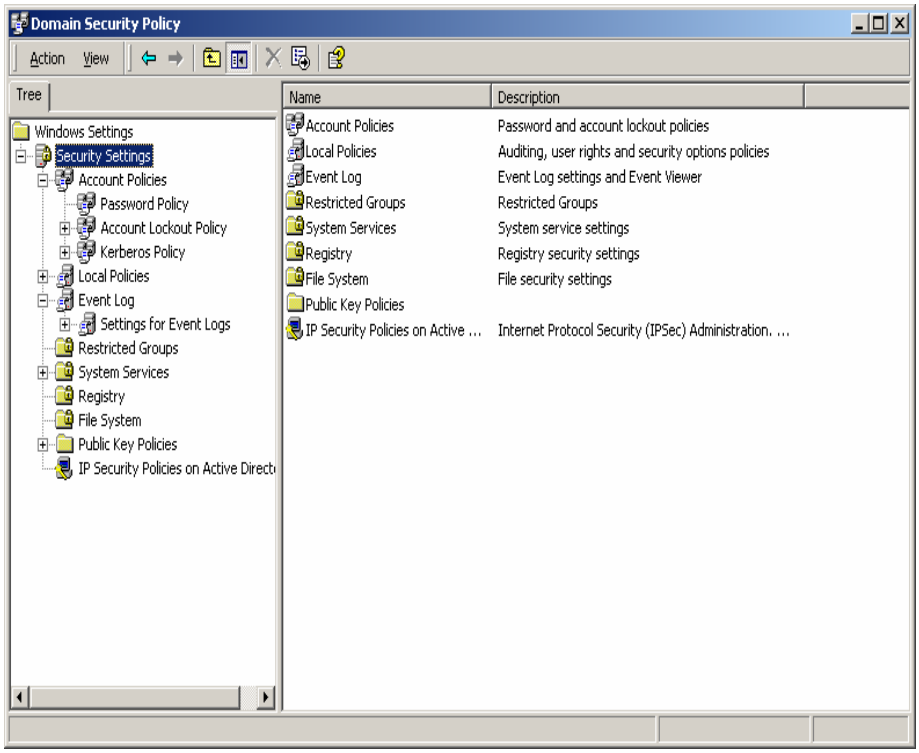


Domain Security policy

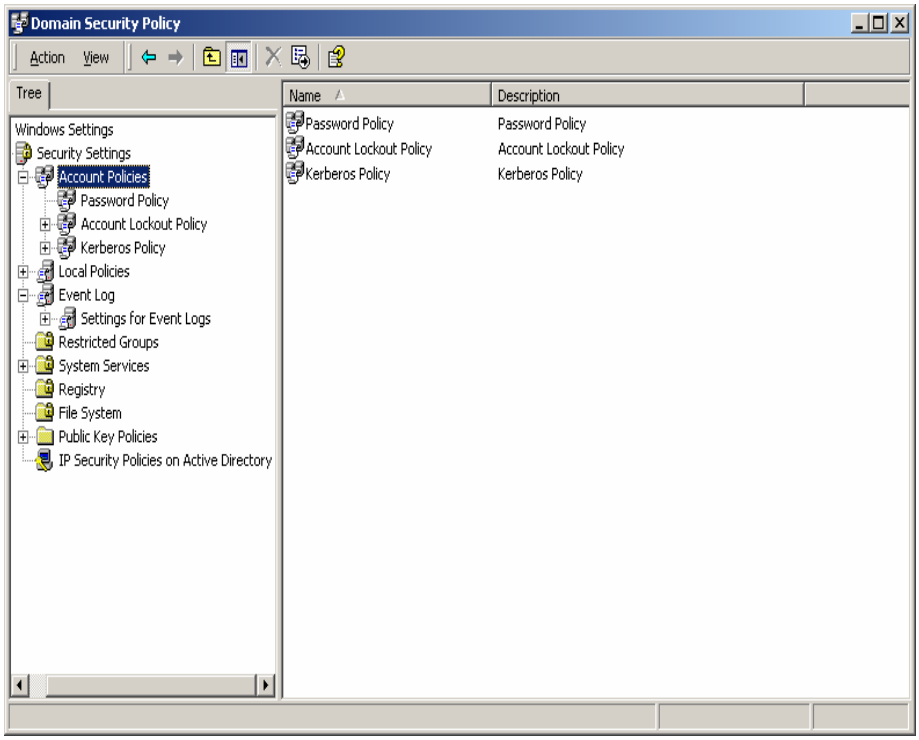




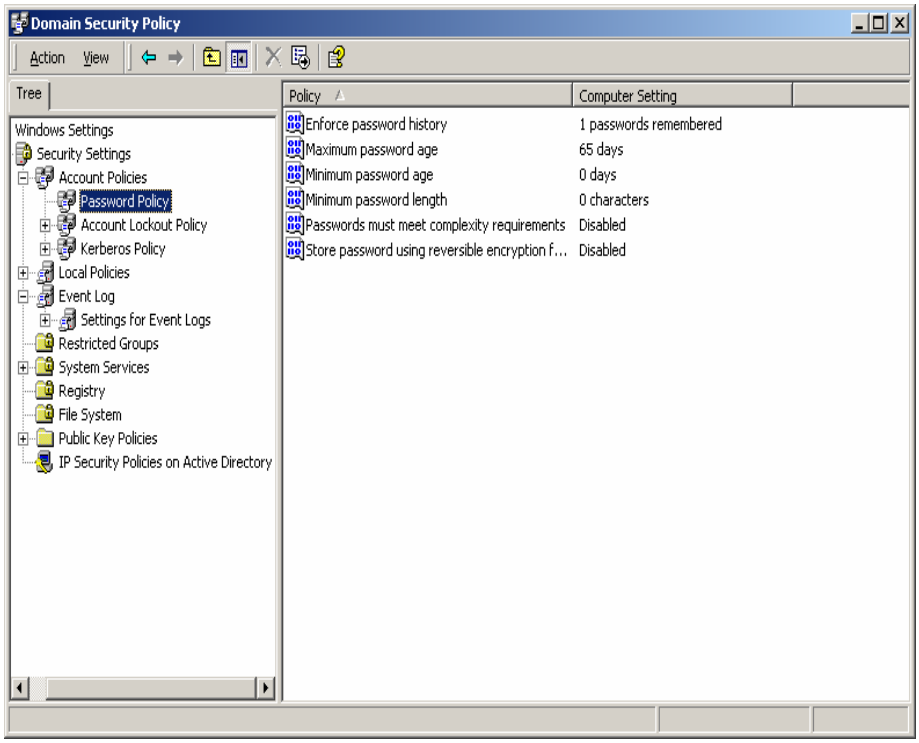
Domain Security Policy - Menu



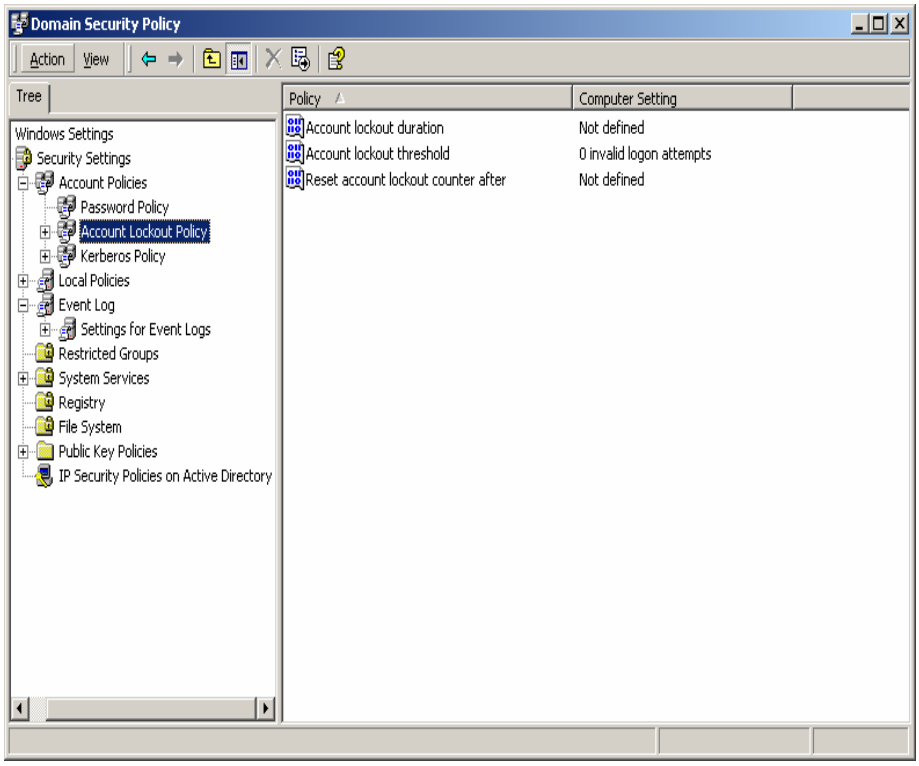
Security Settings Menu



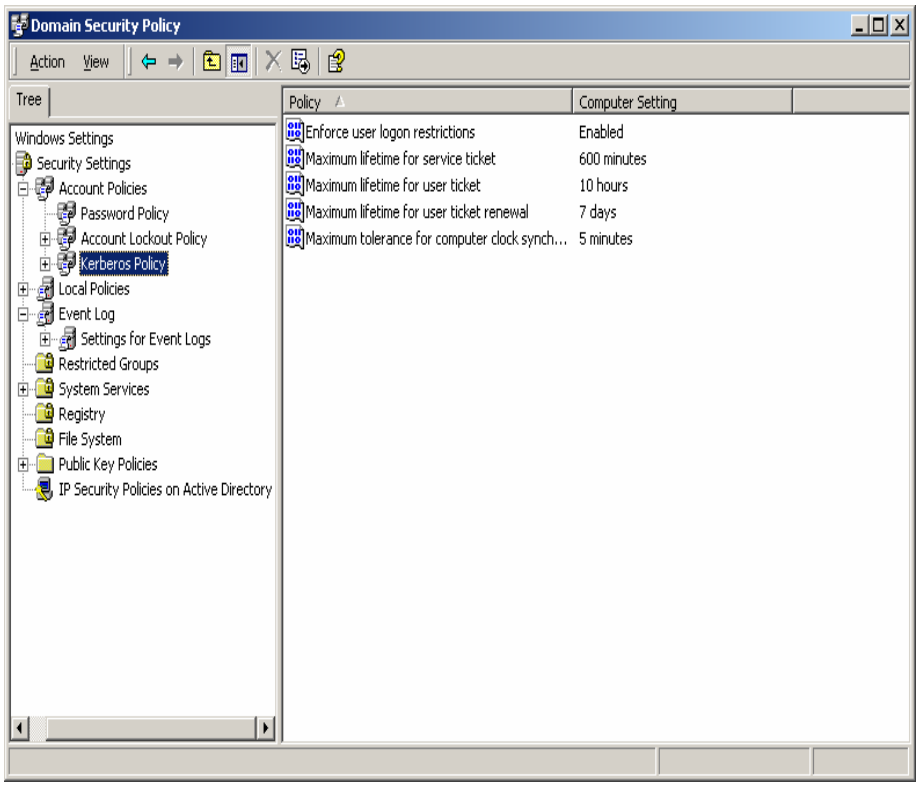
Account Policies: Password, Lockout, Kerberos



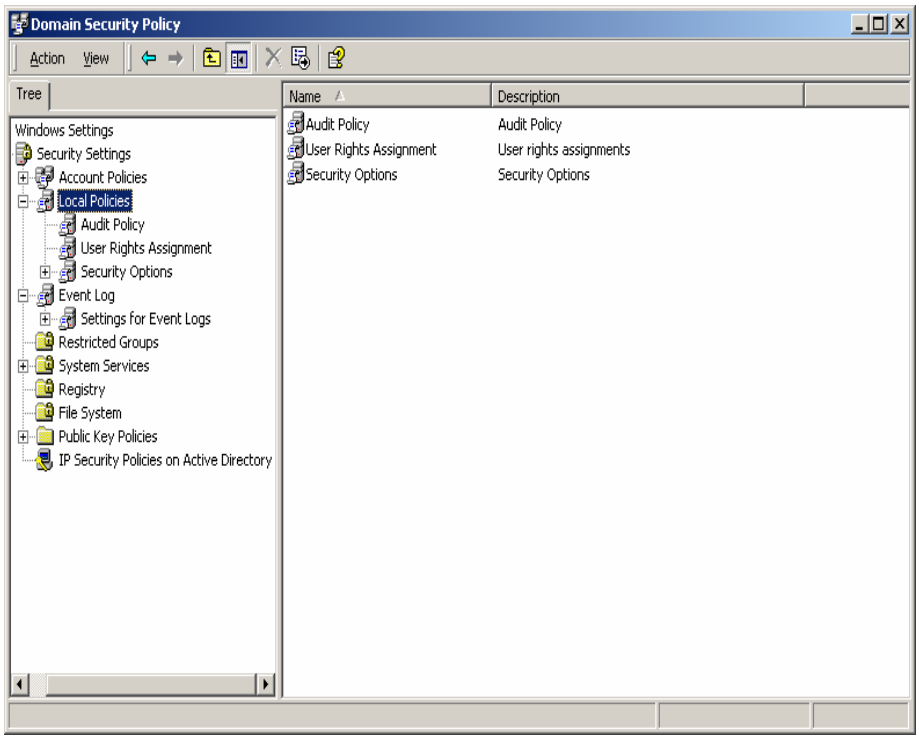
Password Policies: enforce history, maximum age, minimum age, minimum length, complexity requirements, store using reversible encryption



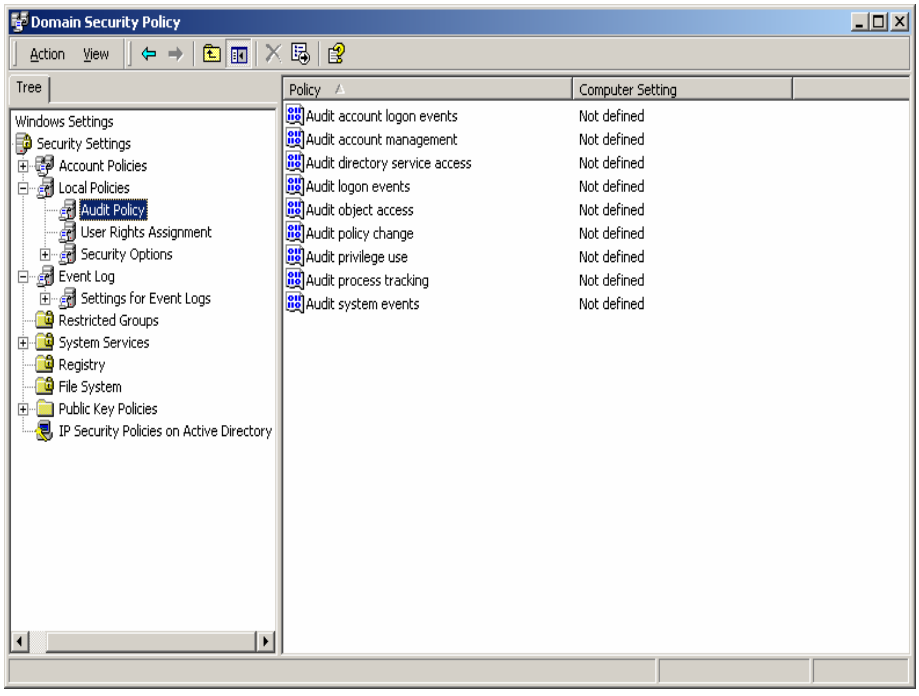
Account Lockout Policy: lockout duration, threshold, reset counter



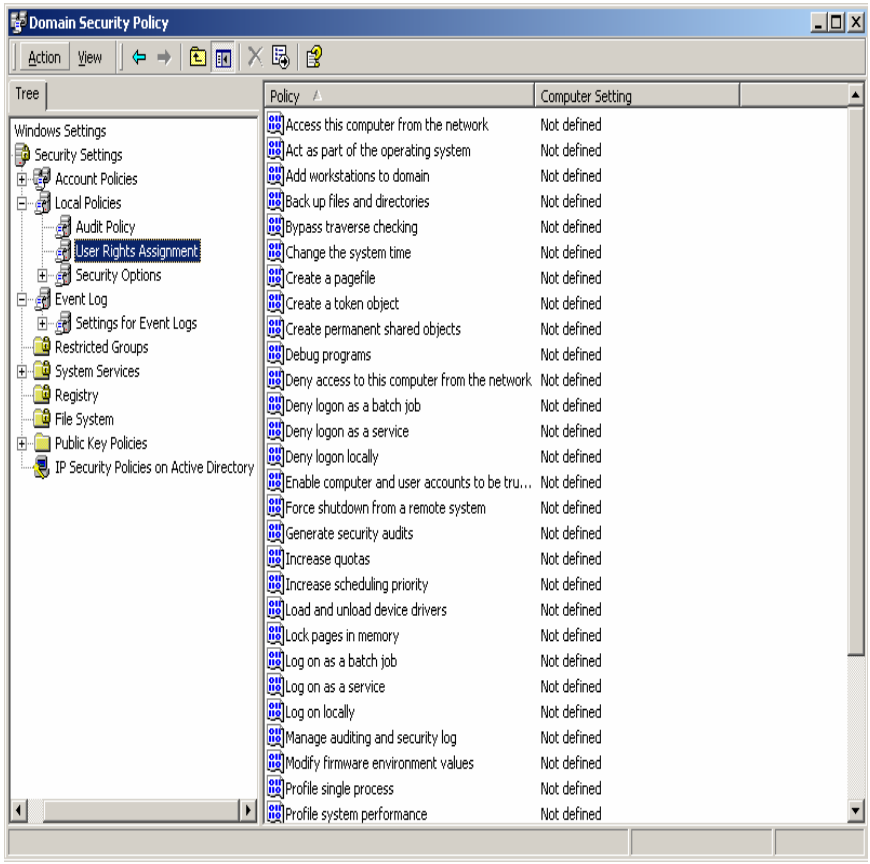
Kerberos policy: enforce logon restrictions, max lifetime for service ticket, max lifetime for user ticket, max lifetime for user ticket renewed, max tolerance for computer clock synch

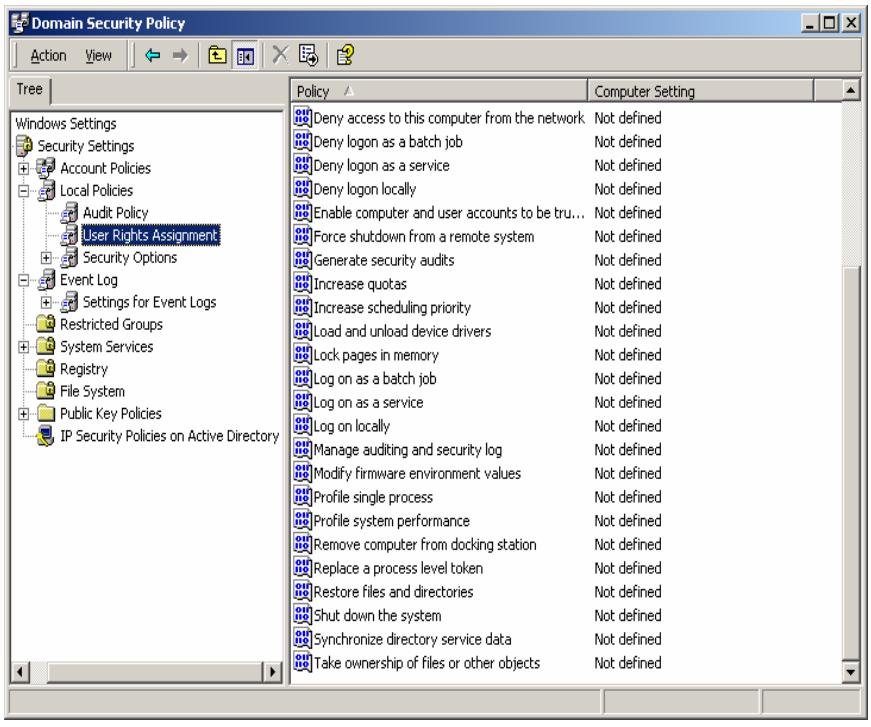


Local Policies: audit, user rights, security options

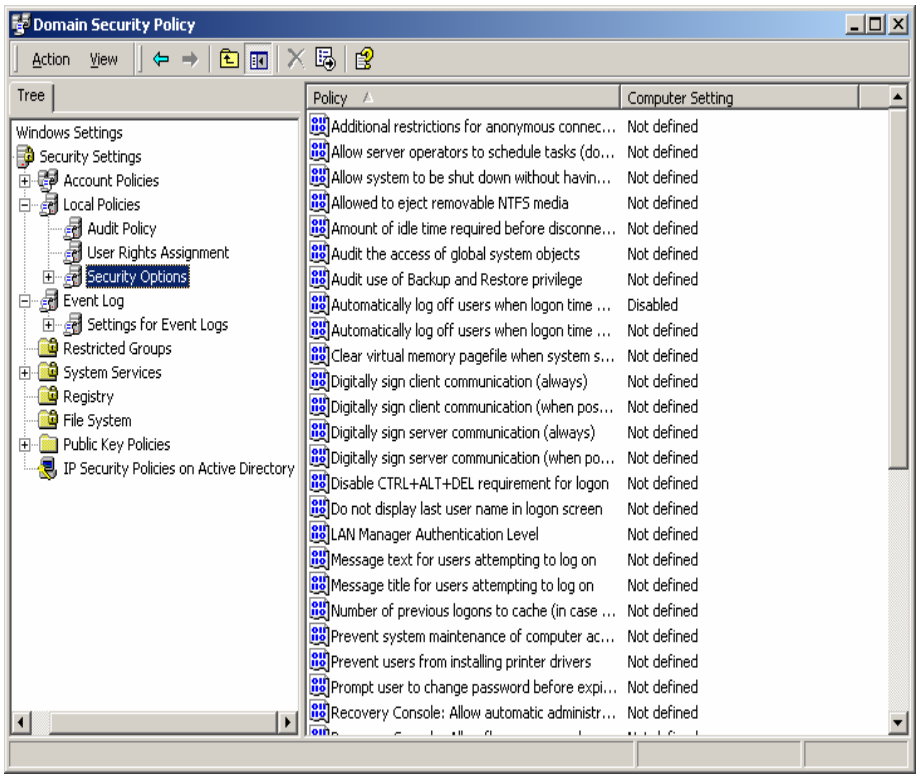


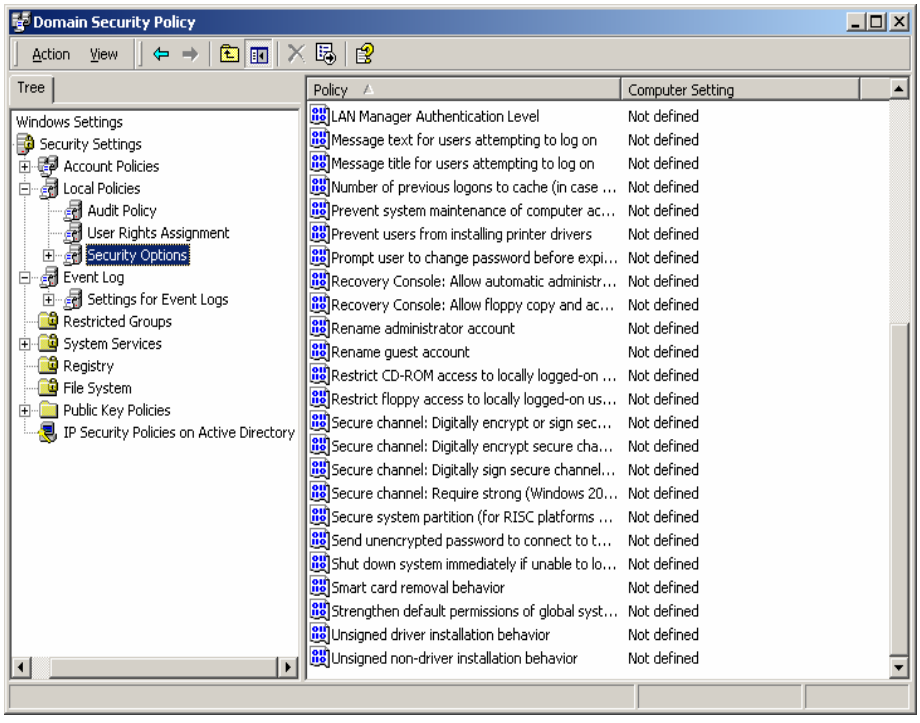
Audit policies:
account logon events
account management
directory service access
logon events
object access
policy change
privilege use
process tracking
system events



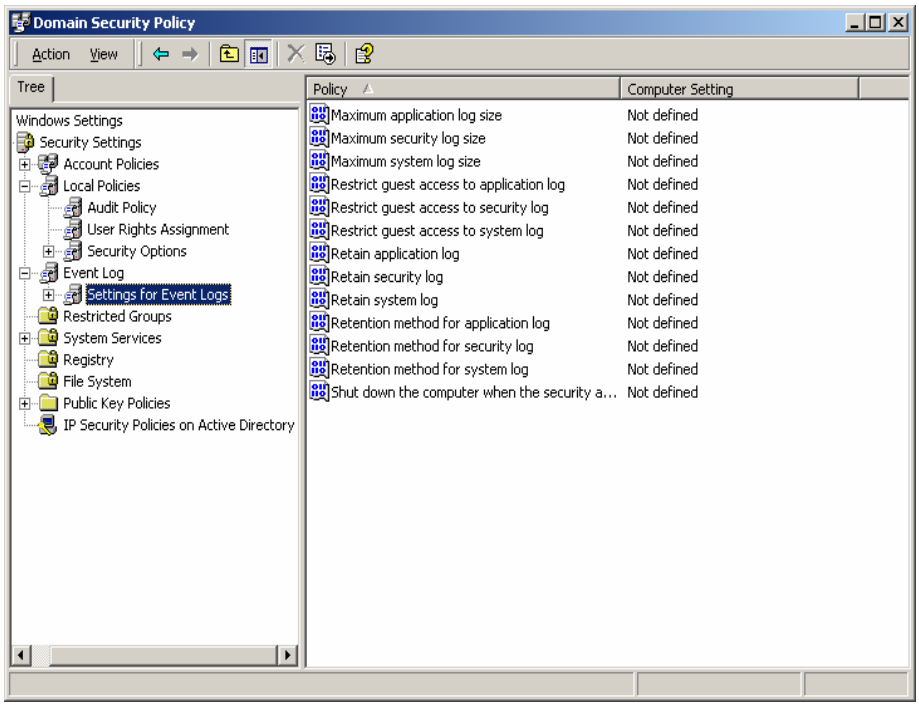


User rights assignment (none defined)

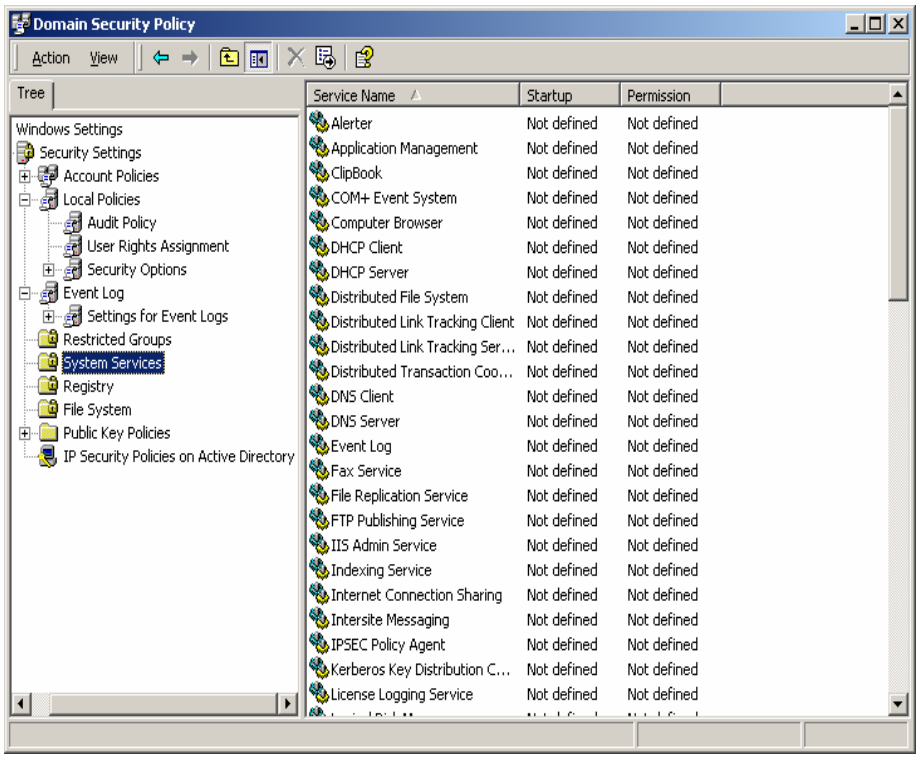


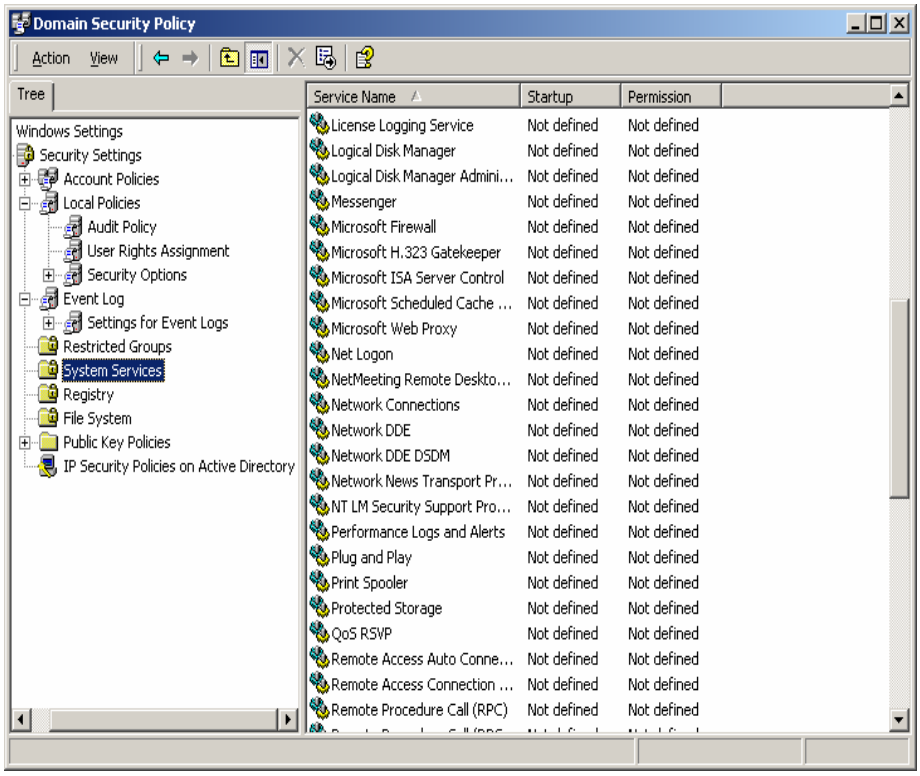


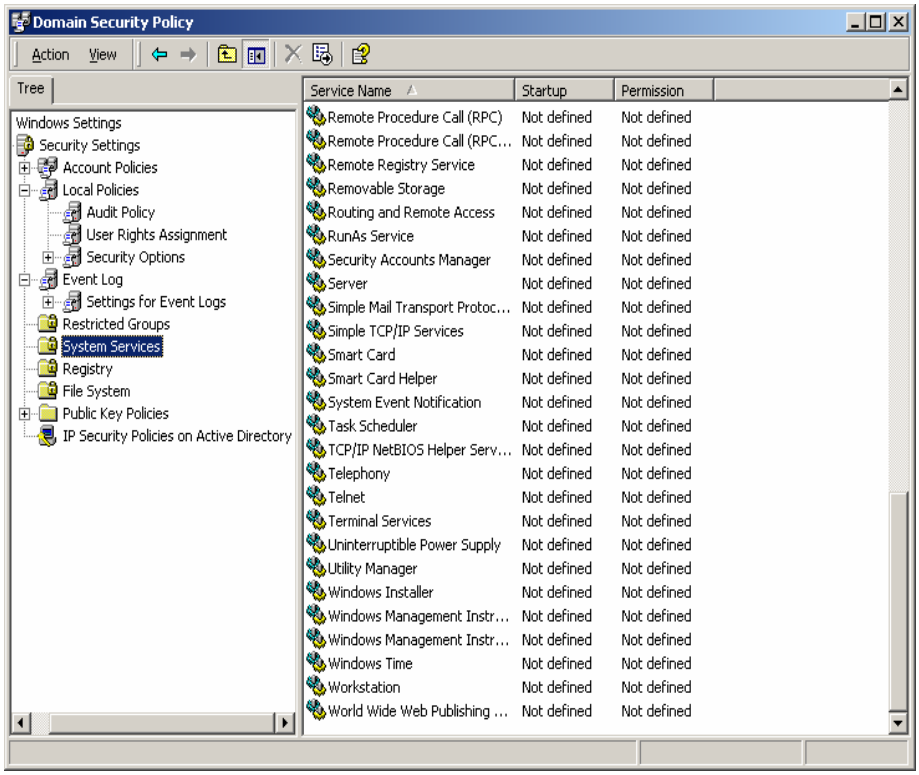
Security Options (all undefined or disabled)



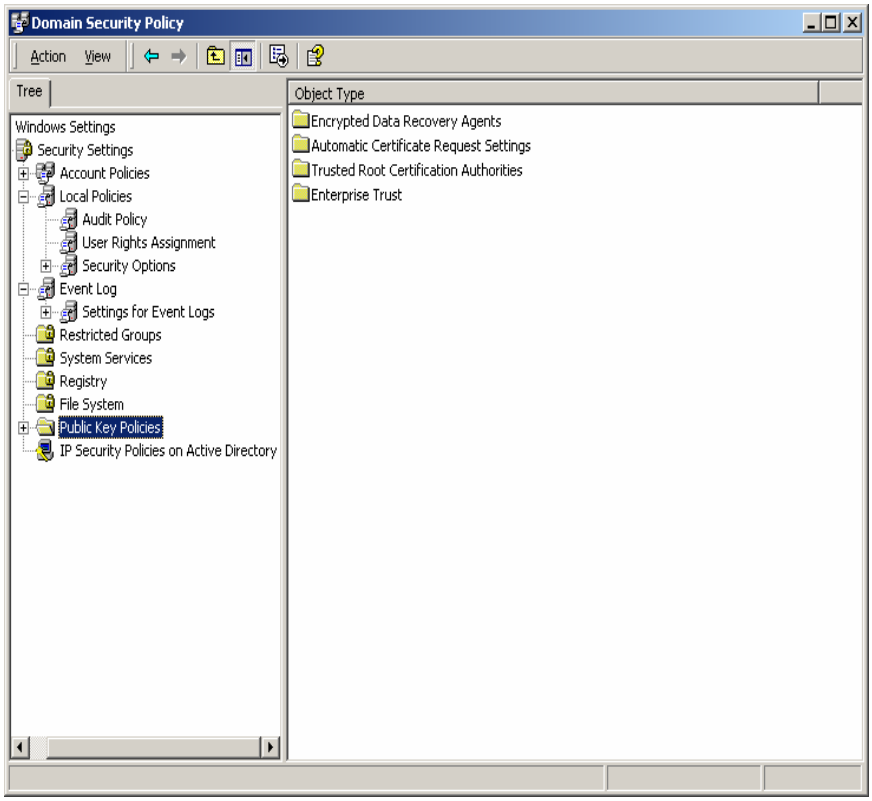
Event Log - Settings for event log



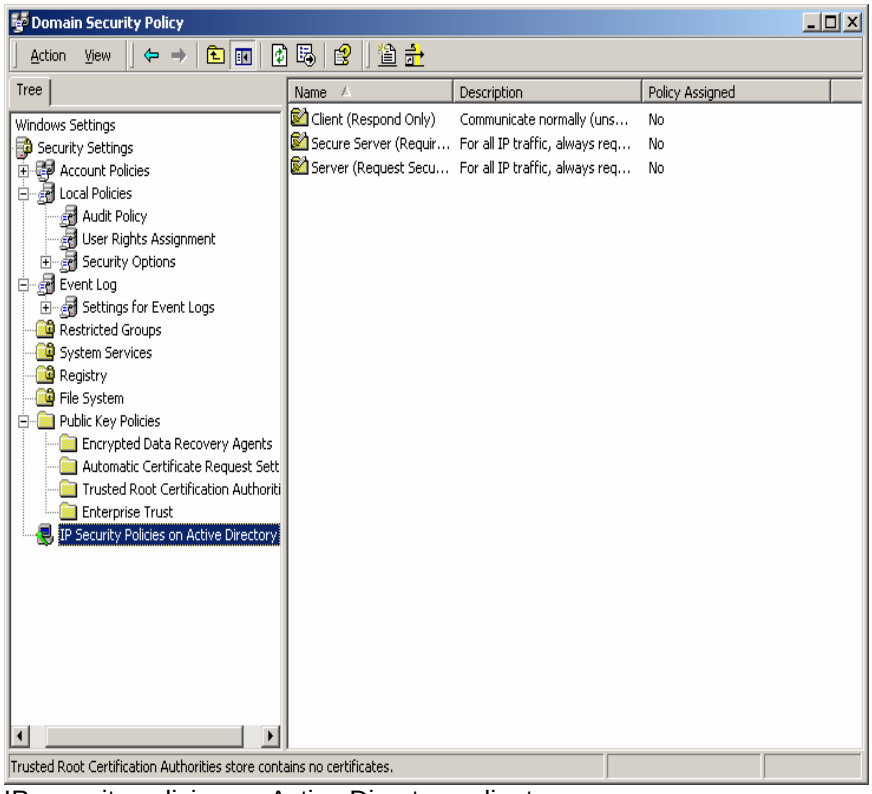




System services (all undefined)



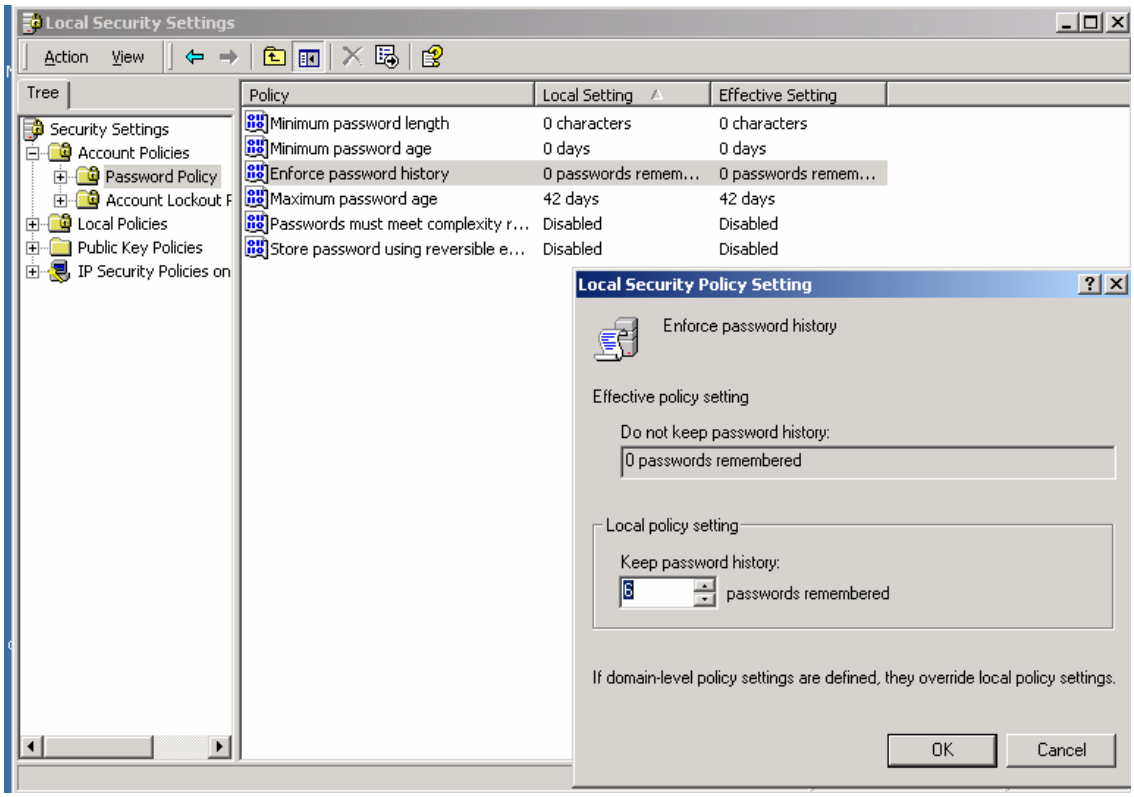
Public Key Policies: encrypted data recovery agents, automatic certificate request settings, trusted root certification authorities, enterprise trust



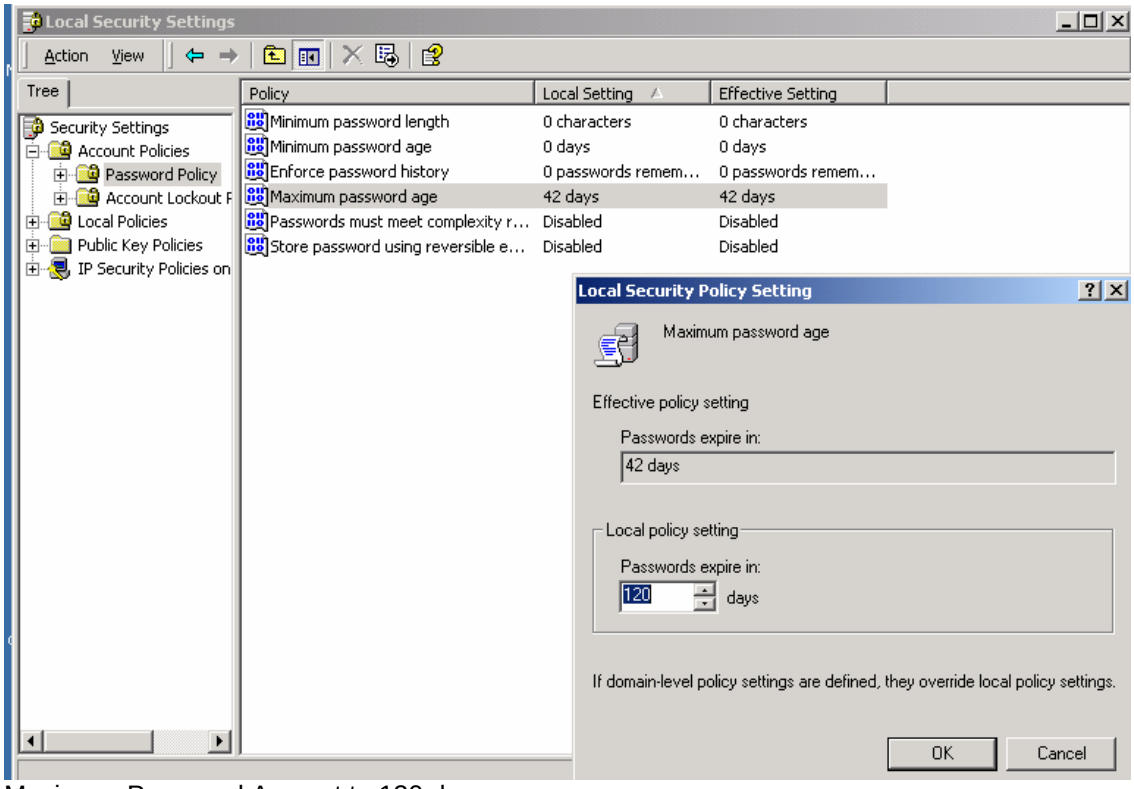
IP security policies on Active Directory: client, secure server, server

APPENDIX B

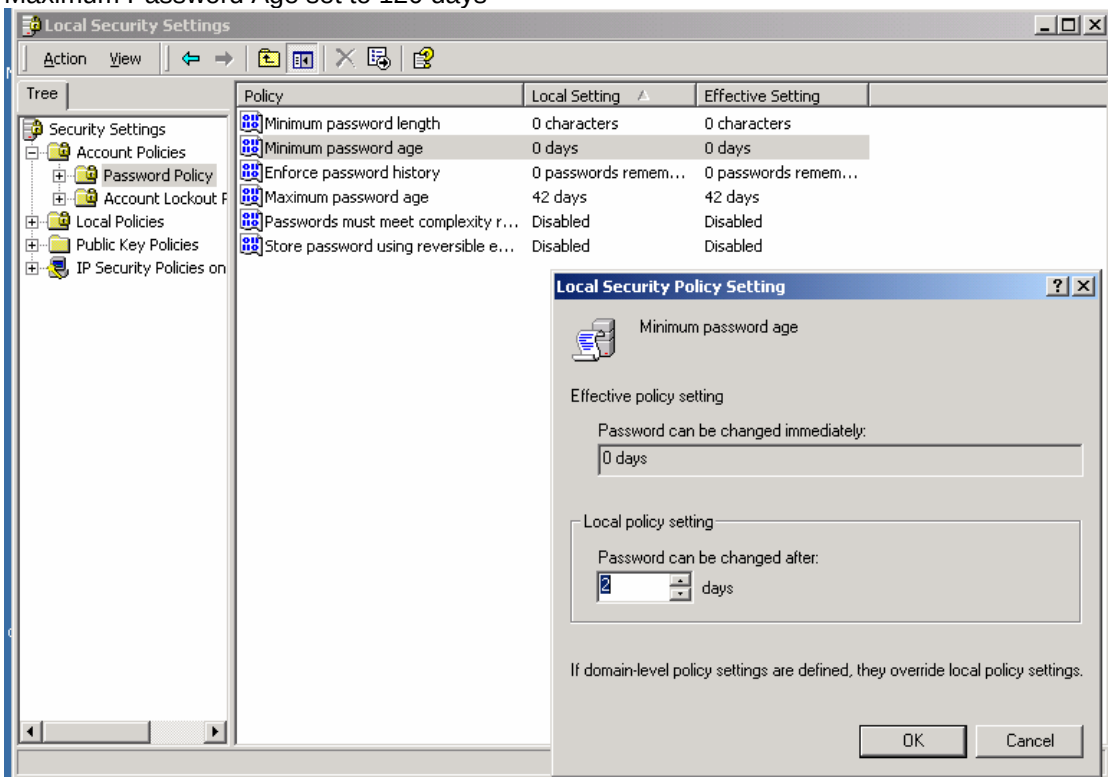
DOMAIN SECURITY POLICY - IMPLEMENTED



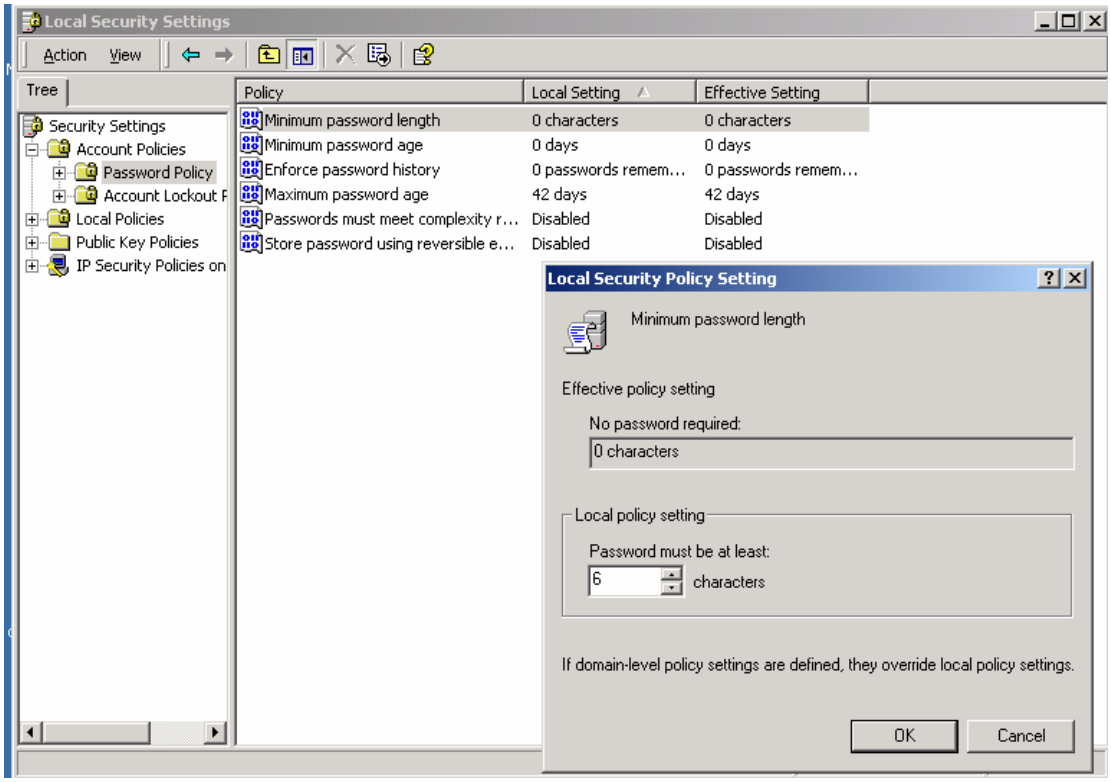
Enforce Password History set to 6 passwords



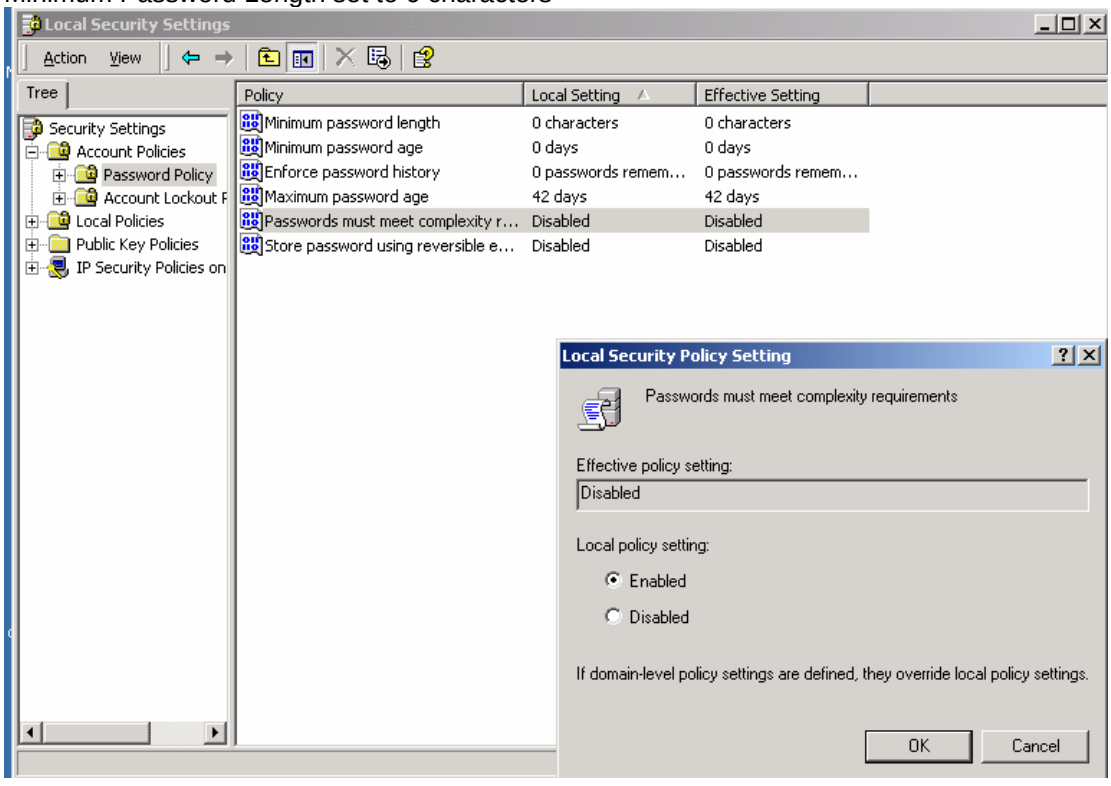
Maximum Password Age set to 120 days



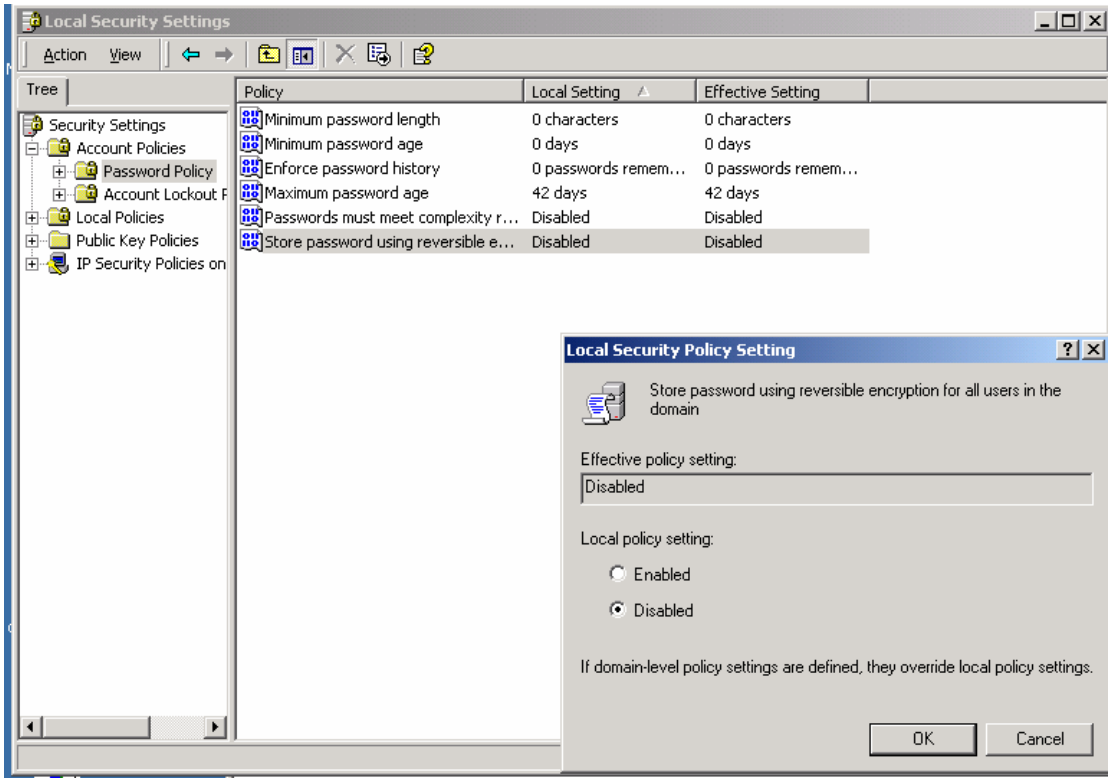
Minimum Password Age set to 2 days



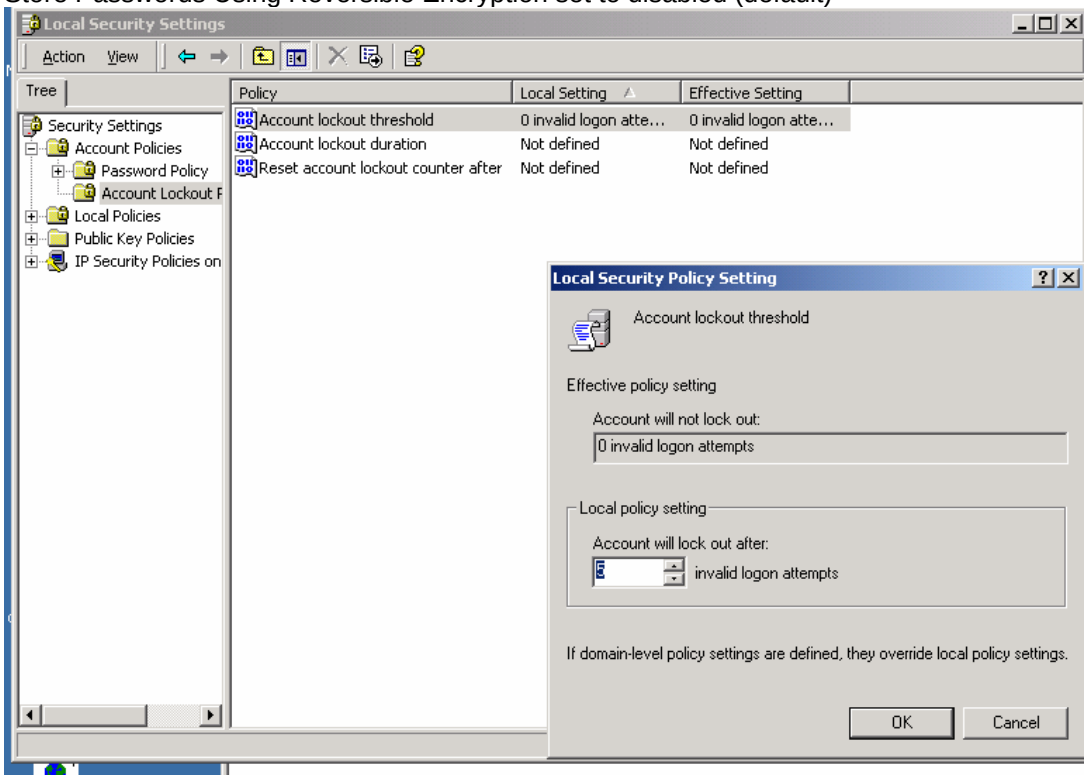
Minimum Password Length set to 6 characters



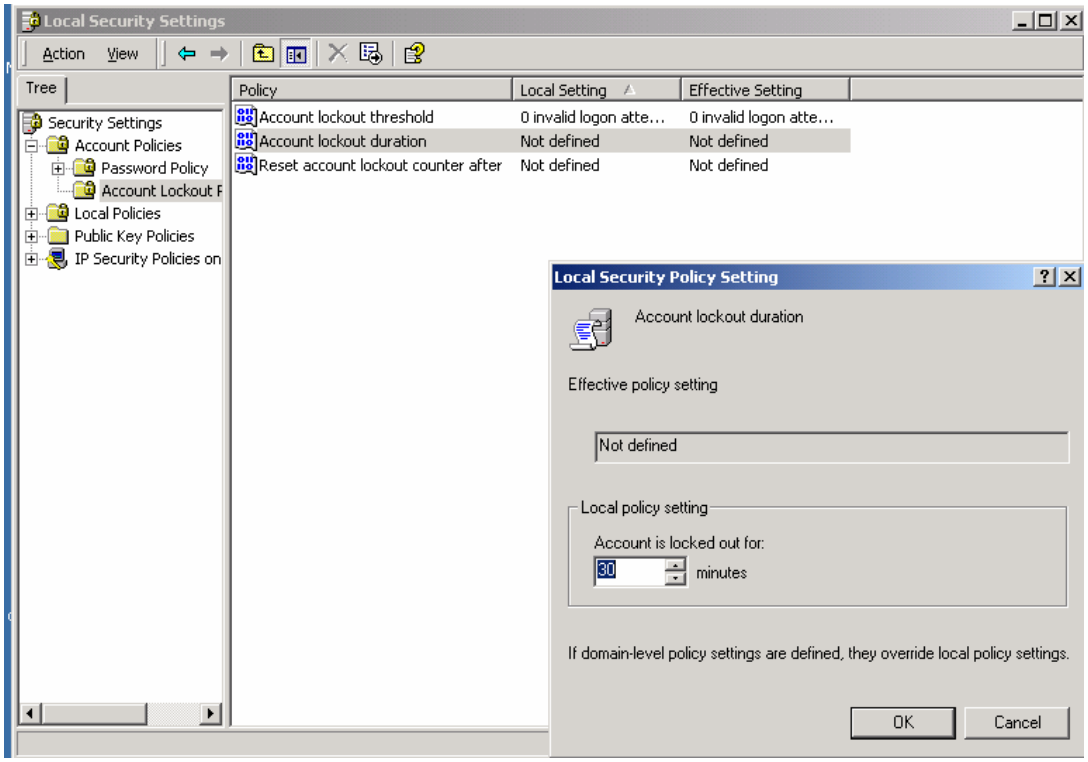
Passwords Must Meet Complexity Requirements set to enabled



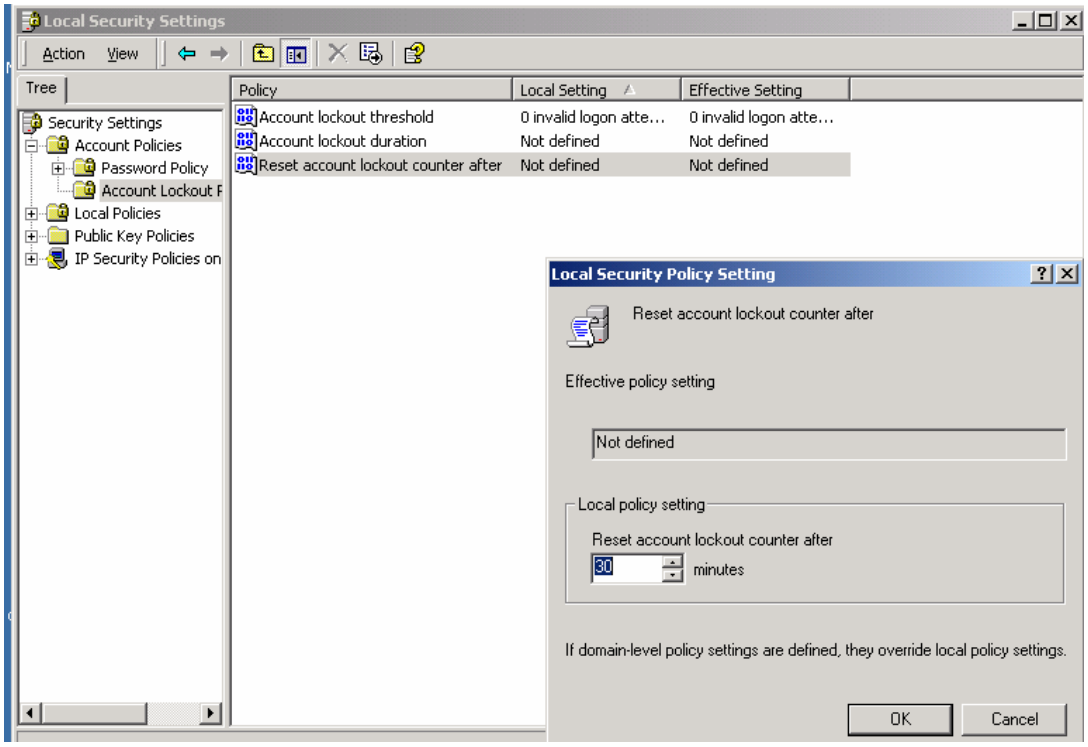
Store Passwords Using Reversible Encryption set to disabled (default)



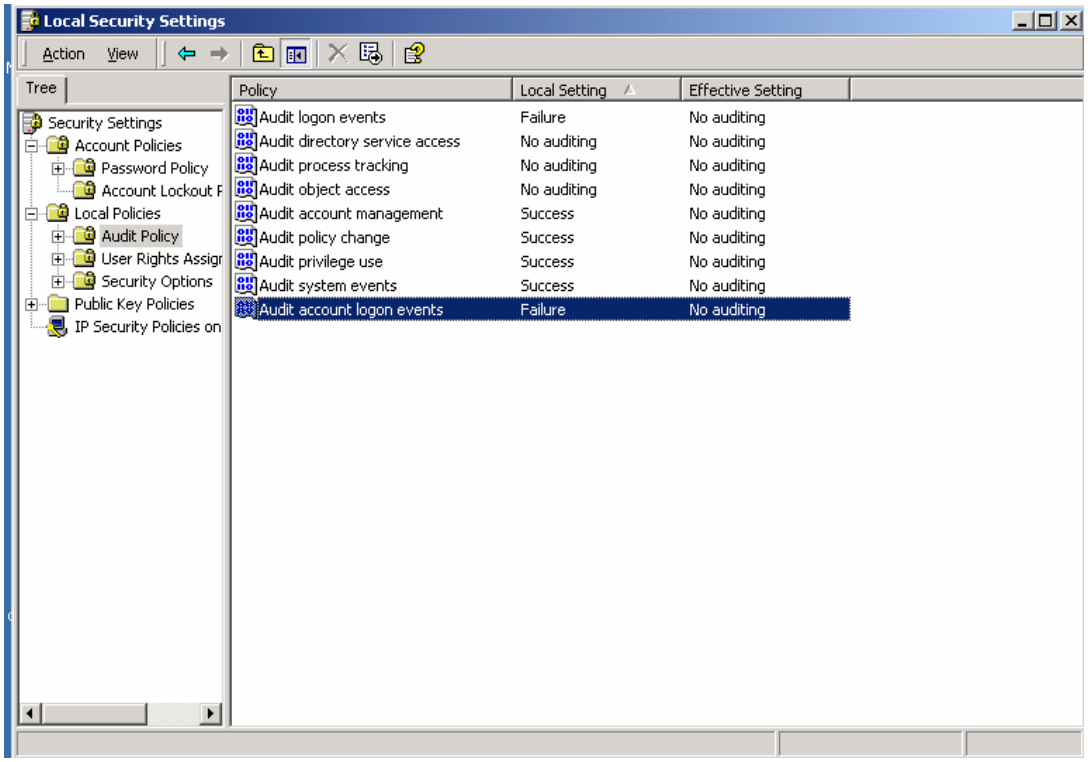
Account Lockout Threshold set to 5 attempts



Account Lockout Duration set to 30 minutes



Reset Lockout Counter set to 30 minutes



Auditing Policies set as depicted

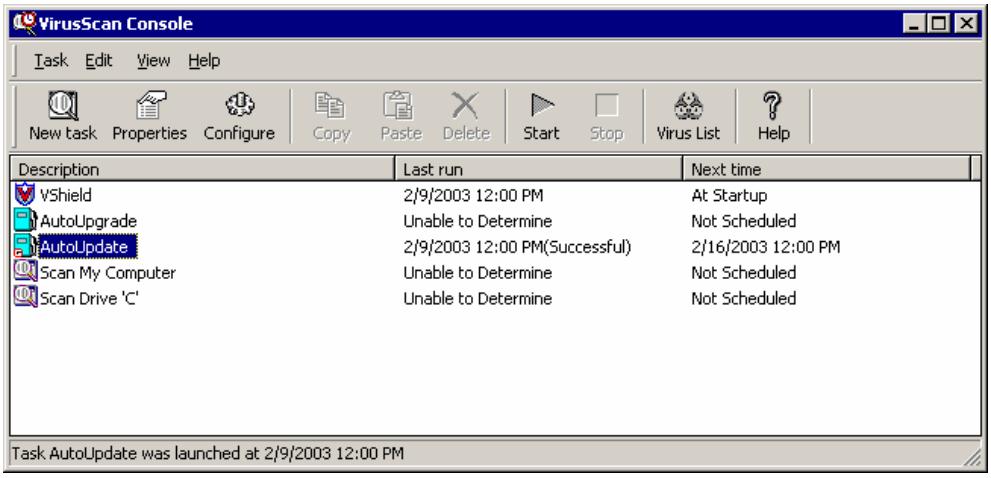
APPENDIX C

ANTIVIRUS SOFTWARE – AUTO UPDATE

Anti-Virus
Automatic Update Configuration Using FTP

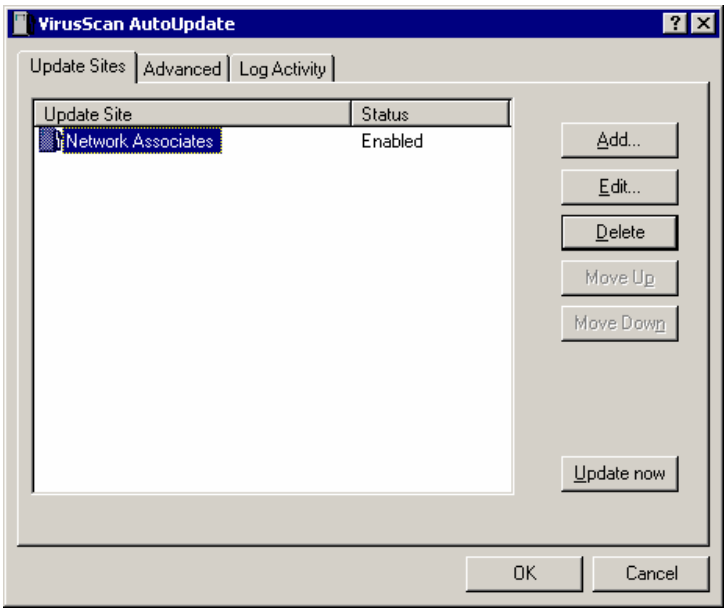
Note: You must have Administrative privileges on the computer to perform the following steps.

1. Go to Start; Programs; Network Associates; VirusScan Console
2. Dbl click on AutoUpdate

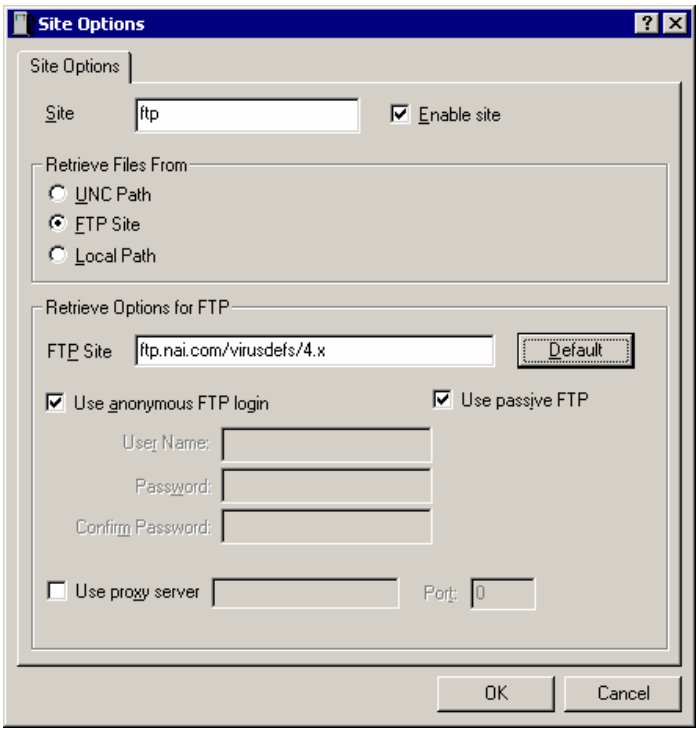


3. Click Configure

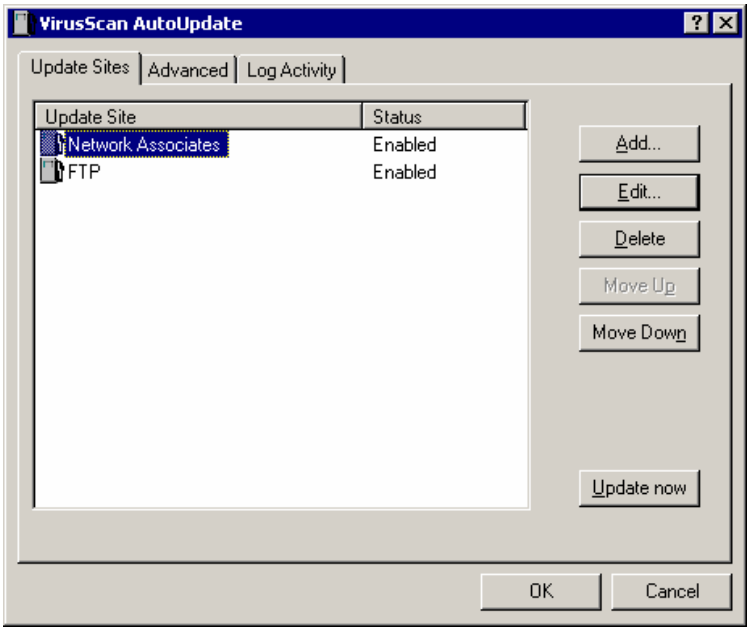
4. Click Add



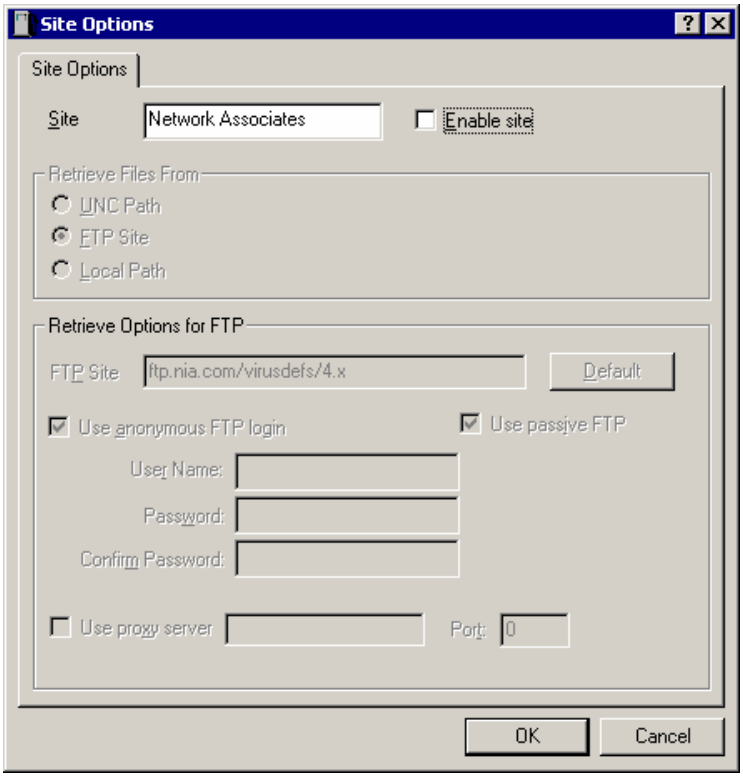
5. Enter the new site name: ftp
   Click Default to provide the path
   Click OK



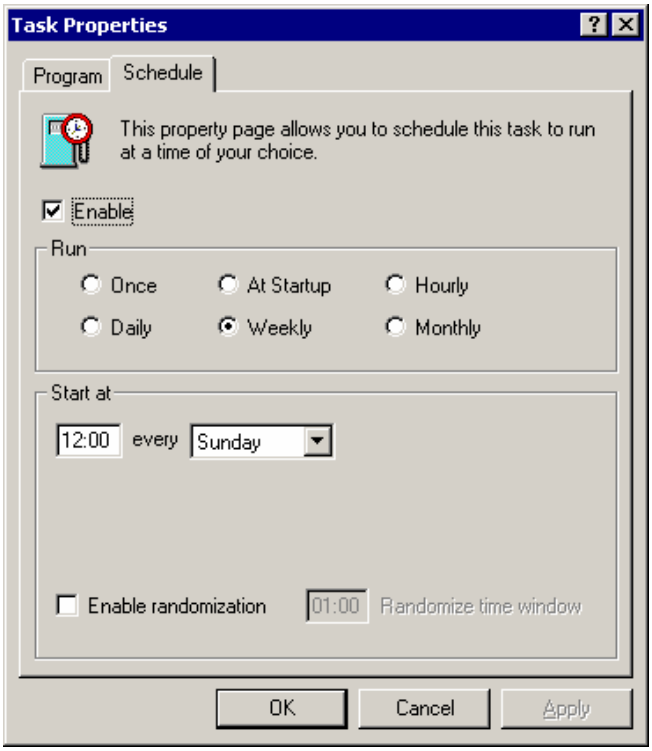
6. Highlight 'Network Associates' and click Move Down
7. Highlight Network Associates and click Edit



8. Uncheck the Enable site box then click OK



9. Click OK on the VirusScan AutoUpdate window
10. On the Task Properties window, click the Schedule Tab
    Check the Enable check box, then select the Weekly radio button
    Enter 12:00 every Sunday, then click OK



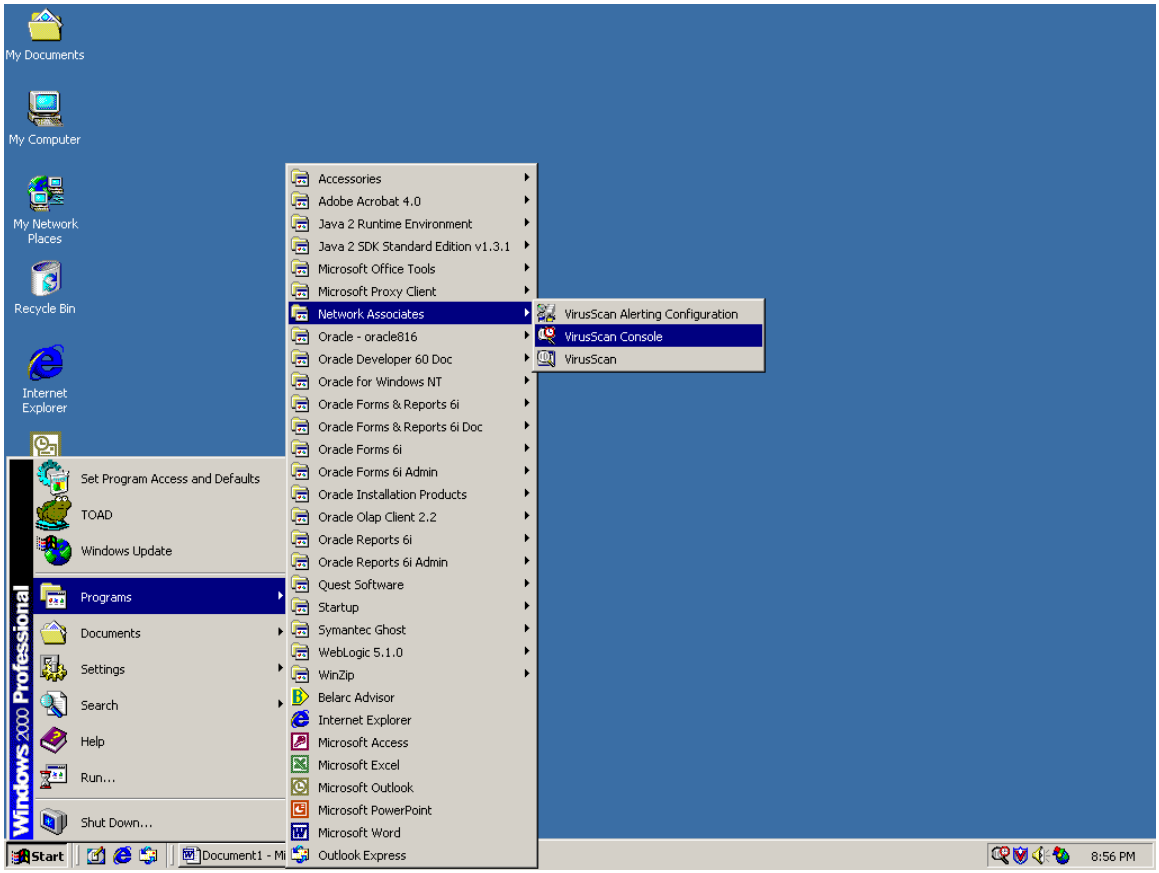
11. Close the VirusScan Console window

APPENDIX D

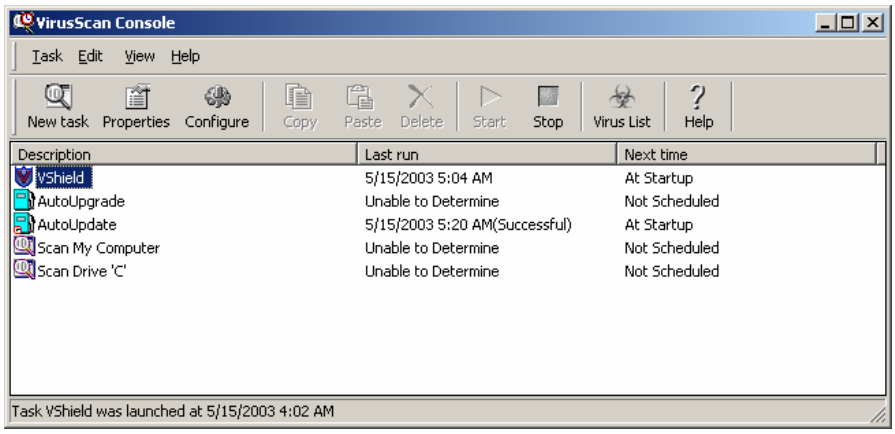
ANTIVIRUS SOFTWARE – AUTOSCAN

AUTOSCAN Setup: downloads and media access

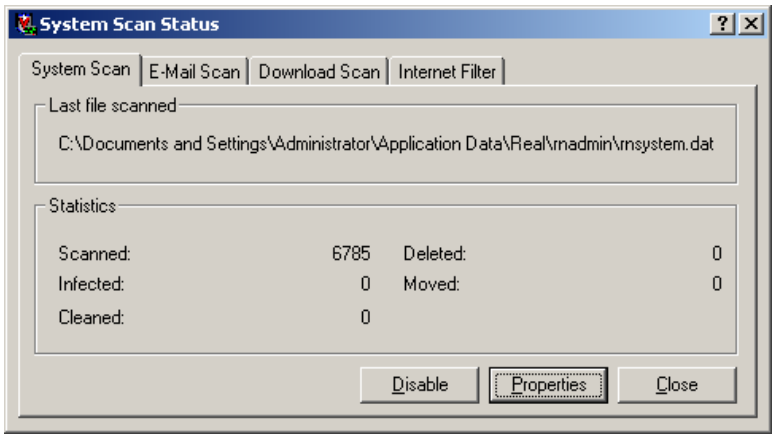
Start then *Programs* then *Network Associates* then *VirusScan Console*



Double-click *VShield*



From *System Scan Status* click *Properties*



Under *Detection* tab, check *Enable system scan*

Scan *Inbound files* and scan floppies on *Access*; deselect *Outbound files* and *Shutdown*

Scan *All files* including *compressed files*

General: uncheck *system scan can be disabled*; check *Show icon in the Taskbar*

Select *Action* tab

Under *Action* tab, select *Prompt for user action* from dropdown menu

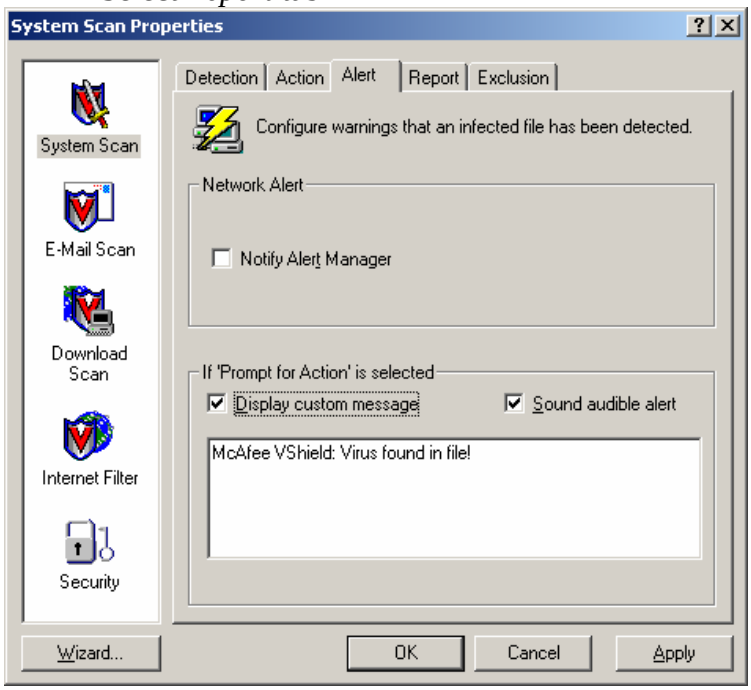
In *Possible Actions* box, check all boxes

Select *Alert* tab

Under *Alert* tab, uncheck *Notify Alert Manager*

In *If ' Prompt for Action' is selected*, check all boxes

Select *Report* tab

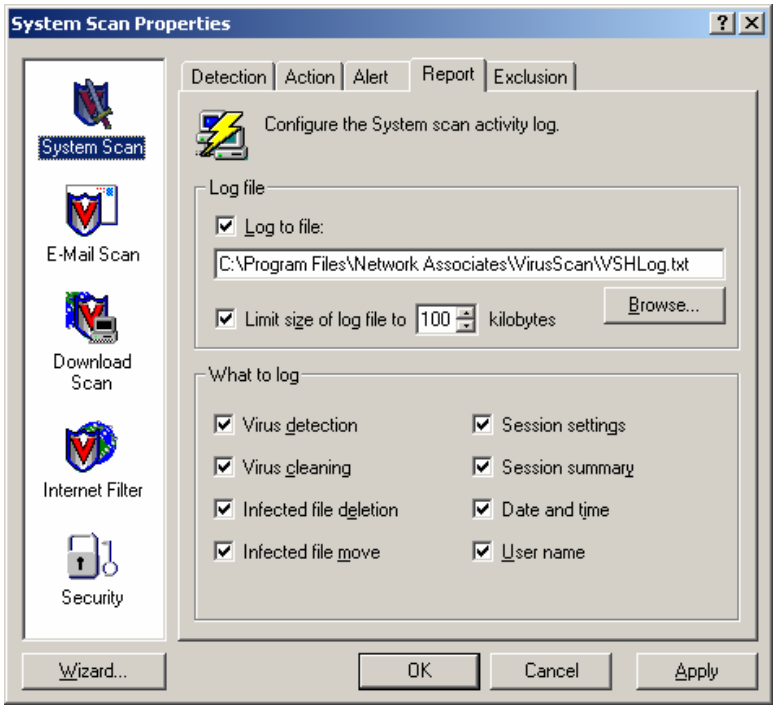


Under *Report* tab, check both boxes in *Log File* box

Check *Limit size of log file* box; leave file path as default, limit size at 100Kb

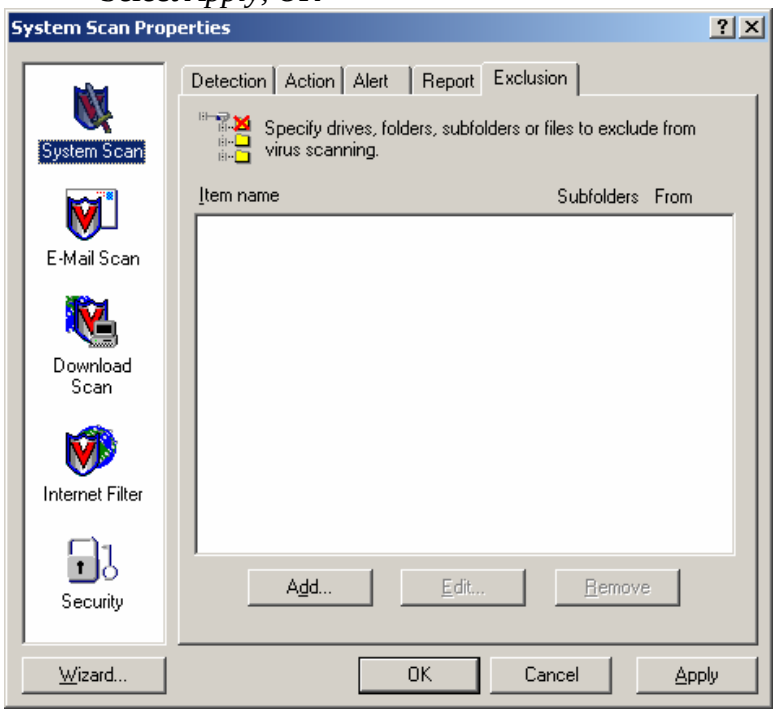
In *What to log* box, check all boxes

Select *Exclusion* tab

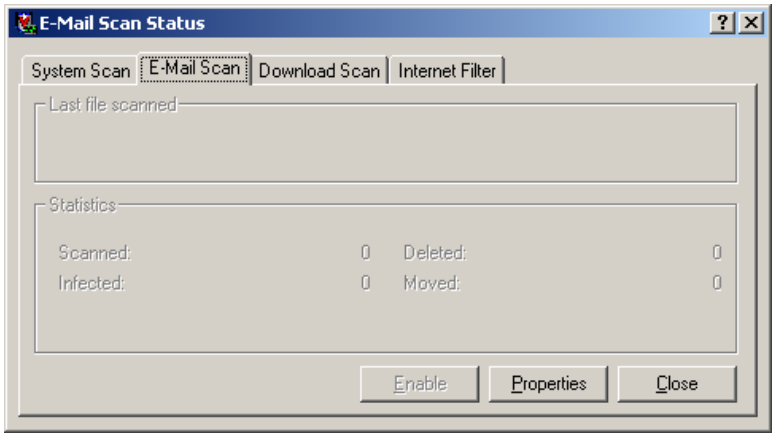


Under *Exclusion* tab, leave as default

Select *Apply, OK*



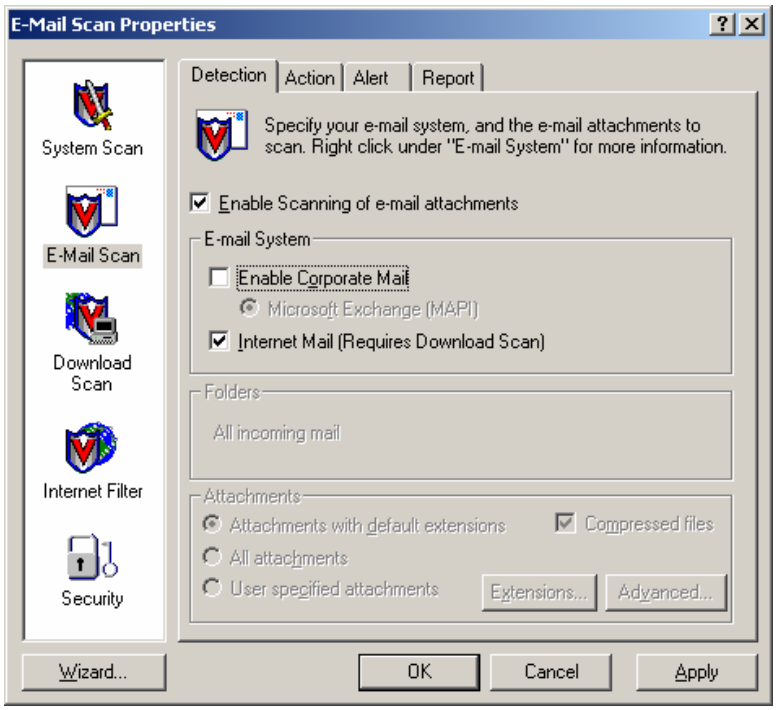
In *System Scan Status* window, select *E-Mail Scan, Properties*



Under *Detection* Tab, select *Enable scanning of e-mail* attachments and *Internet Mail*; when *Vshield notification* window opens, click *yes*

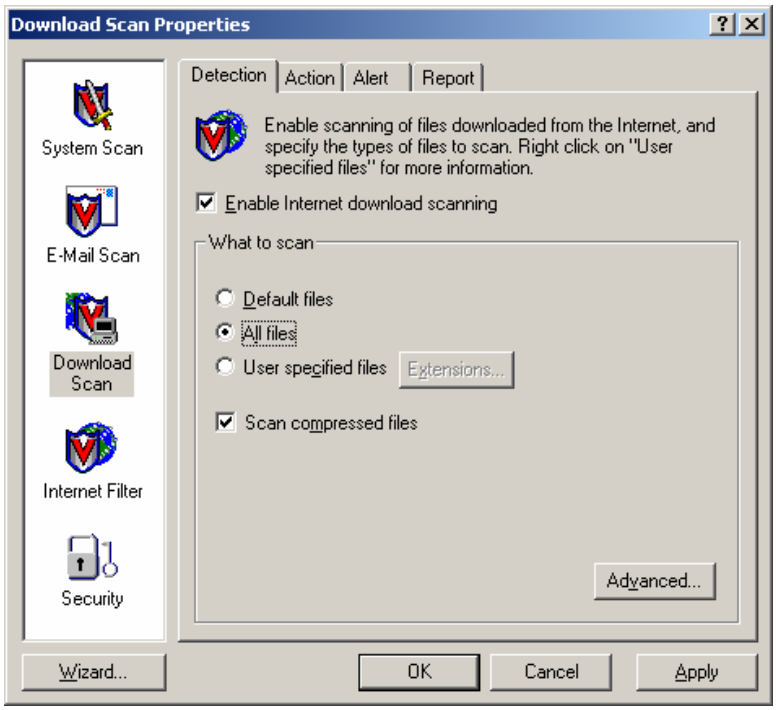
Select *Apply* and *OK*

If *Vshield Configuration Manager* window opens, select *yes* (to enable Download Scan)



Select *Download Scan*; under *Detection* tab:

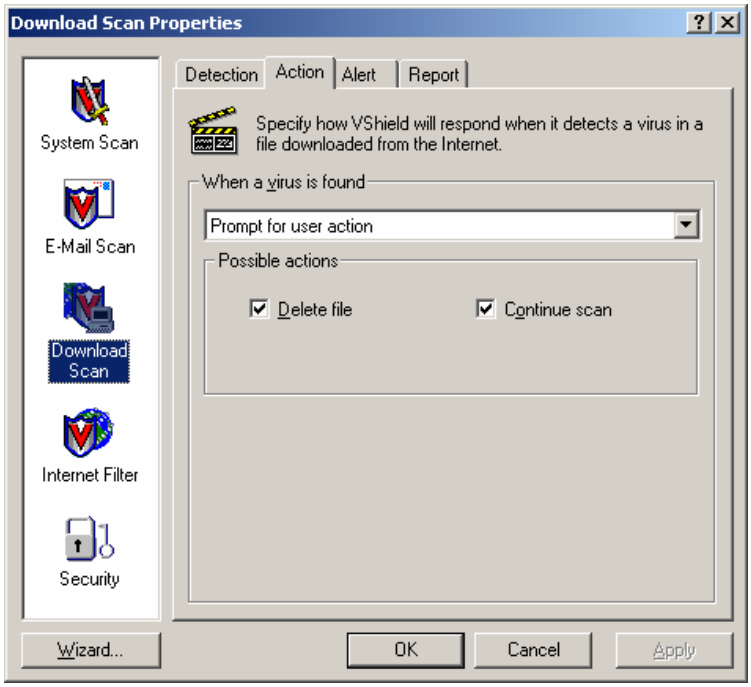
Check *Enable Internet Download Scanning*, *All Files* and *Scan compressed files*



Select *Action* tab

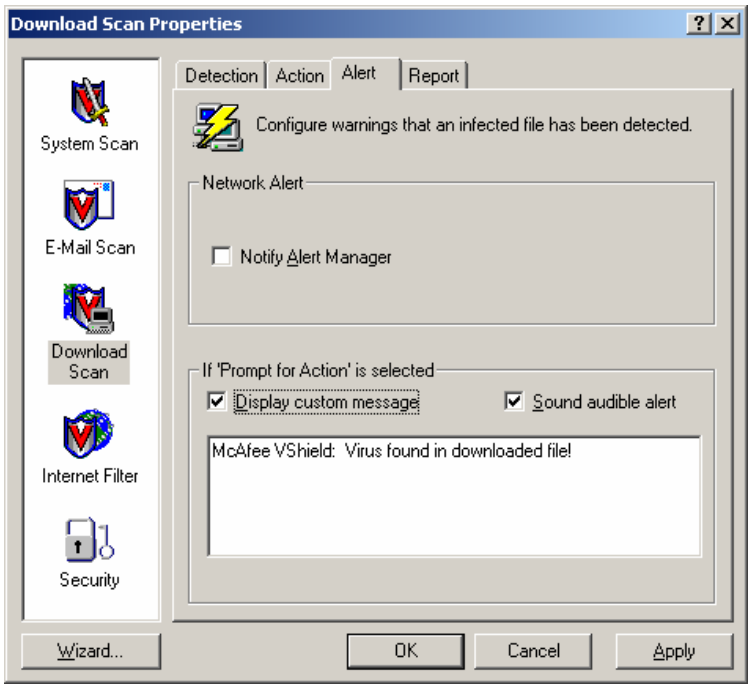
Select *Prompt for user action* from pulldown menu

Check *Delete file* and *Continue scan* boxes



Select *Alert* tab

Check *Display custom message* and *Sound audible alert* boxes



Select *Report* tab; Check *Log to file* box

Check *Limit size of log file to* box; leave file path as default, limit size at 100Kb

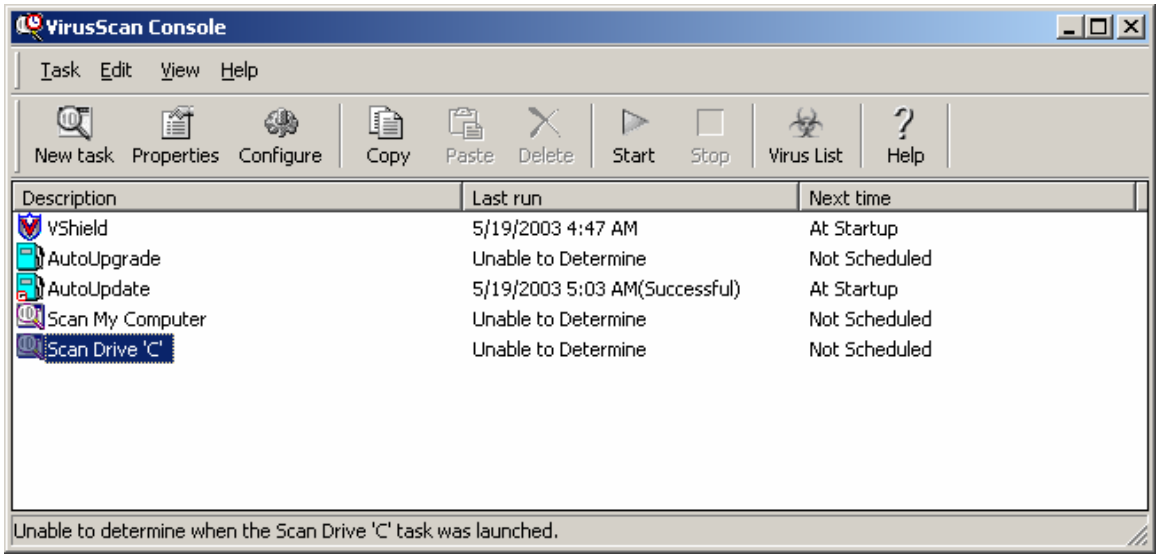
In *What to log* box, check all boxes; Select *Apply* and *OK*

If *Vshield Configuration Mgr* window opens, select *yes* (enables *Download Scan*)

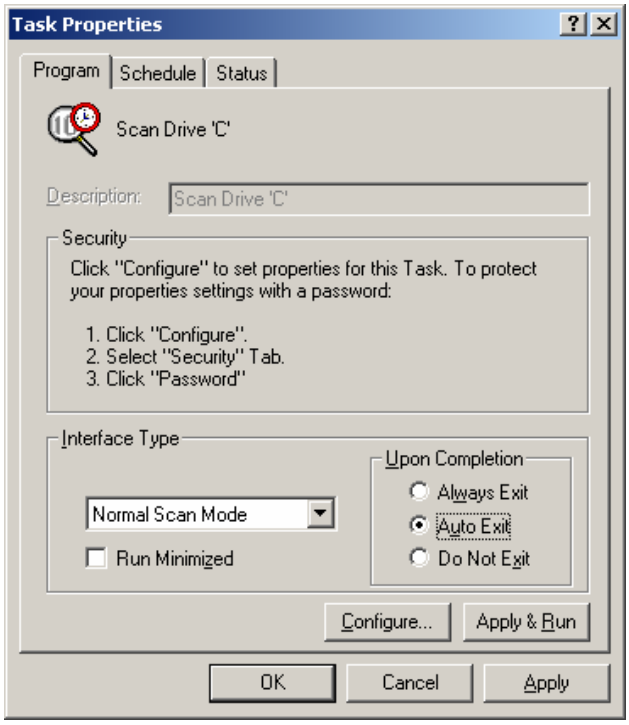
Close *Download Scan Properties* window

AUTOSCAN Setup

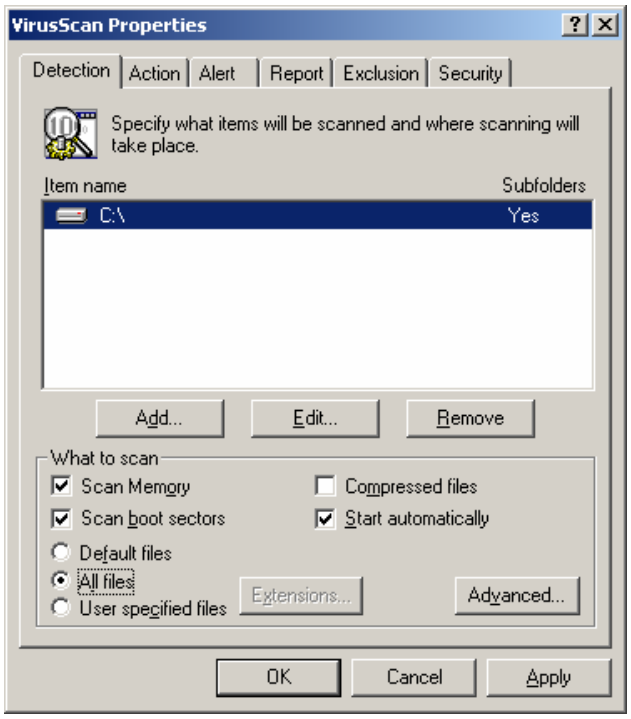
From VirusScan Console, double-click *Scan Drive 'C'*



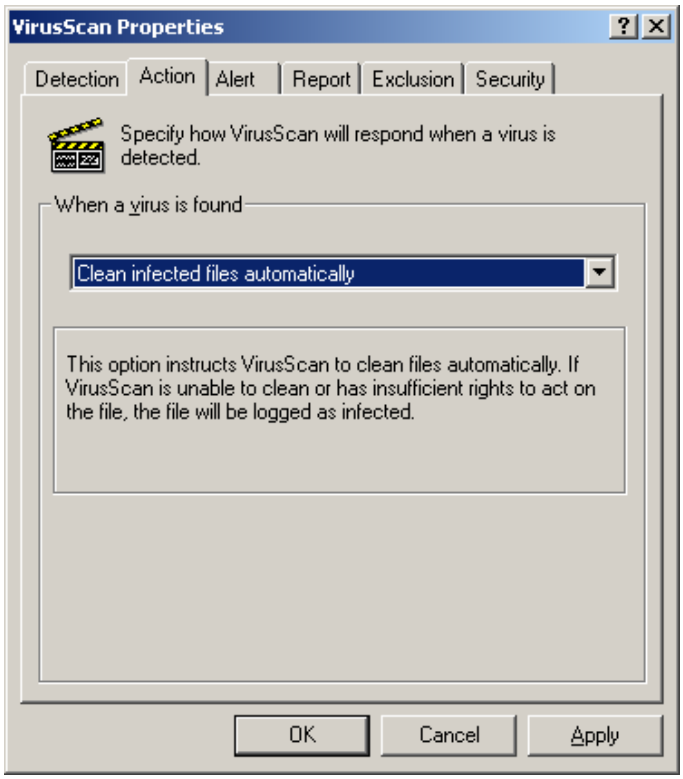
From *Program* tab, select *Normal Scan Mode* from pulldown menu
Select *Auto Exit* radial button
Select *Configure*



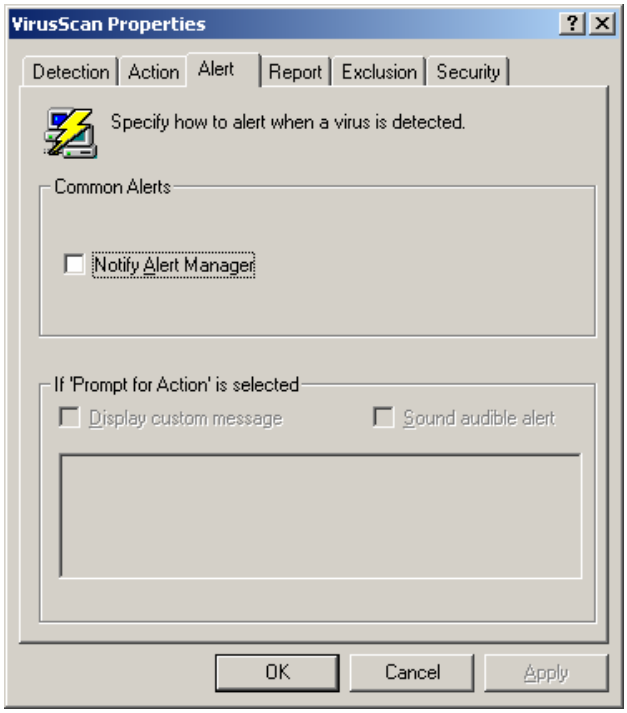
In *Detection* tab, check *Scan Memory*, *Scan Boot Sectors*, and *Start automatically* boxes
Select *All files* radial button



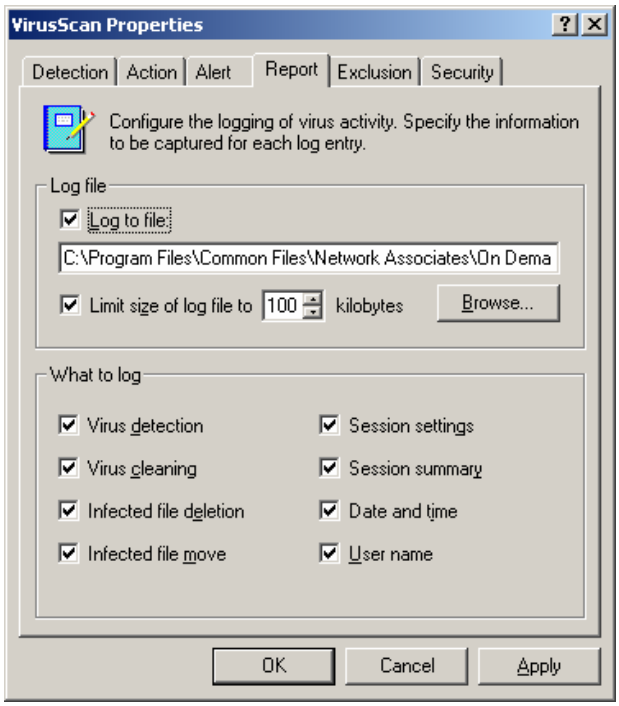
In *Action* tab, select *Clean infected files automatically*



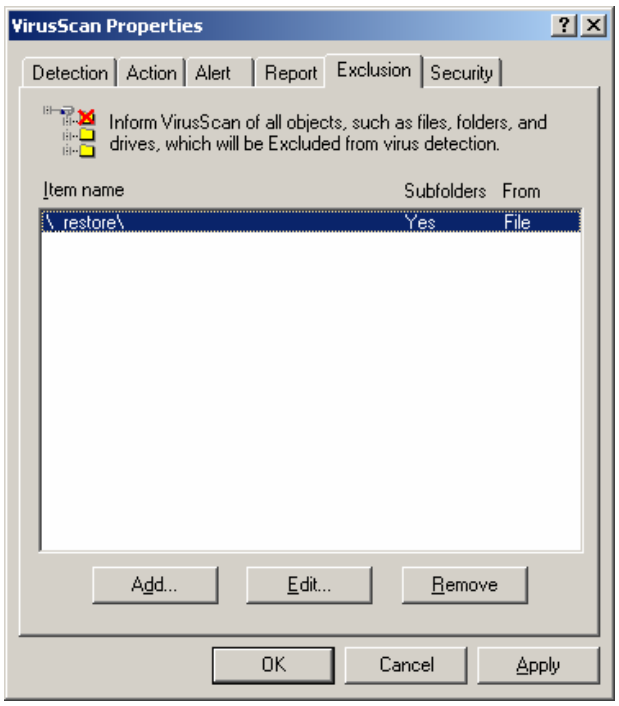
Select *Alert* tab, uncheck all boxes



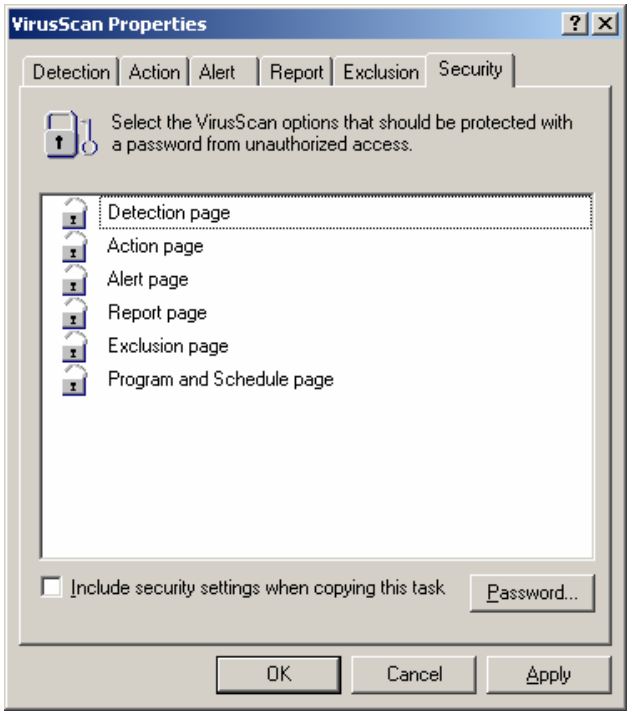
Select *Report* tab, check *Log to file* box, leave file path as default
Check *Limit size of log file to*, select 100kb
In *What to log*, check all boxes



In *Exclusion* tab, leave all blank



Select *Security* tab; leave all options without a password; leave box unchecked
Select *Apply, OK*



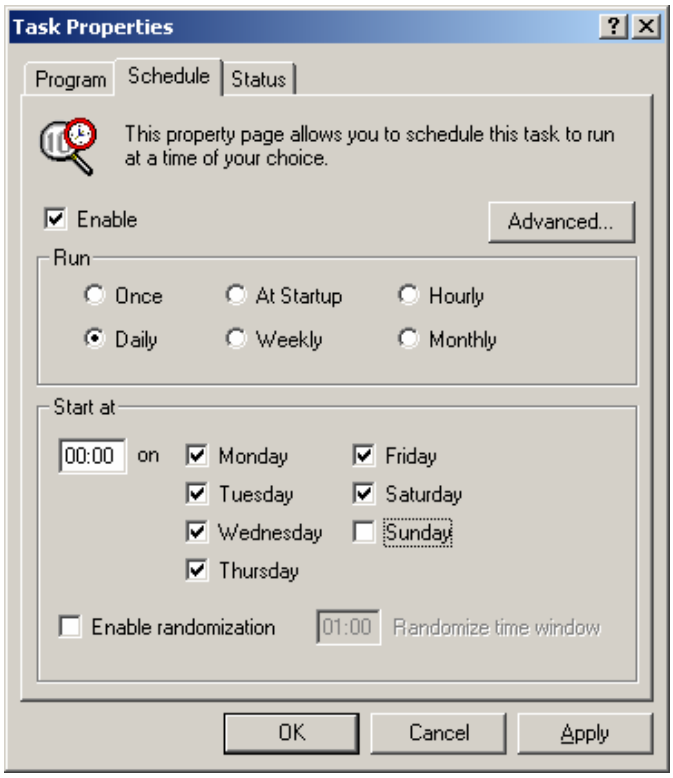
Back at *Task Properties* window, select *Schedule* tab; check *Enable* box

Select *Daily* radial button

Start at *00:00*; check all day boxes except Sunday

Uncheck *Enable randomization* box

Select *Apply* and then *OK*



Check *VirusScan Console* to ensure *Scan Drive 'C'* is now scheduled for next night at 12:00 A.M.

Exit *VirusScan Console*

APPENDIX E

SECURITY POLICY – RECOMMENDED GUIDELINES

*** Note: Below Draft policies have not been coordinated with Regis University administrative or legal staff. Before any attempt is made to implement these policies, such coordination should occur. Highlighted text indicates an area where appropriate Regis titles/positions/offices should be incorporated.**

REGIS UNIVERSITY
INFORMATION SYSTEMS SECURITY POLICY

1. PURPOSE

The purpose of this policy is to:

- ensure that the University complies with state laws and regulations regarding the use of and security of Information Resources
- establish prudent and reasonable practices for the protection and security of Information Resources
- educate employees, students, and others who may use Information Resources about the responsibilities associated with such use
- protect automated information resources against accidental or unauthorized disclosure, contamination, modification or destruction, as well as to ensure the security, reliability, integrity and availability of information

Regis University policy is to protect all data and information technology resources to the maximum extent possible in accordance with state and federal regulations.

2. GENERAL GUIDELINES

- Access to University information resources must be controlled. University owned information resources shall be used only for official academic purposes.

- Confidential information must be protected from unauthorized access or modification.

- Data essential to critical Regis University functions must be protected from loss, contamination, or destruction.

- Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value to both the University and potential intruder.

- The integrity of data, its source, its destination, and processes applied to it are critical to its value. Changes to data must be made only in authorized and acceptable ways.

- In the event a disaster or catastrophe disables information processing and related telecommunication functions, the ability to continue critical University services must be assured.

- Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.

- Security awareness of employees must be continually emphasized and reinforced at all levels of management. All individuals must be accountable for their actions relating to information resources.

- The University information security program must be responsive and adaptable to changing vulnerabilities and technologies affecting information resources.

- The University must ensure adequate separation of functions for tasks that are susceptible to fraudulent or other unauthorized activity.

3. RESPONSIBILITIES FOR INFORMATION RESOURCE SECURITY

Various classes of persons have responsibilities for the security of data, software, hardware and other information resources at Regis University:

- Information Security Officer - responsible for coordinating the University's information security function. The Information Security Officer is charged with:
    - Recommending policies and establishing procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information assets against unauthorized or accidental modification, destruction or disclosure
    - Documenting and maintaining an up-to-date information security program
    - Monitoring the effectiveness of defined controls for critical information
    - Reporting, at least annually, to the President or his/her designated representative on the effectiveness of information resources security controls

- Owner of an Information Resource - A person responsible for a business function and for determining controls and access to information resources supporting that business function. Owners are responsible and authorized to approve access and formally assign custody of an information asset, judge the asset's value, specify data control requirements and convey them to users and custodians, and ensure compliance with applicable controls.

- Custodian of an Information Resource - The person responsible for implementing owner-defined controls and access to an information resource. Custodians also provide physical and procedural safeguards for information resources, assist owners in evaluating the cost-effectiveness of controls and monitoring, and implement monitoring techniques and procedures for detecting, reporting and investigating breaches in information security. Because custodians, by virtue of their system responsibilities, have access to information resources that are generally outside the scope of their positions, they also have additional ethical and procedural responsibilities, shown in the System Administrator Code of Ethics in section 4, below.

- User of an Information Resource - An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules. Users of information resources have the following responsibilities:

  Individuals authorized to use University computing resources are prohibited from attempting to violate the security of other computer users on any system accessible via the University computer network. The violation or attempted violation of system security is grounds for revocation of computer access privileges, suspension or discharge of employees, suspension or expulsion of students, and prosecution under one or more of the following laws or policies:

  - Federal Copyright Law, Title 17, Section 117;
  - the Family Educational Rights and Privacy Act of 1974 (FERPA)

  Individuals are responsible for the security of any computer account issued to them and will be held accountable for any activity that takes place in their accounts. Any discovered violation or attempted violation of system security must be reported immediately to the Information Security Coordinator.

  Each Regis University faculty and staff member (including student staff) who has access to the University's central computer systems or any terminal or workstation device connected to the University computer network is responsible for using only those resources and materials required to fulfill his or her job functions. Moreover, such use must be appropriate and consistent with those job functions and must not violate or compromise the privacy or security of any data and/or systems accessible via the University computer network. Users will formally acknowledge that they will comply with the University security policies and procedures.

  Users must follow recommended security procedures for machines under their control, including but not limited to the use of virus scanning software and application of software and operating systems updates, and

will be held accountable for any activity that takes place on those machines.

Users are responsible for insuring that backup copies of essential data and software used on personal computers under their control are made frequently enough to prevent unacceptable loss of such data and software.

Each person having access to an administrative database is responsible for insuring the privacy and security of any information accessible to him/her in the normal course of his/her work.

Each person is responsible for the security of any terminal or workstation device accessible to him/her in the normal course of his/her work.

4. SYSTEM ADMINISTRATOR CODE OF ETHICS

Certain designated persons are given broader access to the resources of computer systems because their job responsibilities require such access. Typically, such persons are responsible for providing administrative services on the designated computer(s), services such as system maintenance, data management, and user support. The term "broader access" covers a range -- from wider access than given to an ordinary system user, up to and including complete access to all resources on the computer system. Persons with the broadest (complete) access are sometimes called "superusers."

This code of ethics applies to all persons given broader-than-normal access to any resources on Regis multi-user computer systems. It also applies to persons who authorize such access. The points contained in this code are considered additions to the responsibilities acknowledged by all ordinary computer users and by the authorizers of computer privileges.

Responsibilities of Privileged Access Users

Superusers (individuals with full access to files) and all other persons given broader-than-normal access privileges on Regis University computer systems agree:

- Not to "browse" through the computer information of system users while using the powers of privileged access unless such browsing: is a specific part of their job description (e.g., a corporate computer auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior or possible violations of University policy; or is specifically requested by, or has the approval of, the person who authorized their privileged access. Browsing should never be accomplished unless it is in the best interest of Regis University.
- Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.

- Not to copy any computer information for any purpose other than those authorized under their defined job responsibilities or pursuant to an authorized investigation or review.
- Not to intentionally or recklessly damage or destroy any Regis computing resources.
- Not to accept favors or gifts from any user or other person potentially interested in gaining access to University computer systems.
- Not to do any special favors for any user, member of management, friend, or any other person regarding access to Regis information systems. Such a favor would be anything that circumvents prevailing security protections or standards.
- Not to tell or disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.
- Not to attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.
- Not to change or develop any computer software in a way that would disclose computer information to persons not authorized to have it, or make it possible to to retain any special access privilege once that authorized privilege has been terminated by management.
- Not to make arrangements on computer system(s) under their charge that will impair the security of other systems. In order to comply with this restriction, a system administrator setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.

Furthermore, superusers and all other persons given broader-than-normal access privileges on Regis information systems agree that they will:

- Report all suspicious requests, incidents, and situations regarding Regis information systems to an appropriate member of local campus system administration and/or information security management.
- Use all available software protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.
- Take steps to the best of their ability to comply with all computer security standards and policies in force at Regis University and furthermore, to advise management and/or designated computer security representatives at Regis of deficiencies in these standards.
- Conduct themselves in a manner that will foster security awareness and understanding among users.

Responsibilities of Management

Management should restrict the number of persons granted privileged access to a minimal practicable number. Management should tell the person who is responsible for overall administration of a system the names of all other persons who have been granted privileged access and what functions those persons have been assigned. Persons who are

to be given privileged access to a University computer system should be selected (or approved) by the Department Head owning or managing the operation of the computer system or by another member of management to whom this responsibility has been delegated.

5. RISK ANALYSIS PROCEDURES

Risk analysis is the vehicle for systematically evaluating the vulnerabilities of an information system and its data to the threats facing it in its environment. It is an essential part of any security and risk management program. Although absolute security against all threats is unachievable, risk analysis provides a framework for weighing losses which may be expected to occur in the absence of an effective security control against the costs of implementing such a control. Risk management is intended to ensure that reasonable steps have been taken to prevent situations that can interfere with accomplishing the University mission. To that end, the following measures shall be taken:

- An internal audit of the information security function shall be performed periodically, based on risk assessment, as directed by the President or the Associate Vice President for Computing and Communications Services acting on delegated authority for risk management decisions.

- Owners of information resources shall periodically complete and/or commission a risk analysis of all information resources in their custody. The degree of risk acceptance (i.e. the exposure remaining after implementing appropriate protective measures, if any) must be identified and documented.

- The Associate Vice President for Computing and Communications Services shall biennially complete and/or commission a risk analysis of information resources considered essential to the University's critical mission and functions. He or she shall also prepare or commission and maintain a written and cost-effective Disaster Recovery Plan that provides for the prompt and effective continuation of critical University missions in the event of a disaster. The Disaster Recovery Plan will be tested and updated periodically to assure that it is valid and remains current.

6. PERSONNEL PRACTICES

- People are the most important components of an information security program. People also represent the greatest threats to information security; therefore, maintaining employee awareness and motivation is an integral part of the security program. Managers are responsible for taking all measures necessary to insure that departmental staff maintain an appropriate level of confidentiality of information retrieved from University information sources. Examples of such information include personnel and payroll records, transcript and grade records,

financial aid information, and other sensitive data. Use of such information for unauthorized purposes is prohibited, as is access to such information in any form whatsoever by unauthorized individuals.

- The University has developed and maintains an Acceptable Use Policy that details specific steps that should be taken to protect information resources at Regis. The use of University information resources implies that the user has knowledge of and agrees to comply with the procedures contained and referenced in the policy. Managers are responsible for insuring that all faculty, staff, and student members of their respective departments, including part-time or temporary employees, read and agree to the policies and procedures as outlined in this policy.

- The IT Department shall provide literature and/or training to emphasize security awareness and the importance of individual responsibility with respect to information security. Supervisors must continually reinforce the value of security consciousness in all employees whose duties bring them into contact with confidential or sensitive information resources.

- Supervisors are responsible for insuring that access privileges are revoked or modified as appropriate for any employee in their charge who is terminating, transferring, and/or changing duties. Supervisors should provide notification to the appropriate custodian of an information resource whenever an employee's access privileges should be revoked or changed as a result of the employee's change in status. The custodian of each information resource shall establish procedures to insure that all security privileges associated with an employee's job function are revoked once it is known that the employee has ceased employment with the University. The separating employee shall cease to have any further access to confidential and sensitive information via University information system resources.

7. PHYSICAL SECURITY PROCEDURES

Without physical control over the access to information resources, there can be no security from unauthorized use of those resources because malicious or inexperienced persons could obtain access to the operating system of servers and/or desktop machines and thereby view, copy, delete, or otherwise cause harm to the files on the system. Therefore, the following procedures are critical to protecting the University’s information resources:

- All University information processing areas must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations.

- Managers shall conduct reviews of physical security measures annually as well as whenever facilities or security procedures are significantly modified.

- Physical access to centrally administered computer facilities is restricted to individuals having prior authorization from the IT Department. Authorized visitors shall be supervised.

- The responsibility for securing departmentally administered computer facilities and/or equipment from unauthorized physical access and/or improper use rests with the manager responsible for the facility and/or equipment.

- Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in appropriate responses in case of emergencies or equipment problems. Emergency procedures shall be developed and regularly tested.

- No terminal or workstation logged in to a current job session capable of accessing confidential or sensitive information shall be left unattended unless appropriate measures, such as password protected keyboard locking, have been taken to prevent unauthorized use. The owner of the logged-in account is responsible for any activity that occurs during a job session logged-in under that account.

- Data and software essential to the continued operation of critical University functions will be backed up. The security controls over the backup resources will be as stringent as the protection required of the primary resources. Backup of data and software stored on centrally administered computer systems is the responsibility of the IT Department. Departments administering networks are responsible for establishing regular schedules for making backup copies of all mission-critical data and software resident on their networks and for ensuring that the backups are stored in a safe location.

8. INFORMATION SAFEGUARDS

- The IT Department will purchase and maintain virus protection software for use on all University-owned or operated computers.

- Each University department shall, as part of its contingency plan, provide for an alternate means of accomplishing its program objectives in case the system or its communication network becomes unavailable. Alternative procedures shall be established that enable University personnel to continue critical day-to-day operations in spite of the loss of the communication network.

- When confidential or sensitive information from another university or state agency is received by Regis in connection with the transaction of official business, Regis shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency or university.

- Except for public users of systems where such access is authorized, or for situations where risk analysis demonstrates no need for individual accountability of users, each user of a multiple-user automated system shall be assigned a unique personal identifier or user identification. User identification shall be authenticated before the system may grant that user access to automated information.

- Mission-critical University systems which use passwords for authentication shall conform to the federal standard on password usage contained in the Federal Information Processing Standard Publication 112 (FIPS PUB 112), which specifies minimum criteria and provides guidance for selecting additional password security criteria when appropriate.

- Appropriate audit trails shall be maintained to provide accountability for changes to confidential or sensitive information, software and automated security or access rules.

- Encryption techniques for storage and transmission of information shall be used based on documented agency security risk management decisions.

- Test functions shall be kept either physically or logically separate from production functions. Copies of production data shall not be used for testing unless all personnel involved in testing are authorized access to the production data.

- Appropriate information security and audit controls shall be incorporated into new systems. Each phase of systems acquisition shall incorporate corresponding development or assurances of security controls.

- Public access systems must authenticate the identity of any individual retrieving, creating, and/or updating sensitive or confidential information about themselves.

- Public access systems must have security procedures in place to protect the privacy and confidentiality of individuals who access those systems, in accordance with federal and state laws.

- Any individual who connects a machine to a campus network is responsible for maintaining security on that system (including password security) and for performing appropriate security updates so as to prevent security breaches to the University network.

- The custodian of an information resource must take steps where possible, such as using an encryption system, to ensure that passwords cannot be obtained by interception of data communications transmissions or access to a storage device.

- Network access to an application containing confidential or sensitive data, and data sharing between applications, shall be as authorized by the application custodians and shall require authentication of any user of the application.

9. SECURITY BREACHES

Breaches to information resource security controls shall be investigated promptly by the owner of the information system, assisted by the IT Department Security Coordinator if such assistance is requested. If criminal action is suspected, the owner or investigating agency must contact the University Police, who shall investigate and take appropriate legal action. Violations of policy shall be reported to a faculty or staff member's supervisor or, if the violation is by a student, to the Center for Student Rights and Responsibilities.

10. SANCTIONS

- Machines on the campus data communications network will be disconnected if they are deemed by the IT Department Security Coordinator to be dangerous to the remainder of campus or to the Internet in general.
- Penalties for violation of this policy range from loss of computer resource usage privileges to dismissal from the University, prosecution, and/or civil action. Each case will be determined separately on its merits. Referrals for legal action will be made through the Office of the Vice Chancellor and General Counsel.
- If the offender is a faculty member, the procedures to be followed are those specified in accordance with the Regis Faculty Discipline Policy.
- If the offender is a staff member, the procedures to be followed are those specified in the Performance Counseling and Discipline Procedure
- If the offender is a student, the procedures to be followed are those specified in the Code of Student Conduct. If the student in violation of this policy is also an employee of the University, sanctions may include termination of employment.

REGIS UNIVERSITY
ACCEPTABLE USE OF INFORMATION RESOURCES

I. Introduction

Regis University provides a wide variety of computing and networking resources to qualified members of the university community. Access to computers, computing systems and networks owned by Regis University is a privilege which imposes certain responsibilities and obligations and which is granted subject to university policies and codes, and local, state and federal laws. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources including wireless. The purpose of this policy is to promote the efficient, ethical and lawful use of Regis University's computer and network resources.

II. Scope

This policy applies to all users of Regis University computing and network resources, whether initiated from a computer and/or network device located on or off campus.

III. Policy Statement

Individuals using computer resources belonging to Regis University must act in a responsible manner, in compliance with law and University policies, and with respect for the rights of others using a shared resource. The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information. While Regis University's network administration desires to provide a reasonable level of privacy, management cannot guarantee the confidentiality of information stored on any network device belonging to Regis. For security and network maintenance purposes, authorized Regis system administrators may monitor system devices at any time. Electronic information on University networks or equipment, including, but not limited to, electronic mail and personal information, is subject to examination by the University where:

1. It is necessary to maintain or improve the functioning of University computing resources;
2. There is a suspicion of misconduct under University policies, or suspicion of violation of Federal or State laws; or
3. It is necessary to comply with or verify compliance with Federal or State law.

IV. Acceptable Use Guidelines

The specific usage guidelines that follow are not intended to be comprehensive, but rather to establish and clarify the intent of this policy. Situations not enumerated here will inevitably arise, and they should be interpreted according to the spirit of this policy.

Each person using Regis University's computer and network resources should:

1. **Take no actions that violate the Codes of Conduct and Academic Integrity, Classified Staff Personnel Policy Manual, University Handbook for Appointed Personnel, or other applicable policy or law.** This is not a comprehensive list of applicable University policies. In the event of a conflict between policies, the more restrictive use policy shall govern.

   See the following related manuals/documents for more information:

Faculty and Staff Manuals:
Student Code of Conduct:

2. **Use security measures to protect the integrity of information, data, and systems.** Users shall protect their computer systems and accounts by using strong passwords and employing anti-virus software consistent with management directives. Users are responsible for safeguarding their passwords, and for using them only as authorized. Users are also responsible for ensuring removable media are virus-free prior to accessing such media in University information systems. Examples of misuse include using a computer account and/or obtaining a password that you are not authorized to use, using the University network to gain unauthorized access to any computer system, attempting to alter established University security settings, and using a "sniffer" or other methods in an attempt to "crack" passwords.

   See the following related documents for more information:
   Regis University Electronic Privacy Statement:
   Regis University summary of FERPA:
   Guidelines for Collection, Use and Disclosure of Personal Information at Regis University:

3. **Clearly and accurately identify one's self in electronic communications.** Do not forge or misrepresent one's identity. Concealing or masking the identity of electronic communications such as altering the source of an email message by making it appear as if the message was sent by someone else is a violation of this policy.

   See the following related polices for more information:
   Electronic Mail Policy:
   Official Student E-mail Policy:

4. **Use computer and network resources efficiently.** Computing resources are finite and must be shared. Users may use the University's computer and network resources for incidental personal purposes, provided that such use does not (A) unreasonably interfere with the use of computing and network resources by other users, or with the University's operation of computing and network resources; (B) interfere with the user's employment or other obligations to the University; or (C) violate this policy or other applicable policy or law. Regis retains the right to set priorities on use of the system, and to limit recreational or personal uses when such uses could reasonably be expected to cause, directly or indirectly, strain on any computing facilities, or to interfere with research, instructional or administrative computing requirements, or to violate applicable policies or laws. Examples of inappropriate use include sending unsolicited e-mails via listservs, newsgroups, or other means (SPAM), sending "chain letters" or engaging in pyramid schemes.

5. **Do not harass or intimidate or use computer and network resources for unlawful acts.** The University, in general, cannot and does not wish to be the arbiter of content maintained, distributed or displayed by users of the University's computing and network resources. For example, the University, in general, cannot protect users from receiving e-mail they may find offensive. Using the University's computer or network resources for illegal activities, however, is strictly prohibited. Unlawful use of University computer and network resources can expose the individual user and the University to damages claims, or potential criminal liability. Unlawful uses may include, but are not limited to: harassment and intimidation of individuals on the basis of race, sex, religion, ethnicity, sexual orientation or disability; obscenity; child pornography; threats; any illegal activity (forgery,

harassment, intimidation, willful misrepresentation, defamation or unauthorized copying of anything); theft; attempting unauthorized access to data; attempting to breach security measures on any electronic communications software or system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws. Do not use computer systems to send, post, or display abusive, slanderous or defamatory messages, text, graphics, or images. By using the University's computer and network services, each user accepts the responsibility to become informed about, and to comply with, all applicable laws and policies.

6. **The use of university computer resources and networks is for legitimate academic or administrative purpose.** Incidental personal use is permissible to the extent that it does not violate other provisions of this policy, interfere with the performance of employee's duties, or interfere with the education of students at Regis. Use of your computer account or the network for commercial activities that are not approved by appropriate supervisory University personnel consistent with applicable policy, or for personal financial gain (except as permitted under applicable academic policies) is prohibited. Examples of prohibited uses include using your computer account for engaging in unauthorized consulting services, software development, advertising products/services, and/or other private commercial activity.

7. **Respect copyright and intellectual property rights.** Users must adhere to the U.S. Copyright Act, and the terms and conditions of any and all software and database licensing agreements. Any form of original expression fixed in a tangible medium is subject to copyright, even if there is no copyright notice. Examples include music, movies, graphics, text, photographs, artwork and software, distributed in any media -- including online. The use of a copyrighted work (such as copying, downloading, file sharing, distribution, public performance, etc.) requires either (A) the copyright owner's permission, or (B) an exemption under the Copyright Act. Adhere to the terms of software licenses and other contracts. Persons loading software on any University computer must adhere to all licensing requirements for the software. Except where allowed by University site licenses, copying software licensed for University use for personal use is a violation of this policy. The law also makes it unlawful to circumvent technological measures used by copyright owners to protect their works. Copyright infringement exposes the user, and possibly the University, to heavy fines and potential criminal liability. Therefore, without limitation of other possible sanctions, the University may refuse, suspend and/or terminate computer and network access, with respect to any user who violates the copyright law, or who uses the University's computer or network resources contrary to the terms of the University's software or database license agreements.

   See the following related document for more information:
   United States Copyright Office {*http://www.loc.gov/copyright*}

8. **Respect University property.** Misuse of University property includes, but is not limited to, theft or damage of equipment or software, knowingly running or installing computer viruses or password cracking programs, attempting to circumvent installed data protection methods that are designed and constructed to provide secure data and information, or in any way attempting to interfere with the physical computer network/hardware, or attempting to degrade the performance or integrity of any campus network or computer system.

9. **Make only appropriate use of data to which you have access.** Authorized University personnel (e.g. system, network and database administrators, among others) may have

access to data beyond what is generally available. Privileged access to data may only be used in a way consistent with applicable laws, University policies, and accepted standards of professional conduct. Those who have access to databases that include personal information shall respect individual privacy and confidentiality, consistent with applicable laws and University policies regarding the collection, use and disclosure of personal information. Users should be aware, however, that state laws and Regis University policies, guidelines and regulations may prevent the protection of certain aspects of individual privacy. Both the nature of electronic communications, and the public character of the University's business make certain uses less private than users may anticipate. For example, in certain circumstances, the University may permit the inspection, monitoring or disclosure of e-mail, consistent with applicable laws and with the University's Electronic Mail Policy.

See the following related polices/documents for more information:
Regis Electronic Privacy Statement:
Electronic Mail Policy:
Regis summary of FERPA:
Guidelines for Collection, Use and Disclosure of Personal Information at Regis University:

10. **Respect and adhere to other departmental/college/Internet Service Provider's acceptable use policies.** When using a University computer system and/or network to connect to a non-Regis University system or network, adhere to the prevailing policies governing that system or network. This does not in any way release your obligation to abide by the established policies governing the use of Regis University computer systems and networks.

V. Consequences of Misuse and/or Non-Compliance

Users who misuse University computing and network resources or who fail to comply with the University's written usage policies, regulations and guidelines are subject to one or more of the following consequences:

- Temporary deactivation of computer/network access
- Permanent deactivation of computer/network access
- Disciplinary actions taken by the department or Dean of Students Office up to and including expulsion from school or termination of employment
- Subpoena of data files
- Legal prosecution under applicable Federal and State laws
- Possible penalties under the law, including fines and imprisonment

Violations, complaints and questions should be reported to the Regis University Security Incident Response Team (SIRT) by email (sirt@regis.edu) or call xxx-xxxx.

I have read the above conditions of service.

Signature _____ Date _____ Name (typed) _____

APPENDIX F

JOURNAL LOG

November 06, 2002: Colorado Springs (2.0 hours/2.0 total)
Introduction to the NLP with previous NLP team. Received rundown on the ARN and how the NLP program works. Monitored group's progress in the CS Lab.

November 13, 2002: Colorado Springs (1.75 hours/3.75 total)
Monitored previous NLP team's progress as they worked to load Windows 2000 Server and downloaded Service Pack 3. Began to familiarize myself with the CS Lab network.

November 20, 2002: Colorado Springs (1.75 hours/5.5 total)
Monitored previous NLP team's progress as they attempted to load MS Outlook on PC#3. Load was unsuccessful; received successful "ping" but PC did not recognize *exchange.cs.Regis.local* as expected. Tier III leader determined the fault with Outlook and subsequently successfully e-mailed to the other lab PCs.

December 14, 2002: Lowell (5 hours/10.5 total)
NLP introduction at the Regis Lowell Campus by Dan Likarish. Dan explained the NLP concept to new NLP students and discussed program requirements, to include: project responsibility; basic skills; mandatory meetings; journaling; and Tier I-III descriptions. After a brief on the methodology of presenting the final project, Dan described how the various pieces of the ARN fit together architecturally. He also briefed the waterfall/spiral methodologies for student focus. This was followed by a discussion of current work at the various campuses: NOC and Lab admin; security monitoring; transport and communication; VM Ware; and Oracle development. We followed up with campus representatives giving us a status update for the various NLP projects at each campus.

January 07, 2003: Colorado Springs (1 hour/11.5 total)
Introductory meeting between previous and current NLP groups for information exchange and project status update. Bob Bowles, project advisor, discussed project proposals and Lab availability for weekly meetings. NLP students began to divide up the priority projects for the CS Lab. Given my interest in security, I opted to tackle the Lab's security policy and implementation.

January 11, 2003: Lowell (6 hours/17.5 total)
Meeting commenced with monthly campus updates. Dan Likarish then went over the "new" MSCN 696 and discussed the final paper (to include expected writing style and format) and project presentation. Dan covered the significance of basic MSDOS understanding, faculty mentoring responsibilities, and the intent to support middleware and implement SAN solutions. He also discussed the *TrackIT* application and how to employ it in support of system requirements. We closed with some comments on moving toward an MSCIT portal that would support students, faculty, and staff alike.

January 16, 2003: Colorado Springs (4 hours/21.5 total)
Full NLP group gathered: Bob Bowles (Advisor); Sonny Cordova (Tier II/III); Tim Krueger; Paul Mackenzie; Jim Reid; Beverlie Ascher; and myself. We discussed administrative matters (meeting time and project prioritization), then discussed ghosting and familiarized ourselves with basic Windows 2000 functionality. We created our domain administrative accounts and finalized project assignments (mine will be security and hopefully backing Tim on the firewall implementation).

January 23, 2003: Colorado Springs (3.5 hours/25.0 total)
Bob Bowles opened the weekly CS meeting with a discussion on project proposals. We then walked through the Ghost Server setup and moved on to review how the BelArc Advisor tracks the CS Lab equipment listing. Led by Sonny, we looked at the network connections. Since the connection out showed us to be down, we powered up the servers and successfully pinged. We moved on to do some basic cable management as the server closet wiring was in poor condition. We hooked up the KVM switch to our three servers (PDC, Primary Domain Controller; Ghost; and MS Exchange), and subsequently installed the *Smoothwall* firewall.

January 30, 2003: Colorado Springs (3 hours/28.0 total)
We worked on ensuring automatic update of the Macafee antivirus software DAT files on a weekly basis. We first attempted to do so by pointing the clients to a shared folder that we created on the PDC, but this failed to function properly. We then used the VirusScan console to attempt to have the clients utilize ftp to go out through the network to ftp.nai.com/virusdefs.4x for automatic updates. This effort appeared to be successful, and we scheduled the weekly update to occur at 12:00 on Sundays.

February 06, 2003: Colorado Springs (2 hours/30.0 total)
We attempted to work some ghosting, but were unable to log on to the ghost server due to an incorrect password. Upon checking the antivirus automatic update, we discovered that it had indeed updated at 12:00 Sunday as programmed. As we scanned the software load on the PDC, we discovered that, according to our notes, Advance Server had been loaded 10/24/02; given a 120-day license, the software would be due to expire approximately 24 February.

February 09, 2003: Home (5 hours/35.0 total)
Reviewed previous project proposals for content and format. Drafted an NLP Project Proposal covering network security to send to Bob Bowles.

February 13, 2003: Colorado Springs (3 hours/38.0 total)
Accomplished screen captures for the NAI antivirus autoupdate and e-mailed it to all NLP members. I checked each of the client machines, and again each had successfully updated DAT files as of Sunday. Spent most of the evening researching Microsoft Windows 2000 security background documentation.

February 20, 2003: Colorado Springs (2.5 hours/40.5 total)
Again attempted to access the Ghost server, with no success. Sonny will work with Bob to see why we are encountering password trouble. A check of the software licensing and talks with Bob indicate that we are in no danger of software expiration at this time (given that we are working off of student licensing). NAI antivirus check still good on all clients; Macafee is updating both DAT files and engine version. Sonny assisted me in reviewing where domain security policy applications reside within MS Active Directory.

February 27, 2003: Colorado Springs (2.75 hours/43.25 total)
Continued to review pertinent security policy doctrine. Located and reviewed extremely helpful tutorial from Sans.org titled "How to Bootstrap Information Security in Your Organization." Very thorough yet basic white paper. We logged on to the *Smoothwall* firewall and reviewed its default settings. We attempted to log on remotely from the green (internal) side with no joy.

March 08, 2003: Lowell (6 hours/49.25 total)
Led off with campus overviews and discussed accessing *SharePoint*. Outstanding guest lecture on "Thin Infrastructure" by Mr. Morten Roising of NCD and Mr. Mike Wright of Global Village. Very clear and thoughtful look at the promise of thin client computing.

March 25, 2003: Colorado Springs (3 hours/52.25 total)
Checked local (workstation #3) security policy to see what was in place. Spent the evening reviewing how Windows 2000 implements security policy via Active Directory (AD). Researched and read up on how security policy is implemented at the hierarchical Organizational Unit (OU), Domain, Site, and Local levels. AD employs an object-oriented approach to simplify policy management, grouping shared resources, user accounts, and domains, applications, services, and security policies as objects to be applied to the network.

April 01, 2003: Colorado Springs (7 hours/59.25 total)
Reviewed the Sans "Bootstrap" white paper. Began to outline requirements for a security policy (i.e., identification of what to protect, risk assessment, vulnerabilities, management "buy-in," user appreciation/understanding, accountability). Also reviewed several Microsoft "best practices" documents dealing with establishment of a sound security policy. Conducted further research on Active Directory structure/policy.

April 12, 2003: Lowell (6 hours/65.25 total)
Led off with campus updates. For CS, we mentioned having to reload MS Exchange due to a corrupt OS, but that we needed the key. Dan directed us to TrackIT. We also raised the Smoothwall configuration issue and whether the proxy should be on the server or the firewall. Jim Lupo mentioned that it came down to a disk space issue, and that the Denver Tech Center had initially used the proxy but found it difficult when any imaging was required. We remain unable to push a good Ghost image to date; Dan remarked that we should come up to DTC to observe how an image push is accomplished. Dan also covered how MSCN 696B/C work, and reiterated his earlier comments on the mechanics of the presentation itself.

April 15, 2003: Colorado Springs (4 hours/69.25 total)
Continued review of security best practices. Researched security account policies: passwords, lockout, and Kerberos. Studied AD application of domain-level security policy and how that policy is implemented in Windows 2000 environment down to the local accounts. Looked into local policies for the clients, but implementation of a security policy will be implemented at the domain level here at the CS Lab.

April 22, 2003: Colorado Springs (2 hours/71.25 total)
Personal research. Focused on CERT recommendations for implementing security policy in the Windows environment. Found a helpful document in the "tech_tips" section of the CERT website that provides information on the changes Microsoft made in the move from Windows NT to Windows 2000. Information deals mainly with the transition to Active Directory and the Distributed File System along with Kerberos and improved file/folder encryption.

April 29, 2003: Colorado Springs (1.75 hours/73.0 total)
Continued to research MS security configuration and study CERT documentation for MS Win 2000 security policy. Called up current Domain Policy settings on Domain Controller; as I assumed, all settings were to default Windows 2000 "factory settings," indicating that I'll be starting with a clean slate. I have now drafted a set of security policy criteria for the domain settings; will review with Sonny prior to implementation to ensure I'm not making changes that will cause difficulties for those accessing the network.

May 06, 2003: Colorado Springs (3.25 hours/76.25 total)
Implementation! Began by sitting down with Sonny and logging on to the PDC. I stepped through the various domain security settings and made my recommended adjustments to the defaults. Specifically, implemented password (history/age/minimum age/minimum length/complexity/reversible encryption), account (lockout duration/threshold/reset account), and Kerberos settings. Must have done my homework – Sonny concurred with all recommendations. A small step for him, but a giant leap for me!

May 10, 2003: Lowell (6 hours/82.25 total)
Monthly business meeting in Denver. Commenced with standard campus updates, followed by a good network reconnaissance brief by Jeff. Jeff covered nmap utility (for looking at the network's open ports, and what we should be seeing from both TCP as well as UDP port activity. Interesting discussion on running open ports from behind the firewall and ensuring they are blocked to outside traffic. Dan then covered the nGen Vlab Enterprise Architecture and access to the server farm to allow students to practice bringing up services, loading, and administering to the network. Dan also briefed the progress in SAN technology, stressing the fact that SAN is a network to itself, with intelligence built-in. He mentioned IPSAN and its limitations and applications. Network Area Storage (NAS) and SAN combination provide a good way of looking at both active storage and archival storage of data.

May 15, 2003: Colorado Springs (3 hours/85.25 total)
Had to change my password at logon….which is good, because it means my password setting changes have taken effect. While researching other security issues, I realized that, while we have implemented automatic update of the Macafee antivirus DATs and engine, we have not yet set the clients to run an autoscan. Sure enough, autoscan data is not enabled. I consider this to be an important element of an overall security policy, so I will take this item for action and provide the other NLP students with a set of screen captures allowing them to easily complete an autoscan setting for their client PC.

June 12, 2003: Colorado Springs (3 hours/88.25 total)
Back from leave….where was I? Ah, yes – autoscan setup. Worked the screen captures to walk through the setup; given low turnout tonight, I will try to accomplish as many of the PC updates as possible on my own. Ended up batting .500 – completed workstations 3, 5,6, and 7. Paul was using 2 all evening; on 4 I received a "config32.exe" error; 8 shows no NAI application even loaded to the machine; and 9 appears not to be connected to the CS domain. Will revisit these four workstations next week.

June 14, 2003: Lowell (5 hours/93.25 total)
Campus updates as lead item. Discussed pending 696B registration and my pending three-month absence (TDY to Norfolk) with Dan. Dan advises me to register for CS 696B course, but not attend, and he will deal with issue later. Mentions not to worry about the "F" I'll receive, and that he will take care of it. We spent most of the morning looking at the network architecture with an emphasis on firewall implementation and use of encryption. Variety of implementations: the DTC is going with a packet filter; Broomfield with a Shorewall, and CS and Fort Collins with Smoothwall firewalls. Phase One of the implementation incorporates a VPN between the DTC, Broomfield, and the Adult Learning Center; Phase Two will extend the VPN to CS and Fort Collins. Dan and Jim covered the implementation of wireless APs at the ALC. Some good news: CS will apparently receive some new PCs in the near future that will be a modest upgrade from those we now employ at the Lab!

June 19, 2003: Colorado Springs (2 hours/95.25 total)
First item of the day was to check the status of the weekly antivirus scan to ensure it was successful on the four PCs I completed earlier. Check of the VirusScan console showed scans of the hard drives had occurred as scheduled. Still no joy with the remaining PCs; Sonny's recommendation is to not bother with the final four, given that we will soon be replacing the PCs altogether and will therefore need to reconfigure the autoscan anyway. Spent some time reviewing security registry settings.

June 26, 2003: Colorado Springs (2 hours/97.25 total)
Checked the autoscan again; antivirus autoupdate and autoscans both running smoothly on configured machines. I noted a couple of screen capture errors I had made in the autoscan process and corrected them to ensure new PCs would be properly configured when the time comes.

July 18, 2003: Norfolk, VA (5 hours/102.25 total)
Research: Internet Explorer Security Zone settings

July 19, 2003: Norfolk, VA (5 hours/107.25 total)
Research: Domain Policy and Security Settings

July 27, 2003: Norfolk, VA (3.25 hours/110.5 total)
Research: Windows 2000 Server baseline security

August 03, 2003: Norfolk, VA (4.5 hours/115.0 total)
Research: Internet Explorer and active script issues

August 10, 2003: Norfolk, VA (4.0 hours/119.0 total)
Research: Administrator and Guest Account issues

August 16, 2003: Norfolk, VA (4 hours/123.0 total)
Paper organization, Outline

August 17, 2003: Norfolk, VA (3 hours/126.0 total)
DRAFT – Title, Front Matter

August 23, 2003: Norfolk, VA (3.25 hours/129.25 total)
DRAFT – Chapter 1

August 24, 2003: Norfolk, VA (4.5 hours/133.75 total)
DRAFT – Chapter 2

August 30, 2003: Norfolk, VA (4.0 hours/137.75 total)
DRAFT – Chapter 3

August 31, 2003: Norfolk, VA (4.25 hours/142.0 total)
DRAFT – Chapter 4

September 06, 2003: Norfolk, VA (5.0 hours/147.0 total)
DRAFT – Chapter 4

September 07, 2003: Norfolk, VA (3.5 hours/150.5 total)
DRAFT – Chapter 4

September 20, 2003: Norfolk, VA (5.0 hours/155.5 total)
DRAFT – Chapter 5

September 21, 2003: Norfolk, VA (4.25 hours/159.75 total)
DRAFT – Journal Log

September 27, 2003: Norfolk, VA (3.5 hours/163.25 total)

DRAFT – Journal Log

September 28, 2003: Norfolk, VA (5 hours/168.25 total)
DRAFT – Appendices (screen captures)

October 04, 2003: Colorado Springs (4.5 hours/172.75 total)
DRAFT – Chapter 4

October 12, 2003: Colorado Springs (3.75 hours/176.5 total)
Review of MLA Handbook: writing style, citing references

October 18, 2003: Colorado Springs (4.0 hours/180.5 total)
DRAFT – Works Cited (bibliography)

October 26, 2003: Colorado Springs (4.0 hours/184.5 total)
EDIT – Chapters 1 and 2

November 02, 2003: Colorado Springs (3.75 hours/188.25 total)
EDIT – Chapters 3 and 5

November 09, 2003: Colorado Springs (5.25 hours/193.5 total)
EDIT – Chapter 4