# A Risk Assessment Approach to NT Security

Glenn Davis, Sept 2000

> "*Testing can be used to show the presence of bugs, but never to show their absense*" Edsger Dijkstra

## Abstract

New security vulnerabilities and exploits are announced daily, even hourly, but generally do not provide any information regarding the risk. Where risk assessments are provided, the risk is often understated (usually by vendors) or do not apply to the specific environment under consideration. To exploit a vulnerability three conditions must exist: a security flaw and exploit, a vulnerable system, and someone to take advantage of these conditions.

Security is a chain; it's only as secure as the weakest link. Identification of security risks and using a standardized process to assessing risk based on the business environment, permits prioritization of risks and solutions focusing on the weak links. This process is commonly referred to as a security audit. System auditing is part of a continuous improvement life cycle. The characteristics of audits are: quantifiable, consistent, repeatable, and independently verifiable. An audit process usually includes identifying: where are we now, where do we need to be, and how do we get there. [Halprin]

This paper describes a process with these characteristics, and provides an sample implementation.

## Process

The process in this paper is based on a continuous improvement system lifecycle: identify the problem, evaluate the risk and decide to accept it or fix the problem, repair the vulnerability, assess effectiveness of repair, and feedback learning's into policies and procedures.

Systems should be built based on specific configuration guidelines based on best practices, which are in turn based on company security policy. The guidelines should be specific, step by step, procedures for configuring new systems and all systems should be built to standard. Maintaining standard configurations reduces management overhead, and decreases the probability of a system being vulnerable to attack. On the other hand, if a vulnerability is detected, all systems are at risk.

Identification of risk or vulnerability is the first step in the improvement cycle. Information sources include: vendor security mailing lists, hacker or full disclosure mailing lists, incident handling services such as CIAC, CERT, or FIRST, security conferences, SANS mailing lists, the news media, and security web sites. System administrator and security professionals must keep an ear to the ground for security problems that will affect their company or systems to provide proactive response to the threats.

After discovering a problem the next step is to assess its potential impact, by performing a situation appraisal and risk assessment. The purpose of a situation appraisal is to clarify the issues, break down complex problems into more manageable form, and a brief review of the existence of vulnerable or potentially compromised systems. It may take the form of an adhoc individual decision, or formal process involving a group. The analyst who identifies a security risk may decide that the organization is not vulnerable due to the absence of the software in the company, or knowledge that the flaw has already been patched. If there exists a potentially vulnerable system, then a risk assessment should be performed.

A risk assessment evaluates the risk to the organization, identifies corrective actions, and business impact of implementing corrective actions. After corrective actions are implemented, an assessment of the veracity of the repair should be performed and the system configuration guidelines and policies should be reviewed and updated as required.

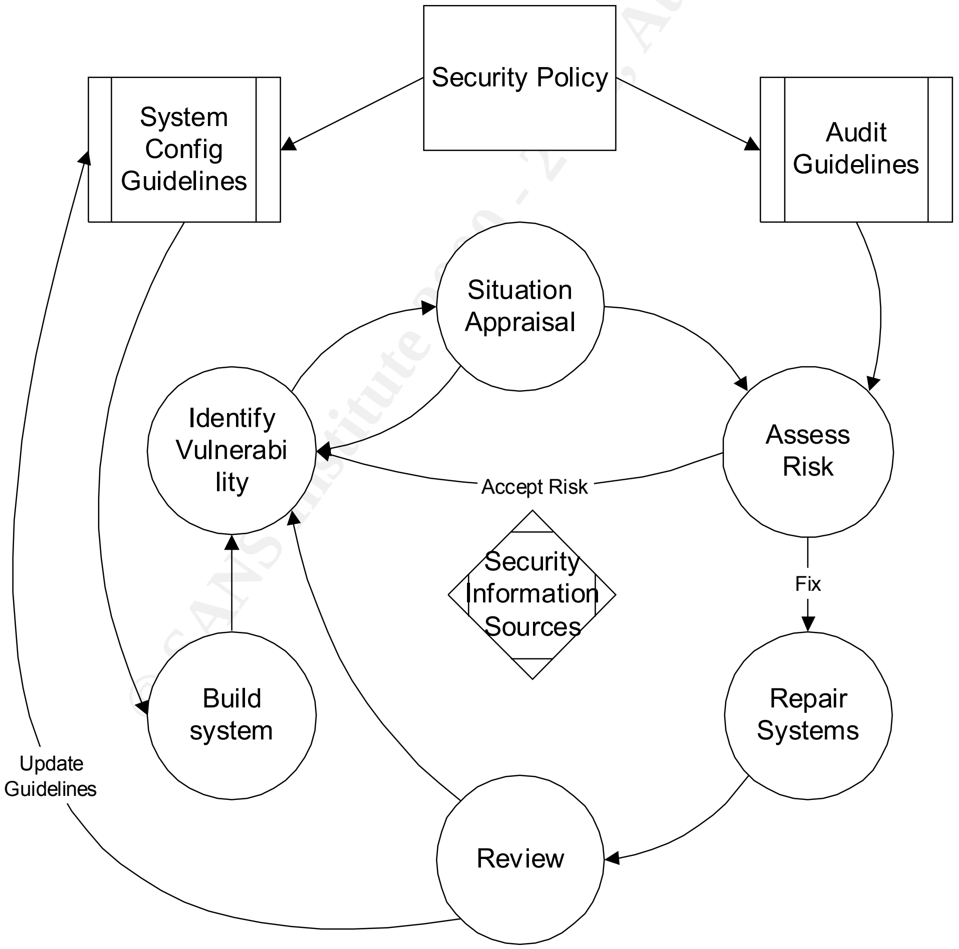


Figure 1: Continuous Improvement Life Cycle

## Risk Dimensions

Risk is a measure of potential loss that considers both the magnitude of a loss and the probability of it occurring. [Kepner] One approach to quantifying risk is to assign values to impact and probability then calculate the product of the impact of a risk, or the magnitude loss, and the probability of it's occurrence.

Risk Controls are measures that reduce or control risks that have been identified through a risk assessment. There are several types of risk controls: preventative, protective, contingent, corrective, and interim. A preventive action is any action that prevents an incident from occurring. Protective actions reduce the impact of a potential loss, contingent actions alters the outcome of a failure once it has occurred, corrective actions permanently addresses a risk, and interim actions partially address a risk before longer term measures are implemented.

The decision to implement specific solutions should be based on business principles balancing acceptable risk against cost and how much the control reduces risk. Acceptable risk is usually based on industry best practices, prior experience, and other existing risks. After control measures have been applied, the residual risk is the level of risk remaining.

### Measuring impact and probability

It is very difficult to obtain exact probabilities for the occurrence of a system compromise, and each situation is unique. A $10M cost may be an extreme risk for one company, but acceptable to another; if the probability of the risk occurring is one in a million/year, then spending $10M/year to reduce the impact makes little business sense.

Grouping probabilities and impacts into five categories makes estimation somewhat easier. A standard template that takes into consideration the business environment should be developed by each organization. It is important to document risk assumptions so that a consistent approach can be used to evaluate all risks. This facilitates quantifiable, and repeatable, decisions so that when comparing different risks solutions are chosen that provide the best overall cost benefit result.

The risk impact table reflects the type of business, and could also include measures for: environmental damage (e.g. computerized pollution control systems), adverse publicity, industrial espionage, or physical harm to individuals (e.g. medical systems, air traffic control).

| | **Risk / Impact** | | | |
|---|---|---|---|---|
| | **Confidentiality** | **Integrity** | **Availability** | **Cost** |
| **1** | Internal company telephone list | non-critical or honeypot system compromised | 1 minute outage | < $10K |
| **2** | Disclosure of non-critical email | | 1 hour outage | $10K |

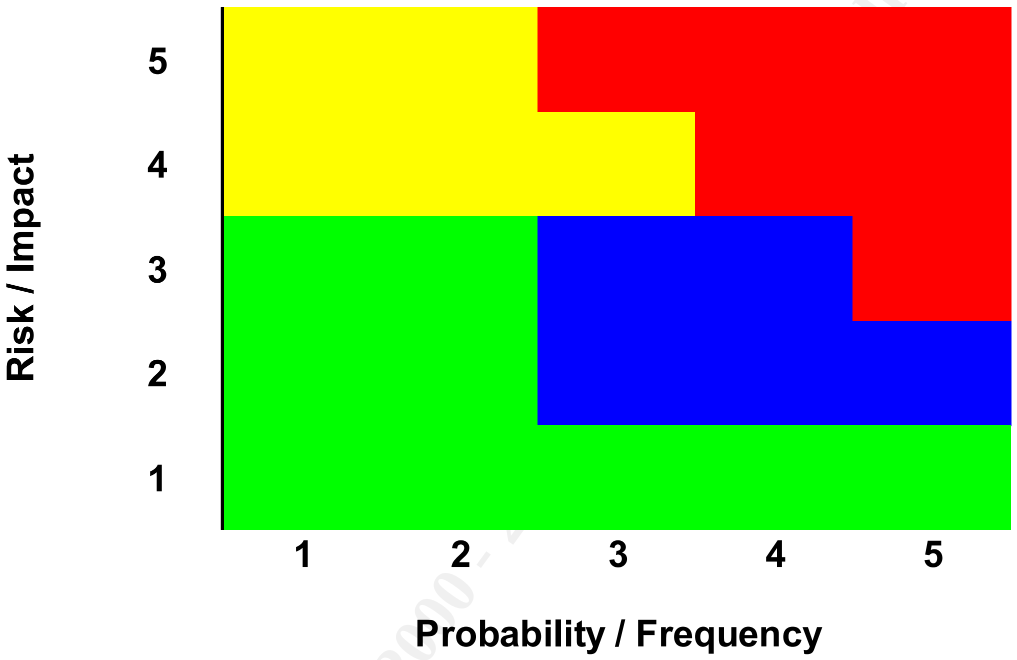
|  | Risk / Impact |  |  |  |
|---|---|---|---|---|
|  | **Confidentiality** | **Integrity** | **Availability** | **Cost** |
| **3** | Encrypted passwords copies | Non permanent data loss – recovery from backup required. | 1 day outage, or single system | $100K |
| **4** | Disclosure of personnel records, Credit cards, etc. | Backups destroyed, unauthorized modification of data. | 1 week outage, | $1M |
| **5** | Exposure of strategic business advantage information | Full system compromise; with destruction of data and backdoor access. | > 1 month outage, or several systems affected | > $1M |

Useful metrics for estimating the probability of occurrence of the successful exploitation of a security vulnerability are: exploit phase, system environment, and estimates on frequency of successful exploit. The exploit phase describes the lifecyle of a vulnerability in terms of window of exposure. The window opens with the discovery of an exploit, closing when all vulnerable systems have been patched. [Schneier] System connectivity and configuration has a large impact in estimating probability. For example: a system not connected to a network is far less likely to be attacked than one connected to the Internet.

|  | Probability / Frequency |  |  |
|---|---|---|---|
|  | **Exploit Phase** | **System connectivity** | **Probability** |
| **1** | Before the vulnerability is discovered. The vulnerability exists, but no one can exploit it. | System not connected to a network, or has very restrictive connectivity. | Exploit occurs less than once in 10 years or more. |
| **2** | After the vulnerability is discovered, but before it is announced. Few people know about the vulnerability, no one knows to defend against it. | System with dialout modem only | Unlikely to occur during life cycle of system. |
| **3** | Vulnerability is publicly announced. More people learn about the problem, the risk increases. | Perimeter defense, host based IDS, virus protection with current pattern file | Exploit may occur at least once in life cycle of system (typically once in 3 years). |
| **4** | Automatic attack tool to exploit the vulnerability publicly available; number of people who can exploit it grows exponentially. | System located behind perimeter defense. | May occur several times during life cycle of system or at least once per year. |
| **5** | Vendor has issued a patch, but patch not yet installed. | System is visible from the Internet. | May occur repeatedly during life cycle of system or at least once per month. |

## Calculating Risk

The following table shows the calculation of a risk value based on impact and probability values. The risk values are used to decide if controls will be implemented, and determine the effectiveness of a control based on how much a control reduces the risk. This risk value is sometimes referred to as annual loss expectancy (ALE) in the literature.



| | | |
|---|---|---|
| 🟥 | 4 | Extreme Risk - unacceptable |
| 🟨 | 3 | High impact risk - MUST implement risk controls |
| 🟦 | 2 | Moderate Risk - may require some controls |
| 🟩 | 1 | Low Risk - Some risk controls may still be justified |

### Example Risk Assessment

| Problem | Impact | Prob. | Risk |
|---|---|---|---|
| User and administrative accounts could be compromised by password cracking program. | 5 | 4 | 4 |

The assessment identified the risk level as extreme, or unacceptable; measures to reduce the risk level are mandatory.

| Actions | Resid. Impact | Resid. Prob. | Resid. Risk |
|---|---|---|---|
| **Preventative (decrease probability)**: | | | |
| • Virus scanners that detect password crackers | 4 | 1 | 3 |
| **Protective (decrease impact)**: | | | |
| • Disable profile caching to limit number of accounts compromised | 3 | 4 | 2 |
| • Remove login over network right for admin accounts | 2 | 4 | 2 |
| • Secure SAM database (NTFS permissions, repair disk, don't run IIS on a domain controller) | 3 | 4 | 2 |
| • Enable 128-bit encryption of passwords in SAM | 3 | 4 | 2 |
| • Enforce password quality rules, password expiry, and account lockout. | 1 | 4 | 1 |
| • Implement a good password policy | 2 | 4 | 2 |
| • Enforce NTLMv2 to make password cracking more difficult (Disable LANMAN authentication) | 1 | 4 | 1 |
| **Contingent (alters outcome)**: | | | |
| • Limit physical access to domain controllers | 3 | 3 | 2 |
| • Different admin and user accounts for sysadmins | 3 | 3 | 2 |
| • Rename Administrator account | 3 | 3 | 2 |
| **Corrective (permanent fix)**: | | | |
| • None – all passwords are crackable given sufficient time. | | | |
| **Interim**: | | | |
| • Audit account usage for unusual patterns | 3 | 4 | 2 |
| • Install host based intrusion detection system on domain controllers | 3 | 3 | 2 |

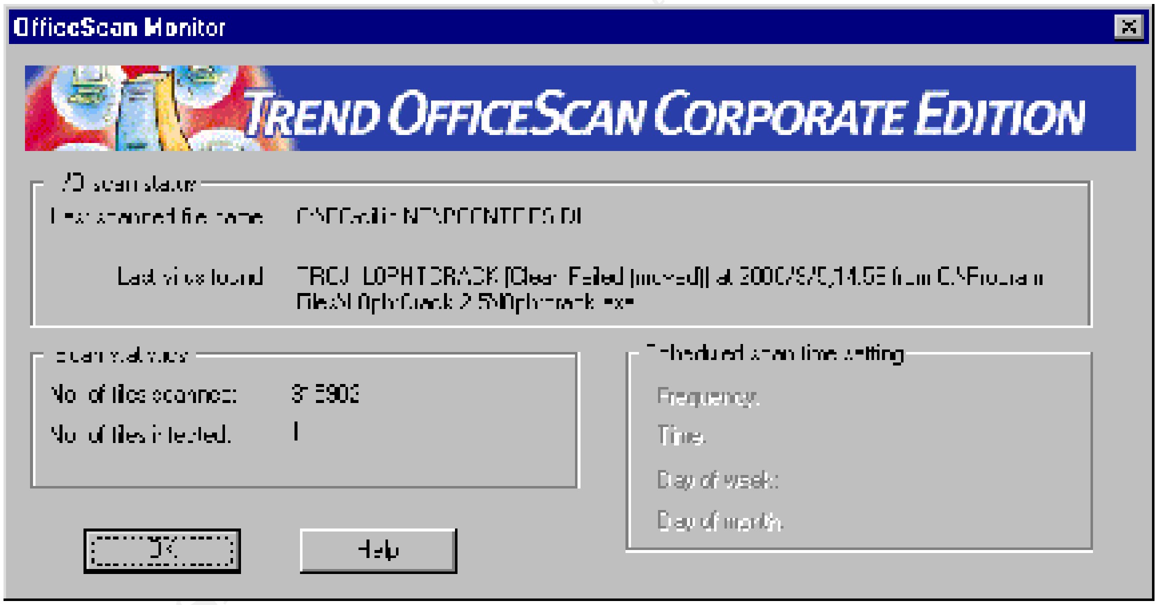
The actions that provide the greatest risk reduction are: enforcing a good password policy, and implementing better encryption to protect the passwords.

**Virus scanners that detect password crackers**

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Estimated software cost of $20/system/year and 8 admin person-hours/system/year | 4 | 1 | 3 | 1 |

This control significantly reduces the probability that a password cracker will be run. However, the password could still be cracked by: disabling the virus scanner by booting from a floppy, obtaining a copy of the hashed passwords, and then running the password cracker on a different machine. It does not reduce the impact of passwords being cracked, which results in a decrease in risk by one and therefore the effectiveness of this control is rated LOW.

Virus scanners, such as TREND OfficeScan, can find L0ftcrack and other password crackers. By using the appropriate scanner, and reviewing the scanner logs you can determine if a password cracker has been installed. Best practices for managing virus scanners are: ensure a virus scanner is running on each desktop machine, password protect the application to prevent users from stopping the virus scanner, set the action on detect to prevent access to the file and report the violation to system administrators.



I/O scan status

Last scanned file name: [illegible]

Last virus found: TROJ_L0PHTCRACK [Clean Failed (moved)] at 2000/8/5,14:53 from C:\Program Files\L0phtCrack 2.5\l0phtcrack.exe

Scan statistics

No. of files scanned: [illegible]

No. of files infected: 1

Scheduled scan time setting

Frequency:

Time:

Day of week:

Day of month:

Figure 2: L0phtcrack password cracker discovered by Trend OfficeScan

Tools like lsadump and L0phtcrack can be used to identify which accounts have been compromised. If the data files have been removed from the system, forensic tools like "undelete" or "Expert Witness" may be used to examine the contents of deleted files.

### Disable profile caching to limit number of accounts compromised

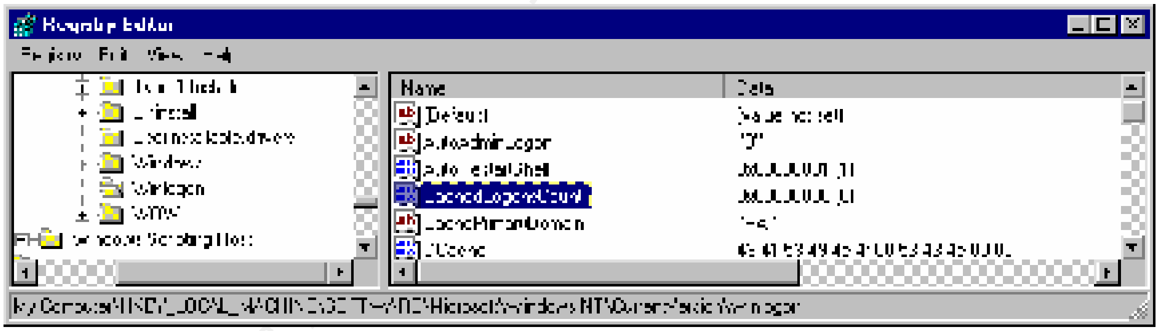
| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Prevents laptop users from logging on when not connected to network, and prevents users from logging in when network or system problems prevent access to domain controller. | 3 | 4 | 2 | 2 |

Disabling profile caching has a MEDIUM effectiveness because risk level is reduced to moderate through decreased impact. The probability of a password cracker being run does not change, but there will be no cached passwords stored on the disk to crack. This action should not be implemented on laptops, as it limits their usability.

By default, NT caches the logon credentials for the past 10 users who logged on interactively. The purpose of this functionality is to let a user still log on to the system even if you disconnect the system from the network or if the domain controllers are unavailable.

To disable credential caching, change the CachedLogonsCount entry (type REG_DWORD, value 0) in:

HKEY_LOCAL_MACHINE\SOFTWARE Microsoft\Windows NT\CurrentVersionWinlogon Registry key.



| Name | Data |
|---|---|
| (Default) | (value not set) |
| AutoAdminLogon | "0" |
| AutoRestartShell | 0x00000001 (1) |
| CachedLogonsCount | 0x00000000 (0) |
| DefaultDomainName | [illegible] |
| DCache | 45 41 53 49 45 4[illegible] |

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Figure 3

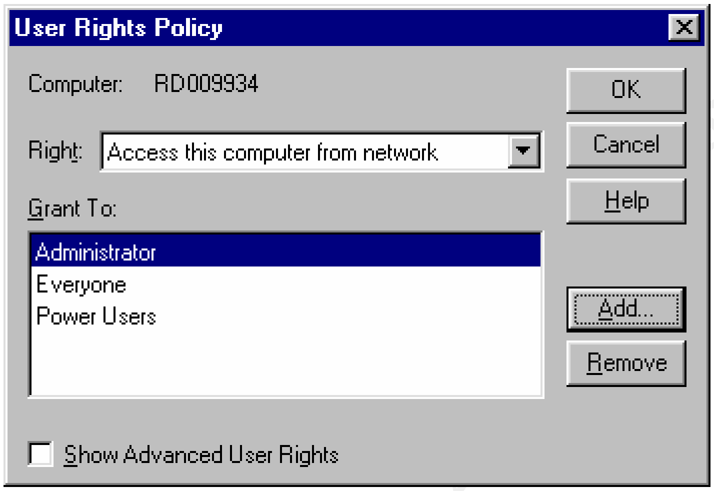
### Remove login over network right for admin accounts

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Increased administration overhead. | 2 | 4 | 2 | 2 |

This action has a MEDIUM effectiveness because it decreases the impact of administrator accounts being cracked. However, implementation may not be possible due increased system management overhead because remote administration is not more difficult.

Using “User Manager”, “Policies”, “User Rights”: remove the “Administrator account from the list of users granted “Access this computer from the network”.

Before


User Rights Policy

Computer: RD009934

Right: Access this computer from network

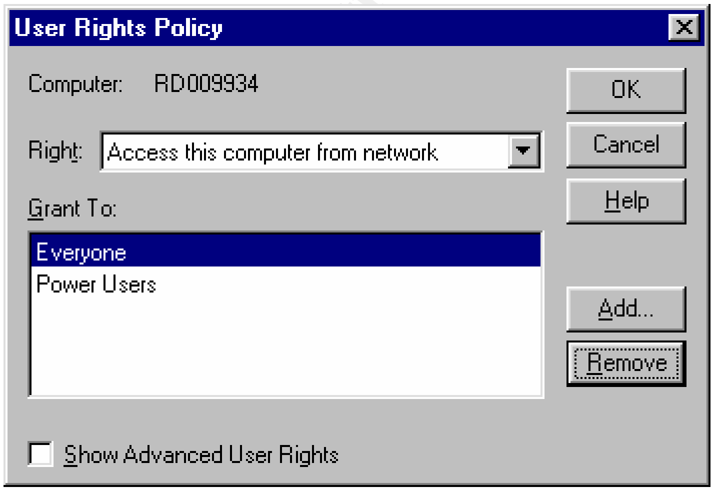
Grant To:

- Administrator
- Everyone
- Power Users

□ Show Advanced User Rights

Figure 4: List of users with network access rights

After


User Rights Policy

Computer: RD009934

Right: Access this computer from network

Grant To:

- Everyone
- Power Users

□ Show Advanced User Rights

Figure 5: Remove network access right from Administrator

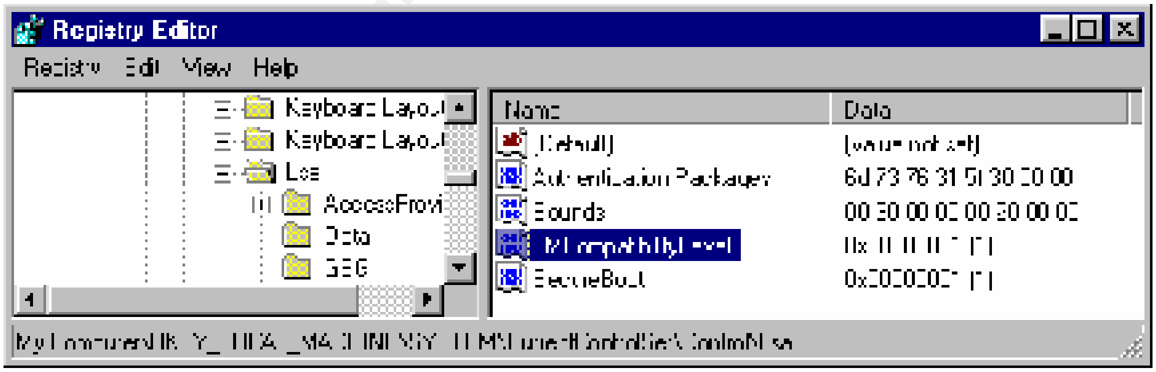
**Enforce NTLMv2 to make password sniffing more difficult**
**Disable LANMAN authentication**

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Require registry setting on all systems, and will result in interoperability problems with non SP4 NT systems and windows 95/98. | 1 | 4 | 1 | 3 |

This is a highly effective control because better encryption makes cracking passwords much harder, compared to cracking the LANMAN hash. However, this only protects password sniffing, not cracking the SAM. Due to interoperability problems the safest setting is to attempt NTLMv2 authentication first, but fall back to LANMAN and NTLMv1 if NTLMv2 is not accepted by the server.

Settings for HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel are:

| Value | Client | Domain Controller |
|---|---|---|
| 0 | Default. Send LANMAN and NTLMv1 | Accept NTLMv2 if requested |
| 1 | Try NTLMv2, but fallback to LM and NTLMv1 | Accept NTLMv2 if requested |
| 2 | NTLMv1 only | Accept NTLMv2 if requested |
| 3 | NTLMv2 only | Accept NTLMv2 if requested |
| 4 | NTLMv2 only | Refuse LANMAN, accept NTLMv1 or NTLMv2 |
| 5 | NTLMv2 only | Accept only v2 (refuse LANMAN and NTLMv1) |



| Name | Data |
|---|---|
| (Default) | (value not set) |
| Authentication Packages | 6d 73 76 31 5f 30 00 00 |
| Bounds | 00 30 00 00 00 20 00 00 |
| LMCompatibilityLevel | 0x00000001 (1) |
| SecureBoot | 0x00000001 (1) |

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

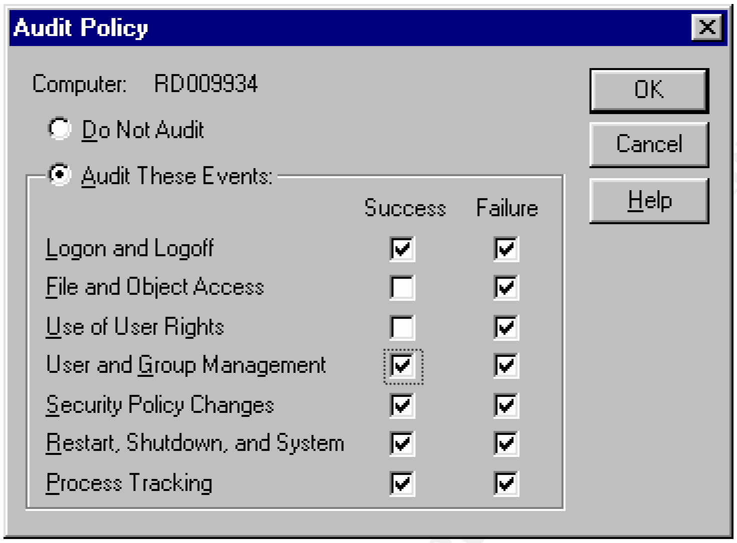
Figure 6: Set compatibility level to try NTLMv2, but fallback to LANMAN/NTLMv1 if required

**Audit account usage for unusual patterns**

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Increased effort to monitor audit logs. | 3 | 4 | 2 | 2 |

Auditing account usage has a MEDIUM effectiveness in controlling password cracking problems.

Logging of logon and logoff events, including password failures, can be turned on by setting the audit policy for a machine. This may be performed manually on the domain controllers, or preferably by using the security configuration editor, SCE.



Computer: RD009934

○ Do Not Audit

● Audit These Events:

| | Success | Failure |
|---|---|---|
| Logon and Logoff | ☑ | ☑ |
| File and Object Access | □ | ☑ |
| Use of User Rights | □ | ☑ |
| User and Group Management | ☑ | ☑ |
| Security Policy Changes | ☑ | ☑ |
| Restart, Shutdown, and System | ☑ | ☑ |
| Process Tracking | ☑ | ☑ |

Figure 7: Enable auditing of account usage

Audit logs should be consolidated, and automated tools used to report discrepancies. Audit logs can be dumped into CSV format using tools like DUMPEL.EXXE from the Windows NT Resource Kit, or logged to a unix syslog host using Adiscon EvntSLog. (http://www.adiscon.com/) Other options are alerting to an enterprise network management tool like HP Openview using SNMP traps.

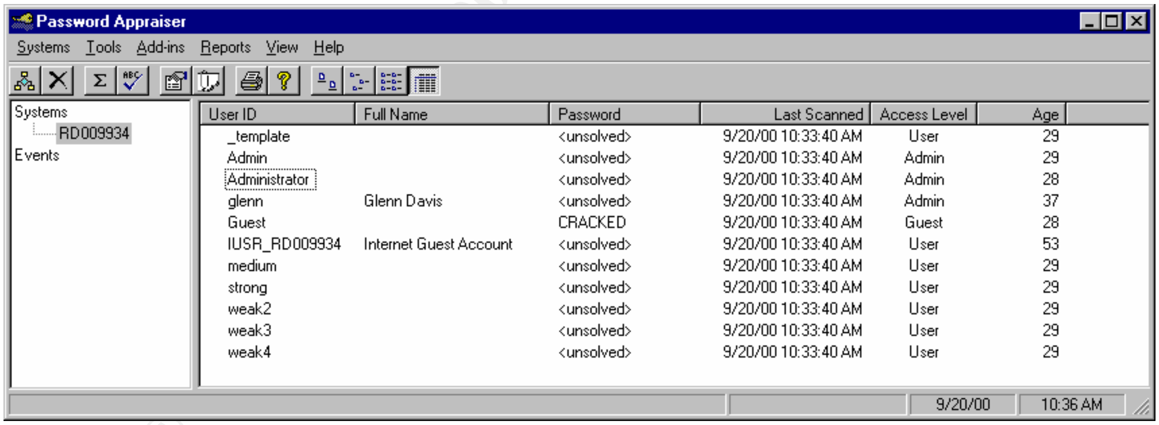
**Automate the enforcement of password complexity rules, password expiry, and account lockout**

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| User complaints that passwords are difficult to remember, and increased help desk calls to reset passwords. Requires installation of DLL and registry setting on domain controllers, and systems must be rebooted for change to take effect. | 1 | 4 | 1 | 3 |

Enforcing password complexity rules is a very effective control, rated HIGH due to the decrease in impact.

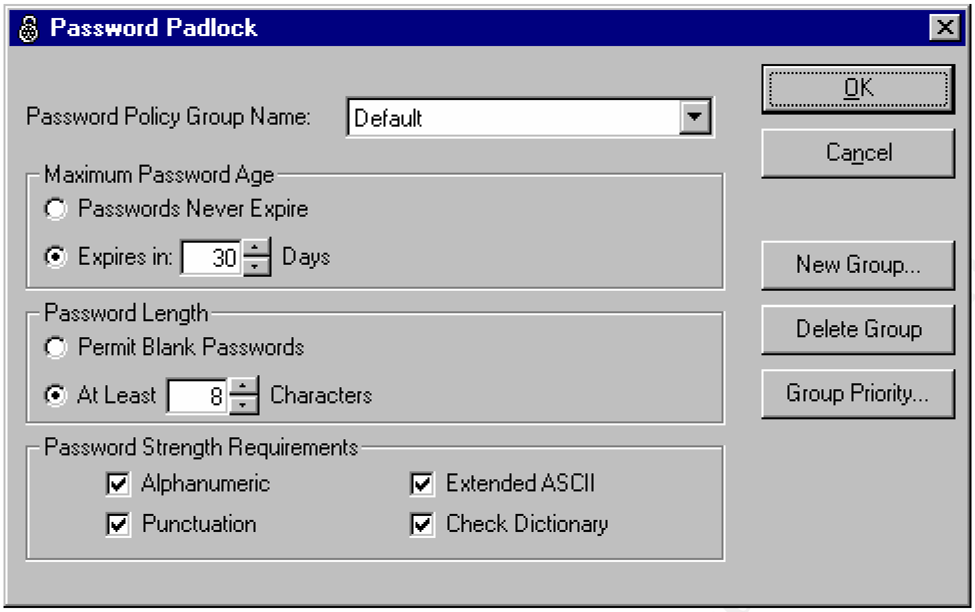
Microsoft provides a template passfilt.dll that enforces password quality by requiring: two of: uppercase, lowercase, numeric or special characters. While this is a good policy, a more restrictive policy could be implemented by modifying the template source code.

A better solution is to use a tool like Quakenbush password appraiser ( http://www.quakenbush.com/ ). Password appraiser permits setting of password policies based on the user level, administrators, or groups. Password strength may be selected based on: alphanumeric, punctuation, extended ASCII, and may also include a dictionary check . The length and age requirements can be set separately for each level of access. This tool will also find accounts with weak passwords and automatically respond by: sending an email, disabling the account, forcing password change on next logon, or a combination of these choices.



| User ID | Full Name | Password | Last Scanned | Access Level | Age |
|---|---|---|---|---|---|
| _template | | <unsolved> | 9/20/00 10:33:40 AM | User | 29 |
| Admin | | <unsolved> | 9/20/00 10:33:40 AM | Admin | 29 |
| Administrator | | <unsolved> | 9/20/00 10:33:40 AM | Admin | 28 |
| glenn | Glenn Davis | <unsolved> | 9/20/00 10:33:40 AM | Admin | 37 |
| Guest | | CRACKED | 9/20/00 10:33:40 AM | Guest | 28 |
| IUSR_RD009934 | Internet Guest Account | <unsolved> | 9/20/00 10:33:40 AM | User | 53 |
| medium | | <unsolved> | 9/20/00 10:33:40 AM | User | 29 |
| strong | | <unsolved> | 9/20/00 10:33:40 AM | User | 29 |
| weak2 | | <unsolved> | 9/20/00 10:33:40 AM | User | 29 |
| weak3 | | <unsolved> | 9/20/00 10:33:40 AM | User | 29 |
| weak4 | | <unsolved> | 9/20/00 10:33:40 AM | User | 29 |

Figure 8



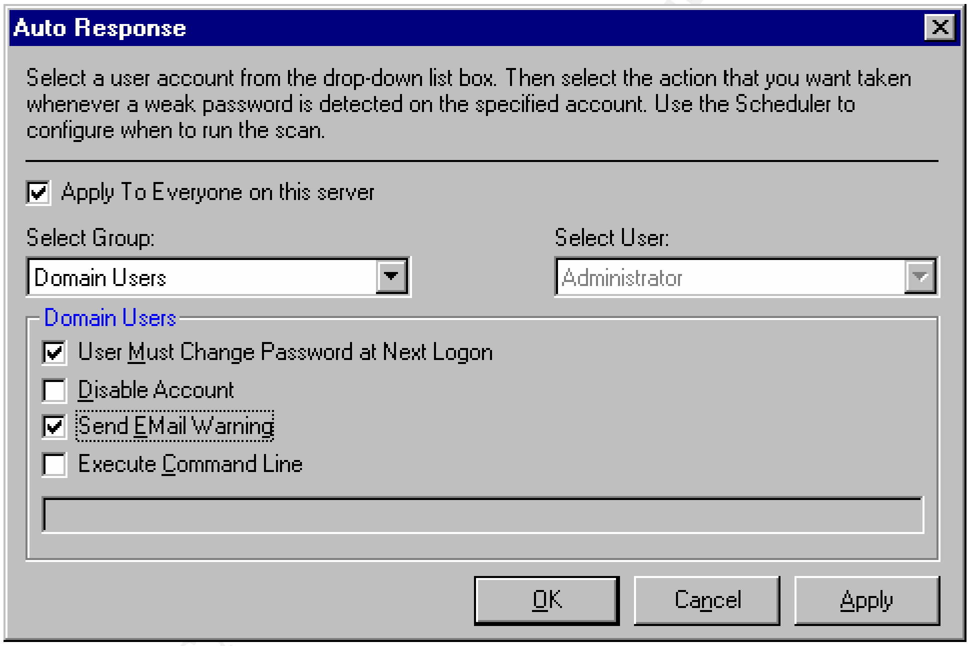
Password Policy Group Name: Default

Maximum Password Age
○ Passwords Never Expire
● Expires in: 30 Days

Password Length
○ Permit Blank Passwords
● At Least 8 Characters

Password Strength Requirements
☑ Alphanumeric ☑ Extended ASCII
☑ Punctuation ☑ Check Dictionary

Figure 9: Password characteristics, and expiry options



Select a user account from the drop-down list box. Then select the action that you want taken whenever a weak password is detected on the specified account. Use the Scheduler to configure when to run the scan.

☑ Apply To Everyone on this server

Select Group: Domain Users

Select User: Administrator

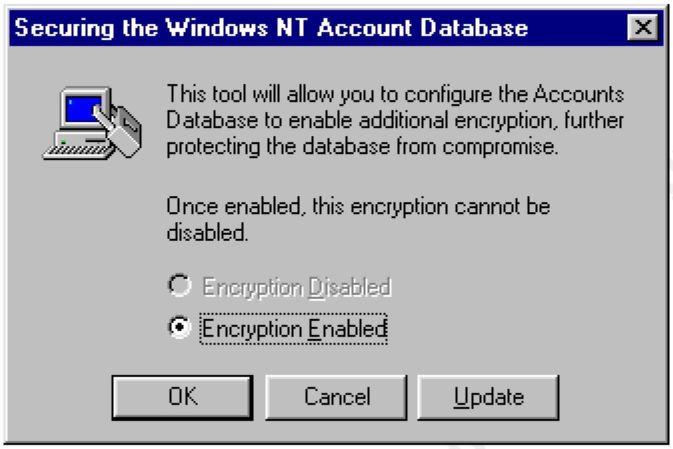
Domain Users
☑ User Must Change Password at Next Logon
□ Disable Account
☑ Send EMail Warning
□ Execute Command Line

Figure 10: auto response options available with Password Appraiser

### Enable 128-bit encryption of passwords in SAM using SYSKEY

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Requires visiting and rebooting each machine to be secured (domain controllers) and may make system recovery more difficult in the event of system corruption. | 3 | 4 | 2 | 2 |

SYSKEY is a moderately effective control, as it reduces impact by making passwords more difficult to crack. If attackers obtain a copy of your SAM database, they won't be able to extract valid password hashes. However the system key won't stop users logged on with administrative authority from dumping the SAM database into a crackable format using pwdump2 for use with tools such as L0phtCrack



Securing the Windows NT Account Database

This tool will allow you to configure the Accounts Database to enable additional encryption, further protecting the database from compromise.

Once enabled, this encryption cannot be disabled.

○ Encryption Disabled

● Encryption Enabled

Figure 11: Enabling system key

System key allows detection of an attack in which a bootable disk is to gain access to the system and moving the SAM database file, and rebooting the machine. When the system reboots, NT finds no SAM database and creates a new one with Administrator and Guest accounts with blank passwords. With system key when the machine boots it won't present the regular Logon dialog box.

**Implement password policy**

| Business Impact | R. I. | R. P. | R. R. | E. |
|---|---|---|---|---|
| Potential increased help desk calls for forgotten passwords. Some user complaints until the policy has been accepted as necessary. | 1 | 4 | 2 | 3 |

A good password policy is one of the most effective control for reducing impact of the use of password crackers. In combination with disabling LANMAN hashes, password cracking becomes time consuming.

Update policy manual with password best practices, for example:

- Use a password with mixed-case letters. Do not just capitalize the first letter; add uppercase letters in the middle of the password.
- Use a password that contains alphanumeric characters and include punctuation, where supported by the operating system.
- Use a password that can be typed quickly, without having to look at the keyboard. This makes it harder for someone to obtain a password by "shoulder surfing".
- Change passwords regularly. The more critical an account to network integrity (such as root on Unix host or Administrator on Windows NT), the more frequently the password should be. This change reduces the window of use for someone who has already compromised an account.
- DO NOT use a network login ID in any form (reversed, capitalized, doubled as a password.
- DO NOT use your first, middle or last name in any form. Do not use your initials or any nicknames you may have.
- DO NOT use a word contained in English or foreign dictionaries, spelling lists, or other word lists.
- DO NOT use other information easily obtained about you. This includes pet names, license plate, telephone numbers, identification numbers, the brand of your automobile, the name of the street you live on, and so on. Such passwords are very easily guessed by someone who knows the user.
- DO NOT use a password of all numbers, or a password composed of alphabetic only characters. Mix numbers and letters.
- DO NOT write a password on sticky notes, desk blotters, calendars, or store it online where it can be accessed by others.
- DO NOT reveal a password to anyone.
- DO NOT use shared accounts. Accountability for group access is extremely difficult.
- If account passwords have to be shared by a group of administrators, distribute the passwords in encrypted form (e.g. PGP)

**Assessment and Follow-up Actions:**

Actions that were identified, but not acted on were:

1. Update configuration guidelines to rename Administrator account
2. Different admin and user accounts for system administrators
3. Review virus scanner pattern files to be certain they can detect the most common password cracking programs.
4. Consider implementing a host based intrusion detection system.
5. Review physical security for NT servers, and implement access controls
6. Review file systems security.
7. Review IIS server security.

**Conclusion**

There will always be bugs in software, some of them leading to security vulnerabilities. A standard risk based process approach to security provides: clarity when selecting among competing solutions to a vulnerability, and it allows the prioritization of risks so that the weakest links in the security chain are addressed first.

## References

Fossen, Jason, J. Kolde, "*Securing Windows NT: Step-by-Step, Parts 1,2,3*", version 3.6, SANS conference notes, Ottawa, ON, Aug 2000.

Halprin, Geoff, "*A System Administrators Guide to Auditing*", #6 Short Topics in Systems Administrations, Willian LeFebve Ed., USENIX Association, July 2000.

Jumes, James G., Neil F. Cooper, Paula Chamoun, Todd M. Feinman, "*Windows NT 4.0 Security, Audit, and Control*", Microsoft Press, 1999.

Kepner, Charles H., Benjamin B.Trego, "*The New Rational Manager*", Princeton Research Press, Princeton, 1981.

McInerney, Michael, "*Windows NT Security*", Prentice Hall, 2000.

Osborne, Sandra, "*Windows NT Registry: A Settings Reference*", New Riders Publishing, 1998.

Schneier, Bruce, "*Secrets and Lies: Digital Security in a Networked World*", Wiley Computer Publishing, 2000.