Global Information Assurance Certification Paper

Auditing the RSA SecurID infrastructure

Option 1: An Auditors perspective

Karim Merabet

SANS GSNA Practical V2.1

September 5, 2003

Assignment #1 Research in Audit, Measurement Practice And Control

Identify the system to be audited

Abstract

The objective of this paper is to assess the security level of the SecurID infrastructure. A basic explanation of the RSA SecurID process can be found here:
http://www.rsasecurity.com/products/securid/whitepapers/AS51_SB_0203.pdf

Our primary goal is to audit the authentication protection level of the machine and to analyze the effectiveness of the SecurID ACE/Agent – ACE/Server framework. We will not deal with general Win2k hardening techniques (for both the server and agent stations) that are not related to OS passwords and OS password

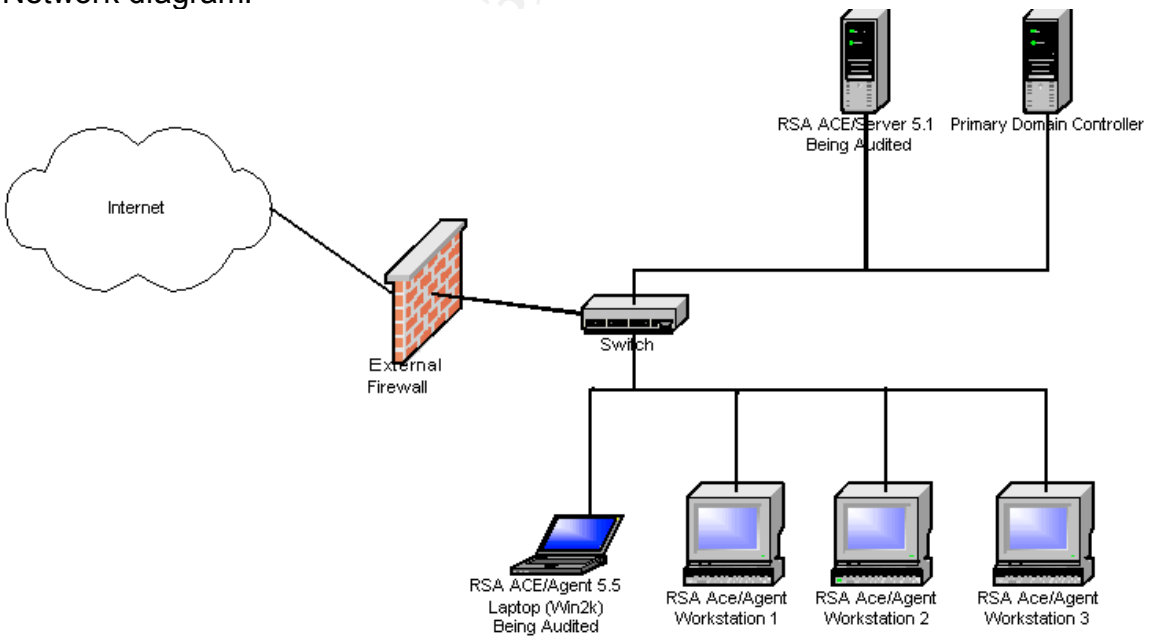
policies. OS password protection levels and OS password policies will be audited since they are part of the RSA SecurID authentication process. The SecurID process relies on proper implementation of OS level passwords as a last line of defense. We will also limit our client analysis to the RSA ACE/Agent software and will not deal with third party SecurID enabled clients.

General external network security measures (Firewall logs and rules, IDS sensor logs, etc…) will not be audited.

The audit will be restricted to two machines: An ACE/Agent client that is running Windows 2000 Pro SP3 with ACE/Agent version 5.5 and an authentication server running Windows 2000 Server SP3 with ACE/Server 5.1.

The ACE/Agent is mainly used as an Internet research machine and workstation. Its level of importance and security is considered to be the same as normal workstations in the enterprise. The ACE/Server is assumed to be a critical infrastructure device and its level of security should reflect this security level. The SecurID framework is currently protecting all network devices on the intranet including servers and workstations.

Network diagram:



Evaluate the risk to the system

These risks are divided into categories. They are all directly related to the SecurID infrastructure.

General Business related risks:

Risk: SecurID authentication is inefficient and critical documents are revealed.
Likelihood: The storing of sensitive information requires a high level of security. SecurID authentication is only one of many security measures required for proper handling of sensitive documents.
Consequence: Loss of information. Business plans could be revealed prematurely and cause a great deal of harm and hurt the reputation of the company.

Risk: Critical servers are improperly secured.
Likelihood: The Ace/Server is the most important server for access control and authentication in the enterprise. It is responsible for the two-factor authentication used by all servers and desktops. It is considered to be a critical system and its security level should reflect this status.
Consequence: Poor security in critical servers can lead to higher exposure to attack. These servers are essential to the well being of the network.

Physical access related risks:

Risk: Ace/Agent is stolen from the building.
Likelihood: General physical access controls are in place (sign-out forms and swipe cards, camera monitoring etc…). Unfortunately, some things are more at risk for theft than others.
Consequence: Ace/Agent contains sensitive information that might prove to be embarrassing. Trade secrets could be revealed if the machine is stolen.

Risk: Machine is rebooted with a boot diskette.
Likelihood: Gaining physical access to the machine is fairly easy for an employee with the proper credentials.
Consequence: Circumvention of the whole authentication procedure can allow an intruder full access to private documents on the system. On the Ace/Server, this could lead to corruption of the data and could lead to a complete lockout of all desktops and servers (a basic Denial of Service).

Implementation related risks:

Risk: The SecurID username is compromised
Likelihood: Medium: Malicious employee might see the username when it is being typed in.

Consequence: Minimal. The PIN will have to be broken. The impact should be minimal.

Risk: The SecurID token is compromised or lost
Likelihood: Medium: SecurID tokens can be lost or stolen.
Consequence: the compromised token will have to be matched to a Username and a PIN. If the token is lost without any other information, the impact will be small. A new token will be issued and the old one will be revoked.

Risk: The PIN is compromised
Likelihood: Low: Someone could see the PIN when it is being entered
Consequence: Without the SecurID token, the impact is low. If the Token is also compromised, then the impact will be high.

Risk: Easy SecurID PIN used
Likelihood: Medium: The Security policy should detail proper password creation methods.
Consequence: A weak PIN can be guessed or brute forced. A weak PIN reduces the effectiveness of the whole SecurID authentication process.

Risk: Network outage causes loss of connection to ACE/Server
Likelihood: Medium: Loss of connectivity to the authentication server is possible during network maintenance.
Consequence: SecurID Authentication cannot be completed and the station will be locked out.

Risk: Reserve password is too weak.
Likelihood: Reserve passwords are often used as a way to access the machine when the Ace/Server is unavailable. The Reserve password should be compliant with the password requirements detailed in the Security policy.
Consequence: A compromised reserve password would allow a malicious user free access to the machine. OS password authentication will have to be broken to get access to the machine.

Risk: Network Cable is unplugged while authentication is being performed
Likelihood: Medium: Possible due to random network outages.
Consequence: The authentication cycle will fail and access will be denied. If a reserve password is set, the fallback feature will be invoked.

Risk: ACE/Server Log reviews are sporadic
Likelihood: Low: Logs should be reviewed daily.
Consequence: important forensic clues could be missed. This will increase the exposure time to attack.

Risk: SecurID Level of Encryption used is poor

Likelihood: Low: SecurID uses IKE and MD5 or SHA1 hashes. These are known protocols and are considered to be sound.
Consequence: The machine could be compromised and passwords could be sniffed.

Operating System related risks:

Risk: Easy or non-existent OS passwords and weak password policies.
Likelihood: Medium: A sense on complacency might set in, and OS passwords might seem irrelevant to the users.
Consequence: SecurID does not protect Network shares. Administrator level passwords and user passwords should be protected even if SecurID is present.

Risk: Faulty installation of the ACE/agent.
Likelihood: Low: The Agent was not installed properly or not enabled on reboot.
Consequence: Complete lack of protection. This machines OS password can be guessed or brute forced.

Risk: Machine is infected with a virus.
Likelihood: Medium: The Ace/Agent or Ace/Server's anti-virus software is not current.
Consequence: a malicious hacker could uninstall the Ace/Agent or Ace/Server remotely.

Risk: Network shares are poorly implemented and secured
Likelihood: High: Network Shares are often used to transfer files.
Consequence: Potential loss of data and integrity. The SecurID infrastructure does not protect network shares.

Risk: null sessions connections are permitted
Likelihood: High: null sessions connections are available by default.
Consequence: Potential loss of data and integrity if the machine is easy to access. Potential hackers can gather important information with a null session.

Risk: Machine is running unnecessary services
Likelihood: High: A lot of unnecessary services are installed by default
Consequence: A known bug or exploitable service could allow the machine to be compromised. This will bypass any SecurID security measures.

Risk: Patching is not up-to-date
Likelihood: High: Users control their own desktop machines and are required to keep them up-to-date.
Consequence: An exploit could be used to compromise the machine. Personal documents and intellectual property could be revealed.

Network related risks:

Risk: Traffic is sniffed, and information is leaked.
Likelihood: High: Communication between the Ace/Server and Ace/Agent is intercepted.
Consequence: A user from a different department could gain some basic information on the network layout and amount of Ace/Agents deployed. The loss of information would be small, but could lead to more precise attacks. The location and number of Ace/Servers could be determined.

Malicious insider related risks:

Risk: A malicious user gains administrator powers.
Likelihood: The OS must be hardened properly. This will ensure that SecurID software will not be interfered with.
Consequence: The malicious user could use his new position to attack other machines on the network.

Risk: A malicious user changes critical SecurID files on the Ace/Agent
Likelihood: Medium: access to important configuration files is possible.
Consequence: If the Ace/Agent service crashes, the machine will be locked out.

Current State of Practice

Auditing of a SecurID infrastructure is nearly inexistent. SecurID infrastructure auditing is a new field and specific implementation information, not found on the RSA web site, was hard to find. A Search on Google (String: SecurID audit) resulted in general SecurID hits and nothing of great use for an actual audit of the infrastructure.

Here are some resources that can help the audit process in general:

Weaknesses in SecurID,
http://www.tux.org/pub/security/secnet/papers/secureid.pdf

A more general Cryptanalysis examination of the RSA protocol itself can be found here:

Cryptanalysis of RSA http://www.sans.org/rr/papers/20/1006.pdf

And some it's potential weaknesses
http://crypto.stanford.edu/~dabo/abstracts/lowRSAexp.html and
http://www.atstake.com/research/reports/acrobat/initial_securid_analysis.pdf

Sample request form for a SecurID token from the Governor's Office of Administration Commonwealth of Pennsylvania that details some user policies: http://www.oalansupport.state.pa.us/oalan/lib/oalan/doc/securid_remote_access_request_blank_form.doc

OS policy/password references:

OS policy/password audit tools and procedures are fairly well known and can complement the security benefits of SecurID. The OS password will become the last line of defense if SecurID fails. OS policies guide the way passwords are implemented in the OS.

The most famous auditing tool for windows passwords is L0phtCrack: (http://www.atstake.com/research/lc).

Auditing Windows 2000: Audit policies
http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9633

Windows 2000 Default Security Policy Settings
https://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGca.asp

ASSIGNEMENT #2 Audit Checklist

Checklist

Item #1: Physical Security

Reference: RFC2196 (http://www.faqs.org/rfcs/rfc2196.html), RUSecure http://rusecure.rutgers.edu/secplan/cklst.html

Control objective: Reduce the likelihood of theft or unauthorized physical access to the machines.

Risk:

Potential Threat: Theft or unauthorized external access to classified or sensitive data.

Threat level: Medium: Physical security is one of the most important and basic aspect of a defense in depth approach.

Likelihood: Theft of equipment can be common in the workplace if minimal physical security levels are not met.

Impact: The risk of losing expensive assets if theft becomes common can severely influence budgets and hinder productivity. Public disclosure of sensitive information could hurt the business as a whole.

Compliance: A basic level of Physical security is required for compliance. A minimum level of theft deterrent (like locks or anti theft devices) and some basic access control mechanism (swipe cards to access the room) should be in place.

Testing: This Item can be tested by analyzing the procedures guests and visitors have to take to access the premises. A basic walkthrough of the premises should also be done to check for the presence of alarms or simply to see if some one will challenge your presence. Determine if a Physical security policy document is available (like procedures for storing, locking and disposing of IT assets).

Test type: Objective. Depending on the level of sensitivity of the information, basic physical security compliance must be met. The physical security level of the enterprise should match the requirements detailed in the Security Policy. The Policy should cover all physical access controls including those related to desktops and workstations.

Item #2: Response time to security events

Reference: Measuring detection and reaction time to cyberattacks is a key element of an infosecurity plan
http://infosecuritymag.techtarget.com/articles/june00/features2.shtml

Control objective: Reduce/test the average time taken by users to report a breach of security (like a lost token or a compromised PIN). Test the exposure time when a security breach occurs.

Risk:

Potential Threat: The time it takes to report a breach in security is too long. Exposure time to the attack will be increased.

Threat level: High: Reaction time is often crucial in helping to deal with security threats. Normal users must take the security measures seriously or risk undermining the effectiveness of the whole process. In essence, it is very important to keep the report time to a minimum and limit the exposure to attack.

Likelihood: General careless behavior in reporting security breaches can be quite common. Some users might also feel that they will be viewed in a bad light if they report breaches in security (like losing a piece of paper that contains a SecurID PIN (writing down a PIN should never happen in the first place), or losing a SecurID token).

Impact: The loss of a PIN or SecurID token is obviously a great security risk. This risk can only be mitigated by a prompt response time. Also, The shorter the response time, the lower the potential risk will be. Due to the Two-Factor nature of the RSA SecurID framework, the loss of only one of the Items will not be catastrophic. But it is still imperative, that these errors and omissions be dealt with rapidly.

Compliance: The minimum baseline response time is relative to the sensitivity of the Data protected by the SecurID framework. Compliance should be tested for all levels of data classifications and should fall between the required ranges.

Testing: Testing of this can be quite tricky. General social engineering techniques could be used to extract information about PINs from users. These inquires should be reported in a timely fashion (obviously with proper guidance and support form the administration). Please refer to this article for further information http://www.securityfocus.com/infocus/1527 on Social engineering.

An informal interview should be conducted with some of the staff about their general perceptions on what would constitute a high/medium/low level security breach. Basically, to see if the loss of a token or a PIN is a big deal or not. I do not actually recommend, “acquiring” an actual token from a user (even with the proper permissions). This will cause undue harm to the audit process and is not worth the potential backlash.

If management agrees, a simple Social engineering response time audit can be done. The importance of this test is dependant on the level of security required by the company.

For more information on Social engineering Techniques, please refer to http://www.sans.org/rr/paper.php?id=920 and http://www.securityfocus.com/infocus/1533

Obviously the attack attempts have to be noticed by the victims. The goal is to test the alert response time of these attacks.

General Social engineering attacks

Risks	Tactics used	Response Time to attack
Phone attacks (Help Desk/Administrator/repair man)	Impersonation and persuasion attempts over the phone	
On site access	Unauthorized physical access and impersonation of an “important person”	
Office access	Shoulder surfing	
Reverse social engineering	Leave fake business card on desk (so that the user calls the attacker first)	
Snooping	Wandering through halls looking for open doors or offices	

Mail room or “common room” attacks	Insertion of forged memos requiring users to call A number and change their passwords	
Machine room/Phone closet	Attempt Gain and install a sniffer	
Phone or PBX access	Stealing phone toll access codes	
Dumpsters access	Dumpster diving for information and passwords	
External attacks	Forged emails requiring users to send credentials	
Office attacks (physical)	Attempt stealing sensitive documents	
General Social engineering	Impersonation of an employee	

The required response time for all these events should fall between 15 minutes and 1 hour.

Response time importance level inquiry

Action	Perceived Level of Importance from user (1 to 10 scale)	Response Time
Loss of PIN		
Loss of Token		

Here is a range of values for acceptable response times based on the level of access.

Event	Administrator	Normal User
Compromised Token	15 Minutes for High Security level to 1 Hour for Low	Maximum of 24 Hours
Compromised PIN	15 Minutes for High Security level to 1 Hour for Low	Maximum of 24 Hours
Compromised Username	1 Hour for High Security level to 24 Hours for Low	Maximum of 24 Hours

Test type: Objective. The response time is dependent on the level of access the token/PIN provides. The average response time should fall between the established ranges.

Item #3: Loss/Compromise of SecurID Token/PIN

Reference: Partially based on the user responsibilities found here http://www.oalansupport.state.pa.us/oalan/lib/oalan/doc/securid_remote_access_request_blank_form.doc and RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify the procedures when a token or PIN is lost/compromised. This checklist item will verify that the handling and management of the Tokens and PINs is adequate.

Risk:

Potential Threat: Tokens or PINs can be accidentally lost or compromised. Hopefully, only one will be lost/compromised, and not both at the same time. Losing both the PIN and Token could give a malicious hacker easy access to machines on the network.
Threat level: High: PINs are easy to acquire if the users are not careful. Tokens (especially Key fobs) can be lost if attached to key chains.
Likelihood: Medium: Tokens are often lost in the enterprise.
Impact: The two-factor nature of the Token/PIN combo reduces the risks associated with the loss of only one of the factors. The factors are complementary and allow for a more robust and error resistant authentication mechanism. If both are compromised, the workstations or servers being protected by SecurID will have to rely on a proper implementation of the OS level password.

Compliance: The loss or compromise of Token's, PINs or Usernames must be reported to the SecurID administrators. The Administrator must have procedures in place that will allow the proper administration and management of the tokens. The handling of the tokens must meet the normal procedures outlined in the company policies.

Testing:

This Item can be tested by analyzing the way users and administrators use the SecurID tokens and PINs. An informal review should be conducted with users and administrator. Response times must match the criteria described in Checklist item #2.

Guidelines:

Verify that the Token's are stored and used properly:

- Tokens should not be kept on desks or unlocked drawers. This will reduce the likelihood of theft

- “Credit Card” sized token’s should not be kept in wallets (they are not resistant to shock, and can break easily if slightly bent).

- Key fobs type tokens should not be kept in personal key chains (car keys, house key’s, etc…) to minimize the amount of time the key chains are used. This will lower the odds of the Key fob being lost.

- Expired tokens must be reported immediately.

Verify that the PINs are used correctly.

- Personal Identification Numbers should be kept private.
- Personal Identification Numbers should meet the company’s password guidelines.
- Personal Identification Numbers should not be reused once revoked.

Test type: Objective. The guidelines must be met.

Item #4: Null Sessions

Reference:

http://www.sans.org/top20/#W5 SANS/FBI top 20 vulnerabilities
http://www.brown.edu/Facilities/CIS/CIRT/help/netbiosnull.html - _Toc25025301
HTTP://WWW.GIAC.ORG/PRACTICAL/MICHAEL_KRISS_GCIH.DOC
http://www.sans.org/rr/paper.php?id=286

Control objective: Validate the User Account security measures of the machine being audited. Restrict the amount of information leaked by the system. This test has an impact on the effectiveness of the SecurID infrastructure.

Risk:

Potential Threat: Malicious hackers can gather important windows information from null sessions.

Threat level: High. This is one of the top vulnerabilities on the SANS top20 vulnerabilities for windows systems.

Likelihood: Null sessions are enabled by default in most windows installations.

Impact: Leakage of important information. Usernames and machine names can be found. Usernames should remain private. OS level security is important in the event that SecurID is compromised.

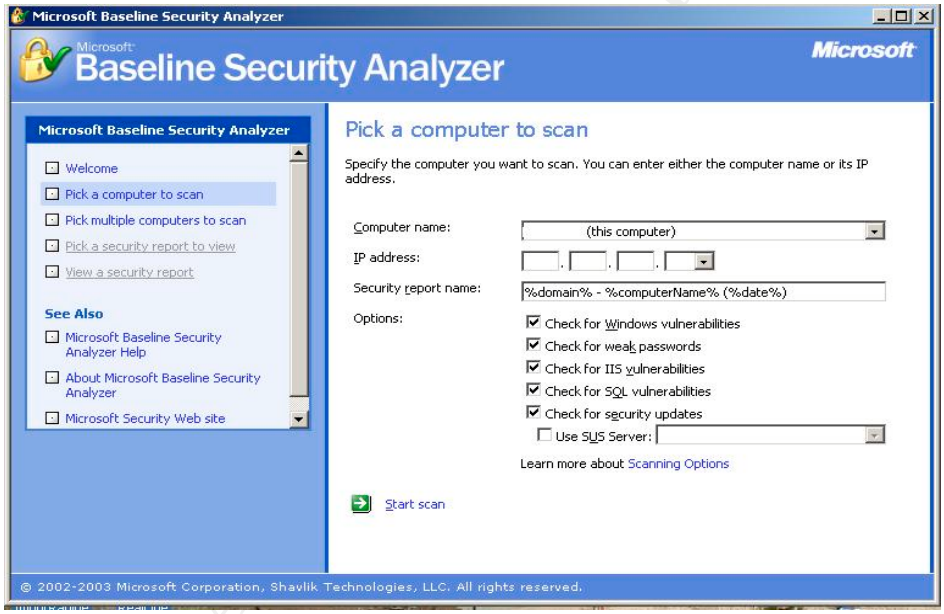
Compliance: Checking for a null session is a binary check. Null sessions must be blocked.

Testing:

Null session: Open a CMD prompt (Start->Run->CMD) and run the following command:

net use \\123.456.789.123\ipc$ "" /user:""
You are vulnerable if the command is successful.

Alternative method: Run the Microsoft Baseline Security Analyzer on the local machine. The install process is self-explanatory. Run all the tests shown below.



Check the results of the Restrict Anonymous test. The Restrict Anonymous variable must be equal to 2.

Test type: Checking for the existence of null sessions is objective. Either they are present or not.

Item #5: After Loss of connectivity to ACE/Server, check that the reserve password is strong enough

Reference: Original contribution although a general guideline on how to achieve Strong passwords can be found here:
http://www.sans.org/resources/policies/Password_Policy.pdf
RSA SecurID Best Practices for Maximum Security,
http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify that the reserve password is implemented properly. Test the effectiveness of the reserve password feature and minimize the risks it contains.

Risk:

Potential Threat: Reserve password is easy to guess or is compromised. An attacker can bypass SecurID protection.

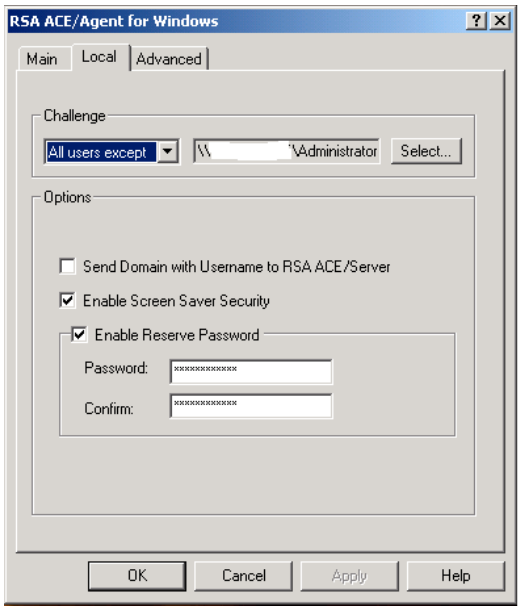
Threat level: Medium: The reserve password is a good failsafe measure during a network outage. But often, the same password is used on each machine. If the password is compromised, an attacker can gain access to the machine. You will note that you need to login with the OS password before getting access to the SecurID login Screen (by default) and as such a potential external hacker would have to acquire a valid OS password first. Current users could potentially bypass the SecurID process with the reserve password. This potential vulnerability to attack should be weighted with the benefits of having a backdoor into the system.

Likelihood: Low: Knowledge of the reserve passwords is on a need to know basis. The passwords are unique to the machine (although the pattern used to create the password is universal for all machines).

Impact: Complete access to the machine. A compromised reserve password can lead to the bypass of the whole SecurID protection framework.

Compliance: Compliance is binary. The password must meet the minimum password requirements of the Security policy.

Testing:
As an administrator on the machine: Open My computer->Control Panel-> RSA ACE/Agent tab. Go to the Local tab and see if a reserve password is set.



You could also test for simple passwords by yourself (disconnect the machine and try to guess the passwords). Brute forcing the reserve password can be tricky considering that after 3 failed attempts, the query window times out and the authenticating process is restarted (Insert OS login/Password again, followed by the reserve password query window). The password is stored in the registry and is encrypted. Brute force attempts to crack this registry value could be difficult. Brute forcing the reserve password from the login screen with a script is possible but unpractical. This is one of the few cases where asking the local administrators for the method used to create the password would be advisable.

Test type: Objective. Either the password matches the minimum criteria or it does not.

Item #6: OS Password complexity (Stimulus/Response)

Reference: http://rusecure.rutgers.edu/secplan/cklst.html Accounts and password section and http://www.sans.org/resources/policies/Password_Policy.pdf for a policy guide.

Control objective: Validate the OS Password protection level of the Ace/Server and Ace/Agent. The OS password is an important part of the SecurID authentication process and should be properly secured.

Risk:

Potential Threat: The SecurID frameworks complements the deficiencies found in OS passwords. Someone who compromises the OS password could connect to administrative shares (if Netbios is enabled) and bypass all the SecurID security measures.

Threat level: Medium: Strong passwords are essential in a secure infrastructure.

Likelihood: High. Normal users can often use easy passwords.

Impact: Access to administrative shares (C$). This gives malicious hackers access to all the files on the machine.

Compliance: A complete audit of the password files should be performed (using tools like L0pthcrack or John the ripper). The password must meet the Security policies minimum password requirements or meet the guidelines found here: http://www.sans.org/resources/policies/Password_Policy.pdf). This will ensure that the password will not be broken by a simple dictionary attack.

Testing:

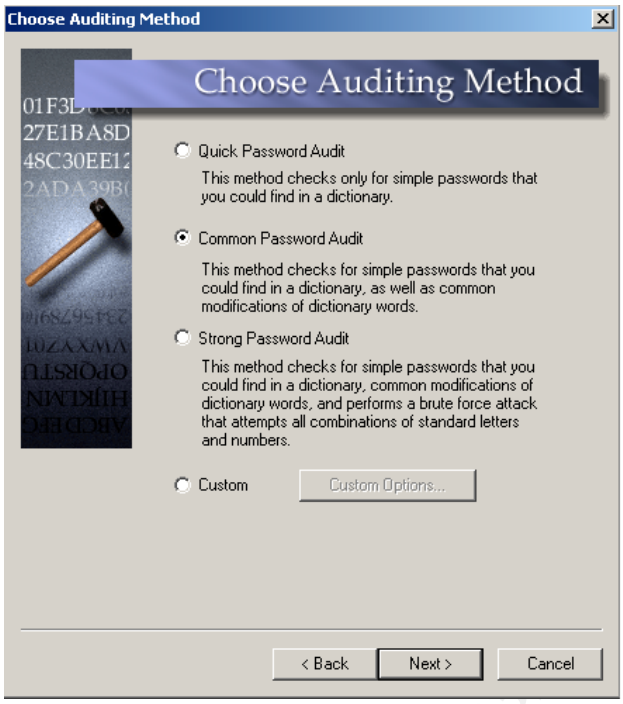
Every password can eventually be cracked by a brute force attack. A basic dictionary attack can be performed to test the level of security of your passwords.

Go to http://www.atstake.com/research/lc/download.html and download the Trial version of L0phtcrack 4 (Trial version is sufficient for this test).

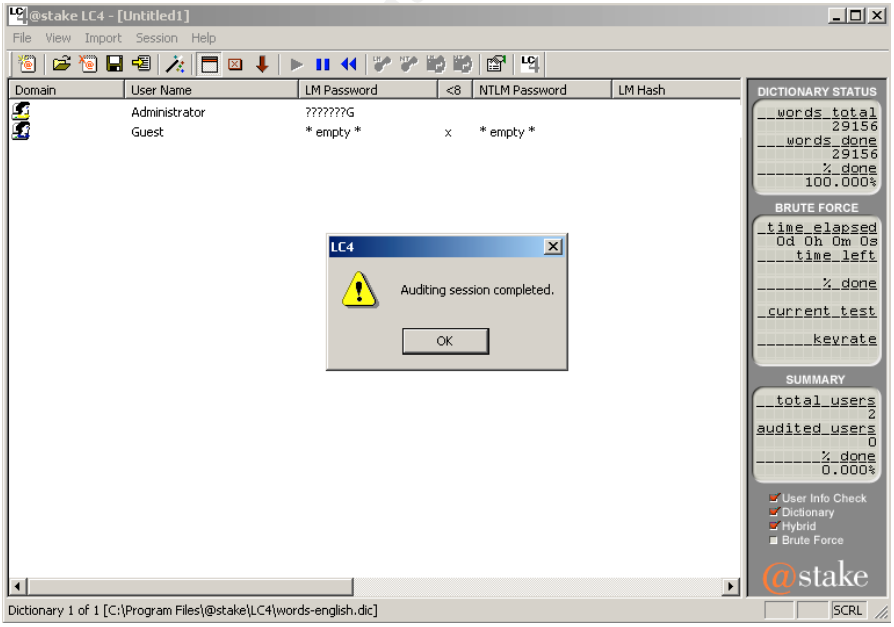
Install L0phtcrack on the machines that require to be audited (Client and Server).

Start L0phtcrack and use the retrieve from local machine setting:

Click on Next, and then select a Common Password Audit (Trial version does not support the brute force option).



Click Next to run the scan.



You will also have to attempt to change a password to a value that is easy to guess (like 12345678).

Test type: Objective. Any password that is easily cracked (the amount of time can depend on many factors like CPU speed, etc…) should be changed rapidly. Any password that is guessable by a basic dictionary attack should also be changed.

Item #7: Account policies check.

Reference: http://www.cisecurity.org/bench_win2000.html Level-1 Benchmark for Windows 2000 (v1.1.7).

Control objective: This test will validate the password policy settings and account policies of the Ace/Server and Ace/Agent. This will ensure that both machine's policies meet the minimum guidelines.

Risk:

Potential Threat: Vulnerabilities exists in the OS that can affect the security level of the machine. An improper password policy setting might reduce the security level of the machine and also cause a false sense of security. A precise check should be done.

Threat level: Medium: Some Password policy settings might not meet the security level required by the security policies. The default values are generally insufficient.

Likelihood: Low: Only administrators have access to security settings on the machine but there is always a chance that proper change control measures were not followed, and settings were changed. Default settings might still be implemented.

Impact: Password policies and Account policies are important to the SecurID process. They govern the behavior of OS passwords on the protected machines. A poor implementation of those policies could lead to a compromise.

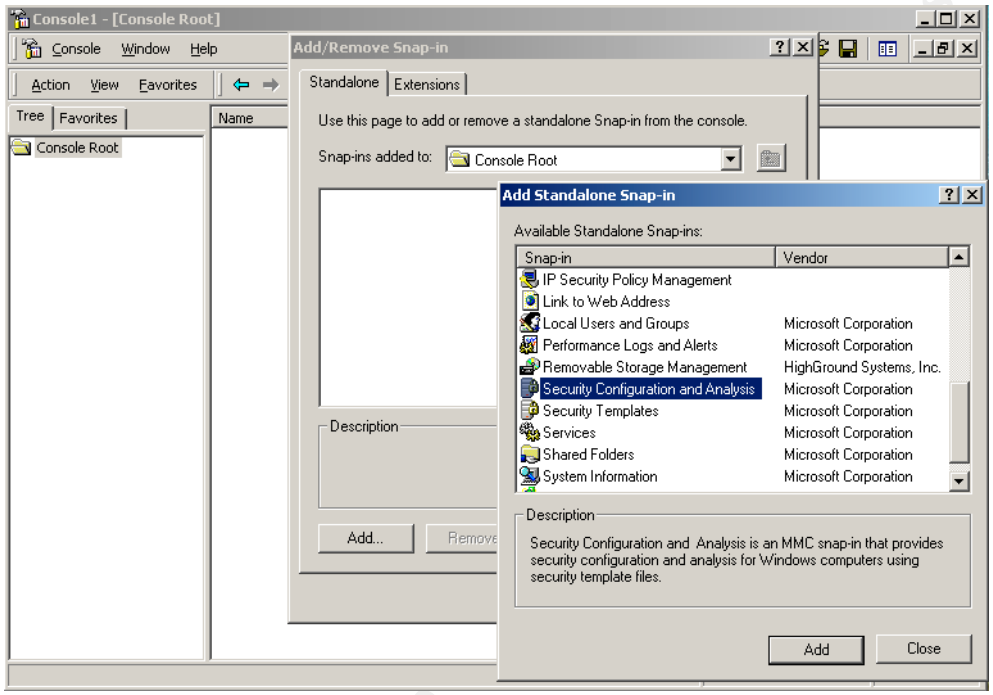
Compliance: Verify if the machines meet the OS password security level outlined in the Security policies. Test the current machine settings with a known standard like the Win2k gold Standard or the Level I Template. The results must match or exceed the values in the templates.

Testing:

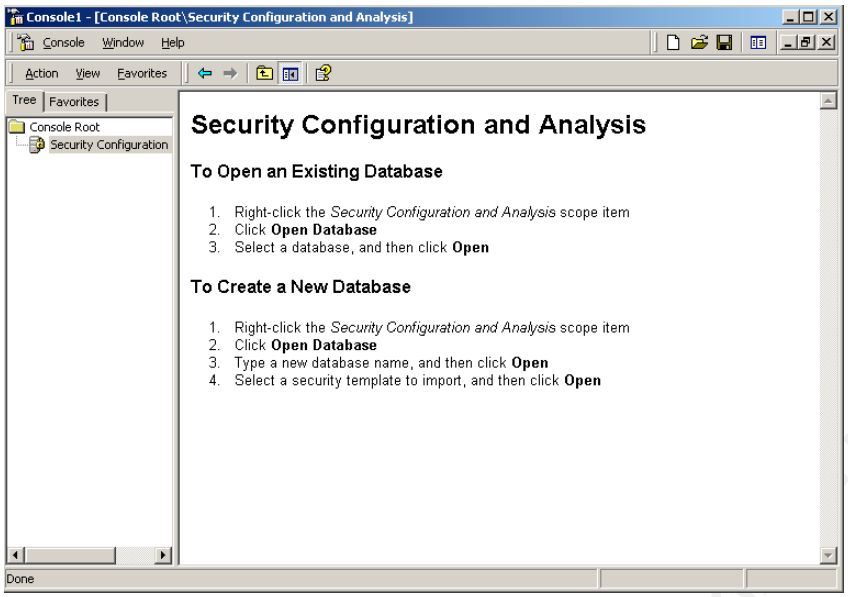
Download and install the CIS scoring tool and Common baseline templates (http://www.cisecurity.org/bench_win2000.html).

Open up the MMC: Start->Run->MMC
Click on Console->Add remove snap-In then Click on Add

Double click on The Security configuration and Analysis then click on Close
Click OK to come back to the main MMC window

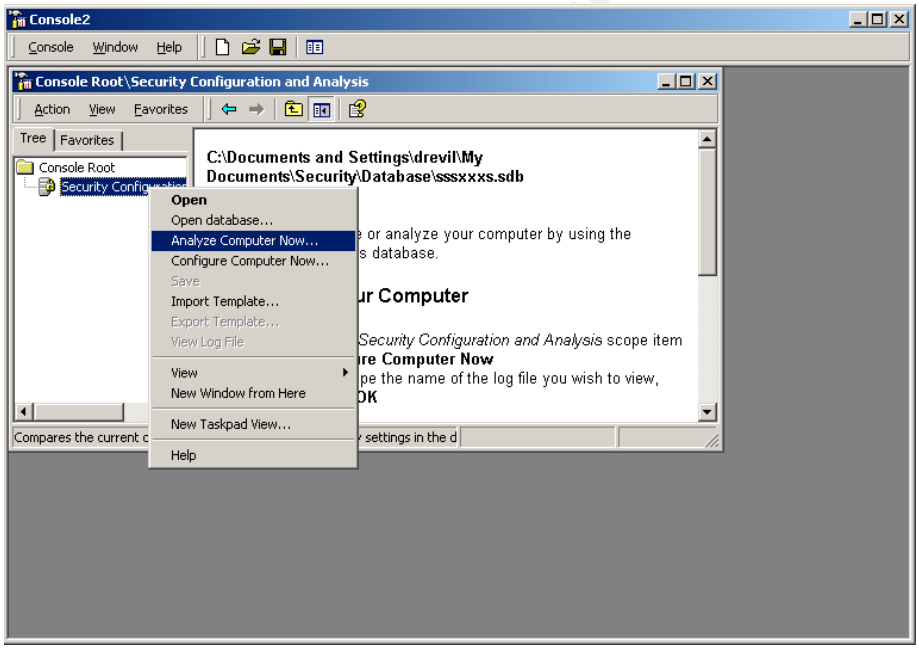


Follow the instruction on screen and create a new database

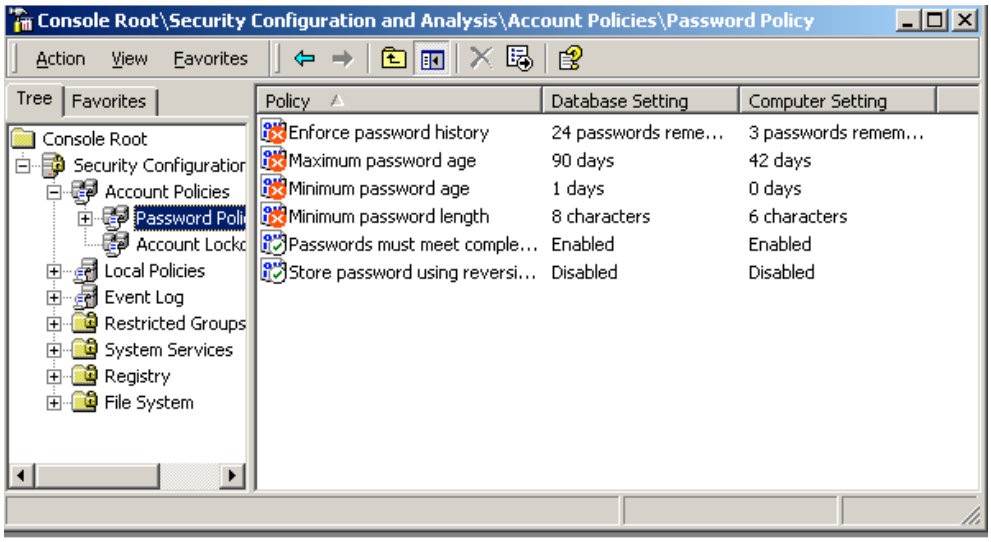


When you are prompted to import a template, use CIS-Win2K-Level-I-v1.1.7.inf file from the CIS scoring tool install directory.

Right click on the SEC tab and Start to analyze the machine.



Compare the results with the template (Database setting is the template, Computer Setting Is the current settings).



You will note that the SEC snap-in compares the current settings with the ones in the template standard in a binary fashion. If they match exactly, it will return a positive check; If they don't (for whatever reason) it will return a false result (red cross).

If the machine setting and template setting are different, the MMC snap-in will return a false value. Even if the machine settings are better.

Another template could be used, for example, The Win2k Gold standard. This template can be very strict and a full implementation on production machines (with no testing of the consequences, especially on network applications) should be done very carefully.

Test type: Objective (if tests are performed on the Baseline or a personalized template built in-house). The values must match or exceed the template settings (CIS-Win2K-Level-I-v1.1.7.inf).

Item #8: auth before or after logon

Reference: Original submission.

Control objective: Verify that the auth before or after logon features are implemented properly. This test will validate the order of authentication on the Ace/Agents (OS->SecurID or SecurID->OS).

Risk:

Potential Threat: The OS password can be brute forced or guessed if the SecurID authentication logon is done after the OS password screen.

Threat level: Medium: OS passwords should be secured even if SecurID is installed on the machine

Likelihood: Low: Standard password safekeeping policies should be enforced.

Impact: If an OS password is compromised, a potential attacker could gain access to the machine with other means (like through a Netbios administrator share).

Compliance: Either the SecurID screen is available before the OS logon, or it is not. To pass the test the logon screen must meet the security requirements of the enterprise.

Testing:

Visual inspection of the logon process is all that is required. Once the order is determined. The reasoning behind the order should be examined. The only drawback of the Authentication before logon is that this method can only be applied to all users. There is no "All users except" clause available.

Test type: Objective, before logon authentication is required/wanted or it is not.

Item #9: All users "except:" clause is invoked

Reference: Original contribution

Control objective: Verify that the all users "except:" clause is used properly. This test validates the users/groups that are exempt from authenticating with SecurID.

Risk:

Potential Threat: The all users except clause is used improperly. The group used in the "except" clause is not restrictive enough and impacts too many users (like the Power User group or administrator group). The amount of users in the group should be very limited.

Threat level: High: Generally, the "except" clause is often used for the administrative group. This is not ideal, considering the availability of the reserve password. Most intrusion attempts will be done against administrator level accounts and administrators should not be allowed to avoid the authentication process.

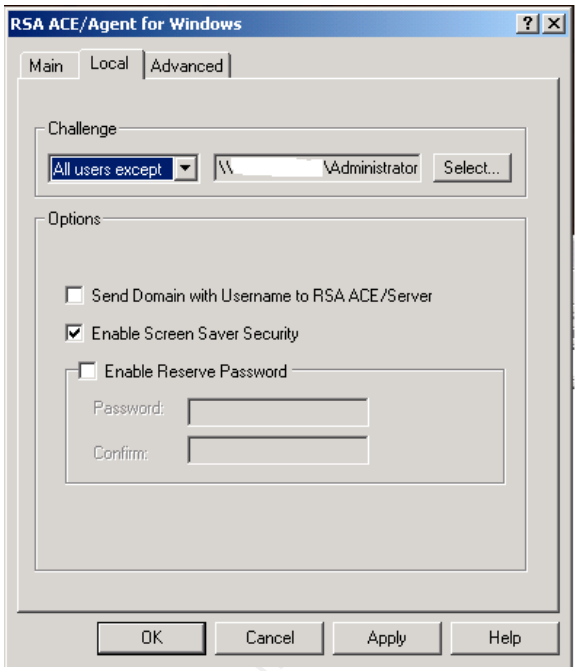
Likelihood: Medium. Administrators can sometimes use the all users except clause for debugging. The setting should be removed or switched to the reserve password once testing is finished.

Impact: Complete bypass of the SecurID architecture. This removes all the added security features.

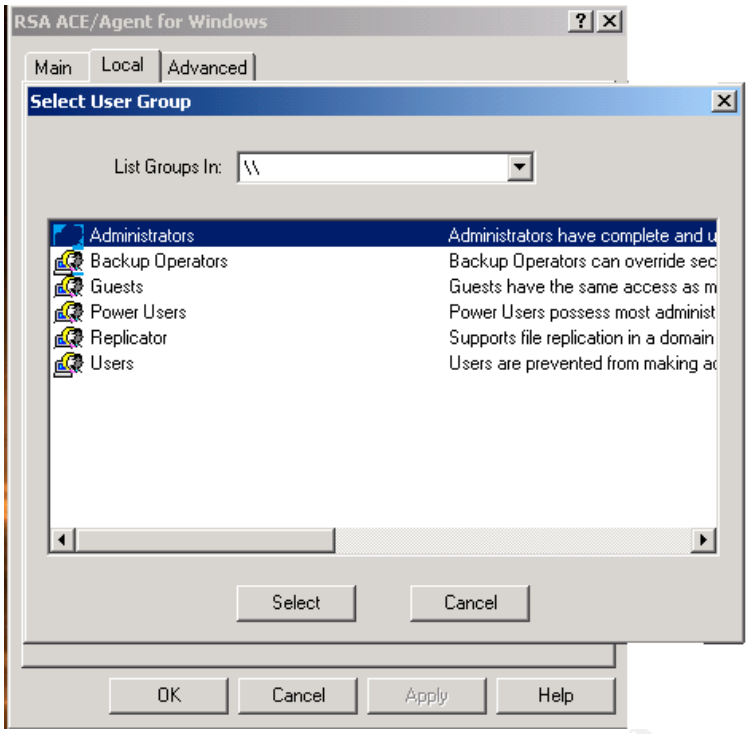
Compliance: Binary: Either the "All users except" clause is invoked or it is not. If the clause is invoked, then there should be a justification on why this was enabled. It should not be used with the administrators group.

Testing:

As an administrator: Open My computer->Control Panel-> RSA ACE/Agent tab. Go to the Local tab and see what the Challenge field is showing.



If the "All users except" clause is used; check that the group in question has limited user rights.



Test type: Objective. Either the all users except clause is used or it is not. Is the administrative group exempt? If the clause is used, the justification should match the Security Policy guidelines.

Item #10: Sdconf.rec file used is current and the same as the one generated on the Server.

Reference: Inspired in part on the SecurID and checkpoint FW-1 FP implementation guide. http://www.mail-archive.com/fw-1-mailinglist@beethoven.us.checkpoint.com/msg14519.html

Control objective: Validate the communication between the Ace/Agents and Ace/Server. Make sure that the configuration files are current and match the latest files on the Ace/Server.

Risk:

Potential Threat: Configuration files on the client side were tampered with or not up-to-date. The Sdconf.rec file is usually created on the ACE/Server and copied to the Client stations. The Ace/Agents use this information to connect to the Ace/Server.

Threat level: Medium: Client connection can be broken if the Sdconf.rec file is erased or damaged. The file must be kept up-to-date to allow proper communication with the ACE/Server.

Likelihood: Low: This file is secured on the ACE/Server and can be recreated.

Impact: Deletion of the file could lead to a loss of communication with the ACE/Server and in turn could lead to an attack (if the reserve password is used). A Client machine could potentially be reconfigured to authenticate to another ACE/Server (this would require complete control of the machine). This is not a great risk but it could cause networking issues and make troubleshooting harder.

Compliance: The latest Sdconf.rec file on the ACE/Server must match the one on the Ace/Agent machines.

Testing:

Download md5sum.exe (http://www.etree.org/md5com.html) and compare the 2 files in questions

ACE/Server: Go to the RSA configuration directory (usually C:\RSA\ACE\Data\Config_files)

Copy the Sdconf.rec file to a floppy (Rename file to Server-Sdconf.rec)

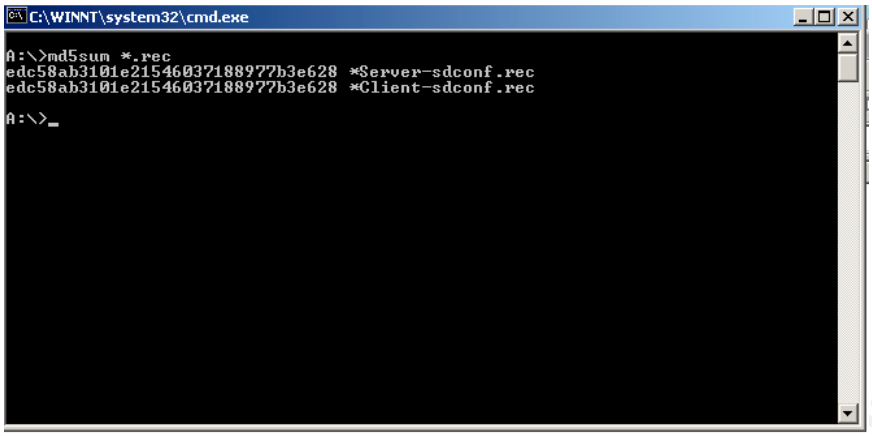
Client: Search for the Sdconf.rec file on the client (Start->Search->For Files or Folders) and copy it to the same floppy (Rename file to Client-Sdconf.rec).

Copy md5sum.exe to the same floppy

Open a CMD window (Start->Run->CMD) and go to the floppy drive (type A:)

At the prompt type “md5sum *.rec”

You will get an output similar to this:



The Checksums must match. If the checksums are different, the Sdconf.rec from the client is not up-to-date.

Test type: Objective. The files must be identical to pass the test.

Item #11: Patch level of Client and host are up-to-date (SecurID software only)

Reference: RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify that the Ace/Agent and Ace/Server software is current. Validate the SecurID software to minimize exposure to attack and lower the risk of software failure.

Risk:

Potential Threat: An unpatched client or Server leads to a compromise (with a Buffer overflow for example :(http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html)). An unpatched server or client could also lead to several software bugs or issues.

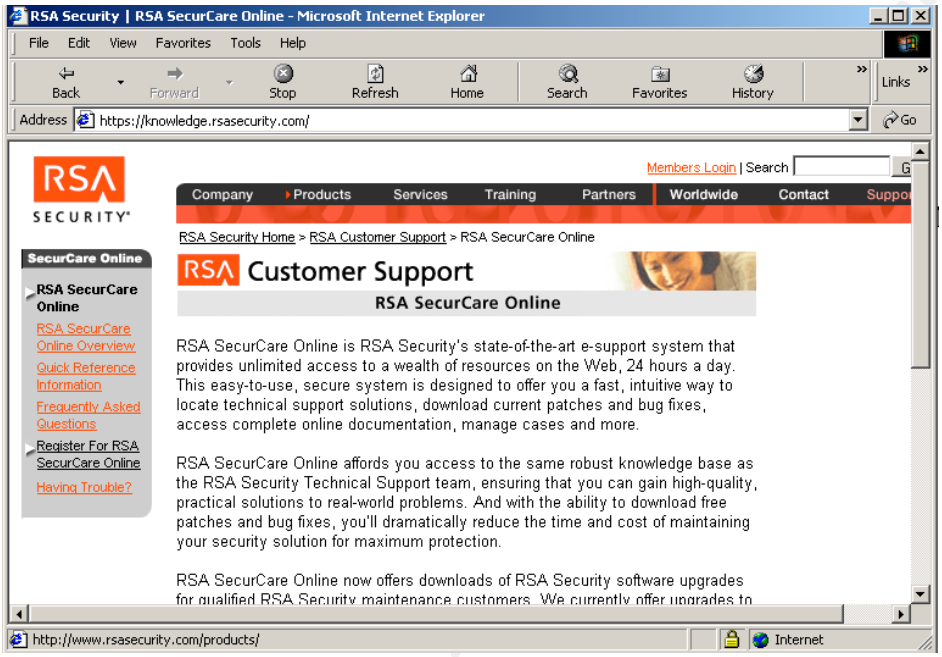
Threat level: Medium: Keeping software up-to-date is a normal computing practice. It helps resolve intermittent problems and assures that new vulnerabilities in the systems are dealt with effectively.

Likelihood: Medium: A change control and patch deployment policy should be in place.

Impact: Potential loss of information and hijacking of network resources by an unauthorized 3rd party if a major vulnerability is discovered and left unpatched.

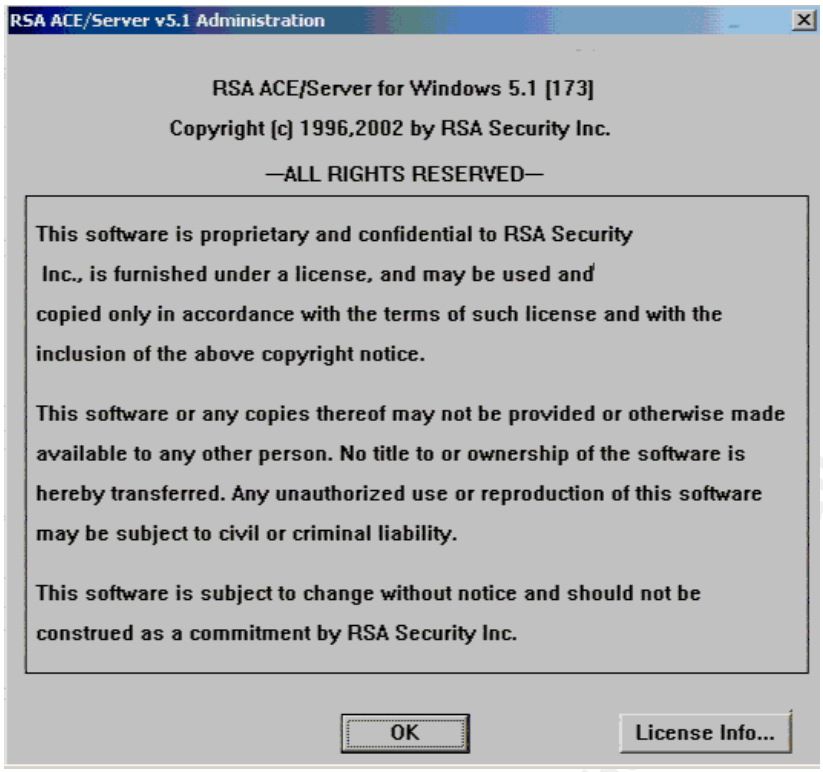
Compliance: ACE/Server and Ace/Agent software must be kept current.

Testing:
Log into your RSA SecurCare Online (https://knowledge.rsasecurity.com/) and check for the latest patches and software revisions.



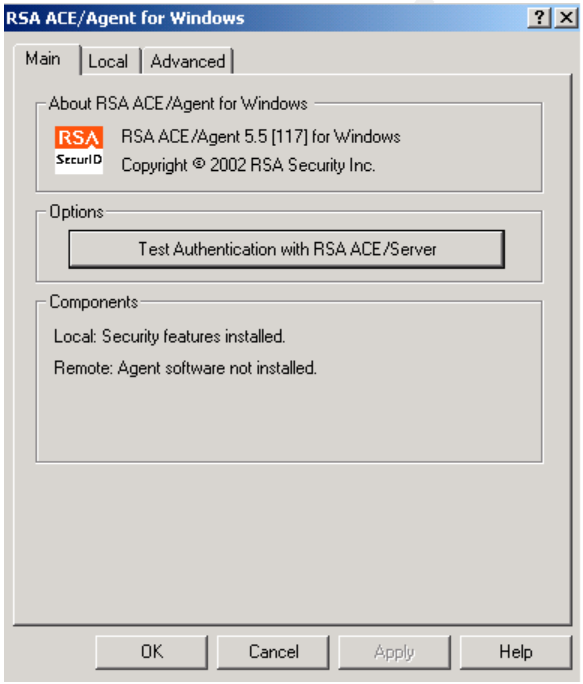
Log onto the ACE/Server Administrator (Start->Program->RSA ACE Server-> Database Administration Host Mode) on the ACE/Server machine

Then Click on Help->About Database administration and find the Server Version number



Log onto the Client Machine as an Administrator

Go to the Control Panel's RSA ACE/Agent tab (My computer->Control Panel-> RSA ACE/Agent) and check the version number.



Test type: Objective. Server and Client software must be current.

Item #12: SecurID next tokencode checks (Stimulus/Response)

Reference: Fala SecurID Information Center policies, http://www.fala.com/fala_securid.cfm

Control objective: Validate the proper implementation of the Next tokencode protection feature. Verify that the Next tokencode feature is enabled and sufficiently restrictive.

Risk:

Potential Threat: The value for the Next Token Code Mode/Disable token Mode is not strict enough and gives to much freedom to the users.

Threat level: Low: The default value is adequate for most deployments. The values should be adjusted for more critical infrastructures.

Likelihood: Low: The default values are adequate and will deter most brute force attempts at guessing the "PIN+TokenCode" passwords.

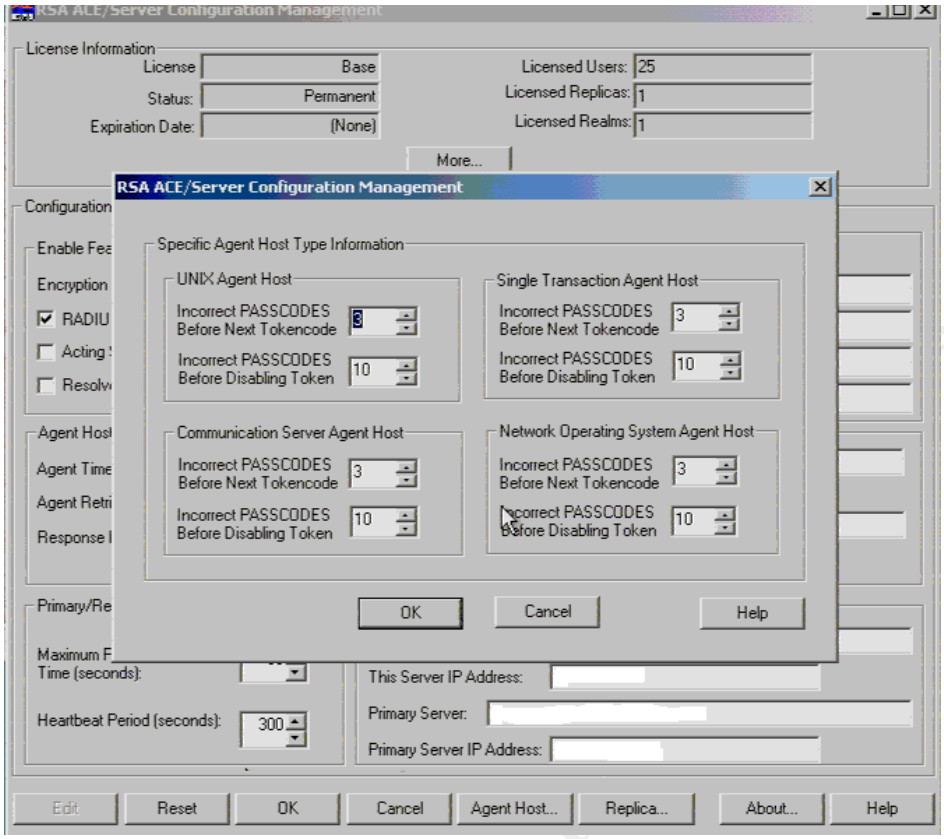
Impact: If the value is set too high. An attacker could possibly guess a value and successfully log on the system.

Compliance: The values must match the minimum and default values guidelines for failed authentication attempts (incorrect Passcodes before next tokencode mode = 3 and Incorrect Passcodes before disabling token = 10).

Testing:

ACE/Server: Open up the Configuration Management console (Start->Programs -> RSA ACE/Server -> Configuration Management

Click on Agent



You will now see the values set for the following 2 actions

Next tokencode mode
Disable token

Verify that the values meet the standard failed login practices in the enterprise. The next tokencode mode is designed to counter the guessing of passwords. After a certain number of failed attempts, the RSA ACE/Server will require the agent, to authenticate with two consecutive passwords. This will ensure that the user actually has the token.

The disabling token mode is self-explanatory. After the set amount of consecutive failed logins, the token is simply disabled.

Have a token issued to you.
Test the following cases.

3 consecutive failed logons followed by a successful logon
Verify that the token was set to next tokencode mode.

10 consecutive failed logons followed by a successful logon

Log onto the Administration Console and verify that the Token is disabled (click on Report and verify the disabled status of the token in the logs).

Test type: Objective. The setting must match the minimum default values.

Item #13: SecurID Access logs are backed/maintained and consulted regularly (Stimulus/Response)

Reference: RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify that the SecurID logs and events are monitored regularly and installed properly. This will reduce the exposure time to an attack.

Risk:

Potential Threat: Access logs contain valuable information about the daily workings of your SecurID infrastructure. If they are not reviewed regularly and properly stored/secured, the response time for detecting and stopping an attack can be greatly increased. Which in turn will lower the level of Security of the enterprise. Logs have to be backed up regularly and secured so that their integrity remains intact.

Threat level: Medium: The benefits of logging events are dependent on the regularity of log reviews. If the administrators are not diligent enough, security issues could go unnoticed for an unacceptable length of time

Likelihood: High: Reviewing logs is not generally a task that is enjoyed by administrators. An attack could potentially go unnoticed for long periods of time.

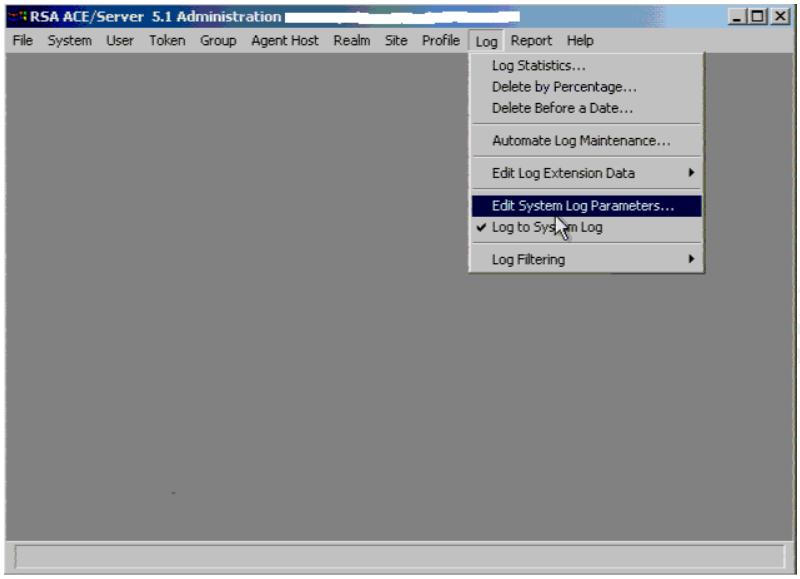
Impact: Higher response time due to poor awareness could lead to extended exposure. An attack could go unnoticed for a long period of time. The loss of information or Intellectual property could be small if the response time was kept low.

Compliance: There must be a log review schedule in place in the Security policy, and the administrator staff must enact it diligently. All possible fields must be logged and the logging mechanism has to be working properly. The log handling practices should meet the standards defined in the company policies and the minimum values.

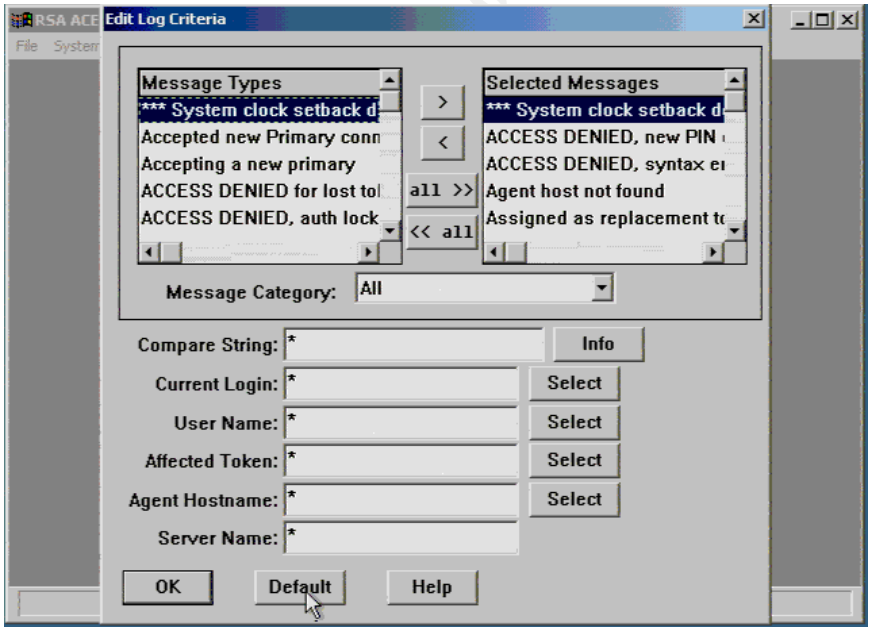
Testing:

Verify that the fields being logged are adequate.

In the SecurID ACE/Agent administrator click on Log-> Edit System Log Parameters



The fields being logged must match the minimum default values. If a high level of security is required. All message fields should be enabled.



Once logs are validated. The storing methods of logs and the frequency at witch they are examined must be analyzed.

A simple informal inquiry with the SecurID administrators should be enough to determine the common practices in the company.

Questions to be asked:

How do you store your logs?
How often are logs rotated?
How often are logs reviewed for unusual Errors?
How often are logs reviewed for Access violations?
What is your backup strategy for the ACE/Server and how often are backups performed?

The answers given should be compliant with the Information/Data management and practices described in the Security Policy.

Here are some minimum values:

Question	Response
How do you store your logs?	Offsite location
How often are logs rotated?	Every 6-12 months
How often are logs reviewed for unusual Errors?	Biweekly for low security, Daily for normal and Hourly for high
How often are logs reviewed for Access violations?	Biweekly for low security, Daily for normal and Hourly for high
What is your backup strategy for the ACE/Server and how often are backups performed	Daily incremental or differential and weekly full backups

You must check that events are properly displayed in the logs.

Have a new account made for the auditors.

Use that account and see if your generated events are logged properly (for example, failed login attempts). Verify that all previous test events were logged properly.

Test type: The test is objective (all fields should be logged, the procedures should meet the policy requirements and all events should be logged properly). The log handling practices should meet the standards defined in the company policies and the minimum values.

Item #14: Licensing is current

Reference: RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify that SecurID license is current. Verify that official support channels are available for the Ace/Server and Ace/Agent software.

Risk:

Potential Threat: License is not current and could lead to poor performance or loss of features. Invalid Licensing could reduce the possibility of access to recent patches and personalized support in case of an emergency.
Threat level: Medium. Keeping your licensing current is a good idea. This will guarantee that administrators have all the tools necessary to deal with problems right away.

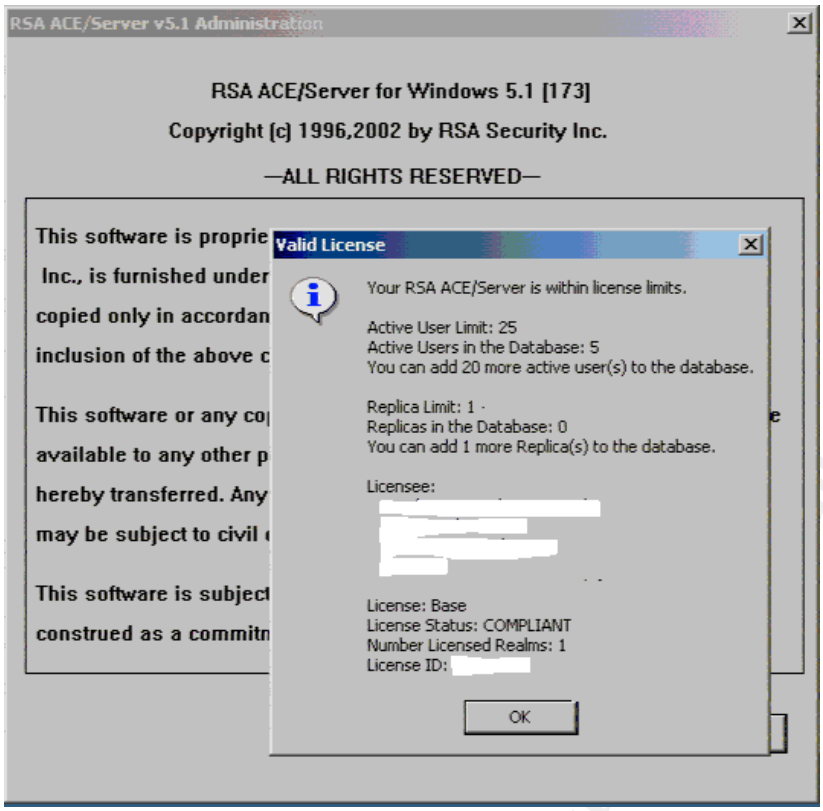
Likelihood: Medium. Licenses are often time limited. With the continuing evolution of computing, old technologies (and support licenses associated with them) are often left behind. Keeping you support licenses current will ensure that you will have access to the latest bug fixes and revisions.

Impact: An expired license can reduce the amount of support you receive from the vendor. This can make troubleshooting your servers harder for the SecurID administrators. If you don't have access to patches and revisions, you will expose yourself to unnecessary risk and important bugs and potential exploits will not be fixed.

Compliance: The license must be current and compliant.

Testing:

Start the administration console. Click on Help->About Database administration-> license info



Make sure that the license is within limits and the License status is: COMPLIANT

Test type: Objective. License must be current and compliant.

Item #15: The Ace/Server features are properly used

Reference: RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Validate the SecurID Ace/Server settings and remove the potentially dangerous features.

Risk:

Potential Threat: Potentially dangerous features are enabled but are not required.

Threat level: High. Some settings have a greater impact on the behavior and security level of the SecurID Ace/Server

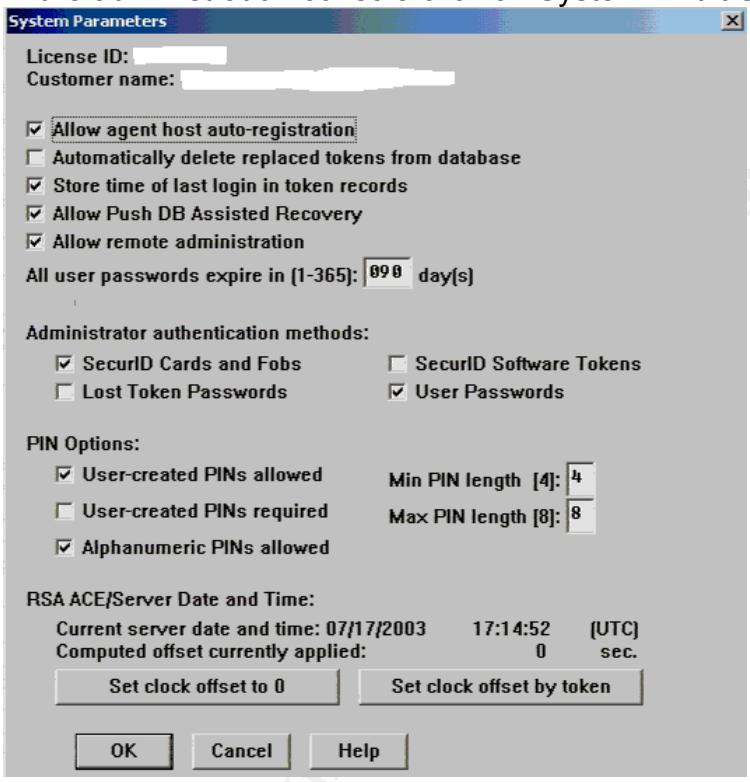
Likelihood: High. Some of the settings can be considered dangerous if improperly used.

Impact: Unnecessary exposure to attacks. This could lead to loss of information and lower security.

Compliance: The settings must be justified. The enabling of features that can ease the administration of the SecurID infrastructure must be weighed with the security risks they create. For most cases, the values must match the common default implementation described in the testing phase.

Testing:

In the administration console click on System->Edit System parameters



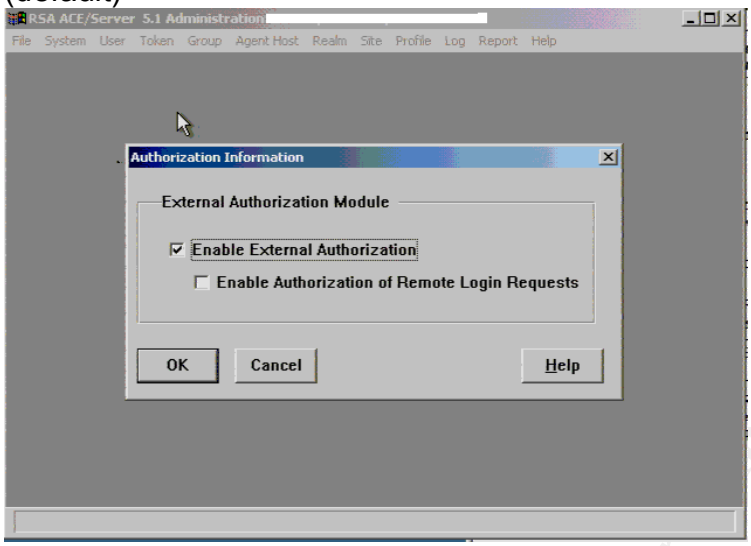
Make sure that the “allow agent host auto-registration” and the “allow remote administration” tabs are unchecked.

Host auto-registration allows remote host agents to “add themselves” to the ACE/Server. This feature is only useful for very large deployment of SecurID. A more controlled approach, where the administrators manually add machines is more appropriate for a more structured and secure deployment.

Remote administration is only necessary if administrators will be accessing the console from remote machines. This setting should be disabled if the feature is not needed.

Check the authorization parameters.

Check that the authorization or remote logins requests setting is unchecked (default)



These settings control the authorization parameters.

Enable External Authorization allows the customized external authorization programs to work with the SecurID ACE/Server authentication. This setting allows users to log in the local machine only.

Test type: Objective. The settings must match the values in the test for most implementations

Item #16: User password expiration date is set to a proper time

Reference: RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify that the password timeouts are set correctly and that normal passwords are not available. Test that all active users are using SecurID two-factor authentication.

Risk:

Potential Threat: Password are often lost or compromised. If this compromised password is never detected, an attacker could access the system for long periods of time.

Threat level: low: Using user passwords defeats the benefits of using token based authentication

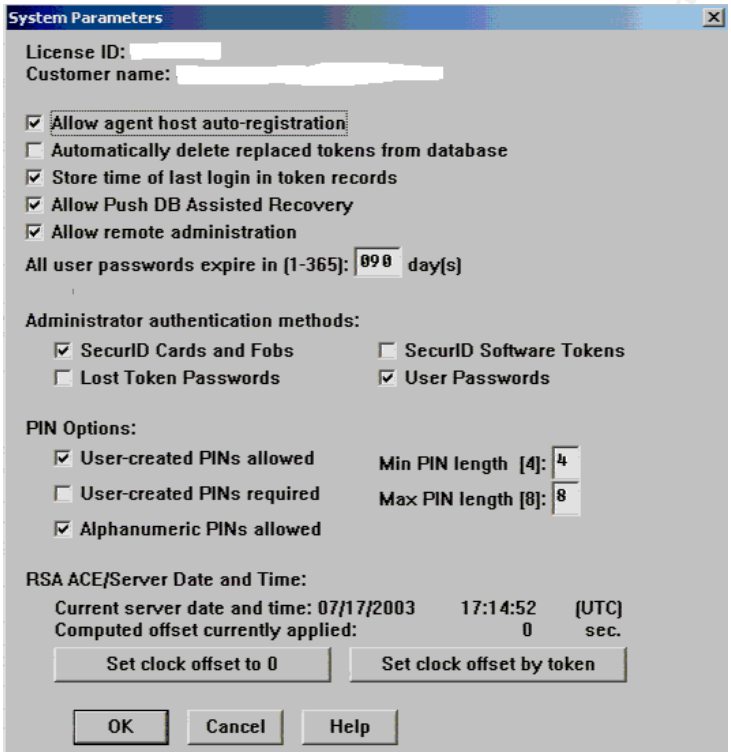
Likelihood: Low: This is manly a debugging feature or a workaround in the event that administrators run out of tokens.

Impact: A compromised user password can lead to a compromise of the machine. This can lead to loss of information or improper use of computing equipment.

Compliance: The value should be set to 90 days at the very least. This value should be lowered for a more secure deployment.

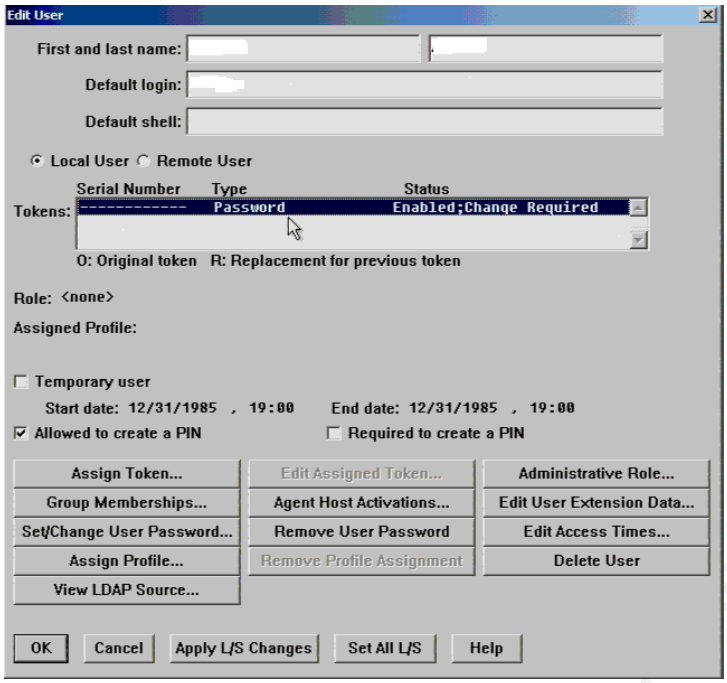
Testing:

Verify that the password expiration date is set to 90 days. Open the Administration console then click on System->Edit System parameters



Check that no users have a user password set (they should all be assigned tokens)

Start the Administration console. Click on user->edit users-> then go through each user and make sure that passwords are not assigned. Tokens should be assigned for all active users.



In this example, the user has a user password set.

Test type: Objective. Normal users should be using two-factor authentication tokens. The timeout for a user password should be 90 days (only for debugging).

Item #17: PIN Length and type is correct. (Stimulus/Response)

Reference: RSA SecurID Best Practices for Maximum Security, http://www.rsasecurity.com/worldwide/securIDbestpractice/SecurIDBP.pdf

Control objective: Verify that the PINs are secure and meet the minimum requirements of the password policies.

Risk:

Potential Threat: A weak PIN can be guessed easily.

Threat level: High: The safety of the PIN is critical for the proper implementation of SecurID. An easy to guess PIN or a very short one can reduce the level of protection of SecurID.

Likelihood: High: Users will often use easy PINs like 1234 or easily guessable ones (birthday, phone number). Also, short PINs are more susceptible to brute forces and guess type attacks.

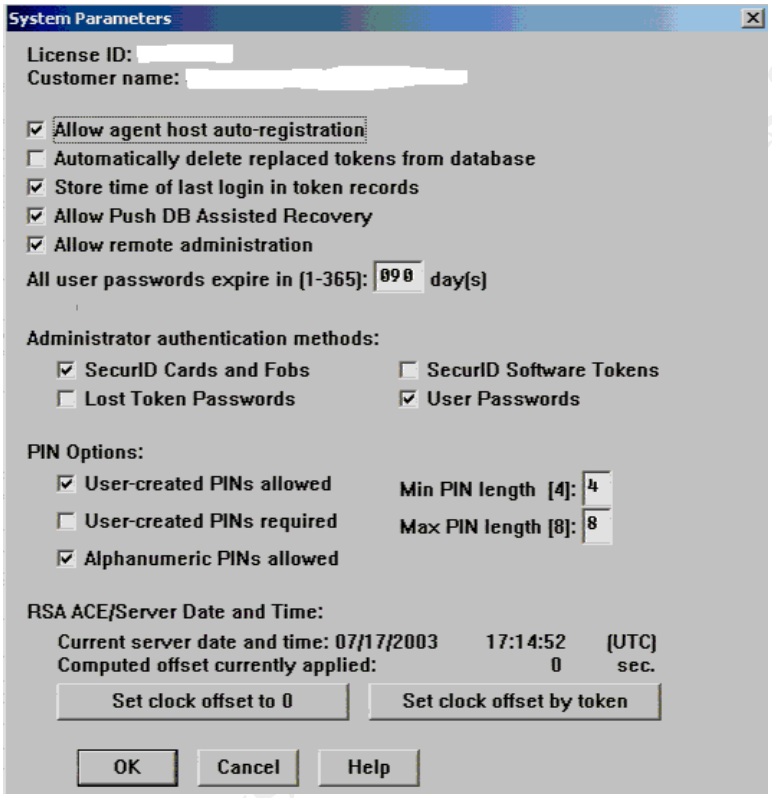
Impact: If a Token is compromised, the security of the architecture is dependant on the complexity and size of the PIN. If the PIN is easy to

guess or is small, unauthorized personnel could access the machine. This can lead to loss of information and could lead to abuse of the computer facilities.

Compliance: The PIN should be complex enough to resist standard guess attempts. The minimum length should be set to 4 and the maximum to the max value of 8. PIN should contain alphanumeric characters.

Testing:

Open the Administration console and click on System->Edit System Parameters.



Min Pin Length should be at least: 4
Max Pin Length should be the Maximum allowable value: 8
Alphanumeric PINs should be allowed (this allows letters in the PIN. This greatly increases the number of possible passwords).

Have a token assigned to an auditor and when the PIN creation window appears, attempt to create a 3 character PIN or a 9 character PIN.

Verify that alphanumeric characters are allowed.

Test type: Objective. The values must match the minimum settings.

Item #18: Access times are set correctly (Stimulus/Response)

Reference: Cert.org Control contractor access to your systems, http://www.cert.org/security-improvement/practices/p022.html

General Access time control software can be found here: http://www.fspro.net/lat/

Control objective: Validate the access time controls settings on the Ace/Server. Verify that the token's access time settings match the work schedules of the users.

Risk:

Potential Threat: Improper access time settings can raise the level of exposure to attack if a Token and PIN is compromised. The attacker will have all the time in the world to access your computing assets.

Threat level: High: Access time controls can be a great help in lowering the exposure time to an attack.

Likelihood: High. Most administrators leave the default settings (no access time limits)

Impact: An attacker could access the machines after normal working hours. Or when nobody is around. This can raise the amount of information that an attacker could extract from a machine. For example, if someone sneaks into the computing room during the night with the proper credentials (PIN and Token). He will not be permitted to log into the machine during nighttime, this can also limit the after-hours use of machines for recreation purposes.

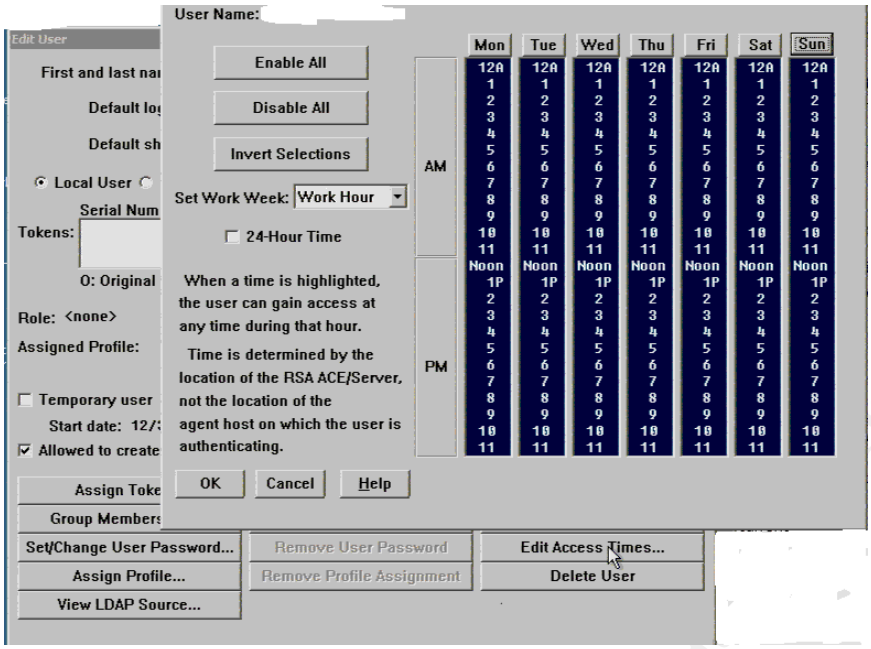
Compliance: Access times should be set to restrict the access to computing machines to normal working hours (plus minus a fixed set time) for normal users. This can greatly limit the exposure to attack. Access times should be set on a user-by-user basis.

Testing:

Start the Administration console. Click on user->edit users

For each users click on Edit Access times

Make sure that the Access time is set to normal working hours + Offset time.



Have an administrator create a user account for an auditor. Attempt to login/authenticate on the machine at an improper time (you can use the Test connection menu on the ACE/Agent). Check logs to verify the process.

Test type: Objective. Access times should be set for all normal users and reflect the normal periods when the machine is used.

Item #19: Communication between the ACE/Agent and the ACE/Server is OK.

Reference: Testing SecurID Server-to-Client Communication, http://www.vineyard.net/vni/docs/pm3/html/manuals/RadiusNT/securidconfig.html - 11557

Control objective: Test SecurID Ace/Agent to Ace/Server communication channels. Validate the proper installation of the SecurID software.

Risk:

Potential Threat: Improper communication between the Ace/Agent and the ACE/Server could block access to the machine. Communication to a non-authorized server can cause problems.

Threat level: Medium: There should be proper communication established between all clients and the ACE/Server.

Likelihood: Medium: Network outages and routing issues could cause loss of communication and can block access to the machine.

Impact: Machine cannot authenticate with the Ace/Server and resources are blocked.

Compliance: RSA Ace/Server communication test should be successful.

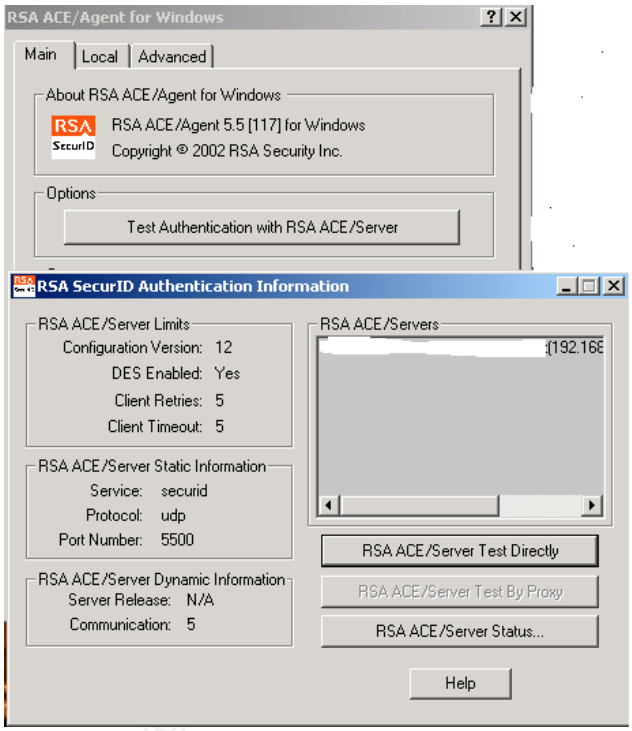
Testing:

On a Client machine

As an administrator: Open My computer->Control Panel-> RSA ACE/Agent tab

Click on the RSA ACE/Server Test Directly

An authentication window will appear.
Log in as you would normally and make sure that the test is successful.



Test type: Objective. Connection test must be successful.

Item #20 Check logon success and logon failure auditing

Reference: Audit Logon events, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/518.asp

Control objective: This test will help verify the OS logging settings of the Ace/Agent and Ace/Server and enhance the quality of the information that can be gathered after a machine is compromised.

Risk:

Potential Threat: Logon logging is important for the forensic process. Important information could be lost if logon successes aren't logged. Logon success will give administrator a list of successful logon's on the machine and the logon failures will help administrators pinpoint potential brute force attacks on OS passwords.

Threat level: Medium: Logon successes can confirm that a machine was successfully broken into.

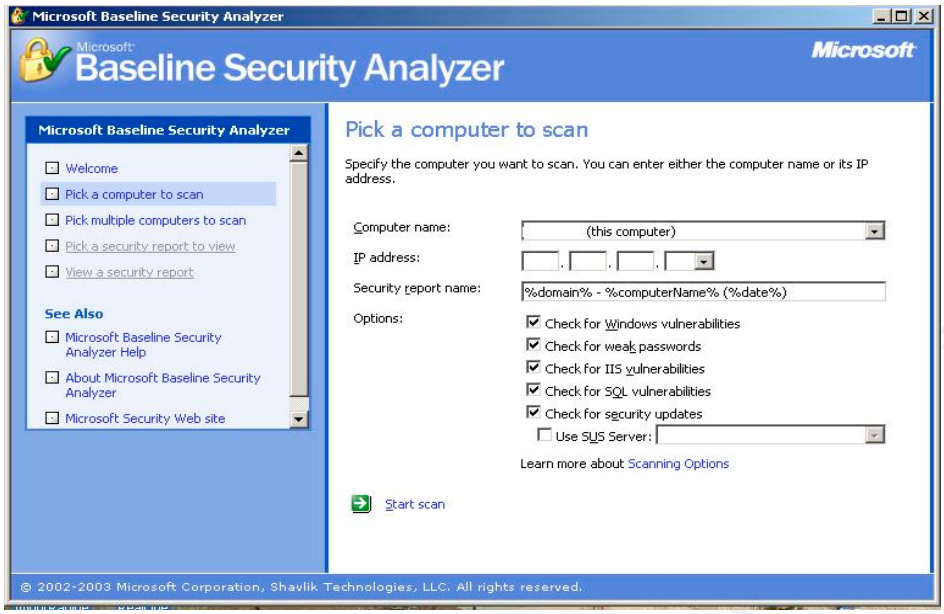
Likelihood: Most administrators believe that logging success logons is enough.

Impact: Logging logon failures by themselves will not help an administrator determine if a brute force attack was successful. Multiple logon failures followed by a logon success is a good indication that one of the passwords was successfully broken. It is important that logon successes be logged properly.

Compliance: Both logon success and logon failures must be enabled. This will guarantee that brute force attacks are detected properly.

Testing:

Run the Microsoft Baseline Security Analyzer on the local machine. The install process is self-explanatory. Run all the tests shown below.



Make sure that that Logon Success and Logon Failure auditing are both enabled on the Ace/Server and Ace/Agent.

Test type: Objective. The values detected by the Baseline Analyzer must be correct.

Assignment #3 Audit Evidence

Tests performed

Test #4 TEST FAILED
Null Sessions

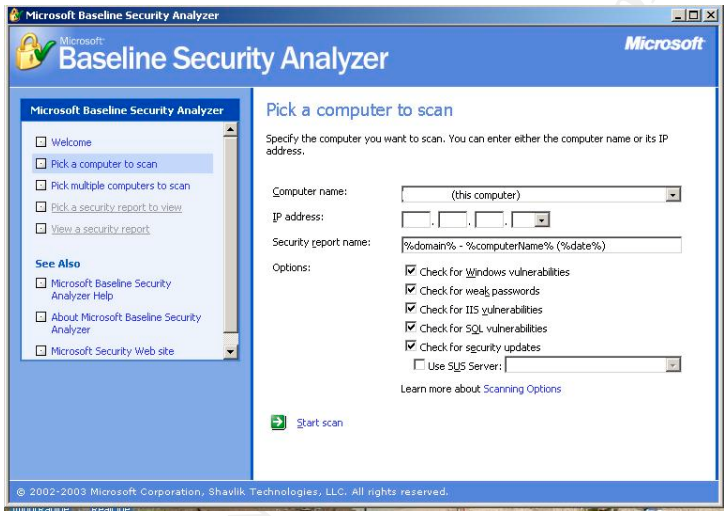
Testing Results:
Null session: Opened a CMD prompt (Start->Run->CMD) and ran the following command:

net use \\123.456.789.123\ipc$ "" /user:""

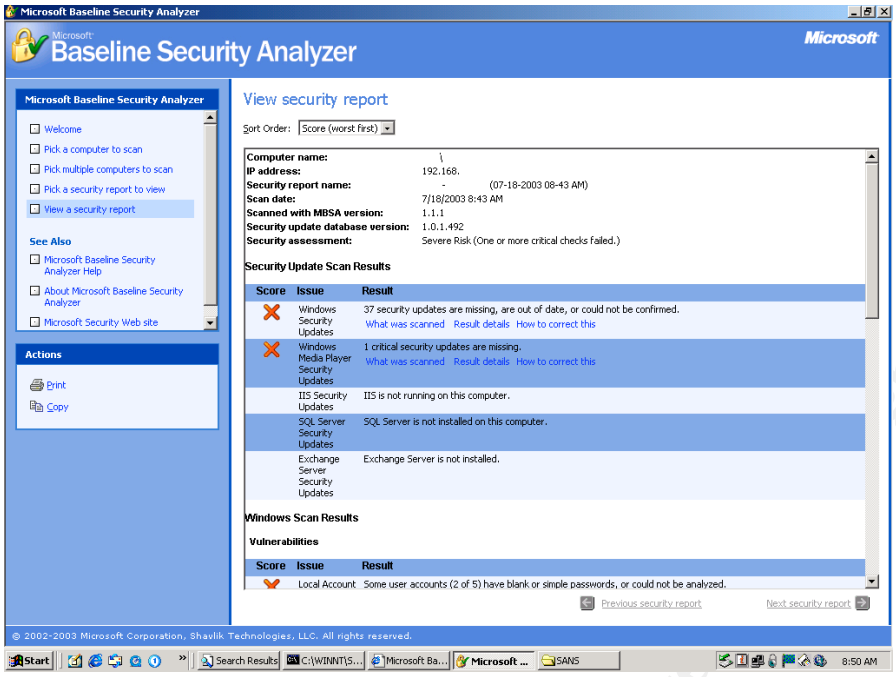
The command was run for the ACE/Server and the Ace/Agent machine (client)

Both commands were successful, which means that both machines are susceptible to attack. (Findings 1)

Run the Microsoft Baseline Security Analyzer on the local machine. Run all the tests shown below.



Ace/Agent Results:



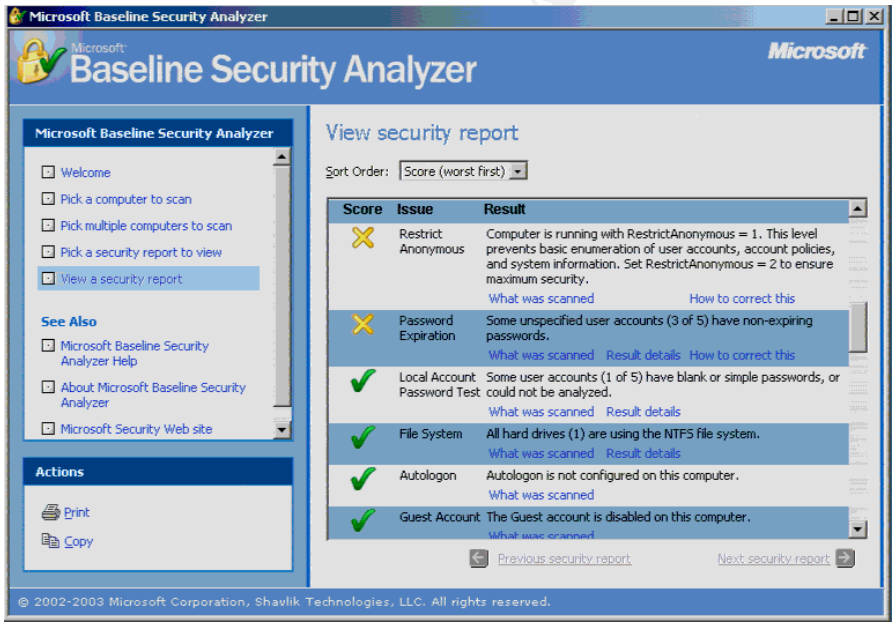
Complete Ace/Agent Results:

Test	Score	Issue	Details
Security updates	Vulnerabilities Check failed (critical)	Windows Security Updates	37 security updates are missing, are out of date, or could not be confirmed.
Security updates	Vulnerabilities Check failed (critical)	Windows Media Player Security Updates	1 critical security updates are missing.
Security updates	Vulnerabilities Check not performed	Exchange Server Security Updates	Exchange Server is not installed.
Security updates	Vulnerabilities Check not performed	SQL Server Security Updates	SQL Server is not installed on this computer.
Security updates	Vulnerabilities Check not performed	IIS Security Updates	IIS is not running on this computer.
Windows Scan Results	Vulnerabilities Check failed (critical)	Local Account Password Test	Some user accounts (2 of 5) have blank or simple passwords, or could not be analyzed.
Windows Scan Results	Vulnerabilities Check failed (non-	Password Expiration	Some unspecified user accounts (4 of

	critical)		5) have non-expiring passwords.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Restrict Anonymous	Computer is running with RestrictAnonymous = 1. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. (Findings 1)
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Administrators	More than 2 Administrators were found on this computer.
Windows Scan Results	Vulnerabilities Check passed	File System	All hard drives (1) are using the NTFS file system.
Windows Scan Results	Vulnerabilities Check passed	Guest Account	The Guest account is disabled on this computer.
Windows Scan Results	Vulnerabilities Check passed	Autologon	Autologon is not configured on this computer.
Windows Scan Results	Additional System Information	Additional information	Windows Version Computer is running Windows 2000 or greater.
Windows Scan Results	Additional System Information	Best practice Auditing	Logon Success and Logon Failure auditing are both enabled.
Windows Scan Results	Additional System Information	Additional information	Shares 0 share(s) are present on your computer.
Windows Scan Results	Additional System Information	Best practice Services	Some potentially unnecessary services are installed.
Internet	Additional System	Best practice	IIS is not running

Information Services (IIS) Scan Results	Information	IIS Status	on this computer.
SQL Server Scan Results	Product Status	SQL Server Status	SQL Server is not installed on this computer.
Desktop Application Scan Results	Vulnerabilities Check failed (critical)	IE Zones	Internet Explorer zones do not have secure settings for some users.
Desktop Application Scan Results	Vulnerabilities Check failed (non-critical)	Macro Security	Macro Security 4 Microsoft Office product(s) are installed. Some issues were found.
Desktop Application Scan Results	Vulnerabilities Check passed	Outlook Zones	Microsoft Outlook 2000: No security issues were found.

Ace/Server Results:



Complete Ace/Server Results

Test	Score	Issue	Details
Security updates	Vulnerabilities Check failed	Windows Security Updates	12 security updates are

	(critical)		missing, are out of date, or could not be confirmed.
Security updates	Vulnerabilities Check failed (critical)	Windows Media Player Security Updates	1 critical security updates are missing.
Security updates	Vulnerabilities Check passed	IIS Security Updates	No critical security updates are missing.
Security updates	Vulnerabilities Check not performed	Exchange Server Security Updates	Exchange Server is not installed.
Security updates	Vulnerabilities Check not performed	SQL Server Security Updates	SQL Server is not installed on this computer.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Password Expiration	Some unspecified user accounts (3 of 5) have non-expiring passwords.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Restrict Anonymous	Computer is running with RestrictAnonymous = 1. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. (Findings 1)
Windows Scan Results	Vulnerabilities Check passed	Local Account Password Test	Some user accounts (1 of 5) have blank or simple passwords, or could not be analyzed.
Windows Scan Results	Vulnerabilities Check passed	File System	All hard drives (1) are using the NTFS file system.
Windows Scan Results	Vulnerabilities Check passed	Guest Account	The Guest account is disabled on this computer.

Windows Scan Results	Vulnerabilities Check passed	Autologon	Autologon is not configured on this computer.
Windows Scan Results	Vulnerabilities Check passed	Administrators	No more than 2 Administrators were found on this computer.
Windows Scan Results	Additional System Information	Additional information	Windows Version Computer is running Windows 2000 or greater.
Windows Scan Results	Additional System Information	Best practice Auditing	Logon Success and Logon Failure auditing are both enabled.
Windows Scan Results	Additional System Information	Additional information Shares	0 share(s) are present on your computer.
Windows Scan Results	Additional System Information	Best practice Services	Some potentially unnecessary services are installed.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (critical)	Sample Applications	Some IIS sample applications are installed.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (critical)	Parent Paths	Parent paths are enabled in some web sites and/or virtual directories.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (critical)	IIS Lockdown Tool	The IIS Lockdown tool has not been run on the machine.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (non-critical)	Msadc and Scripts Virtual Directories	MSADC virtual directory was found under the default web site. Scripts virtual directory was found under the default web site.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check passed	IIS Admin Virtual Directory	IISADMPWD virtual directory is not present.

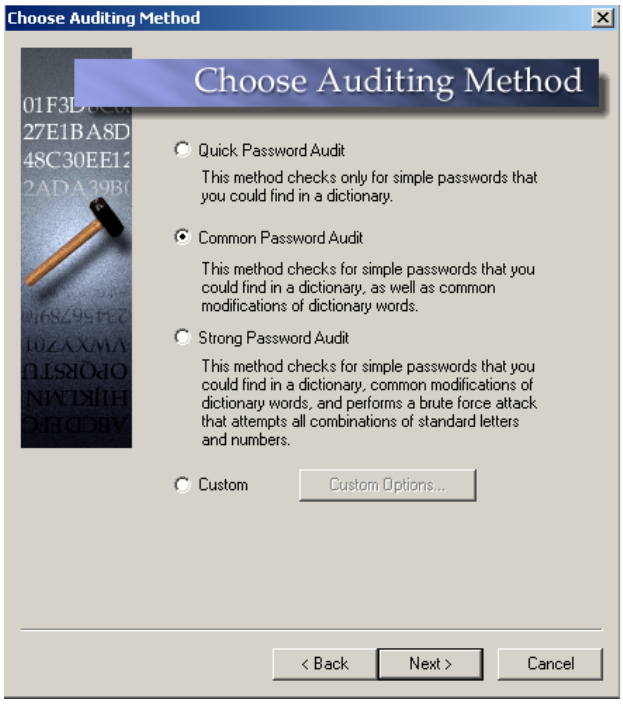
Internet Information Services (IIS) Scan Results	Additional System Information	Best practice Domain Controller Test	IIS is not running on a domain controller.
Internet Information Services (IIS) Scan Results	Additional System Information	Best practice IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options.
SQL Server Scan Results	Product Status	Best practice SQL Server Status	SQL Server is not installed on this computer.
Desktop Application Scan Results	Vulnerabilities Check passed	IE Zones	Internet Explorer zones have secure settings for all users.
Desktop Application Scan Results	Vulnerabilities Check not performed	Outlook Zones	No Microsoft Office products are installed
Desktop Application Scan Results	Vulnerabilities Check not performed	Macro Security	No Microsoft Office products are installed

Conclusion:
The RestrictAnonymous variable is set to 1 (for both machines) and does not match the standard. Considering that both machines are susceptible to attack (by null session), this test has failed.

Test #6 (Stimulus/Response #1) TEST FAILED
Test OS Password complexity

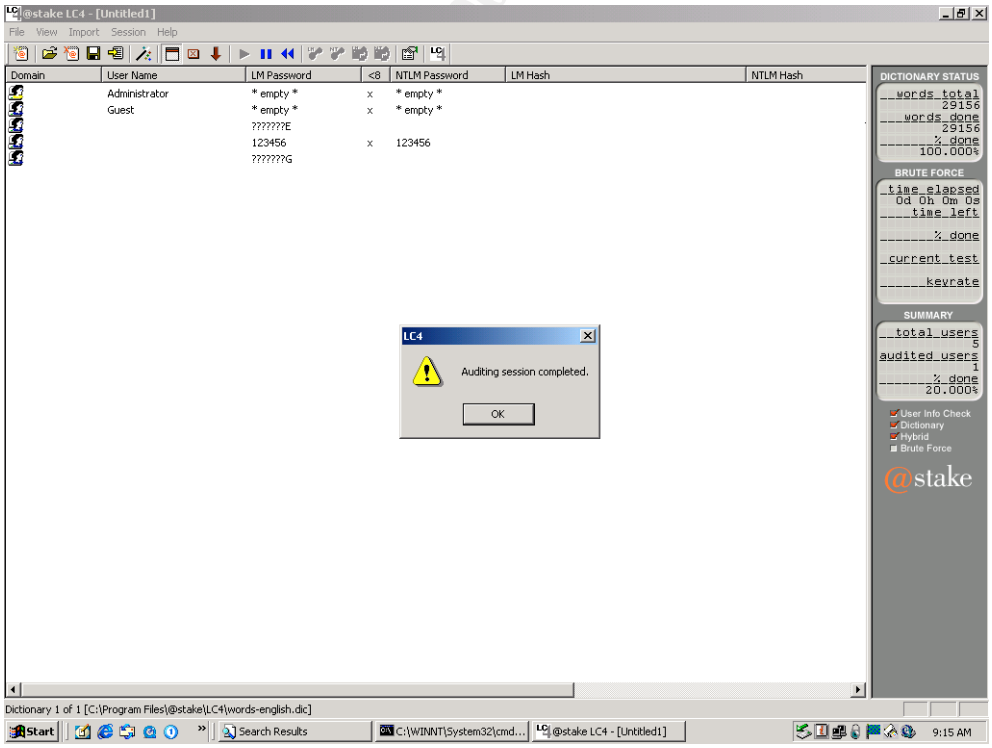
Testing Results:

Installed LC4 locally on Ace/Agent and Ace Server.
Selected a Common Password Audit (Trial version does not support the brute force option).



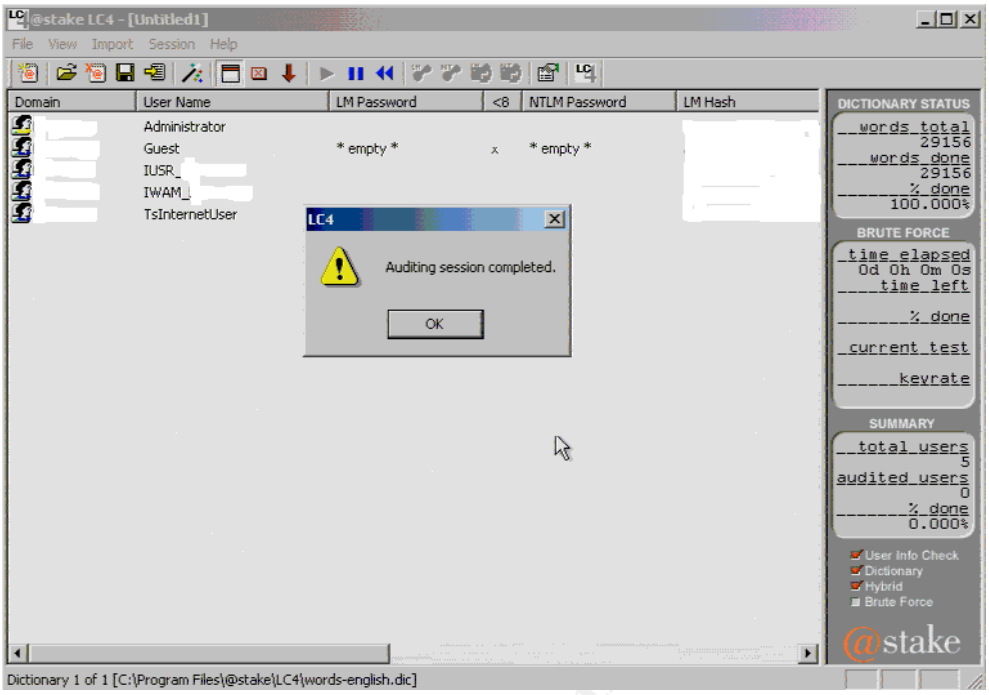
Ace/Client Results:

The usernames/hashes were “blanked” for security reasons



(Findings 2)

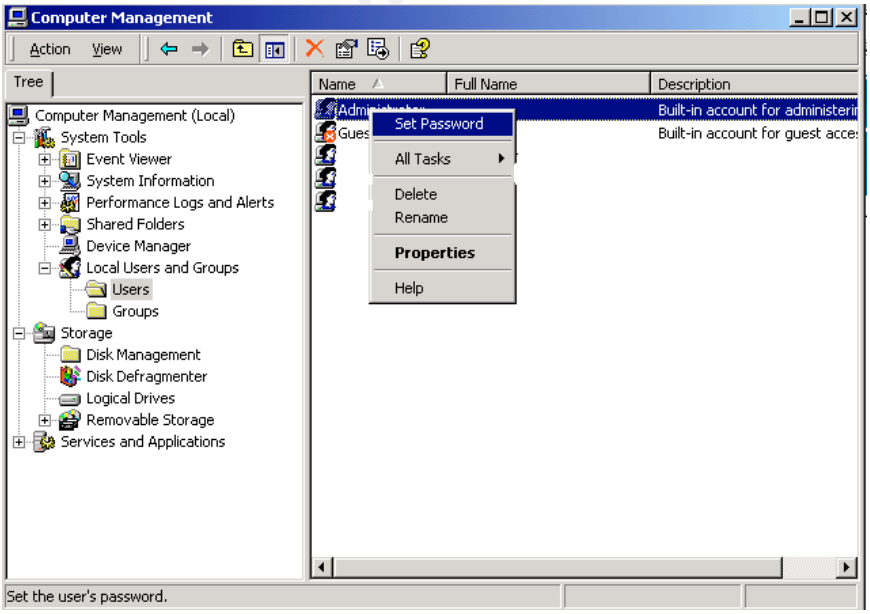
Ace/Server Results:

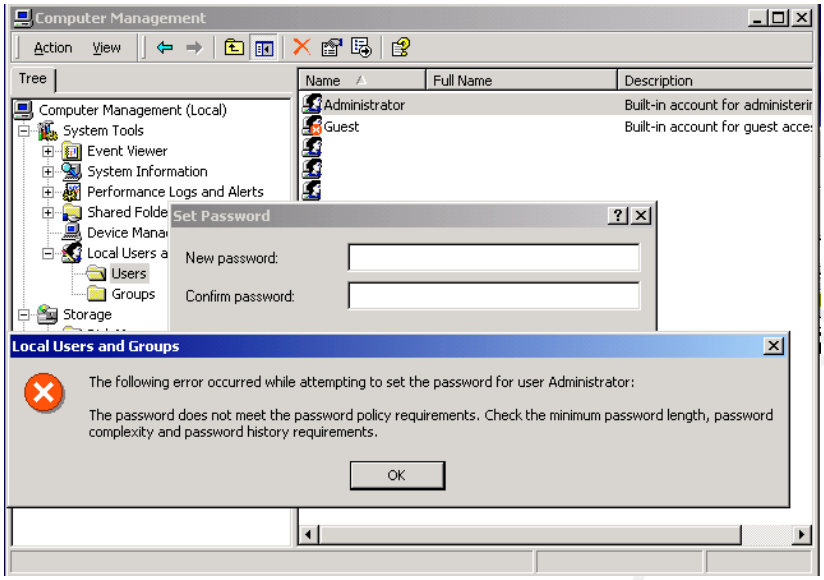


(Findings 3)

Attempt to change administrator password to a value of 123456 on Ace/Agent and Ace/Server

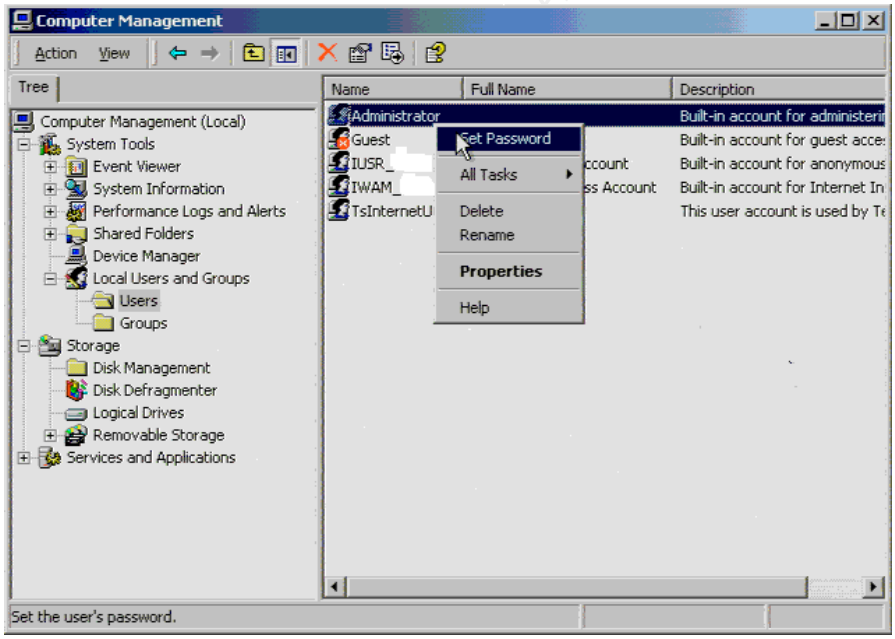
Ace/Agent Results

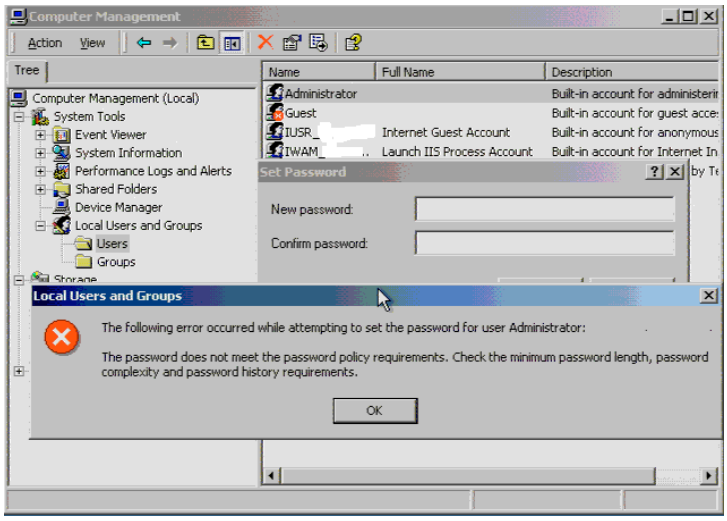




The change attempt was refused. (Findings 4)

ACE/Server





The change attempt was also refused. (Findings 4)

Conclusion:
An ACE/Agent password was cracked easily and does not meet the complexity requirements. Test has failed.

Test #7 TEST FAILED
Account policies check.

Testing Results:

Downloaded and installed the CIS scoring tool and Common baseline templates (http://www.cisecurity.org/bench_win2000.html).

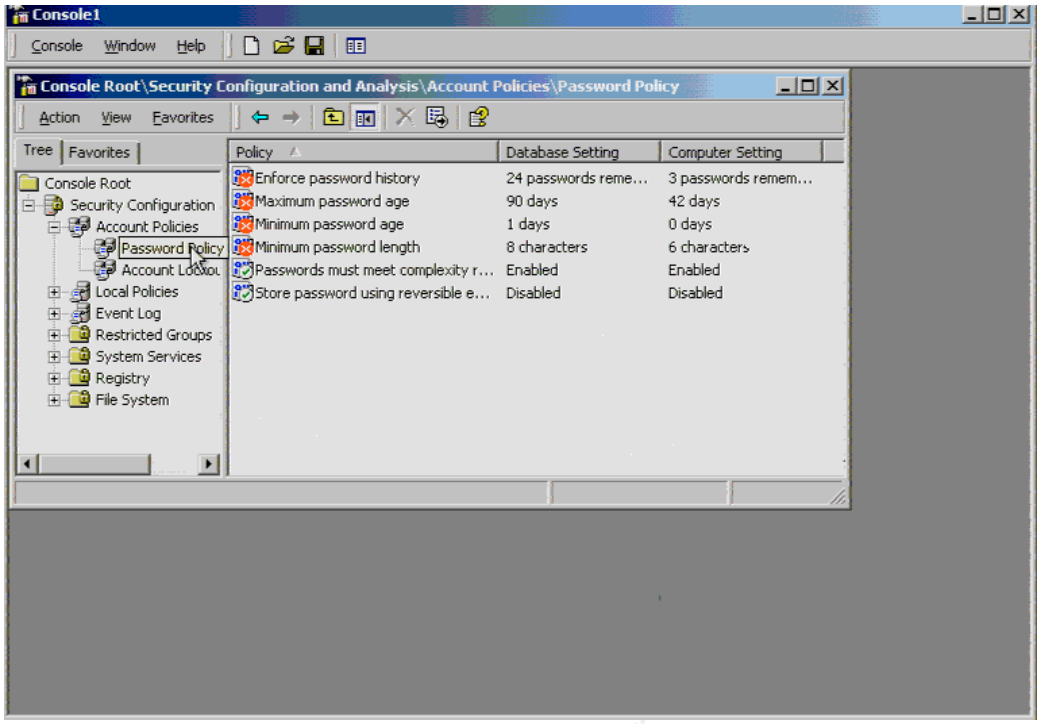
Open up the MMC: Start->Run->MMC
Click on Console->Add remove snap-In then Click on Add
Double click on The Security configuration and Analysis then click on Close
Click OK to come back to the main MMC window
Follow the instruction on screen and create a new database

When you are prompted to import a template, use **CIS-Win2K-Level-I-v1.1.7.inf** file from the CIS scoring tool install directory.

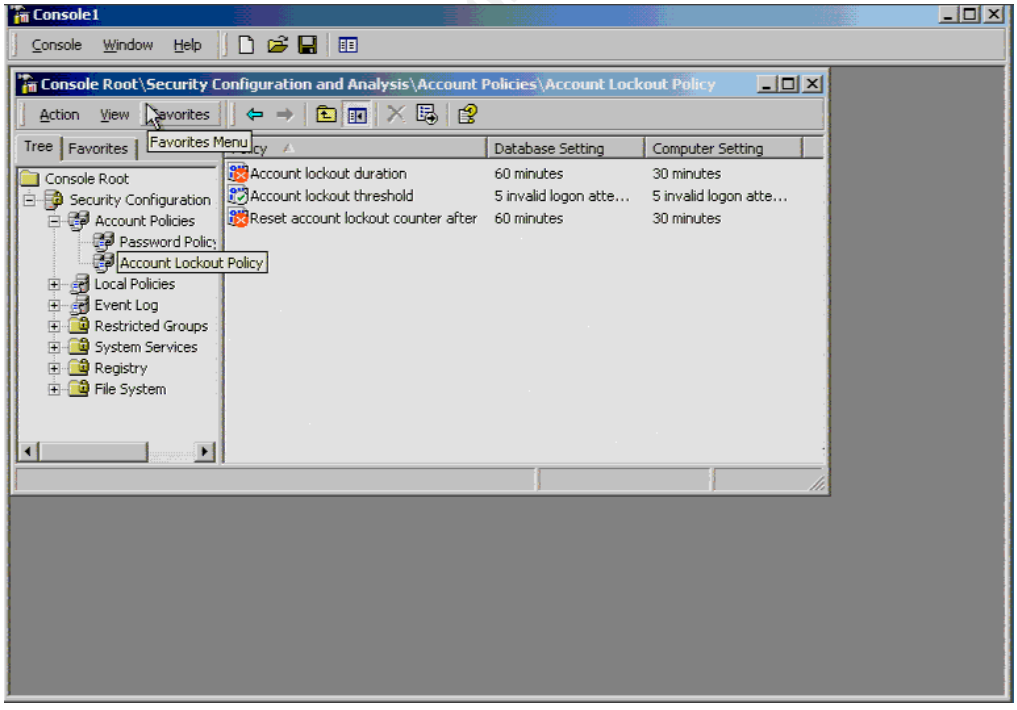
Right click on the SEC tab and Start to analyze the machine.

Compare the results with the template (Database setting is the template, Computer Setting Is the current settings).

ACE/Server Results:



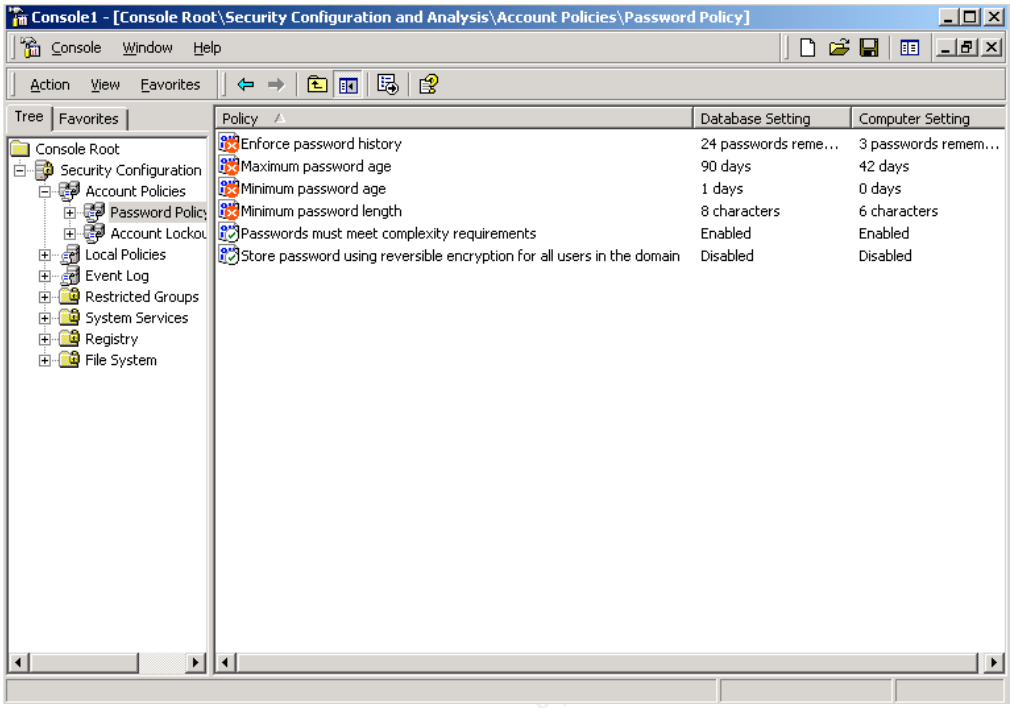
Minimum password length is too small (Findings 5)
Password history is too short



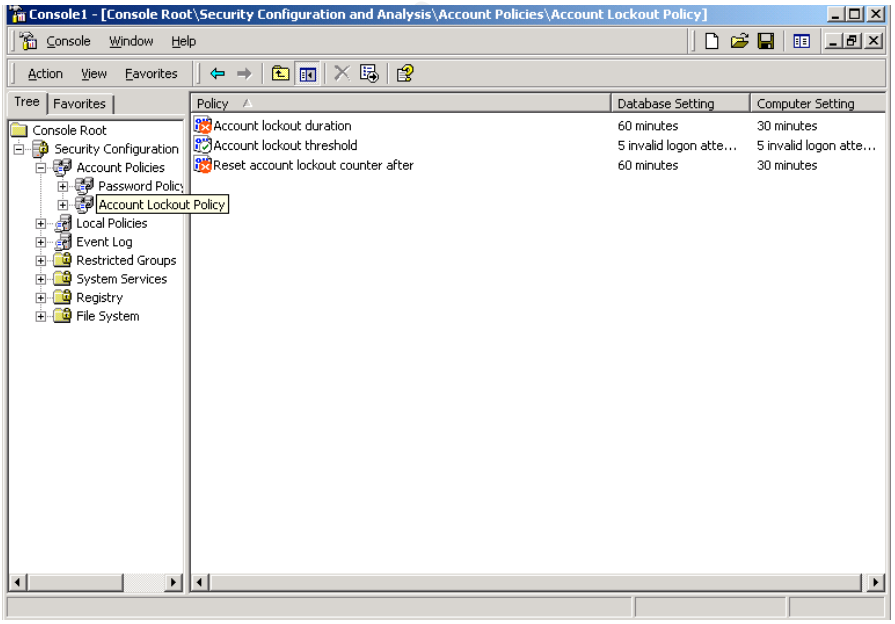
Account lockout duration too short (Findings 6)

Account lockout counter too short

Ace/Agent Results



Minimum password length is too small (Findings 7)
Password history is too short



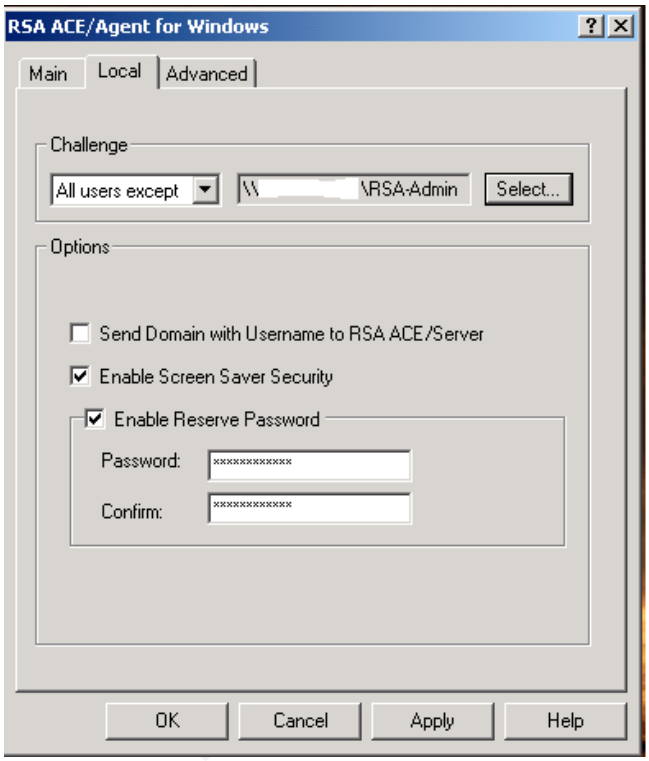
Account lockout duration too short. (Findings 8)
Account lockout counter too short.

Conclusion:
All test have failed. The settings are not restrictive enough.

Test #9 TEST PASSED
All users “except:” clause is invoked

Testing Results:

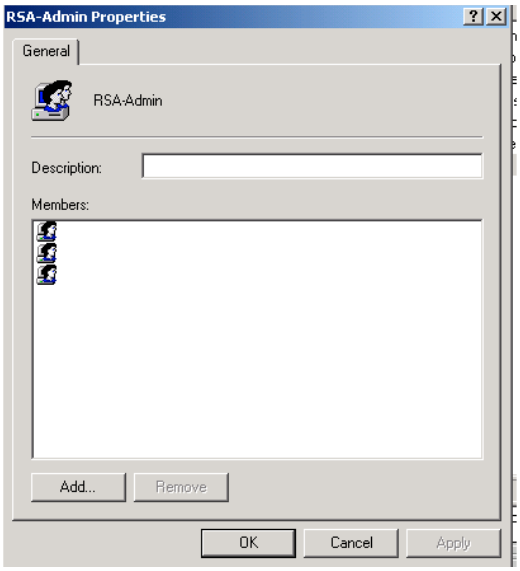
As an administrator: Open My computer->Control Panel-> RSA ACE/Agent tab. Go to the Local tab and see what the Challenge field is showing.



(Findings 9)

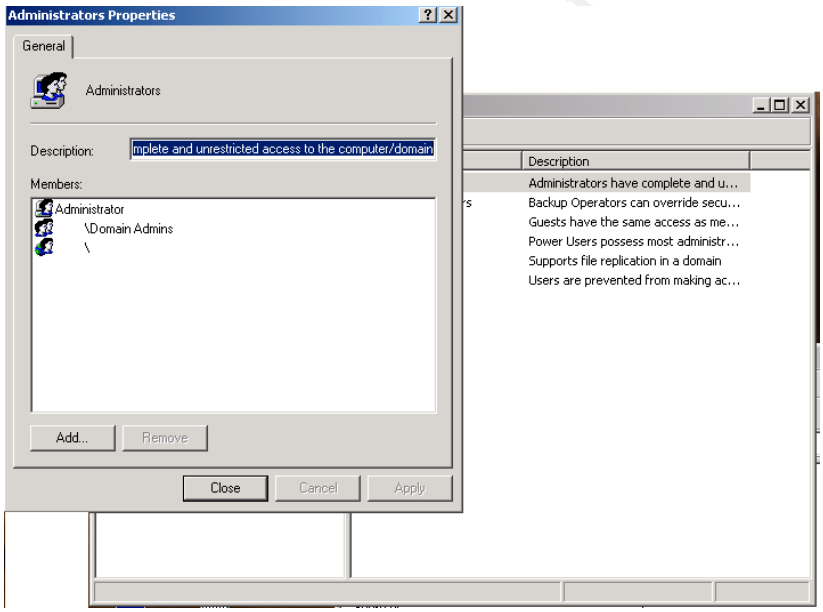
Since the “All users except” clause was used we must check that the group in question is not an administrator group

These are the accounts belonging to the RSA-Admin group.
(Account names were blanked)



Now we have to make sure that the accounts do not belong to the Administrator group. (Findings 9)

Here are the members of the Administrator Group:



The accounts belonging to the RSA-Admin group do not belong to the administration group of the machine or the domain. (Findings 9)

Conclusion:
Test Passed. RSA-Admin group accounts do not have administrator privileges.

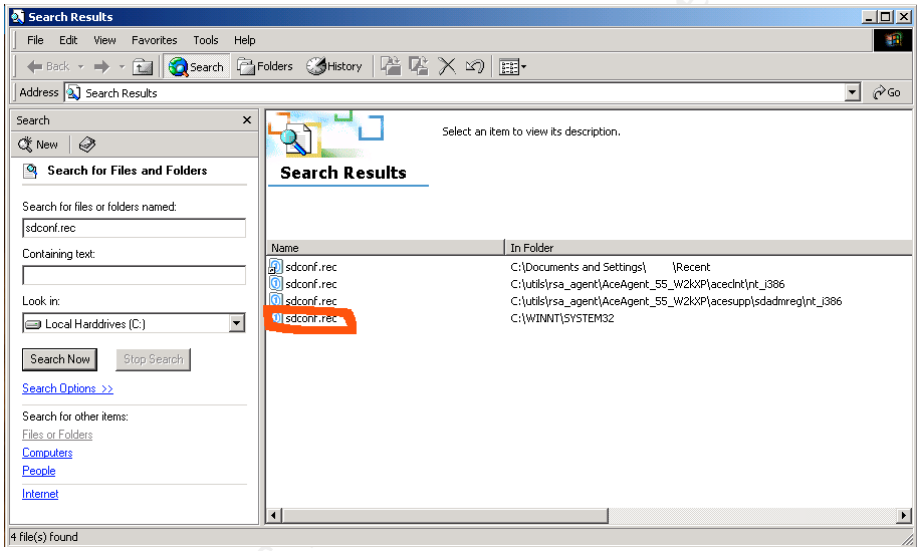
Test #10 TEST FAILED
Sdconf.rec file used at install is current and the same as the one generated on the Server.

Testing Results:

Downloaded md5sum.exe (http://www.etree.org/md5com.html) and compared the 2 files in questions

ACE/Server: Go to the RSA configuration directory (usually C:\RSA\ACE\Data\Config_files)
And copied the Sdconf.rec file to a floppy (Renamed file to Server-Sdconf.rec)

Client: Searched for the Sdconf.rec file on the client (Start->Search->For Files or Folders) and copied it to the same floppy (Renamed file to Client-Sdconf.rec).

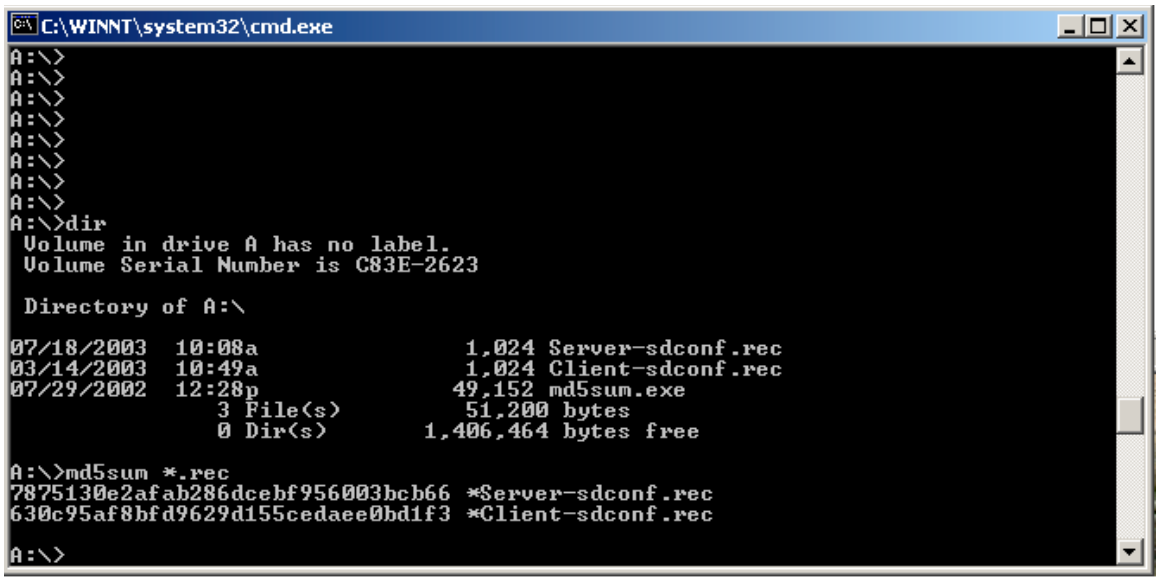


Copy md5sum.exe to the floppy

Open a CMD window (Start->Run->CMD) and go to the floppy drive (type A:)

At the prompt type “md5sum *.rec”

Output



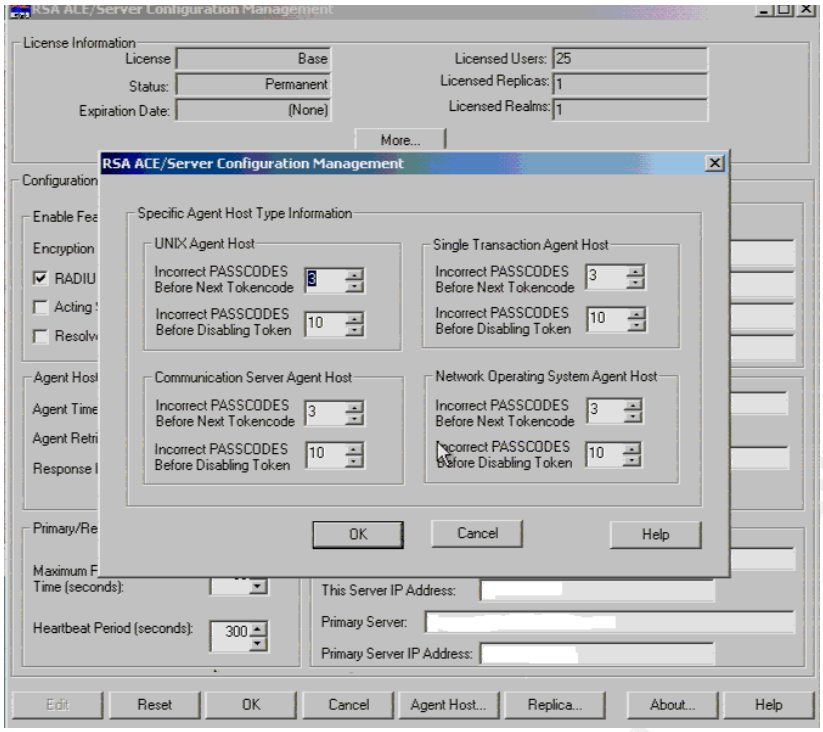
(Findings 10)
Conclusion:
The Checksum's do not match. This means that the files are not identical.
Test has failed.

Test #12 (Stimulus/Response #2) TEST PASSED
SecurID next tokencode checks

Testing Results:

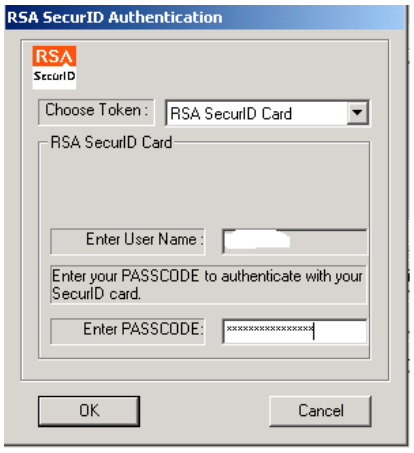
ACE/Server: Open up the Configuration Management console (Start->Programs -> RSA ACE/Server -> Configuration Management

Click on Agent



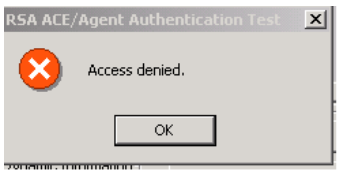
The Values match the default minimum values. (Findings 11)

Now we must test that 3 consecutive failed logons will put the token into Next token Mode.



We input random passwords (4 times). Each time we get the same results:

The access denied screen

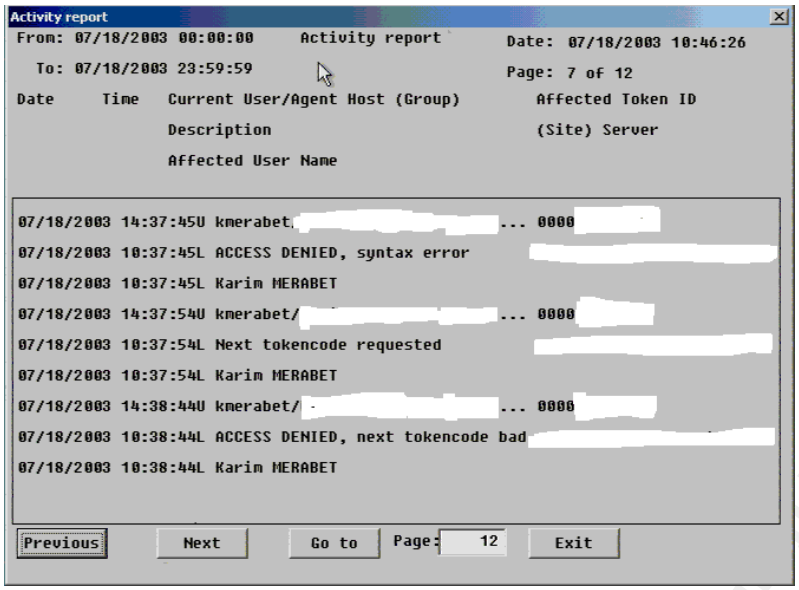


When we enter a valid Passcode, we get the following screen:

(Successful logon after at least 3 consecutive failed attempts)

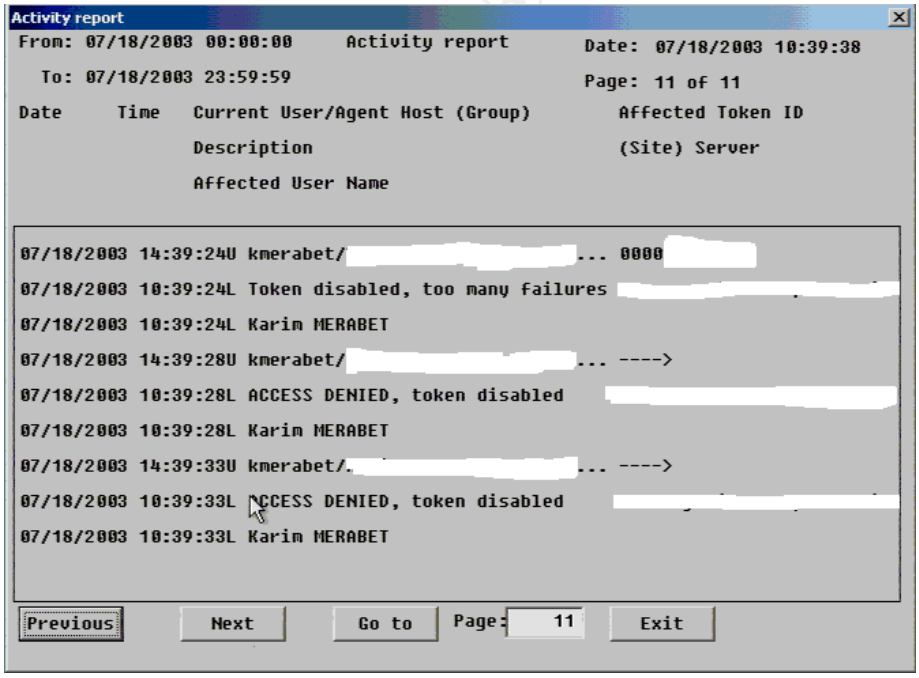
This implies that our failed attempts successfully set the Token to Next Token mode. (Findings 11)

Now we must verify that the Ace/Server Logs reflect the change.



(Findings 11)

We will now test 10 consecutive failed attempts.
Like on the previous test, the 10 consecutive failed logins resulted in the Access Denied Screen. We then checked the ACE/Server Logs to verify that the token was indeed disabled:



(Findings 12)

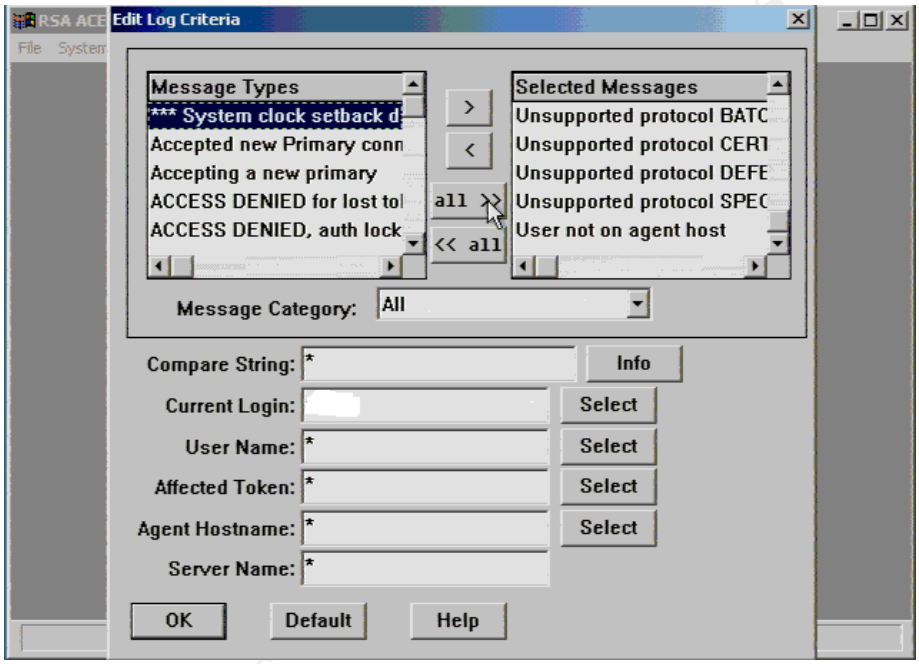
Conclusion:
Both checks were successful. Test Passed.

Test #13 (Stimulus/Response #3) TEST PASSED
SecurID Access logs are backed/maintained and consulted regularly

Testing Results:

Verify that the fields being logged are adequate.

The fields being logged must match the minimum Default values. If a high level of security is required. All message fields should be enabled.



(Findings 13)

All Logging fields are enabled.

We now inquired on the current log management methods.

Question	Response
How do you store your logs?	On Tape, at an Offsite location.
How often are logs rotated?	They haven't been rotated yet. Far from HD limit.
How often are logs reviewed for unusual Errors?	Everyday
How often are logs reviewed for	Everyday

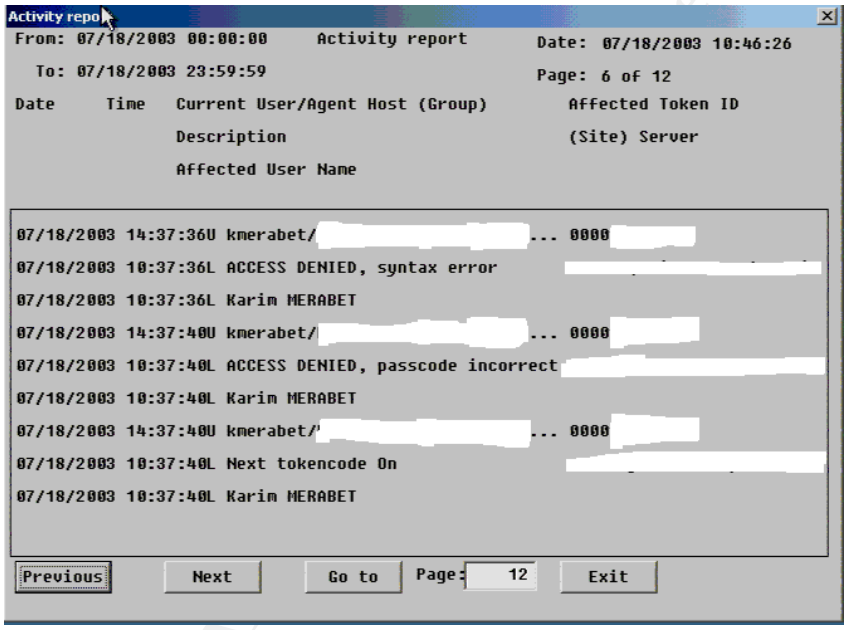
Access violations?	
What is your backup strategy for the ACE/Server and how often are backups performed	Full Backups are made each week, With Incremental backups made everyday at 1:00 AM.

The answers are compliant with the Security Policy guidelines and meet the minimum guidelines. The general behavior of administrators matches the survey results (log reviews were performed regularly, backup tapes were examined, and proof of offsite storage was shown).

Now we must generate some events and see if they are logged properly.

An account was created for the auditor and the auditor generated some failed logons.

The Logs showed the following results:



(Findings 14)

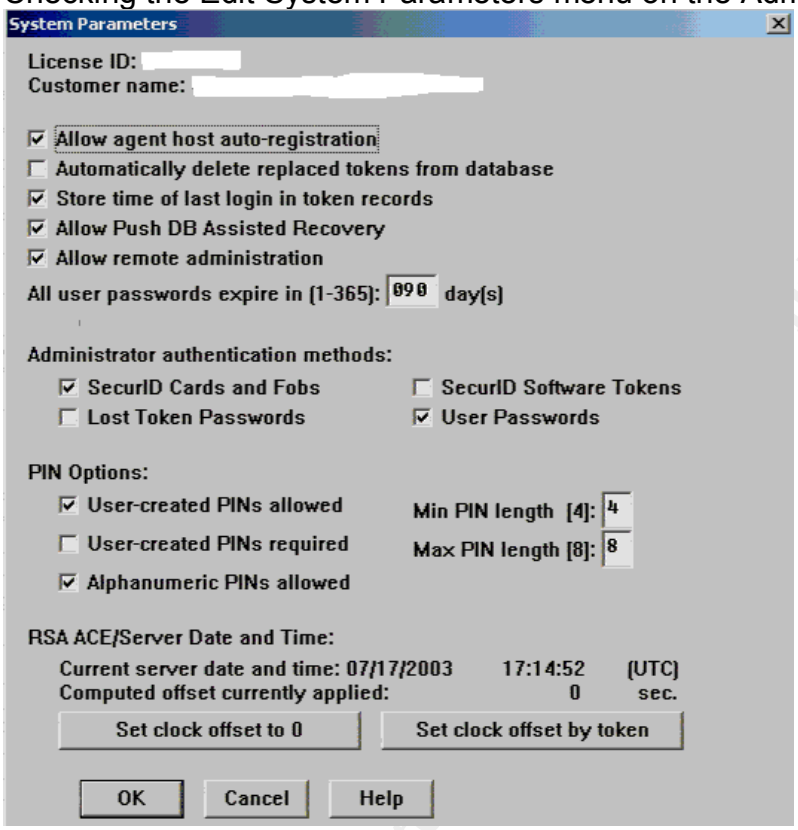
The Failed logons were successfully logged. Logging seems to be working properly and all prior test events were found.

Conclusion:
Logging is working as intended. All fields are logged and seem to be behaving properly. Test Successful.

Test #17 (Stimulus/Response #4) TEST PASSED
PIN Length and type is correct

Testing Results:

Checking the Edit System Parameters menu on the Administration Console:

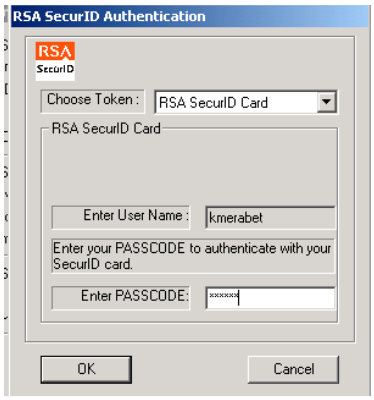


Min Pin Length = 4
Max Pin Length = 8
Alphanumeric PINS should be allowed = Checked
(Findings 15)

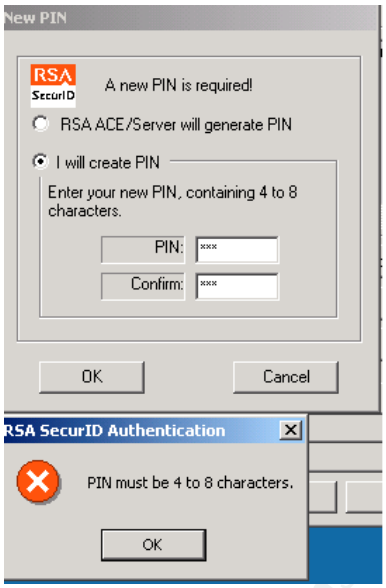
The Settings match the default values.

Now we must check if the ACE/Server will accept wrong values and verify that alphanumeric PINs work.

New Token was assigned to auditor and Set to New PIN Mode.
Auditor must input only the token number to get access to the Create Pin Screen:



At the Create New PIN Menu
Attempt to create a 3 Char PIN:



Command Failed.

At the Create New PIN Menu
Attempt to create a 9 Char PIN:

More than 8 characters PIN not allowed (cannot fit in box)

(Findings 16)

Attempt to create an alphanumeric PIN:

The PIN was allowed. Test was successful.

(Findings 17)

Conclusion:
All tests were successful. Test is then successful.

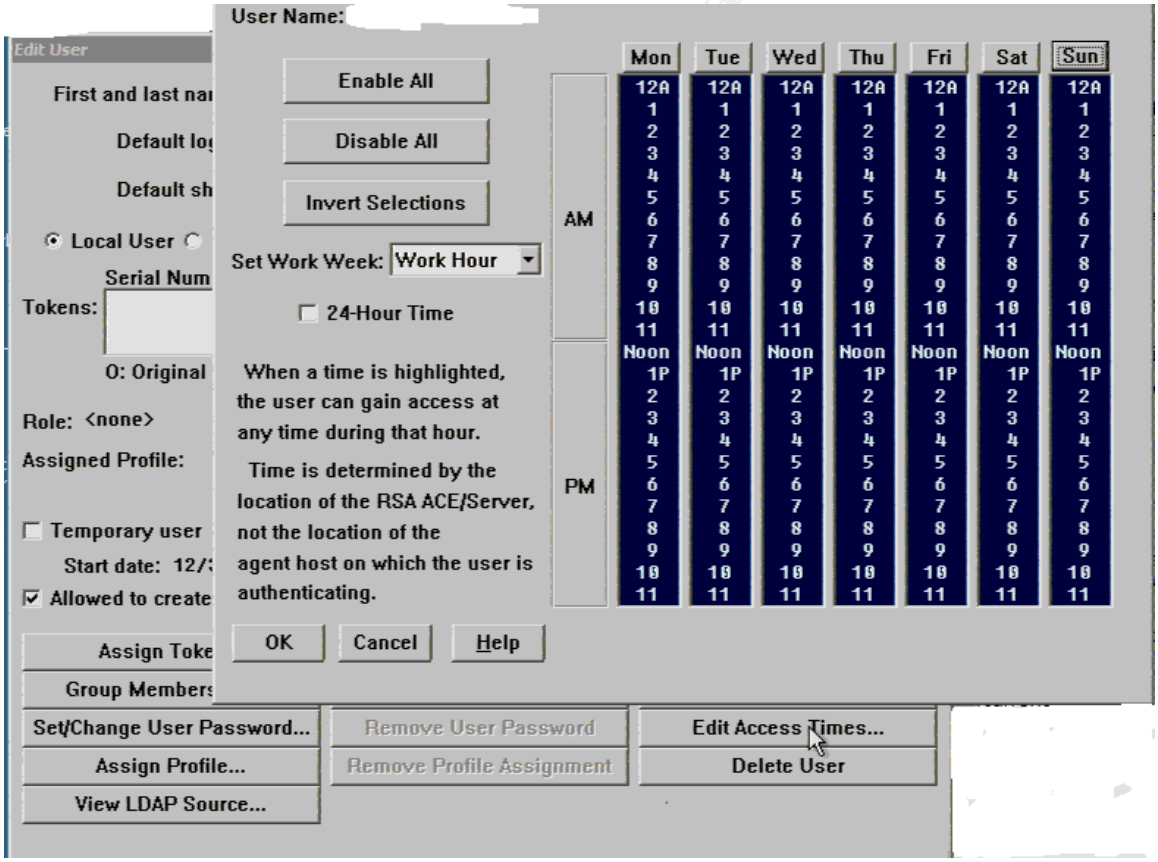
Test #18 (Stimulus/Response #5) TEST PASSED
Access times are set correctly

Testing Results:

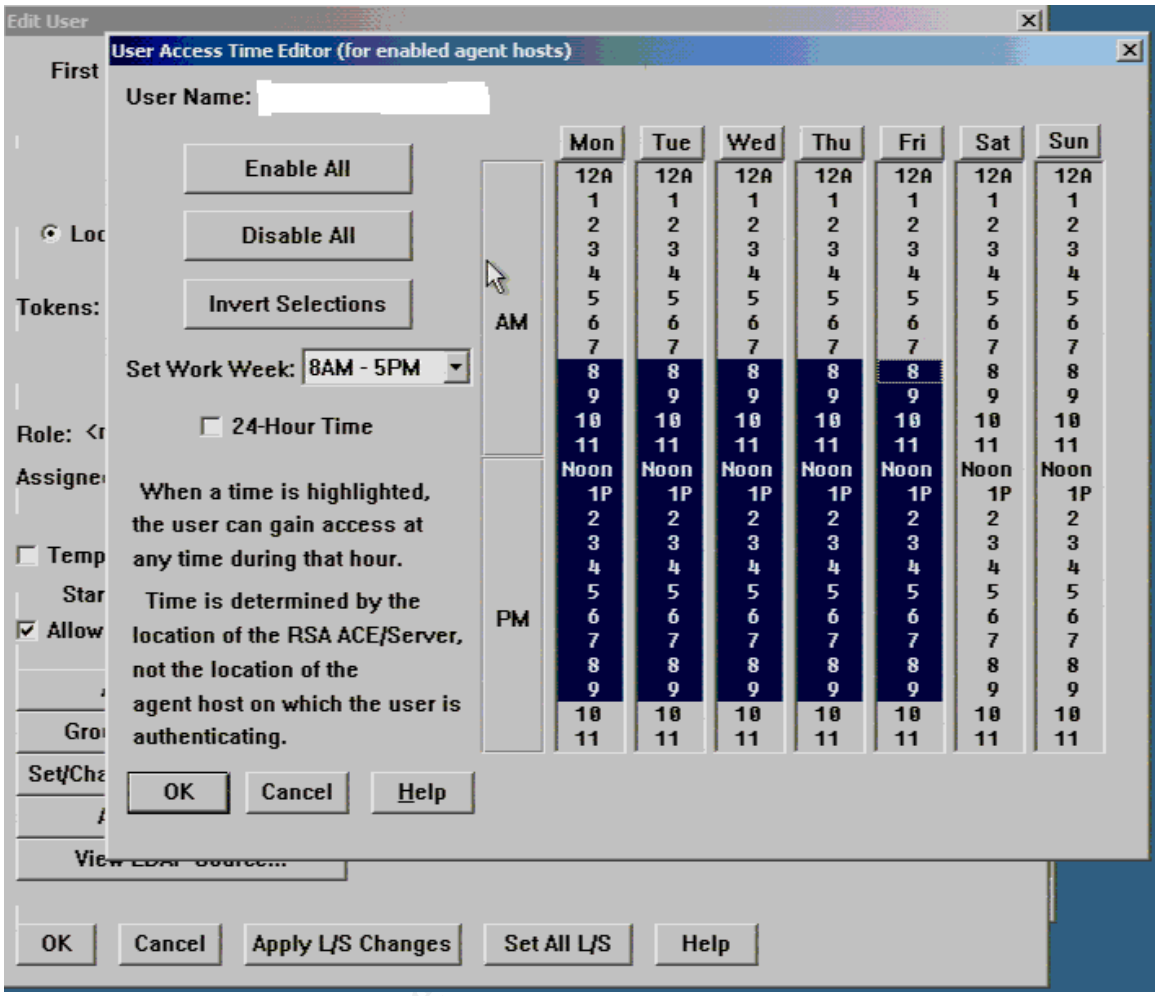
Start the Administration console. Click on user->edit users

For each users Click on Edit Access times

Make sure that the Access time is set to normal working hours + Offset time.



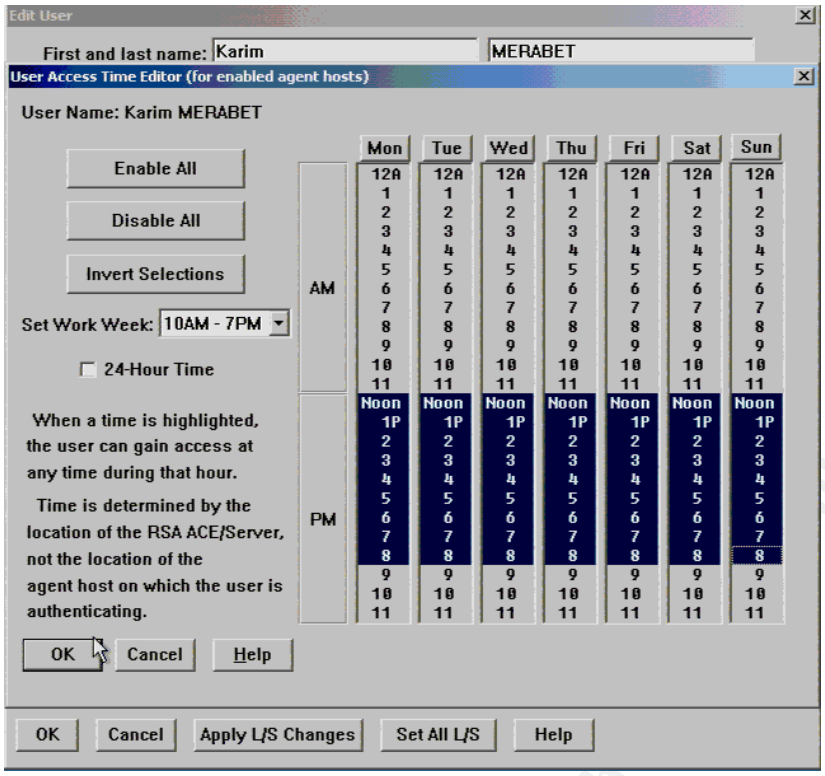
Access times limits are not set for administrators. SecurID authentication is allowed at all hours. These are “general use” machines and administrators are allowed to use them at all hours. This is an acceptable policy for this particular infrastructure. Normal users are restricted to normal work hours + 5.



(Findings 18)

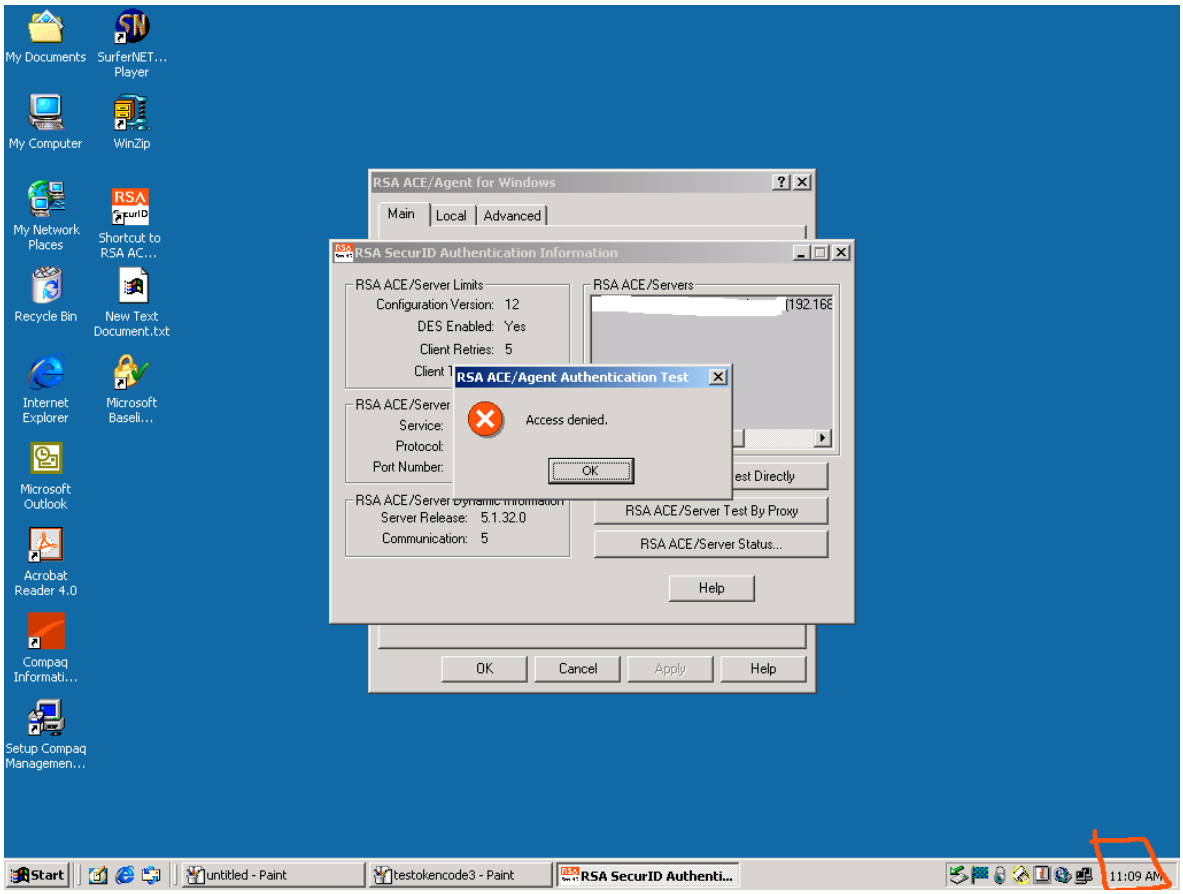
We must still test the effectiveness of the Access time feature.

The auditor's SecurID access time was changed for testing purposes. Access Time was set from NOON to 8PM

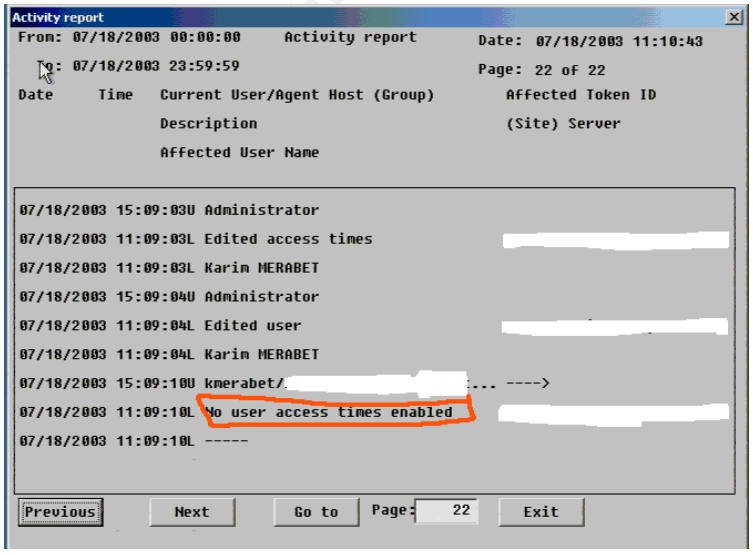


The auditor now attempted to logon at an improper time with the Test Connection Directly of the ACE/Agent.

Test connection on ACE/Agent machine at 11:09 AM



Now we must verify that the logs reflect this attempt at logon.
Logs on Ace/Server



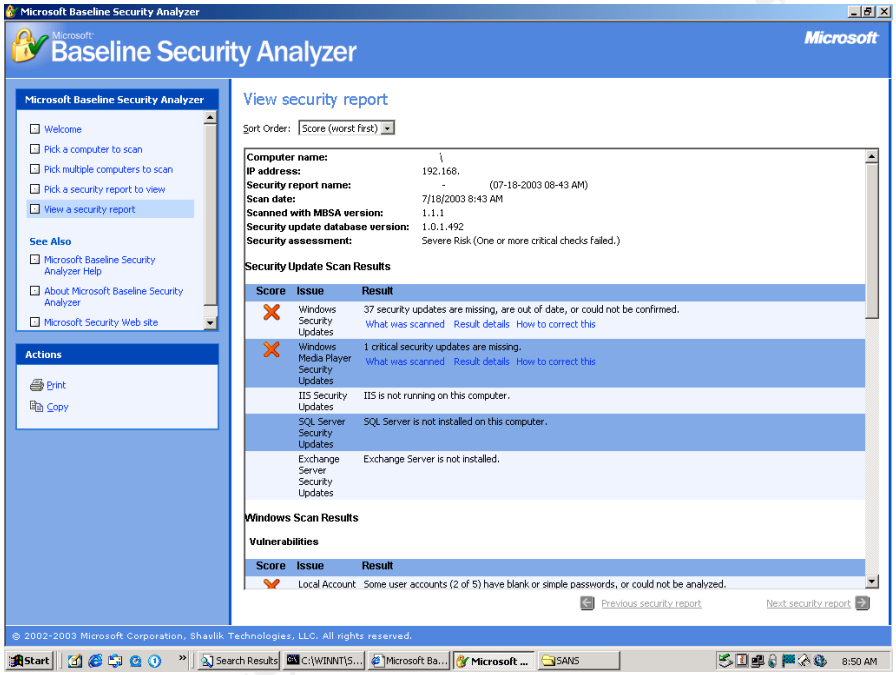
(Findings 19)

Conclusion:
Test was successful; all features are working as intended.

Test #20 TEST PASSED
Check logon success and logon failure auditing

Testing Results:

Ace/Agent Results:



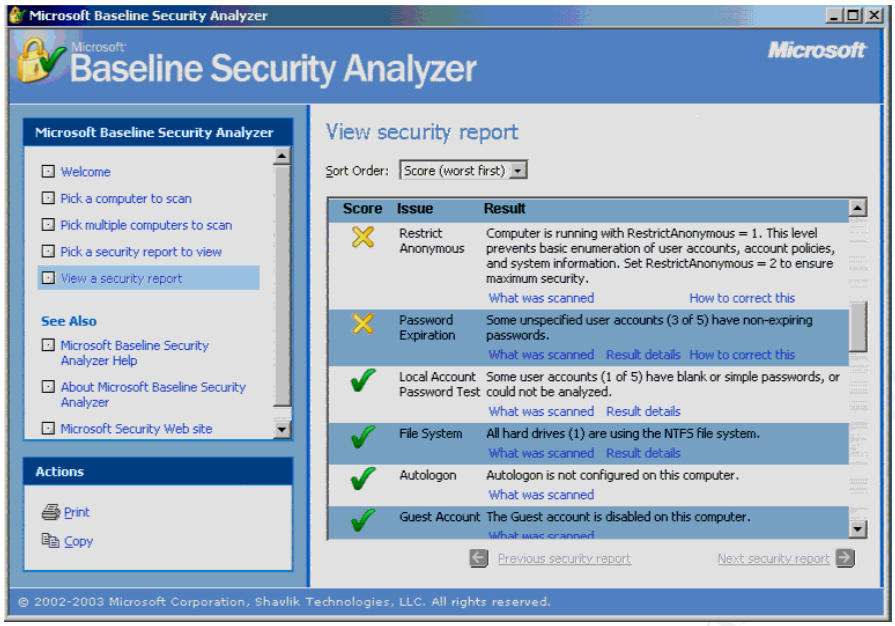
Complete Ace/Agent Results:

Test	Score	Issue	Details
Security updates	Vulnerabilities Check failed (critical)	Windows Security Updates	37 security updates are missing, are out of date, or could not be confirmed.
Security updates	Vulnerabilities Check failed (critical)	Windows Media Player Security Updates	1 critical security updates are missing.
Security updates	Vulnerabilities Check not	Exchange Server Security Updates	Exchange Server is not installed.

	performed		
Security updates	Vulnerabilities Check not performed	SQL Server Security Updates	SQL Server is not installed on this computer.
Security updates	Vulnerabilities Check not performed	IIS Security Updates	IIS is not running on this computer.
Windows Scan Results	Vulnerabilities Check failed (critical)	Local Account Password Test	Some user accounts (2 of 5) have blank or simple passwords, or could not be analyzed.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Password Expiration	Some unspecified user accounts (4 of 5) have non-expiring passwords.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Restrict Anonymous	Computer is running with RestrictAnonymous = 1. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Administrators	More than 2 Administrators were found on this computer.
Windows Scan Results	Vulnerabilities Check passed	File System	All hard drives (1) are using the NTFS file system.
Windows Scan Results	Vulnerabilities Check passed	Guest Account	The Guest account is disabled on this computer.
Windows Scan Results	Vulnerabilities Check passed	Autologon	Autologon is not configured on this computer.
Windows Scan	Additional System	Additional	Windows Version

Results	Information	information	Computer is running Windows 2000 or greater.
Windows Scan Results	Additional System Information	Best practice Auditing	Logon Success and Logon Failure auditing are both enabled. (Findings 20)
Windows Scan Results	Additional System Information	Additional information	Shares 0 share(s) are present on your computer.
Windows Scan Results	Additional System Information	Best practice Services	Some potentially unnecessary services are installed.
Internet Information Services (IIS) Scan Results	Additional System Information	Best practice IIS Status	IIS is not running on this computer.
SQL Server Scan Results	Product Status	SQL Server Status	SQL Server is not installed on this computer.
Desktop Application Scan Results	Vulnerabilities Check failed (critical)	IE Zones	Internet Explorer zones do not have secure settings for some users.
Desktop Application Scan Results	Vulnerabilities Check failed (non-critical)	Macro Security	Macro Security 4 Microsoft Office product(s) are installed. Some issues were found.
Desktop Application Scan Results	Vulnerabilities Check passed	Outlook Zones	Microsoft Outlook 2000: No security issues were found.

Ace/Server Results:



Complete Ace/Server Results

Test	Score	Issue	Details
Security updates	Vulnerabilities Check failed (critical)	Windows Security Updates	12 security updates are missing, are out of date, or could not be confirmed.
Security updates	Vulnerabilities Check failed (critical)	Windows Media Player Security Updates	1 critical security updates are missing.
Security updates	Vulnerabilities Check passed	IIS Security Updates	No critical security updates are missing.
Security updates	Vulnerabilities Check not performed	Exchange Server Security Updates	Exchange Server is not installed.
Security updates	Vulnerabilities Check not performed	SQL Server Security Updates	SQL Server is not installed on this computer.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Password Expiration	Some unspecified user accounts (3 of 5) have non-expiring passwords.
Windows Scan Results	Vulnerabilities Check failed (non-critical)	Restrict Anonymous	Computer is running with RestrictAnonymous

			= 1. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.
Windows Scan Results	Vulnerabilities Check passed	Local Account Password Test	Some user accounts (1 of 5) have blank or simple passwords, or could not be analyzed.
Windows Scan Results	Vulnerabilities Check passed	File System	All hard drives (1) are using the NTFS file system.
Windows Scan Results	Vulnerabilities Check passed	Guest Account	The Guest account is disabled on this computer.
Windows Scan Results	Vulnerabilities Check passed	Autologon	Autologon is not configured on this computer.
Windows Scan Results	Vulnerabilities Check passed	Administrators	No more than 2 Administrators were found on this computer.
Windows Scan Results	Additional System Information	Additional information	Windows Version Computer is running Windows 2000 or greater.
Windows Scan Results	Additional System Information	Best practice Auditing	Logon Success and Logon Failure auditing are both enabled. (Findings 20)
Windows Scan Results	Additional System Information	Additional information Shares	0 share(s) are present on your computer.
Windows Scan Results	Additional System Information	Best practice Services	Some potentially unnecessary services are

			installed.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (critical)	Sample Applications	Some IIS sample applications are installed.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (critical)	Parent Paths	Parent paths are enabled in some web sites and/or virtual directories.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (critical)	IIS Lockdown Tool	The IIS Lockdown tool has not been run on the machine.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check failed (non-critical)	Msadc and Scripts Virtual Directories	MSADC virtual directory was found under the default web site. Scripts virtual directory was found under the default web site.
Internet Information Services (IIS) Scan Results	Vulnerabilities Check passed	IIS Admin Virtual Directory	IISADMPWD virtual directory is not present.
Internet Information Services (IIS) Scan Results	Additional System Information	Best practice Domain Controller Test	IIS is not running on a domain controller.
Internet Information Services (IIS) Scan Results	Additional System Information	Best practice IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options.
SQL Server Scan Results	Product Status	Best practice SQL Server Status	SQL Server is not installed on this computer.
Desktop Application Scan Results	Vulnerabilities Check passed	IE Zones	Internet Explorer zones have secure settings for all users.
Desktop Application Scan Results	Vulnerabilities Check not performed	Outlook Zones	No Microsoft Office products are installed
Desktop Application Scan Results	Vulnerabilities Check not performed	Macro Security	No Microsoft Office products are installed

Ace/Agent values are ok.
Ace/Server values are ok.

Conclusion: Both machines login values are correct. Test is successful.

Measure Residual Risk

The SecurID infrastructure seems to be working as intended but some residual risk remains.

General Business related risks and Physical access related risks outlined in Assignment #1 are generally within acceptable levels.

Unfortunately, some residual risk remains in the other categories:

Implementation related risks.

Residual Risk: Improper implementation of the SecurID software (Test #10)
Recommendation: Make sure that all Sdconf.rec files are updated regularly. This check should be added to the general patching process.
Cost: Very minor.

The implementation and deployment of the SecurID infrastructure is good.

Operating System related risks.

Residual risk: Null Sessions are available (Test #4)
Recommendation: Remove null sessions from all systems. Information/Registry values can be found here: http://www.jsiinc.com/subf/tip2600/rh2625.htm
Cost: Very minor. A simple registry key change is all that is required.

Residual Risk: Easy or non-existent OS passwords and weak policies (Test #6 and Test #7)
Recommendation: Users/Administrators must harden the OS passwords and policies on the machines. A good guide could be found here: http://www.sans.org/resources/policies/Password_Policy.pdf. Registry values must match the template (CIS-Win2K-Level-I-v1.1.7.inf).
Cost: Low to medium, Administrators must enforce the Password security polices in place. An information session could created to help users better understand the password security process.

Network related risks.

Residual Risk: Traffic is sniffed, and SecurID information is leaked.
Recommendation: Hubs should be replaced with Switches if possible. This will limit the amount of information that can be sniffed.

Cost: Medium to high depending of the size of the company and amount of IT assets. Upgrading legacy networking equipment should be considered for various security reasons.

Malicious insider related risks.

Residual Risk: A malicious user changes critical SecurID files on the Ace/Agent.
Recommendation: Access to important configuration files should be limited and strict OS level file access policies should be put in place.
Cost: Minimal, most of the file permission settings can be implemented during the initial deployment of the machines (with Ghost images).

General comments.

Overall, the SecurID infrastructure is implemented and deployed correctly. Unfortunately, the general OS security of the machines is lacking. OS level password policies and general password usage should be examined and should be made compliant with the security practices defined in the Security Policies. These residual risks are fairly easy to fix and should be addressed rapidly with minimal costs.

Considering the audit performed and it's scope, the auditor can state the control objectives goals were achieved. The SecurID infrastructure was properly secured and the general level of the protection provided by the framework is good. The major residual risks that were left were mostly related to the underlining OS. The OS security level is very important to a secure SecurID deployment and should be protected properly. A more thorough deployment of the CIS-Win2K-Level-I-v1.1.7.inf template would fix most of the password complexity and password policies issues and assure a minimum baseline level for the OS. A stricter template like the Win2k Gold Standard could also be used to strengthen the underlying OS. The costs of deploying these templates should be small.

Is the system auditable?

The SecurID system is auditable in general. Most features can be tested properly following the audit steps mentioned in this paper. The audit's general objective was to evaluate the security level of the SecurID infrastructure. The infrastructure can be secured properly if the audits steps outlined in this document are followed. This audits recommendations should be considered as a minimum baseline for a proper deployment of SecurID. Networks that contain classified information would require a more strict approach for most of the tests in this audit and the checklist items values should be revised accordingly.

The OS password policies and settings were part of the audit process. The password policies and settings should meet minimum requirements after the

completion of this audit. Third-party SecurID enabled applications (like VPN clients) would also require different audit steps but were not part of the scope of this paper. This audit only dealt with an Ace/Agent – Ace/Server deployment and these checklist items should provide a proper level of security

In general, The Control Objectives used in this audit can be considered essential for a secure configuration. Most can be verified and implemented properly although Checklist Item #13 (Verify that the SecurID logs and events are monitored regularly and installed properly) is hard to measure reliably. The survey done in the test is a good indication of the current procedures in place, but it does not assure us that the procedures are followed regularly. The second part of this Control Objective dealt with the proper implementation of logging and it was successfully tested by the testing procedure. The first part of this Control Objective can be considered to be non conclusive (although the survey can give an indication of the importance of log reviews) but taken as a whole, this test is still worthwhile. The combination of the survey and the logging settings will help achieving the Control Objective at a respectable level.

Assignment #4 – Audit Report or Risk Assessment

Audit Report.

Executive summary

This audit's goal was the proper deployment of a SecurID infrastructure on the network. The audit scope was limited to the SecurID infrastructure and underlying OS password policies. In general the security level is within acceptable limits. Most of the control objectives were met and the system is behaving in accordance to the guidelines detailed in this document.

General Audit findings

The SecurID portion of the infrastructure is, in general, used and deployed properly. Only one of the tests that dealt with SecurID failed to meet the requirements and it was mostly due to poor update/patch management (Please refer to the Audit findings section below for more details). The failed items are listed below:

- Sdconf.rec file was not updated correctly.

The OS password portion of the infrastructure did not meet security requirements. Most tests that dealt with Passwords and Account policies did not meet the necessary requirements. The failed items are listed below:

- Null sessions were available. This is a great source of information for malicious hackers.
- OS passwords did not meet the minimum requirements.
- Account policies did not meet the requirements.

General Recommendations

- Establish a proper Patch/Update process that will insure that all software is updated regularly.

- Remove null sessions from machines. This can influence the backup process.

- Enforce the Password policies found in the Security policy. Ensure that all OS passwords meet the requirements.

- Deploy/Use the CIS-Win2K-Level-I-v1.1.7.inf security template or create a custom template for all machines.

The issues discovered during this audit can be corrected. In light of the general poor implementation of the OS account policies on the Ace/Agent and Ace/Server; a more careful examination of the OS would be advisable (service/port audit, OS security audit). This will maximize the security benefits of the SecurID infrastructure and limit the exposure to attack.

Audit findings

Please refer to Assignment 3 for screenshot evidence of the findings.

Test #4 TEST FAILED
Null Sessions.

Findings 1: The Ace/Server and Ace/Agent allow null session connections. Null sessions are considered to be a major security risk. Null Sessions take advantage of flaws in the CIFS/SMB architecture found in most windows machine. No username or password is required to connect to the machine. Malicious hackers can gather a great deal of information like the list of users, list of machines, list of shares and SID (security identifiers) on the network.

Test #6 (Stimulus/Response #1) TEST FAILED
Test OS Password complexity

Findings 2: On the Ace/Agent, 3 accounts were cracked easily. Administrator, Guest accounts and another administrator level account. The Administrator and Guest accounts had no passwords and the second Admin account had a password of 123456. These passwords do not meet the complexity requirements and were cracked very easily.

This is obviously a great security risk that reduces the effectiveness of the SecurID infrastructure. Remote users could connect to the Admin shares (like C$) and have access to all the data on the machine. Remote administration Trojan's/tools like DAMEWARE (http://www.dameware.com/) could give complete control of the machine to malicious hackers.

Findings 3: the Ace/Server passwords were not cracked and passed the complexity test.

Findings 4: We could not change the current account passwords of the test user to a value of 123456 on either the ACE/Server or the Ace/Agent. You will note, from the previous findings, that the second admin account currently has a password of 123456. We can only conclude that this value was set prior to the change of password policy and that setting a password of this type is currently not possible.

Test #7 TEST FAILED
Account policies check.

Ace/Server:

Findings 5: The Minimum password length is too small and the Password history is too short. They do not meet the minimum standards of the Security Template. You can also note that the template is a baseline minimum security level for all machines and considering the importance of the ACE/Server, the template is not restrictive enough. Another template should be used for a more secure implementation (like the Win2k gold standard). So these settings are clearly not adequate. A short password is vulnerable to brute force attacks and a short password history can lower the effectiveness of the password used (Malicious hackers know that users like to reuse old passwords).

Findings 6: The Account lockout duration and Account lockout counter are too short. They do not meet the minimum common baseline requirements. Accounts that have too many failed login attempts should be locked out, for a greater period of time, to minimize the effectiveness of a brute force attack.

Ace/Agent

Findings 7: Minimum password length is too small and the Password history is too short. These values should be changed to meet common baseline practices. Although the importance of the ACE/Agent is not as great as the Ace/Server, it is as likely to be brute forced as the Server itself.

Findings 8: The Account lockout duration and the account lockout counter are too short. Both of these values should be changed to meet the requirements.

Test #9 TEST PASSED
All users “except:” clause is invoked

Findings 9: The Except clause was used and the RSA-Admin group invoked does not have any administrators (Domain or Local). This is a good implementation of this feature. An Administrators account that is exempt of authentication with SecurID would be a key target for a malicious hacker.

Test #10 TEST FAILED
Sdconf.rec file used at install is current and the same as the one generated on the Server.

Findings 10: The Sdconf.rec files do not match. An older version of the file was not properly updated. The file should be kept updated to ensure proper communications with the Ace/Server. Item #19 of the audit was performed and communication was successful. This indicates that the Sdconf.rec was not forged by a malicious user, but is simply an older version.

Test #12 (Stimulus/Response #2) TEST PASSED
SecurID next tokencode checks

Findings 11: All tests were successful and the token values were set correctly. The token was properly set to next token mode after more than 3 consecutive failed logon attempts. The logs also reflect the change of status of the token. This feature is working as intended.

Findings 12: The token was properly disabled after more than 10 consecutive failed logons. The token must be manually enabled by an administrator to function properly. This feature is working as intended

Test #13 (Stimulus/Response #3) TEST PASSED
SecurID Access logs are backed/maintained and consulted regularly

Findings 13: The Ace/Server logs all events possible and the log policies followed by the administrators are correct. This ensures that the information provided by the SecurID infrastructure is being dealt with the proper importance.

Findings 14: Events generated by the auditors were successfully logged. This ensures that the logging mechanism is working correctly and assures the administrators that the events have in fact happened. You will also note that all events generated by this audit were logged successfully.

Test #17 (Stimulus/Response #4) TEST PASSED
PIN Length and type is correct

Findings 15: The values for Min, Max and PIN type are correct. They were set for a minimum of 4 and a Maximum of 8. The Alphanumeric tab was checked and as such greatly increases the pool of possible values. This greatly lowers the chance of a successful brute force attack.

Findings 16: Attempts to change the PIN to improper values failed. This feature is working properly and ensures that users cannot pick improper and less secure PINs.

Findings 17: The Alphanumeric PIN was accepted. The use of alphanumeric characters in passwords raises the complexity level of the password. A successful brute force attack on the password will become more difficult to achieve.

Test #18 (Stimulus/Response #5) TEST PASSED
Access times are set correctly

Findings 18: Access times limits were not set for administrators. After an inquiry with the administrator and managers it was determined that access is required at all hours. This approach was necessary due to the mobility of work hours and off peak patching. This is an acceptable risk for this particular infrastructure and the managers are aware of it. Normal users have access during work hours + 5 hours. Normal users can request greater access on a case-by-case basis.

Findings 19: The logging attempt at an unauthorized time was blocked and logged successfully. This validates the access restrictions.

Test #20 TEST PASSED
Check logon success and logon failure auditing

Findings 20: Logon Success and Logon Failure auditing are both enabled on the Ace/Server and Ace/Agent. Proper logging is important for the forensic process. Important information could be lost if the correct fields are not enabled.

Background/risk

In general, the risks associated with SecurID are often due to human nature. Loss of tokens and PINs are common and can lead to sensitive data being compromised by unauthorized users. The security the SecurID infrastructure provides is heavily reliant on the proper use of the tokens and the infrastructure. Report time for suspicious behavior should be low and users must be made aware of general social engineering methods. A Low report time leads to a low exposure period.

In general the non-compliant tests were due to poor OS hardening or a poor implementation of general OS hardening techniques. These are important issues that lower the effectiveness of the SecurID infrastructure. Hackers will use the simplest way to get to your data. The loss of IP and information contained on the Servers being protected can be devastating to the company. Improper OS hardening can allow hackers to freely roam the internal network and cause Denial of Service attacks. Also, once a machine is compromised on your network, it could be used to attack other machines found on the Internet, this could lead to a loss of reputation or even legal liability.

Audit recommendations

General Recommendations

In general, we have found that the SecurID infrastructure is working as intended. The machines were correctly implemented and used. Unfortunately, other security methods were not followed and the overall effectiveness of the infrastructure is lower because of it. OS hardening should be performed on All Ace/Agents and on the Ace/Server.

Each failed test denotes a general area were security can be improved. Methods and polices should be devised to deal with these issues. For example a special OS installation CD could be created, insuring that null sessions and OS passwords meet minimal standards. This will ensure that machines are deployed correctly.

Change control methods should be improved to eliminate improper changes to the settings. Normal users should be made aware of the different types of attacks and information sessions for all personnel should be scheduled. This will greatly reduce the risks associated with PINs being lost, tokens being compromised and Social engineering issues.

The likelihood of attack is pretty substantial. Tokens are often lost and PINs are often written down. An attacker can potentially acquire both a PIN and a token and could cause damage. Proper training of all staff should be imperative.

The risk of a network based attack on the Ace/Server by disgruntled employees or a malicious hacker is real. Access controls for authentication for physical access are correct (thanks to SecurID), but networking access controls might be somewhat lacking based on the account policies checks we performed. An attacker will always use the easier approach to get to what he needs.

The cost of properly deploying SecurID greatly offsets the potential cost of the loss of control of your networking resources or the loss of extremely valuable data (like transaction records, Credit card numbers and Intellectual property).

Unfortunately, some more thorough examinations of the SecurID implementations could be necessary for an audit requiring a very high level of security (for classified documents). For example, the level of encryption between the ACE/Server and Ace/Agent was not tested. The methods to audit these features would require access to the source code or a greater level of cooperation from the manufacturer. Users generally trust the manufacturer to properly implement these encryption methods. For highly classified data, a more robust test would be advisable.

A more careful analysis of the physical network infrastructure would also be advisable for a proper deployment (Hubs should be removed to minimize the chance of traffic being sniffed).

Specific Recommendations

Test #4 TEST FAILED
Null Sessions.

Close null sessions on all machines on the network. This might potentially break backup processes. A Patch deployment strategy should be implemented. This will ensure that all machines meet the security requirements and are patched regularly. A basic secure install CD should be developed. This CD will contain all basic patches and security setting and should be used to install new machines. This will ensure that new machines being deployed on the network are compliant.

Test #6 (Stimulus/Response #1) TEST FAILED
Test OS Password complexity

All passwords should meet the minimum password complexity requirements described in the Security Policy. If necessary, the current Security Policy should be updated to reflect current “best practice” values.

Test #7 TEST FAILED
Account policies check.

A more restrictive template should be used for Servers. The Win2k Gold template is a good start, but it will require some tweaking before being deployed. The template is very restrictive and most network applications will not work well if it is applied blindly. A general minimum level template can also be created. The level 1 minimum level template should be used on all workstations. This will ensure that the passwords settings meet the requirements. The Security Policy in place should be updated to reflect these issues.

Test #10 TEST FAILED
Sdconf.rec file used at install is current and the same as the one generated on the Server.

All critical files should be kept updated. A patching policy should be developed for all software, including SecurID. This will ensure that all the software is being used correctly.

Costs

The cost of hardening the machines is very low and usability should not be affected by these changes. These recommendations try to solve the root cause of the problems found during testing.

Test #4 (Null Sessions)

The costs associated with the development of the patching strategy should be minimal. Network administrators should be able to develop it by themselves. They know the network's layout very well and should be able to create a good working model. Creating a custom CD should also be done by the administrators and would only require a few days of work/testing. The hours spent on these small projects will benefit the whole organization in the long run.

Test #6 (Test OS Password complexity)

The cost of changing all the passwords is also small. A memo or email could be sent to all users explaining the new password policies. The changing of the password policies should be invisible to normal users and would only take a few hours. The loss of productivity would be minimal. The template developed for Test #7 should incorporate the new password policies.

Test #7 (Account policies check)

There is no cost associated with using existing templates. They are available for free and can easily be integrated in the current infrastructure. Developing a custom template could become costly if done by external consultants (consulting

fees vary from 50$/hour to 250$hour). If done internally, the costs would be small (a few work days for 1-2 administrators).

Test #10 (Sdconf.rec file used at install is current and the same as the one generated on the Server)

Same costs as Test #4. Checking that all current Ace/Agents configuration files are current could take a while (depending on the size of the infrastructure). Costs should be fairly low if the patching strategy developed for Test #4 includes SecurID software.

Compensating controls

These recommendations will reduce the risks with minimal expenditure. They might not address the root cause of the problems but will solve the immediate problems.

Test #4 (Null Sessions)

Administrators could manually go through every machine in the enterprise and remove all null sessions. This will fix the immediate problem but does not address the overall issue (like a proper patching strategy would). The loss in productivity to perform this task would be fairly small.

Test #6 (Test OS Password complexity)

It would only take a few hours for administrators to manually apply the level 1 basic template on all machines. The loss in productivity should be small.

Test #7 (Account policies check)

The loss in productivity should be small if administrators apply the basic templates on all machines.

Test #10 (Sdconf.rec file used at install is current and the same as the one generated on the Server)

Manually checking the Sdconf.rec files on all workstations might take some time (this could be performed at the same time as the other tests). This should be done internally.

References

RSA Security, *Content Library*, http://www.rsasecurity.com/doc_library/index.asp

Frederico Cid, Carlos, *Cryptanalysis of RSA*: a Survey
http://www.sans.org/rr/papers/20/1006.pdf

Boneh, D and Durfee, G, *Cryptanalysis of RSA with private key* d *less than* $N^{0.292}$
http://crypto.stanford.edu/~dabo/abstracts/lowRSAexp.html

Mudge and Kingpin, *Initial Cryptanalysis of the SecurID algorithm*
http://www.atstake.com/research/reports/acrobat/initial_securid_analysis.pdf

Windows NT Security Audit Program
,http://www.auditnet.org/docs/WindowsNTSecurity.pdf

Fraser, B, *RFC2196*, (http://www.faqs.org/rfcs/rfc2196.html),

*RUSecur*e, http://rusecure.rutgers.edu/secplan/cklst.html

Granger, Sarah, *Social Engineering Fundamentals, Part I: Hacker Tactics*,
http://www.securityfocus.com/infocus/1527

Gragg, David, *A multi-level Defense against Social Engineering*
http://www.sans.org/rr/paper.php?id=920

Cox, Philip, Hardening Windows 2000,
http://www.sys-exp.com/tutors/hardenWin2K.pdf

BlackViper, *Windows 2000 Professional and Server Services Configuration 41*1
http://www.blackviper.com//WIN2K/servicecfg.htm.

SANS, *Password Policy Resources*,
http://www.sans.org/resources/policies/Password_Policy.pdf