GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Server Security in a Citrix Presentation/Terminal Server Environment

GSEC Gold Certification

Author: Shane Wescott, shane.wescott@appsense.com

Adviser: Jim Purcell

Accepted: February 12, 2006

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

Abstract

Application deployment via Citrix Presentation Server/Terminal Services (CPS/TS) is an ever expanding area of IT.

This document serves to discuss the special security needs of this environment, and to recommend strategies for its implementation.

It will cover the following areas:

1. Introduction
2. CPS/TS Server Hardening
3. User Profile Security and Lockdown
4. Application Security and Lockdown, and
5. Auditing and Monitoring.

Finally there will is a Security Checklist to summarise the strategies and recommendations made in this document.

As is the case with all security strategies, planning is the key. Time well spent planning the security structure and policies of the implementation can greatly reduce the time spent installing and configuring the servers.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

Table of Contents

1. Introduction 4
   1.1 Overriding Caveats 5
2. Citrix Presentation Server/Terminal Server Hardening 6
   2.1 Windows 2003 Server Hardening 6
   2.2 Windows 2003 Terminal Server hardening 6
   2.3 Citrix Presentation Server hardening 10
3. User Profile Security and Lockdown 13
   3.1 Security Tools for Profile Management 15
4. Application Security and Lockdown 16
5. Auditing and Monitoring 22
6. Conclusion 25
7. Security Checklist 26
8. References 28

© SANS Institute 2007, Author retains full rights.

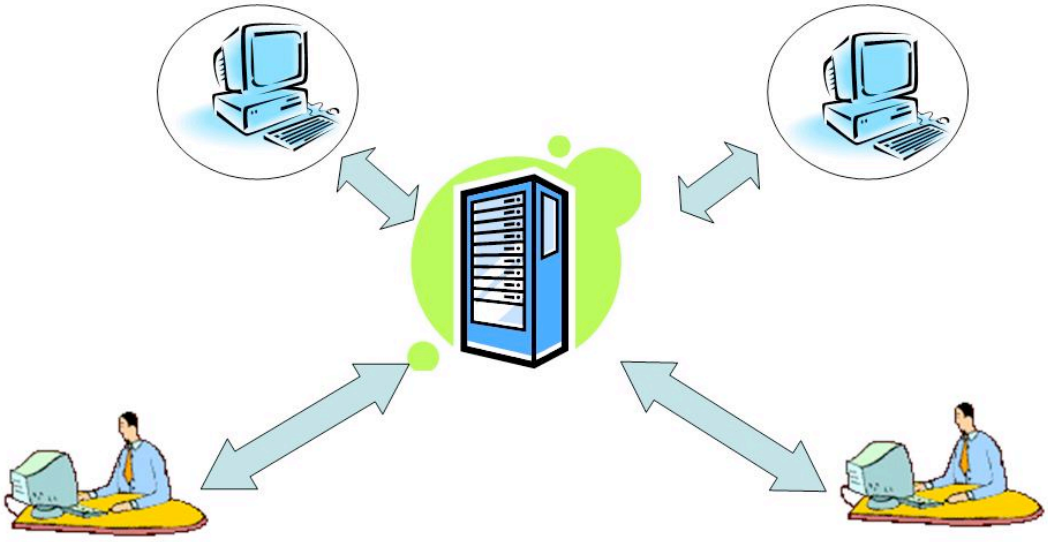
© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

1. Introduction

As a refresher, the diagram below shows the basic concept of a CPS/TS installation.

Basic Citrix Presentation Server/Terminal Server Diagram



Essentially both users are running applications on their own virtual desktop hosted on a central server running Windows 2003 and CPS/TS. Unlike a VMware or VDI implementation, all users on the server share one "image" of the operating system.

Key strokes, mouse clicks and video information are transmitted to the users' access device which can be a PC, Thin Client, or Mobile PDA.

The main business drivers for CPS/TS are:

1. Reduce Management costs by centralizing application management to simplify application deployment, and
2. Reduce infrastructure costs, by extending desktop lifecycles and reducing communications bandwidth requirements.

From a security perspective, by centralizing the applications and data, users can view data, but don't have physical access to copy data. The term commonly used for this in the CPS/TS world is

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

"Eyes Only" security.

In some cases these implementations are "Published Application", while others are "Full Desktop".

In a "Published Application" environment the user typically clicks on a desktop shortcut on their PC and the application is launched via a CPS/TS session from the server. This environment is often divided into "Silos" where a group of servers will deliver App A for example, and another group of servers will deliver App B.

In a "Full Desktop" environment, to the user, it looks and feels like they have their own desktop. This is typically the way thin client devices (Wyse, HP etc) are implemented.

While the end user interaction in these two scenarios is different, the security issues are the same:

1. Make sure users can only perform the tasks you want them to do, and
2. Ensure users can't make operating system or application changes which will affect other users on the server.

Essentially the security model needs to be a combination of Server hardening, and User lockdown to ensure the environment remains stable and reliable.

1.1 Overriding Caveats

1. This paper is focused on Windows 2003 Terminal Services and Citrix Presentation Server 4. Previous versions of Citrix/Terminal Services will benefit from these strategies, however the commands and tools used may differ.
2. While Citrix Web Interface(WI) is a popular element of CPS/TS deployments, it is not discussed in this paper.
3. This paper addresses security at the Server level. Client level security and security of connectivity is outside the scope of this document.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

2. Citrix Presentation Server/Terminal Server Hardening

Like any other Windows 2003 Server, CPS/TS servers need to be protected from security threats.

These threats may come in the form of internal or external attacks. The hardening of a server against these threats needs to cover three distinct areas:

2.1 Windows 2003 server hardening

2.2 Windows 2003 Terminal Services hardening

2.3 Citrix Presentation Server 4 hardening

These three areas will be covered separately.

2.1 Windows 2003 server hardening

The purpose of this document is not to reinvent the wheel when it comes to Windows 2003 Server hardening. There is a wealth of resources available which cover this subject, including numerous documents in the SANS Reading Room.

Microsoft has an excellent guide at:

http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

But as a quick guide, it's all the standard stuff:

1. Only use NTFS partitions
2. Make sure the server is patched.
3. Make sure AV software is up to date.
4. Disable all unused services.
5. Check for open network ports and close unused ones
6. Remove all unused Users and Groups.
7. Audit and monitor the server.

2.2 Windows 2003 Terminal Services hardening

On top of the normal Windows 2003 Server hardening, the following Terminal Services specific areas should be addressed:

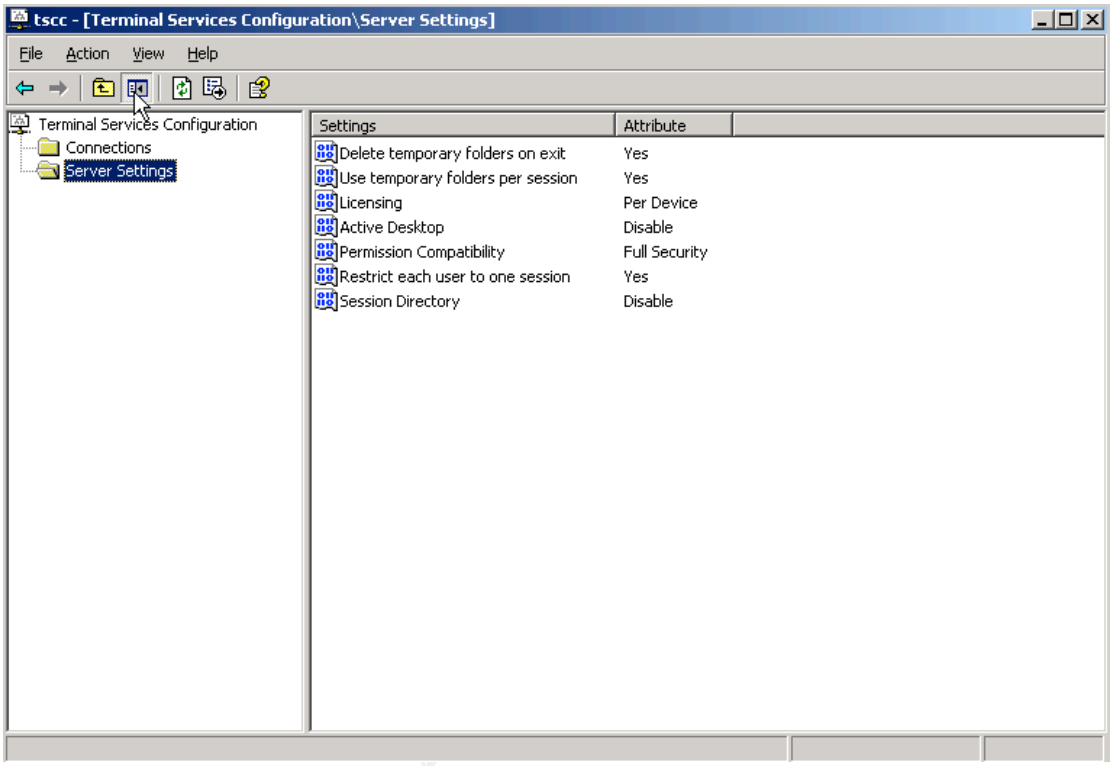
1. Terminal Services Configuration Settings
2. Permission Compatibility

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

3. Remote Desktop Users Group, and
4. Remote Control of Terminal Server sessions.

The screenshot below shows the default settings for the configuration of a Terminal Server



Using temporary folders for sessions and deleting those folders on exit is one way to help control any malware or malicious code which finds it's way onto the server during a user session.

These settings can be configured using the Terminal Services Connection Configuration (TSCC) utility or via a Group Policy object.

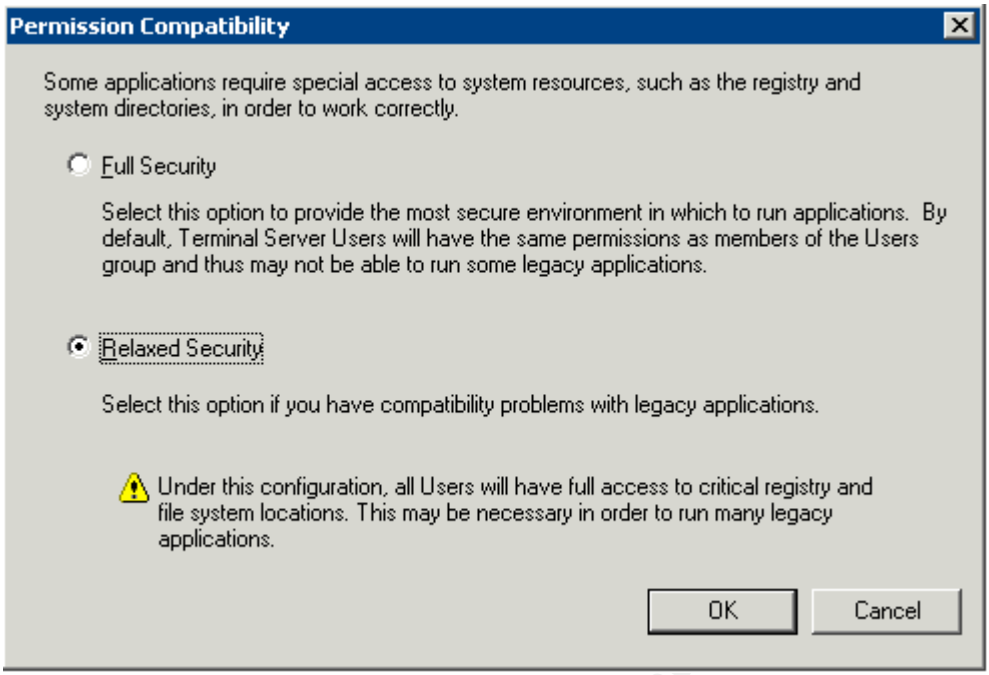
One very important topic for discussion on CPS/TS hardening is the installation setting "Permission Compatibility".

During installation of Terminal Services on Windows 2003 the administrator is asked to select either:

1. Full Security, or
2. Relaxed Security.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.



It is important to understand the implications of both these options as this is an area where people commonly leave their CPS/TS servers open to accidental or deliberate security breaches.

The setting has been included to assist with legacy applications which sometimes need higher levels of access to areas of the file system or registry.

Keep in mind the applications users run in a CPS/TS session are all designed to run on a PC, and still think they are running on a PC. Therefore if a legacy application needs full access to certain system registry settings on a PC it will also require the same level of privileges during a CPS/TS session.

If during installation the Administrator selects "Full Security" basically nothing changes. All of the standard permissions associated with the users and the groups they are members of will apply.

If, however, the Administrator selects "Relaxed Security" the logon process will add the TSUserSID to the security token for the user during each session.

Essentially this adds the user to a very powerful local group called TSUser, which is almost equivalent to being a member of the Power User group.

The local TSUser group has Modify permissions to the Program Files directory, and the ability to add and modify registry keys in the HKLM\Software key set.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

This effectively gives these users the ability to install new software and have it work correctly.

Obviously this is a large security hole. It is almost as bad as another common CPS/TS security issue, adding users to the Local Administrators group.

The alternative to both of these techniques for legacy application compatibility is to assign the required permissions to the exact file and registry locations.

Tools like RegMon and FileMon, available from http://www.microsoft.com/technet/sysinternals/default.mspx, are helpful in isolating these requirements.

The local Remote Desktop User group gives users the ability to logon to a Terminal Server session on a particular server. There is always a temptation to add the Authenticated Users group to this local group to save management of which users have access to the CPS/TS server and which users do not.

As with a lot of settings in security, more is less. If you open up access to every authenticated user, then you are probably giving access to a large group of users who don't need access.

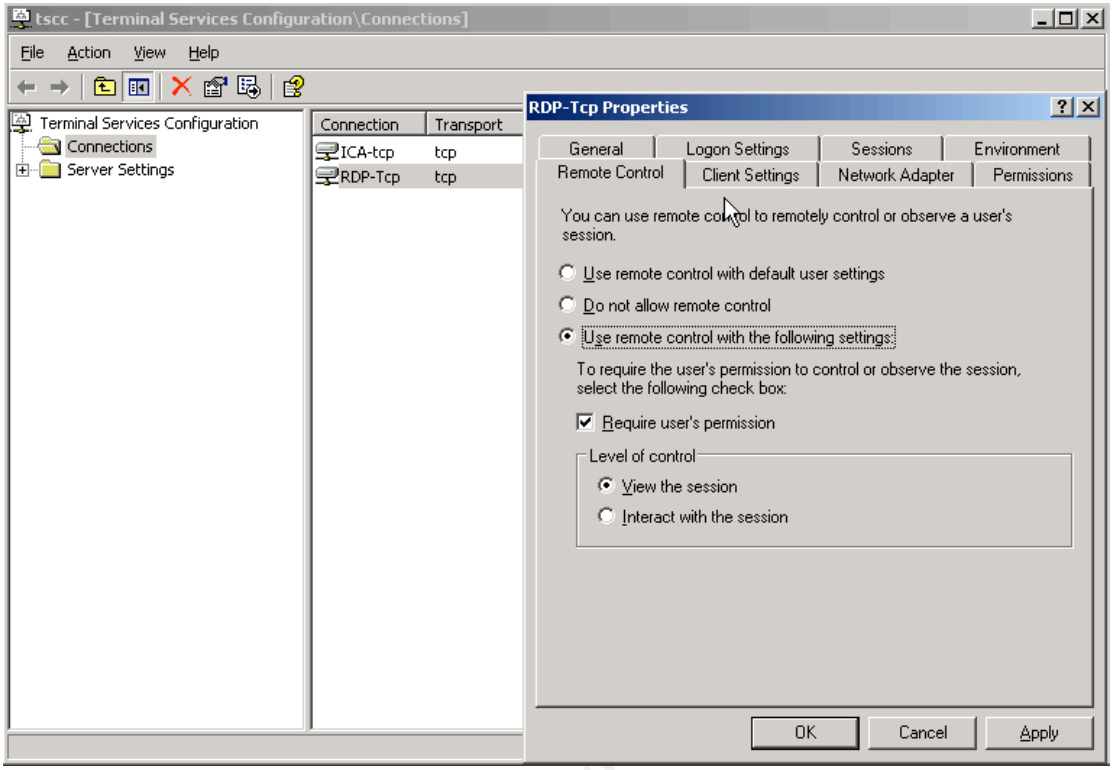
Consider creating application specific user groups, for example "Lotus Notes Users", and adding those to the "Remote Desktop Users" group. In this way only the users who need to access the applications via Terminal Services will have access. While this obviously involves more management of users and groups, the security benefits are obvious.

Remote Control (called Shadowing in the Citrix world) is a method of monitoring or taking control of a user session. This is usually done for help desk purposes.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.



Unfortunately this feature can be configured so session monitoring can occur WITHOUT alerting the user. Obviously this can be a major security issues in the wrong hands so careful consideration should be given before enabling this feature.

2.3 **Citrix Presentation Server hardening**

Hardening of the CPS server revolves around restricting access to the Citrix Management Console (CMC) and the functionality included in that console.

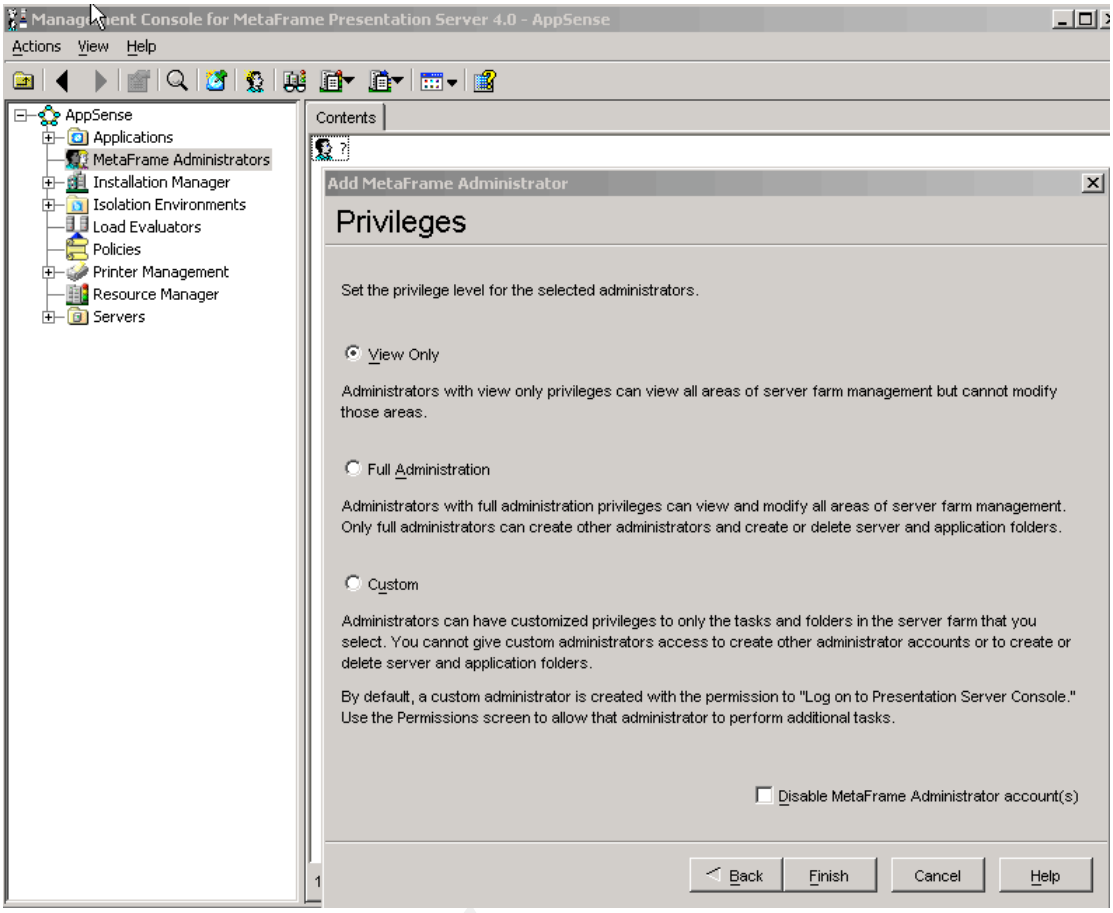
The CMC controls aspects of the CPS servers as well as defining Published Applications, and the users who have access to those applications. For these reasons it is critical only authorized Citrix administrators have access to the CMC.

For anyone other than Citrix Administrators, the executable ctxload.exe should be blocked via an SRP or other mechanism. This console can be run from a remote PC so restriction at the desktop level is also recommended.

Another recommendation is to create a Global group purely for Citrix Administrators. This group would be a subset of the "Domain Admins" group, but not all Domain Administrators need to have access to administer the CPS servers.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.



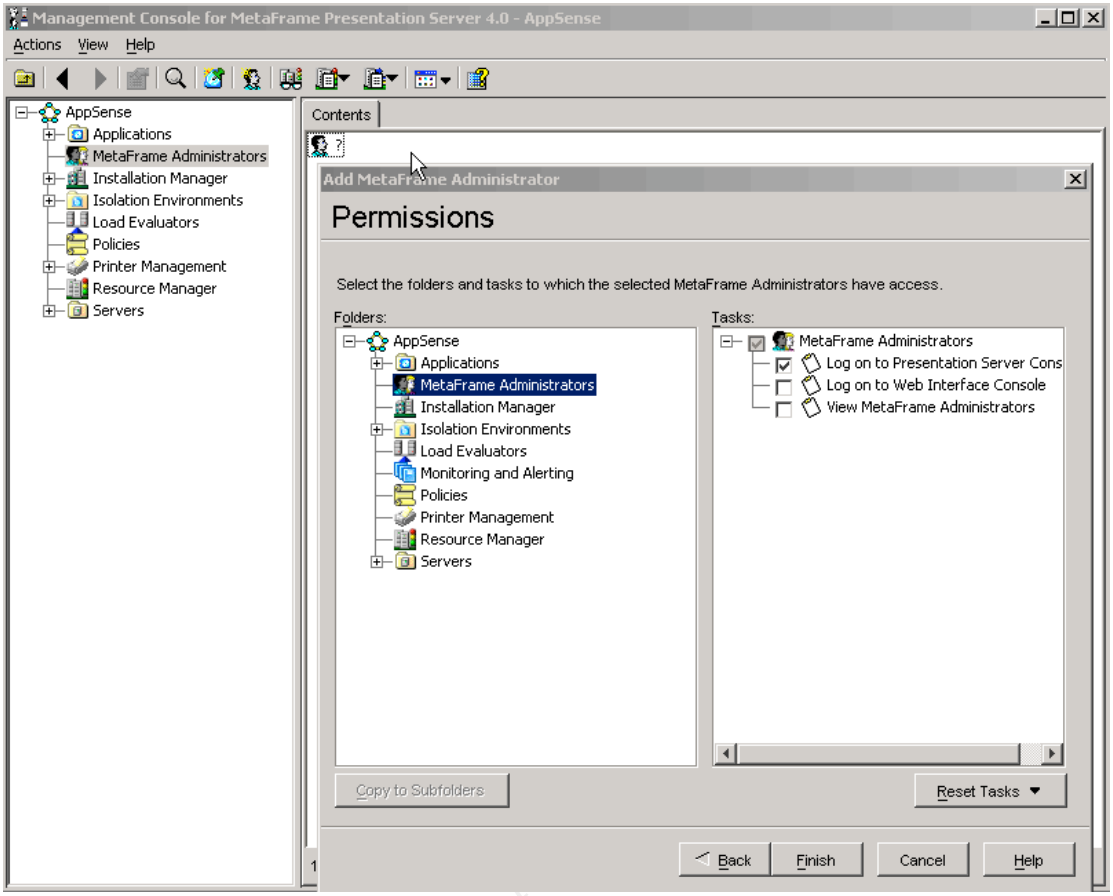
The screen shot above shows the "MetaFrame Administrators" wizard in the Citrix Management Console.

This wizard allows the administrator to configure different levels of access for different members of the CPS management team. "View Only" will allow the team member to view settings, but not change anything, while "Full Administration" is designed for the main Citrix admin team.

The "Custom" setting can be used to tailor the administrative requirements to meet individual needs. For example, you may want to give the group "Level 2 Help Desk Admins" the rights to reset or logout disconnected Citrix User sessions, but not the rights to create new Published Applications.

The screen shot below shows the "Permissions" screen used to provide this level of granularity.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.



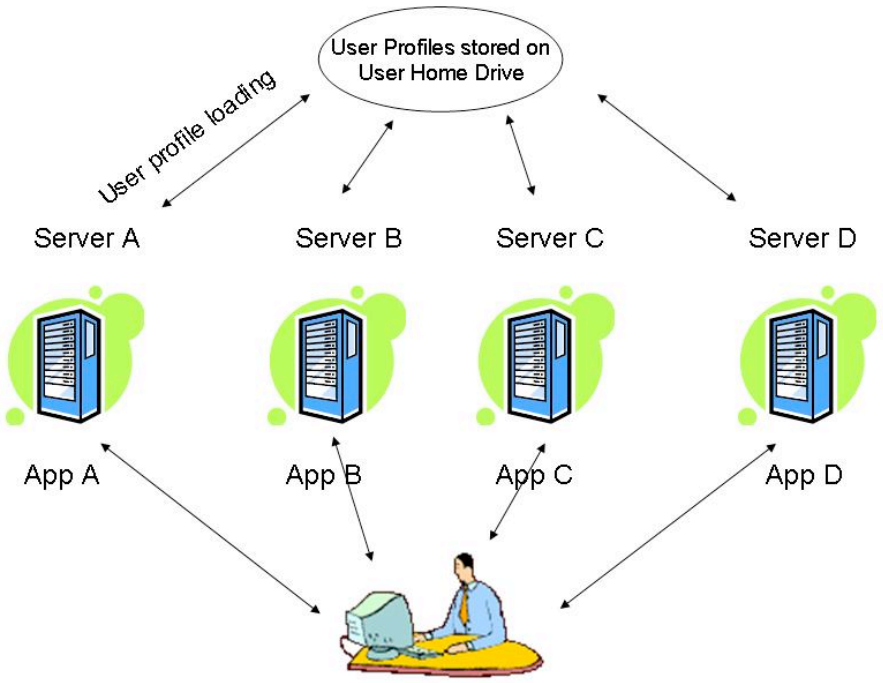
© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

3. User Profile Lockdown and Security

User Profiles can become more of an issue in a Published Application environment, especially when Roaming Profiles are used. This is shown in the diagram below.

User Profiles in a Citrix Presentation Server/ Terminal Server Environment



As you can see, our user is operating in a Silo'ed "Published Application" environment. When the user starts App A, his user profile will be loaded onto Server A. When he starts App B, his user profile will be loaded onto Server B.

This creates three issues:

1. Multiple copies of the profile travels across the network, generating additional network traffic,
2. Any changes made to the profile on one server are not reflected in the profile on another server, and
3. Multiple copies of the profile will be copied back to the one location at logout time, which may result in profile corruption. The likelihood of this increases as the size of the profile increases.

There are three types of profiles which are used in the CPS/TS world.

They are:

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

1. Roaming Profiles,
2. Mandatory Profiles, and
3. Hybrid Profiles, which combines a Mandatory profile with some pre defined areas of the registry where user changes are retained.

Each has their own pros and cons.

Roaming Profiles:

Positive: Easy to setup, simple in concept, all user changes are retained.

Negative: Prone to corruption in a CPS/TS environment, slow to load at login time as they grow in size.

Mandatory Profiles:

Positive: Simple to manage, fast to load, no corruptions.

Negative: No user changes saved, inflexible.

Hybrid Profiles:

Positive: Best of both worlds, user changes can be retained as required, and fast to load with a greatly reduced chance of corruptions.

Negative: Can be complex to setup, and in some cases complex to manage.

From a security perspective there is no question that Mandatory profiles are the preferred option. The server settings are all preserved from session to session, and any changes the user makes either deliberately or accidentally are wiped at their next login, minimizing any disruption they may cause.

Unfortunately security is all about balance and sometimes the need to retain user changes out weighs the need for a restrictive security policy.

This is where the Hybrid profile becomes the preferred option. Important system settings are secured and hence protected, while user changes can be retained if required.

These user settings or areas of the registry are typically "hived in" at Login time, and "hived out" at Logout time. These registry hive operations usually involve the transfer of very small files so the chance of these becoming corrupted is minimal.

Another strategy used to improve profile security is the redirection of various elements of the profile. This can be useful to lock down elements of a Roaming profile.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

The most common elements of the user profile for this type of lockdown from a security perspective are:

1. Start Menu
2. Desktop
3. Startup
4. NetHood, and
5. PrintHood.

By locking down these elements to Read Only versions it ensures that any changes made by users either deliberately or accidentally are not retained.

3.1 Security Tools for Profile Management

The following is a list of tools commonly used to help secure and manage User Profiles in the CPS/TS space. It should be noted the tools listed are ones I have come across in Australia/New Zealand which are being used in todays market.

The tools vary on their functionality, cost, ease of use, and support services, so I recommend you research and evaluate before making a decision.

1. AppSense Environment Manager http://www.appsense.com
2. Citrix Consulting Hybrid Profiles http://www.citrix.com
3. Flex Profile Kit http://www.loginconsultants.com
4. ScriptLogic http://www.scriptlogic.com

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

4. Application Security and Lockdown

There are two common strategies used to restrict the applications available to users in a CPS/TS environment. This is where the security of the CPS/TS server is similar to the security employed on a desktop PC.

These are:

1. Group Policies/Software Restriction Policies, and
2. Third Party products like AppSense, SecureWave and triCerat.

A primary function of these methods can be to block new applications from being installed and executed, either deliberately or accidentally by users. This helps mitigate the risk posed by Spyware and Malware.

Essentially all of these strategies involve either:

1. A White List, a list of apps the user is allowed to run,
2. A Black List, a list of apps the user is NOT allowed to run,
3. Trusted Ownership, some form of monitoring who owns the apps a user wants to run, or
4. A combination of the above, White List plus Trusted Ownership for example.

Software Restriction Policies (SRP) can be used to implement the above strategies.

It should be noted up front that SRP's do not apply to Driver or Kernel level programs or any program executed by SYSTEM.

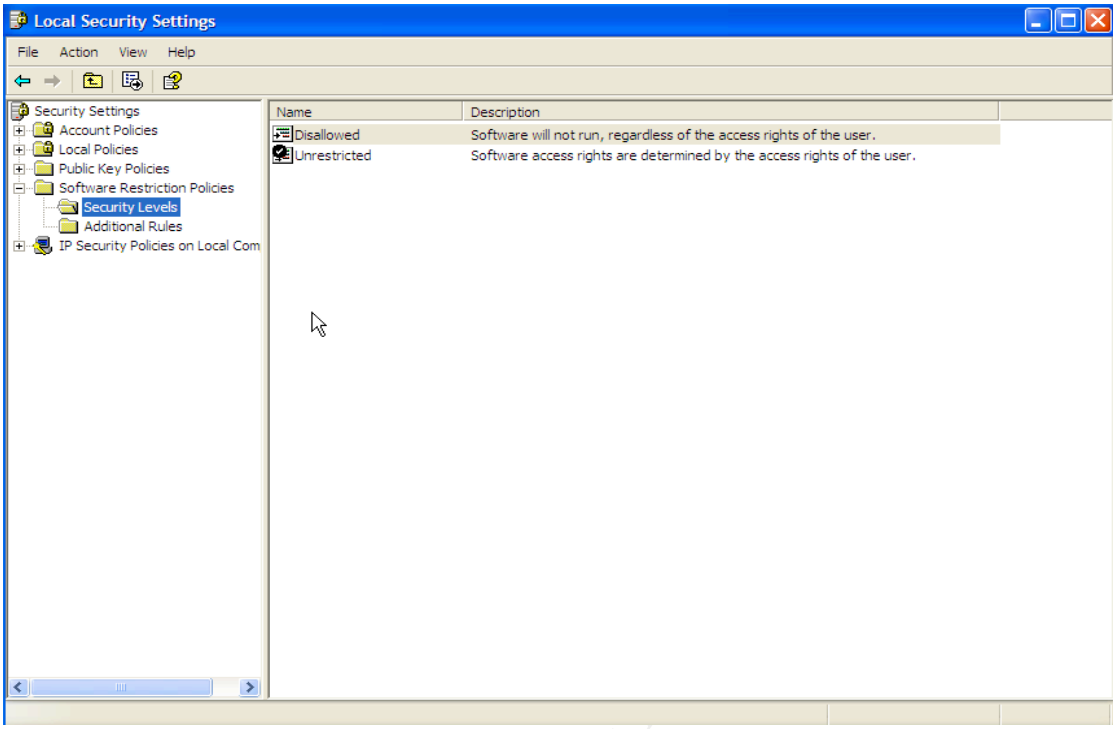
There are two security levels which control how the SRP's will work:

1. Unrestricted, effectively Allow All, and
2. Disallowed, effectively Deny All.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.



The security levels are then combined with the 4 rules available in SRP's to implement the required security policy. These rules, listed in order of precedence are:

1. Hash Rule
2. Certificate Rule
3. Path Rule, and
4. Internet Zone Rule.

Each of these rules has their own pros and cons, and specific areas they are targeted to address.

Hash rules specify an exact file which needs to be either allowed or restricted. This rule can be used to ensure no version change or other modification of a file is allowed.

It should be noted that the filename is not included in the hash process so copying or changing the name of the file will not affect the rule being applied.

Unfortunately a hash needs to be created for each file, and will need to be recreated if the version of the file changes. This can lead to a large amount of management overhead.

Certificate rules check the certificate used to sign a file and allow or restrict execution based on that certificate. They work well to allow exceptions to Path rules and are commonly used

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

to allow regular updates to system files, for example Windows updates signed by Microsoft.

Again there can be management overhead as each Trusted Authority needs to be specified in the rule.

Path rules restrict or allow files based on the file location, file name or extension. Wildcards can be used with Path rules, but unfortunately the rule can be easily bypassed by changing the name, extension or location of the file.

Internet Zones rules govern whether MSI files downloaded by Internet Explorer can be run or not. A different rule can be applied to each zone, but these are of limited use as they only apply to MSI files.

The three commercial products mentioned earlier (AppSense, SecureWave and triCerat) address the short comings of SRP's in different ways to protect against unauthorized applications:

1. AppSense Application Manager uses a principle called "Trusted Ownership". When a user attempts to execute some code, Application Manager checks the NTFS Ownership permissions of the file and compares this to a list of "Trusted Owners". If the owner of the file is a trusted owner, the file is allowed to execute, if not it is blocked.

AppSense Application Manager also has the ability to create White Lists, Black Lists, Digital Signatures, and includes extensive Auditing capabilities.

Further information on AppSense Application Manager is available from http://www.appsense.com

2. SecureWave's Sanctuary Application Control simplifies the creation and management of Hashes or Digital Signatures for Allowed executables, and effectively works on the White List approach. Templates for common Microsoft applications can be used and there are a number of reporting options available.

Any application without the correct digital signature will be automatically blocked by Sanctuary Application Control.

For more information on SecureWave's Sanctuary product visit http://www.securewave.com

3. triCerat's Simplify Lockdown uses a customised replacement shell for the Windows Explorer called triShell. By default, users have no access to any applications. The required applications are then authorized through a management interface. Because Simplify Lockdown uses a replacement

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

shell, users are not only blocked from executing applications, but are also blocked from "seeing" applications or the icons associated with them.

Simplify Lockdown can also be used to configured aspects of the users desktop environment, like Start Menus etc.

Further information on Simplify Lockdown is on their website at http://www.tricerat.com

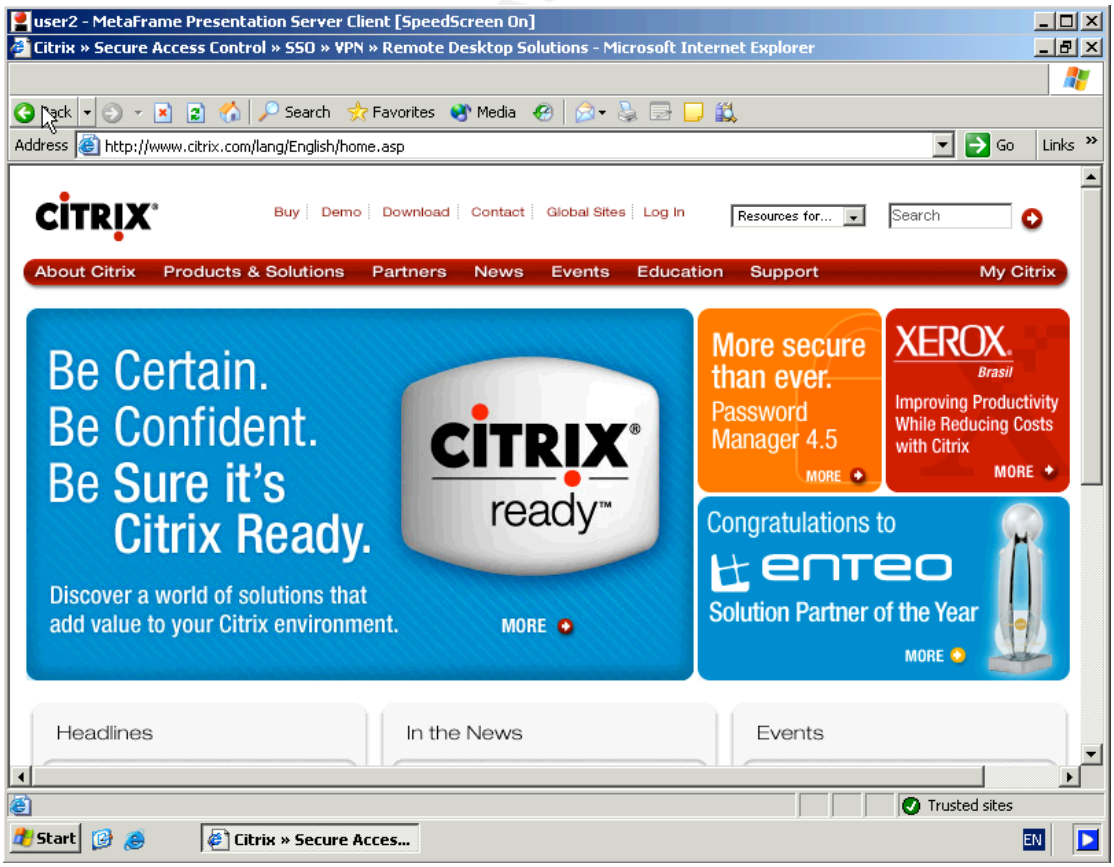
With these and any other commercial security product, testing is the key to seeing how the tools meet your organizational needs, and assessing the level of ongoing management required.

It's then a matter of comparing the benefits gained against the cost associated with the product.

Once you have decided which applications users should be allowed to use, the next step is securing functionality **inside** those applications

This can be done to simplify application usage for users, or to block potential back doors and security holes.

An example of an Internet Explorer lockdown is shown below:

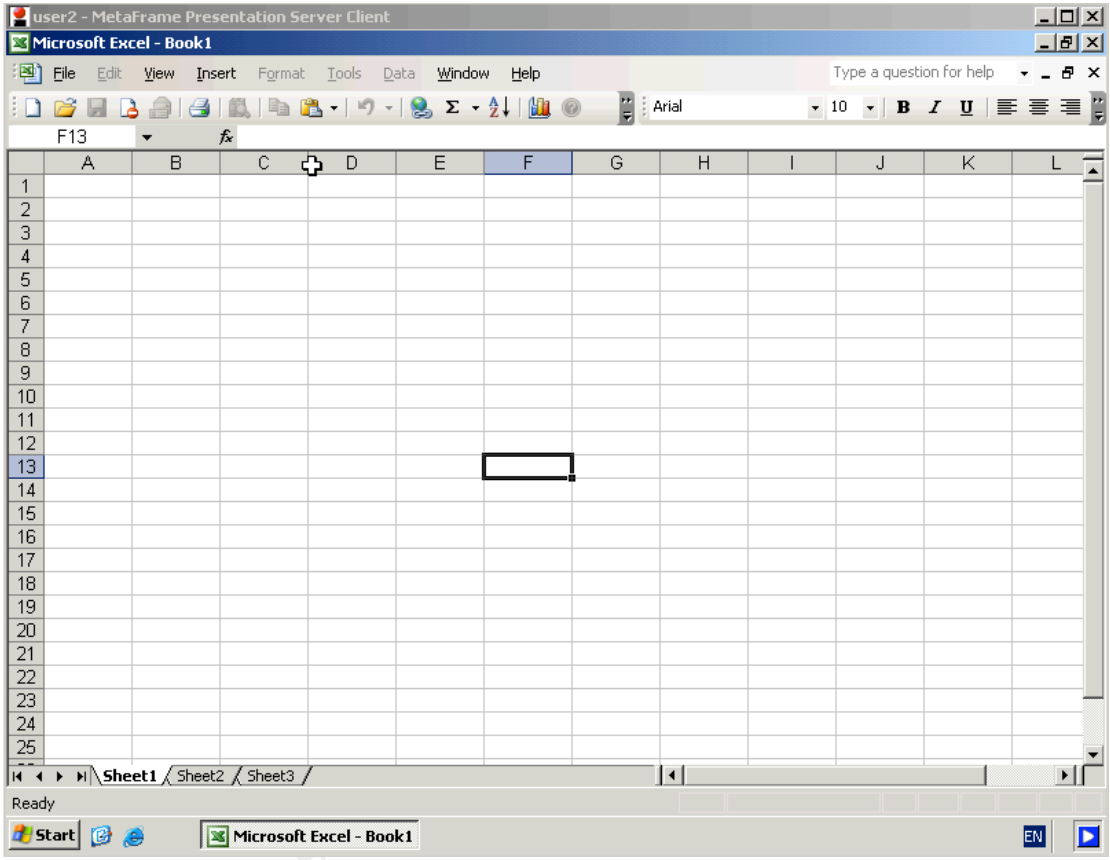


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

In the example above you can see that all the menu items normally available in Internet Explorer have been disabled and hidden from view. As well as simplifying the use of the application for the user this also prevents Help Desk calls caused by "User Configuration" of features like Proxy settings etc.

The example below shows Microsoft Excel 2003:



In this case menu items have been locked (grayed out) and button functionality has been removed. This may be done to prevent users from modifying data in a spreadsheet, or to remove functions that may impact performance in a CPS/TS environment.

These types of lockdowns can be implemented in one of two ways:

1. Group Policy/ADM Template lockdowns, or
2. Third Party products like AppSense Environment Manager and triCerat Simplify Lockdown

Key to this form of locking down applications is the amount of time and effort required to create and deploy them. In this case, the third party products provide significant benefits over

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the use of standard Group Policies.

As an example the lockdowns shown above were created with AppSense Environment Manager, and took only minutes to create and deploy to the CPS/TS server.

As stated earlier, testing is the key to ensure the selected tool will do the required job without large increases in management overhead.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

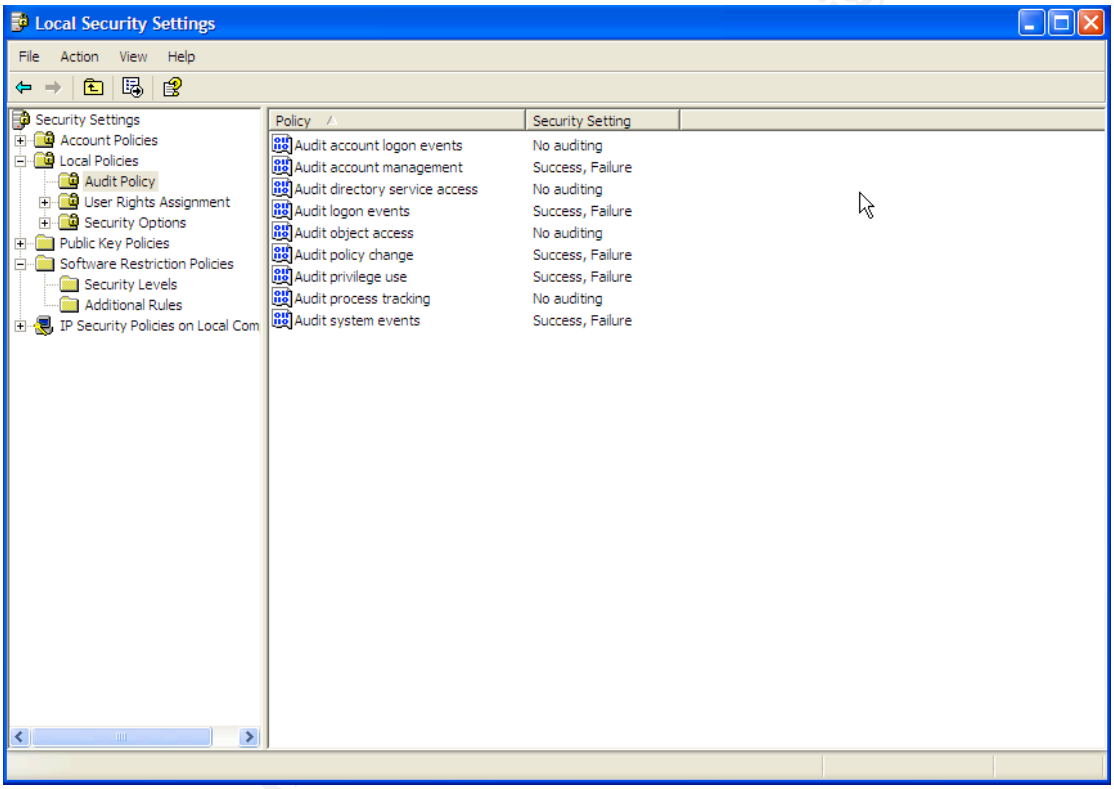
Server Security in a Citrix Presentation/Terminal Server Environment.

5. Auditing and Monitoring

One crucial step which is often overlooked in the CPS/TS world is Auditing and Monitoring. Without effective auditing and monitoring there is no way to determine if the security policies in place are effective or not.

In simple terms, you don't know what you don't know.

Essentially the mechanism for auditing built into Windows 2003 will log events in the event log.



The various elements for audit logging are shown above. Their relevance to a CPS/TS server is discussed below:

1. Audit Account Management. This setting will audit events like creating or deleting of users or groups on the CPS/TS server. This is particularly critical to monitor due to the number of users who will have Logon Locally privileges, and potentially the number of users who have Local Admin rights on the CPS/TS servers.

2. Audit Logon Events. This setting provides information on login patterns and can be used to trap any suspicious failed login attempts. Once again, access to the CPS/TS server will be widespread, so it is critical to make sure

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the login events are monitored.

3. Audit Policy Change. This setting monitors User Rights, Audit Policies, and Domain Trusts. Any changes to these settings will generate auditing events in the event log. While Domain Trusts are more relevant on a Domain Controller, the granting of User Rights and changes to Audit Policies are important and need to be monitored in the CPS/TS world.

4. Audit Privilege Use. This setting is useful in monitoring events like Shutting down the system, Acting as part of the operating system, Taking ownership of objects etc. Failure events associated with Privilege can indicate network issues, or attempted hacker attacks. These events are of particular importance to the CPS/TS world due to the larger number of users with local login access to the servers.

5. Audit System events. These events also track system startup and shutdown, as well as attempts to clear the Security Log. These events should be monitored to make sure all available information is collected in the event of a security breach.

I've skipped over Auditing of Account Logon Events, and Directory Services Access as these are more relevant to a Domain Controller.

The Auditing of Process tracking is a good technique for learning how an application interacts with the operating system. This information can be used to determine access requirements etc for an application in the CPS/TS world. This method of auditing can generate a large amount of events so it should only be used for troubleshooting etc.

Auditing Object Access is another technique useful in the CPS/TS world. By turning this mechanism on, and then setting the SACL's on relevant files or registry keys, the admin team can learn the exact user rights required to allow an application to run successfully in a CPS/TS environment. This process negates the need to use the sledge hammer approach of adding users to the Local Admin group when configuring applications for use in the CPS/TS world.

Software Restriction Policies will also log blocked application execution requests to the event log. The key to remember here is that SRP's will only log requests that it blocks. If a user has found a method to bypass the SRP no logging event will be generated.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

When assessing the commercial products discussed in the "Application Security and Lockdown" section, a review of their auditing capabilities should be included.

Logging events to the event log is one thing, but if there is to be any value in collecting this information is must be monitored and reviewed regularly.

Firstly you need to establish a baseline so you have an idea what is "normal". From there you can compare events to the baseline and monitor by exception rather than wading through every event.

There are a number of excellent tools designed to manage event logs. Two of the best are:

1. EventCombMT , and
2. Logparser 2.2

Both are downloadable from Microsoft's website.

EventCombMT can collect event logs from many servers at once and parse these logs for event id's or even for specific text within an event. This tool has a flexible user interface and greatly simplifies monitoring of event logs for a CPS/TS server farm.

Logparser 2.2 is one of those hidden gems in the Microsoft world. It can parse and filter information from event logs or text files using SQL like queries. Its use is only limited by the imagination, and examples can be found on the website www.logparser.com and in the book "Microsoft Log Parser Toolkit"

A final word on Best Practises for auditing and monitoring, make sure all your systems are time synchronized. If you need to correlate events across servers you have to make sure you can compare times with confidence.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

6. Conclusion

The CPS/TS environment is unique in that it is a combination of server and desktop technology.

The security strategies for this environment need to reflect this and I hope I've helped to outline some of the current best practises being used in the CPS/TS market.

A Security Checklist and references are detailed below to help summarise the information.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

7. Security Checklist

1. **Windows 2003 Server Hardening:**
    - SANS Reading Room
    - Microsoft guide at:http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx
    - Only use NTFS partitions
    - Make sure the server is patched.
    - Make sure AV software is up to date.
    - Disable all unused services.
    - Check for open network ports and close unused ones
    - Remove all unused Users and Groups.
    - Audit and monitor the server.

2. **Windows 2003 Terminal Services Hardening:**
    - Check TS Configuration settings
    - Set Permission Compatibility for Full Security
    - Never add users to the Local Administrators group as a workaround for application compatibility
    - Restrict user membership to Remote Desktop User Group
    - Restrict access to Remote Control (and Shadowing on CPS)

3. **Citrix Presentation Server Hardening:**
    - Restrict access to the Citrix Management Console application ctxload.exe
    - Create a Citrix Admins group as a subset of the Domain Admins group
    - Use Custom settings to tailor task permissions to admin roles

4. **User Profile Lockdown and Security:**
    - Use Mandatory profiles where possible
    - If using Hybrid profiles research and evaluate Third

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Party tools to assist with profile management

5. **Application Security and Lockdown:**
    - Block users from downloading or installing software wherever possible
    - White List, Black List, Trusted Ownership, or a combination, research which is best for your organisation
    - Assess Software Restriction Policies for their effectiveness in your environment
    - Assess and test Third Party products to see where they can add value and save management overhead
    - Lockdown functionality where possible to increase security and simplify applications for users
    - Assess Group Policy/ADM Templates against Third Party products for application lockdown

6. **Auditing and Monitoring:**
    - You don't know what you don't know
    - Decide what you want to audit
    - Establish a Baseline
    - Effective monitoring is the key
    - Use tools like EventCombMT and Log Parser to help
    - Time synchronise all systems

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Server Security in a Citrix Presentation/Terminal Server Environment.

8. References:

General References:

Citrix Website: http://www.citrix.com

Microsoft Website : http://www.microsoft.com

Citrix Presentation Server/Terminal Services Community References:

Brian Madden's website: http://www.brianmadden.com

Brian's site has a wealth of information on CPS/TS infrastructure and his BriForum events have an excellent reputation in the technical community

Doug Brown's website: http://www.dabcc.com

Doug's Methodology In A Box (MIAB) is legendary in the CPS/TS world

Bernhard Tritsch's website: http://www.WTStek.com

Benny's site is full of great information, as is his book listed below

Community Website: http://www.msterminalservices.org

Formally www.thethin.net is an excellent resource for the CPS/TS user community

Books:

Tritsch, Bernhard (2004). Microsoft Windows Server 2003 Terminal Services. Redmond, Washington: Microsoft Press.

Smith, Ben, & Komar, Brian. (2005). Microsoft Windows Security Resource Kit, Second Edition. Redmond, Washington: Microsoft Press.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.