# Security Audit of Citrix NFUSE WWW Server Published Application Infrastructure

“An Auditor Perspective”

**GIAC Systems Network Auditor Certification (GSNA)**
**Practical Assignment version 3.1**

**Date: 18 June 2004**
**Version: 1.1**
**Author: David James O’Neill**

## Abstract

This practical assignment details a technical audit of the infrastructure required to facilitate the remote and public access via the World Wide Web of a Citrix Nfuse published application. The published application is an Internet Explorer Internal web page. In my case I am looking at the various base components, which I have broken into logical zones at a higher level which are required to be in place and functioning in a secure manner to provide remote access to the published application. The audit would be used as a solid base for an organization that has employed this type of remote access, without considering the security considerations, risks and vulnerabilities of such access. Typically businesses add this type of extended Nfuse connectivity to an existing Internal Citrix deployment that has not had external security planning. The basic audit checklist is broken into the following zones, Physical Zone, Network Zone, Citrix in a DMZ Nfuse Zone, Citrix Meta frame Zone and the Windows Active Directory and authentication zones. The purpose of the zone break down is to audit the basic infrastructure to facilitate the remote external access, focusing on areas from experience that are commonly high risk and to allow for detailed expansion on any zone at a later stage or specifically as a later requirement. The checklist basic steps are to identify and assess risks, develop the audit checklist, perform the audit and report on the findings.

# Table of Contents

## 1. Introduction

The growing popularity of remote and mobile computing has seen the increased need to provide user access to many business applications over infrastructure such as the internet. Remote Access and its availability and reliability have become an increased business asset and its availability a major risk.

Citrix has become a widely popular method to deliver applications or remote desktop access to remote users. An administrator can publish applications that can then be accessed via a Citrix network neighborhood client with the ICA protocol.

Citrix Meta Frame Server is a server that sits on top of a Windows NT or Windows 2000 Server. This is the big brother so to speak of the Microsoft Terminal Services Product which utilizes the Remote Desk Top Protocol. Application's or desktops access are installed and configured on the Citrix Meta Frame Server and then published for access to users. User access is authenticated with an NT SAM user database or Windows 2000 Kerberos and Active Directory.

A web portal product from the Citrix family known as Nfuse can also be used to present published applications to the internet, utilizing Microsoft Internet Information server or other web server applications. This adds a further level of granular access control, by incorporating the Citrix Secure Gateway Server which reverse proxies as such the ICA protocol back to the Citrix Server.

**Confidentiality** - Data housed in the target company system and database repositories are frequently confidential, therefore a key requirement is the segregation of customer data from the public and other customers.

- **Integrity** - The integrity of data is critical in the management of data on behalf of customers and suppliers.

- **Availability** - Availability of Application via the NFUSE systems and networks is necessary as customer services are dependent upon these applications which in turn depend on these services.

# I. Research in Audit Measurement Practice and Control

## 2. Research

### 2.1 System Identification

Scope of this Audit is to cover the transport or delivery architecture of the published application, which will include the following main areas or "key security zones" of the Infrastructure required to publish Citrix applications to the end user on the World Wide Web.

Physical Access to Hardware.

Logical Network Access, including External Firewall Rules.

Citrix Nfuse Application Server Configuration, Citrix Secure Gateway Configuration and Windows 2000 Base Operating System.

Logical Network Access, including Internal Firewall Rules.

Citrix Terminal Server ICA Communications configuration.

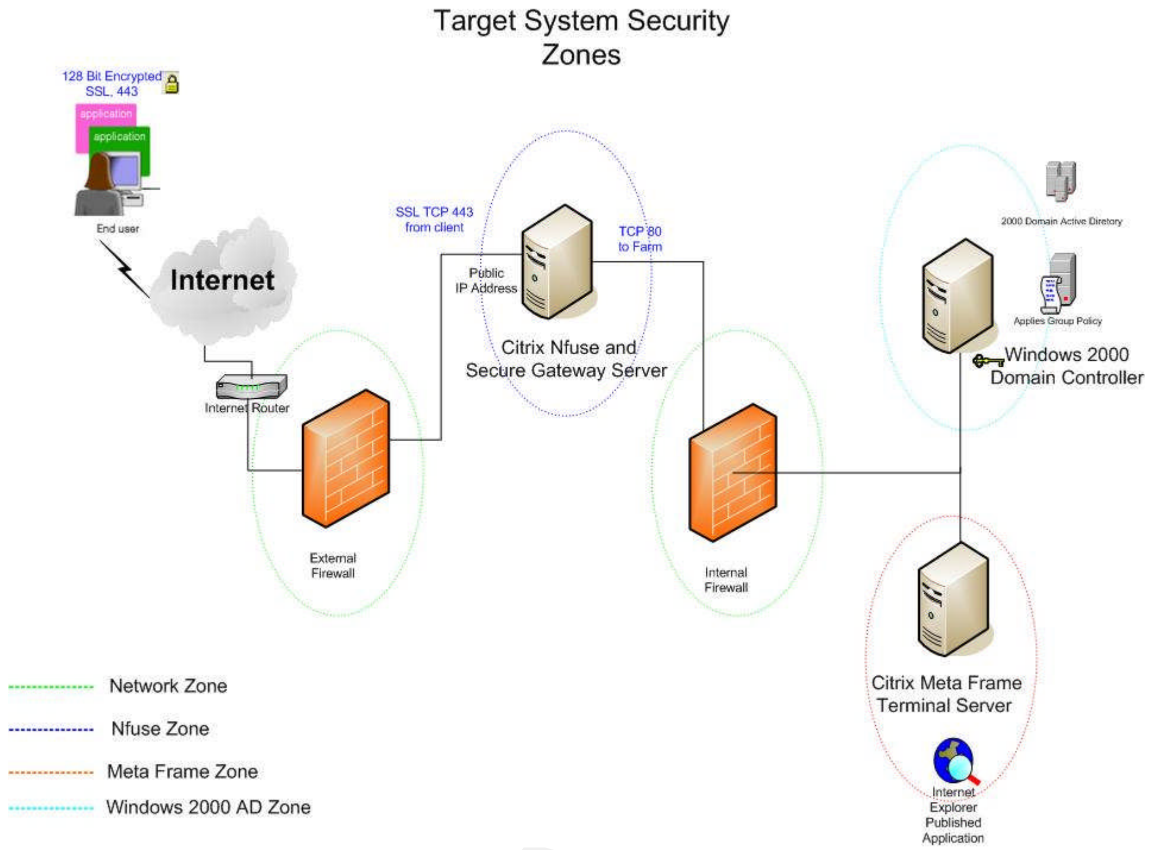
Windows 2000 Group Policy – Domain User Accounts, Specific Citrix User Account Policies and Citrix Terminal Server Machine Account Policies within the Windows 2000 Domain Active Directory.

The scope here is to focus on auditing the base architecture with regards to Citrix recommended best practice configuration, logical design and Base Operating System platform.

Windows 2000 server base configuration is based on the MS Windows Baseline Security Analyzer Service Packs, critical updates and same basic good practice related to an Internet exposed web server. The scope does not included analyzing the Operating System as highly secure build of windows 2000, compliant with such groups as the National Institute of Standards and Technology (**NIST**) ,Nessus or Center for Internet Security Scanners interpretations of Operating System security levels

The concept I am trying to achieve in breaking this audit down into "logical zones" and covering only some base key areas is a "high level" base architectural audit. The scope can be logically extended as a "stage two" approach, by focusing in much more detail on any particular zone.

This audit will not cover the security of the stored data in the published application (Internet Explorer intranet web page) itself.


Target System Security Zones
128 Bit Encrypted SSL, 443
application
application
End user
Internet
Internet Router
External Firewall
SSL TCP 443 from client
Public IP Address
Citrix Nfuse and Secure Gateway Server
TCP 80 to Farm
Internal Firewall
2000 Domain Active Diretory
Applies Group Policy
Windows 2000 Domain Controller
Citrix Meta Frame Terminal Server
Internet Explorer Published Application
Network Zone
Nfuse Zone
Meta Frame Zone
Windows 2000 AD Zone

### 2.2 Significant Risks Assessment

Remote Access to business applications is the critical business asset that needs to be protected in terms of the [1]C.I.A Triad (Confidentiality, Integrity and Availability.)

This is the primary goal and fundamental principle of a Security Program.

The level of security required to accomplish these principles varies per company because their security goals and requirements may be different. All security controls, mechanisms and safeguards are implemented to provide one or more of these principles and all risk, threats and vulnerabilities are measured in their potential capability to compromise these principles.

#### 2.2.1 Risk Analysis

The risk ratings described in this section take into account potential attacks from internal as well as external sources. Some of these attacks would require advanced skills to execute from an external point of view, but are relatively simple if attempted on the same network. Risks are assigned assuming an attacker has corporate network access, and are elevated for attacks that could be performed over the Internet. This table can be further utilised by management and security personnel to define the required risk (the risk level the management is prepared to accept), and then a countermeasure priority rating, to assist in reducing the outstanding risks.

The Risk Table is based on the approach taken by the [2]AS/NZ Standard 4360 and the Australian Communication Security Instruction (ACSI) 33 published by the Defence Security Directorate (DSD).

The following definitions are used for each section.

| **Likelihood** | **Definition** |
|---|---|
| Negligible | Unlikely to occur |
| Very Low | Likely to occur every two or three years |
| Low | Likely to occur every year |
| Medium | Likely to occur every six months or less |
| High | Likely to occur once a month or less |
| Very High | Likely to occur multiple times per month or less |
| Extreme | Likely to occur daily |

| **Impact** (underlined)<br>**(Consequence)** | **Definition** |
|---|---|
| Minor | Will have almost no impact |
| Significant | Will result in some tangible harm, albeit small. Will require some expenditure of resources to repair. |
| Damaging | May cause damage to the reputation of system management, and or loss of confidence in the system’s resources or services. Will require expenditure of significant resources to repair. |
| Serious | May cause extended system outage, and/or loss of customers or business confidence. May result in compromise of large amounts of information. |
| Grave | May cause system to be permanently closed or moved to another environment |

Risk can be expressed as *“threat likelihood x consequence = risk”*

| | | **Consequence** | | | | | |
|---|---|---|---|---|---|---|---|
| **Threat** | | Insignificant | Minor | Significant | Damaging | Serious | Grave |
| | Negligible | nil | nil | nil | nil | nil | Nil |
| | Very Low | nil | low | low | low | medium | medium |
| | Low | nil | low | medium | medium | high | High |
| | Medium | nil | low | medium | high | high | critical |
| | High | nil | medium | high | high | critical | extreme |
| | Very High | nil | medium | high | critical | extreme | extreme |
| | Extreme | nil | medium | high | critical | extreme | extreme |

Countermeasures to the risks may relate to:

- Addition of security measures.
- Risk avoidance through change of service and system specification.
- Acceptance of residual risk.
- Minimisation of harm through response or control mechanisms.

### 2.2.2 Physical Risk Analysis

Physical Security Access Risks are generally from unauthorized physical hands on access available to a potential malicious user. Physical deterrents such as Locked Server Rooms with a key pass or swipe card access control mechanism, Video surveillance or Security Guard Monitoring, Locked Rack doors front and rear and signing in and out procedures can mitigate such risks.

Risks include unauthorized users being able to plug a network sniffer into the wire to collect passwords, physically unplug systems as a form of Denial of Service, or reboot machines with bootable floppy disks that can reset Local Administration passwords in order to gain high privileged system access. Other risks include theft of Hard disk drives, Backups Tapes and in some cases whole machines. Backup Tapes and Hard Disk Drives are easy “Soft Targets” as NTFS or FAT formatted disks can be mounted on other machines or tapes catalogued, inventoried or restored on alternate systems.

Additional System Board countermeasures where supported, include using a BIOS password in order to prevent users changing BIOS system settings, a Boot password to prevent the system from being booted and restricting bootable devices such as floppy disk drives and CD ROM Drives. The password policy for BIOS and boot password should match the level of complexity of that of your operating system password policy to maintain a consistency.

IT Security Policy [3]'A security policy is an indication of management’s direction and support for Information Security in the organisation' (ISO 17799:2001). The absence of such a policy creates an exposure in that without management support and direction the implementation of security controls will in all likelihood be ad hoc and inconsistent. Further the investigation of any security related incidents will be hampered by the absence of a direction from management.

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| PHY001 | No Business Security Policy | No IT Security Policy leads to Mismanagement and no standards or guidelines of usage | High | Moderate | Medium |
| PHY002 | Physical Access to Servers | DOS attack, Theft, ( See Above ) | Medium | Serious | Extreme |

### 2.2.3 Network / Internet Risk Analysis

A firewall is generally the primary perimeter protection in most organizations, if configured incorrectly the consequences could be disastrous.

[4]"Default Deny Stance: That which is not explicitly permitted is denied"

This is a failsafe stance by prohibiting what we don't know; it involves understanding the services that are required to safely provide the desired service.

Best Practice firewall configuration is to simply drop a packet, rather than reject a packet which may with some firewall vendors send a response with the reject.

Routing considerations are also important to consider especially with DMZ hosts as the principle of explicit thirty two bit network mask, host based routing should be applied to effectively limit the logical networking capability of connectivity

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| NET001 | Incorrect External Firewall rules | Additional access to Nfuse Server or DMZ | Medium | Serious | Extreme |
| NET002 | Incorrect Internal Firewall rules | Additional access to Nfuse Server or Internal LAN | Medium | Serious | Extreme |
| NET003 | Default or Additional Routes to internal Network | The DMZ Nfuse server can logically connect to the internal network | High | Serious | Very High |

### 2.2.4 Windows Base Operating System Analysis

Microsoft provide the www.windowsupdate.com website to aid in keeping the Windows 2000 Operating system up to date with the latest critical updates, service packs and hot fixes.. This is referenced by the MS baseline security analyzes.

The hot fixes and updates are for various flaws and exploits in the base Operating system. An example of some is

- Q320206 Authentication Flaw in Windows Debugger can Lead to Elevated Privileges
- Q318138 Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution
- Q326886 Flaw in Network Connection Manager

- Q323172 Flaw in Digital Certificate Enrolment Component Allows Certificate Deletion
- Q328145 Certificate Validation Flaw Could Enable Identity Spoofing

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| OS001 | Service Packs and Critical Updates not installed and up to date | Published exploits will be available on the internet therefore rendering the server highly vulnerable | Very High | Grave | Extreme |
| OS002 | Unwanted Services are not removed | Unwanted entry points and resource usage | Very High | Serious | Extreme |
| OS003 | Warning Legal Banner not Used | Prosecution may not be viable without explicitly explaining prohibited access | Medium | Significant | Low |
| OS004 | Additional Default users enabled | Guest and IIS users could be compromised to gain access | High | Serious | Medium |

### 2.2.5 Citrix Nfuse Risk Analysis

There are some recommendations involving the use of the IIS LockDown tool available from Microsoft http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp) and the URLScan tool available from Microsoft (http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q307608&).

Citrix have also recommended securing the Nfuse server by running the IIS Lockdown on an IIS server running Nfuse https://support.citrix.com article number CTX101778 to disable and reset some of the following parameters, Back up metabase, Lock httpext.dll, remove script mappings and *.idq

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| CNF001 | Non Encrypted Web service | Password sent in clear text | Very High | Deadly | Extreme |
| CNF002 | IIS Server not Hardened or Lockdown | Compromise web server and execute scripts etc | Very High | Serious | Extreme |
| CNF003 | Guest Logins allowed on Nfuse service | Reconnaissance | High | Serious | High |
| CNF004 | Access to Nfuse Administration Web Site | Full control of Nfuse configuration | Extreme | Serious | Extreme |
| CNF005 | | | | | |

### 2.2.6 Citrix Secure Gateway Analysis

The Citrix Secure Gateway is a solution that is designed to protect a customer's Network infrastructure, data and published applications. All Citrix ICA traffic traversing the Internet between client devices and the Citrix Secure Gateway server is encrypted using Internet standard SSL technology, ensuring the secure transfer of data across public networks. It protects remote users of Citrix Independent Computing Architecture (ICA®) across the Internet by functioning as a Secure Sockets Layer (SSL) gateway between Citrix Metaframe servers and Citrix ICA client devices. It also provides a single point of entry and secure access to Citrix Metaframe server farms.

Citrix Secure Gateway removes the need to publish the address of every Citrix Metaframe server across the Internet. Citrix Metaframe servers are hidden from the Internet and cannot be accessed or directly as it provides a single secure point of access into the Citrix Metaframe server farm.

Incorrect configuration can lead to direct access and non encrypted sessions which may in turn lead to a loss of remote service delivery

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| CSG001 | CSG not configured with 128 Bit digital Certificate | Non Encrypted www traffic and proxy service to Secure Ticket Authority | Medium | Serious | Extreme |
| CSG002 | No timeout policy for disconnected and idle sessions | Hijack user session | Very High | Serious | Extreme |
| CSG003 | Citrix Logging not enabled | No audit trail | Very High | Serious | Extreme |
| CSG004 | Unlimited connections | Citrix Service DOS | Very High | Serious | Very High |

### 2.2.7 Citrix Meta frame Server Configuration

The properties of the ICA Connection settings need to be examined for configuration with the default settings. This means that users accessing applications on the Meta Frame server farm via Nfuse could expose the applications to malicious users. If a user was using an application from an internet café via Nfuse and walked away from the terminal without ending the session, currently the session would remain active. A timeout policy for disconnected and idle sessions should be addressed

Citrix recommend that Active Directory (AD) groups be used to assign a user rights to launch a specific application, therefore specific access will be granted via the users Group Membership assigned against the application rather than an everybody basis

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| CMF001 | ICA Protocol access not explicitly defined | Any TCP device can establish a connection | High | Serious | Extreme |
| CMF002 | RDP Protocol access not explicitly defined | Any TCP device can establish a connection | High | Serious | Extreme |
| CMF003 | Default Install File permissions on Meta frame server | Users have the ability by default to browse the Meta frame server C: Drive and install, edit and copy files etc | High | Serious | Very High |
| CMF004 | No Group Policies applied to Specific Citrix Computer Accounts | Applications and user access difficult to restrict | Very High | Deadly | Extreme |
| CMF005 | No Administrative Templates applied to Specific Citrix Users | Users have ability to launch a remote desktop, Execute run from task bar, use Open from IE Launch bar | Very High | Deadly | Very High |
| CMF006 | Latest Citrix Service Packs not installed | Remote DOS attack as per [5]www.securityfocus.com | Very High | Deadly | Very High |
| CMF007 | Auditing Policy Not Defined | Lack of accountability, tracking and auditing | High | Medium | High |

### 2.2.8 Published Application Risks Analysis

Citrix provides the ability to publish applications via its Nfuse and CSG portal. A granular approach to security of the applications is available to the administrator with the ability to lock down the Citrix remote access protocol and application in which a user has access if configured with explicit security group permissions.

The consequences of incorrect configuration of these security roles or permissions is grave as the confidentiality and integrity of the application being accessed is no longer guaranteed

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| CPA001 | Latest Citrix Feature Pack not installed | Lack of Auditing Administrators | Medium | Serious | High |
| CPA002 | Applications not published on a per group basis | Un restricted Application Access | High | Serious | Extreme |

### 2.2.9 Active Directory User Account Risk Analysis

Microsoft Active Directory gives us the ability to provide User Account Policies which are non discretionary which in turn can be reflected in the Company IT security Policy. This means consensus best practice around, enforcing password history; Maximum password age, Minimum password age, Minimum password length, Passwords must meet complexity requirements and Store passwords using reversible encryption. This provides us with a level of protection around the common password attacks such as brute force and password cracking.

| Audit Category Reference | Threat | Capacity to Inflict damage | Likelihood (N/VL/L/M/H/VH/E) | Impact (M/S/D/S/G) | Consequence (N/VL/L/M/H/VH/E) |
|---|---|---|---|---|---|
| ADUSR001 | Group Domain User Password Policy not defined | Weak password, re use password | Very High | Serious | Extreme |
| ADUSR001 | Group Domain Account Lockout Policy not defined | Password susceptible to Brute Force attack | Very High | Serious | Extreme |

### 2.2.10 Major Information Asset Assessment

The major asset to the business provided by Citrix Nfuse published applications is the ability to provide "Remote Access to Applications" This may be in some case critical to the businesses ability for example to supply access to internal applications to customers.

| Audit Category Reference | Audit Subject | Major Information Asset Effected |
|---|---|---|
| PHY001 | Security Policy | Remote Access to application |
| PHY002 | Infrastructure | Remote Access to application |
| NET001 | Infrastructure | Remote Access to application |
| NET002 | Infrastructure | Remote Access to application |
| NET003 | Infrastructure | Remote Access to application |
| OS001 | Infrastructure | Remote Access to application |
| OS002 | Infrastructure | Remote Access to application |
| OS003 | Infrastructure | - |
| OS004 | Infrastructure | Remote Access to application |
| CNF001 | Infrastructure | Remote Access to application |
| CNF002 | Infrastructure | Remote Access to application |
| CNF003 | Infrastructure | Remote Access to application |
| CNF004 | Infrastructure | Remote Access to application |
| CSG001 | Infrastructure | Remote Access to application |
| CSG002 | Infrastructure | Remote Access to application |
| CSG003 | Infrastructure | - |
| CSG004 | Infrastructure | Remote Access to application |
| CMF001 | Infrastructure | Remote Access to application |
| CMF002 | Infrastructure | Remote Access to application |
| CMF003 | Infrastructure | Remote Access to application |
| CMF004 | Infrastructure | Remote Access to application |

| | | |
|---|---|---|
| CMF005 | Infrastructure | Remote Access to application |
| CMF006 | Infrastructure | Remote Access to application |
| CMF007 | Infrastructure | Remote Access to application |
| CPA001 | Infrastructure | - |
| CPA002 | Infrastructure | - |
| ADUSR001 | Infrastructure | Remote Access to application |
| ADUSR002 | Infrastructure | Remote Access to application |

### 2.2.11 Audit Subject Vulnerabilities

| **Audit Category Reference** | **Audit Subject** | **Major Vulnerability** | **Degree of Exposure (L/M/H)** | **Potential Impact (M/S/D/S/G)** |
|---|---|---|---|---|
| PHY001 | Security Policy | Mismanagement and no standards or guidelines of usage | High | Serious |
| PHY002 | Infrastructure | Theft, DoS ( see 2.2.2 ) | Medium | Grave |
| NET001 | Infrastructure | Compromise NFUSE Server additional DMZ access | High | Grave |
| NET002 | Infrastructure | Compromise NFUSE Server additional LAN access | High | Grave |
| NET003 | Infrastructure | Additional LAN access | Medium | Serious |
| OS001 | Infrastructure | Can provide access to services DoS such as SASSER exploit | High | Grave |
| OS002 | Infrastructure | Can provide access to services i.e. task Scheduler | High | Serious |
| OS003 | Infrastructure | - | Low | Significant |
| OS004 | Infrastructure | Guest Access | High | Damaging |
| CNF001 | Infrastructure | Unencrypted passwords | High | Grave |
| CNF002 | Infrastructure | DoS i.e. Code Red | High | Grave |
| CNF003 | Infrastructure | Access Nfuse Configuration | High | Serious |
| CNF004 | Infrastructure | Alter Nfuse Configuration | High | Grave |
| CSG001 | Infrastructure | Sniff Network traffic | High | Serious |

| | | | | |
|---|---|---|---|---|
| CSG002 | Infrastructure | Session hijacking | High | Serious |
| CSG003 | Infrastructure | No audit trail | High | Serious |
| CSG004 | Infrastructure | DoS See Footnote 5 | High | Serious |
| CMF001 | Infrastructure | Session hijacking | High | Serious |
| CMF002 | Infrastructure | Session hijacking | High | Serious |
| CMF003 | Infrastructure | Compromise Meta Frame Server | High | Serious |
| CMF004 | Infrastructure | Published Application Security | High | Serious |
| CMF005 | Infrastructure | Published Application Security | High | Serious |
| CMF006 | Infrastructure | DoS See Footnote 5 | High | Serious |
| CMF007 | Infrastructure | No Audit Trail | High | Serious |
| CPA001 | Infrastructure | No Administrator Audit Trail | High | Serious |
| CPA002 | Infrastructure | Unrestricted Application Access | High | Serious |
| ADUSR001 | Infrastructure | Ease of Password Compromise | High | Serious |
| ADUSR002 | Infrastructure | Brute Force password attack | High | Serious |

### 2.3 Current State of Practice

The current primary resource for Citrix and its associated infrastructure can be found at www.support.citrix.com . Citrix have a fully maintained and searchable web site for researching the current best practices for deploying Nfuse and Citrix Secure Gateway in a number of essential guides and checklists. The current state of hot fixes and service packs can be researched here. The auditor not having a primary Citrix background found this an invaluable tool and research point for a definitive answer or instruction for ascertaining configuration and related information.

Initiatives by many web based security groups such as www.incident.org www.cert.org and www.iss.net, www.bagtrack.com and www.atstake.com list and maintain vulnerabilities databases, best practices and checklist guides, security scanning tools and subscriptions list. These are as essential as tools themselves to the auditor's tool kit. The security auditing arena is also filled with many great text books which list tools, guidelines and instructions for use. I recommended the [6]GSEC Security Essentials Toolkit and [7]HACKING EXPOSED Network Secret and Solutions as reference points for current tools and practices. Microsoft is more committed to security these days as well with excellent resources, guidelines and references available at www.microsoft.com.au/security . The auditor in particular referenced http://www.microsoft.com/technet/security/chklist/iis50srg.mspx guide to securing IIS 5.0 server prior to commencing this audit.

The SANS GSEC Track 1 Security Essentials 1.5 Windows Basics provides a basic 10 step approach to securing a windows server along with a “Vendor Neutral“ approach to best practices around concepts such as Account Lockout and User Account Password Policy and auditing. SANS Institute have also have produced a guide called “Securing Windows 2000 Step By Step” which is a consensus document produced by security professionals around the world. This is an excellent reference point as it is a consensus Internet community opinion on elements of windows 2000 security and best practice.

The Windows NT Security Guidelines is a study for the National Security Agency by the Trusted Systems Services which outlines considerations & guidelines for securely configuring Microsoft Windows.

## II. AUDIT CHECKLIST DEVELOPMENT

### 4. Audit Checklist

### Audit Item 1 – IT Security Policy

| | |
|---|---|
| **Audit Category Reference** | PHY001 |
| **Title** | IT Security Policy |
| **Reference** | A Security Policy is the first point in the businesses commitment to Security within the business. It must be explicit, well defined and enforced by the mechanisms within the system which provide the security of the business assets |
| **Risk Area** | In the event of mismanagement and/or no standards or guidelines of usage, the degree of exposure to the business would be high and the severity in event of exploitation would be grave. |
| **Compliance** | Current and enforced IT Security Policy relating to Remote Access and configuration |
| **Test Method** | Conduct Staff Interviews.<br>Sight and review IT security Policy in relation to remote access procedures and policies |
| **Test Type** | Subjective |
| **Evidence** | Policy Document relating to Remote Access and configuration |
| **Findings** | |

### Audit Item 2 – Physical Access

| | |
|---|---|
| **Audit Category Reference** | **PHY002** |
| **Title** | Physical Access |
| **Reference** | CISSP Guide, Harris, Shon. Chapter 6 page 279 – Physical Security |
| **Risk Area** | A medium degree of exposure to physical infrastructure could result in a total loss of service rendering business processes shut down. |
| **Compliance** | Secured Access Points, alarms and video monitoring |
| **Test Method** | 1. Organise a visit to the Data Center housing Citrix Servers.<br>2. Attempt unauthorised physical access to building, network and Server console<br>3. Check Physical Controls |
| **Test Type** | Subjective |
| **Evidence** | Door Locks, access control systems to building and Data Center, Security Guards, alarms and Video surveillance. |
| **Findings** | |

**Audit Item 3 – Incorrect External Firewall Rules**

| | |
|---|---|
| **Audit Category Reference** | **NET001** |
| **Title** | Incorrect External Firewall Rules |
| **Reference** | O'Reillys Building Internet Firewalls |
| **Risk Area** | Unnecessary or unsecured services running on the DMZ Nfuse server can be connected to if the firewall has incorrect rules allowing additional access Unnecessary or unsecured services running on the DMZ Nfuse server can be connected to if the firewall has incorrect rules allowing additional access |
| **Compliance** | All traffic not explicitly required by Citrix Nfuse WWW server dropped |
| **Test Method** | [8]Nmap Port scan internet Citrix IP addresses.<br>Nmap –P0 –v –Sc <NFUSE Server- PUBLIC Address><br>Examine results<br>Check results of Nmap by executing a telnet to any open ports listed by Nmap |
| **Test Type** | Objective |
| **Evidence** | Citrix Nfuse only requires SSL Port 443 for external access. |
| **Findings** | |

**Audit Item 4 – Incorrect Internal Firewall Rules**

| | |
|---|---|
| **Audit Category Reference** | **NET002** |
| **Title** | Incorrect Internal Firewall Rules |
| **Reference** | O'Reillys building internet firewalls |
| **Risk Area** | Unnecessary or unsecured services running on the DMZ Nfuse server can be connected to if the firewall has incorrect rules allowing additional access |
| **Compliance** | All traffic not explicitly required by Citrix Nfuse WWW server dropped |
| **Test Method** | [9]Nmap Port scan internet Citrix IP addresses.<br>Nmap –P0 –v –Sc <NFUSE Server- Internal Address><br>Examine results<br>Check results of Nmap by executing a telnet to any open ports listed by Nmap |
| **Test Type** | Objective |
| **Evidence** | Citrix Nfuse only requires HTML Port 80 for XML and TCP Port 1494 for internal access to Metaframe Server. |
| **Findings** | |

**Audit Item 5 – Default or additional Routes to internal network**

| | |
|---|---|
| **Audit Category Reference** | **NET003** |
| **Title** | Default or additional Routes to internal network |
| **Reference** | Personal work experience using MS Windows and Unix varieties have seen poor network configurations. |
| **Risk Area** | Compromise of internal resources may be possible by leveraging off a compromised DMZ host with broad network routing to internal networks i.e. 10.0.0.0./8 |
| **Compliance** | Specific 32bit subnet mask host routes as required |
| **Test Method** | Netstat – rn to display route tables.<br>Ping, telnet and Map Network drive tests to a known critical internal host. |
| **Test Type** | Objective |
| **Evidence** | The Nfuse DMZ server only requires one explicit 32 bit subnet mask host route to internal Metaframe server, eliminating the connectivity to other internal hosts |
| **Findings** | |

**Audit Item 6 – Service Packs and Critical Updates not installed or up to date**

| | |
|---|---|
| **Audit Category Reference** | **OS001** |
| **Title** | Service Packs and Critical Updates not installed and up to date |
| **Reference** | [10] www.windowsupdate.com |
| **Risk Area** | [11] Code Red Worm , ida/idq (indexing services ASAPI) buffer overflows |
| **Compliance** | Service Packs and Critical Updates up to date as per MS Baseline Security analyser report |
| **Test Method** | 1. Run MS baseline security analyser<br>2. Download latest secure XML<br>3. View analyse and compare output |
| **Test Type** | Objective |
| **Evidence** | Windows update web site and MS baseline security analyser should reveal no critical updates required and ( 0 security updates are missing or are out-of-date in MS Baseline Report ) |
| **Findings** | |

### Audit Item 7 – Unwanted Services are not running and disabled

| | |
|---|---|
| **Audit Category Reference** | **OS002** |
| **Title** | Unwanted Services are not removed |
| **Reference** | Hacking Exposed 2000 Network Security Secrets and Solutions SCAMBRAY, Joel and MCCLURE, Stuart. – Scheduled Jobs page 188 |
| **Risk Area** | Schedule service can be used to launch Trojan programs or commands for an intruder to connect. |
| **Compliance** | Unnecessary services removed. |
| **Test Method** | 1. Run Foundstone's fport (FPort v2.0 - TCP/IP Process to Port Mapper Copyright 2000 by Foundstone, Inc. http://www.foundstone.com)<br>2. Execute net start command<br>3. Examine outputs for running services and compare against disabled services in MS Services MMC Console |
| **Test Type** | Objective |
| **Evidence** | The following services are not required for the Windows 2000 Nfuse servers and would be expected to be disabled, Alerter, Computer Browser, DHCP Client , Distributed File System, Distributed Link Tracking Client, IPSEC Policy Agent, IIS Admin Service, License Logging Service, Messenger, Print Spooler, Remote Registry Service, Removable Storage, RunAs Service, Server, Task Scheduler, SNMP, TCP/IP NetBIOS Helper Service, Telnet, Terminal Services, Workstation, IIS FTP, IIS SMTP |
| **Findings** | |

### Audit Item 8 – Warning Legal banner not used

| | |
|---|---|
| **Audit Category Reference** | **OS003** |
| **Title** | Warning Legal banner not used |
| **Reference** | Introduction to Computer Law, 3rd Edition, BAINBRIDGE, David. – Page 152 Liability and Negligence, Duty of Care |
| **Risk Area** | Legal prosecution more difficult to attain. |
| **Compliance** | Use Warning Legal Banner stating restricted system usage and criminal prosecution for unauthorised offenders |
| **Test Method** | 1. Perform standard logon to Nfuse Server<br>2. Observer any banner or disclaimer and at which stage during the logon process notification occurs |
| **Test Type** | Objective |
| **Evidence** | Legal Banner displayed upon logon |
| **Findings** | |

### Audit Item 9 – Additional Default users enabled

| | |
|---|---|
| **Audit Category Reference** | **OS004** |
| **Title** | Additional Default users enabled |
| **Reference** | Guest Account enabled<br>Hacking Exposed 2000 Network Security Secrets and Solutions SCAMBRAY, Joel and MCCLURE, Stuart. – Page 99 mid page paragraph stating guest account has blank password by default on Windows 2000. |
| **Risk Area** | Malicious user may leverage off guest account for initial system access. |
| **Compliance** | Disabled, deleted guest account |
| **Test Method** | 1. Execute a net use \\<nfuseserver>\ipc$ * -u /u:guest<br>Enter no password when prompted |
| **Test Type** | Objective |
| **Evidence** | If the guest account is disabled system error 1331 should display "logon failure: account disabled" |
| **Findings** | |

### Audit Item 10 – Non encrypted Web service

| | |
|---|---|
| **Audit Category Reference** | **CNF001** |
| **Title** | Non encrypted Web service |
| **Reference** | WWW.support.citrix.com Best practices for securing a Citrix Secure Gateway Deployment page 4 Citrix Nfuse. |
| **Risk Area** | Non encrypted traffic can be captured with packet sniffing programs and passwords will be exposed in clear text. |
| **Compliance** | Encrypted NFUSE WWW server connection, 128bit Digital CA certificate installed, and requiring 128bit encryption for connection. |
| **Test Method** | 1. Connect Auditors machine to Network device on subnet of Citrix Nfuse server and set NIC to promiscuous mode.<br>2. Capture Traffic with Ethereal Packet Capture tool<br>3. Analyse pack capture for usernames and password in clear text |
| **Test Type** | Objective |
| **Evidence** | Packet capture data payload should not contain any usernames or password if encrypted data should be unreadable |
| **Findings** | |

### Audit Item 11 – IIS Server not hardened or Lockdown

| | |
|---|---|
| **Audit Category Reference** | **CNF002** |
| **Title** | IIS Server not hardened or Lockdown |
| **Reference** | WWW.support.citrix.com Running IIS Lockdown on an IIS server running Nfuse or Web Interface<br>Document ID: CTX101778 |
| **Risk Area** | [12] Code Red Worm , ida/idq (indexing services ASAPI) buffer overflows |
| **Compliance** | IIS Lockdown Tool Run and configured as per above |
| **Test Method** | Look for evidence of lock down tool run.<br>Test for remediation done with the lockdown tool as per Document ID: CTX101778, including traverse www directory, execute script files and removal of default install components. |
| **Test Type** | Objective |
| **Evidence** | Testing all objectives of Document ID: CTX101778 remediation should fail. |
| **Findings** | |

### Audit Item 12 – Guest Logins allowed on Nfuse Services

| | |
|---|---|
| **Audit Category Reference** | **CNF003** |
| **Title** | Guest Logins allowed on Nfuse Services |
| **Reference** | Web Interface for Metaframe XP Administration – Authentication configuration |
| **Risk Area** | Malicious user may leverage off guest account for initial system access. |
| **Compliance** | Guest logins not allowed |
| **Test Method** | Attempt guest login to Nfuse Application via web browser |
| **Test Type** | Objective |
| **Evidence** | Nfuse Application via web browser should be denied if guest logins to Nfuse are disabled |
| **Findings** | |

### Audit Item 13 – Access to Nfuse Administration on Website

| | |
|---|---|
| **Audit Category Reference** | **CNF004** |
| **Title** | Access to Nfuse Administration on Website |
| **Reference** | Personal work experience has seen administration web interface access https://companyhost/Citrix/MetaFrameXP/WIAdmin/default.asp via bypassing administrator access or passwords. |
| **Risk Area** | Web Access to Nfuse administration and configuration website not secured. |
| **Compliance** | Explicit access to administrators only |
| **Test Method** | Attempt login as regular user ( account used for testing ) to Nfuse administration and configuration website console |
| **Test Type** | Objective |
| **Evidence** | Access to Nfuse administration and configuration website console should be denied. |
| **Findings** | |

### Audit Item 14 – CSG not configured with 128 Bit digital Certificate

| | |
|---|---|
| **Audit Category Reference** | **CSG001** |
| **Title** | CSG not configured with 128 Bit digital Certificate |
| **Reference** | WWW.support.citrix.com Best practices for securing a Citrix Secure Gateway Deployment. Page 4 Process Flow point 5 |
| **Risk Area** | Non encrypted traffic can be captured with packet sniffing programs and passwords will be exposed in clear text. |
| **Compliance** | Citrix secure gateway configured explicitly for only SSL traffic |
| **Test Method** | Attempt connection to www Nfuse default login page ( home page ) with http ( TCP Port 80 ) connection |
| **Test Type** | Objective |
| **Evidence** | The client web browser should report an error stating https ( SSL TCP port 443 ) is required for the connection to this web site ( default login page) |
| **Findings** | |

**Audit Item 15 – No timeout policy for disconnected and idle sessions**

| | |
|---|---|
| **Audit Category Reference** | **CSG002** |
| **Title** | No timeout policy for disconnected and idle sessions |
| **Reference** | Personal work experience has seen this as critical as remote users cannot be monitored by business employees offering the remote service. |
| **Risk Area** | Unattended session may be accessed by unauthorized user resulting in data theft, alteration or perusal. |
| **Compliance** | Timeout policy enabled and enforced. |
| **Test Method** | 1. Login to Citrix Nfuse www site from a public network with supplied user account.<br>2. Simulate idle time ( go make a coffee ) endeavouring to keep track of idle time on stopwatch<br>3. Check the original Citrix session is still connected.<br>4. Check Server Configuration against time out |
| **Test Type** | Objective |
| **Evidence** | The original Citrix Nfuse session should disconnect if idle time exceeds the configured Idle Timeout setting |
| **Findings** | |

**Audit Item 16 – Citrix Logging not enabled**

| | |
|---|---|
| **Audit Category Reference** | **CSG003** |
| **Title** | Citrix Logging not enabled |
| **Reference** | WWW.support.citrix.com Best practices for securing a Citrix Secure Gateway Deployment page 6 Summary of Best Practices. |
| **Risk Area** | Audit Trail not possible if logging is not enabled. Auditing enhances accountability, without it administrators cannot detect or trace possible intrusion. |
| **Compliance** | Secure gateway event log enabled in Windows 2000 event viewer |
| **Test Method** | Commit a (non impacting) change to the configuration of the Nfuse server<br>Open and view change in Windows 2000 event viewer logs |
| **Test Type** | Objective |
| **Evidence** | Change should appear in Windows 2000 event viewer logs |
| **Findings** | |

### Audit Item 17 – Unlimited connections

| | |
|---|---|
| **Audit Category Reference** | **CSG004** |
| **Title** | Unlimited connections |
| **Reference** | http://www.securityfocus.com/archive/1/220885<br>ISS Security Advisory: Citrix Meta Frame Remote Denial of Service Vulnerability<br>Citrix Meta Frame Remote Denial of Service Vulnerability |
| **Risk Area** | Citrix service unavailable therefore remote access impossible. |
| **Compliance** | Latest Citrix hot fixes installed |
| **Test Method** | Initiate multiple fake sessions against target host ( gain approval from business )<br>Examine installed hot fixes against www.suport.citrix.com recommended hot fixes |
| **Test Type** | Objective |
| **Evidence** | Denial of Service Vulnerability should be prevented by installed hot fixes being up to date |
| **Findings** | |

### Audit Item 18 – ICA Protocol access not explicitly defined

| | |
|---|---|
| **Audit Category Reference** | **CMF001** |
| **Title** | ICA Protocol access not explicitly defined |
| **Reference** | Personal Work Experience where default installation allows everybody access. |
| **Risk Area** | Microsoft Windows 2000 Active directory authentication bypassed by use of default "everybody access" |
| **Compliance** | Specific ICA Protocol access granted to only Citrix users |
| **Test Method** | Attempt a connection to the ICA Metaframe server on TCP Port 1494 from other IP stack devices i.e. a Unix Server with out domain authentication running Netscape.<br>Observe if a connection can be established |
| **Test Type** | Objective |
| **Evidence** | Connection for non authenticated AD users should be denied |
| **Findings** | |

### Audit Item 19 – RDP Protocol access not explicitly defined

| | |
|---|---|
| **Audit Category Reference** | **CMF002** |
| **Title** | RDP Protocol access not explicitly defined |
| **Reference** | Personal Work Experience where default installation allows everybody access. |
| **Risk Area** | Microsoft Windows 2000 Active directory authentication bypassed by use of default "everybody access" |
| **Compliance** | Specific Remote Desktop Protocol access granted to only Citrix users as requiring a desktop. |
| **Test Method** | Attempt a connection to the RDP Metaframe server on TCP Port 3389 from other IP stack devices i.e. a Unix Server with out domain authentication running Netscape.<br>Observe if a connection can be established. |
| **Test Type** | Objective |
| **Evidence** | Connection for non authenticated AD users should be denied |
| **Findings** | |

### Audit Item 20 – Default install File permissions on Meta frame server

| | |
|---|---|
| **Audit Category Reference** | **CMF003** |
| **Title** | Default install File permissions on Meta frame server |
| **Reference** | Personal Experience |
| **Risk Area** | The ability to read, write and execute a files on the Metaframe Server remove the Confidentiality, integrity and availability of the remote access application |
| **Compliance** | Compliant behaviour should be no access to any file system area on the Meta Frame server publishing the application |
| **Test Method** | 1. Log into Citrix Metaframe server and Launch Internet Explorer.<br>2. From the View menu select View Folders.<br>3. From the folder tree view attempt to<br>4. Read file from Virtual drive on Meta Frame server<br>5. Write file from Virtual drive on Meta Frame server<br>6. Execute file from Virtual drive on Meta Frame server |
| **Test Type** | Objective |
| **Evidence** | Access to local File Systems should be denied |
| **Findings** | |

### Audit Item 21 – No Group Policies applied to Citrix Computer Accounts

| | |
|---|---|
| **Audit Category Reference** | **CMF004** |
| **Title** | No AD Group Policies applied to Specific Citrix Computer Accounts |
| **Reference** | Group Policy applied specifically to Citrix Computer Accounts is recommended best practice[13] with regards to a granular approach to applying mandatory Policy around key areas such as User Rights Assignments, Audit Policy and Security Options ( we will test the user right to logon locally) |
| **Risk Area** | Regular users may have permissions to logon on to Metaframe Server desktop. |
| **Compliance** | Group Policy applied limiting logon local permissions |
| **Test Method** | Test logon to Metaframe Server console with a test account that is not granted Citrix ICA session access |
| **Test Type** | Objective |
| **Evidence** | The user should not be able to logon locally to the Metaframe console |
| **Findings** | |

### Audit Item 22 – No Administrative Templates applied to Specific Citrix Users

| | |
|---|---|
| **Audit Category Reference** | **CMF005** |
| **Title** | No Administrative Templates applied to Specific Citrix Users |
| **Reference** | |
| **Risk Area** | Additional options and menus may be open to change settings or run commands that may be used to bypass security controls. |
| **Compliance** | Application access to Internet Options Configuration Parameters is restricted |
| **Test Method** | Login to Citrix and Launch the Application in question Internet Explorer.<br>After Default home page loads attempt to enter the Internet Options area to change parameters |
| **Test Type** | Objective |
| **Evidence** | The ability to alter Internet Options and change parameters should be denied. |
| **Findings** | |

### Audit Item 23 – Latest Citrix Service Packs not installed

| | |
|---|---|
| **Audit Category Reference** | **CMF006** |
| **Title** | Latest Citrix Service Packs not installed |
| **Reference** | [14] Citrix has identified several Denial of Service (DoS) vulnerabilities on Citrix Metaframe servers. These vulnerabilities occur during the ICA protocol initialization phase prior to any authentication or establishment of encryption |
| **Risk Area** | (Dos) as above |
| **Compliance** | All Service Packs & Latest hot fixes as relevant for our Citrix Metaframe XP 1.0 installation on windows 2000 Server as current at time of writing report from http://support.citrix.com/hotfixes<br>For details please see Appendix 2 |
| **Test Method** | 1. Logon to Citrix management Console, select the Metaframe Server properties and Identify Current Citrix Version<br>2. Obtain current list of Service packs and hot fixes from Citrix support to ascertain the definitive compliance list.<br>3. Logon to Citrix management Console, select the Metaframe Server properties and Identify current installed hot fixes<br>4. Compare against definitive Citrix List verses installed hot fixes on Metaframe Server |
| **Test Type** | Objective |
| **Evidence** | All Service Packs & Latest hot fixes should be installed |
| **Findings** | |

### Audit Item 24 – Auditing Policy not defined

| | |
|---|---|
| **Audit Category Reference** | **CMF007** |
| **Title** | Auditing Policy not defined |
| **Reference** | Audit Policy should be defined in an Acitive Directory Group Policy, As recommended in the [15]SANS Securing Windows 2000 Step by Step ( see settings in Appendix 5 ) |
| **Risk Area** | Accountability can not be determined and an audit trail in the event of an attack or compromise |
| **Compliance** | Auditing enabled |
| **Test Method** | Test logon successfully and unsuccessfully and examine log entries in the Windows 2000 Event Viewer Security Log<br>Complete the same test for all items as listed in Appendix 5 and examine log entries in the Windows 2000 Event Viewer Security Log |

| | |
|---|---|
| **Test Type** | Objective |
| **Evidence** | Even it audited in Windows Event viewer Security Logs |
| **Findings** | |

**Audit Item 25 – Latest Citrix Feature Pack not installed**

| | |
|---|---|
| **Audit Category Reference** | **CPA001** |
| **Title** | Latest Citrix Feature Pack not installed |
| **Reference** | Citrix has identified several Denial of Service (DoS) vulnerabilities on Citrix Metaframe servers. These vulnerabilities occur during the ICA protocol initialization phase prior to any authentication or establishment of encryption |
| **Risk Area** | (DoS) as above |
| **Compliance** | Feature pack 3 is the current Feature pack for Meta Frame XPe |
| **Test Method** | 1. Logon to Citrix management Console, select the Metaframe Server properties and Identify Current Citrix Feature Pack and Metaframe OS Version<br>2. Obtain current list of Feature Packs from Citrix support to ascertain the definitive compliance list. |
| **Test Type** | Objective |
| **Evidence** | Feature pack 3 installed on Meta Frame Server |
| **Findings** | |

**Audit Item 26 – Applications not published on a per group basis**

| | |
|---|---|
| **Audit Category Reference** | **CPA002** |
| **Title** | Applications not published on a per group basis |
| **Reference** | Citrix Metaframe Advanced Technical Design Guide , Chapter 15 Security Page 638 |
| **Risk Area** | Additional Access to applications |
| **Compliance** | Access only to the nominated application associated with the Active Directory Group assigned in Citrix Management Console Security Permissions |
| **Test Method** | Logon to the Citrix Nfuse Server with testing account given.<br>Check available applications ( if any ) against testing account, CMC Management Console permissions for published Internet Explorer application |
| **Test Type** | Objective |
| **Evidence** | The compliant result expected would be after logging on to only have access to the one application Internet Explorer as requested with the test account provided |
| **Findings** | |

### Audit Item 27 – Group Domain User Password Policy not defined

| **Audit Category Reference** | **ADUSR001** |
|---|---|
| **Title** | Group Domain User Password Policy not defined |
| **Reference** | Microsoft Prescriptive Guidance, Security Operations Guide for Windows 2000 Server recommends Group Policy enforced User Account Policy non discretionary password settings |
| **Risk Area** | Strong password policies are a best practice of a "Defence in Depth Model" [16] |
| **Compliance** | Password Policy set on ( as recommended by [17]Microsoft )<br>• Enforce password history<br>• Maximum password age<br>• Minimum password age<br>• Minimum password length<br>• Passwords must meet complexity requirements<br>• Store passwords using reversible encryption |
| **Test Method** | Change test account password to test compliance conditions ( as above ) including a blank password, weak password, re use password etc |
| **Test Type** | Objective |
| **Evidence** | Password Policy set in relation to Compliance criteria should prevent, weak or blank passwords, reusing password etc. |
| **Findings** | |

### Audit Item 28 – Group Domain Account Lockout Policy not defined

| **Audit Category Reference** | **ADUSR002** |
|---|---|
| **Title** | Group Domain Account Lockout Policy not defined |
| **Reference** | Microsoft Prescriptive Guidance, Security Operations Guide for Windows 2000 Server recommends Group Policy enforced Lockout Policy |
| **Risk Area** | Subject to Brute Force attack |
| **Compliance** | Account is locked out for 30 minutes after 3 failed attempts of logon |
| **Test Method** | Attempt logon using the test account supplied to WWW Nfuse Server with an incorrect password in a repeated fashion until account is locked out |
| **Test Type** | Objective |
| **Evidence** | The logon page on the WWW Citrix Nfuse server should display the account is locked out after 3 attempts. The Windows 2000 server security log and AD Users and Computers MMC should also display the account as locked out with the check box in the "Account Tab "being checked. |
| **Findings** | |

## III. CONDUCTING THE AUDIT TESTING, EVIDENCE AND FINDINGS

### 5. Technical Audit – Basic Risk Analysis

### 5.1 Pre Audit Notes

Audit was performed by under the following conditions

The auditor was invited to colleagues Data Center on a specific date and time
The colleague gave explicit written (email) permission for the audit.
The auditor arrived to find an access card entry door preventing direct entry to office area. A phone provided allowed the auditor to call for the colleague, however they were unavailable and another staff member showed the auditor into to a waiting room, where there where no data access points. The colleague arrived shortly after where the auditor commenced this report. The auditor asked for a specific testing account for access to the Citrix Nfuse server that had no additional privileges on the Active Directory Windows 2000 domain and specific access to only the Internet Explorer Published application available on the Internet via Citrix Nfuse.
The auditor asked permission to use [18]LC3 password tool to illustrate flaws in Windows password policies in particular, Brute Force against a non lockout policy, however permission was explicitly denied for this test.

The audit took 9.5 hours to complete.

The auditor used a Windows XP laptop, a Knoppix Laptop and tools as listed in the Appendix 1

This audit report picked fourteen items from the different zones from the audit checklist in section two in an attempt to examine a broad range across the various zones the audit is broken down into; the results have been made anonymous to protect the colleague who was kind enough to allow the testing for this practical.

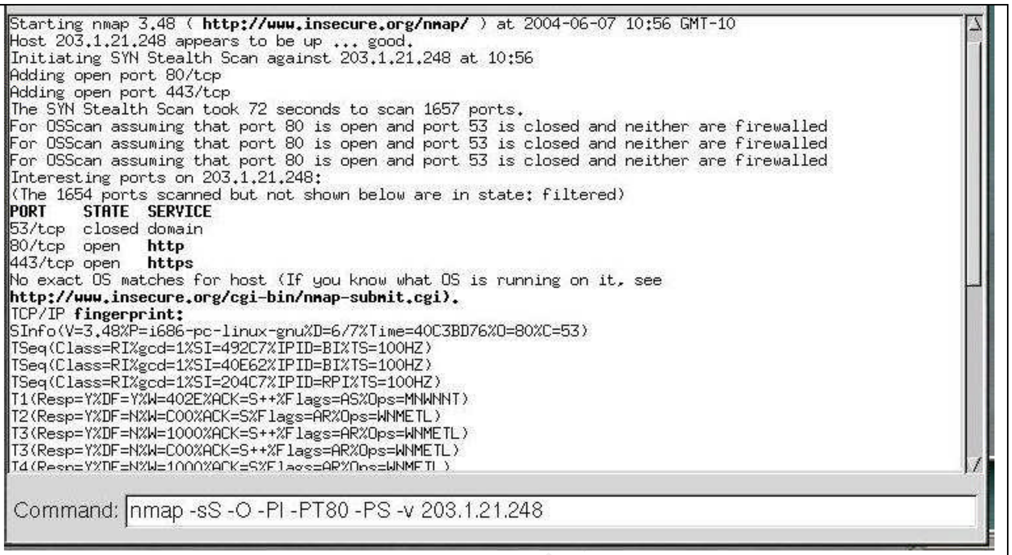
### 5.2 Completed Audit

#### Audit Item 2 – Physical Access

| | |
|---|---|
| **Audit Category Reference** | **PHY002** |
| **Title** | Physical Access |
| **Test Objective** | Attempt Physical Access to Data Center Citrix Servers |
| **Compliance** | Secured Access Points, alarms and video monitoring |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Organise a visit to the Data Center housing Citrix Servers.<br>2. Attempt unauthorised physical access to building, network and Server console<br>3. Check Physical Controls |
| **Actual Outcome** | Subjective |
| **Assessment** | Auditor noted the following physical controls preventing access<br>Central Security Station requiring a sign in for external visitors<br>1. Logged Key Pass Access Level1 to IT Department.<br>2. Logged Key Pass Access Level2 to Data Center,<br>3. Locked Server room racks<br>4. Video surveillance<br>5. sign in for external visitors to Data Center Server Room |
| **PASS / FAIL** | PASS |

#### Audit Item 3 – Incorrect External Firewall Rules

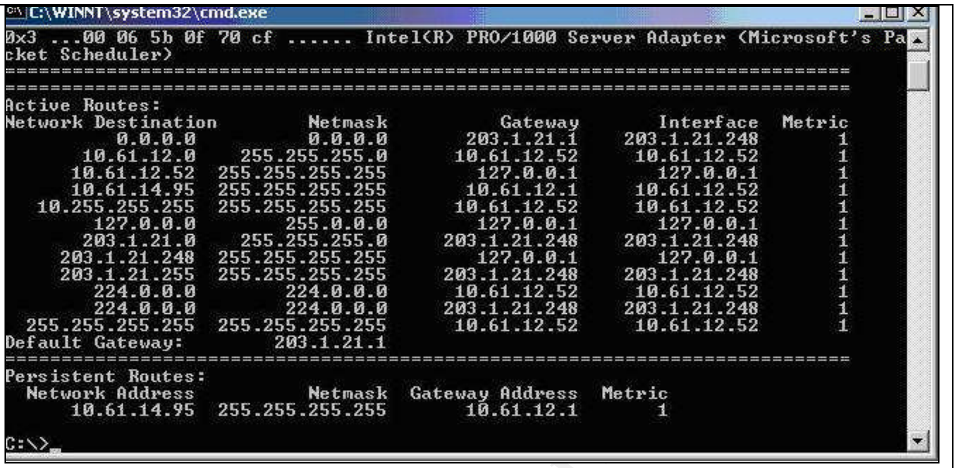
| | |
|---|---|
| **Audit Category Reference** | **NET001** |
| **Title** | Incorrect External Firewall Rules |
| **Test Objective** | Test for Firewall Rule strength. |
| **Compliance** | [19]All traffic not explicitly required by Citrix Nfuse WWW server dropped |
| **Stimulus Response** | Yes |
| **Test Method** | [20]Nmap Port scan internet Citrix IP addresses.<br>Nmap –sS –O –PI-P80 –PS –v <FUSE Server- PUBLIC Address><br>Examine results<br>Check results of Nmap by executing a telnet to any open ports listed by Nmap<br>[21]Nmap Scanning notes for “Firewalled” hosts describe the use Nmap for scanning for filtered ports ( ports with No SYN/ACK, No RST/ACK or ICMP type 3 messages destination unreachable –RFC 1812 ) |
| **Actual Outcome** | |

| | |
|---|---|
| |  |
| **Assessment** | The Nmap scan revealed an additional web listener on port 80 which is not required therefore resulting in a Fail status<br>Citrix Nfuse only requires SSL Port 443 for external access. |
| **PASS / FAIL** | FAIL |

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-06-07 10:56 GMT-10
Host 203.1.21.248 appears to be up ... good.
Initiating SYN Stealth Scan against 203.1.21.248 at 10:56
Adding open port 80/tcp
Adding open port 443/tcp
The SYN Stealth Scan took 72 seconds to scan 1657 ports.
For OSScan assuming that port 80 is open and port 53 is closed and neither are firewalled
For OSScan assuming that port 80 is open and port 53 is closed and neither are firewalled
For OSScan assuming that port 80 is open and port 53 is closed and neither are firewalled
Interesting ports on 203.1.21.248:
(The 1654 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE
53/tcp   closed domain
80/tcp   open   http
443/tcp  open   https
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.48%P=i686-pc-linux-gnu%D=6/7%Time=40C3BD76%O=80%C=53)
TSeq(Class=RI%gcd=1%SI=492C7%IPID=BI%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=40E62%IPID=BI%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=204C7%IPID=RPI%TS=100HZ)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=C00%ACK=S%Flags=AR%Ops=WNMETL)
T3(Resp=Y%DF=N%W=1000%ACK=S++%Flags=AR%Ops=WNMETL)
T3(Resp=Y%DF=N%W=C00%ACK=S++%Flags=AR%Ops=WNMETL)
T4(Resp=Y%DF=N%W=1000%ACK=S%Flags=AR%Ops=WNMETL)

Command: nmap -sS -O -PI -PT80 -PS -v 203.1.21.248
```

### Audit Item 5 – Default or additional Routes to internal network

| | |
|---|---|
| **Audit Category Reference** | **NET003** |
| **Title** | Default or additional Routes to internal network |
| **Test Objective** | Test the logical internal network range available through networking configuration |
| **Compliance** | Specific 32bit subnet mask host routes as required |
| **Stimulus Response** | Yes |
| **Test Method** | Netstat – rn to display route tables.<br>Ping, telnet and Map Network drive tests to a known critical internal host. |
| **Actual Outcome** | |



```
C:\WINNT\system32\cmd.exe
0x3 ...00 06 5b 0f 70 cf ...... Intel(R) PRO/1000 Server Adapter (Microsoft's Pa
cket Scheduler)
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      203.1.21.1    203.1.21.248       1
       10.61.12.0    255.255.255.0     10.61.12.52     10.61.12.52       1
      10.61.12.52  255.255.255.255       127.0.0.1       127.0.0.1       1
      10.61.14.95  255.255.255.255      10.61.12.1     10.61.12.52       1
   10.255.255.255  255.255.255.255     10.61.12.52     10.61.12.52       1
        127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1       1
       203.1.21.0    255.255.255.0    203.1.21.248    203.1.21.248       1
     203.1.21.248  255.255.255.255       127.0.0.1       127.0.0.1       1
     203.1.21.255  255.255.255.255    203.1.21.248    203.1.21.248       1
        224.0.0.0        224.0.0.0     10.61.12.52     10.61.12.52       1
        224.0.0.0        224.0.0.0    203.1.21.248    203.1.21.248       1
  255.255.255.255  255.255.255.255     10.61.12.52     10.61.12.52       1
Default Gateway:        203.1.21.1
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
      10.61.14.95  255.255.255.255       10.61.12.1       1

C:\>
```

A Telnet and Ping to a nominated interna host failed with a timeout

C:\telnet <nominated-internal-host>
Connecting To <nominated-internal-host>...Could not open connection to the host, on port 23: Connect failed

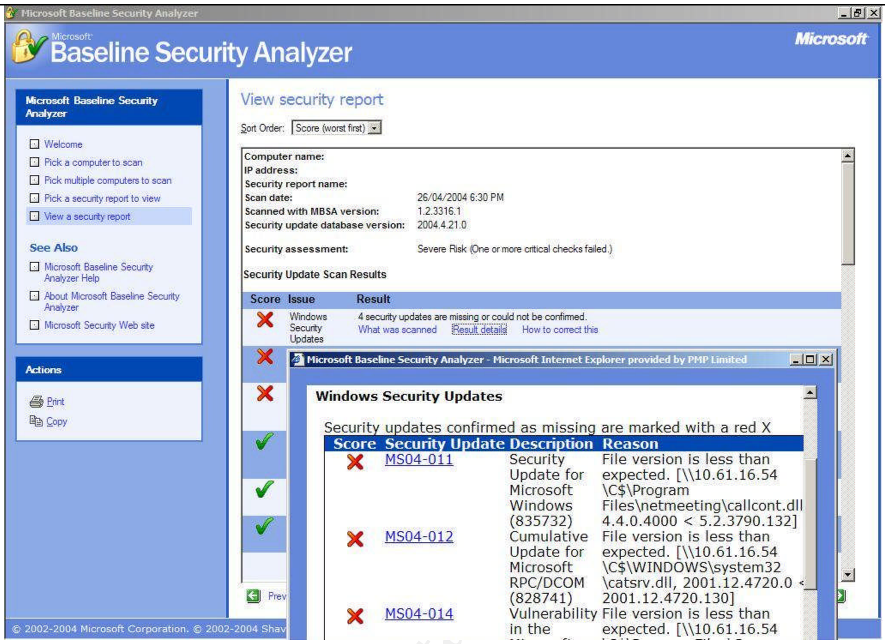
C:\ping <nominated-internal-host>
Pinging <nominated-internal-host> with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

| | |
|---|---|
| **Assessment** | The internal networking configuration of the Citrix NFUSE server allowed for logical network routing specifically to the internal Metaframe server and no other internal network |
| **PASS / FAIL** | PASS |

**Audit Item 6 – Service Packs and Critical Updates not installed or up to date**

| | |
|---|---|
| **Audit Category Reference** | **OS001** |
| **Title** | Service Packs and Critical Updates not installed and up to date |
| **Test Objective** | Ascertain Service Packs and Critical Updates are current as per [22] www.windowsupdate.com |
| **Compliance** | Service Packs and Critical Updates up to date as per MS Baseline Security analyser report |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Run MS baseline security analyser<br>2. Download latest secure XML<br>3. View analyse and compare output |
| **Actual Outcome** | Ms Baseline Output |

| | |
|---|---|
| | <br>Microsoft Baseline Security Analyzer<br>Computer name:<br>IP address:<br>Security report name:<br>Scan date: 26/04/2004 6:30 PM<br>Scanned with MBSA version: 1.2.3316.1<br>Security update database version: 2004.4.21.0<br>Security assessment: Severe Risk (One or more critical checks failed.)<br>Security Update Scan Results<br>Score Issue Result<br>✗ Windows Security Updates 4 security updates are missing or could not be confirmed.<br>Windows Security Updates<br>Security updates confirmed as missing are marked with a red X<br>Score Security Update Description Reason<br>✗ MS04-011 Security Update for Microsoft Windows (835732) File version is less than expected. [\\10.61.16.54\C$\Program Files\netmeeting\callcont.dll 4.4.0.4000 < 5.2.3790.132]<br>✗ MS04-012 Cumulative Update for Microsoft RPC/DCOM (828741) File version is less than expected. [\\10.61.16.54\C$\WINDOWS\system32\catsrv.dll, 2001.12.4720.0 < 2001.12.4720.130]<br>✗ MS04-014 Vulnerability in the File version is less than expected. [\\10.61.16.54 |
| **Assessment** | MS baseline security analyser report revealed 4 security updates missing or could not be confirmed resulting in a fail status<br>Please note this was also compared against the Hfnetchk tool from Microsoft |
| **PASS / FAIL** | FAIL |

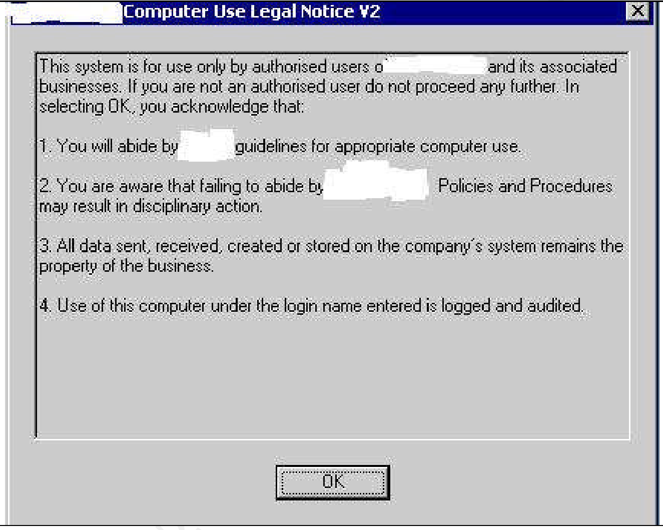
### Audit Item 7 – Unwanted Services are not running and disabled

| | |
|---|---|
| **Audit Category Reference** | **OS002** |
| **Title** | Unwanted Services are not running and disabled |
| **Test Objective** | Testing that unnecessary services removed, |
| **Compliance** | Unnecessary services removed. |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Run Foundstone's fport (FPort v2.0 - TCP/IP Process to Port Mapper Copyright 2000 by Foundstone, Inc. http://www.foundstone.com) |

| | |
|---|---|
| | 2. Execute net start command<br>3. Examine outputs for running services and compare against disabled services in MS Services MMC Console |
| **Actual Outcome** | The auditor was permitted to logon to the console of the Nfuse server and using a DOS prompt executed the net start command<br><br>Output:<br>These Windows 2000 services are started:<br><br>   Ati HotKey Poller<br>   Automatic Updates<br>   CIO Array Management Service 4.01<br>   CIO Event Notifier<br>   CIOArrayManager RPC Command<br>   CIOArrayManager RPC Event<br>   COM+ Event System<br>   DefWatch<br>   Dell OpenManage Server Agent<br>   Dell OpenManage Server Agent Event Monitor<br>   DHCP Client<br>   Disk Management Service<br>   Distributed Transaction Coordinator<br>   DNS Client<br>   Event Log<br>   IIS Admin Service<br>   mr2kserv<br>   Network Connections<br>   NobleNet Portmapper<br>   Plug and Play<br>   Protected Storage<br>   Remote Access Auto Connection Manager<br>   Remote Access Connection Manager<br>   Remote Procedure Call (RPC)<br>   Remote Registry Service<br>   Secure Gateway Service<br>   Security Accounts Manager<br>   Server Administrator<br>   SNMP Service<br>   Symantec AntiVirus Client<br>   System Event Notification<br>   Telephony<br>   Windows Management Instrumentation<br>   Windows Management Instrumentation Driver Extensions<br>   World Wide Web Publishing Service<br><br>The command completed successfully.<br><br>FPort v2.0 - TCP/IP Process to Port Mapper<br>Copyright 2000 by Foundstone, Inc. |

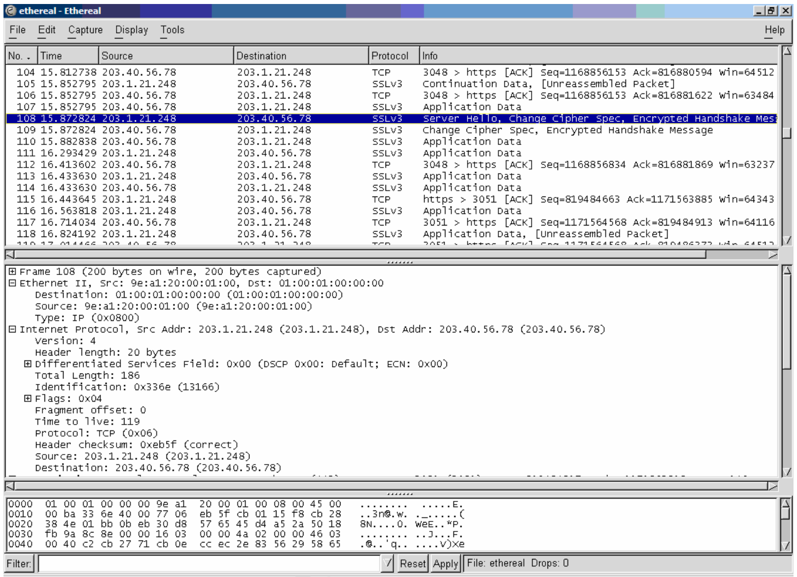
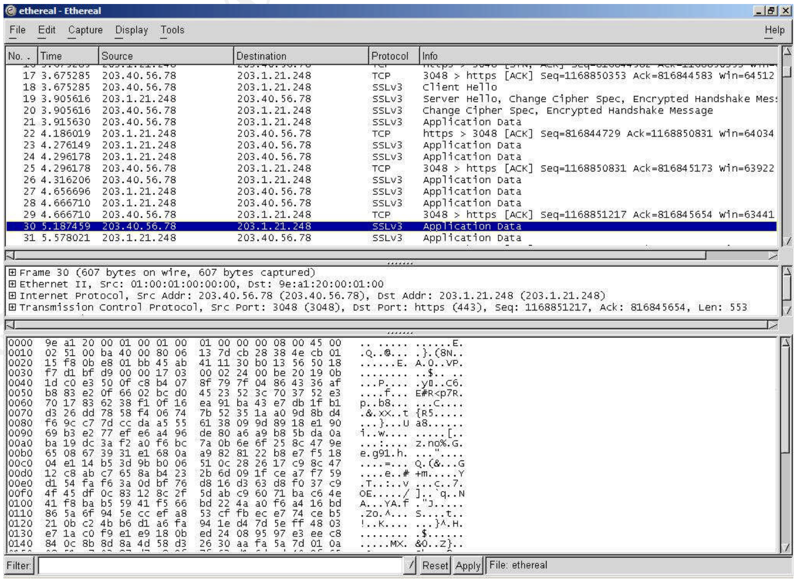
| | |
|---|---|
| | http://www.foundstone.com<br><br>Pid   Process            Port  Proto Path<br>1040  inetinfo       ->  80    TCP   C:\WINNT\system32\inetsrv\inetinfo.exe<br>744   PORTSERV       ->  111   TCP   C:\Program Files\Dell\OpenManage\ihv\CIO\PORTSERV.EXE<br>448   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe<br>8     System         ->  139   TCP<br>600   CtxSecGwy      ->  443   TCP   C:\WINNT\system32\CtxSecGwy.exe<br>1040  inetinfo       ->  444   TCP   C:\WINNT\system32\inetsrv\inetinfo.exe<br>8     System         ->  445   TCP<br>476   msdtc          ->  1025  TCP   C:\WINNT\System32\msdtc.exe<br>964   IOMRPCCM       ->  1027  TCP   C:\Program Files\Dell\OpenManage\ihv\CIO\IOMRPCCM.EXE<br>8     System         ->  1029  TCP<br>1040  inetinfo       ->  1030  TCP   C:\WINNT\system32\inetsrv\inetinfo.exe<br>804   omaws32        ->  1032  TCP   C:\Program Files\Dell\OpenManage\iws\bin\win32\omaws32.exe<br>1596  diagorb        ->  1033  TCP   C:\PROGRA~1\Dell\OPENMA~1\oldiags\vendor\pcdoctor\bin\diagorb.exe<br>1596  diagorb        ->  1034  TCP   C:\PROGRA~1\Dell\OPENMA~1\oldiags\vendor\pcdoctor\bin\diagorb.exe<br>1596  diagorb        ->  1035  TCP   C:\PROGRA~1\Dell\OPENMA~1\oldiags\vendor\pcdoctor\bin\diagorb.exe<br>804   omaws32        ->  1036  TCP   C:\Program Files\Dell\OpenManage\iws\bin\win32\omaws32.exe<br>600   CtxSecGwy      ->  1087  TCP   C:\WINNT\system32\CtxSecGwy.exe<br>804   omaws32        ->  1311  TCP   C:\Program Files\Dell\OpenManage\iws\bin\win32\omaws32.exe<br>476   msdtc          ->  3372  TCP   C:\WINNT\System32\msdtc.exe<br>804   omaws32        ->  8000  TCP   C:\Program Files\Dell\OpenManage\iws\bin\win32\omaws32.exe<br>600   CtxSecGwy      ->  14940 TCP   C:\WINNT\system32\CtxSecGwy.exe<br><br>744   PORTSERV       ->  111   UDP   C:\Program Files\Dell\OpenManage\ihv\CIO\PORTSERV.EXE<br>8     System         ->  137   UDP<br>8     System         ->  138   UDP<br>816   snmp           ->  161   UDP   C:\WINNT\System32\snmp.exe<br>8     System         ->  445   UDP<br>860   VxSvc          ->  2148  UDP   C:\Program Files\Dell\OpenManage\Array Manager\VxSvc.exe<br>1040  inetinfo       ->  3456  UDP   C:\WINNT\system32\inetsrv\inetinfo.exe |
| **Assessment** | Most unnecessary services were not running however [23]SNMP, Dell Open Manger and the IIS Admin service which have known vulnerabilities[24] such as unauthorized privileged access" and "denial-of-service attacks" , were actively running and not disabled, resulting in a fail status |
| **PASS / FAIL** | FAIL |

### Audit Item 8 – Warning Legal banner not used

| | |
|---|---|
| **Audit Category Reference** | **OS003** |
| **Title** | Warning Legal banner not used |
| **Test Objective** | Test a legal banner is displayed upon logon |
| **Compliance** | Legal Banner displayed upon logon stating restricted system usage and criminal prosecution for unauthorised offenders |
| **Stimulus Response** | Yes |
| **Test Method** | Performed a standard logon to Nfuse Server |
| **Actual Outcome** | <br>[redacted] Computer Use Legal Notice V2<br>This system is for use only by authorised users o[redacted] and its associated businesses. If you are not an authorised user do not proceed any further. In selecting OK, you acknowledge that:<br>1. You will abide by [redacted] guidelines for appropriate computer use.<br>2. You are aware that failing to abide by [redacted] Policies and Procedures may result in disciplinary action.<br>3. All data sent, received, created or stored on the company's system remains the property of the business.<br>4. Use of this computer under the login name entered is logged and audited.<br> |
| **Test Type** | Objective |
| **Assessment** | The auditor performed a standard logon to Nfuse Server and a Legal Banner was displayed upon logon. Please note the content of this banner also proved appropriate, when run by an associate lawyer. |
| **PASS / FAIL** | PASS |

### Audit Item 10 – Non encrypted Web service

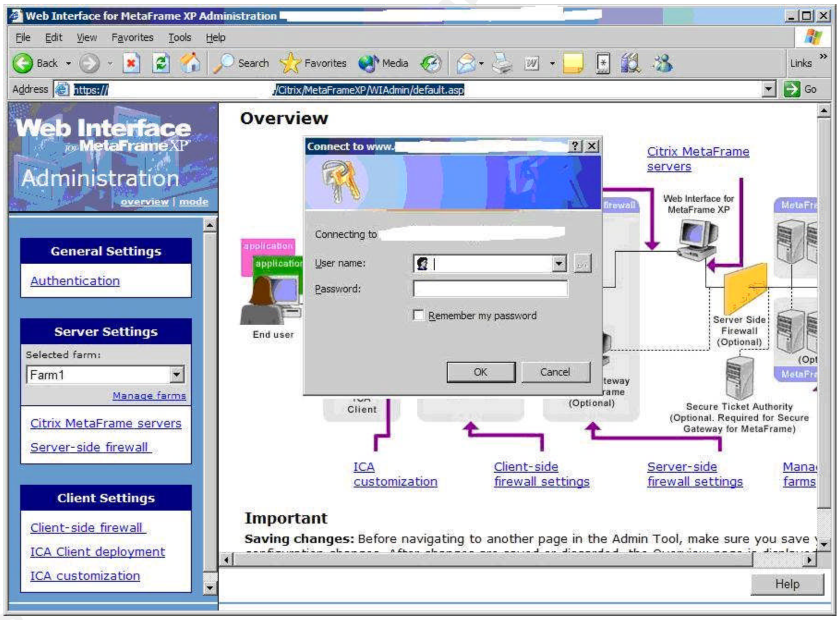
| | |
|---|---|
| **Audit Category Reference** | **CNF001** |
| **Title** | Non encrypted Web service |
| **Test Objective** | Non encrypted traffic can be captured with packet sniffing programs and passwords will be exposed in clear text. |
| **Compliance** | Encrypted NFUSE WWW server connection, 128bit Digital CA certificate installed, and requiring 128bit encryption for connection. |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Connect Auditors machine to Network device on subnet of Citrix |

|  |  |
|---|---|
|  | Nfuse server and set NIC to promiscuous mode.<br>2. Capture Traffic with Ethereal Packet Capture tool<br>3. Analyse pack capture for usernames and password in clear text |
| **Actual Outcome** | Ethereal shows initial traffic between client and NFUSE Server and client browser is https SSLv3<br><br>Encrypted data payload<br> |
| **Assessment** | Packet capture data payload should not contain any usernames or password if encrypted data should be unreadable |
| **PASS / FAIL** | PASS |

```
No. .  Time       Source          Destination     Protocol  Info
  104 15.812738 203.40.56.78    203.1.21.248    TCP     3048 > https [ACK] Seq=1168856153 Ack=816880594 Win=64512
  105 15.852795 203.1.21.248    203.40.56.78    SSLv3   Continuation Data, [Unreassembled Packet]
  106 15.852795 203.40.56.78    203.1.21.248    TCP     3048 > https [ACK] Seq=1168856153 Ack=816881622 Win=63484
  107 15.852795 203.40.56.78    203.1.21.248    SSLv3   Application Data
  108 15.872824 203.1.21.248    203.40.56.78    SSLv3   Server Hello, Change Cipher Spec, Encrypted Handshake Mes
  109 15.872824 203.40.56.78    203.1.21.248    SSLv3   Change Cipher Spec, Encrypted Handshake Message
  110 15.882838 203.40.56.78    203.1.21.248    SSLv3   Application Data
  111 16.293429 203.1.21.248    203.40.56.78    SSLv3   Application Data
  112 16.413602 203.40.56.78    203.1.21.248    TCP     3048 > https [ACK] Seq=1168856834 Ack=816881869 Win=63237
  113 16.433630 203.1.21.248    203.40.56.78    SSLv3   Application Data
  114 16.433630 203.40.56.78    203.1.21.248    SSLv3   Application Data
  115 16.443645 203.1.21.248    203.40.56.78    TCP     https > 3051 [ACK] Seq=819484663 Ack=1171563885 Win=64343
  116 16.563818 203.1.21.248    203.40.56.78    SSLv3   Application Data
  117 16.714034 203.40.56.78    203.1.21.248    TCP     3051 > https [ACK] Seq=1171564568 Ack=819484913 Win=64116
  118 16.824192 203.1.21.248    203.40.56.78    SSLv3   Application Data, [Unreassembled Packet]

⊞ Frame 108 (200 bytes on wire, 200 bytes captured)
⊟ Ethernet II, Src: 9e:a1:20:00:01:00, Dst: 01:00:01:00:00:00
    Destination: 01:00:01:00:00:00 (01:00:01:00:00:00)
    Source: 9e:a1:20:00:01:00 (9e:a1:20:00:01:00)
    Type: IP (0x0800)
⊟ Internet Protocol, Src Addr: 203.1.21.248 (203.1.21.248), Dst Addr: 203.40.56.78 (203.40.56.78)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 186
    Identification: 0x336e (13166)
  ⊞ Flags: 0x04
    Fragment offset: 0
    Time to live: 119
    Protocol: TCP (0x06)
    Header checksum: 0xeb5f (correct)
    Source: 203.1.21.248 (203.1.21.248)
    Destination: 203.40.56.78 (203.40.56.78)

0000  01 00 01 00 00 00 9e a1  20 00 01 00 08 00 45 00   ........ .....E.
0010  00 ba 33 6e 40 00 77 06  eb 5f cb 01 15 f8 cb 28   ..3n@.w. ._.....(
0020  38 4e 01 bb 0b eb 30 d8  57 65 45 d4 a5 2a 50 18   8N....0. WeE..*P.
0030  fb 9a 8c 8e 00 00 16 03  00 00 4a 02 00 00 46 03   ........ ..J...F.
0040  00 40 c2 cb 27 71 cb 0e  cc ec 2e 83 56 29 58 65   .@..'q.. ....V)Xe
```

```
No. .  Time       Source          Destination     Protocol  Info
   17 3.675285  203.40.56.78    203.1.21.248    TCP     3048 > https [ACK] Seq=1168850353 Ack=816844583 Win=64512
   18 3.675285  203.40.56.78    203.1.21.248    SSLv3   Client Hello
   19 3.905616  203.1.21.248    203.40.56.78    SSLv3   Server Hello, Change Cipher Spec, Encrypted Handshake Mes:
   20 3.905616  203.40.56.78    203.1.21.248    SSLv3   Change Cipher Spec, Encrypted Handshake Message
   21 3.915630  203.40.56.78    203.1.21.248    SSLv3   Application Data
   22 4.186019  203.1.21.248    203.40.56.78    TCP     https > 3048 [ACK] Seq=816844729 Ack=1168850831 Win=64034
   23 4.276149  203.1.21.248    203.40.56.78    SSLv3   Application Data
   24 4.296178  203.1.21.248    203.40.56.78    SSLv3   Application Data
   25 4.296178  203.40.56.78    203.1.21.248    TCP     3048 > https [ACK] Seq=1168850831 Ack=816845173 Win=63922
   26 4.316206  203.40.56.78    203.1.21.248    SSLv3   Application Data
   27 4.656696  203.1.21.248    203.40.56.78    SSLv3   Application Data
   28 4.666710  203.1.21.248    203.40.56.78    SSLv3   Application Data
   29 4.666710  203.40.56.78    203.1.21.248    TCP     3048 > https [ACK] Seq=1168851217 Ack=816845654 Win=63441
   30 5.187459  203.40.56.78    203.1.21.248    SSLv3   Application Data
   31 5.578021  203.1.21.248    203.40.56.78    SSLv3   Application Data

⊞ Frame 30 (607 bytes on wire, 607 bytes captured)
⊞ Ethernet II, Src: 01:00:01:00:00:00, Dst: 9e:a1:20:00:01:00
⊞ Internet Protocol, Src Addr: 203.40.56.78 (203.40.56.78), Dst Addr: 203.1.21.248 (203.1.21.248)
⊞ Transmission Control Protocol, Src Port: 3048 (3048), Dst Port: https (443), Seq: 1168851217, Ack: 816845654, Len: 553

0000  9e a1 20 00 01 00 01 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  02 51 00 ba 40 00 80 06  13 7d cb 28 38 4e cb 01   .Q..@... .}.(8N..
0020  15 f8 0b e8 01 bb 45 ab  41 11 30 b0 13 56 50 18   ......E. A.0..VP.
0030  f7 d1 bf d9 00 00 17 03  00 02 24 00 be 20 19 0b   ........ ..$.. ..
0040  1d c0 e3 50 0f c8 b4 07  8f 79 7f 04 86 43 36 af   ...P.... .y▯..C6.
0050  b8 83 e2 0f 66 02 bc d0  45 23 52 3c 70 37 52 e3   ....f... E#R<p7R.
0060  70 17 83 62 38 f1 0f 16  ea 91 ba 43 e7 db 1f b1   p..b8... ...C....
0070  d3 26 dd 78 58 f4 06 74  7b 52 35 1a a0 9d 8b d4   .&.xX..t {R5.....
0080  f6 9c c7 7d cc da a5 55  61 38 09 9d 89 18 e1 90   ...}...U a8......
0090  69 b3 e2 77 ef e6 a4 96  de 80 a6 a9 b8 5b da 0a   i..w.... .....[..
00a0  ba 19 dc 3a f2 a0 f6 bc  7a 0b 6e 6f 25 8c 47 9e   ...:.... z.no%.G.
00b0  65 08 67 39 31 e1 68 0a  a9 82 81 22 b8 e7 f5 18   e.g91.h. ..."....
00c0  04 e1 14 b5 3d 9b b0 06  51 0c 28 26 17 c9 8c 47   ....=... Q.(&...G
00d0  12 c8 ab c7 65 8a b4 23  2b 6d 09 1f ce a7 f7 59   ....e..# +m.....Y
00e0  d1 54 fa f6 3a 0d bf 76  d8 16 d3 63 d8 f0 37 c9   .T..:..v ...c..7.
00f0  4f 45 df 0c 83 12 8c 2f  5d ab c9 60 71 ba c6 4e   OE...../ ]..`q..N
0100  41 f8 ba b5 59 41 f5 66  bd 22 4a a0 f6 a4 16 bd   A...YA.f ."J.....
0110  86 5a 6f 94 5e cc ef a8  53 cf fb ec e7 74 ce b5   .Zo.^... S....t..
0120  21 0b c2 4b b6 d1 a6 fa  94 1e d4 7d 5e ff 48 03   !..K.... ...}^.H.
0130  e7 1a c0 f9 e1 e9 18 0b  ed 24 08 95 97 e3 ee c8   ........ .$......
0140  84 0c 8b 8d 8a 4d 58 d3  26 30 aa fa 5a 7d 01 0a   .....MX. &0..Z}..
```

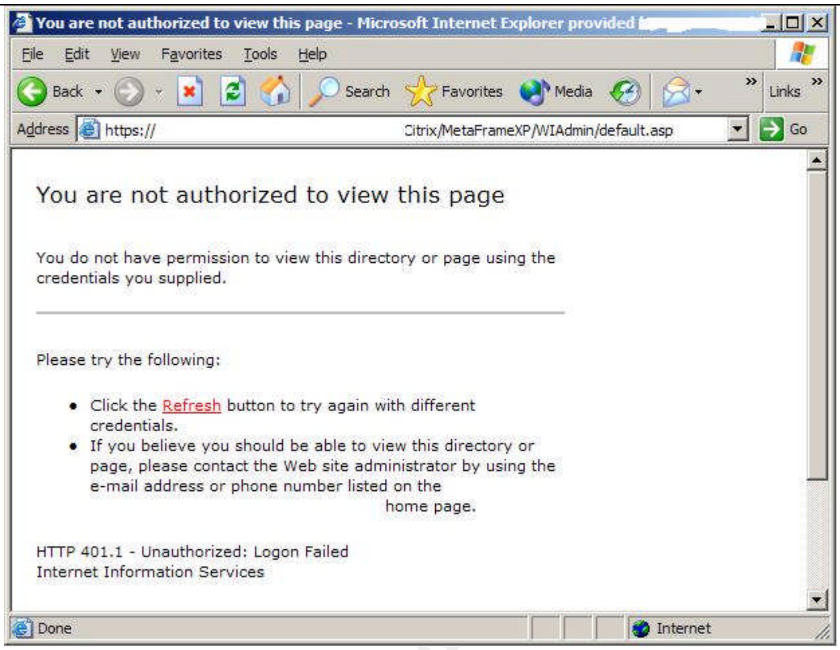
### Audit Item 13 – Access to Nfuse Administration on Website

| **Audit Category Reference** | **CNF004** |
|---|---|
| **Title** | Access to Nfuse Administration on Website |
| **Reference** | Personal work experience has seen administration web interface access https://companyhost/Citrix/MetaFrameXP/WIAdmin/default.asp via bypassing administrator access or passwords. |
| **Risk Area** | Web Access to Nfuse administration and configuration website not secured. |
| **Compliance** | Explicit access to administrators only |
| **Test Method** | Attempt to logon to the Administration Web console with the test account used for the audit. |
| **Actual Outcome** |  |

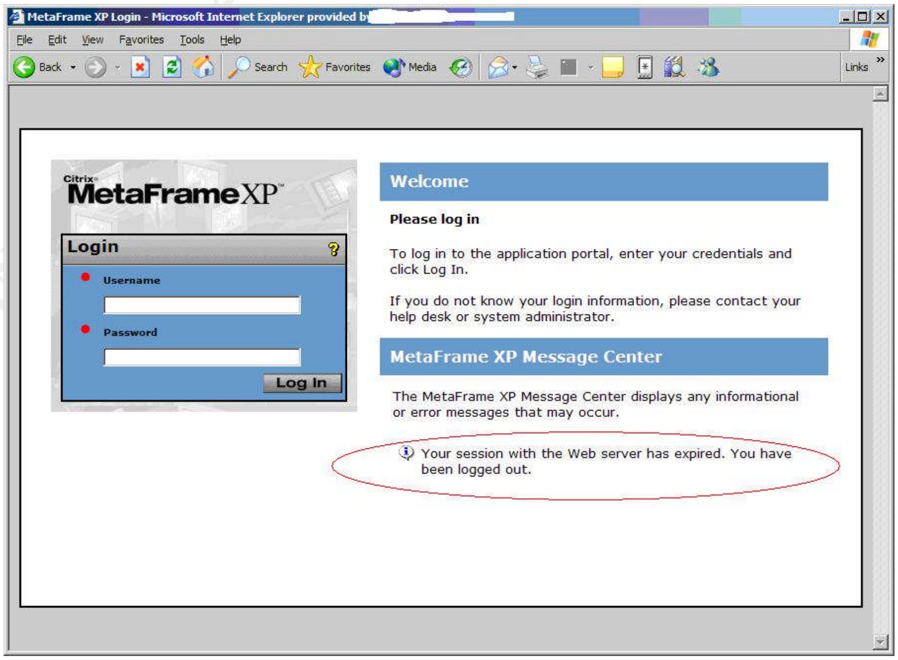
Web Interface for MetaFrame XP Administration
File Edit View Favorites Tools Help
Back Search Favorites Media Links Go
Address https:// /Citrix/MetaFrameXP/WIAdmin/default.asp
Web Interface for MetaFrame XP
Administration
overview | mode
General Settings
Authentication
Server Settings
Selected farm:
Farm1
Manage farms
Citrix MetaFrame servers
Server-side firewall
Client Settings
Client-side firewall
ICA Client deployment
ICA customization
Overview
Connect to www.
Connecting to
User name:
Password:
Remember my password
OK
Cancel
Citrix MetaFrame servers
Web Interface for MetaFrame XP
Server Side Firewall (Optional)
Secure Ticket Authority (Optional. Required for Secure Gateway for MetaFrame)
End user
ICA Client
(Optional)
ICA customization
Client-side firewall settings
Server-side firewall settings
Manage farms
Help

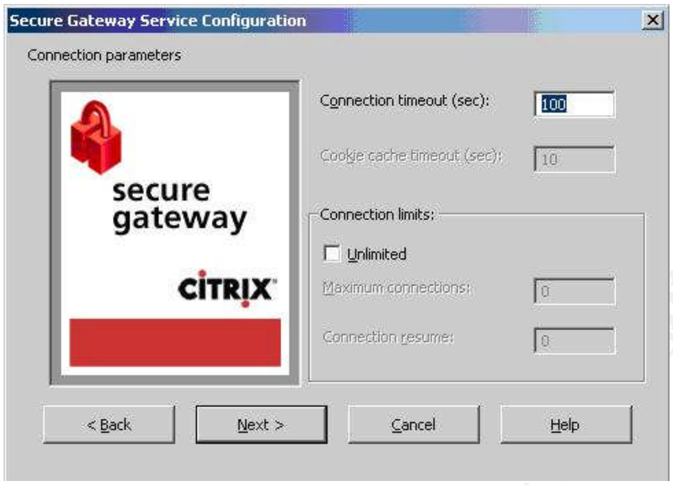
Important

**Saving changes:** Before navigating to another page in the Admin Tool, make sure you save

| | |
|---|---|
| | <br> You are not authorized to view this page - Microsoft Internet Explorer provided [redacted]<br>File Edit View Favorites Tools Help<br>Back Search Favorites Media Links<br>Address https:// Citrix/MetaFrameXP/WIAdmin/default.asp Go<br>Done Internet<br>You are not authorized to view this page<br>You do not have permission to view this directory or page using the credentials you supplied.<br>Please try the following:<br>• Click the Refresh button to try again with different credentials.<br>• If you believe you should be able to view this directory or page, please contact the Web site administrator by using the e-mail address or phone number listed on the home page.<br>HTTP 401.1 - Unauthorized: Logon Failed<br>Internet Information Services |
| **Assessment** | Attempting to logon to the administration web console proved unsuccessful resulting in a Pass status |
| **PASS / FAIL** | PASS |

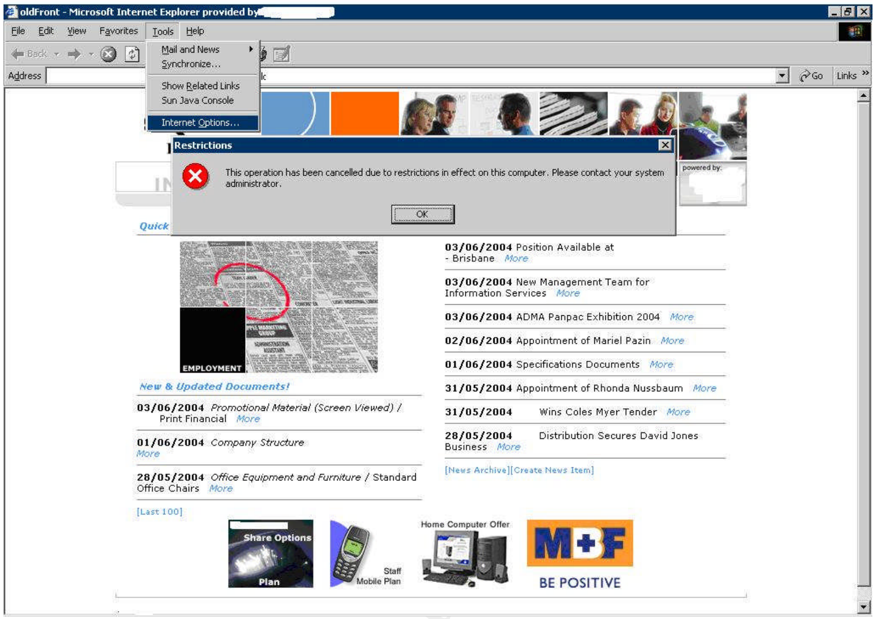
### Audit Item 15 – No timeout policy for disconnected and idle sessions

| | |
|---|---|
| **Audit Category Reference** | **CSG002** |
| **Title** | No timeout policy for disconnected and idle sessions |
| **Test Objective** | Testing that an idle www Nfuse Citrix session disconnects the user and the user is forced to re authenticate to logon. This is of a serious nature seeing the public availability of the remote access Citrix service. [25]The idle session timeout is configured to specify the amount of time a session can stay in a live state before the Metaframe server disconnects and resets the connection |
| **Compliance** | Timeout policy enabled and enforced. |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Login to Citrix Nfuse www site from a public network with supplied user account.<br>2. Simulate idle time ( go make a coffee ) endeavouring to keep track of idle time on stopwatch<br>3. Check the original Citrix session is still connected.<br>4. Check Server Configuration against time out |
| **Actual Outcome** | The auditor was permitted to logon www Nfuse server and authenticate to the Citrix Metaframe server. The auditor then made a coffee. When the auditor returned the session was disconnected ( see below )<br><br>MetaFrame XP Login - Microsoft Internet Explorer provided b[redacted]<br> File Edit View Favorites Tools Help<br>Back Search Favorites Media Links<br>Citrix MetaFrameXP<br>Login<br>Username<br>Password<br>Log In<br>Welcome<br>Please log in<br>To log in to the application portal, enter your credentials and click Log In.<br>If you do not know your login information, please contact your help desk or system administrator.<br>MetaFrame XP Message Center<br>The MetaFrame XP Message Center displays any informational or error messages that may occur.<br>Your session with the Web server has expired. You have been logged out. |

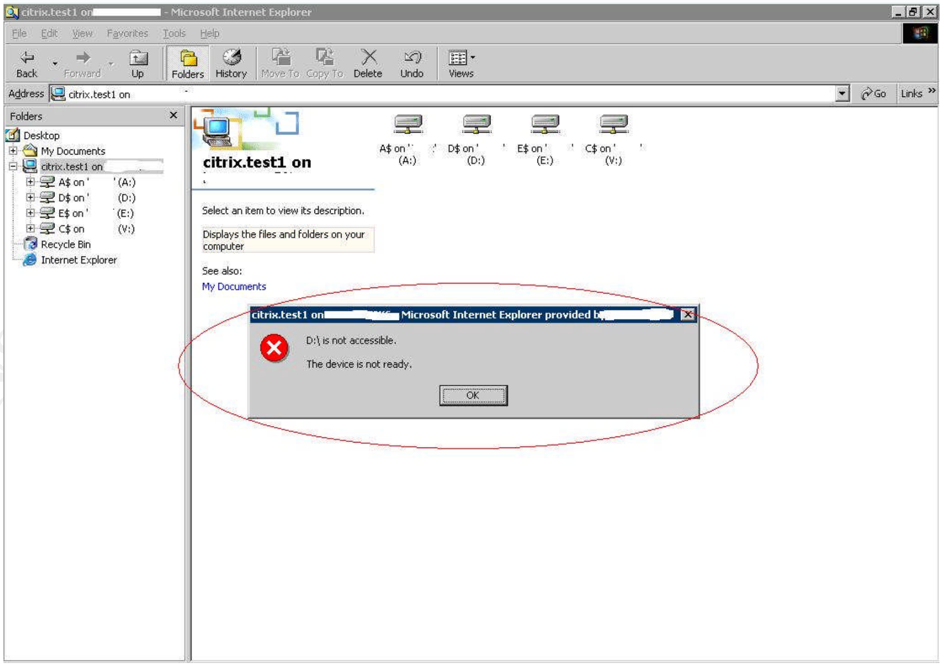
| | |
|---|---|
| | Configuration was later confirmed<br><br> Secure Gateway Service Configuration<br>secure gateway<br>CiTRIX<br>< Back<br>Next ><br>Cancel<br>Help<br>Connection parameters<br>Connection timeout (sec): 100<br>Cookie cache timeout (sec): 10<br>Connection limits:<br>□ Unlimited<br>Maximum connections: 0<br>Connection resume: 0 |
| **Assessment** | The test proved successfully that an idle session would be disconnected in less than two minutes resulting in a Pass status |
| **PASS / FAIL** | PASS |

### Audit Item 22 – No Administrative Templates applied to Specific Citrix Users

| | |
|---|---|
| **Audit Category Reference** | **CMF005** |
| **Title** | No Administrative Templates applied to Specific Citrix Users |
| **Test Objective** | Test the accessibility with given user account to Internet Options Configuration Parameters |
| **Compliance** | Application access to Internet Options Configuration Parameters is restricted |
| **Stimulus Response** | Yes |
| **Test Method** | Login to Citrix and Launch the Application in question Internet Explorer.<br>After Default home page loads attempt to enter the Internet Options area to change parameters and configuration settings |

|  |  |
|---|---|
| **Actual Outcome** | <br>oldFront - Microsoft Internet Explorer provided by [redacted]<br>File Edit View Favorites Tools Help<br>Mail and News<br>Synchronize...<br>Show Related Links<br>Sun Java Console<br>Internet Options...<br>**Restrictions**<br>This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.<br>OK<br>Quick<br>EMPLOYMENT<br>*New & Updated Documents!*<br>**03/06/2004** *Promotional Material (Screen Viewed) /* Print Financial More<br>**01/06/2004** *Company Structure* More<br>**28/05/2004** *Office Equipment and Furniture /* Standard Office Chairs More<br>[Last 100]<br>**03/06/2004** Position Available at - Brisbane More<br>**03/06/2004** New Management Team for Information Services More<br>**03/06/2004** ADMA Panpac Exhibition 2004 More<br>**02/06/2004** Appointment of Mariel Pazin More<br>**01/06/2004** Specifications Documents More<br>**31/05/2004** Appointment of Rhonda Nussbaum More<br>**31/05/2004** Wins Coles Myer Tender More<br>**28/05/2004** Distribution Secures David Jones Business More<br>[News Archive][Create News Item]<br>powered by: [redacted]<br>Share Options Plan<br>Staff Mobile Plan<br>Home Computer Offer<br>MBF BE POSITIVE |
| **Assessment** | The use of Administrative Templates enforced by a Group Policy applied to the user who performed this test prevented the user from changing configuration settings in the Internet Options Menu. Note: the administration template applied by Group Policy also restricted the user using most of the file edit and view menus. Please see full template details collected in Appendix 3 |
| **PASS / FAIL** | PASS |

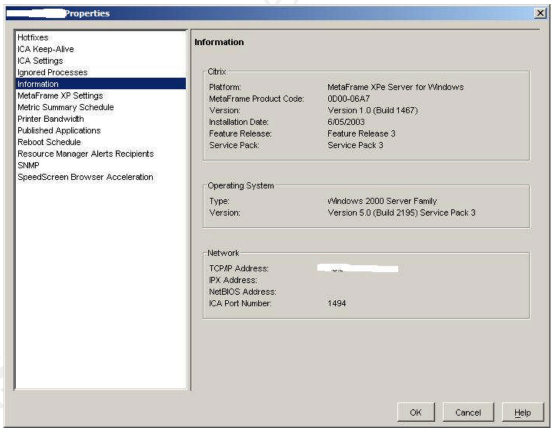
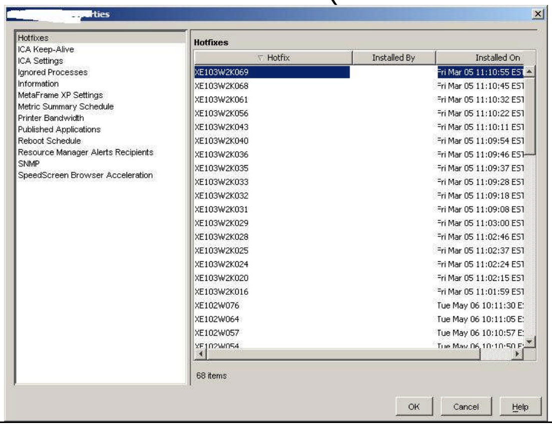
### Audit Item 20 – Default install File permissions on Meta frame server

| | |
|---|---|
| **Audit Category Reference** | **CMF003** |
| **Title** | Default install File permissions on Meta frame server |
| **Test Objective** | Test the ability to read, write and execute a file from the folders view in Internet Explorer. |
| **Compliance** | Compliant behaviour should be no access to any file system area on the Meta Frame server publishing the application |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Log into Citrix Metaframe server and Launch Internet Explorer.<br>2. From the View menu select View Folders.<br>3. From the folder tree view attempt to<br>4. Read file from Virtual drive on Meta Frame server<br>5. Write file from Virtual drive on Meta Frame server<br>6. Execute file from Virtual drive on Meta Frame server |
| **Actual Outcome** | The administrator was able to logon to the Citrix Nfuse server, Launch Internet Explorer and Select the Folder View from the View Menu. Attempting to Read, Write or Execute on any Citrix Virtual Drives areas from the Folders View produced the following Access error<br><br>citrix.test1 on [redacted] - Microsoft Internet Explorer<br>citrix.test1 on [redacted] Microsoft Internet Explorer provided b[redacted]<br>D:\ is not accessible.<br>The device is not ready.<br>OK |
| **Assessment** | The testing for compliance proved successful in this case gaining a PASS of the compliance test. Strictly speaking this is compliance however a recommendation will be, to apply an Administration Template control to block access to the Folders View menu item. |

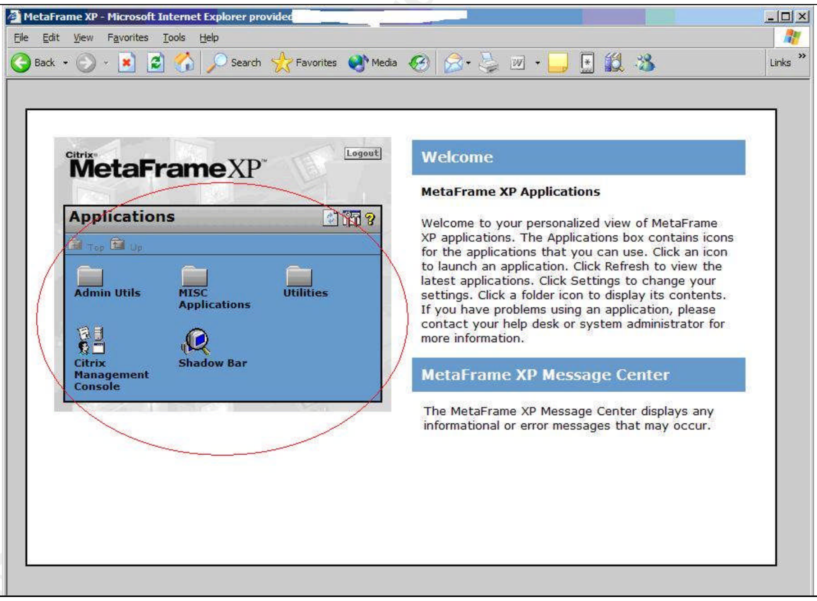
File Edit View Favorites Tools Help
Back Forward Up Folders History Move To Copy To Delete Undo Views
Address citrix.test1 on
Go Links
Folders
Desktop
My Documents
citrix.test1 on
A$ on (A:)
D$ on (D:)
E$ on (E:)
C$ on (V:)
Recycle Bin
Internet Explorer
citrix.test1 on
Select an item to view its description.
Displays the files and folders on your computer
See also:
My Documents

| | |
|---|---|
| | |
| **PASS / FAIL** | PASS |

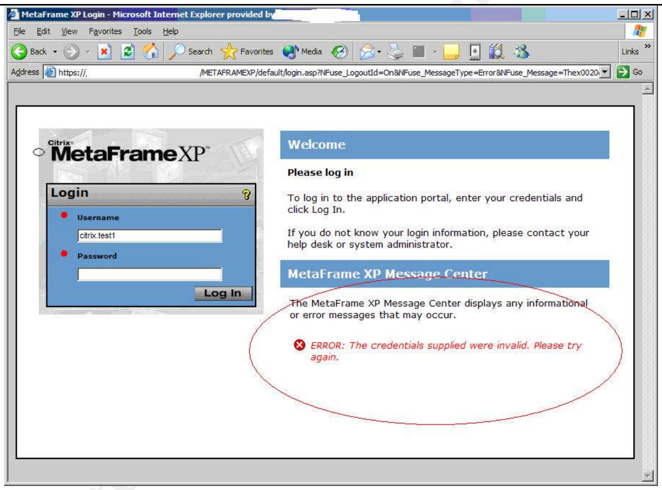
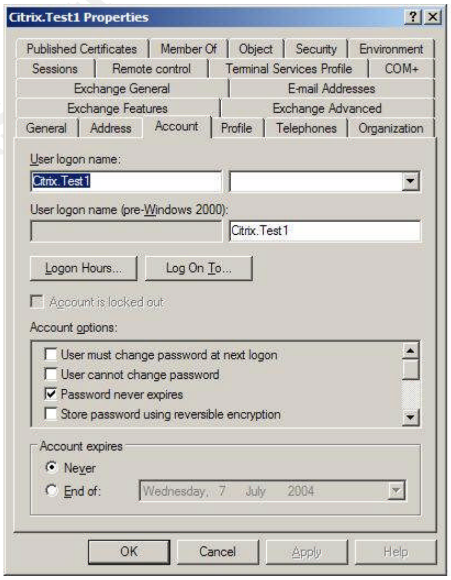
**Audit Item 23 – Latest Citrix Service Packs not installed**

| **Audit Category Reference** | **CMF006** |
|---|---|
| **Title** | Latest Citrix Service Packs and Hot fixes not installed |
| **Test Objective** | [26] Citrix has identified several Denial of Service (DoS) vulnerabilities on Citrix Metaframe servers. These vulnerabilities occur during the ICA protocol initialization phase prior to any authentication or establishment of encryption |
| **Compliance** | All Service Packs & Latest hot fixes as relevant for our Citrix Metaframe XP 1.0 installation on windows 2000 Server as current at time of writing report from http://support.citrix.com/hotfixes<br>For details please see Appendix 2 |
| **Stimulus Response** | Yes |
| **Test Method** | 1. Logon to Citrix management Console, select the Metaframe Server properties and Identify Current Citrix Version<br>2. Obtain current list of Service packs and hot fixes from Citrix support to ascertain the definitive compliance list.<br>3. Logon to Citrix management Console, select the Metaframe Server properties and  Identify current installed hot fixes<br>4. Compare against definitive Citrix List verses installed  hot fixes on  Metaframe Server |
| **Actual Outcome** | Installed Citrix Service Pack<br><br>[redacted] Properties<br>Information<br>Citrix<br>Platform: MetaFrame XPe Server for Windows<br>MetaFrame Product Code: 0D00-06A7<br>Version: Version 1.0 (Build 1467)<br>Installation Date: 6/05/2003<br>Feature Release: Feature Release 3<br>Service Pack: Service Pack 3<br>Operating System<br>Type: Windows 2000 Server Family<br>Version: Version 5.0 (Build 2195) Service Pack 3<br>Network<br>TCP/IP Address: [redacted]<br>IPX Address:<br>NetBIOS Address:<br>ICA Port Number: 1494<br> Hotfixes<br>ICA Keep-Alive<br>ICA Settings<br>Ignored Processes<br>Information<br>MetaFrame XP Settings<br>Metric Summary Schedule<br>Printer Bandwidth<br>Published Applications<br>Reboot Schedule<br>Resource Manager Alerts Recipients<br>SNMP<br>SpeedScreen Browser Acceleration<br>OK<br>Cancel<br>Help<br>Installed Citrix Hot fixes ( shortened for readability )<br><br>[redacted]rties<br>Hotfixes<br>Hotfix / Installed By / Installed On<br>XE103W2K069 Fri Mar 05 11:10:55 EST<br>XE103W2K068 Fri Mar 05 11:10:45 EST<br>XE103W2K061 Fri Mar 05 11:10:32 EST<br>XE103W2K056 Fri Mar 05 11:10:22 EST<br>XE103W2K043 Fri Mar 05 11:10:11 EST<br>XE103W2K040 Fri Mar 05 11:09:54 EST<br>XE103W2K036 Fri Mar 05 11:09:46 EST<br>XE103W2K035 Fri Mar 05 11:09:37 EST<br>XE103W2K033 Fri Mar 05 11:09:28 EST<br>XE103W2K032 Fri Mar 05 11:09:18 EST<br>XE103W2K031 Fri Mar 05 11:09:08 EST<br>XE103W2K029 Fri Mar 05 11:03:00 EST<br>XE103W2K028 Fri Mar 05 11:02:46 EST<br>XE103W2K025 Fri Mar 05 11:02:37 EST<br>XE103W2K024 Fri Mar 05 11:02:24 EST<br>XE103W2K020 Fri Mar 05 11:02:15 EST<br>XE103W2K016 Fri Mar 05 11:01:59 EST<br>XE102W076 Tue May 06 10:11:30 E<br>XE102W064 Tue May 06 10:11:05 E<br>XE102W057 Tue May 06 10:10:57 E<br>XE102W054 Tue May 06 10:10:50 E<br>68 items<br> Hotfixes<br>ICA Keep-Alive<br>ICA Settings<br>Ignored Processes<br>Information<br>MetaFrame XP Settings<br>Metric Summary Schedule<br>Printer Bandwidth<br>Published Applications<br>Reboot Schedule<br>Resource Manager Alerts Recipients<br>SNMP<br>SpeedScreen Browser Acceleration<br>OK<br>Cancel<br>Help |
| **Assessment** | Comparison of the installed service packs were compliant however hot fixes were missing such as  XE103W2K066,  XE103W2K082, XE103W2K115 resulting in a fail status |
| **PASS / FAIL** | FAIL |

### Audit Item 26 – Applications not published on a per group basis

| | |
|---|---|
| **Audit Category Reference** | **CPA002** |
| **Title** | Applications not published on a per group basis |
| **Test Objective** | To test that applications are published on a per group basis therefore restricting inadvertently accessing unintended or unplanned applications |
| **Compliance** | Access only to the nominated application associated with the Active Directory Group assigned in Citrix Management Console Security Permissions |
| **Stimulus Response** | Yes |
| **Test Method** | Logon to the Citrix Nfuse Server with testing account given.<br>Check available applications ( if any ) against testing account, CMC Management Console permissions for published Internet Explorer application |
| **Actual Outcome** |   MetaFrame XP - Microsoft Internet Explorer provided<br>File Edit View Favorites Tools Help<br>Back Search Favorites Media Links<br>Citrix MetaFrameXP<br>Logout<br>Applications<br>Top Up<br>Admin Utils<br>MISC Applications<br>Utilities<br>Citrix Management Console<br>Shadow Bar<br>Welcome<br>MetaFrame XP Applications<br>Welcome to your personalized view of MetaFrame XP applications. The Applications box contains icons for the applications that you can use. Click an icon to launch an application. Click Refresh to view the latest applications. Click Settings to change your settings. Click a folder icon to display its contents. If you have problems using an application, please contact your help desk or system administrator for more information.<br>MetaFrame XP Message Center<br>The MetaFrame XP Message Center displays any informational or error messages that may occur. |
| **Assessment** | This test was a simple test that resulted in a Fail status as additional applications in particular the Citrix Management Console and Shadow Task Bar ( execution and privilege levels of these application was not tested ) were available to this test user. Our test user account was requested to be a very basic access account with access to only our nominated application; therefore it can be assumed this is the norm for a regular user. This is a very disappointing result. |
| **PASS / FAIL** | FAIL |

### Audit Item 28 – Group Domain Account Lockout Policy not defined

| | |
|---|---|
| **Audit Category Reference** | **ADUSR002** |
| **Title** | Group Domain Account Lockout Policy not defined |
| **Reference** | |
| **Compliance** | Account is locked out for 30 minutes after 3 failed attempts of logon |
| **Stimulus Response** | Yes |
| **Test Method** | Attempt logon using the test account supplied to WWW Nfuse Server with an incorrect password in a repeated fashion until account is locked out |
| **Actual Outcome** | <br>MetaFrame XP Login - Microsoft Internet Explorer provided by [redacted]<br>Address https://. /METAFRAMEXP/default/login.asp?NFuse_LogoutId=On&NFuse_MessageType=Error&NFuse_Message=Thex0020<br>Citrix MetaFrame XP<br>Login<br>Username: citrix.test1<br>Password:<br>Log In<br>Welcome<br>Please log in<br>To log in to the application portal, enter your credentials and click Log In.<br>If you do not know your login information, please contact your help desk or system administrator.<br>MetaFrame XP Message Center<br>The MetaFrame XP Message Center displays any informational or error messages that may occur.<br>ERROR: The credentials supplied were invalid. Please try again.<br><br>Citrix.Test1 Properties<br>Published Certificates \| Member Of \| Object \| Security \| Environment \| Sessions \| Remote control \| Terminal Services Profile \| COM+ \| Exchange General \| E-mail Addresses \| Exchange Features \| Exchange Advanced \| General \| Address \| Account \| Profile \| Telephones \| Organization<br>User logon name: Citrix.Test1<br>User logon name (pre-Windows 2000): Citrix.Test1<br>Logon Hours... Log On To...<br>□ Account is locked out<br>Account options:<br>□ User must change password at next logon<br>□ User cannot change password<br>☑ Password never expires<br>□ Store password using reversible encryption<br>Account expires<br>● Never<br>○ End of: Wednesday, 7 July 2004<br>OK Cancel Apply Help |

| | |
|---|---|
| **Assessment** | This test resulted in a fail status as fifteen attempts to logon to the WWW Nfuse Server with an incorrect password did not lock the account out. This proved that Group Policy Password Account Lockout Policy was not applied to the test user account and an inspection of the Active Directory Users and Computers Console also confirmed the account did not lock out during this testing process. This test could be further enhanced with a Brute Force password attack with a utility such as LC3. |
| **PASS / FAIL** | FAIL |

## IV. AUDIT REPORT

## 6. AUDIT REPORT

### 6.1 Executive Summary

The audit was designed to examine from a holistic view the infrastructure required to deliver the remote access of a Citrix published application. The audit was broken into specific security zones for analysis of key critical components for the service delivery of the key business asset. I believe the audit objectives were achieved and with a focus on the key aspects of Technical security, Business security and Vendor best practices.

The audit identified fourteen items from the checklist of which seven items received a failed status. A detailed analysis shows the risks and consequences associated with the failing checks as grave and serious.

Our test case has shown a consolidated attempt to address infrastructure security however the risks associated with the failed checklist items identify a lack of process ( Operating & Application System patching ), technical knowledge ( application and networking ) and planning, design and implementation security considerations.

The business asset of "Remote Access" to applications is clearly at severe risk under the current circumstances and the business would be advised to undertake immediate remediation, business impact assessments and risk analysis as soon as possible.

### 6.2 Audit Findings

The audit identified fourteen items from the checklist of which there were seven items which the evidence strongly illustrates a failed status, resulting in fifty percent of checks failing. A detailed analysis shows the risks and consequences associated with the failing checks as grave and serious.
These results identify a the security methodologies and industry accepted best practices have not been implemented

| Audit Item Reference | Audit Item | Test | Audit Outcome |
|---|---|---|---|
| PHY002 | Physical Access | Attempt unauthorised physical access to building, network and Server console | PASS |
| NET001 | Test for Firewall Rule strength | Nmap Port scan internet Citrix IP addresses | FAIL |
| NET003 | Test the logical internal network range available through networking configuration | Netstat – rn to display route tables.<br>Ping, telnet and Map Network drive tests to a known critical internal host. | PASS |
| OS001 | Ascertain Service Packs and Critical Updates are current as per www.windowsupdate.com | Run MS baseline security analyser<br>Download latest secure XML<br>View analyse and compare output | FAIL |
| OS002 | Unnecessary Service Removed | Run Foundstone's fport (FPort v2.0 - TCP/IP Process to Port Mapper Copyright 2000 by Foundstone, Inc. http://www.foundstone.com)<br>Execute net start command<br>Examine outputs for running services and compare against disabled services in MS Services MMC Console | FAIL |
| OS003 | Legal Banner not displayed upon logon | Perform a Standard logon to Nfuse server | PASS |
| CNF001 | Encrypted WWW service for Nfuse | Connect Auditors machine to Network device on subnet of Citrix Nfuse server and set NIC to promiscuous mode.<br>Capture Traffic with Ethereal Packet Capture tool<br>Analyse pack capture for usernames and password in clear text | PASS |

| | | | |
|---|---|---|---|
| CNF004 | Access to Nfuse Administration Website | Attempt to logon to the Administration Web console with the test account used for the audit. | PASS |
| CSG002 | Time out Policy for idle sessions | Login to Citrix Nfuse www site from a public network with supplied user account.<br>Simulate idle time ( go make a coffee ) endeavouring to keep track of idle time on stopwatch<br>Check the original Citrix session is still connected.<br>Check Server Configuration against time out | FAIL |
| CMF003 | Default Install File Permissions on Metaframe Server | Log into Citrix Metaframe server and Launch Internet Explorer.<br>From the View menu select View Folders.<br>From the folder tree view attempt to<br>Read file from Virtual drive on Meta Frame server<br>Write file from Virtual drive on Meta Frame server<br>Execute file from Virtual drive on Meta Frame server | PASS |
| CMF005 | No Administrative Templates applied to Specific Citrix Users | Login to Citrix and Launch the Application in question Internet Explorer.<br>After Default home page loads attempt to enter the Internet Options area to change parameters and configuration settings | PASS |
| CMF006 | Latest Citrix Service Packs and Hot fixes not installed | Logon to Citrix management Console, select the Metaframe Server properties and Identify Current Citrix Version<br>Obtain current list of Service packs and hot fixes from Citrix support to ascertain the definitive compliance list.<br>Logon to Citrix management Console, select the Metaframe | FAIL |

|  |  |  |  |
|---|---|---|---|
|  |  | Server properties and Identify current installed hot fixes Compare against definitive Citrix List verses installed hot fixes on Metaframe Server |  |
| CPA002 | Applications not published on a group basis | Logon to the Citrix Nfuse Server with testing account given.<br>Check available applications ( if any ) against testing account, CMC Management Console permissions for published Internet Explorer application | FAIL |
| ADUSR002 | Group Domain Account Lockout Policy not defined | Attempt logon using the test account supplied to WWW Nfuse Server with an incorrect password in a repeated fashion until account is locked out | FAIL |

### 6.3 Audit Recommendations

The auditor recommends a risk analysis be undertaken to, prioritize the risks and identify areas for immediate improvement in addressing the vulnerabilities. A quantitative risk analysis is valuable in attempting to assign real numbers to the costs of countermeasures and the amount of damage that can take place. The risk analysis can, assign value to information and assets, estimate potential loss per risk, perform a threat analysis, derive the overall loss potential per risk, choose remedial measures to counteract each risk and reduce, assign or accept the risks.

Risks can be calculated as follows

[27]EF (Exposure Factor) = Percentage of asset loss caused by an identified threat.
SLE (Single Loss Expectancy) = Asset value * Exposure Factor
ARO (Annualized Rate of Occurrence) = Estimated frequency a threat will occur within a year.
ALE (Annualized Loss Expectancy) = Single Loss Expectancy * Annualized Rate of Occurrence

Note a purely quantitative risk analysis is not possible because the method is attempting to quantify qualitative items.

The audit outcomes reinforce the recommendation that a Business Impact Assessment be undertaken to understand the impact of a disruptive event.
The impact may be financial (quantitative) or operational (qualitative, such as the inability to respond to a customer via a service like Remote Access).

The goals of a Business Impact Assessment is to identify the following areas, Criticality Prioritization and the impact of a disruptive event must be evaluated; Downtime Estimation which estimates the MTB / Maximum Tolerable Downtime that the business can tolerate and still remain a viable company and Resource Requirements for the critical processes are also identified at this time

The auditor recommends examining in further detail the zones i.e. the zone reflected in Audit Category Reference "OS###" as it has a very high risk spectrum. The auditor has included in Appendix four a report stating a score of 6 out of 10 for the host according to a level 1 template scanned with the Center for Internet Security Windows 2000 scanning tool.

The auditor also recommends an immediate review of the seven fail status check list items ( as their remediation can be quickly addressed) and a review of process around critical updates, hot fixes and service packs as a fail status was achieved in both application and operating system. The undertaking of a thorough Risk Assessment and Business Impact Assessment should also help establish a business case for an ongoing annual security budget.

### 6.4 Cost Considerations

When calculating the countermeasures and risks the following formular should be considered.

[28]Value of safeguard to the company = (ALE before implementing safeguard) - (ALE after implementing safeguard) - (annual cost of safeguard)
Total risk = threats * vulnerability * asset value
Residual risk = (threats * vulnerability * asset value) * control gap

There is not a large amount of remediation work required to bring the seven checklist items up to a pass status. The internal resources with the appropriate training and guidance should be able to complete this work in approximately twenty five hours including planning and testing. The auditor recommends research and consulting the Industry best practices resources available on the internet and as listed in the footnotes of this paper.

### 6.4 Compensating Controls

There is a high likelihood that our test company will experience a lack of service from their business asset "remote access" in the near future as risks are spread across the various "zones" of infrastructure required to bring the Remote access to the World Wide Web and the businesses customers. A large amount of financial support has been put behind the implementation of physical security, which has created an illusion of a physical compensating control.

An enterprise State full inspection Firewall has been purchased and configured in an External and Internal DMZ (Demilitarized Zone) also giving the illusion of high security, however the rules relating to our application in question are clearly incorrectly configured. The target company for this paper now needs to make a decision regarding its next step forward in managing or even accepting its residual risk around the vulnerabilities exposed by this technical audit. The business may choose to invest in internal resources, technical training and education to further enhance the good work undertaken with Physical security and a Security Policy development.

The auditor recommends the target test company consider the risks and vulnerabilities identified in this audit and the cost of the recommended remediation, along with a process review in relation to critical updates, hot fixes and patching as identified.

**Appendix 1**

**Tools Reference**

Nmap scanning Tool – www.insecure.org

Knoppix www.knoppix.org

Ethereal www.ethereal.com/

Foundstone Fport - http://www.foundstone.com

Citrix Management Console

TCP Suite including: Netstat, ping, telnet

Active Directory Users & Computers Management Console

MS Baseline Security Analyzer www.microsoft.com.au/security

MS Windows XP

Center for Internet Security www.cisecurity.org

References (See Footnotes)

**Appendix 2**

This is a current list of hot fixes as relevant for our Citrix Metaframe XP 1.0 installation on windows 2000 Server as current at time of writing report.
This is available from
http://support.citrix.com/hotfixes

1. Hotfix XE103W2K117 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX104136, Posted: May 21, 2004
2. Hotfix XE103W2K119 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX104121, Posted: May 20, 2004
3. Hotfix XE103W2K115 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX104040, Posted: May 4, 2004
4. Hotfix XE103W2K098 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX103899, Posted: Apr 27, 2004

5. Hotfix XE103W2K100- For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX103975, Posted: Apr 27, 2004
6. Hotfix XE103W2K066 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX103962, Posted: Apr 27, 2004
7. Hotfix XE103W2K082 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX103787, Posted: Apr 9, 2004
8. Hotfix XE103W2K069 - For MetaFrame XP 1.0 for Windows 2000 - English
   CTX103433, Posted: Feb 10, 2004
9. Hotfix XE103W2K061 - For MetaFrame XP 1.0 for Windows 2000 Server - English
   CTX103371, Posted: Feb 2, 2004
10. Hotfix XE103W2K068 - For MetaFrame XP 1.0 for Windows 2000 - English
    CTX103309, Posted: Jan 21, 2004
11. Hotfix RME103W2K005 For MetaFrame for XP 1.0 for Windows 2000 Server - English
    CTX103039, Posted: Nov 24, 2003
12. Hotfix XE103W2K033 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102961, Posted: Nov 14, 2003
13. Hotfix XE103W2K043 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102925, Posted: Nov 4, 2003
14. Hotfix XE103W2K032 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102815, Posted: Oct 17, 2003
15. Hotfix XE103W2K040 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102753, Posted: Oct 8, 2003
16. Hotfix XE103W2K029 - For MetaFrame XP 1.0 for Windows 2000 - English
    CTX102681, Posted: Sep 18, 2003
17. Hotfix XE103W2K035 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102624, Posted: Sep 8, 2003
18. Hotfix XE103W2K028 - For MetaFrame XP for Windows 2000 Server - English
    CTX102508, Posted: Aug 8, 2003
19. Hotfix XE102W083 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102485, Posted: Aug 6, 2003
20. Hotfix XE103W2K024 - For Metaframe XP 1.0 for Windows 2000 Server - English
    CTX102481, Posted: Aug 6, 2003
21. Hotfix XE103W2K020 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102413, Posted: Aug 5, 2003
22. Hotfix XE102W081 - For MetaFrame XP 1.0 for Windows 2000 Server - English

CTX102308, Posted: Jul 17, 2003

23. XE103W2K013 - For MetaFrame XP for Windows 2000 Server - English
    CTX102296, Posted: Jul 10, 2003
24. Citrix MetaFrame XP Server for Windows® Feature Release 3/Service Pack 3
    CTX434343, Posted: Jun 30, 2003
25. Hotfix XE102W080 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX102092, Posted: Jun 13, 2003
26. Hotfix RME102W013
    CTX102091, Posted: Jun 5, 2003
27. HotFix XE102W076 - For MetaFrame XP 1.0 for Windows 2000 Server - English
    CTX101742, Posted: Apr 30, 2003

28. Hotfix XE102W057 - If a user attempts to launch an application from a server that does not publish that application, the user will launch a published desktop instead.
    CTX101672, Posted: Mar 19, 2003
29. HotFix XE102W054 - The IMA Service sometimes experienced a fatal system error when an administrator was browsing the Installation Manager folder in the Citrix Management Console.
    CTX101638, Posted: Mar 13, 2003
30. Hotfix XE102W028 - When using Chfarm.exe to create a new server farm using a SQL data store, the following message appeared: "The farm name does not correspond with the specified data store. Verify that you have selected the right (good) data store for the specified server farm or enter another name for the server farm."
    CTX243227, Posted: Oct 21, 2002
31. Hotfix XE102W014 - The server intermittently experienced a kernel trap when the server was in ThinWire 1 (TWI) mode.
    CTX324520, Posted: Oct 10, 2002
32. Silent Hotfix Installation
    CTX626399, Posted: Aug 30, 2002
33. Hotfix XE102W015 - If a user logged on as a domain administrator to a server in an Active Directory domain, drive remapping became unresponsive.
    CTX107122, Posted: Aug 12, 2002
34. Hotfix RME101W001 - This hotfix addresses problems with the IMA service crashing and/or database corruption when a user with a user name containing 16 or more characters logs on to a server.
    CTX536345, Posted: Jul 31, 2002
35. Hotfix XE102W012 - Some applications, including JavaScript in Internet Explorer and forms in Microsoft Access, displayed the current time in the server's time zone rather than converting it to the client's time zone.
    CTX089019, Posted: Jul 11, 2002
36. The Word Taskbar Icon for a Published Application Changes After Applying Hotfix XE101W009
    CTX693701, Posted: Jun 7, 2002
37. Hotfix XE102W001 - Smart card authentication to a MetaFrame server using

Schlumberger CSP Version 4.1 smart cards did not always work.
CTX364523, Posted: May 20, 2002

38. 🔧 Hotfix XE102W004 - Users in an ICA session using the Linux Client were unable to connect to the client printer.
CTX241074, Posted: May 17, 2002

39. Readme - Citrix Crystal Reports Templates for Resource Manager for MetaFrame XPe 1.0, Feature Release 2/Service Pack 2
CTX392860, Posted: May 14, 2002

40. 🔧 Hotfix NME102U001 - Adds Support for CA Unicenter 3.0
CTX722221, Posted: Apr 5, 2002

## Appendix 3

### Administrative Templates current settings

| Property | Value |
|---|---|
| Disable Boot/Shutdown/Logon/Logoff status messages | Enabled |
| Don't Display Welcome screen at logon | Enabled |
| User Group Policy Loop back processing mode | Enabled |
| Run startup scripts asynchronously | Enabled |
| *Run startup scripts visible* | Enabled |

### User Configuration\Admin Templates\Windows Com\IE\BM

| Property | Value |
|---|---|
| File menu: Disable Save As... menu option | Enabled |
| File menu: Disable New menu option | Enabled |
| File menu: Disable Open menu option | Enabled |
| File menu: Disable Save As Web Page Complete | Enabled |
| File menu: Disable closing the browser and Explorer windows | Not configured |
| View menu: Disable Source menu option | Enabled |
| View menu: Disable Full Screen menu option | Not configured |
| Hide Favourites menu | Enabled |
| Tools menu: Disable Internet Options... menu option | Enabled |
| Help menu: Remove 'Tip of the Day' menu option | Enabled |
| Help menu: Remove 'For Netscape Users' menu option | Enabled |
| Help menu: Remove 'Tour' menu option | Enabled |
| Help menu: Remove 'Send Feedback' menu option | Enabled |
| Disable Context menu | Enabled |
| Disable Open in New Window menu option | Enabled |

| Property | Value |
|---|---|
| Disable Save this program to disk option | Enabled |

**User Configuration\Admin Templates\Windows Com\IE\Toolbars**

| Property | Value |
|---|---|
| Disable customizing browser toolbar buttons | Enabled |
| Disable customizing browser toolbars | Enabled |
| Configure Toolbar Buttons | Enabled;Show Back,Forward, Stop, Refresh |

**User Configuration\Admin Templates\Windows Com\Explorer**

| Path | Computer Setting |
|---|---|
| Enable Classic Shell | Enabled |
| Removes the Folder Options menu item from the Tools menu | Enabled |
| Remove File menu from Windows Explorer | Enabled |
| Remove "Map Network Drive" and "Disconnect Network Drive" | Enabled |
| Remove Search button from Windows Explorer | Enabled |
| Disable Windows Explorer's default context menu | Not configured |
| Hides the Manage item on the Windows Explorer context menu | Enabled |
| Only allow approved Shell extensions | Enabled |
| Do not track Shell shortcuts during roaming | Enabled |
| Hide these specified drives in My Computer | Enabled |
| Prevent access to drives from My Computer | Enabled |
| Hide Hardware tab | Not configured |
| Disable UI to change menu animation setting | Not configured |
| Disable UI to change keyboard navigation indicator setting | Not configured |
| Disable DFS tab | Enabled; A,B, C and D drives only |
| No "Computers Near Me" in My | Not configured |

| Path | Computer Setting |
|---|---|
| Network Places | |
| No "Entire Network" in My Network Places | Not configured |
| Maximum number of recent documents | Not configured |
| Do not request alternate credentials | Enabled |
| Request credentials for network installations | Enabled |
| Hide the common dialog places bar | Enabled |
| Hide the common dialog back button | Not configured |
| Hide the dropdown list of recent files | Enabled |

**User Configuration\Admin Templates\Windows Com\Desktop**

| Path | Computer Setting |
|---|---|
| Disable Active Desktop | Enabled |

**User Configuration\Admin Templates\Windows Com\Control Panel**

| Path | Computer Setting |
|---|---|
| Disable Control Panel | Enabled |

**User Configuration\Admin Templates\Windows Com\System**

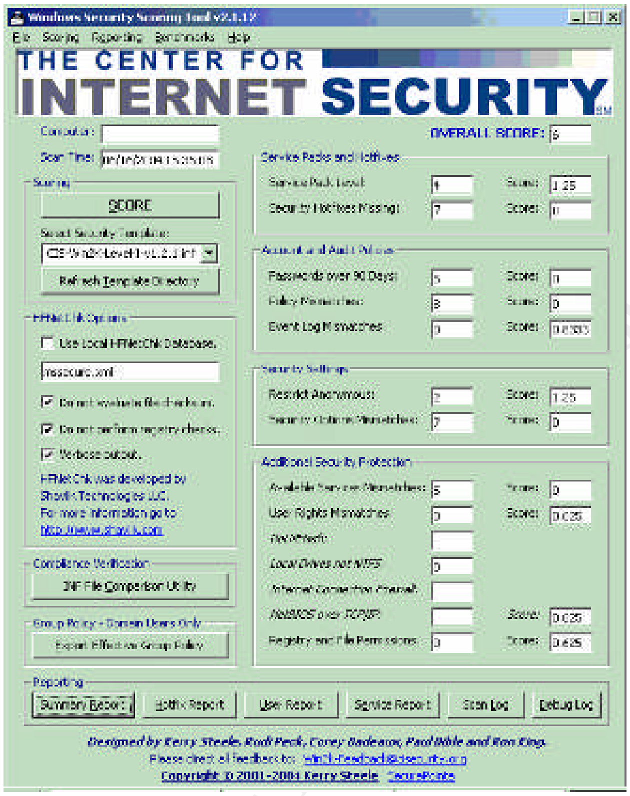
| Path | Computer Setting |
|---|---|
| Disable Command Prompt | Enabled |
| Run only allowed Windows applications | Enabled; AcroRd32.EXE, activConsole.EXE, desktop.EXE, EXCEL.EXE, logoff.exe, OUTLOOK.EXE, POWERPNT.EXE, PrintQueueToolv1_1_1.exe, pwrplay.EXE, WINWORD.EXE, AD Logon.cmd, AL Logon.cmd, BE Logon.cmd, BR Logon.cmd, BU Logon.cmd, FF Logon.cmd, IFMEMBER.EXE, Laptop Logon.cmd, PE Logon.cmd |

**User Configuration\Admin Templates\Windows Com\System**

| Path | Computer Setting |
|---|---|
| Disable Command Prompt | Enabled |

## Appendix 4

Results from scan of WWW Nfuse server
The Center for Internet Security Scanning tool available from
http://www.cisecurity.org/


Windows Security Scanning Tool v2.1.17
File Scoring Reporting Benchmarks Help
THE CENTER FOR INTERNET SECURITY
SCORE
Refresh Template Directory
HFNetChk was developed by Shavlik Technologies LLC. For more information go to http://www.shavlik.com
INF File Comparison Utility
Export Effective Group Policy
Summary Report
Hotfix Report
User Report
Service Report
Scan Log
Debug Log

Computer:
Scan Time: 06/16/2004 15:25:08

OVERALL SCORE: 5

Scoring
Select Security Template: CIS-Win2K-Level-1-v1.2.1.inf

HFNetChk Options
☐ Use Local HFNetChk Database.
mssecure.xml
☑ Do not evaluate file checksums.
☑ Do not perform registry checks.
☑ Verbose output.

Compliance Verification

Group Policy - Domain Users Only

| Service Packs and Hotfixes | | | |
|---|---|---|---|
| Service Pack Level: | 4 | Score: | 1.25 |
| Security Hotfixes Missing: | 7 | Score: | 0 |

| Account and Audit Policies | | | |
|---|---|---|---|
| Passwords over 90 Days: | 5 | Score: | 0 |
| Policy Mismatches: | 8 | Score: | 0 |
| Event Log Mismatches: | 0 | Score: | 0.0333 |

| Security Settings | | | |
|---|---|---|---|
| Restrict Anonymous: | 2 | Score: | 1.25 |
| Security Options Mismatches: | 7 | Score: | 0 |

| Additional Security Protection | | | |
|---|---|---|---|
| Available Services Mismatches: | 5 | Score: | 0 |
| User Rights Mismatches: | 0 | Score: | 0.025 |
| DLL Effects: | | | |
| Local Drives not NTFS: | 0 | | |
| Internet Connection Firewall: | | | |
| NetBIOS over TCP/IP: | | Score: | 0.025 |
| Registry and File Permissions: | 0 | Score: | 0.625 |

Reporting

*Designed by Kerry Steele, Rudi Peck, Corey Badeaux, Paul Bible and Ron King.*
Please direct all feedback to: win2k-feedback@cisecurity.org
Copyright © 2001-2004 Kerry Steele SecurePoints

## Appendix 5

| Property | Success | Failure |
|---|---|---|
| Audit Account Logon Events | Yes | Yes |
| Audit Account Management | Yes | Yes |
| Audit Directory Service Access | Yes | Yes |
| Audit Logon Events | Yes | Yes |
| Audit Object Access | Yes | Yes |
| Audit Policy Change | Yes | Yes |
| Audit Privilege Use | Yes | Yes |
| Audit Process Tracking | No | No |
| Audit System Events | Yes | Yes |

## Footnotes / Bibliography

[1] CISSP Certification Exam Guide , Harris, Shon page 64, bottom paragraph

[2] AS/NZS 4444.2:2000 “Specification for Information Security Management Systems”, AS/NZS ISO/IEC 17799.2001 “Information Technology – Code of Practice for Information Security Management”, AS/NZ 7799.2:2003 “Information Security Management – Specification for Information Security Management Systems”, HB 231:2000 “Information Security Risk Management Guidelines”, HB 171-2003 “Guidelines for the Management of IT Evidence”.

[3] www.standards.com.au

[4] Building Internet Firewalls, Internet and Web Security 2nd Edition, O’Reilly, Zwicky, Cooper & Chapman

[5] http://www.securityfocus.com/archive/1/220885

ISS Security Advisory: Citrix Meta Frame Remote Denial of Service Vulnerability

Citrix Meta Frame Remote Denial of Service Vulnerability

Synopsis:

ISS has discovered a remote Denial of Service (DoS) vulnerability
In Citrix Meta Frame. Citrix Meta Frame is an application server that
works with Windows Terminal Services. This vulnerability causes a
Meta Frame installation to crash or "blue screen" and requires an
Affected system to be restarted manually. No local access is needed
to exploit this vulnerability.

[6] GSEC Security Essentials Toolkit, Cole Eric SANS Press

[7] HACKING EXPOSED Network Secret and Solutions, SCAMBRAY, Joel and MCCLURE, Stuart

[8] The Art of Port Scanning http//www.insecure.org/nmap/p51-11.txt

[9] The Art of Port Scanning http//www.insecure.org/nmap/p51-11.txt

[10] Microsoft provide the www.windowsupdate.com website to aid in keeping the Windows 2000 Operating system up to date with the latest critical updates, service packs and hot fixes.. This is referenced by the MS baseline security analyzes.

The hot fixes and updates are for various flaws and exploits in the base Operating system. An example of some is

- Q320206 Authentication Flaw in Windows Debugger can Lead to Elevated Privileges

- Q318138 Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution
- Q326886 Flaw in Network Connection Manager
- Q323172 Flaw in Digital Certificate Enrolment Component Allows Certificate Deletion
- Q328145 Certificate Validation Flaw Could Enable Identity Spoofing
- Q324380 Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure
- Q296441 WebDAV Service Provider Can Allow Scripts to Levy Requests as User
- Q319733 Cumulative Patch for Internet Information Service
- Q321599 Heap overrun in HTR Chunked Encoding Could Enable  Web Server Compromise

[11] Hacking Exposed 2000 Network Security Secrets and Solutions SCAMBRAY, Joel and MCCLURE, Stuart, Osborne / McGraw-Hill. -Code Red Worm July 17th 2001 page 217

[12] Hacking Exposed 2000 Network Security Secrets and Solutions SCAMBRAY, Joel and MCCLURE, Stuart, Osborne / McGraw-Hill. -Code Red Worm July 17th 2001 page 217

[13] Citrix Metaframe XP, Advanced Technical Design, Second Edition, Madden Brian – Group Policy, Pages 191-192

[14]  Based on information reported by the security firms Internet Security Systems, Inc. (http://www.iss.net and http://xforce.iss.net), and @stake (http://www.atstake.com), Citrix has identified several Denial of Service (DoS) vulnerabilities on Citrix Metaframe servers. These vulnerabilities occur during the ICA protocol initialization phase prior to any authentication or establishment of encryption. These vulnerabilities cause a Metaframe installation to use 100% of the CPU or to crash. An affected server machine needs to be rebooted. No user account or local access is needed to exploit this vulnerability. These vulnerabilities were duplicated at Citrix and a server-side fix has been produced.

[15] SANS Securing Windows 2000 Step by Step  A consensus document by Security Professionals Version 1.5 Page 21

[16] Windows NT Security Guidelines , Trusted Systems Services A study for NSA Research , Author Steve Sutton Trusted Systems Services , Sponsor Scott Cothrell ( National Security Agency ) page 59

[17] Microsoft Best Practices for password Policies http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-

us/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/windows_password_protect.asp

[18] http://www.atstake.com.au/research/lc3

[19] Building Internet Firewalls, Internet and Web Security 2nd Edition, O'Reilly, Zwicky, Cooper & Chapman

[20] The Art of Port Scanning http//www.insecure.org/nmap/p51-11.txt

[21] HACKING EXPOSED, SCAMBRAY, Joel and MCCLURE, Stuart, Osborne / McGraw-Hill , Chapter 11 Firewalls, P486

[22] Microsoft provide the www.windowsupdate.com website to aid in keeping the Windows 2000 Operating system up to date with the latest critical updates, service packs and hot fixes.. This is referenced by the MS baseline security analyzes.

The hot fixes and updates are for various flaws and exploits in the base Operating system. An example of some is

- Q320206 Authentication Flaw in Windows Debugger can Lead to Elevated Privileges
- Q318138 Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution
- Q326886 Flaw in Network Connection Manager
- Q323172 Flaw in Digital Certificate Enrolment Component Allows Certificate Deletion
- Q328145 Certificate Validation Flaw Could Enable Identity Spoofing
- Q324380 Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure
- Q296441 WebDAV Service Provider Can Allow Scripts to Levy Requests as User
- Q319733 Cumulative Patch for Internet Information Service
- Q321599 Heap overrun in HTR Chunked Encoding Could Enable Web Server Compromise

[23] Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run http://www.microsoft.com/technet/security/bulletin/MS02-006.mspx

[24] CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP) http://www.cert.org/advisories/CA-2002-03.html

[25] Citrix Metaframe XP, Advanced Technical Design, Second Edition, Madden Brian, BrianMadden.com Publishing– Session Timeout, Pages 643-647

[26] Based on information reported by the security firms Internet Security Systems, Inc. (http://www.iss.net and http://xforce.iss.net), and @stake (http://www.atstake.com),

Citrix has identified several Denial of Service (DoS) vulnerabilities on Citrix Metaframe servers. These vulnerabilities occur during the ICA protocol initialization phase prior to any authentication or establishment of encryption. These vulnerabilities cause a Metaframe installation to use 100% of the CPU or to crash. An affected server machine needs to be rebooted. No user account or local access is needed to exploit this vulnerability. These vulnerabilities were duplicated at Citrix and a server-side fix has been produced.

[27] Information Security Management Handbook, Fifth Edition (CD-ROM edition) Micki Krause, CISSP (Editor) Section #2 CBK Security Management Practices

[28] Information Security Management Handbook, Fifth Edition (CD-ROM edition) Micki Krause, CISSP (Editor) Section #2 CBK Security Management Practices