



Who's watching your back?

Got Citrix? Hack IT!

Shanit Gupta

August 7th, 2008

Who Am I?

```
...element* item = el->FirstChildElement();  
GroupDesc::ElementDesc elDesc;  
  
std::wstring sp_name = item->Attribute( "name" );  
std::wstring spritename = item->Attribute( "spritename" );  
  
float x = boost::lexical_cast<float>( item->Attribute( "x" ) );  
float y = boost::lexical_cast<float>( item->Attribute( "y" ) );  
float offset = boost::lexical_cast<float>( item->Attribute( "offset" ) );  
unsigned layer = 50; // default  
if ( item->Attribute( "layer" ) != NULL )  
{  
    layer = boost::lexical_cast<unsigned>( item->Attribute( "layer" ) );  
}  
  
elDesc.name_ = sp_name;  
elDesc.spriteName_ = spritename;  
elDesc.x_ = x;
```

- ▶ Principal Consultant – Foundstone Professional Services
- ▶ Code Review / Threat Modeling / Application Security
- ▶ Masters from Carnegie Mellon

Agenda

- ▶ Background
- ▶ Demo 1: Kiosk Mode
- ▶ Demo 2: Unauthenticated Access
- ▶ Demo 3: (Un)Hidden Hotkeys
- ▶ Demo 4: Restricted Desktop Access
- ▶ Demo 5: Attack Microsoft Office
- ▶ Remediation Measures

False Sense of Security



Demo1: Kiosk Mode

The screenshot shows a Citrix Desktop window titled "Citrix Desktop - Citrix Presentation Server Client [SpeedScreen On]". The website content is as follows:

- Navigation:** SERVICES, COMPANY, EDUCATION, RESOURCES, CONTACT, CAREERS, BLOG
- McAfee FOUNDSTONE PRODUCTS** logo in the top right.
- Main Image:** Silhouettes of four people walking with the text "Who's watching your back?".
- Foundstone A division of McAfee** logo, oriented vertically.
- Section Header:** >> Welcome
- Text:** Ensuring the protection of your organization takes time and proven expertise. High levels of client satisfaction confirm that Foundstone Professional Services delivers sound advice and thought leadership with a portfolio of services and free tools that help protect our customers' systems.
- Bill Hau Vice President Foundstone
- Service Links:**
 - Get Our Services Now
 - Got Hacked? Get 911 Response
 - Free Tools & Resources
- Target Audience:** For Executives, For Security Professionals, For Software Security Professionals, For Auditors
- White Paper:** NEW Virtualization White Paper
- Footer:** services | company | education | resources | contact | privacy policy | site map | McAfee.com | Copyright © 2003-2007 McAfee, Inc. All Rights Reserved.

Demo1: Kiosk Mode (Attack Vectors)

- ▶ Ctrl + h – View History
- ▶ Ctrl + n – New Browser
- ▶ Shift + Left Click – New Browser
- ▶ Ctrl + o – Internet Address (browse feature)
- ▶ Ctrl + p – Print (to file)
- ▶ Right Click (Shift + F10)
 - Save Image As
 - View Source
- ▶ F1 – Jump to URL...
- ▶ Browse to <http://download.insecure.org/nmap/dist/nmap-4.53-setup.exe>

I Hope You Are Patching 😊

The screenshot shows a Mozilla Firefox browser window displaying the Secunia website search results for 'Citrix'. The browser's address bar shows the URL 'http://secunia.com/search/?search=Citrix'. The page title is 'Search Advisory, Vulnerability, and Virus Database - Secunia - Mozilla Firefox'. The search results section is titled 'Found: 37 Secunia Security Advisories, displaying 1-25'. A table lists the results, with the first 10 items highlighted in a pink box. The table has two columns: 'Title' and 'Date'. Below the table, there is a link for 'Next 12 matches >>'. At the bottom of the search results, it says 'Found: 0 Viruses, displaying 0-0'. On the left side of the browser window, there is a sidebar with navigation links and a promotional message from Secunia.

Found: 37 Secunia Security Advisories, displaying 1-25

Sort by: [Match](#), [Title](#), [Date](#)

Title	Date
Citrix Presentation Server IMA Service Buffer Overflow Vulnerability	2008-01-17
Citrix Web Interface Unspecified Cross-Site Scripting Vulnerability	2007-12-19
Citrix EdgeSight Configuration File Information Disclosure Weakness	2007-12-05
Citrix Netscaler Web Management "standalone" Cross-Site Scripting	2007-12-04
Citrix Presentation Server Published Application Execution Weakness	2007-11-15
Citrix Access Gateway Multiple Vulnerabilities	2007-07-20
Citrix Presentation Server Clients Content-Redirection Vulnerability	2007-07-06
Citrix Products Session Reliability Service Security Bypass	2007-05-23
Citrix Presentation Server Client Unspecified Code Execution	2007-03-01
Citrix Presentation Server Print Provider Buffer Overflow Vulnerability	2007-01-25
Citrix ICA Client ActiveX Control Buffer Overflow Vulnerability	2006-12-06
Citrix Advanced Access Control Two Vulnerabilities	2006-11-15
Citrix Access Gateway Appliance Information Disclosure	2006-11-15
Citrix Presentation Server IMA Service Vulnerabilities	2006-11-10
Citrix Access Gateway Advanced Access Control Authentication Bypass	2006-09-18
Citrix MetaFrame Insecure Default Registry Key Permissions	2006-07-19
Citrix Program Neighborhood Client Buffer Overflow Vulnerability	2005-12-16
Citrix Products Login Page Cross-Site Scripting Vulnerability	2005-12-01
Citrix Metaframe Presentation Server Policy Filtering Bypass	2005-10-03
Citrix Program Neighborhood Agent Two Vulnerabilities	2005-04-26
Citrix MetaFrame Password Manager Secondary Password Disclosure	2005-03-16
Citrix Metaframe XP Unspecified Buffer Overflow Vulnerability	2004-12-22
Citrix MetaFrame Presentation Server Client Debugging Security Issue	2004-11-22
Citrix Secure Gateway OpenSSL Vulnerability	2004-08-09
Citrix MetaFrame Password Manager Authentication Information Disclosure	2004-04-05

[Next 12 matches >>](#)

Found: 0 Viruses, displaying 0-0

Do you know which vulnerabilities exist within YOUR network and what patches you REALLY need?

Secunia
covers more than 15,000 OSes and software

*Source: <http://secunia.com>

Demo 2: Unauthenticated Access

- ▶ 9 publicly accessible exploits 2007 – 08
- ▶ Particularly interesting
 - Citrix Presentation Server IMA Service Buffer Overflow Vulnerability
 - Social Engineering: Malicious ICA files

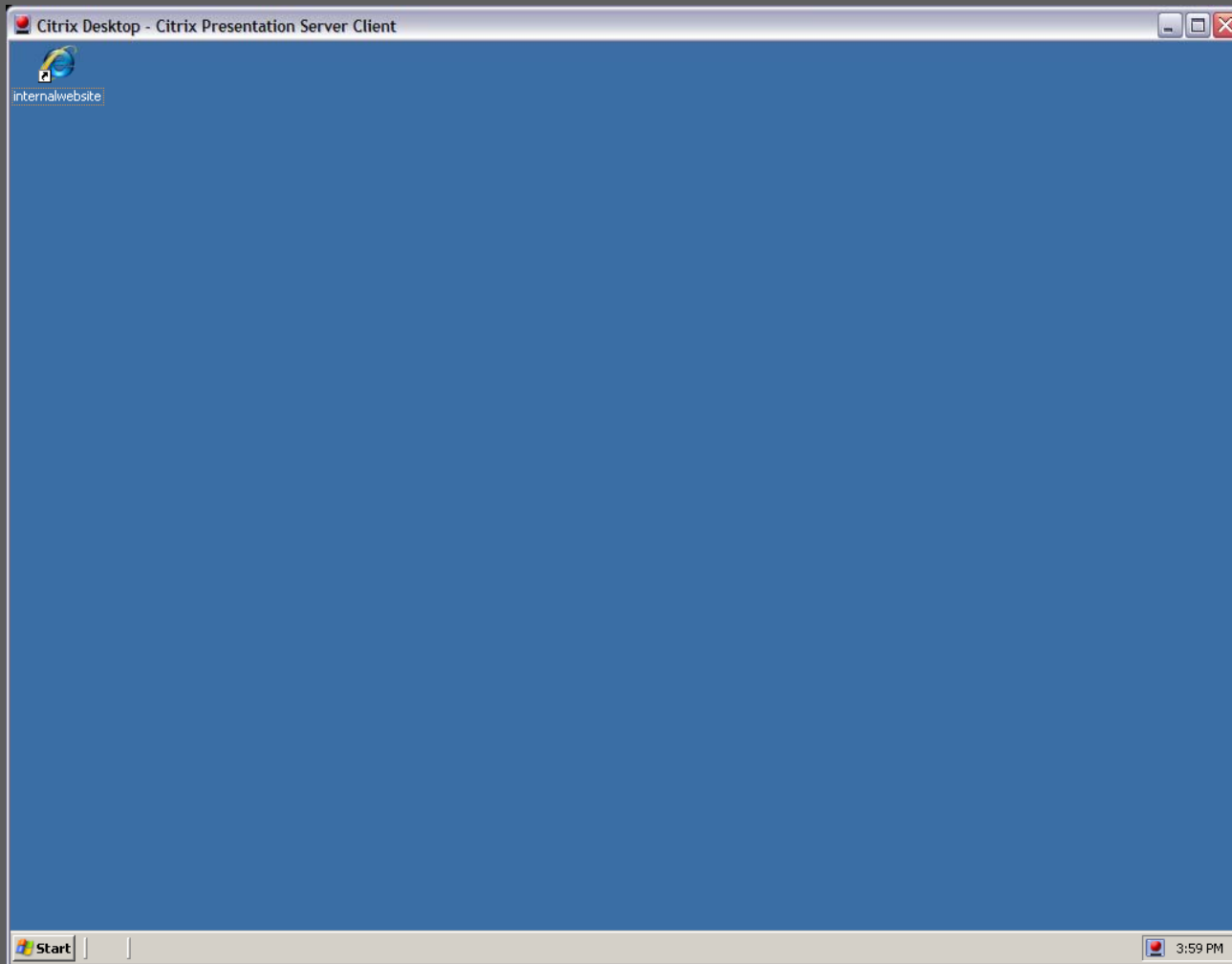
Demo 2: Unauthenticated Access

- ▶ Good Old Brute Force
 - One account is all you need
 - I am sure you are using 2 factor authentication ;-)

Demo3: (Un)Hidden Hotkeys

- ▶ SHIFT+F1: Local Task List
- ▶ SHIFT+F2: Toggle Title Bar
- ▶ SHIFT+F3: Close Remote Application
- ▶ CTRL+F1: Displays Windows Security Desktop – Ctrl+Alt+Del
- ▶ CTRL+F2: Remote Task List
- ▶ CTRL+F3: Remote Task Manager – Ctrl+Shift+ESC
- ▶ ALT+F2: Cycle through programs
- ▶ ALT+PLUS: Alt+TAB
- ▶ ALT+MINUS: ALT+SHIFT+TAB

Demo4: Restricted Desktop



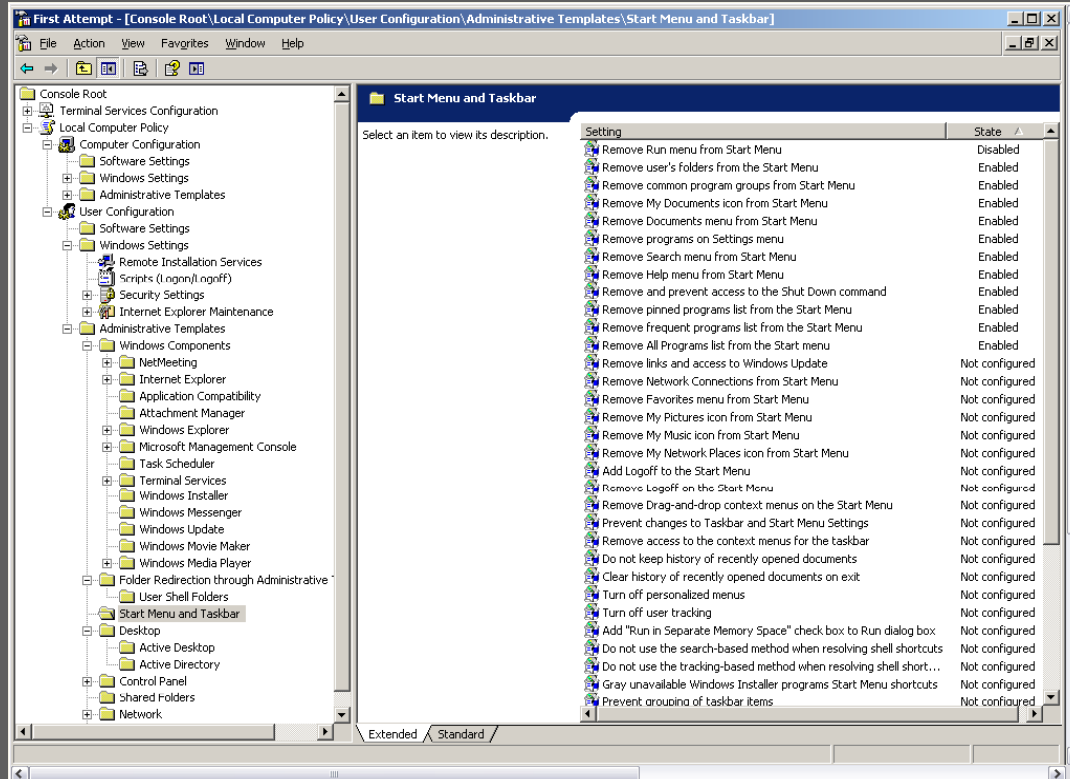
Demo4: Restricted Desktop

- ▶ Shortcut to C:\
- ▶ Create Batch File
 - CMD.exe
- ▶ Host Scripting File (filename.vbs)
 - Set objApp = CreateObject("WScript.Shell")
 - objApp.Run "CMD C:\"

Demo5: Attack Microsoft Office

- ▶ File->Save As
 - Browse Files and Launch CMD.exe
- ▶ Press F1
 - Search Microsoft
 - Click Suites Home Page
- ▶ Macros
 - Remote Shell
 - Privilege Escalation

Remediation Strategies



- ▶ 1300 different registry settings
- ▶ It is HARD!



Remediation Strategies

▶ Lock Down Tools

- Commercial
- Freeware
- <http://updates.zdnet.com/tags/lockdown.html>

Questions or Concerns?

