Who's watching your back?

Got Citrix? Hack IT!

Shanit Gupta
August 7th, 2008
Who Am I?

- 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
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](http://download.insecure.org/nmap/dist/nmap-4.53-setup.exe)
I Hope You Are Patching 😊

*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
Questions or Concerns?