security-assessment.com

Internet Kiosk Terminals The Redux

Paul Craig – Security-Assessment.com

Defcon 19 – Las Vegas

- **Hello Defcon 19**
  - My name is Paul Craig
  - I work at Security-Assessment.com as a penetration tester.
  - I love to hack stuff, its my life, and my profession.
  - If you have any questions or comments – Please email me
    - Paul@ha.cked.net

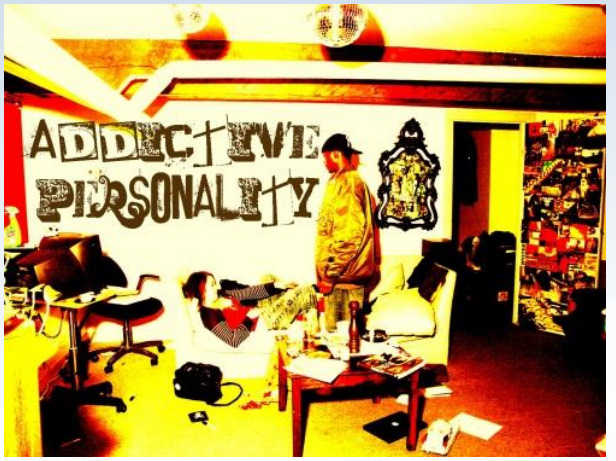
- **My colleagues at SA know me as "That Crazy Kiosk Guy"**
  - "All I do is Hack Internet Kiosks"
  - Its my secret addiction.
- **Whenever I see an Internet Kiosk, I have to hack it.**
  - I cant stop myself.
  - I **have** a problem, its an addiction.

People in my life have told me that I have an

Addictive Personality

My obsession with Kiosk hacking began to have a negative effect on my life... Hacking Kiosks controlled me.

"Paul, You just need a distraction"



- **The 8 Stages of Grief: #7 Acceptance**
  - "Someone has to be hacking these damn Kiosks, so why not you?"
  - I am the **only** guy in the world with a Kiosk addiction.

Without my effort the vendors might win.

  - I decided to take ownership of my passion
  - Embrace my addiction

  - **"Ill just fucking hack all of them"**
    - Every vendor, every product, every platform.
    - Yeah fuck it, why not.?
  - One guy from NZ vs The Kiosk Software Industry

- **The Overview**
  - What is a Kiosk
  - How Kiosk Security Works
  - What is iKAT
  - My Methodology and Approach
  - iKAT v4 – Whats New

  - Demos, Demos, Demos, Demos
    - Hacking Kiosks with Paul
    - Live Demos

- **What is an Internet Kiosk ?**
  - A machine that takes payment to let you surf the internet
  - Typically an x86 desktop running Windows or Linux
  - Found at hotels, motels, airports, libraries, lobbies, casinos..

They look like this:

How Kiosks Are Secured

security-assessment.com

- **Kiosk vendors take security seriously**
  - The majority of functionality in Kiosk software is security related
  - A secure Kiosk is an expensive Kiosk
  - Lock Downed, Secured, Hardened, Protected Environments

This is because hackers LOVE hacking Kiosks!

- Monitors and protects the operating system against manipulation by computer vandalism and hacking
- Secures system drives, folders and files from unauthorized access
- Protects the terminal against most viruses, trojans, and destructive scripts
- Allows access to programs and applications specifically authorized by the administrator
- Deactivates undesired function keys and system critical key combinations
- Restrict or prohibit the downloading of files from the Internet

User Access & System Security Management (PC lock-down)

SiteKiosk safeguards Windows computers as soon as it boots up agains
maintenance-free operation of your computers 24/7. Our software locks d
user account with limited user access rights. Users are prevented from a
restrict user access to certain drives, folders, programs and URLs. Syste
blocked and a software watchdog monitors your computers.

- Security
  - Privacy - All user information, cookies and session information are removed as soon as the user session is over.
  - Ad-ware blocked: All pop-ups that are not authorized by the configuration are blocked.
  - Secure Internet access - filters and trap unsecured scripts user may find on un-trusted websites
  - URL access control
    - captive (fixed URL)
    - white list/black list
    - script filtering
    - Boot Control and OS lock-down - Users cannot access the underlying operating system or bios. All key combinations and menus are controlled.
  - File download blocking - KINGnet kiosk prevents all file downloads
  - Keyboard filtering - All key combinations and mouse right clicks are filtered so that users cannot jeopardize the kiosk integrity
  - Software watchdog
    - Monitors kiosk software
    - Expects a heartbeat signal
    - Performs soft-boot if no signal is received by the Software Watchdog

How Kiosks Are Secured

security-assessment.com

1. User Interface Security

- Graphically jailed into a Kiosk interface
- Cut-down/reduced functionality desktop
- No way to get back to “Windows” or run explorer, cmd.exe

2. Activity Blacklist

- Everything you do is monitored and unlawful activity is blocked
- Configurable blacklists:
  - Windows displayed, Buttons clicked
  - Processes executed, API’s called

3. Locked-Down Host Environment

- Kiosk user has no rights, no privileges
- Cannot run binaries on the Kiosk

- **Four things I have learnt about Kiosks**
  - **1) Blacklists Just Don't Work**
    - The security industry knows this, why don't Kiosk vendors ?
    - Thousand different ways to do anything
    - Kiosk blacklists are never able to stop EVERY method
  - **2) Websites Visited From A Kiosk Are Overlooked**
    - A remote website often has more access to the Kiosk than you.
    - Kiosks rely on a default browser security policy (Typically Internet Explorer)
  - **3) Browsers Implement 'Security By User Interaction'**
    - Browser technology will trust the person on the keyboard
    - "Are you sure you want to run this?"

- **4) Physical Access Always Wins.**

  Microsoft's Ten immutable laws of security.

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore

  - Operating systems will trust the local user
  - Kiosk software must go against the grain of design

- **"It Only Takes One Instance"**
  - Every instance of trusting the local user has to be blocked
  - It only takes one instance of trust to hack a Kiosk

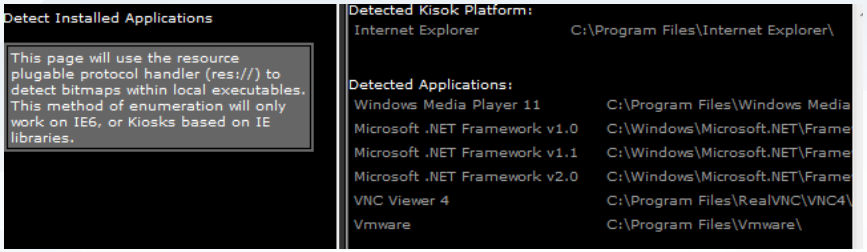
- **Hacking Kiosks**
  - The great thing about hacking Kiosks is that its easy!
  - Its like solving a puzzle or doing a Sudoku
  - Our goal: Pop Shell (Spawn cmd, explorer, xterm)
  - How could you run cmd.exe on Windows
    - If you only had Internet Explorer open
    - And no Task Bar (“Start”)
  - In a nut shell this is what Kiosk hacking is all about.
  - Finding a way of escaping the Kiosk environment

- **What is iKAT ? – Interactive Kiosk Attack Tool**
  - iKAT is a SAAS website that you visit from a Kiosk
  - One-Stop-Shop for escaping jailed browser environments
  - Contains simple tools in one handy place
  - First launched at Defcon 16, iKAT is now up to v4
  - Defcon 19 - **iKAT V**engeance Edition
  - iKAT has become the de facto standard for Kiosk hacking
  - On average 25-30 Kiosks per day ‘visit’ iKAT
  - During Defcon 18 my traffic stats increased ten fold!

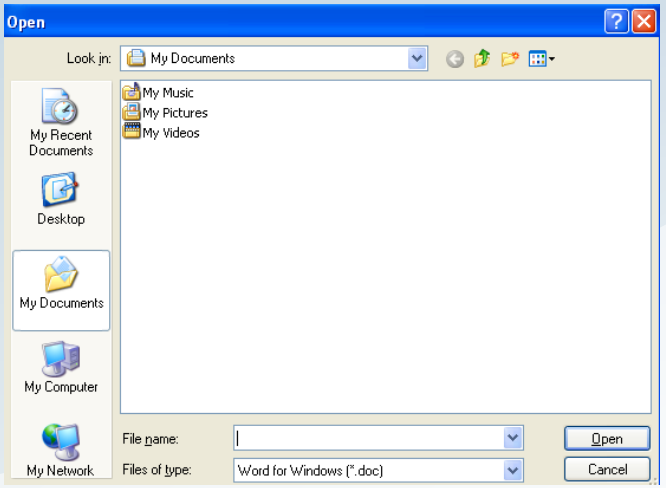
- **My Approach for Hacking Kiosks:**
  - This is how I break Kiosk software

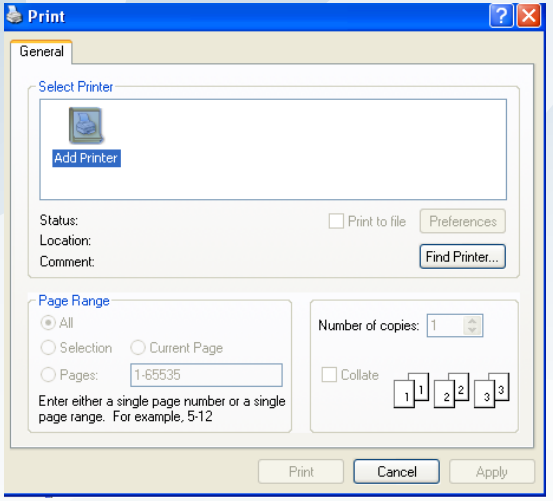
- **#1 - Identify the platform and vendor software in use**
  - Look for a logo or brand name associated with the Kiosk
  - Is the look and feel similar to Windows, or Linux ?
  - Determining the platform allows for specific targeting
  - Find what applications are installed

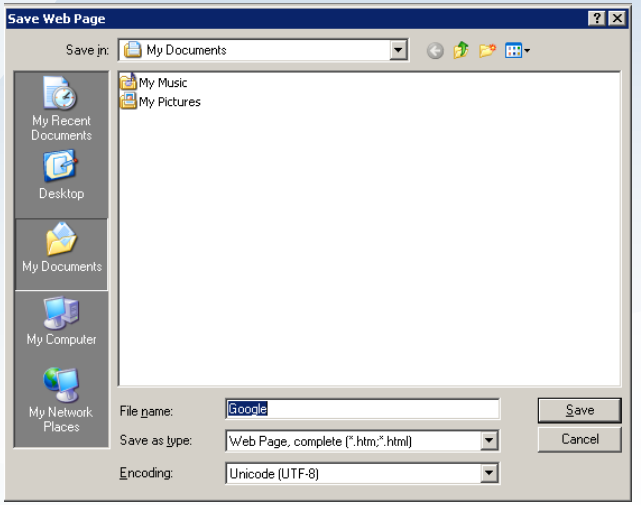
  - iKAT : “Detect Installed Applications”



- # #2 – Enumerate All Available Windows
  - Systematically click every button, window, link
    - Shift-Click, Ctrl-Click, Double Click, Right Click
    - Can you spawn a common Dialog ?
      - File -> Open, File -> Save, File-> Print
    - Common Dialogs have Explorer controls
      - Browse to C:\Windows\system32, cmd.exe open…
    - Controls are also WebDAV Enabled (They can Download / Upload)







- **#3 – Enumerate Registered File Handlers**
  - Any installed application can be used to escape a Kiosk
  - Image Viewer, Media Player, PDF Reader
  - Use an innocent file type to spawn a binary or escape the Kiosk
    - PDF File with /Launch cmd.exe
    - ASX With embedded web content
    - DOCX with embedded binaries
    - XLS with embedded VBA Macro's

  - What file types will the Kiosk let us download
    - Direct file type "test.exe", "test.exe?.txt"
    - Content Disposition attachment download
    - Flash DownloadURL object

- **#4 – Enumerate Registered URI Protocol Handlers**
  - Spawn an application from a URI handler
  - mailto://. Callto://, hcp://, shell::, file://, mms://, ftp://
  - Image Viewer, Media Player, PDF Reader
  - Can we spawn one of these URI handlers
    - Does the handling application contains a common dialog ?
    - Can we launch content from within the URI handler
  - Does the Kiosk software support any internal URI handlers ?
    - Admin://
    - Skconfig://

- **#5 – Can I Install / Run My Own Browser Add-on**
  - ActiveX, Click Once(.NET), Java, SilverLight, Flash
  - Java, ActiveX and ClickOnce can spawn processes.
  - They can also create Common Dialogs
  - iKAT v1 was full of browser add-ons.
- Vendors caught up quickly: ”Trusted CA ***Signed*** Add-ons only”
- Signed Vs Unsigned Code: The $500 Problem.
  - “Please donate to iKAT so I can buy a Code Signing Certificate”
  - iKAT now supports 100% signed code, from a trusted CA

- **#6 – Crash the Kiosk**
  - The fastest way to escape a Kiosk jail is to crash it.
    - Emo-Kiosking: *"I cut myself to release the pain"*
    - Create an unhandled exception in the browser
  - Crash the browser back to the desktop
    - Flash, ActiveX, Java, JavaScript, VBScript, PDF files, HTML Rendering, Malformed Images
    - Browsers just love to crash!

  - Unhandled exceptions are a huge security issue with Kiosks.

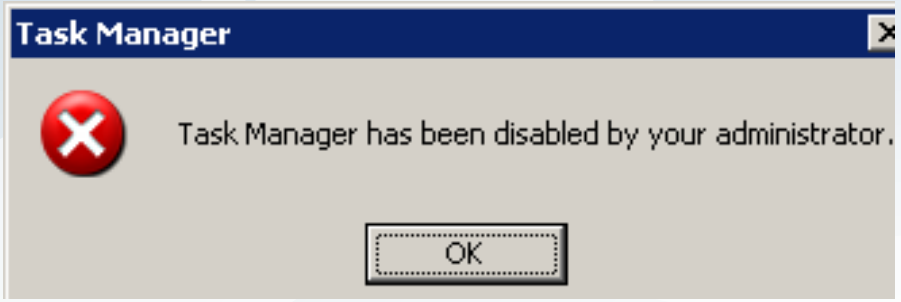
- **#7 – Win Shell Hacking**
  - iKAT features tools to help you hack the Windows Shell environment.
  - **Make Visible** – Use ShowWindow() to enable all hidden Windows
    - Anti Virus, Backup, Remote Admin, Kiosk Software often have hidden Windows that are set WS_Visible False.
      - Debug Windows
      - Hidden Administrative Windows
      - Log messages

iKAT – What's New?

security-assessment.com

- **When iKAT was first launched it had GREAT success**
  - "5 seconds, 50 shells."
  - Then the vendors found out and fixed my attack vectors.
  - Some vendors simply blocked ikat.ha.cked.net
  - Other vendors used iKAT as a testing bed for their own security.
- **Cat and Mouse Game**
  - Every year I find new vulnerabilities in Kiosk products
  - Every year the vendors fix the vulnerabilities I discover
  - The following year it gets harder.
  - Its getting much harder.. But I keep trying!
  - Finding new features to add to iKAT also becomes harder

- **Windows Group Policy + SRP Bypass**
  - Kiosk admins love to implement Windows group policy
    - "Command Prompt has been Disabled by your System administrator"
  - iKAT V features an extensive collection of "Unlocked" Windows binaries
    - cscript, cmd, osk, regedit, explorer, control, taskmgr, sc, wscript, runonce, rasphone.
  - Pre-patched Windows binaries which will not validate any local group policies
  - Modified to bypass SRP + App Locker rules (hash, certificate, file name)



- **iKAT has added MetaSploit Magic**
  - The iKAT server now hosts a dedicated Metasploit instance
  - Serving download_exec payloads which will run iKAT payloads

  - Dedicated “AutoPwn” Server
  - One Click – Shells.

  - Most Kiosks are shipping with unpatched browser libraries
  - Kiosks themselves are not patched
  - Metasploit Autopwn has a good rate of success.

- **File Reflection**
  - The iKAT server now services to help you compromise a Kiosk
  - “Send me content from a Kiosk via File Upload and iKAT will analyse it for you”
    - Windows Registry Files
    - Web Based Hex Editor
    - Cache Analyser

- **Ok, enough talking**
  - Lets hack some Kiosks.

- **Conclusions**
  - I am addicted to Kiosks
  - Hacking Kiosks is easy, enjoyable and creative
  - If you haven't done it before, try it.

  - If one guy from NZ can do this, just think what you can do.
  - Ideas, Comments? Please send me suggestions: Paul@ha.cked.net