KIOSK Hacking

Ideas of hacking kiosk machines is to improve the security of kiosks.

Prepared By: @souravbaghz

> ### Checklist:

▼ **Interrupting the Boot Process**

- □ What operating system is it running?
- □ Does the boot process allow keyboard input (assuming a keyboard is installed)? If yes then try entering into BIOS by key combination according to OS.
- □ Will the BIOS allow the kiosk to boot from an alternative media like a DVD or USB drive? This is only relevant if the ports on the kiosk are exposed.
- □ Does the kiosk automatically log into a user account? In the case of Windows holding down the SHIFT key will often disable the auto-login and potentially allow you to log into a different user account.

▼ **USB Interface**

- □ Check if USB is enabled, make your USB bootable using “Konboot.” This will give access to the file system directly without any Windows login.
- □ Check if USB is enabled, try to run unauthorized code (exe or batch file) directly from the USB or using the autorun feature of the USB.
- □ Check for keyboard emulations or keystroke injections.

▼ Keyboard

- □ Try to exit from kiosk mode with the help of hotkeys[Alt+F4 (close active window) and Win+Ctrl, Alt+Tab, and Alt+Shift+Tab (switch task)].
- □ Try pressing SHIFT key 5 times to get access to sticky-key feature.
- □ Check for high contrast mode (Left Alt-Left Shift-Print Screen) can render the kiosk nearly unusable if the user doesn't know how to disable them.

▼ Additional Applications & Dialog Box

- □ Check if the kiosk makes use of a web browser to display it's content and try clicking on links, email addresses or any to ensure if it gives you access to explore system files and web browser.

▼ Web Browser

- □ Browse the local file system (i.e. "C:")
- □ Check for browser version.
- □ Check for known vulnerabilities(CVEs) of identified browser version.
- □ Click on links for email addresses, phone numbers and PDF documents may launch other applications or dialog windows granting you access to the file system.
- □ Check other URLs and browser’s attribute https://github.com/souravbaghz/Att-URLs

▼ Watchdog

- □ Ensure that the kiosk application is always running and restart the kiosk application if it crashes. if you can find a way to crash the kiosk application you may find yourself sitting at the OS Desktop(Windows/Android).

▼ Network Interface[WIFI & Ethernet]

- □ Check if the kiosk is connected to any wireless Access Point.
- □ Scan the network for open ports and services.
- □ Does it connects to rogue access point with same SSID which it was connected previously[try after DeAuthentication attack].
- □ Analyze traffic for any sensitive data exposure.
- □ Check for ethernet port is exposed and accessible easily. If yes then perform network scan through the ethernet.

▼ **Business Logic & Error Handling**

- □ Put long characters in any input field to crash the application.
- □ Perform unusual actions to make application crash or generate error with sensitive info.