Owning Windows 8 with Human Interface Devices

Nikhil “SamratAshok” Mittal

EU SEC WEST

About Me

- SamratAshok
- Twitter - @nikhil_mitt
- Blog – http://labofapenetrationtester.blogspot.com
- Creator of Kautilya and Nishang
- Interested in Offensive Information Security, new attack vectors and methodologies to pwn systems.
- Previous Talks
  - Clubhack'10, Hackfest'11, Clubhack'11, Black hat Abu Dhabi'11, Black Hat Europe'12, Troopers'12, PHDays'12, Black Hat USA'12, RSA China'12

Overview

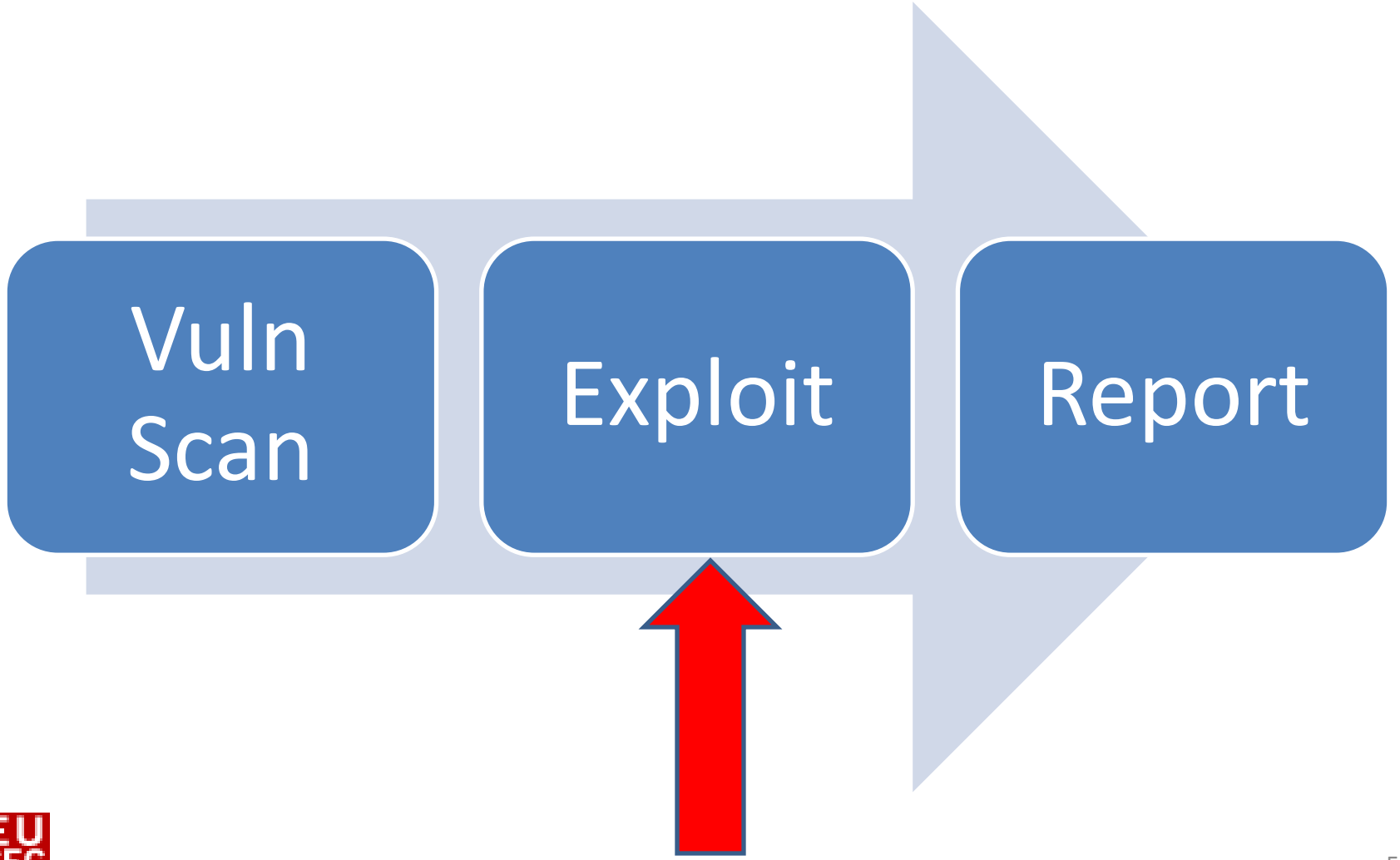
- A typical Penetration Test
- Using HIDs in Penetration Tests
- HID of choice – Teensy++
- Kautilya
- Windows 8
- Attacks Demo
- Comparison
- Limitation
- Defence
- Conclusion

EU SEC WEST

A typical Penetration Test

- A client engagement comes our way with some details.
- We need to complete the assignment in very restrictive time frame.
- Pressure is on us to deliver a “good” report with some high severity findings. (That “High” return inside a red colored box)

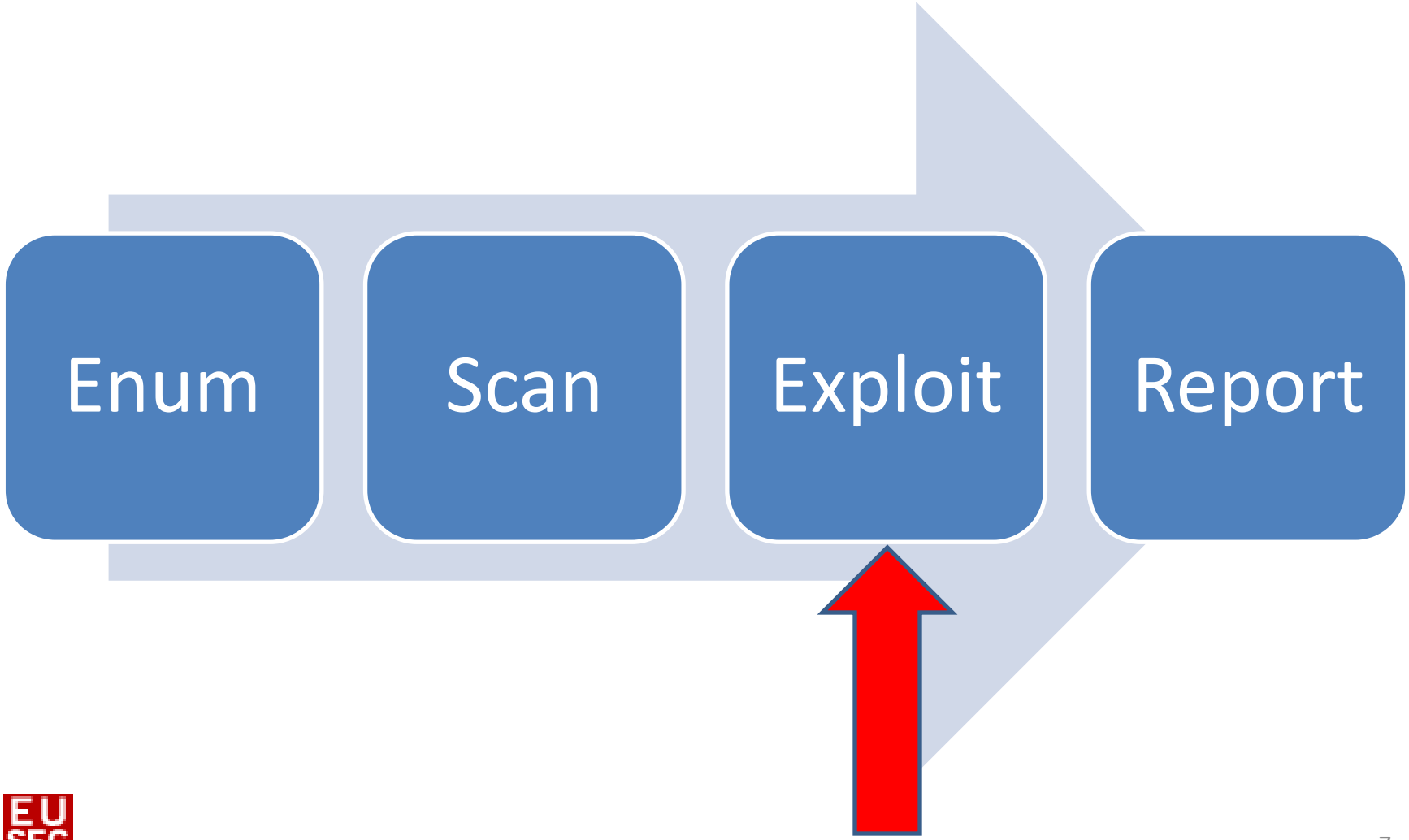
How the threats are Tested



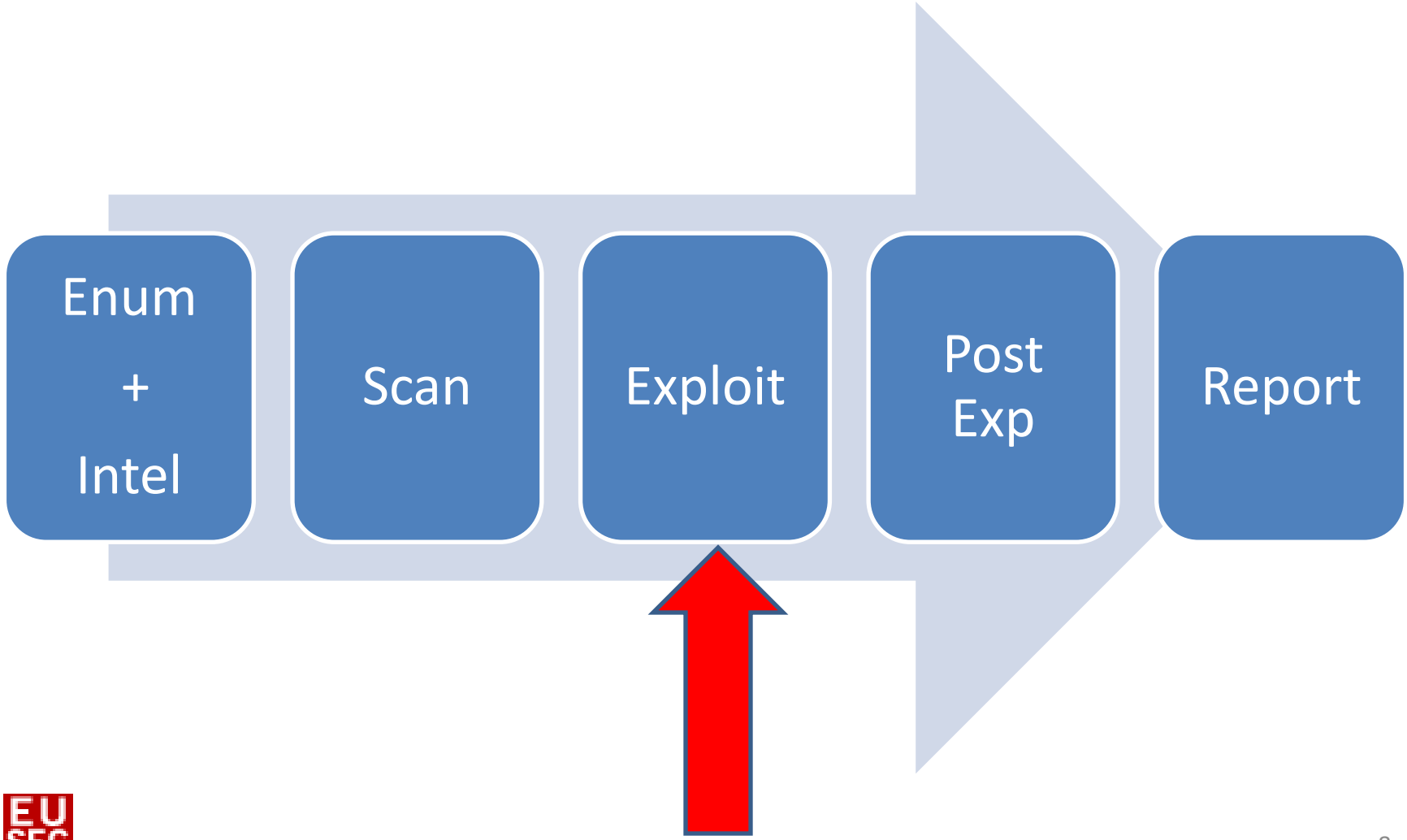
Best Scenario

- Previous one was a best case scenario.
- Only lucky ones find that.
- Generally legacy Enterprise Applications or Business Critical applications are not upgraded and are the first and easy targets.
- There is almost no fun doing it that way.

Some of us do it better



Some of us do it even better



Why do we need to exploit?

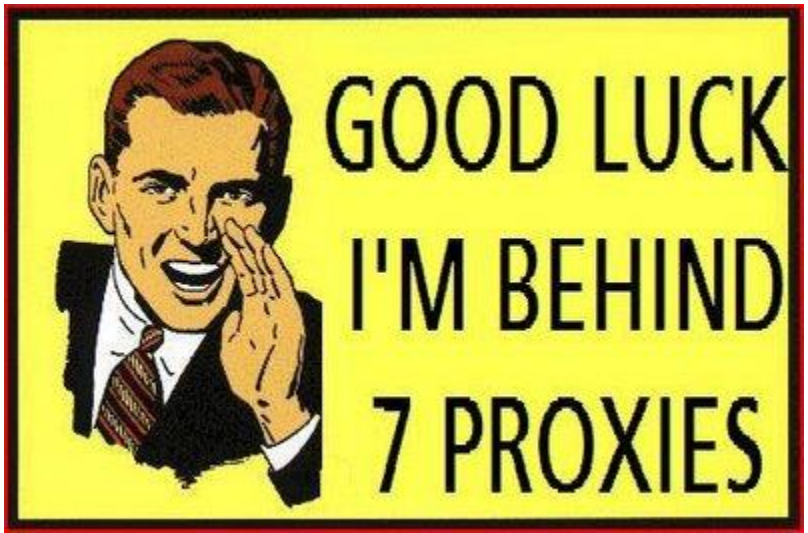
- To gain access to the systems.
- This shows the real threat to clients that we can actually make an impact on their business. No more “so-what” ☺
- We can create reports with “High” Severity findings which bring $$$

What do we exploit?

- Memory Corruption bugs.
  - Server side
  - Client Side
- Mis-configurations
- Open file shares.
- Sticky slips.
- Man In The Middle (many types)
- Unsecured Dumpsters
- Humans
- <Audience>

Worse Scenario

- Many times we get some vulnerabilities but can't exploit.
  - No public exploits available.
  - Not allowed on the system.
  - Countermeasure blocking it.
  - Exploit completed but no session was generated :P



http://goo.gl/NdvE3

Worst Scenario

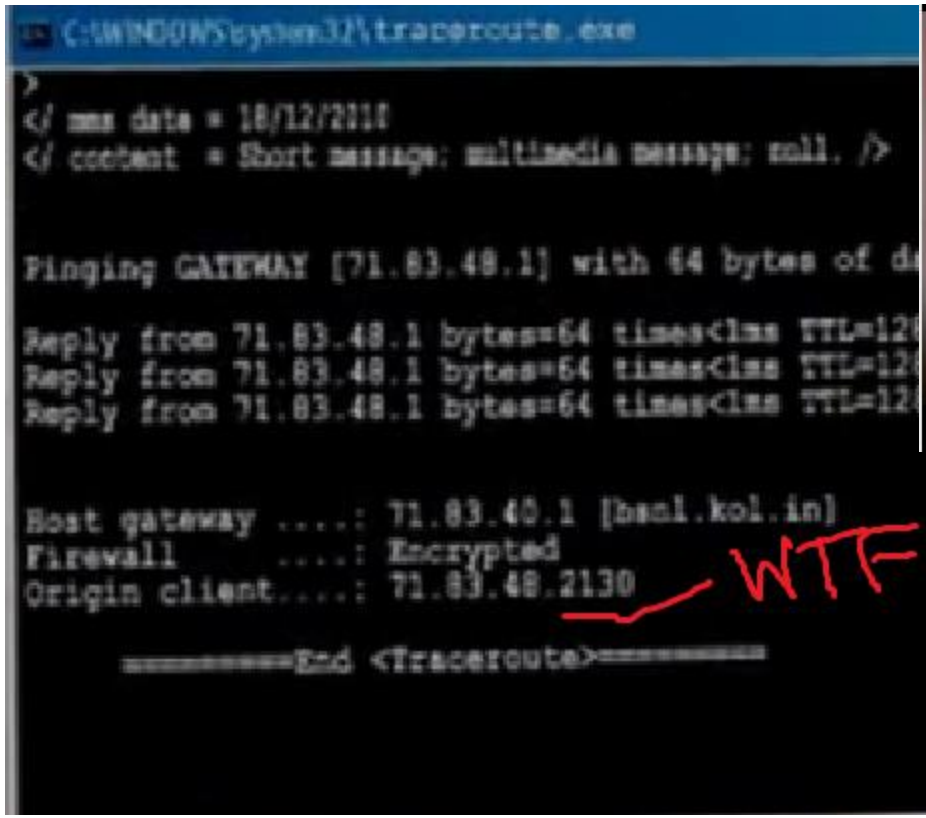
- Hardened Systems
- Patches in place
- Countermeasures blocking scans and exploits
- Security incident team monitoring and blocking attacks.
- No network access

- We need alternatives.

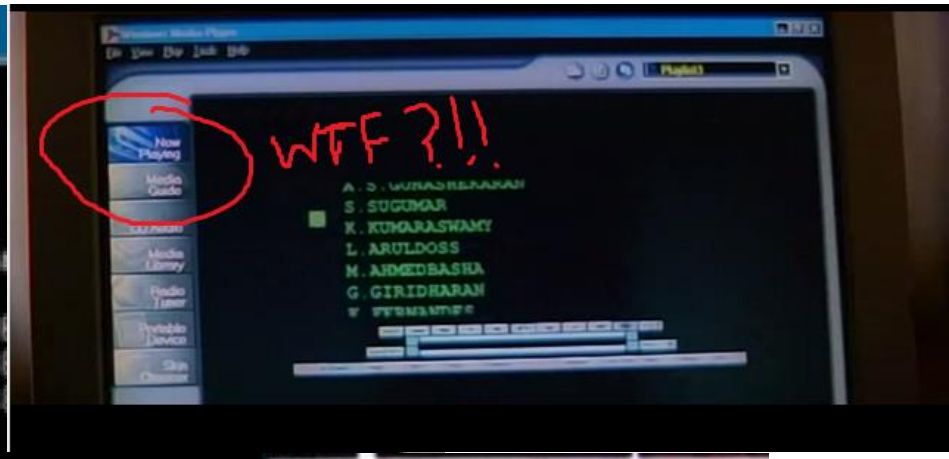
Need for new methods to break into systems

- Breaking into systems is not as easy as done in the movies.
- Those defending the systems have become smarter (at many places :P) and it is getting harder to break into “secured” environments.
- Everyone is breaking into systems using the older ways, you need new ways to do it better.

Best Alternatives



http://goo.gl/bkUWG



http://goo.gl/8LpoL

HID anyone?

- Wikipedia – "*A human interface device or HID is a type of computer device that interacts directly with, and most often takes input from, humans and may deliver output to humans.*"
- Mice, Keyboards and Joysticks are most common HID.
- What could go wrong?

http://goo.gl/uniYB

HID of Choice – Teensy++

- A USB Micro-controller device.
- Storage of about 130 KB.
- We will use Teensy ++ which is a better version of Teensy.
- Available for $24 from pjrc.com
- Can be used as a Keyboard, mouse and much more.

From pjrc.com

Key Features:

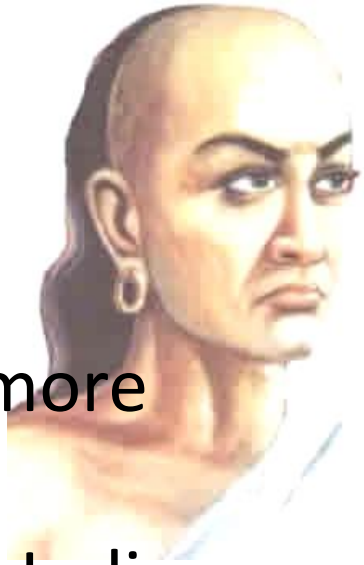
- USB can be any type of device
- AVR processor, 16 MHz
- Single pushbutton programming
- Easy to use Teensy Loader application
- Free software development tools
- Works with Mac OS X, Linux & Windows
- Tiny size, perfect for many projects
- Available with pins for solderless breadboard
- Very low cost & low cost shipping options

Specification	Teensy 2.0	Teensy++ 2.0
Processor	ATMEGA32U4	AT90USB1286
Flash Memory	32256	130048
RAM Memory	2560	8192
EEPROM	1024	4096
I/O	25	46
Analog In	12	8
PWM	7	9
UART,I2C,SPI	1,1,1	1,1,1
Price	$16	$24

How we will use Teensy?

- As a programmable keyboard.
- We will program the device to do a defined set of activities when it is connected to a system.
- We will utilise the privileges of the currently logged in user and any higher privileges accessible to the user.
- Aim is to mimic a user sitting in front of the target.

Kautilya



- It’s a toolkit which aims to make Teensy more useful in Penetration Tests.
- Named after Chanakya a.k.a. Kautilya, an Indian Teacher, Strategist and Politician (370-283 BC)
- Written in Ruby.
- It’s a menu drive program which let users select and customize payloads.
- Aims to make Teensy part of every Penetration tester’s tool chest.

Windows 8

- Latest in Desktop family of Windows.
- Got praise for improved security in numerous tech articles and researches.
- Some fantastic research was presented at BHUS'12 "Windows 8 Heap Internals" by Chris Valasek and Tarjei Mandt.
- What will happen to our Pen Tests?

http://goo.gl/4xr81

Windows 8

- What about HIDs?
- Are there any improvements how Windows 8 handle HID input?
- Doesn’t seem so :)

Payloads and Demo

- Payloads are written for teensy without SD Card.
- Pastebin is extensively used. Both for uploads and downloads.
- Payloads are commands, powershell scripts or combination of both.
- Payload execution of course depends on privilege of user logged in when Teensy is plugged in.

Limitations with Teensy

- Limited storage in Teensy. Resolved if you attach a SD card with Teensy.
- Inability to “read” from the system. You have to assume the responses of victim OS and there is only one way traffic.
- Target system should be unlocked.

Limitations with Kautilya

- Many payloads need Administrative privilege.
- Lots of traffic to and from pastebin.
- Inability to clear itself after a single run.
- For payloads which use executables you manually need to convert and host them.

Defence

- Use the Group Policy to “Prevent Installation of Removable Devices”.
- Physically lock the USB ports.

Thank You

- Questions?
- Insults?
- Feedback?
- Kautilya is available at http://code.google.com/p/kautilya/
- Follow me @nikhil_mitt
- http://labofapenetrationtester.blogspot.com/