Kautilya: Teensy beyond shell

Nikhil Mittal (SamratAshok)

About Me

- SamratAshok
- Twitter – @nikhil_mitt
- I am interested in Offensive Information Security, new attack vectors and methodologies to pwn systems.
- Previous Talks
  - Compromising a highly secure environment Clubhack’10
  - Here are your keystrokes Hackfest’11
  - Compromising a highly secure environment part 2 Clubhack’11

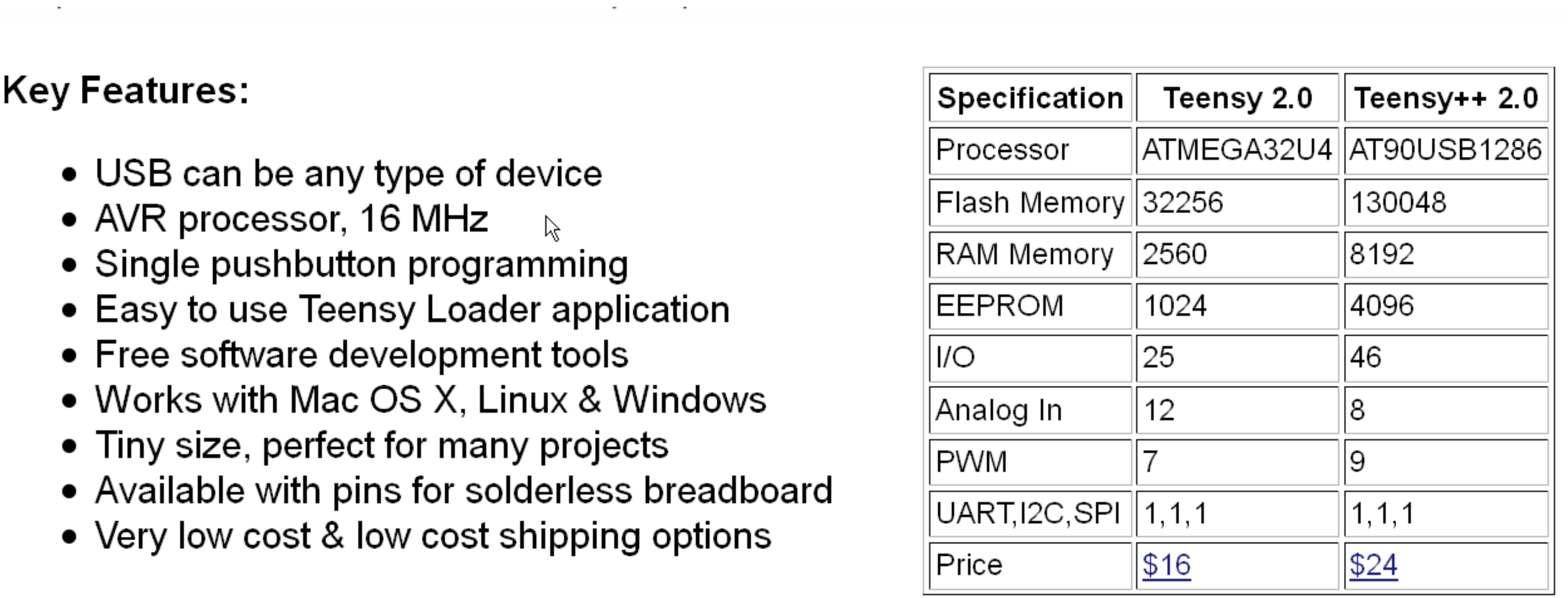
Overview

- Teensy
- Current usage of Teensy
- What else can be done using Teensy
- Kautilya
- Payloads in Kautilya
- Current state of pentesting
- Pen Test Stories
- Limitations
- Future
- Conclusion

About Teensy

- A USB Micro-controller device.
- Storage of about 130 KB.
- Introduced to hackers by Irongeek at Defcon 18.
- We will use Teensy ++ which is a better version of Teensy.
- Available for $24 from pjrc.com

From pjrc.com



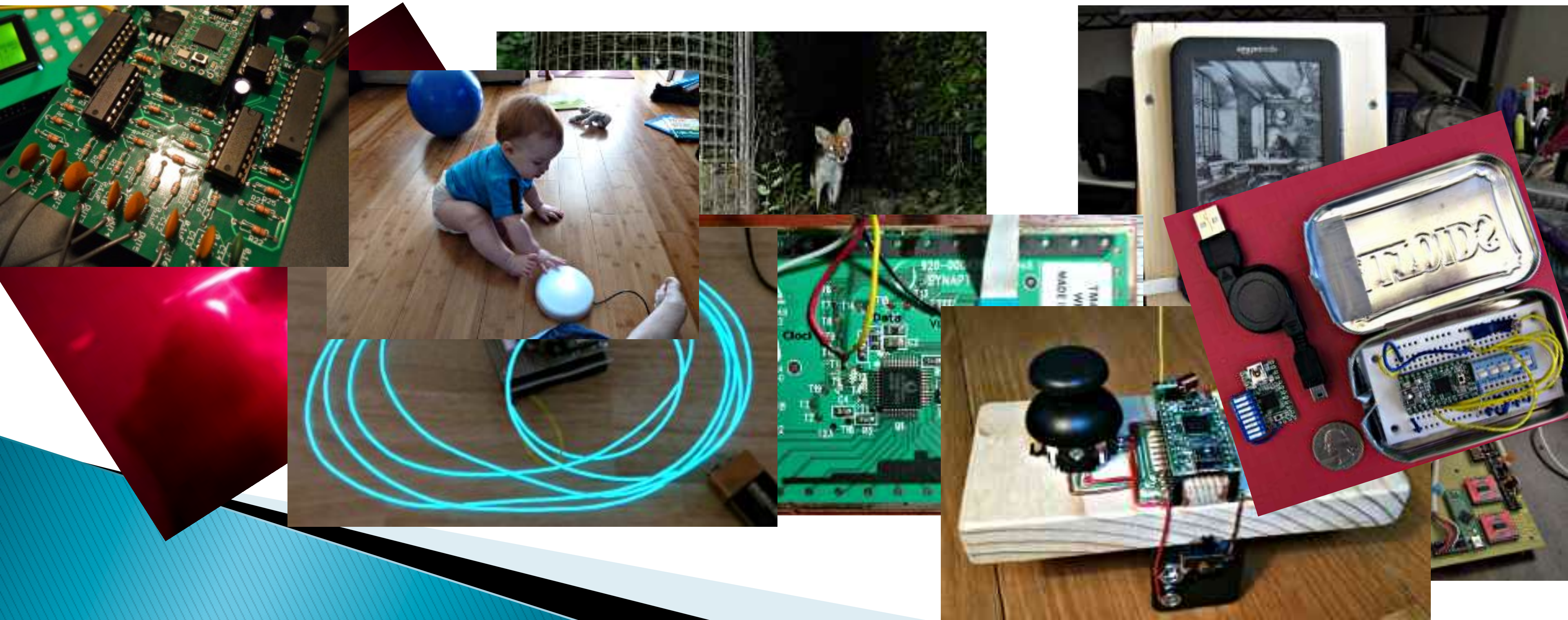
Key Features:

- 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

Current usage of Teensy

- http://www.pjrc.com/teensy/projects.html
- Really cool projects.
- Please do not compare my code with any of the above. I am a new kid in the town ☺



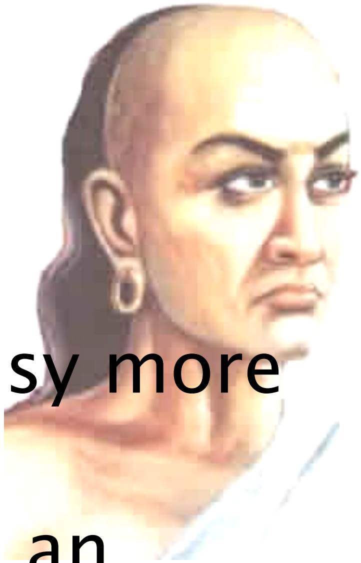
Current usage of Teensy

- Arduino-Based Attack Vector in Social Engineering Toolkit (SET) by ReL1K.
- Contains really awesome payloads.
- Great for popping shells.
- Homemade Hardware keylogger by Irongeek

What else can be done using Teensy

- Teensy can be used for many tasks in a Penetration Test.
- It can be used for information gathering, pre-exploitation, exploitation and post-exploitation tasks.
- If you know victim OS well, almost anything can be done using Teensy.

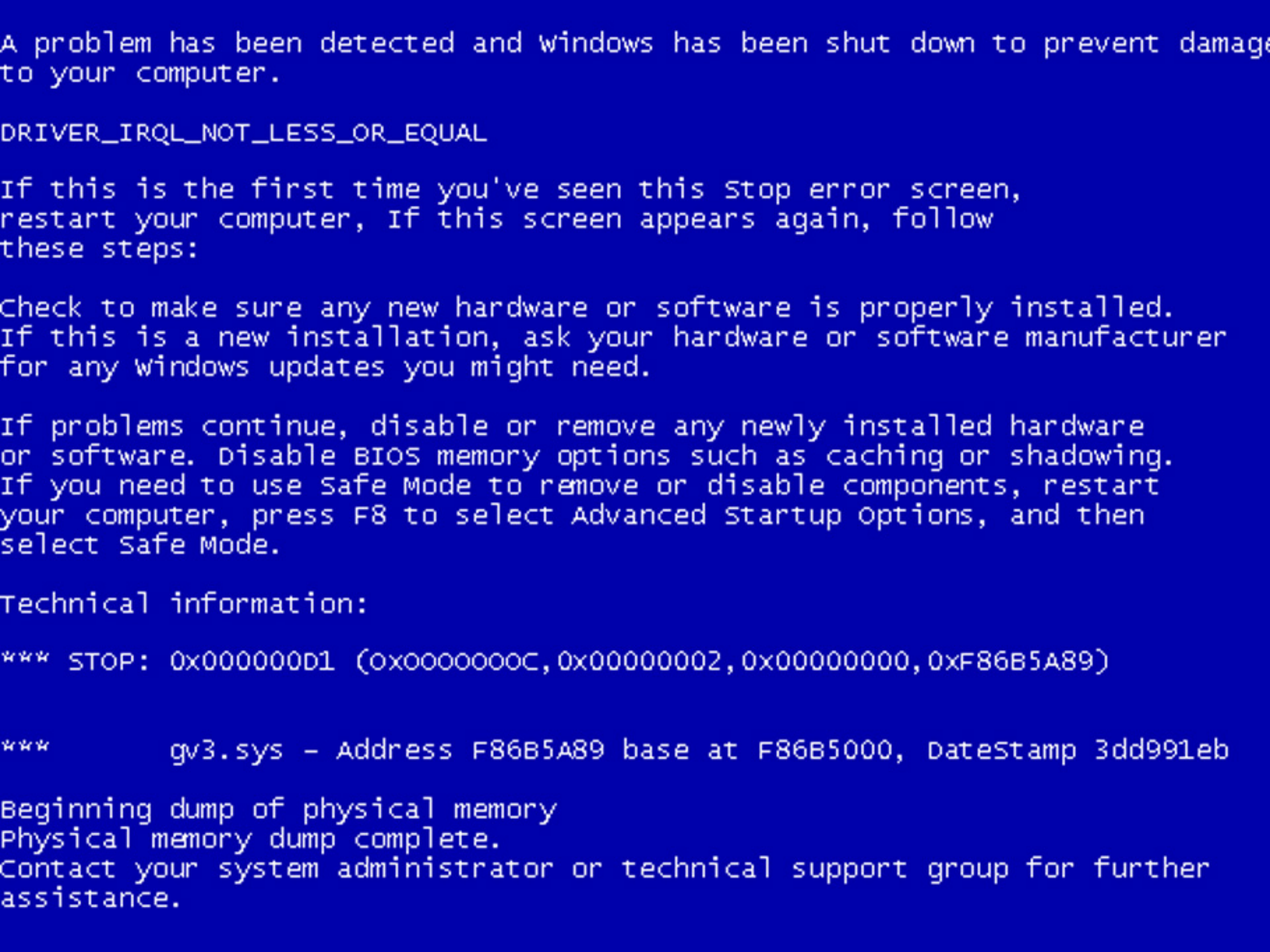
Kautilya



- It’s a toolkit which aims to make Teensy more useful in Penetration Tests.
- Named after Chanakya a.k.a. Kautilya, an Indian Teacher and Politician (370–283 BC)
- Written in Ruby.
- It’s a menu drive program which let users select and customize payloads.
- Payloads are mostly for Windows as the victim of choice generally is a Windows machine. ☺

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.



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer, If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)


***       gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

Windows User Add

- Adds a user with Administrative privileges on the victim.
- Uses net user command.

Default DNS

- Changes the default DNS for a connection.
- Utilizes the netsh command.

Edit Hosts File

- Edit hosts file to resolve a domain locally.

Enable RDP

- Enables RDP on victim machine.
- Starts the service.
- Adds exception to Windows firewall.
- Adds a user to Administrators group.

Enable Telnet

- Installs Telnet on victim machine.
- Starts the service.
- Adds exception to Windows firewall.
- Adds a user to Administrators group and Telnetclients group..

Forceful Browsing

- Adds user defined website as secondary home page to Internet Explorer.
- As an attempt to keep it stealthy, the home page is set to Microsoft website.

Download and Execute

- Downloads an exe in text format from pastebin, converts it back to exe and executes it.

Sethc and Utilman backdoor

- Using registry hacks, calls user defined executable or command when Shift is pressed 5 times or Win + U is pressed.
- When the system is locked, the called exe is executed in System context.

Uninstall Application

- Uninstalls an msiexec application silently.

Information Gather

- Dumps valuable information from registry, net command and hosts file.

Tweet

- Tweets a text using user define Twitter username and password.
- This payload is visible i.e. it works on browser windows not on command line.

Hashdump

- This payload pulls powerdump script of msf from pastebin, schedules it as taks to run in system context and upload the hashes to pastebin.

Code Execution

- This payload pulls the code execution script (as on exploit-Monday blog) and executes it on the victim.

Keylogging

- This payload logs keys and pastes it to pastebin every twenty seconds.
- There is a separate script to parse the output.

Sniffer

- This payload pulls the sniffer (as by Robbie Fost) and executes it on the victim.
- The output is compressed and uploaded to ftp.

Chrome RDP

- This payload uses opens up chrome, launches Remote Desktop plugin, enters credentials and copies the access key to pastebin.
- This payload operates on browser window.

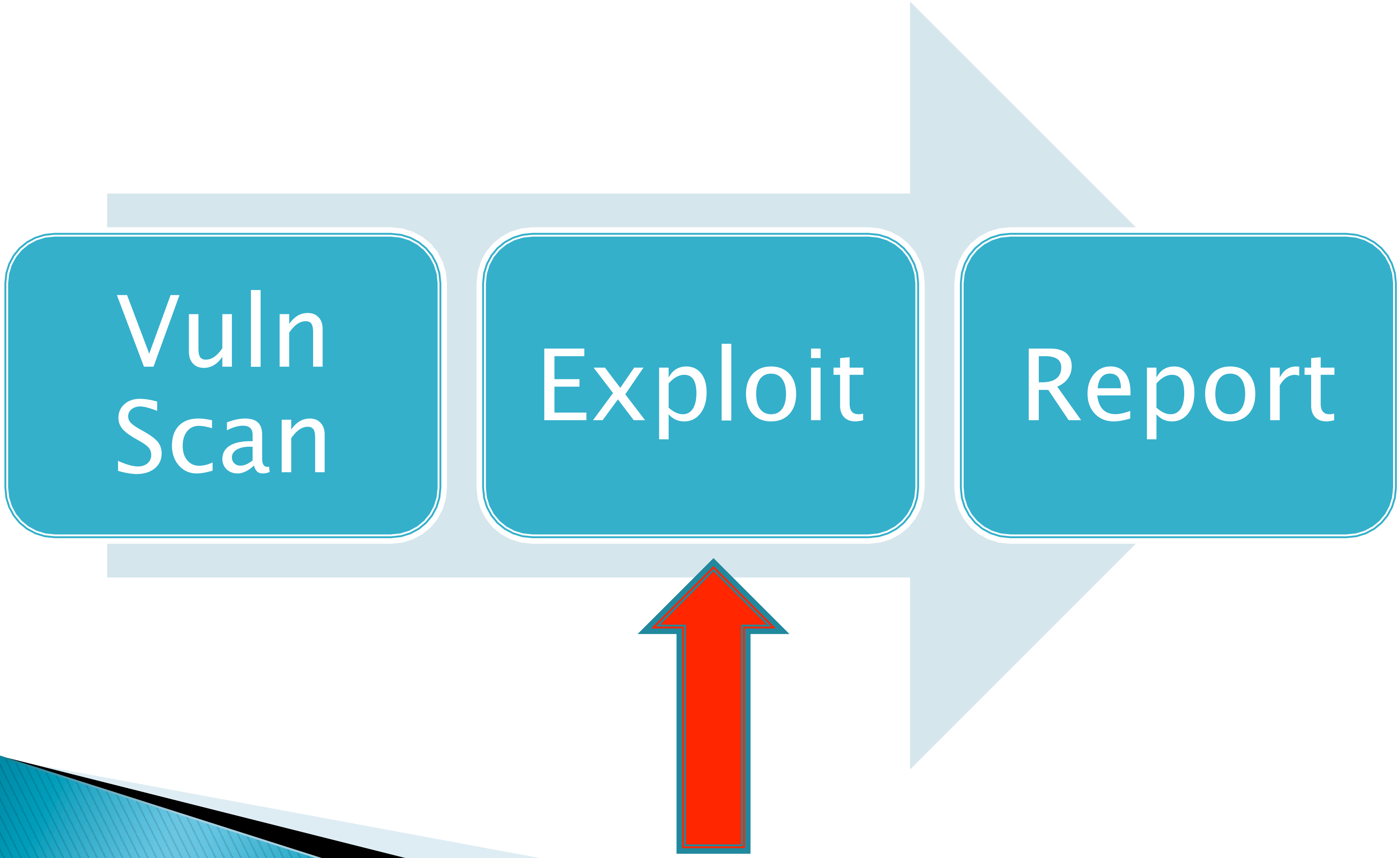
Wireless Rogue AP

- This payload creates a hosted network with user define SSID and key.
- It also adds a user to Administrators and TelnetClients group.
- It installs and starts telnet and adds it to windows firewall exception.

A typical Pen Test Scenario

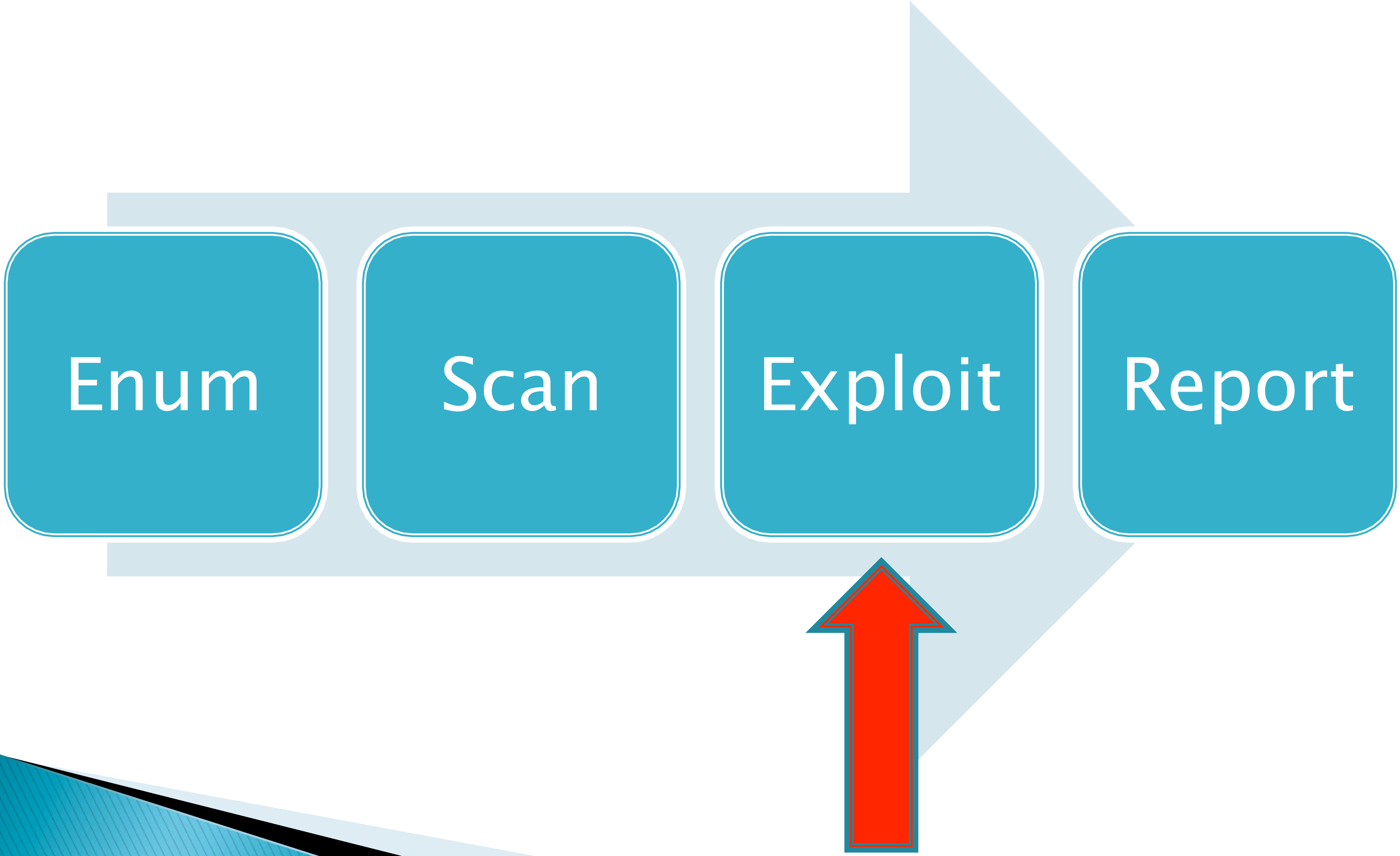
- A client engagement comes with IP addresses.
- We need to complete the assignment in very restrictive time frame.
- Pressure is on us to deliver a “good” report with some high severity findings. (That “High” return inside a red colored box)

Current State of Pentesting



- This is a best case scenario.
- Only lucky ones find that.
- Generally legacy Enterprise Applications or Business Critical applications are not upgraded.
- There is almost no fun doing it that way.

Some of us do it better



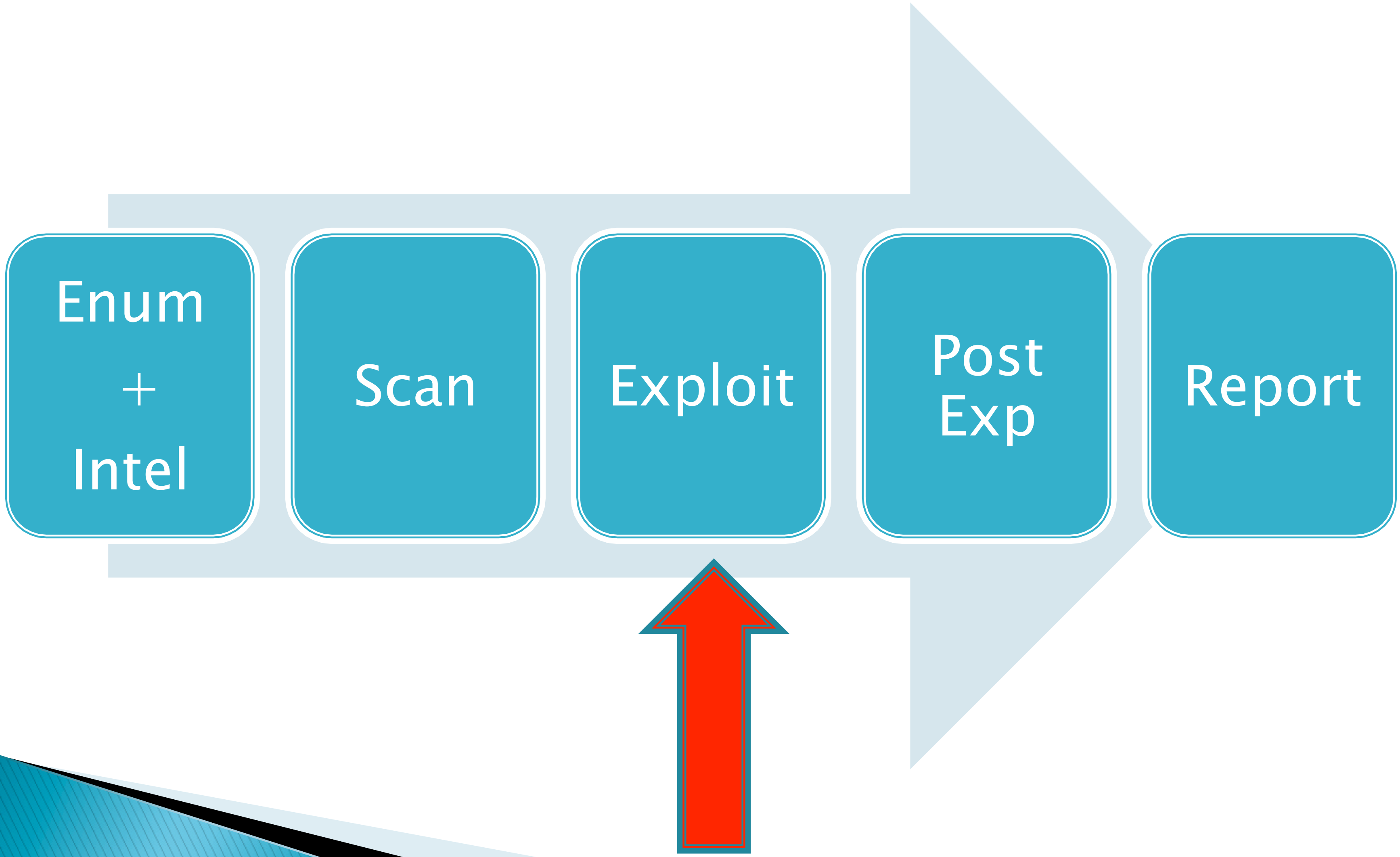
Enum

Scan

Exploit

Report

Some of us do it even better



Enum + Intel

Scan

Exploit

Post Exp

Report

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.

What do we exploit?

- Memory Corruption bugs.
  - Server side
  - Client Side
- Humans
- Mis-configurations

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

Worst Scenario

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

Alternatives

- Open file shares.
- Sticky slips.
- Social Engineering attacks.
- Man In The Middle (many types)
- SMB Relay
- Dumpster Diving

Best Alternative

Rajnikant > Chuck Norris

Pen Test Stories
Library Fun

- We were doing internal PT for a large media house.
- The access to network was quite restrictive.
- The desktops at Library were left unattended many times.
- Teensy was plugged into one system with a sethc and utilman backdoor.
- Later in the evening the system was accessed and pwnage ensued.

Pen Test Stories
Breaking the perimeter

- A telecom company.
- We had to do perimeter check for the firm.
- The Wireless rogue AP payload was used and teensy was sold to the clients employees during lunch hours.
- Within couple of hours, we got a wireless network with a administrative user and telnet ready.

Pen Test Stories
Help by the Helpdesk

- A pharma company.
- We replaced a user's data card with a Teensy inside the data card's cover.
- The payload selected was Keylogger.
- "Data card" obviously didn't worked and we got multiple keylogging for the user and the helpdesk.
- Helpdesk guys had access to almost everything in the environment and over a workday, it was over.

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.

Limitations with Kautilya

- Many payloads need Administrative privilege.
- Lots of traffic to and from pastebin.
- Inability to clear itself after a single run.
- Not very reliable as it is a new tool and has not gone through user tests.
- For payloads which use executables you manually need to convert and paste them to pastebin.

Future

- Improvement in current payloads.
- Implementation of SD card.
- Use some payloads as libraries so that they can be reused.
- Implementation of payloads from SET.
- Support for Non-English keyboards.
- Maybe more Linux payloads.
- Implementation of some new payloads which are under development.

Thanks To

- Irongeek for introducing this device at Defcon 18
- David Kennedy for implementing this in Social Engineering Toolkit.
- Stackoverflow and MSDN for code samples and answers.
- Matt from Exploit-Monday for really useful blog.
- pjrc.com for this great device.

Thank You

- Questions