



More fun using Kautilya

or

Is it a thumb drive? Is it a toy? No,
it's a keyboard

Nikhil Mittal (SamratAshok)

About Me

- SamratAshok
- Twitter - @nikhil_mitt
- Blog – <http://labofapenetrationtester.blogspot.com>
- Creator of Kautilya
- 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
- Upcoming Talks
 - Hack In Paris'12, PHDays'12, Training at GrrCON'12

Overview

- A Typical Pen Test scenario
- Current state of pentesting
- Why do we need new methods to break into systems
- The Thumb Drive
- The Toy
- The Keyboard
- Kautilya
- (New and Shiny) Payloads in Kautilya
- Limitations
- Future
- Conclusion

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

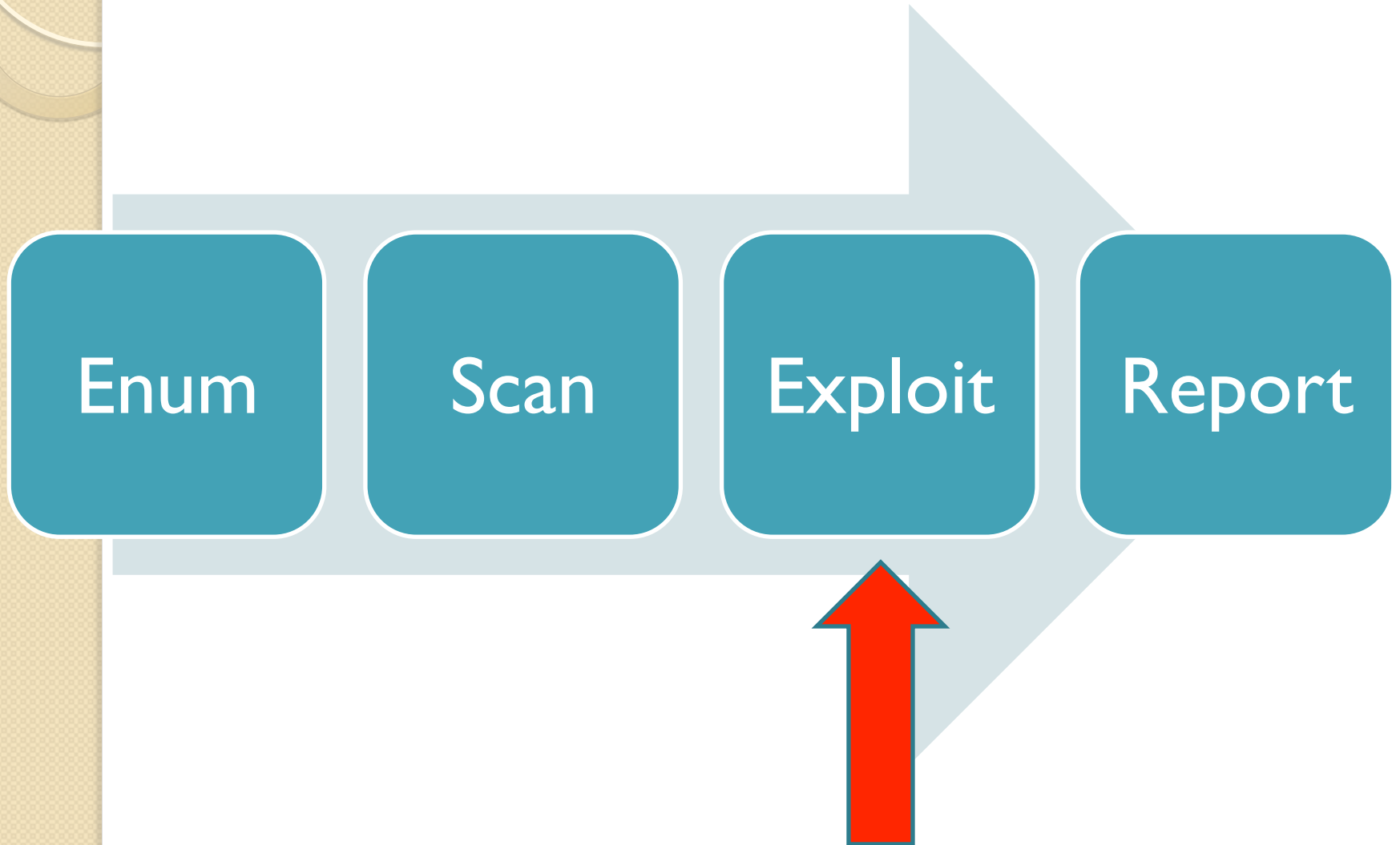
Vuln
Scan

Exploit

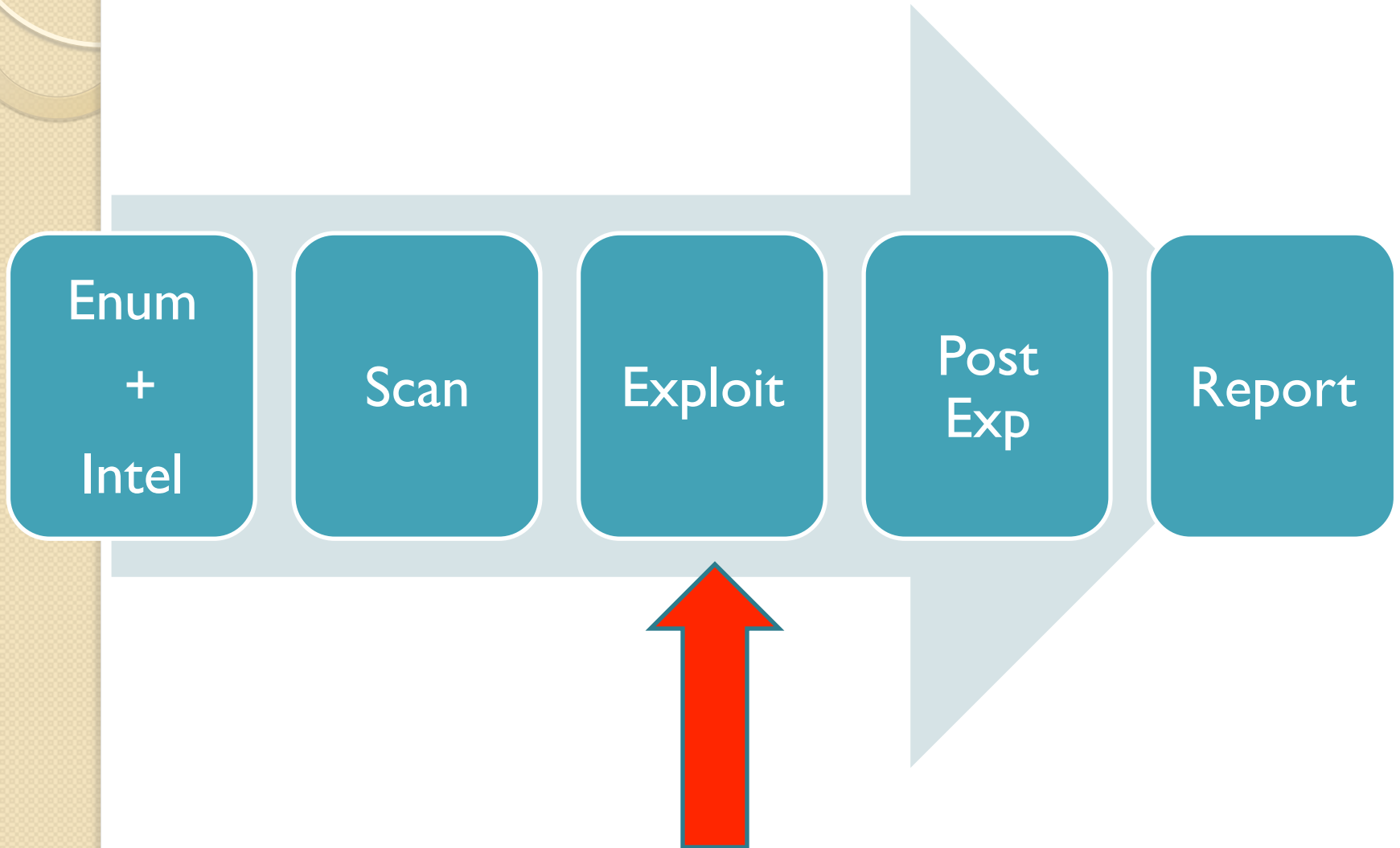
Report

- 
- This is a best case scenario.
 - Only lucky ones find that.
 - There is almost no fun doing it that way.

Some of us do it better



Some of us do it even better



What do we exploit?

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

Why do we need new methods to break into systems?

- 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.

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

- We need alternatives...

Best Alternative



Rajnikant > Chuck Norris



The Thumb Drive

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

The USB Toy

- A financial service company.
- Cute USB dolls were left on many girls' desks ;)
- Next day almost all of them connected that happily to their systems, the toy didn't work for them but for us it was a meterpreter session ready for more pwnage.

No one discovered what it really was



The Keyboard

- 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

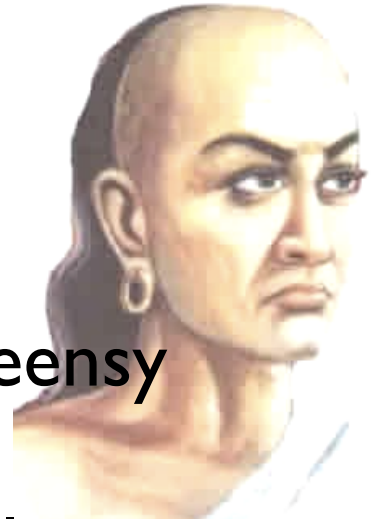
Specification	Teensy 2.0	Teensy++ 2.0
Processor	ATMEGA32U4	AT90USB1286
Flash Memory	32256	130048
RAM Memory	2560	8192
EEPROM	1024	4096
I/O	25	46
Analog In	12	8
PWM	7	9
UART,I2C,SPI	1,1,1	1,1,1
Price	\$16	\$24

What 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, 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.



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.



Linux Payloads



Windows Payloads

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.
- Support for Non-English keyboards.
- Maybe more Linux payloads.
- Implementation of some new payloads which are under development.

Thanks To

- Troopers crew for allowing me to speak here.
- Stackoverflow and MSDN for code samples and answers.
- pjrc.com for this great device.

Thank You

- Questions?
- Insults?
- Feedback?

- Kautilya will be available at <http://code.google.com/p/kautilya/>
- Follow me @nikhil_mitt
- <http://labofapenetrationtester.blogspot.com/>