PIPEREVSKI
& ASSOCIATES

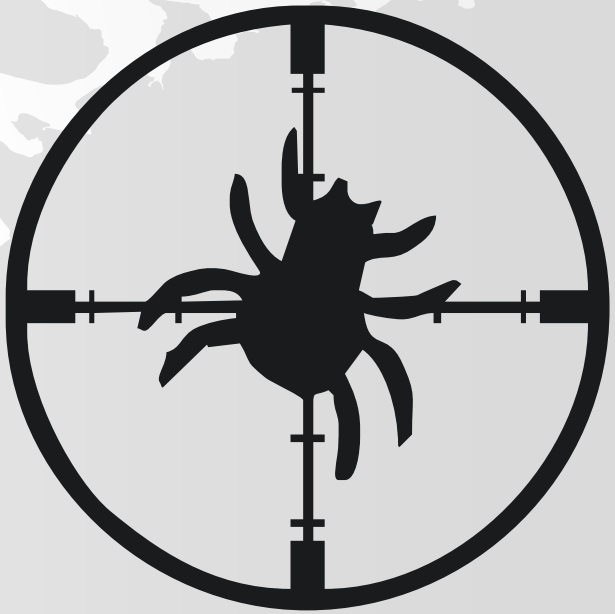
at

BalCCon2k17

U CNT CTRL ME

BalCCon2k17

PIPEREVSKI
& ASSOCIATES

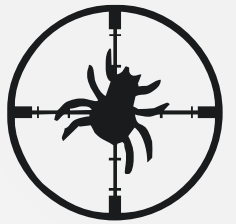


METHODOLOGY FOR VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT

Presenter m-r Mane Piperevski

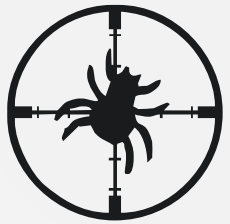
BalCCon2k17 Novi Sad, Serbia 2017

PIPEREVSKI
& ASSOCIATES



WORLD OF BUGS

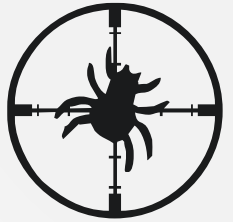
PIPEREVSKI
& ASSOCIATES



HOW DIFFICULT IS VULNERABILITY RESEARCH?

1. Learning used technology
2. Learning hacking tools and techniques
3. Choosing the right approach method
4. Found one … What next???
5. How much money will I earn?
6. How much money should I spend?

PIPEREVSKI
& ASSOCIATES

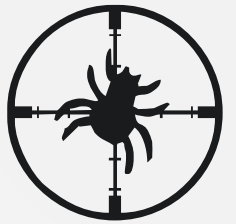


HOW DIFFICULT IS VULNERABILITY RESEARCH?

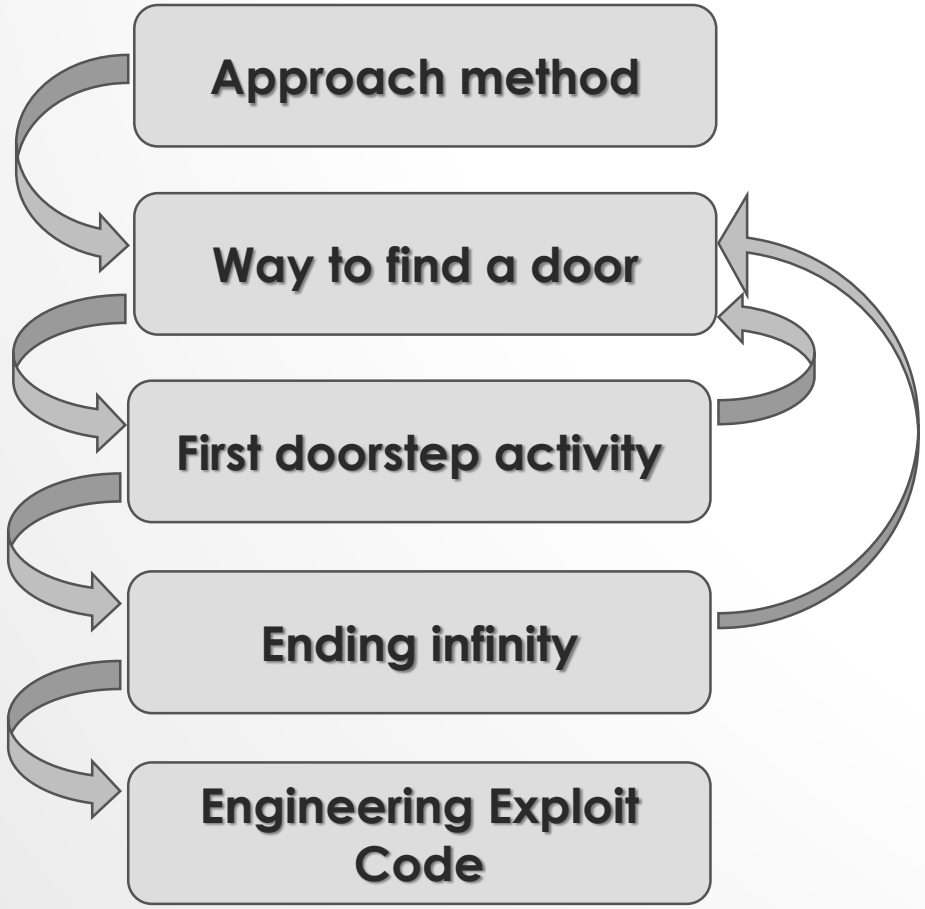
All Things are
Difficult

Before they are
Easy

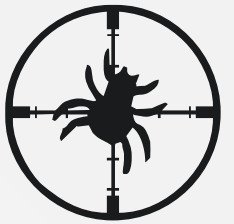
PIPEREVSKI
& ASSOCIATES



METHODOLOGY FOR VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT

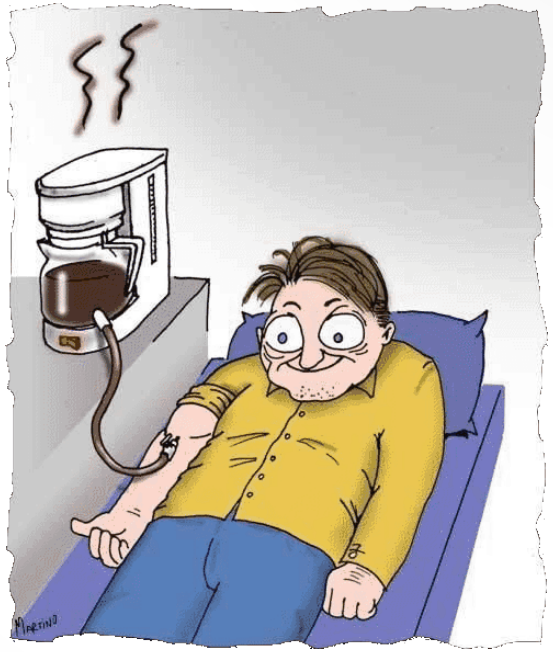


PIPEREVSKI
& ASSOCIATES

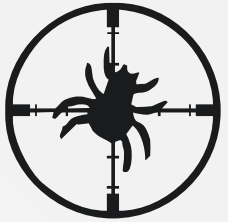


METHODOLOGY FOR VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT

Don’t forget to do this before you begin



PIPEREVSKI
& ASSOCIATES



METHODOLOGY PHASE 1
APPROACH METHOD

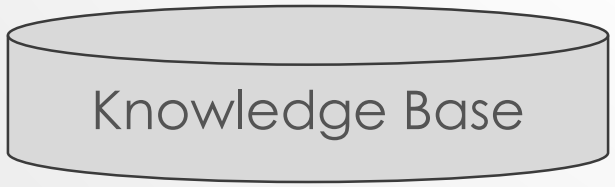
Vendor dependent

Automated testing

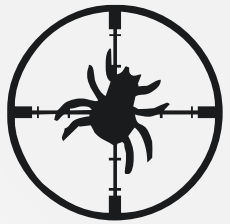
- Loud
- Detectable
- Non Efficient

Manual testing

- Quiet
- Intelligent
- Time Consuming



PIPEREVSKI
& ASSOCIATES



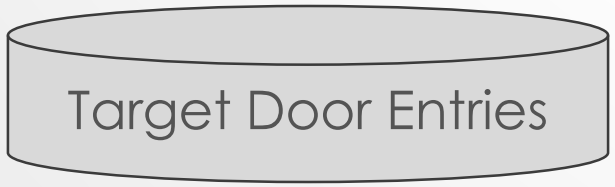
METHODOLOGY PHASE 2
WAY TO FIND A DOOR

If possible, try them all

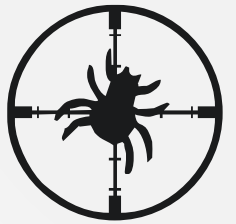
Enumeration
- Discover Inputs
- Discover Activities
- Discover the Surface

Thinking
- Business Process Overview
- Identify hidden opportunities

Diffing
- Identify differences
- Discover how they differ
- Time Consuming



PIPEREVSKI
& ASSOCIATES



METHODOLOGY PHASE 3
FIRST DOORSTEP ACTIVITY

If applicable, try them all

Bruteforce
- Use of Fuzzing
- Easily Detectable
- Inefficient on Production Env.

Hapax
- Unique Activity
- It can be done only once
- Related with business logic

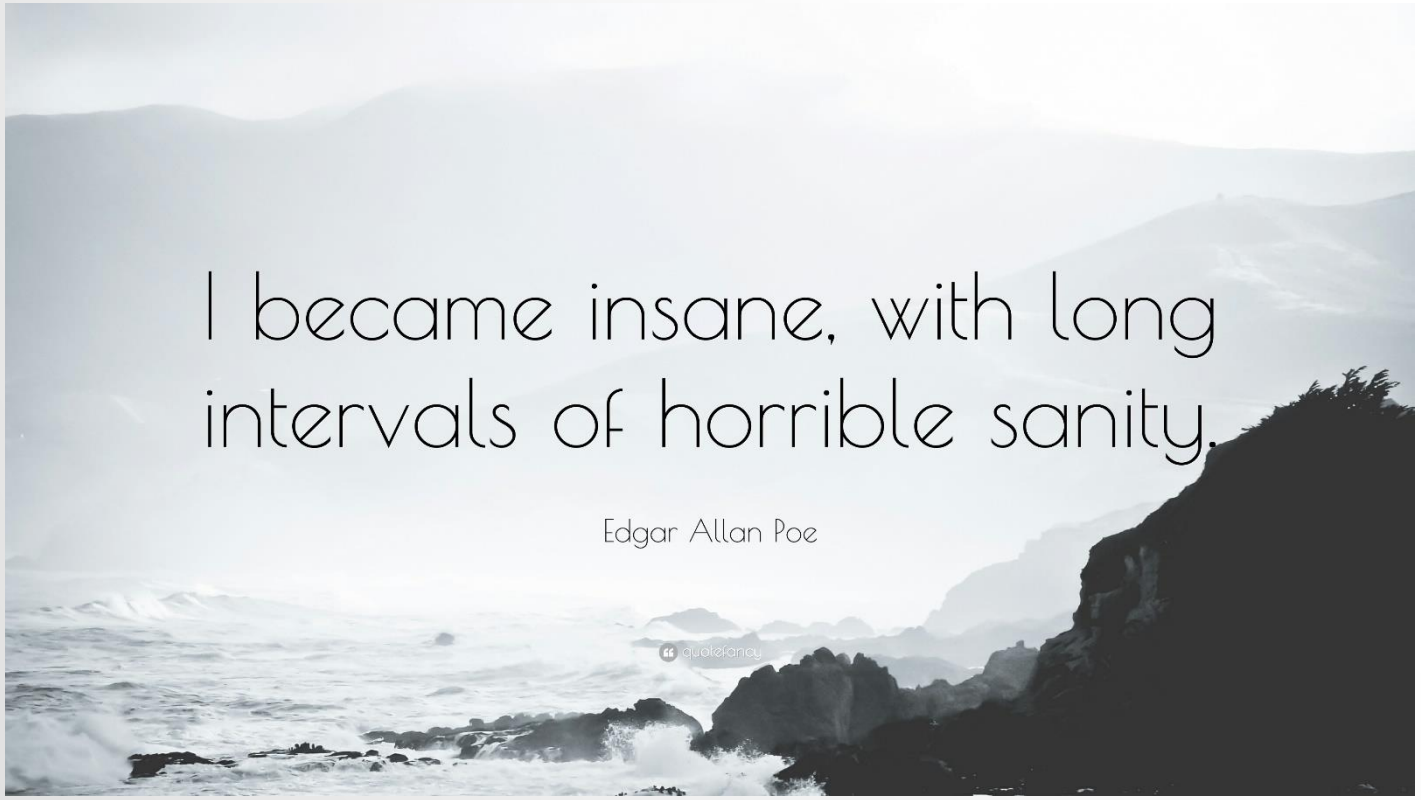
Incantation
- Predefined set of activities
- Smart Fuzzing
- Related with business logic

Target Door Entries
Tested without outcome

Discovered
Vulnerabilities

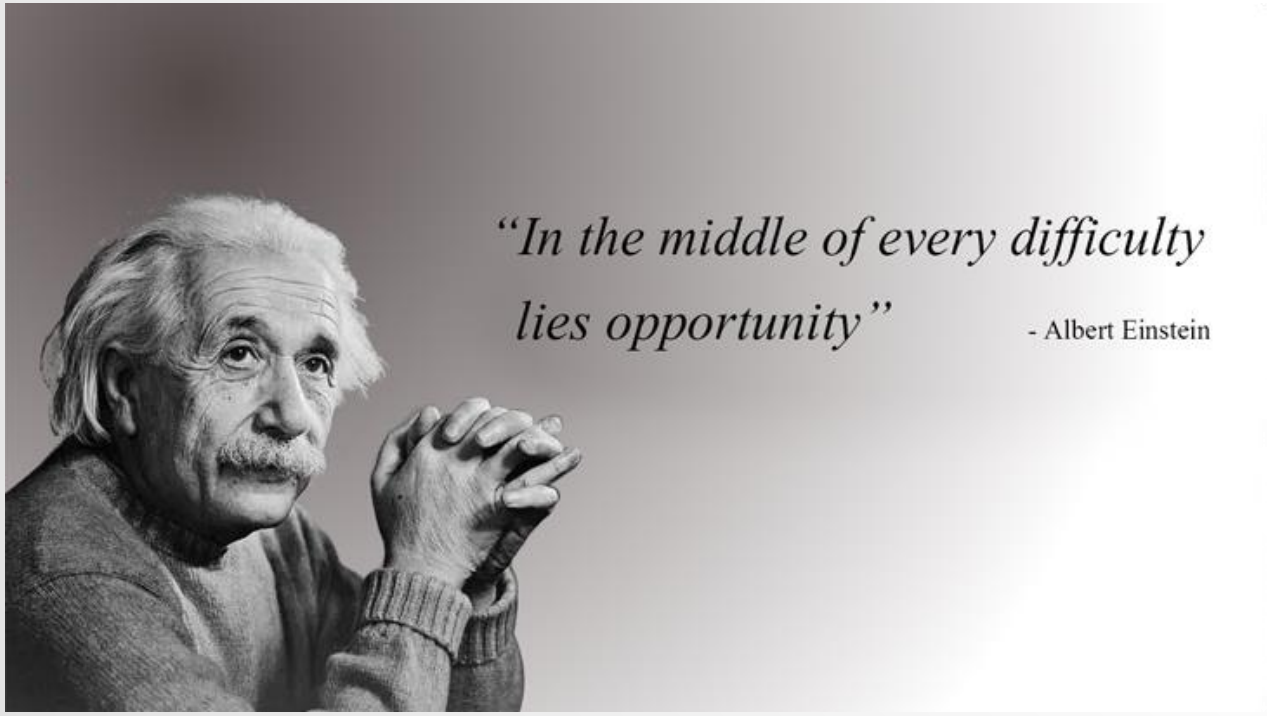
PIPEREVSKI
& ASSOCIATES

METHODOLOGY PHASE 3
FIRST DOORSTEP ACTIVITY

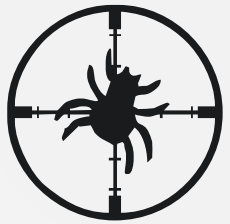


PIPEREVSKI
& ASSOCIATES

METHODOLOGY PHASE 3
FIRST DOORSTEP ACTIVITY



PIPEREVSKI
& ASSOCIATES

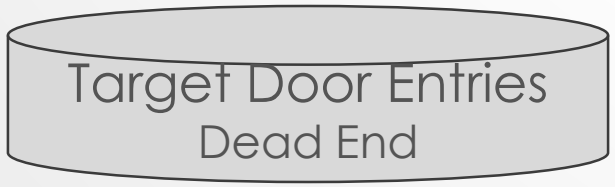


METHODOLOGY PHASE 4
ENDING INFINITY

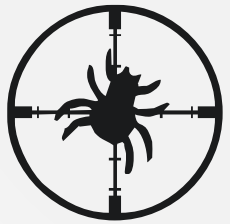
Lucky choice

Bonanza
- Time Solve Problem
- Look from Different Point
- New Ideas/Techniques

Breakdown
- Review the Logic
- Make Mind Map
- Repeat previous steps again



PIPEREVSKI
& ASSOCIATES



METHODOLOGY PHASE 5
ENGINEERING EXPLOIT CODE

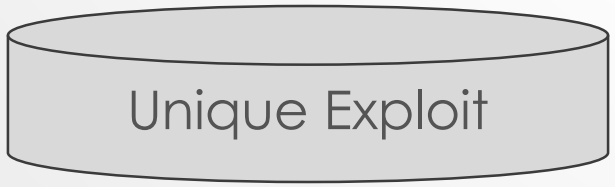
Depends on the goal

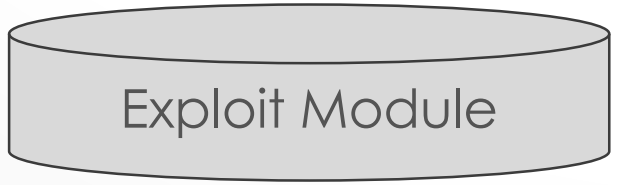
Totum
meaning
totally

- Develop from scratch
- Custom modules
- Opportunity to sell it

Pars
meaning
partly

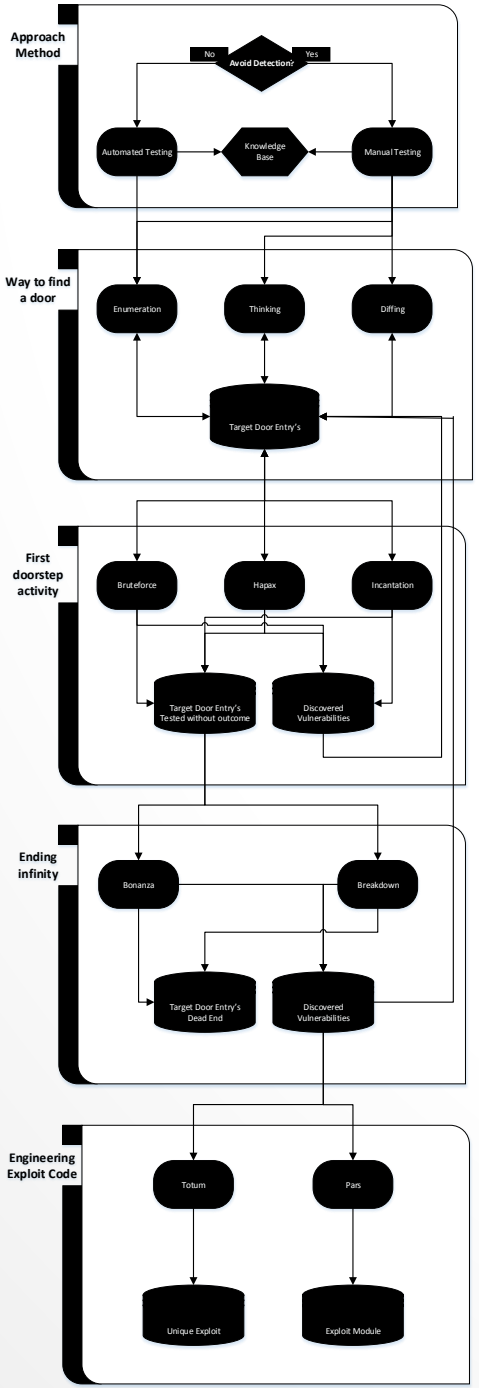
- Use of Metasploit
- Proof of concept
- Short time to build



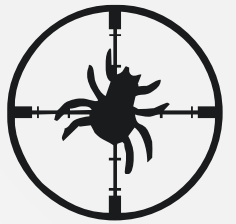


PIPEREVSKI
& ASSOCIATES

DIAGRAM VIEW

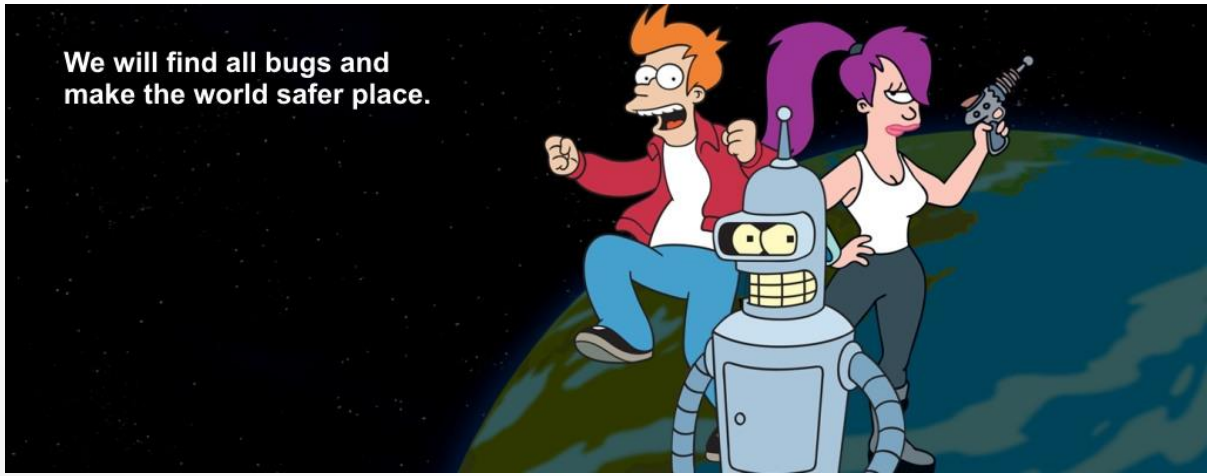


PIPEREVSKI
& ASSOCIATES

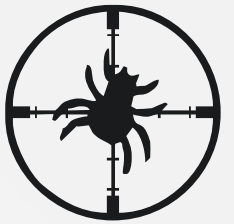


FUTURE DEVELOPMENT AND VISION

- Building testing guide for every element
- Create multiple practical examples
- Create OWASP project
  - Vulnerability Research and Exploit Development Methodology

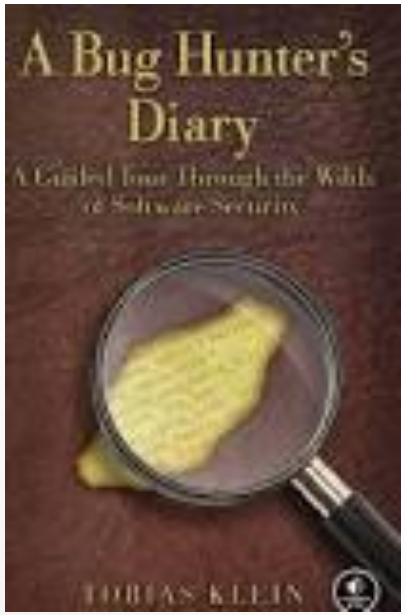


PIPEREVSKI
& ASSOCIATES



PRACTICAL EXAMPLE

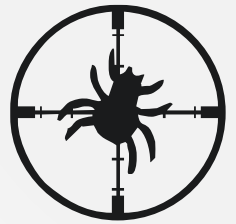
- Desktop Standalone Application
  - Поинт Финансии (http://www.point.com.mk/)
- Microsoft Technologies
- Use of tools
  - Sysinternals Suite of tools
  - x64dbg
- Recommended starting point



PIPEREVSKI
& ASSOCIATES

QUESTIONS !!!

PIPEREVSKI
& ASSOCIATES



THANKS FOR ATTENTION