METHODOLOGY FOR VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT

Presenter m-r Mane Piperevski

BalICCon2k17 Novi Sad, Serbia 2017
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?
HOW DIFFICULT IS VULNERABILITY RESEARCH?

All Things are Difficult Before they are Easy
METHODOLOGY FOR VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT

- Approach method
- Way to find a door
- First doorstep activity
- Ending infinity
- Engineering Exploit Code
METHODOLOGY FOR VULNERABILITY RESEARCH AND EXPLOIT DEVELOPMENT

Don’t forget to do this before you begin
METHODOLOGY PHASE 1
APPROACH METHOD

Vendor dependent

Automated testing
• Loud
• Detectable
• Non Efficient

Manual testing
• Quiet
• Intelligent
• Time Consuming

Knowledge Base
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

Target Door Entries
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
METHODOLOGY PHASE 3
FIRST DOORSTEP ACTIVITY

I became insane, with long intervals of horrible sanity.

Edgar Allan Poe
METHODOLOGY PHASE 3
FIRST DOORSTEP ACTIVITY

“In the middle of every difficulty lies opportunity”
- Albert Einstein
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

Target Door Entries
Dead End

Discovered Vulnerabilities
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

Unique Exploit

Exploit Module
FUTURE DEVELOPMENT AND VISION

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

- Desktop Standalone Application
  - Поинт Финанси (http://www.point.com.mk/)
- Microsoft Technologies
- Use of tools
  - Sysinternals Suite of tools
  - x64dbg
- Recommended starting point
QUESTIONS !!!
THANKS FOR ATTENTION