EliteDevs

YAKSAS CSC

Your Guardian in the Cyber World

YCSC Lab
Exploitation Basics

ASLR Bypass + Stack Pivoting Part 2

Uday Mittal

OSCP, CISSP, CISA, CISM

https://yaksas.in

Assumptions

- Knowledge of
  - Assembly level language
  - Kali Linux
  - Peach Fuzzer
  - Immunity Debugger

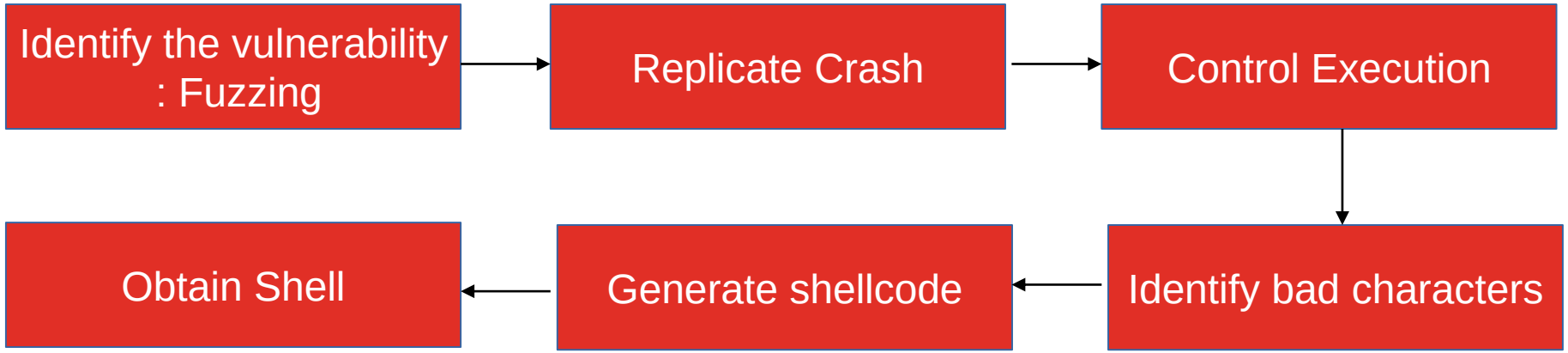
What to do if I need to learn above?

- Check out the resources mentioned at the end of this video

Module Structure

- Introduction
- Fuzzing
- PoC Creation
- Controlling the Execution
- Bad Character Analysis
- Cracking the shell

Exploit development process flow



Fuzzing bird's eye view

- A method for discovering faults in software by providing unexpected input and monitoring for exceptions.

- Types of fuzzers:
  - Mutation-based
  - Generation-based

- Fuzzing Targets:
  - Environment variables and Arguments
  - Web application and server
  - File Format
  - Network Protocol
  - Web browsers
  - In-memory

Source: Fuzzing: Brute-force vulnerability discovery by Michael Sutton, Adam Greene, Pedram Amini

Our target software

- Microsoft Windows Vista
- CoolPlayer+ Portable
  - Vulnerability discovered in 2009 (CVE-2009-1437)
  - Rating: 9.3 / 10
  - A malformed M3U file triggers a local stack-based buffer overflow vulnerability

CVE Link: https://www.cvedetails.com/cve/ CVE-2009-1437 /

Peach Pit Structure

- Peach Pit files are XML files that contain all of the information needed for Peach to perform a fuzzing run. When you fuzz something with Peach you will be creating a Peach Pit file.

- Peach Pit files contain the following:
  - General Configuration
  - Data Modeling
  - State Modeling
  - Agents and Monitors
  - Test Configuration

Documentation link: http://community.peachfuzzer.com/v3/PeachPit.html

Learning Resources

- **Kali Linux** – Kali Linux Revealed by Offensive Security (https://www.kali.org/download-kali-linux-revealed-book/)
- **Metasploit** - Metasploit: The Penetration Tester's Guide by David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni
- **Assembly Language** – SLAE course by SecurityTube (https://www.pentesteracademy.com/course?id=3)
- **Peach Fuzzer** - Peach 3 Documentation (http://community.peachfuzzer.com/v3/PeachQuickStart.html)
- **Immunity Debugger** - Immunity Debugger basics (https://sgros-students.blogspot.com/2014/05/immunity-debugger-basics-part-1.html)
- **Exploit Development** - https://www.fuzzysecurity.com/tutorials.html

YAKSAS CSC

Your Guardian in the Cyber World

Thank you ☺

https://yaksas.in

Yaksas CSC

@yaksas443