EElliteDevs

YAKSAS CSC

Your Guardian in the Cyber World

YCSC Lab
Exploitation Basics

Egg Hunters
Part 2

Uday Mittal

OSCP, CISSP, CISA, CISM

https://yaksas.in

Assumptions

- Knowledge of
  - Assembly level language
  - Kali Linux
  - Spike
  - Immunity Debugger

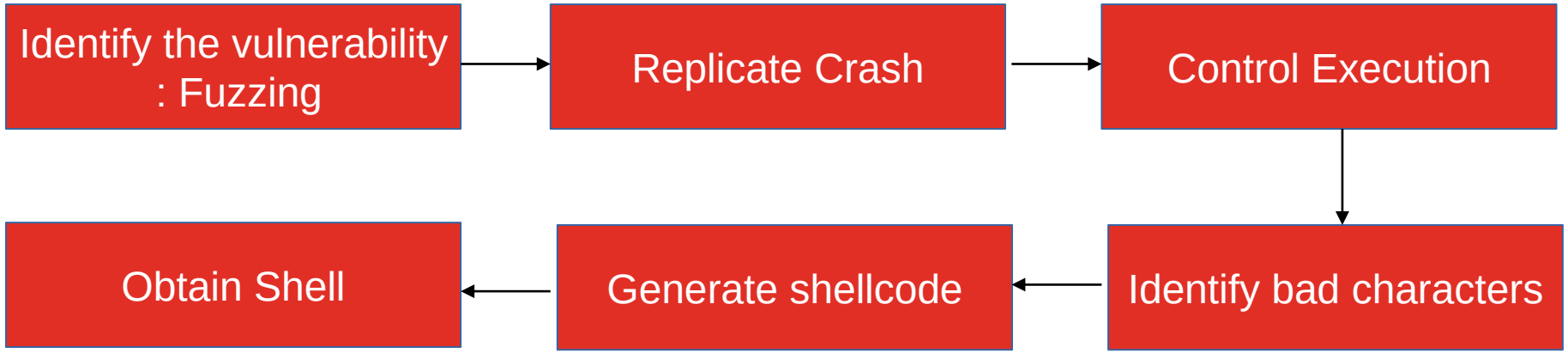
What to do if I need to learn above?

- 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 XP SP3
- Vulnserver.exe
  - Vulnerable on purpose
  - Multiple commands are vulnerable to buffer overflow
  - We will be exploiting the vulnerability in KSTET command

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)
- **Spike** - An Introduction to Fuzzing: Using fuzzers (SPIKE) to find vulnerabilities
- **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