ElliteDevs

YAKSAS CSC

YOUR GUARDIAN IN THE CYBER WORLD

Uday Mittal

OSCP, CISSP, CISA, CISM

https://yaksas.in

YCSC Lab
Exploitation Basics

Limited Buffer Space
Part 2

Assumptions

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

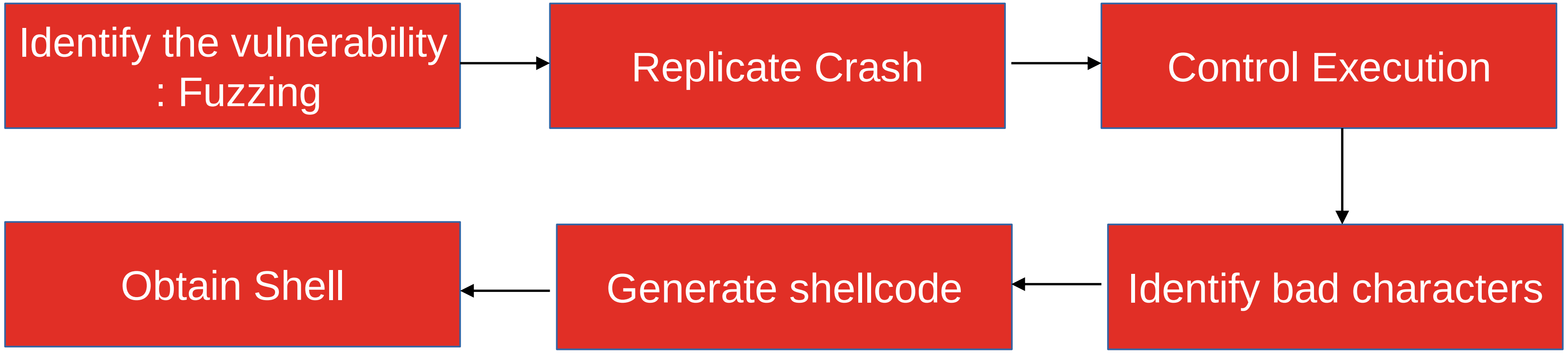
What to do if I need to learn above?

- 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



© ElliteDevs

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

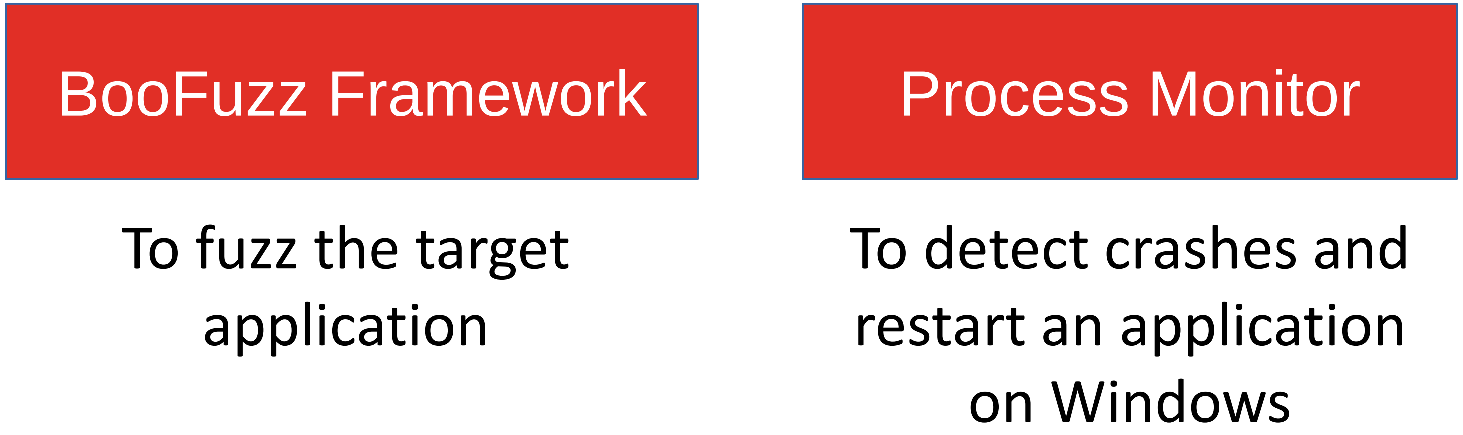
BooFuzz – Fuzzing Framework

- Boofuzz is a fork of and the successor to the Sulley fuzzing framework.
- Features:
  - Easy and quick data generation.
  - Instrumentation – AKA failure detection.
  - Target reset after failure.
  - Recording of test data.
  - Online documentation.
  - Support for arbitrary communications mediums.
  - Built-in support for serial fuzzing, ethernet- and IP-layer, UDP broadcast.
  - Better recording of test data -- consistent, thorough, clear.

To learn more about BooFuzz: https://github.com/jtpereyda/boofuzz

BooFuzz – Fuzzing Framework

- Two components



BooFuzz Framework

To fuzz the target application

Process Monitor

To detect crashes and restart an application on Windows

To learn more about BooFuzz: https://github.com/jtpereyda/boofuzz

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** – Assembly Language Step by Step by Jeff Duntemann
- **BooFuzz** - https://boofuzz.readthedocs.io/en/latest/
- **Immunity Debugger** - Immunity Debugger basics (https://sgros-students.blogspot.com/2014/05/immunity-debugger-basics-part-1.html)
- **Exploit Development** – Fuzzy Security (https://www.fuzzysecurity.com/tutorials.html)

YAKSAS CSC

YOUR GUARDIAN IN THE CYBER WORLD

Thank you ☺

https://yaksas.in

Yaksas CSC

@yaksas443