ElliteDevs

YAKSAS CSC

YOUR GUARDIAN IN THE CYBER WORLD

Uday Mittal

OSCP, CISSP, CISA, CISM

https://yaksas.in

YCSC Lab

Exploitation Basics

Egg Hunters
Part 5

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

Bad Character Analysis

- Send all possible characters, from 0x00 to 0xff, as part of our buffer, and see how these characters are dealt with by the application, after the crash occurs.
- 0x00 – A bad character by default as it represents a null byte

Identified Bad Characters

- Bad Characters: 0x00
- This character when converted to ASCII translates into following:
  - 0x00 - null byte

- Null byte is a global terminator and hence truncates any characters that appear after it. The line feed and end of file truncate the buffer and hence treated as bad characters in this case.

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