EliteDevs

YAKSAS CSC

Your Guardian in the Cyber World

YCSC Lab
Exploitation Basics

ASLR Bypass + Stack Pivoting Part 5.1

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
- Bad Character Analysis
- Controlling the execution
- Cracking the shell

Grabbing the control

- Identify the location of character which overwrites EIP register
- Verify the location
- Redirect the execution to EBP
  - Hard code EBP address OR
  - Find an accessible, reliable address in memory that contains an instruction such as JMP EBP
    - Pre-requisites for the memory address
      - Should not be affected by DEP or ASLR
      - Should not contain bad characters
- Jump forward, if required

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