ElliteDevs

YAKSAS CSC

YOUR GUARDIAN IN THE CYBER WORLD

YCSC Lab
Exploitation Basics

ASLR Bypass + Stack Pivoting Part 5.2

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?

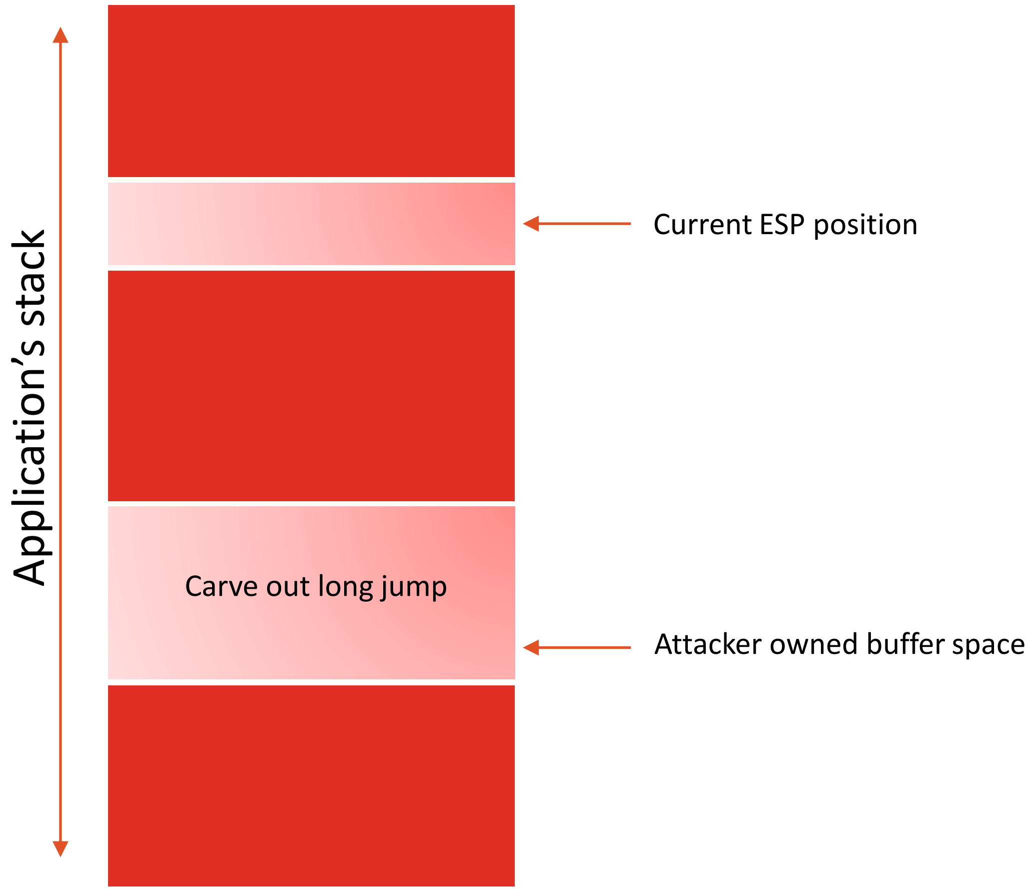
- Check out the resources mentioned at the end of this video

Module Structure

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

Stack Pivoting

- Carve out long jump in the buffer space controlled by us



© ElliteDevs

Stack Pivoting

- Assembly code for stack pivoting

Save stack pointer

```
0156E08A   8BC4           MOV EAX,ESP
```

Carve out long jump

```
0156E08C   53             PUSH EBX
0156E08D   5C             POP ESP
0156E08E   83C4 40        ADD ESP,40
0156E091   51             PUSH ECX
0156E092   66:81C1 2601   ADD CX,126
0156E097   66:51          PUSH CX
0156E099   66:81C1 6AE8   ADD CX,0E86A
0156E09E   66:51          PUSH CX
```

Restore stack

```
0156E2FA   50         PUSH EAX
0156E2FB   5C         POP ESP
```

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