



Uday Mittal  
OSCP, CISSP, CISA, CISM  
<https://yaksas.in>

## YCSC Lab Exploitation Basics

### ASLR Bypass + Stack Pivoting Part 3

# 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
- Controlling the Execution
- Bad Character Analysis
- Cracking the shell

# Our target software



- Microsoft Windows Vista
- CoolPlayer+ Portable
  - Vulnerability discovered in 2009 (CVE-2009-1437)
  - Rating: 9.3 / 10
  - A malformed M3U file triggers a local stack-based buffer overflow vulnerability

*CVE Link: <https://www.cvedetails.com/cve/CVE-2009-1437/>*

# Proof of Concept



- A script or a program to replicate the crash
- Can be written in any language (I will be using Python)
- Enhanced further to create an exploit

# 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>



Thank you 😊



<https://yaksas.in>



Yaksas CSC



@yaksas443