



Course: Hands-on Exploit Development

Module 1: Stack-based buffer overflow

Title: Assignment 1

Objective: Create a working exploit for JetAudio jetCast Server 2.0

- Develop this exploit for Windows 7 SP1 (x86)
- Use the existing exploit to understand where the vulnerability exists
- Using a bind tcp shell or reverse tcp shell payloads.
- Create a write-up or a short video explaining your methodology step by step.
- Send the link to write-up or video on csc@yaksas.in with the subject 'Assignment Submission: JetAudio jetCast Server 2.0'

Tools required for this assignment

- Virtualization software (VirtualBox or VMWare)
- Linux
 - Kali Linux 2018.1 (VM)
 - Python 2.7
 - Sublime Text or Notepad ++
- Windows
 - Microsoft Windows 7 (VM)
 - Immunity Debugger
 - Mona library for Immunity Debugger
 - JetAudio jetCast Server 2.0 -> Target software | Download link: <https://www.exploit-db.com/apps/aa8b0ffe339644e7b73da49c72c1fb39-JCS2000.exe>
 - Sublime Text or Notepad ++
 - Python 2.7

Questions

- Where does the vulnerability lie and how to exploit it?
- What are the bad characters for this exploit?
- Which encoder did you use to encode the payload shellcode?