YAKSAS CSC

SECURITY IS EVERYONE'S RESPONSIBILITY

Course: Hands-on Exploit Development

Module 1: SEH Overwrite

Title: Assignment 2

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: DeviceViewer 3.12.0.1

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
  - DeviceViewer 3.12.0.1 -> Target software | Download link: https://www.exploit-db.com/apps/4d10486a079bd1f1864c30e86cd2aa80-DeviceViewer.exe
  - Sublime Text or Notepad ++
  - Python 2.7

Questions

- Where does the vulnerability lie and how to exploit it?
- How do you bypass the process of finding bad chars for this exploit?
- Which encoder did you use to encode the payload shellcode?