



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

YCSC Lab Exploitation Basics

Limited Buffer Space Part 3

Assumptions



- Knowledge of
 - Assembly level language
 - Kali Linux
 - BooFuzz
 - 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 7 SP1
- Vulnserver.exe
 - Vulnerable on purpose
 - Multiple commands are vulnerable to buffer overflow
 - We will be exploiting the vulnerability in KSTET command

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** – Assembly Language Step by Step by Jeff Duntemann
- **BooFuzz** - <https://boofuzz.readthedocs.io/en/latest/>
- **Immunity Debugger** - Immunity Debugger basics (<https://sgros-students.blogspot.com/2014/05/immunity-debugger-basics-part-1.html>)
- **Exploit Development** – Fuzzy Security (<https://www.fuzzysecurity.com/tutorials.html>)



Thank you 😊



<https://yaksas.in>



Yaksas CSC



@yaksas443