Course Objectives

This class is for everyone who want to be a security expert that will come up with 0-day and various (restricted computing environment) escape strategies.

Learning Level

- Advance

Course Duration

- 5 Days

Course Prerequisite

- None

Target Group

- Technical Security Expert

Course Outline

Day 1

- Advanced Network Attack
- Accessing the Network
- Manipulating the Network
- Take Advantage of network protocols

Day 2

- Modes of Encription
- Encryption and Obfuscation

Cryptographic Attacks

Escaping from Restricted Computing Environment

Day 3

- Python For Exploit Researcher
- The Art and Science of Fuzzing
- Creating Packets in Scapy
- Fuzzing Techniques
- Fuzz Testing using Sulley
- Fuzzing Code Coverage Determination

Day 4

- Exploit Linux Environment
- Memory
- Dynamic Memory
- Linux Shellcode
- Smashing the Stack
- Advanced Stack Smashing
- Defeat Stack Protection
- Bypassing Address Space Layout Randomisation

Day 5

Investigating Windows OS Protections and Complier-Time Control

Introduction to Windows Exploitation

Windows Overflows

Defeating DEP, ASLR, and Windows 8 ROP Protection

Building and Importing Metasploit Modules

Windows Shellcode

Official Training Partner