Zero-day vulnerability development and exploit writing areas

- Zero-day vulnerability development
  - Fuzzing
  - Reverse engineering
  - static and Dynamic analysis
  - Binary diffing
  - Binary Analysis
  - Analysis of a windows Kernel vulnerabilities
- Zero-day exploit development
  - Advanced windows exploitation
  - Exploit writing techniques'
  - Advanced Heap spray exploits
  - Windows kernel debugging and exploitation
  - Windows kernel exploit development techniques
  - Enhanced Mitigation Experience Toolkit (EMET) bypassing
  - Defeating exploit mitigation techniques
  - Advanced usage of IDA pro and WinDBG
  - Crash Analysis using debuggers
  - Python for hackers
  - Basic assembly language
- Shellcode writing
  - Antivirus bypassing
  - Writing different types of shellcode
  - Extracting shellcode from exploits
- Exploit customization
  - Defeating DEP and ALSR using ROP
  - Antivirus bypassing
  - Defeating exploit mitigation techniques
  - Use-after-free bugs and vtable overwrites
  - Advanced Browser exploits
  - Advanced PDF exploits
  - Advanced Heap spray techniques'
  - Advanced Malware analysis