Certified Information Security Expert Level-2 EXPLOIT WRITING:-

1. INTRODUCTION TO EXPLOIT WRITING
    - Program execution
    - Memory Management
    - The Stack
    - The Heap
    - Memory Corruption

2. PROGRAMMING BASICS
    - Programming in Python
    - Variables
    - Strings
    - Loops
    - Tuples
    - Branching and Conditionals
    - Sockets
    - Standard Libraries

3. ASSEMBLY LANGUAGE
    - Theoretical Foundation
    - CPU Allocation
    - Basic Instructions
    - Structure of an Assembly Program
    - The assembly compiler
    - Coding a simple Assembly program
    - Strings
    - Conditional branching
    - Unconditional Branching

4. DEBUGGING
    - Ollydbg
    - Immunity Debugger
    - Ggdb

5. STACK BASED BUFFER OVERFLOW
    - The Stack Architecture
    - Stack Operaions
    - Smashing the stack

6. UNDERSTANDING WINDOWS SHELLCODE
    - Msfpayload
    - Msfencode
    - Payload components

7. FUZZERS
    - Spike
    - Metasploit

8. OUTLINE
    - Architecture
    - Flaws
    - Heap Overflow

9. EXPLOITING/GS CANARY PROTECTED PROGRAMS
    - Terminator Canaries
    - Random Canaries
    - Random XOR Canaries

10. EXPLOITING SAFESEH PROTECTED PROGRAMS
    - SEH
    - SafeSEH
    - Bypassing SafeSEH Protections

11. DENIAL OF SERVICE

12. BYPASSING DEP & ASLR
    - DEP- Bypassing DEP
    - ASLR-BypassingASLR

13. ADVANCED SHELLCODING
    - Reverse Payloads
    - Staged/stager payload
    - Bind Payloads
    - Binary payloads & Antivirus Evasion
    - Binary Payload Encoding

14. ENCODERS & WRITING CUSTOM ENCODERS

15. DLL HIJACKING

16. CLIENT SIDE EXPLOITS
    - Browser Exploits
    - Browser fingerprinting

- Client side smb-exploits

17. FROM VULNERABILITY TO EXPLOIT
    - Stacked based overflows
    - Understanding windows payload
    - From vulnerability to exploit

18. METASPLOIT FRAMEWORK
    - History
    - Explots
    - Auxiliary
    - Payloads
    - Plug-ins
    - Mixins
    - Scripts
    - MsfCli
    - Resource files
    - Binary payload generator
    - Generating Shellcode
    - Nops
    - Exploitation with Metasploit

19. BINARY PAYLOADS & ANTIVIRUS EVASION
    - Msfpayload
    - Msfencode

20. EXPLOIT TO METASPLOIT
21. CAPTURE THE FLAG EXERCISE