CWL
CyberWarFare Labs

Certified Exploit Development Professional (CEDP)

@CyberWarFare Labs

I. Introduction to CEDP

1.1 Tailored for beginners

1.2 Includes study materials such as videos and PDF slides

1.3 Covers the fundamentals of exploit development

1.4 Provides an in-depth understanding of stack exploitation

1.5 Ideal for anyone looking to jump-start their journey into exploit development

II. Information Syllabus

The course contents are divided into 2 modules listed below:

2.1 Linux Exploit Development

- 2.1.1 Anatomy of buffer overflows in Linux applications.
- 2.1.2 Exploiting stack-based buffer overflows on Linux.
- 2.1.3 Using ret2libc, Return-Oriented Programming (ROP) to bypass security mechanisms (NX bit).
- 2.1.4 Bypass Address Space Layout Randomization (ASLR)
- 2.1.5 Both real world examples & simulated examples
- 2.1.6 Using GDB for debugging

II. Information Syllabus

2.2 Win32 Exploit Development

- 2.2.1 Practical exploration of Windows elements such as processes, PE files, and threads.
- 2.2.2 Shedding light on win32 SEH (Structured Exception Handling).
- 2.2.3 Understanding the exploitation of SEH.
- 2.2.4 Discussion on various ASLR bypass techniques.
- 2.2.5 Hands-on experience with different debuggers and disassemblers.

III. Prerequisites

3.1 VMWare Workstation (Evaluation or Pro)

3.2 Ubuntu 20.04.6 LTS x86_64

3.3 Windows 10 22H2

3.4 Basic knowledge of c, c++, python, assembly language

3.5 Basic understanding on debuggers (gdb, Windbg, x64dbg)

IV. Target Audience

4.1 Reverse Engineers

4.2 Red Team / Penetration Testers

4.3 Student and Aspiring Cybersecurity Professionals

4.4 Security Enthusiasts and Researchers

4.5 Individuals Looking to Begin Exploit Development

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live