



[Back to Product Page](#)

Advanced Exploitation Revealed Course

1 Sessions -

3 Hours of Interactive Training

The Advanced Exploitation Revealed training course is the 5th and final step in the CPT Engineer series which is based on 5 key elements of Pen Testing; information, gathering, scanning, enumeration, exploration and reporting. In this course, expert Duane Anderson will help you understand the nature of exploits. You will learn about the tools and techniques that protect your systems and network from exploitation. This course also walks you through the necessary steps to document and report your findings. Upon completion of this course you will be prepared to pass the CPT Engineer Certification Exam, formerly known as CPTS.

Benefits

- Prevent buffer and heap overflows
- Prevent your systems from exploitation
- Understand how to effectively document your penetration tests

Session 1

Section A: The Nature of Exploits

- Exploits
- Format Strings
- Race Conditions
- Memory Organization
- Buffer Overflow
- Buffers and Stacks
- Stack Function
- How a Buffer Overflow Works
- Heap Overflow
- Heap Spraying
- Prevention

Section B: Exploit Development and the Tools

- Exploit Development
- Shellcode Development
- Metasploit
- Meterpreter
- Fuzzers
- Milw0rm
- SAINTexploit
- CORE IMPACT
- Tool Comparison

Section C: Metasploit at Work

- Update Metasploit
- Metasploit Demo
- Exploit List

Section D: SAINT and CORE IMPACT at Work

- SAINTexploit Demo
- Exploits
- SAINTwriter
- CORE IMPACT Demo
- Results
- Analyzing the Results

Section E: Documentation and Risk Analysis

- Documentation Assets
- The Report
- Supporting Documentation
- Analyzing Risk
- Report Results Matrix
- Findings Matrix

Section F: Report Content and Delivery

- Delivering the Report
- Stating Fact
- Recommendations
- Executive Summary
- Technical Reports
- Scope of Testing
- Summary Recommendations
- Summary Observations
- Detailed Findings
- Strategic/Tactical Directives
- Statement of Responsibility

About The Author

Duane Anderson, for the last two decades, has been working in the IT Security Training and Consulting Arena. He has worked with US and foreign military branches, U.S. government agencies, banking and regulated industries and fortune 500 companies. Duane has contributed to mile2's security curriculum with Certified Penetration Testing Engineer, Certified Digital Forensics Examiner and Certified Wireless Security Engineer. In addition, he has coordinated and executed IT counter-hacking & security courses for the US Marine Corps, US Army, US Air Force, U.S. Treasury, Sprint, IBM, Washington Mutual and Service Canada. Duane brings a vast wealth of experience and holds the following professional qualifications -- Security+, CPTS, CPTE, CDFE, CEH and Mile2 Certified Instructor.

- Payloads
- Command Line Metasploit
- RPC DCOM Exploit
- Metasploit Web Interface
- Restart
- Input Options
- Client Side Attack
- msf Exploit
- Verifying the Exploit
- Pressing the Exploit