Certified Penetration Testing Engineer
August 3-7, 2015

The C(PTE course is compromised of the following modules and appendices:

- Logistics of Penetration Testing
- Linux Fundamentals
- Detecting Live System
- Enumeration
- Vulnerability Assessments
- Malware Goes Undercover
- Windows Hacking
- Hacking UNIX/Linux
- Advanced Exploitation Techniques
- Pen Testing Wireless Networks
- Networks, Sniffing, IDS
- Injecting the Database
- Attacking Web Technologies
- Project Documentation
- A1: Understanding Penetration Testing
- A2: Financial Sector Regulations
- A3: Access Controls
- A4: Protocols
- A5: Cryptography
- A6: Economics and Law

The Certified Penetration Testing Engineer course will help obtain real world security knowledge that enables vulnerabilities to be recognized along with exploit system weaknesses and help safeguard against threats, and to learn the art of ethical hacking with a professional edge. C(PTE's foundation is built firmly upon proven penetration testing methodologies. The course presents information based on the five Key Elements of Pen Testing: Information Gathering, Scanning, Enumeration, Exploitation and Reporting. The lasted vulnerabilities will be discovered using these tried and true techniques.

ALPENA
COMMUNITY COLLEGE