Course Catalog
2020
About Us

Cyber Mission Training, a Jacobs service, provides fully interactive, proficiency-based classes that make it easy for cybersecurity professionals to meet their training requirements. Using a proven offensive methodology framework, we educate cyber professionals to exploit and expand access into remote networks and to locate and respond to malicious threats with the Survey, Secure, Protect, and Recover method. We also instruct cyber leaders about the cyber threat landscape, enhancing understanding of the field’s current and future needs. We strive to provide the highest quality, most relevant curricula for our students.

Our training programs serve the most demanding cyber operations missions for customers across the U.S. Department of Defense (DoD) and various federal agencies. We have been named an official cybersecurity provider by the U.S. Department of Homeland Security (DHS), and our courses appear in the National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog.

JACOBS

Jacobs leads the global professional services sector delivering solutions for a more connected, sustainable world. With approximately $12 billion in revenue and a talent force of more than 50,000, Jacobs provides a full spectrum of services including scientific, technical, professional and construction- and program-management for business, industrial, commercial, government and infrastructure sectors. For more information, visit www.jacobs.com, and connect with Jacobs on LinkedIn, Twitter, Facebook, and Instagram (@JacobsConnects).

ACE CREDIT®

The American Council on Education’s College Credit Recommendation Service (CREDIT®) was established in 1974 to connect workplace learning with colleges and universities by helping students gain access to academic credit for formal training taken outside traditional degree programs. With over 35,000 programs reviewed, CREDIT has been the national leader in the evaluation process for education and training obtained outside the classroom including courses, exams, apprenticeships, and other types of nontraditional forms of training.
What We Offer

• **Proficiency-based learning that goes beyond theory** because cyber mission training is most effective through hands-on, practical exercises that simulate complexities of real operational environments.

• **Hands-on labs in every class**, where lectures are accompanied by exercises that reinforce the material and allow students to delve deeper into the subject at their own pace.

• **Experienced instructors** who have a wide variety of industry certificates, including CISSP, CCNA, CASP, CEH, Security+, and Network+, and have solved some of the most complicated cyber challenges for our critical national agencies.

• **Multiple delivery methods** to cater to individual students’ needs. Students select the method that fits best with their schedule without sacrificing instructor support.

• **Continuous curriculum improvement** because the cyber world is always changing. Our instructors continuously monitor new and emerging threats and are committed to keeping course curriculum up to date and relevant.

• **Courses that map to National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework** to help our students identify knowledge, skills, and abilities that are needed for certain positions in the cybersecurity field.

Contact Us Today

- **410.904.5200**
- cybertraining@jacobs.com
- www.jacobs.com/cyber-mission-training/courses
<table>
<thead>
<tr>
<th>Course</th>
<th>Recommended</th>
<th>Description</th>
<th>Duration</th>
<th>ACE Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Leader Course (CLC)</td>
<td>Leadership</td>
<td>Introduces processes, techniques and terminology used by cyber professionals to explain, discover and prevent threats to enterprise networks.</td>
<td>2 days</td>
<td>N/A</td>
</tr>
<tr>
<td>Cyber Mission Foundations (CMF)</td>
<td>Intermediate</td>
<td>Provides multi-dimensional foundation to help students confidently and effectively carry out business in the digital environment.</td>
<td>8 weeks</td>
<td>12</td>
</tr>
<tr>
<td>Digital Forensics &amp; Analysis (DFA)</td>
<td>Intermediate</td>
<td>Teaches digital forensic knowledge of the inner workings of Windows malware analysis, preparing students to become malware hunters and defenders.</td>
<td>10 days</td>
<td>3</td>
</tr>
<tr>
<td>Windows Exploitation &amp; Analysis (WEA)</td>
<td>Intermediate</td>
<td>Teaches the essentials of offensive methodology that focus on Windows systems and modern techniques.</td>
<td>5 days</td>
<td>N/A</td>
</tr>
<tr>
<td>Offensive Methodology &amp; Analysis (OMA)</td>
<td>Advanced</td>
<td>Teaches current cyber attack methods to develop strategies to protect and defend networks and critical information.</td>
<td>10 days</td>
<td>3</td>
</tr>
<tr>
<td>Windows &amp; Linux Scripting (WLS)</td>
<td>Advanced</td>
<td>Introduces PowerShell and Python scripting, beginning with the fundamentals and finishing with students creating fully executable scripts.</td>
<td>10 days</td>
<td>N/A</td>
</tr>
<tr>
<td>Advanced Offensive Methodology &amp; Analysis (AOMA)</td>
<td>Expert</td>
<td>Trains students in advanced cyber-attack methods to develop strategies for protecting and defending networks and critical information.</td>
<td>5 days</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Overview

CYBER THREAT LANDSCAPE OVERVIEW
- Discuss current real-world hacking events
- Review hacker methodologies
- Demonstrate common exploitation techniques

THREATS AND MALWARE OVERVIEW
- Describe malware, such as worms, viruses and rootkits
- Learn hacker strategies to bypass network defenses
- Demonstrate real-world techniques

CYBER POLICY
- Understand different roles in the cyber workforce
- Discuss key policy documents and their implications
- Examine legal and industry regulation

CYBER DEFENSIVE STRATEGIES
- Demonstrate cyber defense operations
- Discuss the functions of security devices, such as firewalls, intrusion detection systems and antivirus

INCIDENT RESPONSE
- Describe the functions of incident-response teams
- Learn the incident-response lifecycle
- Exercise building an incident-response plan
Overview

- Learn to identify, monitor and defend Windows systems
- Detect and resolve threats against a wide range of Unix systems
- Analyze network traffic and gain an in-depth knowledge of how systems communicate
- Bolster security, conduct situational awareness surveys and explore the malware engineering

SECURITY CONCEPTS

- Understand the mindset, conduct and protocol to create and maintain secure environments
- Assess the state of existing environments
- Make informed decisions based on system integrity

WINDOWS

- Learn the ins and outs of a Windows system
- Identify suspicious activity
- Understand executable code persistence

UNIX

- Quickly assess system integrity
- Develop skills for applying Solaris and Linux techniques

NETWORKING

- Learn how system and data communication works within local and wide area networks
- Traverse networks using tunneling and redirection
Overview

PROCESS INTERROGATION

• Learn about the Sysinternals Suite and native tools (e.g., netstat, tasklist, etc.)
• Begin PowerShell scripting to automate process analysis
• Locate running malware and discover persistence vectors

FILE SYSTEM ANALYSIS

• Search for forensic artifacts and perform a timeline analysis
• Copy a hard drive using open-source tools

SUPPLEMENTAL ARTIFACTS

• Analyze the following artifacts:
  • Prefetch files
  • Volume Shadow Copy Service
  • Interesting Registry Keys
  • Shellbags

RESPONSIVE ACTIONS

• Become a more proficient cyber-mission defender running malware executables
• Create signatures for malware executables as Indicators of Compromise (IOC) and check other systems on the network for these IOCs

CAPSTONE

• This course concludes with a full-day capstone that combines the skills learned throughout the course
Overview

INFORMATION GATHERING
• Analyze the offensive methodology and information gathered using open-source tools

SCANNING AND ENUMERATION
• Use open-source tools to scan networks and servers

GAINING ACCESS
• Send exploits using the Metasploit Framework (MSF)
• Redirect traffic for obfuscating point of origin and lateral movement within a network using tunneling techniques
• Compile and deploy actual malware to set up a small botnet using client-side exploits

EXPANDING ACCESS
• Learn about the Windows Registry, Offensive Digital Forensics and Windows Active Directory queries
• Manage open-source and native tools to find files of interest
• Discover how to crack passwords and use the pass-the-hash technique to move around a remote Windows network

Learn the essentials of offensive methodology
• Use the Browser Exploitation Framework (BeEF) to control clients
• Deploy and control an IRC based botnet
• Learn Windows security bypass techniques
Overview

INFORMATION GATHERING
• Mine a website for key information
• Practice techniques to discover new servers

SCANNING AND ENUMERATION
• Scan and enumerate network-based environment using command line tools
• Discover exploits using web browser enumeration

GAINING ACCESS
• Practice Metasploit exploits and techniques
• Discover port redirection and tunneling techniques
• Learn Cross-Site Scripting (XSS), SQL Injection and file inclusion
• Execute client-side exploits and botnet deployment

EXPANDING ACCESS
• Check system safety and security
• Learn methods for discovering files of interest
• Practice methods to crack passwords
• Enumerate Unix and Linux systems

SUSTAINING ACCESS
• Detect antivirus tools and intrusion detection systems
• Learn techniques for sustaining access
Overview

- Identify differences between various sequences and primitive data types
- Define the concept and importance of scoping, object-oriented programming and classes
- Demonstrate the ability to use the command line interpreter
- Learn the proper use of a function and multi-threaded scripting

INTRODUCTION

- Identify the fundamentals, terms and definitions of PowerShell and Python scripting
- Use command line interpreter to execute basic code
- Recognize differences between various sequences and data types

PYTHON ON LINUX

- Understand constructs used in scripting decision-making processes
- Learn to import and use scripting modules
- Define the concept and importance of scoping

MICROSOFT WINDOWS POWERSHELL

- Exhibit the proper use of a function
- Recognize using regular expressions to match patterns in strings
- Identify the importance of input validation
Overview

ANTIVIRUS EVASION

• Learn to encode, encrypt and pack malware to evade detection
• Increase exploit effectiveness by modifying payloads and stagers to avoid detection
• Extractions of both mobile devices and removable media will be conducted, as well as database analysis, and other applicable file analysis

ADVANCED CREDENTIAL ATTACKS

• Perform pass-the-hash techniques with antivirus-evading payloads
• Learn to migrate between 32-bit and 64-bit payloads on Windows systems
• Explore alternative credential attacks used for lateral movement within a network

MALWARE COMMAND AND CONTROL

• Learn command and control techniques used by modern malware
• Employ beaconing malware to minimize detection
• Gain interactive access through a beaconing backdoor

HOST FIREWALL MANIPULATION

• Disable or manipulate host-based firewalls on exploited systems
• Enable lateral movement inside a target network

PHYSICAL ACCESS

• Gain access to a system using a live-boot operating system
• Implant malware on a system compromised through physical access
Contact Us Today

📞 410.904.5200

✉️ cybertraining@jacobs.com

🌐 www.jacobs.com/cyber-mission-training/courses