2018
Cyber Mission Training
Course Catalog
# TABLE OF CONTENTS

Courses at a Glance................................................................................................................. 3
What We Offer.......................................................................................................................... 4
Cyber Leader Course (CLC)..................................................................................................... 5
Cyber Mission Foundations (CMF)......................................................................................... 6
Offensive Methodology & Analysis (OMA)........................................................................... 7
Windows Exploitation & Analysis (WEA)............................................................................... 8
Digital Forensics & Analysis (DFA)....................................................................................... 9
Windows & Linux Scripting (WLS)........................................................................................ 10
Mobile Digital Forensics (MDF)............................................................................................ 11
Getting Started....................................................................................................................... 12
About Parrot Labs Cyber Mission Training........................................................................ 13
## Courses at a Glance

All courses are offered in our Hanover, MD, training lab—or, we can bring our Persistent Cyber Training Environment (PCTE-M), a mobile solution, to you.

<table>
<thead>
<tr>
<th>Course</th>
<th>Recommended For</th>
<th>Description</th>
<th>Class Duration</th>
<th>ACE Recommended Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Leader Course (CLC)</td>
<td>Leadership</td>
<td>Introduction to processes, techniques and terminology used by cyber professionals to explain, discover and prevent threats to enterprise networks and sensitive information.</td>
<td>2 Days</td>
<td>N/A</td>
</tr>
<tr>
<td>Cyber Mission Foundations (CMF)</td>
<td>Intermediate Students</td>
<td>Provides multi-dimensional foundation to help students confidently and effectively carry out business in the digital environment in four modules, including: (1) Windows, (2) Unix, (3) Networking/Packet Analysis, (4) Security Concepts</td>
<td>8 Weeks or 4 Two-Week Modules</td>
<td>3 Undergraduate for each of the four modules for a total of 12 credits</td>
</tr>
<tr>
<td>Offensive Methodology &amp; Analysis (OMA)</td>
<td>Advanced Students</td>
<td>Students learn current cyber attack methods to develop strategies to protect and defend their networks and critical information.</td>
<td>2 Weeks</td>
<td>3 Undergraduate</td>
</tr>
<tr>
<td>Windows Exploitation &amp; Analysis (WEA)</td>
<td>Intermediate Students</td>
<td>Teaches the essentials of offensive methodology that focus on Windows systems and modern techniques.</td>
<td>1 Week</td>
<td>N/A</td>
</tr>
<tr>
<td>Digital Forensics &amp; Analysis (DFA)</td>
<td>Intermediate Students</td>
<td>Teaches in-depth digital forensic knowledge of the inner workings of Windows 7 malware analysis while preparing students to become proficient cyber-mission malware hunters and defenders.</td>
<td>2 Weeks</td>
<td>3 Undergraduate</td>
</tr>
<tr>
<td>Windows &amp; Linux Scripting (WLS)</td>
<td>Advanced Students</td>
<td>Introduces PowerShell and Python scripting, beginning with the fundamentals and finishing with students creating fully executable scripts.</td>
<td>2 Weeks or 2 One-Week Modules</td>
<td>N/A</td>
</tr>
<tr>
<td>Mobile Digital Forensics (MDF)</td>
<td>Advanced Students</td>
<td>Teaches the ins and outs of mobile devices and how they relate to hacking and forensics.</td>
<td>2 Days</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The ACE CREDIT logo is a federally registered trademark of the American Council on Education and cannot be used or reproduced without the express written permission of the American Council on Education.
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. Each class balances technique with hands-on learning exercises so that you learn classroom techniques for approaching cyber challenges and practice solving them.

**Hands-On Labs in Every Class,** where lectures are accompanied by real-time opportunities for students to follow the lesson on their own workstations. Lectures are followed 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. They also continuously monitor new and emerging threats and are committed to keeping course curriculum up to date and relevant.

**Persistent Cyber Training Environment** that provides all of the technology you need to be successful in class. Each student at Parrot Labs is provided an individual workstation with two wide-screen monitors for conducting research and running exercises, using between 20 and 40 virtual machines throughout the course. All you need to bring is yourself!

**Learning on the Go** through a self-contained, fully functional PCTE-M. This robust virtual cybersecurity training environment allows you to complete the proficiency training you need to meet your mission requirements—all from the convenience of your own facility.

**Potential to Earn Undergraduate College Credit Recommendations** for select Parrot Labs courses evaluated by the American Council on Education’s College Credit Recommendation Service (CREDIT®).

**Courses That Map to National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework** to assist our students. The NICE Framework supports cybersecurity professionals in exploring tasks and work roles and identifying knowledge, skills and abilities that are valued by employers and needed for certain positions in the cybersecurity field.
Cyber Leader Course

**Course 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

**Course Details**
- Focused on providing hands-on exploitation experience, with “big picture” information
- Realistic scenarios for leaders who are involved in cybersecurity fields with an emphasis on learning through experience
- Leave the class with an understanding of the current cyber environment, modern techniques
- Gain the ability to hold meaningful technical discussions with security-minded coworkers
Course 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

Course Details

- Students receive a course book to accompany classroom instruction
- Each student works on a personal sandboxed network of 70-90 virtual machines, including devices, firewalls and Windows systems
- Realistic target network includes routers and Active Directory domains
OFFENSIVE METHODOLOGY & ANALYSIS (OMA)

Course 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

Course Details
- Students receive a course book to accompany classroom instruction
- Each student practices on a personal sandboxed network of 60-90 virtual machines, including switches, routers, and firewalls with Unix and Windows systems
- Each realistic target network has routers and Active Directory domains populated with simulated personal data to immerse students in detailed scenarios
## WEA
Windows Exploitation & Analysis

<table>
<thead>
<tr>
<th>Course</th>
<th>Recommended For</th>
<th>Description</th>
<th>Class Duration</th>
<th>ACE Recommended Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Exploitation &amp; Analysis (WEA)</td>
<td>Intermediate Students</td>
<td>Teaches the essentials of offensive methodology that focus on Windows systems and modern techniques.</td>
<td>1 Week</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 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

### Course Details

- Receive a course book to accompany classroom instruction
- Gain proficiency-based, hands-on training using a variety of tools to gain access to a remote network
- Learn in-depth tactics, techniques and procedures an attacker may use to gain access to your networks
- Perform exercises and scenarios in a sandboxed network, allowing you to practice and learn
Digital Forensics & Analysis (DFA)

<table>
<thead>
<tr>
<th>Course</th>
<th>Recommended For</th>
<th>Description</th>
<th>Class Duration</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Forensics &amp; Analysis</td>
<td>Intermediate Students</td>
<td>Teaches in-depth digital forensic knowledge of the inner workings of Windows 7 malware analysis while preparing students to become proficient cyber-mission malware hunters and defenders.</td>
<td>2 Weeks</td>
<td>3 Undergraduate</td>
</tr>
</tbody>
</table>

Course 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

**SUSTAINING ACCESS**
- Detect antivirus tools and intrusion detection systems
- Learn techniques for sustaining access

Course Details

- Know what looks suspicious and have the tools to investigate and identify malware at a forensic level
- Perform exercises and scenarios in a sandboxed network, learning at your own pace without affecting other students
- Analyze rootkits and malware in a realistic network with routing and servers set up to perform the malware delivery chain

Parrot Labs CYBER MISSION TRAINING

2018 Cyber Mission Training Course Catalog | 9
### WLS
Windows & Linux Scripting

<table>
<thead>
<tr>
<th>Course</th>
<th>Recommended For</th>
<th>Description</th>
<th>Class Duration</th>
<th>ACE Recommended Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows &amp; Linux Scripting (WLS)</td>
<td>Advanced Students</td>
<td>Introduces PowerShell and Python scripting, beginning with the fundamentals and finishing with students creating fully executable scripts.</td>
<td>2 Weeks or 2 One-Week Modules</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Course 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

**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

**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

**Course Details**

- Learn to identify the fundamentals of scripting in Python and PowerShell using the command line
- Analyze and create fully functional scripts
- Perform exercises and scenarios in a sandboxed network
Course Overview

INTRODUCTION

- Learn about cell phone channels, cellular network technologies, mobile components and the components that assist with mobile device information
- Cover codes and protocols, including Long Term Evolution, Frequency Division Multiple Access, Time Division Multiple Access, Code Division Multiple Access and Global System for Mobile Communications

ANDROID

- Explore key features of the Android OS, including interface, applications, memory management, virtual reality and versioning
- Study file systems, memory partitions and the background of SQLite files
- Defend against malware, recover forensic data and explore hacking concepts applicable to the Android OS

iOS

- Cover the iOS framework, software updates, the boot sequence and file system basics
- Analyze the iOS file system, where the operating system's files and application files reside
- Learn about the OS X standard directories, sandboxed applications and general file “sneakiness”

Course Details

- Gain a better understanding of mobile forensics
- Compare Android and Apple operating systems, apply forensic processes to mobile devices and interpret mobile hacking concepts
- Perform exercises and scenarios in a sandboxed network, allowing you to practice and learn at your own pace without affecting other students
Getting Started

Getting started is easy. Simply contact Parrot Labs on 410.904.5200 to register for the desired course(s).

About Parrot Labs Cyber Mission Training

Parrot Labs Cyber Mission Training, a KeyW Service, offers interactive, proficiency-based Cyber Mission Training classes with industry-leading instructors that make it easy for cybersecurity professionals to meet their training requirements. Using a proven offensive methodology framework, Parrot Labs educates defenders to locate and respond to malicious threats with the Survey, Secure, Protect and Recover method, and instructs cyber leaders about the cyber threat landscape.

KeyW is a pure-play national security solutions provider for the Intelligence, Cyber and Counterterrorism Communities’ toughest challenges. We support the collection, processing, analysis and dissemination of information across the full spectrum of their missions. We employ and challenge more than 2,000 of the most talented professionals in the industry with solving such complex problems as preventing cyber threats, transforming data into intelligence and combating global terrorism. For more information, please visit www.KeyWCorp.com or follow KeyW on Twitter @KeyWCorp.
CONTACT US

cybertraining@keywcorp.com
410.904.5200
KeyWCorp.com/cyber-mission-training
@KeyWCorp