Q: How many of the Fortune 500 are compromised?
A: 500

- Mikko Hyppon, @mikko

Cyber Mission Training for the Real World

Hands-on courses from Parrot Labs offer Cyber Offense, Defense and Programming skills that go beyond theory

Cyber terrorists, organized crime and other "bad" actors focus tremendous effort on finding the weak links in government and business IT. When successful, these weak links provide access to valuable information or back doors to even bigger targets, including critical infrastructure and networks. Therefore, your organization's security methods must be as sophisticated and as unrelenting as the adversary's attack methods or else your proprietary tools and information won't be private for very long.

KeyW's Parrot Labs delivers in-depth cyber security curricula developed from real-world expertise defending the largest agencies and enterprises in the world. Parrot Labs delivers relevant training to help identify and mitigate real world threats. Our instructors assess, train, and prepare numerous cyber professionals using state-of-the-art classrooms and equipment.

The courses listed below provide the building blocks for information technology and cyber teams to grow their skills in protecting their systems. Students who successfully complete these courses will receive a deep understanding of the latest methodologies, practice their skills in a simulated real-world environment, and develop advanced cyber defensive abilities.

Network Exploitation	Offensive Methodology & Analysis
	Windows Exploitation & Analysis
Forensics	Tactical Digital Forensics
Cyber Leadership	Cyber Leader Course

Due to the technical skill set being developed, a strong background in information technology is recommended to qualify for these courses. These courses are taught at KeyW Headquarters in Hanover, MD. Customized classes can also be developed for delivery at a customer's site. For more details, visit www.keywcorp.com/cyber-mission-training.

Offensive Methodology & Analysis (OMA)

This two week course teaches students current cyber-attack methods in order to develop business strategies to protect and defend their networks and critical information. Classroom discussion and exercises focus on client-side exploitation and botnet deployment using a realistic targeting network with network devices and populated active directory domains that immerse students in a simulated corporate system much like the one they protect and maintain in real-life. Students have the freedom to explore detailed scenarios within a sandbox network that includes routers, firewalls, and computer systems built on Unix and Windows operating systems to develop and hone their skills.

Tactical Digital Forensics (TDF)

This two week course teaches students to perform the fast and efficient digital forensics required to discover and investigate an Advanced Persistent Threat. Students learn the types of tactics and procedures a threat actor uses to evade detection, and develop the real-world skills to locate malicious elements on a network and respond appropriately. Students acquire a fundamental understanding of how to effectively discover breaches and triage attacks within a network. A hands capstone exercise assesses students' abilities in response to an intrusion detection incident and grades each individual on the user of forensics analysis techniques to determine the attack method, associated implants, embedded tools and files, attack timeline, and origin of the attack.

Windows Exploitation & Analysis (WEA)

This one week course teaches the essentials of remote network exploitation by demonstrating the methodologies in a coherent framework for use in developing business strategy to protect and defend networks and critical information. Students will learn how to analyze remote Windows networks, locate user credentials, and expand access across a network. WEA provides an in-depth look at the essentials of remote network exploitation, from scanning and enumeration of a network space to performing client-side attacks. This course is for computer network professionals, software developers, and security professionals who are responsible for protecting Windows networks and data from threats.

Cyber Leader Course (CLC)

This two day course introduces leaders to the processes, techniques, and terminology used by cyber professionals to explain, discover, and prevent threats to enterprise networks and sensitive business information. Students in this class take on the role of a hacker and learn to attack a private company in our lab environment using real techniques and easily accessible tools. The exercises in this course are designed to teach leaders to make better decisions in order to protect their organization's critical information. Students will leave the class with in-depth knowledge of the current cyber environment, modern exploitation techniques, and the technical terminology used by security professionals

cybertraining@keywcorp.com | 410.904.5200 | www.keywcorp.com/cyber-mission-training

Parrot Labs
CYBER MISSION TRAINING