R9B

R9B CYBERSECURITY TRAINING

BUILDING THE FOUNDATION

We believe knowledge is the fundamental building block in developing the next generation of cybersecurity operators and analysts. Our curriculum combines a thorough understanding of cyber tactics, techniques, and procedures with handson technical skills needed to confidently confront and defend against a range of cyber adversaries. Each course is led by an expert instructor, eager to pass on lessons learned in the ongoing effort to secure enterprise infrastructure. Class participants will be challenged, but those who successfully complete courses are rewarded with official certification and a deeper knowledge base from which they will launch and add value to their professional journey.

ATT - ADVERSARY TACTICS AND TECHNIQUES (5 WEEKS)

The five week Adversary Tactics and Techniques course is an intense hands-on course that teaches students the methodology and technical details of how attackers recon, gain access to, pivot, and remain hidden within a target network and any artifacts their actions may leave behind. Whether students are on a path to become pen-testers, red team members, or cyber defenders, the Adversary Tactics and Techniques course prepares students to excel by establishing a foundation in operational cyber exploitation methodologies. This course enables students with a basic understanding of computers and computer networks to execute fundamental exploitation operations in Windows and Linux environments.

CTIA - CYBER THREAT INTELLIGENCE ANALYSIS (1 WEEK)

The one week Cyber Threat Intelligence Analysis course teaches network defenders to collect, analyze, and apply targeted intelligence to defensive operations in order to proactively act on and adapt to sophisticated, dedicated attacks by cyber adversaries. This course applies the intelligence analysis process to the full-spectrum cycle of proactive network defense. The principle objective of this course is to equip network defenders, intelligence analysts, and other security operations personnel with a modern methodology to characterize, investigate, attribute, and respond to advanced cyber threats in a collaborative, real-time environment.

HUNT (WINDOWS) (1 WEEK)

The one week HUNT course for Windows operating systems introduces cybersecurity professionals to the digital arena of real-time, proactive adversary detection and identification. This course teaches students how to efficiently characterize and interrogate remote Windows systems to collect, analyze, and identify advanced cyber threats that evade traditional detection mechanisms. Students will demonstrate the ability to recognize indicators of malicious code, lateral movement, and evidence of adversary presence within Windows hosts. This course is ideal for cybersecurity professionals to learn how to HUNT within their Windows networks for advanced persistent threats that have eluded detection by automated enterprise security solutions.

HUNT [LINUX] [1 WEEK]

The one week HUNT course for Linux operating systems provides cybersecurity professionals with methodologies to actively defend Linux systems and discover advanced threats. Students will demonstrate the ability to characterize systems, perform local and remote enumeration, collect data, and perform real-time analysis, detection, and identification of adversary attacks. Students will learn the tactics and techniques employed by adversaries with an emphasis on Linux system manipulation and persistence techniques to bypass cybersecurity systems and infrastructure. This course is designed for cybersecurity professionals to learn the skills, knowledge and methodologies required to determine if an adversary successfully avoided detection from automated security products.

HUNT [NETWORKS] [1 WEEK]

The one week HUNT course for network infrastructure focuses on preservation of the integrity of devices and systems that serve as the conduit of information across networks. This course emphasizes the aggregation, correlation, and analysis of data across multiple network systems (i.e., IDS, Syslog/Windows Events, Netflow, Authentication) to identify sophisticated and tailored adversary attacks. Students will demonstrate how to actively and passively enumerate and characterize systems, verify configurations, and validate the integrity of those systems and the data flows between them. Adversary tactics, techniques, and procedures will be replicated in a controlled environment where students will perform HUNT operations to detect malicious activity.

HUNT CERTIFICATION PROGRAM

The HUNT certification is the industry's first hands-on certification to provide cybersecurity professionals with the opportunity to prove their skills and ability to detect advanced cyber threats that defeat automated cybersecurity devices and solutions. R9B provides candidates access to a controlled environment with replicated advanced persistent threats. R9B evaluates candidates on their proficiency in: network enumeration and characterization, data collection and analysis, identification of indicators of compromise, and response actions while HUNTing for the threat actors. R9B's series of three HUNT courses [Windows, Linux, and Networks] provide the foundation and knowledge required to successfully complete this certification assessment.

POWERSHELL FOUNDATIONS FOR CYBER OPERATIONS [1 WEEK]

This one week course will educate students on the basics of scripting and PowerShell. This will ensure that all students understand the same terminology to equalize those who have had exposure to PowerShell and those who haven't. After foundational information, the course will proceed with a balance of instructor lectures and course exercises. Each lesson will progress the student, leveraging information learned from previous lessons to create a study flow of development and concept reinforcement.

PYTHON FOR CYBER OPERATIONS [1 WEEK]

This one week course provides an overview of Python scripting and programing for cyber operations professionals. Students will learn to craft efficient, maintainable code that controls program flow and allows for code reuse. Then, they will apply the Python skills developed in this course to demanding scenarios and challenges with a focus on cyber operations.

ABOUT R9B

Based in Colorado Springs, CO, R9B (root9B, LLC) is a leading provider of advanced cybersecurity services and training for commercial and government clients. Combining cutting-edge technology, tactics development, specialty tools, and deep mission experience, R9B personnel leverage their extensive backgrounds in the U.S. Intelligence Community to conduct advanced vulnerability analysis, penetration testing, digital forensics, incident response, industrial control system (ICS) security, and active adversary pursuit (HUNT) engagements on networks worldwide. For more information, visit root9B.com.

TO LEARN MORE, VISIT

ROOT9B.COM