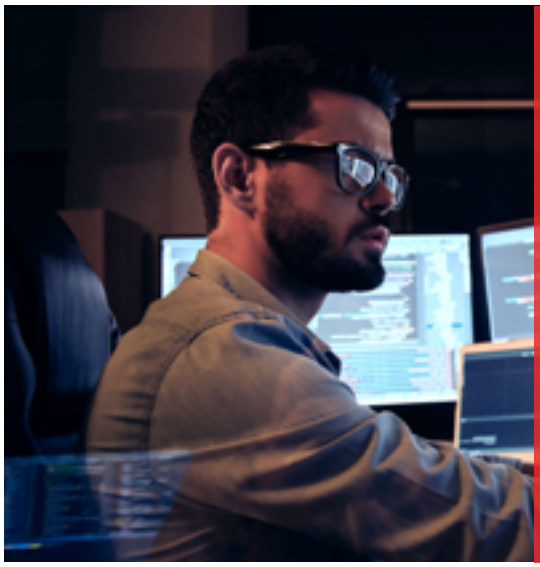
k>fivefour

RED TEAM TRAINING PROGRAM

TRAINING THE NEXT GENERATION OF CYBER OPERATORS

OUR MISSION

k>fivefour's mission is to empower cybersecurity professionals through superior, hands-on cyber operations training. We believe that cybersecurity is an applied, skills-driven domain, whose practitioners must be able to demonstrate their abilities through hands-on training and certification. This approach ensures those who are certified Red Team operators have demonstrated the ability and aptitude to conduct cyber operations. In short, they can 'walk the walk'. We believe students should be taught by experts, with decades of combined experience in real-world cyber operations, and a true passion for their tradecraft. This ensures our students learn the latest techniques, and that our training is current and relevant to today's threats.



"Hands down this was the best Red Team Operator training course I've attended. The hands-on labs were the best I've encountered yet and the instructors were prompt and extremely helpful."

MEET THE K>FIVEFOUR PROGRAM

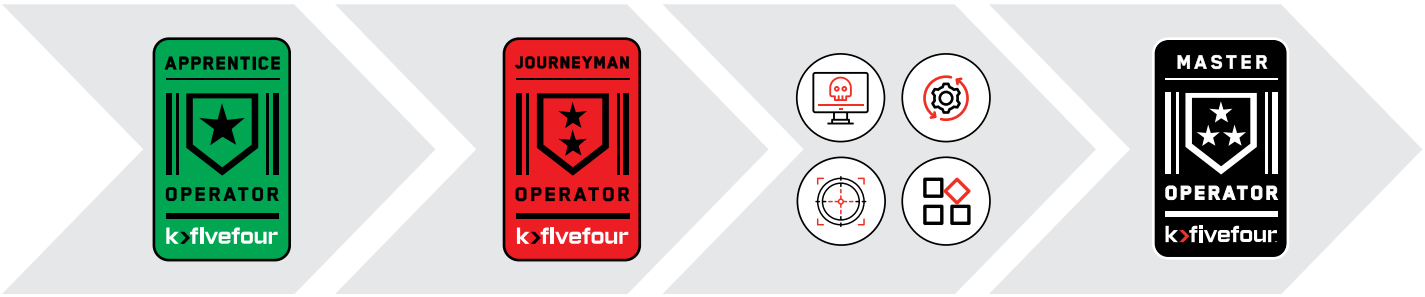
- Courses instructed by red team operators
- Portrayal of holistic Red Team mentality and methodology
- Tradecraft and techniques that are applicable in today's target environments
- Realistic scenarios and infrastructure
- Courses developed based on current techniques used in real-world operations
- A hands-on prove it exam

RIGOROUS CERTIFICATION STANDARDS

All **k>fivefour** courses end with a comprehensive hands on certification examination that challenges students to use knowledge gained in the course to conduct a simulated cyber operations assessment. This assessment is then audited to ensure quality Red Team tradecraft was used.

CERTIFICATION PROGRESSION

The **k>fivefour** Red Team Training Program uses a tiered model that aligns operator skills to expected job duties. To attain each operator level, an individual must complete the appropriate course and pass the certification exam.



RED TEAM APPRENTICE

Students start the Red Team Training Program progression by enrolling in and passing this 6 day course.

RED TEAM JOURNEYMAN

Students wishing to take their Red Team skillsets to the next level can attempt the 10 day Journeyman Course and exam.

SPECIALIZATION COURSES

Students may enroll in any of the upcoming **k>fivefour** specialization courses.

RED TEAM MASTER

Students who certify in two **k>fivefour** specialization courses may choose to enroll in this course.

CERTIFICATION CREDENTIALS

When an individual enrolls in the **k>fivefour** Red Team Training Program by signing up for RTAC, they receive a **k>fivefour** backpack with designated areas for operator certification patches. When an individual passes a certification exam, they are assigned a unique operator number and a certification kit containing: a certification patch, a metal operator ID card engraved with the individual's name and operator number, and a paper certification.

BATTLEGROUNDS

k>fivefour Battlegrounds is an online training environment that enables students to continually train, augment, and perfect their cybersecurity skills. Available 24/7, using only a web browser, Battlegrounds does not require any special software to use. Users are given a set of credentials to login and access their unique subscription-based training environment. During each course, students utilize Battlegrounds as their virtual lab. This virtual training environment allows students to stop, continue, save, and reset to a clean state at any time during their training session. These persistent sessions allow students to pick up where they left off with their attack platforms intact to continue mastering the tactics, techniques, and procedures they learn each day.

INDIVIDUALLY ASSIGNED VIRTUAL ENVIRONMENTS

All Battlegrounds environments are isolated to ensure students have complete control over their own virtual machines and will not interfere with other students in Battlegrounds.

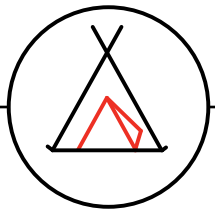
"I've been through many virtual environments such as Pentester Academy's, HackTheBox's, Offensive Security and Zero Point Security and this was (by far) the most realistic virtual environment of them all. Everything was very real world and I thoroughly enjoyed my time in Battlegrounds"

BATTLEGROUNDS FEATURES

- Available 24/7 via web browser
- Independent non-shared environments
- Contains course-specific toolsets and lab environments
- Contains unique, custom-built Red Team attack scenarios at various difficulty levels
- Ability for students to upload open source toolsets
- Fully built active directory forests contain trusts, users, etc
- Team mode: Allows users to share their environment with other Battlegrounds users

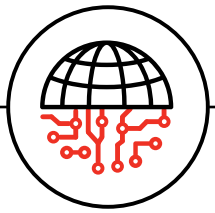
BATTLEGROUNDS SCENARIOS

Battlegrounds access comes with a number of Red Team attack scenarios that drop students into completely new enterprise environments to challenge their cyber operations skillsets. These scenarios are assigned a difficulty rating along with a short description of what the student can expect as they complete them. **k>fivefour** developers are constantly building and publishing new Red Team attack scenarios that contain the latest popular cyber security techniques/vulnerabilities.



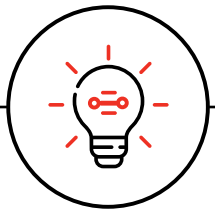
RTAC+

Designed and customized for students who successfully pass RTAC. Challenge your newfound Apprentice skills by pivoting throughout the Campgrounds domain to eventually discover and generate effects against a "hardened host" which contains trade secrets about an upcoming Campsite location. Students learn new tunneling techniques, compromising insecure fileservers, and more.



GAMEPLANET

Our hardest scenario to date! Gameplanet has tasked you to evaluate their large sprawling enterprise network and determine if potential adversaries could gain access to their intellectual property. Full of twists and turns as you complete this scenario you may realize there are other "actors" at play in the Gameplanet network. It is recommended students complete RTJC before attempting this scenario.



LINKLIGHT

A smaller company with an even smaller digital footprint, Linklight has tasked you to evaluate their DMZ implementation and ensure it is properly isolated from their corporate assets. Students who choose to complete this scenario will encounter a world of new Linux systems, SQL servers, remote code execution exploits, and more!

CONSTANTLY EVOLVING

Battlegrounds is the platform that all **k>fivefour** cyber security courses leverage for realistic hands on cyber security scenarios. This platform is in use daily as customers continue to practice, refine, and learn new cyber security toolsets. As such, Battlegrounds is constantly being updated and evolving with new features, scenarios, and requirements.

While our team is continuing to develop new scenarios, we encourage all students to submit feedback and feature requests. This ensures Battlegrounds continues to evolve as it becomes the industry standard platform for realistic cybersecurity training.

RED TEAM APPRENTICE COURSE (6 DAYS)

The Red Team Apprentice Course (RTAC) leads students through fundamental security topics and covers Red Team operations to prepare them for a career in emulating nation-state level cyber threats and adversaries. Over five class days, students are guided through a hands-on, engaging, lab-driven network attack scenario, utilizing our purpose-built training environment, Battlegrounds. Students who successfully pass the Apprentice certification exam are deemed **k>fivefour** Red Team Apprentice operators.

RTAC EXAMINATION

RTAC concludes with a nine hour (on the 6th day) hands on certification examination. Using Battlegrounds, students conduct an assessment from start to finish, using the skills and tradecraft taught during the Red Team Apprentice Course. Students may pass this exam by completing the assessment within the time allotted, and following proper techniques expected of a Red Team Apprentice operator.

REQUIRED PRE-REQUISITES

- Experience using command line applications
- Experience navigating a Windows or Linux file system via command-line (cd, ls, dir)
- Understanding of the TCP/IP model (common ports/services)
- Experience typing specific and technical commands
- Basic understanding of Active Directory users/groups
- Basic understanding of the operating system concepts such as processes, user accounts, permissions and privileges

"The Red Team Apprenticeship course exceeded my expectations. The instructor clearly had relevant, hands on experience and was able to teach in an understandable way. The hands-on labs really helped solidify the topics covered and I feel confident I can take the knowledge gained and apply it to my current job."

LEARNING OBJECTIVES

1. ***Red Team Foundations***
   - Networking
   - Active Directory
   - Windows Registry
   - Microsoft Command Line utilities
2. ***Mission Preparation***
   - Rules of Engagement
   - Setting up attack platform and C2 infrastructure
   - Activity Logging
3. ***Open Source Intelligence (OSINT) Collection and Analysis***
   - OSINT collection techniques
4. ***Active Reconnaissance***
   - Nmap scanning techniques
5. ***Target Exploitation***
   - Gaining initial access utilizing various techniques/vectors
6. ***Post Exploitation Activities***
   - User and system-level persistence techniques
   - Privilege escalation
   - Active Directory enumeration
   - Active Directory domain pivoting
   - Generating/manipulating Authentication Tokens
   - Process Migration
   - Remote execution methods
7. ***Mission Objective***
   - Targeted Active Directory data mining
   - Tunneling to Linux systems
   - Keylogging

LEARNING OBJECTIVES

- Microsoft Windows COM Object Hijacks
- Remote Code Execution (RCE) Exploitation
- Web shell customization/deployment
- C++ Hijack DLL's Creation and Deployment
- C# Assembly Payloads Creation and Deployment
- Build, Configure, and Secure Covert Infrastructure
- Windows Active Directory Enumeration
- Windows Privilege Escalation
- Domain Fortification
- Advanced Remote Execution
- Advanced User and Administrative Persistence
- Domain Pivoting
- Privilege Escalation
- TCP/IP Tunneling Techniques
- Linux Tunneling
- Antivirus Bypass Techniques
- Advanced Initial Access Execution Techniques
- Payload Obfuscation
- Advanced Lateral Movement Techniques
- Shellcode Generation and Deployment
- Local Privilege Escalation Enumeration

RED TEAM JOURNEYMAN COURSE (10 DAYS)

The Red Team Journeyman Course (RTJC) is a ten-day course (two certification days included) that challenges Apprentice certified operators to grow their cyber skillsets and master new and advanced Red Team techniques. RTJC students launch themselves into a completely new **k>fivefour** Battlegrounds environment gaining initial access, escalating privileges, pivoting between domains, and finally setting up complex TCP/IP tunnels through Linux machines to compromise a hardened enclave. With 37 individual labs and 40+ virtual machines in the Lab network, this course is for operators wanting to take their skillsets to the next level.

RTJC EXAMINATION

RTJC concludes with a nineteen hour hands-on certification examination. This exam challenges students to demonstrate in a lab environment what they learned during their scenario based Red Team course instruction. To pass, students will be evaluated to determine if proper Red Team tradecraft was used.

REQUIRED PRE-REQUISITES

- Expert mastery of all RTAC techniques and tactics
- Experience using complex command line applications
- Advanced experience with networking and a basic understanding of TCP/IP tunnels
- Basic understanding of programming principles (IF statements, variables)

"Great course content containing real world tools and techniques, excellent instructors, and the training you need to force you to think outside of the lecture materials. I definitely added more than a few new techniques to my tool kit during this class."

RED TEAM MASTER OPERATOR

After certification as a Red Team Journeyman operator, students have the option of pursuing the final certification in the training program, the Red Team Master operator.

Red Team Master operators are the experts in Red Team tools, techniques, and tradecraft. To become a Red Team Master operator, a Journeyman operator must take and certify in any 2 of the available upcoming **k>fivefour** specialization courses.

After meeting the specialization certification requirements, prospective Master operators enroll in a 1-week culmination course that includes: various cyber-attack scenarios, a two-day hands on certification examination, and a technical board with 3 existing master operators.

UPCOMING SPECIALIZATION COURSES

NETWORK EXPLOITATION

REVERSE ENGINEERING/ MALWARE ANALYSIS

OFFENSIVE FORENSICS/HUNT

WEB APPICATION EXPLOITATION

The Red Team Master certification will be reserved for those few passionate individuals who have truly mastered Red Team operations.

JOB QUALIFICATION REPORT (JQR)

The Apprentice and Journeyman Job Qualification Report (JQR) contains 200+ learning objectives and goals students should complete as they work towards certifying as an Apprentice or Journeyman operator. Each line item asks the trainee to describe a topic or to perform a hands-on activity in a virtual environment.

The JQR is an excellent tool organizations can use to track employee training progress as they complete each learning objective. Each individual training objective is certified by a senior operator in an organization ensuring the trainee demonstrated mastery of that specific objective.

"This training course was an extremely helpful introduction to red team concepts and I'm leaving here confident I can hop on a keyboard and assist my team with ops."

	Millennium Red Team Apprentice JQR - Knowledge	Certifier Initials	Certified Date
1	**Phase 1 - Mission Preparation**		
1.1	**Authority / ROE**		
1.1.1	Describe what needs to be in place before any Red Team operation may begin.		
1.1.2	Explain what a Rules of Engagement (ROE) is to a Red Team operation.		
1.1.3	Explain the Red Team concept of "non-attribution" when it comes to reporting specific users.		
1.1.4	Define what a trusted agent is and discuss the importance of having one in place.		
1.2	**Deconfliction**		
1.2.1	Explain deconfliction in regards to Red Team operations.		
1.2.2	Discuss the purpose of deconfliction in Red Team operations.		
1.2.3	Explain the importance of conducting deconfliction accurately and timely.		
1.3	**Scoping**		
1.3.1	Describe the difference between an IP blacklist and an IP whitelist.		
1.3.2	Describe the difference between a black box and white box test.		
1.3.3	Explain what a "white card" is and its importance.		
1.3.4	Explain the difference between a traditional penetration test and a Red Team assessment, as well as how their goals differ.		

Sample Excerpt of the Apprentice JQR.

MEET OUR TEAM

k>fivefour employees have decades of cyber operations experience supporting various DOD Red Teams, developing Red Team toolsets, leading teams, and even training upcoming DOD operators.

BEN CLARK

Chief Technology Officer (CTO)

Ben started his career in the Intelligence Community 18 years ago and now leads a team of 50+ Red Team operators directly supporting multiple certified DOD Red Teams. As one of the creators of k>fivefour, he helps drive the technical vision and strategy for both Millennium and k>fivefour. He has published several books, including the Red Team Field Manual (RTFM).

MATTHEW HULSE

Chief Information Security Officer (CISO)

Matt has 19 years of experience in IT, with 13 of those in Red Teaming, supporting dozens of assessments for military and commercial clients. Currently serving as Millennium's Director of Cybersecurity and Solutions, he manages the k>fivefour team, as well as Millennium's corporate cybersecurity and IT infrastructure. Matt designed the original lab infrastructure and virtual training environments that Battlegrounds is built upon, and continues to support the team's development of new and innovative training products and solutions.

NICHOLAS DOWNER

Senior Manager, Cyber Operations Training

Nicholas has 9+ years of operations, development, and training experience supporting DOD red team customers. One of the original founders of the k>fivefour Red Team Training Program, Nicholas aided in the development of Battlegrounds, RTAC, and RTJC. Nicholas has a wide range of experience both instructing and developing red team solutions.

JACOB KINGSTON

Principal Instructor

Jacob has served various DOD organizations for over 10 years providing expert support as a senior red team operator and trainer. He currently supports k>fivefour as both a red team operator and in the training program instructing classes and continuing to develop k>fivefour training solutions.

TRUSTED IN THE DOD AND COMMERCIAL WORLD

169th CPT, Maryland Army National Guard

Army 1st IO Command

Army Core of Engineers

Army Cyber Protection Brigade

Dell Technologies

DOT&E ACO (Advanced Cyber OPFOR)

FBI (Federal Bureau of Investigation)

Intel Corporation

Naval Air Station (NAVAIR) Red Team

Naval Sea Systems Command

NAVWAR Red Team

TSMO (Threat Systems Management Office)

Training over half the DOD certified Red Teams

The Standard for Red Team Training

CYBER OPERATIONS TRAINING CENTER

Our Cyber Operations Training Center converges technical innovation, cyber operations expertise, software factory capability, and leading-edge Red Team training to create the future workforce and technical capabilities that are founded on an adversarial mentality. Our 1,650 square feet classroom space holds 30 desks, each with dual monitor setups. Each side of the room has high-definition projectors and 75" televisions for displaying content. The training center can hold over 30 students with changes to the configuration, and Millennium's legacy training classroom provides an additional 600 square feet with similar AV capabilities.

ABOUT K>FIVEFOUR

k>fivefour is a pioneering startup challenging the status quo of cybersecurity education. Founded in 2018, **k>fivefour's** flagship Red Team Training Program has helped hundreds of students develop the critical hands-on technical skills needed in the cybersecurity workforce. Our radically unique Battlegrounds experience places students 'in the action' of realistic environments that they can expect to encounter.

While our foundation is in offensive security, we strive to improve the skills and capabilities of defensive cyber professionals as well, by helping them understand what they're up against.

k>fivefour is affiliated with Millennium Corporation, the leading provider of technical expertise to the Department of Defense's Red Team community. Our instructors, developers, and operators, work hand-in-hand to support Millennium's mission, executing hundreds of cybersecurity assessments for 3 of the 11 National Security Agency (NSA) certified and U.S. Cyber Command (USCYBERCOM) accredited Red Teams. Learn more at **https://kfivefour.com/**

Phone 256.666.4417
info@kfivefour.com
kfivefour.com
340 The Bridge Street | Suite 212 | Huntsville AL, 35806