Red Team Operator Training

An Offensive Mindset

The cornerstone of Millennium Red Team Operator Training is understanding how our adversaries accomplish high-profile attacks. The training is founded in realistic attack tactics and techniques found in open source, industry threat reports on nation state attributed adversaries. This training leverages the same methodology used by our Millennium Red Team Operators and covers the same topics used to prepare them for their career in emulating nation-state level cyber attacks.

Not Just for the Bad Guys

While this training focuses on the network attack methodology of Red Team Operators, it isn't just for offensive cyber operators. Understanding attackers' motives and methodology as well as how they use the victim's native operating environments for their own gain is immensely valuable for any cyber defender.

Course Format

This course curriculum mimics the structure of nation state actors. Using individually assigned training environments, each student is tasked with conducting their own red team operation against a simulated, Windows domain network. Students spend the first 5 days in a guided, hands-on lab driven network attack scenario – followed by an optional 1 day follow-on practical certification exam to test their knowledge gained in the course.

Course Details	
Course Length:	**5 days**
Exam Format:	**8 hour practical**
Location:	**Huntsville, AL** or *Customer Location*

What We Believe

Traditional text book and classroom-based training do NOT prepare students for real world cyber operations careers. Traditional, paper-test style certifications are inadequate at measuring an individual's capabilities and knowledge.

Millennium cyber training is based on an immersive, hands-on, lab first experience. Every person benefits from understanding the way attacks work, and that **the key to a strong defense is a strong offense**.

Topics Covered

- Open Source Intelligence Collection
- Preparing successful phishing campaigns
- Methods of persistence
- Network enumeration
- Lateral movement inside target networks
- Local privilege escalation attacks
- Domain privilege escalation attacks
- Understanding Windows security model
- Data exfiltration techniques
- Cyber effects (mission impact)

Who is Millennium

Millennium Corporation is a strategic management, cybersecurity and IT consulting firm and committed partner to the Government– driven by results and people focused. We have a dedicated team of security consultants trained by the Department of Defense (DoD) including testers, assessors, trainers and instructors, hackers, administrators, and technical Subject Matter Experts (SMEs).

How to Acquire Services

Millennium Red Team Operator Training is purposely designed to make it easy for customers to engage us on a long term, short term or even ad hoc basis. Our goal is always to maximize the quality of services and minimize costs and burden to our customers.

Our access to a broad portfolio of contract vehicles and partners sets the standard for excellence – spanning the lifecycle of professional services, including:

- ARDEC LRED
- GSA IT 70
- JPEO CBD OPETS
- Seaport-e 8(a)
- SSC PAC CSRETI
- B2S2
- GSA 00CORP PSS
- NAVAIR Cyber Warfare Detachment (CWD)
- USPS OIG Penetration Testing Service

Staff Certifications

- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Offensive Security Certified Expert (OSCE)
- GIAC Penetration Tester (GPEN)
- Offensive Security Certified Professional (OSCP)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- CISSP –Information Systems Security Management Professional (ISSMP)
- Cisco Certified Network Associate (CCNA)
- Red Hat Certified System Administrator (RHCSA)
- Microsoft Certified Professional (MCP)

Case Study

Customer's Challenge:
Over the past 7 years, Red Team operators have become high-demand, low-density assets. To bridge this gap DOT&E refined and expanded the use of long-duration Red Teaming, termed the Persistent Cyber Opposing Force (PCO). PCO is far better at emulating advanced, persistent nation-state cyber threats, while more efficiently utilizing scarce Red Team resources.

Millennium's Response:
Millennium Red Team members have been instrumental in the execution of PCO activities which have identified, and rapidly addressed, serious vulnerabilities. Millennium has been able to continuously provide an extremely high level of expertise by only hiring the best in the industry. Our DoD Red Team customer said it best: "Red Teaming is extremely complex and rapidly changing, and Millennium has routinely exceeded the government's expectations. If we did not have the support of Millennium, government systems would be put in jeopardy of not being able to defend against foreign or domestic cyber invaders. Millennium has shown a great, if not unique, ability to find the right people at the right time. Millennium management has demonstrated they know brilliant cyber operators."

Millennium Contacts

Ben Clark
Director, Cybersecurity & IT
256-876-2062
ben.clark@millgroupinc.com

Keith Cromack
VP Business Development
703-447-6711
keith.cromack@millgroupinc.com

MILLENNIUM CORPORATION