CYBER TACTICS

Defense Assessments

Providing Red Team and Vulnerability Assessments to improve organizational readiness

Cyber Tactics penetration testing involves mimicking the actions of computer attackers to identify vulnerabilities in a target organization, and exploiting them to determine what kind of access an attacker can gain.

Cyber Tactics Red Team Testing employs simulated adversarial threat-based approaches to expose and exploit government Computer Network Defense (CND) vulnerabilities as a means to identify weaknesses and to improve the security posture and operational procedures used to protect Information Systems & Computer Networks.

Our Red Team exercises go a step further than traditional assessments and have the goals of improved readiness of the organization, better training for defensive practitioners, and inspection of current performance levels. The Red Team will provide insights about the existence of vulnerabilities and about the efficacy of defenses and mitigating controls already in place and even those planned for future implementation.

The Vulnerability Assessments focus on identifying critical flaws within an organizations network that could be exploited. Using manual techniques and automated tools to perform testing of security posture.

The result provides deeper insight into the business risks of various vulnerabilities by showing whether and how an attacker can compromise machines, pivot to other systems inside a target organization, and gain access to sensitive information.

- Red Team / Blue Team
- Big Data Analytics
- Cybersecurity Engineering
- Computer Forensics, eDiscovery
- Mobile Security
- IT Compliance (Audit, Consulting, Advisory) PCI, PII
- Cloud and Big Data Security
- SCADA Security
- Advanced Persistent Threat (APT) Detection
- Federal / Defense Incident Response
- Network Security Engineering, Design, Implementation
- Governance

Cyber Tactics, LLC | McLean VA | (p) 800-342-3301 | info@cybertactics.com | www.cybertactics.com