Penetration Testing

KRATOS

Identify and Mitigate Data Breaches & Maintain Compliance with Kratos Penetration Testing

Kratos Penetration Testing helps protect vital business data from external and internal cybersecurity attacks by preparing organizations to defend against social engineering and insider threats. Kratos' Penetration Testing methodology provides realistic insight into potential security gaps within an organization's networks, IoT devices, web applications and client-side applications by identifying vulnerabilities before adversaries do. Leveraging Kratos Penetration Testing Services will not only help organizations understand vulnerabilities but will also provide detailed solutions and countermeasures to reduce overall risk to critical assets.

External and Internal Penetration Testing

External testing examines various network attack surfaces that might be compromised through internet connected servers or by individuals utilizing external equipment and who lack the required credentialing. External testing provides an understanding of the attack surface, identifies potential attacker ingress points, and can locate flaws in publicly accessible infrastructure. Kratos external penetration testing supports the following testing types:

- Open Source Intelligence (OSINT)
- Social Engineering Testing
- Network Testing
- Web Application Testing
- API Testing
- Client-Side Application Testing

While external testing examines avenues that might be hacked with external forces remote hackers might use to breach networks, internal testing simulates an insider threat (e.g., compromised workstation or malicious employee). Such testing identifies routes for privilege escalation or pivoting, locates egress points for sensitive information and identifies vulnerable hosts and services.

Application Penetration Testing

For hackers and malicious insiders, web applications and client-side applications represent an opportunity to seize valuable data or launch a cyber-attack. Kratos Application Testing uncovers vulnerabilities in code and violations of secure programming best practices to uncover backdoors, and identify poor input validation, unchecked buffers, and session strength.

Client-Side Application Testing

Kratos' client-side application testing currently supports Android, iOS, MacOS, Windows, and Linux (common flavors) operating systems.

Basic Methodology

- OSINT
- Content and Functionality Mapping
- Code Analysis
- Permissions Review
- Review of Log Data and Local Cache
- Authorization Exploitation
- Data Storage Exploitation
- Data in Transit Exploitation

Benefits of Secure Applications

- Mitigate cybersecurity risk
- Identify software development life cycle weaknesses
- Raise awareness of application security
- Prevent downtime and improve productivity
- Identify vulnerabilities before they are exploited

Vulnerability Assessments

Kratos' Vulnerability Assessments evaluate the overall security of an organization's network, operating system, web applications and web server for exploits or vulnerabilities. This provides a valuable baseline for determining appropriate safeguards and helps comply with federal regulations.

Kratos uses a combination of industry tools (open source and commercial software) and in-house techniques to probe the network for vulnerabilities, test the integrity and effectiveness of Internet-facing elements and identify potential areas of risk. Kratos then analyzes scan results and provides detailed, pragmatic guidance to prioritize vulnerabilities and enact quick, effective remediation.

Benefits of a Vulnerability Assessment

- Improve organizational security posture through vulnerability identification and remediation
- Minimize downtime by discovering vulnerabilities before they become security incidents
- Eliminate false positives with expert custom analysis, which is included as part of the vulnerability scan
- Meet regulatory and government security requirements (e.g., FedRAMP, FISMA, PCI, and NIST)

Red and Purple Teaming

Kratos' penetration testers are skilled at red team exercises, purple team exercises, and other hacker simulations. Testers can deploy customized malware simulations, compromise hosts and services while evading detection, and perform credential harvesting. Organizations that need to understand the real-world impact of weaknesses in their systems can use these exercises to help prioritize logging and monitoring and identify where efforts provide the most protection.

About Kratos Cybersecurity Services

Kratos cybersecurity services support the development and operation of proactive cybersecurity programs, the development of enterprise cloud security strategies, and the establishment of sound and practical information security architectures tailored to organizational needs. With years of robust compliance and certification experience in government and commercial standards requirements as an authorized Federal Risk and Authorization Management Program (FedRAMP), authorized Third Party Assessment Organization (3PAO) and more recently, a Cybersecurity Maturity Model Certification (CMMC) C3PAO, Kratos is viewed as a trusted compliance and governance partner by the Department of Defense (DoD), Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations.