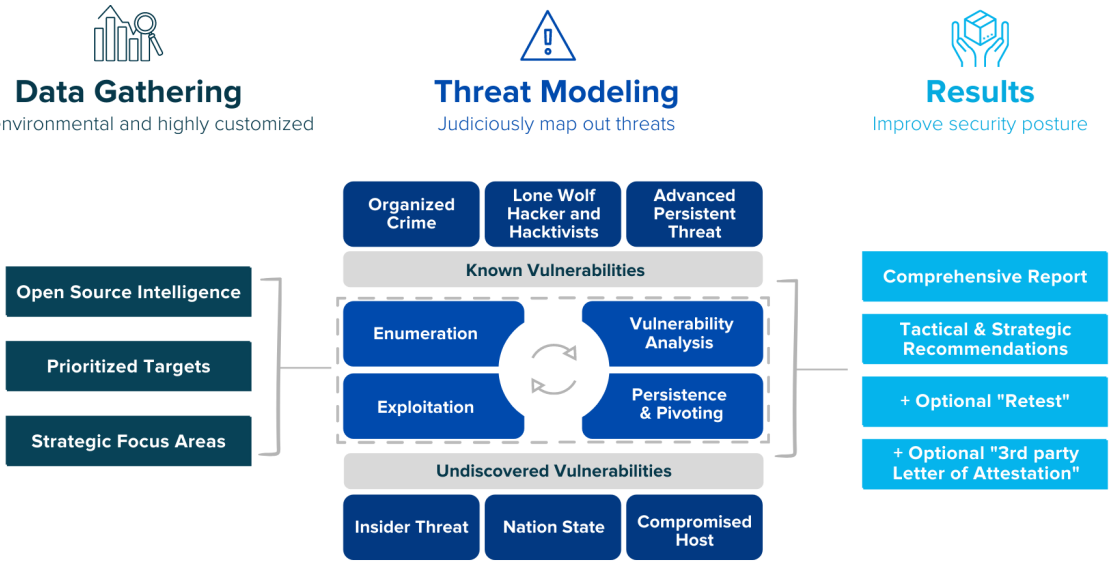
K logix
Be confident.

K logix Network Penetration Test

K logix's Network Penetration Testing Services provide measurable value through the identification, detailed assessment, and exploitation of network and system assets. Security controls are often measured by their intended value, but security teams may best identify gaps in implementation through active attempts at exploitation.

K logix Penetration Testing Services provide in-depth assessments of security posture and maturity to our clients through tailored penetration testing methodologies. Our penetration testers provide expertise in identifying and exploiting vulnerabilities across a wide variety of environments and technology stacks. Our testing services are intended to simulate adversary techniques and tactics, often chaining together several vulnerabilities to achieve compromise. The output from our assessments provides vulnerability details, exploit replication, actionable remediation guidance, along with strategic and tactical recommendations to mitigate risk and improve security posture.

METHODOLOGY



K logix's highly customizable approach to testing incorporates areas of client concern and prioritization in addition to common attack surface based on network design and technology stacks.

Penetration testers dedicate time to enumerating a network asset inventory coupled with Open Source Intelligence (OSINT) data gathering techniques. Our testing team identifies gaps in target systems by leveraging decades of offensive security experience to find areas of potential exploitation.

Areas of coverage incorporate the latest security threats including: Active Directory, cloud technologies, IoT, patch management, deployment configuration, architectural, and common internal and external threats. In some instances, coverage may include web applications, social engineering, API security, physical security, and wireless.

K logix
Be confident.

Network Penetration Testing Results

Deliverables include a comprehensive penetration test report including industry-leading tactical and strategic recommendations. These include reproduction steps of techniques and exploits used to successfully achieve an end-to-end proof-of-concept, which can be used in validation of identified issues by remediation teams.

Deliverables are tailored to individual organizational needs and may include these focus areas:

External Assessments

Simulation of external threat actors with only Internet access to client resources assumed. Open-Source Intelligence and reconnaissance, attack surface mapping, exploitation of vulnerable services, security misconfigurations, and weak or default passwords to gain access to internal network.

Internal Assessments

Simulation of internal threat actors or assumed breach from external threat actors. The exploitation of vulnerable software, security misconfigurations, weak credentials, from the perspective of initial unprivileged internal network access.

Windows/Active Directory Environments

Kerberos misconfigurations, man-in-the-middle attacks, weak access control, delegation token abuse, password attacks, insecure file shares, operating system and software vulnerabilities, enterprise patch management, and more.

Linux/Unix Environments

Remote exploitation of vulnerable services, SSH password attacks, weak protocols, misconfigured NFS or Samba shares, privilege escalation, Java application vulnerabilities, database systems, operating system and software vulnerabilities, and more.

Wireless

Evaluates the effectiveness of authentication and encryption mechanisms within both authorized and rogue wireless access points, client interaction with wireless SSIDs, and identification of insufficient network segmentation between guest and employee networks.

Social Engineering

Targeting the human element of organizations to gain access to sensitive information, infrastructure, and other critical pieces of data could lead to or enable further attacks on the organization. Launch campaigns targeting specific users and groups such as phishing and spear-phishing, vishing, false websites, and other methods.

Cloud Environments

Identify gaps between security best practices and configuration of products and services. Assess IAM roles for excessive permissions. Discover exploitable applications and services that may enable pivoting into private clouds or other internal networks.

Security Host Configuration Review

A detailed review and verification of configuration settings of operating systems, network devices & applications to measure the security effectiveness of controls in place and perform gap analysis against standard security frameworks, such as NIST or CIS.

K logix
Be confident.

Network Penetration Testing Results

Matching client objectives with outcomes may include focusing on these objectives to add further value:

TARGETING OF CRITICAL DATA

Target access to PII/PAN/PHI data stored in SQL, NoSQL, Redis or other datastores, and simulated data exfiltration.

COMPROMISE OF CRITICAL ACTIVE DIRECTORY ASSETS

Focused on accessing domain controllers, critical service and administrative accounts, and high value targets such as C-level executives.

TARGETING OF DEVELOPMENT AND RELEASE WITHIN CI/CD PIPELINE

Targeting areas of an organization's CI/CD pipeline to identify threats and assist in securing connections between components. Identification of weak access control and overly permissive objects and build automation, leaked secrets or shared passwords, vulnerabilities in underlying development technologies, and test application security stance with Dynamic and Static Analysis Security Testing (DAST & SAST).

GAIN FOOTHOLD TO INTERNAL INFRASTRUCTURE

Assess the network perimeter and identify gaps in coverage that may allow unauthorized access to network resources or allow for entry into the internal network environment. Elements may include:

- Creating an external asset mapping
- Targeting weak user credentials
- Targeting unpatched assets
- Externally facing applications
- Vulnerabilities within 3rd party software or systems

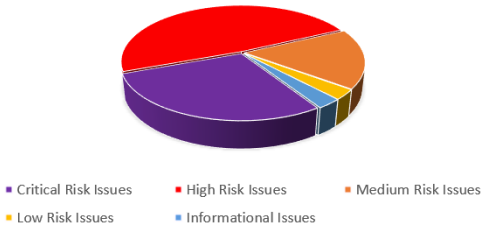
GAP ANALYSIS OF SECURITY CONTROLS AGAINST DEFINED FRAMEWORKS

Identify controls that are not configured to best practice and develop recommendations that will meet requirements that are feasible for the organization.

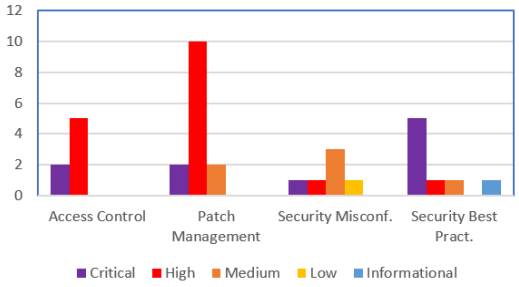
Comprehensive penetration test report includes:

- **Executive summary**: Overview of the attack chain and key findings in a digestible narrative form.
- **Comprehensive risk scoring**: Factors in impact and likelihood of vulnerability exploitation.
- **Graphical breakdown**: Includes discovered vulnerabilities by criticality and by vulnerability category.
- **Individual vulnerability details**: Breakdown and background information on discovered vulnerabilities with replication details and actionable remediation steps.
- **Tactical and strategic recommendations**: Technical and policy-oriented security

Sample: Vulnerability Risk Severity Breakdown



Sample: Vulnerability Category Breakdown



K logix

Be confident.

Network Penetration Testing Outcomes

Identify security gaps within the network environment through attack simulation, verification and validation of security controls.

Assist organizations and security teams in covering common problem areas to better defend networks, systems and build layered defenses and robust security programs.

Deliver value to teams and organizations with thoughtful approaches to recommendations and remediations with high-level strategies and tactics for improved security posture.

Identify critical network security vulnerabilities that could be exploited by malicious threat actors.

Highlight issues by criticality and risk scores, allowing effective triage of highest impact vulnerabilities.

Categorize vulnerabilities to identify areas of strength and weakness in the network security posture.

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.