GOTHAM SECURITY

AN ABACUS GROUP COMPANY

Risk Reduction

White Box Network Penetration Testing

We identify technical, architectural and logical design vulnerabilities that contribute to the risk profile (confidentiality, integrity, and availability) of your organization's data and information systems. Our process entails a hybrid approach of utilizing both OWASP v4 and PTES (Penetration Testing Execution Standard) guidelines, which results in a robust white box base testing framework that spans over 80+ security testing procedures.

Objectives:

- Collect, scan and analyze information system configurations in order to generate a prioritized comprehensive list of environment vulnerabilities, weaknesses and risks. These include:
  - Network / server / virtualization / storage infrastructure
  - Workstations
  - Operating systems and mission critical applications
- Outline the potential impact and severity of each vulnerability, weakness, and risk including observed deviations from standard information security best practices and principles.
- Identify the root causes behind the vulnerabilities, weaknesses, and risks that were identified in the assessment, while conveying how those problems relate to the inherent security posture of your organization.
- Provide your organization with a full due diligence report including information such as:
  - Vulnerability/weakness/risk details
  - Risk mitigation recommendations
  - Analysis methods
  - Information system statistics
  - Network diagrams
  - And more...

Standard Engagement Process:

Typical Timeline of Initial Test: Dependent on environment complexity
Scheduling Kickoff: Within 2 weeks after ROE is signed
Remediation Retest Policy: Free within 30 days of initial report delivery

- Once the client has financed the project, Gotham Security will provide the client with a Rules of Engagement (ROE) document that outlines the scope of the tested client information systems, project assumptions, and Gotham's commitment to our client's information systems' Confidentiality, Integrity and Availability (CIA).
- White box analysis of client information systems requires that Gotham Security either ships or hand delivers Gotham's network scanning appliance.
- Gotham requires certain standard prerequisites to be satisfied before the project is officially started. These prerequisites include:
  - Any diagrams and documentation pertinent to network and sever infrastructure.
  - A list of all corporate VLANs / subnets (in CIDR notation).
  - A list of all point-of-interest infrastructure IP addresses (AD DC's, Hypervisors, Firewalls, Core Switches, etc.).
  - Full read-only access to all configuration files pertaining to any of the following information systems:
    - Network Infrastructure (firewalls, switches, routers, WAPs, etc.)
    - Active Directory
    - Hypervisors
    - Servers (Windows and/or Linux)

- Once the client has satisfied all the project prerequisites, Gotham Security will perform the white box network penetration testing in a 24×7 format over the course of the predefined project timeline. Special attention is provided to ensure client information system CIA remains unaffected throughout the project. During this time, Gotham focuses on assessing the client's information systems for weaknesses and vulnerabilities by collecting and analyzing corporate network traffic and system configurations.
- After the first white box network penetration test is completed, Gotham will present the report findings with the client and discuss the mitigation recommendations provided in the report.
- Gotham will provide the client with 30 days to remediate prioritized risks for their information systems.
- After the 30 day remediation period, Gotham will perform rescanning/analysis of the same information systems to validate if previous risks were indeed remediated.
- Gotham will then present and provide the client with a post risk remediation white box network penetration test report.

Dynamic / Static Code Analysis and Architecture Review

Gotham's Dynamic / Static Code Analysis evaluates both web and non-web applications. Through advanced modeling we detect flaws in your software's inputs and outputs that cannot be seen through web scanning alone. We utilize several overlapping tools and techniques including data flow analysis, taint analysis, and control flow graphs which require the software source code. The purpose of these techniques is to discover architectural and logical design vulnerabilities within the application.

Objectives:

- Analyze your organization's application software source code using many overlapping tools with a team of multiple Gotham software security engineers.
- Identify vulnerabilities introduced to the application through dependency tree structures.
- Map all input and output application data flows.
- Generate a prioritized comprehensive list of software vulnerabilities, weaknesses and risks.
- Outline the potential impact and severity of each vulnerability, weakness, and risk, including observed deviations from standard information security best practices and principals.
- Provide your organization a full due diligence report including information such as:
  - Vulnerability/weakness/risk details
  - Risk mitigation recommendations
  - Analysis methods and tools
  - Diagrams of main application functions
  - Data flows
  - Dependencies
  - And more...
- Includes technical risk management recommendations that are mapped to OTGv4 (OWASP The Guide v4) as well as OWASP SAMM (Software Assurance Maturity Model) principles.

(212) 696-0500
hello@gotham-security.com