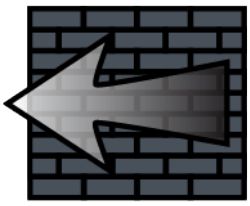

Network Assessment & Penetration Testing

Phases of Maturity in Cyber Defense

1 Integrate Security into Existing Business Processes

- Policy Program Development or Review
- Information Security Policy & Procedure Development or Review
- Information Security Risk Assessment
- Security Awareness Program Development or Review
- Disaster Recovery & Business Continuity Program Development or Review
- Secure SDLC Program Development or Review
- PII and Sensitive Information Heatmap

2 Evaluate Specific Systems Within Your Organization

- Network Architecture Design / Review
- Cloud Security & Virtual Infrastructure Security Assessment
- Server Configuration Reviews
- Firewall and Router Configuration Reviews
- VPN Configuration Reviews
- Voice over IP Assessments
- Physical Security Reviews
- Software Source Code Reviews
- Application Threat Modeling and Design Reviews
- PCI Quarterly Scans
- PCI Report on Compliance Assessment or Gap Analysis

3 Conduct Penetration Testing on Your Organization

- External Network
- Internal Network
- Wireless Network
- Web Application
- Social Engineering
- Credential Risk Assessment
- Mobile Application Assessment
- Control System (CS Baseline)

R9B

ICN has partnered with cybersecurity experts at R9B to protect corporate networks and customer information. R9B conducts penetration testing, manages security events and alerts, and actively pursues and eliminates threats through its proprietary HUNT platform, ORION.

ICN

Grimes State Office Bldg.
400 East 14th Street
Des Moines, IA 50319

icn.iowa.gov
(800) 572-3940
icn.css@iowa.gov

SERVICE OVERVIEW - SECURITY REVIEWS

Integrate Security into Existing Business Processes

Policy Program Development or Review

We will review these by applying industry best practices and applicable regulatory frameworks as the source for the reviews and resulting recommendations. The industry frameworks, standards, etc., we may apply include:

- NIST Guidelines
- SANS Critical Security Controls
- Federal Information Processing Standard (FIPS) Standards
- International Organization for Standardization (ISO) 27002
- DISASTIG
- CIS Security Benchmarks
- Other State Laws and Standards as applicable

Information Security Policy and Procedure Development or Review

Evaluating existing information security policies and advising whether the appropriate policies have been established, the degree of policy compliance, and recommend the creation of policies where needed.

Policies routinely reviewed include:

>> Incident Response | Infrastructure Growth Policy | Data Handling | Password Policy | Onboarding | Offboarding

Information Security Risk Assessment

The objective of an Information Security Risk Assessment is to provide recommendations to maximize the protection of confidentiality, integrity, and availability while still providing functionality and usability. Root9B will help our users understand how to categorize and establish thresholds for violations of established controls and when to classify violations as security events.

Security Awareness Program Development or Review

In support of in-house cybersecurity awareness and outreach, we support efforts to socialize, advocate, and inform staff on the need to maintain a steady state of cybersecurity awareness and caution. We offer both on-demand and recurring cybersecurity and security awareness training that will inform users and staff of cybersecurity threats.

Disaster Recovery and Business Continuity Program Development or Review

Our approach assists users to decide what your critical business functions are and their associated risk factors. This allows us to help you develop and implement the detailed plans of action needed to ensure your organization maintains continuity of operations before, during, and after a disaster.

Secure SDLC Program Development or Review

Guiding you in the successful development and implementation of a new (or evaluation of an existing) Systems Development Life Cycle (SDLC) program. This process review is not specific to any software development methodology, but rather is tailored to the particular organization. It is therefore applicable to organizations that use Agile-based methodologies, the Unified Process (UP), Waterfall, or any methodology in between.

PII and Sensitive Information Heatmap

We scan, locate, monitor and analyze historical data to detect where confidential data is stored and processed throughout the client's network. Root9B employs a Symantec Data Loss Prevention Enforcement Platform, a web-based management console and incident repository to perform a broad range of PII monitoring and analysis. This analysis allows us to develop detailed heatmaps showing where PII is stored and processed.

Evaluate Specific Systems Within Your Organization

Network Architecture Designs / Reviews

The purpose of the Network Architecture Design Review is to find design flaws / weaknesses and to assess the implemented architecture against industry standards and best practices.

SERVICE OVERVIEW - SECURITY REVIEWS

Cloud Security and Virtual Infrastructure Security Assessment
Data breach risk significantly increases as organizations move data into publicly accessible cloud virtual infrastructures. One of the biggest issues in virtualization and cloud security is effective implementation of virtualized access controls to prevent other virtual accounts or systems from accessing client information and systems. To address this concern, a comprehensive testing and assessment of a client's virtualized environment(s) will be performed.

Server Configuration Reviews
Proper server configuration is dependent upon business context, the server environment and the unique requirements of each server. Our approach treats server configuration reviews as one element in a larger overall security strategy. We synchronize our server security analysis and audit activities to align with your Group Policy, Active Directory, and Domain Name Server (DNS) configuration requirements.

Firewall and Router Configuration Reviews
We conduct a thorough review of the network architecture and configuration to determine if appropriate design, configuration, and access controls are in place. Scanning in-scope portions of the network using well-known automated tools will occur.

VPN Configuration Reviews
We conduct a thorough review of the VPN and its configuration to determine if appropriate design, configuration, and security controls are in place. The review will focus on VPN standards, guidelines, and procedures, as well as the implementation and governance of these activities.

Voice over IP Assessments
We will evaluate the VoIP infrastructure to determine if vulnerabilities exist. If they do, it will be determined if they could lead to network breach or facilitate future exploit attempts. An in-depth analysis of implemented protocols, system and security configurations, VoIP communication security, etc will be provided.

Physical Security Reviews
We look at security holistically and apply similar cybersecurity threat and risk mitigation strategies to physical defense of facilities. The Physical Security Assessments consists of an exhaustive search of open source intelligence on the user. This research can reveal unexpected information about the target location including staff hierarchy, interior layouts, and even employee badges.

Software Source Code Reviews
During the assessment, we will review the target code for security problems and categorize the findings based on the weakness categories (e.g., authentication, authorization). We assign each finding a risk rating of High, Medium, Low, or Informational. The findings and the weaknesses discovered will be presented in a Summary Report that your development team can use for improving code base quality.

Application Threat Modeling and Design Reviews
Application assessments incorporate guidance from the OWASP Application Security Verification Standard whereas our inventory, configuration, and architecture assessment methodology is based on practical application of the Sherwood Applied Business Security Architecture (SABSA) and National Institute of Standards and Technology (NIST) Cybersecurity Frameworks. Each assessment is tailored based on the specific requirements of the user. We also incorporate industry best practices, as well as proprietary tools and testing.

PCI Quarterly Scans
Our quarterly or annual PCI Cybersecurity Pentesting and Vulnerability Assessments meet or exceed mandated requirements set by Payment Card Industry Data Security Standard (PCI DSS).

PCI Report on Compliance Assessment or Gap Analysis
PCI Compliance reporting and analysis specifically covers PCI DSS mandated topics and is scoped, structured, and formatted for direct submission or easy integration with PCI assessment reporting mandates. By extension, root9B PCI analysis and reports provide a fuller understanding of the threat and the remediation needed to help clients protect payment data before, during, and after a purchase.

SERVICE OVERVIEW - PENETRATION TESTING

Conduct Penetration Testing on Your Organization

External Network

This testing requirement seeks to demonstrate how an attacker would gain unauthorized access to your IT environment through e-mail systems, firewalls, routers, web servers, and other network devices. The security assessment will apply standards-based methodology and a series of assessment techniques:

>> Intelligence Gathering | Vulnerability Analysis | Discovery and Probing | Exploitation | Post-Exploitation

Internal Network

We examine system/network weaknesses from inside the network. Analysts simulate a successful breach of the network to see how an attack could progress without prior knowledge of the internal network's architecture. We also consider how an insider might execute an attack given various types of access and credentials.

Wireless Network

Testing identifies the critical vulnerabilities that are present in a wireless infrastructure. Our risk-based approach focuses on the following assessment:

>> Assessing Level of Risk | Understand Vulnerabilities | Actionable Recommendations

Web Application

We use automated and manual tools to explore your websites and associated databases. The web application assessment process covers the major aspects of web application security (e.g., authentication, authorization, session management, input/output validation, injection, misconfiguration, privilege escalation, and sensitive data handling/exposure).

Social Engineering

Social Engineering assessments have increasingly become the most powerful tool to deter a network attack. We will assess the effectiveness of user training, corporate policy and procedures, and whether there are lapses in employee security vigilance. The assessment includes both technical and non-technical social engineering techniques whereby root9B analysts interact with employees to obtain network access specific information.

Social Engineering assessment are critical to understand how an adversary exploits email, corrupted documents, and social media to access your systems, and how they will use this access to attack your critical business processes.

- Phishing emails
- Direct interactions with client staff.
- Creation of fake users through LinkedIn and other social media.
- Direct or indirect contact via telephone, email, and other mediums.
- Spear-phishing campaigns with trojanized documents, web-browser hooks, or exploitation.

Credential Risk Assessment

This assessment assists users in countering the greatest source of unauthorized network access – stolen or misused credentials. Our credential assessment service maps the current state of credentials across the Windows domain and illuminates weaknesses. Our security architecture team will conduct a thorough technical, policy, and procedure assessment of your Identity Access Management (IAM) program.

Mobile Application Assessment

Your mobile applications are often just as vulnerable as your web applications. We will assess your mobile environment using the application security verification standards and industry best practices.

Control System (CS Baseline)

Applies the external and internal assessment methods, while adjusting for and tailoring each assessment methodology using the specifics of your CS implementation and its unique network attributes. Our objective is to determine an adversary's ability to reach and compromise your CS baseline from other attack surfaces (e.g., external/internal corporate networks, wireless networks).