IANS

CONSULTING SERVICE BRIEF

Penetration Testing

PENETRATION TESTING

WE DO OUR WORST SO YOU CAN BE YOUR BEST

IANS' Penetration Tests are all led by world-recognized leaders in the industry — several being founding members of the *Penetration Testing Execution Standard (PTES)*. In addition, many of the industry standard tools used in pen testing, such as *SamuraiWTF* and *MobiSec*, are projects created and run by IANS Faculty.

With more than 50 such experts to choose from, our clients can regularly rotate pen testers without the inconvenience of switching providers. IANS Faculty members each have their own styles, tool preferences, and perspectives. So, you have the chance to test your security defenses against the best, and against a constantly evolving skillset. The bad guys, unencumbered by a need to do productive work, never rest.

Consider these couple facts:

- IANS does hundreds of pen-test engagements a year
- IANS has been able to defeat the defenses of 100% of those companies that engaged us.

In the unlikely event that your organization were to be the first exception to our track record, you would have significant bragging rights (or proof points) to share up, down, and across your chain of command. More likely, we will surface vulnerabilities and recommendations for remediation.

IANS will tailor each engagement to meet the needs, concerns, and environment of your organization. Separately or concurrently we run the following types of penetration tests (authenticated and unauthenticated):

** Network   * Application   * Wireless   * Social engineering   * Physical*

For the external testing of networks, we support three approaches:

✓ ***Blackbox*** assumes no knowledge of the attack target. This approach most closely simulates what a bad actor would see and often includes social engineering components.

✓ ***Greybox*** begins with some knowledge of the target such as IP ranges, applications, and domain names.

✓ ***Whitebox*** starts with full knowledge of the attack target including the network architecture. This approach saves time usually spent in reconnaissance work (search of the internet, public sources, and social networking sites for information on the target organization.) That time savings translates into cost savings as well.

A comprehensive report details findings and recommendations, but critical findings will be communicated immediately. Working as a trusted partner, IANS' experts attack your organization in the ways a malicious adversary would use — before the bad guys get the chance to do it for real.

KEY OUTCOMES

✓ Evaluate the security of your external network

✓ Determine if the internal network is properly segmented from the rest of the network

✓ Identify vulnerabilities in the external-facing network systems and infrastructure

✓ Identify vulnerabilities in the internal network, especially those that could be leveraged to compromise any PCI-related system

✓ Attempt to gain unauthorized access to confidential information or sensitive systems

✓ Test for unauthorized access or data leakage of accounts

✓ Exploit weaknesses in the user-facing aspect of the infrastructure to gain further access to systems or data

✓ Recommend remediation and security controls to improve the security of the network

Web Application Pen Test:

- Demonstrate the ability to gain unauthorized access to an in-scope internal network
- Obtain user or service account credentials (default passwords, unsecured credentials, etc.)
- Demonstrate the ability to access data not intended for public release via an externally accessible system (SQL injection, unauthorized access using credentials, etc.)
- With a non-privileged account, demonstrate the ability to pass data for another user.

All penetration test engagements are designed, managed, and executed by industry leading security practitioners who have demonstrated hands-on experience in security architecture, operations, and innovation.

Methodology and tools

Testing is performed based on standards and guidelines including: *PCI-DSS*, *OWASP*, *ISO27001*, *NIST*, and others as needed.
The approach consists of four steps: reconnaissance (external only), mapping, discovery, and exploitation.

We use a number of open-source and commercially available tools throughout testing. Since each test performed produces different vulnerabilities and opportunities for exploitation, the specific tools utilized on every test are determined throughout the testing process. Commonly used tools include (but aren't limited to):

• Samurai WTF • BeeF • Metasploit • Nessus • NMap • DBVisualizer • Kali • Burp Suite Pro • Wireshark • Cain & Abel

Project deliverable: CRA Report

The final step of the penetration testing engagement is a written report. In addition to the written report, our clients sometimes ask us to develop and deliver an executive summary presentation to executive stakeholders.

Executive Summary	History, purpose and overview of engagement — suitable for non-technical and executive audience to understand scope and outcome of project.
Purpose and methodology	The technical reasons for the testing as well as the methodology used
Findings* & recommendations	This section is naturally the longest, most detailed, and highly technical part of the report — the substance and value of the engagement
Conclusion	Summary of engagement and findings suitable for technical audience

* Each finding is classified as a *Critical*, *High*, *Medium*, or *Low Risk*, based on considerations of potential threats, the likelihood of attack, and the possible impact of a successful attack against the organization. Each of these factors is assessed individually and in combination to determine the overall risk designation. These assessments are based on IANS' professional judgment and experience providing consulting services to enterprises across the country. Appropriate screen shots, snippets of code, and examples will be provided for each finding, as well as high-level, actionable remediation recommendations applicable for the organization's operations and technical environment.

The IANS difference

IANS (Institute for Applied Network Security) is a Boston-based decision support and consultancy organization exclusively focused on information security, regulatory compliance, and IT risk management. IANS uses a peer-based research methodology within a highly-engaged community of security practitioners. IANS faculty members are security experts recognized as ex-CISOs of Fortune 1000 companies, builders of global teams, and thought leaders across the industry.

- IANS believes strongly in taking a detailed approach with open communication
- IANS practitioners will be in contact at all times, working collaboratively with our clients, committed to both proactive and responsive contact by phone, text, and email. We meet deadlines and keep our promises.
- IANS will deliver status updates against the project plan throughout the engagement tracking overall progress, open action items, and deliverables. Critical findings will be communicated immediately — no surprises
- IANS combines expertise, advice, and execution. We don't just recommend actions, we help take them.