JacarTech Corp.

Building Trust

Information Security in a Borderless World

Network Penetration Testing Services – Internal or External

We simulate real-world attacks to provide a point-in-time assessment of vulnerabilities and threats to your network infrastructure.

Web Application Penetration Testing Services

In addition to the *Open Source Testing Methodology Manual* (OSSTMM) and the *Penetration Testing Execution Standard* (PTES) *JacarTech* application penetration testing service leverages the *Open Web Application Security Project* (OWASP), a comprehensive framework for assessing the security of web-based applications, as a foundation for our web application assessment methodology.

Mobile Application Penetration Testing Services

As the widespread use of mobile applications continues to grow, consumers and corporations find themselves facing new threats around privacy, insecure application integration, and device theft. We go beyond looking at *API* and web vulnerabilities to examine the risk of the application on a mobile platform. We leverage the *Open Web Application Security Project* (OWASP), *Open Source Security Testing Methodology Manual* (OSSTMM), and *Penetration Testing Execution Standard* (PTES) methodologies to thoroughly assess the security of mobile applications.

IoT and Internet-Aware Device Testing

Internet-aware devices span from ubiquitous, commercial *Internet of Things* (IoT) devices and systems to automotive, healthcare and mission critical *Industrial Control Systems* (ICS). Our testing goes beyond basic device testing to consider the entire ecosystem of the target, covering areas such as communications channels and protocols, encryption and cryptography use, interfaces and *API*s, firmware, hardware, and other critical areas. Our deep dive manual testing and analysis looks for both known and previously undiscovered vulnerabilities.

Social Engineering Penetration Testing Services

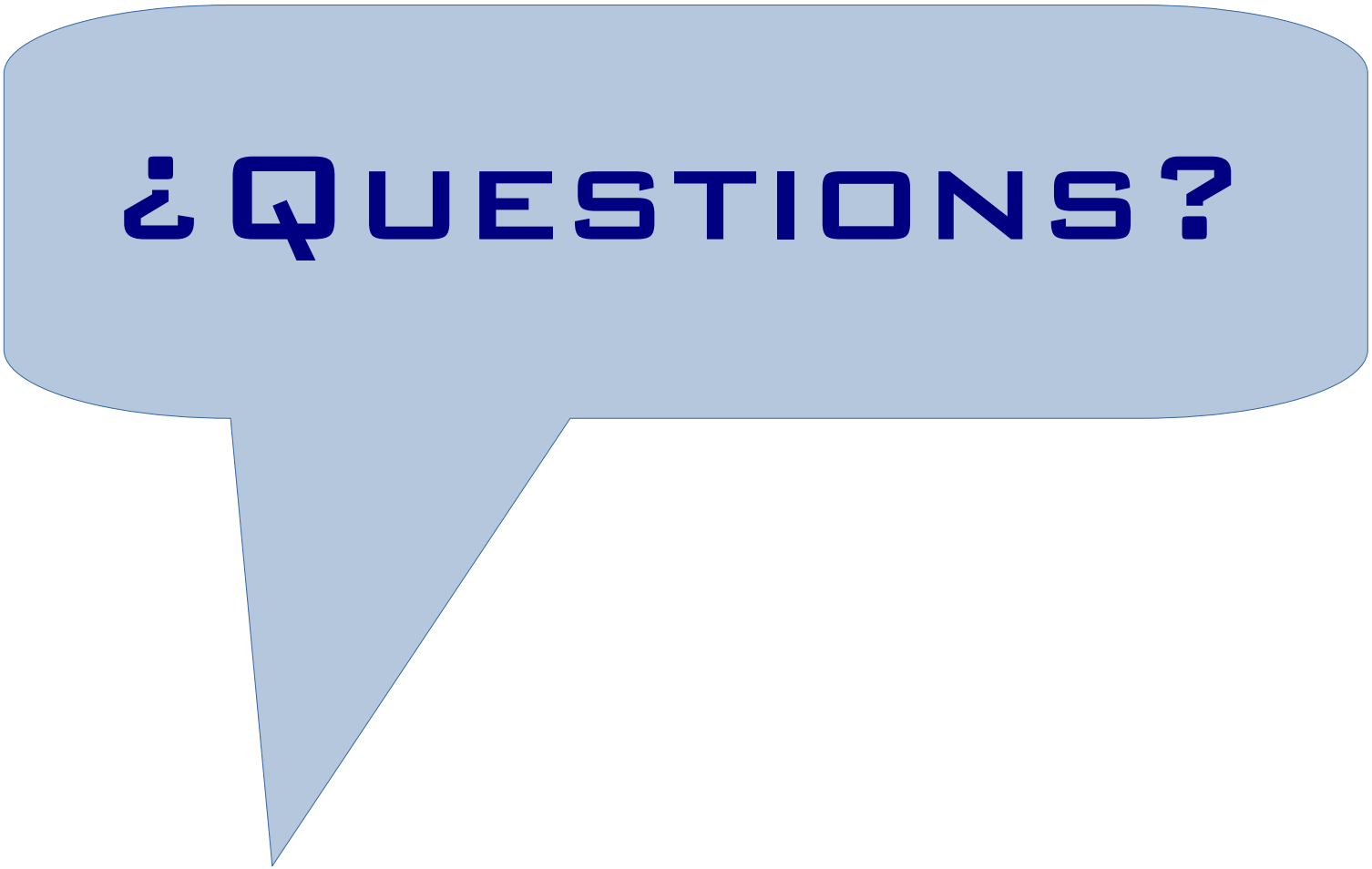
Malicious users are often more successful at breaching a network infrastructure through social engineering than through traditional network/application exploitation. To help you prepare for this type of strike, we use a combination human and electronic methodologies to simulate attacks. Human-based attacks consist of impersonating a trusted individual in an attempt to gain information and/or access to information or the client infrastructure. Electronic-based attacks consists of using complex phishing attacks crafted with specific organizational goals and rigor in mind. *JacarTech* will customize a methodology and attack plan for your organization.

Red Team Attack Simulation

Want to focus on your organization's defense, detection, and response capabilities? *JacarTech* works with you to develop a customized attack execution model to properly emulate the threats your organization faces. The simulation includes real-world adversarial behaviors and tactics, techniques, and procedures (TTPs), allowing you to measure your security program's true effectiveness when faced with persistent and determined attackers.

Wireless Network Penetration Testing Services

We leverage the *Open Source Security Testing Methodology Manual* (OSSTMM) and the *Penetration Testing Execution Standard* (PTES) as a foundation for our wireless assessment methodology, which simulates real-world attacks to provide a point-in-time assessment of vulnerabilities and threats to your wireless network infrastructure.


¿QUESTIONS?

Thank you!

For more information, please contact ...

Jaime CADAVID

M +1 917 443 7120

M +57 319 228 0213

e jaime.cadavid@jacartech.com

w www.jacartech.com