Raxis Penetration Testing Services

The Next-Level Reality Check for Corporate Cybersecurity

Fight Hackers with Hackers

Raxis security professionals are an elite team of highly skilled hackers who have performed hundreds of penetration tests, successfully breaching corporate America's most sophisticated security systems more than 85% of the time.

Using innovative, real-world tactics, the Raxis team has cracked a virtual bank vault and transferred money, operated critical infrastructure through SCADA and IoT breaches, and transferred thousands of private medical records.

Raxis live-fire attacks don't stop when a vulnerability is found. Every breached system is used as a new vector of attack against the rest of your infrastructure to help you understand the potential scope of damage. You'll gain a a first-hand understanding of adversarial techniques as your own systems are compromised and become bridgeheads for further attacks.

Is your network secure? Test it against the Raxis team and be sure.

PENETRATION TESTING SERVICES

EXTERNAL	Identify and exploit security risks through live-fire attacks against your internet facing systems.
INTERNAL	Attack your internal systems from the perspective of a malicious insider.
APPLICATION	Specifically target your applications and attempt to exploit the application code, web server configuration, database, or underlying operating system.
WIRELESS	Attempt to breach your wireless network security controls and obtain access to systems.
WEB and API	Test your REST, SOAP, or any other API standard to validate your security controls are working appropriately.
MOBILE	Target your mobile applications, attempting privilege escalation, restricted data exfiltration, or performing restricted operations against the mobile server.
SOCIAL ENGINEERING	Penetration testing coupled with social engineering using phishing techniques to gain user credentials that are then leveraged in the penetration test.

See other Raxis Attack and Assess Solutions at raxis.com

THE RAXIS VALUE

- See and learn from actual exploit attempts made by professional hackers
- Pivot attempts and persistent attacks to higher value systems reveal full scope of the vulnerability
- Exfiltration of restricted data helps determine the business impact and makes the risks tangible
- End of project reporting details step-by-step instructions to recreate the attack
- Clear and actionable remediation steps on how to block the exploited paths and improve security posture