PALADION
HIGH SPEED CYBER DEFENSE

ahornloesungen
deutschland gmbh

Network Penetration Testing

Identify exploitable vulnerabilities and verify that your infrastructure is resilient against the most advanced network level attacks.

Why Penetration Testing?

Given enough time and effort, sophisticated modern day hackers will find existing weaknesses in your network. That is why we spend time and effort identifying vulnerabilities before hackers can exploit it

Our penetration testing uses ethical hacking and controlled exploits to identify weaknesses in your network, so you know your security posture.

Don't Rely On Vulnerability Scans

A traditional vulnerability scan is performed using an automated security scanner that detects patterns and signatures that match a pre-defined set of vulnerabilities. However, scans are not "context-aware," and are incapable of understanding critical business functions or important security controls and need to be verified using manual testing techniques.

The Network Penetration Test Process

Paladion experts have developed an exhaustive penetration test process evolving from decades long experience in the industry.

The Penetration Testing Solution

Dependency on vulnerability scans may result in missing critical security flaws and insecure configurations. Our manual penetration tests leverages the knowledge provided by vulnerability scanners and goes beyond it to analyze and make decisions on how to best protect your network.

Information Gathering

The Network Penetration Process begins with a comprehensive survey of your network including architecture mapping and a complete network scan.

Scanning

The testing process continues with port scanning and war dialing that includes scanning open ports, closed ports and filtered ports.

Fingerprinting

After scans are complete, OS fingerprinting is conducted evaluating OS type, patch level and system type followed by protocol identification.

Vulnerability Scanning

Once fingerprinting is concluded, a vulnerability scan is completed using automated scanning with access to a vulnerability database, where any vulnerabilities and exploits are verified.

Exploit Verification

Using manual verification and password cracking, available exploits are checked and retested if necessary to validate results before reports are produced.

Reports

On conclusion of a network penetration test, comprehensive reports are created to provide findings, suggest solutions, and make recommendations.

Paladion Security Testing Labs

Paladion's Testing Labs has over 16 years of experience performing penetration tests for network layers such as firewalls, web servers, email servers, and FTP servers; application layers including all major development languages, all major web servers, all major operating systems, and all major browsers.

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its AI platform - AI.saac and advanced managed security services. Paladion is consistently rated and recognized by leading independent analyst firms, and awarded by CRN, Asian Banker, Red Herring, amongst others. For 18 years, Paladion has been actively managing cyber risk for over 700 customers from its five AI-Driven SOCs placed across the globe.

Please visit www.paladion.net for more information.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-703-956-9468.

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net