

Cyber Vulnerability Assessment



Network Vulnerability Analysis and Penetration Testing

Pendulum, powered by Ardham Technologies, is pleased to offer network vulnerability analysis and penetration testing.

The world and the devices we use are more and more connected every day, and while this enhances our lives and businesses, there are significant risks to our data and business security. We no longer live in a compartmentalized network model; we live in a borderless network where servers, storage, desktops, printers, phones, and security systems—and even lighting, HVAC systems, and coffeemakers—are all interconnected. This integration improves the quality of our lives and enables great success in our businesses but also introduces increased risk of business interruption, network breaches, service outages, and loss of valuable confidential data. Additionally, you may be subject to federally mandated industry security regulations.

Ardham Technologies' Networking Security Engineers combine top-tier network assessment methodology, custom coding, and in-depth testing tools with years of security, testing, and remediation experience. We identify real-world threats and provide recommendations for protecting your valuable data—and your business.

Cyber Vulnerability Assessment

Given the severe costs to an organization's reputation, operations, and finances in the event of a network breach or outage, a proactive approach to security is essential. Pendulum and Ardham Technologies offer a Cyber Vulnerability Assessment that provides an organization with a high-level analysis of the overall effectiveness of its information security measures and expert advice on improvements.

Using two types of penetration tests, Ardham Technologies professionals can safely access and test a network, revealing its strengths and its limitations, including design weaknesses, technical flaws, and vulnerabilities. The Cyber Vulnerability Assessment includes:

- **External Penetration Testing:** An Ardham Technologies specialist will conduct external penetration testing of up to 16 public IP addresses remotely. This testing focuses on servers, infrastructure, and the underlying software comprising the target and finds vulnerabilities that could be exploited in an external attack on these systems.
- **Internal Penetration Testing:** As part of an on-site assessment, internal penetration testing of up to 254 private IP addresses will be conducted. This part of the assessment is designed to discover and analyze what vulnerabilities can be exploited once an attacker is inside your network. Internal testing looks at the structure and security of your network, including the security of end-user accounts, and the information that can be that can be extracted from it, such as confidential employee or customer data.
- **Immediate Notification of Critical Vulnerabilities:** If, in the process of testing, the Ardham Technologies specialist discovers a critical issue in the network, this will be immediately reported to your IT staff for mitigation.

On the day of the on-site assessment, an Ardham Technologies specialist will provide briefings on the issues discovered over the course of the off-site external testing and the on-site internal test. A final written report that includes findings, the actual or potential impact of problems discovered, and recommendations will be provided to guide the organization in mitigating vulnerabilities.

Help protect your business: Call Pendulum at (888) 815-8250 or email info@PendulumRisk.com



What is Penetration Testing?

Penetration testing is a way for IT professionals to test your network's security for vulnerabilities, including its operating system, service and application flaws, improper configurations, and end-user behavior. This helps Ardham Technologies validate the efficacy of your security system and for you to monitor end-users with security policies.

Penetration tests are performed by IT professionals using manual or automatic technologies that safely and systematically target:

- Servers
- Endpoints
- Web applications
- Wireless networks
- Network devices
- Mobile devices
- Other access points of exposure

Once Ardham Technologies professionals have successfully detected weaknesses, they can begin to create strategic conclusions and prioritize related interventions.

Why Penetration Testing Helps

Penetration testing is an important tool used to detect weaknesses within your network so that your business's data is not compromised. In addition to detecting threats, penetration testing offers:

- **Early detection:** Penetration testing saves on costs related to security breaches by detecting them before they become larger issues.
- **Safeguarding of information:** Technology is growing and changing every day, meaning we need to be able to consistently look for new vulnerabilities and attacks that are evolving in our technology-dominated climate.
- **Identification and prioritization of risks:** With penetration testing, Ardham Technologies can evaluate your organization's ability to protect its networks, applications, endpoints, and internal/external attempts for unauthorized access.

Ardham Technologies performs penetration testing for its clients on a regular basis to create more consistent network security management. This helps us detect new threats and emerging vulnerabilities as well as create regularly scheduled analysis and assessments as required by regulatory mandates.

About Ardham Technologies

With its more than 200 years of combined IT experience and in-demand expertise, Ardham Technologies is a company you can trust. The company's IT technicians have bachelor's degrees in information technology or management information systems (MIS) as well as industry certifications that ensure they are current on the latest developments in the networking and security fields.

Help protect your business: Call Pendulum at (888) 815-8250 or email info@PendulumRisk.com