HIPAA Network & Penetration Testing

ProjX's Network Scanning and Penetration Testing process, Advanced Expose*Scan (*AES*),* incorporates Nexpose software from Rapid 7. This is a security risk intelligence solution that proactively supports the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting, and mitigation.

Our AES process is designed for organizations with large networks and virtualized infrastructure deployments requiring the highest levels of scalability, performance, and deployment flexibility. In this way, our AES helps organizations effectively improve their risk posture.

AES is divided into two sections- External Penetration Testing and Internal Network Testing. The intent of the **External Penetration Test** is to identify any weaknesses in the network from an outside penetration environment that may allow the network to be compromised. The ability to accomplish this gives an organization a starting point from which to implement remediation procedures for any identified vulnerabilities.

Internal Network Scanning seeks to identify vulnerabilities that allow internal users, or malicious programs, to exploit the weaknesses of workstations, servers, and other network attached devices. These vulnerabilities could allow information to escape the confines of the organization and cause a security breach.

Benefits

Malware and Exploit Exposure identifies exploits and malware attacks that can breach vulnerabilities found in your environment and enables you to prioritize risk.

Vulnerability Chaining mimics an attack to find vulnerabilities thus enabling you to reduce your risk exposure

Intelligent Integrated Scanning helps reduce operational and license costs by identifying networks, operating systems, data bases, web applications, and systems platforms in use.

False Positive Findings help reduce operational costs.

Vulnerability Validation helps strengthen security by validating if vulnerabilities are exploitable in your current environment.

ZERO DOWNTIME

Neither the Internal Network Scans nor the Penetration Tests cause any system downtime.

System Requirements

Remote access will be required to install the scanning software from our server on-site, which resides on the client network. This scanning software is a requirement for the internal phase of the testing and will be removed after the scanning and testing procedures are completed.

ProjX will work closely with the client IT team to ensure t all the identified components of the client network are sufficiently scanned.

Deliverables

- A detailed report for the IT staff will be created at the conclusion of the process and will identify all found vulnerabilities.
- A summary report will be created for the client management team.

ProjX Incorporated