Penetration Testing Services

•**External Basic Penetration Testing:** Performed remotely with no internal access provided to our security experts. The goal is to identify and classify the weaknesses and penetrate the internet-facing IT assets of an organization such as Web Servers, Network Gateways, VPN, E-mail Servers, and Firewalls.

•**Internal Basic Penetration Testing:** Performed from within the premises of the target organization, usually to identify & classify threats and vulnerabilities in internal network presented by someone who already have access to the organization's network such as an employee, contractor, or guest. It also helps an organization to determine its compliance on global or local policies, standards and procedures in terms of information security, data protection and segmentation of network.

Rather than simply listing all individual vulnerabilities in every IT asset, our approach is to find the systematic issues in the organization that led to these issues. We often use a sampling methodology in our approach to focus on the root causes and prioritize the most important remediation steps.

When performing Basic Penetration Testing, we limit our tests to relatively safe checks designed to limit any negative impact on the organization's production environment.

ASR Team, LLC
30 Newbury Street Suite 3
Boston, MA 02169
www.asrteam.com

Penetration testing process consists of the following steps:

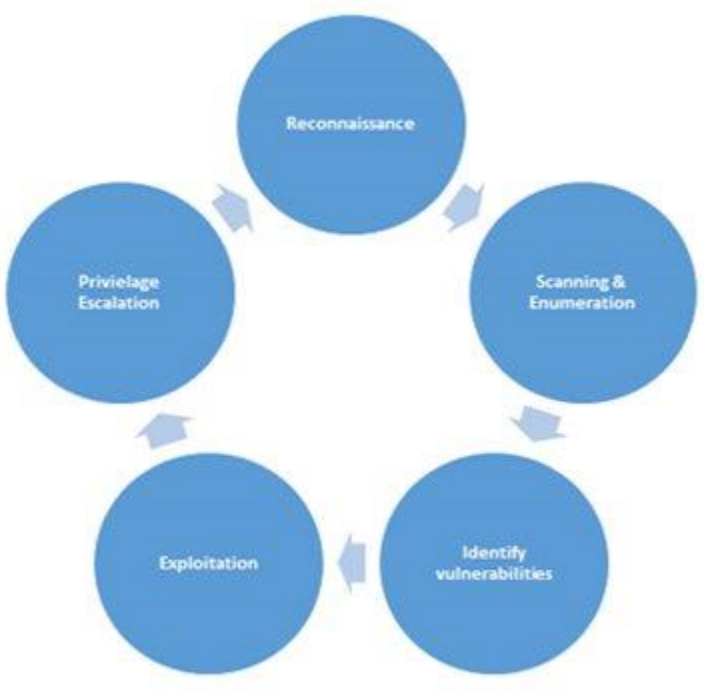
•**Reconnaissance:** gathering preliminary data or intelligence on the target organization. The data is gathered in order to better plan for the attack. Information gathered in this step includes IP address ranges, public email addresses, web sites, and others.

•**Scanning & Enumeration:** gathering more information about the connected systems and running applications and services in the organization's network. Information such as operating system type and version, user accounts, email addresses, service version and release numbers are also gathered.

•**Identify vulnerabilities:** based on information gathered in the previous two phases, we will identify weak services running in your network or applications that have known vulnerabilities.

•**Exploitation:** Using readily available code or create customized one to take advantage of identified vulnerabilities to gain access to target vulnerable system.

•**Privilege escalation:** In some cases, the existing vulnerability provides low level access only such as normal user access with limited privileges. In this step, we will attempt to gain full administrative access on the machine.



Questions?

support@asrteam.com

Deliverables:

Upon completion of the Basic Penetration Testing, a detailed report will be sent to client, including the following:

Executive Summary: Summary of the purpose of this assessment, as well as brief explanation of the threats that the organization is exposed to from a business perspective.

Findings: A detailed, technical explanation of the findings of the assessment along with steps and proofs of the findings.

Conclusion & Recommendations: This section provides final recommendations and summary of the issues found during the security assessment.

Questions?

support@asrteam.com