ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Penetration Testing

Penetration Testing (Pen Testing) actively attempts to 'exploit' vulnerabilities and exposures in a companies environment. Through exploiting the security weakness, a Penetration Test will attempt to gain read/write access to system resources, gain shell access to operating systems and obtain comprehensive access to application and database resources. Once a device has been compromised, a Penetration Test will look to branch out and gain further access to system resources that reside on DMZ and internal networks. Highly skilled Ethical Hacker's perform Penetration Tests and their approach is to simulate the tasks and efforts that a real world attacker might look to exploit, but without damaging or disrupting any of an organization's production services.

Black Box Testing

In a Black Box test, the client provides only the details of the IP addresses that are exposed to the Internet, and our testers will attempt to enumerate all publicly accessible information regarding the client that could be useful during the assessment. Valuable information can be garnered from Social Networking sites or other public forums and this can be reused to aid in breaching the companies defenses.

What a lot of organizations fail to realize is that their security is only as good as its weakest link, and this could be something as simple as a firewall rule that is not specific or a single server that was commissioned without adequate change management. Our testing regime will identify weaknesses in any services that are accessible externally, these could be standard web services or custom services that have been developed in-house. We will also see if it is possible to obtain useful information by validating the procedure that your help-desk use to identify your users when resetting users' passwords for example.

White Box Testing

In a White Box test, clients provide ASM with basic information about the applications and infrastructure prior to the commencement of the testing engagement. The logic behind this style of testing is that an attacker can test your system for extended periods of time whilst our consultants have limitations in the time they can spend, and in some instances an adversary may have access to this type of information, therefore this type of testing can provide more realistic results. Our services will also look to provide you with excellent coverage of all vulnerabilities found, not only the first flaw that we find that may allow unauthorized access to your systems.

Grey Box Testing

A Grey Box test is a blend of Black Box testing techniques and White Box testing techniques. In Grey Box testing, clients provide ASM with more detailed information to help with the testing procedures such as network diagrams. This results in a more focused test than in Black Box testing as well as a reduced time-frames and budget for the testing engagement.

Internal Tests

Internal tests will provide an organization with a review of their security conducted from the point of view of an internal privileged user, a temporary worker, or an individual that has physical access to the organization's buildings, such as janitorial or maintenance personnel.

They are conducted from within an organization, over their Local Area Network, or via a VPN connection. Tests will determine whether it is possible to gain access to sensitive company information, including Databases, critical applications and authentication services such as Active Directory.

Internal tests will also assess whether it is possible to remove data from the corporate environment without triggering detection systems, or leaving an audit trail of what data leakage may have occurred and where it was moved to. Internal tests will assess whether an internal user can circumvent existing security controls, in order to grant themselves inbound access to the infrastructure through the installation of backdoor channels used by attackers in APT (Advanced Persistent Threat) for example.

Our reporting aims to provide executive summaries that can be used in presenting the risk to senior stakeholders without the danger of jargon reducing the effectiveness of the message, with easy to interpret risk ratings and recommendations, whilst our detailed reporting sections can be communicated to the technical teams in order to ensure effective remediation.

All of testing methods are non-destructive, so no DOS (Denial of Service) attacks are undertaken, and our testing is non-exploitative, meaning that we will only attempt to gain control of systems if this is approved by the client on a case by case basis.

To find out more about how ASM can help you with your Security Testing requirements, please complete our contact form, and a Consultant will respond to your enquiry.