**渗透测试选择题**

渗透测试是一种通过模拟攻击、漏洞扫描和安全评估等手段来评估系统和网络的安全性的过程。在进行渗透测试之前，渗透测试人员需要根据特定的情景和需求，选择合适的测试方法和工具。下面将介绍一些与渗透测试相关的选择题，以帮助读者更好地理解和应用渗透测试。

1. 在渗透测试中，以下哪种是主动型攻击测试？

A. 漏洞扫描

B. 社会工程

C. 网络嗅探

D. 安全审核

2. 渗透测试中常用的系统漏洞扫描工具是什么？

A. Wireshark

B. Nessus

C. Metasploit

D. Nmap

3. 渗透测试通常会使用哪种类型的测试方法对系统或应用进行评估？

A. 黑盒测试

B. 白盒测试

C. 灰盒测试

D. 蓝盒测试

4. 渗透测试人员通过侦查和信息搜集获取目标系统的信息，确定潜在的攻击点。以下哪项不属于信息搜集的常用手段？

A. 端口扫描

B. 社交媒体分析

C. SQL注入

D. WHOIS查询

5. 渗透测试人员在攻击目标系统前，通常需要先获取系统的授权。以下哪一种授权方式是非法的？

A. 白帽子渗透测试授权

B. 黑客攻击获取授权

C. 合法授权书

D. 签署免责声明

6. 渗透测试人员通过模拟攻击对目标系统实施攻击，以评估系统的安全性。以下哪种方法是对系统进行暴力破解？

A. 钓鱼攻击

B. 缓冲区溢出攻击

C. 密码破解攻击

D. 嗅探攻击

7. 在渗透测试中，以下哪种技术可以有效地隐藏攻击者的身份？

A. 防火墙

B. 加密通信

C. 匿名化代理

D. 反向代理

8. 渗透测试人员在进行渗透测试时，需要与被测系统的管理员或团队进行沟通和合作。以下哪项是渗透测试基本守则？

A. 不与管理员沟通，保持匿名

B. 尽量避免沟通，专注于攻击

C. 和管理员团队建立良好的合作关系

D. 披露测试结果前先要求高额报酬

以上是关于渗透测试选择题的一些题目，通过对这些题目的了解和答题，可以帮助用户更好地理解渗透测试的相关知识和方法，并在实际应用中做出正确的选择。同时在进行渗透测试时，也需遵守相关法律法规，获得合法的授权并与相关团队进行合作，保障测试过程的合法性和安全性。