一次完整的渗透测试流程

原创 渗透之巅 关注
发表于 2021-12-25 19:13:56 最近一篇更新于 2022-01-18 ... 阅读数 8847

目录
渗透测试
信息收集
漏洞扫描
漏洞利用
内网探测
内网渗透
痕迹清除
撰写渗透测试报告

渗透测试

渗透测试是利用现代网络攻击手段对目标系统进行测试，对网络进行一步一步的渗透，发现其中存在的漏洞和薄弱环节，然后撰写一份渗透测试报告，提出相应的解决方案，帮助企业提高网络安全防御能力。对网络进行漏洞扫描，以防止黑客入侵！

渗透测试的目标是发现网络中的安全漏洞，并提供解决方案。渗透测试通常是在网络安全防御的同时——为了保证网络安全性——进行的。这意味着，在网络受到攻击之前，对网络进行漏洞扫描，以防止黑客入侵！

渗透测试的目标是发现网络中的安全漏洞，并提供解决方案。渗透测试通常是在网络安全防御的同时——为了保证网络安全性——进行的。这意味着，在网络受到攻击之前，对网络进行漏洞扫描，以防止黑客入侵！

渗透测试分为四个阶段：

- 信息收集阶段是为渗透目标网站漏洞挖掘做准备，信息收集的情况对于对进行渗透，有直接影响和间接影响
- 漏洞扫描阶段是为渗透目标网站进行漏洞挖掘，漏洞扫描的程度，直接决定了渗透的成功率，漏洞扫描是对网站的渗透

我们现在要编写漏洞扫描程序，这个程序能够自动进行扫描，这样可以提高效率，我们现在可以选择编写Python，Perl，Ruby，Lua，Bash或其他语言来编写漏洞扫描程序。

当我们编写了一个漏洞扫描程序之后，第一步该做些什么呢？

信息收集

信息收集是渗透测试的第一步，在这一步中，我们会从目标网站收集信息，以便为后续的渗透测试做准备。信息收集的目的是为了发现目标网站的漏洞，以便为后续的渗透测试做准备。信息收集的方法有很多种，可以通过网络扫描、端口扫描、漏洞扫描、社会工程学、搜索引擎、社交媒体、网络嗅探、DNS查询、WHOIS查询、SNMP查询、SMB查询、NetBIOS查询、LDAP查询、RPC查询、SSH查询、Telnet查询、FTP查询、HTTP查询、HTTPS查询、SMTP查询、POP3查询、IMAP