《Attacking Network protocols》 学习记录_翻译部分（一）C9漏洞根本原因（上）

SiameseJuly / 2018-10-18 21:57:57 / 浏览数 2395 新手 入门资料 顶(2) 踩(0)

$$前言：$$最近在看《Attacking Network Protocols》这本书，感觉写的不错，比较适合新手，记录下来，方便以后查阅，顺带整理和ctf相关的知识，这一个系列分翻译和总结两部分。

第九章 漏洞的根本原因

这章描述因协议履行导致的安全漏洞的常见根本原因，这类漏洞不同于第七章描述的源自协议规范的漏洞。异常不必直接利用就可以将其视为漏洞。它可能会削弱协议的

 阅读这章之后，你将开始了解协议中的模式，这将有助于你在分析过程中帮确认安全漏洞（直到第十章我讨论如何利用不同的类别）

在这一章节中，我假定你使用了所有可能的方法调查了协议，包括分析网络流量，对应用的二进制文件进行逆向工程，阅读了源代码，手动测试客户端和服务器以确定实际漏

漏洞种类

当你处理安全漏洞时，将漏洞分为不同类别的集合来评估漏洞造成的风险是很有用的方法。例如，设想一个漏洞，当被利用时，可以允许攻击危害运行应用程序的系统

远程代码执行（Remote Code Execution）

远程代码执行是指允许攻击者在实现协议的应用程序的上下文中运行任意代码。这可能导致通过劫持应用的逻辑或者影响这正常操作期间创建的子进程的命令行来实现的。

远程代码执行漏洞，通常是安全的最关键点，因为这类漏洞允许一个攻击者通过正在执行的应用程序危害系统。这样的攻击将使攻击者能够访问应用程序可以访问的任何内容

拒绝服务（Denial-of-Service）

一般来说，应用程序被设计用来提供服务，如果存在这样一个漏洞，当该漏洞被利用导致应用程序崩溃或无响应时，攻击者可以使用该漏洞拒绝合法用户访问特定应用程序及

 我们可以把拒绝服务漏洞分为持久型和非持久型。

- 持久性漏洞会永久阻止合法用户访问该服务，至少持续到管理员解决这个问题。原因是利用此漏洞会破坏某些存储状态，以确保应用程序在重新启动时崩溃
- 只要攻击者发送的数据满足拒绝服务条件，非持久性漏洞就会持续存在。通常，如果允许应用程序自行重启或给定足够的时间，服务将恢复

信息泄露(Information Disclosure)

许多应用程序是黑箱，在正常操作中只能通过网络向用户提供某些信息。如果有办法让应用程序提供最初未设计提供的信息，例如内存信息、文件系统路径或身份验证凭据，

认证绕过（Authentication bypass）

许多应用程序需要用户提供一个认证凭据来完全访问一个应用程序，有效的凭据可能是用户名和密码，或者一个更加复杂的验证，比如一个加密地安全交换。认证限制了对资

如果有方法在不提供所有身份验证凭据的情况下对应用程序进行身份验证，则应用程序中存在身份验证绕过漏洞。这样的漏洞可能就像应用程序错误地检查密码一样简单 - 例如，因为它比较了密码的简单校验和，这很容易暴力破解。或者漏洞可能是由于更复杂的问题，例如SQL注入。

授权绕过（authorization bypass）

用户权限并不都是平等的。应用程序通过同样的接口可以支持多种类型的用户，比如只读，低权限或者管理员。如果应用程序提供了访问资源（比如文件）的方式，基于认证

当攻击者能够获得额外的权限或者访问他们没有权限访问的资源时，则存在授权绕过漏洞。比如，攻击者可能直接更改经过身份验证的用户或用户权限，或者协议可能无法正

> 重点：不要把认证绕过和授权绕或混为一谈，二者之间的主要差异是身份验证绕过允许您从系统的角度作为特定用户进行身份验证;
> 授权绕过允许攻击者从不正确的身份验证状态访问资源（实际上可能是未经身份验证的）

定义完漏洞的类别之后，我们来了解一下更多细节并探索一些促使你会发现这些漏洞的协议结构。

下一部分

漏洞构成原因部分的翻译，再加一部分总结

点击收藏 | 3 关注 | 4

上一篇：2018hack.lu Write... 下一篇：2018hack.lu CTF W...

1. 0 条回复
   - 动动手指，沙发就是你的了！