黑客技巧

黑客的方式有很多，这个话题非常有趣。作为一名业余的白帽黑客，我发现这个领域有很多知识值得学习。在这里，我将记录一些我探索过的方法。

默认密码

一些网站，包括政府机构的网站，仍然使用默认密码。虽然许多公司或用户会更改默认凭证，但也有一些没有做到。用户往往懒惰，像 `12345678` 这样的密码仍然常见。这在老旧或小众系统中尤为突出。

nmap 或 Netcat

这些工具用于扫描服务器的端口。特别要注意常用的端口，如 80、22 和 443。对于 AWS 实例，默认用户名是 `ec2-user`。对于 Azure 实例，默认用户名是 `azure-user`。对于 Google Cloud 实例，默认用户名通常是 `ubuntu` 或 `google-cloud`。对于其他云实例，通常是 `root`。

使用浏览器控制台

浏览器控制台对于检查隐藏的信息非常有用。有时，关键数据嵌入在 HTML 或 JavaScript 代码中，但在页面上不可见。

后门

在生活中，后门提供了未经授权的进入建筑物的方式，通常不被注意或没有防范，比如停车场或侧门。类似地，系统也可能有隐藏的后门，绕过正常的安全协议。

社会工程学

人们的昵称、生日和社交媒体发布的内容可以揭示很多个人信息。这些细节通常被用来构建弱密码。对于 Wi-Fi 网络，知道某人的门牌号或其他身份信息可以帮助猜测他们的 SSID 或密码。

SQL 注入

对于任何输入字段，使用 `or 1=1` 进行测试是一种常见的技术，用于识别漏洞和潜在的 SQL 注入点。

Actuator 或健康 API

对于 API 服务器，像 Spring Boot 这样的应用程序提供了`/actuator` 端点，提供机器和应用程序的健康数据。其他 Web 框架也有类似的功能，可能暴露敏感的服务器信息。

流量监控

要了解前端如何与后端交互，可以使用像 Charles Proxy 这样的代理应用程序，在 macOS 上记录并分析请求日志。这可以让你深入了解组件之间的路径和数据交换。

API 的限制和边界情况

测试 API 或服务器的限制和边界情况非常重要。分布式拒绝服务（DDoS）攻击试图压垮请求限制。此外，边界情况是 API 可能允许访问受限数据的情境。测试这些可以帮助确保正确的访问控制已经到位。

管理面板

有时，管理员或内部面板并没有得到充分的保护。值得尝试访问像`/admin` 这样的路径，或访问像`admin.xx.com` 这样的子域名，检查这些区域是否得到妥善保护。