黑客攻擊

黑客手法多種多樣，這個話題也相當有趣。作為一名業餘的白帽黑客，我發現這個領域有許多知識值得學習。在這裡，我將記錄一些我所探索到的方法。

默認密碼

一些網站，包括政府機構的網站，仍然使用默認密碼。雖然許多公司或用戶會更改默認憑據，但有些則未能做到。用戶往往懶惰，像 `12345678` 這樣的密碼仍然常見。這在較舊或小眾的系統中尤其如此。

nmap 或 Netcat

這些工具用於掃描服務器的端口。特別注意常用的端口，如 80、22 和 443。對於 AWS 實例，默認用戶名是 `ec2-user`。對於 Azure 實例，是 `azure-user`。對於 Google Cloud 實例，默認用戶名通常是 `ubuntu` 或 `google-cloud`。對於其他雲實例，通常是 `root`。

使用瀏覽器控制台

瀏覽器控制台對於檢查隱藏信息非常有用。有時，關鍵數據嵌入在 HTML 或 JavaScript 代碼中，但頁面上不可見。

後門

在生活中，後門提供了未經授權進入建築物的途徑，通常不被注意或無人看守，如停車場或側門。同樣，系統可能隱藏著繞過正常安全協議的後門。

社交工程

人們的暱稱、生日和社交媒體帖子可以揭示大量個人信息。通常，這些細節用於構建弱密碼。對於 Wi-Fi 網絡，知道某人的門牌號或其他識別細節可以幫助猜測他們的 SSID 或密碼。

SQL 注入

對於任何輸入字段，使用`? 1=1` 進行測試是識別漏洞和潛在 SQL 注入點的常見技術。

Actuator 或 Health API

對於 API 服務器，像 Spring Boot 這樣的應用程序提供了一個`/actuator`端點，提供機器和應用程序健康數據。其他 Web 框架也有類似的功能，可能會暴露敏感的服務器細節。

流量監控

要了解前端如何與後端交互，可以使用像 macOS 上的 Charles Proxy 這樣的代理應用程序來記錄和分析請求日誌。這可以讓你深入了解組件之間的路徑和數據交換。

API 的限制和邊緣情況

測試 API 或服務器的限制和邊緣情況非常重要。分布式拒絕服務（DDoS）攻擊試圖壓垮請求限制。此外，邊緣情況是 API 可能允許訪問受限數據的場景。測試這些可以幫助確保適當的訪問控制。

管理面板

有時，管理或內部面板沒有得到充分保護。值得嘗試訪問像`/admin`這樣的路徑或訪問像`admin.xx.com`這樣的子域，以檢查這些區域是否得到適當的保護。