

# Exploit

## Exploit

"Exploit" 是指一種利用軟件、硬體或協議中的漏洞或弱點，以實現攻擊者目標的程式碼或技術。Exploit 的目的是利用系統或應用程式中的漏洞，使攻擊者能夠繞過正常的安全措施，取得未授權的訪問權限或進行其他不當的操作。Exploits 可能針對操作系統、應用程式、網絡協議、服務或其他計算機系統組件中的安全漏洞。

Exploit 的類型和使用方式多種多樣，以下是一些常見的 Exploit 類型：

1. **緩衝區溢出 (Buffer Overflow)**：通常發生在應用程式中，攻擊者通過向應用程式的緩衝區寫入超過其預期大小的數據，從而修改相鄰內存的內容，並可能執行任意的程式碼。
2. **SQL 注入 (SQL Injection)**：在應用程式中對資料庫的 SQL 查詢，攻擊者在用戶輸入中插入惡意的 SQL 代碼，以獲得未授權的資料或執行未授權的操作。
3. **漏洞利用**：利用已知的漏洞或安全弱點，攻擊者使用相應的 Exploit 來入侵系統，例如操作系統漏洞、應用程式漏洞或服務漏洞。
4. **零日漏洞利用 (Zero-Day Exploits)**：利用廠商還未知曉或尚未修復的漏洞。由於這些漏洞還未公開，因此防禦措施通常還未能應對。
5. **社交工程攻擊**：通過利用用戶的社交行為，欺騙他們進行某種操作，如點擊惡意連結或下載惡意附件。
6. **漏洞掃描和利用工具**：使用特殊工具，如Metasploit，可自動掃描和利用系統中的漏洞。

Exploits 是黑客和安全專業人員之間的一場競賽，防守方通常會定期更新和修補系統，以防止已知漏洞被利用。同時，實行最佳安全實踐，如限制用戶權限、加密敏感數據等，也是降低系統被 Exploit 的風險的重要手段。

---

🕒 修訂版本 #4

★ 由 treeman 建立於 29 🕒 Q🕒🕒🕒 2023 11:58:01

✍ 由 treeman 更新於 11 🕒 Q🕒G🕒🕒 2023 01:14:54