【Linux】【提權】GTFOBins

GTFOBins 是一個安全工具，用於收集和提供攻擊者在 Linux 和 Unix 系統上濫用的 "提升權限" 或 "逃逸" 技術。它的全名是 "GTFO (Get The Fudge Out) Bins"，而 "Bins" 指的是二進制文件，即執行檔。GTFOBins 有一個簡單的目標：提供一個易於搜索和使用的資源，以查找關於不同系統命令和二進制文件的特權提升技術的信息。

以下是使用 GTFOBins 的基本步驟：

1. **瀏覽 GTFOBins 網站：** GTFOBins 的官方網站是 https://gtfobins.github.io/ 。你可以直接在網頁上搜索特定命令或二進制文件，也可以瀏覽不同的類別。
2. **搜尋技術：** 在網站上使用搜索功能，輸入你感興趣的命令或二進制文件名稱，然後查看相應的結果。每個結果都提供了有關如何使用這些二進制文件進行特權提升的信息。
3. **了解特權提升技術：** 對於每個命令或二進制文件，GTFOBins 提供了相關的技術和實例，說明攻擊者如何使用這些工具來提升特權。這可能涉及到濫用系統漏洞或執行一些特殊的命令來達到目的。
4. **謹慎使用：** 請注意，GTFOBins 提供的信息主要是為了教育和安全意識而設計的。請勿將這些技術用於非法或未獲授權的活動。使用這些技術來測試自己的系統或獲得授權的測試是可行的，但必須遵從相應的法律和道德標準。

總的來說，GTFOBins 是一個有用的資源，可以幫助安全專業人員和系統管理員了解和防禦濫用系統的方法。

修訂版本 #1
★由 treeman 建立於 3 ?Q?G?? 2023 11:26:33
由 treeman 更新於 7 ?@?? 2024 19:30:26