

# 【AD】【列舉】ADRecon

ADRecon (Active Directory Reconnaissance) 是一種用於對Active Directory (AD) 環境進行信息收集和分析的工具或技術。Active Directory是由Microsoft開發的用於管理和組織網絡中的計算機、用戶和資源的目錄服務。ADRecon的主要目的是幫助安全專業人員、紅隊和藍隊人員了解AD環境的結構和配置，以便更好地評估安全風險、進行紅隊測試或加強防禦措施。

<https://github.com/adrecon/ADRecon>

```
wget https://github.com/adrecon/ADRecon/blob/master/ADRecon.ps1
```

```
git clone https://github.com/adrecon/ADRecon.git
```

```
# 將資料產出  
.\ADRecon.ps1 -Quputtype html
```

ADRecon通常執行以下任務：

1. **信息收集**：探查AD環境，收集有關域控制器、用戶帳戶、群組成員資訊、計算機、GPO (Group Policy Objects) 等的信息。
2. **權限和訪問權限分析**：獲取有關用戶和群組的權限信息，以識別潛在的安全風險。這包括檢查哪些用戶具有高權限、哪些用戶可以訪問關鍵資源等。
3. **攻擊表面分析**：分析AD環境的攻擊表面，包括識別可能的弱點、不安全的設定和可能的攻擊向量。
4. **密碼破解和哈希收集**：尋找弱密碼、空密碼或使用弱加密算法的帳戶，以及收集用戶帳戶的哈希。
5. **枚舉域控制器和服務**：了解AD環境中的域控制器、LDAP服務和其他重要服務的信息。
6. **藍隊測試**：在授權的情況下，模擬攻擊者的行為，以測試防禦機制的有效性。
7. **風險評估**：通過分析AD環境的結構和配置，評估安全風險並提出建議的改進措施。

要注意的是，ADRecon通常由安全專業人員或網絡安全團隊使用，並且在使用之前必須獲得授權，以避免非法入侵或濫用。此類工具和技術的使用主要是為了加強網絡安全，發現潛在的弱點，並提高對潛在攻擊的警覺。

---

🕒 修訂版本 #4

★ 由 treeman 建立於 10 🕒👤👤👤👤 2023 10:24:51

🔧 由 treeman 更新於 7 🕒@👤👤 2024 19:30:26