

# 【AD】【列舉】BooldHound

BooldHound (BloodHound) 是一個用於Active Directory (AD) 環境的安全分析和攻擊模擬工具。它旨在幫助安全專業人員、紅隊人員和藍隊人員更好地理解 and 評估AD環境中的安全風險，尤其是針對橫向移動和權限提升的風險。

<https://github.com/BloodHoundAD/BloodHound>

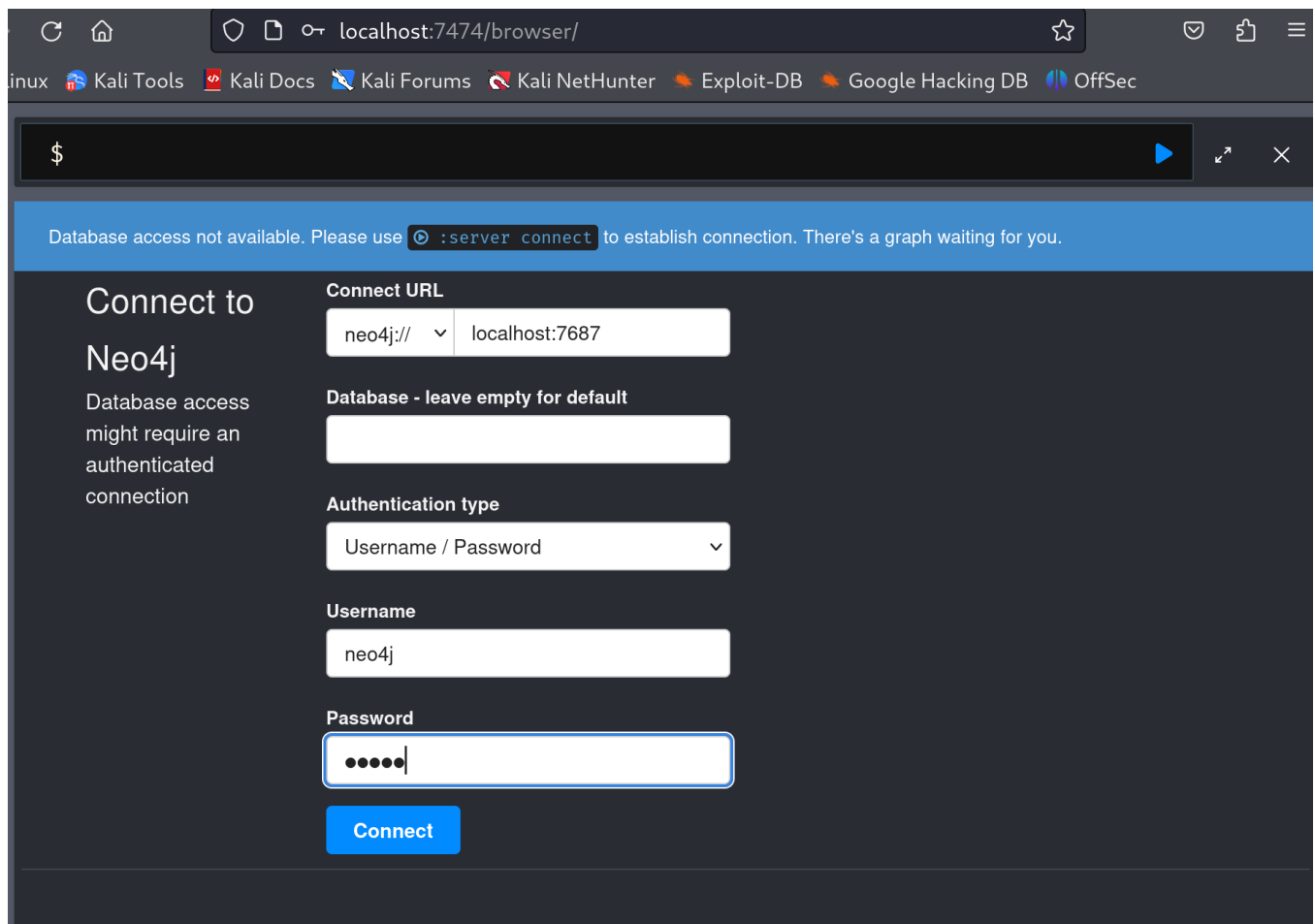
```
# 安裝
sudo apt install -y bloodhound

# 啟動圖形化資料庫
sudo neo4j start

Started neo4j (pid:70263). It is available at http://localhost:7474
There may be a short delay until the server is ready.
```

```
#修改密碼 -> firefox 開啟 https://localhost:7474
```

username / password => neo4j



Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you.

**Connect to Neo4j**

Database access might require an authenticated connection

**Connect URL**

neo4j:// localhost:7687

**Database - leave empty for default**

**Authentication type**

Username / Password

**Username**

neo4j

**Password**

.....

**Connect**

修改密碼

# Connect to Neo4j

Database access might require an authenticated connection

New password



OR

Generate

Repeat new password



Change password

```
# shell 輸入bloodhound
bloodhound
```

```
#填入帳密 neo4j / {修改後的密碼}
```



BLOODHOUND

Log in to Neo4j Database

bolt://localhost:7687



Neo4j Username

Neo4j Password

☐ Save Password

Login

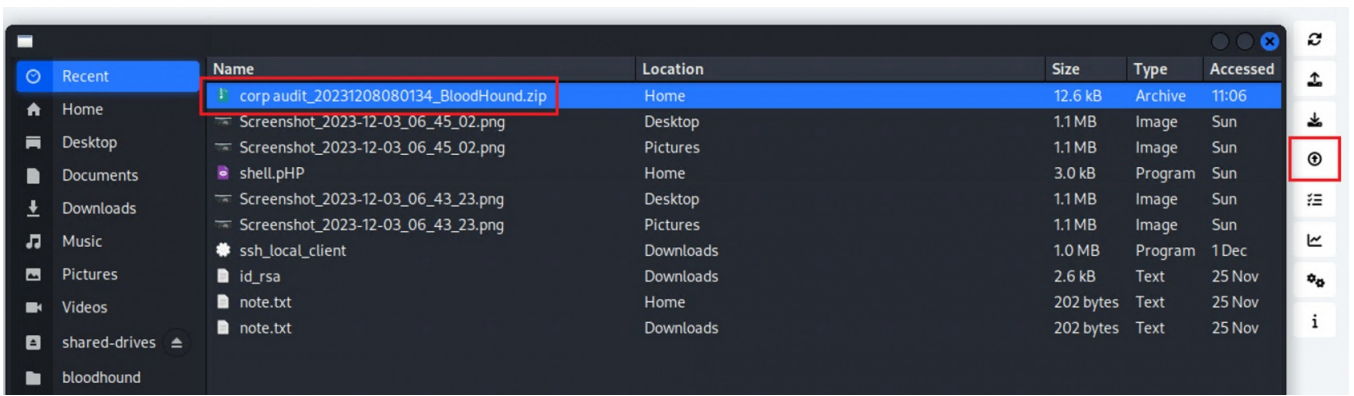
使用 SharpHound 搜集資料 <https://bookstack.treemanou.com/books/treemanoscp/page/adsharphound>

```
Invoke-BloodHound -CollectionMethod All -OutputDirectory C:\tools\ -OutputPrefix "corp_audit"
```

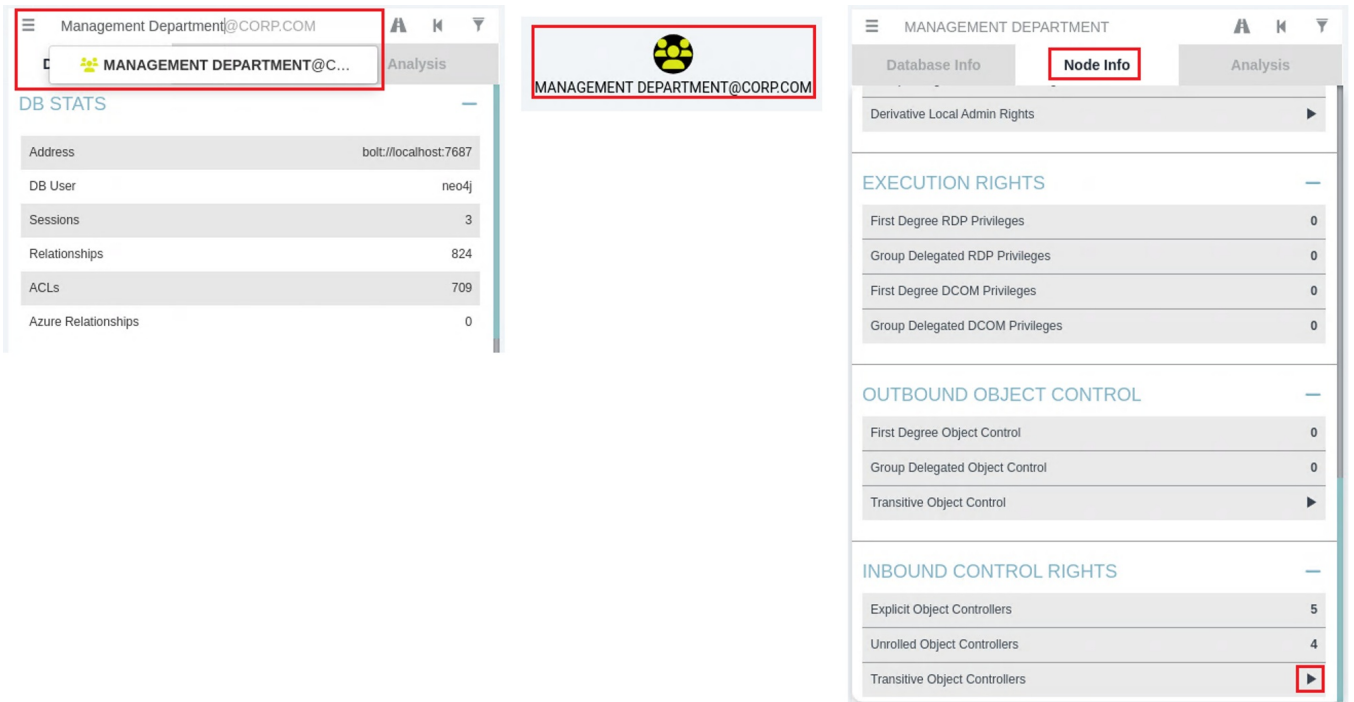
或是使用 Bloodhound.py

```
# kali install
sudo apt install -y bloodhound.py
# 使用
bloodhound-python -u {username} -p {password} -c all -d corp.com -ns 192.168.210.70
```

上傳分析資料



先在左上框框搜尋Management Department，然後出現畫面會出現節點，點選節點後，Node Info頁籤會出現東西，拉至最底下 Transitive Object Controllers 旁邊的箭頭，點下去。



然後右邊功能設定，都先設定Always Display，Node Info頁籤點選Explicit Object Controllers，就會出現以下圖表，其中找到Owns的線所對應的就是答案DOMAIN ADMINS。

