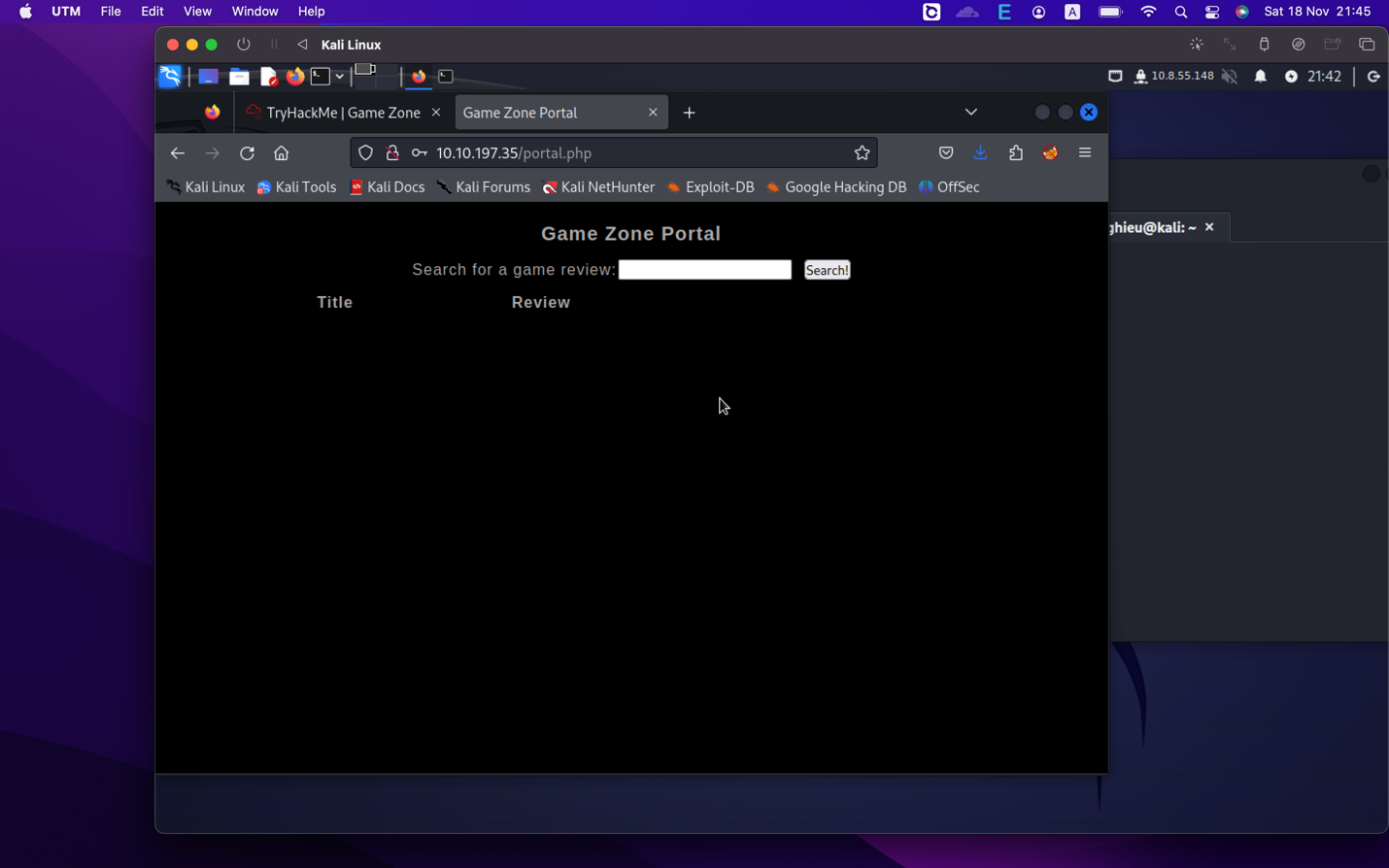


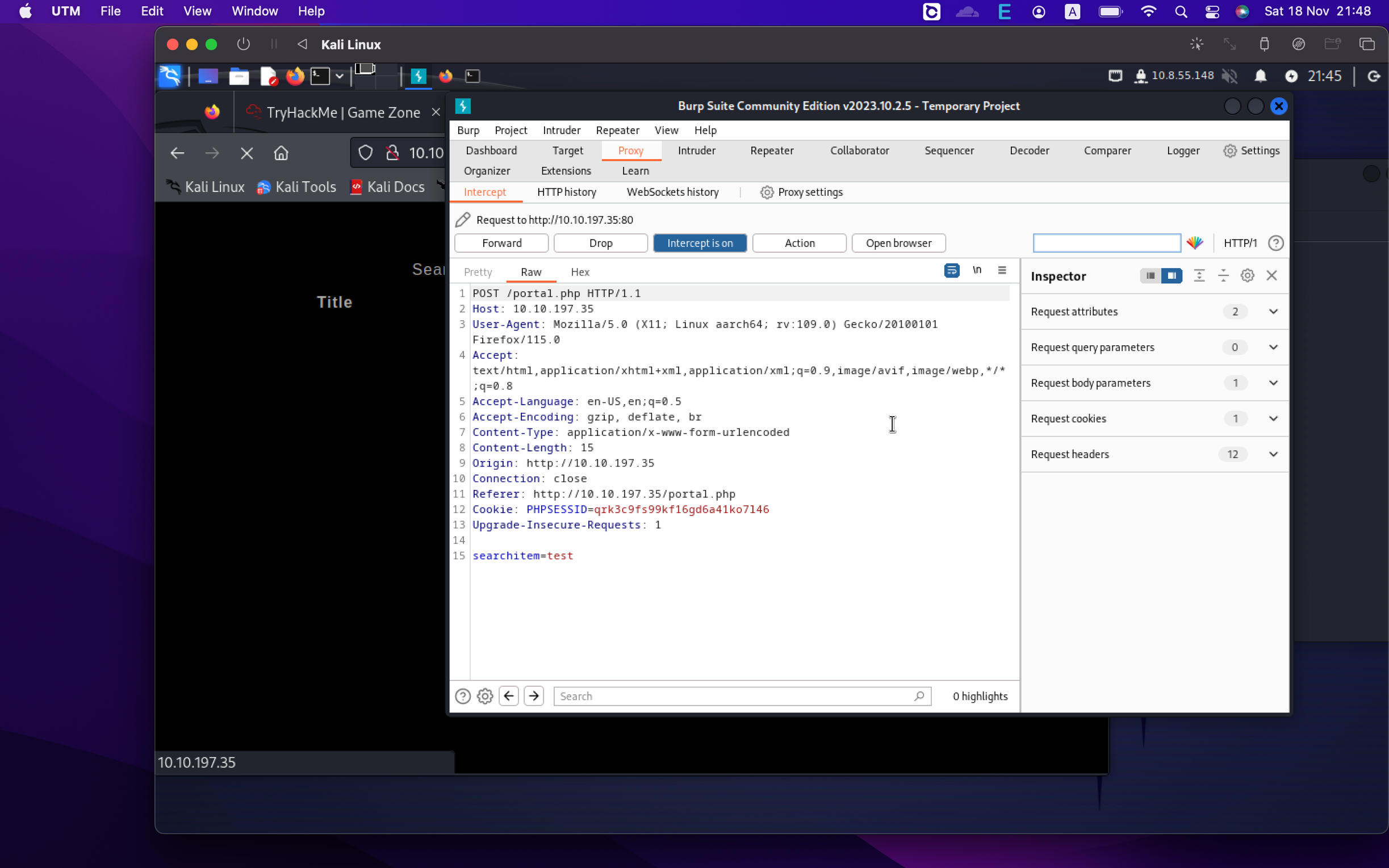
Username: admin' or 1=1#

Pass: admin



**Using SQLMap**

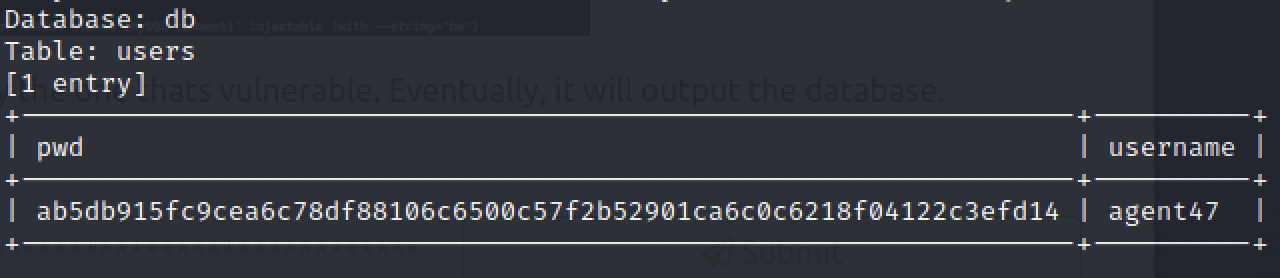
Đầu tiên, chặn yêu cầu để tìm kiếm:

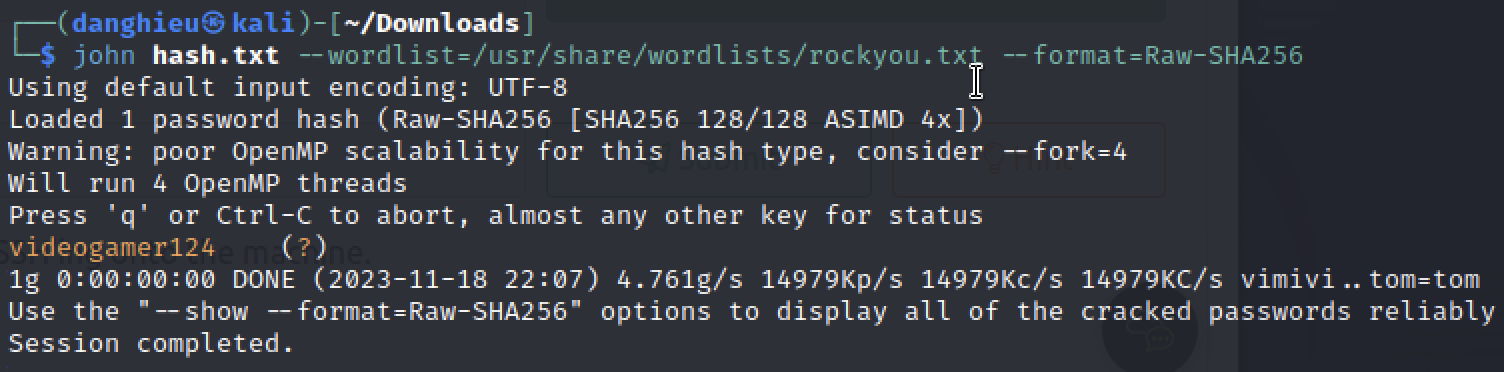


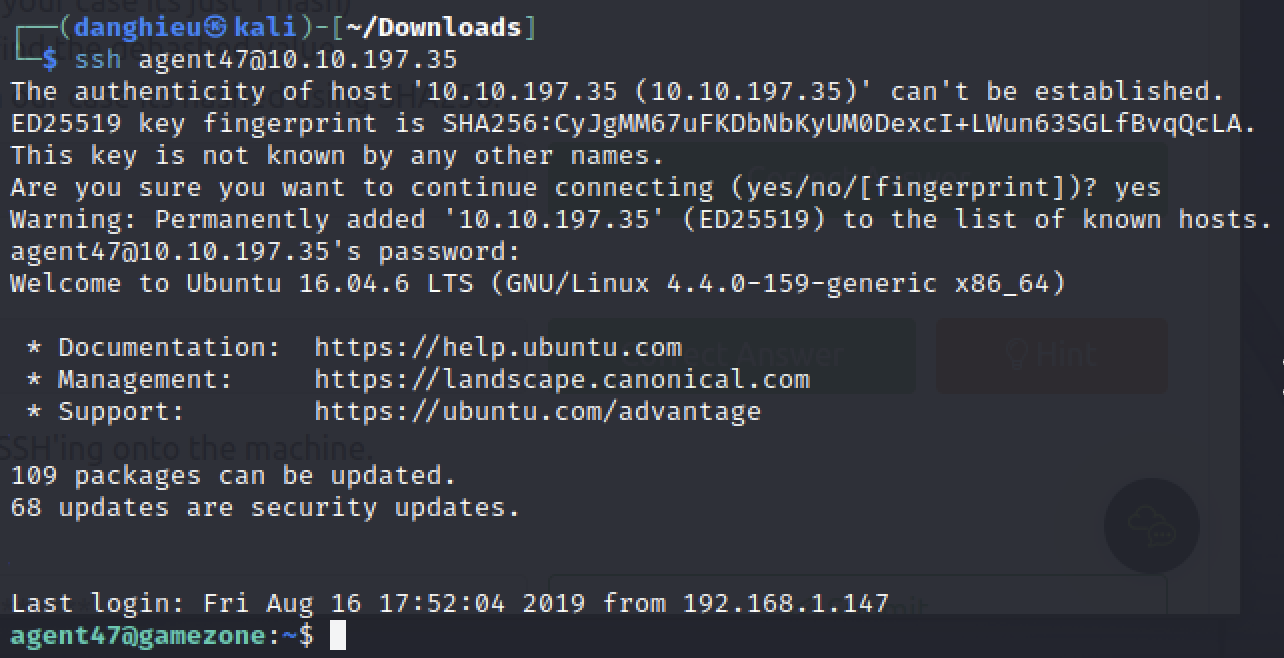
Lưu yêu cầu thành 1 file text. Gửi qua SQLMap để xác thực phiên.

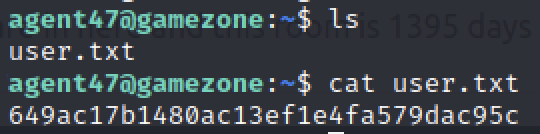
sqlmap -r request.txt --dbms=mysql --dump

SQLMap sẽ thử nhiều cách khác nhau và xác định cái có lỗ hổng. Sau đó sẽ dump dữ liệu.

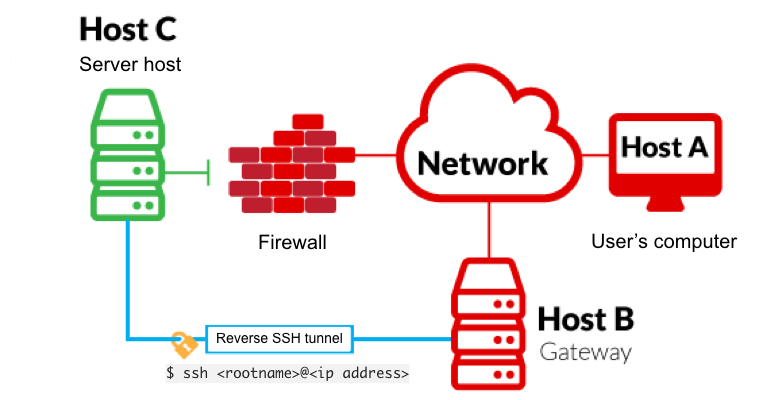








**Phát hiện các dịch vụ bằng reverse SSH tunnels**



Reverse SSH port forwarding chỉ định 1 port trên máy chủ đích được chuyển tiếp sang 1 máy chủ và port khác ở máy cục bộ.

-L là local tunnel (You 🡨 Client). Nếu 1 trang web bị chặn, bạn có thể chuyển tiếp lưu lượng đến 1 máy chủ của bạn. Ví dụ, nếu trang imgur bị chặn, bạn có thể :

ssh -L 9000:imgur.com:80 user@example.com

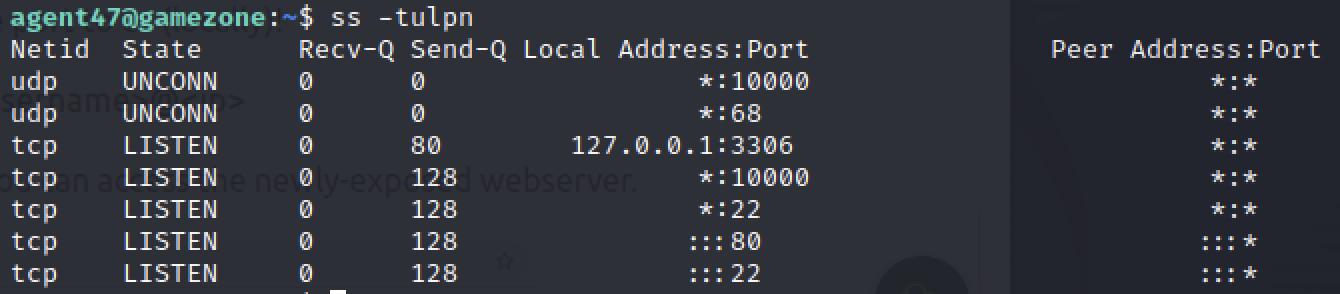
localhost:9000 trên máy cục bộ sẽ tải lưu lượng của trang imgur.

-R là remote tunnel (You 🡪 Client). Bạn chuyển lưu lượng của bạn sang 1 máy chủ khác để xem. Tương tự như trên, nhưng ngược lại.

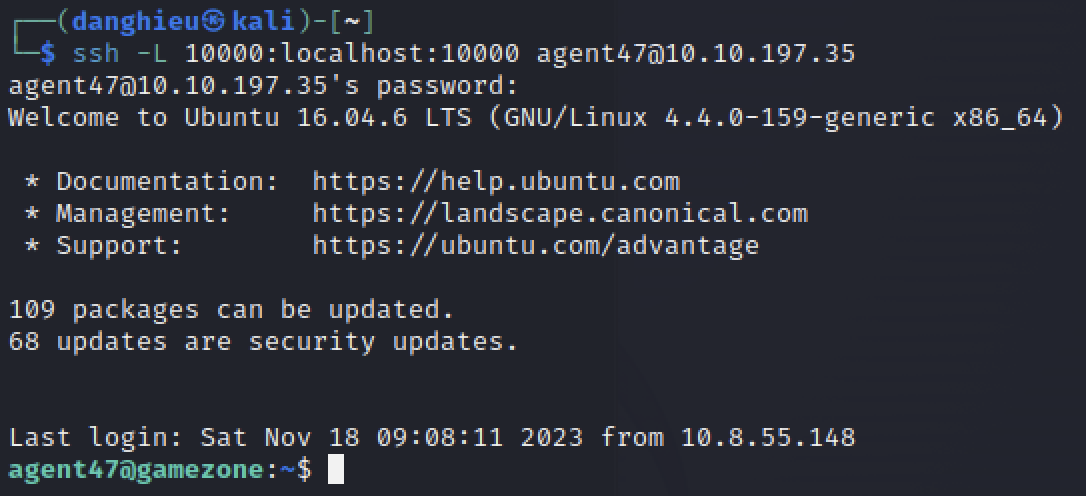
Chúng ta sẽ dùng 1 công cụ gọi là ss để điều tra các sockets đang chạy trên máy chủ:

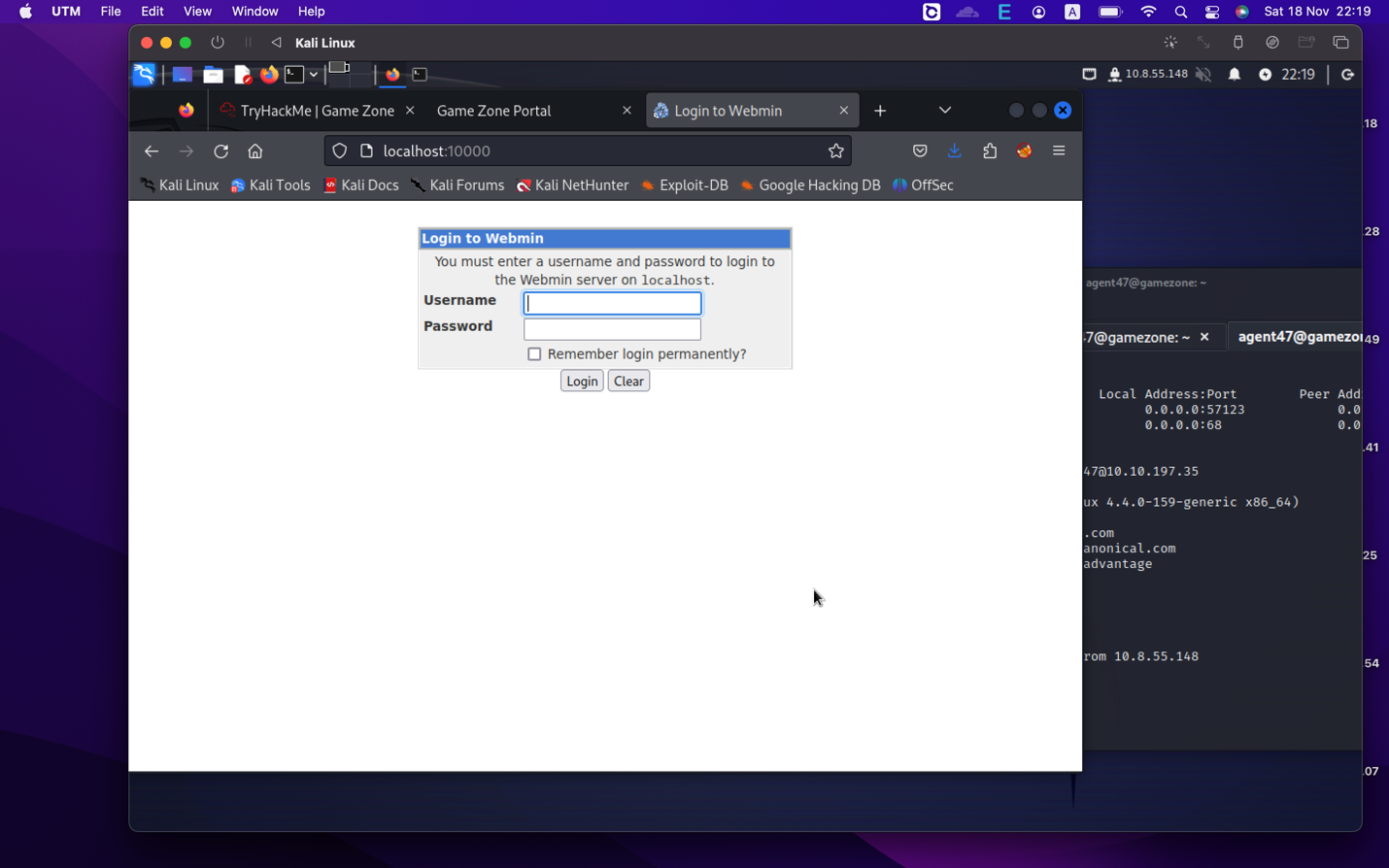
ss -tulpn

|  |  |
| --- | --- |
| **Argument** | **Description** |
| -t | Display TCP sockets |
| -u | Display UDP sockets |
| -l | Displays only listening sockets |
| -p | Shows the process using the socket |
| -n | Doesn't resolve service names |



Chúng ta có thể thấy 1 dịch vụ đang chạy ở cổng 10000 nhưng bị chặn ở tường lửa (xem ở IPtable list). Dùng SSH tunnel có thể expose port ở máy cục bộ.





Tên của CMS: webmin, version: 1.580

