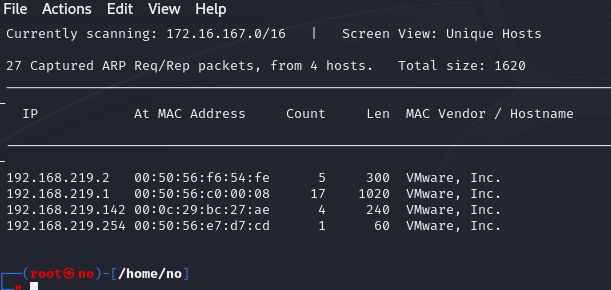
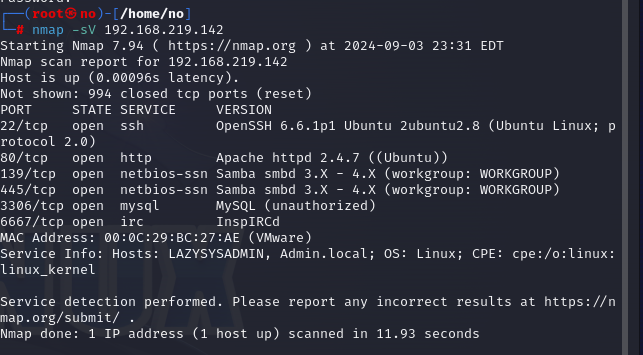
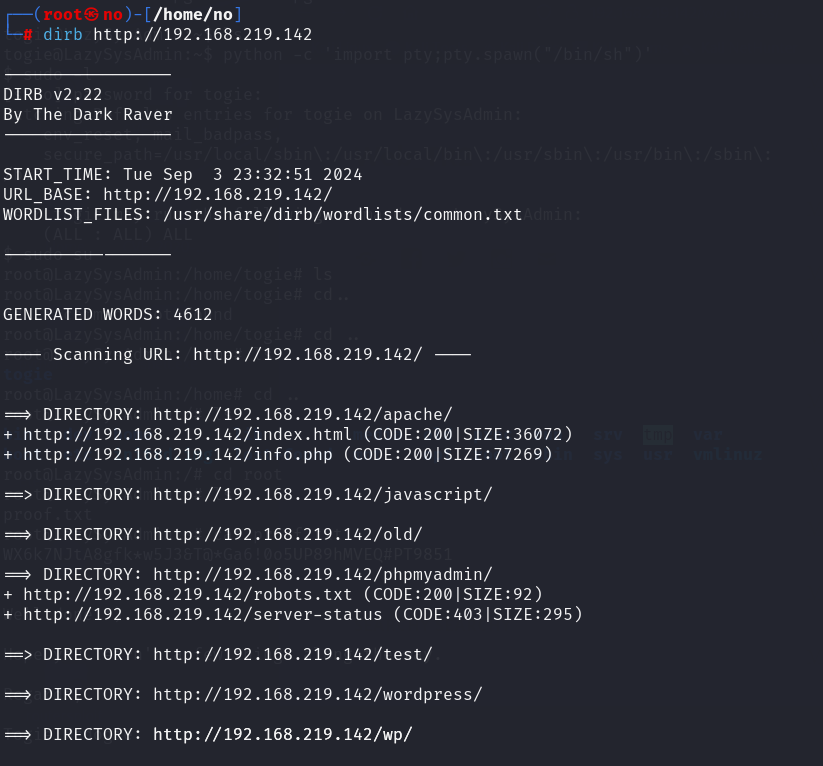
Sử dụng netdiscover để tìm ra IP trên mạng nội bộ của mạng ảo, tìm được IP taget 192.168.219.142



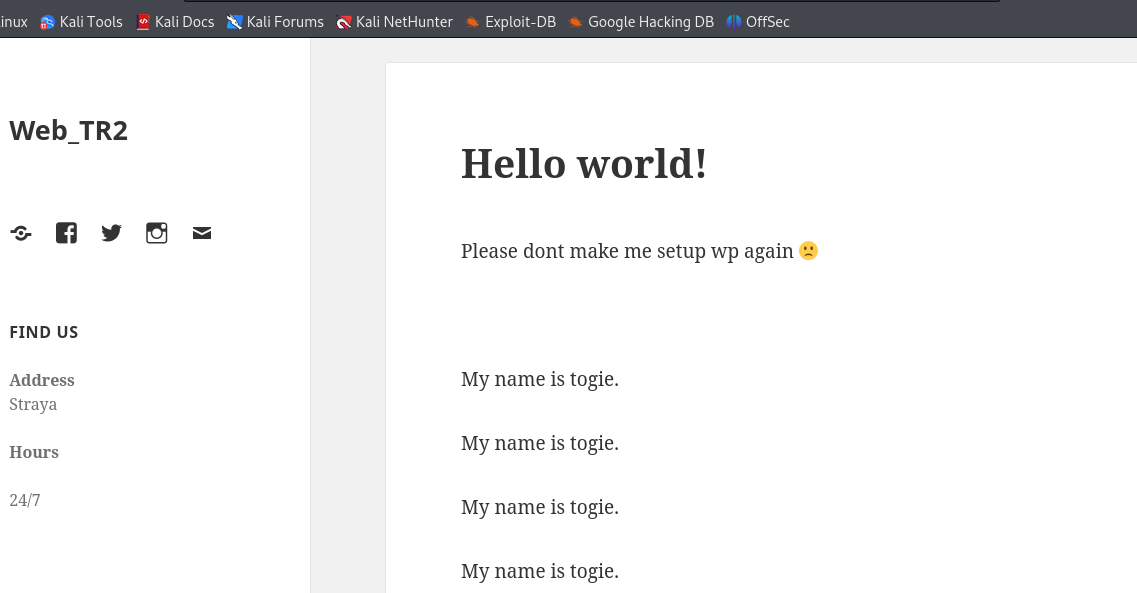
Sử dụng Nmap để quét các cổng taget để tìm các cổng và dịch vụ đang mở



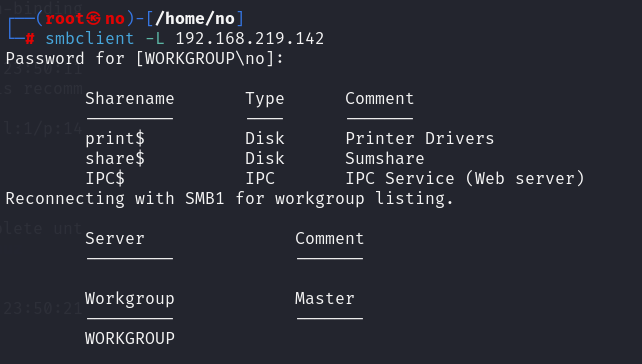
Sử dụng dirb để duyệt tất cả các thư mục để xem các thư mục có trong trang web. Sau khi quét tìm được 1 số thư mục như wordpress,wp,test,..



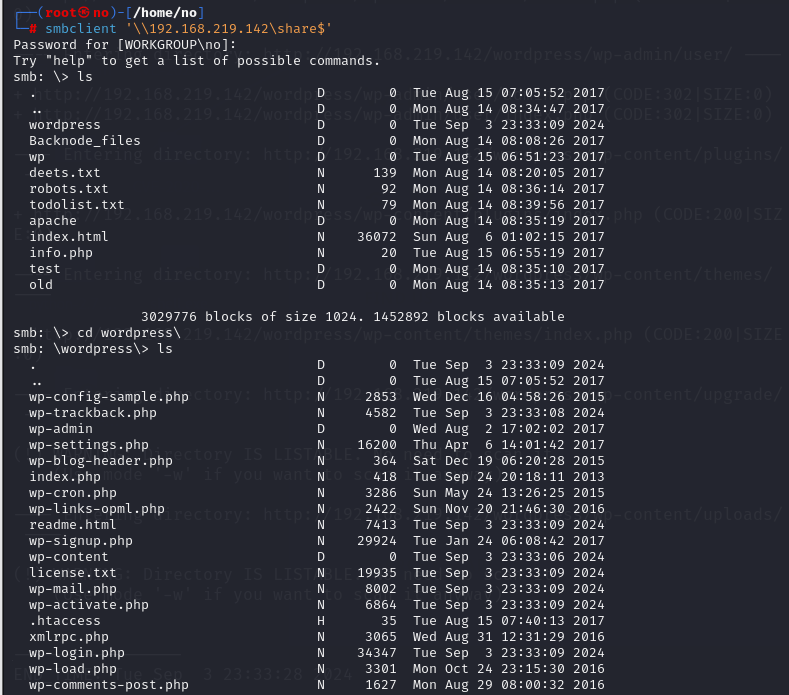
Mở wordpress tìm được trong thư mục có tên người dùng togie



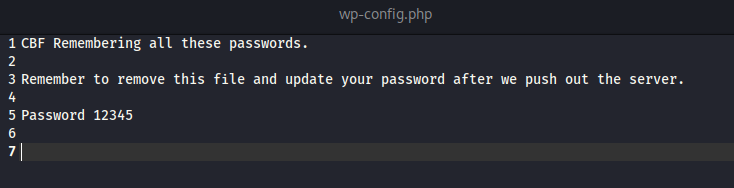
liệt kê các chia sẻ (shares) có sẵn trên một máy chủ sử dụng giao thức SMB



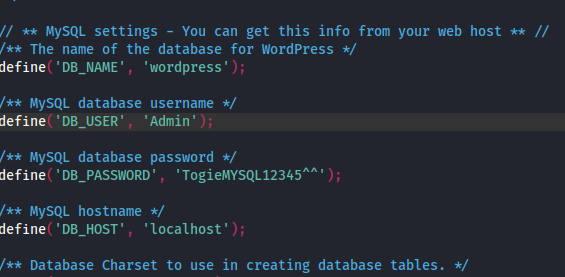
Kiểm tra nội dung “share$” để tìm kiếm thông tin hữa ích



Kiểm tra trong file deets.txt tìm được thông tin 1 password 12345

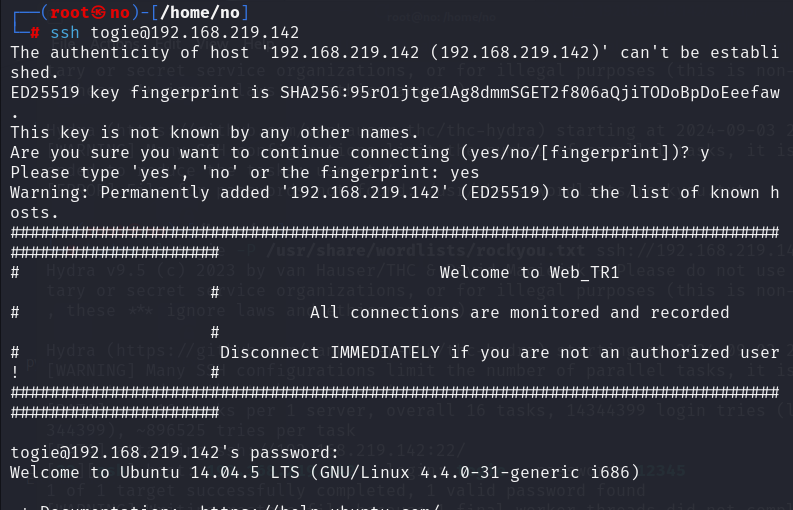


Trong wp-config.php có thông tin cơ sở dữ liệu

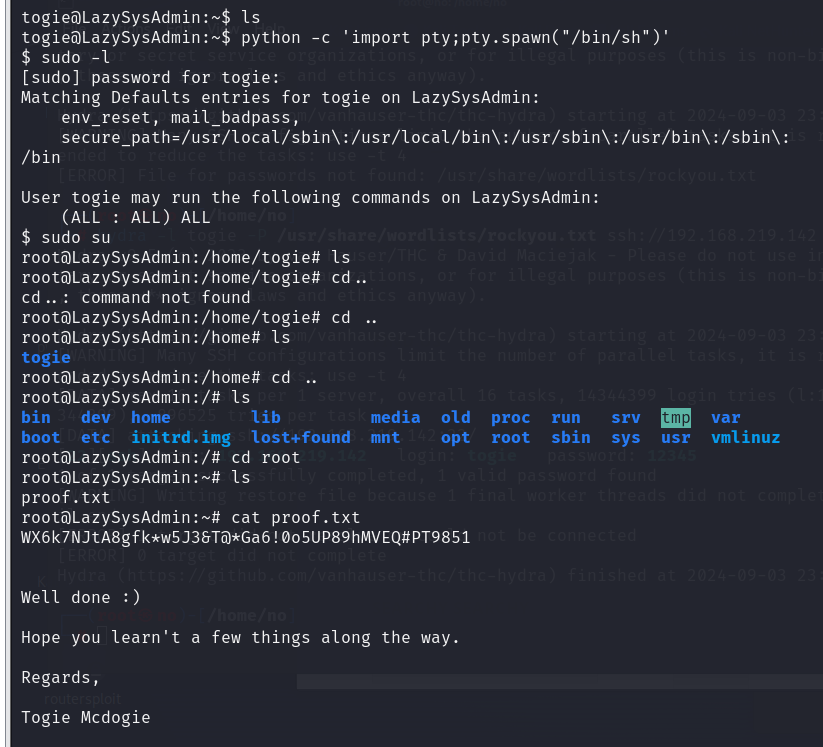


**Tùy chọn 1 cố gắng truy cập ssh**

Thử truy cập ssh vào trang web với username và password tìm được bên trên

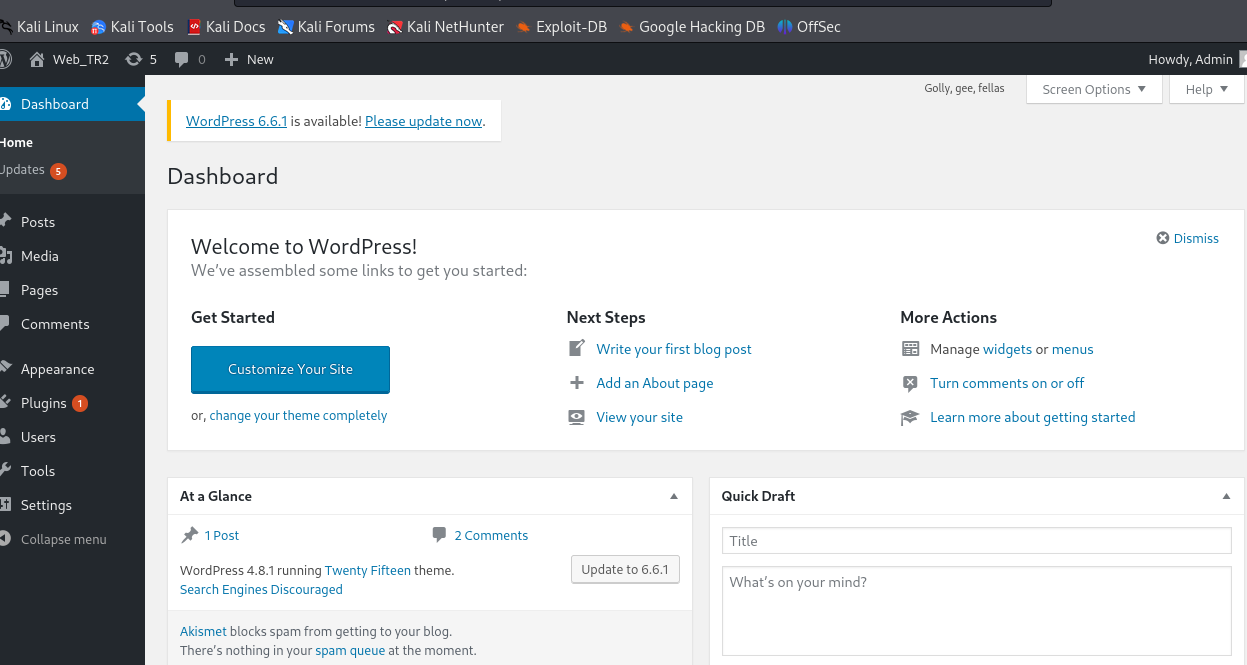


Truy cập thành công, tăng đặc quyền :

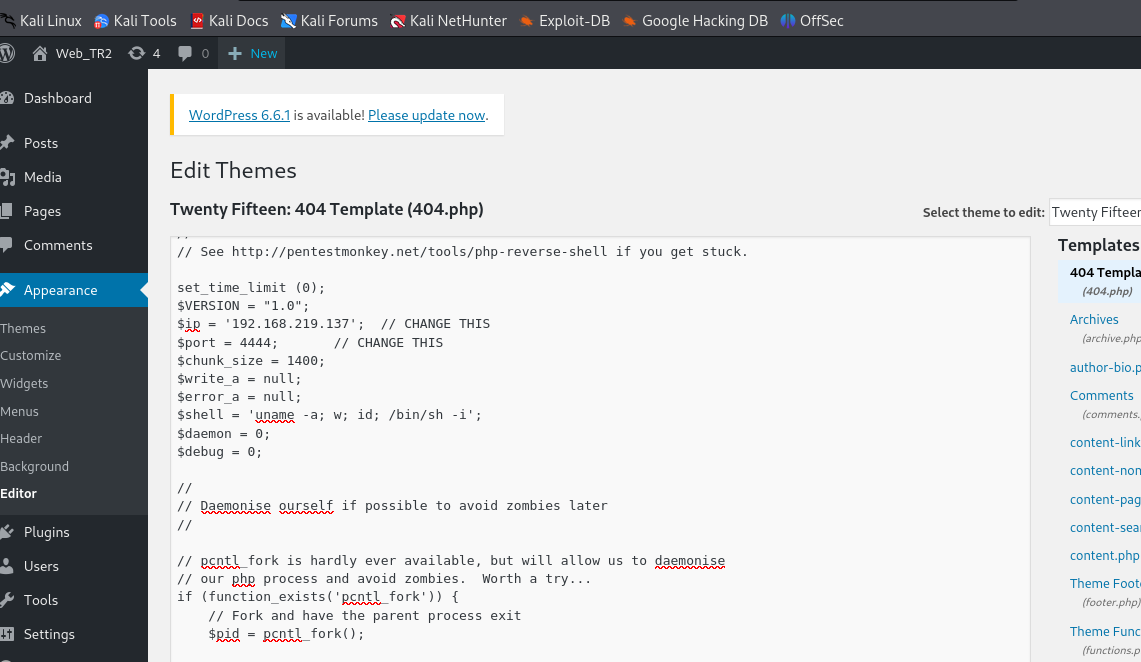


**Tùy chọn 2 Khai thác wordpress**

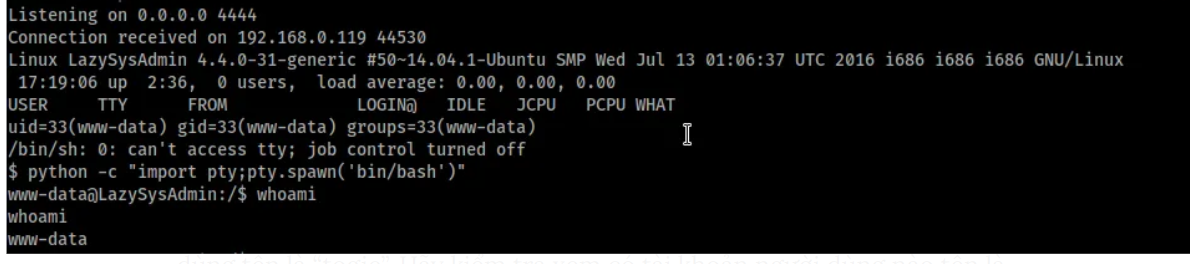
Truy cập bằng usernamr password MySql database bên trên thông qua trang wp-login

****

thay thế mã 404.php bằng PHP-reverse-shell

****

Chạy 404.php và sử dụng netcat để lắng nghe và chặn bắt thông tin phải hồi

****