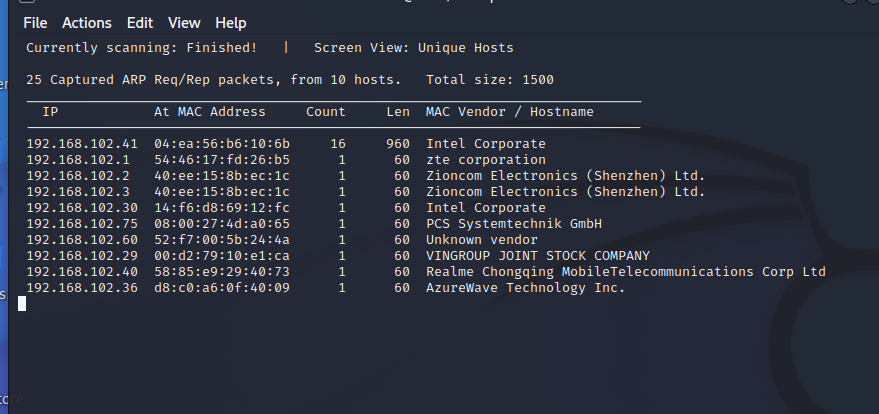
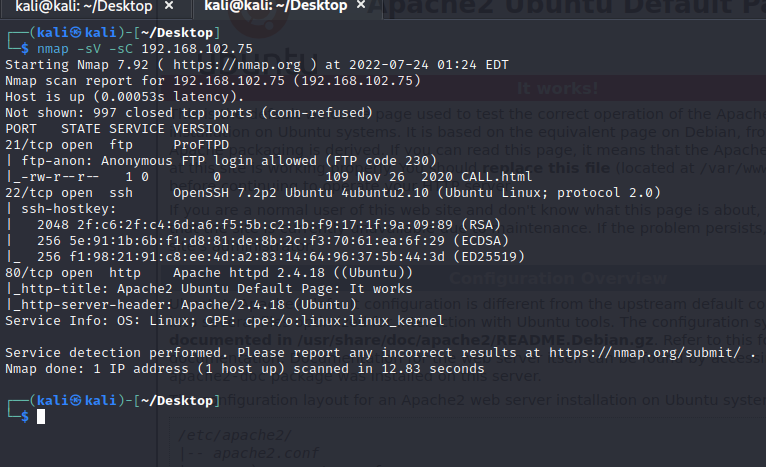
- Dùng netdiscover để quét ra ip của máy bị tấn công

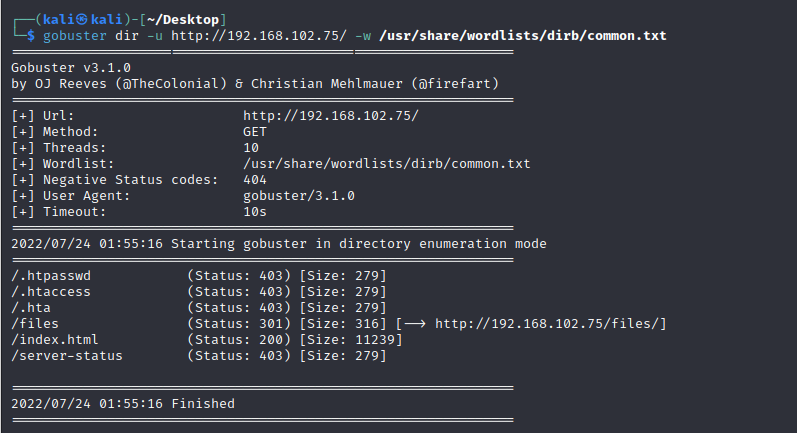


(192.168.102.75 là ip của máy nạn nhân)

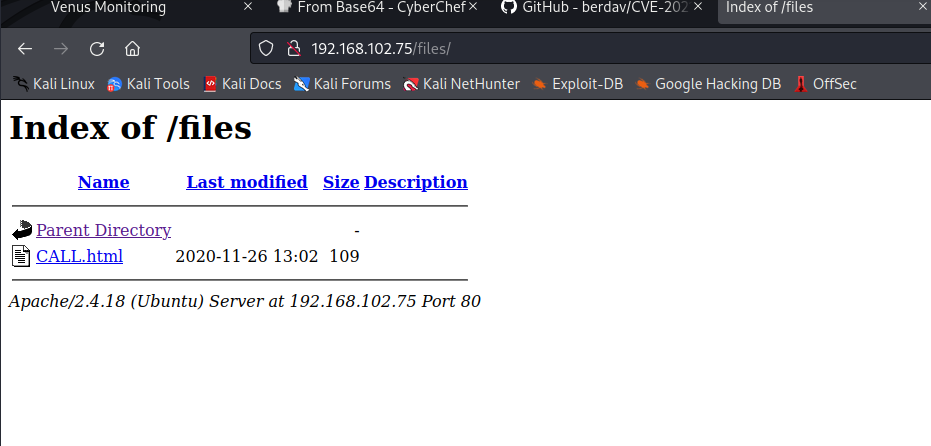
- Dùng nmap để dò ra các port đang có



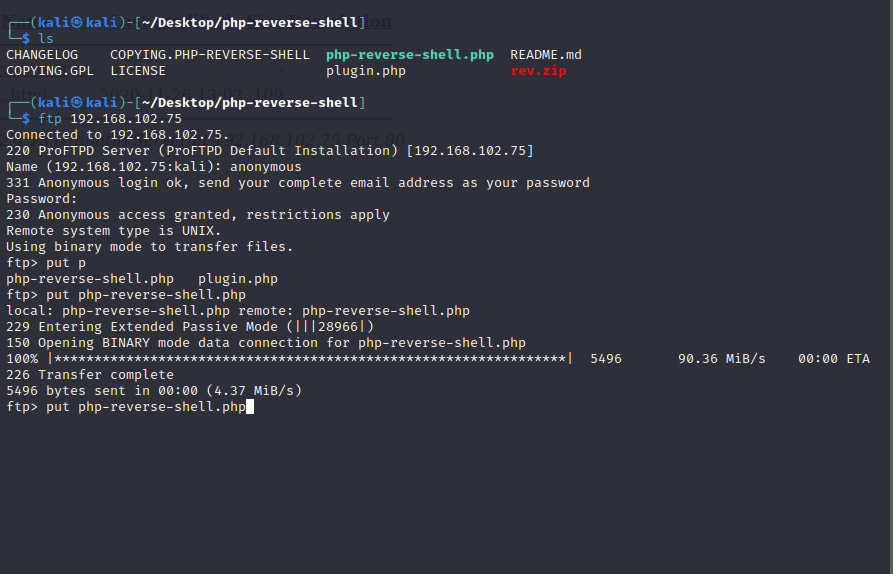
- gobuster để tìm kiếm các đường dẫn ẩn

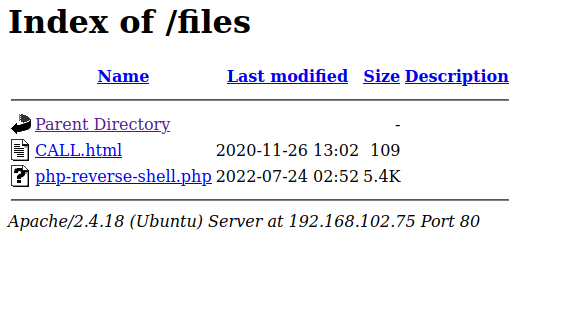


- Tới port 80 và /files để kiểm tra

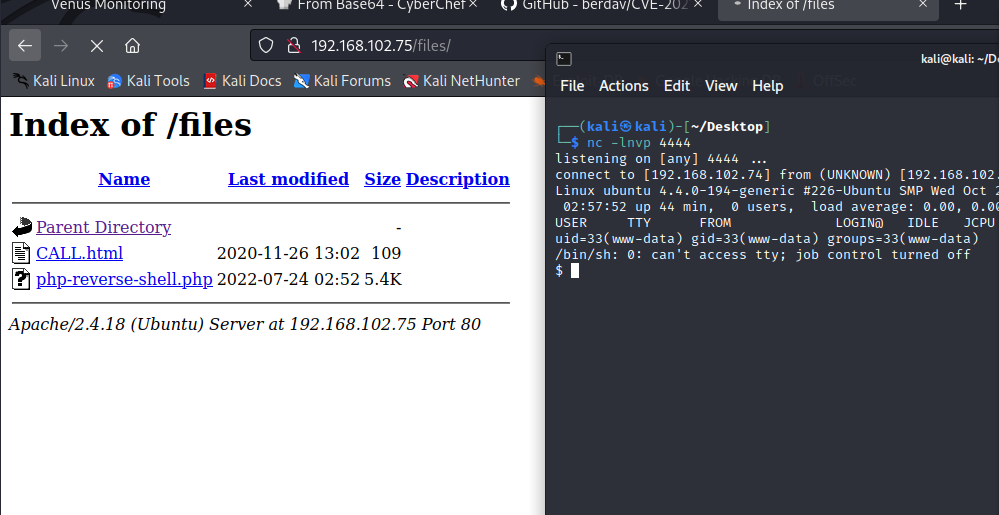


- Vào ftp và up shell lên

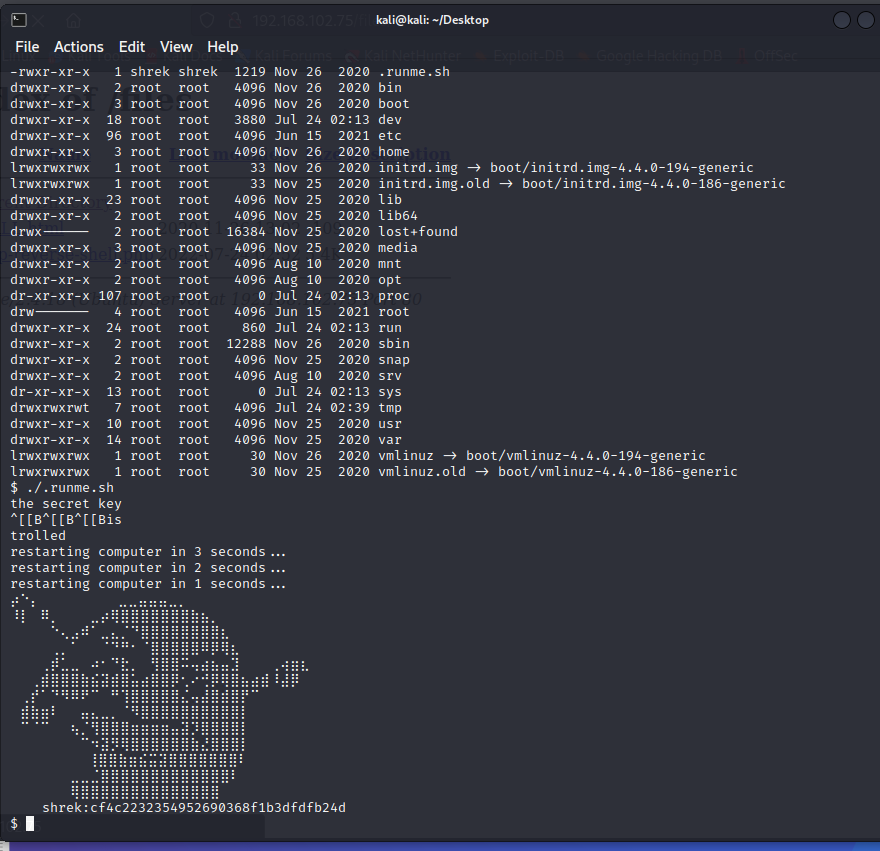




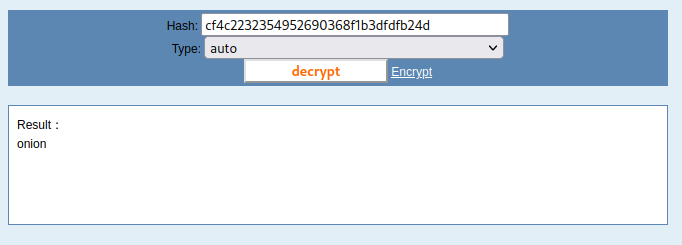
- Thiết lập listener và chạy shell để vào máy chủ nạn nhân



- Tìm kiếm, phát hiện có file .runme.sh, ta chạy thử



- Sử dụng hàm băm để giải mã mật khẩu (cf4c2232354952690368f1b3dfdfb24d) và ta có onion

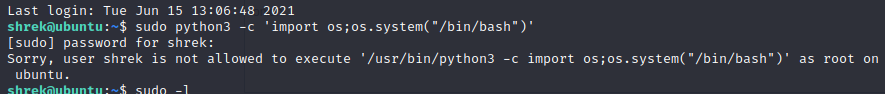


- Giờ ta ssh vào 192.168.102.75 bằng user shrek và nhập mật khẩu (onion)

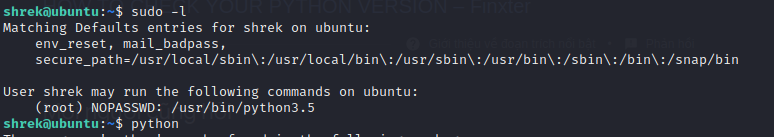


- Thử chạy lệnh spawn shell cơ bản để xem có lên được quyền root liền hay không

sudo python3 -c 'import os; os.system("/bin/bash")'



- Dùng lệnh sudo -l để kiểm tra các quyền chạy lệnh



- T thấy nó sử dụng python3.5, thử chạy lại lệnh spawn shell bằng python3.5



- Vậy là đã lên được root, giờ chúng ta chỉ còn việc kiếm root flag là xong