Báo cáo thực hành cuối kỳ  
Network Security

**Môn học: An toàn mạng**

*GVHD: Nghi Hoàng Khoa*

**Nhóm: Bài cá nhân**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT521.M11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trần Hoàng Khang | 19521671 | 19521671@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | *Alpha Local* | 100% |
| 2 | *Alpha Proof* | 100% |
| 3 | *Kevin Local* | 0% |
| 4 | *Kevin Proof* | 0% |
| 5 |  |  |

BÁO CÁO CHI TIẾT

Note: Ban đầu em không biết nên lỡ viết trên github nên anh có thể đọc write-up ở github cho tiện.

Alpha Local & Alpha Proof: [CTF-Writeup-Practice/Alpha\_Local\_Proof.md at master · AlastorCreeper/CTF-Writeup-Practice (github.com)](https://github.com/AlastorCreeper/CTF-Writeup-Practice/blob/master/Web/University/Network_Security/Final_term/Machine/Alpha_Local_Proof.md)

**Write-up:**

# [A picture containing text Description automatically generated](https://camo.githubusercontent.com/49ca4e13824db07490bd6d57c0dea5887adaa9708a2eb8d72acb841e72507af6/68747470733a2f2f696d672e69636f6e73382e636f6d2f65787465726e616c2d77616e69636f6e2d6c696e65616c2d636f6c6f722d77616e69636f6e2f36342f3030303030302f65787465726e616c2d6d616368696e652d6269672d646174612d77616e69636f6e2d6c696e65616c2d636f6c6f722d77616e69636f6e2e706e67) MACHINE: Alpha Local - Alpha Proof

* IP Address: 192.168.19.150
* Hint: ✍
  + json
  + Thử lại dirsearch

## Write-up - Alpha Local:

* Scan các port bằng **nmap**, đây là payload nmap mình thường dùng nhất nmap -Pn -sV -sC -p- -A -T4 -vv 192.168.19.150  
  Ta có các port sau:

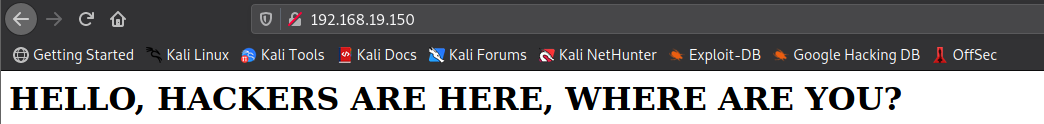
22/tcp open ssh syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

80/tcp open http syn-ack nginx 1.18.0 (Ubuntu)

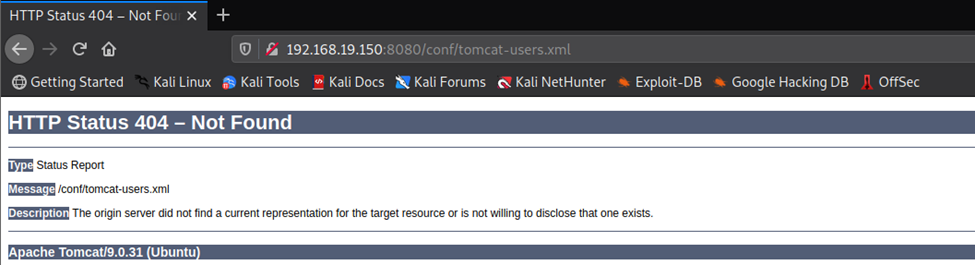
443/tcp open ssl/http syn-ack nginx 1.18.0 (Ubuntu)

8080/tcp open http syn-ack Apache Tomcat

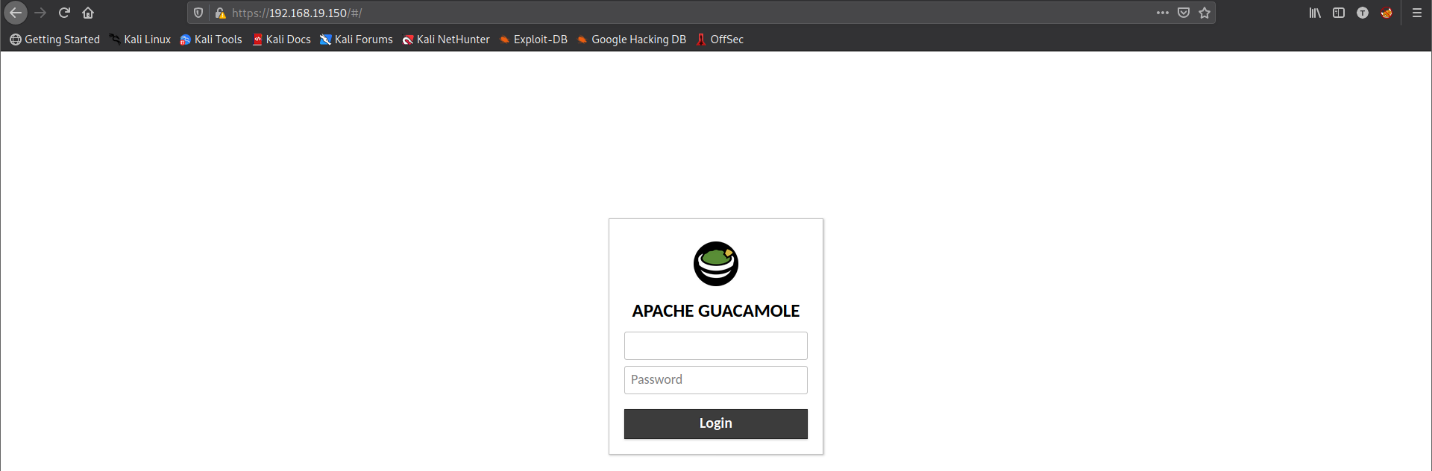
Ở đây chúng ta thấy có web Apache Server Tomcat. Thử vào web:

[](https://user-images.githubusercontent.com/48288606/147381303-bb9607a6-3bcb-4139-8eac-a606f92dd120.png)

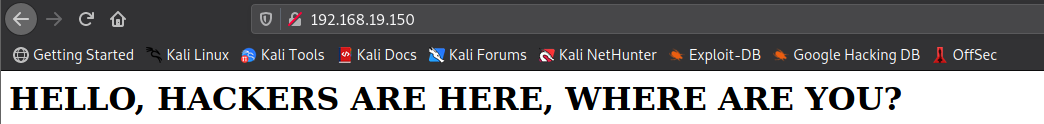
Chỉ là một trang web html. Sau một hồi lục lọi trong web ở port 8080 thì có tìm thêm được thông tin version của server Tomcat **(9.0.31)** , nhưng về sau không khai thác được gì ở chỗ này.

[](https://user-images.githubusercontent.com/48288606/147381409-f8ccc62c-0b40-4d84-bd09-bb3d38b11743.png)

Ngoài ra còn có thêm trang đăng nhập của server nhưng ta chưa có chứng thực

[](https://user-images.githubusercontent.com/48288606/147381678-4aa28505-bdd0-4d65-83b1-9f67a771978e.png)

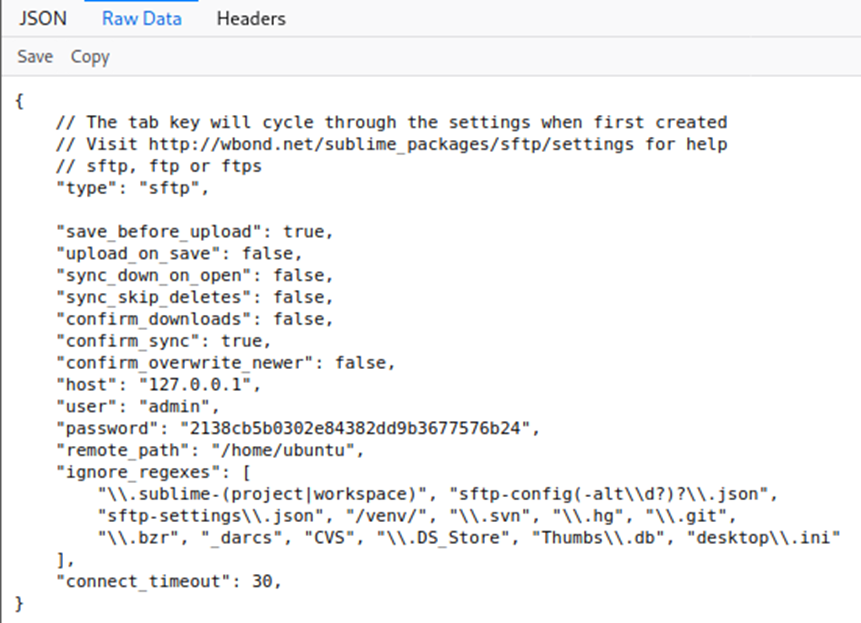
Theo hint, thử sử dụng tool **dirsearch** để tìm kiếm tập tin nhạy cảm hoặc có tồn tại trong server trên URL.  
Command: dirsearch -u http://192.168.19.150

[](https://user-images.githubusercontent.com/48288606/147381362-00656923-d97a-4fe1-9a9f-3bf6f7e3a61c.png)

Ta thấy có 2 file **/index.php** và **/sftp-confing.json** là trả về thành công (Code: 200). File **/index.php** là file html ở trên, ta thử "examine" file json (vừa đúng theo hướng của hint).

[](https://user-images.githubusercontent.com/48288606/147381485-77ffcdb9-27e6-4f61-915f-51268dd54eaa.png)

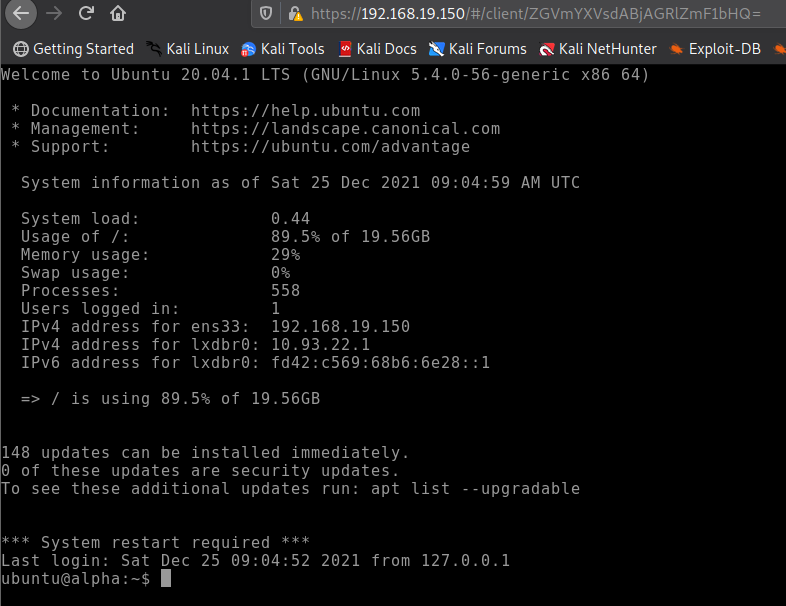
Vào mục "Raw data"

[](https://user-images.githubusercontent.com/48288606/147381491-51c06ca7-232f-4031-a066-fda8e6b027a8.png)

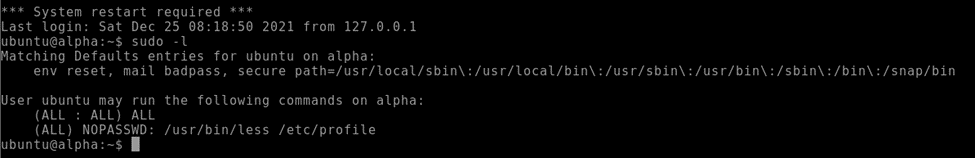
Dữ liệu của file json dường như là một chứng thực của account nào đó, ta thấy tài khoản là **admin**, password thì đã bị hash. Ta thử crack password trên tại trang web [Hash crack](https://hashes.com/en/decrypt/hash)

[](https://user-images.githubusercontent.com/48288606/147381619-830272b9-aaf5-4af0-bf0f-2f03b10467bd.png)

Vậy là ta đã có chứng thực với user: admin và password: password@123. Đăng nhập vào trang login trên.

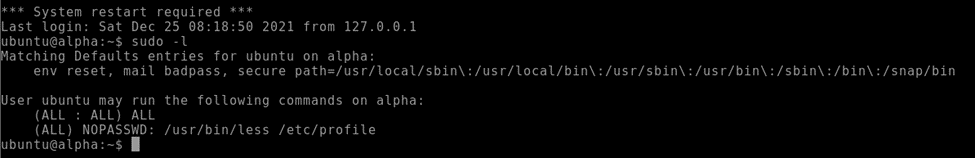
[](https://user-images.githubusercontent.com/48288606/147381721-b2c5d8a7-79ab-45c5-9658-2381f788fff5.png)

Ta đã vào được Web Server. Xem file ở thư mục hiện hành thấy có file **local.txt** và đọc file để lấy flag.

[](https://user-images.githubusercontent.com/48288606/147381820-6182f8f5-d60b-46cd-95aa-847ac9aaf1c4.png)

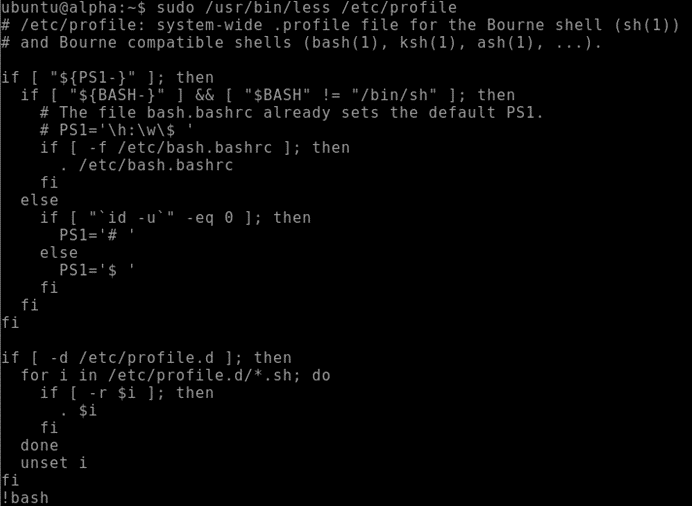
## Leo thang đặc quyền - Alpha Proof:

Dùng lệnh sudo -l để xem quyền hạn thực thi

[](https://user-images.githubusercontent.com/48288606/147381800-78e7cfdc-092b-4581-b34c-a58eb767bd25.png)

Với setup trên, lệnh **less** có thể được thực thi với quyền root tại thư mục **/etc/profile**. Vì thế mình đã tham khảo cách "Escalate Priviledge" của lệnh này tại link sau - [Những cách leo thang đặc quyền với các lệnh phổ biến](https://viblo.asia/p/leo-thang-dac-quyen-trong-linux-linux-privilege-escalation-0-using-sudo-rights-3Q75w8x2KWb).

* Ta nhập lệnh sudo less /etc/profile để thực thi lệnh **less** dưới quyền root trên file **/etc/profile** theo cấu hình cho trước của người administrator
* Trong khi đang ở trong lệnh **less**, nhập !bash và ta đã vào được **root mode**.

[](https://user-images.githubusercontent.com/48288606/147381955-0c322761-860a-484d-bdaa-7c80fdaf9670.png)

Với user **root**, ta đã có thể truy tìm được file \*\*proof.txt" và đọc để lấy flag.

[image](https://user-images.githubusercontent.com/48288606/147381968-602f5382-5390-4c2d-85be-79d5ed4e12b1.png)

### Flag:

* Local.txt: **Wanna.One{@n\_kh0ng\_du@c\_th1\_01\_r@\_ph@i\_kh0ng}**
* Proof.txt: **Wanna.One{nqu0j\_cu4\_c0nq\_ckunq\_pk4j\_dj\_v40\_l0nq\_nqu0j,\_cku\_dunq\_dj\_v40\_l0nq\_d4t}**