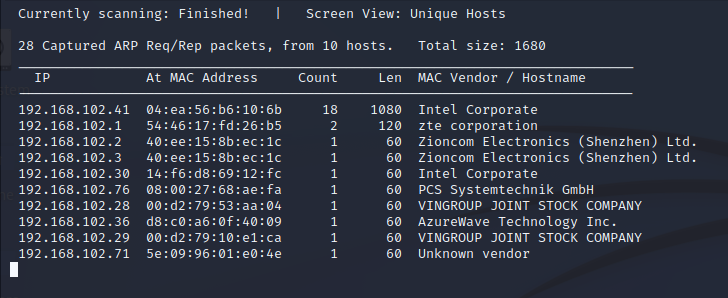
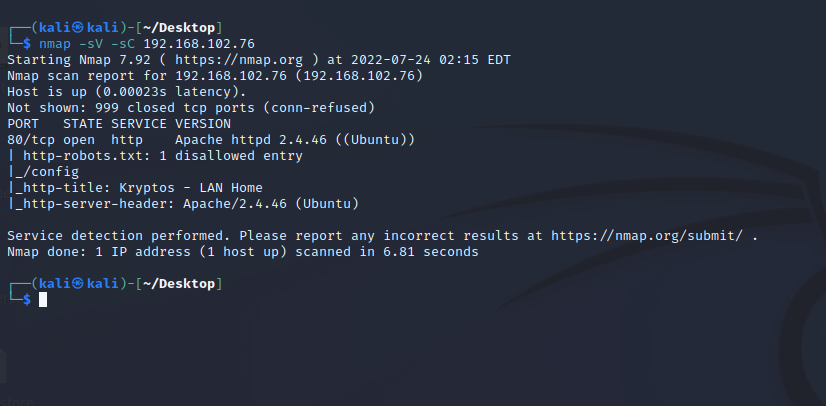
- Dùng netdiscover để dò ra ip của máy nạn nhân

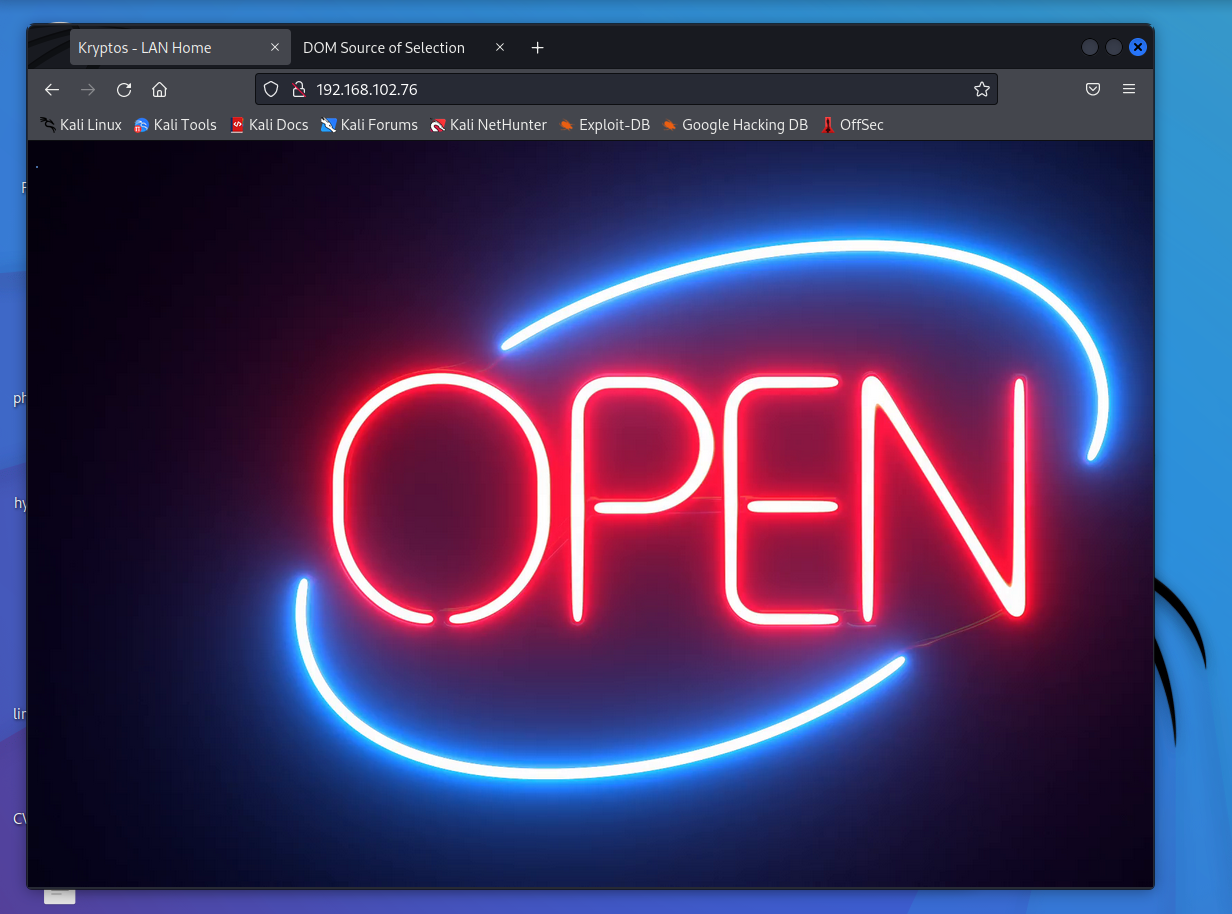


(192.168.102.76 chính là ip của nạn nhân)

- Dùng nmap để kiểm tra các port



- Cổng 80 đang mở, ta mở trình duyệt lên kiểm tra



- Sau khi xem source code thì ta phát hiện jubiscleudo có thể chính là username

<html lang="pt-br"><head>

<meta charset="UTF-8">

<meta http-equiv="X-UA-Compatible" content="IE=edge">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="[https://fonts.googleapis.com/css?family=RocknRoll+One](view-source:https://fonts.googleapis.com/css?family=RocknRoll+One)" rel="stylesheet">

<link rel="stylesheet" type="text/css" href="[css/file.css](view-source:http://192.168.102.76/css/file.css)">

<title>Kryptos - LAN Home</title>

</head>

<body>

<a href="[#](view-source:http://192.168.102.76/)" class="menu-open"><img src="[imagens/logo\_menu.png](view-source:http://192.168.102.76/imagens/logo_menu.png)" width="2" height="2"></a>

<div class="overlay"></div>

<div class="menu">

<a href="[#](view-source:http://192.168.102.76/)" class="menu-close">×</a>

<ul>

<li><a href="[login\_page/login.html](view-source:http://192.168.102.76/login_page/login.html)" target="\_blank">Login</a></li>

</ul>

</div>

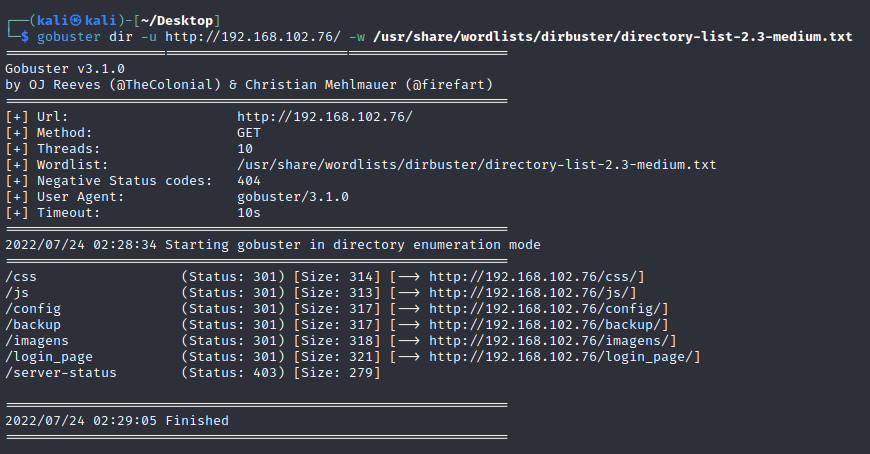
<!-- "Please, jubiscleudo, don't forget to activate the port knocking when exiting your section, and tell the boss not to forget to approve the .jpg file - dev\_suport@hackable3.com" -->

<script src="[https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js](view-source:https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js)"></script>

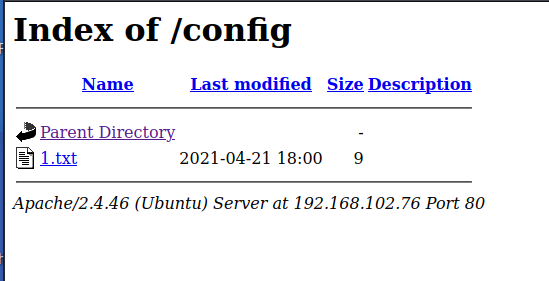
<script src="[js/script.js](view-source:http://192.168.102.76/js/script.js)"></script>

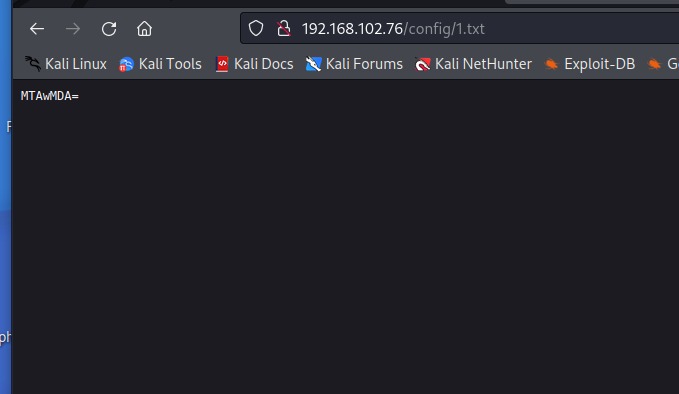
</body></html>

- Dùng gobuster để tìm ra hết các đường dẫn bị ẩn

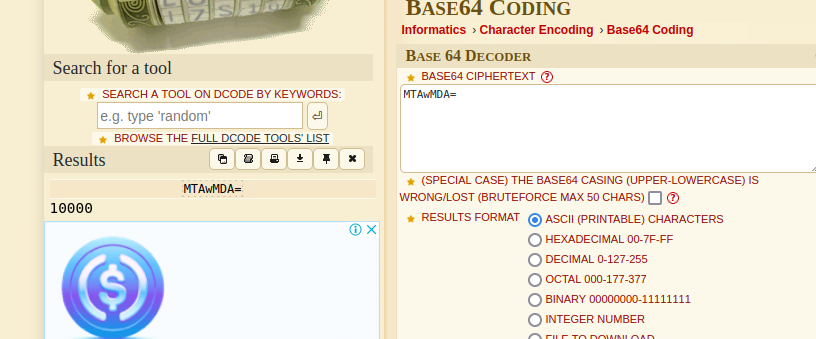


- Vào /config



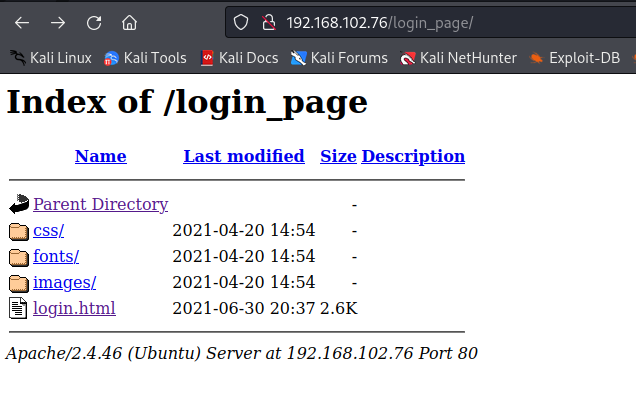


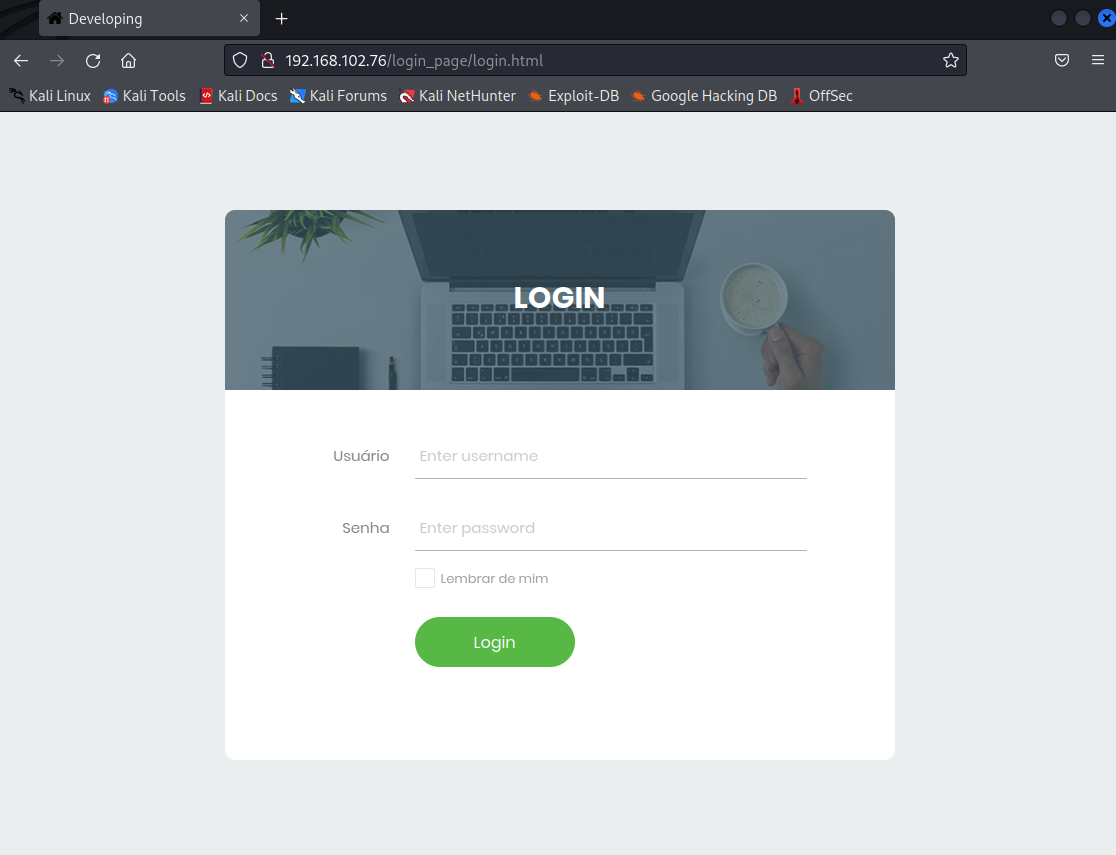
- Đoạn mã đầu tiên, dùng base64 để decode



- Kết quả đầu tiên: 10000 (Đây sẽ là port đầu tiên để lát nữa ta sẽ dùng thủ thuật truy cập khác là port knocking)

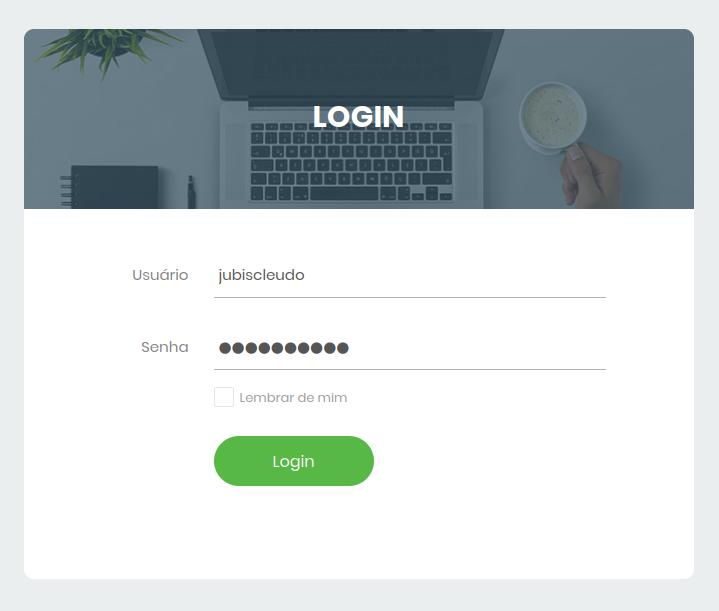
- Vào /login\_page



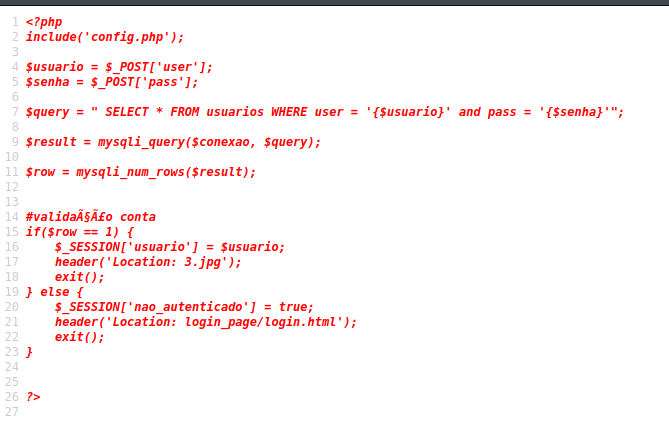


- Sử dụng sql injection và để username là jubiscleudo

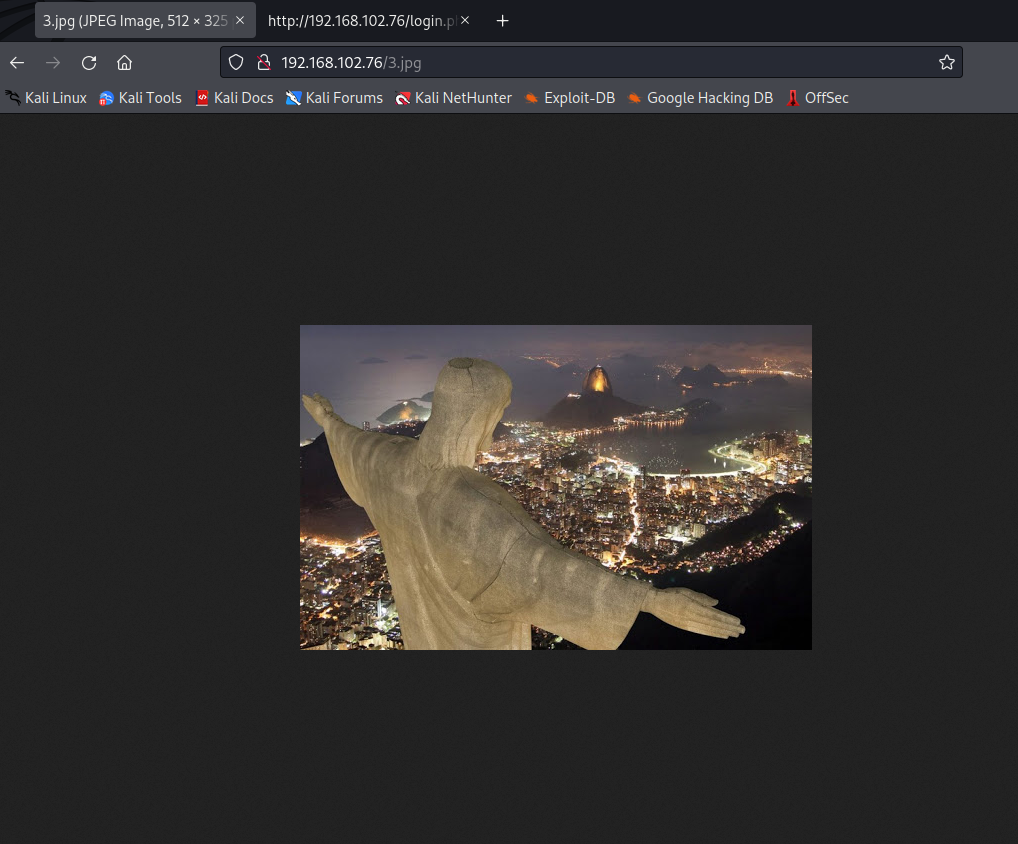
- Phần mật khẩu là ‘ or 1=1--



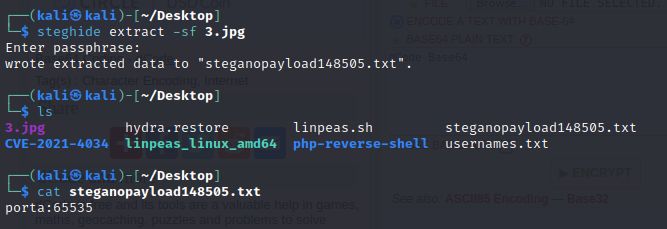
- Sau khi login xong thì view page source



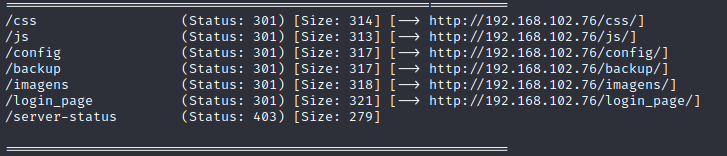
- Kiểm tra 3.jpg



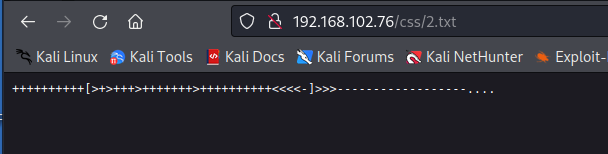
- Tải ảnh về và dùng tool steghide để kiểm tra các dữ liệu bị ẩn



- Kết quả: 65535 (Đây là port thứ 3 để knocking vì theo hint bức ảnh là số 3)



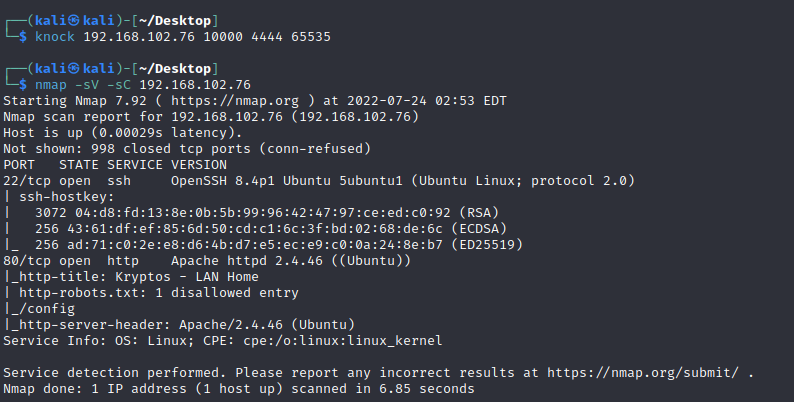
- Kiểm tra hết từng đường dẫn để tìm ra port cuối cùng





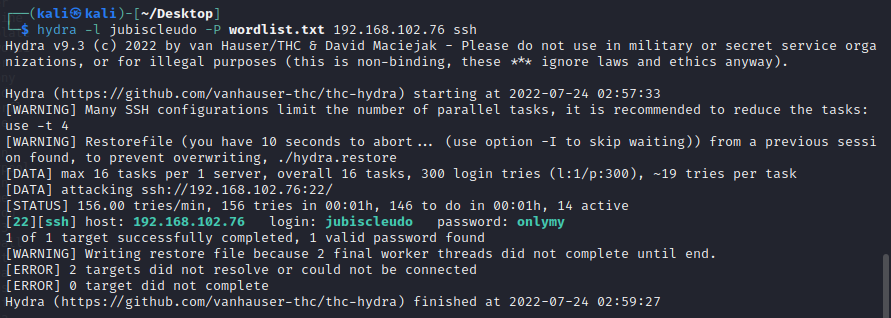
- Kết quả: 4444 (Đây là port cuối cùng để knocking)

- Triển khai knocking sau đó nmap lại, ta phát hiện cổng 22 có sử dụng ssh



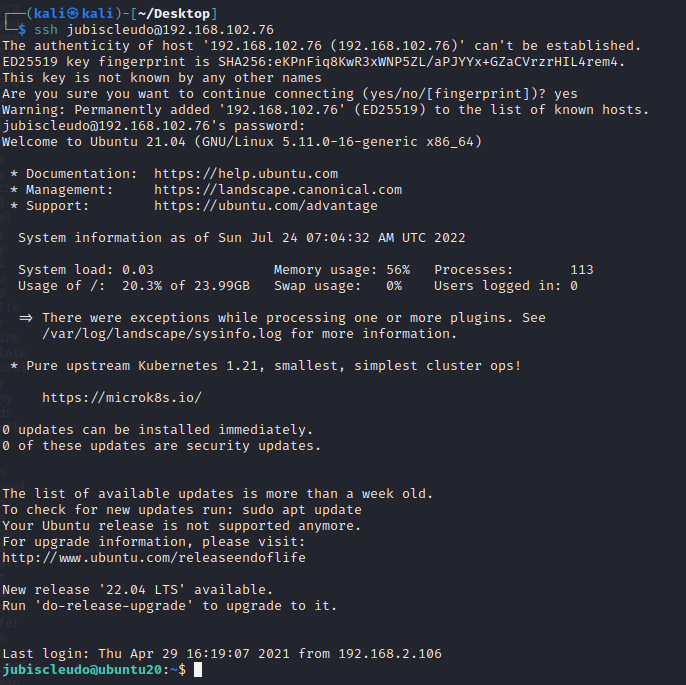
- Dùng hydra để bruteforce mật khẩu cho username jubiscleudo

- Lúc mà ta dùng gobuster để tìm đường dẫn, ở phần /backup, nó có cho ta một cái wordlist.txt để ta bruteforce

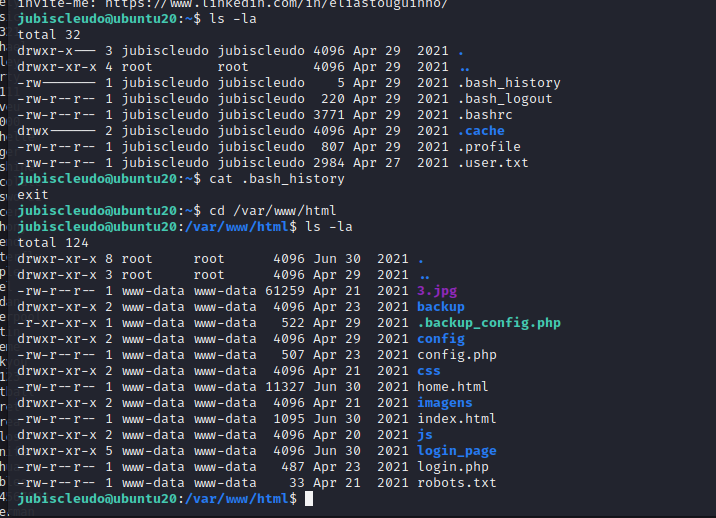


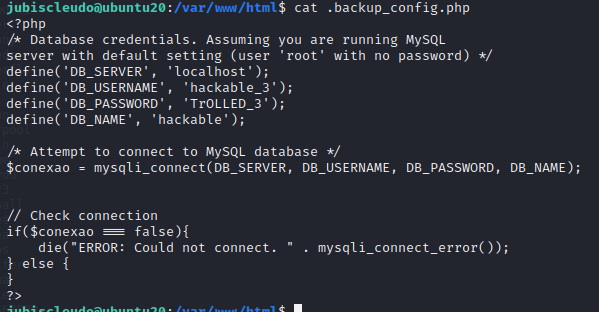
- Sau khi bruteforce thì ta tìm ra được mật khẩu của username jubiscleudo là onlymy

- Dùng nó để ssh vào máy chủ nạn nhân



- Tìm và đọc file backup vì đó là nơi thay đổi user và mật khẩu mà ta có thể can thiệp vào đó để leo thang





- Đổi user

