

CTF Report

Full Name: Oluwatobi Akinlaja

Program: HCS - Penetration Testing 1-Month Internship

Date: 12/08/2024

Category: {OSINT (SOCIAL HUNT)}

Description: One of my tech-savvy friends constantly claims that using Linux these days is akin to trying to light a fire with stones. We often tease him by saying, 'One day, you'll be the one known as the LinuxKiller and go by the online persona of 'LinuxKiller69'. Despite not being a frequent social media user, he occasionally checks his account, where the platform's mascot is 'Snoo'. We're curious to know where else he has created accounts and what tech-related thoughts he's sharing there.

Challenge Overview: The challenge includes identifying and mapping out social media and other online accounts of 'LinuxKiller69', who is rumored to use Linux and has a social media persona with the mascot 'Snoo'. The username 'Linuxkiller69' was searched on the webpage and an Instagram page was found. On the Instagram page, the picture element was inspected and the flag was uncovered.

This report outlines the systematic approach required to uncover the flag in the Social Hunt CTF challenge, leveraging various ethical hacking methodologies to explore, exploit, and extract the necessary information.

Flag: flag{cr0ss_pl4tf0rm}



Category: {CRYPTOGRAPHY (RULE THE WORLD)}

Description: Mr. Bob sent us this file and asked us to retrieve the secret, he also mentioned that follow these electrical impulses, it will take you to the destination. Focus on the formation! It's! =Binary & don't fall in the trap! Two persons are involved in this, so both of them are needed, a single one won't make it for you.




Challenge Overview: This challenge involves analyzing a provided file to retrieve a secret by applying decryption techniques and carefully interpreting the data. The file contains a set of binary number which serves as the encrypted code. To decrypt this, decryption tool (Baudot-Murray-Code, <https://v2.cryptii.com/ita2/text>) was utilized to transform the binary codes to text. Once done the hidden flag was identified.

This report outlines the systematic approach required to uncover the flag in the Rule the world ctf challenge, exploring different encryption and decryption techniques.

Flag: `flag{notaregularbinary}`

INTERPRET AS
BAUDOT-MURRAY-CODE ▼

CONVERT TO
TEXT ▼

Separator	Transform
10010 11000 01010 00001 11100 00100 00110 10110 00101 00111 11100 00100 01001 11000 10010 11000 01010 00100 00101 00110 10000 00100 00011 11100 00001 10000 11011 01100 00100 11111 01110 11000 01100 00101 00001 01110 10000 00001 10000 00111 01010 00100 00011 01001 00110 10110 00110 00101 01110 00110 01100 11010 00100 00001 10010 00110 10000 11011 01100 00100 11111 00101 00001 01001 00100 01001 11000 00100 00001 00110 00111 00101 11100 11000 01001 00100 10000 00001 11100 10110 11000 01010 00100 00110 01100 01110 00110 01001 00110 01001 00111 01100 10000 00100 00111 10000 00100 10010 00011 11001 11000 01010 00001 00100 00001 10000 00100 01001 11000 10010 11000 01010 00001 00100 11100 00011 11010 01100 00011 00100 00011 10010 00110 10111 00111 00011 11011 11100 00100 11111 00111 10000 00100 00001 01100 00110 11100 00100 00011 01001 00100 11100 00110 01100 00110 11100 00100 11110 00001 01100 00110 00011	<div>None ▼</div> <p>lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. flagnotaregularbinar</p> <div>   466</div>

Category: {WEB 2.0(LOCK_WEB)}

Description: "It's important to follow good content discovery methodology on sites you are testing. This is NOT always something like dirbuster or other bruteforcing approaches."

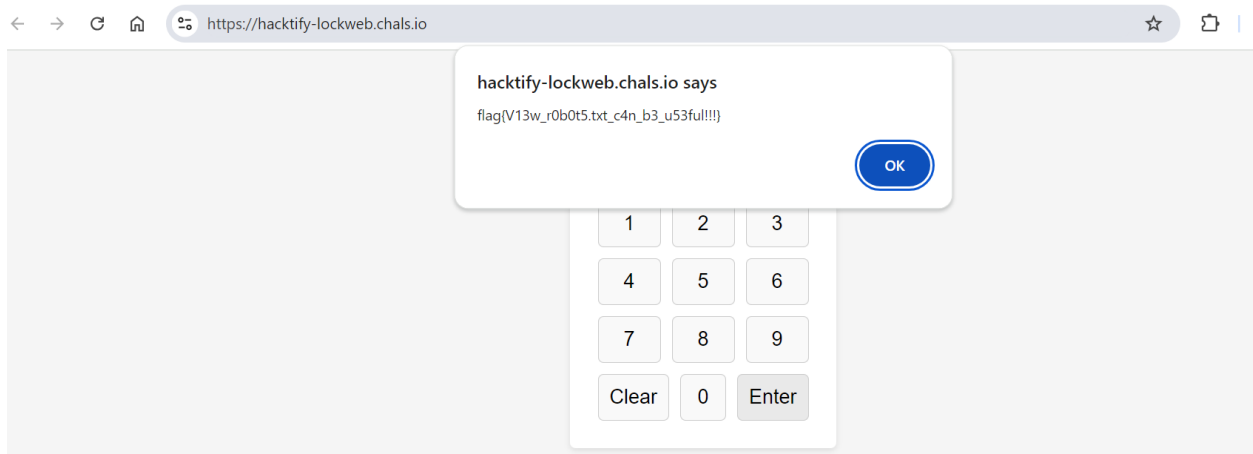
Challenge Overview: This challenge involves reviewing the URL's source code, using browser developer tools to inspect the HTML forms, cookies, etc. Possible vulnerabilities were determined by conducting reconnaissance to local field inputs and test for vulnerabilities such as SQL, XSS, etc. The technique used robot.txt brute force analysis where different passwords/pin were injected to determine the correct pin. Tool used was python.

The challenge requires a multi-faceted approach: examining the webpage's source and inputs, identifying vulnerabilities, utilizing `robots.txt` for credential testing guidance, and employing python to uncover hidden directories and files.

Pin: 1928

Flag: flag{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

```
Response for PIN 1925: {'success': False}
Response for PIN 1926: {'success': False}
Response for PIN 1927: {'success': False}
Response for PIN 1928: {'success': True, 'secretText': 'flag{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}'}
Correct PIN found: 1928
Finished checking all PINs.
```



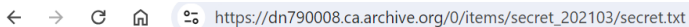
Category: {OSINT (TIME MACHINE)}

Description: Mr. Trojan Hunt has power to travel time. He is hiding some extremely confidential file from the government. Can you help NIA to get secrets of Trojan Hunt?

Challenge Overview: This challenge requires assisting the National Intelligence Agency (NIA) in locating a highly confidential file hidden by Mr. TrojanHunt, who can travel through time. The file, crucial for national security, has been concealed to evade government detection.

To uncover it, various investigative and technical strategies were employed, including pattern analysis, tracing time-related clues, and exploring hidden files. Ultimately, the file was found on the website [archive.org/details/secret_202103] (https://archive.org/details/secret_202103), where the `secret.txt` file was successfully recovered.

Flag: `flag{Tr0j3nHunt_t1m3_tr4v3l}`



`flag{Tr0j3nHunt_t1m3_tr4v3l}`

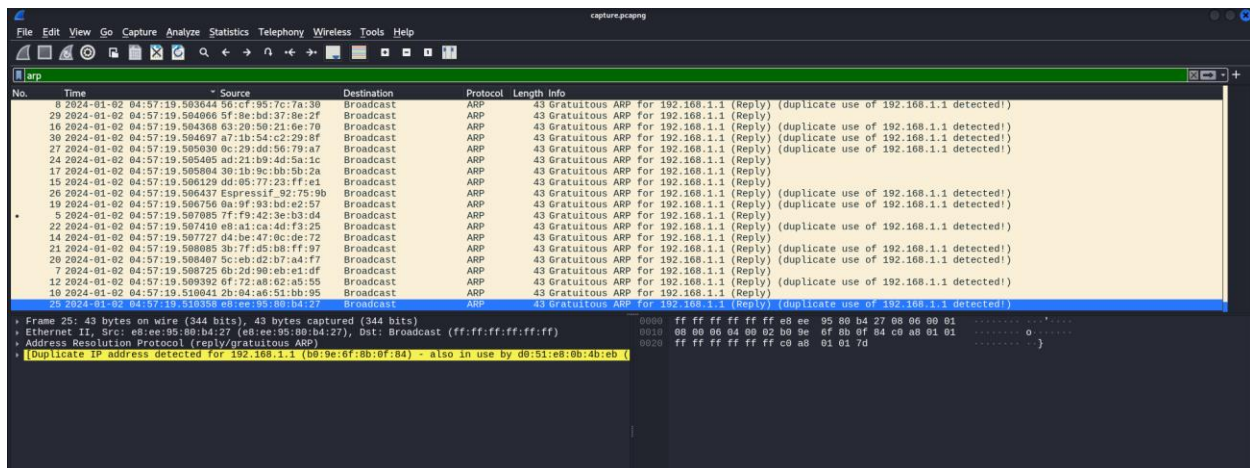
Category: {NETWORK FORENSICS (MYSTIC CONNECTIONS)}

Description: Are you ready to unravel the hidden secrets of network communication and showcase your prowess with your sharp analysis? Sharpen your analysis skill to unhide the hidden secret.

Challenge Overview: The hidden intricacies of network communication are found in the fine details of signal transmission, hardware constraints, addressing, routing, error checking, and protocols, all of which can affect performance and security. Through careful analysis, these complexities and potential issues come to light, uncovering opportunities for optimization and ensuring data integrity.

The file was analyzed in Wireshark by applying an 'arp' filter to focus solely on ARP packets. After sorting the ARP packets by the time column to understand their sequence, each packet was inspected for encrypted data, decoded to reveal the codes, and the flag was retrieved from the decoded information.

Flag: flag{ARP_b31ng_s1mpl3}}



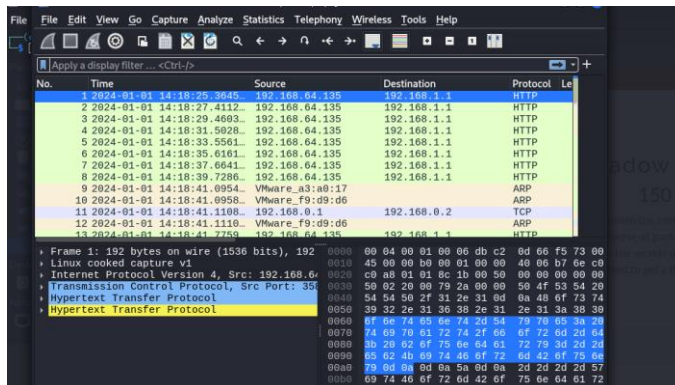
Category: {NETWORK FORENSICS (SHADOW WEB)}

Description: Unravel hidden data within the intricate landscape of protocols. This Multiverse of packets contains some Form Data which can reveal the secrets of the Web. Try to find this secrets that are scattered to get a flag.

Challenge Overview: This challenge involves uncovering hidden data in complex network protocols. It includes analyzing captured packets to identify protocols like HTTP or HTTPS handling form data, filter for POST requests to isolate form submissions, and then inspect and decode the payloads to uncover any hidden or encrypted information.

The packet capture file was first analyzed in Wireshark to inspect the network traffic. After thoroughly examining the packets, we utilized Tshark with the command: `tshark -r capture.pcapng -T fields -e http.file_data -Y "http.request.method == POST"`. This command extracted the payload data from HTTP POST requests. Each packet was then carefully inspected to identify the relevant characters. These characters were examined in the hex view section of the packets. To find the flag, sort the ARP packets by their timestamp to arrange them chronologically. The flag is encoded at the end of each hex value, marked by the letters (X Z). Combine these letters to form a string. Finally, open a terminal and decode this string using the following command: `echo <letters> | base64 --decode`. Replace <letters> with the combined string of letters you identified.

Flag: flag{mult1pl3p4rtsc0nfus3s}



```

Z\r\n---WebKitFormBoundary\r\n
m\r\n---WebKitFormBoundary\r\n
x\r\n---WebKitFormBoundary\r\n
h\r\n---WebKitFormBoundary\r\n
Z\r\n---WebKitFormBoundary\r\n
3\r\n---WebKitFormBoundary\r\n
t\r\n---WebKitFormBoundary\r\n
t\r\n---WebKitFormBoundary\r\n
d\r\n---WebKitFormBoundary\r\n
W\r\n---WebKitFormBoundary\r\n
x\r\n---WebKitFormBoundary\r\n
O\r\n---WebKitFormBoundary\r\n
M\r\n---WebKitFormBoundary\r\n
X\r\n---WebKitFormBoundary\r\n
B\r\n---WebKitFormBoundary\r\n
s\r\n---WebKitFormBoundary\r\n
M\r\n---WebKitFormBoundary\r\n
3\r\n---WebKitFormBoundary\r\n
A\r\n---WebKitFormBoundary\r\n
O\r\n---WebKitFormBoundary\r\n
c\r\n---WebKitFormBoundary\r\n
n\r\n---WebKitFormBoundary\r\n
R\r\n---WebKitFormBoundary\r\n
z\r\n---WebKitFormBoundary\r\n

```

Category: {WEB 2.0 (HIDDEN PATHWAYS)}

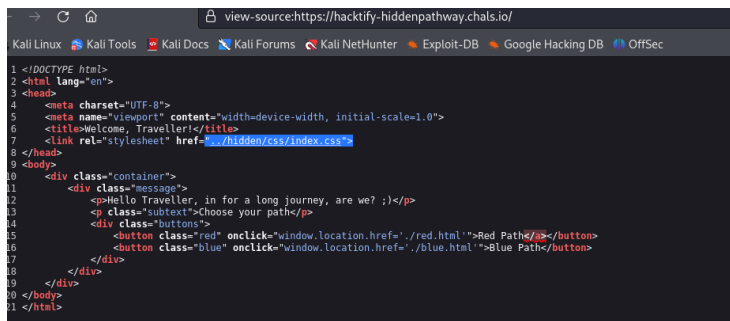
Description: Dare to venture into the unknown, and may the thrill of discovery guide you on your journey!

Challenge Overview: This challenge involves analyzing the source code of the URL to discover hidden secret paths.

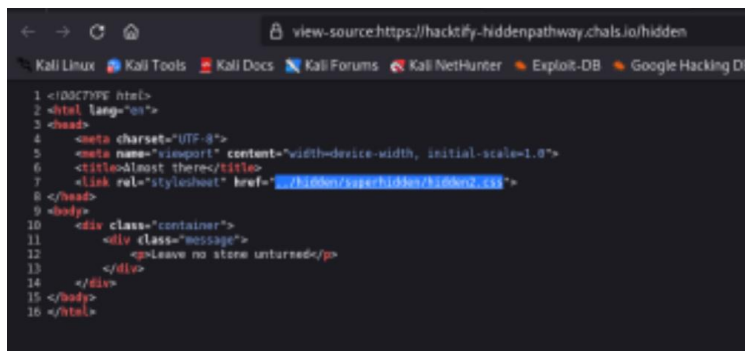
Upon examining the source code of the URL <https://hacktify-hiddenpathway.chals.io/>, a hidden path /hidden was discovered. By appending this path to the URL and viewing the source code again, a further hidden path /hidden/super hidden was found.

To retrieve the flag, navigate to this newly discovered path by updating the URL:
<https://hacktify-hiddenpathway.chals.io/hidden/superhidden>

Flag: flag{w3ll_d0n3_tr4v3ll3r!}



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Welcome, Traveller</title>
7   <link rel="stylesheet" href="/hidden/css/index.css">
8 </head>
9 <body>
10   <div class="container">
11     <div class="message">
12       <p>Hello Traveller, in for a long journey, are we? ;)</p>
13       <p class="subtext">Choose your path</p>
14       <div class="buttons">
15         <button class="red" onclick="window.location.href='./red.html'">Red Path</button>
16         <button class="blue" onclick="window.location.href='./blue.html'">Blue Path</button>
17       </div>
18     </div>
19   </div>
20 </body>
21 </html>
```



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Almost there</title>
7   <link rel="stylesheet" href="/hidden/superhidden/hidden2.css">
8 </head>
9 <body>
10   <div class="container">
11     <div class="message">
12       <p>Leave no stone unturned</p>
13     </div>
14   </div>
15 </body>
16 </html>
```

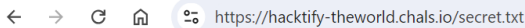
Category: {WEB 2.0 (THE WORLD)}

Description: Welcome to "The World" challenge! You've landed on a webpage saying "Hello World!" Looks simple, right? But there's more to it than meets the eye.

Challenge Overview: The challenge involves identifying hidden paths and potentially sensitive information through various vulnerabilities.

To solve the challenge, inspect the page source code for comments, links, or references to hidden paths. Then use vulnerability scanner tool Dirbuster to find hidden directories or files. Various URL parameters and path manipulations to uncover hidden endpoints were tested. Secret.txt which is a hidden path was discovered. To retrieve the flag, navigate to this newly discovered path by updating the URL: <https://hacktify-theworld.chals.io/secret.txt>

Flag: flag{Y0u_hav3_3xpl0reD_th3_W0rLd}



FLAG{Y0u_hav3_3xpl0reD_th3_W0rLd}