Penetration Testing Hackathon 2024

Prepared by: Isabelle Jaber, Rohan Shah, and Felix Mukunzi

INTRODUCTION: Pickle Rick

This Rick and Morty-themed challenge required us to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.

Goals

Scan the machine

Locate credentials

Find ingredients to save Rick

Tools and Methods

Nikto

Web vulnerability scanning

Gobuster

File and directory brute forcing

CLI

Command input method

NMAP

Scan the network of the Target IP address

Process

Legend:
Target IP Address = TiP

NMAP

`nmap -sV [TiP]`

Found open ports 22 (SSH) and 80 (HTTP)

Web

Visited
`http://[TiP]`

Inspected the page source and found username `R1ckRul3s`

Gobuster

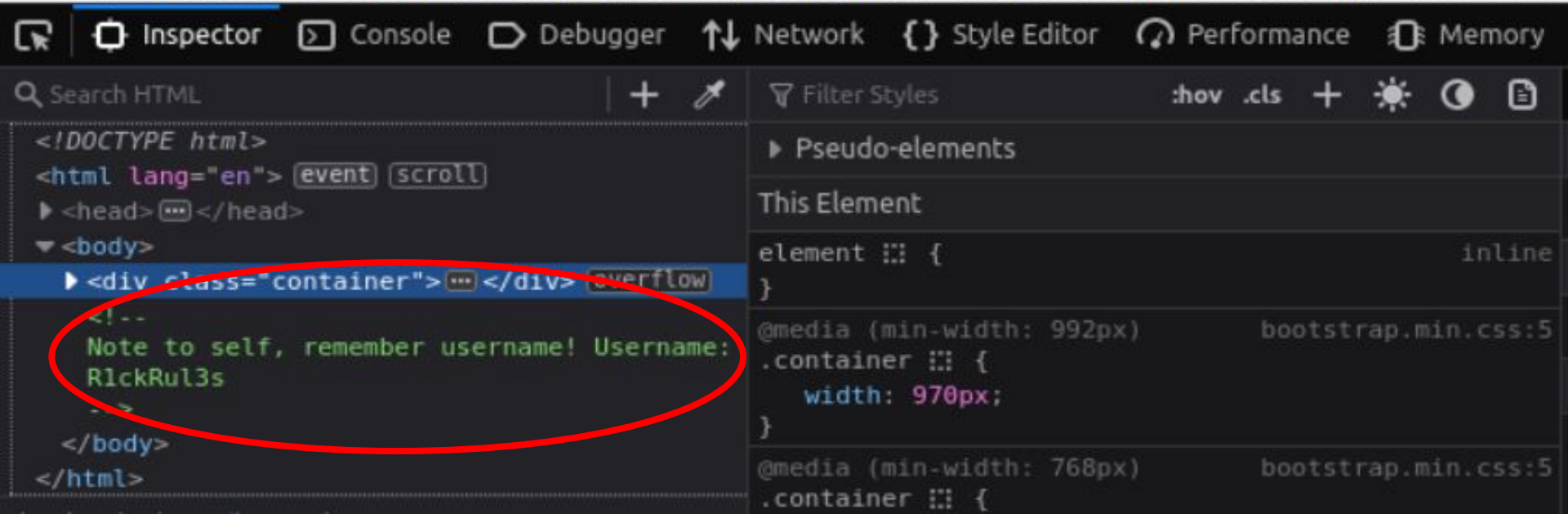
`gobuster dir -u [http://TiP] -w /usr/share/dirb/wordlists/common.txt`

This revealed a `/robots.txt` file

Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to fin



Process

NMAP

`nmap -sV [TiP]`

Found open ports 22 (SSH) and 80 (HTTP)

Web

Visited **`http://[TiP]`**

Inspected the page source and found username `R1ckRul3s`

Gobuster

`gobuster dir -u [http://TiP] -w /usr/share/dirb/wordlists/common.txt`

This revealed a `/robots.txt` file

Process (Continued)

Web

http://[TiP]/robots.txt

Revealed the associated password as `Wubbalubbadubdub`

Nikto

nikto -h [TiP]

Revealed a `/login.php` page

Web

Log into

http://[TiP]/login.php

Gave access to a command panel within the webpage where Linux commands could be run

Rick is sup4r cool — Mozilla Firefox

Rick is sup4r cool

10.10.73.35/login.php

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

Portal Login Page

Username:

Password:

Login

Process (Continued)

Web

http://[TiP]/robots.txt

Revealed the associated password as `Wubbalubbadubdub`

Nikto

nikto -h [TiP]

Revealed a `/login.php` page

Web

Log into

http://[TiP]/login.php

Gave access to a command panel within the webpage where Linux commands could be run

Process (Continued)

CLI

`ls -la`

Revealed hidden files and directories and permission within that php page

Revealed `Sup3rS3cretPickl3Ingred.txt` file

CLI

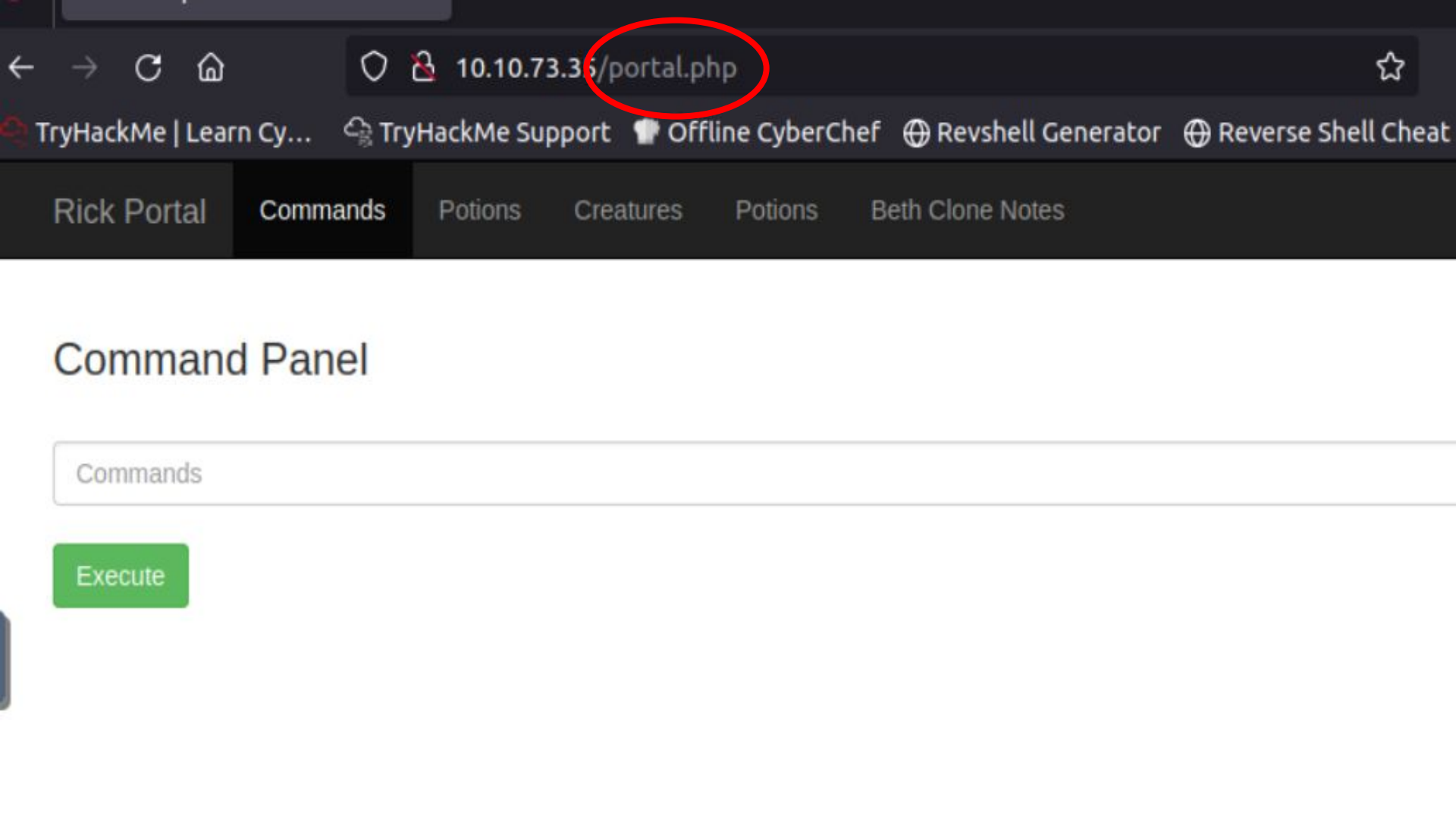
`find /name * ingredient *`

Found the file `/home/rick/'second ingredients'`

CLI

`find /name * 3 *`

Found the file `/root/3rd.txt`


10.10.73.36/portal.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat
Rick Portal
Commands
Potions
Creatures
Potions
Beth Clone Notes
Command Panel
Commands
Execute

Process (Continued)

CLI

`ls -la`

Revealed hidden files and directories and permission within that php page

Revealed `Sup3rS3cretPickl3Ingred.txt` file

CLI

`find /name * ingredient *`

Found the file `/home/rick/'second ingredients'`

CLI

`find /name * 3 *`

Found the file `/root/3rd.txt`

Process (Continued)

`less Sup3rS3cretPickl3 Ingred.txt`

Revealed the flag `mr. meeseek hair` as the first ingredient.

`less /home/rick/'second ingredients'`

Revealed the flag `1 jerry tear` as the second ingredient

`sudo less /root/3rd.txt`

Revealed the flag `fleeb juice` as the third and final ingredient.

Lessons Learned

Challenges

Unsuccessful SSH connection.

After Gobuster was used to find the password, an initial attempt was made to access the server via SSH. This was unsuccessful despite having the correct credentials. This highlighted the importance of thorough enumeration before attempting exploitation, as key information (such as hidden directories or files) may be overlooked if initial efforts fail.

Unexpected Findings

The **password was found in the `/robots.txt` file**. This exposed a potential vulnerability where sensitive information was unintentionally made accessible, underscoring the need for secure web server configurations.

The **`cat` command** in the `/login.php` page CLI was **restricted**. Adopting the use of the `less` command, circumvented this unexpected restriction.

Adaptations

The exercise required deviation from the standard approach when the SSH login attempt was denied. Instead of focusing solely on SSH, the team shifted to further **web-based enumeration** using tools like **Nikto**, which ultimately revealed the `/login.php` page. This adaptability was crucial in overcoming the challenge and successfully completing the task.

Recommendations - Enhance Security Posture

01

Web Server/Password Management Configurations

Restrict access to sensitive files files like Robots.txt.

02

Enumeration and Testing

Incorporate automated tools and manual techniques to institute thorough enumeration.

03

Password Management

Strengthen password policies and implement MFA.

Recommendations - Mitigations

01

Regular Security Audits

Restrict access to sensitive files files like Robots.txt.

02

User Education and Awareness

Educate users so they adhere to strong security practices, such as using unique, complex passwords and avoiding sharing credentials.

03

Principle of Least Privilege

Review user accounts to enforce principle of least privilege to minimize the impact of a breach.

Thank you!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**