SOCAT

BOOT2ROOT CHALLENGES

Introduction

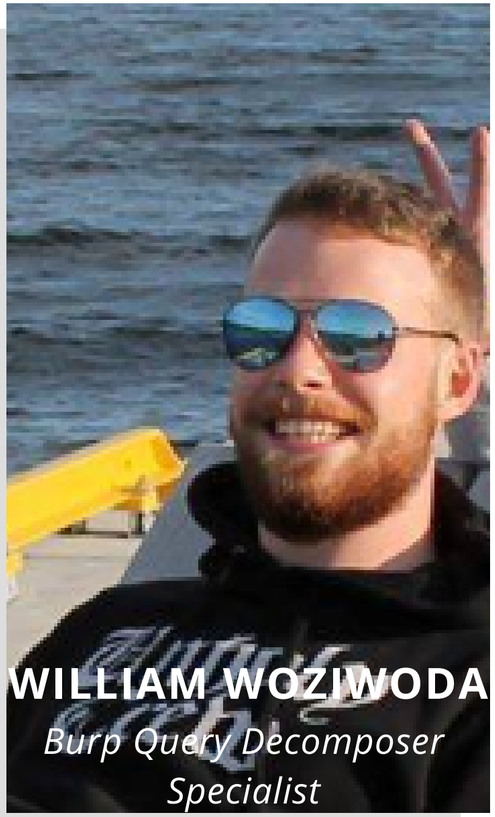
TRYHACKME WALKTHROUGH

Welcome to this comprehensive TryHackMe walkthrough presentation. It showcases our journey through various boot2root challenges hosted on TryHackMe. Our focus is on privilege escalation, exploiting CVEs, discovering internal ports, and SSH tunneling. We aim to enhance our ethical hacking skills and cybersecurity knowledge through these exercises. Join us as we explore the technical depths of these challenges, discuss the tools and methodologies used, and share our experiences and insights. This walkthrough is a collaborative effort by our dedicated team of cybersecurity enthusiasts.

Our Team

LUCAS FIXARI

Lead Researcher and Exploitation Expert



WILLIAM WOZIWODA

Burp Query Decomposer Specialist

PIERRE ROCHETTE

Happiness Manager & Theory Expert Student

THE CROWD

Helping knowledge and useful sounds

WEB ENUMERATION

Technologies Used

Web enumeration and vulnerability scanning are critical first steps

Nmap

A powerful network scanner for detecting open ports, services, and potential vulnerabilities.

- **nmap -sC -sV** *<TARGET IP>*: Runs default scripts and version detection.
- **nmap -A** *<TARGET IP>*: Performs OS detection, version detection, script scanning, and traceroute.
- **nmap -p** *<PORTS>* *<TARGET IP>*: Scans specific ports.

Gobuster

Used for brute-forcing directories on web servers, helping to uncover hidden files and directories

- **gobuster dir --wordlist /usr/share/wordlists/rockyou.txt -u http://***<TARGET IP>*: Brute-forces directories with specified wordlist.
- Additional flags: **-x php,txt,html,sh,cgi,bak** (file extensions), **-q** (quiet mode).

Fuff

Fast web fuzzer that allows directory discovery, virtual host discovery and GET and POST parameter fuzzing

- **ffuf -u http://***<TARGET IP>***/FUZZ -w /usr/share/wordlists/rockyou.txt -o** ***ffufoutput.txt***: Fuzzes directories and saves output to a file.

ACCESS AND ENUMERATION

Technologies Used

Once potential vulnerabilities are identified, gaining access and further enumeration are the next steps

SSH

Secure shell access, which is crucial for remote management of servers

- **ssh** *<USER>@<TARGET IP>*: Connects to target via SSH.
- **ssh -i id_rsa** *<USER>@<TARGET IP>*: Uses a specified private key for SSH connection.

Netcat

Known as the "Swiss army knife" of networking, it allows for reading from and writing to network connections

- **nc -lnvp** *<PORT>*: Listens on a specified port.
- **nc** *<LOCAL MACHINE IP> <PORT>*: Connects to a specified IP and port.

LinPEAS

Local privilege escalation enumeration script to discover misconfigurations and potential paths for privilege escalation

- **Lin**ux **P**rivilege **E**scalation **A**wesome **S**cript

DECODING AND DECRYPTION

Technologies Used

Decoding and decryption are vital for uncovering hidden information and breaking through encoded defenses

Decoder

For various encoding formats like Base64, hexadecimal, and Base32

- Base64: **base64 -d**
- Hexadecimal: **xxd -r -p**
- Base32: **base32 -d**

John the Ripper

A powerful password cracking tool to break encrypted passwords

- **john --wordlist=/usr/share/wordlists/rockyou.txt** *hashes.txt*

Steghide

For extracting data hidden within images
Use **stegseek** if the password is unknown

- **steghide extract -sf** *<image>*.jpg
- **stegseek** *<image>.jpg* /usr/share/wordlists/rockyou.txt

GPG

For handling encrypted files

- **gpg --import** *.hidden-key*
- **gpg -d -o** *<file>*.xlsx *<file>*.xlsx.gpg

ADDITIONAL TOOLS

Technologies Used

In addition to core tools, we employs several specialized tools

Hydra

Used for brute-force attacks on login services

- **hydra -L** ***username*****.txt -P** ***password*****.txt** *<TARGET SERVICE>*
- Additional flags: **-l** (known username), **-p** (known password).

Sqlmap

An automated SQL injection tool that helps in identifying and exploiting SQL injection flaws

- **sqlmap -u** *<URL>* **--dbs**
- **--dbs:** Names of the available databases

Curl

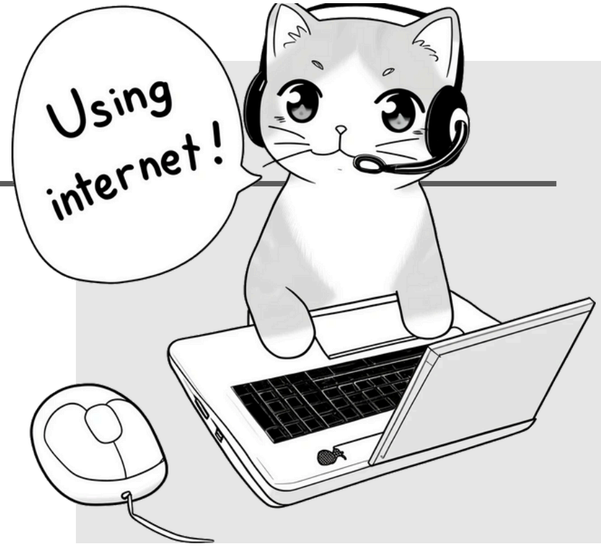
A versatile command-line tool for data transfer, utilized for interacting with web applications via commands

- **curl -X POST -H "***Content-Type: application/json***" -d '{"***key***":"***value***"}' http://***<TARGET IP>***: <PORT>/api/***<username>***

WPScan

Specifically for scanning WordPress sites for vulnerabilities

- **wpscan -e u --url http://***<TARGET IP>***/wordpress -U** ***admin*** **-P /usr/share/wordlists/rockyou.txt**
- Additional flags: **-e u** (users), **-e p** (plugins), **-e t** (themes), **-U** <username> (username for brute-forcing), **-P** ***<path to wordlist>*** (path to a password wordlist for brute-forcing).

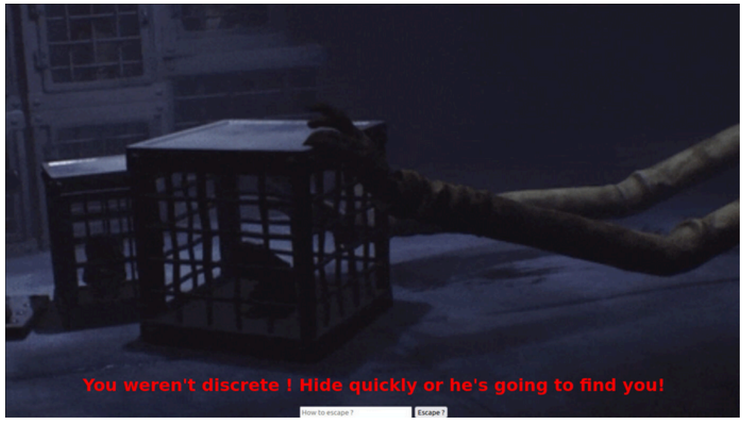


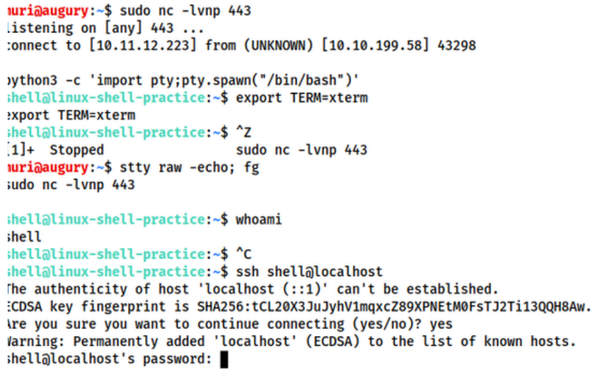
Websites Used

We utilized various online resources to assist with decoding, vulnerability research, and additional cybersecurity tasks.
These resources were instrumental in guiding our walkthroughs, providing critical information, and enhancing our understanding of various cybersecurity concepts and techniques.

- **Hashes.com**: A comprehensive resource for hash decryption.
- **dcode.fr**: An online tool for identifying and decrypting various types of ciphers and codes.
- **Exploit-db.com**: A database of public exploits and proof-of-concept for known vulnerabilities.
- **Crackstation.net**: A powerful online password cracking tool that uses large precomputed hash databases.
- Pentestmonkey.net - **Reverse Shell Cheat Sheet**: A resource for reverse shell commands and techniques.
- **GTFO Bins**: A curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.
- **GPG Documentation**: Official documentation for GPG, a tool for secure communication and data storage.
- WordPress Reverse Shell Documentation - **Hacking Articles**: A guide for creating and deploying reverse shells in WordPress environments.
- Reverse Shell - **Pentester Academy Blog**: An article on exploiting Jenkins Groovy script console to gain a reverse shell.
- **Google Translate**: 한국어를 이해하는 데 도움이 될 수 있는 텍스트 번역을 위한 다용도 도구

Challenges Faced



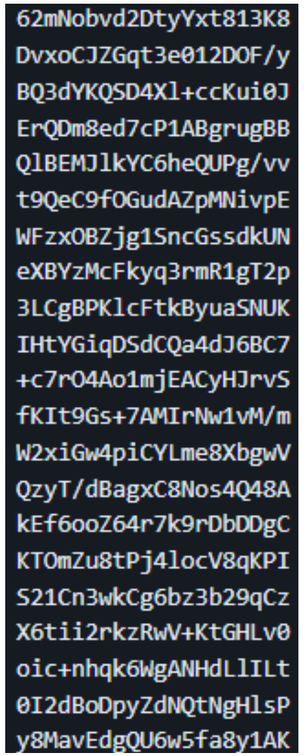


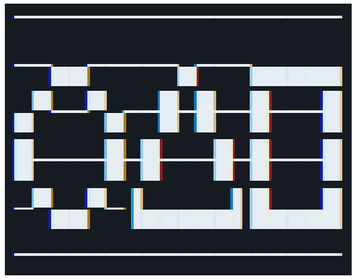
Firewall Bypassing: Many targets had robust firewalls, making initial access difficult. We had to employ advanced techniques to bypass these protections.

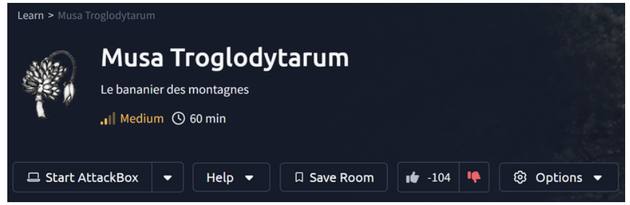
Complex CVE Exploits: Some vulnerabilities required detailed research and precise execution. Understanding and leveraging these CVEs was time-consuming but rewarding.

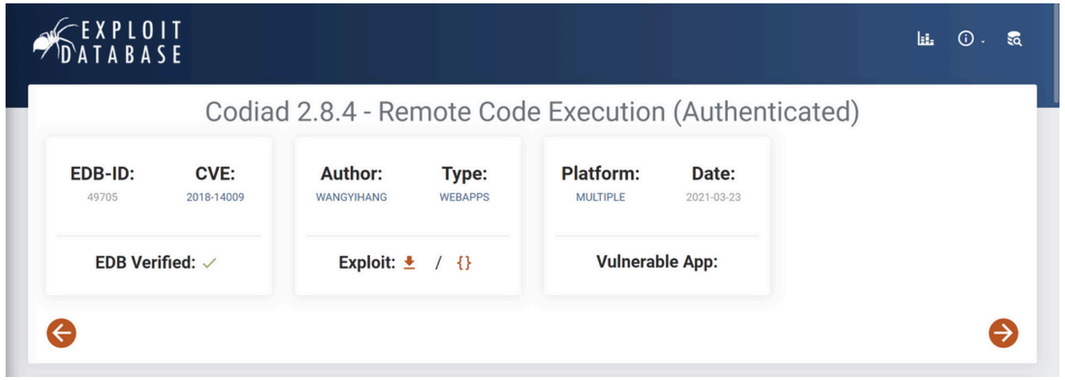
Maintaining stable connections: Maintaining stable connections via SSH tunneling was challenging, especially with network instability.

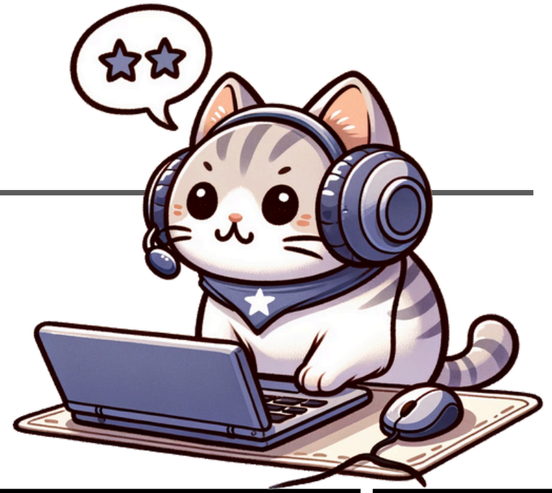
Decoding Complex Data: Encountering heavily encoded or encrypted data posed significant hurdles. It required the use of multiple tools and methods to decode effectively.











Room Ratings

We evaluated each room based on difficulty and learning value, assigning ratings from 0 to 4 stars

ROOM NAME	LUCAS	WILLIAM	PIERRE
TOSS A COIN	★☆☆☆	★★☆☆	★★★☆
YER A WIZARD	★★★☆	★★★☆	☐☐☐☐
MUSA TROGLODYTARUM	☆☆☆☆	★☆☆☆	☐☐☐☐
SECRETS OF THE MAW	★★★★	★★☆☆	☐☐☐☐
THE BINDING OF CYBER	★★★☆	☐☐☐☐	☐☐☐☐

ROOM NAME	LUCAS	WILLIAM	PIERRE
DALGONA	★★☆☆	☐☐☐☐	☐☐☐☐
GRAND LINE	★★★☆	☐☐☐☐	☐☐☐☐
SILENCE	★★☆☆	☐☐☐☐	☐☐☐☐
UN PEPENE	★★★☆	☐☐☐☐	☐☐☐☐
AROUND THE WORLD	★★☆☆	☐☐☐☐	☐☐☐☐
DIABOLICAL BOX	☐☐☐☐	☐☐☐☐	☐☐☐☐
PATIENCE	☐☐☐☐	☐☐☐☐	☐☐☐☐

Most Useful Information

Here are some critical tips and commands that proved invaluable during our TryHackMe walkthroughs

```
python3 -c "import pty; pty.spawn('/bin/bash')"
<USER>@<TARGET MACHINE>:~# ^Z
[1]+  Stopped
root@<LOCAL MACHINE>:~# stty raw -echo
<-- fg & enter
<USER>@<TARGET MACHINE>:~#
```

Stabilizing Terminal

```
ssh -R <PORT>:127.0.0.1:<PORT> root@<LOCAL MACHINE IP>
```

Port Forwarding via SSH

GTFOBins

Room Overview

ALL ROOMS

Path Progress (82%)

Basic - Privilege Escalation

- 💯 Toss a coin: Sing with me this amazing song!
- 💯 Yer a Wizard: Find out about the secret wizarding school!
- 💯 Musa Troglodytarum: Le bananier des montagnes
- 💯 Secrets of the Maw: Uncover the secrets of the maw, and don't get caught!
- 💯 The Binding of Cyber: Try not to lose yourself in this devilish room

Medium - CVE and SSH Tunneling

- 💯 Dalgona: 오징어 게임에 참여하여 456억의 당첨 기회를 잡으세요!
- 💯 Grand Line: I am going to be the pirate king!
- 💯 Silence: What does it take to climb the world's first 9c?
- 💯 Un Pepene: Efectuați un test de penetrare

Advanced - Realistic Boxes

- 🔷 Around The World: Discover the secret track of the famous duo!
- Diabolical Box: Every puzzle has an answer!
- Patience: Cookies are baking, wait for them to cook ... or find another way

Thanks

We want to extend our heartfelt gratitude for your time and attention. This project was a collaborative effort filled with challenges and learning experiences that significantly enhanced our cybersecurity skills. We hope our walkthroughs and insights will be valuable to you in your own journey. Special thanks to TryHackMe for providing such an engaging and educational platform. We also appreciate the support from our peers. Thank you for being part of our journey, and we look forward to continuing to explore the fascinating world of cybersecurity together. ~~(no)~~

Contact

Feel free to explore each room and enhance your skills in cyber security. Happy hacking

https://github.com

https://tryhackme.com